# Digital Forensics And Watermarking 10th International

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Workshop on Digital-forensics and Watermarking (IWDW 2011) held in Atlantic City, NJ, USA, during October 23-26, 2011. The 37 revised full papers presented were carefully selected from 59 submissions. Conference papers are organized in 6 technical sessions, covering the topics of steganography and steganalysis, watermarking, visual cryptography, forensics, anti-forensics, fingerprinting, privacy and security.

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.

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.

This book constitutes the refereed proceedings of the 7th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2015, held in Seoul, South Korea, in October 2015. The 14 papers and 3 abstracts were selected from 40 submissions and cover diverse topics ranging from tactics of cyber crime investigations to digital forensic education, network forensics, and international cooperation in digital investigations.

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.

The popularity of multimedia content has led to the widespread distribution and consumption of digital multimedia data. As a result of the relative ease with which individuals may now alter and repackage digital content, ensuring that media content is employed by authorized users for its intended purpose is becoming an issue of eminent importance to both governmental security and commercial applications. Digital fingerprinting is a class of multimedia forensic technologies to track and identify entities involved in the illegal manipulation and unauthorized usage of multimedia content, thereby protecting the sensitive nature of multimedia data as well as its commercial value after the content has been delivered to a recipient. "Multimedia Fingerprinting Forensics for Traitor Tracing" covers the essential aspects of research in this emerging technology, and explains the latest development in this field. It describes the framework of multimedia fingerprinting, discusses the challenges that may be faced when enforcing usage polices, and investigates the design of fingerprints that cope with new families of multiuser attacks that may be mounted against media fingerprints. The discussion provided in the book highlights challenging problems as well as future trends in this research field, providing readers with a broader view of the evolution of the young field of multimedia forensics. Topics and features: Comprehensive coverage of digital watermarking and fingerprinting in multimedia forensics for a number of media types. Detailed discussion on challenges in multimedia fingerprinting and analysis of effective multiuser collusion attacks on digital fingerprinting. Thorough investigation of fingerprint design and performance analysis for addressing different application concerns arising in multimedia fingerprinting. Well-organized explanation of problems and solutions, such as order-statistics-based nonlinear collusion attacks, efficient detection and identification of colluders, group-oriented fingerprint design, and anti-collusion codes for multimedia fingerprinting. Presenting the state of the art in collusion-resistant digital fingerprinting for multimedia forensics, this invaluable book is accessible to a wide range of researchers and professionals in the fields of electrical engineering, computer science, information technologies, and digital rights management.

This book constitutes the refereed proceedings of the 6th International Workshop, IWDW 2007, held in Guangzhou, China, in December 2007. The 24 revised full papers together with 3 invited papers were carefully reviewed and selected from 81 submissions. The papers are organized in topical sections on watermark security; steganalysis; authentication; reversible data hiding; robust

watermarking; poster session; theory and methods in watermarking.
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.

