Journal of Korea Multimedia Society Vol. 12, No. 7, July 2009(pp. 979-988)

스트리밍 콘텐츠의 초유통을 위한 중계파일 설계 및 구현

김태민[†], 양영규[††]

요 약

디지털 콘텐츠의 불법 복제와 저작권 침해는 디지털 콘텐츠의 산업의 발전을 저해하고 있다. 이러한 문제로 인해 다양한 DRM(Digital Rights Management) 시스템이 개발되고 있다. 그러나 초기 DRM 시스템은 콘텐츠의 사용 권리가 있는 사용자만이 해당 콘텐츠를 접근할 수 있기 때문에 사용자가 다른 사용자에게 콘텐츠를 재배포하는 것은 쉽지 않았다. 이러한 문제를 해결하기 위해 다운로드 콘텐츠에 국한되어 재배포를 위한 초유통 서비스 구조가 출현하였다. 하지만 스트리밍 콘텐츠는 사용자가 직접 스트리밍 서버에 접속하여 콘텐츠를 접근하기 때문에 초유통이 제한되었다. 본 논문에서는 스트리밍 콘텐츠의 초유통을 위한 스트리밍 서버와 사용자를 연결할 수 있는 중계파일을 제안하였다.

Design and Implementation of Relay File for Superdistribution of the Streaming Contents

Tae-Min Kim[†], Young-Kyu Yang[††]

ABSTRACT

Illegal reproductions and subsequent copyright infringement have curtailed development of digital content industry. Many DRM systems have been developed and utilized for this purpose. However, current DRM system allow only authorized user to access the contents, and as such, redistribution to other user without getting license again entails cumbersome process. Currently, super-distribution system which can be used for redistribution of downloaded contents in more streamlined fashion is being widely conducted. But for streaming type content, it is still very difficult to redistribute with super-distribution system because the client must directly connect to streaming server to access the content. Accordingly, a new DRM streaming service structure is required to allow streamed contents to be redistributed as easily as the downloaded contents. In this paper, we proposed the relay file structure that can connect the streaming server and the user for super-distribution of the streaming contents.

Key words: DRM(디지털저작권관리), Copyright(저작권), Streaming(스트리밍), Superdistribution(초유통)

1. 서 론

1990년 후반 이래 인터넷의 속도는 증가되고 고화질의 디지털 콘텐츠가 등장했다. 디지털정보의 편리성으로 디지털 콘텐츠에 대한 수요가 증가하고, 제작 및 유통이 용이함으로서 디지털 콘텐츠의 제작은 더욱 증가되고 있다. 이러한 콘텐츠의 유통의 증가는 전자상거래, 콘텐츠 제작업체, 지불업체 등 다양한 분야의 산업 활성화를 가져오게 될 것이다[1].

그러나 디지털 콘텐츠는 복제, 변형, 불법 유통이 쉽기 때문에 저작권자 및 유통업체의 피해를 가져오고, 수익 창출의 어려움으로 콘텐츠 산업의 심각한

※ 교신저자(Corresponding Author) : 양영규, 주소 : 경기도 성남시 수정구 복정동(461-701), 전화 : 031)750-5660, FAX : 031)750-5662, E-mail : ykyang@kyungwon.ac.kr
접수일 : 2008년 9월 12일, 완료일 : 2009년 5월 26일
[†]준회원, 경원대학교 전자계산학과 박사과정 (E-mail : scc0309@paran.com)
[††]정회원, 경원대학교 컴퓨터미디어학과 교수
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2009-C1090-0902-0040)

문제가 되고 있다. 또한, 인터넷으로 콘텐츠의 유통 및 지불이 이루어지므로 보안상의 문제가 심각하게 대두되고 있다. 따라서 무분별한 불법 유통을 막고, 저작권자 및 유통업체의 수익 분배를 위한 관리시스템이 필요하다. DRM 시스템은 디지털 콘텐츠를 허가된 소비자에게만 안전하게 전달 및 사용 가능하게 하는 시스템으로 디지털 콘텐츠의 문제점들의 해결 방안으로 제시되고 있는 기술이다[1].

DRM 시스템은 일반적으로 서버로부터 콘텐츠를 넘겨받아 소비자에서 분배되며, 프로그램에서 승인된 콘텐츠의 접근을 수행한다. 이러한 DRM 시스템은 전체 시스템을 모니터 할 수 있어야 하며, 시스템과 독립적으로 설계되어야 한다. 또한, 소비자들의 권한을 확인하고, 그들을 감시하는 기능을 가져야 한다[1,2].

DRM 기술은 디지털 콘텐츠 유통 과정에서 발생하는 에이전트 사이의 권리와 신뢰성, 콘텐츠의 안전성 및 재 활용성, 유통의 투명성을 보장하는 종합적인 구조로 정의할 수 있다[3]. 그러므로 DRM은 암호화 기술, 워터마킹 기술, 변조방지 기술을 포함하고 콘텐츠의 가치 사슬을 지원하고 저작권자, 유통업자, 소비자 사이에 신뢰를 제공하지만, 근본적으로 요소 기술이 아니기 때문에, 특정 시스템이 DRM 체계를 갖추었는지 구별하기가 쉽지 않다. 디지털 콘텐츠 시스템이 DRM 체계를 갖추었는지는 몇 가지 관점으로 알 수 있다. 해당 상거래 시스템이 저작권자와 유통업자 사이에 서로 신뢰할 수 있게 구조적인 체계의 지원여부, 유통업자가 소비자 사이에 콘텐츠의 안전한 전송과 사용이 보장여부, 2차 배포 지원여부 등이다[4,5].

