디지털 방송 콘텐츠 보호 유통 시스템 설계 및 구현

이 혜 주[†] · 최 범 석[††] · 홍 진 우[†††] · 석 종 원[††††]

요 약

디지털 콘텐츠의 이용 증가와 함께 디지털 콘텐츠의 저작권 보호 및 유통이 점점 부각되고 있으며 이를 위한 디지털 저작권 관리(DRM, digital rights management) 기술은 다양한 종류의 디지털 콘텐츠 뿐만 아니라 저작권 권리를 보호하기 위해 적용 가능하다. 뿐만 아니라, 디지털 방송 기술 도입과 개인용 비디오 녹화기와 같은 저장 장치의 등장으로 저장되는 디지털 방송 콘텐츠에 대한 보호 기술도 요구되어 지고 있다. 현재 방송 콘텐츠에 대한 보호 방법은 특정 채널에 대한 시청자의 접근을 제어하는 제한 수신 시스템(CAS, conditional access system)으로, 이것은 디지털 방송 콘텐츠의 자유로운 콘텐츠 2차배포를 제한시킨다. 본 논문에서는 불특정 다수를 대상으로 방송되는 방송 콘텐츠에 대한 저장과 사용을 제어하고 자유로운 2차배포(superdistribution)를 허용하기 위해 암호화와 라이센스를 이용하는 DRM의 개념을 적용하고, 각 부분들의 기능 검증을 위한 구현 결과를 보인다. 본 논문의 구현 시스템은 시청자의 STB(Set-top box)에 방송콘텐츠의 녹화를 허용하고, 사용자에 의한 2차배포가 가능하다는 장점이 있다. 따라서, 콘텐츠 제공자와 소비자 모두에게 신뢰성 있는 콘텐츠 보호 및 유통환경을 제공가능하다.

Design and Implementation of a Protection and Distribution System for Digital Broadcasting Contents

Hyejoo Lee[†] · BumSeok Choi[††] · Jinwoo Hong[†††] · Jongwon Seo[††††]

ABSTRACT

With the increase of digital content usages, the protection for digital content and intellectual property becomes more important. The DRM(digital rights management) technologies are applicable to protect not only any kind of digital contents but also intellectual property. Besides such techniques are required for recorded digital broadcasting contents due to introduction of digital broadcasting techniques and storage devices such as personal video recorder. The conventional protection scheme for broadcasting content is the CAS(conditional access system) by which the access of viewer is controlled on the specific channels or programs. The CAS prohibits the viewer from delivering the digital broadcasting content to other person, so it results in restriction of superdistribution on the digital broadcasting content. In this paper, for broadcast targeting unspecfic many people, we will design the service model of the protection and distribution of digital broadcasting content using encryption and license by employing the concept of DRM. The results of implementation are also shown to verify some functions of each component. An implemented system of this paper has some advantages that the recording of broadcast content is allowed on set-top-box and superdisttribution is available by consumer. Hence it provides content providers and consumers with trustworthy environment for content protection and distribution.

키워드 : 디지털방송콘텐츠(Digital Broadcasting Contents), DRM, 라이센스(License), 패키징(Packaging), 2차배포(Superdistribution), 유통(Distribution)

1. 서 론

디지털 콘텐츠 사용 증가와 함께 불법 사용에 대한 디지털 콘텐츠 및 저작권 보호의 중요성이 부각되고 있다. 콘텐츠 보호를 위해 암호화, 전자서명, 인증 등과 같은 암호학적 기법[1-3]을 이용한 전통적인 방법에서 워터마킹[4-6], DRM 기술[7-8] 등 다양한 보호 기술들이 제안되어 왔다. 지금까지 콘텐츠 보호의 대상은 MP3와 같은 인터넷에서 유통되는 콘텐츠, 혹은 DVD와 같은 기록매체를 통하여 유통되는 콘텐츠들이 대표적이다. 최근에는 디지털 방송의 도입으로 고선명(high definition, HD) 콘텐츠의 방송과 개인용 비디오 녹화기(personal video recorder, PVR)와 같은 디지털 저장 매체의 개발로 인하여 고화질의 디지털 방송 콘텐츠 저장이 가능함에 따라 디지털방송 콘텐츠 보호의 중요성이 증가되고 있다. 그 결과로 MPEG 표준화 그룹에서는 MPEG-2 TS(transport stream)와 PS(program stream)에 대해 워터마킹, 암호화와 같은 보호 툴 등을 적용할 수 있는 MPEG-2 IPMP(in-

※ 본 논문은 정보통신부 지원 대형국책사업인 "지능형통합정보방송(Smart TV) 기술개발" 과제의 일환으로 작성되었기에 관계자 여러분에게 감사의 뜻을 드립니다.
† 정 회 원 : 한국전자통신연구원 방송미디어연구그룹 선임연구원
†† 정 회 원 : 한국전자통신연구원 방송미디어연구그룹 연구원
††† 정 회 원 : 한국전자통신연구원 방송미디어연구그룹 그룹장(책임연구원)
†††† 정 회 원 : 창원대학교 교수
논문접수 : 2004년 4월 1일, 심사완료 : 2004년 8월 25일

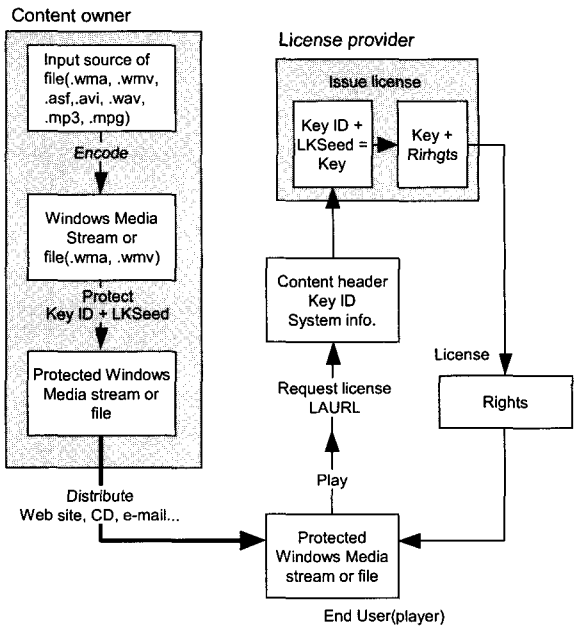
tellectual property management protection)[9]를 표준화하였으며, 미국FCC(federal communications commission)는 2005년 7월까지 DTV 신호를 수신하는 모든 장치에 '방송깃발(broadcast flag)'를 장착하는 법안을 승인하였다[10]. 이외에도 디지털 방송 콘텐츠에 대한 접근제어, 복사방지 등에 대한 많은 연구가 이루어지고 있다[11-16].

