Preface

In the last two decades, the development of information and communication technology (ICT) and multimedia processing techniques has revolutionized the ways we create, exchange, and manipulate information. Most people, if not all, with access to computers and the Internet, can not only share information instantly at insignificant cost, but also creatively produce their own media of various forms, such as text, audio, speech, music, image, and video. This wave of ICT revolution has undoubtedly brought about enormous opportunities for the world economy and exciting possibilities for every sector of the modern societies. Educators are now equipped with *e-tools* to deliver their knowledge and expertise to the remote corners of the world with Internet access. Harnessing these ICT resources, *e-governments* can now provide various aspects of *e-services* to the people. Willingly or reluctantly, directly or indirectly, we are all now immersed in some way in the cyberspace full of *e-opportunities* and *e-possibilities* and permeated with data and information. However, this type of close and strong interweaving poses concerns and threats. When exploited with malign intentions, the same tools provide means for doing harms at a colossal scale. These concerns create anxiety and uncertainty about the reality of the media we deal with.

In response to these issues, the last decade has seen the emergence of the new interdisciplinary field of multimedia forensics and security, which aims at pooling expertise in various areas, such as signal processing, information theory, cryptography, and so forth to combat the abuses of ICT and multimedia techniques. In particular, digital watermarking schemes have been proposed to meet copyright protection needs, for example, ownership identification, copy control, transaction tracking, and to deal with content authentication and integrity verification. Challenged by its competing steganalytical techniques, steganographic methods have been developed and are being constantly improved for data hiding and embedding applications. Multimedia forensic techniques have also been studied and derived for providing evidences to aid with resolving civil and criminal court cases. Added to the excitement of the races between new measures and countermeasures in this new area is the difficulties in striking a balance between conflicting requirements. For example, in the context of digital watermarking, high robustness is usually gained at the expense of high distortion, while, in the context of steganography, low distortion is, most of the times, achieved at the cost of low payload.

This book aims to create a collection of quality chapters on information hiding for multimedia forensics and security contributed by leading experts in the related fields. It embraces a wide variety of aspects of the related subject areas covered in 16 chapters and provides 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 multimedia forensics and security.

This book consists of three main components. The first component, comprised of Chapters I to VII, aims at dissemilating the idea of digital watermarking and its applications to multimedia security in general and copyright protection in particular. The second component, which covers Chapters VIII to XIII, is concerned with the two competing arts of steganography and steganalysis. The third component, comprising Chapters XIV to XVI, deals with methods that harness the techniques of data hiding and cryptography for the applications of multimedia forensics.

Chapter I, *Authentication Watermarkings for Binary Images*, presented by Hae Yong Kim, Sergio Pamboukian, and Paulo Barreto, is concerned with a class of data hiding techniques and the analysis of which of them are suitable for authenticating binary images. Ways of detecting and localising tamper, aiming at revealing the attacker's possible intention, are described. A new irreversible scheme for authenticating JBIG2-compressed binary images and a new reversible algorithm for authenticating general binary images are presented.

In Chapter II, *Secure Multimedia Content Distribution Based on Watermarking Technology*, Shiguo Lian defines the performance requirements of watermarking-based multimedia distribution schemes for multimedia communication applications and reviewed a number of related schemes, with their characteristics and limitations discussed. A new scheme combining fingerprinting and encryption, which realises both confidentiality protection and copyright protection, is then presented to address the issues, such as traitor tracing, robustness, and imperceptibility, surrounding multimedia distribution and to meet the defined requirements.

In Chapter III, *Digital Watermarking in the Transform Domain with Emphasis on SVD*, Maria Calagna first introduces the main mathematical tools, such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) and their applications in digital watermarking and then places emphasis on presenting and comparing related work on SVD watermarking. To overcome the flaws found in the watermark extraction component of some discussed SVD-based schemes, Calagna proposes a new SVD-based scheme for watermarking geographical and spatial images exchanged among a group of GIS users.

In Chapter IV, *Digital Video Watermarking and the Collusion Attack*, Roberto Caldelli and Alessandro Piva present a taxonomy of video watermarking techniques according to data formats and signal processing tools employed for implementation. The idea and types of collusion attacks are then analysed. In particular, the effects of applying temporal frame averaging (TFA) to the watermarking systems implemented with spread spectrum (SS) and spread transform dither modulation (STDM) are studied in great details. This chapter identifies the main advantages and limitations of the SS- and STDM-based schemes in the face of TFA collusion attack.

