Chapter 1

Introduction
INTRODUCTION

The last two decades has seen remarkable advancement in digital communication and computer technology. The advantages they offer are efficient transmission of data, high computing power, availability of high bandwidth, easy editing of digital contents, etc. It is now easy to copy digital content without any loss in the quality of the digital media. The progress in this technology has also brought some problems beside its advantages. The problem of ease to copy a digital content, edit and transfer, it can violate copyright protection. Digital watermarking has been proposed as a solution to prove ownership of digital data [1]. A watermark data (an additional signal) is embedded into the original data (host signal) in such a way that it remains present as long as the perceptible quality of the content of host signal is at an acceptable level. The owner of the original data proves his/her ownership by extracting the watermark data from the watermarked content (watermarked signal) in case of multiple ownership claims.

1.1 Overview

The techniques used for data security are cryptography, steganography and watermarking. Cryptography deals with securing contents of a message (host signal), after encryption the message looks like noise and is useless. However, encryption systems do not completely solve the security problem; because once decryption is performed, there is no control on dissemination of the data [2], [3]. Hence, a technique is required which always provide security to host signal. Steganography and watermarking are regarded as the techniques which give protection to host signal all the time. The basic idea of steganography is to embed a secret message in a media which is interpreted by the intended user only. Steganography deals with concealing the message, while watermarking has an additional requirement of securely concealing the message, such that the message cannot be tampered. A good steganographic system can embed large amount of information with no perceptual degradation to the multimedia data, but a good watermarking system would embed information that cannot be altered or removed without making the multimedia signal unusable. A watermarking system involves trade off between imperceptibility, robustness and embedding capacity [2]. It consists of two steps, viz. watermark
embedding and watermark detection/extraction. Encryption and watermarking techniques are shown in Figure 1.1. Basic block diagram of watermark embedding and detection is shown in Figure 1.2. Encryption key is a secret which is used in cryptography to make hidden information more secure. The watermark data may be a random number that is generated using a secret key which is known as seed of watermark. Embedding is a process by which watermark data is fused with the original signal (also known as host signal) to give watermarked signal. Detection process checks the presence of watermark data in the watermarked signal but extraction process finds the watermark data from the watermarked signal. User keys are secret which are used for watermark embedding. These keys may be watermark length, watermark location, watermark scaling factor etc.

![Figure 1.1](image)

**Figure 1.1** Illustration of (a) Cryptography (b) Watermarking techniques applied on images.
1.1.1 Applications of Watermarking

The main motivation behind the digital watermarking is copyright protection, but it can also be used for content authentication, broadcast monitoring, fingerprinting, and covert communication [4]-[7].

The application of watermarking for copyright protection is to evade other parties from claiming the copyright of digital media. It is done by embedding additional information (watermark data) that identifies the copyright owner of the digital media. The content owner is recognized by his signature which can be embedded as a watermark data.

Content authentication [4]-[5] is a detection process to ascertain whether the contents of a digital media have changed. As a solution, a fragile watermark data [6]-[7] embedded to the digital content (host signal) indicates whether the host signal has been altered. If any tampering has occurred in the host signal, the change will also occur in the recovered/detected watermark data. Content authentication can also provide information about any part of the host signal that has been altered.
By embedding watermark data into commercial advertisements, it can be monitored whether the advertisements are broadcast at the correct instants by means of an automated system [4]-[5]. The system receives the broadcast and searches these watermark data, identifying where and when the advertisement has to be broadcast.

Fingerprinting is an approach to trace the source of illegal copies [4]-[5]. The owner of the digital content (host signal) may embed different watermark data in the copies of digital content customized for each recipient. In this manner, the owner can identify the customer by extracting the watermark data in the case the host signal is supplied to third parties.

Secret communication is another possible application of digital watermarking [4]-[5]. A watermark data can be embedded imperceptibly to a host signal to communicate information from sender to an intended receiver while maintaining low probability of intercept by other unintended receivers.

1.1.2 Requirements for Watermarking

The requirements for an effective watermarking scheme are imperceptibility, robustness to intentional or unintentional signal processing operations and embedding capacity. The efficiency of a digital watermarking process is evaluated according to the properties of perceptual transparency (imperceptibility), robustness, embedding capacity, computational cost, recovery of data with or without access to the original host signal etc. [4], [5], [8]-[14], [16].