본 논문은 시청자가 방송 콘텐츠를 단지 시청하고 끝나는 것이 아니라 자신의 PVR에 방송 콘텐츠를 저장하고 이를 홈 네트워크, 인터넷과 같은 네트워크를 통해 자유롭게 이용할 수 있도록 하면서 콘텐츠를 보호하기 위한 서비스 모델을 설계하고 이를 구현한다. 즉, 디지털 방송 콘텐츠 유통 서비스 모델의 하나로써 녹화된 콘텐츠의 재생시에 사용료를 부과하는 모델을 제안한다. 시청자들은 방송 중인 콘텐츠를 시청할 수 있으나, 녹화된 콘텐츠를 다시 재생을 하고자 하는 경우 콘텐츠 이용에 따른 사용료를 지불하도록 한다. 이러한 비즈니스 모델을 고려하는 경우에, 방송사는 방송 콘텐츠 내에 방송 콘텐츠 유통 서비스를 위한 데이터들을 다중화하여 전송하여야 하고, 다중화된 데이터들을 기반으로 STB(set-top-box)에는 암호화를 포함한 패키징 및 유통 제어 모듈이 제공되어야 한다. 또한, 네트워크 또는 저장매체를 이용한 저장된 디지털 방송 콘텐츠의 2차배포(super-distribution)도 고려되어야 한다.

본 논문에서는 위의 디지털 방송 콘텐츠 보호 및 유통 서비스를 제공하기 위해 콘텐츠 제작자, 방송사, STB, 유통서버로 구성된 방송 콘텐츠 보호 및 유통 시스템을 제안한다. 논문의 구성은 다음과 같다. 먼저 2장에서는 콘텐츠 보호기술의 소개 및 제안하는 디지털 방송 콘텐츠 유통 서비스에 대해 간략하게 기술한다. 그리고, 3장에서는 제안한 방송 콘텐츠 유통 서비스를 위한 방송사, 시청자, 그리고 STB간의 상호 흐름과 각 단계에서 필요한 기능들을 기술한다. 4장에서는 방송 콘텐츠 보호 및 유통 시스템을 구성하는 각 부분들의 기능 검증을 위한 구현 결과를 나타내고, 결론으로써 5장에서는 디지털 방송콘텐츠 유통 서비스를 위한 향후 고려사항을 기술한다.

2. 디지털 방송 콘텐츠 보호 및 유통 서비스

콘텐츠 보호 기술은 크게 복제방지 기술, DRM, 제한 수신시스템(conditional access system, CAS)으로 분류될 수 있다[11]. 복제 방지 기술은 장치간에 전송되는 콘텐츠의 불법 복제를 방지하는 기술로 주로 CD, DVD와 같은 기록매체에 적용되고, 다양한 권한 제어가 불가능하다. 또한, DRM 기술은 다양한 콘텐츠에 대해 권한제어 및 유통 제어가 가능하다. 대표적으로 Microsoft의 WMRM(windows media rights management) 방식[18]은 다음과 같은 DRM 절차로 이루어진다.

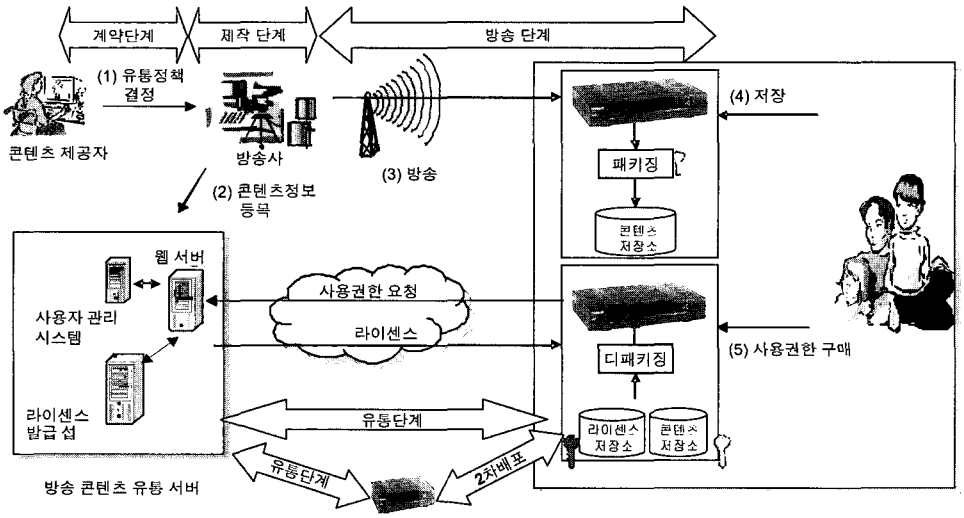


(그림 1) WMRM의 DRM 과정

(그림 1)에서와 같이 콘텐츠 소유자는 윈도우즈 미디어 스트림 또는 파일을 Key ID와 LKSeed를 이용하여 암호화하여 이를 배포하고, 사용자가 콘텐츠를 재생할 때 라이센스 제공자에게 라이센스를 요청하여 라이센스를 얻게 된다. 그러나, DRM 기술들은 규격이 표준화되지 않아 상호운용성(interoperability)이 불가능하다. 마지막으로 다양한 콘텐츠를 대상으로 하는 앞의 방법과 달리 방송 콘텐츠를 보호하기 위한 특정 기술인 CAS는 특정 채널이나 프로그램에 대해 허가된 시청자에게만 접근을 허용하는 시스템으로 스크램블(scramble)을 이용한 접근 제어 및 가입자 관리 시스템을 기반으로 이루어진다[15-16]. 특히 스크램블된 콘텐츠는 동일한 CAS가 적용되는 특정 단말에서만 이용가능하여 2차배포를 허용하지 않는다. 이것은 사용자의 콘텐츠 배포, 공유 등 다양한 서비스를 제공하는 것이 쉽지 않게 한다. 이러한 경우를 고려하여 방송되는 콘텐츠가 시청자의 STB에 저장되고 2차배포되는 것을 가정한 방송 콘텐츠 보호 및 유통 서비스를 제안한다.

