Multimedia Security Steganography And Digital Watermarking Techniques For Protection Of Intellectual Property

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This special issue contains five selected papers that were presented at the Workshop on Pattern Recognition for IT Security, held in Darmstadt, Germany, in September 2010, in conjunction with the 32nd Annual Symposium of the German Association for Pattern Recognition, DAGM 2010. It demonstrates the broad range of security-related topics that utilize graphical data. The contributions explore the security and reliability of biometric data, the power of machine learning methods to differentiate forged images from originals, the effectiveness of modern watermark embedding schemes and the use of information fusion in steganalysis.

Security is a major concern in an increasingly multimedia-defined universe where the Internet serves as an indispensable resource for information and entertainment. Digital Rights Management (DRM) is the technology by which network systems protect and provide access to critical and time-sensitive copyrighted material and/or personal information. This book equips savvy technology professionals and their aspiring collegiate protégés with the latest technologies, strategies and methodologies needed to successfully thwart off those who thrive on security holes and weaknesses. Filled with sample application scenarios and algorithms, this book provides an in-depth examination of present and future field technologies including encryption, authentication, copy control, tagging, tracing, conditional access and media identification. The authors present a diversified blend of theory and practice and focus on the constantly changing developments in multimedia applications thus providing an admirably comprehensive book. * Discusses state-of-the-art multimedia authentication and fingerprinting techniques * Presents several practical methodologies from industry, including broadcast encryption, digital media forensics and 3D mesh watermarking * Focuses on the need for security in multimedia applications found on computer networks, cell phones and emerging mobile computing devices

Understand the building blocks of covert communication in digital media and apply the techniques in practice with this self-contained guide.

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often

combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This fourth issue contains five contributions in the area of digital watermarking. The first three papers deal with robust watermarking. The fourth paper introduces a new least distortion linear gain model for halftone image watermarking and the fifth contribution presents an optimal histogram pair based image reversible data hiding scheme.

The growth of the World Wide Web (WWW) has enabled the personal computer to be used as a general communications tool. As in the case of other forms of communication there is a wish for security and privacy. With literally millions of images moving on the Internet each year, it is safe to say that digital image Steganography is of real concern to many in the IT security field. Digital images could be used for a number of different types of security fear. In the business world, the sending of a harmless looking bitmap file could actually hide the latest company secrets. Steganography (literally, covered writing) is concealing of a secret message within another seemingly innocuous message, or carrier. Digital carriers include e- mail, audio, and images. Steganography, like cryptography, is a means of providing secrecy. Steganography does so by hiding the very existence of the communication, while cryptography does so by scrambling a message so it cannot be understood. A cryptography message can be intercepted by an eavesdropper, but the eavesdropper may not even know the existence of a steganographic message. This thesis discusses the issues regarding Steganography and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems. In the fundamental part, we identify a few key elements of Steganography through a layered structure. Data hiding is concerned to be as a communication problem where the embedded data is the signal to be transmitted. The tradeoff for two major categories of embedding data using spatial domain and frequency domain win be discussed. In addition, we have found that unevenly distributed embedding capacity brings difficulty in data hiding. We propose a complete solution to this problem, addressing considerations for choosing constant or variable embedding rate and enhancing the performance for each case. In the design part, we present new data hiding algorithms for binary images, grayscale and color images, covering such applications as annotation, fingerprinting, and ownership protection.

This book constitutes the refereed proceedings of the 14th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security, CMS 2013, held in Magdeburg, Germany, in September 2013. The 5 revised full papers presented together with 11 short papers, 5 extended abstracts describing the posters that were discussed at the conference, and 2 keynote talks were carefully reviewed and selected from 30 submissions. The papers are organized in topical sections on biometrics; applied cryptography; digital watermarking, steganography and forensics; and social network privacy, security and authentication.

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 refereed proceedings of the 6th International Conference on Information Processing, ICIP 2012, held in Bangalore, India, in August 2012. The 75 revised full papers presented were carefully reviewed and selected from 380 submissions. The papers are organized in topical sections on wireless networks; image processing; pattern recognition and classification; computer architecture and distributed computing; software engineering, information technology and optimization techniques; data mining techniques; computer networks and network security.