DRM 기술이 적용되는 콘텐츠는 문서, 이미지, VOD, 음악 등이 있다. 스트리밍 방식의 콘텐츠는 원본을 서버에 두어 스트리밍 서비스 후 소비자에 콘텐츠가 저장되지 않아 다운로드 콘텐츠에 비해 저작권 침해에 안정적이다. 하지만 스트리밍 방식의 콘텐츠는 유통의 흐름에 둔감하고 2차 배포가 어렵다. 통상 스트리밍 콘텐츠의 2차 배포는 소비자들 사이의 URL 링크 공유, 온라인 광고이기 때문에 2차 유통이 영구적이지 못하고 정적이다. 스트리밍 서비스의 장점을 살리면서 다운로드 콘텐츠와 같이 소비자들 사이의 2차 배포를 가능하게하고, DRM 기술을 적용하여 면허 발급 기능을 통한 서비스를 통해 스트리밍 콘텐츠의 저작권 보호와 유통의 활성화를 이룰 수 있다.

본 논문에서는 스트리밍 콘텐츠의 초유통 구조를 가능하게 할 수 있는 중계파일인 SDI(Streaming Distribution Information)의 구조를 설계하여 구현하였고, DRM 시스템을 구현하여 SDI를 통한 서비스를 설명하였다. 논문의 구성은 2장에서 DRM 기술의 관련 분야를 다루고, 3장에서는 스트리밍 콘텐츠의 2차 배포를 위한 SDI 구조를 설계하고, 4장에서는 제안된 SDI의 구현 및 실험을 기술하며, 5장에서는 결론 및 기대 효과를 기술한다.

2. 관련 연구

2.1 DRM 시스템

디지털 콘텐츠를 보호하기위한 DRM 기술은 크게 3가지 형태로 구분할 수 있다. 첫 번째는 콘텐츠에 대한 정의 및 암호화를 위한 패키징, 두 번째는 면허를 발급하고 관리하기 위한 면허 서버, 세 번째는 면허를 발급받고 실행하기 위한 소비자이다. 이외에도 웹 서버, 스트리밍 서버와 같은 다양한 서비스가 필요하다[6,7].

그림 1에서 디지털 콘텐츠는 패키져를 통해 암호화되고 정보를 저장하게 된다. 소비자는 저장된 정보를 이용하여 콘텐츠를 구매하게 되면 면허 서버로부터 해당 콘텐츠에 대한 면허를 발급받고 웹 서버 또는 스트리밍 서버로부터 콘텐츠를 제공받아 실행 할 수 있다[6,7].

2.2 초유통

초유통은 콘텐츠 사용자가 자신이 구입한 콘텐츠를 E-mail, CD-ROM, 디스켓 등을 통해 다른 사람에

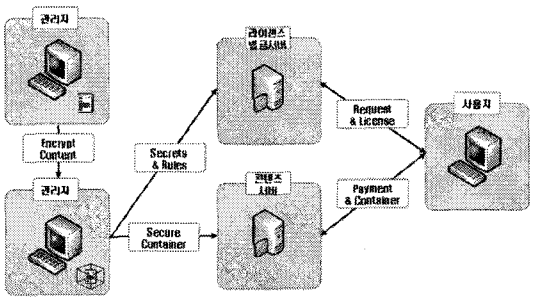


그림 1. Microsoft사의 DRM [7]

게 반복적으로 배포할 수 있게 하여, 콘텐츠의 급속한 확산을 가능하게 하는 기술이다. 초유통은 DCF (DRM Content Format)형태의 콘텐츠에 대한 배포를 허용하며 초유통된 콘텐츠의 사용을 위해 권한을 발급받을 수 있게 해준다. 디바이스는 DCF의 권한이력필드에 정의된 URL을 통해 권한발급 요청을 하게 된다. 기존 안전한 배포 기술은 사용자에게 종속적인 키를 이용하여 콘텐츠를 암호화함으로써 콘텐츠의 이동을 크게 제한한 반면 초유통은 콘텐츠의 이동 및 복사는 자유롭게 허락하되 사용 시점에서 사용권한을 획득해야만 콘텐츠의 이용이 가능한 기술적 매커니즘을 통해 디지털 콘텐츠의 안전한 유통을 유도한다.

2.3 DRM 클라이언트 에이전트

DRM 클라이언트 에이전트는 암/복호화 기능을 지원함으로써 디지털 콘텐츠에 대한 보안 서비스 강화 및 정당한 절차를 거쳐 면허를 구매한 소비자에 대한 인증 기능을 수행한다. 또한, 디지털 콘텐츠의 면허에 따라서 복제 방지, 사용 횟수 제한, 사용 기간 제한 등과 같이 다양한 사용 규칙을 적용해서 디지털 콘텐츠의 유료 사용을 위한 과금 관리 기능의 지원 및 영화, 음악, 만화, 문서, 게임 등 다양한 디지털 콘텐츠의 특성에 따라서 기존의 플레이어에 플러그인 추가하거나 특정 콘텐츠만을 재생시킬 수 있는 자체 플레이어를 통해서 소비자에게 이미 전달된 디지털 콘텐츠의 불법 접근을 통한 해킹이나 디지털 콘텐츠 플레이에서 복호화 된 데이터의 복사, 저장, 인쇄, 화면 캡쳐 등을 방지하는 기능을 제공한다[8].

