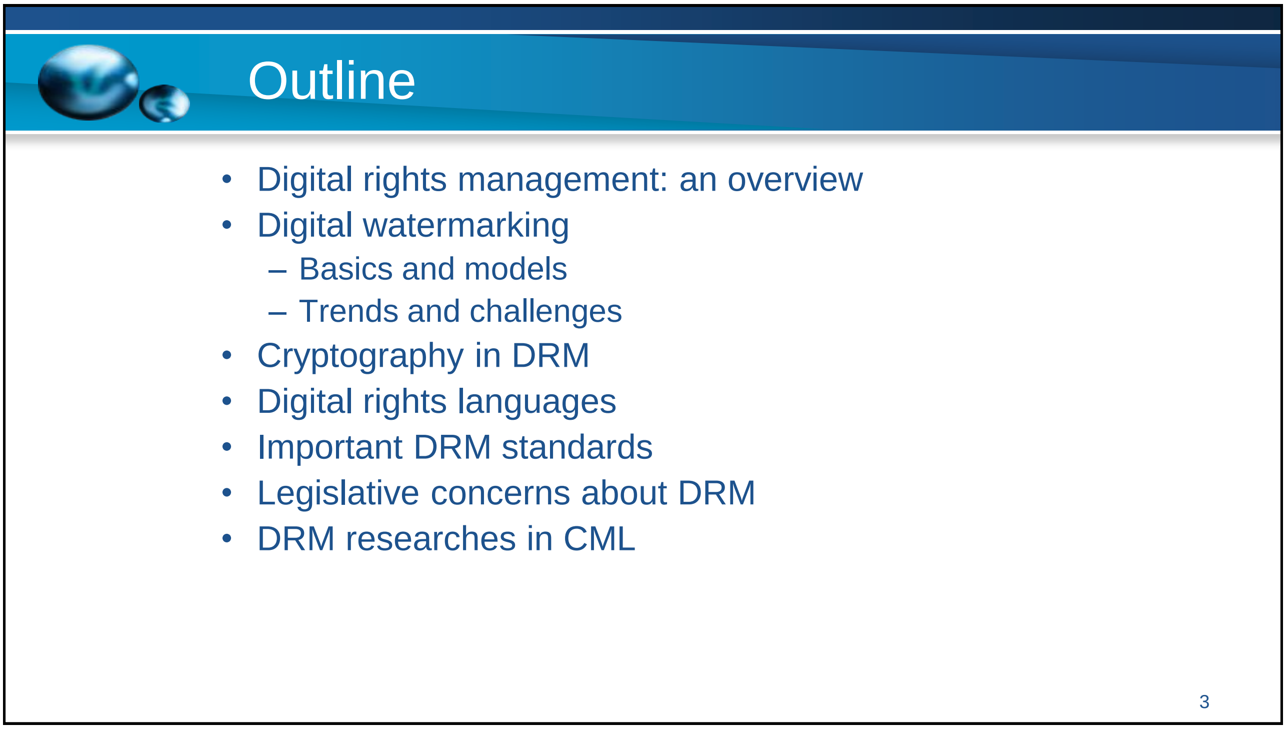
INTRODUCTION TO
Digital Rights Management (DRM)

Dr. Bashar M. Nema

PhD Course-2021

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

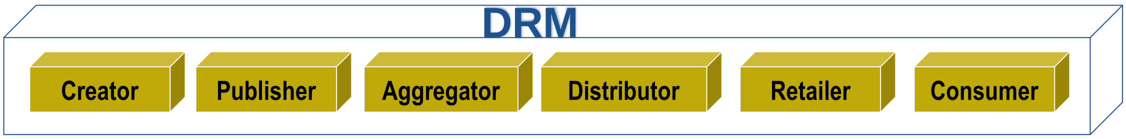
Why Content Protection Is a Must?

