Multimedia Security Watermarking Steganography And Forensics

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
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.
Multimedia SecurityWatermarking, Steganography, and ForensicsCRC Press
Transactions on Data Hiding and Multimedia Security VI
Transactions on Data Hiding and Multimedia Security VIII
Communications and Multimedia Security
17-20 January 2005, San Jose, California, USA.
Transactions on Data Hiding and Multimedia Security X

"The digital revolution is affecting our daily activities, changing our habits and indeed reshaping cultures around the world. The intellectual products of today are now primarily created and distributed in digital format. Furthermore, the Internet has become a pervasive communication and sharing network. All of these factors naturally have led to concerns over the security of digital information. Among the many proposed solutions to such concerns, digital watermarking has proven to be unique by its not requiring a safe auxiliary communication channel. However, proposed watermarking techniques and attacks against such methods make the watermarking problem dynamic, complicated, and challenging. We show that several of the requirements in watermarking applications can be mapped onto convex constraints or can be closely approximated as convex constraints. These include watermark detectability, robustness to added noise, multiple watermark detectability, imperceptibility, robustness against lossy compression, robustness against lowpass filtering attacks, robustness against non-linear soft/hard wavelet shrinkage denoising attacks, and fragility under aggressive compression. This approach allows determination of feasible solutions by using the powerful method of projections onto convex sets (POCS). The POCS algorithm is employed to create a watermarked image that satisfies all watermarking requirements simultaneously. We further extend the POCS formulation of watermark design into constrained optimization formulations for the scenarios where a single performance criterion may need to be optimized. We propose an algorithmic framework for solving these optimal embedding problems via a multi-step feasibility approach that combines projections onto convex sets (POCS) based feasibility watermarking with a bisection parameter search for determining the optimum value of the objective function and the optimum watermarked image. The framework is general and can handle optimum watermark embedding problems with convex and quasi-convex formulations of constraints and furthermore the algorithm has assured convergence to the global optimum. The proposed scheme is a natural extension of set-theoretic watermark design and provides a link between convex feasibility and optimization formulations for watermark embedding. We demonstrate a number of optimal watermark embeddings in the proposed framework corresponding to maximal robustness to additive noise, maximal robustness against compression, minimal frequency weighted perceptual distortion, and minimal texture watermark visibility. Experimental results demonstrate that the framework is effective in optimizing the desired characteristic while meeting the constraints. The results also highlight both anticipated and unanticipated competition between the common requirements for watermark embedding. Utilizing the same framework, we also pose the problem of determining a steganographic image as a feasibility problem subject to constraints of data communication, imperceptibility, and statistical indistinguishability with respect to the steganalyzer's features. A stego image is then determined using set theoretic feasible point estimation methods. The proposed framework is applied to a state of the art steganalysis method based on higher order statistics (HOS) steganalysis. We show that the steganographer can significantly reduce the classification performance of the steganalyzer by employing a statistical constraint during embedding, although the image is highly distorted. Then we show that the steganalyzer can develop a counter-strategy against the steganographer's actions to gain back some classification performance. This interchange represents an empirical iteration in the game between the steganographer and steganalyzer. Finally, we consider mixture strategies to find the Nash equilibrium of the interplay. The framework is general and suits many other important multimedia security problems such as fingerprinting, multiple watermark embedding, fractional Fourier transform domain watermark embedding, and improved embedding efficiency for pre-coding. We describe a set theoretic formulation of some of these problems as well. The set theoretic approach in watermarking design is systematic, flexible, and it has desirable properties that are hard to replicate in other methods. Specifically, it enables many requirements defined in various transform domains to be handled simultaneously, and it offers great flexibility of the design formulation"--Page viii-ix.

Modern internet-enabled devices and fast communication technologies have ushered in a revolution in sharing of digital images and video. This may be for social reasons or for commercial and industrial applications, where the data is more likely to include sensitive personal or confidential information. In any event, the shared imagery is intended only for the end-user. Attackers can steal this data or manipulate it for their own uses, causing financial and emotional damage to the owners. Many applications generate important information in the form of images and video, where efficient security is critical. This drives the need for advanced security solutions and the need to continuously develop and maintain security measures in an ever-evolving battle against fraud and malicious intent. There are various techniques employed in protecting digital media and information, such as digital watermarking, cryptography, stenography, data encryption, etc., In addition, sharing platforms and connected nodes themselves may be open to vulnerabilities and can suffer from security breaches. This book reviews present state-of-the-art research related to the security of digital imagery and video, including developments in machine learning applications. It is particularly suited for those that bridge the academic world and industry, and allows readers to understand the security concerns in the multimedia domain by reviewing present and evolving security solutions, their limitations, and future research directions. Key Features Latest trends in the multimedia security domain Includes Machine Learning for multimedia security Insight to different security concerns (attacks) Reviews present challenges & future opportunities Potential & promising solution to the security concerns

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.

Security, Steganography, and Watermarking of Multimedia Contents
Applications to Watermarking, Steganography, Fingerprinting, and Beyond
Digital Watermarking and Steganography
Set Theoretic Framework for Multimedia Security and Data Hiding

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.

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 intends to provide a comprehensive overview on different aspects of mechanisms and techniques for information security. It is written for students, researchers, and professionals studying in the field of multimedia security and steganography. Multimedia security and steganography is especially relevant due to the global scale of digital multimedia and the rapid growth of the Internet. Digital watermarking technology can be used to guarantee authenticity and can be applied as proof that the content has not been altered since insertion. Updated techniques and advances in watermarking are explored in this new edition. The combinational spatial and frequency domains watermarking technique provides a new concept of enlarging the embedding capacity of watermarks. The genetic algorithm (GA) based watermarking technique solves the rounding error problem and provide an efficient embedding approach. Each chapter provides the reader with a fundamental, theoretical framework, while developing the extensive advanced techniques and considering the essential principles of the digital watermarking and steganographic systems. Several robust algorithms that are presented throughout illustrate the framework and provide assistance and tools in understanding and implementing the fundamental principles.