In this book, you will learn how to build from scratch a criminal records management database system using Java/PostgreSQL. All Java code for cryptography and digital image processing in this book is Native Java. Intentionally not to rely on external libraries, so that readers know in detail the process of extracting digital images from scratch in Java. There are only three external libraries used in this book: Connector / J to facilitate Java to PostgreSQL connections, JCalendar to display calendar controls, and JFreeChart to display graphics. Digital image techniques to extract image features used in this book are grascaling, sharpening, invertering, blurring, dilation, erosion, closing, opening, vertical prewitt, horizontal prewitt, Laplacian, horizontal sobel, and vertical sobel. For readers, you can develop it to store other advanced image features based on descriptors such as SIFT and others for developing descriptor based matching. In the first chapter, you will learn: How to install NetBeans, JDK 11, and the PostgreSQL connector; How to integrate external libraries into projects; How the basic PostgreSQL commands are used; How to query statements to create databases, create tables, fill tables, and manipulate table contents is done. In the second chapter, you will learn querying data from the postgresql using jdbc including establishing a database connection, creating a statement object, executing the query, processing the resultset object, querying data using a statement that returns multiple rows, querying data using a statement that has parameters, inserting data into a table using jdbc, updating data in postgresql database using jdbc, calling postgresql stored function using jdbc, deleting data from a postgresql table using jdbc, and postgresql jdbc transaction. In the second chapter, you will learn the basics of cryptography using Java. Here, you will learn how to write a Java program to count Hash, MAC (Message Authentication Code), store keys in a KeyStore, generate PrivateKey and PublicKey, encrypt / decrypt data, and generate and verify digital prints. In the third chapter, you will learn how to create and store salt passwords and verify them. You will create a Login table. In this case, you will see how to create a Java GUI using NetBeans to implement it. In addition to the Login table, in this chapter you will also create a Client table. In the case of the Client table, you will learn how to generate and save public and private keys into a database. You will also learn how to encrypt / decrypt data and save the results into a database. In the fourth chapter, you will create an Account table. This account table has the following ten fields: account_id (primary key), client_id (primarykey), account_number, account_date, account_type, plain_balance, cipher_balance, decipher_balance, digital_signature, and signature_verification. In this case, you will learn how to implement generating and verifying digital prints and storing the results into a database. In the fifth chapter, you create a table with the name of the Account, which has ten columns: account_id (primary key), client_id (primarykey), account_number, account_date, account_type, plain_balance, cipher_balance, decipher_balance, digital_signature, and signature_verification. In the sixth chapter, you will create a Client_Data table, which has the following seven fields: client_data_id (primary key), account_id (primary_key), birth_date, address, mother_name, telephone, and photo_path. In the seventh chapter, you will be taught how to create Crime database and its tables. In eighth chapter, you will be taught how to extract image features, utilizing BufferedImage class, in Java GUI. In the nineth chapter, you will be taught to create Java GUI to view, edit, insert, and delete Suspect table data. This table has eleven columns: suspect_id (primary key), suspect_name, birth_date, case_date, report_date, suspect_ status, arrest_date, mother_name, address, telephone, and photo. In the tenth chapter, you will be taught to create Java GUI to view, edit, insert, and delete Feature_Extraction table data. This table has eight columns: feature_id (primary key), suspect_id (foreign key), feature1, feature2, feature3, feature4, feature5, and feature6. In the eleventh chapter, you will add two tables: Police_Station and Investigator. These two tables will later be joined to Suspect table through another table, File_Case, which will be built in the seventh chapter. The Police_Station has six columns: police_station_id (primary key), location, city, province, telephone, and photo. The Investigator has eight columns: investigator_id (primary key), investigator_name, rank, birth_date, gender, address, telephone, and photo. Here, you will design a Java GUI to display, edit, fill, and delete data in both tables. In the twelfth chapter, you will add two tables: Victim and File_Case. The File_Case table will connect four other tables: Suspect, Police_Station, Investigator and Victim. The Victim table has nine columns: victim_id (primary key), victim_name, crime_type, birth_date, crime_date, gender, address, telephone, and photo. The File_Case has seven columns: file_case_id (primary key), suspect_id (foreign key), police_station_id (foreign key), investigator_id (foreign key), victim_id (foreign key), status, and description. Here, you will also design a Java GUI to display, edit, fill, and delete data in both tables. Finally, this book is hopefully useful for you.

