Chapter 1

Introduction

The advancement of Information and Communication Technology is a significant component of society and brings immense attention to digital information protection and data integrity. And nowadays, the concept of sharing secret data conventionally has shifted. Information and Communication Technology allows researchers to construct systems that are used to connect anonymously. Different strategies, such as steganography, cryptography, and watermarking are used for hiding information. These are popular techniques available for information security which is a prime concern while communicating on the internet. Steganography aims at hiding digital information in covert media so that one can conceal the information and prevent the detection of the secret message. The term "Steganography" derives from the Greek word "steganos", meaning "covered or secret", and "graphy" means "writing or drawing". In other words, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in a cover media. One of the earliest examples of steganography involved a Greek fellow named Histiaeus. As a prisoner of a rival king, he needed a way to get a secret message to his army. He made the solution by shaving the head of a willing slave and tattoo his message. When the slave's hair grew back, he sent the slave to the army, who shaved the slave's head again and revealed the message. Generally, certain terms are used to characterize hidden information. In this thesis, "cover image" represents the image intended to conceal the secret information and "stego image" is used for the image that contains the embedded information. The term "key" corresponds to the parameter used to prevent other parties from retrieving the secret information from the stego image. The efforts of statistical analysis needed for breaking steganography algorithms are known as "steganalysis" or "attacks."

Steganographic schemes can be grouped mainly into three specific domains, such as spatial, transform, and compress. These domains have their advantages and disadvantages according to hiding capacity, visual quality, security, storage space, robustness, and execution time. In the spatial domain, valuable information is encoded within the pixel values of cover media. In the transform domain, the cover media is transformed into coefficients and the coefficients are modified for data embedding, whereas the series of compress code is used for image representation in compress domain. Embedding data is done by modifying the compress code. Robustness of transform domain steganography is higher than that of spatial domain steganography.

In many application areas, reconstruction of the cover image along with the extraction of the secret data is very important. The reversibility can be achieved by exploring the techniques of

Difference Expansion, Histogram Shifting, Prediction Error, etc, whereas irreversible schemes use the techniques of Pixel Value Difference, Weighted Matrix, etc. and have higher embedding capacity. Moreover, dual image based reversible steganographic techniques are often being used nowadays. In the embedding phase, dual image based techniques can generate two similar copies of stego images from the cover image to enhance the security and increase the embedding capacity. It is hard for an attacker to reveal the hidden information until he receives both stego images simultaneously.

Steganography is the process of hidden data communication through multimedia documents. It provides secure and private communication which becomes the essential requirement in various human-centric applications. It is useful in covert communication, forensic tracking, tamper detection, authentication, and many other real-life applications. As this procedure is used to suppress the presence of secret data in a stego media, the imperceptibility becomes the most significant factor for every steganographic scheme. The security of the scheme can be increased by reducing the changes made in the stego image during data embedding. One of the main purposes of the recently developed steganographic schemes is to increase the embedding capacity. The performance of a reversible steganographic scheme is evaluated based on three aspects: imperceptibility (measured by PSNR in dB), embedding capacity (measured by bpp), and computational complexity. Every steganographic system always tries to maintain a good trade-off among capacity, quality, and security.

An effective steganographic scheme should possess the following desired characteristics:

Imperceptibility: Imperceptibility is one of the most important factors that every steganographic algorithm should possess. The invisibility of the secret data increases with the increase in the visual quality of the stego image. The visual quality is measured by PSNR (in dB) in which a high value means a lower degree of distortion in the image and vice versa.

Payload: Payload represents the amount of data embedded within the stego image. It is measured by some relative measurement or absolute value. The importance of a steganographic scheme is based on the trade-off between stego image quality and payload. So, a steganographic scheme is considered as acceptable if it improves image quality while keeping the payload at a good level.

Robustness: Robustness of a scheme makes it difficult for an attacker to suspect the presence of a secret data in an image. A steganographic scheme is considered as effective, when it is able to sustain multiple steganographic attacks.

Security: One of the essential factors, which is necessary for the protection of the valuable information in all steganographic schemes, is security. The hidden data cannot be extracted from the host medium, by an unauthorized user, without the knowledge of the required secret key.

Accurate extraction: It is one of the most important challenges to extract the exact secret data which had been embedded. The extraction of the hidden data from the stego medium should be exact and intact.

Use of steganography for secured data communication is increasing day by day. Therefore, maintaining the good quality of the stego image along with reasonable payload and more robustness, is a challenge in this research area. Apart from these, steganography can also be used by illegal organizations for social instability, criminal activity, and endangering public safety. Thus security analysis (steganalysis) plays an important role as a counter process of steganography. Specific steganalysis and universal steganalysis are the two main types of steganalysis. According to Fridrich et al. [1], when the secret message size is very small compared to the cover image size, it is very much difficult to identify the hidden message within a stego image. The secret data can be retrieved by specific steganalysis, nevertheless it is limited to a particular embedding algorithm. In universal steganalysis, the steganographic algorithm is not required to be known. Hence, an algorithm can be designed, which is independent of any steganographic algorithm. The Regular Singular (RS) analysis is developed by Fridrich et al. [2] which can detect the LSB embedded within an image.

Every steganographic scheme published at any point of time gets replaced by a modified system later on. Consequently, new techniques evolve after the removal of defects from their older version. The importance of the research work is to develop a technique to hide the data inside the digital image which can be difficult to detect and only the legitimate receiver can detect it. Hence, a steganographic scheme will be a failure if an adversary suspects the secret information hidden in the cover media. In this thesis, some new steganographic schemes have been designed and implemented concerning the major characteristics of steganographic scheme like imperceptibility and embedding capacity.

1.1 Literature Review

A brief review of some existing steganographic schemes in both spatial and transform domain have been described here. In spatial domain based steganography, the value of the pixel of an image is directly manipulated to embed secret data. In most of the cases, the LSB of the pixel value is changed using some standard techniques. The main advantage of these schemes is the optimized payload with the improved visual quality of the stego image. But, these techniques are vulnerable to steganalysis and are less secure. So, extra measures need to be carried out to make the scheme secure. Moreover, these schemes are prone to any type of image transformations like compression, rotation, scaling, etc. In the following, three different types of protocols like (i) pixel value difference, (ii) weighted matrix based, and (iii) graph-based steganography have been discussed.