특히, 그림 2의 SSD(Secure Storage Device) Driver는 면허데이터, 콘텐츠복호화 키 및 Secure Container에 들어있는 비즈니스규칙 등의 데이터를 소비자가 임의로 조작하지 못하도록 하여 신뢰할 수 없는 DRM 클라이언트 시스템 하에서 디지털 콘텐츠를 안전하게 보호함으로써 보다 안정적으로 디지털 콘텐츠가 유통될 수 있는 DRM 환경을 제공하게 된다[8].

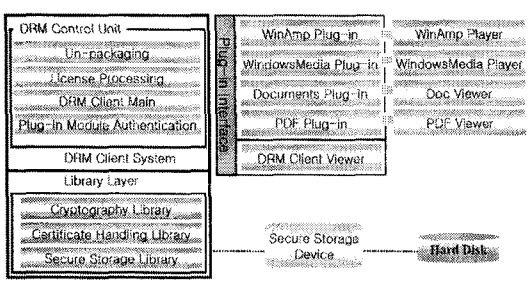


그림 2. DRM 클라이언트 시스템의 세부 모듈[8]

2.4 스트리밍 DRM 콘텐츠의 유통

스트리밍 콘텐츠는 크게 두 가지의 특징을 갖는다. 첫째, 파일이 전송되면서 콘텐츠가 실행된다는 점, 둘째, 전송이나 실연이 완료된 후에 소비자의 하드디스크 드라이브에 파일의 복제가 이루어지지 않는다는 점이다. 물론, 최근에는 콘텐츠와 같은 유형에 머무르지 아니하고 소프트웨어의 경우까지 스트리밍이 가능하다고 한다[9,10].

그림 3은 스트리밍 DRM 서비스모델이다. 다운로드 콘텐츠의 유통 솔루션과 큰 차이는 없다. 차이점으로는 스트리밍 콘텐츠의 특징처럼 서비스 후 소비자에 저장되지 않고 메타데이터 전송을 통한 서비스가 이루어진다.

유통적인 측면에서 위에서 언급한 특징처럼 1차 배포 후 2차 배포가 어렵다. 스트리밍콘텐츠의 배포는 홈페이지의 광고, 배너, 온라인 광고 등으로 이루어진다. 기존의 유통방식이 아닌 새로운 방법으로 스트리밍 콘텐츠의 장점을 살리면서 2차 배포를 원활히 할 수 있어야 한다.

2.5 플레이리스트 파일

플레이리스트 파일은 일반적인 텍스트파일로 되어있고 간단한 태그로 오프라인과 HTTP 서버상의 미디어 파일을 연결시켜 주며 미디어 플레이어의 여러 가지 정보를 정의하고 미디어 플레이어에서 재생

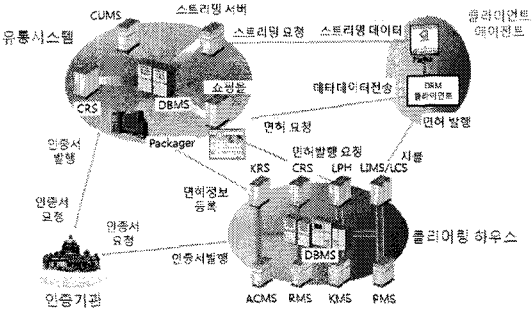


그림 3. 스트리밍 서비스의 유통시스템

표 1. 플레이리스트 파일 구성 예[11]

구분	ASX	M3U
태그예	<Asx Version ="3.0"> <Entry> <title>제목</title> <author>가수</author> <copyright>저작권자 </copyright> <ref href="mms://test.com/test.wmv"/> </Entry> </Asx>	#EXTM3U #EXTINF: http://test.com/music/1.mp3 #EXTINF: http://test.com/music/2.mp3 #EXTINF: http://test.com/music/3.mp3

할 파일의 목록과 그 파일의 정보를 담고 있다. 널리 알려진 플레이리스트 파일의 종류는 마이크로소프트의 ASX와 M3U 포맷이 대표적이다[11]. ASX와 M3U의 구성은 다음 표 1과 같다.

보통 플레이리스트 파일은 콘텐츠의 리스트 정보와 메타데이터 등으로 구성된다. 플레이리스트 파일은 평문으로 사용자 사이에서 배포되어지기 때문에 수정이 가능하다. 콘텐츠의 URL이 노출되어 불법 프로그램을 통해 스트리밍 콘텐츠를 다운로드 받을 수 있기 때문에 저작권 침해의 위험이 있다. 위와 같은 이유 때문에 상업적인 콘텐츠로서는 활용 되지 않고 있다.

3. 제안하는 스트리밍 콘텐츠의 중계파일 구조

3.1 SDI(Streaming Distribution Information) 메커니즘

본 논문은 스트리밍 콘텐츠 초유통 구조를 가능하게 하는 SDI 구조를 제안하고, 그 운용 방법에 관한 것이다. 디지털 콘텐츠 배포는 1차 배포와 2차 배포로 구분할 수 있다. 먼저 1차배포는 디지털 콘텐츠 제작업체의 서버가 소비자의 요청에 해당하는 디지털 콘텐츠를 해당 소비자에게 제공하는 것을 의미한다. 이때 디지털 콘텐츠는 전송방식에 따라 다운로드 콘텐츠와 스트리밍 콘텐츠로 구분할 수 있다.

다운로드 콘텐츠와는 달리 스트리밍 콘텐츠는 실시간으로 전체 콘텐츠의 일부분을 제공받아 실행되는 디지털 콘텐츠를 의미한다. 다음으로, 2차 배포는 소비자가 자신의 단말기에 저장된 디지털 콘텐츠를 다른 소비자에게 제공하는 것을 의미한다. 지금까지의 2차 배포는 암호화된 디지털 콘텐츠를 소비자의 단말기로 다운로드하는 과정을 거쳐 이루어졌다.

