# Preface

The last two decades have seen the unprecedented development of information and communication technology (ICT), computational hardware, and multimedia techniques. These techniques have revolutionized the ways we exchange information and run businesses. 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. Traders can now operate their e-business without distance constraint. 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 provide various aspects of 'e-services' to the people. Willingly or reluctantly, directly or indirectly, we are all now immersed in some ways 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 either. When exploited with malign intentions, the same tools provide means for doing harm on a colossal scale. These concerns create anxiety and uncertainty about the reality of the information and business we deal with. Due to the rise of digital crime and the pressing need for methods of combating 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 field of digital forensics and investigation, which aims at pooling expertise in various areas to combat the abuses of the ICT facilities and computer techniques.

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 legal issues and trends in information security regulations. It encompasses a wide variety of aspects of the related subject areas covered in twenty two 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 digital forensics and investigation.

The first four chapters aim at dissimilating the idea of biometrics and its applications. In Chapter 1 the privacy requirements, the major threats to privacy, and the best practices to employ in order to deploy privacy sympathetic systems, are discussed within the biometric framework. Presented in Chapter 2 is the joint research work between the University of Cagliari and Raggruppamento Carabinieri Investigazioni Scientifiche (Scientific Investigation Office) of the Arma dei Carabinieri, Italy, which studies the state of the art methods and algorithms for automatic analysis of latent fingerprint images and for fake fingerprints identification. Chapter 3 focuses on the principles behind methods currently used for face recognition, which have a wide variety of uses from biometrics, surveillance and forensics. Chapter

4 overviews the methods of face processing, including face detection, face recognition and processing of facial features, and the main strategies as well as the methods applied in the related fields. Conclusions concerning human processing of faces that have been drawn by the psychology researchers and neuroscientists are also described.

Chapters 5 and 6 are concerned with the imaging device identification and content integrity verification. Chapter 5 considers published research and identifies research gaps which address the general challenges of digital image provenance with an explicit emphasis on evidence related to the camera or other digital source. Chapter 6 discuss the idea of using distinctive imprints left on the media during the image acquisition process and any post-processing operations, as a sort of digital fingerprint for identifying imaging devices and authentication.

Chapter 7 to 9 deal with methods that harness the techniques of data hiding and cryptography for the applications of document forensics. Chapter 7 gives an overview of three complementary technologies for judging the authenticity and integrity of digital documents, namely forensic methods, perceptual hashes and digital watermarks. It also surveys the state-of-the-art methods of the three technologies and provides an analysis of their strength and weaknesses. Chapter 8 focuses on image authentication through the exploitation of two novel transforms for semi-fragile watermarking, using the Slant transform (SLT) as a block-based algorithm and the wavelet-based contourlet transform (WBCT) as a non-block based algorithm. Chapter 9 discuss a powerful reversible data hiding algorithm in JPEG images based on a new multilevel DCT. This lossless data hiding algorithm features a key-dependent (multilevel structure) coefficient-extension technique and an embedding location selector, and it can achieve high quality reconstructed images with disparate content types.

Chapter 10 and 11 focus on the use of forensic tools. Chapter 10 argues that digital forensics tools must exhaustively examine and interpret data at a low level, because data of evidentiary value may have been deleted, partially overwritten, obfuscated, or corrupted. This chapter considers recent hardware trends and argue that multicore CPUs and Graphics Processing Units (GPUs) offer one solution to the problem of maximizing available compute resources. Chapter 11 proposes an experimental framework that helps digital forensic experts to compare sets of digital forensic tools of similar functionality based on specific outcomes. The results can be used by an expert witness to justify the choice of tools and experimental settings, calculate the testing cost in advance, and be assured of obtaining results of good quality. Two case studies are provided to demonstrate the use of our framework.

