Multimedia Security Watermarking Steganography And Forensics

Multimedia SecurityWatermarking, Steganography, and ForensicsCRC Press
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.
This book constitutes the refereed proceedings of the 12th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security, CMS 2010, held in Ghent, Belgium, in October 2011. The 26 revised papers presented were carefully reviewed and selected from 52 submissions. The papers are organized in topical sections on usability, architecture and framework security, mobile identity management, secure hardware platforms, biometrics, multimedia security, network security and authentication.

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.

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.

"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 precoding. 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.

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.

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.

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.

The volume contains the papers presented at the fifth working conference on Communications and Multimedia Security (CMS 2001), held on May 21-22, 2001 at (and organized by) the GMD -German National Research Center for Information Technology GMD - Integrated Publication and Information Systems Institute IPSI, in Darmstadt, Germany. The conference is arranged jointly by the Technical Committees 11 and 6 of the International Federation of Information Processing (IFIP) The name "Communications and Multimedia Security" was first used in 1995, Reinhard Posch organized the first in this series of conferences in Graz, Austria, following up on the previously national (Austrian) "IT Sicherheit" conferences held in Klagenfurt

(1993) and Vienna (1994). In 1996, the CMS took place in Essen, Germany; in 1997 the conference moved to Athens, Greece. The CMS 1999 was held in Leuven, Belgium. This conference provides a forum for presentations and discussions on issues which combine innovative research work with a highly promising application potential in the area of security for communication and multimedia security. State-of-the-art issues as well as practical experiences and new trends in the areas were topics of interest again, as it has already been the case at previous conferences. This year, the organizers wanted to focus the attention on watermarking and copyright protection for e commerce applications and multimedia data. We also encompass excellent work on recent advances in cryptography and their applications. In recent years, digital media data have enormously gained in importance.

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.

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

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.

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 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.

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.

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.

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 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.

Information Hiding: Steganography and Watermarking - Attacks and Countermeasures deals with information hiding. With the proliferation of multimedia on the Internet, information hiding addresses two areas of concern: privacy of information from surveillance (steganography) and protection of intellectual property (digital watermarking). Steganography (literally, covered writing) explores methods to hide the existence of hidden messages. These methods include invisible ink, microdot, digital signature, covert channel, and spread spectrum communication. Digital watermarks represent a commercial application of steganography. Watermarks can be used to track the copyright and ownership of electronic media. In this volume, the authors focus on techniques for hiding information in digital media. They analyze the hiding techniques to uncover their limitations. These limitations are employed to devise attacks against hidden information. The goal of these attacks is to expose the existence of a secret message or render a digital watermark unusable. In assessing these attacks, countermeasures are developed to assist in protecting digital watermarking systems. Understanding the limitations of the current methods will lead us to build more robust methods that can survive various manipulation and attacks. The more information that is placed in the public's reach on the Internet, the more owners of such information need to protect themselves from theft and false representation. Systems to analyze techniques for uncovering hidden information and recover seemingly destroyed information will be useful to law enforcement authorities in computer forensics and digital traffic analysis. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures presents the authors' research contributions in three fundamental areas with respect to image-based steganography and watermarking: analysis of data hiding techniques, attacks against hidden information, and countermeasures to attacks against digital watermarks. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures is suitable for a secondary text in a graduate level course, and as a reference for researchers and practitioners in industry.

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.

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.

Multimedia services involve processing, transmission and retrieval of multiple forms of information. Multimedia services have gained momentum in the past few years due to the easy availability of computing power and storage media. Societyisdemandinghuman-likeintelligentbehaviour,suchasadaptationand generalization, from machines every day. With this view in mind, researchers are working on fusing intelligent paradigms such as arti?cial neural networks, swarm intelligence, arti?cial immune systems, evolutionary computing and multiagents with multimedia services. Arti?cial neural networks use neurons, interconnected using various schemes, for fusing learning in multimedia-based systems. Evolutionary c- puting techniques are used in tasks such as optimization. Typical multiagent systems are based on

Belief-Desire-Intention model and act on behalf of the users. Typical examples of intelligent multimedia services include digital - braries, e-learning and teaching, e-government, e-commerce, e-entertainment, e-health and e-legal services. This book includes 15 chapters on advanced tools and methodologies pertaining to the multimedia services. The authors and reviewers have c- tributed immensely to this research-oriented book. We believe that this - search volume will be valuable to professors, researchers and students of all disciplines, such as computer science, engineering and management. We express our sincere thanks to Springer-Verlag for their wonderful e- torial support.

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.

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 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.

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.

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

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.

Includes Proceedings Vol. 7821

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.