Advances in Digital Video
Content Protection

E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk and E. J. Delp

Proceedings of the IEEE, VOL. 93, NO. 1, January 2005
Outline

- Content Protection Overview
  - Key players in content protection
- Digital Rights Management (DRM)
  - Basics
  - Legal and technical solutions
  - Methods and tools
- Research Issues
- Conclusion
Motivations

- Illegal copying and distribution on a massive scale facilitates misuse, piracy, plagiarism and misappropriation.
  - Example
    - Peer-to-peer (P2P) architecture based systems create considerable challenges for copyright enforcement.
      - P2P with anonymity
      - DRM for P2P

http://www.kazaa.com/
http://www.edonkey.com/
http://www.bittorrent.com/
http://www.morpheus.com/
Failed Copy Protection Schemes (1/2)

- ContentScramblingSystem (CSS)
  - To protect prerecorded movies stored on DVD, including
    - Encryption to scramble the video data
    - Decryption keys are stored on special areas only accessible for compliant reader
  - A protocol for obfuscating the communication between the DVD player and attached device
  - Copy protection for digital/analog outputs
  - **DeCSS** software was successfully developed!
    - Once the encryption for a movie is broken, illegal copies can be played by DVD reader.

**Failed Copy Protection Schemes (2/2)**

- **Secure Digital Music Initiative (SDMI)**
  - SDMI a forum that has brought together more than 200 companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry, and Internet service providers to develop and standardize technologies that “protect the playing, storing and distribution of digital music”
  - The SDMI “public challenge” was announced in September 2000 to invite members of the public to try to break the technologies SDMI developed
  - Defeated by S. A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. S. Wallach, D. Dean and E. W. Felton.

[http://www.cs.princeton.edu/sip/sdmi/]
Market values of Content Protection

- According to the IIPA report,
  - The copyright-based industries are one of the fastest growing and most dynamic sector of the U.S. economy.
  - Excluding Internet piracy, the annual worldwide losses of copyrighted materials are estimated to be $20 billion to $22 billion.
  - Three types of industries are devoted to the digital content protection arena
    - Motion picture, consumer electronics and information technology
<table>
<thead>
<tr>
<th><strong>ATSC</strong></th>
<th>Advanced Television Systems Committee [13] is an international, non-profit organization developing voluntary standards for digital television.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CEA</strong></td>
<td>Consumers Electronics Association [14] represents more than 1000 companies within the U.S. consumer technology industry.</td>
</tr>
<tr>
<td>Key Players in Content Protection (2/5)</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>CPTWG</strong></td>
<td>Copy Protection Technical Working Group [15] was formed in early 1996 with the initial focus of protecting linear motion picture content on DVD. Supported by the motion picture, consumer electronics, information technology, and computer software industries, the scope of CPTWG now covers a range of issues from digital watermarking to protection of digital television.</td>
</tr>
<tr>
<td><strong>DVD Forum</strong></td>
<td>DVD Forum [16] is an international association of hardware manufacturers, software firms and other users of Digital Video Discs.</td>
</tr>
</tbody>
</table>
### Key Players in Content Protection (3/5)

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCTE</td>
<td>Society of Cable Telecommunications Engineers [17] is a non-profit professional organization which is involved in the development of cable television standards.</td>
</tr>
<tr>
<td>MPAA</td>
<td>Motion Picture Association of America [18] represents the American motion picture, home video and television industries.</td>
</tr>
<tr>
<td>Key Players in Content Protection (4/5)</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>IETF</strong></td>
<td>Internet Engineering Task Force [19] is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture.</td>
</tr>
<tr>
<td><strong>MPEG</strong></td>
<td>Moving Pictures Expert Group [20] developed a family of international standards used for coding audio-visual information.</td>
</tr>
<tr>
<td>Key Players in Content Protection (5/5)</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>DVB</strong></td>
<td>Digital Video Broadcasting Project [21] is a consortium of over 300 broadcasters, manufacturers, network operators, software developers, regulatory bodies committed to designing standards for the global delivery of digital television and data services.</td>
</tr>
<tr>
<td><strong>TV-Anytime</strong></td>
<td>The global TV-Anytime Forum [22] is an association of organizations which seeks to develop specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer platforms.</td>
</tr>
</tbody>
</table>
Objectives of DRM