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.

Annotation This work explores the myriad of issues regarding multimedia security. It covers various issues, including perceptual fidelity analysis, image, audio, and 3D mesh object watermarking, medical watermarking, and error detection (authentication) and concealment.

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This third issue contains five contributions in the areas of steganography and digital watermarking. The first two papers deal with the security of steganographic systems; the third paper presents a novel image steganographic scheme. Finally, this volume includes two papers that focus on digital watermarking and data hiding. The fourth paper introduces and analyzes a new covert channel and the fifth contribution analyzes the performance of

additive attacks against quantization-based data hiding methods.
[Administration (référence électronique)].
Intellectual property owners who exploit new ways of reproducing, distributing, and marketing their creations digitally must also protect them from piracy. Multimedia Security Handbook addresses multiple issues related to the protection of digital media, including audio, image, and video content. This volume examines leading-edge multimedia securit
Advanced image and video processing abilities in smart phones and digital cameras make them popular means to capture multimedia. In addition, the integration of internet into such devices users seek to capture and easily share multimedia right from their smartphone while most steganography techniques are computer based. Hence, it is of utmost importance that the multimedia be processed for steganography right within the devices for multimedia authentication. In this thesis, we first implement steganography into mobile smart devices that can capture multimedia. For devices such as smart phones, we propose a method to hide payload bits within video frames. The solution takes relatively less time and memory to process as opposed to existing computer based solutions. This is a major achievement over traditional techniques that have longer running times leading to power inefficiencies. The idea proposed is to divide the video frames being processed into smaller blocks and perform embedding at block levels, thus localizing any processing that is to be performed. Simulation results show that the solution proposed can perform about 60 percent faster and 40 percent BER improvement than conventional approach of video steganography. This thesis takes the foregoing solution to a greater height by using the same algorithm for steganography within Image Sensor Pipeline in digital cameras. The objective behind this is to ensure all images generated from all forms of digital cameras are watermarked automatically. The solutions that exist now are largely dependent on extraction of camera component information. The proposed steganography technique is image centric and aims to resolve existing issues in areas such as image source identification, discrimination of synthetic images and basic image forgery. After experiments, Peak Signal to Noise Values with a least value of 70 dB even for the worst compression quality (Q) factor of 50 shows how the perceptual quality of the image is preserved. Bit Error Rate of about 5 % for the same quality (Q=50) puts light on the robustness of the technique against JPEG compression.
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.
Digital audio, video, images, and documents are flying through cyberspace to their respective owners. Unfortunately, along the way, individuals may choose to intervene and take this content for themselves. Digital watermarking and steganography technology greatly reduces the instances of this by limiting or eliminating the ability of

third parties to decipher the content that he has taken. The many techiniques of digital watermarking (embedding a code) and steganography (hiding information) continue to evolve as applications that necessitate them do the same. The authors of this second edition provide an update on the framework for applying these techniques that they provided researchers and professionals in the first well-received edition. Steganography and steganalysis (the art of detecting hidden information) have been added to a robust treatment of digital watermarking, as many in each field research and deal with the other. New material includes watermarking with side information, QIM, and dirty-paper codes. The revision and inclusion of new material by these influential authors has created a must-own book for anyone in this profession. This new edition now contains essential information on steganalysis and steganography New concepts and new applications including QIM introduced Digital watermark embedding is given a complete update with new processes and applications

Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual PropertySteganography and Digital Watermarking Techniques for Protection of Intellectual PropertyIGI Global

This book is a collection of outstanding content written by experts working in the field of multimedia security. It provides an insight about various techniques used in multimedia security and identifies its progress in both technological and algorithmic perspectives. In the contemporary world, digitization offers an effective mechanism to process, preserve and transfer all types of information. The incredible progresses in computing and communication technologies augmented by economic feasibility have revolutionized the world. The availability of efficient algorithms together with inexpensive digital recording and storage peripherals have created a multimedia era bringing conveniences to people in sharing the digital data that includes images, audio and video. The ever-increasing pace, at which the multimedia and communication technology is growing, has also made it possible to combine, replicate and distribute the content faster and easier, thereby empowering mankind by having a wealth of information at their disposal. However, security of multimedia is giving tough time to the research community around the globe, due to ever-increasing and efficient attacks carried out on multimedia data by intruders, eves-droppers and hackers. Further, duplication, unauthorized use and mal-distribution of digital content have become a serious challenge as it leads to copyright violation and is considered to be the principal reason that refrains the information providers in freely sharing their proprietary digital content. The book is useful for students, researchers and professionals to advance their study.

