

Multimedia Information Systems

Samson Cheung

EE 639, Fall 2004

Lecture 23: Digital Watermarking I

Compiled from lecture notes by Prof. Ja-Ling Wu of National Taiwan University and Prof. Nasir Memon of Polytechnic University, Boston

Outline

- **What is watermarking?**
- **Watermarking vs. Steganography vs. Cryptography**
- **Application of watermarking**
 - **Focus on content authentication**
- **Properties of watermarking schemes**

What is a watermark?

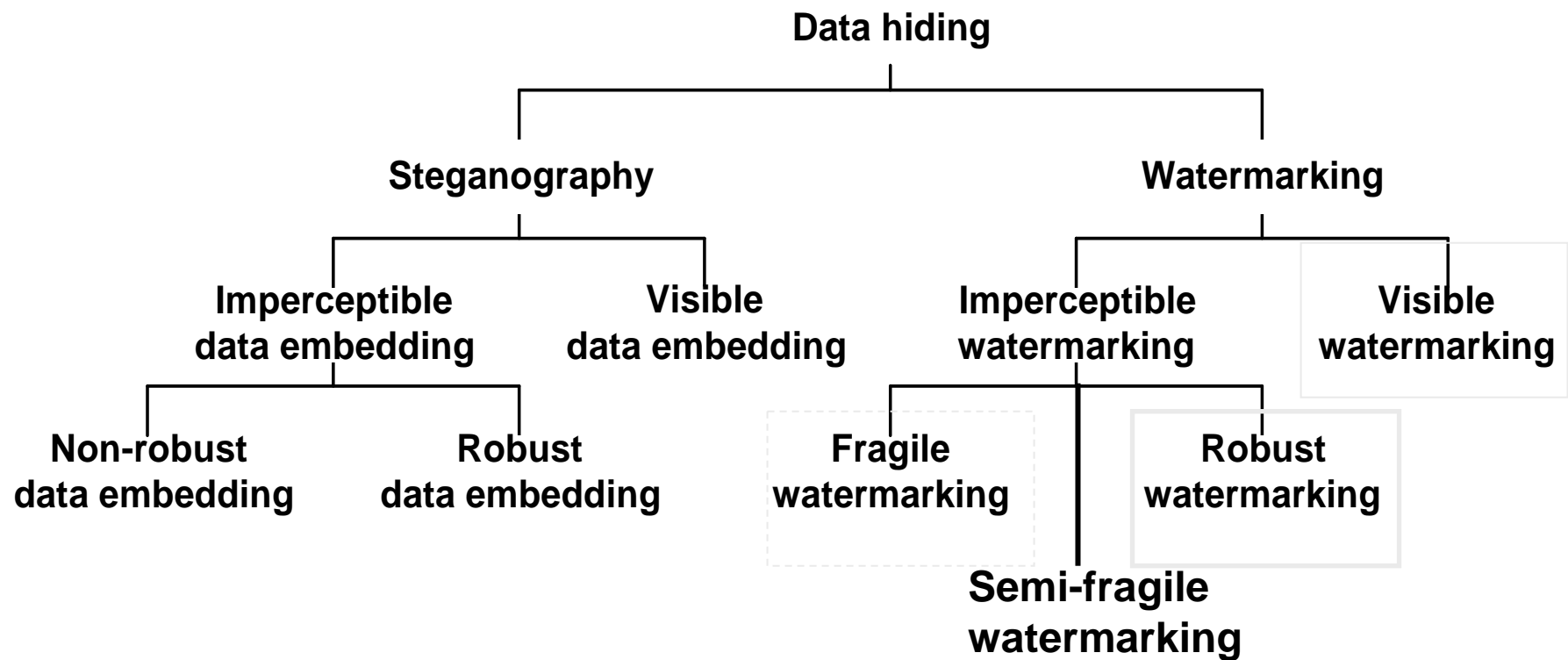
- Watermarking is an important mechanism applied to physical objects like bills, papers, garment labels, product packing...
- Physical objects can be watermarked using special dyes and inks or during paper manufacturing.



Characteristics of watermarks

- The watermark is hidden from view during normal use, only become visible by adopting a special viewing process.
 - E.g. hold the bill up to light
- The watermark carries information about the object in which it is hidden.
 - E.g. the authenticity of the bill
 - E.g. the trademark of the paper manufacturer

IPR related information technologies



Information hiding

- **Data hiding**
 - **Containing a large range of problem beyond that of embedding message in content**
 - Making the information imperceptible
 - E.g. watermarking
 - Keeping the existence of information secret
 - E.g. anonymous usage of network
 - E.g. hiding portions of database for non-privileged users

Steganography

- A term derived from the Greek words “steganos” and “graphia” (The two words mean “covered” and “writing”, respectively)
 - The art of concealed communication.
 - The very existence of a message is kept secret.
 - E.g. a story from Herodotus
 - Military Messages tattooed on the scalp of a slave

Watermarking v.s. Steganography

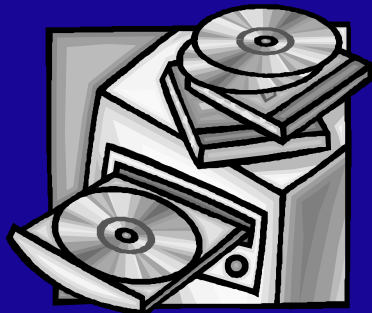
- **Watermark messages contain information related the cover work**
- **In steganographic systems, the very existence of the message is kept secret.**
 - **If the message tatoood on the slave is “the slave belongs to somebody”, then we can regard it as an example of watermarking**

