다양한 컨텐츠 보호 툴과 라이센스를 적용한 MP3 재생제어 시스템

최 범 석, 홍 진 우
한국전자통신연구원

MP3 playback control system using various protection tools and the license

Bum Suk Choi, Jin Woo Hong
ETRI
161 Gajeong-dong, Yuseong-gu, Taejon, Korea
E-mail : bschoi@etri.re.kr, jwhong@etri.re.kr

요 약

본 논문에서는 디지털 컨텐츠를 보호하기 위한 다양한 암호화 알고리즘이나 워터마크 알고리즘이 하나의 사용자 단말에서 작동할 수 있도록 시스템을 구성하였으며, 컨텐츠의 재생 처리 과정 중에 다수의 제어 포인트를 두어 다중적인 컨텐츠 보호를 가능하게 하였다. 또한 라이센스 개념을 사용하여 다양한 컨텐츠 사용 규칙을 적용할 수 있도록 하였으며 컨텐츠와 라이센스를 독립적으로 관리하므로 사용자들 사이의 컨텐츠 전송을 가능하게 하였다.

1. 서 론

최근 멀티미디어 디지털 컨텐츠 산업이 발전함에 따라 양질의 컨텐츠를 보호하기 위한 다양한 알고리즘들이 개발되고 있다. 소비자 입장에서는 하나의 사용자 단말로 다양한 컨텐츠 서비스 회사들의 컨텐츠를 이용할 수 있기를 원한다. 그러나 각 컨텐츠 서비스 회사들은 보안상의 이유로 대부분 자신들이 제공하는 컨텐츠에 대한 독자적인 보안 기술을 개발하고 있으므로 이들간의 호환성을 찾기가 어렵다. 이는 디지털 컨텐츠 보안 메카니즘에 대한 표준화를 어렵게 하고 단말의 범용성을 막는 최대의 걸림돌이 될 수 있다. 또한 각 보호 알고리즘들은 크게 암호화 알고리즘과 워터마킹 알고리즘으로 나눌 수 있으며 이들은 각각 장·단점들을 가지고 있으므로 어느 한 기술에 의존하는 컨텐츠 보호 방법은 해킹의 위험에 노출되기 쉽다. 마지막으로 사용자의 다양한 소비형태를 지원하고 사용자 상호 간의 컨텐츠 전송을 가능하게 하도록 하는 것은 컨텐츠 소비를 촉진하고 양질의 컨텐츠를 널리 유포시키는데 반드시 필요한 기능이라 할 수 있다. 본 논문에서는 사용자 단말 시스템에서 이러한 보호 알고리즘들 간의 상호 운용성, 다중 보호 알고리즘 적용, 다양한 사용 룰 정의 및 사용자들 간의 super-distribution 기능을 만족시킬 수 있는 방법을 제안하고, 이를 MP3 플레이어에 적용시킨 예를 보여준다.

2. 제 안

여기서는 앞 절에서 언급한 사용자 단말에서 필요로 하는 각 기능을 만족시킬 수 있는 기본적인 방법을 제안하도록 한다.

2.1 보호 알고리즘들 간의 상호 운용성

하나의 사용자 단말에서 다양한 보호 알고리즘들을 적용할 수 있기 위해서, 사용자 단말 시스템은 선택한 컨텐츠를 소비하기 위하여 필요한 보호 알고리즘을 유일하게 식별할 수 있어야 하며, 이를 작동시키기 위한 파라미터들을 호출된 알고리즘에 전달할 수 있어야 한다. 이를 가능하게 하기 위하여 다음의 과정이 필요하다.

(1) 알고리즘 등록: 알고리즘 제공자는 자신의 알고리즘을 알고리즘 등록 센터에 등록한다. 이 때, 알고리즘 등록 센터는 툴들간 인터페이스를 위한 기본적인 메시지를 규정하고 이 메시지 규칙에 따라 알고리즘이 작동하는 것을 확인한 후, 정식으로 알고리즘을 등록하고 그 알고리즘 만의 고유한 ID를 부여한다.

