디지털 방송 컨텐츠 보호 기술

Electronics and Telecommunications
Research Institute

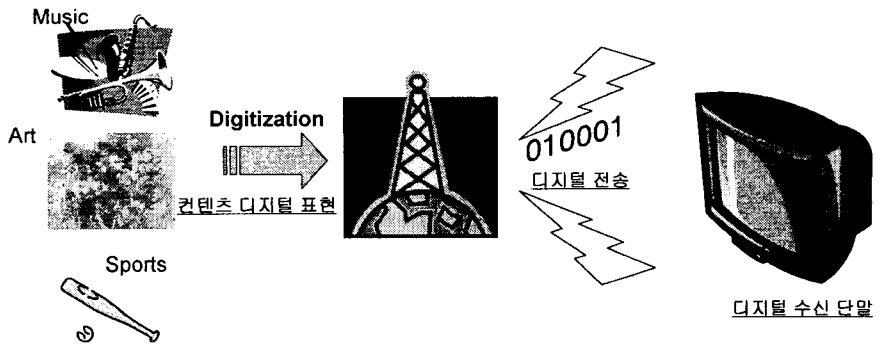
Jin Woo Hong

Jwhong@etri.re.kr

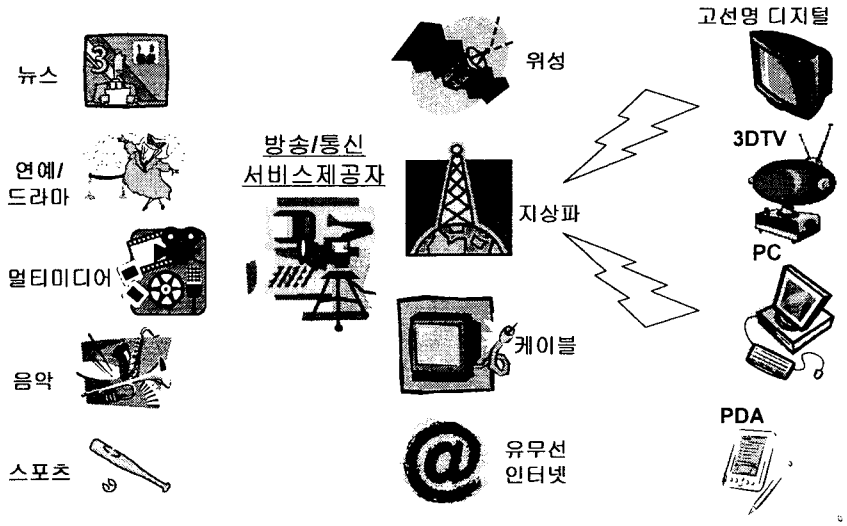
목 차

디지털 방송 컨텐츠 보호의 필요성

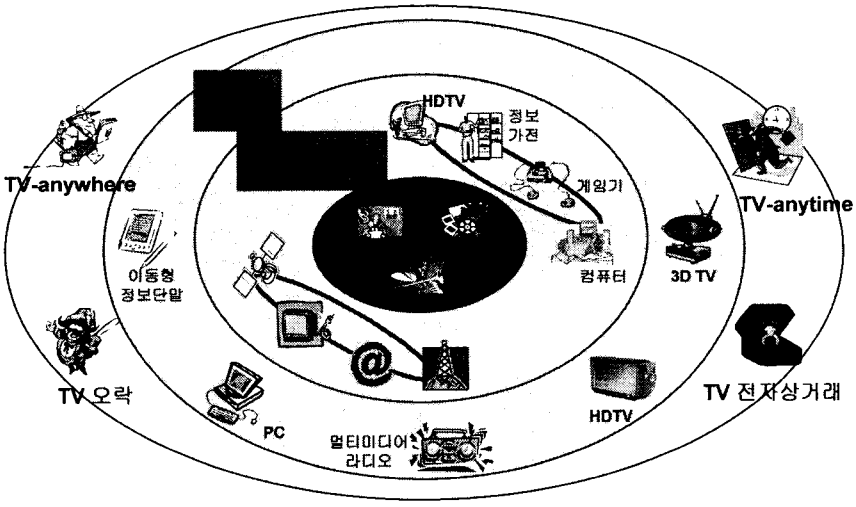
미래의 방송 → 디지털화



미래의 방송 → 서비스 및 수신기 다양화



미래의 방송 → 방송/통신 통합



디지털 정보의 특성

- 디지털화된 정보에 접근이 용이함.
- 복제가 쉬울 뿐 아니라 이에 따른 비용 역시 비싸지 않음.
- 복제된 디지털 정보는 정보의 손실 없이 원본과 동일함.
- 복제된 디지털 정보의 재사용 및 조작이 쉬움.
- 복제된 디지털 정보의 배포(네트웍이나 하드디스크와 같은 저장 장치를 통해)가 쉽고 빠름
- 방송과 통신(인터넷)의 융합으로 하나의 컨텐츠가 다매체에 다수 사용

⇒ 디지털 컨텐츠의 보호를 어렵게 하는 요인.