Classification of information hiding systems

	<i>Cover Work Dependent Message</i>	<i>Cover Work Independent Message</i>
Existence Hidden	Steganographic Watermarking	Covert Communication
Existence Known	Non-Steganographic Watermarking	Overt Embedded Communication

Importance of digital watermarking

- The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content
- copyright-protected digital contents are easily recorded and distributed due to:



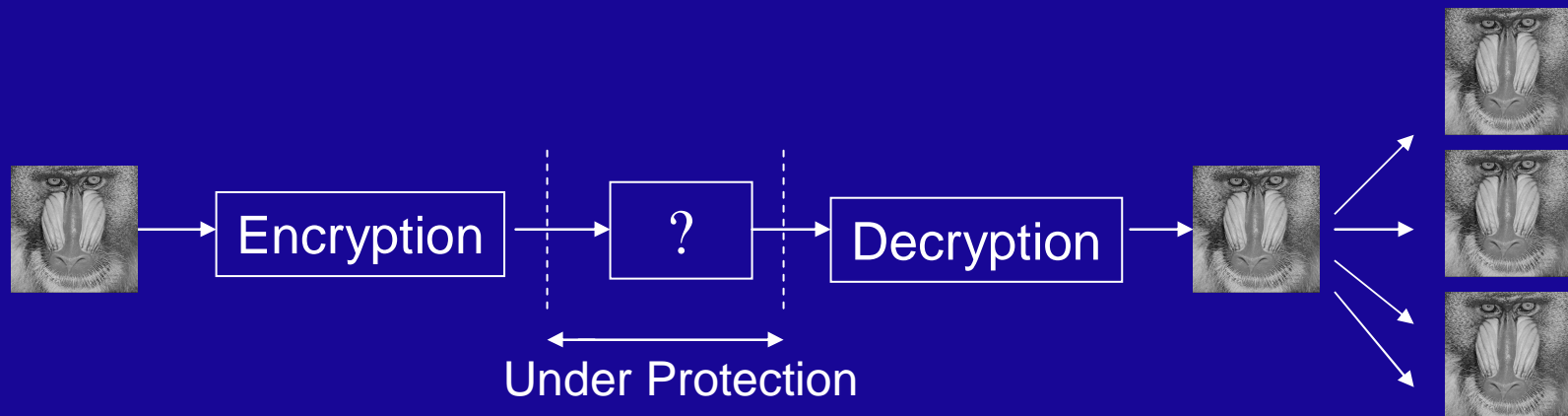
prevalence of high-capacity digital recording devices



the explosive growth in using Internet

Watermarking v.s. cryptography

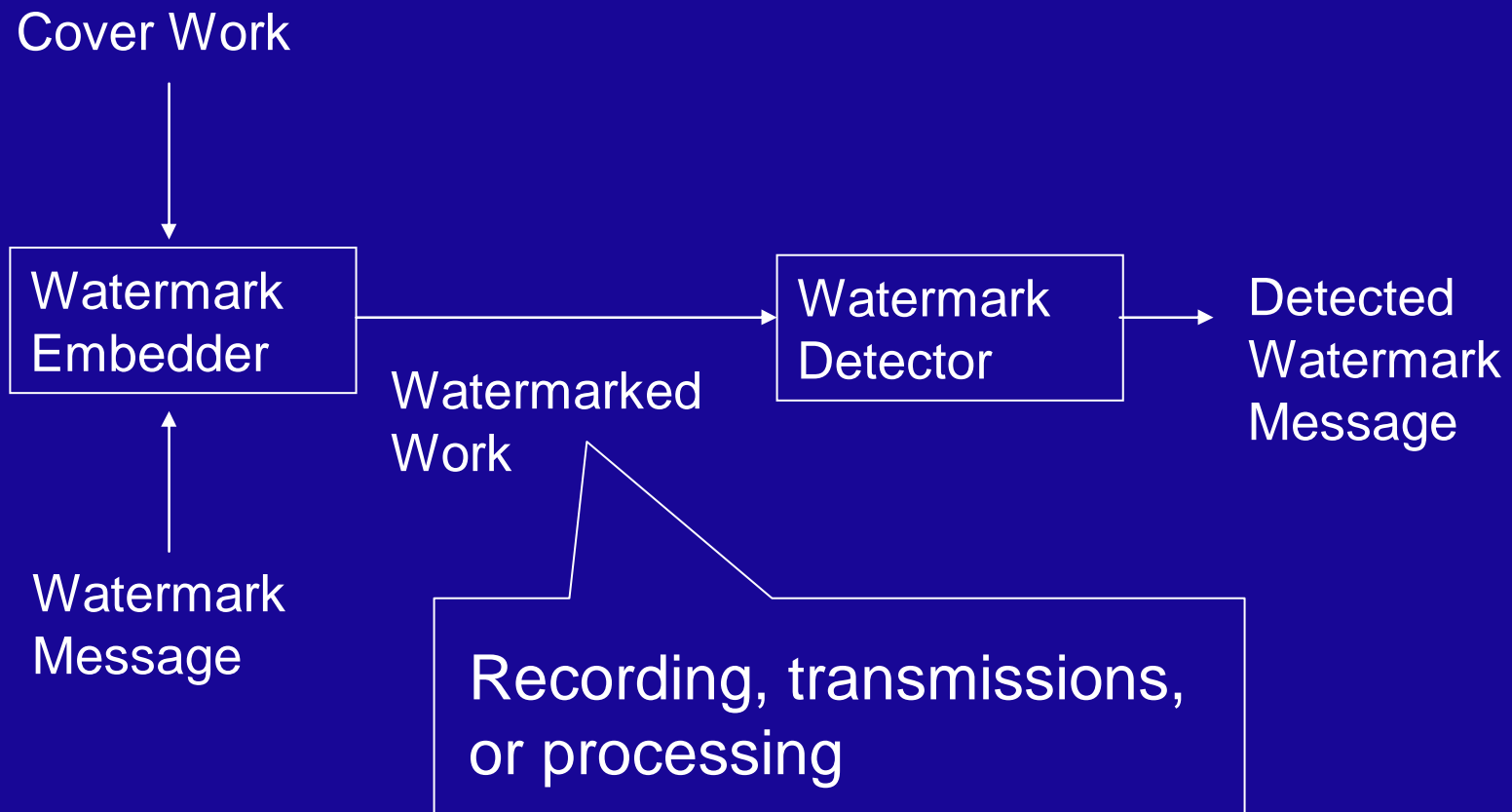
- Cryptography is the most common method of protecting digital content and is one of the best developed science.
- However, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption.
- Digital watermarking can protect content even after it is decrypted.