그러나 스트리밍 콘텐츠는 특성상 스트리밍 서버에서 소비자로의 1차 배포만 가능하고, 다른 소비자로의 2차 배포는 어려웠다. 이는 스트리밍 콘텐츠가 스트리밍 서버로부터 전체 콘텐츠의 일부분만이 소비자의 단말기로 전송되어 실행되기 때문에 초기 서비스를 제공받는 소비자가 다른 소비자에게 배포할 수 없기 때문이다. 다시 말해 스트리밍 콘텐츠는 암호화된 디지털 콘텐츠가 소비자의 단말기에서 연속적으로 실행되는 구조를 가지기 때문이다. 따라서 DRM의 개념이 도입된 상태에서 2차 배포가 가능한 디지털 콘텐츠는 다운로드 콘텐츠에 국한되고, 스트리밍 콘텐츠의 경우에는 2차 배포가 어렵다.

디지털 콘텐츠 제작자 입장에서는 DRM을 만족하는 상태에서 다양한 형태의 2차 배포가 이루어져 암호화된 디지털 콘텐츠의 배포가 원활하게 이루어지는 것이 효율적이다. 따라서 거의 대부분의 디지털 콘텐츠는 2차 배포가 가능한 다운로드 콘텐츠 형태를 가지게 된다. 그러나 모바일 환경에서는 용량과 처리 능력의 한계, 통신 대역폭의 문제로 대용량의 다운로드 콘텐츠를 서비스하는 것은 쉽지 않다.

이와 같이 기존의 디지털 콘텐츠 서비스는 2차 배포가 가능한 모바일용 다운로드 콘텐츠의 경우 그 용량이 극히 제한되는 문제점이 있다. 또한 다운로드 콘텐츠에 비해 용량 문제를 해결할 수 있는 스트리밍 콘텐츠의 경우 그 특성상 2차 배포가 불가능한 문제점이 있다. 결국, 용량 제한 또는 2차 배포가 불가능하여 제작자 및 소비자 양측의 디지털 콘텐츠 활용의 불편을 가중시키는 문제를 유발하게 된다.

그래서 본 논문에서는 스트리밍 콘텐츠의 재배포가 가능하고 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 사용료 부과와 결제 대행 등 콘텐츠의 생성에서 유통관리 해줄 수 있는 스트리밍 콘텐츠의 중계역할을 하는 SDI 구조를 제안 하였고, SDI를 통한 스트리밍 콘텐츠의 재배포를 위한 시스템을 구현하여 설명하였다.

3.2 SDI 개념

SDI는 스트리밍 DRM 콘텐츠와 소비자를 중계하여 스트리밍 DRM 콘텐츠의 재배포를 위한 중계파일이다. 그림 4는 SDI를 통한 스트리밍 서비스를 나타낸다. 소비자는 콘텐츠 배포자 서버에 접속하여

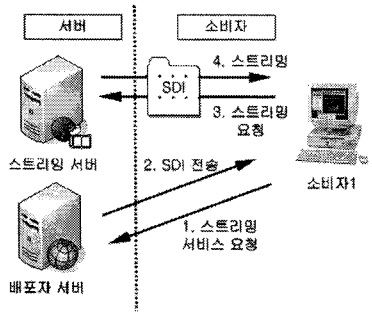


그림 4. SDI 1차 배포

SDI를 1차 배포 받는다. 소비자 사이에서 배포된 SDI는 소비자와 스트리밍 서버를 연결시킨다. SDI는 소비자가 직접적으로 스트리밍 콘텐츠에 접근하지 않고 스트리밍 콘텐츠에 연결 할 수 있도록 중계 역할을 한다.

그림 5와 같이 SDI를 1차 배포 받은 소비자1은 소비자2에게 SDI를 2차 배포 한다. 2차 배포 된 SDI는 스트리밍 콘텐츠의 접근방법과 콘텐츠의 저작권 정보, 내용, 제목의 콘텐츠 메타정보와 면허의 권한 정보, 면허 서버 접근정보를 사용하여 DRM 서비스를 가능하게 함으로써 스트리밍 콘텐츠의 재배포를 가능하게 한다. 이러한 SDI의 구조 및 SDI를 이용한 DRM 시스템흐름은 다음 단에서 자세히 다루도록 한다.

3.3 SDI를 위한 구성요소

배포자 서버로부터 배포되어진 SDI는 소비자의 클라이언트 에이전트를 통해 면허획득 및 콘텐츠의 복호화를 통해 서비스가 진행된다. SDI의 재배포를 통한 서비스를 위해서는 그림 6과 같은 객체들의 역할이 필요하다.

공급자 서버는 콘텐츠를 생산하여 제공하는 개체로서 원본 콘텐츠를 암호화된 콘텐츠로 패키징한다. 스트리밍 서버에 암호화된 콘텐츠를 전송하고, 배포자 서버에는 SDI 생성정보를 전송하며 면허 서버에