방송 환경의 변화 가속화

◈ 미디어의 유연성, 양방향성 증대
◈ 방송과 인터넷의 결합, 전자상거래 연동
◈ 방송과 통신의 융합
  ➢ 다양한 뉴미디어의 등장으로 방송 사업의 경쟁
◈ 방송의 소비 형태 변화
  ➢ 고품질 정보의 무한 반복 재현, 가공재생, 저장에 의한 시공간 초월
  ➢ 정보 창조자로서의 역할
    단순 시청형 → 정보 선택형 → 정보 요구형 → 정보 창조형

⇒ 디지털 정보(컨텐츠)의 다양화, 차별화, 고품질화, 접근 용이성 등으로 귀착 → 디지털 컨텐츠의 중요성 대두

서비스 다양화, 방송/통신 융합 특성

▸ 고품질의 다양한 컨텐츠를 다양한 수신기에 제공.
▸ 컨텐츠 저장형 수신기의 등장.
▸ TVanytime, TVanywhere 서비스 도입
▸ Home networking에 의한 컨텐츠 전달
▸ 방송/통신 융합에 의한 one source multiple use.
▸ 사용자 맞춤형 방송 서비스로 인한 컨텐츠 재생산

⇒ 디지털 컨텐츠의 보호 및 관리 필요성 대두

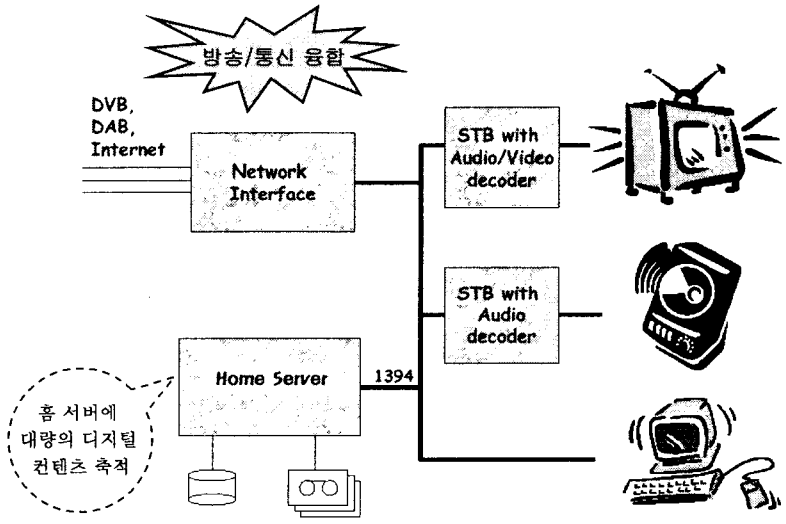
- IPMP : Intellectual Property Management & Protection
- **DRM : Digital Rights Management**
- **RMP : Rights Management & Protection**

예상되는 문제점

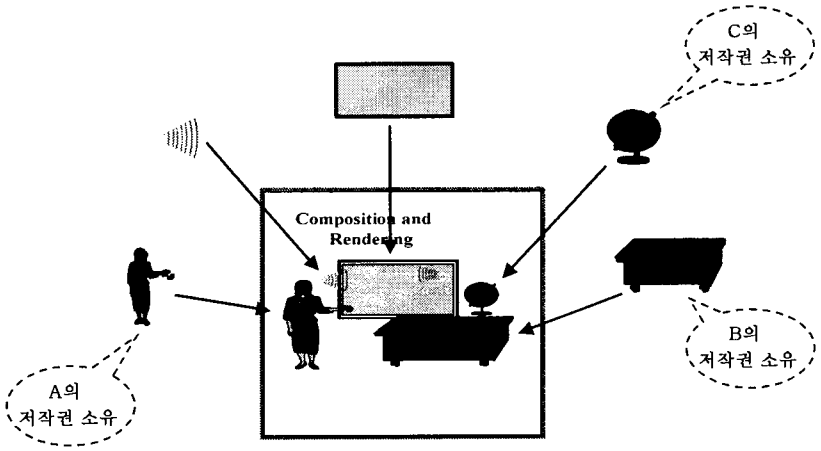
- 디지털 방송 컨텐츠의 저작권 시비
- 디지털 방송 컨텐츠의 불법 복제 및 무단 배포
- 불법 복제된 디지털 컨텐츠의 재가공 및 배포
- 컨텐츠의 무료화 인식 확산

