Preface

The unprecedented development and convergence of information and communication technology (ICT), computational hardware, and multimedia techniques witnessed in the last decade have revolutionized how people exchange information, learn, work, interact with others and go about daily life at the personal level. At the organisational and global level, these techniques have enabled a wide range of services across national borders through e-commerce, e-business, and e-governance powered by the existing IT infrastructures and emerging cloud computing. 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. Willingly or reluctantly, directly or indirectly, we are all now immersed in a cyberspace, full of e-opportunities and e-possibilities, and permeated with rich multimedia and information. However, this type of close and strong interweaving also causes concerns and poses threats. When exploited with malign intentions, the same technologies provide means for doing harms at colossal scale. The £1.3 billion loss of the Swiss banking group, UBS, due to unauthorised trading by a rogue trader in its investment bank is just one of many typical examples. These concerns create anxiety and uncertainty about the reality of the information and business we deal with, the security the information infrastructures we are relying on today and our privacy. Due to the rise of digital crime and the acute need for methods of fighting these forms of criminal activities, there is an increasing awareness of the importance of digital forensics and investigation. As a result, the last decade has also seen the emergence of the new interdisciplinary research field of digital forensics and investigation, which aims at pooling expertise in various areas to combat the abuses of the ICT facilities and computer technologies.

The primary objective of this book is to provide a media for advancing research and the development of theory and practice of digital crime prevention and forensics. This book embraces a broad range of digital crime and forensics disciplines that use electronic devices and software for crime prevention and investigation, and addresses evidential issues. It encompasses a wide variety of aspects of the related subject areas 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 research, use, design, and development of techniques related to digital forensics and investigation. This book is divided into five main sections according to the thematic areas covered by the contributed chapters.

- Section 1. Multimedia Forensics Based on Intrinsic Data
- Section 2. Multimedia Security Based on Extrinsic Data
- Section 3. Applications of Cryptography in Digital Forensics

- Section 4. Applications of Pattern Recognition and Signal Processing Techniques to Multimedia Forensics and Security
- Section 5. Digital Evidence

It should be noted that these five parts are closely related. Such a division is only meant to provide a structural organisation of the book to smooth the flow of thoughts and to aid the readability, rather than proposing a taxonomy of the study of digital forensics.

Section 1. Multimedia Forensics Based on Intrinsic Data

This section of the book is concerned with the use of intrinsic data (i.e., information extracted from multimedia content) in multimedia forensic investigations such as source device identification, device linking, and content integrity verification. Usually the process of acquiring an image with an ordinary digital camera is as follows. The light from the scene enters a set of lenses and passes through an anti-aliasing filter before reaching a colour filter array (CFA) that is intended to admit one of the red (R), green (G) and blue (B) components of the light per pixel for the following semi-conductor sensor to convert the signal into electronic form. A de-mosaicing process is subsequently carried out to get the intensities of the other two colours for each pixel by interpolating the colour information within a neighbourhood. A sequence of image processing operations, such as colour correction, white balancing, Gamma correction, enhancing, JPEG compression, et cetera then take place before the photo is saved in the storage medium. The hardware or software used in each stage in the image acquisition process may leave unique traces in the content, which can lead to the identification of the imaging device. As such, to help with forensic investigations, researchers have proposed ways of identifying and linking source devices, classifying images and verifying the integrity of images based on the detection of existence or local inconsistencies of device attributes or data processing related characteristics, such as sensor pattern noise (SPN), camera response function, re-sampling artefacts, colour filter array (CFA) interpolation artefacts, JPEG compression, lens aberration, et cetera. Other device and image attributes such as binary similarity measures, image quality measures and higher order wavelet statistics have also been exploited to identify and classify source devices.

While many methods require that specific assumptions be satisfied, methods based on sensor pattern noise have drawn much attention due to the relaxation of the similar assumptions. Another advantage of sensor pattern noise is that it can identify not only camera models of the same make, but also individual cameras of the same model. The deterministic component of sensor pattern noise (SPN) is mainly caused by imperfections during the sensor manufacturing process and different sensitivity of pixels to light due to the inhomogeneity of silicon wafers. It is because of the inconsistency and the uniqueness of manufacturing imperfections and the variable sensitivity of each pixel to light that even sensors made from the same silicon wafer would possess uncorrelated pattern noise, which can be extracted from the images produced by the devices. This property makes sensor pattern noise a robust fingerprint for identifying and linking source devices and verifying the integrity of images. Another type of intrinsic data related to sensor is sensor readout noise. This section of the book covers the first three chapters, concerned with the use of sensor-based intrinsic data for multimedia forensic applications.

