디지털 워터마킹 기술의 이해

2002. 4. 9.

호 요 성

광주과학기술원

Contents

- Introduction
- Watermarking 요구사항
- Watermarking Algorithms
- Watermarking 응용
- MPEG-4 IPMP
- OPIMA
- Conclusions

Estimated Trade Losses

(Millions of US$)

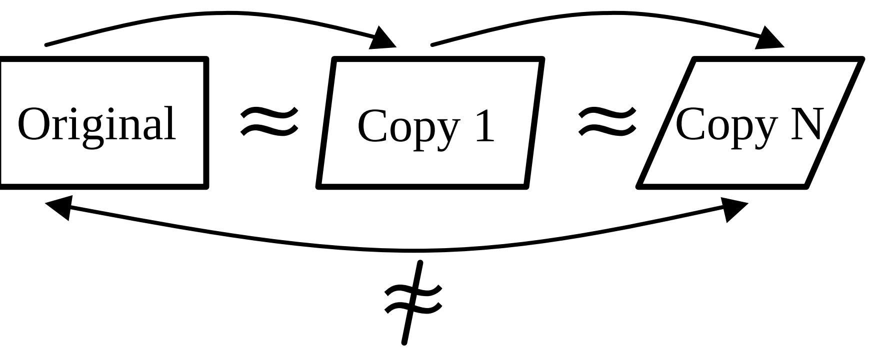
	Motion Picture		Record & Music	
	Loss	Level	Loss	Level
China	120	90%	70	90%
Brazil	120	35%	300	95%
Italy	160	25%	60	25%
Russia	250	90%	200	70%

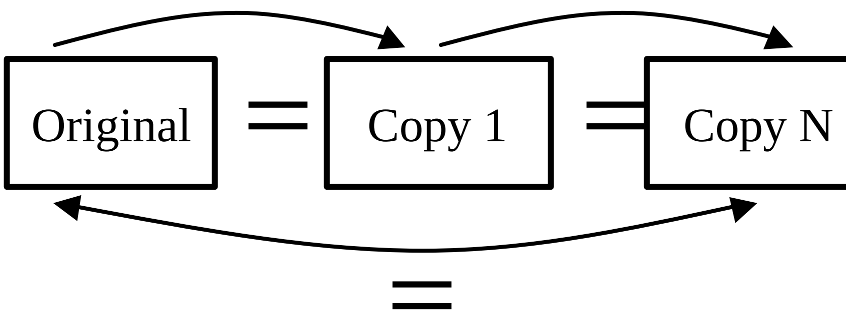
1999 – www.iipa.com

- Total Estimated Loss
  - Motion picture: US$ 1323M
  - Record & music: US$ 1684M

Analog & Digital Multimedia

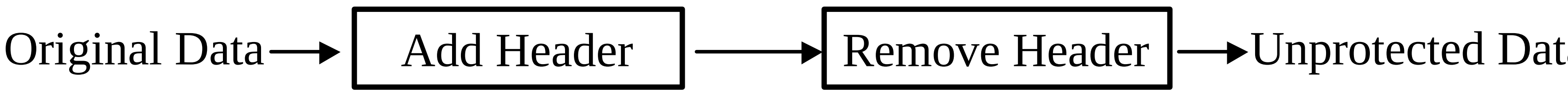
- Analog Media
  – Photocopies, audio cassettes, VHS, *etc*
  – **복사하기 어려움**
- Digital Media
  – PDF, CDs, MP3, MPEG, JPEG, *etc*
  – **복사하기 쉬움**
  – "Free" distribution network: Internet



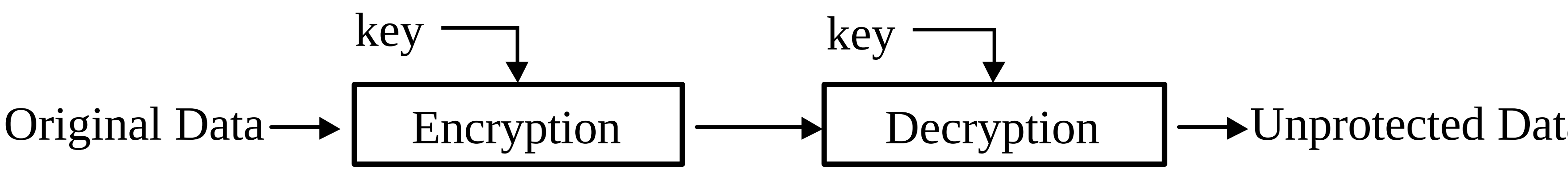


Data Protecting Methods

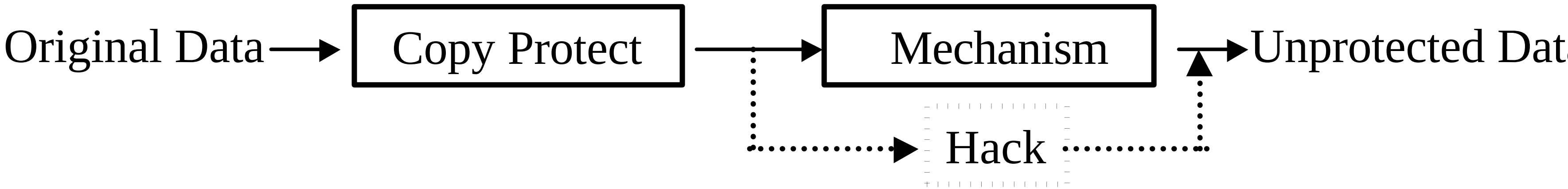
- Access-Control Header: easily removed



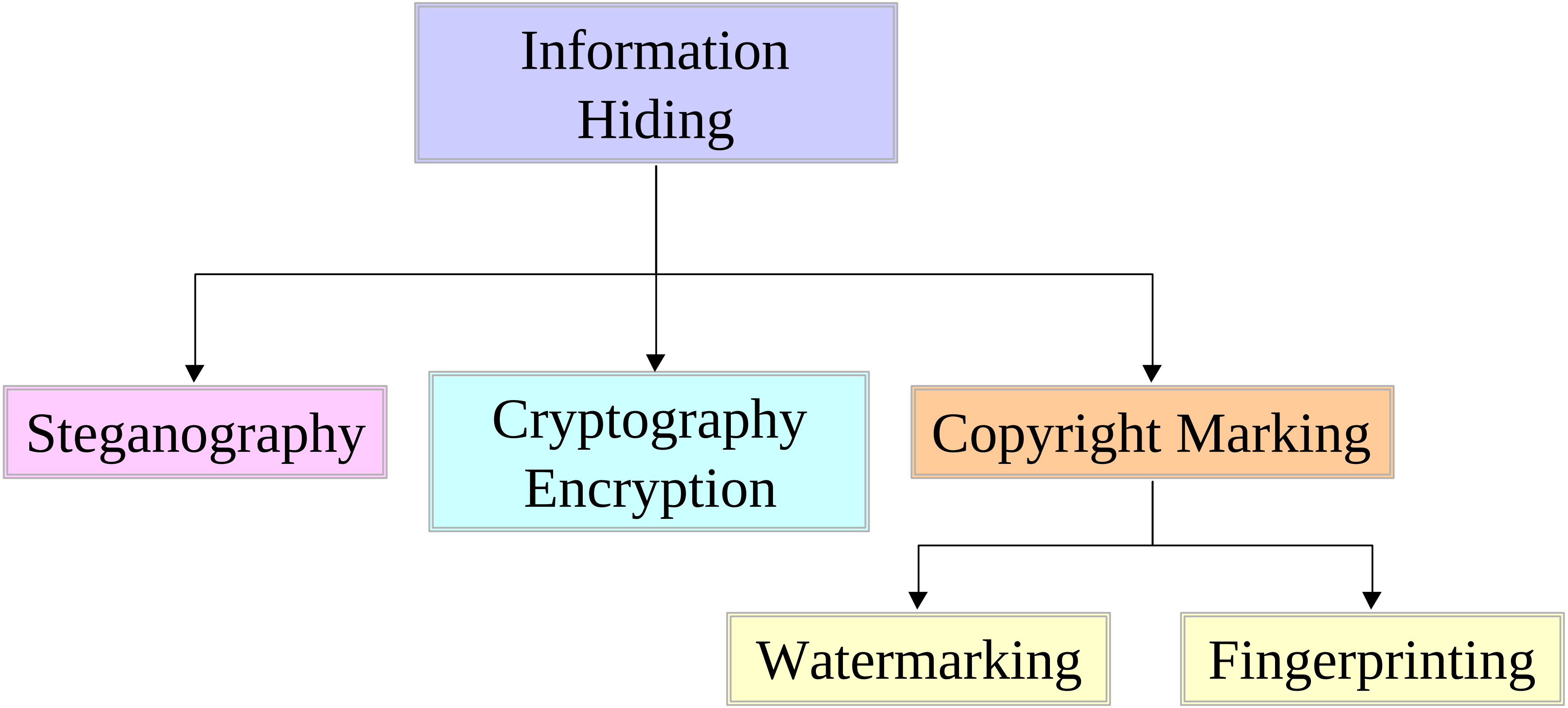
- Encryption: decrypted data → hard to protect



- Copy Protection: sensitive to hacking



Information Hiding



Digital Watermarking

- Watermark = Water (Invisible) + Mark
- Media Copyright Protection
  - **전자 상거래의 발전**
  - **소유권을 보호할 수 있는 마지막 방법**
- Two Different Viewpoints
  - Watermark-as-signal
    - **일반 사용자는 삽입된 신호를 잡음으로 생각**
  - Watermark-as-information
    - **정보 소유자는 삽입된 신호를 정보로 생각**

Why Watermarking?

- Secure Distribution of Digital Contents
  - Unlimited copies of original contents
  - Instant distribution over internet
  - Quick download of compressed streams
- Content Protection
  - Authentication (인증)
  - Encryption/Decryption (암호화)
  - Watermarking (워터마킹)

Why Important?

- Scenario
  - Owner places digital media on a network and wants to detect illegal usage
- Goals
  - Verify the owner of the digital media
  - Detect forgeries of the original media
  - Identify illegal copies of the original media
  - Prevent unauthorized distribution

Watermarking Techniques

- Spatial Watermarking Approach
  - Simple and easy to embed and detect watermarks
  - Weak to general attacks
- Spread Spectrum Approach
  - Combined with FFT/DCT/WT
  - Relatively complex
  - Robust to spatial processing and compression
  - Weak to geometric attacks

Requirements

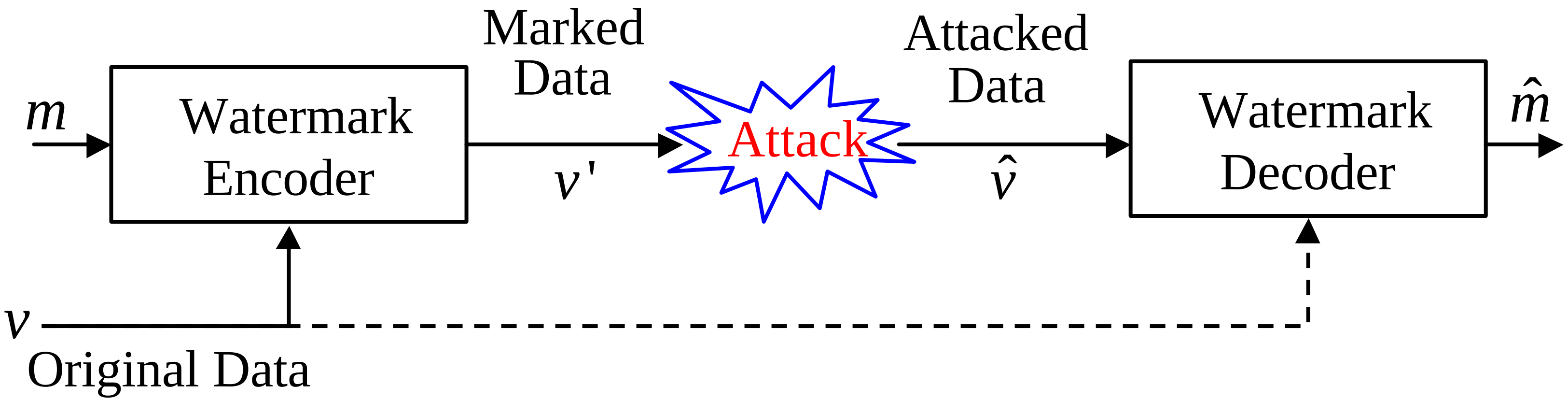
- Imperceptibility
  - Watermarked data ≅ Original data
  - Human perception models
- Robustness
  - Robust to malicious attacks
  - JPEG, resizing, cropping, filtering, *etc*
- Security
  - Kerckhoff's rule: security depends not on the algorithm, but on the secrete KEY

Trade-Off

- Imperceptible to Human Perception
  - Psycho-acoustic model: audibility test
  - Psycho-visual model: visibility test
- Robust to Data Manipulations
  - Maintain or keep the watermark signal
  - Increase watermark strength
  - Resistant to data changes
  - Filtering, cropping, compression, ...

What is attack ?