⇒ 디지털 방송 컨텐츠의 제작/생산 기피 현상 발생

방송.통신 융합에 의한 홈네트웍의 구성 예



예상되는 문제점(재가공의 예)



< AV Objects로부터 재 가공된 디지털 데이터 >

"Ten emerging technologies that will change the world"

- brain-machine interfaces
- flexible transistors
- data mining
- digital rights management
- biometrics
- natural language processing
- micro-photonics
- untangling codes
- robot design
- micro-fluidics

(출처 : MIT Enterprise Technology Review; HTTP://www.technologyreview.com/)

디지털 컨텐츠 보호를 위한 요소 기술

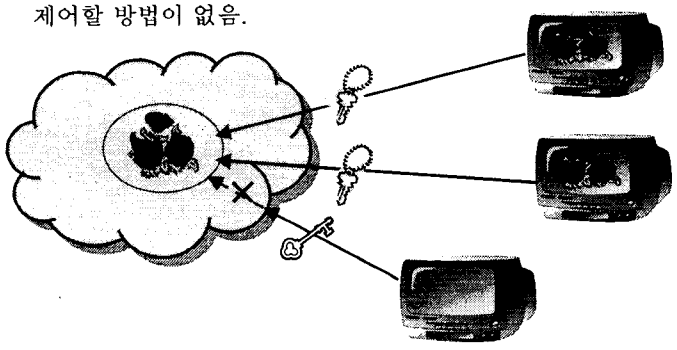
- 접속 제어(Access Control)
  - Protection by Authentication
- 사용 제어(Usage Control)
  - Protection by Scrambling/Encryption
- 내용 제어(Content Control)
  - Protection by Watermarking

접속 제어(Access Control)

▸ 권리가 없는 사용자에게 컨텐츠에 대한 접근을 막는 방법

: 주로 인증 기술을 이용하여 접근을 방어함 → 저작권 보호는 불가능

: 일단 인증키가 풀린 디지털 컨텐츠의 경우
또는 권한이 있는 사용자가 이를 불법으로 배포하고자 할 경우에는
제어할 방법이 없음.

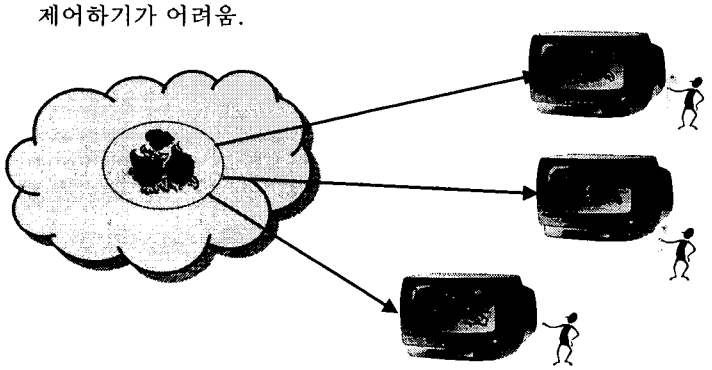


사용 제어(Usage Control)

▶ 정당하지 않은 사용자의 컨텐츠에 대한 사용을 막는 방법

: 주로 인터넷에서 많이 이용되는 방법으로 암호화 키(Key) 등을 이용하여 컨텐츠의 사용 행위(Play, 복사 등)의 조절

: 현실적으로 복사, 배포 등 컨텐츠의 사용과 관련된 모든 행위를 제어하기가 어려움.



