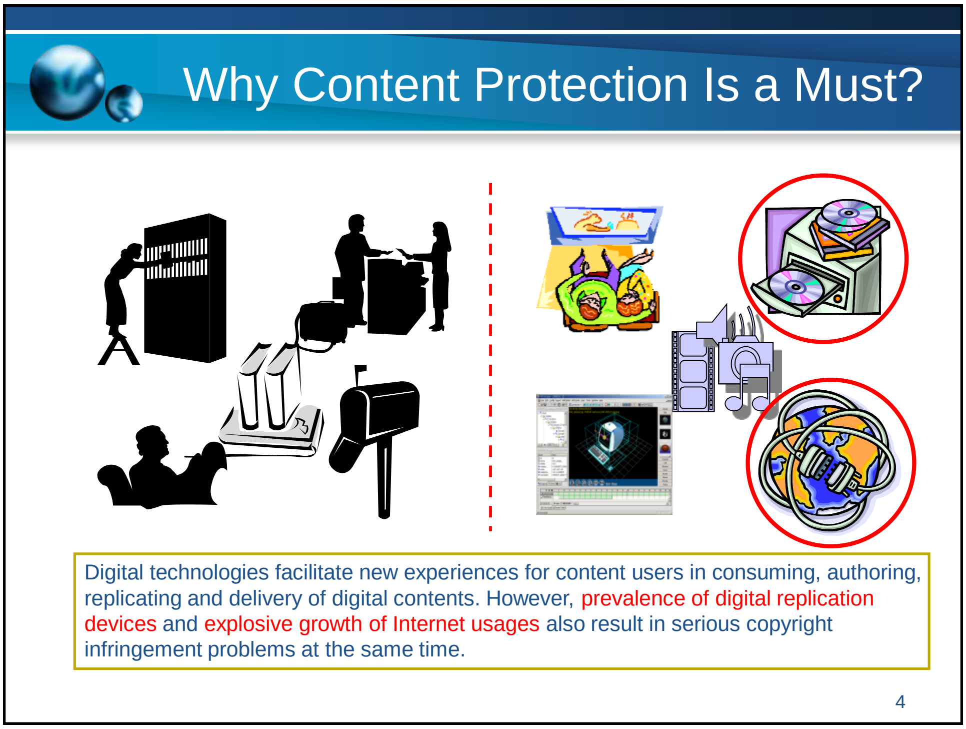
Introduction to Digital Rights Management (DRM)

Multimedia Security

Outline

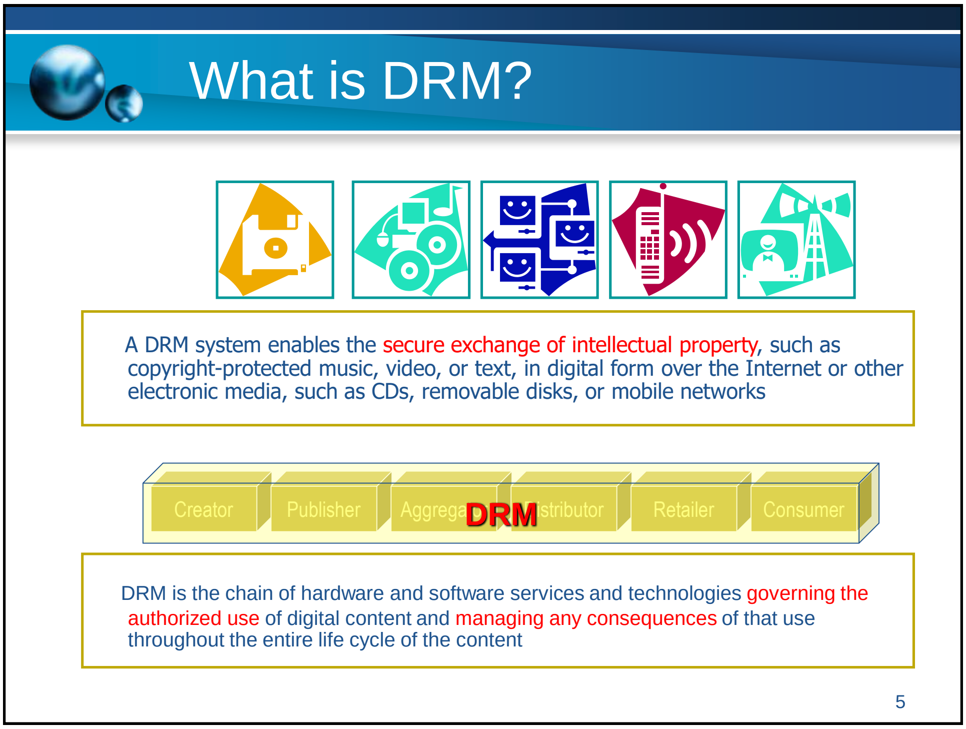
- Digital rights management: an overview
- Digital watermarking
  - Basics and models
  - Trends and challenges
- Cryptography in DRM
- Digital rights languages
- Important DRM standards
- Legislative concerns about DRM
- DRM researches in CML

Digital Rights Management: An Overview



Why Content Protection Is a Must?

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.

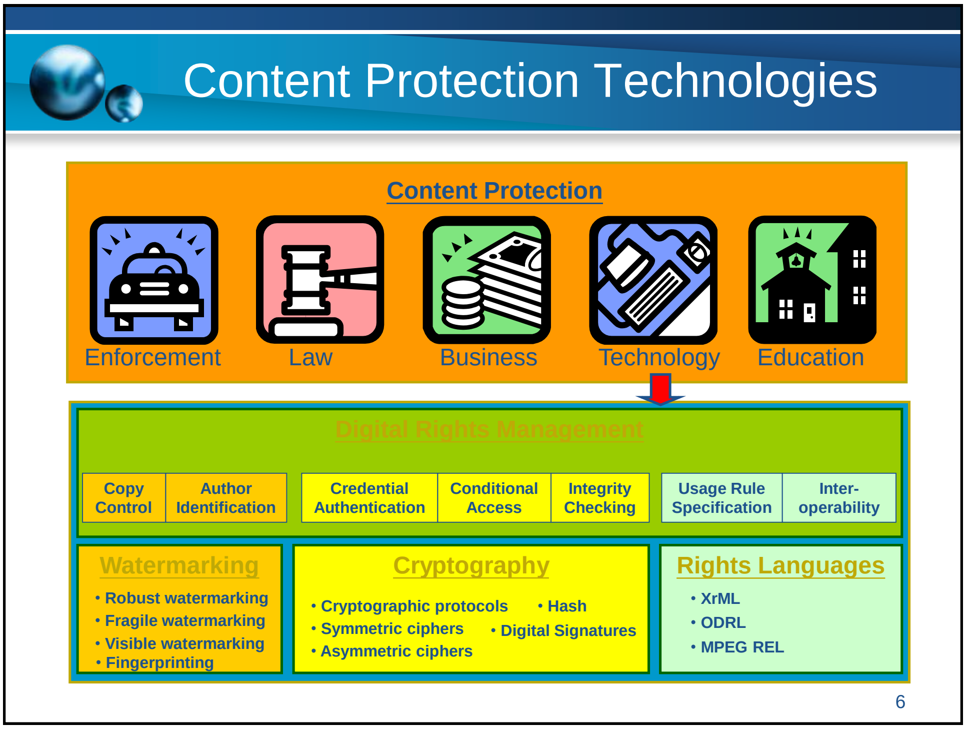


What is DRM?

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

Creator
Publisher
Aggrega
DRM
stributor
Retailer
Consumer

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

Digital Rights Management

Copy Control	Author Identification	Credential Authentication	Conditional Access	Integrity Checking	Usage Rule Specification	Inter-operability

Watermarking

- Robust watermarking
- Fragile watermarking
- Visible watermarking
- Fingerprinting

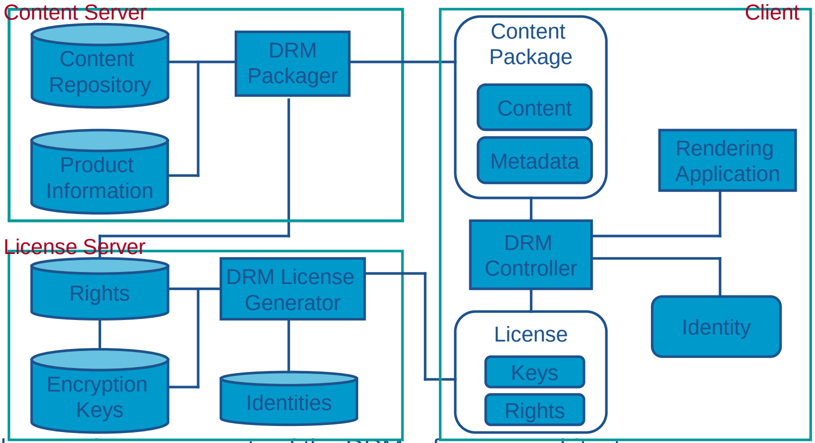
Cryptography

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

Rights Languages

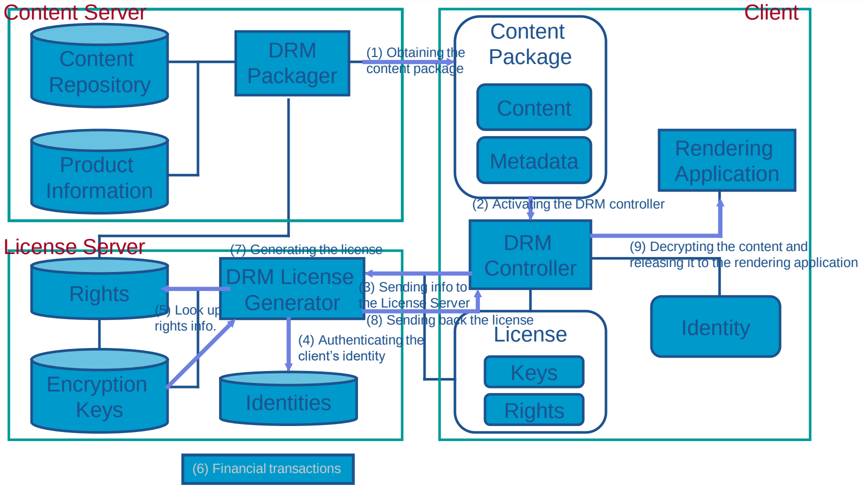
- XrML
- ODRL
- MPEG REL

The DRM Reference Architecture



Three major components of the DRM reference architecture

DRM Events


Content Server
Content Repository
DRM Packager
Product Information
(1) Obtaining the content package
Client
Content Package
Content
Metadata
Rendering Application
(2) Activating the DRM controller
DRM Controller
(9) Decrypting the content and releasing it to the rendering application
License Server
(7) Generating the license
Rights
DRM License Generator
(3) Sending info to the License Server
(8) Sending back the license
(5) Look up rights info.
(4) Authenticating the client's identity
Encryption Keys
Identities
License
Keys
Rights
Identity
(6) Financial transactions