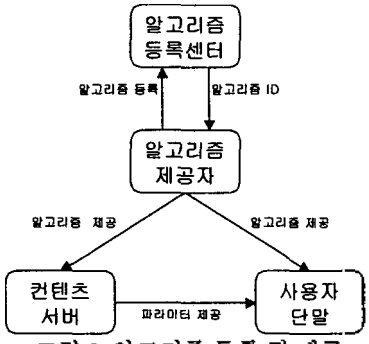
(2) 알고리즘 제공: 알고리즘 제공자는 등록된 알고리즘을 컨텐츠 서비스 제공자와 사용자 단말에 제공 한다. 단 이때 컨텐츠 서비스 제공자에게

제공되는 알고리즘은 컨텐츠 패키징을 위한 것이며, 사용자 단말에 제공되는 알고리즘은 컨텐츠 소비를 위한 것이다.

(3) 알고리즘 적용(컨텐츠 서비스 제공자): 컨텐츠 서비스 제공자는 제공된 알고리즘을 사용하여 컨텐츠를 패키징 한다. 이 때, 컨텐츠 소비를 위하여 필요한 여러 가지 파라미터들을 결정한다. 마지막으로 패키징 된 컨텐츠를 사용자 단말에 배포한다.

(4) 알고리즘 적용(사용자 단말): 사용자 단말에서는 컨텐츠의 소비를 위하여 필요한 알고리즘 ID 와 파라미터들을 컨텐츠 서비스 제공자에게 요청한다. 필요한 알고리즘을 호출하고 파라미터를 알고리즘에 전달한다.

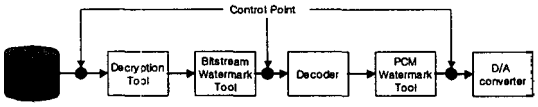
그림 1 은 위의 과정을 도식적으로 나타낸다.



<그림 1. 알고리즘 등록 및 제공>

2.2 다중 보호 알고리즘 적용

암호화 알고리즘들은 그 안전성이 증명되어 있으므로 대부분의 보호 메커니즘이 암호화 알고리즘을 사용하여 컨텐츠를 보호하고 있다. 그러나 CPU 의 성능이 높아짐에 따라 더 많은 비트수의 키를 요구하게 되며 이미 소비자에게 전송된 컨텐츠는 새로운 키를 사용하여 다시 암호화 하기가 어렵다. 또한 한번 복호화 되면 더 이상 그 컨텐츠를 보호할 방법이 없게 된다. 한편 워터마킹 알고리즘들은 컨텐츠 자체에 부가 데이터를 삽입하는 기술로 컨텐츠가 불법적으로 배포된 후에도 컨텐츠에 대한 자신의 권리를 증명할 수 있도록 해 주며 신호 처리 알고리즘을 사용하므로 그 안전성이 CPU 의 성능과는 무관하다 할 수 있다. 또한 삽입된 워터마크를 제거하기 위해서는 어느 정도의 컨텐츠 질의 저하를 피할 수 없으므로 컨텐츠의 가치를 유지시켜 줄 수 있다는 장점이 있다. 그러나 워터마크 알고리즘 자체로는 컨텐츠의 불법적인 사용을 막을 수 없다.[1~2] 따라서 보다 안전한 컨텐츠의 보호를 위해서는 이 두 알고리즘을 조합하여 사용할 필요가 있다. 현재 대부분의 디지털 컨텐츠가 압축된 데이터 형식으로 전송되고 있기 때문에 사용자 단말 시스템은 압축된 컨텐츠를 최종 raw 데이터 형태로 출력하기 전까지 다양한 알고리즘들을 적용하여 컨텐츠를 사용하려는 사용자가 정당한 사용자인지를 검사할 수 있어야 하며 단말 시스템이 소비할 컨텐츠가 정당한 컨텐츠인지를 검사할 수 있어야 한다. 그림 2 는 압축된 컨텐츠가 최종 raw 데이터로 출력되기 전까지 가능한 보호 알고리즘 적용 시점을 나타낸다.[3]