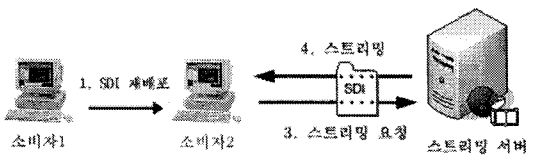


그림 5. SDI 2차 배포

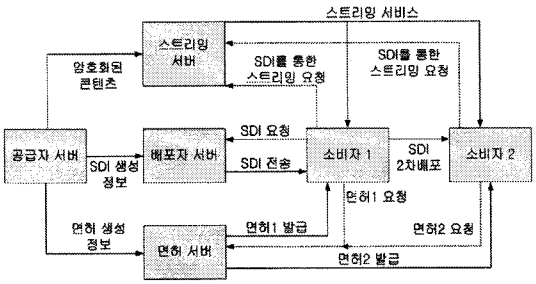


그림 6. SDI의 재배포를 위한 전체시스템 구성

는 면허생성정보를 전송한다. 배포자 서버는 제공받은 콘텐츠에 대한 서비스를 소비자에게 제공하는 개체로써 소비자 관리, 지불 관리, 권리 관리, 콘텐츠 관련 자료 관리 등의 역할을 맡는다. 소비자가 콘텐츠 서비스를 요청하면 SDI의 생성정보를 통해 SDI를 암호화 하여 소비자1에게 배포한다. 면허 서버는 소비자가 요청한 권리에 대한 면허를 발급하는 개체로서 공급자 서버로부터 받은 면허의 권한 정보를 통해 소비자에게 면허를 발급한다. 소비자1은 클라이언트 에이전트를 통해서 스트리밍 서비스를 요청하고 SDI를 배포 받고 비용을 지불하고 콘텐츠를 실행하는 개체이다. 소비자2는 소비자1로부터 SDI를 2차 배포 받는 개체로서 소비자1과 같은 프로세스를 갖는다.

3.4 SDI 구성 데이터

공급자 서버에서는 원본 콘텐츠를 패키징 하여 암호화한 후 스트리밍 서버에 업로드 한다. 이와 함께 공급자 서버는 패키징 할 때 생성되는 콘텐츠 정보를 배포자 서버에게 보낸다. SDI 데이터 구조는 헤더 영역, 콘텐츠 영역, 면허 영역으로 구성되며 그림 7과 같다.

헤더 영역은 SDI의 버전과 식별자, 그리고 배포자와 소비자 식별자가 포함되고, 콘텐츠 영역에는 콘텐

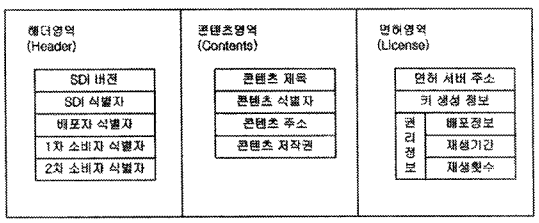


그림 7. SDI의 구조

츠 식별자와 콘텐츠 메타데이터가 포함된다. 그리고 면허 영역에는 키 정보와 권리 정보 및 면허 획득 정보가 포함된다. 각 영역의 정보는 크게 공급자 서버와 배포자 서버, 소비자가 제공하는 정보에 의해 생성된다. 공급자 서버에서 제공되는 정보는 암호화된 스트리밍 콘텐츠의 복호화 키를 생성하기 위한 키 생성 정보, SDI 식별자 정보, 콘텐츠의 메타데이터, 면허 생성 정보이다. 배포자 서버에서 제공하는 데이터는 SDI 식별자 정보이고, SDI 생성 요청 시에 결정된다. 공급자 서버에서 패키징 할 때 발생되는 정보는 배포자 서버의 데이터베이스에 저장되어 SDI 생성요청 시 사용된다. 공급자 서버로부터 배포자 서버에게 보내지는 정보는 다음 표 2와 같고, 배포자 서버에서 생성되는 SDI 데이터는 여러 가지 식별 정보로서 다음 표 3과 같다.

SDI 버전은 SDI의 구조변경에 따른 버전 관리를 위한 것이고, SDI ID는 고유한 스트리밍 콘텐츠에 대한 SDI의 식별자이다. 배포자/ 소비자 식별 정보는 배포자 서버와 계층 별 소비자들의 ID를 명시하여 배포 상황에 따른 이익금 분배, 소비자의 현황을 알 수 있다. 1차 소비자 ID는 최초 배포된 소비자의 식별자로서 최상위 소비자를 뜻한다. 2차 소비자 ID는 1,2

표 2. SDI 생성을 위한 공급자서버 제공정보

구 분	이 름	설 명	데이터
콘텐츠 메타 데이터	제목	배포된 콘텐츠의 제목	경원대학교 홍길동 강의
	식별자	고유한 콘텐츠의 식별자	eixlYTxW873S
	장르	콘텐츠의 장르	교육
	스트리밍 서버주소	스트리밍 서버 주소	mms://kyungwon.ac.kr/ecture01.wmv
	저작권	콘텐츠 저작권 정보	본 영상에 대한 저작권은 경원대학교에 있습니다
면허 생성	면허서버 주소	면허 서버 주소	http://drm.kyungwon.ac.kr/license.asp
	배포횟수	SDI 배포 가능 여부 및 횟수	4
	재생기간	재생기간 권한 내용	2006073020100730
	재생횟수	재생횟수 권한 내용	4
키 생성	Key ID	콘텐츠 복호화키 정보	jkWeslsi83ksdiT

표 3. SDI 생성을 위한 배포자/소비자 제공정보

구 분	이 름	설 명	데이터
SDI 식별 정보	SDI 버전	SDI 버전	1.0
	SDI ID	SDI의 식별자로서 암호화 될 때마다갱신	KyungwonLecture0606051
배포자/ 소비자 식별 정보	배포자ID	배포자에 대한 식별자	kwx07dke9VW
	1차 소비자ID	최초 배포된 소비자 식별자	Gcs320xYWZ7
	2차 소비자ID	2차 배포된 소비자 식별자	82sdSiT0Xxw&92kdiqks0kdafs

차 소비자에 의해 SDI를 배포 받은 소비자 ID이다. 2차 소비자 ID 정보는 2차 소비자의 면허획득 과정 이후에 갱신될 수 있다.