Imperceptibility: A watermark is called imperceptible if the original host signal and its watermarked version (watermarked signal) is perceptually indistinguishable. The watermarks do not create visible artifacts in still images, alter the bit rate of video or introduce audible artifacts in audio signals. Imperceptibility for images and video signals is known as invisibility, but for audio and speech signals, it is known as inaudibility. The imperceptibility of the watermark data is tested by means of subjective experiments [15] such as Mean Opinion Score (MOS) measurement through listening tests for audio and objective tests such as Signal-to-Noise Ratio (SNR), and Objective Difference Grade (ODG) measurements. The
imperceptibility of images can be measured by using objective tests such as Peak SNR (PSNR) and Mean Square Error (MSE).

**Robustness**: Robustness to signal processing operations refers to the ability to detect/extract the watermark data, after the watermarked signal has passed through various signal processing operations. Robustness of a watermarking scheme can vary from one signal processing operation to another. Depending on the application, the digital watermarking technique can support different levels of robustness against changes made to the watermarked content. If digital watermarking is used for copyright owner identification, then the watermark data has to be robust against any modifications.

**Embedding capacity**: The number of watermark hits embedded in a host signal without affecting its imperceptibility is known as embedding capacity. The embedding capacity is also known as payload.

### 1.2 Digital Watermarking of Multimedia Data

Digital watermarking is a technology that is used for the protection of any multimedia data such as text, audio, images and video. In this section we briefly discuss the watermarking methodology for each of these contents briefly.

#### 1.2.1 Text Watermarking

Much of the early watermarking works were done in the area of text watermarking [17]-[19]. These techniques were devised for watermarking electronic versions of text documents such as portable document format (PDF) versions. Most of this work is based on hiding the watermark data into the layout and formatting of the document directly. Formatted text is probably the medium where watermarking can be easily attacked. If the watermark data is in the format, then it can obviously be removed by retyping the whole text using a new character font and a new format where retyping can be either manual or automated using optical character recognition (OCR).
1.2.2 Audio Watermarking

The research on audio watermarking has been focused on either direct watermarking of the audio signal or bit stream embedding where the audio is represented in a compressed format. The use of perceptual models is an important component in generating an effective and acceptable watermarking scheme for audio [19], [21]-[23]. The requirements for audio watermarking are same as requirements of watermarking for other media. The amount of information (watermark data) that can be embedded robustly and imperceptibly is much lower than for visual media (images and video) because audio signals are represented by much less samples per time interval. The problem in audio watermarking is that the human auditory system (HAS) is much more sensitive than the human visual system (HVS) and inaudibility for audio signals is much more difficult to achieve than invisibility for images [21]. There are many watermarking techniques which are applicable to audio [21]-[23]. Three important techniques amongst them are echo coding [21], phase coding [21] and spread spectrum coding [16], [22], [23].

1.2.3 Image Watermarking

Most watermarking research and publications are focused on images [5], [8], [20], [24], [25]. The reason might be that there is a large demand for image watermarking products due to the fact that there are many images available freely on the World Wide Web (WWW) which need to be protected. Several watermarking methods are in fact very similar and differ only in watermark signal design, embedding method and detection/extraction method. Watermarking of images can also be performed by using two dimensional (2D) versions of various transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fractional Fourier Transform (DFRFT) etc.

1.2.4 Video Watermarking

Video sequence consists of a series of consecutive and equally time-spaced still images. Thus, the general problem of watermarking seems very similar for images and video sequences. The idea of image watermarking is directly applicable to video sequences. However, additional requirements for video watermarking are low
complexity, constant bit rate and compressed domain processing. Some video watermarking approaches have already been earlier mentioned by several researchers [19]-[20], [24].

1.3 Objectives of the Thesis

The main objective of this thesis is to develop digital watermarking schemes for multimedia data such as audio signals and images. It can be summarized as follows:

1. To simulate and analyze the performance of a digital audio watermarking scheme using chirp signals as watermark. This scheme is named as Chirp-Based Digital Audio Watermarking (CB-DAWM) which is used for single-level and multi-level embedding.
2. To propose, simulate and evaluate the performance of a Wavelet-Based Digital Audio Watermarking (WB-DAWM) scheme for single-level and multi-level embedding.
3. To simulate and examine the performance of a digital image watermarking scheme in Discrete Fractional Fourier Transform (DFRFT) domain.
4. To propose and simulate a non-blind watermark extraction scheme in DFRFT domain for image watermarking.
5. To propose, simulate and demonstrate the performance of a digital image watermarking scheme in combined DWT and DFRFT domains.