- A DRM system protects and enforces the rights associated with the use of digital content
  - Access control
    - To ensure that access to protected content is only possible under the conditions specified by the content owner
  - Copy control
    - To prevent the creation of unauthorized copies
  - Content tracking
    - To detect and trace each copy
What a DRM System Do?

1. Packaging content
2. Obtaining access conditions specified by content owners
3. Determining if access conditions are fulfilled
4. Temper-proofing DRM components
Content Packaging

- To force all accesses to the protected content to be governed by the DRM system
- Once the security of the package is defeated, the unprotected content will be accessed or copied directly
- Packaging is usually accomplished by encryption
Access Conditions

- Components of access conditions (usage rules)
  - A means of right expression for the content owner
    - XrML, ORDL
  - A mechanism of rights association (persistence)
    - Metadata or watermarking
  - A secure scheme to determine if rules are enforced
    - Obtaining secure authentication, transaction, context information
Temper-proof and Renewability

- Temper-proving
  - Components of DRM systems must be temper-proof to avoid attempts to circumvent, modify, or reverse-engineer the security protocol

- Renewability
  - Security can be restored or upgraded even after some devices have been compromised
    - Device revocation
Relationships between DRM Function Blocks

- **Access Control**
  - Authentication
  - Secure Comm.
  - Renewability
  - Content Packaging
  - Integrity checking
    - Metadata Format
- **Copy Protection**
  - Metadata Definition
  - Temper-proofing
- **Metadata Persistence**
- **Content Tracking**
  - Content Identification

- **How to realize them?**
  - Cryptography
  - Watermarking
  - Interoperable Standards
Layering View of DRM
Building Blocks

Digital Rights Management (DRM)

- Integrity Checking
- Access Control
- Credential Authentication
- Copy Control
- Transaction Tracking
- Rule Specification
- Non-Technical Aspects

Cryptography
- Hashes and protocols
- Block cipher
- Public-key encryption/decryption

Watermarking
- Media specific techniques
- Fingerprinting

Rights Language
- REL
- XrML

Business Model
Legislative Acts
Public Interests
DRM Applications of Encryption

- Packaging
- Forcing devices to adhere to access conditions
- Device authentications
- Secure communications
- Integrity checking
Shortcomings of Encryption

- **Fragile cipher-text**
  - The decryption will fail even only one bit error occurs in cipher-text
  - Hindering lossy or non-sequential video applications
    - Video streaming
    - Scalable video

- **Computational cost**
  - Important for real-time applications or low-cost devices

- **Solutions**
  - Use selective encryption to reduces computation and preserve video structure

- **Issues about encrypting scalable video**
DRM Applications of Watermarking

- Copyright/owner identification
- Copy protection
- Access control
- Content tracking
Video Watermarking

- **Methods**
  - Additive embedding
  - Multiplicative embedding
  - Quantization

- **Embedding domains**
  - Spatial domain
  - Spatial-Temporal domain
  - Frequency domain
  - Accompany audio domain

- **Requirements**
  - Blind-detection
  - Computational costs
    - Compressed-domain watermarking
  - Drifts compensation
  - Rate-control
Research Issues of Encryption and Watermarking

- Selective encryption
- Encryption of scalable video
- Robustness and security of watermarking schemes
- Anti-collusion of content tracking
- Watermarking performance evaluation
- The location of watermarking in video DRM
- Content tracking in broadcast or multicast networks
Other Issues about DRM

- Analog holes
- Temper-proofing of devices
- System renewability
- Countless attackers
- Compromising the whole DRM system after only one success
- Long period
Legislative Efforts

- World Intellectual Property Organization (WIPO)
  - WIPO Copyright Treaty
  - WIPO Performance and Phonograms Treaty