3.5 SDI 서비스 절차

SDI 생성정보가 배포자 서버에 전송되면 배포자 서버의 SDI 생성 모듈에 의해 XML(Extensible Markup Language) 형태로 SDI가 생성된다. SDI 태그는 그림 8과 같다.

SDI XML 태그는 식별자 정보, 콘텐츠 정보, 면허 정보로 구성된다. 소비자가 클라이언트 에이전트를 통해 SDI 요청 시 소비자의 인증과정 후 소비자의 공개키(RSA)로 암호화하여 전송한다. 암·복호화 키 정보는 SDI ID의 정보를 통해 각각 생성된다. 2차 배포된 SDI는 SDI 실행 요청 시 배포자 서버에서 SDI ID의 정보를 통해 SDI ID를 갱신하여 2차 소비

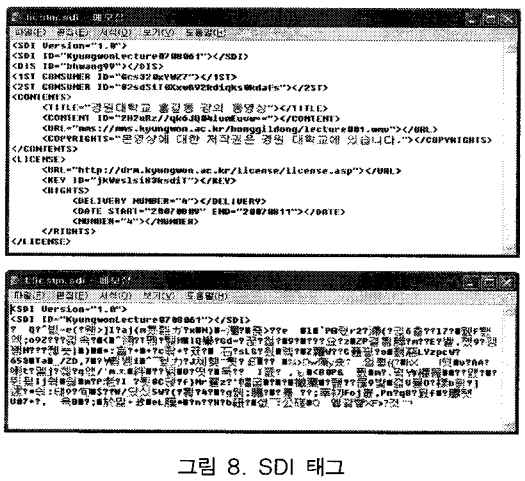


그림 8. SDI 태그

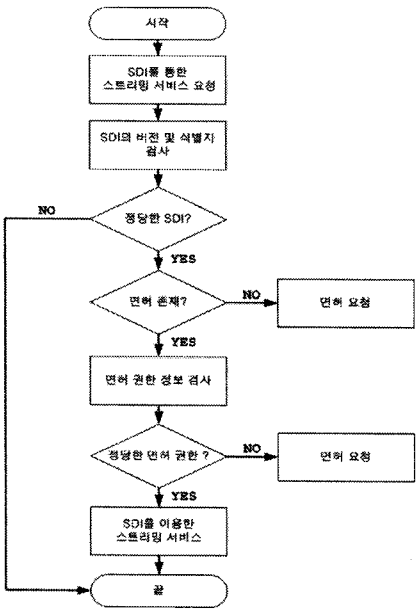


그림 9. SDI 실행 순서도

자의 공개키로 암호화하여 SDI를 2차 소비자에게 전송한다. 2차 배포된 SDI는 클라이언트 에이전트를 통해 복호화 되고 SDI 태그 정보를 통해 스트리밍 서비스, 면허 획득, SDI 갱신 등의 서비스가 진행된다. 그림 9는 획득한 SDI를 클라이언트 에이전트를 통해 스트리밍 서비스가 진행되는 순서도이다.

SDI를 통해 스트리밍 서비스를 요청하면 클라이언트 에이전트를 통해 그림 10과 같이 스트리밍 콘텐츠가 실시간 복호화 되어 재생된다.

SDI에서 추출된 KeyID 정보와 암호화된 스트리밍 콘텐츠의 헤더에 있는 Seed 정보를 통해 복호화 키를 추출한다. 암호화된 콘텐츠는 추출된 복호화 키로 복호화한 후 재생된다. 복호화 이전 사용자의 면허의 유무에 따라 면허의 획득과 갱신이 이뤄지고

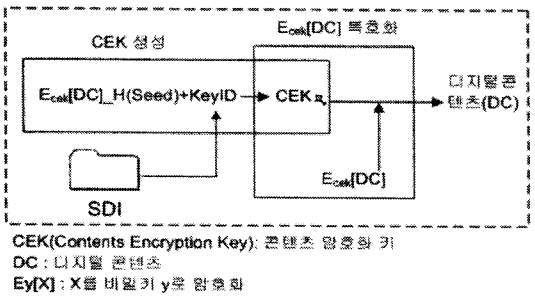


그림 10. 암호화된 스트리밍 콘텐츠 복호화

이 과정에서 SDI의 2차 소비자 ID 리스트에 소비자가 추가되고 SDI 배포 가능 횟수가 갱신된다.

4. 구현 및 실험

제안하는 SDI를 통한 서비스를 위해 서버와 클라이언트 에이전트로 구성하여 실험했다. 서버는 공급자 서버, 면허 서버, 배포자 서버이고, 소비자는 클라이언트 에이전트로 구성한다.

4.1 서버 프로그램

공급자 서버는 스트리밍 서버에 업로드 해야 할 콘텐츠를 암호화하는 파트로써 콘텐츠의 메타데이터, 저작권 정보, 권한 정보 등을 설정하고, 암호화 키를 통해 콘텐츠를 암호화하여 스트리밍 서버에 콘텐츠를 업로드 한다. 그림 11은 공급자 서버와 배포자 서버의 프로그램을 나타낸다.

