6.1 SUMMARY OF THE THESIS

Reversible data hiding has emerged as a major research area due to the phenomenal growth in internet and multimedia technologies. It involves concealing confidential data within another seemingly innocuous cover media such as text, video, audio, images, and compression coding. The embedded data can then be used as authentication codes for protecting intellectual copyrights (Water marking) or as confidential data for sharing information (Steganography). However, in those applications, permanent destruction of the cover media is normally unavoidable, even after the embedded media has been extracted. In some sensitive applications like as medical diagnosis, military, and law enforcement applications, even minor distortion may be unacceptable. A slight distortion may lead to a misinterpretation of final decision. Hence, reversible data hiding schemes are used to restore the cover media without distortion in such sensitive applications. Several algorithms have been proposed in the literature for data hiding over the years. The performance of these systems widely varies from one method to another. This research work is an investigation of certain algorithms for reversible data hiding in spatial and frequency domains. The performance of any reversible data hiding system depends on four important criteria, namely, imperceptibility, data embedding capacity and robustness. As they are interlinked with one another and improvement in one or more factor is
achieved at the cost of distortion of the other. Hence, the proposed works have established a balanced compromise between the three extremities for an optimal data hiding in the natural images.

In chapter 3, reversible data hiding is carried out in spatial domain using edge-oriented Gaussian weighted predictor. The proposed method has utilized the information redundancy exist in the color channels to estimate the edges and hence the prediction error. The edge detectors namely, Sobel, LoG and Canny are used for detecting edges in cover images. Even though canny edges provide more space to embed data, it offers less PSNR compared to Sobel and LoG operators. But it provides an optimal solution to problem of edge detection, especially in the presence of noise. The performance of edge-oriented Gaussian weighted predictor is compared with Median edge detection predictor and Gradient adjusted predictor. As the edge-oriented GWP provides sharper prediction error, the embedding capacity is higher compared to other predictors. Genetic algorithm is used to increase the predictor efficiency. The data embedding is performed by expanding the Gaussian weighted prediction error according to the secret bits. The proposed method yields a PSNR of about 52-59 dB and SSIM of about 0.96 for the embedding rate between 0.1 and 0.5 bpp. Hence, it is proved that the embedded payload is highly imperceptible. As the BER is about 0.2 to 0.4 % of embedded payload, the algorithm is said to be robust against various attacks.

Chapters 4 focused on the two optimality criteria, namely, robustness and reversibility. The frequency domain strategy has been adopted due to its superiority over the spatial domain techniques in certain important aspects like robustness towards signal processing and image processing attacks. Hybrid transform has been proposed based on the unique features of the transforms in the hybrid combination so that it is able to address the
robustness and reversibility criteria. Accordingly, the rotation, scaling and translation properties of the Radon transform and reversibility property of integer lifting transform have been joined together in a hybrid formation. The superiority of this combination is also tested and compared with the other existing works in literature.

As the Radon transform performs rotation, scaling and translation operations on the cover image, it changes the positioning of the secret bits. Hence, it is very difficult to detect the embedded data without taking the inverse Radon transform and subsequently increases the security of the embedded payload. The integer lifting wavelet transform uses arithmetic coding for bit plane compression which guarantees complete reversibility. Middle bit planes are used for embedding as they provide a balanced trade-off between embedding capacity and visual quality of that stego image. The performance of various orthogonal and bi-orthogonal wavelet families in the lifting domain under fixed and varying secret payload is investigated. The cdf1.1 wavelet gives better results among the wavelets used here, followed by cdf1.5 and bs3. As the proposed framework embeds data in red, green and blue channels, it can work well for a variety of images with different distribution of colors. The results have been compared with the existing works in the literature and the proposed method gives an improvement in PSNR of about 10-15% over that of already obtained. The embedding capacity of bit plane 6 is about 95,000 bits whereas for bit plane 4, it is only 86,000 bits. i.e., Higher the bit plane, better the embedding capacity. But at the same time, PSNR drops down when the number of bits embedded in the bit plane increases. Different images provide different quality metrics for the same embedded payload.

When the image intensity is projected at different angles using radon transform, the perceptual quality of the embedded image also gets
changed. As the angle varies from 0 to 90 degrees, the PSNR and SSIM for all test images are also increased. However, as angle varies 90 to 180 degrees, the PSNR and SSIM get reduced. The embedded images are subjected to various intentional and unintentional attacks and tested for robustness and reversibility. As the BER is about 0.15 – 0.35% of embedded payload, the algorithm is robust to attacks. From the simulation results, it is inferred that the proposed algorithm exhibits reversibility due to high NCC values.

Chapter 5 focused on increasing the payload as well as robustness as opposed to the former belief that robustness would have to be compromised for better payload. Robustness of data hiding techniques can be improved if the properties of the cover image could be properly utilized. Hence, the cover image has been transformed into time-frequency domain using FrFT and the optimal pixel locations for hiding the secret data are found by using Firefly algorithm. The optimal location has been found by using the multi-objective function which is the combination of SSIM and BER. The objective function for firefly algorithm is fixed in such a manner that both quality and robustness of the embedded image are within an acceptable value. The histogram shifting technique is used to embed secret data in the optimal pixel locations. The resultant embedded image is better in quality and also able to withstand certain noise and image processing attacks during transmission.

The quality of cover images is analyzed under varying payload by keeping the fractional order constant. The Lena image offers a maximum PSNR of 53.40 dB and SSIM of 0.9988 at the embedding rate of 0.125 bpp. As the PSNR obtained for all cover images is greater than 45 dB, the proposed method is highly imperceptible. The proposed method is compared with the existing methods in the literature and it is observed that there is an improvement in PSNR of about 2 - 12 dB over that of existing methods. It is
found that using FrFT, high visual quality embedded image can be obtained for the same amount of embedding rate as that of other transforms. The quality of stego image gets changed as the fractional order changes. Maximum PSNR and SSIM are obtained for the fractional order of 0.5, i.e., at the rotation angle of 45 degrees for all cover images. It is clear that FrFT makes full use of the additional feature provided by its fractional order ‘a’ to achieve an optimal domain in which PSNR and SSIM values are better than any other two dimensional transforms. After subjecting to various intentional and unintentional attacks, the BER and NCC are measured. As the BER is about 0.15 – 0.25 % of embedded payload, the embedded payload is highly robust to attacks. As the NCC values are greater than 0.98, it is clear that the original cover image is exactly restored.

6.2 FUTURE SCOPE

To improve the robustness of the embedded payload against attacks in the spatial domain and to improve the perceptual quality of standard images at high embedding rates, new approaches can be investigated. Instead of embedding secret data into cover image directly as in conventional steganography, it is better to use cryptography to generate cipher text of the secret message and then embed the cipher text into cover image using an appropriate algorithm. As the conventional prediction error expansion based and histogram based techniques require significant quantity of side information to achieve reversibility, the embedding capacity of the cover image gets affected. Efforts should either investigate the feasibility of new algorithms for enhancing the embedding capacity and achieving better image quality.

Implementation of Reversible data hiding in Orthogonal Frequency Division Multiplexing (OFDM) channel will enhance the robustness and the integrity of the message to be transmitted with higher imperceptibility. The
error-correction codes can be integrated along with data embedding algorithm for effective communication purposes. This decreases the chances of the message being tampered by a third party. Due to the advancement in integrated circuit (IC) technology, data hiding concepts may be implemented on field programmable gate arrays (FPGA) technology. This results in reduction in space, cost and embedding and extraction time in real time applications. As the proposed algorithms have low computational complexity, they can also be used for embedding data in a video file.