Introduction to Digital Rights Management (DRM)

Multimedia Security
Outline

• Digital rights management: an overview
• Digital watermarking
  – Basics and models
  – Trends and challenges
• Cryptography in DRM
• Digital rights languages
• Important DRM standards
• Legislative concerns about DRM
• DRM researches in CML
Digital Rights Management: An Overview
Digital technologies facilitate new experiences for content users in consuming, authoring, replicating and delivery of digital contents. However, prevalence of digital replication devices and explosive growth of Internet usages also result in serious copyright infringement problems at the same time.
What is DRM?

A DRM system enables the **secure exchange of intellectual property**, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks.

DRM is the chain of hardware and software services and technologies governing the **authorized use** of digital content and managing any consequences of that use throughout the entire life cycle of the content.
Content Protection Technologies

Content Protection
- Enforcement
- Law
- Business
- Technology
- Education

Digital Rights Management
- Copy Control
- Author Identification
- Credential Authentication
- Conditional Access
- Integrity Checking
- Usage Rule Specification
- Interoperability

Watermarking
- Robust watermarking
- Fragile watermarking
- Visible watermarking
- Fingerprinting

Cryptography
- Cryptographic protocols
- Symmetric ciphers
- Asymmetric ciphers
- Hash
- Digital Signatures

Rights Languages
- XrML
- ODRL
- MPEG REL
The DRM Reference Architecture

Three major components of the DRM reference architecture:

- Content Server
  - Content Repository
  - Product Information

- License Server
  - Rights
  - Encryption Keys
  - DRM License Generator
  - Identities

- Content Package
  - Content
  - Metadata

- DRM Controller
  - License
    - Keys
    - Rights

Client
- Rendering Application
- Identity
The DRM controller on the client side has to check the rendering application at some time
- To avoid making unauthorized copies
- To check certain rights limits
Digital Watermarking Technologies
What is Watermarking?

Traditional Watermarking

- Watermarking is traditionally an important mechanism applied to physical objects, such as bills, papers, garment labels, product packing.
- The watermark is hidden from view during normal use, and only become visible by adopting a special viewing process.
- The watermark carries information about the object in which it is hidden.

Digital Watermarking (Robust Invisible Watermarking)

- Fidelity
- Capacity
- Robustness

10
Data Hiding, Watermarking and Steganography

- Data hiding
  - Steganography
    - Imperceptible data embedding
      - Non-robust data embedding
    - Visible data embedding
      - Robust data embedding
  - Watermarking
    - Imperceptible watermarking
      - Fragile watermarking
    - Visible watermarking
      - Robust watermarking
Desired Properties of Watermarking

- **High fidelity**
  - Finding adequate perceptual quality index is still an open problem
  - Objective distortion measures are often adopted
- **Strong robustness**
  - Robustness is difficult to define
  - Benchmarks testing various attacks exist
- **Large capacity**
  - Required payload length depends on the purpose of different applications
- **Blind detection**
  - Original content is not required in detection side
  - Non-blind detection limits the applicability of watermarking schemes
- **Low computation complexity**
  - Manufacturing cost and time constraints are important concerns
Importance of Watermarking

Cryptography vs. Digital Watermarking

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Before Protection</th>
<th>Protected</th>
<th>Without Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Encryption</td>
<td>Decryption</td>
<td></td>
</tr>
</tbody>
</table>

Watermarking

<table>
<thead>
<tr>
<th>Before Protection</th>
<th>Protected</th>
<th>Detector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2004 bh

Various Applications of Digital Watermarking Technologies

- Owner identification
- Proof of ownership
- Broadcast monitoring
- Transaction tracking
- Content authentication
- Copy control
- Device control
- Metadata Association
Under the U.S. law, although the copyright notice is not required in every distributed copy to protect the rights of copyright holders, the award to the copyright holders whose work is misused will be significantly limited without a copyright notice found on the distributed materials.