- 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

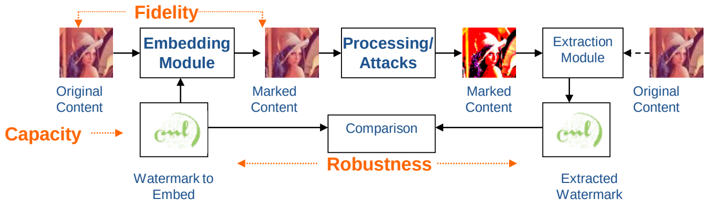
Digital Watermarking Technologies

What is Watermarking?

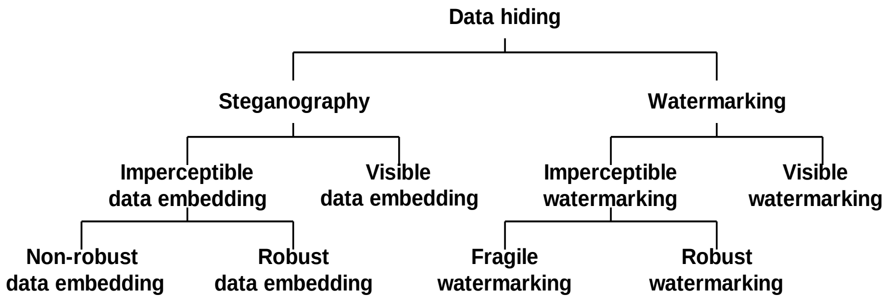
Traditional Watermarking

- 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)



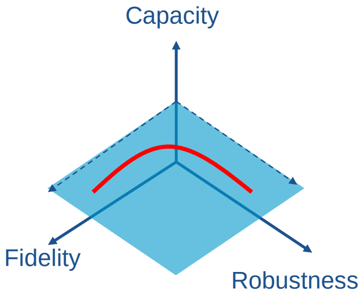
Data Hiding, Watermarking and Steganography

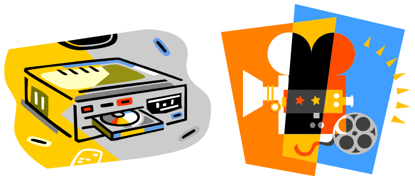


- Data hiding
  - Steganography
    - Imperceptible data embedding
      - Non-robust data embedding
      - Robust data embedding
    - Visible data embedding
  - Watermarking
    - Imperceptible watermarking
      - Fragile watermarking
      - Robust watermarking
    - Visible watermarking

11

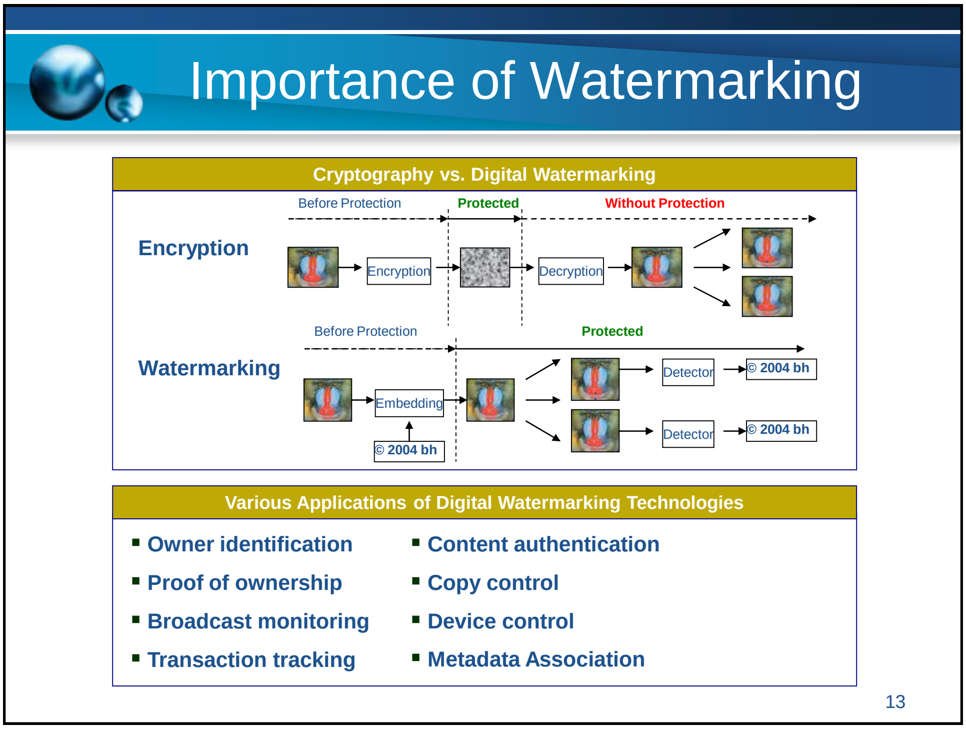
Desired Properties of Watermarking





- 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

12

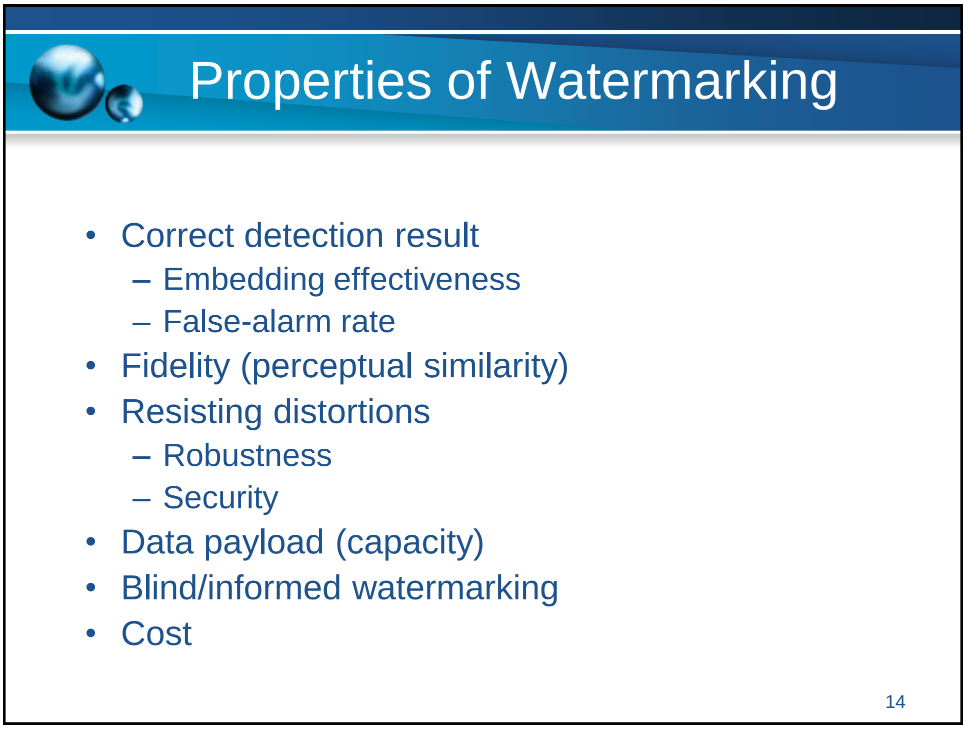


Importance of Watermarking

Cryptography vs. Digital Watermarking

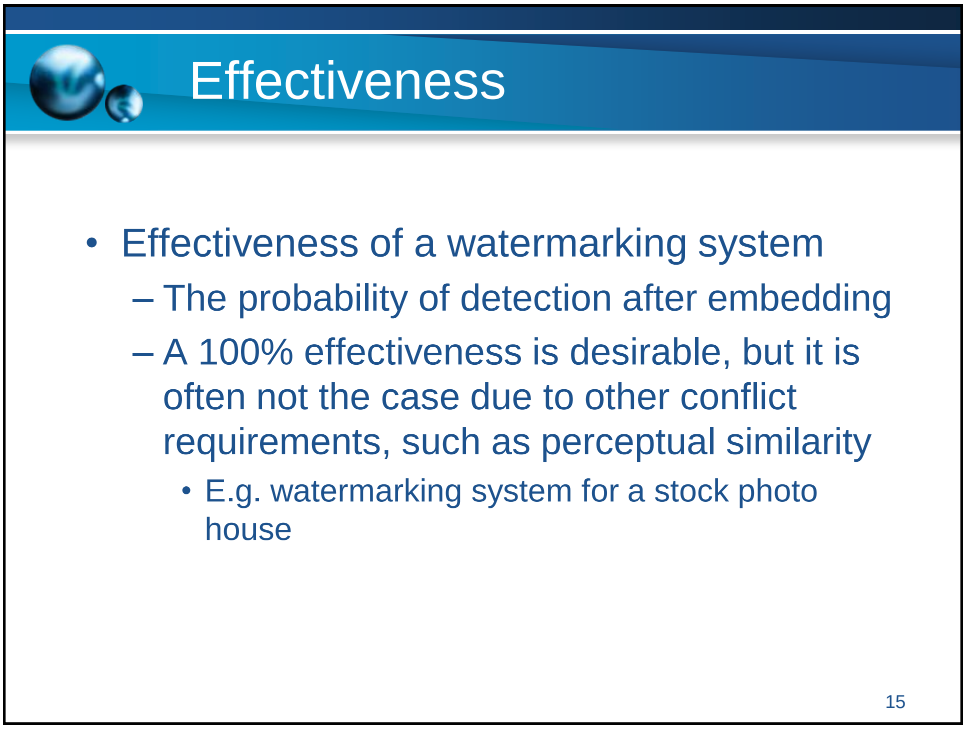
Various Applications of Digital Watermarking Technologies

