IEEE ICME 2007 Tutorial Proposal

Title:

Multimedia Security Technologies for Digital Rights Management

Lecturers:

Prof. Wenjun Zeng, University of Missouri (zengw@missouri.edu)
Dr. Bin Zhu, Microsoft Research Asia (binzhu@microsoft.com)
Dr. Hongxia Jin, IBM Almaden Research Center (jin@us.ibm.com)
Dr. Qibin Sun, Institute of Infocomm Research (qibin@i2r.a-star-edu.sg)
Dr. Ching-Yung Lin*, IBM Watson Research Center (chingyung@us.ibm.com)
Dr. Heather Yu, Huawei Technologies USA (heathery@ieee.org)

*: lecturer for correspondence

Introduction:

The explosive combination of digital signal processing, computing devices and digital networks have enabled pervasive digital media distribution that allows flexible and cost-effective multimedia commerce transactions. The digital nature of information also allows individuals to access, duplicate or manipulate information beyond the terms and conditions agreed upon. For instance, widespread piracy of copyrighted audio or video content using peer-to-peer networking has caused significant tension between members of the entertainment industry and free-speech advocates regarding the *fair use* of digital content. The large-scale acceptance of digital distribution rests on its ability to provide legitimate services to all competing stakeholders. This requires secure e-commerce systems that allow convenient use of digital content while equitably compensating members of the information distribution/consumption chain. Digital Rights Management (DRM), a critical component of such secure e-commerce systems, defines a set of tools that manage the trusted use of digital media content on electronic devices, ranging from personal computer, digital video recorder, DVD player, Music player, PDA, to mobile phones and other embedded devices. Various multimedia security technologies, such as encryption, watermarking, key managements, etc., have been designed to achieve this goal. To make DRM systems trustworthy to all players is more than just a technical issue. A truly effective approach requires solid engineering as well as a social, business and legal infrastructure. The market for DRM products and services is burgeoning and the search for the balance has been on-going.

Target Audience

This tutorial intends to provide a comprehensive coverage of the state-of-the-art multimedia security technologies for the Digital Rights Management (DRM) applications. Although DRM has been in the spotlight in recent years, a thorough

introduction is seldom available, due to its cross-disciplinary nature. We hope this tutorial can bring in the audiences who have ever been intrigued by the buzz-word DRM and are interested in finding out more; who are a manager or engineer developing a DRM system; who plan to offer topic courses on multimedia security in schools; who are curious about the hacking by a Norwegian teenager of the Content Scrambling System defined to protect the content of DVDs; who have been alerted to the on-line music sharing debates; or who are concerned about the potential implications of the recently enacted Digital Millennium Copyright Act in light of the arrest of the Russian programmer who circumvented Adobe Systems' eBook Reader DRM. In particular, this tutorial serves perfectly as a comprehensive introduction on DRM for researchers, system engineers and algorithm developers. It can be also used as a roadmap for graduate students or professors who are starting to research in the field of multimedia security and digital rights management.

Content and Outline

Multimedia Security Technologies for Digital Rights Management is one continuous tutorial that has been harmonized to provide the audience with a comprehensive coverage of the fundamentals and the latest development of multimedia security technologies targeted for the DRM applications. It also reflects other non-technical (i.e., social and legal) aspects of DRM. The lecturers include technology visionary and leading researchers in the field, many of whom are also active DRM standards contributors and industrial practitioners.

1) Introduction to DRM: Fundamental Technologies (1 hr) [Wenjun Zeng]

-- Digital Rights Management
-- DRM system overview
-- Security Consideration of multimedia applications and Security Protocols.
-- Encryption & authentication
-- Key management
-- Digital watermarking

This lecture will introduce the subject of DRM, discusses a number of topics that identify the importance of rights management technologies, and offers an overview of the general technology structure and capabilities of a DRM system. The lecturer will also discuss the importance of interoperability and standardization of DRM systems. This lecture will also present the fundamentals of multimedia security technologies, including cryptographic primitives, security protocols, encryption, key management and digital watermarking.

(2) Multimedia Encryption (1 hr) [Bin Zhu]

-- Secure Media Streaming
-- Scalable Encryption
-- Multi-Access Control

This lecture presents the fundamentals of multimedia encryption, including cryptographic primitives, application scenarios and design requirements, and an overview of some typical multimedia encryption schemes. It also addresses secure scalable streaming, secure transcoding, and multi-access encryption.

