Chapter 1 : DoktorBook: Read Books Online For Free

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.

Watermarking synchronization Reviews and Testimonials This book aims to create a collection of quality chapters on information hiding for multimedia forensics and security contributed by leading experts in the related fields. Most people, if not all, with access to computers and internets, can not share information instantly at insignificant cost, but also creatively produce their own media of various forms, such as text, audio, speech, music, image and video. This wave of ICT revolution has undoubtedly brought about enormous opportunities for the world economy and exciting possibilities for every sector of the modern societies. However, this type of close and strong interweaving poses concerns and threats either. When exploited with malign intentions, the same tools provide means for doing harms at colossal scale. These concerns create anxiety and uncertainty about the reality of the media we deal with. In response to these issues, the last decade has seen the emergence of the new interdisciplinary field of multimedia forensics and security, which aims at pooling expertise in various areas, such as signal processing, information theory, cryptography, etc, to combat the abuses of the ICT and multimedia techniques. In particular, digital watermarking schemes have been proposed to meet copyright protection needs, e. Challenged by its competing steganalytical techniques, steganographic methods have been developed and are being constantly improved for data hiding and embedding applications. Multimedia forensic techniques have also been studied and derived for providing evidences to aid resolving civil and criminal court cases. Added to the excitement of the races between new measures and countermeasures in this new area is the difficulties in striking a balance between conflicting requirements. For example, in the context of digital watermarking, high robustness is usually gained at the expense of high distortion, while, in the context of steganography, low distortion is, most of the times, achieved at the cost of low payload. The book aims to create a collection of quality chapters on information hiding for multimedia forensics and security contributed by leading experts in the related fields. This book consists of three main components. The first component, comprised of Chapters I to VII, aims at dissimilating the idea of digital watermarking and its applications to multimedia security in general and copyright protection in particular. The third component, comprising Chapters XIV to XVI, deals with methods harnessing the techniques of data hiding and cryptography for the applications of multimedia forensics. Chapter I, Authentication Watermarkings for Binary Images, presented by Hae Yong Kim, Sergio Pamboukian, and Paulo Barreto, is concerned with a class of data hiding techniques and the analysis of which of them are suitable for authenticating binary images. A new irreversible scheme for authenticating JBIG2-compressed binary images and a new reversible algorithm for authenticating general binary images are presented. In Chapter II, Secure Multimedia Content Distribution Based on Watermarking Technology, Shiguo Lian defines the performance requirements of watermarking-based multimedia distribution schemes for multimedia communication applications and reviewed a number of related schemes, with their characteristics and limitations discussed. A new scheme combining fingerprinting and encryption, which realises both confidentiality protection and copyright protection, is then presented to address the issues, such as traitor tracing, robustness and imperceptibility, surrounding multimedia distribution and to meet the defined requirements. To overcome the flaws found in the watermark extraction component of some discussed SVD-based schemes, Maria Calagna proposes a new SVD-based scheme for watermarking geographical and spatial images exchanged among a group of GIS users. In Chapter IV, Digital Video Watermarking and the Collusion Attack, Roberto Caldelli and Alessandro Piva present a taxonomy of video watermarking techniques according to data formats and signal processing tools employed for implementation. The idea and types of collusion attacks are then analysed. Chapter V, A Survey of Current Watermarking Synchronization Techniques, authored by Natasa Terzija, deals with the synchronization issue of watermark detection under the threat of geometric distortions, such as translation, cropping, rotation, scaling, affine transformation,

