Chapter 6

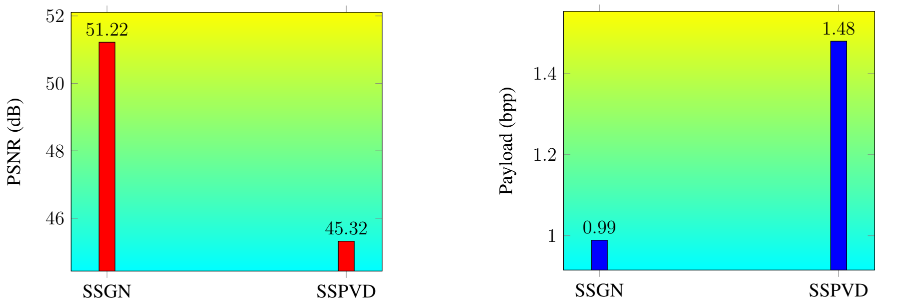
Conclusion and Future Scope

6.1 Summary of the Proposed Works

The work described in this thesis is concerned with the design and analysis of some steganographic schemes in spatial and transform domain. In this chapter, proposed steganographic schemes are analysed through standard evaluation metrics. The comparisons of the suggested schemes with respect to various evaluation metrics are also presented here. Finally, conclusions, limitations, and future scope are discussed.

In this thesis, four new steganographic schemes have been proposed in spatial and transform domain. In spatial domain, two single image based steganographic schemes have been suggested. The first scheme (SSGN) uses graph neighbour and the second scheme (SSPVD) deployed PVD to embed secret data within the stego image. It is observed that the visual quality is better in the graph based scheme (SSGN) whereas the payload is better in PVD based scheme (SSPVD). The SSGN selects pixels in the same range to embed secret data, which helps to increase the visual quality of the stego image. The payload is much better in SSPVD with respect to the SSGN because the PVD method is repeatedly applied to embed secret data within the interpolated pixels of the stego image. The SSGN is not reversible, but reversibility has been achieved in SSPVD with the help of interpolated pixels. The weighted matrix and the reference table play an important role in enhancing the security of the developed schemes. The schemes are compared in terms of visual quality (PSNR) and payload (bpp). The visual quality (measured by PSNR (dB)) and payload (bpp) comparison graphs of SSGN and SSPVD are shown in Fig. 6.1a and Fig. 6.1b respectively. The PSNR (dB) in SSGN is 51.22 where as it is 45.32 in SSPVD.

Two dual-image based steganographic schemes have been suggested using graph neighbourhood (DSGN) and weighted matrix (DSWM) to improve the security and robustness.

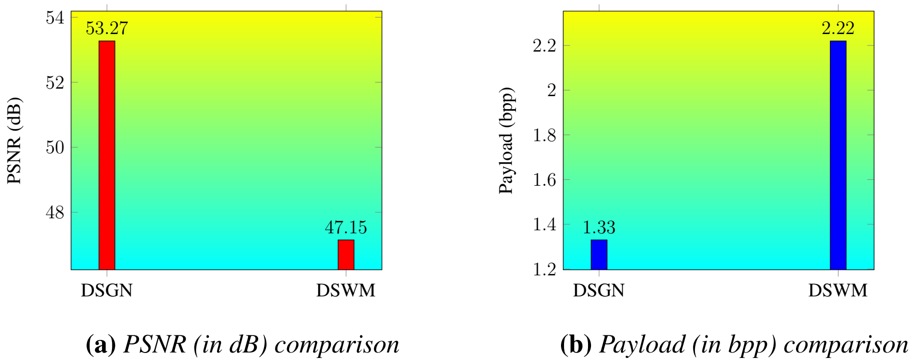


(a) *PSNR (in dB) comparison* **(b)** *Payload (in bpp) comparison*

Figure 6.1: *Comparison of the SSGN and SSPVD schemes in terms of PSNR (dB) and payload (bpp)*