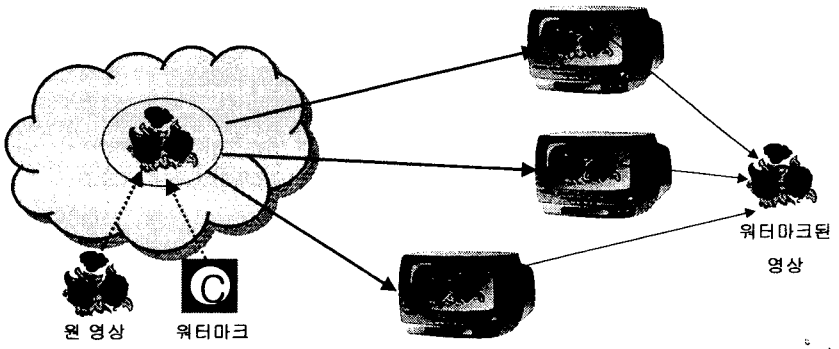
내용 제어(Content Control)

▶ 컨텐츠 내용안에 은닉된 정보를 이용하여 저작권 정보 및 불법적인 복제를 막는 방법

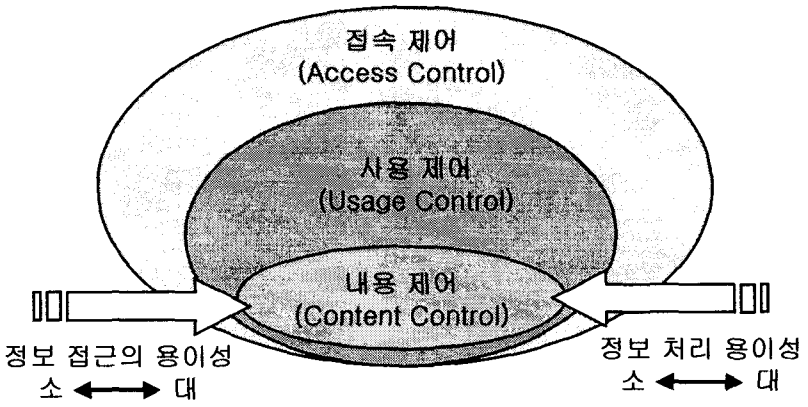
: 지각적으로 감지되지 않는 저작권 정보를 컨텐츠 자체에 삽입

: 암호가 풀린 후에도 소유권을 주장하거나 불법복제를 막을 수 있음.

: 의도적인 공격에 살아 남는 은닉 정보를 삽입하기가 어려움.



디지털 컨텐츠 보호를 위한 요소 기술



* 내용 제어(Content Control, ex. watermark)는 "last line of defense".

보안(Security) 기술

- 요구기능
  - 기밀성(confidentiality)
    - 전달내용을 제3자가 획득하지 못하도록 함
  - 인증 (authentication)
    - 메세지를 보내오는 사람의 신원을 확인
    - 상품대금으로 카드번호가 전달될 경우 실제 카드소유자 확인
  - 무결성 (integrity)
    - 정보전달 도중에 정보의 훼손 여부를 확인
  - 부인방지(non-repudiation)
    - 정보제공자가 정보제공 사실을 부인하는 것을 방지
    - (예) "갑에게 100만원을 지불하겠다" 라는 메시지를 보낸 후, 나중에 부인하는 것을 방지할 수 있어야 함.

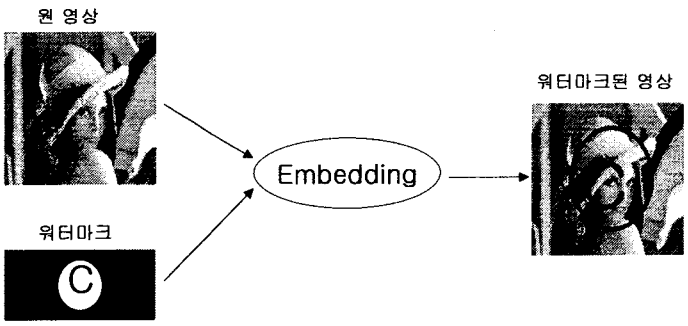
암호화(cryptography) 기술

- 정의
  - Network의 보안상 취약점을 극복하기 위한 방법
  - 보다 안전한 컨텐츠의 전달 및 유통을 위한 알고리즘 기술

- 암호화 기술의 분류
  - 비밀 알고리즘 기반 기술 (*Restricted Algorithm*)
    - 알고리즘이 노출되면 위험: 노출되면 다른 알고리즘 교체
    - 예: 구성원 퇴직으로 인한 노출
    - 안정성 취약
  - 공개 알고리즘 기반 기술 (*Key-Based Algorithm*)
    - 암호화 방법은 공개 , 키(key)를 알아야 복호화 가능
    - key: 매우 큰 숫자중 하나
    - keyspace : 가능한 키값의 범위
    - 분류 : 대칭키 알고리즘, 비대칭키 알고리즘

워터마킹(Watermarking) 기술

- 원신호에 필요한 또는 원하는 은닉 정보(워터마크)를 삽입하는 기술
- 원신호의 정보손실이 없어야 하고, 은닉 정보는 외부의 제어(공격)에 손실되지 않아야 함.