- Traditional textual copyright notices
  - “Copyright date owner”
  - “© date owner”
  - “Copr. date owner”
• Disadvantages for textual copyright notices
  – Easily removed from a document when it is copied
    • E.g. the Lena Sjooblam picture (see the next slide)
  – Copyright notices printed on the physical medium are not copied along with the digital content
    • E.g. the Music CD
  – Occupying a portion of the image and aesthetically reducing the value of artworks
• Since watermarks are imperceptible and inseparable from the work, they are obviously superior to textual copyright notices.
The Story of Lena

• Lena is the most common test image in image processing research!
• However, the copyright notice of this picture was cropped and ignored.
Proof of Ownership

• Textual copyright notices cannot be used to solve the copyright dispute since they can be easily forged
• Registering every work to a central repository is too costly!
  – [http://www.loc.gov/copyright](http://www.loc.gov/copyright)
  – $30 per document
• Watermarking can be of use!
• TV or radio advertisements should be monitored to prevent airtime overbooking!
  – In 1997, a scandal broke out in Japan. Advertisers are paying for thousands of commercials that were never aired!
• Broadcast monitoring
  – By human watchers
  – Passive monitoring
  – Active monitoring
• Passive monitoring
  – Use computers to monitor received signal and compares with a database of known contents
  – Disadvantages
  • Comparing is not trivial
  • Signal degraded due to broadcasting
  • Management and maintenance of the database is quite expensive
• Active monitoring
  – Simpler to implement
  – Identification information can be directly decoded reliably
  – E.g.
    • close captions on VBI or file headers
  – Watermarking is an obvious alternative method of hiding identification information
    • Existing within the content
    • Completely compatible with the equipments
• Watermarks recording the recipient in each legal sale or distribution of the work.

• If the work is misused (leaked to the press or illegally distributed), the owner could find out who is the traitor.

• Visible watermarking is often adopted in this application, but Invisible watermark is even better.
The Defunct DiVX DVD Player

• The DiVX Corporation sold a enhanced DVD player that implements a pay-per-view model.
• Each player will place a unique watermark in the video disk it played.
• Once the video disk is recorded and sold, the adversary can be tracked!
Copy Control (I)

• Encryption is the first and strongest line of defense against illegal copy
  – Overcome an encryption mechanism
    • Decrypt a copy without a valid key
      – Theoretically infeasible for a well designed system
    • Obtain a valid key
      – Reverse-engineering hardware or software
      – E.g. the DeCSS program against the CSS protecting DVD
    • Legally obtain a key and pirate the decrypted content
      – The central weakness of cryptographic protection!
      – The content must be decrypted before it is used, but all protection is lost once decrypted!
• Watermarking in copy control
  – Combining every content recorder with a watermark detector
  – When a copy-prohibit watermark is detected, the recording device will refuse to copy
  – The system has been envisioned by CPTWG and SDMI to protect DVD and audio
Copy Control (III)

- Problems of adopting watermarking module in recording devices
  - Increasing cost
  - Reducing the value of devices
- Solution
  - Include the requirement for a watermark detector in the patent license of CSS instead of enforcing by law
Keep Honest People Honest!

Playback control by encryption

Copy control by watermarking

Legal, encrypted copy

Compliant player

Compliant recorder

Illegal, decrypted copy

Non-Compliant player

Non-Compliant recorder
Device Control

• Copy control belongs to a broader category - device control

• Other applications of device control
  – Automatically turning on/off functions related to special contents
    • E.g Including watermark to skip advertisements
  – Action toys interactive with the TV program
  – Digimarc’s MediaBridge
Properties of Watermarking

• Correct detection result
  – Embedding effectiveness
  – False-alarm rate
• Fidelity (perceptual similarity)
• Resisting distortions
  – Robustness
  – Security
• Data payload (capacity)
• Blind/informed watermarking
• Cost
Effectiveness

