Preface

As rapid and tremendous progress in information technology is constantly being made, and, while an enormous amount of media such as text, audio, speech, music, image and video can be easily exchanged through the Internet and other communication networks, information security issues such as copyright protection, integrity verification, authentication, and access control have became exceptionally acute. As a result, the subjects of security protection in multimedia distribution have been taken as one of the top research and development agendas for researchers, organizations, and governments worldwide. Especially after 1995, multimedia distribution became more and more popular with the achievements in multimedia technology and network technology. The malicious tampering of multimedia content, such as copy, forgery, modification, illegal distribution and so on, threatens multimedia related services. Thus, secure multimedia distribution becomes necessary and urgent.

There exists some solutions for information protection, such as cryptographic techniques. However, multimedia data are different from text or binary data because of such properties as large volumes, high redundancies, and real-time interactions. Thus, multimedia protection is different from binary/text data protection. Additionally, secure multimedia distribution is in close relation with several fields, including cryptography, multimedia processing, and network communication. These properties make secure multimedia distribution a challenging research topic that has attacted more and more researchers and engineers over the past decade.

Until recently, few handbooks mentioned secure multimedia distribution. To access the latest research related to the many disciplines of secure multimedia distribution, I decided to launch a handbook project where researchers from all over the world would assist me in providing the necessary coverage of each respective discipline in secure multimedia distribution. The primary objective of this project was to assemble as much research coverage as possible, related to the disciplines selected for this handbook by defining the technologies, terms, and acronyms related to each discipline, and providing the most comprehensive list of research references related to each discipline.

In order to provide the best balanced coverage of concepts and issues related to the selected topics of this handbook, researchers from around the world were asked to submit proposals describing their proposed coverage and the contribution of such coverage to the handbook. All proposals were carefully reviewed by the editor in light of their suitability, researcher's records of similar work in the area of the proposed topics, and the best proposal for topics with multiple proposals. The goal was to assemble the best minds in the information science and technology field from all over the world to contribute entries to the handbook. Upon the receipt of full entry submissions, each submission was forwarded to at least three expert external reviewers on a peer review basis. Only submissions with strong and favorable reviews were chosen as entries for this handbook. In many cases, submissions were sent back for several revisions prior to final acceptance. As a result, this handbook includes 27 chapters highlighting current concepts, issues, and emerging technologies. All entries are written by knowledgeable, distinguished scholars from many prominent research institutions in more than 10 countries.

The handbook is composed of three sections—Secure Distribution System, Key Technique, and Typical Application. The first section, Secure Distribution System, consists of the chapters describing various secure multimedia distribution systems. The secure distribution systems include:

- *Digital rights mangement for streaming media*. Streaming media is now the most popular manners for online live TV or film services. Compared with non-streaming manners, (e.g., ftp) streaming media has strict requirements in real-time operations. In this chapter, a discussion of some specific issues that arise in the context of streaming media are given, followed by the digital rights management (DRM) system for streaming media, which is different from traditional systems.
- *Digital rights mangement for mobile communication*. Two standards are formed to protect digital rights in mobile communications, they are the Open Mobile Alliance (OMA) Digital Rights Management (DRM) standard and the OMA Mobile Broadcast Services standard (BCAST). The former one specifies offers protection and secure access control for digital content. The latter one specifies the protected content delivery for mobile broadcast applications such as mobile TV. These two standards complement each other, enabling further functionalities and use cases. This chapter provides a technical overview of the OMA DRM and OMA BCAST standards.
- *Digital rights management for peer-to-peer content sharing*. Peer-to-peer (P2P) networks have proliferated and become ubiquitous. However, secure content sharing in P2P networks is still an open issue. This chapter focuses on developing a solution for distributing digital content in P2P networks in a way that established businesses and amateur artists alike can profit. This content distribution system employs digital rights management (DRM) technologies and is independent of the underlying P2P networks.
- *Access control for content distribution*. This chapter suggests DRM solutions based on secure hardware. Secure chips appear today in various form factors (smart cards, USB secure tokens, TPM, etc). They can be used to implement a Secure Operating Environment (i.e., a tamper-resistant storage and execution environment) in any device they are plugged in. This chapter will present different techniques that answer the three questions mentioned above, thanks to such Secure Operating Environment. Finally, the accuracy of these techniques will be illustrated through different commercial DRM scenarios and pervasive healthcare scenarios.
- *Secure video surveillance systems*. This chapter first investigates the advantages of the IP-based video-surveillance systems over the traditional analog ones. Then, it describes the technical challenges and the open research issues which still lack an ultimate solution that permits them to completely abandon the traditional analog technology. Finally, it proposes and verifies, by means of a case study, a methodology to address the design of video-surveillance systems in real deployment.