전체 디지털방송 콘텐츠 보호 및 유통 흐름은 계약단계, 제작단계, 방송단계 그리고 유통단계로 구성되며, 참여자들은 콘텐츠 제공자, 방송사, 유통서버, 그리고 STB로 분류될 수 있다. (그림 2)는 전체 방송 콘텐츠 보호 및 유통 서비스의 흐름을 나타내고 있다.

(그림 2)에 나타난 바와 같이, 계약 단계는 콘텐츠 제공자가 방송사에게 콘텐츠를 제공함과 동시에 방송 콘텐츠에 대한 유통 정책을 결정하는 단계로써, 시청자의 콘텐츠 저장 가능 여부(저장제어정책), 그리고 사용권한 및 조건(사용정책), 지불 정책 등이 유통정책에 포함된다. 특히 PVR의 저장에 대한 제어 정책은 <표 1>과 같이 분류될 수 있다.



(그림 2) 방송 콘텐츠 보호 및 유통 서비스

〈표 1〉 방송 콘텐츠 저장을 위한 저장제어 정책

형 태	의 미
시청 가능, 무료 사용	◦ 방송 콘텐츠의 시청과 저장이 가능 ◦ 저장된 콘텐츠에 대한 이용시 사용권한의 획득 불필요
시청 가능, 유료 사용	◦ 방송 콘텐츠의 시청과 저장이 가능 ◦ 저장된 콘텐츠에 대한 이용시 사용권한의 획득 필요
시청 가능, 저장 불가	◦ 방송 콘텐츠의 시청만 가능 ◦ 방송 콘텐츠의 저장이 불가능한 경우

콘텐츠 제작 단계는 방송사가 콘텐츠 제공자로부터 콘텐츠를 제공받아 자막 삽입, 더빙 작업 등을 수행하여 최종 디지털 방송 콘텐츠를 제작하는 단계이다. 이 단계에서 콘텐츠 제작시 보호방법의 하나로써 워터마킹, 핑거프린팅 혹은 암호화, MPEG-2/4 IPMP와 같은 다양한 보호 방법들을 적용할 수 있다. 콘텐츠 제작이 완료되면, 방송사는 방송 콘텐츠 유통 서비스를 위해 콘텐츠 정보를 비롯한 유통 정책들을 유통 서버에 등록하고, 시청자의 STB에서 콘텐츠 저장, 사용을 제어할 수 있는 보호관리 데이터를 방송 스트림에 다중화하여 콘텐츠를 방송하는 콘텐츠 방송 단계를 거친다. 이때, 시청자의 콘텐츠 저장 요청시 STB는 방송 스트림의 저장제어 데이터를 역다중화하여 콘텐츠 저장을 제어하게 된다. 마지막으로 콘텐츠 유통 단계는 시청자가 저장된 콘텐츠를 재생하고자 할 때, 라이센스 유무 검증 및 발급 절차를 거쳐 콘텐츠를 이용할 수 있는 단계를 의미한다.

방송 콘텐츠를 위한 보호 및 유통 서비스를 위한 시스템 구성 및 기능을 다음 장에서 상세히 기술한다.

3. 방송 콘텐츠 보호 유통 시스템 구성 및 기능

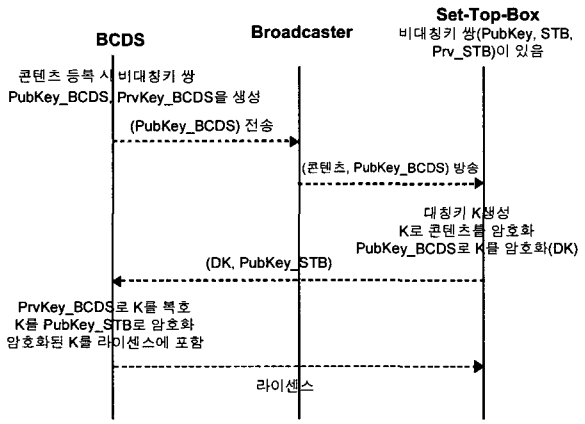
방송 콘텐츠 보호 및 유통 시스템은 A/V TS에 보호 및 유통을 위한 보호관리 데이터의 다중화를 위한 재다중화 시스템, 라이센스 발급을 위한 방송콘텐츠 유통서버(broadcasting content distribution server, BCDS), 그리고 보호 및 유통 관리 모듈이 있는 STB로 구성된다. 콘텐츠 제공자와 유통정책을 결정한 방송사는 콘텐츠 유통 서비스를 제공하는 유통 서버에 콘텐츠 정보를 비롯한 유통 정보를 등록하고, 콘텐츠의 저장 및 유통 보호관리 데이터를 MPEG-2 TS에 다중화하여 방송하는 기능을 제공해야 한다. BCDS는 콘텐츠 정보 관리, 라이센스 발급 등의 기능을, STB의 보호 및 유통관리 모듈은 콘텐츠의 저장을 제어하고 콘텐츠를 암호화하여 패키징하는 기능과 패키징된 콘텐츠의 재생시 사용권한, 즉 라이센스의 유무 검증, 라이센스 발급 및 처리 기능들을 각각 제공하여야 한다. 각 기능에 대한 상세한 내용을 다음에 기술한다

3.1 키 전달 방법

DRM 방식에서 암호화된 콘텐츠를 풀 수 있는 키 전달방식 중에서 동봉(enveloping) 방식이 있다. 이 방식은 콘텐츠를 암호화하고 복호화 키를 콘텐츠 내에 포함시켜 전달하는 방법으로 비대칭 공개키를 이용하여 복호화 키를 암호화하기 때문에 안전성이 제공된다. 대표적인 DRM 기술 중에서 IBM의 Cryptoloe[17]과 Microsoft의 WMRM[18]이 이러한 방식을 이용하고 있다. 제안 방식의 키 전달 방법도 이와 같은 동봉 방식을 이용하지만, 콘텐츠가 서버에서 암호화되어 전달되는 대신에 콘텐츠의 암호화는 단말에서 수행되어진다.