In DSGN, reversibility has been achieved, but data hiding capacity is not up to the current demand. The DSWM scheme solves the hiding capacity problem by embedding 2.22 bpp with high quality (47.15 dB PSNR) stego image. The comparison graph with respect to image quality (PSNR) and payload (bpp) of both the schemes is depicted in Fig. 6.2a and Fig. 6.2b respectively. It is observed that the visual quality (53.27 dB) of DSGN is higher than DSWM, but embedding capacity (1.33 bpp) is lower. It is possible to embed high capacity (2.22 bpp) secret data in DSWM using repeated entry-wise multiplication operation by weighted matrix and store positional values in interpolated pixels of both the stego images. One of the most important features of dual image based steganographic scheme is that the secret data are distributed within the dual images. In DSGN, data distribution depends on block number (even or odd) whereas DSWM uses bit value (0 or 1) of SHA-512 bits secret key. The secrecy depends on SHA-512 bit secret key and weighted matrix used in DSWM. Moreover, the original secret bits are not embedded in DSWM rather it can increase or decrease one bit to embed 4 bits secret information. It is hard to detect and retrieve the secret data without proper secret key and weighted matrix. On the other hand, the attacker needs two stego images simultaneously to retrieve secret data which is under secret sharing problem.

Due to the bandwidth limitation, people try to send images in a compressed format to save time and space. It is essential to investigate secured steganographic scheme through the compressed image, which may sustain under various geometric attacks. In this motivation, two steganographic schemes have been designed in transform domain using DCT (SSDCT) and DWT (SSDWT). In both the SSDCT and SSDWT schemes, the weighted matrix has been employed to embed secret data in DCT and DWT coefficients. The weighted matrix is beneficial because DCT coefficients are very sensitive to a small change, and the weighted matrix can em-

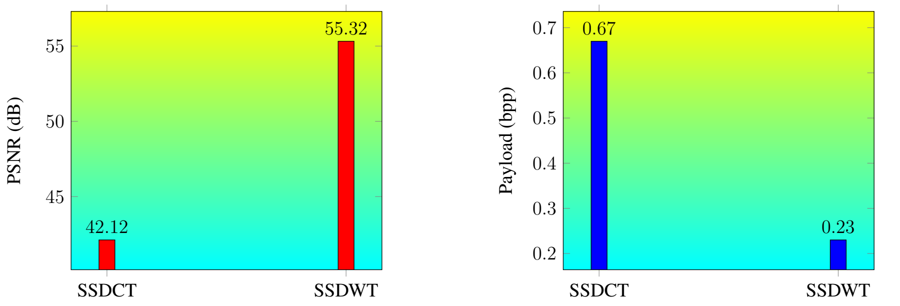


(a) *PSNR (in dB) comparison* **(b)** *Payload (in bpp) comparison*

Figure 6.2: *Comparison of the DSGN and DSWM schemes in terms of PSNR (dB) and payload (bpp)*

bed 4 bits by changing only one bit. Though the embedding capacity in the transform domain is less, the schemes are more secure and robust than spatial domain schemes. The comparison of the schemes SSDCT and SSDWT with respect to visual quality and embedding capacity has been presented in Fig. 6.3a and Fig. 6.3b respectively. It is observed that PSNR is 55.32 dB in SSDWT whereas 42.12 dB PSNR in SSDCT. Finally, we have tested both the schemes using standard steganographic evaluation metrics. It has been observed that the schemes are robust and secured and can sustain uncertain attacking environments.

High fidelity can be achieved using SSDCT, and SSDWT. The embedded secret data is robust against unintentional attacks such as noise contamination, low pass filtering, blurring, contrast stretching, JPEG transcoding. However, in the simulated attacks, the embedded secret data is not robust against other attacks such as rotation, scaling, translation, and cropping etc. Because the DCT coefficient can be distorted significantly if these attacks are applied on stego images.



(a) *PSNR (dB) comparison* **(b)** *Payload (bpp) comparison*

Figure 6.3: *Comparison of the SSDCT and SSDWT schemes in terms of PSNR (dB) and payload (bpp)*

In our experiment, the SSDCT is used to embed more secret bits in the DCT domain of uncompressed images. The secret logo image can be decoded or detected independently using the corresponding weighted matrix. Experimental results show that the SSDCT can embed more than 50,000 bits in a 512×512 color image. The embedded secret logo image is also robust to common unintentional attacks.

