

Multimedia Content Protection in Digital Networks

Ahmet Eskicioglu, City University of New York

Tutorial Outline

A digital home network is a cluster of digital audio/visual (A/V) devices including set-top boxes, TVs, VCRs, DVD players, and general-purpose computing devices such as personal computers. Copyrighted digital multimedia content may be delivered to the consumers from a number of sources including the Internet, and satellite, terrestrial or cable television systems. It may also be made available as prepackaged media (e.g., a digital tape or a digital video disc) at retail stores.

Before releasing their content for distribution, the content owners may require protection by specifying certain access conditions and digital rights. Although legal institutions exist for protecting intellectual property, complimentary technical measures are needed to sustain financial returns and to ensure incentives for new creations. Recently, two fundamental groups of technologies, encryption and watermarking, have been identified for protecting copyrighted multimedia content in digital distribution networks. Encryption-based technologies transform content into unintelligible form. This transformation, being reversible in nature, allows perfect recovery of content before consumption. Technologies based on watermarking embed data directly into content, resulting in imperceptible degradation in visual quality.

Three major industries have a vital interest in this problem: The motion picture industry, the consumer electronics (CE) industry, and the information technology (IT) industry. This tutorial is an overview of the work done for protecting the content owners' investment in intellectual property. It highlights the important developments within several international forums including the Copy Protection Technical Working Group (CPTWG), Secure Digital Music Initiative (SDMI), Advanced Television Systems Committee (ATSC), Digital Video Broadcasting (DVB), Open Cable, Motion Pictures Expert Group (MPEG) and Internet Engineering Task Force (IETF).

Biography of Instructor

Ahmet Eskicioglu (eskicioglu@sci.brooklyn.cuny.edu) received the B.S. degree from the Middle East Technical University (METU), Ankara, Turkey, and the M.S. and Ph.D. degrees from the University of Manchester Institute of Science and Technology (UMIST), England. He was with the Computer Engineering Department, METU from 1983 to 1992, the Department of Computer Sciences, University of North Texas from 1992 to 1995, and Thomson Multimedia Corporate Research, Indianapolis from 1996 to 2001. Dr. Eskicioglu is now with the Department of Computer and Information Science, Brooklyn College of the City University of New York. He has participated in the development of several national and international standards for conditional access and copy protection in the US and Europe. These include the Advanced Television Systems Committee (ATSC) conditional access system, the Electronics Industries Alliance (EIA) National Renewable Security Standard (NRSS), the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) System, and the Content Scramble System (CSS) for DVD players. His interests include image compression, system simulation, data security, conditional access, and digital rights management.

Topics

- INTELLECTUAL PROPERTY & COPYRIGHT
- COPYRIGHT INDUSTRIES
- INFORMATION SECURITY OBJECTIVES
 - CONFIDENTIALITY
 - DATA INTEGRITY
 - AUTHENTICATION
 - NON-REPUDIATION
- DATA HIDING (WATERMARKING)
- TYPES OF CONTENT PIRACY
- CONDITIONAL ACCESS (CA) SYSTEMS FOR SATELLITE, CABLE AND TERRESTRIAL TELEVISION NETWORKS
- DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEMS FOR THE INTERNET
- COPY PROTECTION (CP) SYSTEMS FOR DIGITAL HOME NETWORKS
 - DVD PROTECTION
 - DIGITAL INTERFACE PROTECTION
 - COPY PROTECTION GROUPS/ORGANIZATIONS
 - ATTRIBUTES FOR A COPY PROTECTION SYSTEM
 - GLOBAL ARCHITECTURES FOR COPY PROTECTION
- WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO)
- DIGITAL MILLENIUM COPYRIGHT ACT (DMCA)
- IP MULTICAST SECURITY
 - SECURE MULTICAST APPLICATIONS
 - CORE PROBLEM AREA IN MULTICAST SECURITY
 - EVALUATION CRITERIA
 - CLASSIFICATION OF KEY MANAGEMENT SCHEMES
 - PERIODIC BATCH REKEYING
- WIRELESS NETWORKS AND MOBILE MEMBERS
 - TWO-TIER SERVER ARCHITECTURE
 - DESIGN CRITERIA
 - MOBILE MEMBER JOIN AND LEAVE
 - MOBILE MEMBER TRANSFER
 - BASELINE REKEYING
 - IMMEDIATE REKEYING
 - DELAYED REKEYING
- SECURITY OF WIRELESS LANS

SPEAKER'S PARTICIPATION IN CONTENT PROTECTION RELATED FORUMS

Digital Video Broadcasting (DVB) Consortium, European Union, 2000-2001.