라이센스에 의한 콘텐츠 사용제어를 위해 콘텐츠의 복호화 키는 라이센스에 포함되어야 하는데, STB의 보호 및 유통관리 모듈은 라이센스에 포함시킬 키 값을 BCDS만이 복호가능하도록 안전하게 전달하기 위해 아래와 같은 방법을 적용한다.

라이센스를 구매하지 않은 시청자의 콘텐츠에 대한 접근을 방지하기 위해 STB의 암호모듈은 대칭키 암호 키를 생성하여 콘텐츠 암호화를 수행한다. 이때, 복호키가 포함된 라이센스를 발급 받기 위해서는 암호화에 이용한 생성 키를 BCDS로 전달하여야 한다. (그림 3)과 같이 비대칭키 방식을 이용한 키 전달 방법을 이용하여 STB에서 BCDS로 안전하게 복호키를 전달한다.



(그림 3) 방송 콘텐츠 유통 서비스에서의 키 전달 방식

즉, STB는 대칭키 암호화 키 K를 이용해서 방송된 콘텐츠를 암호화하고, 콘텐츠와 함께 전송된 BCDS의 공개키 PubKey_BCDS로 키 K를 암호화하여 저장한다(이 값을 DK라 한다). 라이센스 발급 요청시 이를 BCDS로 전송하면 비밀키 PrvKey_BCDS를 가진 BCDS만이 복호화가 가능하므로, 안전하게 키 K를 유통서버로 전달할 수 있다. 뿐만 아니라, BCDS는 라이센스 발급시 키 K를 STB의 공개키로 암호화하여 라이센스에 포함시킴으로써 라이센스를 발급한 STB에서만 콘텐츠를 복호할 수 있도록 STB에 전달가능하다.

3.2 콘텐츠 정보의 등록

콘텐츠 정보의 등록은 콘텐츠에 대한 유통 정책과 키 생성 등을 위해 필요하다. 따라서, 콘텐츠를 제작한 방송사는 <표 2>와 같은 콘텐츠 정보를 포함한 유통 정책들을 BCDS에 저장하게 된다.

<표 2> 콘텐츠 등록 정보의 종류

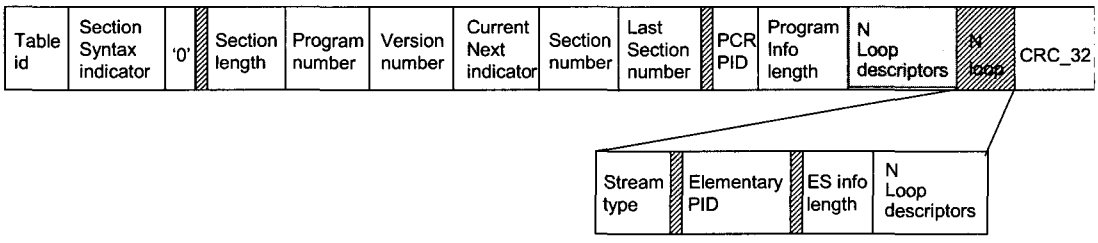
항 목	비 고	
콘텐츠 정보	제목, 장르, 형태, 콘텐츠 ID, 제작년도, 기타	
사용정책	사용권한	재생
	사용조건	횟수제한, 기간제한
과금 정보	사용료	
창작자 정보	[개인] 이름, 주소, 주민등록번호, 연락처, 기타 [업체] 업체명, 주소, 사업자번호, 대표자 성명, 연락처, 기타	
방송사 정보	방송사명, 주소, 사업자번호, 대표자 성명, 연락처, 기타	
저작권 정보	저작권자, 저작물 등록번호, 저작물 등록일자	

특히, 콘텐츠 사용에 대한 사용정책 및 과금 정보는 시청자의 라이센스 발급 요청 시에 시청자에게 제공 되어 시청자가 원하는 사용권한을 선택할 수 있도록 한다. 콘텐츠 정보의 등록이 완료되면 BCDS는 앞에서 기술한 키 전달을 위해 비대칭키 쌍 (PubKey_BCDS, PrvKey_BCDS)를 생성하고, 콘텐츠 ID와 함께 공개키 PubKey_BCDS를 다중화하기 위해 방송사에게 전송한다.

3.3 방송 스트림 다중화

방송사는 BCDS로의 콘텐츠 등록을 끝낸 후, 방송콘텐츠의 저장 및 유통 제어를 위한 보호관리 데이터들을 MPEG-2 TS(transport stream)에 다중화해야 한다. MPEG-2 TS는 4바이트의 헤더와 184바이트의 유료부하(payload)로 이루어진 188바이터의 TS 패킷들로 구성된다. TS 패킷은 프로그램에 관련된 정보를 포함하는 PSI(program specification information) 정보와 A/V(audio/video) ES(elementary stream)를 포함하거나 혹은 private section을 구성하는 패킷들로 이루어진다. 특히 PSI 정보 중에 (그림 4)와 같은 PMT(program map table)는 프로그램에 대한 정보를 포함하고 있는 서술자(descriptor)들이 기술되어 있다.