The communication through the developed scheme is innocent because the values of different evaluation metrics SSIM, NCC, BER and Q-Index provide good results shown in the following figures. Figure 6.4 shows a comparison of average PSNR values of six different proposed schemes. From the figure, it is clear that the SSDWT scheme attains maximum PSNR values among all the proposed schemes. Figure 6.5 shows the comparison of the average payload of our developed schemes. From the figure, it is observed that the DSWM scheme has a higher

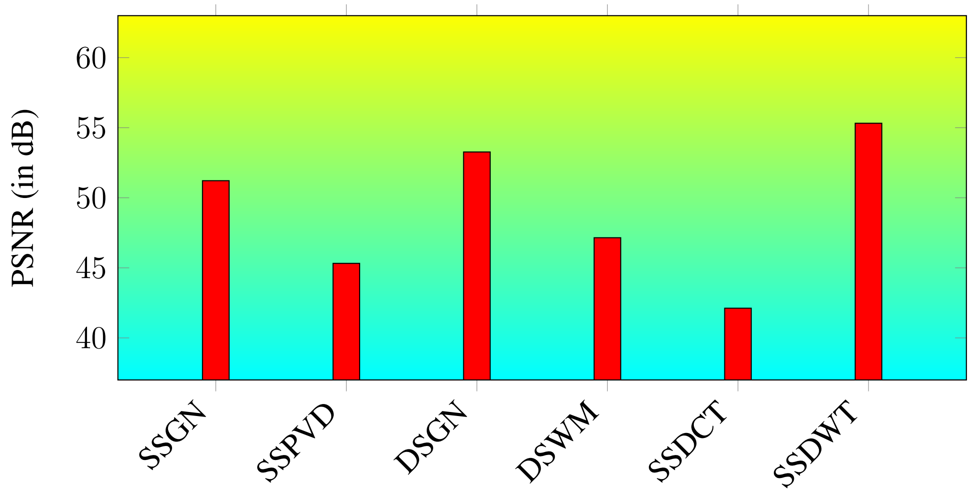


Figure 6.4: *Graphical representation of proposed schemes with respect to PSNR (dB)*

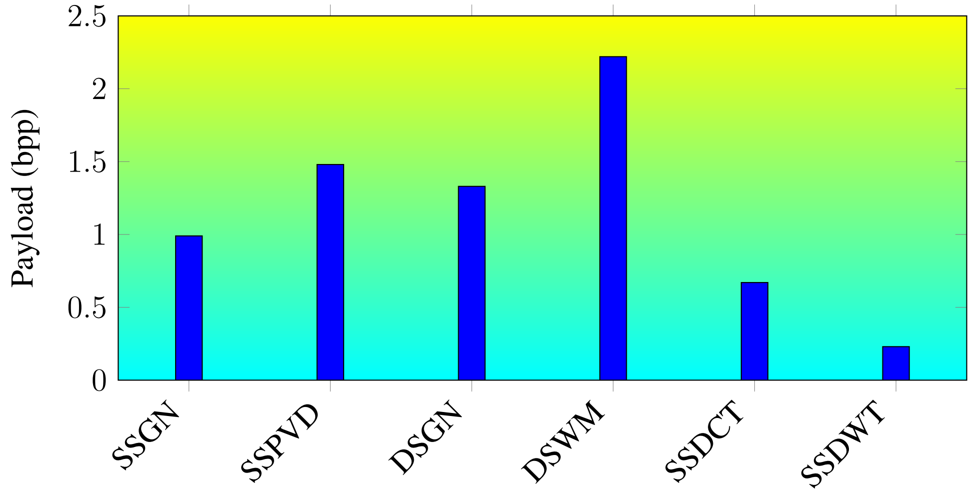


Figure 6.5: *Graphical representation of proposed schemes with respect to payload (bpp)*

payload in terms of bpp. It becomes possible due to the repeated application of the weighted matrix to embed secret data multiple times within the same pixel block of the stego image. Figure 6.6 shows the comparison of SSIM of our implemented schemes. It is found that all the proposed schemes exhibit good SSIM value, but the DSGN scheme has better average SSIM than other schemes. The NCC, BER, and Q-Index values of the proposed schemes are shown in Figure 6.7, 6.8, and 6.9 respectively. It is observed that all the schemes attain good results. It is seen that all the schemes attain good BER values, but the DSGN and DSWM schemes exhibit more BER values than other proposed schemes. It is because of the image interpolation rather than data embedding and it is one overhead of the dual image based steganographic schemes. The Q-Index value is minimum in SSDCT scheme, which indicates that the quality of the stego image in the scheme is better than other proposed schemes.