لماذا حماية المحتوى أمر لا بد منه؟
تسهل التقنيات الرقمية تجارب جديدة
لمستخدمي المحتوى في استهلاك
المحتويات الرقمية وتأليفها وتكرارها
وتسليمها .ومع ذلك ، فإن انتشار أجهزة
النسخ الرقمي والنمو الهائل لاستخدام
الإنترنت يؤدي أيضًا إلى مشاكل خطيرة
في انتهاك حقوق النشر في نفس
الوقت.

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

Creator

Publisher

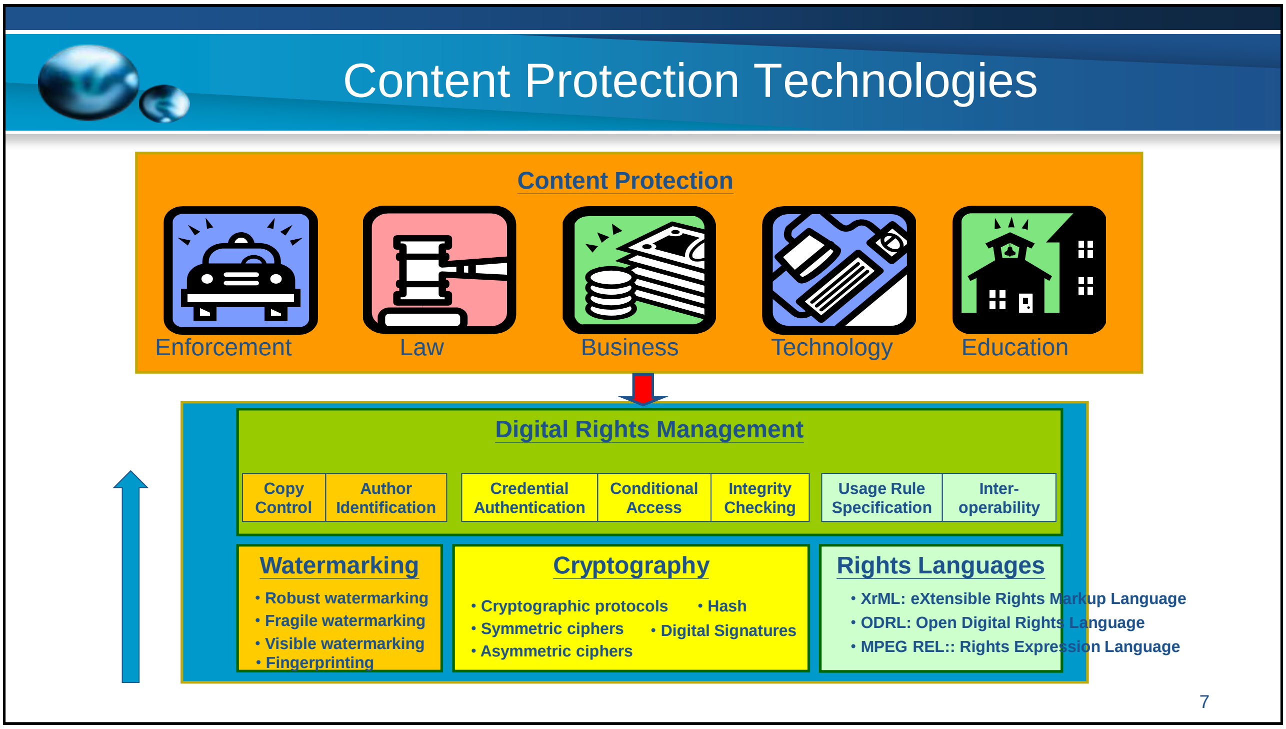
Aggregator

Distributor

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

Enforcement | Law | Business | Technology | Education

Digital Rights Management

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

Watermarking

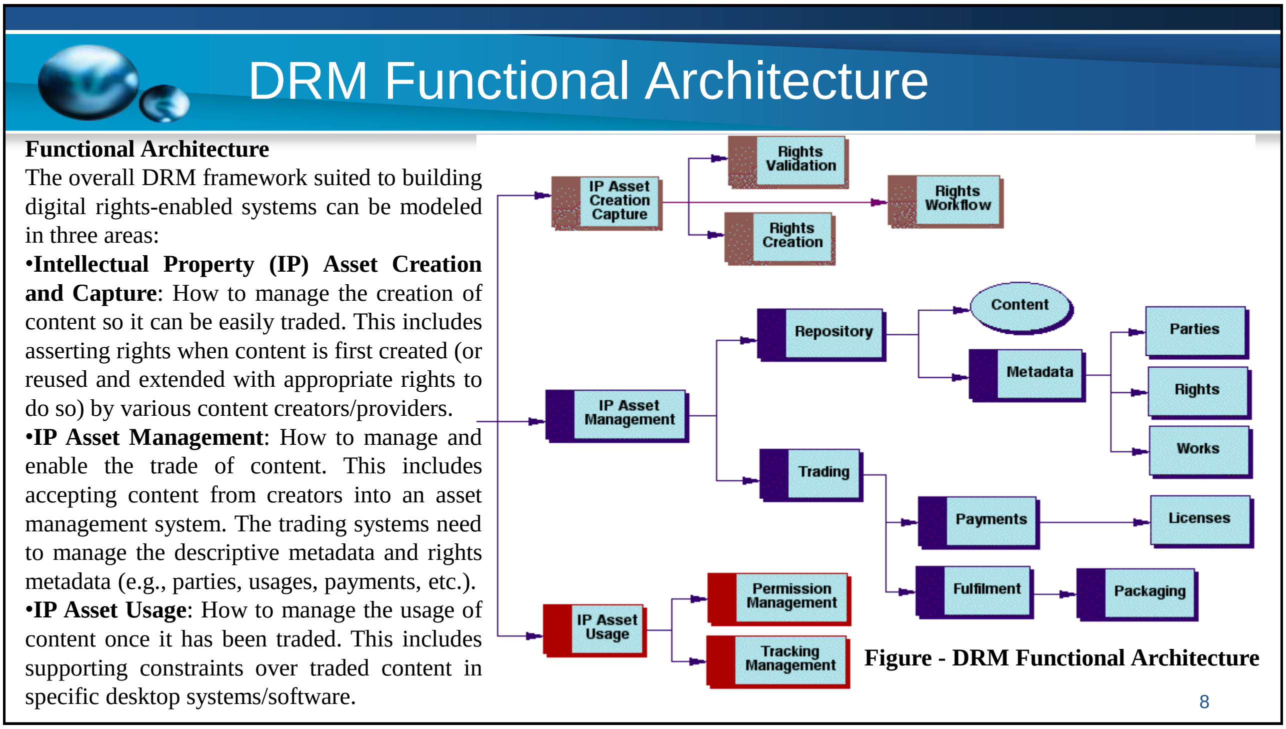
- Robust watermarking
- Fragile watermarking
- Visible watermarking
- Fingerprinting

Cryptography

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

Rights Languages

- XrML: eXtensible Rights Markup Language
- ODRL: Open Digital Rights Language
- MPEG REL:: Rights Expression Language



DRM Functional Architecture

Functional Architecture

The overall DRM framework suited to building digital rights-enabled systems can be modeled in three areas:

•**Intellectual Property (IP) Asset Creation and Capture**: How to manage the creation of content so it can be easily traded. This includes asserting rights when content is first created (or reused and extended with appropriate rights to do so) by various content creators/providers.

•**IP Asset Management**: How to manage and enable the trade of content. This includes accepting content from creators into an asset management system. The trading systems need to manage the descriptive metadata and rights metadata (e.g., parties, usages, payments, etc.).

•**IP Asset Usage**: How to manage the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.

Figure - DRM Functional Architecture

The IP Asset Creation and Capture module supports:

•**Rights Validation** - to ensure that content being created from existing content includes the rights to do so.

•**Rights Creation** - to allow rights to be assigned to new content, such as specifying the rights owners and allowable usage permissions.

•**Rights Workflow** - to allow for content to be processed through a series of workflow steps for review and/or approval of rights (and content).

The IP Asset Management module supports:

•**Repository functions** - to enable the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata. The metadata covers Parties, Rights and descriptions of the Works. (See the Information Architecture section of this article for more details.)