- Attack: any process that may impair the recovery of embedded information



- Robustness
  - Increase watermark strength
  - Artifact in marked data
  - Trade-off

Examples of Image Attacks

- Format Conversion
  - 4:3 → 16:9, frame rate
- Lossy Compression
  - JPEG, MPEG, MP3
- Filtering, Noise
- D/A or A/D Conversion
- Geometric Transform
  - Rotation, scaling
  - Cropping, composition
  - Zooming
- Jitter
  - Interchange of samples
- Histogram Equalization
- Time/Space Scaling
- Collusion
  - Use several differently marked data → estimate original
- Deadlock
  - Generate fake signal

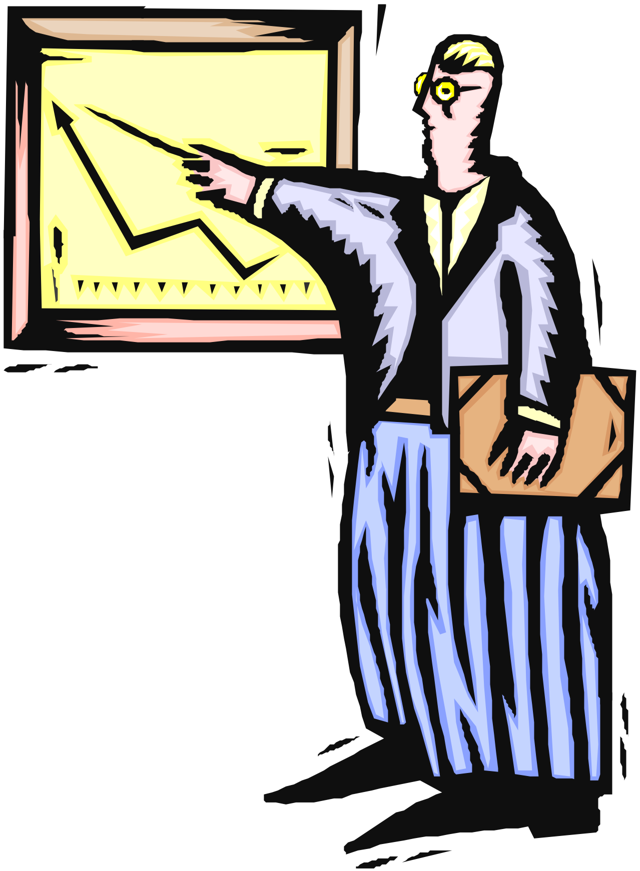
Examples of Audio Attacks

- Linear filtering
- Non-linear filtering
- Time scaling
- Pitch scaling
- Lossy compression (MP3, AAC)
- Data reduction (sub-sampling)
- Transcoding
- D/A, A/D conversion
- Multiple watermarking

Enhancement of Resistance

- Added redundancy
  - Spread spectrum method
  - DFT/DCT/WT domain
- Split in perceptual bands
- Phase spectrum embedding
- Magnitude spectrum embedding

Watermarking Algorithms



- Based on the Media
  - Text Watermarking
  - Image Watermarking
  - Video Watermarking
  - Audio Watermarking
- Based on the Key
  - Private Key
  - Public Key

Basic Components

- Watermark Generation
- Watermark Insertion
  - How to embed the watermark into the original data
- Watermark Retrieval
  - Authentication procedure
  - Determine the integrity, ownership of the marked data

Watermarking 분류 (1)

- Text Watermarking
  - Line-shift coding, word-shift coding, feature coding
- Image Watermarking
  - Watermark design
    - Meaningful watermark, Meaningless watermark
  - Watermark embedding
    - Time-domain embedding, Transform-domain embedding
  - Watermark detection
    - Blind watermarking: without the original data
    - Referenced watermarking: with the original data

Watermarking 분류 (2)

- Video Watermarking
  - Compression domain embedding
  - Uncompression domain embedding
- Audio Watermarking
- Other Media Watermarking
- Based on the Key
  - Private-key watermarking: same keys at the encoder and decoder, symmetric key watermarking
  - Public-key watermarking: asymmetric key watermarking, can read watermark but can't remove → blind watermarking

Text Watermarking

- Word-shift Coding
- Line-shift Coding
- Character Coding

Original text: Now is the time for all men/women to …

Marked text: Now is the time for all men/women to …

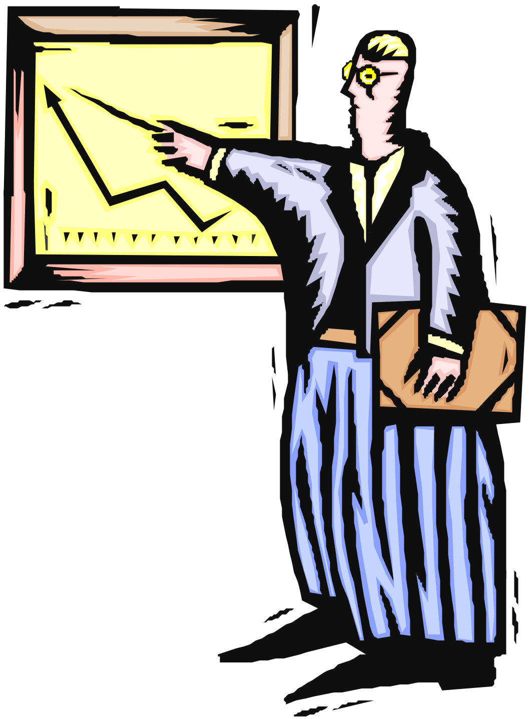
Original text: Now is the time for all men/women to …

Marked text: Now is the time for all men/women to …

Image Watermarking

- Most researches are focused on image
- Watermark Signal
  - Random noise or meaningful binary sequence
- Embedding Methods
  - Spatial-domain insertion: easy to implement, weak to attack
  - Frequency-domain insertion: spread-spectrum concept, robust to attack
- Detecting Methods
  - Blind watermarking or not

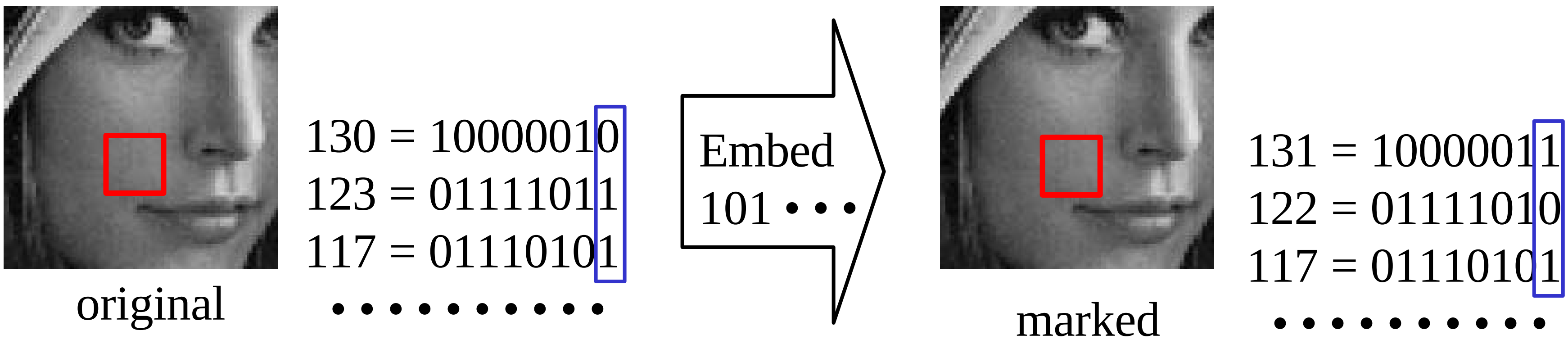
Time-Domain Embedding



- LSB Modulation
- Patchwork
- Sequence Spreading

Least Significant Bit Modulation

- Time Domain Embedding

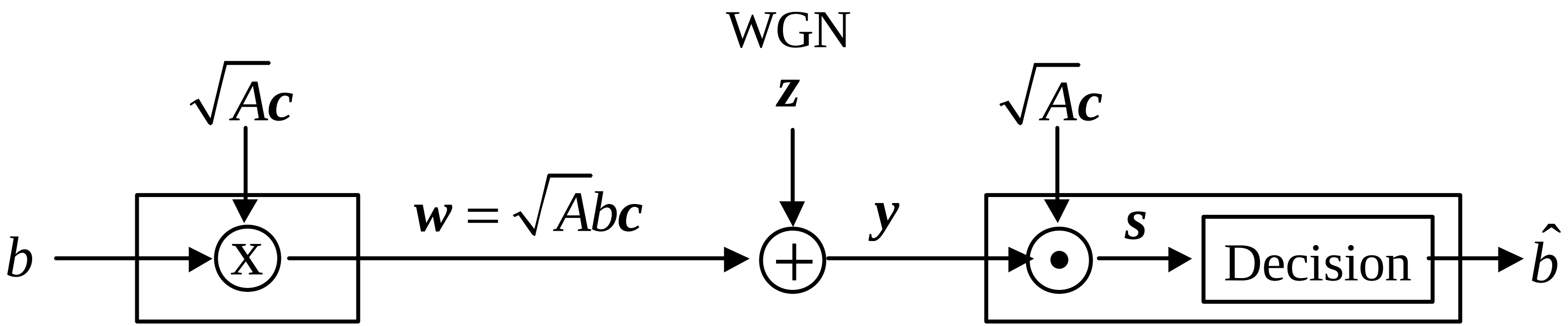


- Imperceptible: modify only LSBs
- Secure
- Not Robust: random change of LSBs

Patchwork Algorithm

- Randomly Selected Two Disjoint Sets
  - Each has n pixels
  - Assumption: $S = \sum_{i=1}^{n} (A_i - B_i) \approx 0$
- Embedding: $A'_i = A_i + 1$ and $B'_i = B_i - 1$
- Detection: $S' = \sum_{i=1}^{n} (A'_i - B'_i) \approx 2n$
  - Watermark is present, if $S' \approx 2n$
- Information via Many Bits → Spread-Spectrum

Sequence Spreading



- Message Bit $b \in \{-1,1\}$
- Signals $\boldsymbol{c},\boldsymbol{w},\boldsymbol{y},\boldsymbol{z}$ of N Samples (N: chip rate) ➔ message is spread
- Spread Sequence with Random Unit Vector $\boldsymbol{c}$, $\|\boldsymbol{c}\|=1$
- Decoder
  – Compute correlation:

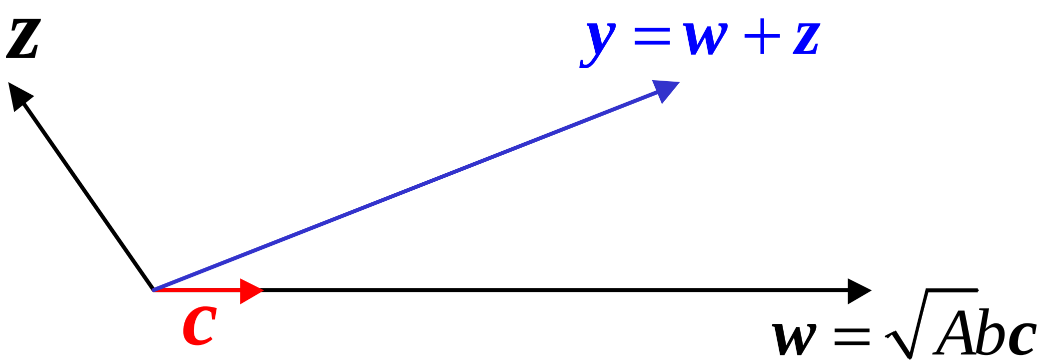
$$s = \boldsymbol{y} \cdot \sqrt{A}\boldsymbol{c} = (\sqrt{A}b\boldsymbol{c}+\boldsymbol{z}) \cdot \sqrt{A}\boldsymbol{c} = Ab + \sqrt{A}\boldsymbol{z} \cdot \boldsymbol{c} \approx Ab$$

  – Maximum-likelihood decision rule

$$\hat{b} = \begin{cases} +1, & s > 0 \\ -1, & s < 0 \end{cases}$$

Vector Space Interpretation

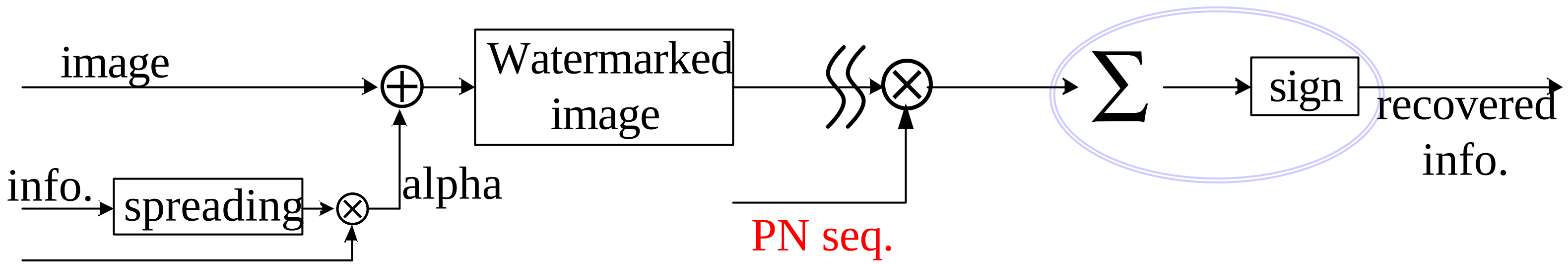
- Treat Signals as Vectors in R^N Space
- Spreading Sequence $\boldsymbol{c}$
  - Points to a specific direction
  - Watermark $\boldsymbol{w}$ along the direction $\boldsymbol{c}$
- Noise $\boldsymbol{z}$
  - Vector of any direction