Welcome to the proceedings of the Fifth International Workshop on Digital Watermarking (IWDW). Since the first IWDW held in Seoul, Korea in 2002, it has been a focal point for meeting in person and disseminating valuable scientific and technological developments in watermarking. IWDW 2006 was held on Jeju, the dream island in Korea. The main theme of the workshop was “Meet the Challenges in this Digital World!” As we all know, digital watermarking and its related technologies have emerged as the key ingredients of this digital world. We report on new developments and discuss how to best utilize the watermarking and its related new technologies to cope with many challenging issues in this digital world. This year, we accepted 34 papers out of 76 highly qualified submissions from 14 different countries. Each paper was reviewed by three reviewers. The acceptance ratio of 44% indicates IWDW’s continuing commitment to ensuring the quality of the workshop. In addition, we had three invited lectures and one panel discussion that shed invaluable insights to the watermarking community on new developments and future directions. The technical program featured such topics as steganography and steganalysis, data forensics, digital right management, secure watermarking, and their applications. The 34 accepted papers, three invited lectures, and the panel discussion covered both theoretical and practical issues that all of us can benefit from. Furthermore, 13 of the 34 papers were arranged in a poster session in order to facilitate more efficient and interactive information exchange.

This book presents medical image watermarking techniques and algorithms for telemedicine and other emerging applications. This book emphasizes on medical image watermarking to ensure the authenticity of transmitted medical information. It begins with an introduction of digital watermarking, important characteristics, novel applications, different watermarking attacks and standard benchmark tools. This book also covers spatial and transform domain medical image watermarking techniques and their merits and limitations. The authors have developed improved/novel watermarking techniques for telemedicine applications that offer higher robustness, better perceptual quality and increased embedding capacity and secure watermark. The suggested methods may find potential applications in the prevention of patient identity theft and health data management issues which is a growing concern in telemedicine applications. This book provides a sound platform for understanding the medical image watermarking paradigm for researchers in the field and advanced-level students. Industry professionals working in this field, as well as other emerging applications demanding robust and secure watermarking will find this book useful as a reference.

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.

This two-volume-set (CCIS 188 and CCIS 189) constitutes the refereed proceedings of the International Conference on Digital Information Processing and Communications, ICDIPC 2011, held in Ostrava, Czech Republic, in July 2011. The 91 revised full papers of both volumes presented together with 4 invited talks were carefully reviewed and selected from 235 submissions. The papers are organized in topical sections on network security; Web applications; data mining; neural networks; distributed and parallel processing; biometrics technologies; e-learning; information ethics; image processing; information and data management; software engineering; data compression; networks; computer security; hardware and systems; multimedia; ad hoc network; artificial intelligence; signal processing; cloud computing; forensics; security; software and systems; mobile networking; and some miscellaneous topics in digital information and communications.

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.

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.

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

As information technology is rapidly progressing, an enormous amount of media can be easily exchanged through Internet and other communication networks. Increasing amounts of digital image, video, and music have created numerous information security issues and is now taken as one of the top research and development agendas for researchers, organizations, and governments worldwide. Multimedia Forensics and Security provides an in-depth treatment of advancements in the emerging field of multimedia forensics and security by tackling challenging issues such as digital watermarking for copyright protection, digital fingerprinting for transaction tracking, and digital camera source identification.

This book presents essential principles, technical information, and expert insights on multimedia security technology. Illustrating the need for improved content security as the Internet and digital multimedia applications rapidly evolve, it presents a wealth of everyday protection application examples in fields including . Giving readers an in-depth introduction to different aspects of information security mechanisms and methods, it also serves as an instructional tool on the fundamental theoretical framework required for the development of advanced techniques.

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.

Welcome to the proceedings of the 10th Pacific Rim Conference on Multimedia (PCM 2009) held in Bangkok, Thailand, December 15-18, 2009. Since its inception in 2000, PCM has rapidly grown into a major conference on multimedia in the Asia- Pacific Rim region and has built up its reputation around the world. Following the success of the preceding conferences, PCM 2008 in Taiwan, PCM 2007 in Hong Kong, PCM 2006 in China, PCM 2005 in Korea, PCM 2004 in Japan, PCM 2003 in Singapore, PCM 2002 in Taiwan, PCM 2001 in China, and PCM 2000 in Australia, the tenth PCM brought researchers, developers, practitioners, and educators together to disseminate their new discoveries in the field of multimedia. Theoretical bre- throughs and practical systems were presented at this conference, thanks to the s- port of Naresuan University, Mahanakorn University of Technology, and the IEEE Thailand Section. PCM 2009 featured a comprehensive program including keynote talks, regular - per presentations, posters, and special sessions. We received 171 papers from 16 countries including Australia, Sweden, German, Italy, Iran, France, Canada, China, Japan, Korea, Malaysia, Singapore, Taiwan, Hong Kong, the UK, and the USA. After a rigorous review process, we accepted only 67 oral presentations and 45 poster pr- entations. Four special sessions were also organized by world-leading researchers.