- Owner identification
- Proof of ownership
- Broadcast monitoring
- Transaction tracking
- Content authentication
- Copy control
- Device control
- Metadata Association



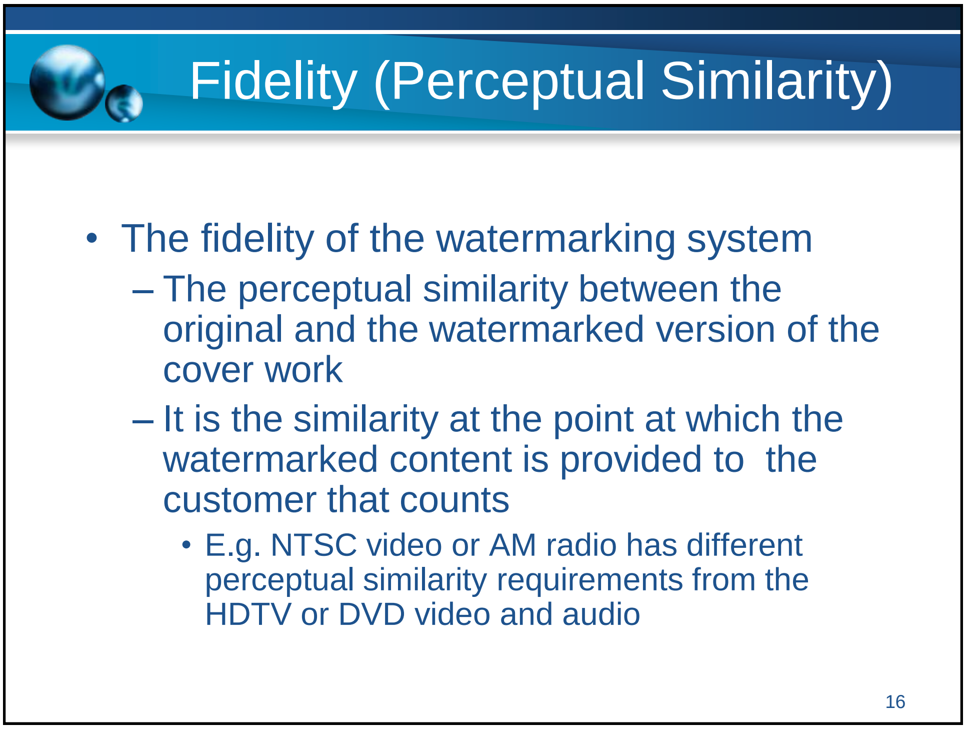
Properties of Watermarking

- 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



Fidelity (Perceptual Similarity)

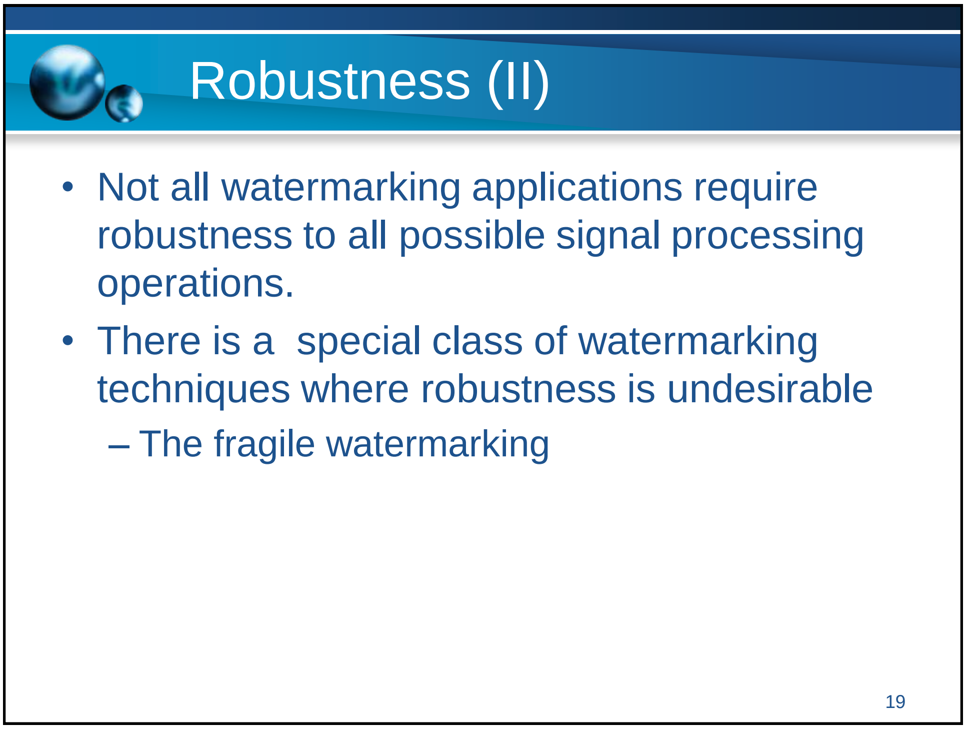
- The fidelity of the watermarking system
  - – The perceptual similarity between the original and the watermarked version of the cover work
  - – It is the similarity at the point at which the watermarked content is provided to the customer that counts
    - E.g. NTSC video or AM radio has different 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: $\dfrac{\sum_{i=1}^{N}(c[i]-c'[i])^2}{\sum_{i=1}^{N}c[i]^2}$
- Finding a quality index completely reflecting the characteristics of the human perceptual model is difficult

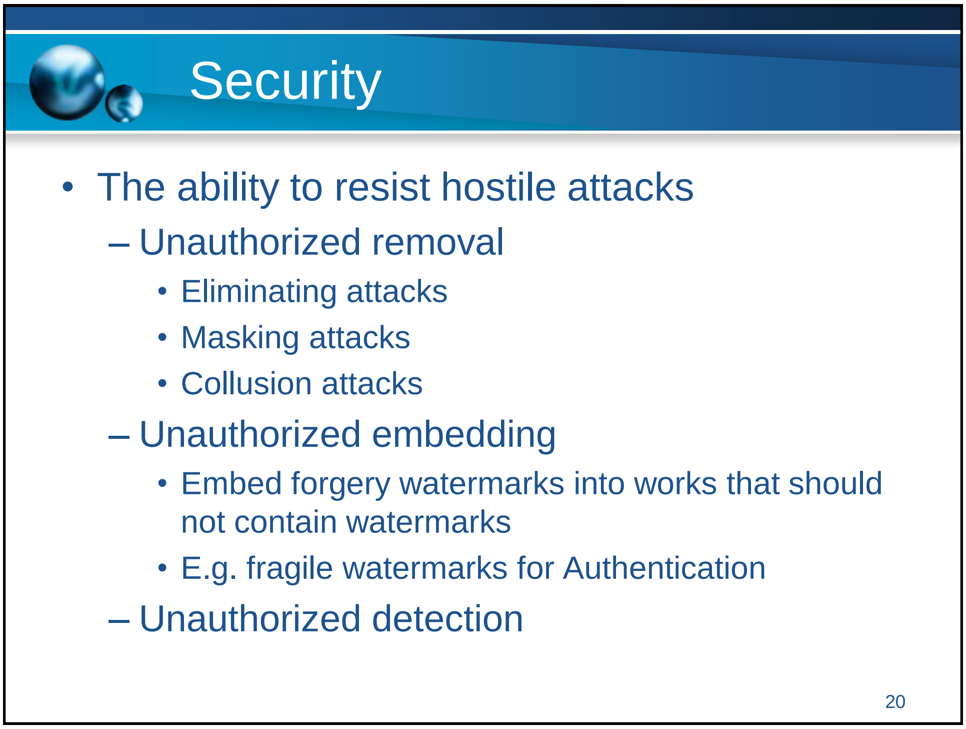
Robustness (I)