projective transformation, etc. Natasa Terija gives an overview of different techniques, including image registration techniques, the exhaustive search, periodical sequences, the use of synchronization marks, content-based approaches and concludes that the existing techniques can only provide partial robustness against geometrical distortions and more efforts are yet to be made before proper solutions can be put in place. In Chapter VI, On the Necessity of Finding Content before Watermark Retrieval â€" Active Search Strategies for Localizing Watermarked Media on the Internet, Martin Steinebach and Patrick Wolf state that embedding digital watermark for copyright protection is only a passive protection and, to complete the protection, an active mechanism capable of finding potentially watermarked media that have been distributed is needed before the watermark extraction can actually be carried out to help fight illegal copies. This chapter discusses important issues regarding the search for watermarked content on the internet and introduces strategies and approaches for retrieving watermarks from the Internet with the help of a media search framework. In Chapter VII, Statistical Watermark Detection in the Transform Domain for Digital Images, Fouad Khelif, Fatih Kurugollu, and Ahmed Bouridane view the problem of multiplicative watermark detection in digital images as a binary decision where the observation is the possibly watermarked samples that can be thought of as a noisy environment in which a desirable watermark may exist. They investigate optimum watermark detection from the viewpoint of decision theory. Different transform domains are considered with generalized noise models and the effects of the watermark strength on both the detector performance and the imperceptibility of the host image are studied. In the face of the fact that many data hiding techniques give rise to changes to the cover media that appear to be noise, Christopher Smith and Sos Agaian state in this chapter that steganography can be defined in terms of adding some type of artificial noise and review a series of state-of-the-art noise-like steganographic schemes. The authors also present information for the reader to understand how noise is unintentionally and intentionally exploited in information hiding and show how passive and active steganalysis can be applied to attack steganographic schemes. Results of using advanced clean image estimation techniques for steganalysis under the active warden scenario are also presented. Among the many conflicting requirements of digital watermarking and data hiding, visibility or embedding distortion inflicted on the host media by the marking process is of significant concern. Chapter IX, Visibility Control and Quality Assessment of Watermarking and Data Hiding Algorithms, contributed by Patrick Le Callet and Florent Autrusseau, deals with both the subjective and objective quality assessment of images and video in the context of digital watermarking and data hiding applications. The deficiencies of some quality metrics for data hiding purpose are highlighted. Subjective experimental protocols are conducted. A quality benchmark aiming at identifying the objective metrics among many that best predicts subjective scores is presented. This allows the reader to look at steganographic secrecy based on reasonable complexity assumptions similar to that ones commonly accepted in modern cryptography. The authors expand the analyses of stegosystems beyond security aspects that practitioners find difficult to implement to the tractability aspects, i. These questions concern the maximum achievable security for different steganography scenarios and the limitations in terms of time efficiency associated with stegosystems that achieve the highest levels of security. In Chapter XI, On Steganalysis and Clean Image Estimation, Christopher Smith and Sos Agaian expand on the idea of exploiting the noise-like qualities of steganography and discuss its competing technology of steganalysis, the art and science of detecting hidden information in media. From these ideas of clean image estimation, the steganalysis problems faced by the passive warden are formulated as a three-stage process of estimation, feature extraction, and classification the EFC formulation. Trends and Challenges, by Hafiz Malik, R. Subbalakshmi provide a detailed overview of the state-of-the-art techniques in steganalysis. The performance of existing steganalysis techniques are compared based on critical parameters such as the hidden message detection probability, the accuracy of the hidden message length and secret key estimates, and the message recovery rate. The growing gap between recent developments in the steganographic research and the state-of-the-art of steganalysis are also discussed. Chapter XIII, Benchmarking SteganalysisDigital Camera Source Identification, presented by Matthew Sorell, is concerned with the identification of the make, the model series and the particular source camera of a particular digital photograph. Chapter XV, Traitor Tracing for Multimedia Forensics, authored by Hongxia Jin, reviews potential pirate attacks on multimedia content distribution systems and discusses how

traitor tracing techniques can be used to defend against those attacks by tracing the attackers and colluders involved in the piracy. This chapter is also concerned with business scenarios that involve one-way digital content distribution and a large set of receiving users. It shows how to address many overlooked practical concerns and brings first hand experience on bringing this technology to practice in the context of new industry standard on content protection for next generation high-definition DVDs. These methods are efficient in terms of the computational costs of encryption. A classical bitstream-based approach employing format-compliant encryption of packet body data is compared against a compression-integrated technique, which uses the concept of wavelet packet transform. Naval Postgraduate School in the second half of He has involved in the organisation of a number of international conferences and workshops and also served as member of the international program committees for several international conferences. His research interests include digital forensics, multimedia security, bioinformatics, computer vision, image processing, pattern recognition, evolutionary computation, machine learning and content-based image retrieval.

Chapter 2 : Multimedia Forensics And Security: Foundations, Innovations, And Applications Download

The book also covers the theme of multimedia forensics and watermarking in the area of information security. That includes highlights on intelligence techniques designed for detecting significant changes in image and video sequences.