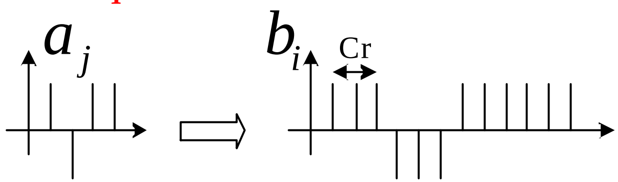
Spreading Sequence의 장점

- Security
  - Generate ***c*** with random number generator
  - Keep seed secrete
- Imperceptibility
  - Random, noise-like ***c***
  - No peak in frequency
  - ***w*** acts like low-noise power
- Robustness
  - Attacker does not know ***c***
  - Spread noise in all directions

Spreading Sequence Algorithm



matched filter:
original image is not needed



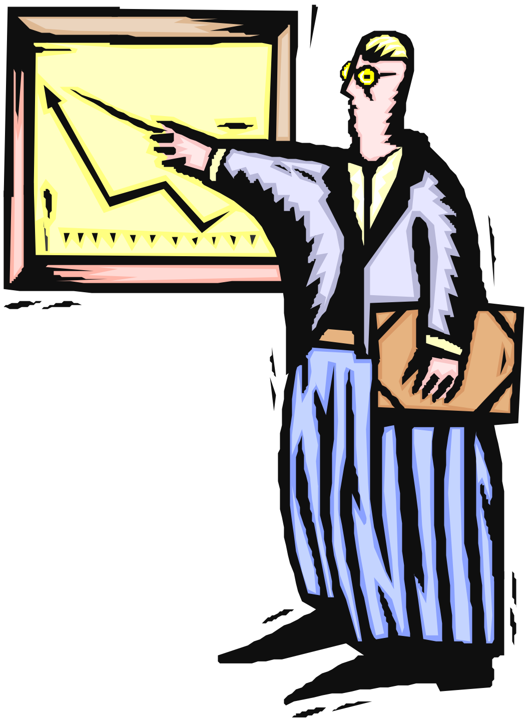
$$a_j \in \{-1,1\}, \quad j \in N \quad a_j : message\ \ bits$$

$$b_i = a_j, \quad j \cdot c_r \le i < (j+1) \cdot c_r, \quad i \in N \quad b_i : spread\ seq.$$

$$w_i = a_i \cdot b_i \cdot p_i, i \in N \qquad w_i : watermark \qquad p_i : PN\ seq.$$

$$\tilde{v}_i = v_i + w_i, \qquad i \in N$$

Transform-Domain Embedding

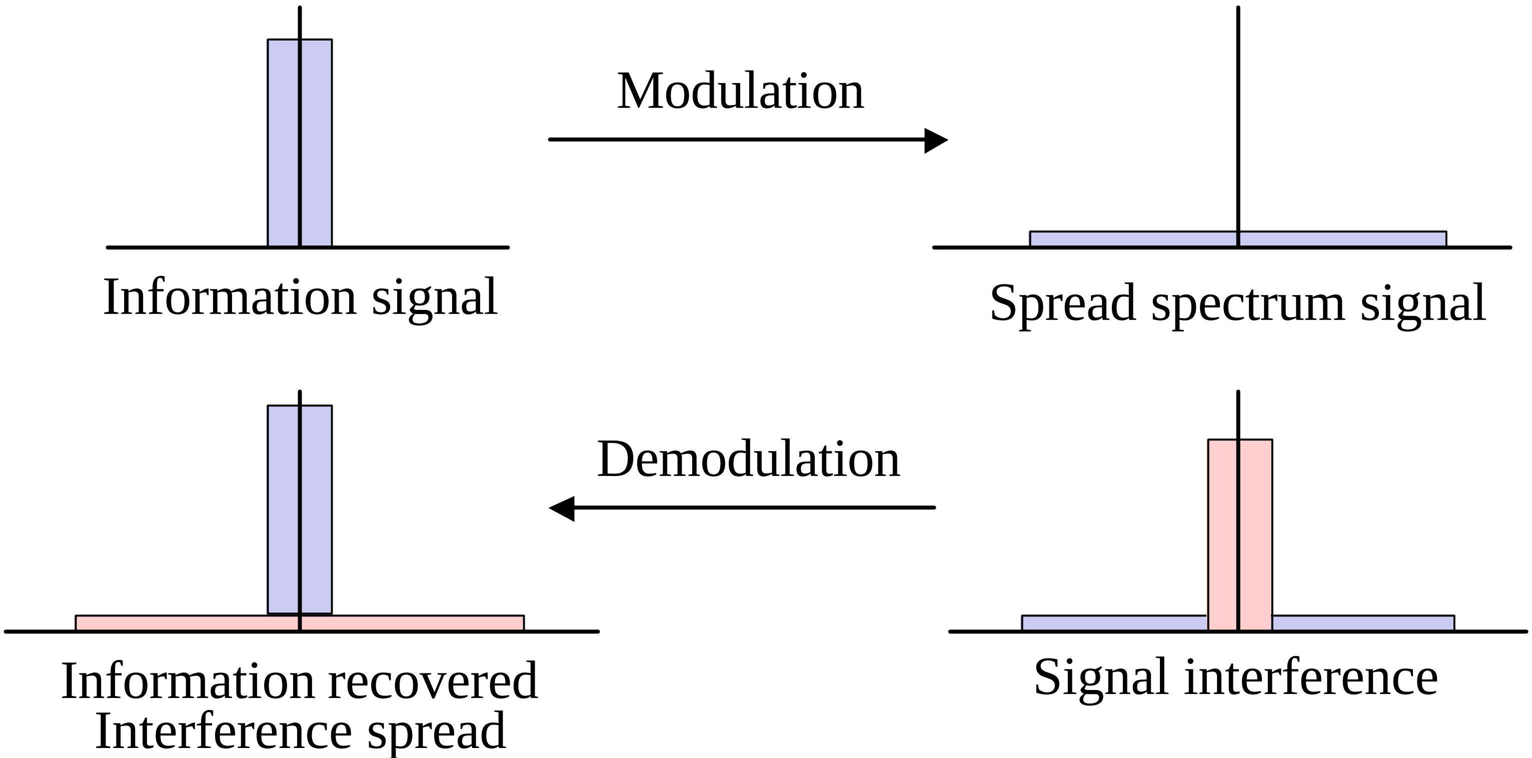


- Processing Gain
- Popular Algorithms
- Results

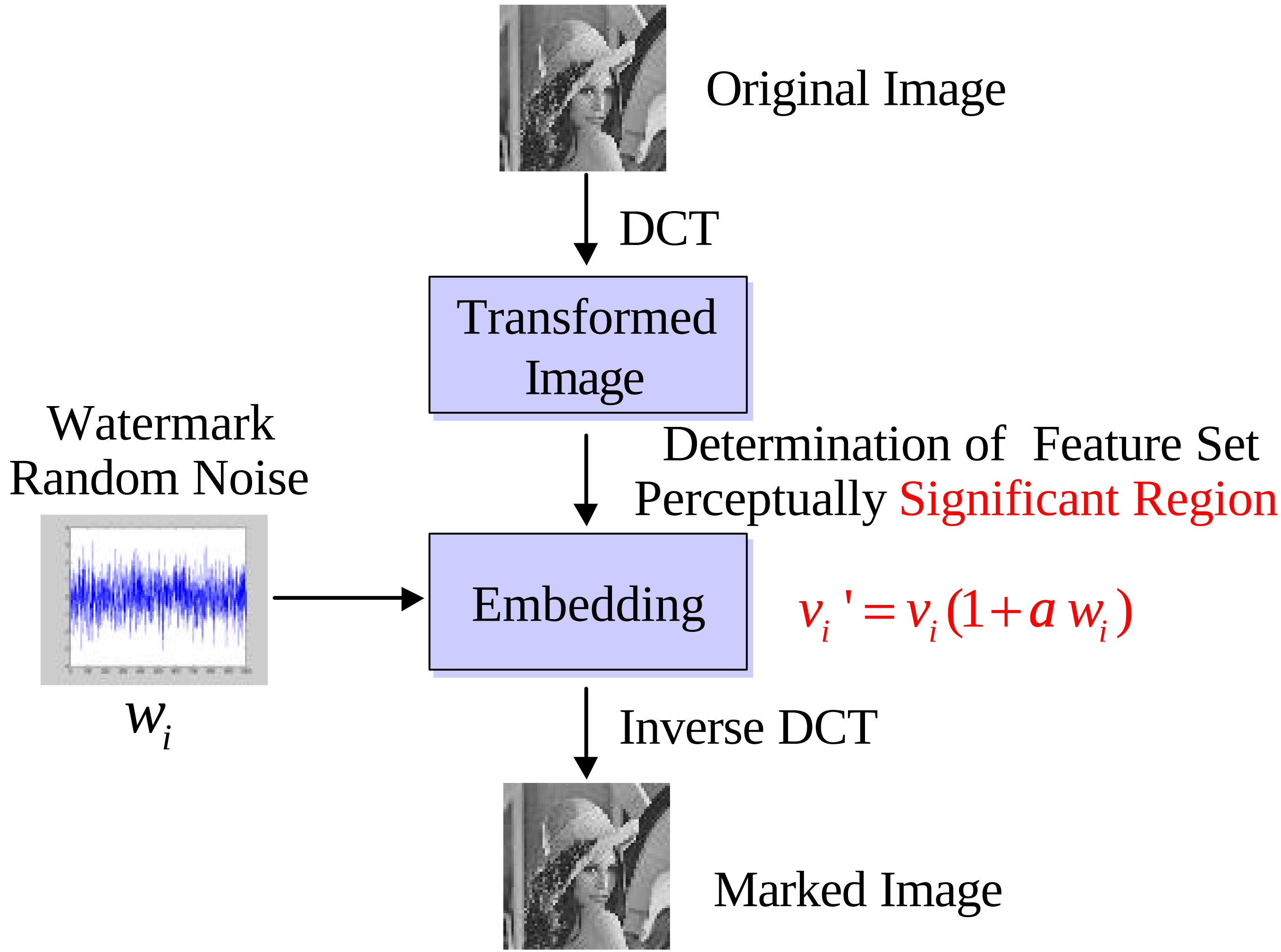
Processing Gain

- Spreading of the BW increases SNR

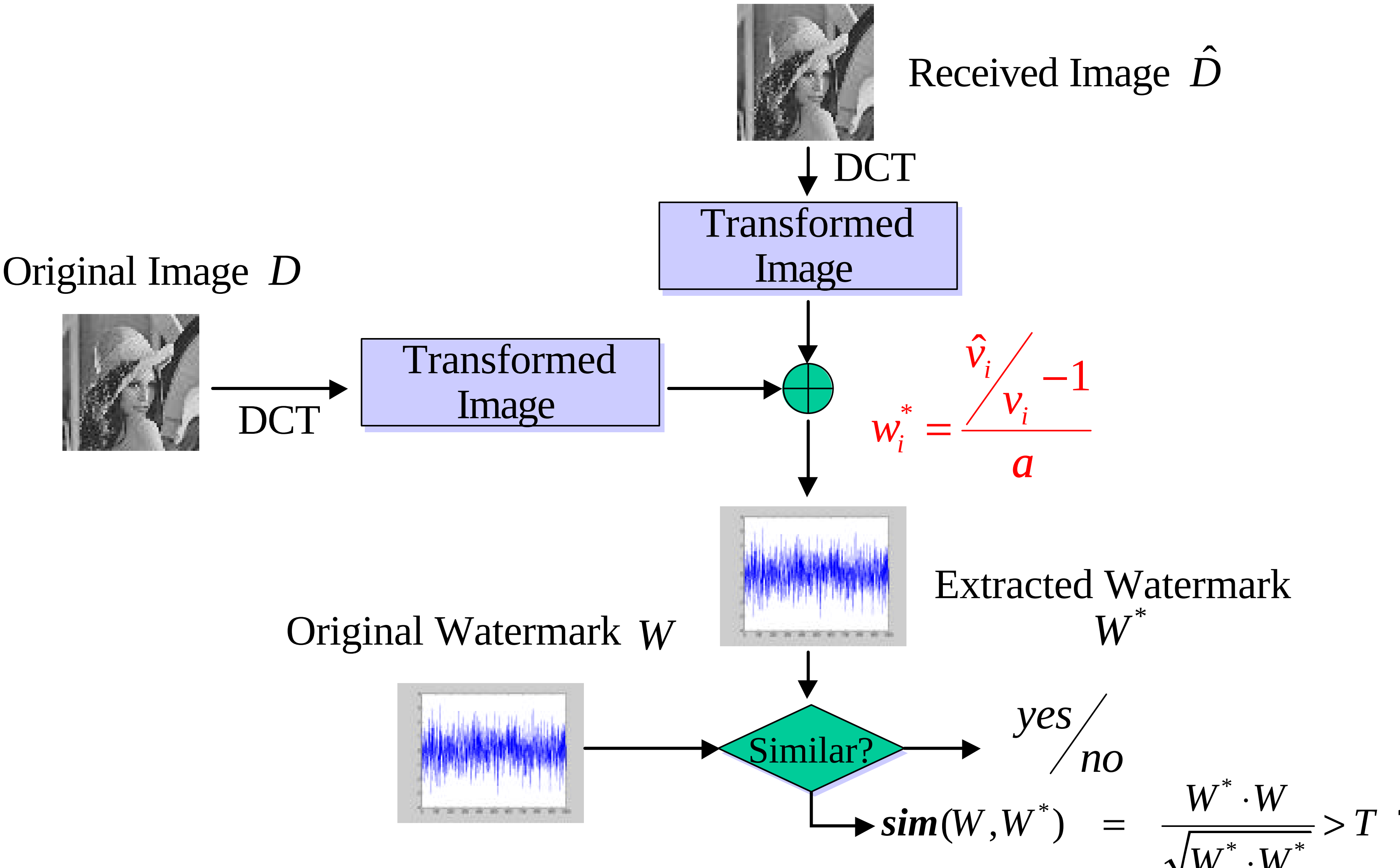
$$\text{Processing Gain} = G_p = \frac{\text{Spread Bandwidth}}{\text{Information Bandwidth}}$$



