Digital Forensics And Watermarking 10th International Workshop Iwdw 2011 Atlantic City Nj Usa October 23 26 2011 Revised Selected Papers Lecture Notes In Computer Science

CHAIM TIANA

Concepts, Methodologies, Tools, and Applications Springer Science & Business Media
This book constitutes the refereed proceedings of the 4th International Symposium on Mobile Internet Security, MobiSec 2019, held in Taichung, Taiwan, in October 2019. The 13 revised full papers presented were carefully reviewed and selected from 44 submissions. The papers are organized in the topical sections: mobile internet security; mobile application and security; vehicular network security; deep learning applications.
5th International Workshop, IWDW 2006, Jeju Island, Korea, November 8-10, 2006, Proceedings IGI Global
This book is a collection of best selected papers presented at the International Conference on Inventive Computation and Information Technologies (ICICIT 2020), organized during 24-25 September 2020. The book includes papers in the research area of information sciences and communication engineering. The book presents novel and innovative research results in theory, methodology and applications of communication engineering and information technologies.
From DeepFakes to Morphing Attacks Springer
Due to the growing use of web applications and communication devices, the use of data has increased throughout various industries, including business and healthcare. It is necessary to develop specific software programs that can analyze and interpret large amounts of data quickly in order to ensure adequate usage and predictive results. Cognitive Analytics: Concepts, Methodologies, Tools, and Applications provides emerging perspectives on the theoretical and practical aspects of data analysis tools and techniques. It also examines the incorporation of pattern management as well as decision-making and prediction processes through the use of data management and analysis. Highlighting a range of topics such as natural language processing, big data, and pattern recognition, this multi-volume book is ideally designed for information technology professionals, software developers, data analysts, graduate-level students, researchers, computer engineers, software engineers, IT specialists, and academicians.
Innovative Data Communication Technologies and Application Springer Science & Business Media
This book constitutes the refereed proceedings of the 5th International Workshop on Digital Watermarking Secure Data Management, IWDW 2006, held in Jeju Island, Korea in November 2006. The 34 revised full papers presented together with 3 invited lectures cover both theoretical and practical issues in digital watermarking.
Techniques and Trends Springer Nature
Lossless Information Hiding in Images introduces many state-of-the-art lossless hiding schemes, most of which come from the authors' publications in the past five years. After reading this book, readers will be able to immediately grasp the status, the typical algorithms, and the trend of the field of lossless information hiding. Lossless information hiding is a technique that enables images to be authenticated and then restored to their original forms by removing the watermark and

replacing overridden images. This book focuses on the lossless information hiding in our most popular media, images, classifying them in three categories, i.e., spatial domain based, transform domain based, and compressed domain based. Furthermore, the compressed domain based methods are classified into VQ based, BTC based, and JPEG/JPEG2000 based. Focuses specifically on lossless information hiding for images Covers the most common visual medium, images, and the most common compression schemes, JPEG and JPEG 2000 Includes recent state-of-the-art techniques in the field of lossless image watermarking Presents many lossless hiding schemes, most of which come from the authors' publications in the past five years

6th International Workshop, IH 2004, Toronto, Canada, May 23-25, 2004, Revised Selected Papers Springer

In recent years, libraries have embraced new technologies that organize and store a variety of digital information, such as multimedia databases, digital medical images, and content-based images. Modern Library Technologies for Data Storage, Retrieval, and Use highlights new features of digital library technology in order to educate the database community. By contributing research from case studies on the emerging technology use in libraries, this book is essential for academics and scientists interested in the efforts to understand the applications of data acquisition, retrieval and storage.