(3) Security System Framework (1 hr) [Hongxia Jin]

-- Key management
-- Broadcast encryption
-- Traitor Tracing
-- DRM in the high definition DVD standard

This lecture introduces broadcast encryption, a relatively recent development in cryptography, and discusses its interesting advantages as a key management scheme for content protection. It also addresses the practical problem of tracing the users (traitors) who instrument their devices and illegally resell the pirated copies by redistributing the content or the decryption keys on the Internet. The lecturer will also introduce the multimedia security mechanism in the next-generation high definition DVD standard.

(4) Multimedia Authentication and Forensics (1hr) [Qibin Sun]

-- Media Authentication Techniques
-- Digital Media Forensics
-- JPEG2000 Security Mechanism

This lecture presents the fundamentals of multimedia authentication, including cryptographic primitives, design requirements of multimedia applications, and an overview of some popular approaches. It also reviews an emerging research area - the passive-blind image forensics, which addresses image forgery detection and image source identification. The lecturer will also introduce the latest security mechanism to be used in the JPEG 2000 standard.

(5) Steganography, Biometrics, and Social Aspects (1hr) [Ching-Yung Lin]

-- Steganography and Steganalysis
-- User authentication via Biometric features
-- Social and Legal Aspects

This lecture presents stegnography and its counterpart, steganography, that aims to detect the presence of hidden data. It also introduces biometric authentication, and highlights its characteristics as pertained to its application to the digital rights management problem. The lecturer will also provide an introductory discussion and analysis of the DRM technologies on its social implications and legal issues.

(6) Emerging Technologies and Applications (1 hr) [Heather Yu]

--DRM for networked home
-- Security in P2P network
-- Mobile DRM
-- DRM for Digital Cinema
-- Open discussions

This lecture presents several emerging multimedia security technologies and applications. It will cover the upcoming issues of DRM for networked home, P2P network and mobile applications. It will also address prevention of unauthorized use of the motion picture content in digital cinema, as well as related standardization efforts and goals. In the end of the lecture, there will be an interactive open discussion session between the audiences and all six lecturers.

Materials to Distribute:

We plan to distribute the following materials in this tutorial:

1. Lecture slides,
2. Reference List – including reference papers, relevant links and on-line resources, introduction of books and potential research topics.

About the Lecturers:

Wenjun (Kevin) Zeng has been an Associate Professor with the Computer Science Department of University of Missouri, Columbia, MO since 2003. He received his B.E., M.S., and Ph.D. degrees from Tsinghua University, China, the University of Notre Dame, and Princeton University, respectively, all in electrical engineering. His current research interests include multimedia communications and networking, content and network security, wireless multimedia, and distributed source and channel coding.

Prior to joining Univ. of Missouri-Columbia in 2003, he had worked for PacketVideo

Corporation, San Diego, CA, Sharp Labs of America, Camas, WA, Bell Laboratories, Murray Hill, NJ, and Matsushita Information Technology Lab, Panasonic Technologies Inc., Princeton, NJ. From 1998 to 2002, He was an active contributor to the MPEG4 Intellectual Property Management & Protection (IPMP) standard and the JPEG 2000 image coding standard, where four of his proposals were adopted. He has authored/co-authored numerous technical papers and standard contributions, and has been awarded 12 patents.

Dr. Zeng has served as an Organizing Committee Member and Technical Program Committee Chair/Member for a large number of IEEE international conferences. He is an Associate Editor of the IEEE Transactions on Multimedia, and is on the Editorial Board of IEEE Multimedia Magazine. He is currently serving as the Technical Program Committee (TPC) Chair for the 2007 IEEE Consumer Communications and Networking Conference (CCNC) to be held in Las Vegas in January 2007. In the recent past, he has served as the TPC vice-Chair for CCNC 2006, the Technical Program Co-Chair, Multimedia Communications and Home Networking Symposium, IEEE Inter. Conf. Communication, Korea, May 2005, and the DRM Workshop Chair for CCNC 2005. He was the Lead Guest Editor of IEEE Transactions on Multimedia's Special Issue on Streaming Media published in April 2004, and is currently guest-editing a Special Issue on Recent Advances in Distributed Multimedia Communications for the Proceedings of the IEEE. He is the editor of the book Multimedia Security Technologies for Digital Rights Management, ISBN: 0-12-369476-0, Elsevier, July 2006.