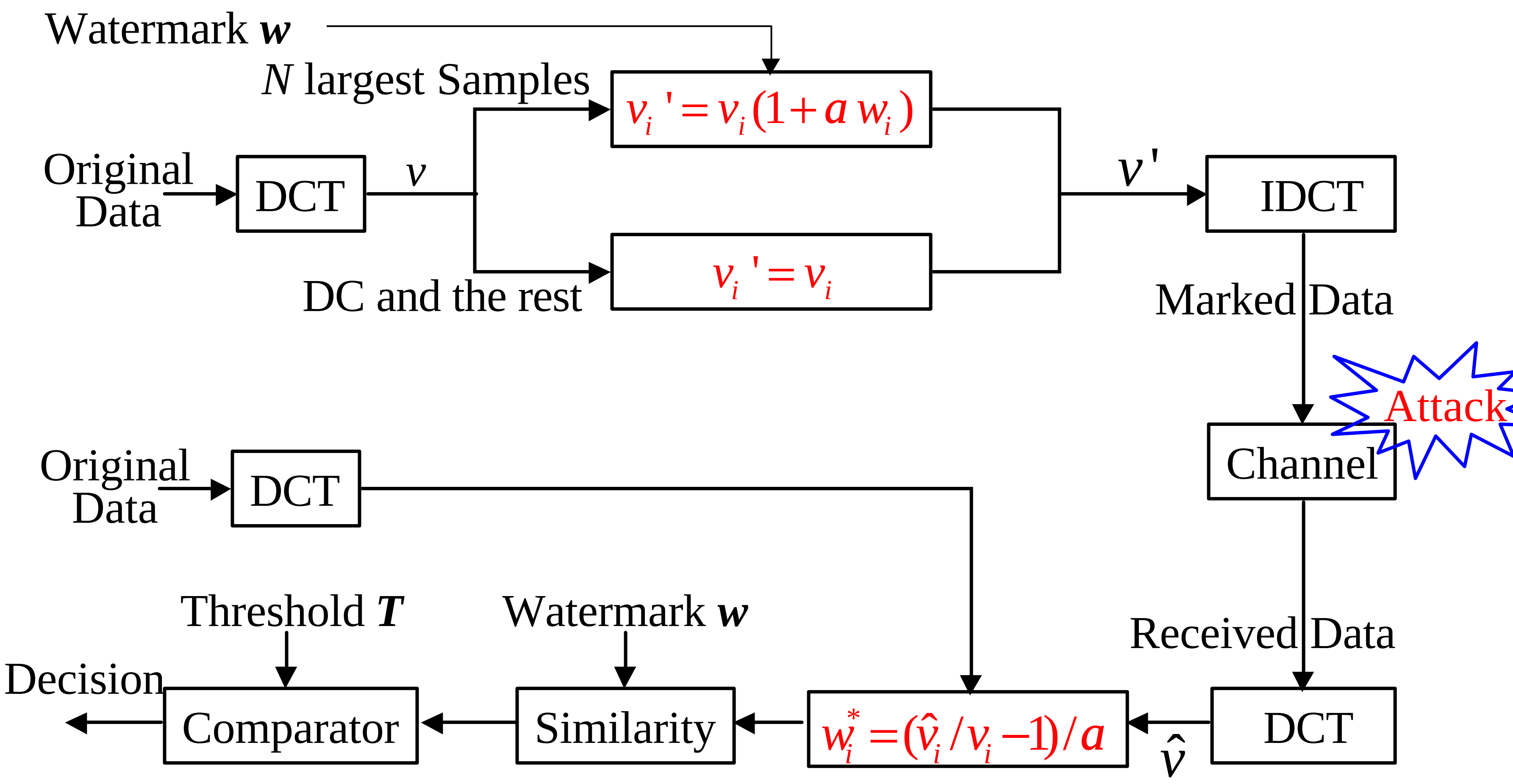
Cox's Scheme: Embedding



Cox's Scheme: Detecting

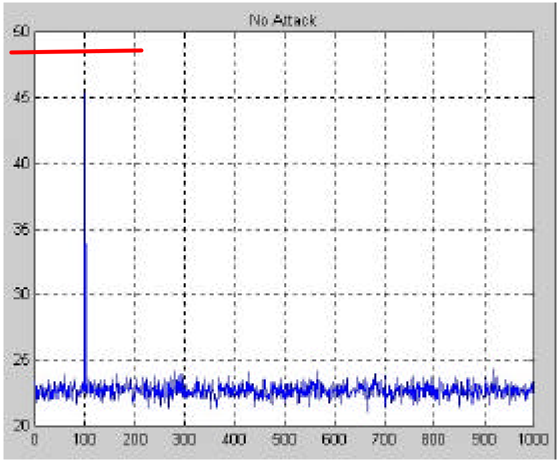


Block Diagram



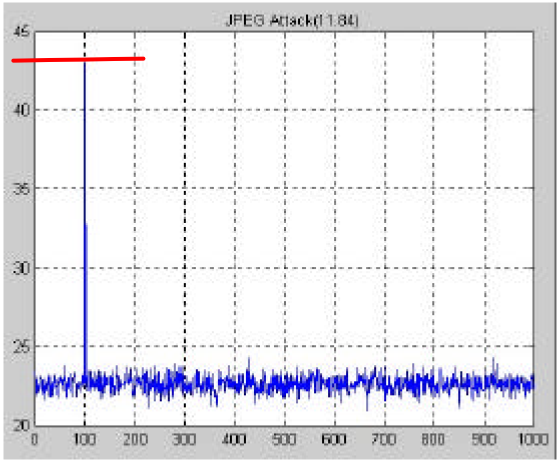
Results

Watermarked Image



Similarity=45.7

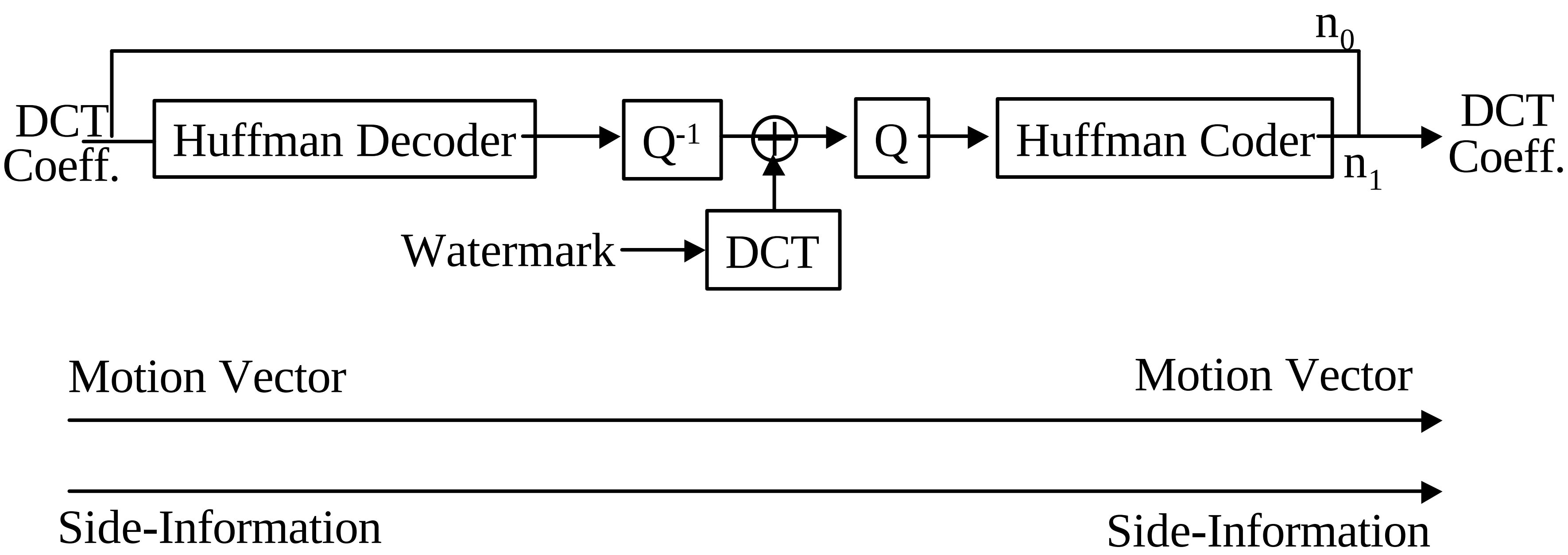
JPEG Attack (Ratio: 11.84)



Similarity =43.1

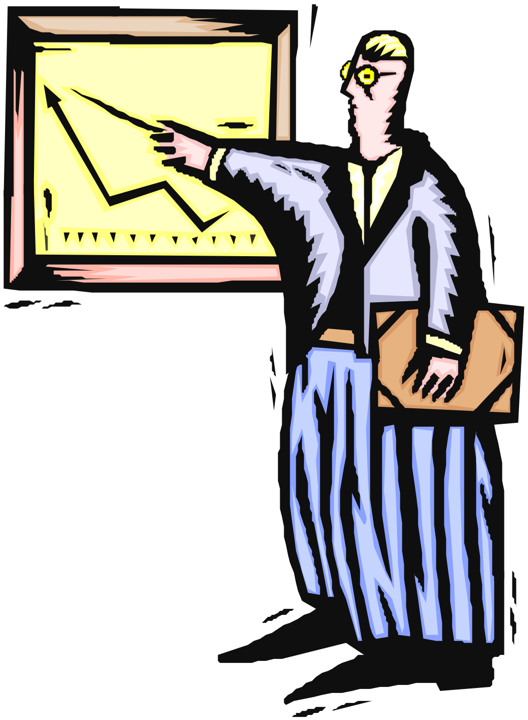
Video Watermarking

- Generic Scheme for Watermarking in Compression Domain



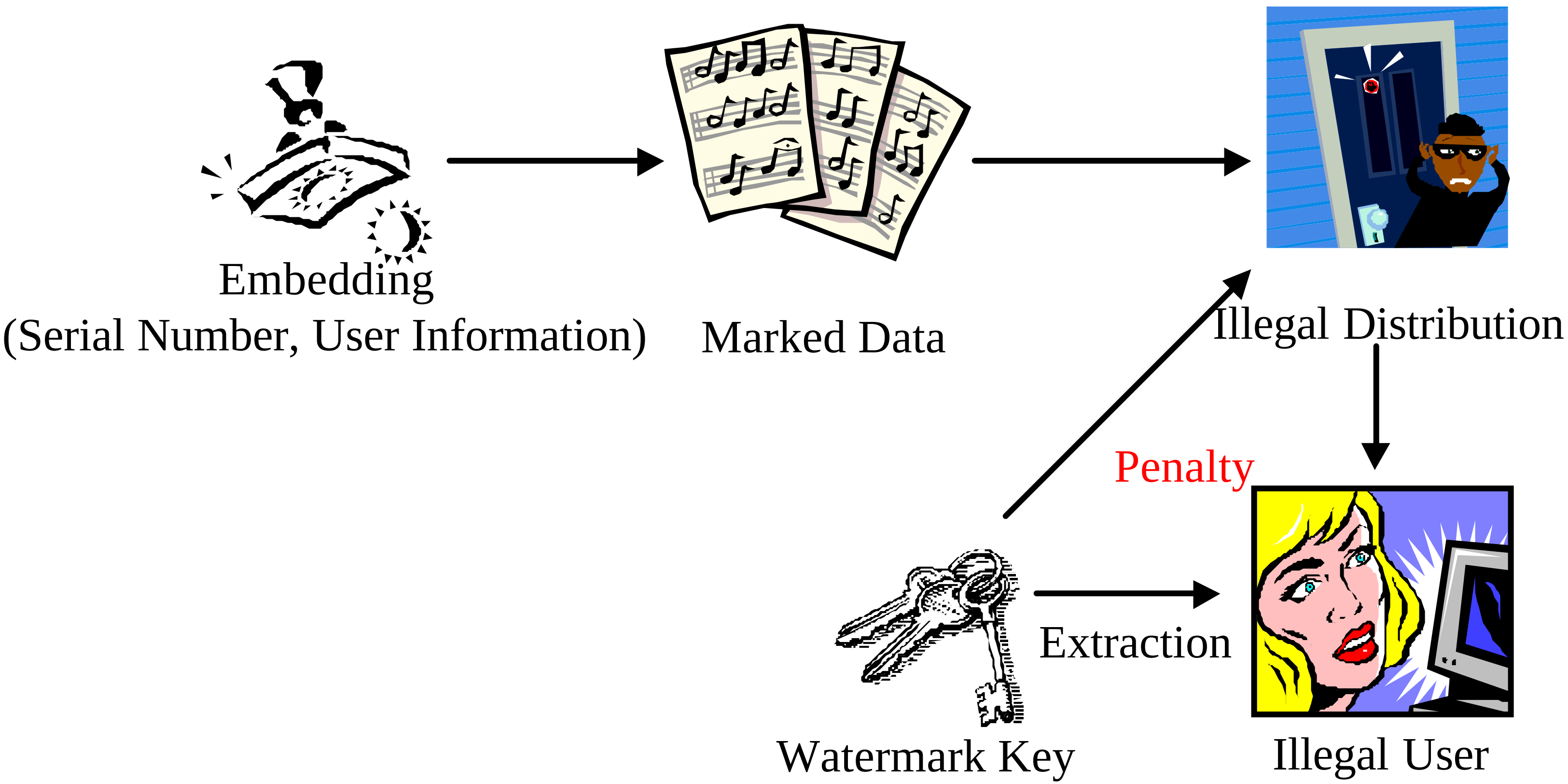
- If $n_1 \leq n_0$, embedding is performed