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field in multimedia security. Two related disciplines, steganalysis and data

forensics, are also increasingly attracting researchers and forming another new research field in multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This inaugural issue contains five papers dealing with a wide range of topics related to multimedia security. The first paper deals with evaluation criteria for the performance of audio watermarking algorithms. The second provides a survey of problems related to watermark security. The third discusses practical implementations of zero-knowledge watermark detectors and proposes efficient solutions for correlation-based detectors. The fourth introduces the concept of Personal Entertainment Domains (PED) in Digital Rights Management (DRM) schemes. The fifth reports on the use of fusion techniques to improve the detection accuracy of steganalysis.

Multimedia Security: Watermarking, Steganography, and Forensics outlines essential principles, technical information, and expert insights on multimedia security technology used to prove that content is authentic and has not been altered. Illustrating the need for improved content security as the Internet and digital multimedia applications rapidly evolve, this book presents a wealth of everyday protection application examples in fields including multimedia mining and classification, digital watermarking, steganography, and digital forensics. Giving readers an in-depth overview of different aspects of information security mechanisms and methods, this resource also serves as an instructional tool on how to use the fundamental theoretical framework required for the development of extensive advanced techniques. The presentation of several robust algorithms illustrates this framework, helping readers to quickly master and apply fundamental principles. Presented case studies cover: The execution (and feasibility) of techniques used to discover hidden knowledge by applying multimedia duplicate mining methods to large multimedia content Different types of image steganographic schemes based on vector quantization Techniques used to detect changes in human motion behavior and to classify different types of small-group motion behavior Useful for students, researchers, and professionals, this book consists of a variety of technical tutorials that offer an abundance of graphs and examples to powerfully convey the principles of multimedia security and steganography. Imparting the extensive experience of the contributors, this approach simplifies problems, helping readers more easily understand even the most complicated theories. It also enables them to uncover novel concepts involved in the implementation of algorithms, which can lead to the discovery of new problems and new means of solving them.

Communications and Multimedia Security is an essential reference for both academic and professional researchers in the fields of Communications and Multimedia Security. This state-of-the-art volume presents the proceedings of the Eighth Annual IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, September 2004, in Windermere, UK. The papers presented here represent the very latest developments in security research from leading people in the field. The papers explore a wide variety of subjects including privacy protection and trust negotiation, mobile security, applied cryptography, and security of communication protocols. Of special interest are several papers which addressed security in the Microsoft .Net architecture, and the threats that builders of web service applications need to be aware of. The papers were a result of research sponsored by Microsoft at five European University research centers. This

collection will be important not only for multimedia security experts and researchers, but also for all teachers and administrators interested in communications security.
"The book discusses new aspects of digital watermarking in a worldwide context"--Provided by publisher.
Multimedia security has become a major research topic, yielding numerous academic papers in addition to many watermarking-related companies. In this emerging area, there are many challenging research issues that deserve sustained study towards an effective and practical system. This book explores the myriad of issues regarding multimedia security, including perceptual fidelity analysis, image, audio, and 3D mesh object watermarking, medical watermarking, error detection (authentication) and concealment, fingerprinting, digital signature and digital right management.
Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. The seven papers included in this special issue were carefully reviewed and selected from 21 submissions. They address the challenges faced by the emerging area of visual cryptography and provide the readers with an overview of the state of the art in this field of research.
Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. The 7 papers included in this issue deal with the following topics: protection of digital videos, secure watermarking, tamper detection, and steganography.
Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. The six papers included in this issue deal with watermarking security, perceptual image hashing, infrared hiding, steganography and steganalysis.
This book constitutes the proceedings of the International Conference on Information and Communication Technologies held in Kochi, Kerala, India in September 2010.
"This book offers an in-depth explanation of multimedia technologies within their many specific application areas as well as presenting developing trends for the future"--Provided by

publisher.