Pixel Value Difference (PVD) method of data hiding was suggested by Wu and Tsai [3]. The difference between two adjacent pixel values is calculated for data embedding. The amount of data bits to be embedded depends on the difference value and a reference table. Two adjacent pixels values are modified to embed secret data. This proposed method is vulnerable to steganalysis based on histogram modification [4]. Wang et al. [5] used modulus function along with PVD to increase the security of Wu and Tsai's [3] scheme. Three Pixel Value Difference (TPVD) based technique was proposed by Chang et al. [6]. Their method provides high embedding capacity and reduces distortion in the stego image. Joo et al. [7] developed a new scheme to solve the problems of the scheme designed by Wang et al. [5]. The scheme is robust against PVD histogram based attack and RS analysis. A new PVD based method was proposed by Luo et al. [8] where the embedding region is selected according to the secret data length and the consecutive pixel value difference.

Hong [9] proposed a new PVD based method which uses a patched reference table. The scheme generates better quality stego image with high embedding capacity. After that, a modified PVD based steganographic method was proposed by Hong and Chen [10]. In this scheme, reference coordinates are generated from the pixel pairs.

Chen [11] proposed the PVD based method to embed the unequal amount of secret information using pixel complexity. In this approach, secret information was embedded in an embedding cell of size (2×2), which was composed of randomized embedding units to reduce the falling of boundary program and eliminate sequential embedding. Each embedding cell has two embedding units; Pivot Embedding Unit (PEU) and Non-Pivot Embedding Unit (NPEU). The difference value of the pair pixel in PEU is calculated to determine the complexity of the pair and to determine the amounts of secret bits to be embedded. More bits will be embedded in the complex area and less in the smooth area. This scheme achieves 47.3 dB PSNR when 54,384 bytes secret data are embedded. Jana et al. [12] designed a dual image based data hiding scheme using pixel value difference expansion. Among n bit secret data, $n-1$ bits are embedded using Pixel Value Difference (PVD) whereas 1 bit is embedded using Difference Expansion (DE). This scheme achieves 38.95 dB PSNR with payload 1.25 bpp. Swain [13] proposed a new PVD based steganographic scheme with modulus function (MFPVD). Here, non-overlapped pixel blocks are used to exploit the edges in five directions. Five difference values with five neighboring pixels are calculated considering a pixel as a central pixel. The data hiding capacity in all the five directions is decided based on the average of these five different values. Li et al. [14] developed a steganographic technique that combines PVD, modulus function, and particle swarm optimization. PVD and the modulus function are used here to embed and extract secret data. To improve the quality of the stego image, particle swarm optimization is used to select the ideal pixel gray values among numerous modulus function solutions.

Ron Crandall [15] introduced matrix encoding as a new steganographic scheme to improve data hiding capacity as well as visual quality. In 2001, A. Westfeld [16] first implemented matrix encoding, which decreases the number of changes during data embedding within steganogram. A new steganographic scheme for embedding a piece of valuable secret information with a binary image using a shared secret key and weighted matrix has been suggested by Tseng et al. [17]. Data hiding in 2-color images has been suggested by Tseng and Pan [18] which ensures that modified bit in the host image must be adjacent to the bit that has some value as the former's new value. As a result, the existence of secret information within the steganogram is difficult to detect or guess. To improve the hiding capacity, Tseng et al. [17] developed data hiding scheme for facsimile images, which can hide $\lfloor log(2^{mn}+1)\rfloor$ bits by changing at most two bits in the host images, when $2mn$ image block size has been considered. Their scheme is secured due to fewer pixel value alteration and undetectability of hidden data existence. Using the block or partition, Tseng et al.'s scheme [17] can conceal 4 bits of secret data in a block by changing at most two pixels. In order to make innocent communication, the secret message is normally encoded within the redundant part of the cover media. The matrix encoding is much different encoding scheme which may increase embedding capacity as well as improve security by reducing the number of necessary changes. Fan et al. [19] suggested a new data hiding scheme for quantized DCT co-efficient of JPEG image, which is sustainable to visual and statistical attack. The new matrix encoding algorithm improves the performance by exploiting the n-layer extension and modifying the form of the original hash function. Lin and Chang [20] proposed two novel compact covering schemes, compress and conceal the repeated bit-blocks of valuable secret information bits into cover images within a single phase, but very sensitive to noise. Mao [21] proposed a fast algorithm for matrix embedding steganography using hamming code and random linear code that uses syndrome to indicate coset leader and it searched for the coset leader by its syndrome for the rest. It has same embedding rate and efficiency as conventional matrix embedding algorithm, but its computational cost is low.

Lucak at. al. [22] proposed color filter array (CFA) zooming before image interpolation to reduce the computational complexity with high-quality output, which is highly essential for hardware implementation. Jung and Yoo [23] suggested a new image interpolation and data hiding approach. This interpolation scheme has low complexity with high-speed calculation through scaling-up neighbour mean interpolation, where secret data can be extracted from stego image without taking help from any extra information. Lee and Huang [24] proposed a high capacity data hiding scheme by employing an image interpolation by neighbouring pixel (INP) on maximum difference value to improve the efficiency proposed by Jung and Yoo [23]. Their scheme achieves high capacity with low cost maintaining a good quality image. Chang et al. [25] developed two-stage image interpolation based data hiding scheme with high capacity and good visual quality through histogram shifting approach. In the first stage, they generate high-quality cover image using enhanced neighbour mean interpolation (ENMI) and embed data by taking the difference from the input and cover pixels. At the second stage, a histogram modification scheme is employed on the difference image to improve capacity and preserve image quality without any distortion.

Gholampour and Khosravi [26] constructed an evaluation framework for the steganographic scheme in terms of relative change waste (RCW) and expected change per pixel (ECP) for various length messages. They encountered the steganographic problem of designing low waste and high efficient method and solved through some theorems, which led us to design waste aware interpolation and convex hull point selection technique. Tang et al. [27] proposed high capacity steganographic scheme through multi-layer embedding (CRS), which helps the user's current demand for total recovery and image reversibility after extracting secret information. This scheme improves Lee and Huang [24] approach maintaining low computational complexity and higher embedding capacity. An adjustable two-stage data hiding method on LSB through histogram shifting was suggested by Tsai et al. [28]. Jana [29] developed RDH scheme through a modified weighted matrix where average hiding capacity is 2.97 bpp with the visual quality of stego image is more than 37.97 dB PSNR.

