CHAPTER 7
RESULTS & CONCLUSIONS

7.1 SUMMARY

This research was taken up with an objective of developing watermarking algorithms for images. We felt that it is essential to first ensure that all the developed watermarking schemes are resistant to at least one attack having the most financial implications to establish a high demand in the commercial market. Therefore, we chose collusion attack resistant nature to be embedded in all developed watermarking schemes. Finding the results reported in literatures, we started to develop the watermarking schemes by choosing classical Middle Band Coefficients Exchange scheme as a base because this scheme was very robust against JPEG compression attack. Chapter 4 discusses the development of watermarking algorithm for Gray scale images and “preprocessing” of the images to add robustness against JPEG compression and histogram equalization attack. Chapter 5 presented a watermarking algorithm for colored BMP images and a study to find the appropriate color channels to carry the watermark data to improve the robustness of the watermarking scheme. In both chapters, the watermarking algorithms are DCT based. After then, we presented a DCT based and a dual (DWT + DCT) based watermarking schemes in Chapter 6 for JPEG images.

7.2 MAIN CONTRIBUTIONS AND HIGHLIGHTS OF THE RESULTS

The proposed watermarking schemes have the following characteristics:

1) These are ICAR in nature. This was achieved by introducing randomness and redundancy in the coefficients exchange criterion in FM region of block DCT and DWT.
2) These are very robust against JPEG compression (even up to JPEG quality factor \( Q = 5 \), compression ratio up to 98 \%) and outperform other existing state-of-the-art watermarking schemes.

3) These are very robust against common image manipulations and known attacks.

4) We introduced the concept of “preprocessing” i.e. minimizing the attack impact before watermarking of the image so that some known attack can not disturb the watermarked images very heavily and thus perform better recovery of the watermark data.

5) We established that if we want to increase the robustness against JPEG compression, the watermark data should be hidden in the GREEN color channel (not in BLUE color channel, as reported in most of the research papers even if poor sensitivity of the eye to the BLUE color channel).

6) We have also correlated image characteristic and watermarking scheme robustness against some attacks. It was found that for multicolored image, if watermark data is hidden in the color channel having the lowest “Standard Deviation”, then the performance against JPEG compression and other common attacks increases.

7.3 FUTURE WORK

1) Considering the huge financial aspects of the watermarking application areas, apart from ICAR, more characteristics against some attacks like forgery attack or multiple watermarking can be embedded.

2) Further studies may be conducted to know the attack impacts on the images and then watermarking schemes to be developed so that those impacts could be minimized before the start of watermarking so that a better recovery of the copyright data could be performed.

3) A watermarking scheme may have some relationship with the image on which it is going to apply. Performance of the watermarking scheme or selection of the watermarking scheme or at least few input parameters of the watermarking scheme must be related to image characteristics.
4) More wavelet transforms should be examined for embedding of the watermark data and robustness against JPEG2000 format conversion.

5) All presented watermarking schemes may be coupled with some special “Geometrical attack resistant” watermarking schemes and thus developing watermarking schemes to ensure maximum converge against malicious attacks.