Definitions about digital watermarking

- **Digital watermarking:**
 - The practice of imperceptually alternating a Work to embed a message about the Work.
 - **Related terms**
 - Work: a specific copy of some electronic signal, such as a song, a video sequence, or a picture
 - Cover Work: the original un-watermarked work
 - Watermark: the messages being embedded, indicating some information about the work

A digital watermarking system



Applications of digital watermarking

- **Owner identification**
- **Proof of ownership**
- **Broadcast monitoring**
- **Transaction tracking**
- **Copy control**
- **Device control**
- **Focus : Content authentication**
 - **Forensic use of watermarking**

Owner identification (I)

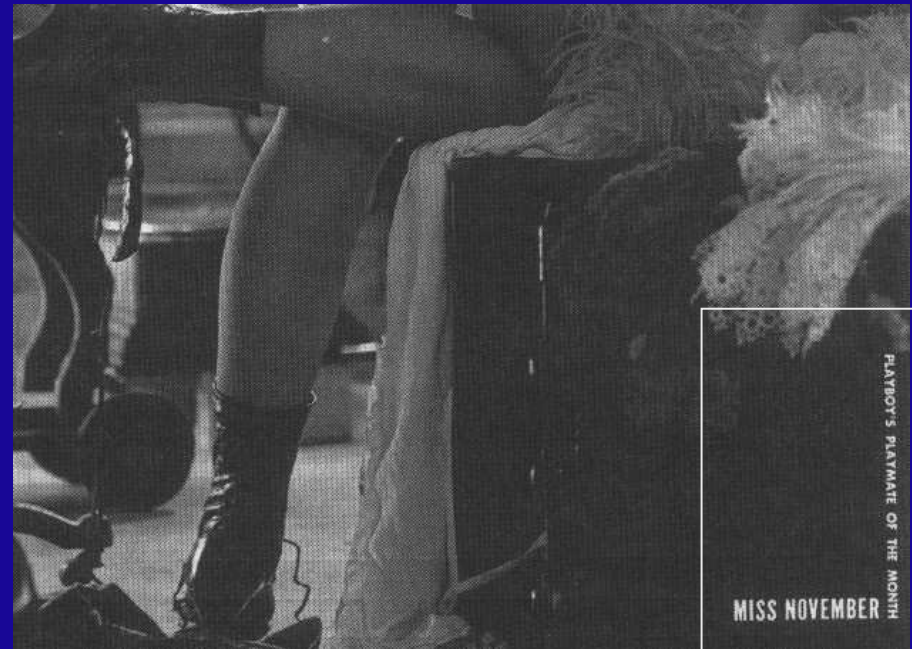
- Under the U.S. law, although the copyright notice is not required in every distributed copy to protect the rights of copyright holders, the award to the copyright holders whose work is misused will be significantly limited without a copyright notice found on the distributed materials.
- Traditional textual copyright notices
 - “Copyright date owner”
 - “© date owner”
 - “Copr. date owner”

Owner identification (II)

- **Disadvantages for textual copyright notices**
 - **Easily removed from a document when it is copied**
 - E.g. the Lena Sjöblom 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 Lena Phenomenon

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



PLAYBOY'S PLAYMATE OF THE MONTH
MISS NOVEMBER

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>
 - \$30 per document
- Watermarking can be of use!

Broadcast monitoring (I)

- 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



Broadcast monitoring (II)

- **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

Broadcast monitoring (III)

- **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

Transaction tracking

- 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!