Watermarking의 응용

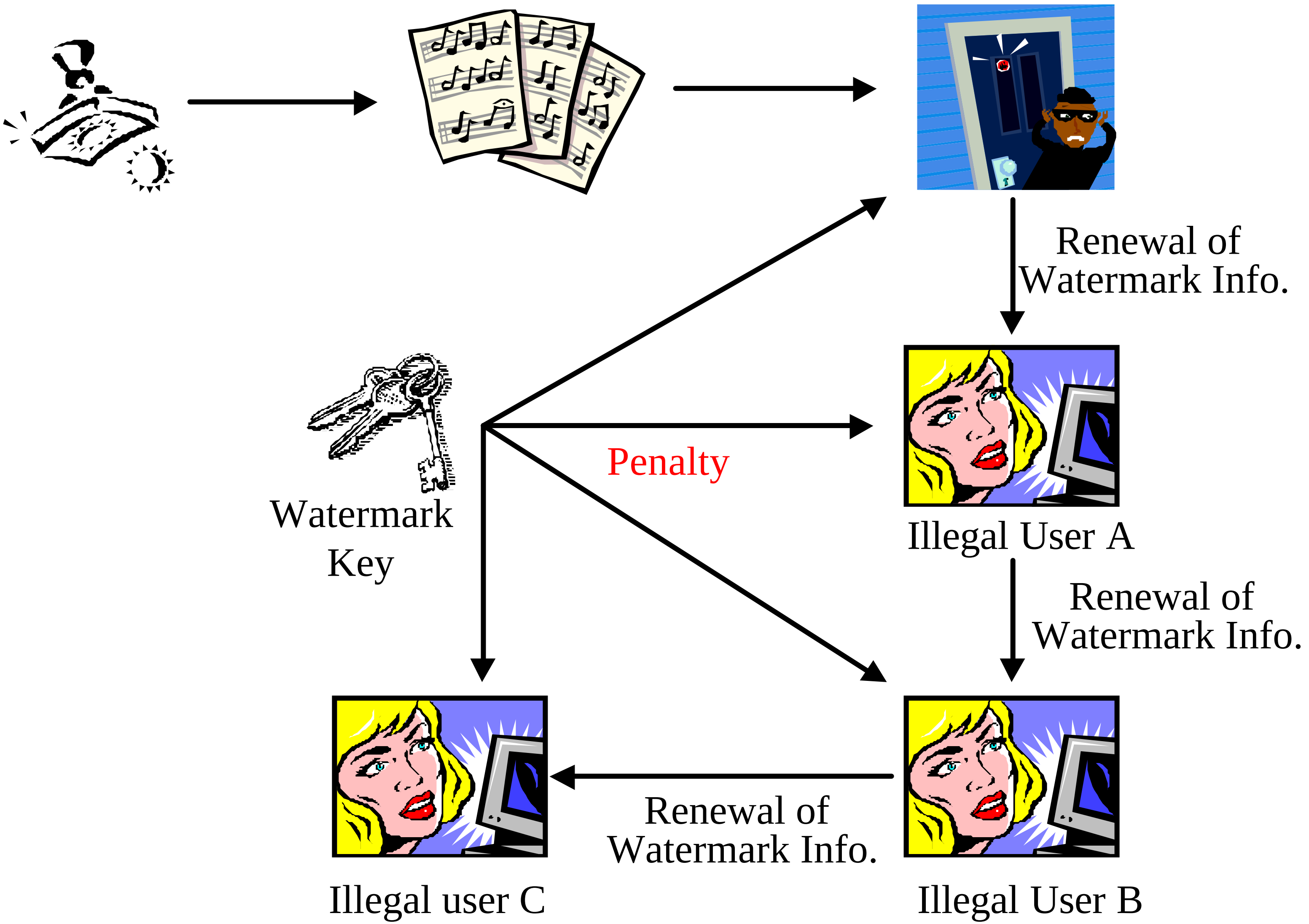


- Buyer Information
- User Information
- Usage Restriction
- Digital Library

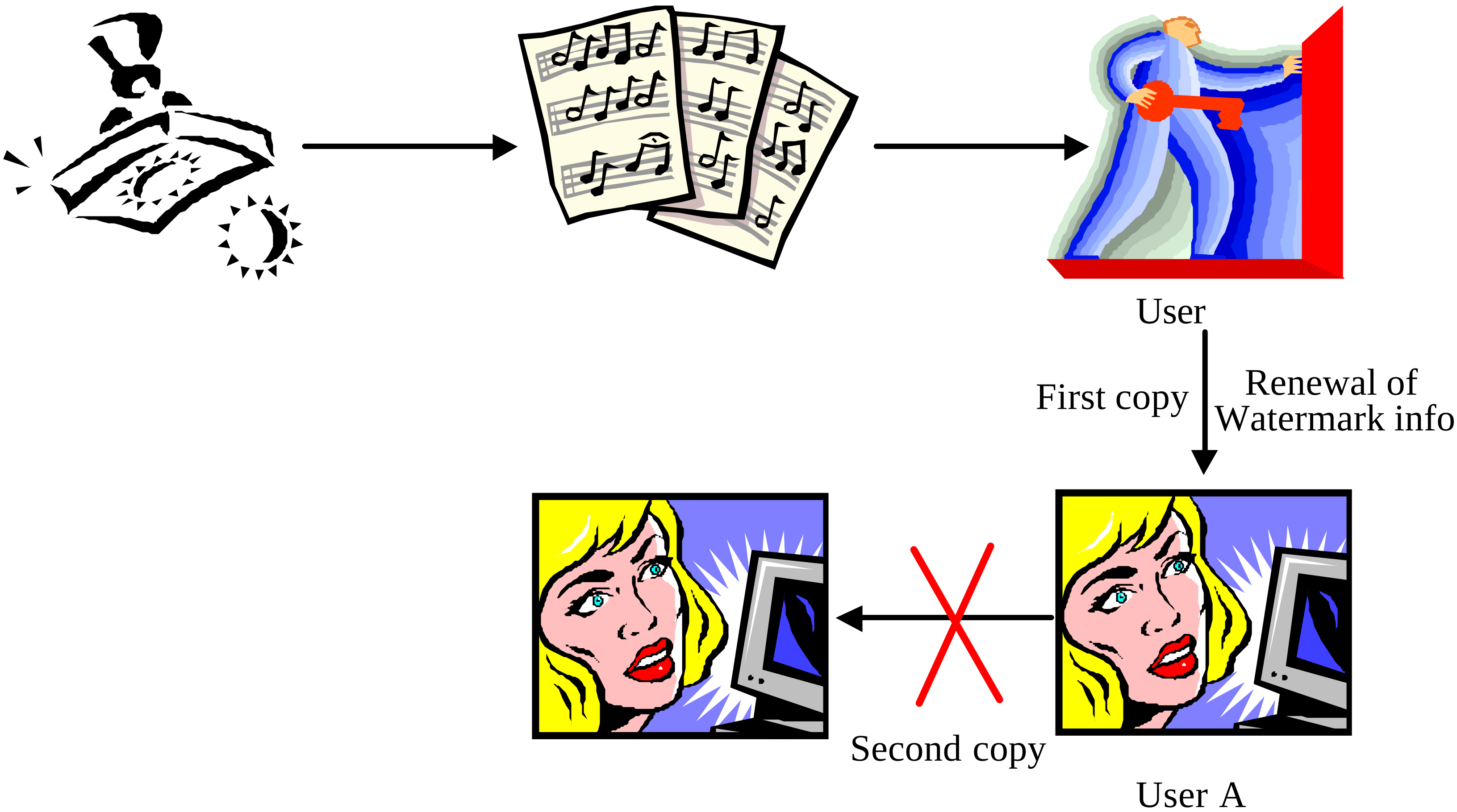
Buyer Information



User Information

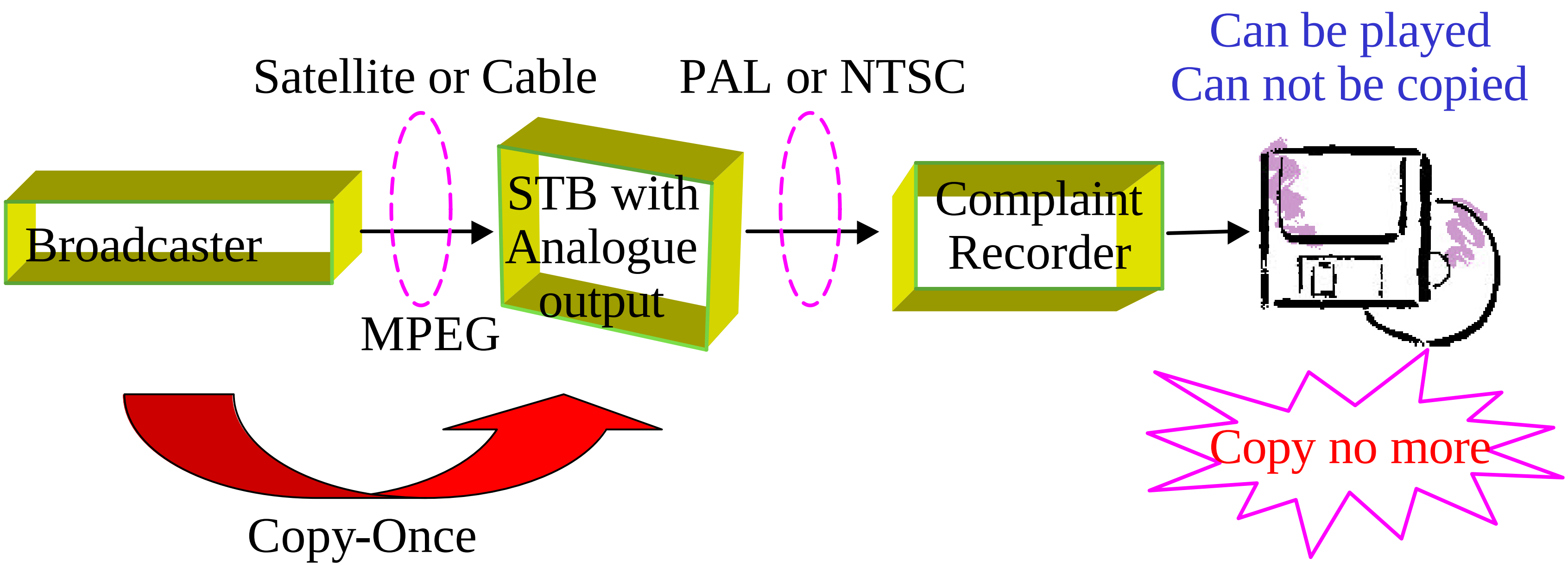


Usage Restriction

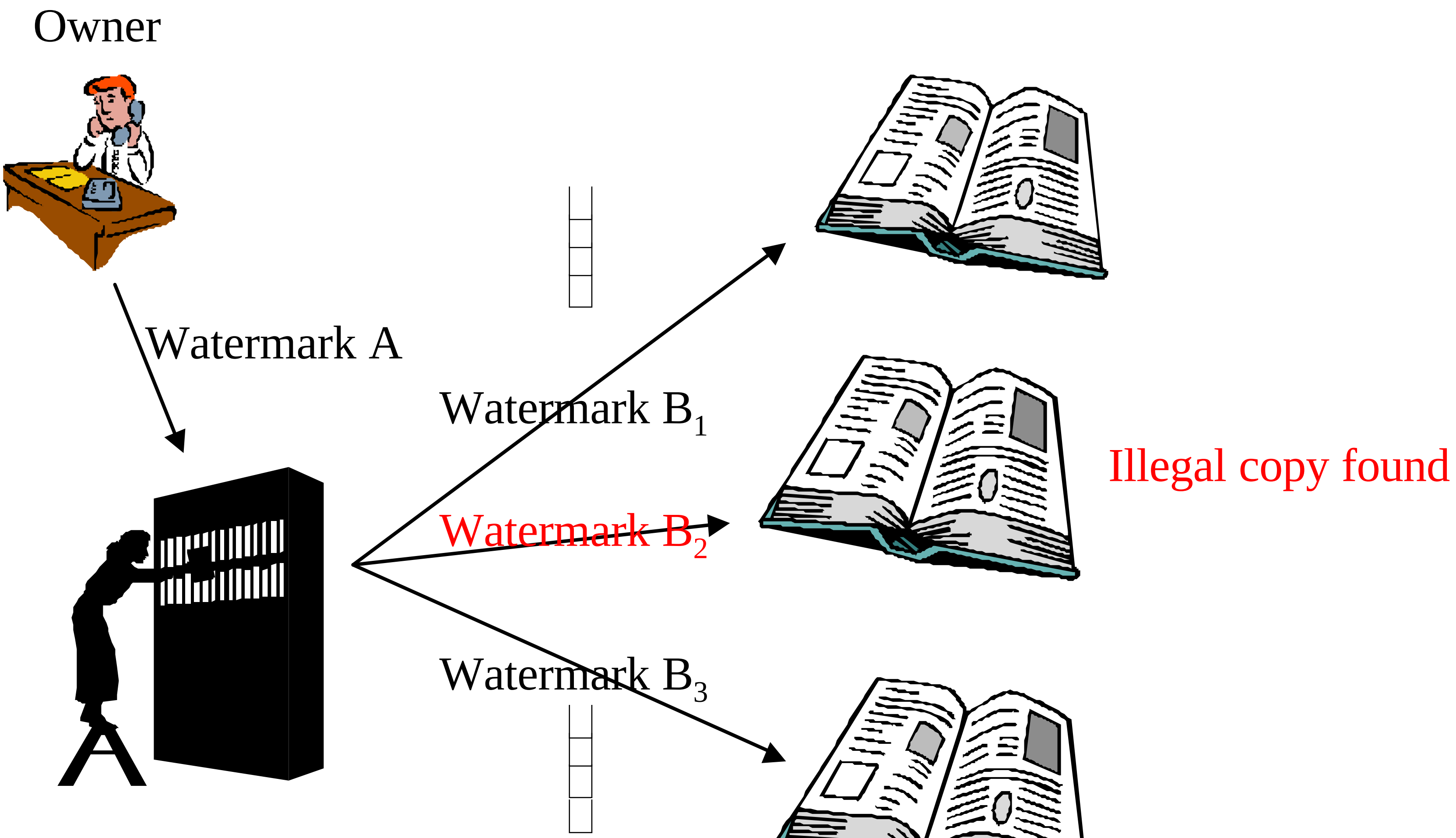


Only one copy is possible by usage restriction

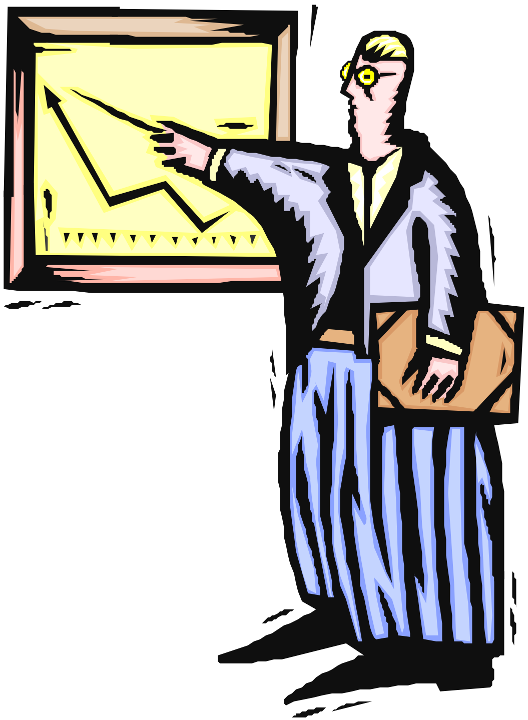
Copy-Once Scenario



Distribution from Library



MPEG-4 IPMP



- Intellectual Property (IP)
- IP Management & Protection
- MPEG-4 IPMP
- Call for IPMP Solutions

MPEG-4 표준과 IP 보호

- Intellectual Property (IP)
  - 작품, 정보, 발명, 표현 등의 제작자의 노력
- Intellectual Property Right (IPR)
  - 국내외 등록 절차를 통해 제작자나 대리인에게 저작품 복사 방지법으로 부여된 법적 권리
  - IPR 소유자의 허락없이 저작품 사용 불가
- IP Management & Protection (IPMP)
  - IPR 소유자들이 저작품 사용 제어를 위한 장치
    - 각 IPR 성분의 확인 (Watermarking)
    - IP 접근 방지 (암호화, CAS)

IP Identification (IPI) Data Set

- IPI Data Set
  - Associated with each A/V object to identify IPR components
  - Stored within the scene descriptor of each object
  - Facilitate the monitoring and tracking of usage
- Example of IPI Data Set
  - Type of Content: **책**, **노래**, **영화**, ...
  - Type of Content Identifier: ISRC, ISAN, ISBN, DOI
  - Content Identification Code: **내용 표시 단일 번호**
  - Supplementary Data: **필요한 다른 데이터**

MPEG-4 IPMP의 배경

- MPEG-4: Standard for Diverse MM Applications
- Conflicting Requirements for Protection
  - Some user data
    - No intrinsic value
    - Need to be protected for privacy
  - Managed content
    - Great value to its creator and/or distributors
    - Need high-grade management and protection mechanisms
- Level and Type of Protection
  - Content’s value and complexity