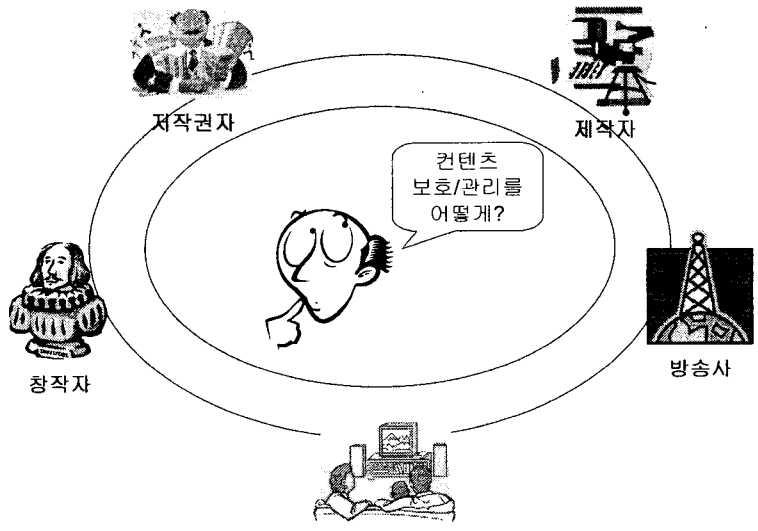


(비디오 워터마킹 삽입의 예)

프로젝트 및 표준화 동향

- 컨텐츠 식별 기술(**ISBN, URI, URN, DOI...**)
  - 컨텐츠에 유일한 식별자를 부여(similar to barcode)
- 메타데이터 기술(**INDECS, XrML, ODRL...**)
  - 컨텐츠 타입 정보, 저작권 정보, 및 사용 권리에 대한 명세 체계
- **IPMP** 관련 기술(**CAS, TALISMAN, OKAPI, OPIMA, cIDf, TV-Anytime, MPEG 4/7/21...**)
  - 식별 기술과 메타데이터 기술 등을 기반으로 저작권 보호 및 관리를 할 수 있는 시스템
- **DRM** 관련 기술(**Intertrust, ContentGuard, MS, Digimarc, W3C...**)
  - 컨텐츠 보호, 관리, 인증 기술 등을 기반으로 컨텐츠 유통을 제어할 수 있는 시스템

방송 환경에서의 고려사항



접근 방식

- **디지털 방송의 특성에 대한 분석**
  - 미래 서비스에 대한 고려
  - 인터넷 전송 과 방송 환경의 차이점 분석
- **보호 및 관리가 무엇인가?**
  - 방송에서의 보호/관리를 위한 필요 기능에 대한 정의
- **방송 환경에서의 보호 관리 프레임워크 기본 모델**
  - 참여자간의 상호 관련성 파악
  - 요소 기술의 구성
  - 상위 레벨에서의 설계
- **요소 기술, 통합 기술 개발**