- 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



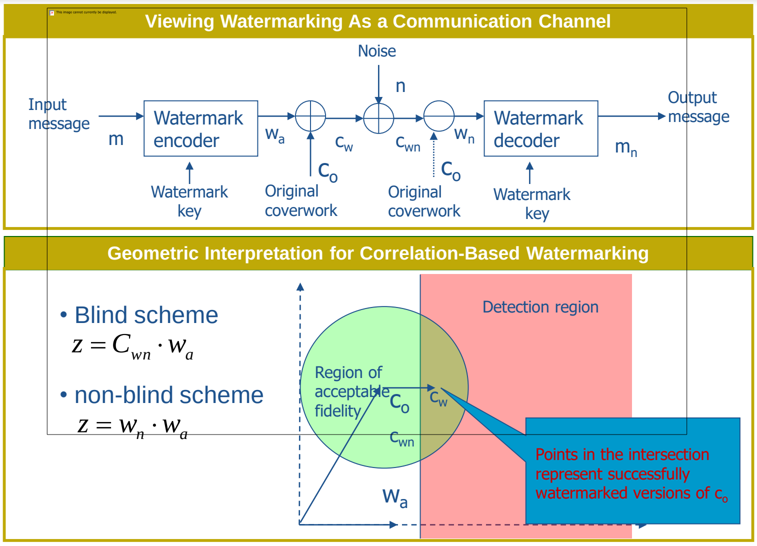
Security

- 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

Models of Digital Watermarking

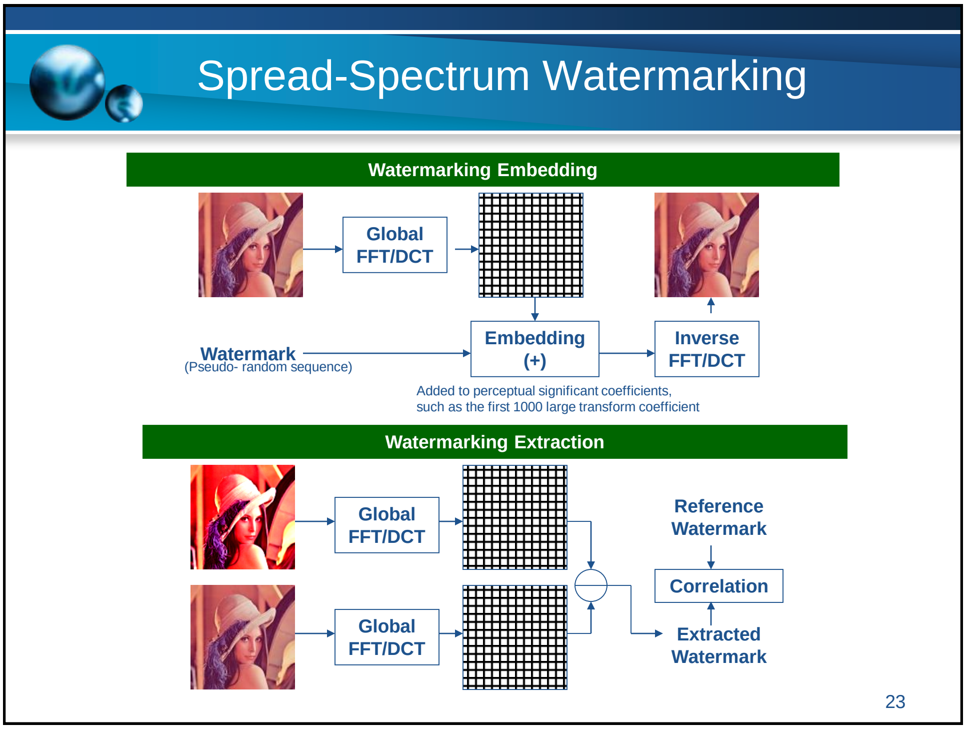


Viewing Watermarking As a Communication Channel

Geometric Interpretation for Correlation-Based Watermarking

- Blind scheme $z = C_{wn} \cdot w_a$
- non-blind scheme $z = w_n \cdot w_a$

Points in the intersection represent successfully watermarked versions of c_o



Spread-Spectrum Watermarking

Watermarking Embedding

Global FFT/DCT

Watermark
(Pseudo- random sequence)

Embedding (+)

Inverse FFT/DCT

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

Watermarking Extraction

Global FFT/DCT

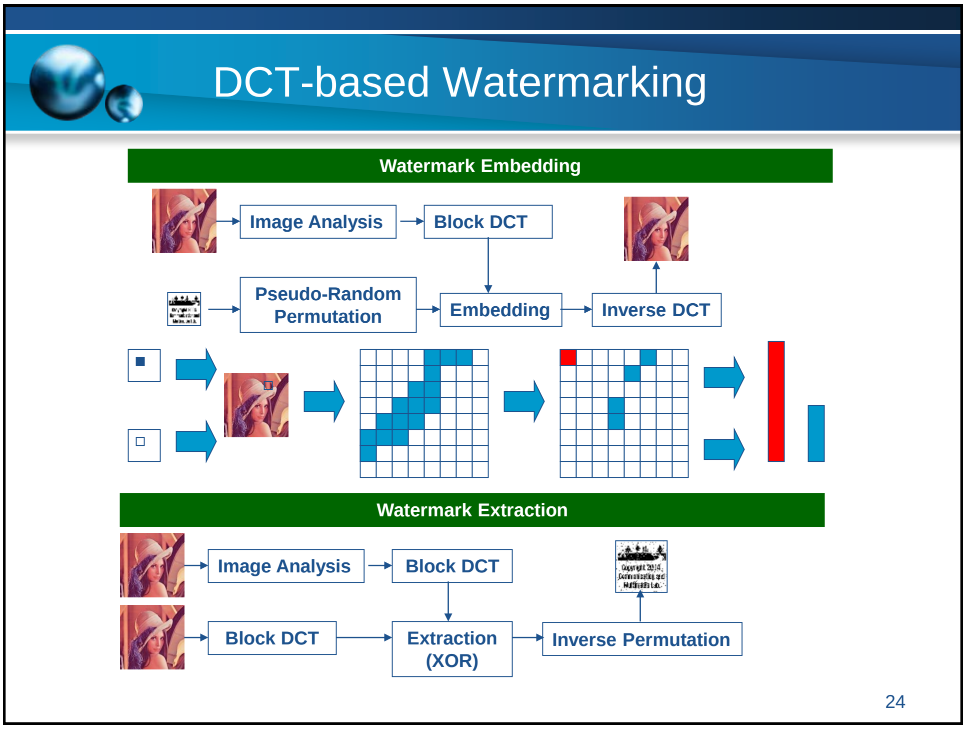
Global FFT/DCT

Reference Watermark

Correlation

Extracted Watermark

23



DCT-based Watermarking

Watermark Embedding

Image Analysis

Block DCT

Pseudo-Random Permutation

Embedding

Inverse DCT

Watermark Extraction

Image Analysis

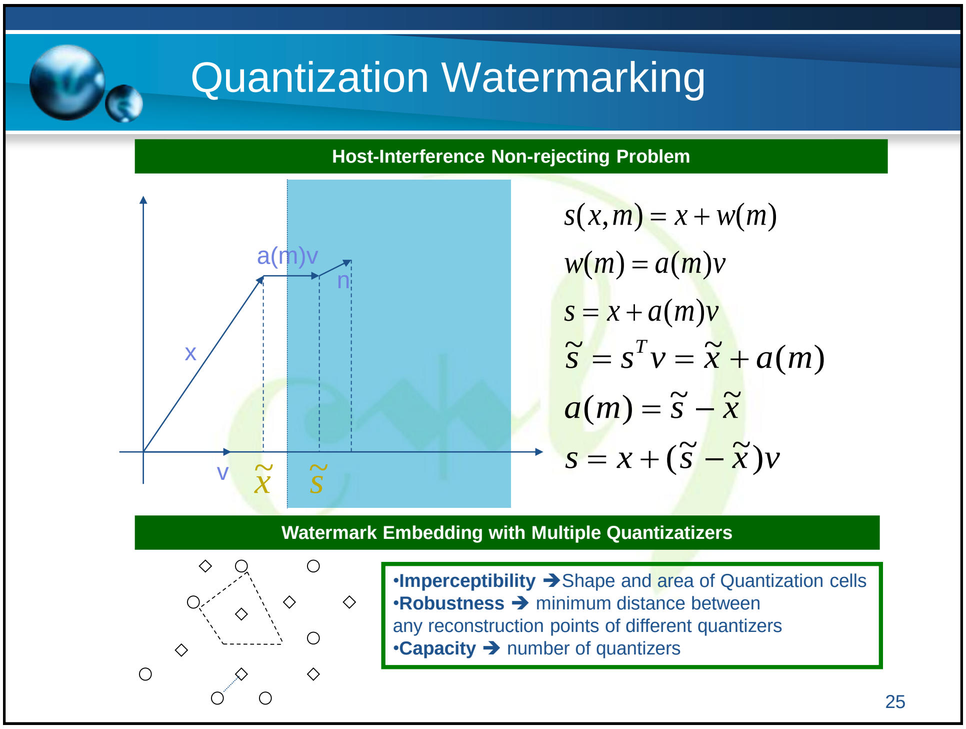
Block DCT

Block DCT

Extraction (XOR)