• Effectiveness of a watermarking system
  – The probability of detection after embedding
  – A 100% effectiveness is desirable, but it is often not the case due to other conflict requirements, such as perceptual similarity
  • E.g. watermarking system for a stock photo house
False-alarm Rate

• Detection of watermark in a work that do not actually contain one
  – The number of false positives occur in a given number of runs of watermark detector

• The false alarm rate of the watermarking system used in DVD recorder should be lower than $1/10^{12}$
  – E.g. a false alarm occurred in a world-series baseball game
The fidelity of the watermarking system
  - The perceptual similarity between the original and the watermarked version of the cover work
  - It is the similarity at the point at which the watermarked content is provided to the customer that counts
    - E.g. NTSC video or AM radio has different perceptual similarity requirements from the HDTV or DVD video and audio
Fidelity Measures

- Commonly used image similarity index
  - MSE: \( \frac{1}{N} \sum_{i=1}^{N} (c[i] - c'[i])^2 \)
  - SNR: \( \frac{\sum_{i=1}^{N} (c[i] - c'[i])^2}{\sum_{i=1}^{N} c[i]^2} \)

- Finding a quality index completely reflecting the characteristics of the human perceptual model is difficult
Robustness (I)

• The ability to detect the watermark after common signal processing operations
  – Common images distortions
    • spatial filtering, lossy compression, printing/scanning, geometric distortions
  – Common video distortions
    • Changes in frame rate, recording to tape…
  – Common audio distortions
    • temporal filtering, recording on audio tape…
Robustness (II)

- Not all watermarking applications require robustness to all possible signal processing operations.
- There is a special class of watermarking techniques where robustness is undesirable
  - The fragile watermarking
Security

• The ability to resist hostile attacks
  – Unauthorized removal
    • Eliminating attacks
    • Masking attacks
    • Collusion attacks
  – Unauthorized embedding
    • Embed forgery watermarks into works that should not contain watermarks
    • E.g. fragile watermarks for Authentication
  – Unauthorized detection
Data Capacity

- The number of bits a watermarking scheme encodes within a unit of time or within a work.
- Different applications require different data capacities, e.g.
  - 4-8 bits for a 5-minutes video of copy control
  - Longer messages for broadcast monitoring
Blind/Informed Detection

- Informed watermarking schemes
  - The detector requires access to the un-watermarked original
    - E.g. transaction tracking,
- Blind watermarking schemes
  - Detectors do not require any information related to the original
    - E.g. DVD copy control module
    - E.g. An automatic image IPR checking robot
Multiple Watermarks

• In certain cases, more than one watermarks are needed.
  – E.g. American copyright grants the right of TV viewers to make a single copy of broadcast programs for time-shift watch. But further copies is not allowed .
  • Adding two watermarks instead of alternating the original watermark to avoid the risk caused by easily changing watermarks
• The costs in deploying watermark embedders and detectors depends on the scenario and the business model.
  – Real-time constraint
    • Broadcast monitoring v.s. proof of copyright
  – Embedder/detector constraint
    • Copy protection v.s. transaction tracking (DIV-X)
Viewing Watermarking As a Communication Channel

- Blind scheme
  \[ z = C_{wn} \cdot W_a \]

- non-blind scheme
  \[ z = W_n \cdot W_a \]
Spread-Spectrum Watermarking

**Watermarking Embedding**

- Watermark (Pseudo-random sequence)
- Global FFT/DCT
- Embedding (+)
- Inverse FFT/DCT

Added to perceptual significant coefficients, such as the first 1000 large transform coefficients.