<그림 2. 가능한 알고리즘 적용시점>

압축된 컨텐츠는 일반적으로 컨텐츠 입력단, 디코더, 출력단을 거쳐서 스피커(또는 모니터)로 최종 출력되게 된다. 따라서 보호 알고리즘의 가능한 적용 시점은 입력단에서 디코더 사이, 디코더에서 출력단 사이가 될 수 있다. 일반적으로 컨텐츠의 입력단에서는 사용자의 해당 컨텐츠에 대한 접근 및 사용 허가의 유무성에 대하여 검사하며, 디코딩 후에는 주로 대상 컨텐츠가 정당한 컨텐츠인가를 확인하는 기능을 갖는다. 각 시점에서 적용되는 보호 알고리즘의 종류로는, 입력부에서는 주로 암호화된 컨텐츠를 복호화 하기 위한 알고리즘과 복호화 된 압축 비트스트림 상으로부터 워터마크를 추출하는 비트스트림 워터마킹 알고리즘이 사용될 수 있으며 디코더 이후에 적용되는 보호 알고리즘은 PCM(Pulse Coded Modulation)레벨에서 워터마크를 추출하는 PCM 워터마킹 알고리즘이 사용될 수 있다.

2.3 다양한 사용 규칙 정의

요즘 사용자들은 단순히 컨텐츠를 한번 구입하고 무한적으로 사용하는 소비 형태에서 벗어나서 컨텐츠 사용 횟수 또는 컨텐츠 사용 시간에 따른 서비스 요금 부과를 달리 할 것을 요구하거나 컨텐츠를 편집하여 일부를 다른 곳에 인용하기도 하며 1 회 컨텐츠 이용 권한을 사서 친구에게 선물 형태로 컨텐츠 사용권리를 전송할 수도 있다. 이러한 다양한 소비 형태를 만족시키기 위하여 사용자의 각 권리를 기술할 수 있는 언어가 필요하다. 현재 XrML, ODRL, cIDf, MPEG REL/RDD 등이 이러한 목적을 위하여 개발되고 있는 대표적인 언어들이다. 디지털 컨텐츠 보호 시스템에서

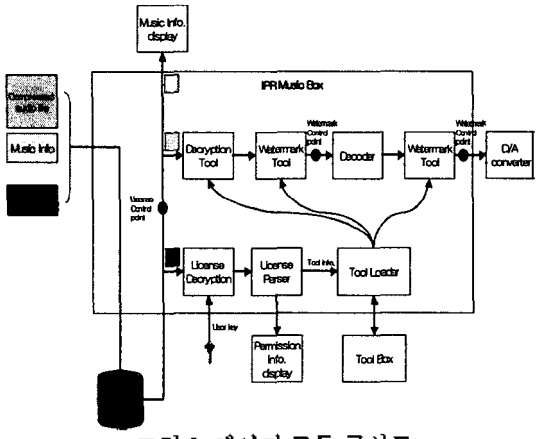
소비자의 컨텐츠에 대한 권리와 권리에 기술된 컨텐츠 사용을 위하여 필요한 정보를 담고 있는 파일을 라이센스(license)라 하며 라이센스의 구조를 라이센스 스키마(schema)라 한다. 라이센스 스키마는 미래의 새로운 권리 기술을 위하여 확장 가능해야 하며 내용의 기밀성 및 무결성 검사를 위한 서명 항목 등이 필요하다.

2.4 사용자들 간의 super-distribution

사용자들 사이의 컨텐츠 공유는 소극적인 면으로는 컨텐츠 불법 배포의 가장 일반적인 형태이지만 이를 적극적으로 이용한다면 컨텐츠 소비를 활성화 시킬 수 있는 가장 강력한 방법 중 하나이다. 이는 컨텐츠와 컨텐츠 사용 권리를 독립적으로 관리하므로 가능하다. 컨텐츠 서비스 제공자는 컨텐츠를 암호화 하여 배포하고 이를 사용하기 원하는 소비자는 그 컨텐츠에 대한 라이센스를 구입하도록 한다. 라이센스는 권리에 대한 비용을 지불한 사람만 사용할 수 있도록 역시 암호화 되어 전송하므로 불법적인 사용자가 다른 사람의 라이센스를 복사하여 컨텐츠를 이용할 수 없도록 한다.