This two volume set constitutes the refereed post-conference proceedings of the Second International Conference on Machine Learning and Intelligent Communications, MLICOM 2017, held in Weihai, China, in August 2017. The 143 revised full papers were carefully selected from 225 submissions. The papers are organized thematically in machine learning, intelligent positioning and navigation, intelligent multimedia processing and security, intelligent wireless mobile network and security, cognitive radio and intelligent networking, intelligent internet of things, intelligent satellite communications and networking, intelligent remote sensing, visual computing and three-dimensional modeling, green communication and intelligent networking, intelligent ad-hoc and sensor networks, intelligent resource allocation in wireless and cloud networks, intelligent signal processing in wireless and optical communications, intelligent radar signal processing, intelligent cooperative communications and networking.

A comprehensive and practical analysis and overview of the imaging chain through acquisition, processing and displayThe Handbook of Digital Imaging provides a coherent overview of the imaging science amalgam, focusing on the capture, storage and display of images. The volumes are arranged thematically to provide a seamless analysis of the imaging chain from source (image acquisition) to destination (image print/display). The coverage is planned to have a very practical orientation to provide a comprehensive source of information for practicing engineers designing and developing modern digital imaging systems. The content will be drawn from all aspects of digital imaging including optics, sensors, quality, control, colour encoding and decoding, compression, projection and display.• Contains approximately 50, highly illustrated articles (ranging from 20-40 pages), printed in full colour throughoutComprehensive 3-volume set, also available on Wiley Online Library. • Over 50 Contributors, with contributors from Europe, US and Asia. Contributors are both and from academia and industryThe 3 volumes will be organized thematically for enhanced usability:Volume 1: Image Capture and Storage• Image Capture and Storage Volume 2: Image Display and Reproduction• Image Display and Projection• Hardcopy Technology• Halftoning and Physical Evaluation• Models for Halftone ReproductionVolume 3: Imaging System Applications• Media Imaging• Remote Imaging• Medical and Forensic ImagingIdeal for engineers and designers in the dynamic global imaging and display industries

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.

th It is our great pleasure to present this volume of the proceedings of the 10 edition of Information Hiding (IH 2008). The conference was held in Santa Barbara - the Ame- can Riviera, California, USA, during May 19–21, 2008. It was organized by three Santa Barbarans on fire, from both industry (Mayachitra) and academia (UCSB). Over the years, Information Hiding (IH) has established itself as a premier forum for presenting research covering various aspects of information hiding. Continuing the tradition, this year, we provide a balanced program including topics such as anonymity and privacy, forensics, steganography, watermarking, fingerprinting, other hiding domains, and novel applications. We received a total of 64 papers from all over the globe, and would like to take this opportunity to thank all the authors who submitted their paper to IH 2008 and thus contributed to the consolidation of the reputation of the conference. The papers were refereed by at least three revi- ers who provided detailed comments, which was followed by discussion amongst the Program Committee members. Only 25 papers were selected for presentation. This rigorous review process will certainly strengthen Information Hiding's po- tion as the top forum of our community.