**Watermarking Extraction**

- Global FFT/DCT
- Global FFT/DCT
- Reference Watermark
- Correlation
- Extracted Watermark
DCT-based Watermarking

Watermark Embedding

Image Analysis → Block DCT → Pseudo-Random Permutation → Embedding → Inverse DCT

Watermark Extraction

Image Analysis → Block DCT → Block DCT → Extraction (XOR) → Inverse Permutation
Host-Interference Non-rejecting Problem

\[ s(x,m) = x + w(m) \]
\[ w(m) = a(m)v \]
\[ s = x + a(m)v \]
\[ \tilde{s} = s^T v = \tilde{x} + a(m) \]
\[ a(m) = \tilde{s} - \tilde{x} \]
\[ s = x + (\tilde{s} - \tilde{x})v \]

Quantization Watermarking

Watermark Embedding with Multiple Quantizers

- **Imperceptibility** ➔ Shape and area of Quantization cells
- **Robustness** ➔ minimum distance between any reconstruction points of different quantizers
- **Capacity** ➔ number of quantizers
Host-Interference Problem

- In a blind watermarking scheme, the host signal may introduce interference for the detection of embedded watermark signal.

**Host-interference Rejection Watermarking**

- Estimating the host signal in the detection side

**Quantization Watermarking**
- Imperceptibility
  - Shape and area of Quantization cells
- Robustness
  - Minimum distance between any reconstruction points of different quantizers
- Capacity
  - Number of quantizers

**Dirty-Paper Watermarking**
- The embedder is told the effect of the host content

![Diagram of a watermarking system](image)
Asynchronous Attacks

• Most existing watermarking schemes fail in face of the asynchronous attacks
  • Solutions
    • Non-blind schemes
      • Content registration before watermark detection
    • Blind schemes
      • Embedding in the RST-invariant domain
      • Exhaustive search
      • Resynchronization through template matching
Watermarking Benchmarks

• Stirmark
  – http://www.petitcolas.net/fabien/watermarking/stirmark/

• Checkmark
  – http://watermarking.unige.ch/Checkmark/index.html

• Optimark
  – http://poseidon.csd.auth.gr/optimark/
Most watermarking schemes employ a shared key between watermark embedder and detector

- All detectors share a single private key
- It’s naïve to assume that these keys will remain secret for long in an adversary environment
- Public-key watermarking schemes have been proposed.
Lossless Data Hiding

- Lossless watermarking is also named as reversible watermarking or invertible watermarking.
- In certain applications, it is desired to reverse the marked media back to the original cover media after the hidden data is retrieved.
- Proposed approach:
  - Reversible visible watermarking
  - Losslessly compressing bit-planes to leave space for data embedding
  - Modulo-addition based scheme
  - Integer Wavelet Transform based scheme
  - Difference expansion based scheme
- Achieving high capacity while maintaining the fidelity constraint
Digital Fingerprinting

- **Fingerprinting**
  - Watermarking different copies with an unique fingerprint signal to deter pirates from distributing illegal copies
  - Fingerprinting code (codebook design + tracing algorithm) + Watermarking scheme

- **Attacks on the fingerprinted media**
  - Unintentional and intentional single user attacks
  - Collusion attack
    - A malicious coalition of users combine their code-words to produce a new codeword so that it cannot be traced back to the coalition.

- **Fingerprinting in a broadcast channel**
Cryptography in DRM
Terminology

- **Scenario**
  - A sender wants to send a message to a receiver securely, that is, to make sure an eavesdropper cannot read the message

- **Messages and Encryption**
  - Plaintext: the message
  - Ciphertext: the encrypted message
  - Encryption: disguising a message to hide its substance
  - Decryption: turning ciphertext back into plaintext
• Symbols
  – Plaintext: M (for message) or P (for plaintext)
  – Ciphertext: C
  – Encryption function: E
  – Decryption function: D

• Formulations
  – $E(M) = C$, the encryption function operates on plaintext to produce ciphertext
  – $D(C) = M$, the decryption function operates on ciphertext to produce plaintext
  – $D(E(M)) = M$, the equality must hold in order to recover the original identity
Goals of Cryptography

• Confidentiality
• Authentication
  – Receiver must be able to ascertain the message’s origin
• Integrity
  – Receiver shall be able to verify that the message is not modified in transit
• Non-repudiation
  – Sender should not be able to falsely deny later that he had sent a message
Restricted Algorithms