Copy control (II)

- **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)

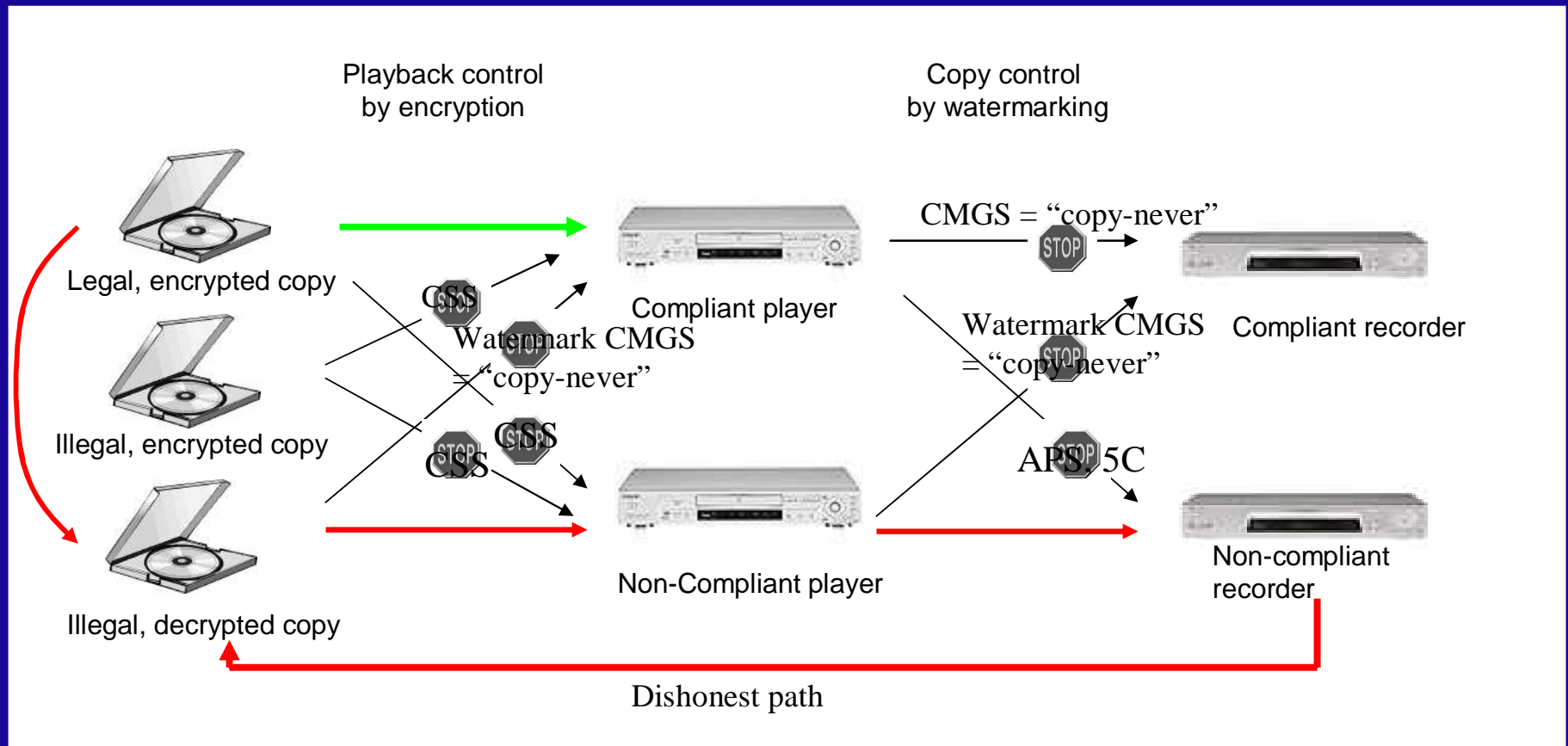
- **Problems of adopting watermarking module in recording devices**
 - Increasing cost
 - Reducing the value of devices
- **Solution**
 - Include the requirement for a watermark detector in the patent license of CSS instead of enforcing by law

DVD Copy detection Systems

Five components (last two not standardized)

1. **Content Scrambling System (CSS)**
 - Scramble the MPEG bit-stream
 - Each compliant player has a player key to decode one of the possible 409 disk keys stored in a DVD, which is then used for descrambling.
 - Disk keys are stored in hidden (lead-in) area of DVD which are not copied.
 - DeCSS exploits unencrypted player keys to impersonate a player.
2. **Analog Protection System (APS)**
 - Feature of compliant DVD players; DVD contains APS bits
 - Automatic Gain Control (AGC) adds bipolar pulse pairs to output signal causing a recording VCR to record a weak, noisy and unstable signal
3. **Copy Generation Management System (CGMS)**
 - Two bits in MPEG header indicating “copy-always”, “copy-never”, or “copy-once”.
4. **5C**
 - allow compliant devices to exchange keys over firewire
5. **Watermarking**
 - for APS and CGMS bits, in case when the content has been decrypted illegally and the header bits erased.