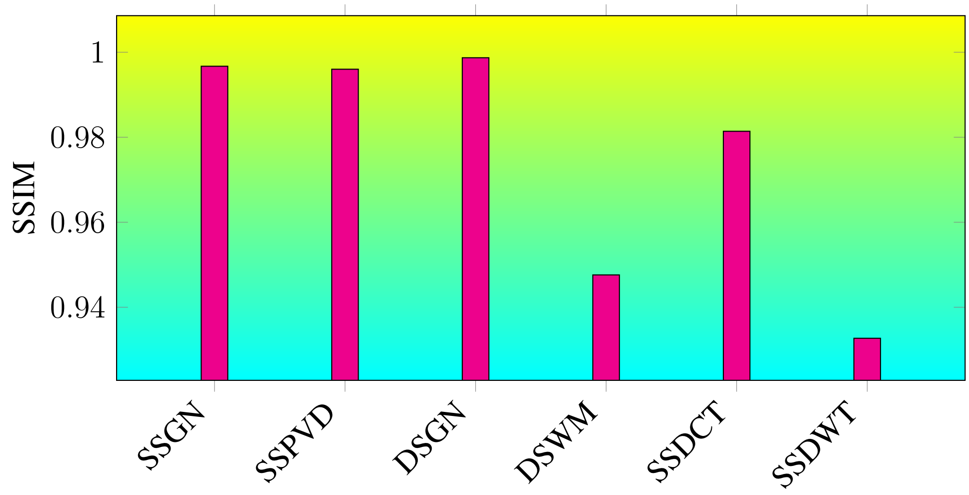


Figure 6.6: *Graphical representation of proposed schemes with respect to SSIM*

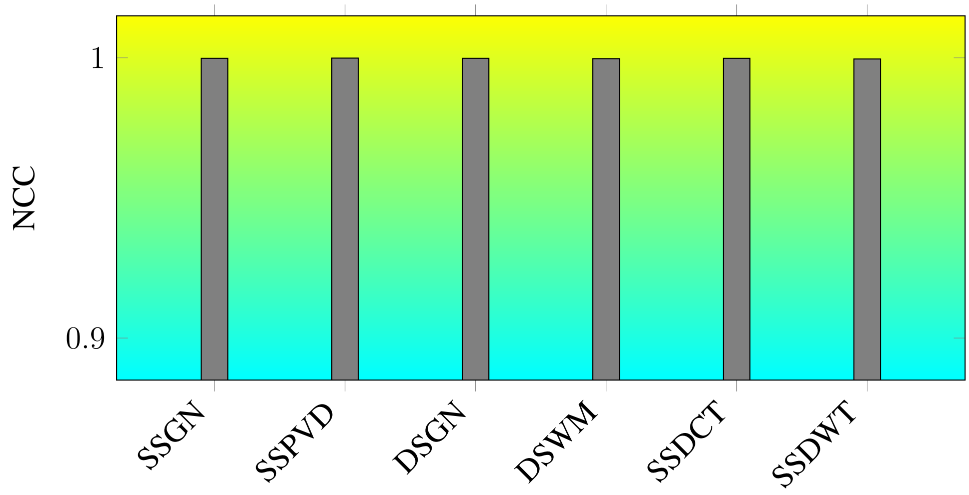


Figure 6.7: *Graphical representation of proposed schemes with respect to NCC*

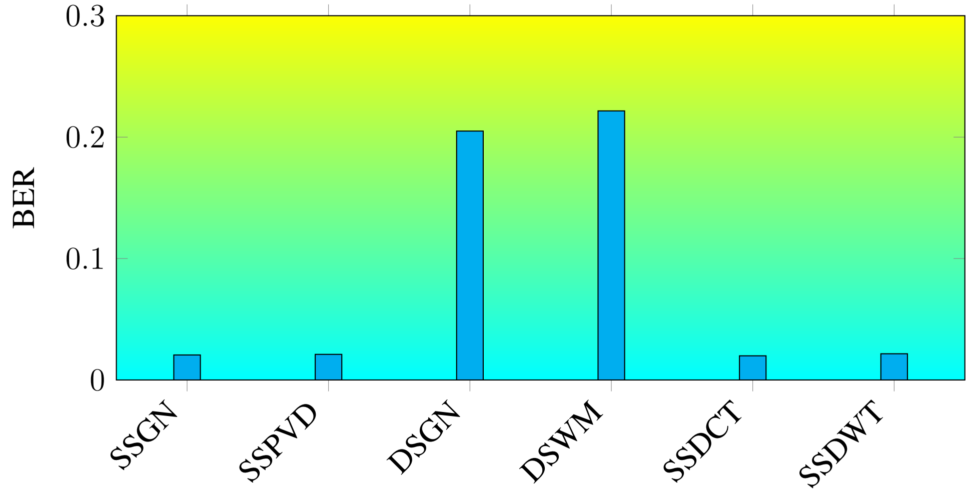


Figure 6.8: *Graphical representation of proposed schemes with respect to BER*

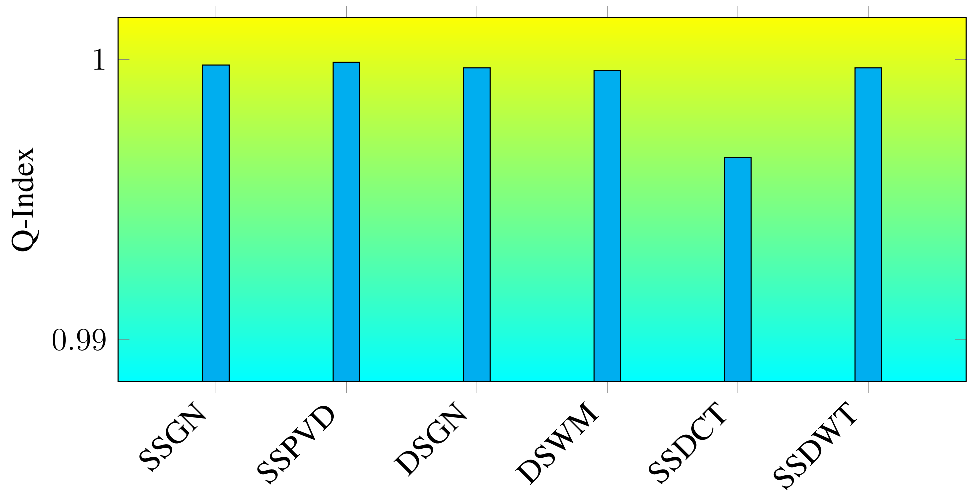


Figure 6.9: *Graphical representation of proposed schemes with respect to Q-Index*

6.2 Conclusion

In this thesis, six new steganographic schemes are designed and implemented. All these developed schemes are validated through various experimental results. Steganography through PVD is not reversible. A new steganographic scheme using PVD (SSPVD) has been proposed which is fully reversible. Here, the reversibility is attained through image interpolation. The SSPVD scheme gains payload 2.22 bpp, that is better than some recently published PVD based steganographic schemes. The proposed SSPVD scheme still maintains good visual quality, which is greater than 43.47 dB PSNR. Weighted matrix based data hiding schemes are not reversible. A new dual image based reversible steganographic scheme has been designed through the weighted matrix (DSWM) using image interpolation. Graph neighbourhood based steganographic schemes suffer from low embedding capacity. Here, some steganographic schemes, using graph neighbourhood (SSGN and DSGN), have been designed to improve the data hiding capacity keeping good visual quality of the stego images. Also, the security of the SSGN scheme is very limited. A dual image based steganographic scheme, using graph neighbourhood (DSGN), has been designed to increase the security of the scheme. A shared secret key (SHA-512) has been introduced to distribute the secret message between two stego images. It is very hard for any attacker to extract the message without the secret key and availability of both the stego images. Controlling the overflow or underflow situations is an overhead in some existing schemes. It has been resolved in the proposed schemes where it was necessary.