- U. S. Congress
  - The Digital Millennium Copyright Act (DMCA), 1998
Effects on Users and Consumers

- The use of DRM is controversial
  - Usage rules of DRM system may contravene the rights and privileges granted to the public under copyright law
  - Information releasing may violate expectations of privacy
  - DRM may reduce competition
  - DRM may increase cost of devices
# Current DRM Systems for Video (1/4)

<table>
<thead>
<tr>
<th>Media protected</th>
<th>Secure delivery of content</th>
<th>Device authentication</th>
<th>Association of digital rights</th>
<th>Licensed technology</th>
<th>System renewability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video on DVD-ROM</td>
<td>encryption</td>
<td>Mutual between DVD drive and PC</td>
<td>metadata</td>
<td>CSS [8]</td>
<td>Device revocation</td>
</tr>
<tr>
<td>Audio on DVD-ROM</td>
<td>encryption</td>
<td>Mutual between DVD drive and PC</td>
<td>metadata</td>
<td>CPPM [35]</td>
<td>Device revocation</td>
</tr>
<tr>
<td></td>
<td>watermark</td>
<td>n/a</td>
<td>watermark</td>
<td>4C/Verance</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Watermark [36]</td>
<td></td>
</tr>
<tr>
<td>Video or audio on DVD-R/RW/ RAM</td>
<td>encryption</td>
<td>Mutual between DVD drive and PC</td>
<td>metadata</td>
<td>CPRM [37]</td>
<td>Device revocation</td>
</tr>
<tr>
<td>Video on digital tape</td>
<td>encryption</td>
<td>n/a</td>
<td>metadata</td>
<td>High Definition</td>
<td>Device revocation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Copy Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[38]</td>
<td></td>
</tr>
<tr>
<td>Digital interface</td>
<td>Encryption</td>
<td>Mutual between source and sink</td>
<td>Metadata</td>
<td>DRM Method</td>
<td>Revocation Type</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-------------------------------</td>
<td>----------</td>
<td>------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>IEEE 1394</td>
<td>encryption</td>
<td>Mutual between source and sink</td>
<td>metadata</td>
<td>DTCP [39]</td>
<td>Device revocation</td>
</tr>
<tr>
<td>Digital Visual Interface (DVI)</td>
<td>encryption</td>
<td>Mutual between source and sink</td>
<td>metadata</td>
<td>HDCP [40]</td>
<td>Device revocation</td>
</tr>
<tr>
<td>NRSS interface</td>
<td>encryption</td>
<td>Mutual between host and removable security device</td>
<td>metadata</td>
<td>Open standards [41]–[43]</td>
<td>Service revocation</td>
</tr>
</tbody>
</table>
## Current DRM Systems for Video (3/4)

<table>
<thead>
<tr>
<th>Broadcast</th>
<th>Encryption</th>
<th>Access</th>
<th>Metadata</th>
<th>Access System</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite</td>
<td>encryption</td>
<td>None</td>
<td>metadata</td>
<td>Conditional access system [44], [45]</td>
<td>Smartcard revocation</td>
</tr>
<tr>
<td>Terrestrial</td>
<td>encryption</td>
<td>None</td>
<td>metadata</td>
<td>Conditional access system [45]</td>
<td>Smartcard revocation</td>
</tr>
<tr>
<td>Cable transmission</td>
<td>encryption</td>
<td>None</td>
<td>metadata</td>
<td>Conditional access system [46]</td>
<td>Smartcard revocation</td>
</tr>
<tr>
<td>Internet</td>
<td>Unicast</td>
<td>encryption</td>
<td>Receiver</td>
<td>metadata</td>
<td>DRM [47], [48]</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>Multicast (A few watermarking schemes have been proposed for multicast data [49])</td>
<td>encryption</td>
<td>Sender and receiver (depends on the authentication type)</td>
<td>metadata</td>
<td>Group key management [49]</td>
</tr>
</tbody>
</table>