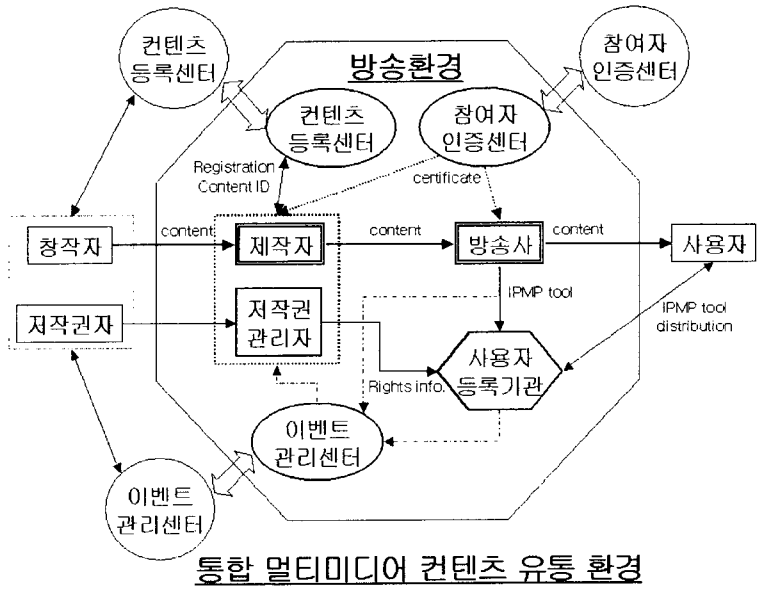
방송 환경의 특징

- **전송 규격이 결정되어 있다.**
  - 디지털 지상파 방송: ATSC
  - 디지털 위성 방송: DVB
  - 비디오 (MPEG-2 video), 오디오 (AAC, AC-3) 등
- **상대적으로 넓은 대역폭을 지닌다.**
  - 1HDTV channel ~ 10Mbps ~ 6MHz
  - 고용량, 고화질, 고품질 데이터
  - 다양한 컨텐츠 (n-channel Video/Audio, Text, Metadata)
- **'방송'은 'one-to-many' 로 컨텐츠 전달이 이루어 진다.**
  - Internet: one-to-one
  - 방송 stream에 대한 접속 제어가 사실상 불가능

방송 환경에서의 보호/관리 기능

- 미래형 서비스 들에 대한 고려
- 참여자 인증
- 컨텐츠 식별
- 신뢰할 수 있는 컨텐츠 전달 방법
- 신뢰할 수 있는 메타데이터 취급 방법
- 사용자의 보호/관리 방법 이용에 관한 방법
- 저작권 정보 표현/저장/관리/인증 방법
- 표준화된 인터페이스
- 참여자 개별적 컨텐츠 보호/관리
- 투명한 이벤트 보고
- 이용자 인증 방법

보호 및 관리 프레임워크 모델



통합 멀티미디어 컨텐츠 유통 환경

MOSES Project

(MPEG Open Security for Embedded Systems)

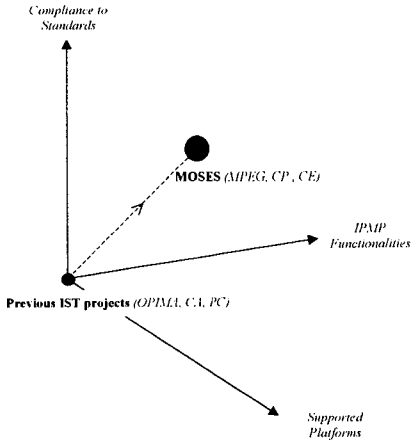
- ▶ EU IST Project (2002 – 2003)
- ▶ IST-11443 OCCAMM Project의 후속 과제
- ▶ *Extending the OPIMA interfaces and architecture to achieve compliance with the most recent security standards*, some of which are still in the making, like MPEG IPMP Extensions and DVB-CP
- ▶ *Expanding the scope as regards business models to encompass operational scenarios* where the full set of functionalities pertaining to IPMP systems is implemented and tested, including means for controlling copying, moving, exporting and importing protected content as well as the relevant business and service data
- ▶ *Porting legacy secure infrastructures to devices other than the PC*, addressing typical CE platforms like mobile terminals and set-top boxes

(OCCAMM ***: Open Components for Controlled Access to Multimedia Material)***

MOSES Project : Consortium Members

- Central Research Laboratories Ltd (CRL) – United Kingdom
- Telecom Italia Lab S.p.A. (TILAB) – Italy
- Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática (ADETTI) – Portugal
- Integrate Systems Laboratory of École Polytechnique Fédéral de Lausanne (EPFL) – Switzerland
- Electronics and Telecommunications Research Institude (ETRI) – South Korea
- Avanti Communications Ltd (Avanti) – United Kingdom
- L'Editrice del Vascello (EdV)– Italy

MOSES Project Scope



BroadcastingMedia TechnologyDepartment

결언

- 디지털 방송 컨텐츠의 중요성과 보호 및 관리의 필요성
- 디지털 방송 컨텐츠 보호 및 관리의 발전 방향

  ⇒ 강인한 내용 제어(워터마크) 기술 개발

  ⇒ 내용제어, 접속제어 및 사용 제어의 결합
- 디지털 방송 환경을 고려한 보호 및 관리 기술 필요

- 미래 디지털 정보 서비스의 성공은 다양한 디지털 컨텐츠에 달려있고, 다양한 디지털 컨텐츠의 창출, 제작, 보급. 이용은 그것의 보호 및 관리에 의해 좌우된다.

  그러므로, 디지털 정보 서비스의 성공은 디지털 컨텐츠의 보호 및 관리에 의해 이루어진다.

BroadcastingMedia TechnologyDepartment