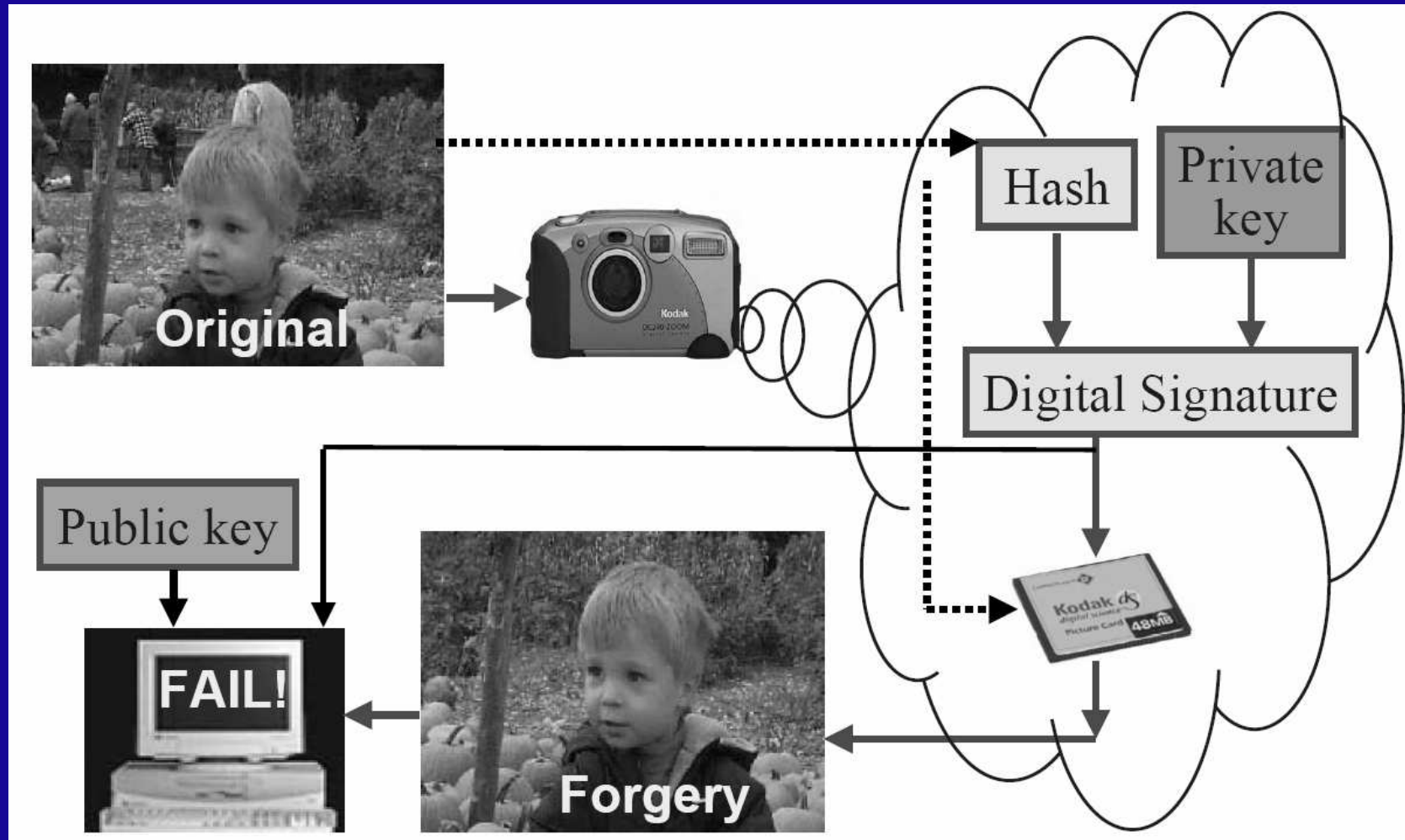
Keep honest people honest



Device control

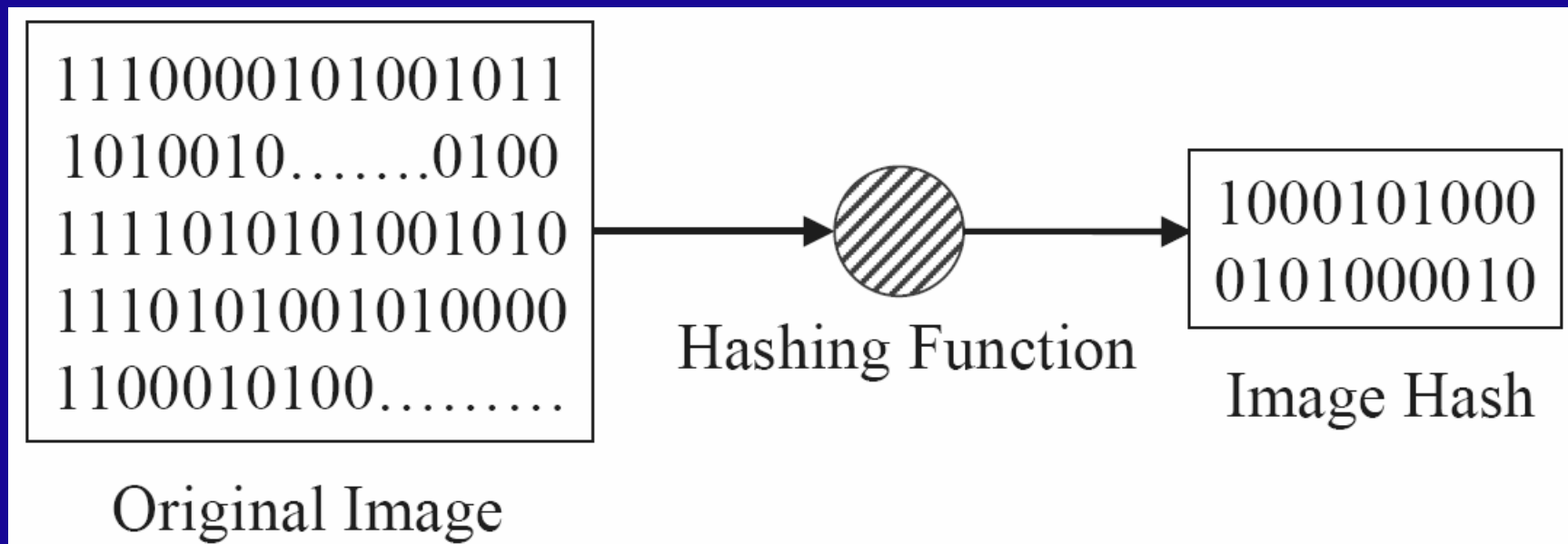
- **Copy control belongs to a broader category - device control**
- **Other applications of device control**
 - **Automatically turning on/off functions related to special contents**
 - E.g Including watermark to skip advertisements
 - **Action toys interactive with the TV program**
 - **Digimarc's MediaBridge**