3. 라이센스와 워터마크를 이용한 MP3 재생 제어

여기서는 위 절에서 제시한 기본 개념을 MP3 플레이어에 적용시킨 시스템을 설명한다. 그림 3 은 라이센스와 워터마크를 이용하여 MP3 오디오 파일의 재생을 제어하기 위한 시스템의 구성도를 보여준다.



<그림 3. 제어기 모듈 구성도>

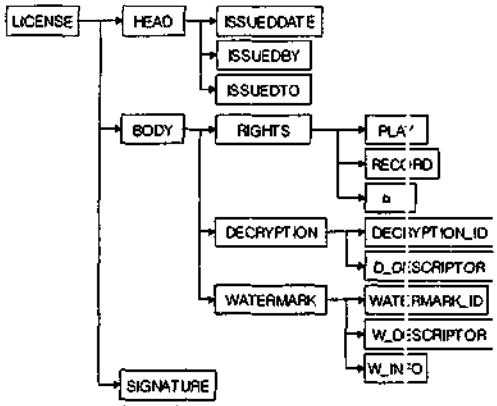
재생 제어기의 입력으로 암호화된 MP3 오디오 데이터와 오디오 데이터에 대한 서비스 정보(곡 제목, 가수 이름, 제작 년도, 리소스 위치, 요금 결재를 위한 URL 등)를 담고 있는 메타데이터 파일 그리고 암호화된 라이센스 정보가 들어가게 된다. 이 모두는 서버로부터 다운로드 되어 클라이언트의 안전한 로컬 스토리지(local storage)에 저장된다고 가정한다.

시스템이 초기화 되면 로컬 디스크에 저장되어 있는 오디오 파일들의 목록을 사용자에게 보여주고, 각 곡에 대한 메타데이터 파일을 읽어 들여 사용자들이 목록 상의 각 곡에 대한 정보를 참고할 수 있도록 한다. 사용자는 메타데이터 정보를 참고하여 재생을 원하는 곡을 선택하게 되고 재생을 시작하면 시스템은 먼저, 선택한 곡에 대한 라이센스 파일이 사용자 단말에 존재하는 지를 검사하게 된다. 라이센스 파일이 있다면 해당 라이센스 파일의 복호화를 위하여 사용자 키를 요구하게 된다. 사용자 키는 사용자 단말(또는 단말 프로그램)의 고유한 키이며 시스템 안에 안전하게 저장되어 있다고 가정한다. 사용자의 키를 요구하는 과정은 함축된 과정(implied process)으로 시스템 안에서 자동적으로 이루어지므로 사용자는 자신의 키를 알 필요가 없다. 따라서 불법적인 사용자가 다른 사람의 라이센스를 가져와 자신의 단말에서 사용하려 한다 할지라도 사용자키가 일치하지 않으므로 이를 사용할 수 없다. 사용자 키에 의하여 복호화 된 라이센스 파일은 라이센스 정보를 추출 하기 위하여 파서(parser)로 보내진다. 파싱을 통하여 추출된 정보 중, 사용자 권리에 대한 정보(재생 허용 회수, 시간 등)는 사용자가 참조할 수 있도록 화면에 디스플레이(display) 되고 암호화된 오디오 파일을 위한 복호화 툴과 삽입된 워터마크의 추출을 위한 워터마킹 툴에 관한 정보, 그리고 툴을 초기화 하는데 필요한 정보들은 Tool Loader 로 보내어지게 된다.

Tool Loader 는 이 정보들을 바탕으로 Tool Box 로부터 필요한 툴들을 로딩하고 초기화 하게 된다. 각 툴의 초기화가 끝나면 오디오 파일은 Decryption Tool 에 의하여 복호화 되고 Watermarking Tool 에 의하여 압축된 오디오 파일에 삽입된 워터마크를 추출하게 된다. 일정 시간동안 Watermarking Tool 에서 추출된 워터마크 정보가 라이센스 안의 워터마크 정보와 일치한다면 오디오 파일의 디코딩과 재생이 정상적으로 수행되고, 만일 정당한 워터마크가 추출되지 않는다면 재생이 멈추게 된다. 마지막으로 수행된 권리에 대하여 라이센스 정보를 갱신하게 된다.