The steganographic schemes in transform domain exhibit less embedding capacity. A new

Table 6.1: *Application areas of the proposed schemes*

Proposed Schemes	Applications
SSGN	Can be used where visual quality of the image has utmost importance.
SSPVD	Can be used where the secret image along with the original cover image is required.
DSGN	Can be used where security along with the visual quality of the stego image is necessary.
DSWM	Can be used when the high volume of secret data needs to be embedded.
SSDCT	Can be applied for highly compressed JPEG images.
SSDWT	Can be applied where robustness and quality of the stego image is required in JPEG2000 images.

steganographic scheme through DCT (SSDCT) has been designed to increase the embedding capacity of the stego image in the transform domain. In SSDCT scheme, the data is embedded by changing the DCT coefficients, which are very sensitive and distort images when changed significantly. The proposed SSDCT scheme embeds data using weighted matrix by changing the minimum number of coefficients than other existing schemes. In transform domain based steganographic schemes, the imperceptibility and the payload of the stego image are always contradictory. So, a new steganographic scheme through DWT (SSDWT) has been designed which maintains a good trade-off between imperceptibility and payload.

The proposed SSDCT and SSDWT schemes embed secret data in JPEG compressed domain. The SSDCT scheme prevents the removal of the secret logo image by re-quantization of DCT coefficients due to the presence of the weighted matrix when the input and output are JPEG images. However, if the input image is highly compressed, not all the bits can be modified in SSDCT. The proposed SSDWT scheme solves this problem and allows to embed the secret image with stronger strength while maintaining the fidelity of the stego images. Experimental results show that when the visual quality of the stego image using SSDCT and SSDWT schemes are similar, the secret logo image of SSDWT scheme is more robust than that of SSDCT scheme. The Table 6.1 summarizes the application areas of the proposed schemes discussed in this thesis.

6.3 Limitations

In spite of various advantages, every steganographic scheme has some limitations. In this thesis, six different steganographic schemes have been proposed. Some of the limitations of the proposed schemes are mentioned below:

- Besides unknown weighted matrix, no other shared secret key is considered for better security in graph neighbourhood based schemes (SSGN and DSGN).
- In graph neighbourhood based schemes (SSGN and DSGN) data hiding capacity depends on the size of the range table and weighted matrix.
- Overflow and underflow situations may arise in the PVD based scheme. So, the preprocessing of the cover image is required before embedding.
- Image interpolation changes the size of the image after embedding secret data.
- The DWT based scheme (SSDWT) needs more analysis for a highly compressed image.

6.4 Future Scope

An ideal steganographic algorithm should have high precision, a higher level of security with good embedding capacity. Simplicity and cost-effectiveness should also be considered. Thus, it is necessary to investigate steganographic problems and solve with different approaches using different domains.

It is observed that the steganographic schemes designed in the transform domain are much better in terms of security as compared to the spatial domain schemes because in the transform domain, the secret message bits are embedded in the DCT or DWT coefficients rather than directly manipulating the pixels as happens in the spatial domain. Due to the advancement of digital technology and the popularity of social media, people are becoming more vulnerable. So, to increase the security, future work may be continued in transform, compress or random domains.

The design and implementation of the proposed schemes presented in this thesis are new. But some limitations still exist. So, there are some areas where the schemes can be extended further..

The concepts of steganography through PVD, weighted matrix, graph neighbourhood, DCT, and DWT are well known. But the idea of combining weighted matrix with graph neighbourhood, DCT, or DWT is quite new. The techniques like weighted matrix, which is predominantly used in the spatial domain, is combined with the techniques used in transform domain like DCT and DWT. In the future, the researchers may give attention to this area and explore how to use spatial domain techniques in transform domain to solve some real-life problems.

A variety of optimization schemes can be used to improve the cost of the steganographic algorithm and enhance the quality of the stego image. These include particle swarm optimization (PSO), ant colony optimization (ACO), neural networks (NN), fuzzy logic, hybrid network and genetic algorithm (GA), etc. These optimization algorithms may help to embed a secret message within a cover image in such a way that it improves stego image quality, embedding capacity, and imperceptibility.

Irrespective of these limitations and future scope, this thesis will be beneficial to the researchers who are perusing research in the field of computer science, engineering, and information technology. The schemes developed here are better than other existing schemes with respect to the payload, visual quality, reversibility, and security. This work would give the prospective researchers an excellent insight into the various new concepts used in steganography.