Photographic imagery has come a long way from the pinhole cameras of the nineteenth century. Digital imagery, and its applications, develops in tandem with contemporary society's sophisticated literacy of this subtle medium. This book examines the ways in which digital images have become ever more ubiquitous as legal and medical evidence, just as they have become our primary source of news and have replaced paper-based financial documentation. Crucially, the contributions also analyze the very profound problems which have arisen alongside the digital image, issues of veracity and progeny that demand systematic and detailed response: It looks real, but is it? What camera captured it? Has it been doctored or subtly altered? Attempting to provide answers to these slippery issues, the book covers how digital images are created, processed and stored before moving on to set out the latest techniques for forensically examining images, and finally addressing practical issues such as courtroom admissibility. In an environment where even novice users can alter digital media, this authoritative publication will do much so stabilize public trust in these real, yet vastly flexible, images of the world around us.

Digital Forensics and Watermarking10th International Workshop, IWDW 2011, Atlantic City, NJ, USA, October 23-26, 2011, Revised Selected PapersSpringer

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

Because it makes the distribution and transmission of digital information much easier and more cost effective, multimedia has emerged as a top resource in the modern era. In spite of the opportunities that multimedia creates for businesses and companies, information sharing remains vulnerable to cyber attacks and hacking due to the open channels in which this data is being transmitted. Protecting the authenticity and confidentiality of information is a top priority for all professional fields that currently use multimedia practices for distributing digital data. The Handbook of Research on Multimedia Cyber Security provides emerging research exploring the theoretical and practical aspects of current security practices and techniques within multimedia information and assessing modern challenges. Featuring coverage on a broad range of topics such as cryptographic protocols, feature extraction, and chaotic systems, this book is ideally designed for scientists, researchers, developers, security analysts, network administrators, scholars, IT professionals, educators, and students seeking current research on developing strategies in multimedia security.

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.

This is volume 77 of Advances in Computers. Since 1960, annual volumes are produced containing chapters by some of the leading experts in the field of computers today. For 50 years these volumes offer ideas and developments that are changing our society. This volume presents eight different topics covering many different aspects of computer science. A wide range of subjects are covered from insights into the different ways individuals can interact with electronic devices to how common law is adapting to and impacting on the Internet.

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.

"This handbook is 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 secure multimedia distribution"--Provided by publisher.

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.

This book constitutes the refereed proceedings of the 10th IFIP TC 12 International Conference on Intelligent Information Processing, IIP 2018, held in Nanning, China, in October 2018. The 37 full papers and 8 short papers presented were carefully reviewed and selected from 80 submissions. They are organized in topical sections on machine learning, deep learning, multi-agent systems, neural computing and swarm intelligence, natural language processing, recommendation systems, social computing, business intelligence and security, pattern recognition, and image understanding.

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.

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.

A successor to the popular Artech House title Information Hiding Techniques for Steganography and Digital Watermarking, this comprehensive and up-to-date new resource gives the reader a thorough review of steganography, digital watermarking and media fingerprinting with possible applications to modern communication, and a survey of methods used to hide information in modern media. This book explores Steganography, as a means by which two or more parties may communicate using invisible or subliminal communication. "Steganalysis" is described as methods which can be used to break steganographic communication. This comprehensive resource also includes an introduction to watermarking and its methods, a means of hiding copyright data in images and discusses components of commercial multimedia applications that are subject to illegal use. This book demonstrates a working knowledge of watermarking's pros and cons, and the legal implications of watermarking and copyright issues on the Internet.

This book constitutes the thoroughly refereed post-conference proceedings of the 9th Interntaional Workshop on Digital Watermarking, IWDW 2010, held in Seoul, Korea, in October 2010. The 26 revised full papers presented were carefully reviewed and selected from 48 submissions. The papers are organized in topical sections on forensics, visual cryptography, robust watermarking, steganography, fingerprinting, and steganalysis.

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 forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics X describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: - Internet Crime Investigations; - Forensic Techniques; - Mobile Device Forensics; - Forensic Tools and Training. This book is the 10th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-two edited papers from the 10th Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Vienna, Austria in the winter of 2014. Advances in Digital Forensics X is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.