Content Authentication



Hash function

- **Hash function:** A computation that takes a variable-size input and returns a fixed-size digital string as output, called the **hash value**.

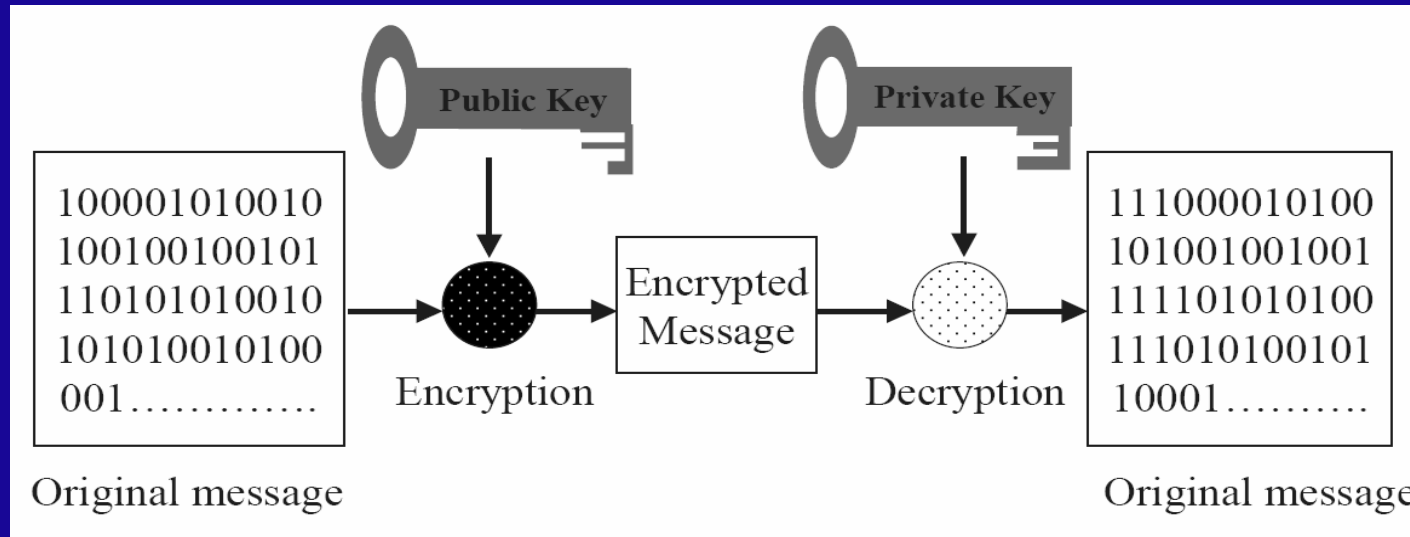


More about hash function

- **One-way hash function:** A hash function that is hard or impossible to invert, also called a **message digest function**.
- The one-way hash value can be thought of as the **digital fingerprint** of an image because:
 - It is extremely unlikely for two different images to hash to the same value: precludes attacker from adding an additional signature to a copy.
 - It is computationally infeasible to find an image that hashes to a given value: precludes an attacker from replacing the original image with an altered image.
- Examples of hash functions used for digital signatures are:
 - 20-byte **secure hash algorithm** (SHA-1) that has been standardized for government applications.
 - 16-byte **MD2**, **MD4**, or **MD5** developed by Rivest.

Public-Key Cryptosystems

- **Public-key cryptography** was invented in 1976 by Diffie and Hellman in order to solve the key management problem.