Member, Technical Module. Participated in determining the commercial requirements for a new DVB Content Protection and Copy Management (CPCM) System to provide a common framework for the protection and management of content beyond the traditional boundaries of DVB compliant conditional access systems.

Consumer Electronics Association (CEA), USA, 1998-2001.

Co-Chair, R4.8 Working Group on Copy Protection. Investigated the impact of copy protection systems on the digital interfaces including the IEEE 1394 and RF Remodulation interfaces. Wrote an extensive report summarizing the proposed systems.

Advanced Television Systems Committee (ATSC), USA, 1997-1999.

Member, T3/S8 Conditional Access Ad Hoc Working Group. Participated in determining the ATSC needs for a conditional access system for digital TV. Reviewed the proposals concerning the essential components such as scrambling algorithms, EMM and ECM generation and distribution, host conditional access software, and copy protection.

Copy Protection Technical Working Group (CPTWG), USA, 1997-1999.

Member, Data Hiding Subgroup. Participated in determining the requirements of a system for watermarking digital video content. Reviewed the submitted proposals.

Electronics Industries Association (EIA) - National Cable Television Association (NCTA) Joint Engineering Committee, USA, 1996-2001.

Member, National Renewable Security Standard (NRSS) Subcommittee. Revised and edited both Part A and Part B of the NRSS. Designed and proposed a system for the protection of the common interface between the host device and the renewable security module.

International Digital Video Disk Forum, USA, 1996-2000.

Member, Copy Protection Technical Working Group. Evaluated proposals for protecting DVD Video and DVD Audio, and participated in the development of copy protection systems for DVD players, DVD recorders and DVD-ROM drives.

Copy Protection Technical Working Group (CPTWG), USA, 1996-1998.

Member, Digital Transmission Discussion Group. Participated in determining the requirements of a system for the protection of digital audio/video data transmitted on the IEEE 1394 serial bus. Reviewed the submitted proposals.

Society of Cable Telecommunications Engineers (SCTE), USA, 1996-1998.

Member, Digital Video Subcommittee. Contributed to the architectural design of a conditional access system for the cable TV industry.

SEMINARS ON THE SAME SUBJECT

1. "Multimedia Security in Group Communications: Recent Developments in Wired and Wireless Networks," Department of Computer and Information Sciences, Fordham University, New York, NY, April 19, 2002.
2. "Technologies and Architectures for Digital Rights Management," MediaSec Technologies, Providence, RI, April 5, 2002.
3. "Multicast Security: Issues in Group Key Management," Thomson multimedia, Inc., Princeton, NJ, March 7, 2002.
4. "An Overview of Multimedia Communications Security in Digital Domains," Department of Computer and Information Sciences, Fordham University, New York, NY, March 5, 2002.
5. "Multimedia Content Protection in the Digital World," Department of Computer and Information Science, Brooklyn College of the City University of New York, New York, NY, February 25, 2002.
6. "Multimedia Content Protection and Digital Rights Management," Telecommunications Research Labs, Winnipeg, MB, Canada, January 4, 2002.
7. "Multimedia Content Protection and Digital Rights Management," University of Manitoba, Department of Computer Science, Winnipeg, MB, Canada, January 3, 2002.
8. "Protection of Multimedia Content in Digital Home Networks," International Symposium on Telecommunications, Tehran, Iran, August 30, 2001.
9. "Cryptography: The Science and Art of Secure Communications," Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, October 27, 2000.
10. "How to Protect Electronic Books with Cryptography?" The Electronic Book Exchange (EBX) Working Group Meeting, New York, NY, September 21-22, 2000.
11. "An Overview of Multimedia Content Protection in Home Networks," Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, April 13, 2000.
12. "Protection of Multimedia Content in Consumer Electronics Devices," Department of Electrical Engineering, Swiss Federal Institute of Technology, Lausanne, Switzerland, February 2000.
13. "Protection of Copyrighted Digital Content," International Conference on Consumer Electronics, Los Angeles, CA, June 1999.