방송 컨텐츠 보호 기술

2000. 11. 3.

무선.방송기술연구소
방송미디어연구부
홍진우 (jwhong@etri.re.kr)

ETRI
한국전자통신연구원

디지털 데이터의 지적 재산권 보호의 필요성

- 디지털 정보의 특성

  0 디지털화된 정보에 접근이 용이함.
  0 복제가 쉬울 뿐 아니라 이에 따른 비용 역시 비싸지 않음.
  0 복제된 디지털 정보는 정보의 손실 없이 원본과 동일함.
  0 복제된 디지털 정보의 재사용 및 조작이 쉬움.
  0 복제된 디지털 정보의 배포(네트웍이나 하드디스크와 같은 저장 장치를 통해)가 쉽고 빠름.

⇒ 이와 같은 디지털 정보의 특성은 디지털 정보의 지적 재산권 보호를 어렵게 하는 요인이 됨

디지털 데이터의 지적 재산권 보호의 필요성

- 예상되는 문제점

0 디지털 컨텐츠의 불법복제 및 배포

: 디지털 방송의 시작되면 대용량의 Set-top Box가 설치되고 이를 통해 저장된 대용량의 디지털 데이터의 불법복사 및 배포가 가능.

: 인터넷 방송의 경우에는 주로 개인용 PC를 이용하게 되므로 더욱 더 손쉽게 불법복사가 가능하고 네트웍을 통해 이를 배포할 수 있게 됨.

: 현재 Set-top Box나 개인용 PC등의 입출력 단자의 간단한 조작을 통해 손쉽게 디지털 데이터의 획득이 가능한 실정임.

: 방송은 24시간 계속해서 양적으로나 질적으로 가장 많은 컨텐츠를 생산하고 있음. 향후 디지털 방송이 시작되어 고품질의 멀티미디어 컨텐츠를 방송을 통해 획득하고 이를 불법으로 유통시킬 경우 멀티미디어 산업 전반에 엄청난 영향을 미치게 될 것임.

디지털 데이터의 지적 재산권 보호의 필요성

- 예상되는 문제점

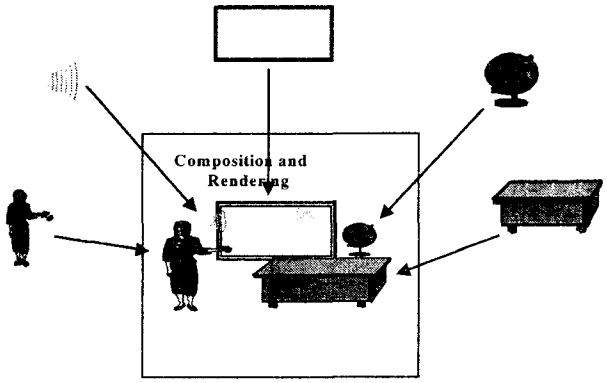
0 불법 복제된 디지털 컨텐츠의 재가공 및 배포

: 불법 복제된 디지털 데이터는 디지털 데이터의 속성 상 손쉽게 재가공될 수 있음. 특히, 향후 디지털 데이터는 MPEG-2, 4, 7 기반의 멀티미디어 데이터가 될 것이고, 이들은 멀티미디어 편집 소프트웨어나 간단한 신호처리적인 조작을 통해 재가공되어 불법적으로 유통될 수 있음.

: 이와 같은 재가공된 디지털 컨텐츠는 소유권이 누구에게 있는지 불분명하게 되므로 새로운 저작권 시비를 불러일으킬 수 있게 됨.

디지털 데이터의 지적 재산권 보호의 필요성

- 예상되는 문제점



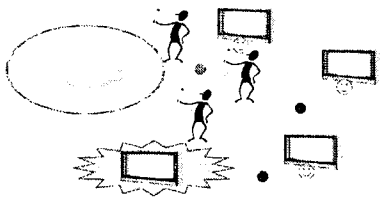
< AV Objects로부터 재 가공된 디지털 데이터 >

지적 재산권 보호를 위한 요소 기술

- 접속제어(Access Control)

0 소유권을 가지지 않은 자의 컨텐츠에 대한 접근을 막는 방법

: 주로 암호화를 이용하여 Scrambling
: 일단 암호가 풀린 디지털 컨텐츠의 경우에는 제어할 방법이 없음
: 권한이 있는 사용자가 이를 불법으로 배포하고자 할 경우에도 이를 제어하기가 불가능함.



< Access Control : 컨텐츠에 접속할 수 있는 권한(Key)이 있어야만 함 >

지적 재산권 보호를 위한 요소 기술

- 사용제어(Usage Control)

: 주로 인터넷에서 많이 이용되는 방법으로 암호화 키(Key)나 디지털 서명 등을 이용하여 컨텐츠의 사용 행위(Play, 복사 등)의 조절
: 이 방법의 경우 현실적으로 복사, 배포, 등의 컨텐츠의 사용과 관련된 모든 행위를 제어하기가 어려움.
: 실제 구현에 있어서의 문제점 : Bad acceptability, no standard agreement, etc.