There are several schemes which use graph theory concept in steganography. Tu et al. [30] proposed a data hiding scheme for polygonal meshes by applying maximum expected level tree based on a message probability. A new data hiding technique which is based on the context of tree and graph databases, developed by Abul et al. [31]. Thiyagarajan et al. [32] designed a reversible steganographic technique using graph coloring approach. This scheme conceals the patient information inside the medical image using a dynamic key which is generated by 3-coloring problem in graph. Dogan [33] proposed a reversible data hiding scheme that uses pixel block as a graph and its pixels as vertices. The degree of neighbourhood of vertices are calculated and the vertices having a value more than the threshold value are selected for embedding data.

Very few researchers have developed steganographic schemes using the concept of graph theory. Designing a new steganographic scheme using graph concept is still an important area in the recent era. In this thesis, some new schemes based on graph neighbour concept have been developed.

Due to the development of social media communications, people send compressed images using transform domain. In transform domain based steganographic schemes, the secret data is embedded by manipulating the orthogonal transform of the image rather than the image itself. Transform domain techniques are suited for processing the image according to their frequency content. The main idea behind the transform domain methods consists of computing a 2-D discrete unitary transform of the image, manipulating the transform coefficients by an operator and then performing the inverse transform. The orthogonal transform of any image has typically two components: magnitude and phase. The restoration of the image to the spatial domain is done by using the phase component. The frequency content of the image is contained in the magnitude component. The transform domain is more secured than the spatial domain. Transform domain steganography can be used in many compressed formats like JPEG and JPEG2000. Moreover, these schemes are comparatively less prone to any type of slight image transformations like compression, rotation, scaling etc.

Transform domain steganographic technique is performed by converting the cover image and modifying the coefficient values. The primary methods of transform domain steganography are used by modifying the coefficients in DFT (Discrete Fourier Transform) [34], DWT (Discrete Wavelet Transform) [35–37] and DCT (Discrete Cosine Transforms) [38, 39]. In 1997, Upham [40] introduced a steganography tool (JSteg) to embed secret data in LSB of the quantized DCT coefficients. Then, Westfield [16] proposed F5 algorithm to increase the data hiding capacity through matrix encoding. In the same year, Fridrich et al. [41] introduced an invertible watermarking scheme for digital image authentication in the transformed domain. Chang et al. [42] presented an RDH scheme based on mid-frequency quantized DCT coefficient to embed secret data in the cover image. Iwata et al. [43] and Chang et al. [44] presented a data hiding scheme that modifies quantized DCT coefficients of each block to hide secret data. After that, Xuan et al. [45] developed a data hiding scheme that shifts the quantized DCT coefficient histogram to embed data based on histogram pairs. Sakai et al. [46] modified Xuan et al.'s [45] scheme to get a better quality stego image by deciding whether a pixel block is suitable for data embedding or not. Later, Cheng et al. [47] proposed a multi-level embedding to reach higher capacity. In 2010, Zhang et al. [48] developed a reversible data hiding scheme using a JPEG image for authentication through the watermarking scheme. Wang et al. [49] suggested a data hiding scheme using quantized DCT coefficients. They divided some elements of the quantization table by an integer and multiplied the corresponding quantized DCT coefficient with the same integer value and added some adjustment to embed secret data. The statistical model of quantized DCT coefficients for the steganalysis of JSteg algorithm has been proposed by Thai et al. [50]. Recently, Singh et al. [51] suggested a watermarking scheme in which a cover image is divided into (2×2) non-overlapping blocks, and from each block, 12 bits watermark are generated from the 5 MSBs of each pixel and embedded into the three LSB of the pixels corresponding to the mapped block. At the same time, Saidi et al. [52] presented an adaptive image steganography using DCT in which they scanned the AC components from LSB to MSB and used the chaotic map to embed secret data. Tavoli et al. [53] proposed weighted PCA for improving Document Image Retrieval System based on keyword spotting. Poljisak et al. [54] designed a steganographic technique for real-time data hiding. Their method is based on modifying DCT coefficients to hide data, and the validity of the method in real-time applications has been proved. Zhang et al. [55] implemented a unique and novel coverless image steganography algorithm based on DCT and Latent Dirichlet Allocation (LDA) topic classification. In this technique, they managed to pass secret information without modifying the original images. Liao et al. [56] developed a new steganographic technique for medical JPEG images based on the dependencies of inter-block DCT coefficients. The differences among DCT coefficients at the same position in adjacent DCT blocks are preserved as much as possible. During embedding, the cost values are allocated dynamically according to the modifications of inter-block neighbors.

Steganography in the transform domain is still an important research issue. The DCT based compression is predominantly used in JPEG images. Here, a new steganographic scheme has been designed for highly compressed JPEG images with good visual quality, and it can resist intentional and unintentional attacks.

In recent years, a variety of investigations have been carried out in the field of transform domain steganography. Abdelwahab et al. [57] proposed a new DWT based data hiding scheme that uses two secret keys to hide data in DWT coefficients. Kumar et al. [58] observed the effect of embedding secret data into different bands of DWT on a stego image in terms of PSNR. An Integer Wavelet Transform (IWT) based image steganographic scheme has been suggested by Acharya et al. [59] which hides multiple secret images and keys in a color cover image. Another DWT based data hiding technique, developed by Baby et al. [60], hides multiple color images into a single color image. Atawneh et al. [61] presented a steganographic scheme that uses diamond encoding (DE) to minimize the distortion that is generally introduced in an image in DWT based steganography. A new steganographic scheme has been advised by Kumar et al. [62] using secret key computation and blocking concept. The scheme, suggested by Lin et al. [63], modified the low-frequency coefficients in the DCT domain for embedding secret data. Another scheme which calculates the difference between two DCT coefficients of the adjacent blocks at the same position to embed secret data has been developed by Parah et al. [64]. The scheme, declared by Chung et al. [65], embeds secret data into U and V components of SVD. Fan et al.'s [66] scheme embeds secret data by changing the relation between the second and the third coefficients in the first column of the U component of SVD. Another SVD-based scheme, proposed by Lai [67], modifies the entries in selected blocks of U component of SVD to embed secret message. A similar scheme was developed by Su et al. [68] that embeds secret data by modifying selected elements of U component. Some steganographic schemes have been presented using DCT or DWT in combination with SVD. Ling et al. [69] suggested a watermarking scheme using DCT in combination with SVD. A hybrid image watermarking technique based on DWT, DCT, and SVD against signal processing attacks has been offered by Singh et al. [70]. The scheme, advised by Zheng et al. [71], combines DWT and SVD where the singular values of U components of SVD are modified to embed secret message. A novel watermarking algorithm has been presented by Ali et al. [72] in which DCT is used in combination with SVD. The advantage of the algorithm is that it automatically chooses the appropriate multiple scaling factors. Agoyi et al. [73] developed a novel watermarking scheme based on DWT, chirp z-transform (CZT), and SVD. A novel scheme to implement blind image watermarking based on the feature parameters extracted from a composite domain including DWT, SVD, and DCT designed by Hu et al. [74]. DWT and SVD are employed in a robust and secure watermarking scheme by Ansari et al. [75]. Makbol et al. [76] used DWT-SVD image transform and human visual system to improve the performance of watermarking scheme where watermark was embedded by modifying several elements in its U matrix. Singh et al. [77] presented a secure multiple watermarking methods based on DWT, DCT, and SVD, where the watermark was embedded in the singular values of DWT sub-bands. A DCT-SVD based digital image watermarking scheme has been proposed by Elayan and Ahmad [78] that made use of Arnold transform with a view to improving the robustness against different types of attacks while preserving the perceptual quality. A similar type of scheme has been developed by Singh [79] which provides a robust hybrid multiple watermarking technique using the fusion of DWT, DCT, and SVD. The scheme provides an extra level of security with the acceptable performance in terms of robustness and imperceptibility. Singh et al. [51] suggested a robust and blind watermarking scheme based on DWT-SVD and DCT with Arnold cat map encryption for copyright protection. Yahya [80] developed a new region-based steganography method, CR-BIS, which hides data in the robust regions of the image. They managed to increase the robustness of the scheme by using higher-level DWT to hide data. Weng [81] proposed an innovative information hiding scheme for Multimedia IoT (MIoT) applications. The scheme uses prediction-error-expansion