1.4 Outcome and Main Contributions of Thesis

In the present work, following are the main contributions:

- A CB-DAWM scheme is presented, simulated and its performance evaluated for single-level and multi-level embedding. Three types of chirp signals, linear, quadratic and logarithmic have been studied. A logarithmic chirp is preferred to encode watermark sequence which is embedded in CB-DAWM scheme because it gives best watermark extraction performance without attack (average BER=0) without affecting imperceptibility of watermarked audio signal. The scheme is found to be robust against most of the audio
watermarking attacks such as low-pass filtering, up-sampling by interpolation, down-sampling by decimation, re-sampling, amplitude scaling, and MP3 compression. This scheme shows limited robustness under high-pass filtering, band-pass filtering and AWGN attacks. This scheme is not resilient against cropping attack. The multi-level CB-DAWM scheme offers 39.68% increased payload capacity compared to single-level CB-DAWM scheme and multiple-level robustness. The multiple-level robustness can be used to embed information having different levels of security into a host audio signal.

- Another audio watermarking scheme using wavelet function, i.e. Wavelet-Based Digital Audio Watermarking (WB-DAWM) scheme is proposed, simulated, evaluated and compared with CB-DAWM scheme. In this scheme, watermark sequence (data) is encoded using ‘Daubechies’ mother wavelet function. This scheme is simulated and evaluated for single-level and multi-level watermark embedding. This watermarking scheme is resilient against most of the audio watermarking attacks such as low-pass filtering, up-sampling, down-sampling, re-sampling, amplitude scaling and MP3 compression. It offers limited robustness against high-pass filtering, band-pass filtering, and AWGN attacks and is not robust under cropping attack. The proposed WB-DAWM scheme is more imperceptible i.e., perceptually transparent compared to CB-DAWM schemes because average ODG obtained for WB-DAWM schemes are very near to zero compared to CB-DAWM schemes. It is also found to be more robust against high-pass filtering, band-pass filtering, and AWGN attacks compared to corresponding CB-DAWM schemes. The proposed single-level WB-DAWM scheme offers 19.05% increased payload capacity with improved imperceptibility compared to single-level CB-DAWM scheme.

- A digital image watermarking scheme in the DFRFT domain has been proposed. In order to extract embedded watermark, a non-blind watermark extraction scheme in DFRFT domain is proposed. Various simulation results to evaluate the performance of this scheme under different attacks have been studied and analyzed. This watermarking scheme shows imperceptibility feature and is compared with existing DWT-based Kundur’s watermarking method. It is evident from the results that this method offers better robustness.
than Kundur's method for some of the attacks such as salt and peppers noise, median filtering, AWGN, and JPEG compression. This watermarking scheme is more secure than other similar schemes because watermark can be embedded using different DFRFT powers as secret keys, without its knowledge watermark can not be extracted.

- A digital image watermarking scheme in combined DWT and DFRFT domains has been proposed for one-level and two-level DWT decomposition with non-blind watermark extraction. Various simulation results of this scheme under different watermark attacks have been reported. There is a problem in DFRFT-based watermarking scheme that it offers higher BER in watermark extraction for attacks such as histogram equalization and sharpening. The proposed watermarking technique improves the watermark extraction performance for these attacks.

### 1.5 Organization of Thesis

In Chapter 2, various digital watermarking techniques for audio signals and images will be reviewed in brief.

A digital audio watermarking scheme using chirp signal as a watermark, CB-DAWM, has been presented in Chapter 3 and its simulation results under various audio watermarking attacks have been discussed. In order to evaluate robustness of this scheme various audio watermarking attacks such as low-pass filtering, high-pass filtering, band-pass filtering, up-sampling by interpolation, down-sampling by decimation, re-sampling, amplitude scaling, addition of white Gaussian noise, cropping and MP3 compression are applied on watermarked audio signals. This chapter also presents simulation results for single-level and multi-level watermark embedding and discusses results against various watermarking attacks.

Chapter 4 proposes single-level and multi-level digital audio watermarking schemes using wavelet function. It also presents simulation results under various audio watermarking attacks and compares it with the corresponding CB-DAWM schemes.
In Chapter 5, digital image watermarking in DFRFT domain has been developed, simulated and its robustness is evaluated under various image watermarking attacks such as median filtering, salt and peppers noise, histogram equalization, JPEG compression, low-pass filtering, addition of white Gaussian noise and sharpening.

Digital image watermarking scheme using combination of DWT and DFRFT transforms has been given in Chapter 6. This scheme is simulated using one-level and two-level DWT decomposition and DFRFT, and its watermark extraction performance in terms of Bit Error Rate (BER) is measured under various image watermark attacks.

Finally, Chapter 7 gives conclusion of the simulation results obtained in Chapters 3 to 6 and provides some directions for further work.