Chapter 6

Conclusion and Future Scope

In this dissertation, six new watermarking techniques have been introduced. A summary of the main experimental results and achievements are discussed. Some limitations and promising directions for future work are described.

6.1 Summary of the Proposed Work

The proposed work in this dissertation is concerned with the design of reversible watermarking technique in the spatial domain. Comparisons of suggested schemes concerning various evaluation metrics are presented here. Also a comparison with respect to different attacks is shown. Finally, conclusions are drawn with respect to proposed methods.

In this dissertation, six different reversible watermarking schemes are proposed to solve the image authentication and tamper detection problem, with the help of LBP, CA, Hamming code and WM. Image interpolation, sub-sample image, and dual image also play an important role in a watermarking scheme to solve these problems. Moreover, the schemes provide improved robustness against several attacks, while maintaining the perceptual quality of the host image including high payload.

Table 6.1 presents the details achievements of our schemes. After developing each algorithm,

Table 6.1: Comparison of proposed schemes with respect to attacks

Proposed Scheme	Methodology/ Tools used	Capacity (bits)	Payload (bpp)	PSNR (dB)	No. of times Image recovered	
					Cover (CI)	Watermark (W)
RWS-WM	WM	21,05,352	8.00	50.03	8	4
RWS-CA	CA, Sub-sample	3,93,216	1.50	50.22	9	5
DRWS-LBP	LBP, Dual Image	6,93,600	2.67	53.51	8	7
RWS-LBP-HC	LBP, Hamming	31,45,728	3.00	45.00	9	9
RWS-LBP-CA	LBP, CA	7,01,784	2.66	48.53	9	7
RWS-LBP-WM-LIP	LBP, WM, LIP	5,40,672	2.06	53.27	10	10

we have analyzed it using various evaluation metrics. We have also applied ten different attacks such as Salt and Pepper noise, Cropping, Copy move forgery, Opaque, Blurring, Median filtering, Inversion, JPEG compression, Rotation, Flipping and tested the robustness of each scheme against these attacks. The dissertation has been organized based on the results against attacks on these schemes. Figure 6.1 shows a comparison of average PSNR values of six different proposed schemes. It is found that DRWS-LBP scheme defined the maximum PSNR among all six

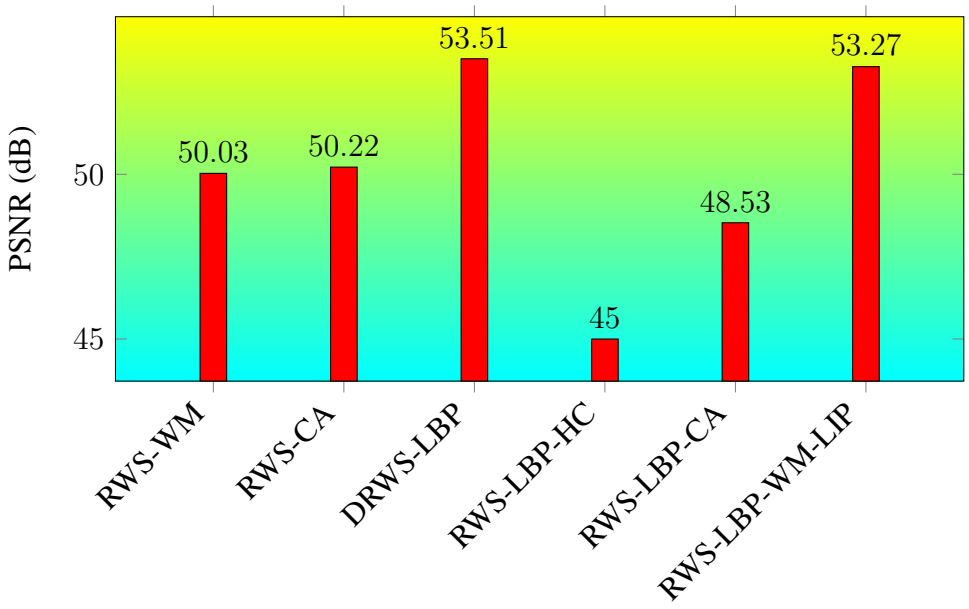

Figure 6.1: Graphical representation of proposed schemes with respect to PSNR (dB)

proposed schemes.

