Chapter 8
Discussion and Conclusion
Chapter 8 Discussion and Conclusion

Introduction

Audio watermarking algorithms are studied in this thesis. Main goal of this thesis is to develop the intelligent encoder and decoder model of robust and secure audio watermarking. We have proposed two basic models one based on spread spectrum technique and other based on patch work algorithm. The implementation procedure and the results obtained for these methods were presented in chapter 5 and chapter 6 respectively. The chapter 7 proposed the models of the watermarking techniques based on the digital communication principles. This chapter concludes the thesis and gives suggestions for the further research.

8.1. Discussion and conclusion

The main aim of the present work is the development of audio watermarking algorithms, with the state-of-the-art performance. The algorithms performance is validated in the presence of the standard watermarking attacks.

In chapter 2 a survey of the key digital audio watermarking algorithms and techniques are presented. The referred algorithms are classified according to domain used for inserting a watermark and statistical method used for embedding and extraction of watermark bits. Scientific publications referred in the literature survey are chosen in order to build sufficient background that helps in identifying and solving the research problems.

The main point of the "magic triangle" concept is that if the perceptual transparency parameter is fixed, the design of a watermark system cannot obtain a high robustness and watermark data rate at the same time. Therefore, the research problem was divided into three specific sub problems. These sub problems are stated in chapter 3. To solve the sub problems stated in chapter 3 we implemented the various algorithms as mentioned.

i) What is the highest watermark bit rate obtainable, under perceptual transparency constraint, and how to approach the limit?
ii) How can the detection performance of a watermarking system be improved using algorithms based on communications models for the system?

iii) How can overall robustness to attacks of a watermark system be increased using an attack characterization at the embedding side?

These problems are tackled as below

1. To obtain a distinctively high watermark data rate, embedding algorithm were implemented in to transform domain.

2. To improve detection performance, a spread spectrum method and patch work algorithms are used, bit error rate is improved using cyclic encoding scheme.

3. To increase the robustness the attack characterization is employed through diversity.

To increase the high bit rate we embed the data in LSB of host audio in wavelet domain. The wavelet domain LSB algorithm is described in chapter 4. The wavelet domain was chosen for data hiding due to its low processing noise and suitability for frequency analysis, because of its multiresolutional properties that provide access both to the most significant parts and details of signal’s spectrum. The wavelet domain algorithm produces stegoobjects perceptually hardly discriminated from the original audio clip even when LSBs of coefficients are modified, in comparison with the time domain LSB algorithm.

The audio watermark is added into the host audio. In this scheme the attempt is made to embed the audio watermark in host audio signal. We have tried to embed the audio data of 0.5 to 5sec duration in 45 sec duration host audio. To measure the imperceptibility between the original signal and the watermarked signal we computed the SNR between them. The computed SNR after embedding the audio of varying length from 0.5 sec to 5 sec is presented in Table 4.2. The observed SNR for all cases is above 28 dB. The test results confirmed that the embedded information is inaudible except for the attacks like time warping and low pass filtering.
The BER is calculated to prove the similarity between the original watermark and the extracted watermark. The results listed in Table 4.3 indicate that the watermarking technique is robust to common signal processing attacks such as compression, echo addition and equalization with poor detection results for low pass filtering. This technique can be used for covert communication. One disadvantage of this technique is that the technique is non blind meaning that it requires original host audio signal to recover the watermark.

To develop the blind watermarking technique and to increase the detection performance of added copy right information we embed the data using spread spectrum method. The spread spectrum based adaptive techniques are proposed in chapter 5. From the test results in table 5.2 it is observed that non blind technique has better SNR compared to the blind detection scheme but it requires the original audio signal to recover the watermark. As in case of non blind techniques number of modifications made to embed the watermark bit is less as compare to the blind technique. In non blind as well as in blind techniques only one bit of information is added in one segment of host audio. To embed one bit of information we modify only one sample in the host audio segment in case of non blind technique, where as we modify each and every sample of host audio to implement blind watermarking technique.

In table 5.2 the results obtained for the proposed blind technique implemented in DWT/LWT domain are also presented. Though the SNR in these cases is below 20 dB the listening test confirms that there is no perceptual difference between the original watermark and the recovered watermark. The BER test between the original watermark and recovered watermark indicate that DWT based blind detection technique is slightly more robust than LWT based blind detection technique.

To make the scheme adaptive we compute the scaling parameter $\alpha(k)$ for each segment by making assumption of the expected SNR between the original segment coefficients and the modified segments coefficients. The selection criteria for the value of SNR in computation of $\alpha(k)$ and the selection criteria for segment length is decided based on the results presented in table 5.3. From the table 5.3 it is clear that the optimized results are obtained for segment length 256 and SNR between 40 – 60
dB. To provide the security to the system and to make the system secure the PN sequence is used as a secret key to embed the watermark. The embedded watermark cannot be recovered without the knowledge of the PN sequence used.