- 워터마킹(Watermarking)

: 지각적으로 감지되지 않는 저작권 정보를 컨텐츠에 삽입
: 암호가 풀린 후에도 소유권을 주장할 수 있음.
: 의도적인 공격에 살아 남기가 대단히 어려움.

지적 재산권 보호를 위한 요소 기술

- 향후 발전방향

: 각각의 요소 기술들의 결합을 통한 방법 : 즉, 위에서 언급한 각각의 저작권 보호를 위한 요소 기술들의 특징을 결합하여 통합적인 저작권 보호 기술을 개발하고자 하는 노력이 활발히 이루어지고 있음.

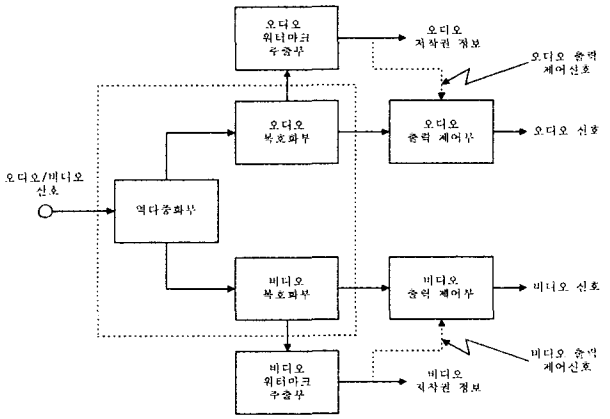
: 복제조절정보(CCI : Copy Control Information)를 워터마크로 삽입하여 워터마크 검출 시 한번 이상 복사되었으며 자동으로 Play가 멈추게 하거나 접속 권한이 없을 경우 자동으로 Scrambling 기능이 작동되게 함
⇒ 워터마크, 접속제어 및 사용 제어의 결합

: Play되는 시간정보를 워터마크로 삽입하게 하여 자동으로 과금이 Check 되게 함

: 깨지기 쉬운(Fragile) 워터마크를 이용한 디지털 컨텐츠에 대한 불법적인 변형 여부의 판별

지적 재산권 보호를 위한 요소 기술

- 향후 발전방향



< 워터마킹과 접속 및 사용 제어의 결합 >

Digital Watermarking의 정의

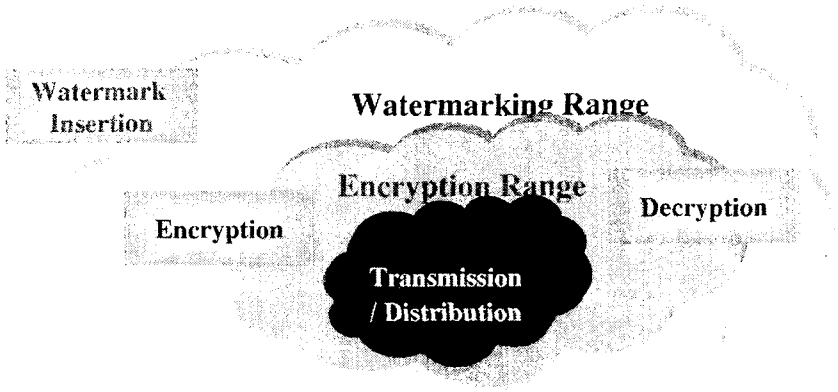
Robust and invisible embedding of an IP protection information

(a code) into a digital content (still image, video sequences, sound, text)

Characteristics:

- **Secret** watermark: readable only with the secret key used to embed
- Code which allows to associate **IP protection information** with the content and/or to **identify** the content
- **Robust** against "attacks" and **resistant** to compression, ideally not erasable without the secret key
- **Always present**, even after multiple generations, format conversion, diffusion chain,...
- Totally **undetectable** and **transparent** to users

Encryption vs. Watermarking



Digital Watermarking의 기능

- 소유권 주장 (Ownership)
  : 자신의 데이터에 Watermark를 삽입하여 Watermark 삽입된 영상을 유통시키고 원본 Watermark, 그리고 Watermarking에 사용된 키를 보관하여 차후 소유권 주장에 사용

- Fingerprinting
  : 불법복제와 불법유통을 막기 위해 각 Copy 마다 고유의Watermark를 삽입
  : 불법복제/유통된 데이터가 발견되면 Fingerprint를 추출하여 그 침해자를 알아냄

Digital Watermarking의 기능

- 인증 및 무결성 (Authentication and Integrity)
  : 내용이 조작/변형 여부를 확인하면서 송신자 확인 가능(수신자보호)
  : 추출된 Watermark의 무결성 입증 및 송신자 인증