3.1 라이센스 정보

본 시스템에 적용된 라이센스 정보는 XML 기반으로 기술되었으며 그 구조는 그림 4 와 같다. [4~5]



<그림 4. 라이센스 엘리먼트 구조>

먼저 HEAD 엘리먼트는 라이센스의 발행날짜를 나타내는 ISSUEDDATE 엘리먼트와 라이센스 발행처를 나타내는 ISSUEDBY 엘리먼트, 그리고 라이센스를 발급하는 대상을 나타내는 ISSUEDTO 엘리먼트로 이루어져 있다. 라이센스의 주 내용을 포함하는 BODY 엘리먼트는 라이센스를 구입한 대상에게 허가되는 권리를 나타내는 RIGHTS 엘리먼트와 복호화 툴과 워터마킹툴에 대한 정보를 갖는 DECRYPTION 엘리먼트와 WATERMARK 엘리먼트로 이루어져 있다. RIGHTS 엘리먼트는 오디오 파일에 대하여 사용자가 애플리케이션 프로그램 상에서 수행할 수 있는 각 권리와 규칙을 나타낸다. 예를 들어 PLAY 의 권리에 대한 규칙은 재생 횟수와 재생 시간으로 제한할 수 있다. DECRYPTION 엘리먼트는 여러 가지 복호화 툴 중에서 필요한 복호화 툴을 식별하기 위한 DECRYPTION_ID 엘리먼트와 복호화에 필요한 Key 및 다른 파라미터들을 위한 D_DESCRIPTOR 엘리먼트로 구성된다. WATERMARK 엘리먼트 역시 다양한 워터마킹 툴들 가운데, 필요한 워터마킹 툴을 호출하기 위한 WATERMARK_ID 엘리먼트와 워터마킹 알고리즘에 사용될 수 있는 Key 및 다른 파라미터들을 위한 W_DESCRIPTOR 엘리먼트, 그리고 컨텐츠에 삽입된 워터마크를 나타내는 W_INFO 엘리먼트로 구성된다. 마지막으로 SIGNATURE 엘리먼트는 해당 라이센스에 대한 무결성을 검사하기 위한 엘리먼트이다.

4. 결론

본 논문에서는 사용자 단말 시스템 상에서 보호 알고리즘들 간의 상호 운용성, 다중 보호 알고리즘 적용, 다양한 사용 규칙 정의 및 사용자들 간의 super-distribution 기능을 만족할 수 있는 방법을 제안하였고 이를 MP3 플레이어에 적용하였다. 보호 알고리즘들 간의 interaction 이 필요한 경우에는 서로 필요한 메시지를 주고 받을 수 있는 메커니즘이 필요하며 이에 대한 연구가 앞으로 이루어져야 할 것으로 보인다. 또한 실제 상용 컨텐츠 서비스에 라이센스를 적용하기 위해서는 라이센스 스키마에 대하여도 더욱 연구가 필요하다.

감사의 글

본 논문은 정보통신부 지원 "디지털 컨텐츠 관리 기술 개발" 과제의 결과물로서 관계자 분들에게 감사의 글을 드립니다.

참고문헌

[1] Mauro Barni, Franco Bartolini, Ingemar J.Cox, Juan Hernandez, Fernando PerezGonzaiez, "Digital Watermarking For Copyright Protection: A Communications Perspective", IEEE Communications Magazine, pp. 90-133, 2001.

[2] Christian Neubauer and Jurgen Herre, "Advanced Watermarking and its Applications", Audio Engineering Society. 109th Convention, 2000.

[3] FPDAM ISO/IEC 14496-1:2001 / AMD3

[4] CONTENTGUARD, "XrML : Extensible rights Markup Language", ver 1.3.

[5] IPR Systems, "ODRL: Open Digital Rights Language", ver 0.8.

[6] Bum Suk Choi, Sarah Jung, Jin Woo Hong, "Application Research of Bitstream Watermark for Contents Protection", ISMC2001, pp. 193-196, 2001.