Chapter 12 to 14 are concerned with network security and forensics. Chapter 12 examines innovations in forensic network acquisition, and in particular in attribution of network sources behind network address translated gateways. A novel algorithm for automatically attributing traffic to different sources is presented and then demonstrated. Finally it discusses some innovations in decoding of forensic network captures and illustrates how web mail can be extracted and rendered and in particular give the example of Gmail as a modern AJAX based webmail provider of forensic significance. Chapter 13 proposes a Service-oriented and User-centric Intrusion Detection System (SUIDS) for ubiquitous networks. SUIDS keeps the special requirements of ubiquitous computing in mind throughout its design and implementation. It sets a new direction for future research and development. Chapter 14 provides an overview of techniques and tools to detect deception on the Internet. A classification of state-of-the-art hypothesis testing and data mining based deception detection methods are presented. A psycho-linguistics based statistical model for deception detection is also described in detail. Passive and active methods for detecting deception at the application and network layer are discussed. Analysis of the pros and cons of the existing methods is presented. Finally, the inter-play between psychology, linguistics, statistical

modelling, network layer information and Internet forensics is discussed along with open research challenges. Chapter 15 reviews the characteristics of current P2P networks. By observing the behaviors of these networks, the authors propose some heuristic rules for identifying the first uploader of a shared file. Also, the rules have been demonstrated to be applicable to some simulated cases. The authors believe that their findings provide a foundation for future development in P2P file-sharing networks investigation. Chapter 16 describes the online risks to identity theft and the technological means for protecting individuals from losing their personal information while surfing the web.

Chapter 17 is aimed at introducing SIM and USIM card forensics, which pertains to *Small Scale Digital Device Forensics* (SSDDF) field. The authors give a general overview on the extraction of the standard part of the file system and present an effective methodology to acquire all the observable memory content. They also discuss some potential cases of data hiding at the file system level, presenting at the same time a detailed and useful procedure used by forensics practitioners to deal with such a problem.

In the light of an increasing number of illegal or inappropriate activities carried out by means of virtual machines, or targeting virtual machines, rather than physical ones, Chapter 18 discusses the implications on the forensic computing field of the issues, challenges, and opportunities presented by virtualization technologies, with a particular emphasis on the possible solutions to the problems arising during the forensic analysis of a virtualized system.

Chapter 19 evokes first the ubiquity and the importance of the so-called 'non-fictional narrative' information, with a particular emphasis on the terrorism- and crime-related data, and show that the usual knowledge representation and 'ontological' techniques have difficulties in finding complete solutions for representing and using this type of information. The author then supplies some details about NKRL, a representation and inferencing environment especially created for an 'intelligent' exploitation of narrative information. This description is integrated with concrete examples to illustrate the use of this conceptual tool in a terrorism context.

Chapter 20 is concerned with issues surrounding source code authorship, including authorship disputes, proof of authorship in court, cyber attacks in the form of viruses, trojan horses, logic bombs, fraud, and credit card cloning, and presents a new approach, called the SCAP (Source Code Author Profiles) approach, based on byte-level n-grams in order to represent a source code author's style. A comparison with a previous source code authorship identification study based on more complicated information shows that the SCAP approach is language independent and that n-gram author profiles are better able to capture the idiosyncrasies of the source code authors. It is also demonstrated that the effectiveness of the proposed model is not affected by the absence of comments in the source code, a condition usually met in cyber-crime cases.

Chapter 21 examines legal issues that must be considered in the use of computational systems in forensic investigations. There is a general framework for the use of evidence relating to legal proceedings, including computational forensic (CF) results that all nations employ. But the authors note some differences in procedures in different countries. And given the expert nature of computational systems and forensics using computation, special issues of reliability relating to science-based forensic conclusions must be addressed. The authors examine those generally (applicable to all CF) and as specifically applied to certain CF methods, examining two case studies on the possible use of CF methods in legal forums.

Chapter 22 reviews regulations and laws that are currently affecting information assurance and security policy in both the public and private sectors. Regulations and laws in different areas and at different levels are considered. Important industry sector regulations are also included when they have a significant impact on information security, such as the Health Insurance Portability and Accountability Act (HIPAA).

Analysis of these regulations including evaluation of their effectiveness, enforceability, and acceptance is presented. Since the regulations in this field are in a state of continuous fluctuation, this chapter also attempts to make proposals for statutory improvements that would make security policy development more comprehensive and consistent, resulting in more secure systems throughout the world. It is also predicted that there will be a need for international information security regulations given the nature of the worldwide internet and cross-border information systems. Such developments will improve digital crime investigations worldwide.

*Chang-Tsun Li*
*Editor*