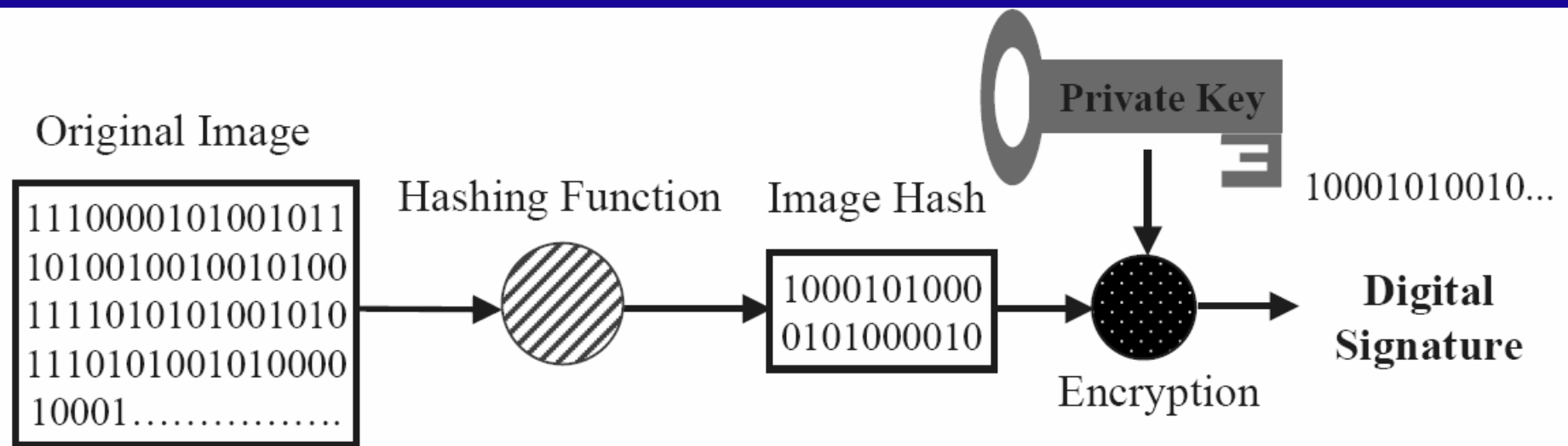


- A **public key**, which is published and can be used to encrypt messages.
- A **private key**, which is kept secret and is used to decrypt messages.
- The most popular public-key encryption in use today is the **RSA** (Rivest-Shamir-Adleman) system.

Public-Key Cryptosystems for Authentication

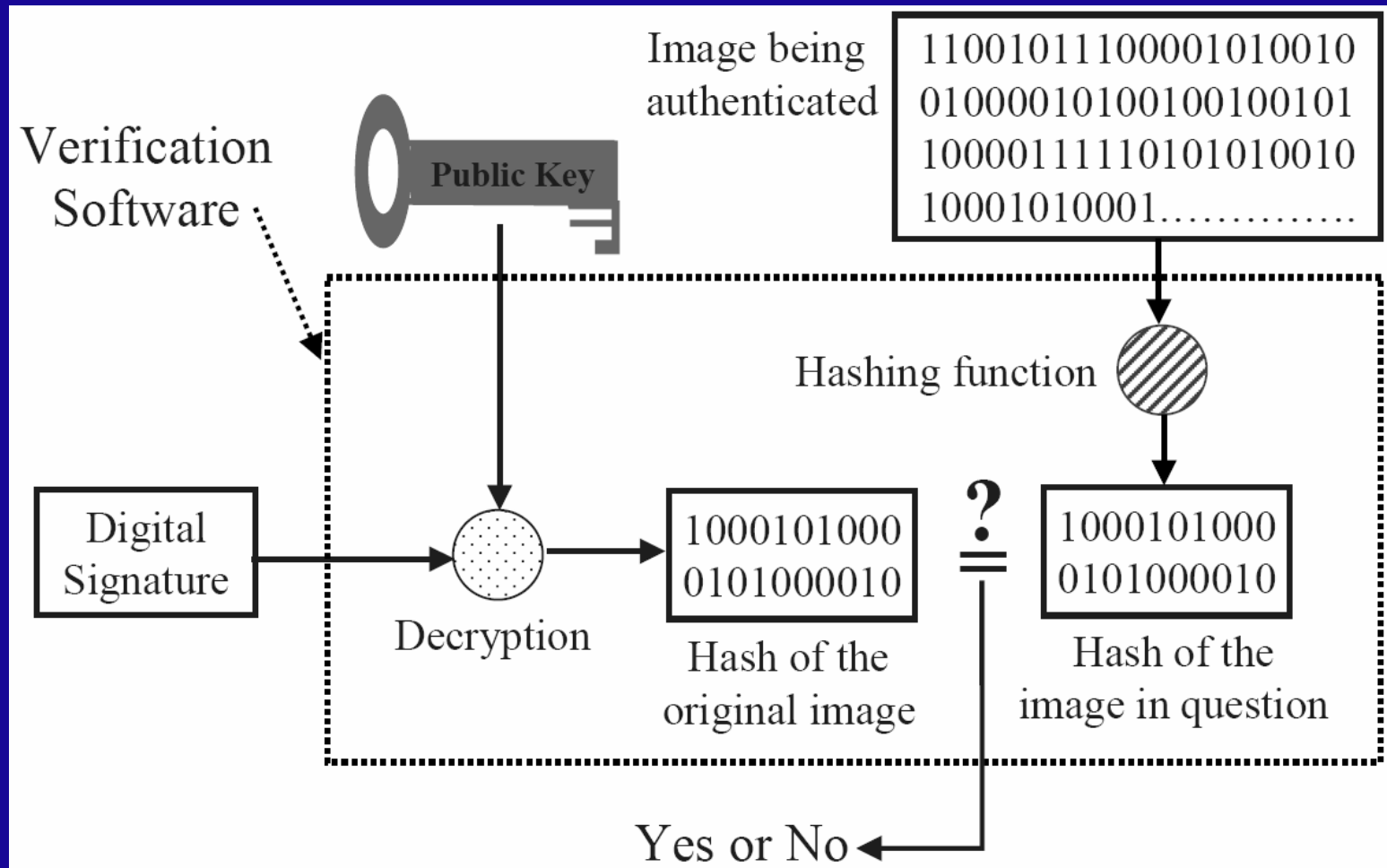
- Certain public-key cryptographic systems in which the roles of the public and private keys in encryption and decryption can be reversed, can also be used for authentication:
 - Prior to sending a message, the sender encrypts the message with his/her private key.
 - The message can be decrypted by the public using the public key of the signatory (no secrecy involved).
 - Since it is computationally infeasible to find the private key from the public key and the known message, the decryption of the message into meaningful text constitutes its authentication.