(PEE) based on prediction-generating-method (PGM) on DWT domain. The PGM is used to generate the predicted image. The message is then concealed into a predicted error between the original image and the predicted image. The higher performance is achieved when more and more prediction errors are closed.

Nowadays, researchers are also trying to use two or more transformation techniques to develop new steganographic schemes. Using multiple domain image steganography or watermarking by combining two or more transforms provides more robustness and imperceptibility. The combinations, those are generally used nowadays, are DWT+DCT, DCT+SVD, DWT+SVD, DWT+DCT+SVD, and so on.

In this investigation, a steganographic scheme has been proposed with DWT in combination with DCT which provides high embedding capacity with good visual quality. The developed scheme provides higher robustness compared to other existing schemes.

1.2 Problem Domain

Steganography is the art of secured concealed communication which carries private message via some multimedia object so that the representation of private message will not draw any attention from the eavesdroppers while they are being moved through an open public channel. There is a high risk of disclosing while they are being transferred through the unsecured public channel. Therefore, achieving secure communication is one of the important objectives of current research.

A new efficient steganographic scheme for grayscale cover image has been proposed by Wu and Tsai [3]. In their technique, the secret data has been embedded by calculating the difference between two pixels of any block called pixel value difference (PVD). This method provides an easy way to embed a large amount of data with a better imperceptible result than simple LSB replacement policy which accomplishes secrecy of valuable information. An improved embedding scheme for variable-length secret data through the correlation between neighbouring pixels has been suggested by Chang and Tseng [82]. They have proposed two-sided, three-sided, and four-sided side match technique for large data embedding capacity without making notable distortion. The advantage of this scheme is that no reference table is required when one extracts the secret data from the stego image and the edge area of the cover image may contain more data than the non-edge area. The combination of both LSB and PVD method has been used in a scheme to conceal the secret data within the cover image and it is developed by Wu et al [83]. In this approach, in the smooth area, secret data is embedded using LSB and in the edge area PVD method has been implied, which improves security level than that of a single PVD method. A high capacity PVD based data hiding approach with modulo function has been suggested by Wang et al. [5] where remainder of two consecutive pixels is modified to embed secret data which gains more flexible and optimal remainder of two pixels at the least distortion. This approach significantly decreases the hiding effect of Wu and Tsai scheme [3]. Wang et al.'s [5] scheme has abnormal increases and fluctuations in PVD histogram, which may reveal the existence of secret data. Joo et al. [7] prevent the abnormality by using turnover policy and a novel adjusting process which devises to remove fluctuations in PVD histogram. To upgrade the hiding capacity compared to PVD, three different directional tri-way pixel value differencing (TPVD) method has been formulated by Chang et al. [6] which gives secrecy protection from different statistical steganographic attacks. Lee et al. [84] proposed a residual value coding approach to compensate for the reduction in quality of the secret image which prevents illegal extraction. An adaptive pixel value differencing technique for data embedding has been developed by Swaim [85] and it inspects vertical and horizontal edge but embeds in the target pixel. The adaptability range has been measured by calculating local statistics of the embedded block.

Steganographic schemes using weighted matrix have been designed by a few researchers. The very first data hiding scheme using weighted matrix was designed by Tseng et al. [17]. They hide 2-bit secret data in a (3×3) pixel block of a binary image. Tseng et al.'s [17] scheme was later improved by Fan et al.'s [86] scheme which is able to hide 4-bit secret data within a (3×3) pixel block. The data hiding capacity of a cover image can be increased by image interpolation, and it was proved by Jung and Yoo's [23] scheme. Data hiding scheme with multi-layer embedding using image interpolation was first suggested by Lee and Huang [24]. The payload of this multi-layer embedding scheme was then improved by Tang et al. [27]. A single weighted matrix has been used for data embedding in the schemes discussed here including Tseng et al. [17] and Fan et al. [86] scheme. There is an opportunity to enhance the security through modification of weighted matrix for every new block using a shared secret key.

Tu et al. [30] proposed a data hiding scheme for polygonal meshes by applying maximum expected level tree based on a message probability. A data hiding technique proposed by Abul et al. [31] is based on the context of tree and graph databases. Thiyagarajan et al. [32] presented a reversible data hiding technique using graph coloring approach. But their embedding capacity is very less. Dogan [33] suggested a reversible data hiding scheme that uses pixel block as a graph and its pixels as vertices. But these schemes have used fixed size pixel block every time. So there is a chance to increase security with good visual quality and embedding capacity with varying pixel block size.

Chang et al. [87, 101] developed some dual image based data hiding scheme. Though the schemes are reversible, their embedding capacity, which is near 1 bpp, is very low compared to today's demand. The dual image based scheme designed by Lee et al. [88] also has very low embedding capacity. So there is a scope to improve the embedding capacity in dual image based steganographic schemes. Moreover, the reversibility in PVD based scheme has been achieved in very few schemes. Designing a dual image based steganographic scheme with good quality and at low cost is a challenge.