Refining Privacy Impact Assessment Springer

This book offers an analysis of privacy impacts resulting from and reinforced by technology and discusses fundamental risks and challenges of protecting privacy in the digital age. Privacy is among the most endangered "species" in our networked society: personal information is processed for various purposes beyond our control. Ultimately, this affects the natural interplay between privacy, personal identity and identification. This book investigates that interplay from a systemic, socio-technical perspective by combining research from the social and computer sciences. It sheds light on the basic functions of privacy, their relation to identity, and how they alter with digital identification practices. The analysis reveals a general privacy control dilemma of (digital) identification shaped by several interrelated socio-political, economic and technical factors. Uncontrolled increases in the identification modalities inherent to digital technology reinforce this dilemma and benefit surveillance practices, thereby complicating the detection of privacy risks and the creation of appropriate safeguards. Easing this problem requires a novel approach to privacy impact assessment (PIA), and this book proposes an alternative PIA framework which, at its core, comprises a basic typology of (personally and technically) identifiable information. This approach contributes to the theoretical and practical understanding of privacy impacts and thus, to the development of more effective protection standards. This book will be of much interest to students and scholars of critical security studies, surveillance studies, computer and information science, science and technology studies, and politics.

11th International Workshop, IWDW 2012, Shanghai, China, October 31--November 3, 2012, Revised Selected Papers John Wiley & Sons

This book is proceedings of the 7th FTRA International Conference on Future Information Technology (FutureTech 2012). The topics of FutureTech 2012 cover the current hot topics satisfying the world-wide ever-changing needs. The FutureTech 2012 is intended to foster the dissemination of state-of-the-art research in all future IT areas, including their models, services, and novel applications associated with their utilization. The FutureTech 2012 will provide an opportunity for academic and industry professionals to discuss the latest issues and progress in this area. In addition, the conference will publish high quality papers which are closely related to the various theories, modeling, and practical applications in many types of future technology. The main scope of FutureTech 2012 is as follows. Hybrid Information Technology Cloud and Cluster Computing Ubiquitous Networks and Wireless Communications Multimedia Convergence Intelligent and Pervasive Applications Security and Trust Computing IT Management and Service Bioinformatics and Bio-Inspired Computing Database and Data Mining Knowledge System and Intelligent Agent Human-centric Computing and Social Networks The FutureTech is a major forum for scientists, engineers, and practitioners throughout the world to present the latest research, results, ideas, developments and applications in all areas of future technologies.

IEM-ICDC 2020 Springer Nature

This book constitutes the refereed proceedings of the 16th International Workshop on Digital Forensics and Watermarking, IWDW 2017, held in Magdeburg, Germany, in August 2017. The 30 papers presented in this volume were carefully reviewed and selected from 48 submissions. The contributions are covering the state-of-the-art theoretical and practical developments in the fields of digital watermarking, steganography and steganalysis, forensics and anti-forensics, visual cryptography, and other multimedia-related security issues. Also included are the papers on two special sessions on biometric image tampering detection and on emerging threats of criminal use of information hiding : usage scenarios and detection approaches.

Springer

This book constitutes the thoroughly refereed post-proceedings of the 11th International Workshop on Digital-Forensics and Watermarking, IWDW 2012, held in Shanghai, China, during October/November 2012. The 42 revised papers (27 oral and 15 poster papers) were carefully reviewed and selected from 70 submissions. The papers are organized in topical sections on steganography and steganalysis; watermarking and copyright protection; forensics and anti-forensics; reversible data hiding; fingerprinting and authentication; visual cryptography.

Digital Forensics and Watermarking IGI Global

As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

Information Hiding Walter de Gruyter GmbH & Co KG

Digital forensic science, or digital forensics, is the application of scientific tools and methods to identify, collect, and analyze digital (data) artifacts in support of legal proceedings. From a more technical perspective, it is the process of reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system or (digital) artifacts. Over the last three decades, the importance of digital evidence has grown in lockstep with the fast societal adoption of information technology, which has resulted in the continuous accumulation of data at an exponential rate. Simultaneously, there has been a rapid growth in network connectivity and the complexity of IT systems, leading to more complex behavior that needs to be investigated. The goal of this book is to provide a systematic technical overview of digital forensic techniques, primarily from the point of view of computer science. This allows us to put the field in the broader perspective of a host of related areas and gain better insight into the computational challenges facing forensics, as well as draw inspiration for addressing them. This is needed as some of the challenges faced by digital forensics, such as cloud computing, require qualitatively different approaches; the sheer volume of data to be examined also requires new means of processing it.