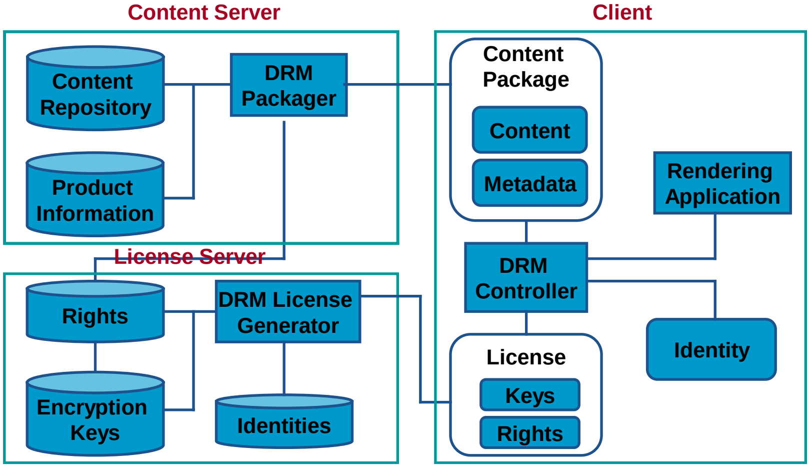
•**Trading functions** - to enable the assignment of licenses to parties who have traded agreements for rights over content, including payments from licensees to rights holders (e.g., royalty payments). In some cases, the content may need to go through fulfillment operations to satisfy the license agreement. For example, the content may be encrypted/protected or packaged for a particular type of desktop usage environment.

The IP Asset Usage module supports:

•**Permissions Management** - to enable the usage environment to honor the rights associated with the content. For example, if the user only has the right to view the document, then printing will not be allowed.

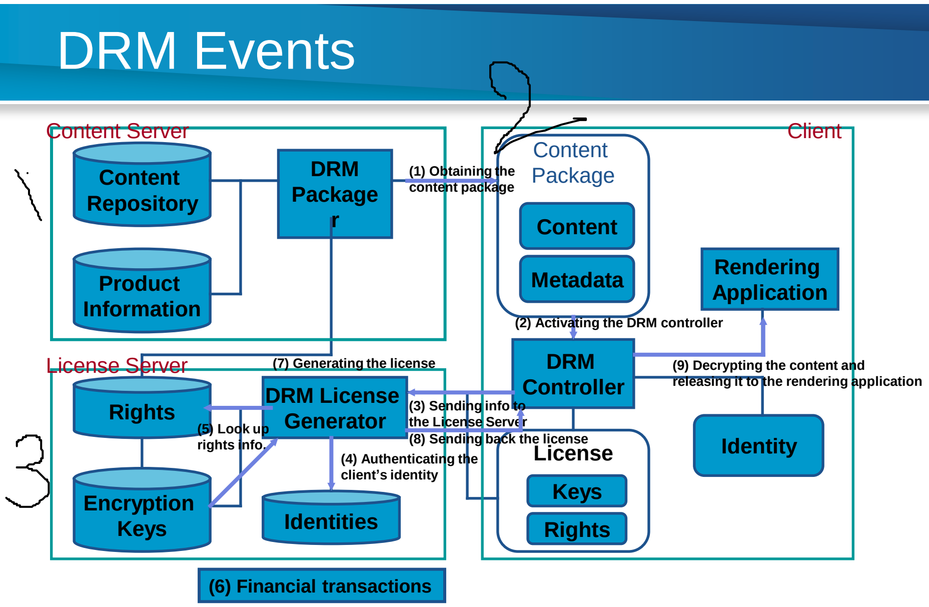
•**Tracking Management** - to enable the monitoring of the usage of content where such tracking is part of the agreed to license conditions (e.g., the user has a license to play a video ten times).

The DRM Reference Architecture



Three major components of the DRM reference architecture

DRM Events



1

Content Server

Content Repository

Product Information

DRM Packager

(1) Obtaining the content package

2

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

Identity

3

License Server

(7) Generating the license

Rights

DRM License Generator

(5) Look up rights info.