Researchers have developed some steganographic schemes in transform domain using DCT, DWT, etc. Saidi et al. [52] presented an adaptive image steganographic method using DCT in which they scanned the AC components from LSB to MSB and used the chaotic map to embed secret data. Both the schemes are not suitable for highly compress JPEG images as they change almost all the DCT coefficients to embed data. In the scheme, suggested by Singh et al. [51], a cover image is divided into (2×2) non-overlapping blocks and from each block 12 bits watermark are generated from the 5 MSBs of each pixel and embedded into the three LSB of the pixels corresponding to the mapped block. Abdelwahab et al. [57] implemented a new DWT based data hiding scheme that uses two secret keys to hide data in DWT coefficients. Kumar et al. [58] observed the effect of embedding secret data into different bands of DWT on a stego image in terms of PSNR. Atawneh et al. [61] developed a steganography scheme that uses diamond encoding (DE) to minimise the distortion that is generally introduced in an image in DWT based steganography. Most of these schemes modify almost all the coefficients to embed secret data, which reduces the imperceptibility of the stego image. So there is a scope to increase the imperceptibility of the stego image by changing the least number of coefficients to embed data in a compressed image in a DCT or DWT domain.

Many steganographic schemes have been developed in different domains exploiting various tools and techniques. Whereas, either embedding capacity or visual quality or both are limited in most of the schemes. So, there is a scope to improve the performance of the steganographic scheme in terms of embedding capacity and visual quality. Here, some steganographic schemes have been designed in the spatial domain and in the transform domain. As steganographic scheme in spatial domain are mainly designed in such a way that researchers can easily increase the embedding capacity. But they have to compromise with the imperceptibility of the stego image. Therefore, the major concern for any steganographic scheme should be imperceptibility instead of embedding capacity or it would be much better if the scheme can maintain a good trade-off between imperceptibility and embedding capacity. Hence we focus to design the steganographic scheme in transform domain to solve this purpose. The major disadvantage of the techniques used in spatial domain is that they are not suitable for images with lossy compression like JPEG images. For this purpose the separate schemes have been developed for the lossy images in transform domain with the intend to increase the embedding capacity without much compromising with the visual quality of the stego image. Finally, the pros and cons of these schemes have also been compared to established the superiority of the schemes.

1.3 Motivations and Objectives of the Thesis

The main objective of this thesis is to design some new secured and of high capacity steganographic schemes in both spatial and transform domain. The steganographic schemes in spatial domain have high embedding capacity and high visual quality but have low robustness. In contrast, transform domain schemes have good visual quality and security but low embedding capacity. Here, some steganographic schemes have been studied in different domains, and the findings are analysed in detail. The key issues of the steganographic schemes are embedding capacity, visual quality, reversibility, security, and robustness.

i) The steganographic schemes through PVD, Graph neighbour, weighted matrix, DCT, and DWT, have a limited embedding capacity. Therefore, the motivation is to increase the data hiding capacity using the said techniques.

ii) The steganographic techniques developed so far using dual image and image interpolation have limited payload and average visual quality. So, the motivation is to design some steganographic schemes with dual image using image interpolation in such a way that its embedding capacity and visual quality can be improved.

iii) Many schemes have been developed in steganography which uses no secret key for security. But, it is clear that these schemes are less secure and it inspires us to design some new steganographic schemes using which messages can be passed through cover media in a very secure way using shared secret keys.

iv) There is a limitation of data hiding capacity in the weighted matrix based steganographic schemes developed so far. Moreover, the existing schemes are not reversible. But, reversibility is an essential requirement in many application areas. So, our motivation is to design some steganographic schemes which can overcome this limitation.

v) Finally, the motivation is to design and analyze some new steganographic schemes through transform domain using DCT and DWT.

The objectives of this thesis have been described elaborately as follows:

i) **Designing some high payload steganography schemes:**

In the literature, there are some techniques using PVD, weighted matrix, graph neighbour, which have certain data hiding capacity. The objective of this thesis is to design some techniques to increase the payload using PVD, weighted matrix, and graph neighbour, which are discussed in Chapters 3 and 4.

ii) **Use of shared secret key in steganography schemes:**

It is seen from the literature survey that the security loop-hole still exists when any message is sent over public network. So, the goal is to make some schemes more secured and robust by using a shared secret key. For this purpose in Chapters 3 and 4, some schemes have been developed using PVD, graph neighbours, and weighted matrix incorporating shared secret keys.

iii) **Reversibility in steganography:**

Till now, very few schemes have been developed using PVD or weighted matrix to achieve reversibility. So, the target is to design some algorithms which achieve reversibility using weighted matrix and PVD. These schemes are explained in Chapters 3 and 4.

iv) **Conservation of perceptibility**

One of the most important requirements in any steganographic scheme is imperceptibility. So, the first and foremost goal is to preserve the imperceptibility in all of the proposed schemes.

v) **Designing some robust steganography schemes in transform domain:**

To study the data hiding capacity, quality, robustness in transform domain, some new steganographic schemes have been implemented using DCT and DWT, which are explained in Chapter 5.

1.4 Contributions

In this thesis, some new steganographic techniques have been designed using Pixel Value Difference (PVD), Graph Neighbourhood, Weighted Matrix (WM), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT). Moreover, the proposed schemes have been analyzed against various evaluation metrics to show the security and robustness of these schemes against these types of attacks. The main contributions of the current work can be summarized as follows:

- Pixel value difference (PVD) based schemes are not reversible. We have achieved reversibility using interpolated pixels and improved the embedding capacity of the proposed scheme.

- Graph neighbourhood based steganographic protocol has been developed to achieve high imperceptibility of the stego image.

- Shared secret key has been used in the developed schemes. The secret message bits are distributed between dual stego images depending on the shared secret key.

- A weighted matrix acts as a second key along with the shared secret key.

- A novel steganographic scheme has been designed for highly compressed JPEG color image.

- The DCT coefficients are very sensitive to a small change, and the quality of the image degrades significantly. An effort has been made to develop a new scheme which modifies the least number of coefficients using a weighted matrix to preserve the quality of the image.

- A shared secret key generated by SHA-512 hashing algorithm and an updated weighted matrix help to improve the security of the steganography scheme.

- To increase the robustness and security of the schemes, Discrete Wavelet Transform (DWT) is used in combination with Discrete Cosine Transform (DCT).