In chapter 1, *A DFT-Based Analysis to Discern between Camera and Scanned Images*, Caldelli *et al.* propose a novel approach to determining as to whether a digital image has been taken by a camera or has been scanned by a scanner. Such a technique exploits the specific geometrical features of the sensor pattern noise (SPN) left in the content by the sensor of the devices in both cases and analyse the frequency spectrum of the images to infer if periodical patterns exist. If periodicity exists in the frequency domain along the scanning direction, the image is deemed as having been taken by a scanner. Experimental results are presented to support the theoretical framework.

The sensor pattern noise and scene details coexist in the high-frequency band of images. Because the magnitudes of scene details tend to be many orders greater than those of the sensor patter noise, the estimated sensor pattern noise is actually highly contaminated by scene details. As such, a central part of sensor pattern noise estimation methodologies is the filter used to sift the high-frequency components. Chapter 2, *Estimate of PRNU Noise Based on Different Noise Models for Source Camera Identification*, presented by Amerini *et al.,* introduces another novel method for estimating sensor pattern noise as device fingerprint for source camera identification. The focus of this work is to study the characteristics of different filters involved in the analysis of sensor pattern noise. Based on the effective application of the MMSE filter in speckle and film-grain noise removal in coherent radiation imaging systems, the author propose to use a MMSE digital filter in the undecimated wavelet domain for estimating sensor pattern noise. They assume that the digital camera noise is dependent on the sensed signal when applying the MMSE filter. The proposed method is compared with the Mihcak filter - a signal-independent noise model. Their experimental results show that when the noise model matches the actual digital image acquisition process, the filter based on such a signal-dependent model (e.g., the MMSE filter) yields better performances if the parameters needed for the filtering operation are accurately estimated.

Chennamma and Rangarajan discussed *Source Camera Identification Based on Sensor Readout Noise* in chapter 3. Readout noise is a unique and intrinsic characteristic of a CCD or CMOS digital imaging sensor, which can be used in multimedia forensic applications by connecting the unique noise pattern to the source camera. First, the authors discuss the related work about source camera identification and describe the basic processing stages carried out inside a typical digital camera. Then they explain the origin of readout noise in digital cameras and how to measure it using the mean-standard deviation plot. Application of the proposed approach to the identification of source camera model based on readout noise is presented to validate their technique.

Section 2. Multimedia Security Based on Extrinsic Data

This section of the book is concerned with multimedia content protection and authentication through the embedding of extrinsic data. This set of techniques is about protecting the value of digital content or verifying the integrity and authenticity by embedding secret data in the host media and matching the hidden secret data against the original version at a later stage. Compared to cryptography, the use of extrinsic data for content protection is a relatively younger discipline. Digital watermarking is a typical example of content protection and authentication based on extrinsic data. It has been an active research area in the past 15 years. This set of digital watermarking techniques have found their applications in copyright protection (e.g., ownership identification, transaction tracking/traitor tracing and copy control), which is of great interest to the multimedia and movie industry. They are also applicable to content integrity verification and authentication, which is of high interest to the security sector, medical community, legal systems, et cetera. To ensure the security of these content protection schemes, the sophistication of countermeasures and attack models have to be in the mind of the developers of the protection schemes.