(3) Sending info to the License Server

(8) Sending back the license

(4) Authenticating the client's identity

License

Keys

Rights

Encryption Keys

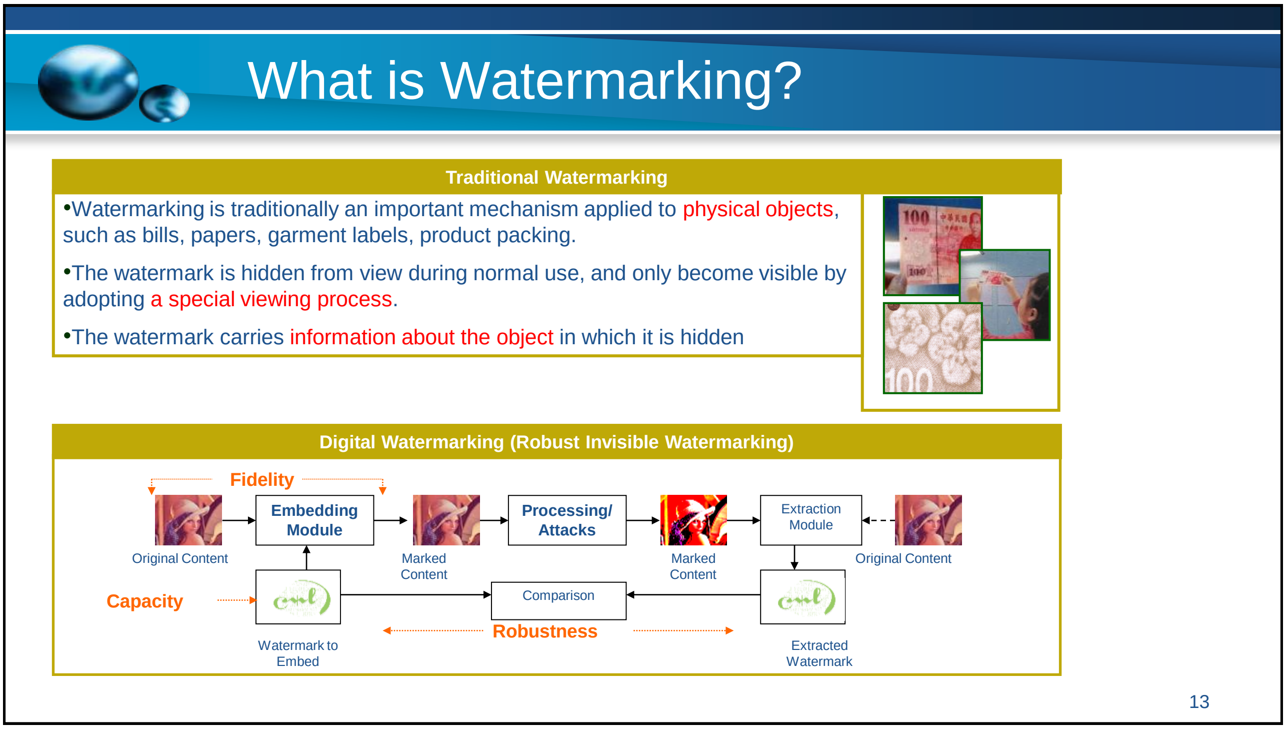
Identities

(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

11

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

Original Content

Embedding Module

Marked Content

Processing/ Attacks

Marked Content

Extraction Module

Original Content

Capacity

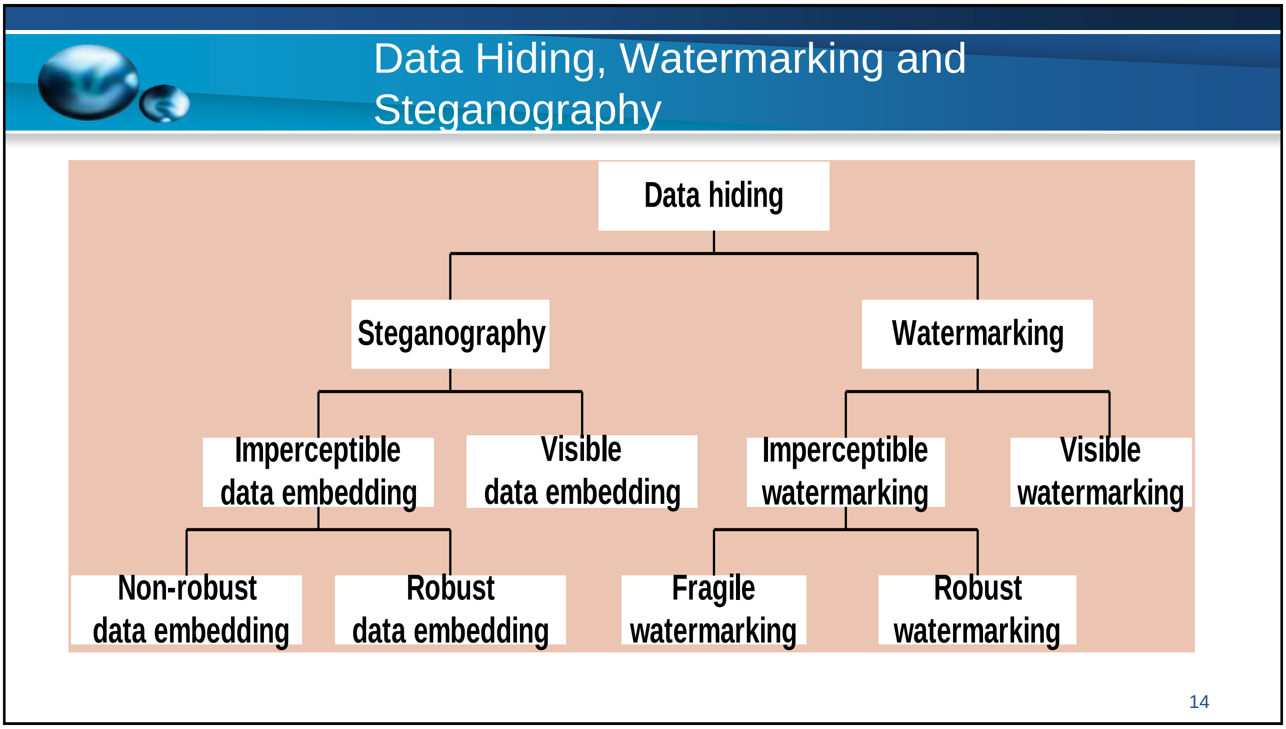
Watermark to Embed

Comparison

Robustness

Extracted Watermark

13



Data Hiding, Watermarking and Steganography

Data hiding

Steganography

Watermarking

Imperceptible data embedding

Visible data embedding