  - Sophistication of associated business models

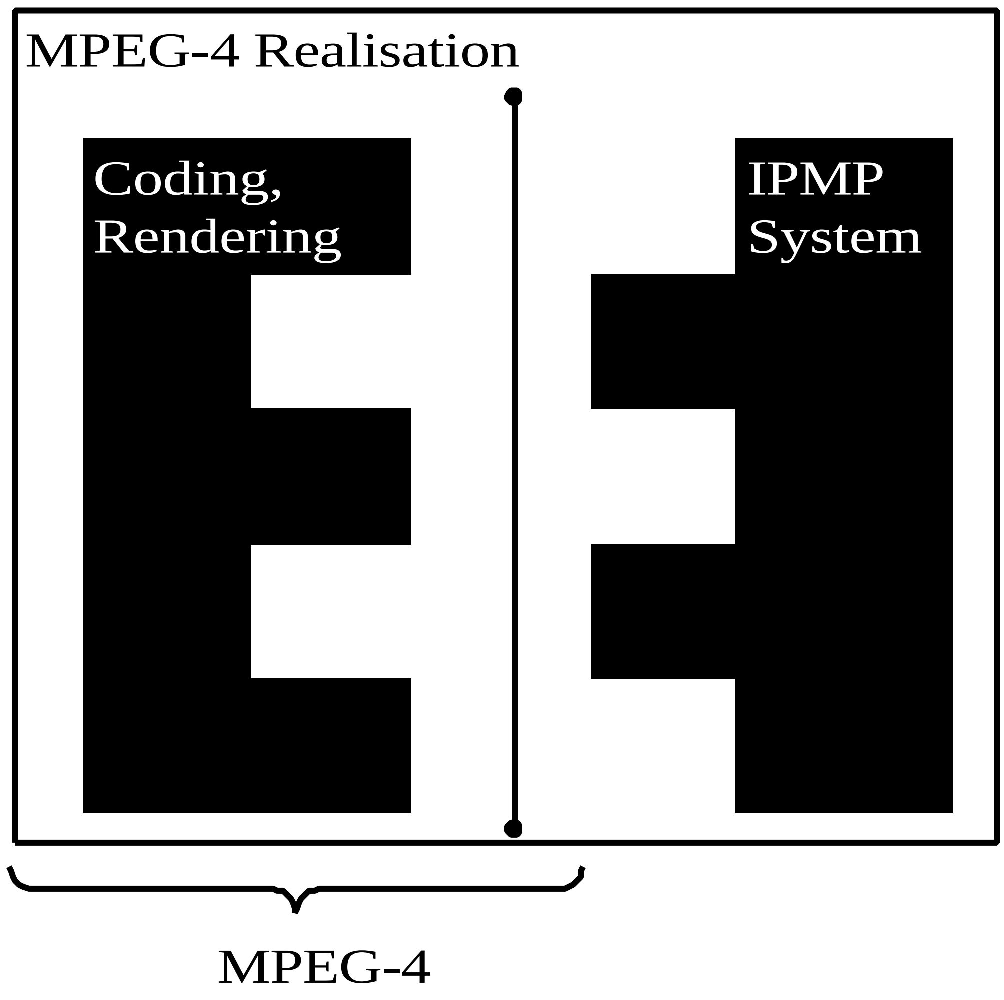
Patented IP Management

- Traditional Model
  - Paying once for a H/W device
  - Device manufacturer and distributors manage the associated royalties
  - Not attractive for MPEG-4 S/W implementations
  - Not clear that one should pay for patents involved in audio rendering unless one processes audio
- IPMP Framework
  - Audit the usage of patent IP in applications
  - Royalty payment based on information gathered

IPMP Interface

- Modular Approach for IPMP
  - Coding & Rendering: Normative part of MPEG-4
  - IPMP Systems: Non-normative part of MPEG-4
  - Separated by IPMP Interface
- MPEG-4 Defines Interface for IPMP Systems
  - MPEG-4 does not standardize IPMP systems
  - It only standardizes MPEG-4 IPMP interface
  - Application builders can construct the most appropriate domain-specific IPMP systems

IPMP Architecture



MPEG-4 IPMP Components

- IPMP Descriptor (IPMP-D)
  - Extension of MPEG-4 Object Descriptor (OD)
  - Indicate which IPMP systems are used
  - Provide information to the system about how to manage and protect the content
- IPMP Elementary Stream (IPMP-ES)
  - Similar to other MPEG-4 elementary streams
- IPMP System (IPMP-S)
  - Users build domain-specific IPMP systems
  - MPEG-4 does not standardize IPMP-S

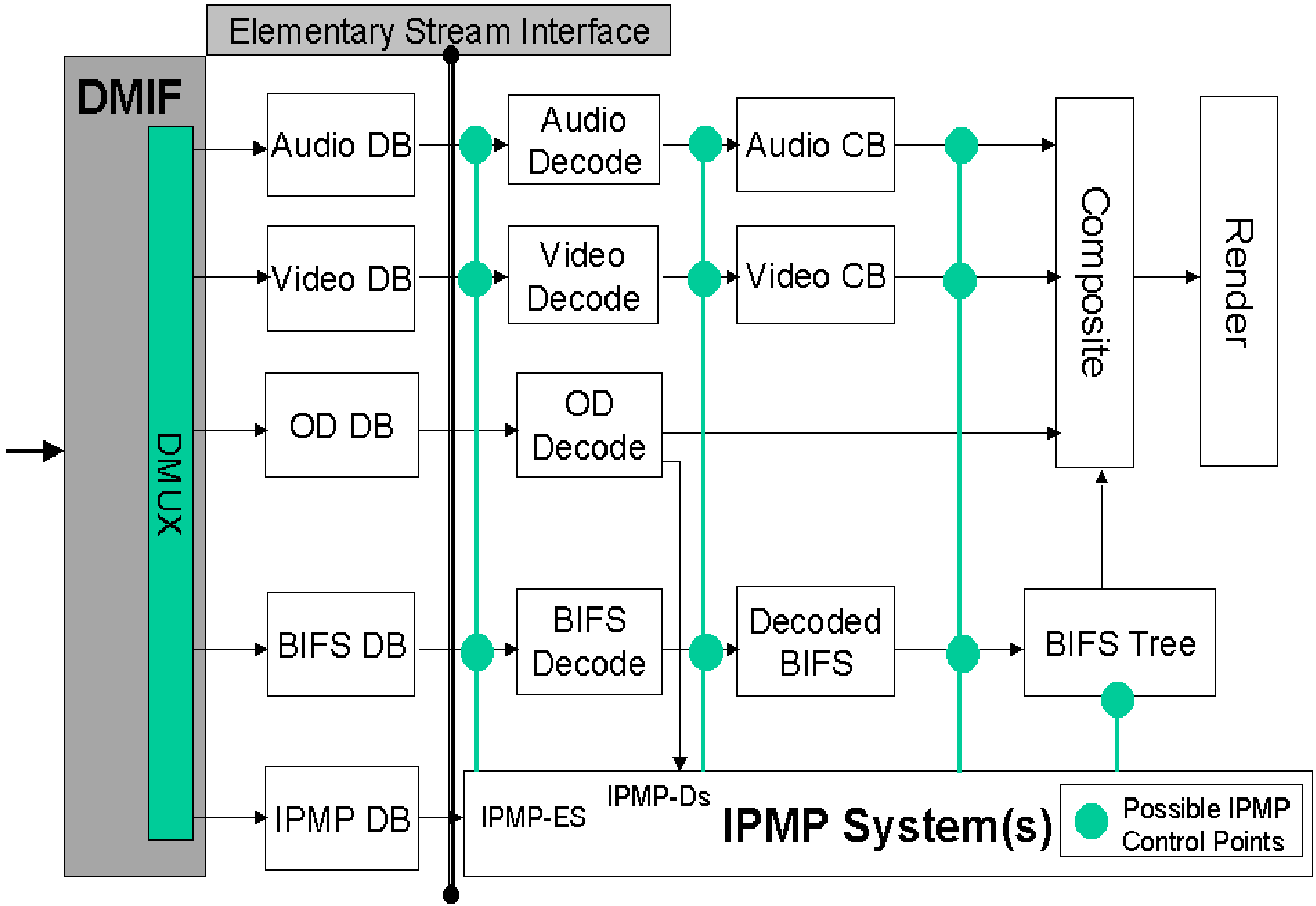
MPEG-4 IPMP

- MPEG-4 standardizes generic IPMP interface to IPMP tools, but not IPMP systems.
- The MPEG-4 IPMP interface consists of fully standardized IPMP-Ds and IPMP-ESs, which provide a communication mechanism between IPMP systems and the MPEG-4 terminal
- Certain applications may require multiple IPMP systems