• Basics of Restricted Algorithms
  – The security of an algorithm is based on keeping the way that algorithm works a secret
  – Of historical interests only, inadequate in today’s applications
    • Frequent changes of algorithm due to user-leaving
    • Difficult to test the security of adopted algorithms
  – Widely used in low-security applications
Keys and Algorithms

- Modern cryptography solves the problems of restricted algorithms with key (or keys), usually denoted by K
- The key may be any one of a large number of values
- The range of possible values of the key is called the keyspace
- All of the security in these algorithms is based in the keys; none is based in the details of the algorithm
• A cryptosystem is composed of
  – An algorithm
  – All possible plaintexts
  – All possible ciphertexts
  – All keys
Encryption/Decryption with Keys

- Both encryption and decryption operations use the same key

\[ E_K(M) = C \quad D_K(C) = M \quad D_K(E_K(M)) = M \]

- Different encryption and decryption keys are used

\[ E_{K1}(M) = C \quad D_{K2}(C) = M \quad D_{K2}(E_{K1}(M)) = M \]
Symmetric Algorithms

- Symmetric Algorithms (Conventional Algorithms)
  - Algorithms where the encryption key can be calculated from the decryption key and vice versa
    - In most symmetric algorithms, the encryption key and the decryption key are the same
- Categories
  - Stream algorithms
  - Block algorithms
Asymmetric Algorithms

• Asymmetric Algorithms (Public-key Algorithms)
  – The key used for encryption is different from the key used for decryption
  – The decryption key cannot be calculated from the encryption key
  – The encryption key can be made public (public key)
  – The decryption key (private key)
Overview of cryptanalysis

- The science of recovering the plaintext of a message without access to the key
- Successful cryptanalysis may recover
  - The plaintext
  - The key
  - Weakness in a cryptosystem that eventually lead to the results above
Cryptanalytic Attacks

• Basic Assumptions
  – The secrecy must reside entirely in the key
  – The cryptanalyst has complete knowledge of the encryption algorithms used

• General types of cryptanalytic attacks
  – Ciphertext-only attack
  – Known-plaintext attack
  – Chosen-plaintext attack
  – Adaptive-chosen-plaintext attack
  – Chosen-ciphertext attack
  – Rubber-hose cryptanalysis
• To meet real-time constraint for audio and video multimedia playback, selective encryption techniques have been proposed
• Simple symmetric cryptographic modules are adopted, such as DES or AES
• Coefficients to be encrypted
  • Header information
  • Significant transform coefficients
  • Motion vectors
  • VLC tables
The most common implementation solution is to combine symmetric key cryptosystems with public key cryptography; namely to overcome the problems related to applying the symmetric key encryption only.

- The plaintext is encrypted using a fast symmetric key scheme.
- The secret key used for symmetric encryption is encrypted with slow public key scheme.
• N: the set of all users
• R: the set of revoked users
• \( S_1, \ldots, S_m \): partition of disjoint subsets of users in \( N-R \)
• K: session key
• M: message
• E, F: encryption function
• D: decryption function

Encryption

• Ciphertext
  \(<[i_1, i_2, \ldots, i_m, E_{L_1}(K), E_{L_2}(K), \ldots, E_{L_m}(K)], F_K(M)>\>

Decryption

• Each user \( u \) can deduce the key \( L_j \) from assigned private information if \( u \) belongs to \( S_j \)
• Compute \( D_{L_j} \) to obtain \( K \), and in turn obtains \( M \)

The center provides the users with \textit{prearranged keys} when they join the system

At some time, the center wish to broadcast a message (e.g. a key to decipher a video clip) to a \textit{dynamic changing privileged subset} of the users only
Digital Rights Language
The MPEG-21 Rights Expression Language
- With core architecture and base technology based on XrML 2.0
- Defined using XML Schema and Namespace Recommendations
Important DRM-related Standards
In 2002 June, MPEG (ISO/IEC JTC1 SC29 WG11) started working on the definition of enabling normative technology for the multimedia applications of the 21st century: MPEG-21 “Multimedia Framework”