Imperceptible watermarking

Visible watermarking

Non-robust data embedding

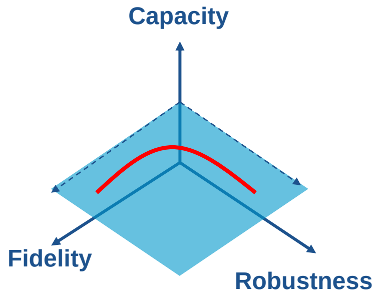
Robust data embedding

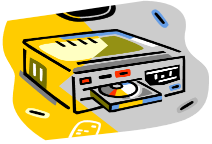
Fragile watermarking

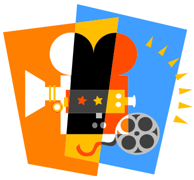
Robust watermarking

14

Desired Properties of Watermarking



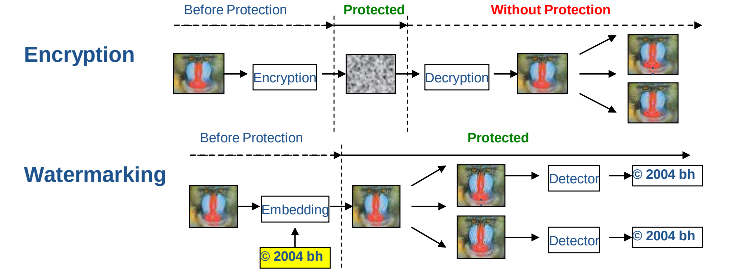




- **High fidelity**
  - Finding adequate perceptual quality index is still an open problem
  - Objective distortion measures are often adopted
- **Strong robustness**
  - Robustness is difficult to define
  - Benchmarks testing various attacks exist
- **Large capacity**
  - Required payload length depends 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