Bin B. Zhu has been with Microsoft Research (MSR) Asia as a researcher since Dec. 2001, where he has been working on system and network security, content protection and digital rights management, watermarking, multimedia processing and communications, P2P networks, encryption algorithms, etc. Before he joined MSR Asia, he worked as a cofounder and Lead Scientist at Cognicity for more than 4 years. Cognicity was a pioneer in the field of audio watermarking and personalized music promotion and advertising enabling technologies. Dr. Zhu is a senior member of IEEE. He has published four book chapters and about 50 peer-reviewed journal and conference papers. He has been awarded 8 US patents with more than 16 pending US patent applications. Dr. Zhu received his B.S. degree in physics from the University of Science and Technology of China in 1986, and M.S. and Ph. D. degrees in electrical engineering from the University of Minnesota, Twin Cities in Sept. 1993 and Dec. 1998.

Hongxia Jin is a Research Staff Member in IBM Almaden Research Center. Dr. Jin's broadcast encryption and traitor tracer mechanisms were chosen as the core technologies for the next generation high-definition DVD standard. (to be completed)

Qibin Sun is the Menager of the Pervasive Media Lab, Institute for Infocomm Research, Singapore. His research interest includes media security, media recognition and media

streaming. Dr. Sun is the lead representative of Singapore for JPEG 2000 standard. (to be completed)

Ching-Yung Lin received his Ph.D. degree from Columbia University in Electrical Engineering. Since Oct 2000, he has been a Research Staff Member in IBM T. J. Watson Research Center, New York, where he is currently leading projects on the IBM Large-Scale Video Semantic Filtering System and People Mining System. He is also an Adjunct Associate Professor at Columbia University and an Affiliate Associate Professor at the University of Washington, Seattle.

His research interest is mainly focused on multimodality signal processing and understanding, with applications on distributed computing, embedded vision system, social computing, and security. Dr. Lin led the first large-scale video semantic annotation project, which includes 23 worldwide research institutes in 2003. His multimedia semantic mining project team has performed best in the US National Institute of Standards and Technology (NIST) semantic video concept detection benchmarking since 2002. Dr. Lin is the Editor of the Interactive Magazines (EIM) of the IEEE Communications Society (2004-2006), an Associate Editor of the IEEE Trans. on Multimedia (2004-), and an Editorial Board Member of the Journal of Visual Communication and Image Representation (2005-). He served as a Guest Editor of the Proceedings of IEEE -- Special Issue on Digital Rights Management, June 2004, a Guest Editor of the EURASIP Journal on Applied Digital Signal Processing -- Special Issue on Visual Sensor Network, 2006, and the Technical Program co-chair of IEEE ITRE 2003. Dr. Lin is a recipient of 2003 IEEE Circuits and Systems Society Outstanding Young Author Award and IBM Invention Achievement Awards in 2001 and 2003. He is the (co-)author of more than 120 journal articles, conference papers, book, book chapters and public release software. Dr. Lin is a Senior Member of IEEE, and a member of ACM, INSNA and AAAS. He teaches the Multimedia Security System course at Columbia University and is an co-editor of the book "Multimedia Security Technologies for Digital Rights Management" published by Elsevier, July 2006.

Heather Yu received her B.S. degree from Beijing University, her M.A. and Ph.D. degrees from Princeton University, all in Electrical Engineering. She joined Huawei Technologies (USA) in 2007. From September 1998 to March 2007, Dr. Yu was a Senior Scientist at Panasonic Princeton Lab, where her major focus is multimedia communication and multimedia security R&D. She published more than 60 technical papers and holds 19 US patents, of which 30 plus papers and 16 granted US patents are related to multimedia security.

Currently, Dr. Yu serves as Editor for ACM Computers in Entertainment and IEEE MultiMedia, voting member of IEEE ComSoc Strategic Planning Committee and Emerging Technologies Committee, and etc. She served as Chair of IEEE Multimedia Communications TC 2003-2006. From 1998-2006, she served as conference program chair, keynote speaker, panelist, panel chair, associate chair, session chair, technical committee member, best paper award committee member, and steering committee

member for numerous conferences, including IEEE Globecom, ICC, CCNC, ICME, and etc. She also served as reviewer for many renowned international journals in the area of multimedia communication, multimedia processing, and multimedia security.