- 내용 라벨링 (Content Labeling)
  : 삽입될 Watermark가 컨텐츠에 관한 정보를 포함

- 사용제한 (Usage Control)
  : 복제하거나 디스플레이할 때 특수 H/W가 필요한 경우 허용 가능한 복제 또는 디스플레이의 횟수를 Watermark로 조절.
  즉, 매 복제마다 Watermark를 수정하여 일정횟수 이상에서는 더 이상 복제될 수 없도록 함

- 내용보호
  : 상업적으로 재사용될 수 없도록 육안이나 귀로 확인할 수 있는 Watrermark 삽입

Attacks

- **Low-pass filtering**: diminishes image quality

- **lines and/or columns removal(cropping)**: implies a resynchronization before retrieval, difficult to face to a certain extend, but the image is smaller

- **Geometrical manipulations** (rotations, rescaling, affine transform): difficult to face to a certain extend, but diminishes image quality

- **D/A/D conversions**: diminishes image quality

- **Additive noise**: diminishes image quality

- **Collusion**: different users having the same image with different watermarks collaborate

Performance Analysis

- Invisibility (major issue)

- Data rate (not always an issue)

- Robustness to compression (major issue)

- Resistance to main attacks (depends on the application)

Approaches

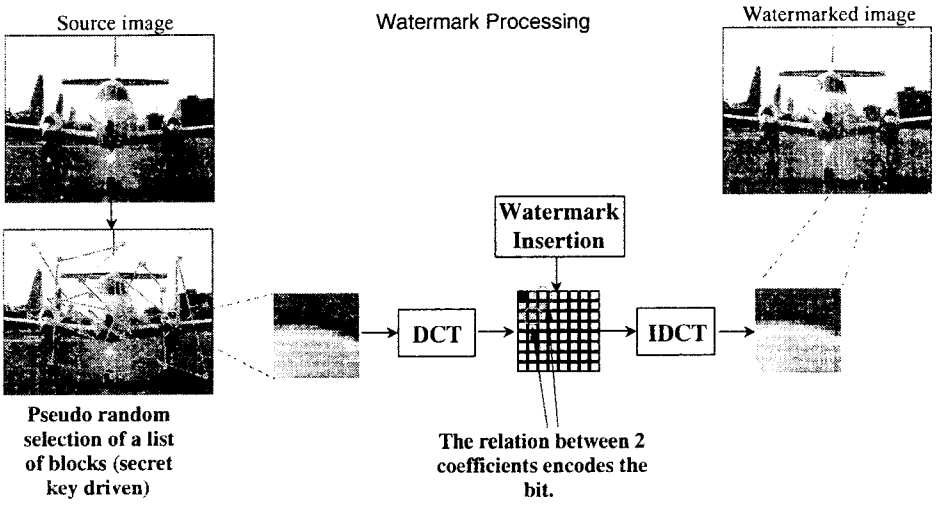
- Spatial domain (most of the methods):
  - luminance modification (Digimarc, Philips, UCL-OCTALIS SW)
  - chrominance modification (literature)

- Transform domain :
  - DCT (IBM/NEC, SONY)
  - DCT blocks (OCTALIS HW)
  - DFT (literature)
  - Fourier-Mellin transform(literature)
  - wavelets (literature)
  - fractals (literature)
  - MPEG (Philips, AT&T)
  - perceptual criteria (UCL, literature)

Commercial Products

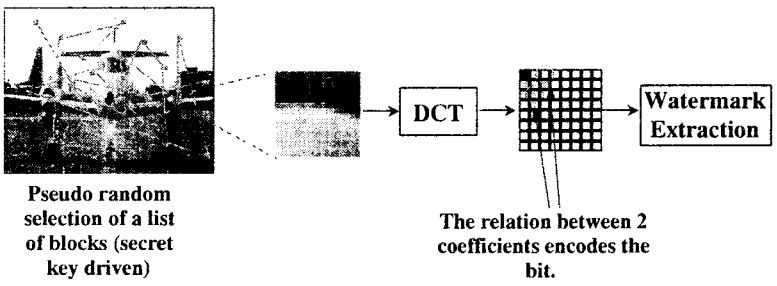
SOFTWARE	HARDWARE
Alpha Tech (Eikonamark)	IBM/NEC
Blue Spike (Giovanni)	Macrovision/DIGIMARC
CRL-Thorn EMI	Matsushita
Datamark	Philips
DIGIMARC	SONY
Informix (NEC)	Hitachi
MediaSec	Telstra
R3S	...
Signafy	
Signum Technologies	

Example : OCTALIS Wateramrking



Example : OCTALIS Wateramrking

Monitoring Processing



Pseudo random selection of a list of blocks (secret key driven)

The relation between 2 coefficients encodes the bit.