보호관리 데이터에 대한 정보들은 'N loop descriptors' 중의 서술자로 기술한다. 먼저, <표 1>의 저장 제어 정책을 지원하기 위해 방송사는 저장 제어를 위한 제어비트로 <표 3>과 같이 2비트의 값으로 표현가능하다.



(그림 4) PMT section 구조

〈표 3〉 저장 제어 비트

비트값	의 미	해당 정책
00	누구든지 저장가능한 콘텐츠임을 지시하며, 녹화 이후 라이센스 발급이 필요없음을 지시함	시청 가능, 무료 사용
01	이미 저장된 콘텐츠로, 라이센스의 발급 요구	시청 가능, 유료 사용
10	저장 가능한 콘텐츠이며, 저장 후 사용하기 위해서는 라이센스가 필요한 콘텐츠로 저장시 암호화 되어야 함을 지시함	
11	콘텐츠 녹화가 불가능한 콘텐츠임을 지시함. 시청자에게 녹화불가능함을 표시함	시청 가능, 저장 불가

<표 4>는 위의 저장 제어 비트를 PMT 내의 기술자로 나타내기 위한 신택스 구조로써 2비트의 storage_control_info 필드가 <표 3>의 저장제어 비트의 "00", "10", "11" 중 하나의 값을 포함한다.

〈표 4〉 저장 제어를 위한 기술자의 신택스

신 택 스	Size

storage_control_descriptor() {
descriptor_tag
descriptor_length
reserved('000')
storage_control_info
retention_state_info
}
	
	8 bsblf
	8 bsblf
	3 bsblf
	2 bsblf
	3 bsblf

STB는 이 storage_control_info 필드를 역다중화하여 저장제어를 수행하는데, 특히 "10"의 storage_control_info 필드는 저장시 "01"의 값으로 변경하여 라이센스가 필요한 콘텐츠임을 표시한다.

저장된 콘텐츠에 대한 라이센스 요청을 위해 필요한 콘텐츠 ID, BCDS의 URL, PubKey_BCDS 등 유통 보호관리 데이터는 <표 5>의 신택스 구조로 구성된다.

〈표 5〉 패키징을 위한 기술자의 구조

신 택 스	Size

packaging_desciptor() {
descriptor_tag
descriptor_length
content_info_length
content_info()
tmall _server_info_length
tmall_server_info()
inclKeydata
If (inclKeydata){
reserved
Keydata_length
Keydata
}
else {
reserved
Keydata_PID
}
}
	
	0×91
	8 uimsbf
	8 uimsbf
	8 uimsbf
	
	8 uimsbf
	1 bsblf
	
	3 bsblf
	12 bsblf
	
	2 bsblf
	13 bsblf

STB에서의 패키징 및 라이센스 발급 요청시 필요한 정보들을 기술하는 packaging_descriptor는 콘텐츠 ID를 비롯한 콘텐츠에 대한 정보를 포함한 content_info() 필드, 라이센스 발급 요청시 연결을 위한 BCDS의 URL을 비롯한 유통서버에 대한 정보를 포함한 tmall_server_info() 필드, 그리고 앞에서 기술한 키 전달을 위한 유통서버의 공개키 PubKey_BCDS를 포함한 Keydata 필드 등이 포함된다. 특히 inclKeydata 필드가 '1'인 경우에는 앞에서 설명한 키 전달을 위한 공개키 PubKey_BCDS가 packaging_descriptor()에 직접 포함이 되지만, '0'인 경우에는 키를 MPEG-2 TS의 private section으로 전달하고, 이 private_section의 PID가 Keydata_PID 필드에 포함된다. 이것은 여러가지 기술자들이 PMT에 기술되어 PMT의 길이가 긴 경우를 대비한 것이다.

3.4 콘텐츠 패키징

시청자가 방송되는 콘텐츠를 저장하기 위해 녹화버튼을 눌렀을 때, STB는 storage_control_descriptor()를 PMT에서 추출하여 녹화가능한 콘텐츠인지, 그리고 녹화가능하면서 암호화가 필요한지를 검사한다. 만일, storage_control_info가 "10"인 경우, 암호화하고 패키징하여 저장하기 위해 STB의 암호모듈은 대칭키 암호화를 위한 암호화 키 K를 생성하고, 방송되는 MPEG-2 TS를 암호화하여 패키징한다. 패키징 결과의 형태를 콘테이너(container)라고 하였을 때, 콘테이너는 (그림 5)와 같이 헤더(header), 바디(body), 서명(signature)부로 이루어진다.

```
Container {
 Header {
   Version
   Content_id_information
   isFree = 1
   Body_info
}
Body {
  content_TS
 }
 Signature
}
```

(a) 무료의 경우

```
Container {
 Header {
   Version
   Content_id_information
   isFree = 0
   Server_url_information
   Key_information
   Body_info
 }
Body {
  Encrypted_Content_TS
 }
Signature
}
```

(b) 유료의 경우

(그림 5) 패키징의 구조

콘테이너는 콘텐츠의 유무료 여부에 따라 다른 구조를 가진다. 콘텐츠가 무료인 경우, 콘테이너의 헤더는 콘테이터 버전정보를 나타내는 'Version' 필드, 콘텐츠 ID의 정보를 포함하는 'Content_id_information' 필드, 콘텐츠의 무료를 나타내는 "isFree=1"과 바디에 포함된 TS의 길이를 나타내는 Body_info 필드가 포함된다. 그리고 콘테이너의 바디는 암호화되지 않은 TS가 그대로 저장된다. 이와 반대로 콘텐츠가 유료인 경우, 콘테이너의 헤더는 'isFree'=0의 값으로 지정되면서 이하 필드가 추가된다. 즉, packaging_descriptor()로부터 추출한 라이센스 획득을 위한 BCDS의 URL을 포함

하는 'Server_url_information' 필드, 콘텐츠 복호화 키를 전송하기 위한 DK 값이 포함되는 'Key_information' 필드가 추가된다. 또한, Body_info 필드는 TS의 길이 정보와 함께 암호화 알고리즘에 대한 정보를 나타내는 'Encryption_Algo_information' 필드가 추가로 포함된다. 그리고 콘테이너의 바디에는 암호화된 TS가 저장된다. 마지막 콘테이너의 서명부는 무결성 체크를 위한 PrvKey_STB로 메시지 M= [Header | TS 중 1Kbyte]을 서명한다.