Inverse Permutation

24



Quantization Watermarking

Host-Interference Non-rejecting Problem

$$s(x,m) = x + w(m)$$

$$w(m) = a(m)v$$

$$s = x + a(m)v$$

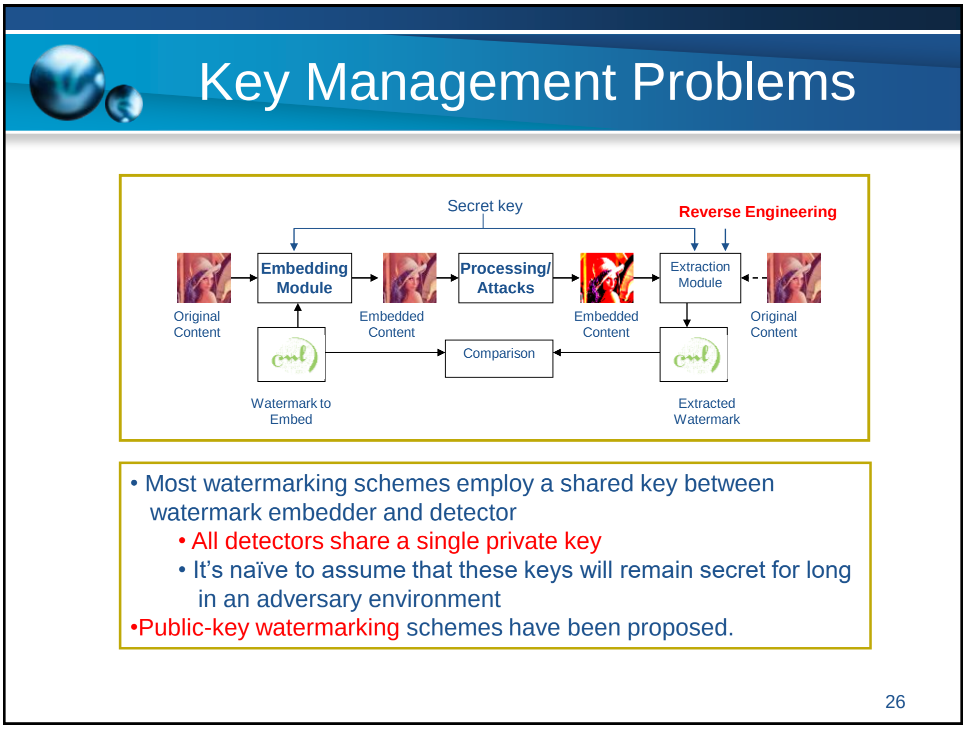
$$\tilde{s} = s^T v = \tilde{x} + a(m)$$

$$a(m) = \tilde{s} - \tilde{x}$$

$$s = x + (\tilde{s} - \tilde{x})v$$

Watermark Embedding with Multiple Quantizatizers

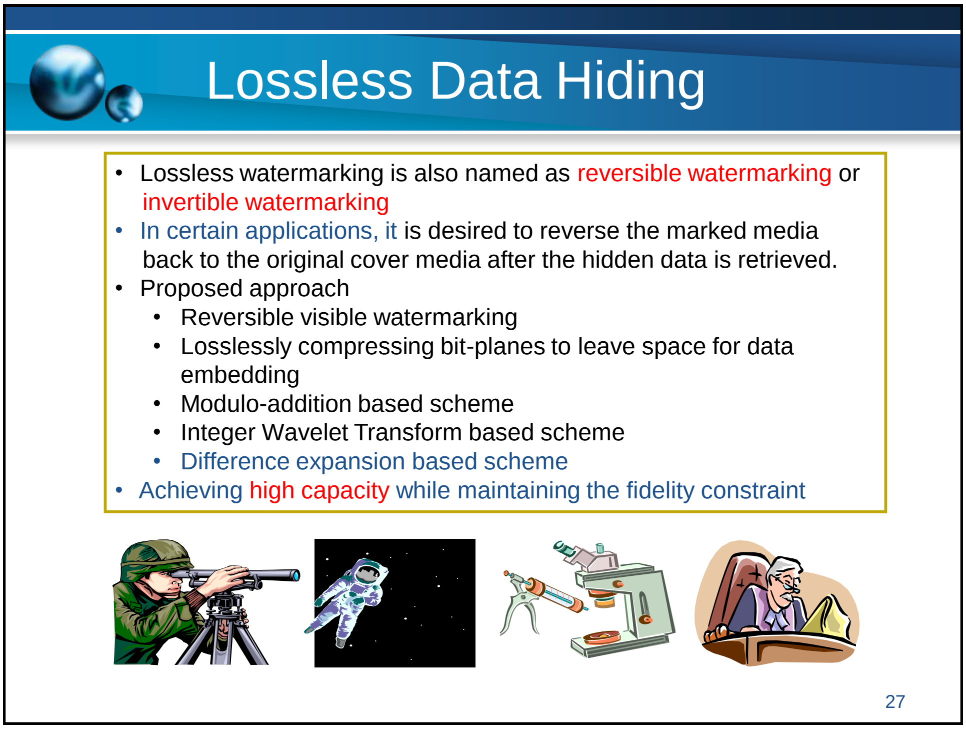
•**Imperceptibility** ➔Shape and area of Quantization cells
•**Robustness** ➔ minimum distance between any reconstruction points of different quantizers
•**Capacity** ➔ number of quantizers



Key Management Problems

- 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

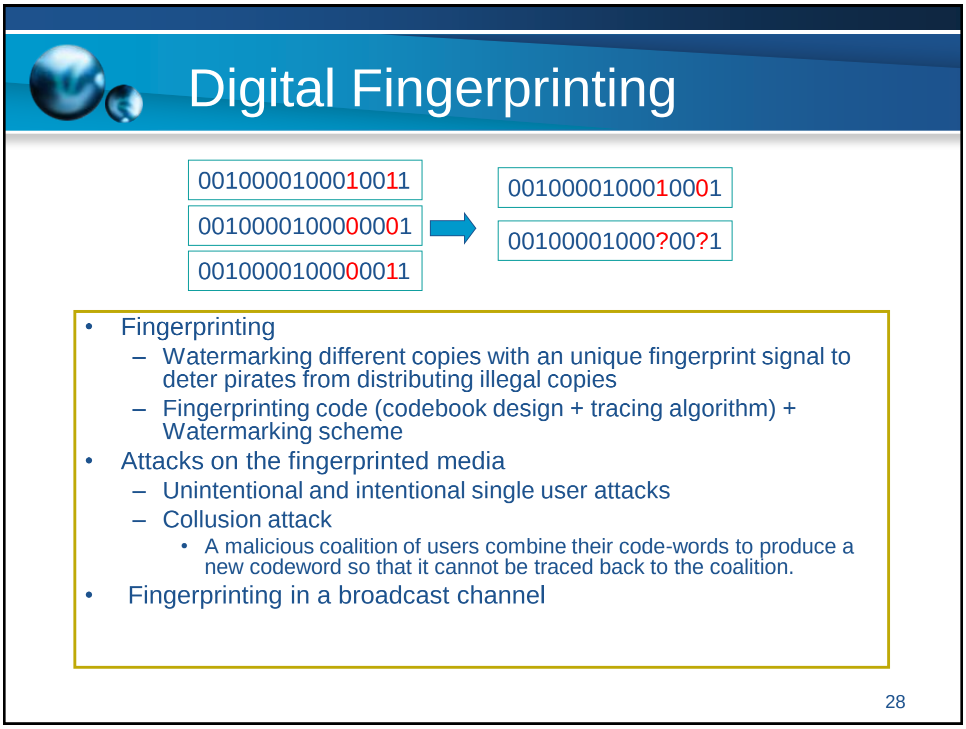
•Public-key watermarking schemes have been proposed.