Semi-fragile and fragile digital watermarking has been widely employed for multimedia authentication and content integrity verification. The main difference between these two classes of watermarking schemes is that the former is made to be sensitive to only malicious manipulations of image content and to remain insensitive to incidental manipulations. These incidental manipulations include compression and mild signal processing operations due to transmission distortion. Because JPEG compression is the most common approach to saving storage and bandwidth, a substantial proportion of semi-fragile watermarking algorithms were designed to tolerate JPEG compression. However, watermarked images may be compressed with unknown JPEG Quality factors (QF). As a result, to be able to authenticate the watermarked images, a pre-determined threshold is set for most watermarking schemes to allow an anticipated QF bound. However, the predetermined threshold is usually rigidly fixed, making the schemes inadaptable to different levels of distortions caused by unknown QF set in the JPEG compression. In chapter 4, *Image Forensics Using Generalised Benford's Law for Improving Image Authentication Detection Rates in Semi-Fragile Watermarking*, Zhao *et al.* analyse the relationship between the QF and threshold, and propose to use the generalised Benford's Law to detect the unknown QF of the images before the scheme carries out watermark extraction. They observed an overall average QF correct detection rate of approximately 99% when 5%, 20%, and 30% of the image content are subjected to manipulation as well as compression using different QFs (ranging from 95 to 65). In addition, the authors also applied different image enhancement techniques (i.e., another form of incidental manipulation) to test images and observed that the QF correct detection rate can still be greater than 90%. The experiments described in this chapter indicate that their image forensic method can adaptively adjust the watermark detection threshold based on the estimated QF, making the proposed scheme more desirable in real-life applications.

While fragile and semi-fragile watermarking schemes (e.g., the schemes introduced in the previous chapter) are mainly intended for integrity verification and authentication, robust watermarking algorithms have been proposed for copyright protection through the embedding of an imperceptible, yet detectable watermark in digital multimedia content. Because the visual quality of the multimedia protected by robust watermarking should not be noticeably compromised by the embedding operation, human perception modelling has been an active research area in the digital watermarking community. The objective of the modelling is to strike a good balance between watermark imperceptibility and robustness. Transform domains such as the DCT or DWT facilitate decomposition of multimedia signals and allow adaptive selection of signal components for human perception modelling. Therefore, human perception modelling in the transform domains has been the mainstream approach. In chapter 5, *Blind Detection of Additive Spread-Spectrum Watermarking in the Dual-Tree Complex Wavelet Transform Domain*, Roland Kwitt *et al.* adapt two blind detector structures for additive spread-spectrum watermarking to the host media characteristics of the Dual-Tree Complex Wavelet Transform (DT-CWT) domain coefficients. The incentive of their research is the superior perceptual characteristics of the DT-CWT and its active use in watermarking. To improve the performance of the existing watermarking schemes in which the host media is modelled as a Gaussian distribution, the authors demonstrate that the Generalized Gaussian properties of Dual-Tree detail subband statistics can be exploited for better detector performance. They found that the Rao detector is has greater advantages over the likelihood-ratio test. They investigate the robustness of the proposed detectors under JPEG and JPEG2000 manipulations and evaluate the perceptual quality of the watermarked images. The results demonstrate that their DT-CWT domain approach significantly outperform the widely used linear-correlation detector. Because only the detection component of a complete watermarking scheme has to be modified to take the advantage of their findings, the proposed methods can be easily adopted in existing DT-CWT watermarking schemes.

Chapter 6 - *Spatio-Temporal Just Noticeable Distortion Model Guided Video Watermarking* - is also concerned with watermark imperceptibility. The authors, Yaqing Niu, Sridhar Krishnan, and Qin Zhang, address the imperceptibility issue surrounding spatio-temporal just noticeable distortion model guided video watermarking. They argue that perceptual watermarking should take full advantage of the outcomes from human visual system (HVS) researches. Just Noticeable Distortion (JND), which refers to the maximum distortion that the HVS cannot perceive, gives designer the reference for assuring watermark robustness without inflicting distortion noticeable to the HVS. The proposed watermarking scheme is based on a more accurate JND visual model which incorporates spatial Contrast Sensitivity Function (CSF), retinal velocity, luminance adaptation, temporal modulation factor, and contrast masking. The proposed watermarking scheme, in which a JND model is fully used to determine scene-adaptive upper bounds on watermark embedding, allows the user to provide the maximum strength transparent watermark.