The graphical representation of proposed schemes with respect to Payload (bpp) have been depicted in Fig. 6.2. It shows that RWS-WM achieves the highest payload than others and this has been obtained by repeated embedding through the weighted matrix.

Comparison of proposed schemes with respect to embedding capacity (bits) of watermark have been depicted in Fig. 6.3. It shows that DRWS-LBP achieves the highest capacity than others and this has been achieved by image interpolation.

The graphical analysis of proposed schemes with respect to PSNR and payload of the watermarked image is depicted in Fig. 6.4. It shows that RWS-WM outperforms than others.

Comparison of proposed schemes after applying different attacks on the watermarked image is depicted in Fig. 6.5. It shows that RWS-LBP-WM-LIP is better than others.

6.2 Limitation

In this age of digitization, no image watermarking scheme can be considered as the ultimate solution for all requirements. In this dissertation, six different image watermarking schemes have been proposed, and schemes have certain limitations. The limitation of the proposed scheme are as follows:

- In this thesis, watermarking schemes have been developed considering only the **image** as

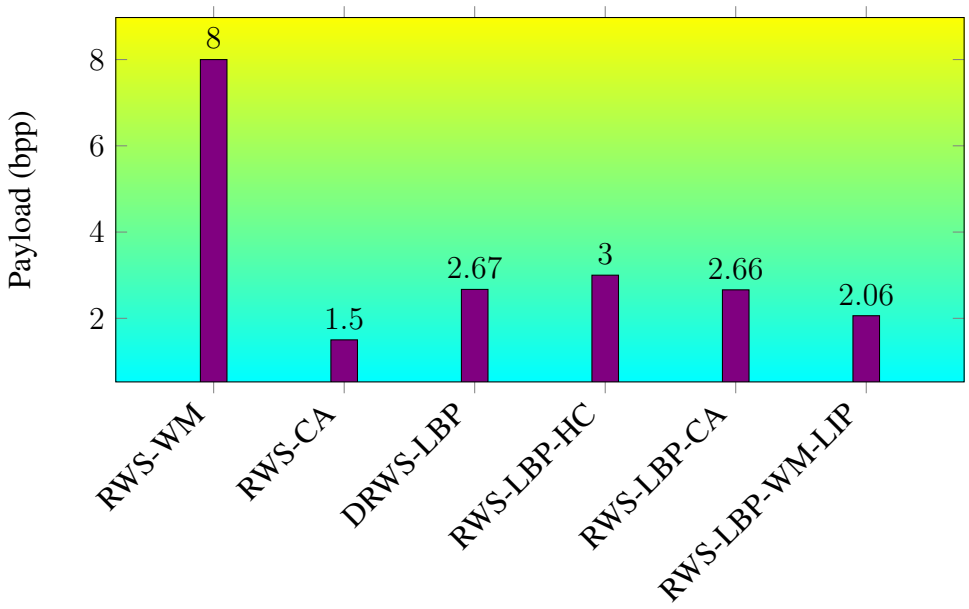

Figure 6.2: Comparison of proposed schemes with respect to Payload (bpp)