The ubiquity of broadband networks and the advance in multimedia technologies have inspired people all over the world to enjoy and share multimedia over networks. However, the same tools that enable us to create and distribute multimedia easily also facilitate the illegal alteration, repackaging and unauthorized redistribution of multimedia. These illicit copies pose serious threats to both governmental operations and commercial applications. Cryptographic tools and access control support the secure delivery of multimedia over networks, whose protection usually terminates after the content is delivered and decrypted. To address the post-delivery protection of multimedia, digital fingerprinting is an emerging technology to identify users who have legitimate access to the plaintext content but use it for unintended purposes. Ensuring the appropriate use of multimedia content, however, is no longer a security issue with a single adversary. A group of attackers with differently fingerprinted versions of the same content can collectively mount attacks known as multi-user collusion attacks and effectively remove the traces of the fingerprints. Multimedia fingerprints should not only be robust against attacks by a single attacker, they should also resist such multi-user collusion. This requires the digital rights enforcer to have a profound understanding of multi-user collusion and design anti-collusion fingerprints for multimedia. The general frame of embedded fingerprinting for multimedia. We take an interdisciplinary approach to understand the challenges and analyze the performance of the digital fingerprinting technology for multimedia content protection. Our research addresses the following issues in multimedia fingerprinting and traitor tracing: One method is simply to synchronize the media signals and average them, which is an example of the linear collusion attack. Another collusion attack, referred to as the copy-and-paste attack, involves users cutting out portions of each of their media signals and pasting them together to form a new signal. Other attacks may employ nonlinear operations, such as taking the maximum or median of the values of corresponding components of individual copies. We examine various types of collusion, including the linear averaging and a few nonlinear collusion attacks, and analyze their effectiveness in removing the fingerprints and the perceptual quality of the colluded copy under different collusion attacks. Traitor tracing capability of multimedia forensic systems In order to facilitate the design of multimedia forensic systems for applications with different protection requirements, one critical research direction is evaluating the resistance performance of specific fingerprinting schemes when considering different types of attacks. We evaluate the fundamental limits of orthogonal multimedia fingerprints, and evaluates the maximum number of colluders that digital fingerprinting systems can withstand as a function of the system parameters, including the fingerprint length, the total number of users, and the system performance requirements. Such analysis enables the digital rights enforcer to understand which factors limits the traitor tracing capability of the forensic systems and provides important guidelines for collusion resistant multimedia fingerprint design. Secure fingerprint multicast The popularity of networked multimedia systems relies on the ability to provide reliable, low-cost, and secure services to all parties in the systems. For networked video applications where a huge amount of data have to be distributed to a large number of users, bandwidth efficiency is an important issue to be addressed by the service providers. In order to accommodate more users, multicast is often used to minimize the communication cost in the data distribution. For streaming applications with traitor tracing requirement, employing digital fingerprinting technology poses new challenges to the secure and efficient distribution of multimedia. This comes from the fact that traditional multicast technology cannot be directly applied to fingerprinted multimedia since copies distributed to different users contain unique fingerprints and are not identical. Our work collectively addresses the security and bandwidth efficiency for networked multimedia systems, and investigates the secure fingerprint multicast technology. Successful "traitor tracing" in real life: A preliminary technology based on robust watermarking was adopted in the Oscar Season and successfully captured a few pirates who helped illegally post Oscar screeners on the Internet.

DOWNLOAD PDF MULTIMEDIA FORENSICS AND SECURITY

Chapter 3 : Special Issue on Data-driven Multimedia Forensics and Security - Call for Papers - Elsevier

Multimedia Forensics and Security pdf This book presents recent applications and approaches as well as challenges in digital forensic science. One of the evolving challenges that is covered in the book is the cloud forensic analysis which applies the digital forensic science over the cloud computing paradigm for conducting either live or static.

Chapter 4 : Multimedia Forensics and Security

Get this from a library! Multimedia forensics and security. [Chang-Tsun Li;] -- "This book 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.

Chapter 5 : MSDF International Symposium on Multimedia Security and Digital Forensics

This book presents recent applications and approaches as well as challenges in digital forensic science. One of the evolving challenges that is covered in the book is the cloud forensic analysis which applies the digital forensic science over the cloud computing paradigm for conducting either live.