Chapter V, *A Survey of Current Watermarking Synchronization Techniques,* authored by Natasa Terzija, deals with the synchronization issue of watermark detection under the threat of geometric distortions, such as translation, cropping, rotation, scaling, affine transformation, projective transformation, and so forth. Watermark synchronization has been an active research area in the last 10 years because even a minor geometric distortion of the watermarked image can dramatically reduce the watermark detectors' the ability to detect the presence of the watermark, that is, the watermark detector can lose the *synchronization*. Terija gives an overview of different techniques including image registration techniques, the exhaustive search, periodical sequences, the use of synchronization marks, content-based approaches, and then concludes that the existing techniques can only provide partial robustness against geometrical distortions and more efforts are yet to be made before proper solutions can be put in place.

In Chapter VI, *On the Necessity of Finding Content before Watermark Retrieval—Active Search Strategies for Localizing Watermarked Media on the Internet*, Martin Steinebach and Patrick Wolf state that embedding digital watermark for copyright protection is only a passive protection and, to complete the protection, an active mechanism capable of finding potentially watermarked media that have been distributed is needed before the watermark extraction can actually be carried out to help fight illegal copies. This chapter discusses important issues regarding the search for watermarked content on the Internet and introduces strategies and approaches for retrieving watermarks from the Internet with the help of a media search framework.

In Chapter VII, *Statistical Watermark Detection in the Transform Domain for Digital Images*, Fouad Khelifi, Fatih Kurugollu, and Ahmed Bouridane view the problem of multiplicative watermark detection in digital images as a binary decision where the observation is the possibly watermarked samples that can be thought of as a noisy environment in which a desirable watermark may exist. They investigate optimum watermark detection from the viewpoint of decision theory. Different transform domains are considered with generalized noise models and the effects of the watermark strength on both the detector performance and the imperceptibility of the host image are studied.

Chapter VIII, *On Noise, Steganography, and the Active Warden*, marks the beginning of the second component of this book. In the face of the fact that many data hiding techniques give rise to changes to the cover media that appear to be noise, Christopher Smith and Sos Agaian state in this chapter that steganography can be defined in terms of adding some type of artificial noise and review a series of state-of-the-art, noise-like steganographic schemes. The authors also present information for the reader to understand how noise is unintentionally and intentionally exploited in information hiding and show how passive and active steganalysis can be applied to attack steganographic schemes. Results of using advanced clean image estimation techniques for steganalysis under the active warden scenario are also presented.

Among the many conflicting requirements of digital watermarking and data hiding, visibility (or embedding distortion inflicted on the host media by the marking process) is of significant concern. Chapter IX, *Visibility Control and Quality Assessment of Watermarking and Data Hiding Algorithms*, contributed by Patrick Le Callet and Florent Autrusseau, deals with both the subjective and objective quality assessment of images and video in the context of digital watermarking and data hiding applications. The deficiencies of some quality metrics for data hiding purpose are highlighted. Subjective experimental protocols are conducted. A quality benchmark aiming at identifying the objective metrics among many that best predicts subjective scores is presented.

In Chapter X, *Computational Aspects of Digital Steganography*, Maciej Liśkiewicz and Ulrich Wölfel focus on the formal analysis of the security of steganographic schemes from a computational complexity point of view and provide models of secure schemes that make realistic assumptions of limited computational resources of involved parties. This allows the reader to look at steganographic secrecy based on reasonable complexity assumptions similar to the ones commonly accepted in modern cryptography. The authors expand the analyses of stego-systems beyond security aspects that practitioners find difficult to implement to the tractability aspects, that is, the question *why* such schemes are so difficult to implement and what makes these systems different from practically used ones. These questions concern the maximum achievable security for different steganography scenarios and the limitations in terms of time efficiency associated with stego-systems that achieve the highest levels of security.

In Chapter XI, *On Steganalysis and Clean Image Estimation*, Christopher Smith and Sos Agaian expand on the idea of exploiting the noise-like qualities of steganography and discuss its competing technology of steganalysis, the art and science of detecting hidden information in media. They define the art of steganalysis in terms of detecting and/or removing a particular type of noise and review a series of steganalysis techniques, including blind steganalysis and targeted steganalysis methods, which either implicitly or explicitly use a clean image model to begin the detection of hidden data. From these ideas of clean image estimation, the steganalysis problems faced by the passive warden are formulated as a three-stage process of estimation, feature extraction, and classification (the EFC formulation).