Digital Signature Generation



- A **digital signature** is created in two steps:
 - A fingerprint of the image is created by using a one-way hash function;
 - The hash value is encrypted with the private key of a publickey cryptosystem. Forging this signature without knowing the private key is computationally infeasible.

Digital Signature Verification



Properties of digital 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 $1/10^{12}$**

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

Problems to determine the fidelity

- **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**

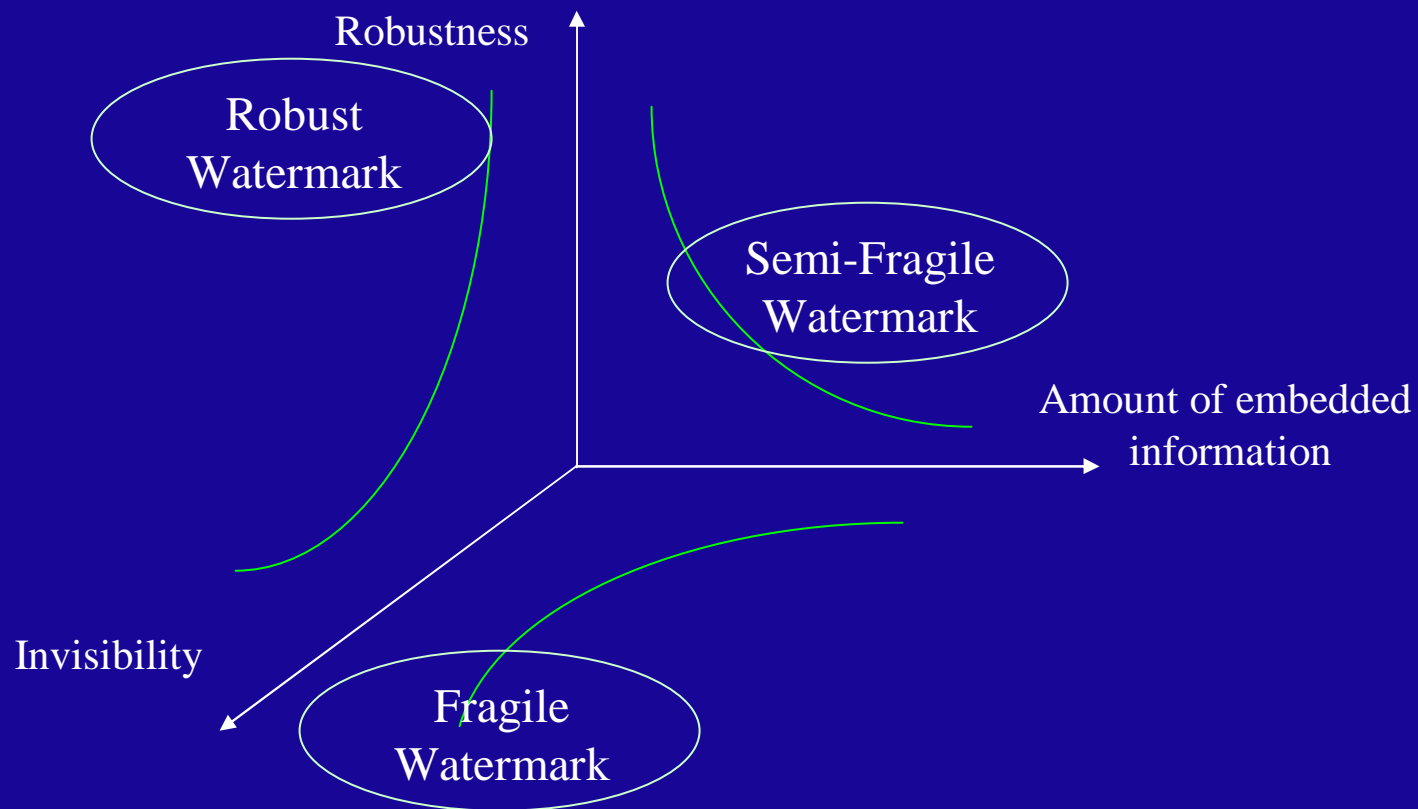
Robustness (I)

- **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**
 - **Fragile watermarking**
 - Watermark is destroyed by any signal processing operation
 - **Semi-fragile watermarking**
 - Watermark survives common signal processing operations but destroyed by large-scale alternation.

Three types of 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**
 - Unauthorized reading

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

Cost

- **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)

Watermarking techniques in current standards

- **The CPTWG (Copy Protection Technical Working Group) tested watermarking systems for protection of video on DVD disks.**
- **The SDMI (Secure Digital Music Initiative) made watermarking a core component in their system for music protection.**
- **Two projects sponsored by the European Union, VIVA and Talisman, tested watermarking for broadcast monitoring.**
- **The ISO (International Organization for Standardization) took an interest in the context of designing advanced MPEG standards. (MPEG-21)**

Companies with watermarking products

- **Digimarc bundled its watermarking system with Adobe's Photoshop**
- **Technology from the Verance Corporation was adopted into the first phase of SDMI and used by some Internet music distributors**