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

27



Digital Fingerprinting

0010000100010011

0010000100000001

0010000100000011

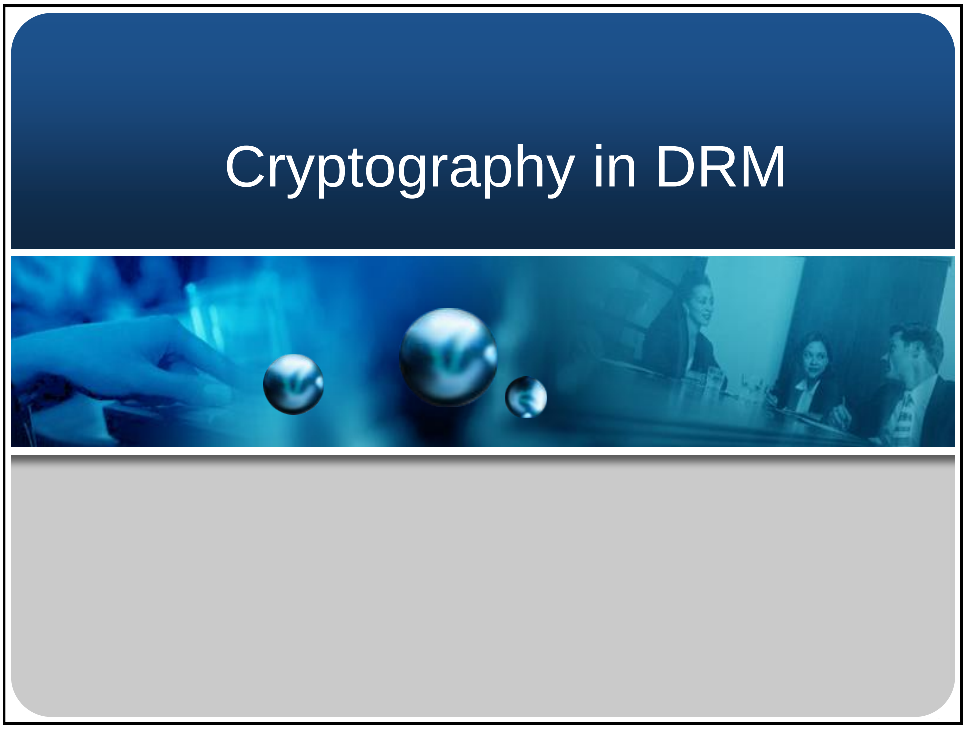
→

0010000100010001

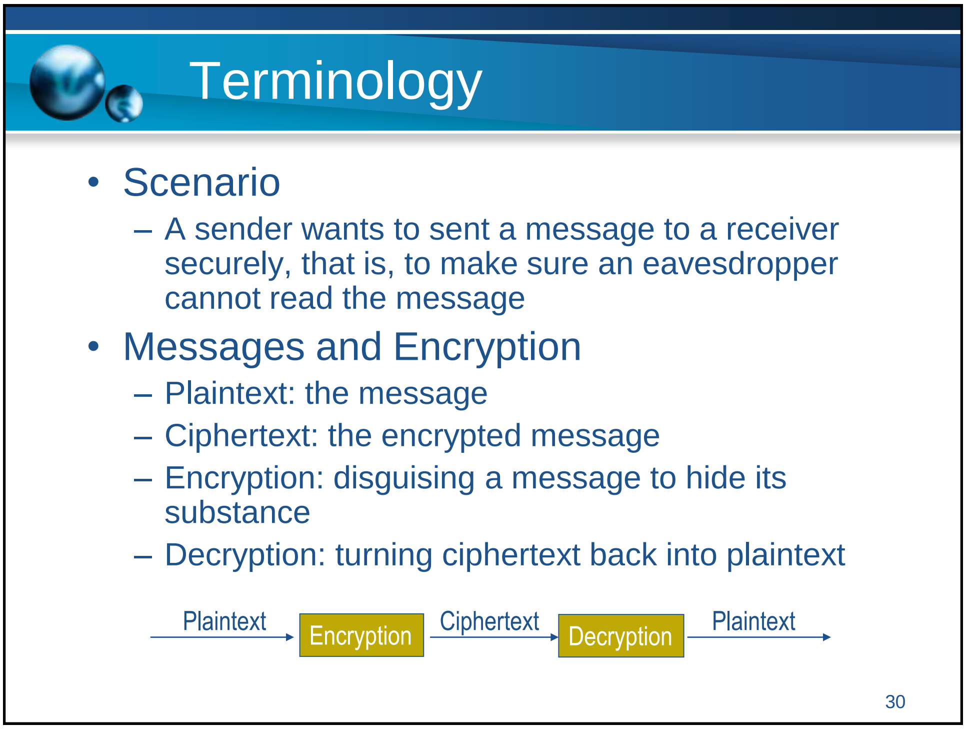
00100001000?00?1

- 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

28



Cryptography in DRM

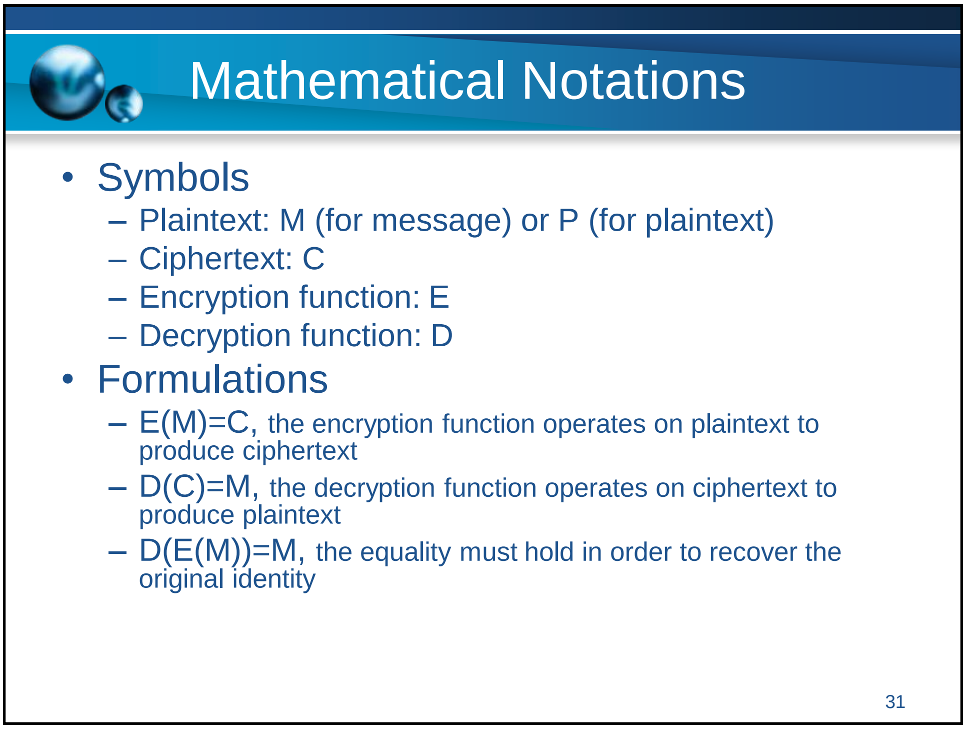


Terminology

- Scenario
  - A sender wants to sent 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

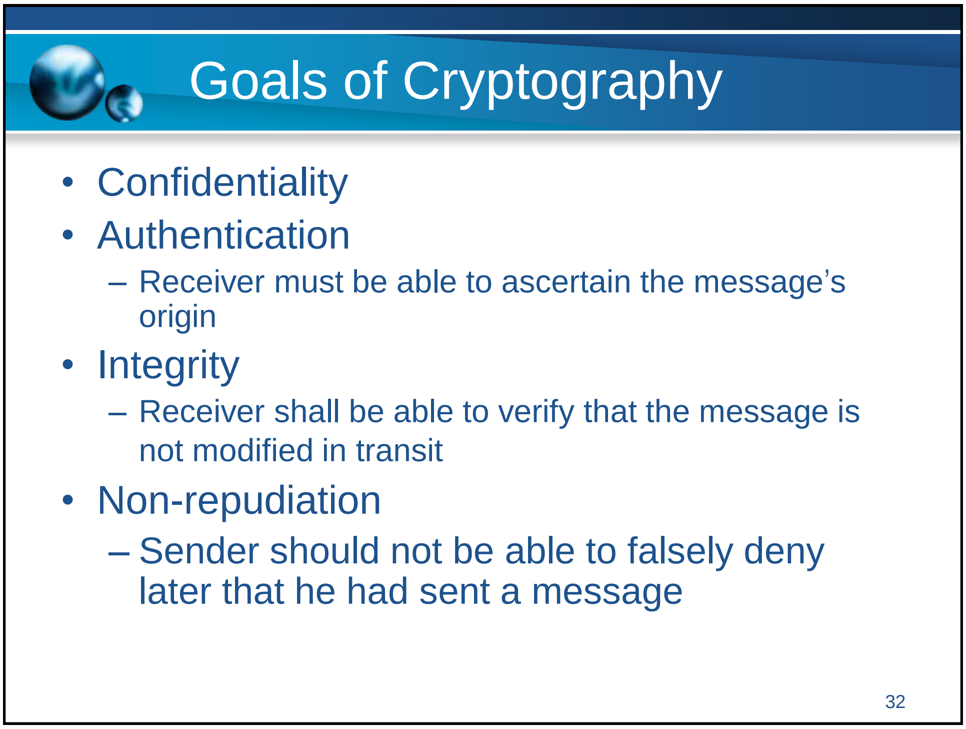
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

30



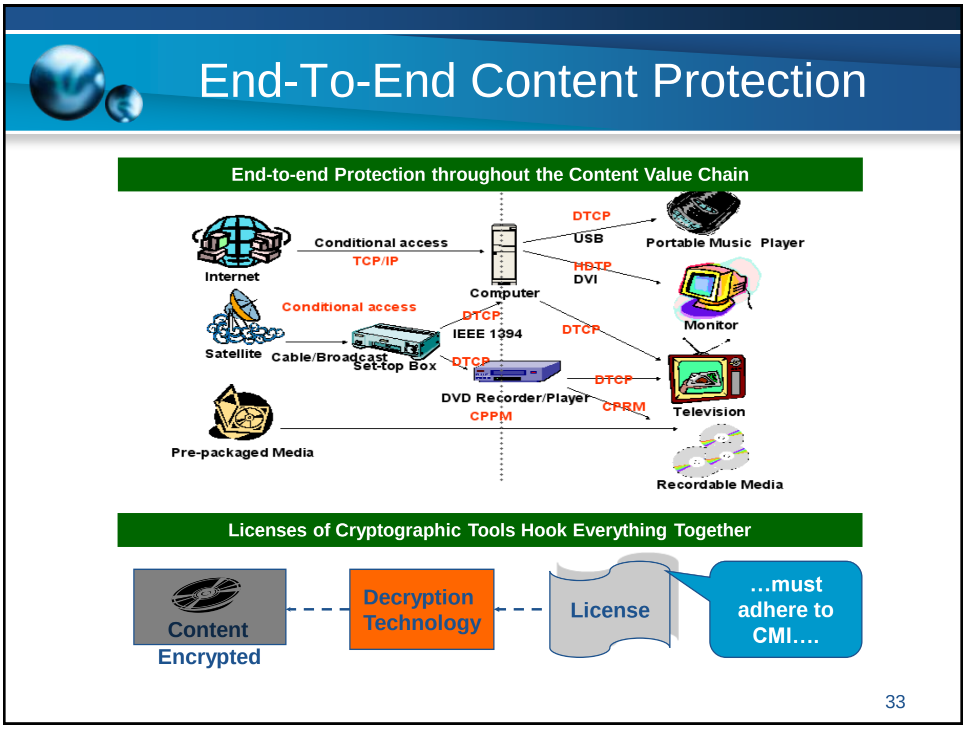
Mathematical Notations

- 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



End-To-End Content Protection

End-to-end Protection throughout the Content Value Chain

Internet
Conditional access
TCP/IP
Computer
DTCP
USB
Portable Music Player
HDTP
DVI
Monitor
Satellite
Conditional access
Cable/Broadcast
Set-top Box
DTCP
IEEE 1394
DTCP
DTCP
DVD Recorder/Player
DTCP
CPRM
Television
CPPM
Pre-packaged Media
Recordable Media