Security of the watermark plays a central part in the design of feasible digital watermarking schemes because counter measures advance as the watermarking techniques evolve and can render new schemes useless if security gaps are left open. Chapter 7 - *Watermark-Only Security Attack on DM-QIM Watermarking: Vulnerability to Guided Key Guessing* - addresses the security of a specific class of common watermarking methods based on Dither Modulation-Quantisation Index Modulation (DM-QIM) with a focus on watermark-only attacks (WOA). DM-QIM is one of the well known lattice structure based watermarking techniques. The vulnerabilities of many lattice structure based watermark embedding schemes and possible attacks on these methods have been introduced in the literature. In this chapter, a watermark-only attack scenario (i.e., the attacker only has access to a single watermarked content) is discussed. In the literature, it is assumed that DM-QIM methods are secure against WOA. However, the authors of this chapter (Matam and Lowe) show that the DM-QIM based embedding schemes are vulnerable to a guided key guessing attack through the exploitation of subtle statistical regularities in the feature space embeddings for time series and images. Using a distribution-free algorithm, they conduct an analysis of the attack and present numerical results for multiple examples of image and time series data.

Section 3. Applications of Cryptography in Digital Forensics

Law enforcement agencies (LEA) quite often encounter encryption in their investigations to in the distribution of child pornography (KP) images and terrorist related information (TI). KP images in circulation are most likely to be encrypted so that the content can avoid being detected by watchful eyes and the anonymity of all involved parties can be preserved. Chapter 8 - *Cryptopometry as a Methodology for Investigating Encrypted Material* – is concerned with the identification of the PGP encrypted material. The authors of this chapter, Niall McGrath *et al.*, indicate that the use of PGP encryption is a major hurdle in the investigations into the distribution of child pornography images and terrorist related information. It is therefore important to enable digital forensic investigators to identify encrypted material, analyse it and finally extract valuable evidence or information from it. This chapter presents *Cryptopometry* - a methodology that facilitates the identification of the PGP encrypted material. A technique for identifying plaintext files that are encrypted is also presented. The incorporated search technique establishes correlation between the ciphertext file under investigation and the original plaintext file. A case study was carried out to validate the methodology. False positive rate is reported to be low.

A robust hash function allows involved parties to extract a consistent key from a common noisy data source (e.g., an image transmitted through a noisy channel), which can then be used to establish a cryptographic session key among the parties without having to transmit the key through a secure channel. This function is desirable in various communication applications, where the security notions are different. In chapter 9 - *Secure Robust Hash Functions and Their Applications in Non-interactive*

Communications - Li and Roy investigate these security notions and forgery attacks, where the objective of the attack is assumed to be the computation of the extracted key (i.e., the hash value) of a given message. They study information-theoretical and computational security against forgery under chosen message attacks and found that it is not possible to ensure information-theoretical security because it is not possible for the hash value in question to have conditional entropy that is not negligible, while keeping enough entropy for the secret key. They found that the entropy of the hash value of a given message can be reduced arbitrarily when sufficient message/hash pairs have been observed. However, they proposed a scheme that is computationally secure. With the scheme, it is computationally infeasible to compute the hash value even its entropy may not be high. They also analyze the collision resistance of robust hash functions in the scenario where the attacker attempts to manipulate messages to create a collision. They formulate a sufficient condition for a collision resistant robust hash function by using a pseudo-random transformation.

Steganography is the technique for covert communication. In Chapter 10, *Steganography in Thai Text*, Samphaiboon and Dailey propose text steganographic scheme with arbitrary documents written in the Thai language as cover media. Redundancies due to the way TIS-620 represents compound characters combining vowel, diacritical, and tonal symbols are exploited in the embedding process. The authors claim that their technique is applicable to any language whose Unicode character sets contain redundancies and the original covertext is not required at decoding side. The embedding capacity is as high as 203 bytes per 100 kilobytes, making the scheme practical for covert communication through text. Because the proposed embedding scheme hides secret data in plain text documents, it is robust against changes in font size and colour. The scheme is also proved to be robust against format changes, e.g., insertion of whitespace between words and line space adjustment. However, as the authors have reported, the scheme is not robust to insertion and deletion of SARA-AE, SARA-AM, and their replacements in the stegotext.

Section 4. Applications of Pattern Recognition and Signal Processing Techniques to Digital Forensics

Forensic investigators and law enforcement agencies quite often find themselves in the situations where evidence collection from electronic devices and scientific investigations into the implication of the evidence are required. This usually entails the use of signal processing and pattern recognition techniques either in the collection of evidence or in the analysis regarding the admissibility of evidence. Pattern recognition and digital signal processing have been in use by expert witnesses in forensic investigations for decades and their role is becoming increasingly important in law enforcement given the pace of the advances of electronic devices and ICT. Section 4 of this book deals with methods that harness these two sets of techniques for biometric applications and multimedia forensics.