Chapter XII, *Steganalysis: Trends and Challenges*, by Hafiz Malik, R. Chandramouli and K. P. Subbalakshmi provide a detailed overview of the state-of-the-art techniques in steganalysis. The performance of existing steganalysis techniques are compared based on critical parameters such as the hidden message detection probability; the accuracy of the hidden message length and secret key estimates; and the message recovery rate. They also provide an overview of some existing shareware/freeware steganographic tools and highlight the pros and cons of existing steganalysis techniques. The growing gap between recent developments in the steganographic research and the state-of-the-art of steganalysis are also discussed.

Chapter XIII, *Benchmarking Steganalysis*, by Andrew Ker, discusses how to evaluate the effectiveness of steganalysis techniques. In the steganalysis literature, numerous different methods are used to measure detection accuracy, with different authors using incompatible benchmarks. Thus, it is difficult to make a fair comparison of competing steganalysis methods. This chapter argues that some of the choices for steganalysis benchmarks are demonstrably poor, either in statistical foundation or by over-valuing irrelevant areas of the performance envelope. Good choices of benchmarks are highlighted, and simple statistical techniques demonstrated for evaluating the significance of observed performance differences. It is hoped that this chapter will make practitioners and steganalysis researchers better able to evaluate the quality of steganography detection methods.

In the light of the fact that digital photographs are becoming a more common form of evidence used in criminal investigation and civil court of laws, Chapter XIV*, Digital Camera Source Identification Through JPEG Quantisation*, presented by Matthew Sorell, is concerned with the identification of the make, the model series, and the particular source camera of a particular digital photograph. Characteristics of the camera's JPEG coder are exploited to demonstrate the possibility of such identification and the likelihood of detecting sufficient residual characteristics of the original coding even when an image has subsequently been recompressed, allowing the investigator to narrow down the possible camera models of interest in some cases. Three sets of techniques, classified according to the employed data, namely, metadata, bullet scratches/fingerprinting, and manufacturer specific information, for camera identification are discussed.

Chapter XV, *Traitor Tracing for Multimedia Forensics*, authored by Hongxia Jin, reviews potential pirate attacks on multimedia content distribution systems and discusses how traitor tracing techniques can be used to defend against those attacks by tracing the attackers and colluders involved in the piracy. This chapter is also concerned with business scenarios that involve one-way digital content distribution and a large set of receiving users. It shows how to address many overlooked practical concerns and brings first hand experience on bringing this technology to practice in the context of new industry standard on content protection for next generation high-definition DVDs.

In Chapter XVI, *Efficient Transparent JPEG2000 Encryption*, given the fact that many multimedia applications such as TV new broadcasting are designed for the *try and buy* scenario, and thus require security on a much lower level than that of copyright protection applications, Dominik Enge, Thomas Stütz, and Andreas Uhl review several selective or partial encryption schemes and investigate two different techniques for transparent/perceptual encryption of JPEG2000 files or bitstreams in the context of digital right management (DRM) schemes. These methods are efficient in terms of the computational costs of encryption. A classical bitstream-based approach employing format-compliant encryption of packet body data is compared against a compression-integrated technique, which uses the concept of wavelet packet transform.

***Chang-Tsun Li** received the BS degree in electrical engineering from Chung-Cheng Institute of Technology (CCIT), National Defense University, Taiwan, in 1987, the MS degree in computer science from U. S. Naval Postgraduate School, USA, in 1992, and the PhD degree in computer science from the University of Warwick, UK, in 1998. He was an associate professor of the Department of Electrical Engineering at CCIT during 1999-2002 and a visiting professor of the Department of Computer Science at U.S. Naval Postgraduate School in the second half of 2001. He is currently an associate professor of the Department of Computer Science at the University of Warwick, UK, Editor-in-Chief of the International Journal of Digital Crime and Forensics (IJDCF)and Associate Editor of the International Journal of Applied Systemic Studies (IJASS). He has involved in the organisation of a number of international conferences and workshops and also served as member of the international program committees for several international conferences. His research interests include multimedia security, bioinformatics, image processing, pattern recognition, computer vision and content-based image retrieval.*