MPEG-4 IPMP Control

- IPMP Interface
  - follows closely the MPEG-4 object/stream model
  - is designed to allow applications designers maximal flexibility
- IPMP Framework
  - indicates a variety of points in the MPEG-4 terminal at which one might desire IPMP control
  - may apply control between Demux and ES decoders
  - may apply control after stream decoding
  - may apply control to post-decode BIFS streams and individual elements

MPEG-4 IPMP Framework



History of MPEG-4 IPMP

- 1997
  - Call for Proposals for IPMP
- 1998
  - Not appropriate to standardise complete systems
  - but just providing the right interfaces
- 1999
  - Technology has matured
  - requirements for systems become clearer
  - better understanding of the role of IPMP technologies in building interoperable devices and services

Call for IPMP Solutions (N3543)

- **배경**
  - Increasing Need for Interworking between different types of devices and services
    - e.g. Broadband Internet Access, New Mobile Services
  - Current MPEG-4 IPMP Framework does not provide the necessary infrastructure to meet their interoperability requirements
- Call for Proposals
  - Requests submission of proposals that would allow interworking between different devices and services designed to play secure digital MPEG-4 content from multiple sources in a simple way

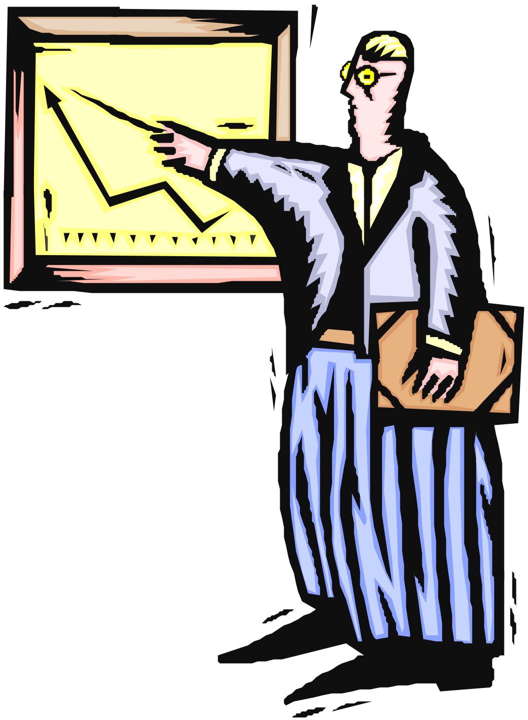
Development Plan

- Jan. 2001
  - Proposed Draft Amendment
- March 2001
  - Draft Amendment
- Dec. 2001
  - Final Draft Amendment

IPMP Solutions

- Basic Requirements
  - should be as complete as possible
  - should be compatible with the MPEG-4 Architecture
- The work
  - will be progressed in harmony with the Multimedia Framework that is being developed in the context of MPEG-21

OPIMA



- Open Platform Initiative for Multimedia Access
- OPIMA Approach
- OPIMA Protocol

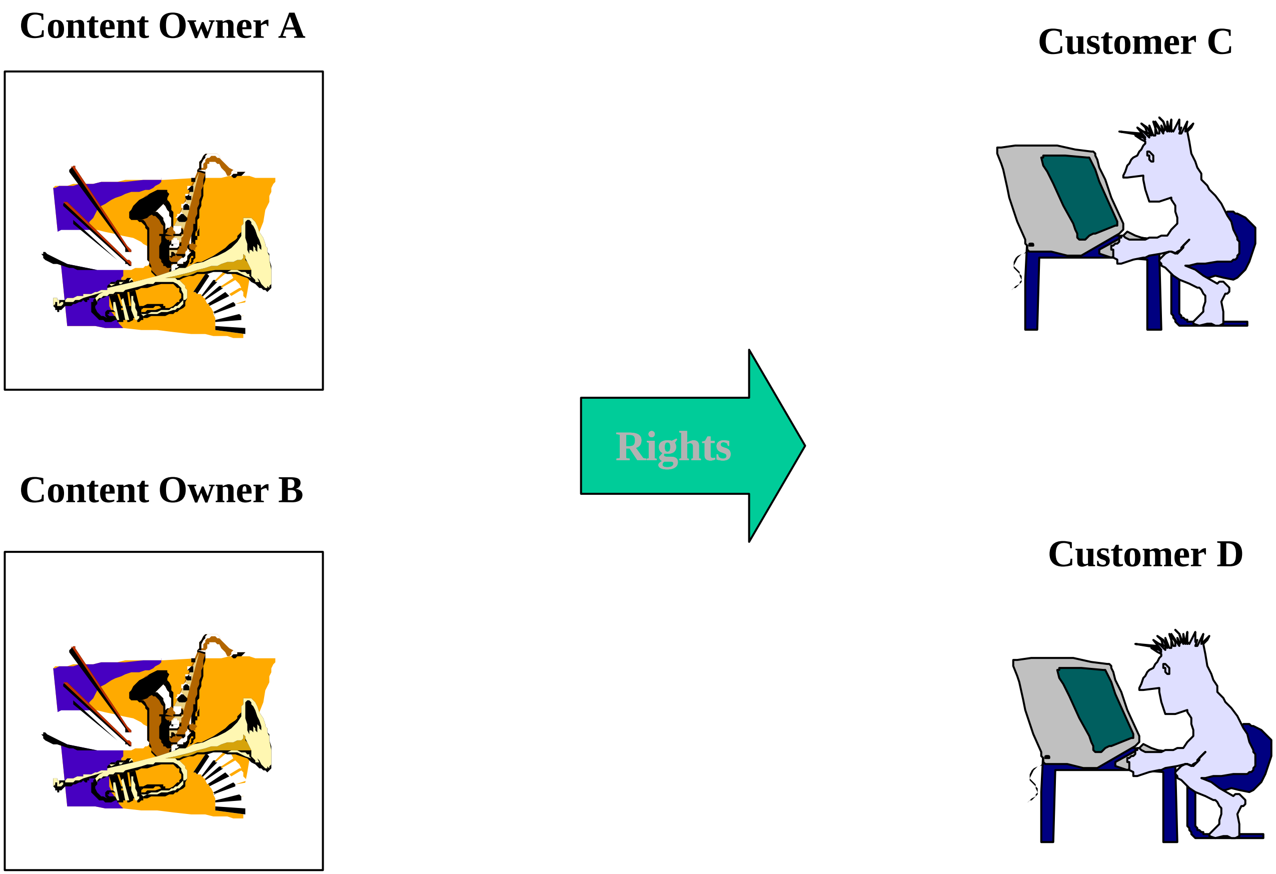
Introduction to OPIMA

- Open Platform Initiative for Multimedia Access
  - Initiative in ITA Program of IEC
  - Define an open and secure platform for multimedia content consumption
    - Open: independent from a specific protection system
    - Secure:
      - protect the content from the machine (OPIMA, DVD, SDMI)
      - protect the machine from content (Java, Unix, firewall)
- Basic Assumptions
  - Content has economic value, is consumed on platforms
  - Content must be protected from the platform
  - The platform remains independent from the adopted content protection system

OPIMA의 목표

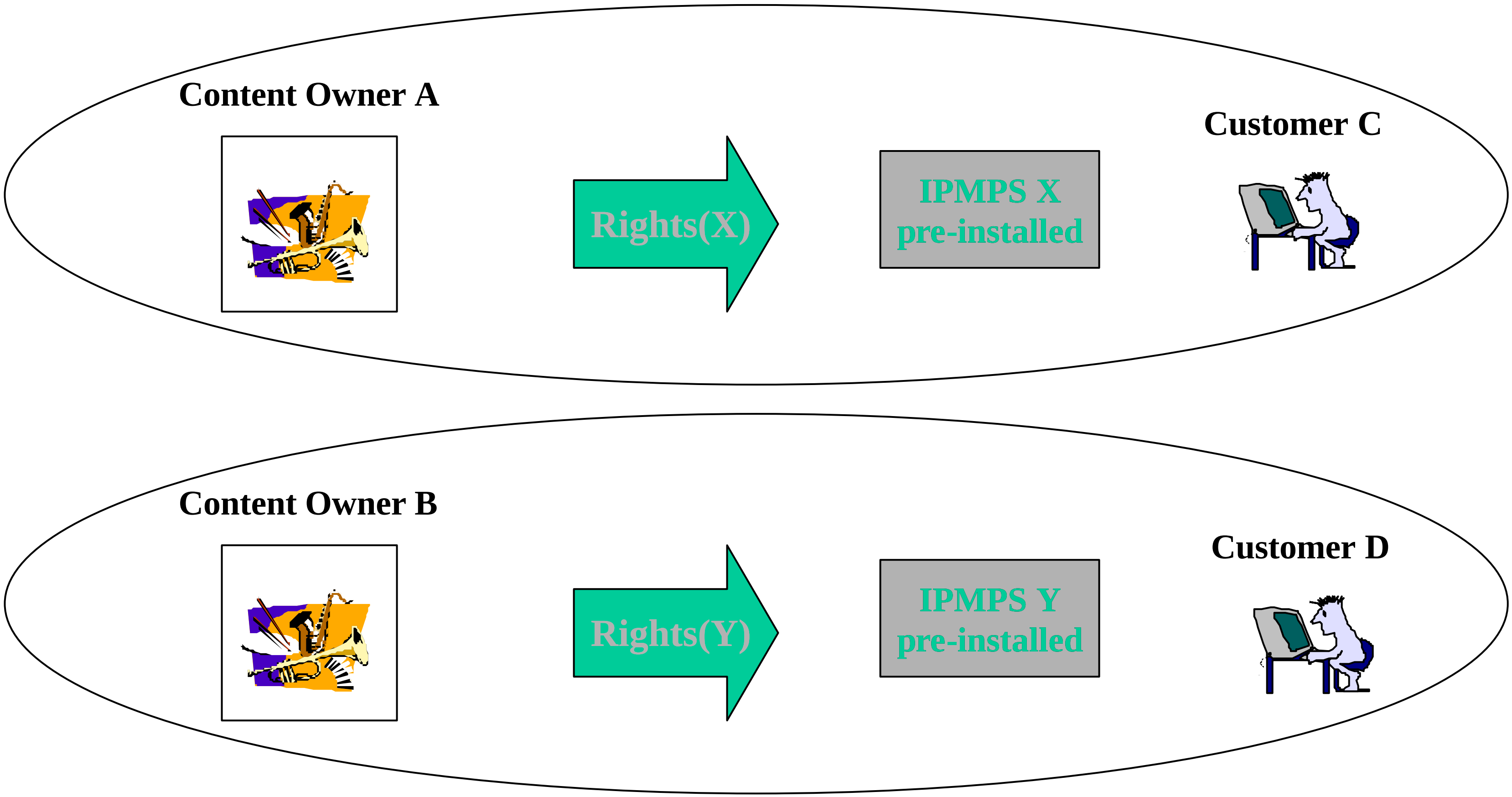
- Establish a “Framework” where
  - Content and service providers can extend the reach of their prospective customers
  - Consumers have the ability to access a wide variety of content and service providers in a context of multiple content protection systems.
  - Inter-operation between OPIMA-compliant devices, called OPIMA peers is possible
  - Code can be executed in the user environment