Contributed by Liu *et al.*, chapter 11 - *Digital Image Forensics Using Multi-Resolution Histograms* - deals with the use of multi-resolution histograms (MRH) both in splicing detection and clone detection. The MRH of an image is employed to serve as the feature for describing the image and is then trained with a Support Vector Machine (SVM) to detect the splicing operations. With the MRH's simplicity and efficiency and the use of an SVM tool, the entire method is simple and highly efficient. Although the detection rate is only 65%, which did not really advance the state-of-the-art in splicing detection, the main contribution is the simplicity gain through the combination of MRH and SVM. To detect the clone operation within an image, the authors examine as to whether there are a number of similar block pairs with the same pair distance in an image or not. Again, MRHs are used as features of each image block.

Weir *et al.* present another splicing detection technique in chapter 12 - *Digital Image Splicing Using Edges*. The authors splice together an image that has been split up by using duplication detection. The nearest pieces are connected using edge searching and matching. For the pieces that have graphics or textures, the matching pieces are sought for using the edge shape and intersection between the two pieces. To start with, they mark the direction of each piece and put the pieces that have straight edges to the initial position to determine the profile of the whole image. The other pieces are then fixed into the corresponding position by using the edge information (shape, residual trace and matching) after duplication or sub-duplication detection. The patches with different edge shapes are searched for using edge duplication detection.

Taking inspiration from the biological vision system of insects, Haltis *et al.* implement a real-time biological vision model using a high dynamic range video camera and a General Purpose Graphics Processing Unit (GPGPU). The implementation of the proposed biologically-inspired vision system is based on the understanding that pixel-wise image processing could be computed in parallel using a parallel processing system designed for such graphics applications. The details are presented in chapter 13, *A Biologically Inspired Smart Camera for Use in Surveillance Applications*. The authors demonstrate the effectiveness of this photoreceptor-based processing in two surveillance applications: 1) dynamic equalization of contrast for improved recognition of scene detail and 2) the use of biologically-inspired motion processing for the detection of small or distant moving objects in a complex scene.

Chapter 14, *Palmprint Recognition Based on Subspace Analysis of Gabor Filter Bank,* by Laadjel *et al.*, presents a novel technique for palmprint recognition based on Fisher Linear Discriminant Analysis (FLDA) and Gabor fireco bank. This approach involves the convolution of a palmprint image with a bank of Gabor filters at deferent scales and orientations for robust palmprint feature extraction. After the features are extracted, FLDA is applied to reduce feature dimension. In order to enhance the recognition accuracy, the authors suggest that, when selecting the appropriate palm region for extracting features, one should take into account the fact that palmprint features are derived from the principal lines, wrinkles and texture along the palm area. To tackle this problem, the authors proposed an improved region of interest (ROI) extraction algorithm, which allows for an efficient extraction of the whole palm area by ignoring all the undesirable areas, such as fingers and background.

Section 5. Digital Evidence

Maintaining the chain-of-custody for evidence is of paramount importance in civil and criminal legal cases. To ensure the admissibility of evidence in the court of law, technical measures applied in the digital forensic investigation procedures are required to assure not only that evidence is not tampered with or manipulated due to their application, but that malicious attacks aiming at hiding or manipulating evidence are effectively detected. To serve these purposes, like physical world forensic investigation, digital forensic investigation usually has to follow three main steps:

1) *Event preservation* which entails, for example, the need for a bit-by-bit duplication of the volatile memory or file systems;
2) *Evidence search* which aims at collecting forensic information such as making timelines of system and file activities, device fingerprint (e.g., sensor pattern noise of digital cameras), keywords, contraband media, telecommunication data, steganography;

3) *Event Reconstruction* which is about interpreting the collected information /evidence in order to establish what have happened and who has involved in what.

To address the need for maintaining the admissibility of digital evidence, the fifth part of this book covers three chapters concerning with technical and legal issues surrounding the chain-of-custody for evidence.