It is also observed that the SNR between original signal and watermarked signal is improved by embedding the watermark in DWT-DCT domain, DWT transform followed by DCT transform of LL₃ (3rd level low frequency) wavelet coefficients. By computing the DCT of 3-level DWT coefficients we can track the required frequency band to embed the information, also DCT has better signal compacting ability for smaller segment signals. This scheme proposed in section 5.4 provides better SNR compared to other two techniques implemented in chapter 5 and is also robust to various signal processing attacks. To embed the data using spread spectrum method we strongly recommend to use DWT-DCT domain to increase the imperceptibility and to obtain the better robustness test. To add the security and to further improve the robustness results the cyclic coding is used. The watermark bits are encoded using cyclic coder before embedding into host audio. At the receiver side the cyclic decoder is used to decode the watermark. Cyclic coding and decoding corrects the one bit errors generated during the watermark recovery. Due to encoding of watermark the opponent will not come to know the statistical behavior of watermark signal and hence can not guess the watermark from the statistical behavior of the audio signal. The results of this scheme are presented in table 5.6 and 5.7 using (6,4) and (7,4) cyclic coder respectively. Since our main goal of watermarking is to increase the robustness and detection performance we preferred to use (7, 4) cyclic coder compared due its superiority to correct errors improving the bit error rate.

Schemes based on patch work algorithm are proposed in chapter 6 in different transform domains. It is observed that this scheme is more imperceptible than the spread spectrum technique. The obtained SNR between the original signal and watermarked signal is increased for this case. The maximum value of SNR obtained using this scheme is 61.0525dB for harmonium signal and 44.5607 for song signal. This is obtained due to the smaller amount of $\delta$ (discrimination parameter) used to embed the information in this scheme. Also we make the modification of the segments if the required condition is not satisfied. Since the less number of modifications are done to embed the watermark this scheme provides better
imperceptibility than the Spread spectrum based method. The results provided in table 6.1, 6.2 and 6.4 again confirm that DWT-DCT domain is the more suitable domain to embed the information. The schemes implemented in this chapter calculate the adaptive scaling parameter in each subsection/GOS preserving the imperceptibility of the watermarked signal and providing good robustness results. The robustness results for the scheme proposed in chapter 5 and chapter 6 indicate that the scheme proposed in chapter 5 is more robust than the scheme proposed in chapter 6.

Chapter 7 proposes the intelligent encoder decoder models of the schemes implemented in chapter 5 and chapter 6. To make the models intelligent robust and secure we added the following features in the proposed model. i) We added synchronization pattern to indicate the start of watermark in the audio, ii) The time diversity is employed to improve robustness. iii) Encoded the watermark using cyclic coder. In both the models watermark is embedded adaptively meaning that discrimination factor used to embed each bit is varied according to the segment characteristics. The observed test results are significant even in timescale modification, low pass filtering. The models we propose are able to embed 1024 bits in 6.5 sec duration signal preserving the imperceptibility of the signal.

The watermark is repeatedly embedded in a longer audio signal and observed the recovery of the same. It is observed that after various attack at least one out of five watermarks embedded provide the minimum BER result. In addition, it is clear that the introduction of the attack characterization module additionally improved the extraction reliability of both algorithms, decreasing the bit error rate, most discernibly in the presence of time scale modification; low pass filtering, echo addition and equalization. From the results presented in this chapter it is again confirmed that the SS based method is more robust than the method based on patch work algorithm. The SS based algorithm obtained high detection robustness and increasing the perceptual transparency of the watermarked signal. Time required to embed and recover the watermark from SS based scheme is 21.131 sec. Time required to embed and recover the watermark from GOS based scheme is 24.401 sec.
8.2. Main contribution of the present research

1. Audio watermarking scheme is proposed to embed an audio watermark in the audio signal.
2. Adaptive blind watermarking algorithms based on SNR are developed using Spread spectrum technique.
3. Spread spectrum based techniques are implemented in different transform domains and recommend using DWT-DCT domain as the suitable domain to imperceptibly embed the watermark.
4. Cyclic coder and attack characterization by diversity is used to increase the robustness of the scheme.
5. Synchronization pattern is added to track the watermark.
6. New intelligent encoder and decoder model is proposed for an audio watermarking system using Spread Spectrum method.
7. Blind watermarking algorithms based on GOS modification are developed in different transform domain.
8. Cyclic coder and attack characterization by diversity is employed to increases the robustness.
9. Synchronization pattern is added to track the watermark.
10. New intelligent encoder and decoder model is proposed for an audio watermarking system using GOS method.

8.3. Future scope

The research in watermarking is progressing along two paths while the new algorithms of watermarking are developed. Researchers are working on attacks on the watermarked signals. Proposing the new attacks and suggesting the counter attack is one of the hot areas of watermarking research. One can work on attacks to propose new attack for the existing algorithms and suggest the counter measures to be taken to survive against that attack. The researchers can work on setting a buyer seller protocol for watermarking techniques. The algorithms can be developed in DWT-DCT domain to meet the requirement of imperceptibility and robustness at the same time. Cryptographic methods can be employed to provide the security to the developed
watermarking technique. Proposing asymmetric watermarking method is also appreciable in the field of watermarking.