Basic Scenario



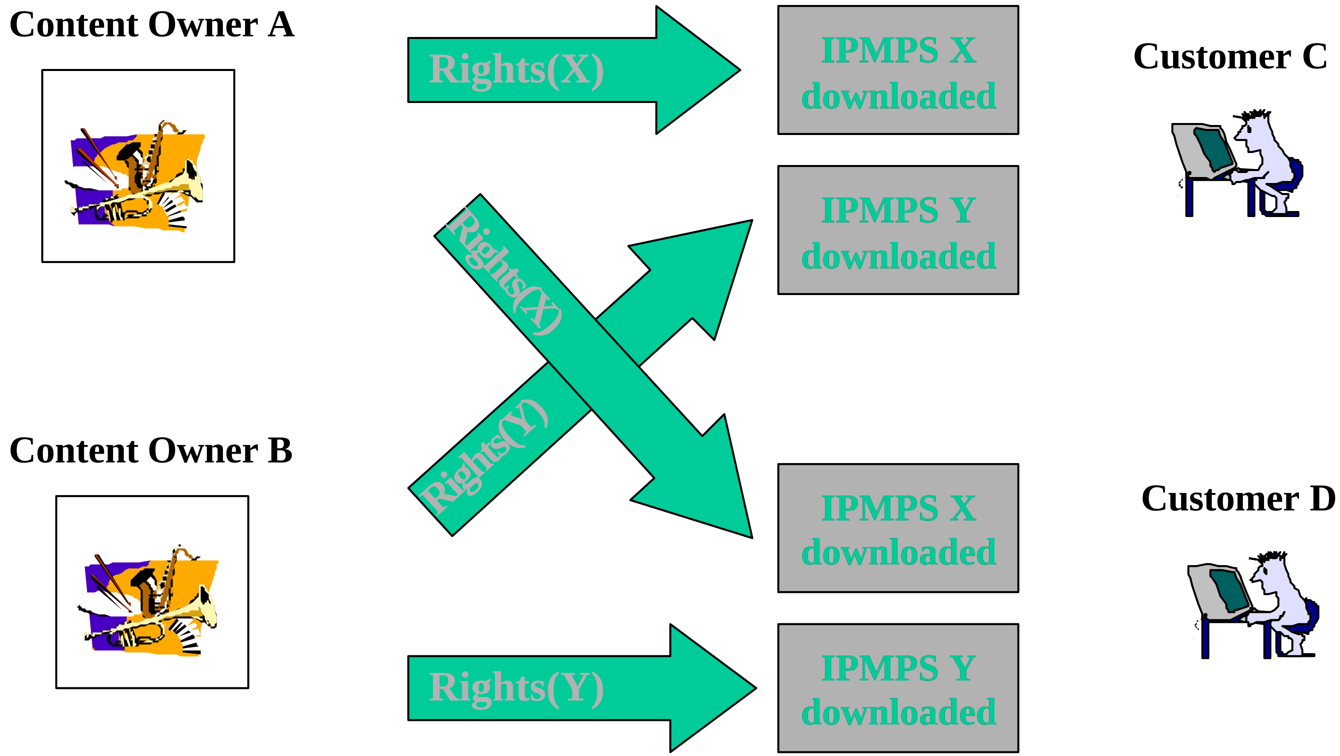
“All-Closed” Approach

- Security: High
- Interoperability: Low



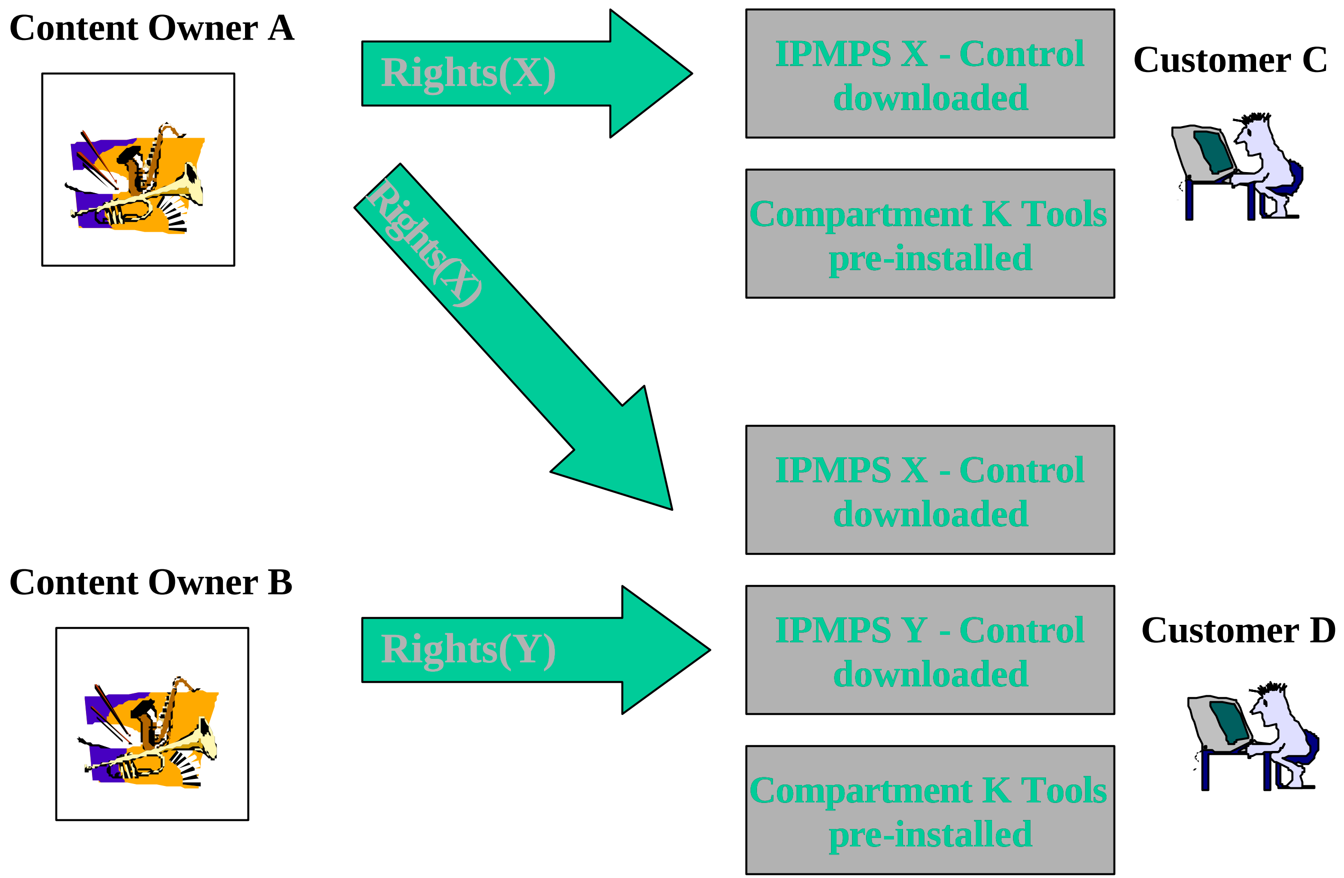
"All-Open" Approach

- Security: Low
- Interoperability: High



OPIMA Approach

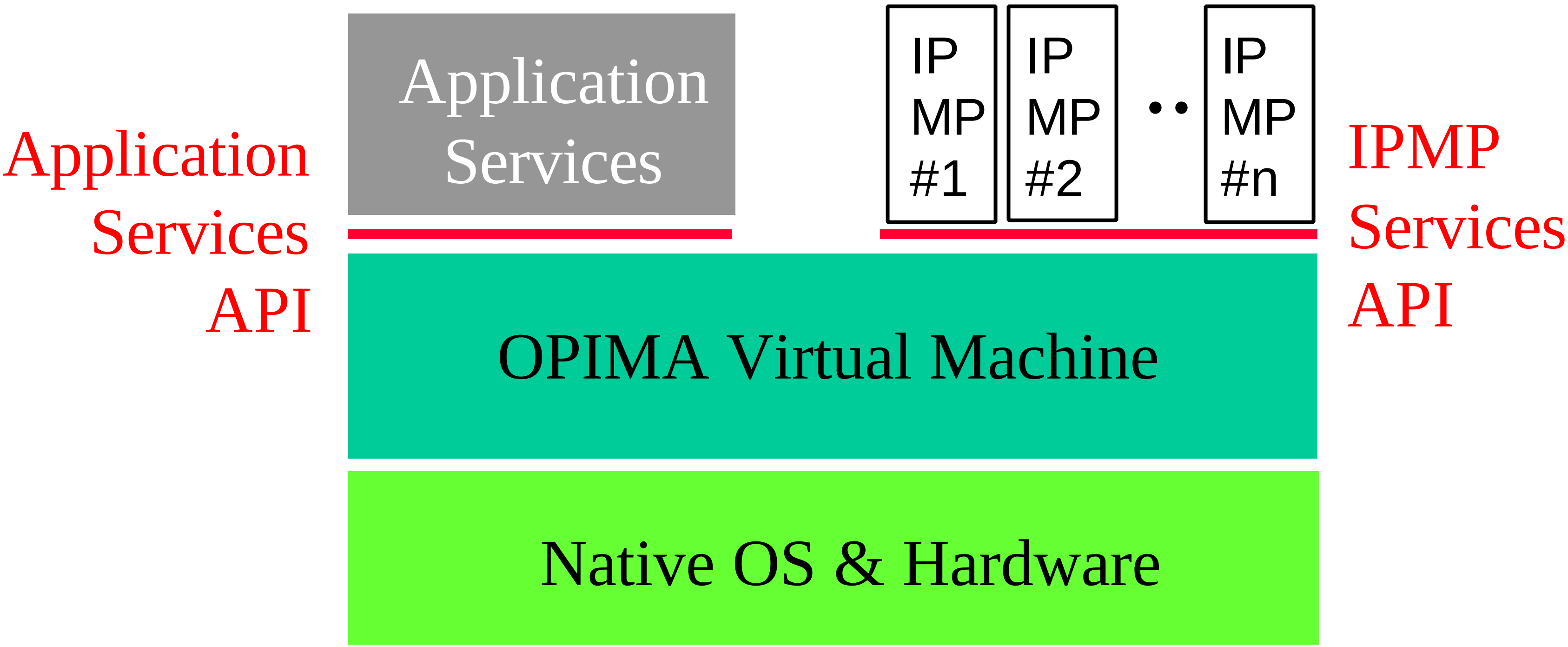
- Security: High
- Interoperability: Medium



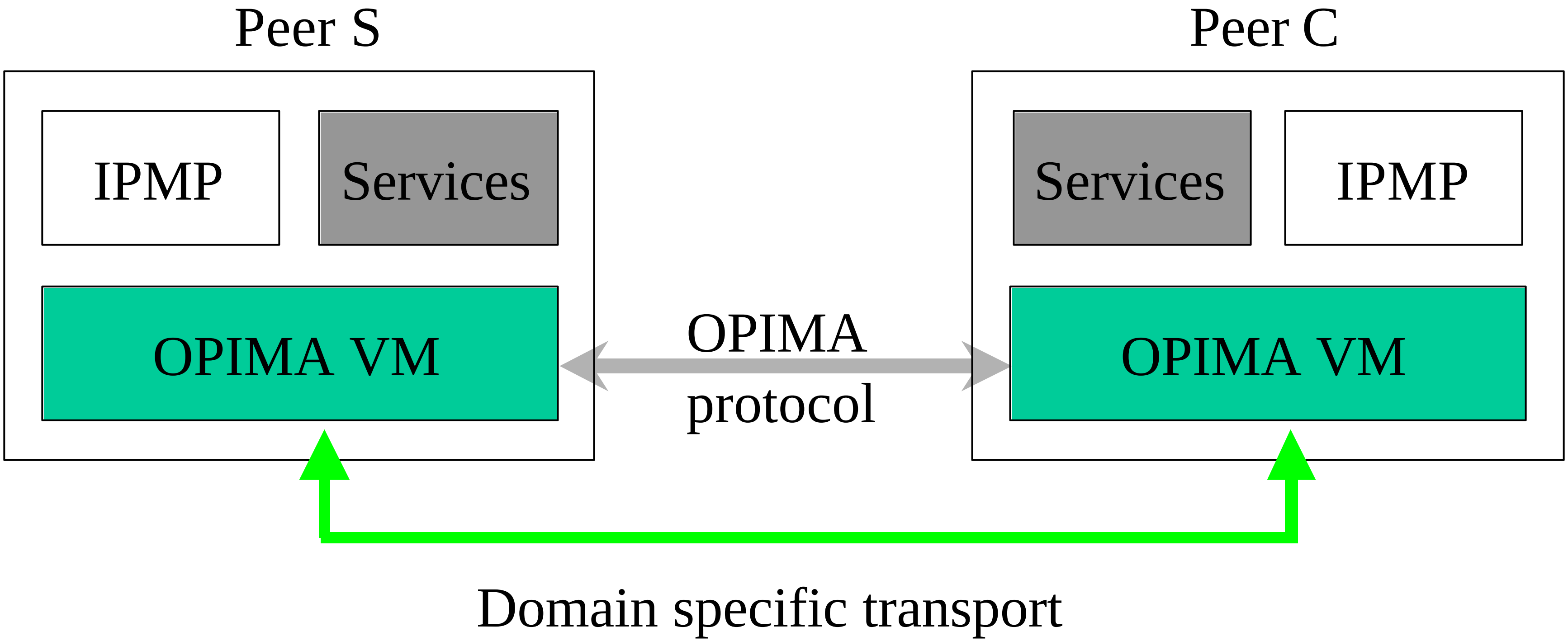
Advantages of OPIMA

- Security
  - All components accessing content are certified
  - SAC mechanism for installing downloadable components
  - Content owners have full control of rule and key management (proprietary mechanisms are allowed)
- Interoperability
  - Guaranteed inside the same ‘compartment’
  - Protected content can be consumed on different platforms
  - Usage rules and commercial policies can be renewed

OPIMA Peer


Application
Services
API
Application
Services
IP
MP
#1
IP
MP
#2
IP
MP
#n
IPMP
Services
API
OPIMA Virtual Machine
Native OS & Hardware

OPIMA Schema



OPIMA Protocol Example

- An Application requests to the OPIMA Virtual Machine (OVM) to access protected content.
- The OVM requests the OS to establish initial network connection.
- The OPIMA Secure Authenticated Channel (SAC) is established on top of this connection.
- The required IPMP system is requested and download by the OVM.

OPIMA, MPEG-7 & MPEG-21

- OPIMA is a flexible and open framework providing standard interfaces and protocols.
- OPIMA does not define everything inside the framework.
- OPIMA aims at striking a balance between security and interoperability.
- OPIMA leaves as many implementations choices as possible to business actors.
- OPIMA does not impose any solution in those fields, but is capable of integrating those that will emerge.

Conclusions

- Digital Watermarking
  - Crucial to secure networked multimedia systems
  - Trade-off between Quality and Robustness
- MPEG-4 IPMP
  - Interface to IPMP Systems
  - Modular Approach for IPMP
  - Call for Proposals for MPEG-4 IPMP
- OPIMA