Preface

In this digital era, the ubiquitous network environment has promoted the rapid delivery of digital multimedia data. Users are eager to enjoy the convenience and advantages that networks have provided. Meanwhile, users are eager to share various media information in a rather cheap way without awareness of possibly violating copyrights. In view of these, digital watermarking technologies have been recognized as a helpful way in dealing with the copyright protection problem in the past decade. Although digital watermarking still faces some challenging difficulties for practical uses, there are no other techniques that are ready to substitute it. In order to push ahead with the development of digital watermarking technologies, the goal of this book is to collect both comprehensive issues and survey papers in this field so that readers can easily understand state of the art in multimedia security, and the challenging issues and possible solutions. In particular, the authors that contribute to this book have been well known in the related fields. In addition to the invited chapters, the other chapters are selected from a strict review process. In fact, the acceptance rate is lower than 50%.

There are eight chapters contained in this book. The first two chapters provide a general survey of digital watermarking technologies. In Chapter I, an extensive literature review of the multimedia copyright protection is thoroughly provided. It presents a universal review and background about the watermarking definition, concept and the main contributions in this field. Chapter II focuses on the discussions of perceptual properties in image watermarking. In this chapter, a detailed description of the main phenomena regulating the HVS will be given and the exploitation of these concepts in a data hiding system will be considered. Then, some limits of classical HVS models will be highlighted and some possible solutions to get around these problems pointed out. Finally, a complete mask building procedure, as a possible exploitation of HVS characteristics for perceptual data hiding in still images will be described.

From Chapter III through Chapter V, audio watermarking plays the main role. In Chapter III, the main theme is to propose a methodology, including

performance metrics, for evaluating and comparing the performance of digital audio watermarking schemes. This is because the music industry is facing several challenges as well as opportunities as it tries to adapt its business to the new medium. In fact, the topics discussed in this chapter come not only from printed sources but also from very productive discussions with some of the active researchers in the field. These discussions have been conducted via e-mail, and constitute a rich complement to the still low number of printed sources about this topic. Even though the annual number of papers published on watermarking has been nearly doubling every year in the last years, it is still low. Thus it was necessary to augment the literature review with personal interviews. In Chapter IV, the aim is to provide a comprehensive survey and summary of the technical achievements in the research area of digital audio watermarking. In order to give a big picture of the current status of this area, this chapter covers the research aspects of performance evaluation for audio watermarking, human auditory system, digital watermarking for PCM audio, digital watermarking for wav-table synthesis audio, and digital watermarking for compressed audio. Based on the current technology used in digital audio watermarking and the demand from real-world applications, future promising directions are identified. In Chapter V, a method for embedding a customer identification code into multimedia data is introduced. Specifically, the described method, *active digital fingerprinting*, is a combination of robust digital watermarking and the creation of a collision-secure customer vector. There is also another mechanism often called *fingerprinting* in multimedia security, which is the identification of content with robust hash algorithms. To be able to distinguish both methods, robust hashes are called *passive fingerprinting* and collision-free customer identification watermarks are called *active fingerprinting*. Whenever we write fingerprinting in this chapter, we mean active fingerprinting.

In Chapters VI and VII, the media content authentication problem will be discussed. It is well known that multimedia authentication distinguishes itself from other data integrity security issues because of its unique property of content integrity in several different levels - from signal syntax levels to semantic levels. In Chapter VI, several image authentication issues, including the mathematical forms of optimal multimedia authentication systems, a description of robust digital signature, the theoretical bound of information hiding capacity of images, an introduction of the *Self-Authentication-and-Recovery Image* (SARI) system, and a novel technique for image/video authentication in the semantic level will be thoroughly described. This chapter provides an overview of these image authentication issues. On the other hand, in the light of the possible disadvantages that watermarking-based authentication techniques may result in, Chapter VII has moved focus to labeling-based authentication techniques. In labeling-based techniques, the authentication information is conveyed in a separate file called *label*. A label is additional information associated with

the image content and can be used to identify the image. In order to associate the label content with the image content, two different ways can be employed and are stated as follows.

The last chapter describes watermarking methods applied to those media data that receives less attention. With the proliferation of digital media such as images, audio, and video, robust digital watermarking and data hiding techniques are needed for copyright protection, copy control, annotation, and authentication of document images. While many techniques have been proposed for digital color and grayscale images, not all of them can be directly applied to binary images in general and document images in particular. The difficulty lies in the fact that changing pixel values in a binary image could introduce irregularities that are very visually noticeable. Over the last few years, we have seen a growing but limited number of papers proposing new techniques and ideas for binary image watermarking and data hiding. In Chapter VIII, an overview and summary of recent developments on this important topic, and discussion of important issues such as robustness and data hiding capacity of the different techniques is presented.