- The positional value of the weighted matrix is embedded instead of the original secret message. This technique provides another level of security and robustness to the proposed schemes.

1.5 Evaluation Metric

In this thesis, some new secured steganographic schemes have been designed in both spatial and transform domain. Developing a new scheme is not enough, but its security and robustness analysis are of paramount importance. In this section, we have discussed some evaluation metrics to measure the performance of our developed schemes.

Mean Square Error (MSE):

The Mean Square Error (MSE) between the cover image (C) and the stego image (SI) is calculated using equation (1.1).

$$MSE = \frac{\sum_{i=1}^{X}\sum_{j=1}^{Y}[C(i,j) - SI(i,j)]^2}{(X \times Y)}, \tag{1.1}$$

where X and Y are the number of pixels along the width and height of the images, respectively.

Peak Signal to Noise Ratio (PSNR):

The Peak Signal to Noise Ratio (PSNR) between the cover and the stego image is calculated using equation (1.2).

$$PSNR = 10\ log_{10}\frac{255^2}{MSE} \quad ,(dB) \tag{1.2}$$

Higher PSNR (in dB) indicates better similarity of the stego image with the cover image.

Data Hiding Capacity (Payload):

The number of bits embedded within the stego image is measured by payload (bpp), and it is calculated using equation (1.3).

$$Payload = \frac{\text{No of bits embedded}}{\text{Number of pixels of the original image}}(bpp) \tag{1.3}$$

Structural Similarity Index Measurement (SSIM):

Structural Similarity Index Measurement [89] (SSIM) is a parameter that measures the similarity between the original and the stego image. The value of SSIM lies between -1 and +1. The

SSIM value approaches to +1 when the images are identical. The SSIM value of the cover and stego image is calculated using equation (1.4).

$$\text{SSIM}(m,n) = \frac{(2\mu_m\mu_n + c_1)(2\sigma_{mn} + c_2)}{(\mu_m^2 + \mu_n^2 + c_1)(\sigma_m^2 + \sigma_n^2 + c_2)} \quad , \tag{1.4}$$

where, μ_m is the average of m, μ_n is the average of n where $m \times n$ is the size of the image.
${\sigma^2}_m$ is the variance of m, ${\sigma^2}_n$ is the variance of n;
σ_{mn} is the covariance of m and n
$c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$, two variables to stabilize the division with weak denominator.
L is the dynamic range of the pixel-values. $k1 = 0.01$ and $k2 = 0.03$ by default.

Regular-Singular Analysis (RS Analysis):

The stego images are analysed in the schemes using RS analysis proposed by J. Fridrich [41]. Consider a cover image of size (M × N). In RS analysis method, first the stego image is divided into disjoint groups G of n adjacent pixels $(x_1, \ldots, x_n)$. Each pixel value is in a set S that is $S = \{0, 1, \ldots, 255\}$. Here, 4 consecutive pixels in a row form a group. A function f, called a discrimination function, is defined. The function returns a real number $f(x_1, \ldots, x_n) \in R$ to each pixel group $G = (x_1, \ldots, x_n)$. The "smoothness" or "regularity" of each group of pixels G is identified by this discrimination function. The function f is defined as:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

An invertible function F, called flipping, is defined and it operates on S. It permutes the pixel values using two-cycles. So, for all x belongs to S, either F^2= Identity or $F(F(x)) = x$. The permutation function F_1 is: $0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$, which flips the LSB of each pixel value. Another function F_{-1} is defined and it is known as shift LSB flipping. The permutation function F_{-1} is: $-1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256$. So, the flipping function F_{-1} can be defined as:

$$F_{-1}(x) = F_1(x+1) - 1 \quad ,$$

for all x belong to S. Regular (R), Singular (S) and Unusable (U) are the three types of group here. The groups are defined depending on the discrimination function f and the flipping operation F. The three groups are defined below depending on the conditions:

$$\begin{cases} G \in R & \text{if } f(F(G)) > f(G) \\ G \in S & \text{if } f(F(G)) < f(G) \\ G \in U & \text{if } f(F(G)) = f(G), \end{cases}$$

where $F(G) = F(x_1), \ldots, F(x_n)$.

A mask value M is used to execute the flipping operation. Here, M is a n-tuple with values -1, 0, and +1. The flipped group $F_M(G)$ is defined as $(F_M(1)(x1), F_M(2)(x2), \ldots, F_M(n)(xn))$. Then, the RS analysis value is calculated through equation (1.5).

$$(|R_M - R_{-M}| + |S_M - S_{-M}|)/(R_M + S_M), \tag{1.5}$$

where R_M and S_M are the number of regular and singular groups with mask M respectively and R_{-M} and S_{-M} are the number of regular and singular groups with mask $-M$ respectively. The scheme is said to be secured if the value of the RS analysis tends to zero.

Relative Entropy:

The relative entropy measures how one probability distribution is different from another. Here, the relative entropy (R) between the cover image (C) and the stego image (SI) is calculated by the equation (1.6).

$$R(SI||C) = \sum SI(x) log \frac{SI(x)}{C(x)} \tag{1.6}$$

When the relative entropy becomes zero, the two distributions become identical and the system is said to be perfectly secured against various attacks. R is a non-negative continuous function and it becomes zero if and only if C and SI coincide. Depending upon the number of secret bits, the relative entropy of the probability distribution of C and SI varies.

Correlation Coefficient (CC):

The similarity and dissimilarity between two digital images are represented by the Correlation Coefficient (CC). The equation (1.7) shows the CC values between the two images. The CC can take a range of values from -1 to +1. A CC value of 0 indicates that there is no association between the two images. A value further from 0 indicates more de-association; that is, the images are not same.

$$CC = \frac{\sum\limits_{m=1}^{M}\sum\limits_{n=1}^{M}(C-\overline{C})(SI-\overline{SI})}{\sqrt{(\sum\limits_{m=1}^{M}\sum\limits_{n=1}^{M}(C-\overline{C})^2)(\sum\limits_{m=1}^{M}\sum\limits_{n=1}^{M}(SI-\overline{SI})^2}} \tag{1.7}$$

Standard Deviation (SD):

From a statistical viewpoint, the standard deviation (SD) of a dataset is actually a measure of the magnitude of deviations between the values of the observations contained in the dataset. From an image processing perspective, the SD can help to know how a stego image is deviated from the original image after embedding secret message. It is calculated using equation (1.8).

$$SD = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C-\overline{C})^2}{(M-1)(N-1)}} \quad , \tag{1.8}$$

where C is the cover image of size $(M \times N)$ and $\overline{C}$ is the mean of the pixels.