공급자 서버는 패키징을 위한 정보 설정, 권한 설정, 저작권 설정 등을 한다. 배포자 서버는 접속된 소비자에게 보유하고 있는 콘텐츠의 리스트를 보여주고 요청된 콘텐츠의 SDI의 생성 및 암호화를 하고 소비자에게 보내준다. 배포한 SDI의 정보를 로그파일에 저장하여 통계 정보를 생성한다. 소비자의 SDI 요청 시 SDI의 생성 데이터를 통해 SDI를 생성하고 소비자에게 배포한다. 면허 서버는 소비자가 SDI를 통해 면허 요청을 하면 면허를 발급한다.

4.2 클라이언트 에이전트

클라이언트 에이전트는 콘텐츠의 획득, 면허 획득,

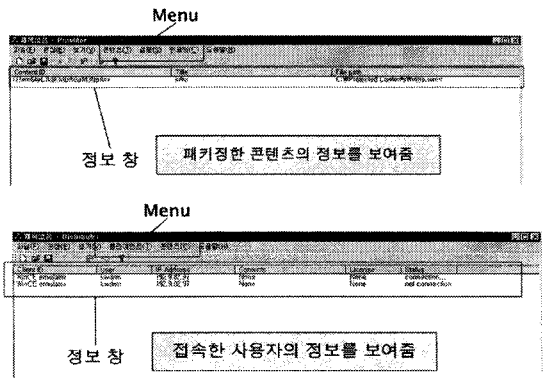


그림 11. 공급자 서버와 배포자 서버 프로그램

그림 12. 클라이언트 에이전트와 SDI 실행 절차

콘텐츠를 재생하는 주요 기능 등으로 구성된다. 클라이언트 에이전트의 화면 구성도와 실행 순서는 그림 12와 같다. 소비자는 로그인을 통해 개인인증 후 배포자 서버에 접속한다. 배포자 서버에 연결되면 배포자 서버가 보유하고 있는 콘텐츠 리스트를 보여준다.

SDI의 콘텐츠ID와 제목을 화면에 표시하여 소비자가 콘텐츠를 선택할 수 있도록 한다. SDI를 요청하면 콘텐츠 ID정보를 배포자 서버에 보내고 해당 SDI를 특정 디렉토리에 다운로드 한다. 스트리밍 서비스를 요청하면 재생 권한의 면허를 요청 및 획득하고 면허 검사 후 스트리밍 콘텐츠의 접근 주소로 연결시켜준다. SDI의 키 정보를 통해 복호화 키를 추출하여 실시간으로 전송되는 스트리밍 데이터를 복호화 하여 동영상을 재생한다. 면허가 만료된 후 재생 요청을 하면 면허 만료 메시지를 보여주고 소비자는 면허 재발급을 통해 동영상을 감상할 수 있다.

SDI는 2차 소비자에게 근거리 통신과 이동저장장치 등을 통해 2차 배포할 수 있고, 2차 배포 받은 SDI는 클라이언트 에이전트를 통해 그림 13의 과정을 거친 후 동영상을 감상할 수 있다. 2차 배포 받은 SDI는 SDI ID 정보를 통해 2차 소비자의 공개키로 재 암호화하여 전송된다. 면허 발급절차를 거친 후 해당 SDI를 통한 스트리밍 서비스가 진행된다.

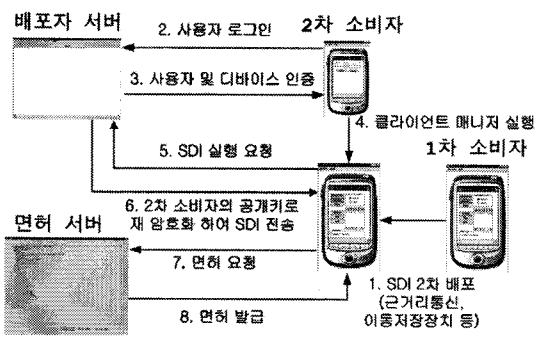


그림 13. 2차 배포된 SDI 실행 절차

4.3 SDI 성능 분석

스트리밍 DRM 콘텐츠의 초유통을 위한 SDI를 설계하여 구현하였고 기존 스트리밍 DRM 시스템이 가지는 유통의 어려움을 해결 할 수 있음을 보였다. 표 4는 제안된 SDI와 기존 DRM 콘텐츠와 플레이리스트 파일을 비교하였다.

기존 스트리밍 DRM 콘텐츠는 다운로드 DRM 콘텐츠와 비교하여 이동성에 제약이 있어서 소비자 사이에 빠른 배포가 어렵다. 이러한 배포의 제약을 기존 스트리밍 콘텐츠의 플레이리스트 파일로써 해결될 수 있지만, 기존의 플레이리스트 파일은 DRM 기능이 적용된 사례가 없기 때문에 스트르밍 콘텐츠의 DRM 기능에 의존하였다. 본 논문은 이러한 문제점을 SDI를 통해 해결하였다. 제안하는 SDI는 스트리밍 DRM 콘텐츠의 2차 배포가 가능하고 DRM 서비스의 면허 발급, 비용 결제 정보를 통해 스트리밍 콘텐츠의 유료서비스가 가능하다. 소비자의 배포 이력 정보를 통해 이익금을 분배 할 수 있는 구조이고, 암호화되어 배포되기 때문에 배포 중 변형 될 가능성이 낮다. 작은 용량의 SDI는 모바일 디바이스 사이에서 쉽게 배포 될 수 있다. 다양한 스트리밍 콘텐츠에 적용 가능하기 때문에 저작권 보호와 스트리밍 콘텐츠 유통의 원활함을 이룰 수 있다.