3.5 라이센스의 획득

사용 권한, 즉 라이센스의 획득은 앞에서 기술한 바와 같이 콘텐츠 저장 이후에 이루어진다. 콘텐츠의 저장이 "유료사용" 정책에 의해 이루어질 때, 단말은 콘텐츠 암호화를 수행함으로써 라이센스를 구매하지 않은 시청자의 콘텐츠 접근을 방지한다. 즉, 3.1에서 기술한 바와 같이 STB는 암호화 키 K를 생성하여 암호화를 수행한 후, 다중화되어 전송된 유통서버의 공개키 PubKey_BCDS를 이용하여 키 K를 암호화하여 콘테이너 헤더의 'Key_information' 필드에 포함시킨다. 유통서버의 공개키로 K를 암호화한 결과를 DK라고 할 때, 라이센스 획득을 위해 STB는 유통서버에 (콘텐츠 ID, DK, PubKey_STB)를 유통 서버에 전달하게 된다. 3개의 파라메터를 전달받은 유통서버는 콘텐츠 ID를 이용하여 콘텐츠 정보를 검색하고, 검색된 콘텐츠에 대한 정보 등을 시청자에게 제공한다. 사용자가 구매하고자 하는 사용권한을 선택하고 지불 정보들을 입력하면, BCDS는 라이센스 발급을 위해 라이센스를 생성하기 위해 전달받은 DK로부터 BCDS의 개인키 PrvKey_BCDS를 이용하여 복호화를 위한 키 값 K를 복호한다. 이 키 값 K는 오직 라이센스를 구매한 STB에서만 복호할 수 있도록 PubKey_STB로 암호화하여 라이센스에 포함시켜 STB에 전송한다.

라이센스는 사용권리를 기술한 XML 기반의 XrML(extensible rights management language)[19]으로 구성하였다. 라이센스는 (그림 6)과 같은 구조를 가진다.

사용권한으로 "재생(play)" 권한만, 사용조건으로 "사용기간(validityInterval)", "사용횟수(exerciseLimit)"에 의해 방송 콘텐츠를 이용할 수 있으며, 유통정책에 따라 이러한 사용권한이나 조건은 다양하게 제공가능하다. 콘텐츠 복호화 키는 otherinfo 내에 keyinfo에 포함되어진다.

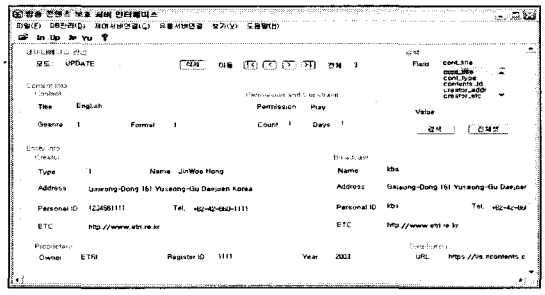
```
<license>
<Inventory> ··· </inventory>
<grant>
  <play/>
 <allconditions>
   <validityInterval> ··· </validityInterval>
   <sx : exerciseLimit> ··· </sx : exerciseLimit>
   <sx : fee> ··· </sx : fee>
 </allconditions>
<otherinfo>
  <metadata> ··· </metadata>
  <keyinfo> ··· </keyinfo>
</otherinfo>
<issuer> ··· </issuer>
<signaure> ··· </signaure>
</license>
```

(그림 6) 라이센스 구조

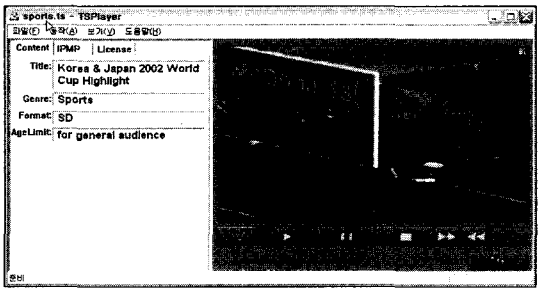
4. 방송 콘텐츠 보호 및 유통 시스템 구현

방송 콘텐츠 보호 및 유통 시스템을 구성하는 각 부분의 기능 검증을 위하여 PC 기반으로 하여 소프트웨어로 구현하였으며, 공격에 대해 각 시스템들은 안전하다고 가정한다.

먼저, 보호 및 유통을 위한 보호관리 데이터의 재다중화 시스템은 XML 문서로 기술된 보호 및 유통 보호관리 데이터를 입력받아 데이터베이스에 저장하고, 메인 A/V TS에 다중화시킨다. (그림 7)은 재다중화 시스템의 사용자 인터페이스로 데이터베이스에 저장된 값들을 검색, 변경 및 삭제 등의 기능이 제공된다.



(그림 7) 보호관리 데이터 다중화 사용자인터페이스



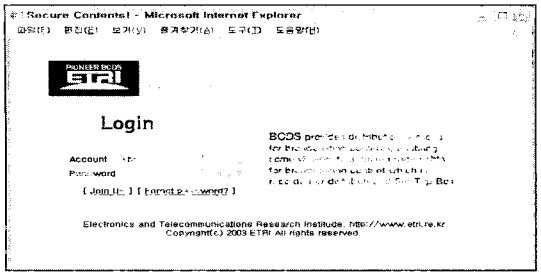
(그림 8) 디지털방송콘텐츠 전용플레이어

(그림 8)은 보호관리 데이터가 다중화된 TS를 콘텐츠 재생 및 녹화를 가능한 전용 플레이어로, 녹화된 콘텐츠를 선택하면 패키징 헤더를 분석하여 라이센스가 필요한 콘텐츠임을 확인하고 라이센스를 검색한 후 라이센스 발급 요청을 수행한다.