Chapter 15, *Suspect Sciences? Evidentiary Problems with Emerging Technologies*, contributed by Gary Edmond, critically examine the response to new forms of incriminating expert opinion evidence in Australia based on recent developments surrounding the admission of expert evidence derived from images and sound recordings. This chapter argues that forensic sciences, biometrics and other forms of expert identification and comparison of evidence, along with incriminating expert opinion evidence, should all be demonstrably reliable before they are relied upon in criminal proceedings. The chapter begins with a succinct introduction to regulations governing the admissibility of expert evidence in Australia and then considers several cases exemplifying the ways Australian courts have responded to new and emerging modalities of expert opinion evidence in order to explain some of the problems with contemporary jurisprudence and practice. Gary Edmond concludes that emerging fields and disciplines should be thinking about forms of *self-regulation* that is scientifically legitimate. These forms of self-regulation should not rely on judges to come up with lists of qualified experts or devise standards and protocols. Judges usually are not expected to undertake such tasks. While self-regulation may involve sanctions and exclusion, perhaps the better approach is to have consensus statements about techniques and processes that have been tested along with the practices. If such statements are grounded in scientific research, developed in conjunction with scientists and experts from other fields, and widely accepted, they will provide practitioners with genuine assistance.

Recent technological advances in mobile phones functionalities and the development of smart phones technologies have provided enormous convenience for people to go about their daily life. However, they also provide powerful aids to criminals operating in many walks of the modern society. This entails effective measures for mobile phone forensic analysis in the fight against crime. Chapter 16, authored by Curran *et al.*, study many aspects of mobile phone forensic analysis, what it means, who avails of it and the commonly used software tools. The author start the chapter with an overview of forensic guidelines drafted by the British Association of Chief Police Officers (ACPO) for handling computer (including mobile phone) based electronic evidence. The authors also examine the process of the extraction of data from the Subscriber Identity Module (SIM) and phones and highlight some popular mobile phone forensics applications.

Cloud computing has emerged, not just as a new concept, but as a new paradigm for applications of information and communications technologies. The last few years has witnessed ICT providers investing heavily in developing technologies and enormous server facilities which allow global end users to access web-based applications and store their data off-site. However new concerns go hand in hand with new wave of ICT evolution. In chapter 17, *Grey Areas? The Legal Dimensions of Cloud Computing,* Michael Davis and Alice Sedsman start with the introduction of the benefits cloud computing has brought about and covers many aspects of human society where cloud computing can have significant impact. These includes payment models, free cloud services, access to data, centralised service, privacy issues and security, some cause of concerns regarding terms of use, intellectual property, and jurisdiction for disputes. The authors believe that in the face of this legal uncertainty, end users and industrial practitioners should be educated about the risks involved in the use of the cloud so that they can make informed choices about the applications for which cloud computing is an appropriate platform. The protection of end users is particularly important when cloud computing end user licence agreements give small players little or no opportunity to negotiate the terms. They conclude that as the world moves online, there is greater need for the laws that apply to these new activities to become more adaptive to international realities.

Narrative information in general is about the account of real-life or fictional scenarios ("narratives") that involve physical or imaginary characters, who would attempt to experience particular situations, attain specific results, manipulate tangible or abstract materials, send or receive messages, conduct transactions, et cetera. Narratives consist of temporally ordered sequences of elementary events. Chapter 18 - *A Conceptual Methodology for Dealing with Terrorism "Narratives",* contributed by Gian Piero Zarri, concerns the use of in-depth symbolic techniques pertaining to the artificial intelligence domain to deal with "narratives" in the crime- and terrorism-related areas in the Intelligent Information Retrieval (IIR) style. The author provides some details about the Narrative Knowledge Representation Language (NKRL), which is a representation and querying/inferencing environment especially designed for advanced exploitations of all sorts of narrative information. This description is integrated with real-life examples that illustrate the use of NKRL tools in two recent defence applications, the first dealing with a corpus of "Southern Philippines terrorism" news stories used in an R&D European project, the second, carried out in collaboration with the French "Délégation Générale pour l'Armement" (DGA, Central Bureau for Armament), which handles news stories about Afghanistan's war.

Chang-Tsun Li
University of Warwick, UK

Anthony T. S. Ho
University of Surrey, UK