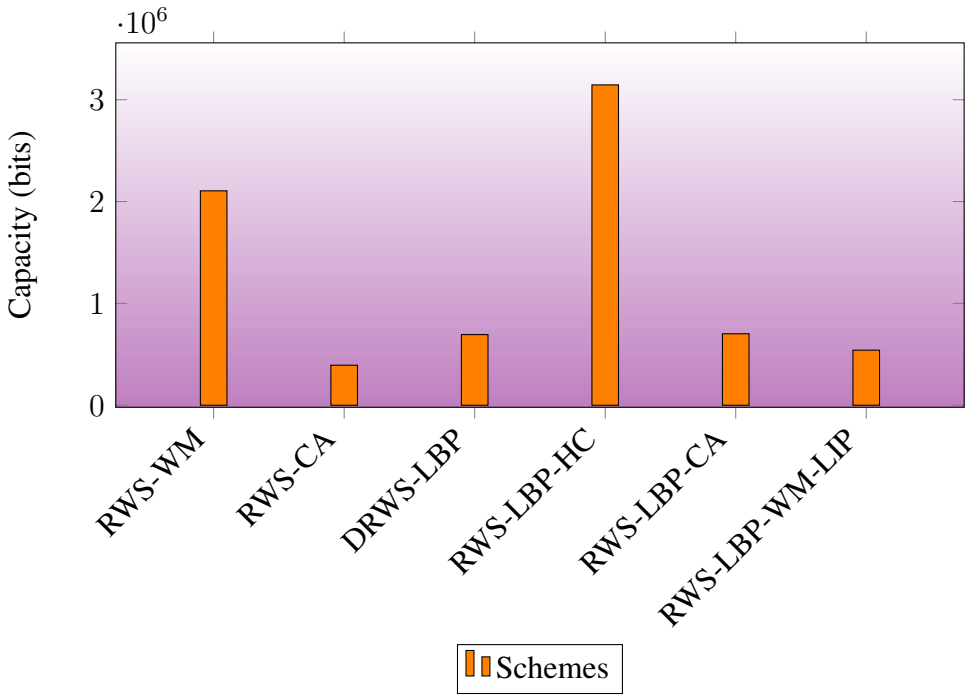

Figure 6.3: Comparison of proposed schemes with respect to watermark embedding capacity (bits)

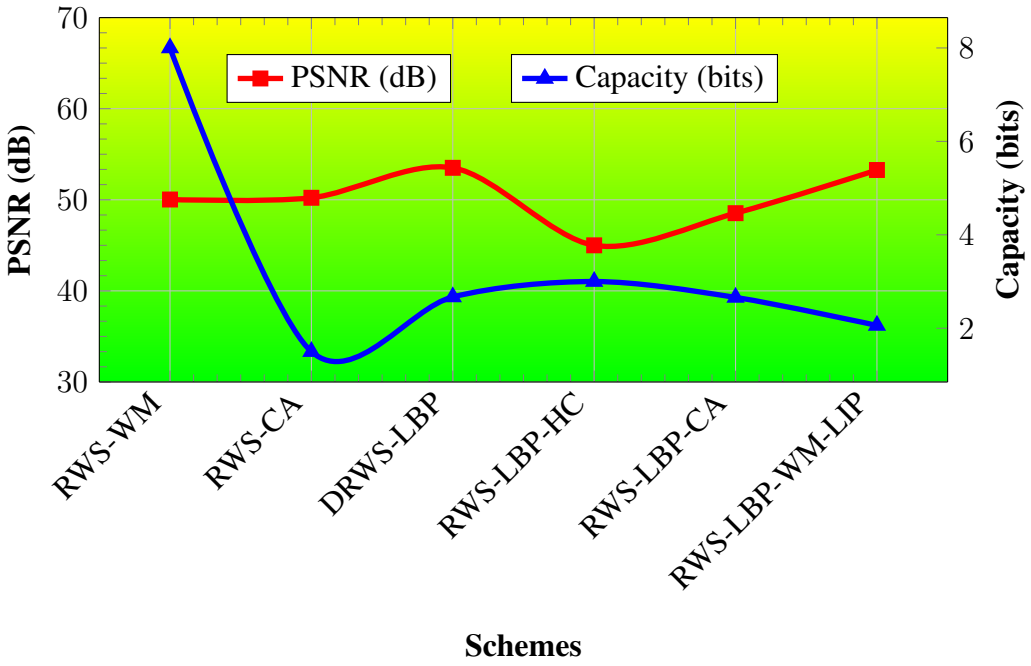

Figure 6.4: Comparison of proposed schemes with respect to PSNR (dB) and Payload (bpp)