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This second issue contains five papers dealing with a wide range of topics related to multimedia security. The first paper introduces Fingercasting, which allows joint fingerprinting and decryption of broadcast messages. The second paper presents an estimation attack on content-based video fingerprinting. The third proposes a statistics and spatiality-based feature distance measure for error resilient image authentication. The fourth paper reports on LTSB steganalysis. Finally, the fifth paper surveys various blind and robust watermarking schemes for 3D shapes.

Every day millions of people capture, store, transmit, and manipulate digital data. Unfortunately free access digital multimedia communication also provides virtually unprecedented opportunities to pirate copyrighted material. Providing the theoretical background needed to develop and implement advanced techniques and algorithms, Digital Watermarking and Steganography: Demonstrates how to develop and implement methods to guarantee the authenticity of digital media Explains the categorization of digital watermarking techniques based on characteristics as well as applications Presents cutting-edge techniques such as the GA-based breaking algorithm on the frequency-domain steganalytic system The popularity of digital media continues to soar. The theoretical foundation presented within this valuable reference will facilitate the creation on new techniques and algorithms to combat present and potential threats against information security.

Since the mid 1990s, data hiding has been proposed as an enabling technology for securing multimedia communication, and is now used in various applications including broadcast monitoring, movie fingerprinting, steganography, video indexing and retrieval, and image authentication. Data hiding and cryptographic techniques are often combined to complement each other, thus triggering the development of a new research field of multimedia security. Besides, two related disciplines, steganalysis and data forensics, are increasingly attracting researchers and becoming another new research field of multimedia security. This journal, LNCS Transactions on Data Hiding and Multimedia Security, aims to be a forum for all researchers in these emerging fields, publishing both original and archival research results. This issue consists mainly of a special section on content protection and forensics including four papers. The additional paper deals with histogram-based image hashing for searching content-preserving copies.

Communications represent a strategic sector for privacy protection and for personal, company, national and international security. The interception, damage or lost of information during communication can generate material and non material economic damages from both a personal and collective point of view. The purpose of this book is to give the reader information relating to all aspects of communications security, beginning at the base ideas and building to reach the most advanced and updated concepts. The book will be of interest to integrated system designers, telecommunication designers, system engineers,

system analysts, security managers, technicians, intelligence personnel, security personnel, police, army, private investigators, scientists, graduate and postgraduate students and anyone that needs to communicate in a secure way.

The 22 full papers and 12 shorts papers presented in this volume were carefully reviewed and selected from 70 submissions. The contributions are covering the following topics: deep learning for multimedia security; digital forensics and anti-forensics; digital watermarking; information hiding; steganography and steganalysis; authentication and security.

This book constitutes the refereed proceedings of the 4th International Workshop on Digital Watermarking Secure Data Management, IWDW 2005, held in Siena, Italy in September 2005. The 31 revised full papers presented were carefully reviewed and selected from 74 submissions. The papers are organized in topical sections on steganography and steganalysis, fingerprinting, watermarking, attacks, watermarking security, watermarking of unconventional media, channel coding and watermarking, theory, and applications.

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 volume constitutes the refereed proceedings of six workshops held at the 9th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, SpaCCS 2016, held in Zhangjiajie, China, in November 2016: the 7th International Workshop on Trust, Security and Privacy for Big Data, TrustData 2016; the 6th International Symposium on Trust, Security and Privacy for Emerging Applications, TSP 2016; the 4th International Workshop on Network Optimization and Performance Evaluation, NOPE 2016; the Second International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications, DependSys 2016; the Annual Big Data Security, Privacy and Trust Workshop, BigDataSPT 2016; and the First International Workshop on Cloud Storage Service and Computing, WCSSC 2016. The 37 full papers presented were carefully reviewed and selected from 95 submissions. The papers deal with research findings, ideas and emerging trends in information security research and cover a broad range of topics in security, privacy and anonymity in computation, communication and storage.