Normalize Correlation Coefficient (NCC):

The robustness of a scheme is measured by the Normalized Correlation Coefficient (NCC). It calculates the difference between the original and stego image. It is defined using equation (1.9).

$$NCC = \frac{\sum\limits_{i=1}^{R}\sum\limits_{j=1}^{C} x(i,j)y(i,j)}{\sum\limits_{i=1}^{R}\sum\limits_{j=1}^{C} |x(i,j)|^2} \quad , \tag{1.9}$$

where R and C are the number of rows and columns in the images, respectively. $x(i,j)$ and $y(i,j)$ are the original image and the stego image, respectively.

Universal Quality Index (Q-Index):

The Universal Quality Index (Q-Index) is used to measure the distortion in an image. It has 3 factors: 1) Luminance distortion, 2) Contrast distortion, and 3) Loss of correlation. It is measured by the following formula:

$$Q = \frac{\sigma_{xy}}{\sigma_x \cdot \sigma_y} \cdot \frac{2\overline{x} \cdot \overline{y}}{(\overline{x})^2 + (\overline{y})^2} \cdot \frac{2\sigma_x \cdot \sigma_y}{\sigma_x^2 + \sigma_y^2} \quad , \tag{1.10}$$

where, $\overline{x} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} x(i,j)$, $\overline{y} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} y(i,j)$,

$\sigma_{xy} = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [x(i,j) - \overline{x}][y(i,j) - \overline{y}]$,

$\sigma_x^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [x(i,j) - \overline{x}]^2$,

$\sigma_y^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [y(i,j) - \overline{y}]^2$,

where two images x and y are considered as the original and stego image with size $(M \times N)$ containing pixel values $x[i,j], y[i,j]$ respectively $(0 \geq i > M, 0 \geq j > N)$. The first component is the CC, and it measures the degree of linear correlation between x and y images. It lies in the range $[-1, 1]$. When x and y are linearly related, the best value 1 is obtained. It means that $y[i,j] = a * x[i,j] + b$ for all possible values of i and j. The second component measures how close the mean luminance is between the images. Its value lies in the range $[0, 1]$. Here, σ_x and σ_y are considered as estimates of the contrast of x and y. The third component measures the similarity of contrasts of the images. Its value lies in the range $[0, 1]$. The Q-Index range is $[-1, 1]$. When the two images are identical, the best value 1 is achieved.

Bit Error Rate (BER):

The rate of occurrence of errors in a transmission system is measured by Bit Error Rate (BER). The BER can be calculated using equation (1.11).

$$BER = \frac{\text{Number of errors}}{\text{Total number of bits transmitted}} \tag{1.11}$$

Computational Environment:

All the schemes discussed here are implemented in Java 8 on Windows 10 (Operating System) environment. The computational platform is an Intel Core i5-6200U processor with a speed of 2.40 GHz and 4 GB RAM.

Standard Benchmark Input Images:

Some benchmark images have been used for experiment and analysis of the proposed schemes. These are collected from “USC-SIPI” image database [90] and “UCID” image database [91].

Figure 1.1 shows the corresponding images of the said databases.

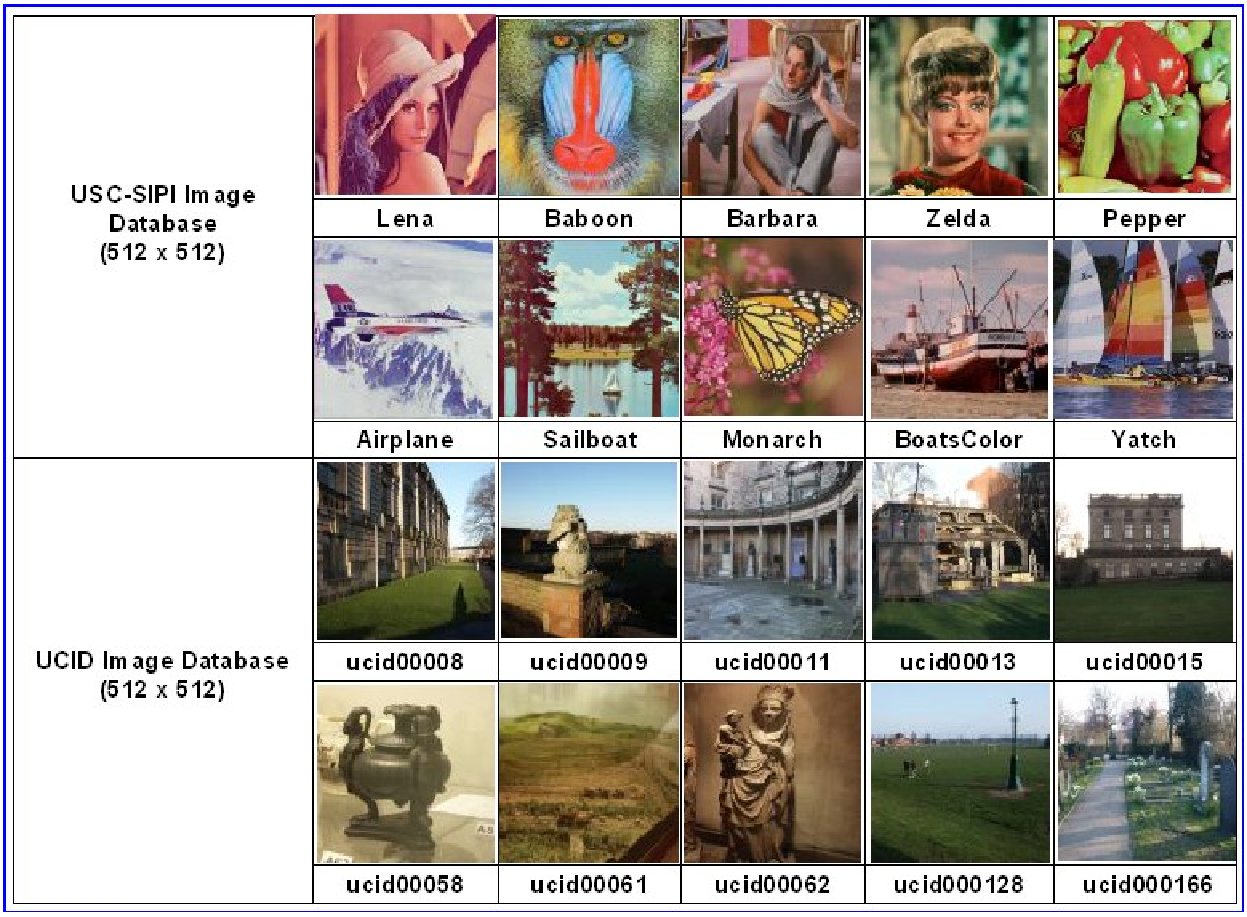

Figure 1.1: *Standard color images* (512×512) *used in the thesis*

1.6 Organization of the Thesis

In this thesis, some secured steganographic techniques have been designed, implemented, and analysed. The thesis is divided into two parts including seven chapters. Part I describes steganographic schemes in spatial domain which contains two chapters, Chapter 3 and 4. Part II describes steganographic scheme in transform domain which contains Chapter 5.