SDI는 다운로드 콘텐츠의 초유통 시스템을 스트

표 4. DRM 디지털 콘텐츠의 특성 비교

구 분	다운로드 DRM 콘텐츠	스트리밍 DRM 콘텐츠	기존 플레이리스트 파일	제안한 SDI
2차 배포	○	스트리밍 다운로드 서비스시 가능	○	○
면허 발급 정보	○	○	×	○
배포 이력 정보	○	○	×	○
암호화	○	○	×	○
메타데이터	○	○	○	○
초유통	○	스트리밍 다운로드 서비스시 가능	×	○

(○ : 가능, ×: 불가능)

리밍 콘텐츠에 접목하여 스트리밍 콘텐츠의 보안을 유지하면서 2차 배포를 가능하게 하고 DRM 서비스를 제공하기 때문에 스트리밍 디지털 콘텐츠 시장의 활성화에 이바지할 수 있다.

5. 결 론

본 논문에서는 스트리밍 콘텐츠의 초유통을 위한 SDI 구조를 제안하고 DRM 시스템을 구축하여 실험하였다. 기존의 스트리밍 콘텐츠는 구조적인 특징 때문에 초유통 구조가 어렵고, 소비자 측에 저장되지 않아 실질적인 소비자 사이에서 2차 배포는 불가능하다. 제안된 SDI는 스트리밍 서비스 요청 시 스트리밍 서버와 소비자의 중계역활을 하는 파일로서 스트리밍 콘텐츠의 2차 배포를 가능하게 하고 자체적으로 DRM 서비스를 위한 정보를 갖고 있다. SDI에 명시되어있는 규칙 안에서 면허가 발급되며 적법한 소비자라 판단되면 스트리밍 콘텐츠의 접근 경로 정보를 통해 스트리밍 서비스가 진행된다. 2차 소비자가 면허를 획득하면 SDI의 2차 소비자 정보가 갱신된다. 배포되는 소비자의 정보를 통해 콘텐츠의 추적이 가능하고 배포 이력 정보를 통한 이익금 분배가 가능하기 때문에 원활한 콘텐츠 배포를 이룰 수 있다.

모바일 디바이스의 통신환경은 나날이 발전되고 있으며 고화질의 콘텐츠의 스트리밍 서비스가 가능해지고 있다. 영화, 음악, E-Learning 등의 다양한 스트리밍 콘텐츠에 적용 가능 할 것이다. 앞으로 스트리밍 디지털 콘텐츠의 저작권을 보호하는 동시에 유통의 원활함을 가능하게 할 수 있는 DRM 기술이 발전되어야 한다. 향후 연구계획은 SDI에 의해 서비스 되는 스트리밍 콘텐츠의 안전하고 신속한 암·복호화 방법을 연구할 것이며, 모바일 환경에서 면허, 키 정보와 같은 중요 데이터를 안전하게 보호하는 방법에 대해서 연구할 것이다.

참 고 문 헌

[1] 이진홍, 김태정, 박지환, "컨텐츠 스트리밍을 위한 안전한 DRM 시스템 설계 및 구현," 정보보호학회논문지, 제13권, 제4호, pp. 177-186, 2003.

[2] P.A. Jamkhedkar and G.L. Heilerman, "DRM as a Layered System," *ACM Workshop RM '04*, pp. 11-21, 2004.

[3] 윤기송, 정연정, "End-to-end 콘텐츠 보호를 위한 DRM 시스템 설계 및 구현," 한국정보처리학회논문지, 제13C권, 1호, pp. 35-44, 2006.

[4] 이창열, "DRM 기술," 정보보호학회논문지, 제12권, 제1호, pp. 1-10, 2002.

[5] 오원근, "DRM 표준화 및 평가 기술," 전자통신동향분석, 제20권, 제4호, pp. 139-154, 2005.

[6] S. Michiels and K. Verslype and W. Joosen and B.D. Decker, "Towards a Software Architecture for DRM," ACM Workshop DRM '05, pp. 65-74, 2005.

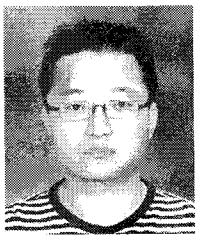
[7] 이혜주, 최범석, 홍진우, 석종원, "디지털 방송콘텐츠 보호 유통 시스템 설계 및 구현," 정보처리학회논문지, 제11-C권, 제6호, pp. 731-738, 2004.

[8] 이기정, 권태경, 황성운, 윤기송, "신뢰할 수 없는 DRM 클라이언트 시스템 하에서 키 보호를 위한 Secure Storage Device의 연구," 정보보호학회논문지, 제14권, 제2호, pp. 3-13, 2004.

[9] 김태정, 이진홍, 신상욱, "WIPI기반의 DRM 컴포넌트 설계 및 구현," 한국정보처리학회, 제11권, 제2호, pp. 1775-1778, 2004.

[10] 박지현, 전연정, 윤기송, "DRM 기술 동향," 전자통신동향분석, 제22권, 제4호, pp. 118-132, 2007.

[11] 고현일, 성미영, "템플릿 기반 멀티미디어 컨텐트 저작도구 구현," 멀티미디어학회논문지, 제7권, 제3호, pp. 368-376, 2004.



김 태 민

2006년 경원대학교 멀티미디어학과 학사

2008년 경원대학교 전자계산학과 석사

2008년~현재 경원대학교 전자계산학과 박사과정

관심분야 : 저작권보호 (DRM), 멀티미디어 응용

양 영 규

1972년 서울대학교 학사
1974년 서울대학교 환경대학원 환경계획 석사
1984년 Texas A&M University 공간정보처리 박사
2003년~현재 경원대학교 IT대학 교수

관심분야 : 공간정보처리, 텔레매틱스