10th International Workshop, IWDW 2011, Atlantic City, NJ, USA, October 23-26, 2011, Revised Selected Papers Springer Science & Business Media

This book presents the latest research in the fields of computational intelligence, ubiquitous computing models, communication intelligence, communication security, machine learning, informatics, mobile computing, cloud computing and big data analytics. The best selected papers, presented at the International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2020), are included in the book. The book focuses on the theory, design, analysis, implementation and applications of distributed systems and networks.

Cryptographic and Information Security Approaches for Images and Videos Springer

This book includes selected papers presented at International Conference on Computational Intelligence, Data Science and Cloud Computing (IEM-ICDC) 2020, organized by the Department of Information Technology, Institute of Engineering & Management, Kolkata, India, during 25-27 September 2020. It presents substantial new research findings about AI and robotics, image processing and NLP, cloud computing and big data analytics as well as in cyber security, blockchain and IoT, and various allied fields. The book serves as a reference resource for researchers and practitioners in academia and industry.

International Conference, ICDIPC 2011, Ostrava, Czech Republic, July 7-9, 2011. Proceedings Springer

It is an honor and great pleasure to write a preface for this postproceedings of the 6th International Workshop on Information Hiding. In the past 10 years, the field of data hiding has been maturing and expanding, gradually establishing its place as an active interdisciplinary research area uniquely combining information theory, cryptology, and signal processing. This year, the workshop was followed by the Privacy Enhancing Technologies workshop (PET) hosted at the same location. Delegates viewed this connection as fruitful as it gave both communities a convenient opportunity to interact. We would like to thank all authors who submitted their work for consideration. Out of the 70 submisions received by the program committee, 25 papers were accepted for publication based on their novelty, originality, and scientific merit. We strived to achieve a balanced exposition of papers that would represent many different aspects of information hiding. All papers were divided into eight sessions: digital media watermarking, steganalysis, digital forensics, steganography, software watermarking, security and privacy, anonymity, and data hiding in unusual content. This year, the workshop included a one-hour rump session that offered an opportunity to the delegates to share their work in progress and other brief but interesting contributions.

Digital Watermarking Springer Science & Business Media

This book constitutes the refereed proceedings of the 8th Interntaional Workshop, IWDW 2009, held in Guildford, Surrey, UK, August 24-26, 2009. The 25 revised full papers, including 4 poster presentations, presented together with 3 invited papers were carefully reviewed and selected from 50 submissions. The papers are organized in topical sections on robust watermarking, video watermarking, steganography and steganalysis, multimedia watermarking and security protocols, as well as image forensics and authentication.

Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing Springer

Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies

Intelligent Multi-Modal Data Processing Springer Science & Business Media

The revolutionary way in which modern technologies have enabled us to exchange information with ease has led to the emergence of interdisciplinary research in digital forensics and investigations, which aims to combat the abuses of computer technologies. Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security presents various digital crime and forensic disciplines that use electronic devices and software for crime prevention and detection. This book provides theoretical and empirical research articles and case studies for a broad range of academic readers as well as professionals, industry consultants, and practitioners involved in the use, design, and development of techniques related to digital forensics and investigation.

Digital Forensics and Watermarking Springer Nature
This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

FutureTech 2012 Volume 1 Artech House
This book constitutes the refereed proceedings of the 17th International Workshop on Digital Forensics and Watermarking, IWDW 2018, held on Jeju Island, Korea, in October 2018.The 25 papers presented in this volume were carefully reviewed and selected from 43 submissions. The contributions are covering the following topics: deep neural networks for digital forensics; steganalysis and identification; watermarking; reversible data hiding; steganographic algorithms; identification and security; deep generative models for forgery and its detection.