Chapter 1 contains an introduction to the overview of some steganographic schemes. A brief review of steganography, problem domain, motivations, objectives, contributions, evaluation metric, and organization of the thesis are included in this section.

Chapter 2 describes some steganographic methodologies which are used to solve different types of steganographic problems. In this thesis, the following methods have been used in the course of development of the new steganographic schemes.

i) Pixel Value Difference (PVD)

ii) Weighted Matrix

iii) Graph Neighbourhood

iv) Discrete Cosine Transform (DCT)

v) Discrete Wavelet Transform (DWT)

Chapter 3 contains two single image based steganographic schemes using PVD and graph neighbourhood. The embedding capacity and perceptibility are the important criteria of a steganographic scheme. Images are partitioned into fixed-sized non-overlapping pixel blocks. Every pixel block is considered as a separate graph where pixels are the nodes of the graph. Each pixel in the pixel block is grouped depending on a given range. The degree of neighbourhood of a node is the number of pixels, belong to the same group, around it. A threshold value is then considered and the pixels, whose degree of neighbourhood is more than the threshold value, are selected. These selected pixels are considered for secret data embedding. Instead of embedding secret data in all these selected pixels, a particular pixel is selected using a weighted matrix to embed data. Selecting the similar pixels for data embedding and introducing a weighted matrix improves the embedding capacity as well as enhance the visual quality of the stego image compared to some other existing state-of-the-art methods of the same kind. Finally, the proposed scheme is tested with different steganographic attacks, and different types of analysis are performed to observe its imperceptibility and robustness.

A color image based reversible steganographic scheme using PVD with image interpolation has been proposed as the second scheme in this paper. Here, the cover image is generated by interpolating the pixels of the input color image. The cover image is partitioned into separate image blocks, and Pixel Value Difference (PVD) method is repeatedly used in each block to embed the secret message. It has been seen that the proposed technique gives 2.22 bpp payload and approx 43.47 dB PSNR. The proposed scheme is fully reversible. So, both the original input image and the secret image can be successfully extracted from the stego image. The proposed method is tested using different steganographic attacks like RS analysis, Chi-square analysis, and Normalized Cross-Correlation (NCC) to show that the scheme is undetectable under these analysis and more robust than some other schemes of the same kind. This scheme provides good embedding capacity with the high visual quality of stego images. Peak Signal to Noise Ratio (PSNR) is calculated to show that the image quality of the proposed method is better compared to some other existing steganographic schemes.

Chapter 4 incorporates two dual image based steganographic schemes. The first scheme is based on the concept of graph theory. In any steganography scheme, the main challenge is to keep high imperceptibility of the stego image with good embedding capacity. The second scheme is a weighted matrix-based steganographic scheme with dual images. The dual images are partitioned into fixed sized pixel blocks for data embedding. In one iteration, the first pixel block of the first image contains the secret message and the first pixel block of the second image carries the location of change made in the first pixel block of the first image. Similarly, in the next iteration, the second pixel block of the second image contains the secret message and the second pixel block of the first image carries the location of change made in the second pixel block of the second image. In this way, the secret message and the data embedding locations are stored in the two images alternately. The weighted matrix is updated before each iteration, which enhances security in the field of steganography.

Chapter 5 holds two steganographic schemes in transform domain with two different approaches. Due to the rapid growth of internet technology and the advent of various image processing tools, people started using digital media for hidden communication to protect valuable information which is important for multimedia commercials, health-care, medical and defense applications. On the other hand, image authentication and tamper detection are essential, especially when it is utilized for evidence of legal action. The main challenge of any image steganographic scheme is to preserve the imperceptibility of the cover image along with undetectability and embedding capacity. In the first approach, a robust, secure, and imperceptible image steganographic scheme combining Discrete Wavelet Transform (DWT) with Discrete Cosine Transform (DCT) has been proposed. In the proposed approach, the cover image is decomposed into 4 sub-bands, LL, LH, HL, and HH using DWT. The sub-bands LH, HL, and HH are partitioned into non-overlapping blocks and DCT is applied to each block. The secret bits from the secret image is embedded into the DCT coefficients with the help of a weight matrix. The purpose of the proposed scheme is to provide less distortion and better undetectability in the final stego image. The proposed scheme is tested using different images from some standard image databases. The effects of rotation, compression, and noise have also been investigated on the proposed scheme. Experimental results show better effectiveness of the proposed steganographic scheme with good visual quality and high embedding capacity. The results also demonstrate the better robustness of the proposed scheme under different image processing attacks compared to some other related existing schemes. In the second approach, a weighted matrix based steganographic scheme has been designed for highly compressed (QF 40%) color image through Discrete Cosine Transform (DCT) to maintain a good balance between payload and imperceptibility. Here, the AC components are collected from (8×8) quantized DCT coefficient matrices of YCbCr channel. Then, a series of (3×3) original matrices are formed to hide secret data. The collection of AC components is controlled by 128 bits shared secret key. A predetermined weighted matrix is employed to select the embedding position within a (3×3) coefficient matrix of a cover image through the sum of the entry-wise multiplication operation. The proposed scheme provides good embedding capacity with high visual quality compared to existing state-of-the-art methods. Finally, different steganographic analysis and attacks are carried out to observe its imperceptibility and robustness.

Chapter 6 analyzes all proposed steganographic schemes. The comparisons of the proposed schemes with reference to data embedding capacity, security, robustness, and visual quality are discussed here. The effects of various steganographic attacks and the results of steganalysis are presented. Also, the comparison of the various domain has been enlisted. Finally, the limitations and recommendation for future works have been summarized.