- To enable transparent and augmented use of multimedia resources across a wide range of networks and devices
- To support transparent and highly automated transactions, especially taking in account
  - Digital rights management (DRM) requirements
  - Multimedia access and delivery using heterogeneous networks and terminals
• The desire to achieve interoperability may be in violation with the requirement to protect the value of the content and the rights of the rights holders
  – DRM systems can go against the very goal of interoperability if they use non-standardized protection mechanism
  – To realize an open multimedia infrastructure, more interoperability in DRM systems are crucial
• IPMP in MPEG series
  – MPEG-4 describes a set of standard interfaces to proprietary intellectual property management and protection (IPMP) systems
  – IPMP is at the very core of the MPEG-21 specifications
In 2000 June, MPEG (ISO/IEC JTC1 SC29 WG11) started working on the definition of enabling normative technology for the multimedia applications of the 21st century: MPEG-21 “Multimedia Framework”

- To enable transparent and augmented use of multimedia resources across a wide range of networks and devices
- To support transparent and highly automated transactions, especially taking in account
  - Digital rights management (DRM) requirements
  - Multimedia access and delivery using heterogeneous networks and terminals

<table>
<thead>
<tr>
<th>Pt.</th>
<th>Title</th>
<th>Publication Date (Est.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Digital Item Declaration, 2nd Edition</td>
<td>April 2005</td>
</tr>
<tr>
<td>3</td>
<td>Digital Item Identification</td>
<td>April 2003</td>
</tr>
<tr>
<td>5</td>
<td>Rights Expression Language</td>
<td>April 2004</td>
</tr>
<tr>
<td>6</td>
<td>Rights Data Dictionary</td>
<td>May 2004</td>
</tr>
<tr>
<td>7</td>
<td>Digital Item Adaptation</td>
<td>Oct. 2004</td>
</tr>
<tr>
<td>8</td>
<td>Reference Software</td>
<td>July 2005</td>
</tr>
<tr>
<td>9</td>
<td>File Format</td>
<td>Apr. 2005</td>
</tr>
<tr>
<td>10</td>
<td>Digital Item Processing</td>
<td>July 2005</td>
</tr>
<tr>
<td>11</td>
<td>Evaluation Methods for Persistent Association Tools</td>
<td>Nov. 2004</td>
</tr>
<tr>
<td>12</td>
<td>Test Bed for MPEG-21 Resource Delivery</td>
<td>Feb. 2005</td>
</tr>
<tr>
<td>13</td>
<td>EMPTY</td>
<td>---</td>
</tr>
<tr>
<td>14</td>
<td>Conformance</td>
<td>Apr. 2006</td>
</tr>
<tr>
<td>15</td>
<td>Event Reporting</td>
<td>Jan. 2006</td>
</tr>
<tr>
<td>16</td>
<td>Binary Format</td>
<td>July 2005</td>
</tr>
<tr>
<td>17</td>
<td>Fragment Identification for MPEG Resources</td>
<td>Apr. 2006</td>
</tr>
</tbody>
</table>
MPEG-21 Part 4: IPMP

- The major focus of MPEG in general
- A consumer centric approach
- Content protected by one IPMP vendor will play on any given Terminal

C-interoperability
- IPMP Tools from different vendors will be able to integrate into the same Terminal implementation concurrently
- An IPMP System is able to comprise IPMP Tools made by one or more vendors
- Goal: to simplify the design of tool and terminal interfaces such that the integration and interoperation of these tools and terminals may be more widespread and economical

M-interoperability
Characteristics of CPPM/CPRM

- Renewing protection settings without online or offline updating
- Each device owns a set of unique keys (based on broadcast encryption theories)
- Block ciphers based on Feistel networks are adopted for patents and efficiency