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

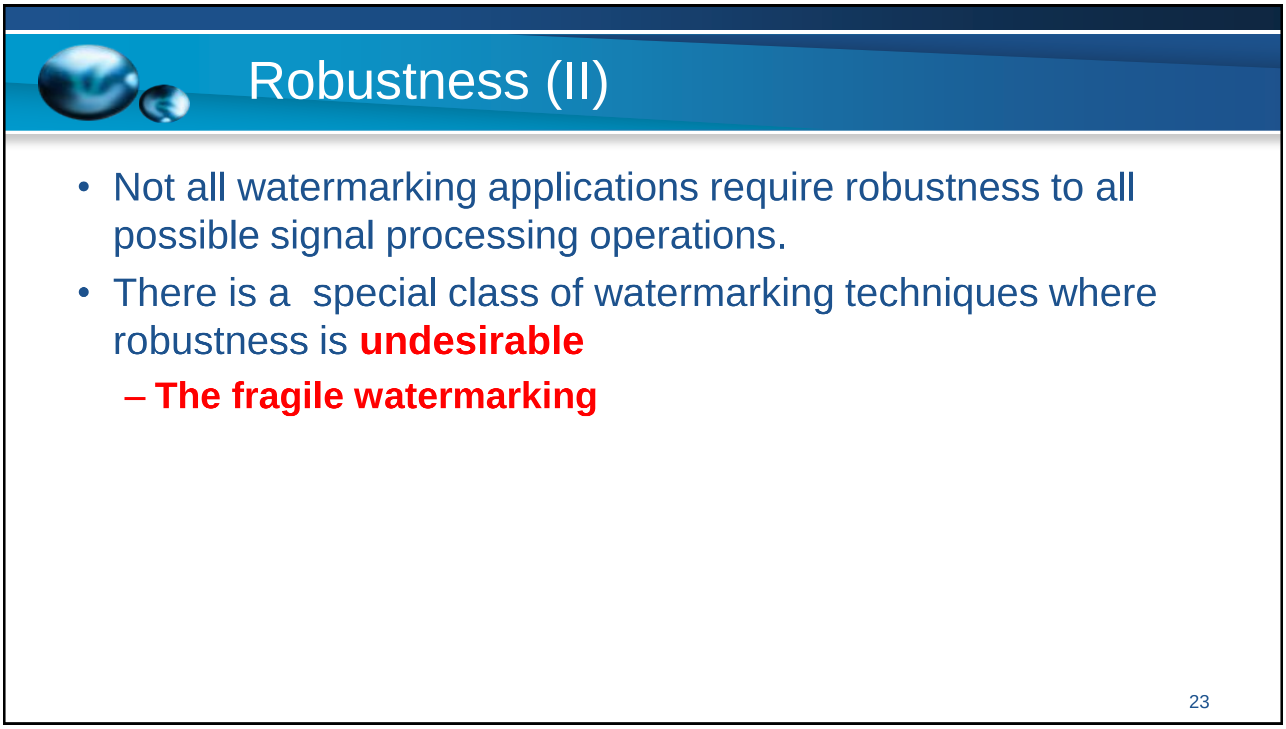
Fidelity Measures

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

Examples of Geometric Distortion



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(العدائية)
  - Unauthorized **removal** من خلال
    1. Eliminating attacks
    2. Masking attacks
    3. Collusion attacks
  - Unauthorized **embedding**
    1. Embed forgery watermarks into works that should not contain watermarks
    2. E.g. Fragile(هشة) 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**

Intellectual Properties

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

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?