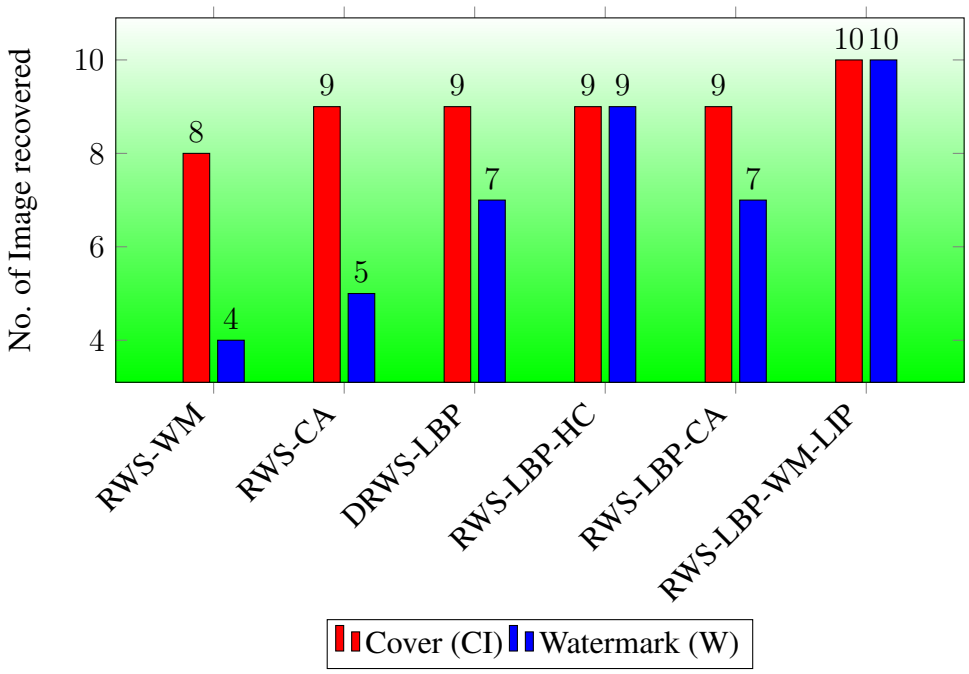

Figure 6.5: Comparison of proposed schemes with respect to Attacks

cover media.

- The proposed algorithm only works on the **spatial domain**.
- Hamming code is used to detect and recover a **single bit error**. So, multi-bit error or block error cannot be recovered by the proposed algorithms.
- The proposed schemes mainly consider **LSB** as the watermarking domain and all the schemes are fragile in nature.
- In one of the proposed schemes, sender has to share an **Index file (InF)** which is complex in nature.

6.3 Future Research Work

In this section, we have mentioned the specific direction for future research. Here we would also like to present a broad classification of intended future research directions. The future research directions can be classified as follows:

(1) **Domain:** In this thesis, all proposed schemes are designed in the spatial domain. So the further investigation can be carried out in the transform domain, compress domain and random domain.

(2) **Medium:** Video telephony is of increasing interest nowadays which needs urgently to solve the privacy and confidentiality that requires complex security of the scheme. But all proposed schemes are based on host media as an image. So there is a scope to find applicability of our schemes in other host media such as audio and video.

(3) **Improved Watermarking Algorithms :** The robustness of any watermarking scheme depends on where the watermark is embedded. So an improved watermarking scheme can be designed with the help of Region of Interest (ROI).

(4) **Mode of Authentication:** The authentication code can be improved with the help of Image Hash, Bio-Hash, Face Image, Finger Print etc.