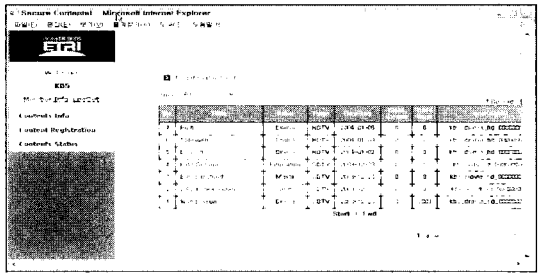
BCDS는 IIS(internet information service) 기반 웹 서버로 구축되며, 그 기능은 사용자 관리, 콘텐츠 관리, 라이센스 발급 및 키 관리, 기타 라이센스 구매 내역 관리 등을 제공한다. BCDS의 사용자는 일반회원(시청자), 방송사, 그리고 관리자로 구성되는데, (그림 9)와 같이 사용자 계정 및 패스워드 확인 방식을 이용하여 사용자 인증을 수행하고 사용자에 따라 서로 다른 웹 화면을 제공하게 된다.

방송사는 콘텐츠 정보 관리 기능인 콘텐츠 등록, 콘텐츠 정보의 변경 등의 기능을 제공받을 수 있다.

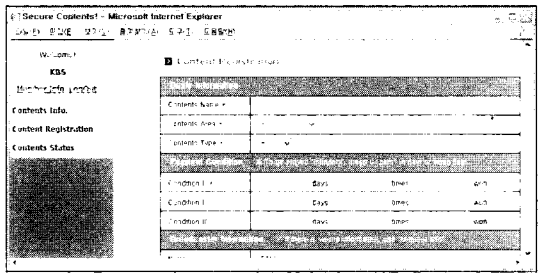
(그림 10)(a)는 현재 등록된 콘텐츠 목록으로, 타이틀의 제목을 선택하면 등록된 콘텐츠의 정보에 대한 상세 정보 및 변경기능을 제공하는 웹 페이지를 제공한다. 그리고 'Content Registration' 메뉴를 선택하면 (그림 10)(b)와 같이 콘텐츠 정보를 등록할 수 있다.



(그림 9) BCDS 사용자 로그인 화면



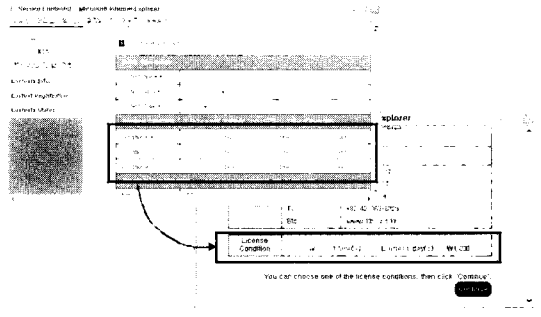
(a) 등록된 콘텐츠 리스트 출력 화면



(b) 콘텐츠 등록 화면

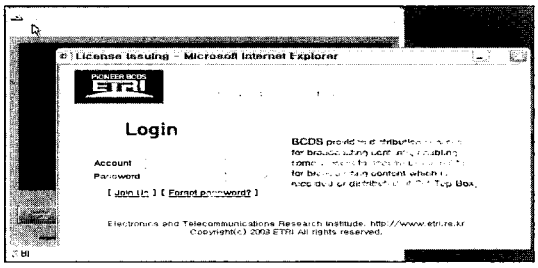
(그림 10) 콘텐츠 등록 화면

BCDS의 가장 중요한 기능은 라이센스 발급 및 라이센스 발급 시 필요한 키 관리 기능이다. 앞에서 기술한 바와 같이 STB에 저장된 콘텐츠를 재생하고자 선택하게 되면 라이센스를 구매하기 위해 BCDS에 접속한다. (그림 11)은 방송사의 콘텐츠 등록 화면의 일부와 라이센스 구매 시 사용자가 사용권한 선택의 일부 화면을 나타내고 있다. 방송사가 콘텐츠 등록 시 사용조건으로 기간(days), 횟수(times), 가격(won)을 등록하면, 라이센스 구매 시 등록한 사용조건을 제공하여 사용자가 사용조건을 선택하도록 한다.

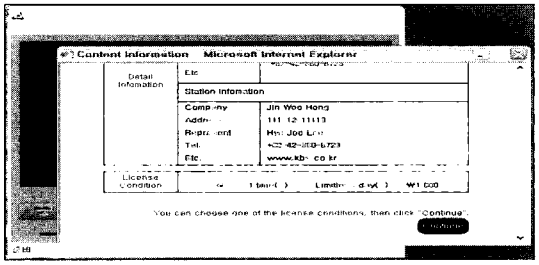


(그림 11) 사용권한 등록 및 사용조건의 지정

시청자가 콘텐츠를 녹화하고 라이센스를 요청하면, STB의 보호 및 유통 관리 모듈은 일단 라이센스가 있는지 확인한다. 라이센스가 없을 경우, 패키징 헤더의 정보를 이용하여 BCDS에 접속하게 된다. (그림 12)는 라이센스 발급 과정으로 BCDS에 접속하여 사용자 로그인을 수행하고 해당 콘텐츠의 사용권한을 선택하게 된다.



(a) 라이센스발급을 위한 사용자 로그인 화면



(b) 사용권한 선택 화면

(그림 12) 라이센스 발급 과정

이 과정 이후에 지불 정보를 입력하고 라이센스를 다운로딩하게 된다.

제안한 방송 콘텐츠 보호 및 유통 시스템의 2차 배포는 콘텐츠를 복호할 수 있는 키 값 DK가 콘테이너 헤더에 포함되어 있기 때문에, 2차 배포된 콘텐츠를 수신한 사용자는 BCDS로부터 동일한 방법으로 라이센스 발급을 요청할 수 있기 때문에 2차 배포가 가능하다.