Licenses of Cryptographic Tools Hook Everything Together

Content Encrypted

Decryption Technology

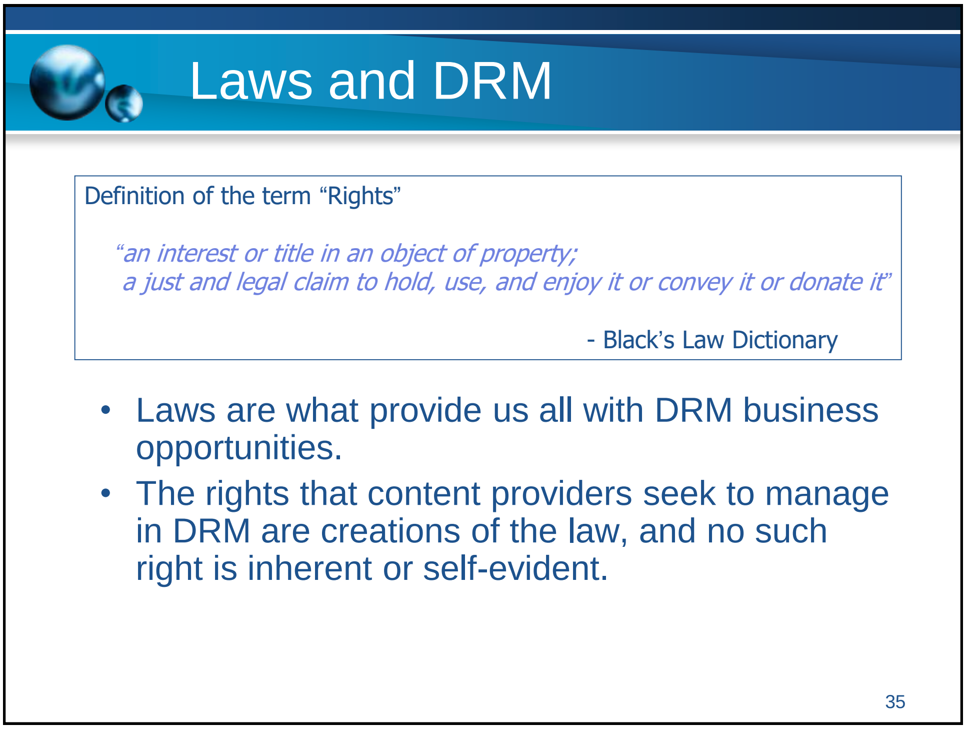
License

…must adhere to CMI….

33

DRM-related Legislative Issues

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

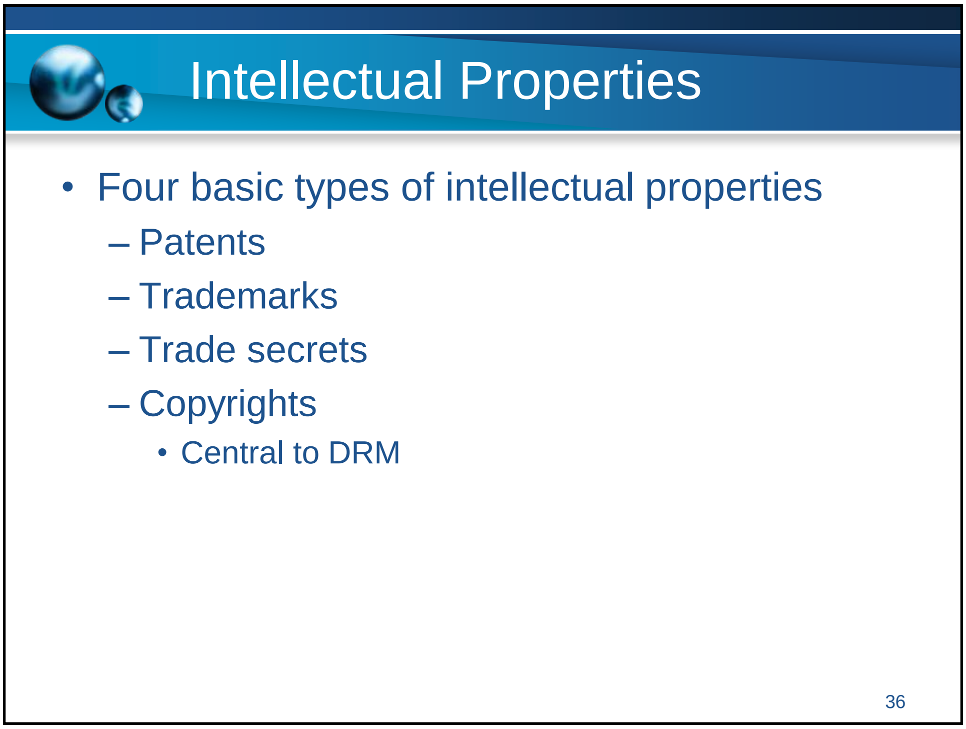


Laws and DRM

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

Patents (cont.)

- 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

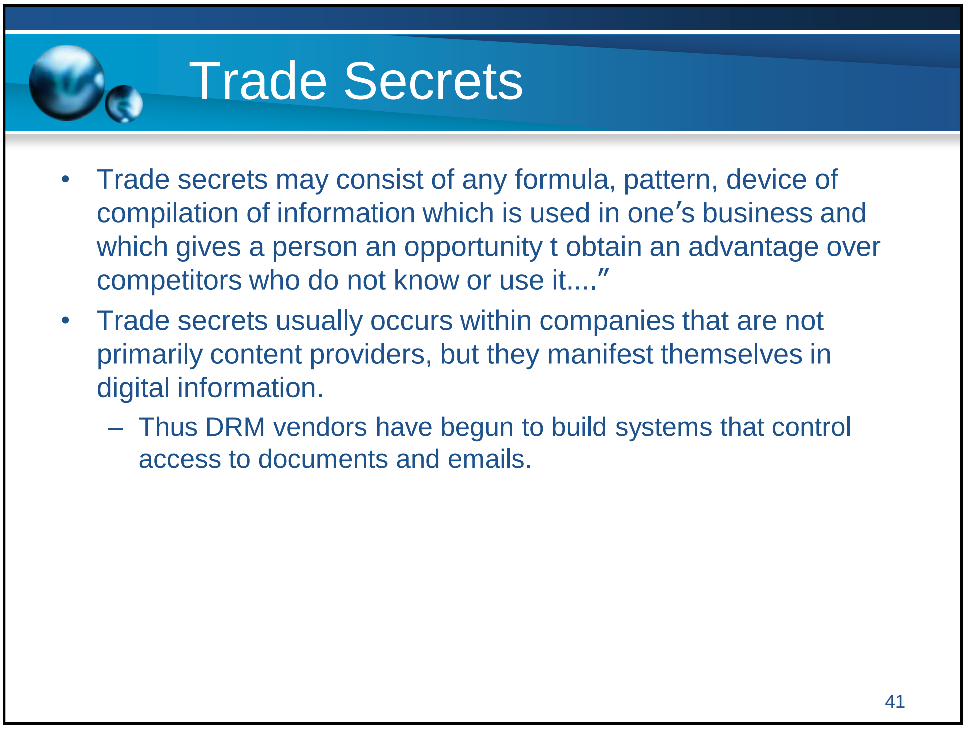
- Patents are not generally the object of DRM systems and applications.
- However, patent rights do play an important role in the creation of DRM systems and applications

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

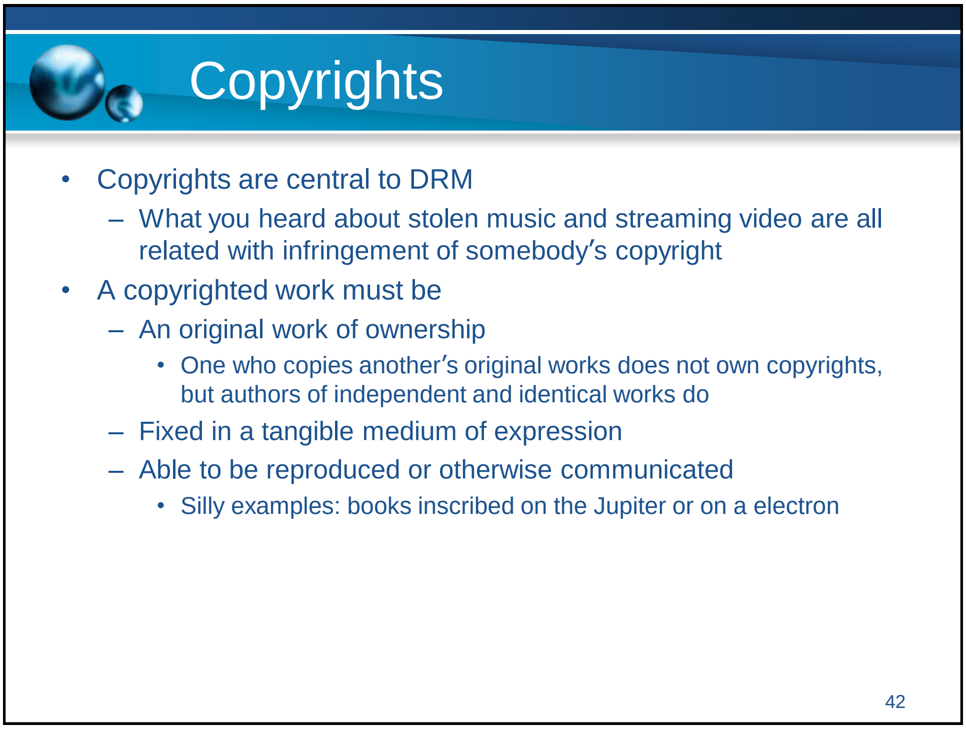
- Trademarks protects logos, trade names, and symbols used to identify a company’s products or services, which could be sounds and smells in addition to graphical symbols.
- The strength of a trademark lies in the answer to the question ”What association does the trademark generate in a consumer’s mind?”
- 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 t obtain an advantage over competitors who do not know or use it....″
- Trade secrets usually occurs 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.