Section II, Key Technique, consists of the chapters introducing various techniques for secure multimedia distribution. The mentioned techniques include:

- *Key exchange protocol*. In secure communication, key exchange is one of the key techniques. Regarding fundamental protocols in cryptography, the Diffie-Hellman (Diffie and Hellman, 1976) public key exchange protocol is one of the oldest and most widely used in today's applications. This chapter describes the security problem in existing key exchange protocols, exposes the various concepts of security, and introduces a new statistical concept specifically designed to serve the assessment of the security of the exchange.
- *Secret sharing*. Secret sharing aims at distributing and sharing a secret among a group of participants efficiently. This chapter firstly proposes a plane-based access structure for secret sharing.

More specifically, if any two among a set of three participants in a graph contain an edge, these participants belong to a prohibited structure which is not able to recover the master key.

- *Multimedia authentication*. Multimedia community is moving from monolithic applications to more flexible and scalable proliferative solutions. Security issues such as access control and authentication of multimedia content, have been intensively studied in the literature. Two chapters aim to give the overview of multimedia authentication techniques. The first one aims to provide an overview of digital video authentication systems and a universal review of the associated methods. The second one describes a flexible stream authentication framework that allows the so called packet independent stream authentication schemes to make transcoding operations on the packets and commit the changes, which are not applicable in packet-based stream authentication schemes.
- *Information hiding*. Establishing hidden communication is an important subject of discussion that has gained increasing importance with the development of the Internet. Digital watermarking and steganography are two typical techniques of information hiding. Digital watermarking embeds some information into a cover media, and the embedded information can survive some operations on the cover media. Steganography is a method to hide data in a cover media so that other persons will not notice that such data is there. Stegoanalysis is the technique to attack a steganography method. There are 3 chapters that describe digital watermarking, steganography, and stegoanalysis, respectively.
- *Wireless video transmission*. For wireless multimedia transmission, the data volumes and error-robustness are two key issues. This chapter concetrates on two techniques, source coding and channel coding. Among them, the former one refers to the multimedia compression, while the latter one refers to error-correction coding.

The final section, Typical Application, consists of the chapters describing various applications based on secure multimedia distribution. The mentioned applications include:

- *Trusted multimedia goods creation*. Security in the value creation chain hinges on many single components and their interrelations. Trusted Platforms open ways to fulfill the pertinent requirements. This chapter gives a systematic approach to the utilization of trusted computing platforms over the whole lifecycle of multimedia products. This spans production, aggregation, (re)distribution, consumption, and charging. Trusted Computing technology as specified by the Trusted Computing Group, provides modular building blocks that can be utilized at many points in the multimedia lifecycle.
- *Copyright protection in mobile multimedia device*. In mobile multimedia device, video and audio data should be protected by lightweight schemes due to the energy-limitation of mobile devices. This chapter introduces an advanced encryption of MP3 and MPEG-4 coder with a quality degradation-based security model, which keeps format compliance, and obtains high-time efficiency though reducing the encrypted the volumes of multimedia contents.
- *Image steganography*. Steganography is the art of hiding secret data inside other innocent media file. Steganalysis is the process of detecting hidden data which are crested using steganography. Steganalysis detects stego-images by analyzing various image features between stego-images and cover-images. Therefore, it needs to have a system that develops more critical stego-images from which steganalysis cannot detect them. Two chapters propose two kinds of steganography methods. The first one is based on Genetic Algorithm (GA), and the second one is based on Structural Similarity Metric.

- *Secure sharing in Ad Hoc Networks*. Secure content sharing in self-organized networks is challenging. This chapter describes the background and framework of content distribution in P2P and ad hoc networks, summarizes the main security solutions proposed so far, and points out some open issues and emergent trends in this research area.
- *Multiple Description Coding based watermarking*. Multiple description coding (MDC) is a promising method for robust transmission of information over non-prioritized and unpredictable networks. It is also interesting to find that multiple description coding can be applied in multimedia watermarking. This chapter reviews the concept, design algorithms and some applications of multiple description coding, and the application of MDC in watermarking.
- *Fractal based secure image distribution*. A pioneer concept in which multiple images are simultaneously considered in the compression and secured distribution frameworks is revealed. This chapter proposes the so-called fractal mating coding scheme to successfully implement the joint image compression and encryption concept through a novel design in the domain pool construction. With the exploration of the intra- and inter-image similarity among multiple images, not only the coding performance can be improved, but also the secured image distribution purpose can be achieved.

The diverse and comprehensive coverage of multiple disciplines in the field of secure multimedia distribution in this authoritative handbook will contribute to a better understanding all topics, research, and discoveries in this evolving, significant field of study. Furthermore, the contributions included in this handbook will be instrumental in the expansion of the body of knowledge in this vast field. The coverage of this handbook provides strength to this reference resource for both secure multimedia distribution researchers and also decision makers in obtaining a greater understanding of the concepts, issues, problems, trends, challenges and opportunities related to this field of study. It is our sincere hope that this publication and its great amount of information and research will provide a scientifically and scholarly sound treatment of state-of-the-art techniques to students, researchers, academics, personnel of law enforcement, and IT/multimedia practitioners who are interested or involved in the study, research, use, design, and development of techniques related to secure multimedia distribution.

Shiguo Lian & Yan Zhang
Editors