5. 결 론

콘텐츠 보호에 대한 DRM 기술은 다양한 형태의 콘텐츠를 대상으로 하고 있다. 디지털방송의 도입으로 다양한 서비스를 제공하기 위해 기존의 CAS 이외의 콘텐츠 보호 방법이 필요하게 되었다. 지금까지의 CAS는 시청시의 접근 제어만을 목적으로 적용되었으나, 시청 이후의 방송콘텐츠의 사용을 제어하기 위해서는 다양한 사용권한을 제공할 수 있는 DRM 기술을 적용할 수 있다. 이에 본 논문에서는 디지털 방송 콘텐츠 보호 및 유통을 위해 디지털 방송 콘텐츠의 저장과 2차 배포 가능한 환경을 고려한 시스템을 설계하고 구현하였다. 제안한 디지털 방송 콘텐츠 보호 및 유통 시스템은 보호 및 유통을 위한 보호관리 데이터를 다중화하는 다중화시스템, 방송되는 방송콘텐츠의 녹화 및 사용을 제어하기 위한 패키징을 수행하는 STB의 보호 및 유통 모듈,

그리고 라이센스 발급 등을 위한 유통서버로 구성되며 각 구성시스템의 기능 및 구현 결과등을 기술하였다. 본 논문에서는 기능검증을 위해 PC를 기반한 소프트웨어로 각 구성부분들을 구현하였으며 구현 결과의 시연을 통하여 기술적 검증을 완료하였다.

향후에는 STB의 하드웨어 구현, 사용권한을 분할하여 사용하거나 사용권한을 다른 이에게 양도할 수 있는 기능 등의 고려가 필요하다. 또한 콘텐츠 보호 및 유통을 위해 STB내의 키 유출과 같은 안전성에 대해 고려할 필요가 있다.

참 고 문 헌

[1] 강주성 외, *현대 암호학*, 경문사, 2000.

[2] 이만영 외, *전자상거래 보안 기술*, 생능출판사, 1999.

[3] W. Zeng et al., "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Transactions on multimedia, Vol.5, No.1, pp.118-129, 2003.

[4] J. Cox et al., *Digital Watermarking*, MOGAN KAUFMANN PUBLISHERS, 2002.

[5] S. Katzenbeisser et al., *Information Hiding : techniques for steganography and digital watermarking*, ARTECH HOUSE, 2000.

[6] *Security and Watermarking of Multimedia Contents V*, SPIE Vol. 5020, 2003.

[7] 박용기, "컨텐츠 보호기술 표준화현황과 대응전략", TTA 저널, 제74호, pp.13-22, 2001.

[8] 강호갑, *DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구*, 한국소프트웨어진흥원 연구보고서, 2003.

[9] Information technology-Generic coding of moving pictures and associated audio information, Part 11 : IPMP on MPEG-2 systems, ISO/IEC FDIS 13818-11, 2003.

[10] http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-273A1.pdf.

[11] Broadcast Protection Discussion Group, *BPDG : Final report to CPTWG*, http://www.mpaa.org/cptwg/Assets/BPDG/home%page.htm, 2002.

[12] DVB CPCM Functional Model Definitions and Applications, DVB-CPT, Sept., 2003.

[13] 석종원, 이혜주 외 2명, "디지털 콘텐츠 저작권 보호 및 관리를 위한 방송 서버 시스템", Telecommunications review, 제13권 제5호, pp.746-758, 2003.

[14] TV-Anytime RMP(rights management and protection) Information for Broadcast Applications, TV-Anytime Forum, S-5-1, June, 2004.

[15] *CAS/IPMP 적용 방안연구*, 한국전자통신연구원 최종연구보고서, 2000.

[16] Conditional Access System for terrestrial broadcast, ATSC A/70, 1999.

[17] Marc A. Kaplan, "IBM Cryptolopes, Superdistribution and Digital Rights Management," http://www.research.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html.

[18] http://www.microsoft.com/windows/windowsmedia/drm/default.aspx.

[19] *eXtensible rights Markup Language(XrML) 2.0 specification*, http://www.xrml.org.

이 혜 주

e-mail : hyejoo@etri.re.kr

1994년 부경대학교 전자계산학과(이학사)

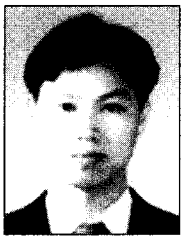
1997년 부경대학교 대학원 전자계산학과 (이학석사)

2000년 부경대학교 대학원 전자계산학과 (이학박사)

2000년~2001년 한국정보통신대학원대학교 박사후 연구과정생

2001년~현재 한국전자통신연구원 방송미디어연구그룹 선임연구원

관심분야 : 멀티미디어 처리 기술, 디지털 콘텐츠 보호 및 관리, 워터마킹



최 범 석

e-mail : bschoi@etri.re.kr

1997년 충남대학교 컴퓨터과학과(이학사)

2001년 충남대학교 대학원 컴퓨터과학과 (이학석사)

2001년~현재 한국전자통신연구원 방송미디어연구그룹 연구원

관심분야 : 입체음향, 디지털 콘텐츠 보호

홍 진 우

e-mail : jwhong@etri.re.kr

1982년 광운대학교 응용전자공학과 (공학사)

1984년 광운대학교 대학원 전자공학과 (공학석사)

1993년 광운대학교 대학원 전자계산기 공학과(공학박사)

1998년~1999년 독일 프라운호퍼연구소(교환연구원)

1984년~현재 한국전자통신연구원 방송미디어연구그룹 그룹장 (책임연구원)

2000년~현재 한국음향학회 교육이사, 뉴미디어음향 학술분과 위원장, 한국방송공학회 학술위원 및 편집위원

관심분야 : 디지털방송 미디어 처리 기술, 디지털 콘텐츠 보호 및 관리, 멀티미디어 프레임워크 기술

석 종 원

e-mail : jwseok@changwon.ac.kr

1993년 경북대학교 전자공학과 학사

1995년 경북대학교 대학원 전자공학과 석사

1999년 경북대학교 대학원 전자공학과 박사

1999년~2004년 한국전자통신연구원 선임연구원

2004년~현재 창원대학교 조교수

관심분야 : 멀티미디어 신호처리, 디지털 콘텐츠 보호 및 관리