16-19 January 2006, San Jose, California, USA.
Algorithm Development, Analysis and Applications
Intelligent Techniques in Signal Processing for Multimedia Security
Transactions on Data Hiding and Multimedia Security III
Multimedia Security Technologies for Digital Rights 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, thu
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
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.
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.
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: D
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 fo
this valuable reference will facilitate the creation on new techniques and algorithms to combat present and potential threats against information security.
Security, Steganography, and Watermarking of Multimedia Contents VI
Security, Steganography, and Watermarking of Multimedia Contents VIII
14th IFIP TC 6/TC 11 International Conference, CMS 2013, Magdeburg, Germany, September 25-26, 2013. Proceedings
Advanced Security Solutions for Multimedia
Fundamentals and Techniques, Second Edition

Proceedings of SPIE present the original research papers presented at SPIE conferences and other high-quality conferences in the broad-ranging fields of optics and photonics. These books provide prompt access to the latest innovations in research and technology in their respective fields. Proceedings of SPIE are among the most cited references in patent literature.
This inaugural issue of the LNCS Transactions on Data Hiding and Multimedia Security contains five papers dealing with a wide range of topics related to multimedia security, from a survey of problems related to watermark security to an introduction to the concept of Personal Entertainment Domains (PED) in Digital Rights Management (DRM) schemes.
Includes Proceedings Vol. 7821
Security, Steganography, and Watermarking of Multimedia Contents IX
Multimedia Watermarking Techniques and Applications
Transactions on Data Hiding and Multimedia Security IV
28-30 January 2008, San Jose, California, USA
Transactions on Data Hiding and Multimedia Security I

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.

This book proposes new algorithms to ensure secured communications and prevent unauthorized data exchange in secured multimedia systems. Focusing on numerous applications' algorithms and scenarios, it offers an in-depth analysis of data hiding technologies including watermarking, cryptography, encryption, copy control, and authentication. The authors present a framework for visual data hiding technologies that resolves emerging problems of modern multimedia applications in several contexts including the medical, healthcare, education, and wireless communication networking domains. Further, it introduces several intelligent security techniques with real-time implementation. As part of its comprehensive coverage, the book discusses contemporary multimedia authentication and fingerprinting techniques, while also proposing personal authentication/recognition systems based on hand images, surveillance system security using gait recognition, face recognition under restricted constraints such as dry/wet face conditions, and three-dimensional face identification using the approach developed here. This book equips perception technology professionals with the latest technologies, techniques, and strategies for multimedia security systems, offering a valuable resource for engineers and researchers working to develop security systems.

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.

19-22 January 2004, San Jose, California, USA
Transactions on Data Hiding and Multimedia Security VII
17-20 January, 2005, San Jose, California, USA
Digital Watermarking
Data Hiding and Its Applications

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

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.

This book focuses on image based security techniques, namely visual cryptography, watermarking, and steganography. This book is divided into four sections. The first section explores basic to advanced concepts of visual cryptography. The second section of the book covers digital image watermarking including watermarking algorithms, frameworks for modeling watermarking systems, and the evaluation of watermarking techniques. The next section analyzes steganography and steganalysis, including the notion, terminology and building blocks of steganographic communication. The final section of the book describes the concept of hybrid approaches which includes all image-based security techniques. One can also explore various advanced research domains related to the multimedia security field in the final section. The book includes many examples and applications, as well as implementation using MATLAB, wherever required. Features: Provides a comprehensive introduction to visual cryptography, digital watermarking and steganography in one book Includes real-life examples and applications throughout Covers theoretical and practical concepts related to security of other multimedia objects using image based security techniques Presents the implementation of all important concepts in MATLAB

Multimedia Security

Multimedia Forensics and Security

Security, Forensics, Steganography, and Watermarking of Multimedia Contents X

8th International Workshop, IWDW 2009, Guildford, UK, August 24-26, 2009, Proceedings

Multimedia Security Handbook

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.

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.

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

Security, Steganography, and Watermarking of Multimedia Contents VII

4th International Workshop, IWDW 2005, Siena, Italy, September 15-17, 2005, Proceedings

Steganography and Digital Watermarking Techniques for Protection of Intellectual Property

Transactions on Data Hiding and Multimedia Security IX

Handbook of Image-based Security Techniques

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.

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.

Intellectual property owners must continually exploit new ways of reproducing, distributing, and marketing their products. However, the threat of piracy looms as a major problem with digital distribution and storage technologies. Multimedia Watermarking Techniques and Applications covers all current and future trends in the design of modern

16-19 January, 2006, San Jose, California, USA

Proceedings of Electronic Imaging Science and Technology : 19-22 January 2004, San Jose, California, USA

Fundamentals and Techniques

Watermarking, Steganography, and Forensics

Special Issue on Visual Cryptography

Data hiding techniques have been widely used to provide copyright protection, data integrity, covert communication, non-repudiation, and authentication, among other applications. In the context of the increased dissemination and distribution of multimedia content over the internet, data hiding methods, such as digital watermarking and steganography, are becoming increasingly relevant in providing multimedia security. The goal of this book is to focus on the improvement of data hiding algorithms and their different applications (both traditional and emerging), bringing together researchers and practitioners from different research fields, including data hiding, signal processing, cryptography, and information theory, among others.

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.