Adopted from the CPPM/CPRM Specifications
End-To-End Content Protection

End-to-end Protection throughout the Content Value Chain

Licenses of Cryptographic Tools Hook Everything Together

Content Encrypted  ---  Decryption Technology  ---  License  ...must adhere to CMI...
DRM-related Legislative Issues

Adopted from Digital Rights Management Business and Technology
Chapter 3: Help from the government: Law and Technology
Laws and DRM

Definition of the term “Rights”

“an interest or title in an object of property; a just and legal claim to hold, use, and enjoy it or convey it or donate it”

- Black’s Law Dictionary

• Laws are what provide us all with DRM business opportunities.
• The rights that content providers seek to manage in DRM are creations of the law, and no such right is inherent or self-evident.
Intellectual Properties

• Four basic types of intellectual properties
  – Patents
  – Trademarks
  – Trade secrets
  – Copyrights
    • Central to DRM
Patents

- Patents protect novel and unique inventions or processes.
  - After you patent your invention, nobody can use it without your permission, and you have essentially unlimited monopoly for a period of years.
  - The details of your invention will be disclosed to the world.
  - After the patent time expires, anyone can freely use your invention.
• The limited time frame provides you with an incentive to create new inventions, and the time limit also ensures that everybody can benefit from your inventions in the long run.

Pharmaceutical companies offer a great example of how patents work in the real world.
Patents and DRM

- Patents are not generally the object of DRM systems and applications.
- However, patent rights do play an important role in the creation of DRM systems and applications.

**Patent Pool:** technology companies pool their various patents and agree to reasonable licenses

**Vision of MPEG-21:** a multimedia framework to enable the transparent and augmented use of multimedia resources across a wide range of networks and devices used by different communities
• Trademarks protects logos, trade names, and symbols used to identify a company’s products or services, which could be sounds and smells in addition to graphical symbols.
• The strength of a trademark lies in the answer to the question “What association does the trademark generate in a consumer’s mind?”
• The licensing of trademarks is more close to rights sales, and is less suited to the application of DRM technology.
Trade Secrets

• Trade secrets may consist of any formula, pattern, device of compilation of information which is used in one’s business and which gives a person an opportunity to obtain an advantage over competitors who do not know or use it.

• Trade secrets usually occur within companies that are not primarily content providers, but they manifest themselves in digital information.
  – Thus DRM vendors have begun to build systems that control access to documents and emails.
Copyrights

• Copyrights are central to DRM
  – What you heard about stolen music and streaming video are all related with infringement of somebody’s copyright

• A copyrighted work must be
  – An original work of ownership
    • One who copies another’s original works does not own copyrights, but authors of independent and identical works do
  – Fixed in a tangible medium of expression
  – Able to be reproduced or otherwise communicated
    • Silly examples: books inscribed on the Jupiter or on a electron
Copyrights and DRM

• The essence of DRM involves these questions
  – Whose copyrights are being abused?
  – Whose copyrights may be abused?
  – How can we prevent that?
  – How can we facilitate the use of such copyrights so that the owner gets paid and the users get access?
Balance of Interests

“…The primary objective in conferring the copyright monopoly lies in the general benefit derived by the public from the labors of authors and their agents. It is said that reward to the author or artist serves to induce release to the public of the products of his creative genius…”

- Sony Corporation v. Universal City Studio, 464 US 416, 428

• The primary intent of copyright is to increase and not to impede the harvest of knowledge
• Those seeking to profit from DRM systems should keep in mind that their enrichment is not the primary consideration of the law.
Benefits of Copyright Law

- For a certain number of years, copyright holder has the exclusive right to
  - Reproduce the work
  - Modify the work by creating new work based on the old work
  - Distribute the work
  - Perform the work publicly
  - Display the work publicly
Registering Copyrights

• Copyright arises upon creation, and registration is not required to a copyright to be considered valid.
• Why bother to register copyrights?
  – To recover monetary damages in any action that you bring against an infringer for your copyright, registration is necessary
• The registration system is now inadequate for automatic electronic registrations and needs an overhaul
• DRM systems shall take copyright identification and registration into consideration