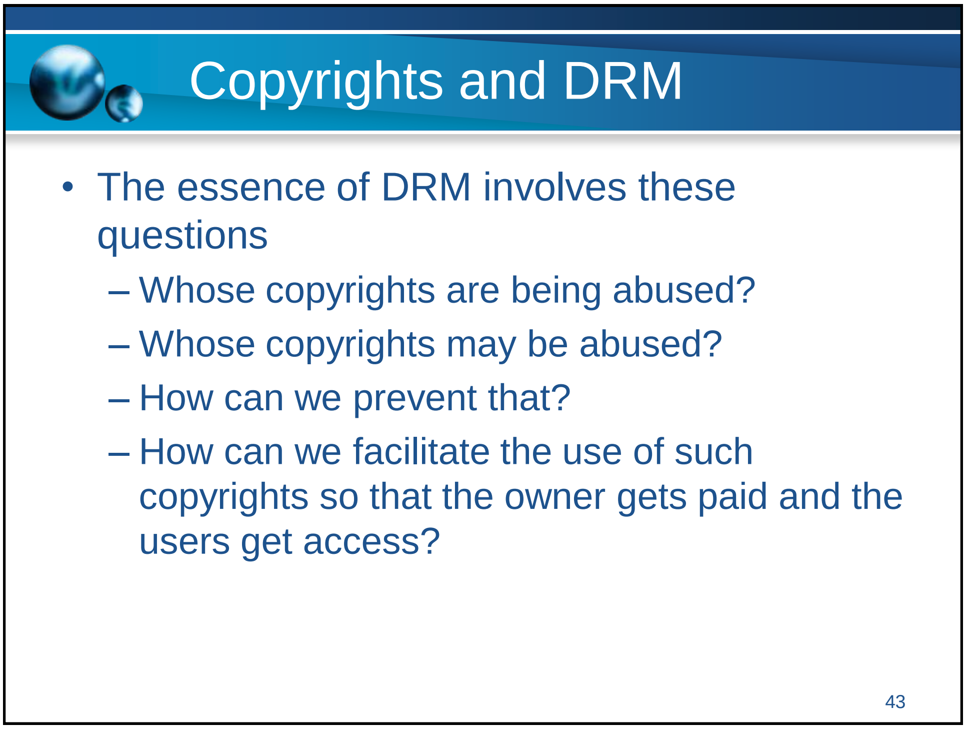
41



Copyrights

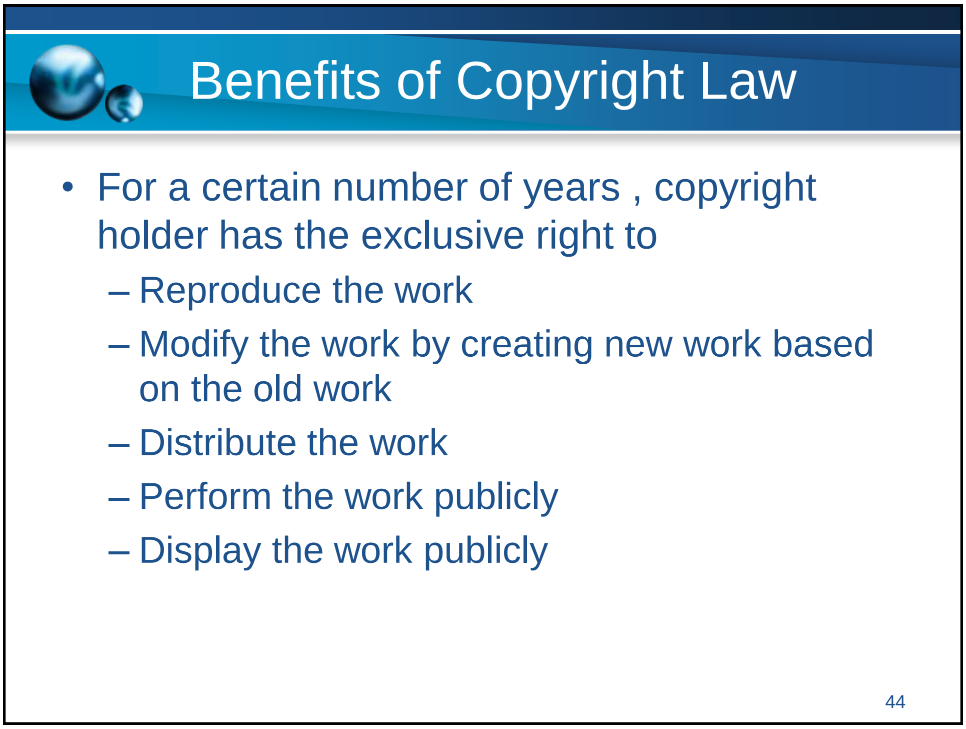
- Copyrights are central to DRM
  - What you heard about stolen music and streaming video are all related with infringement of somebody′s copyright
- A copyrighted work must be
  - An original work of ownership
    - One who copies another′s original works does not own copyrights, but authors of independent 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

42



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?



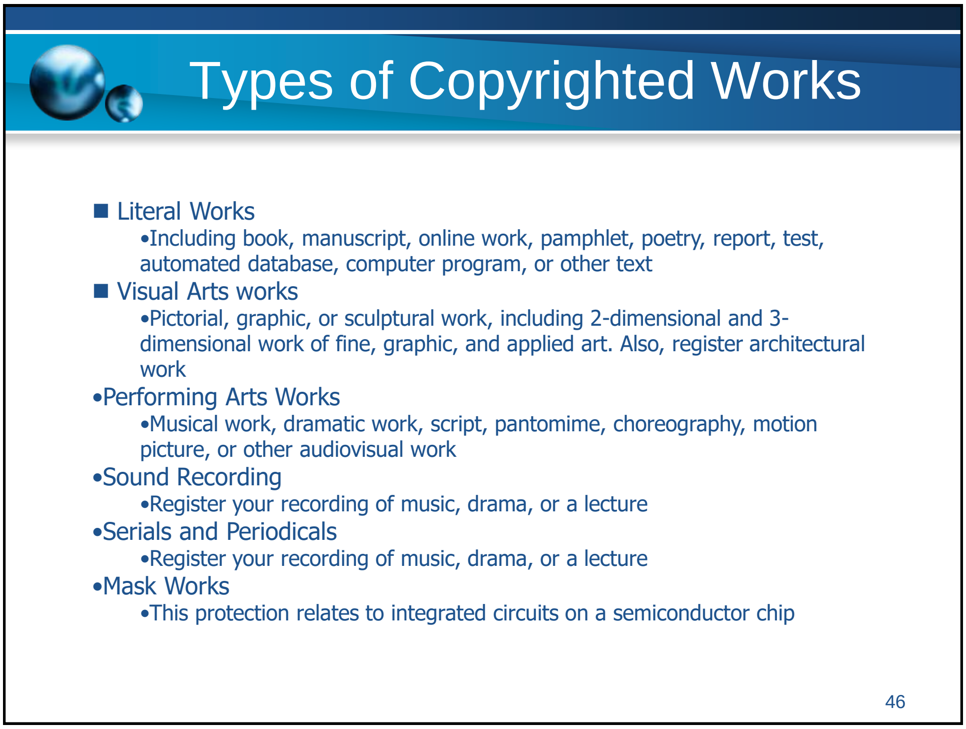
Benefits of Copyright Law

- 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

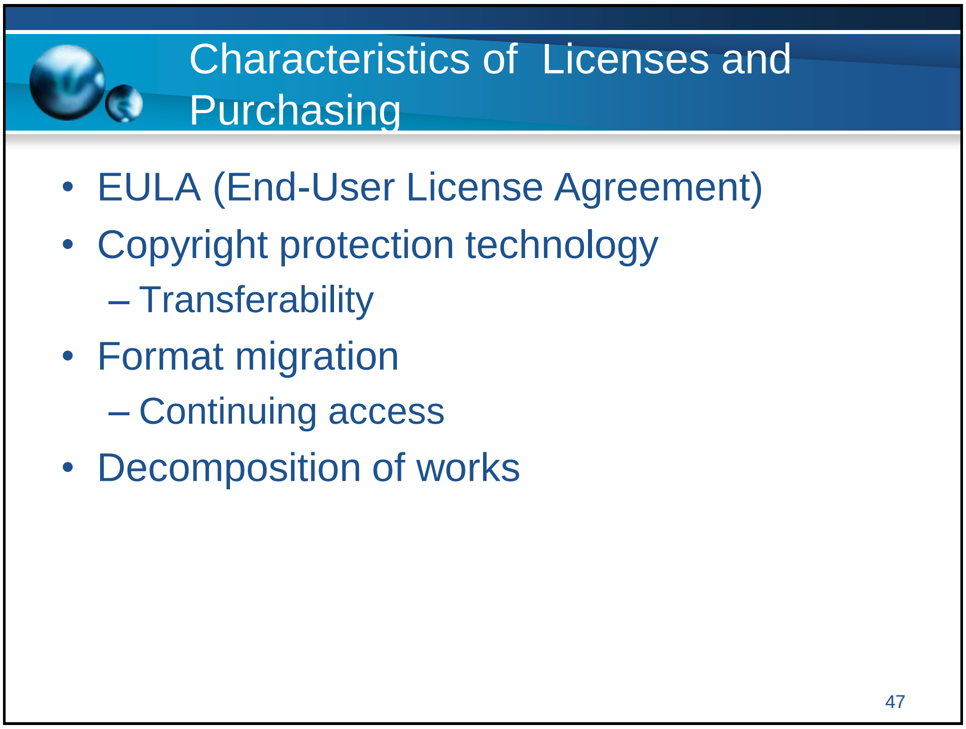
- Copyright arises upon creation, and registration is not required to a copyright to be considered valid.
- Why bother to register copyrights?
  - To recover monetary damages in any action that you bring against an infringer for your copyright, registration is necessary
- The registration system is now 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



Characteristics of Licenses and Purchasing

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