The Copyright Office: http://www.loc.gov/copyright/
Types of Copyrighted Works

- **Literal Works**
  - Including book, manuscript, online work, pamphlet, poetry, report, test, automated database, computer program, or other text

- **Visual Arts works**
  - Pictorial, graphic, or sculptural work, including 2-dimensional and 3-dimensional work of fine, graphic, and applied art. Also, register architectural work
  - Performing Arts Works
    - Musical work, dramatic work, script, pantomime, choreography, motion picture, or other audiovisual work

- **Sound Recording**
  - Register your recording of music, drama, or a lecture

- **Serials and Periodicals**
  - Register your recording of music, drama, or a lecture

- **Mask Works**
  - This protection relates to integrated circuits on a semiconductor chip
Fair Use

• Fair use is one of the limitations on the exclusive rights of copyright
  – The fair use of a copyrighted work is not a infringement of copyright
  – It is a defense to an allegation of copyright infringement
  – Example
    • Small-amount usage for educational purpose
  – Not belonging to fair use
    • Substantial usage, commercial purpose, measurable market effect…
Fair Use Factors

- The purpose and character of the use
- The nature of the copyrighted work
- The amount of the taking
- The effect of the market value of the copyrighted work

Fair use can be regarded as one of the examples that copyright seeks to preserve the balance between the copyright owner and work users.
Can fair use survive DRM systems?

- **Positive opinion**
  - As long as the rights specification language is detailed enough, all possible uses of content can be listed and thus fair use can be provided.

- **Negative opinion**
  - Fair use can only be judged case by case, and cannot be objectively defined in advance.
  - Consumers can easily throw away their fair-use rights by agreeing end user license agreement.
First Sale Doctrine

• The First Sale Doctrine said that one can apply his first sale rights to the specific copy he bought

• The First Sale Doctrine with respect to record and computer software rentals is limited by the US congress
First Sale Doctrine in DRM?

• Most electrical media are now supplied under license, instead of being sold.
  – Consumers can easily give up their first sale doctrine rights by agreeing to certain contract.
  – Example:
    • Can you sell or license a legal copy of Microsoft Windows XP to others?
  – Rights protected by copyright laws are supplanted by a commercial agreement

DRM systems protect the freedom to contract, but disrupt the balance that copyright laws want to strike
Characteristics of Licenses and Purchasing

- EULA (End-User License Agreement)
- Copyright protection technology
  - Transferability
- Format migration
  - Continuing access
- Decomposition of works
Important Legislation

- The Uniform Information Transactions Act
- The Digital Millennium Copyright Act
- The Electronic Signature Act
- The European Copyright Directive
The sale of tangible goods is generally governed by a set of laws in the U.S. known as Uniform Commercial Code (UCC)
  – Whether UCC governs software is not clear
• UCITA is a contract law that will provide a clear body of law for software and information license transactions.
• Arguments between licensors and licensees are still unsolved

UCITA Online: www.ucitaonline.com
DRM-related Legislative Concerns

Basics about DMCA (Digital Millennium Copyright Act)

- Signed into law by U. S. President Clinton on October 28, 1998, is one of the response to the requirements in two World Intellectual Property Organizations (WIPO) treaties.
- The **anti-circumvention** provision is the most controversial part of DMCA since it prohibits making or selling devices or services that circumvent technological measure used to protect copyrighted works.

Exception to Anti-Circumvention Provision

- Government activities
- Decision making of educational institutes
- Reverse-engineering for program interoperability
- Encryption researches
- User privacy protection
- System security testing
- Protection for accessing Internet by minors
The Electronic Signatures Act

- President Clinton signed into law the Electronic Signature Act in June 2000.
- Parties can sign checks and apply for loans without a signature on paper.
  - Contracts are legally effective in electronic form
- An important building block for DRM systems