오디오 저작권 보호 시스템 기술의 현황과 분석

최재각* · 김지홍**

1. 서 론

최근 컴퓨터 네트워크를 통한 디지털 컨텐츠의 유통이 활발해지면서 각종 저작권 문제가 수면 위로 부상하기 시작하였다. 이에 사용자에게는 합법적인 컨텐츠의 편리한 사용을 가능하게 하며, 동시에 저작권자들의 권리를 보호할 수 있는 시스템에 대한 연구가 활발히 진행되고 있다. 특히 오디오 분야에서는 MP3(MPEG-1 layer-3)가 저작권 문제를 해결하지 않고 대중화되어 각 나라에서는 이를 해결하기 위해 많은 노력을 기울이고 있다. 그리고 각 사용자에게 인증된 키(key)를 부여하고 음악을 다운로드할 때 키에 맞는 암호를 걸어 배포하는 등 불법 복제 방지 시스템의 기능을 강화하고 있다. 최근에는 불법으로 유통되던 MP3 오디오가 이러한 불법 복제 방지 시스템의 개발로 인해 네트워크 상에서 유료로 유통이 되기도 한다. 이러한 MP3의 전철을 거듭하지 않기 위해서 MP3보다 음질이 우수한 MP4(MPEG-2 AAC: Advanced Audio Coding)는 처음부터 저작권 보호 시스템에 기반해서 유통될 것이다.

오디오 파일의 안전한 유통을 위하여 AT&T, 삼성전자 등 각국의 정보통신 업체들은 저작권 보호 시스템 개발에 많은 노력을 기울이고 있다. 대표적인 저작권 보호 시스템으로는 AT&T의 PolicyMaker[1], 삼성전자의 SecuMAX[2], 그리고 Liquid Audio사의 Liquidfier Pro 등이 있다. 이와 같이 각 업체들이 다양한 저작권 보호 시스템을 개발하고 있고 또한 현재 상용서비스를 실시하고 있지만, 그들간의 호환성이 결여되어 파일에 맞는 플레이어에서만 음악을 들을 수 있어 사용자는 모든 업체의 플레이어를 설치해야 하는 불편함이 있다. 따라서 이러한 불편함을 없애고 각 국가별로 또는 전 세계적으로 표준을 마련하기 위한 관련 단체들의 움직임이 최근에 들어 활발해지고 있다. 대표적인 단체로서 미국의 음반산업협회(RIAA)[3]를 중심으로 결성된 SDMI(Secure Digital Music Initiative)[4]를 들 수 있다. 국내에서도 한국 음악저작권협회를 비롯한 관련 단체들을 중심으로 저작권 보호를 위한 다양한 활동을 진행중에 있다.

본 논문에서는 SDMI를 비롯한 저작권 보호 단체들의 활동 현황과 규격을 소개하고, 각 정보통신 업체들의 오디오 파일 저작권 보호 시스템에 대해서 설명한다.

2장에서는 오디오 저작권 보호를 위한 국가 및 단체의 규격에 대해 조사 분석하고, 3장에서 현재 개발되어 사용중인 오디오 저작권 보호 시스템을 분석한다. 마지막으로 4장에서 결론을 맺는다.

*동의대학교 컴퓨터공학과 조교수
**동의대학교 영화영상공학과 조교수

2. 국가 및 단체 규격 분석

2.1 개요

오디오 저작권 보호 단체로는 미국의 음반산업협회를 중심으로 구성된 SDMI와 인터넷을 통한 오디오 전송을 목적으로 하는 AES (Audio Engineering Society)의 오디오 저작권 관련 소위원회 AES SC-06-04[5] 등이 있다. SDMI는 RIAA를 비롯하여 세계적인 음악사들과 마이크로 소프트, AT&T, IBM, 소니 등 세계적인 정보통신 업체들이 참여해 만든 국제포럼이다. SDMI는 전세계 MP3 음악 복제방지 표준 시스템을 선정하기 위해서 SecuMAX의 삼성전자와 미국의 Liquid Audio, 독일의 Fraunhofer[6] 등 많은 업체들로부터 제안서를 받았다. SDMI는 두 단계로 표준을 선정하기로 하였는데, 첫단계로서 ARIS사의 MusiCode 워터마크를 불법복제 방지 방법으로 선정하였다.

국내에서는 한국음악저작권협회, 한국연예 제작자협회, 한국레코딩뮤지션협회, 한국음악 출판사협회 등 주요 음악 권리자 단체들이 주축이 되어 PC통신업체, 정보제공업체(IP) 등과 MP3 음악에 대해 불법복제 방지 시스템을 채용할 예정이다. 관련 단체들은 MP3 불법복제 방지 시스템의 요건으로 온라인상의 종·횡·상·하간 불법복제 방지능력, 다운로드의 안정성, 다른 시스템 및 플레이어와의 호환성, 국제표준 만족도, 이용요금 징수현황 관리 등을 정하였다. 국내에서 현재 서비스를 시행하고 있는 시스템으로는 삼성전자의 SecuMAX, LG 전자와 BR 네트콤의 캡슐 오디오[7] 등이 있다.

2.2 SDMI(Secure Digital Music Initiative)

SDMI는 현재 인터넷 상에서 널리 유통되고 있는 MP3 음악 파일과 MP3에 비해 성능이 우수한 MP4 등의 디지털 컨텐츠에 대한 안전한 유통을 위하여 음악사들과 정보통신 업체들이 참여해 1999년 초부터 활동을 시작한 단체이다[4]. SDMI는 특히 1세대 portable device에 대한 규격을 제정하기 위하여 SDMI 산하에 소그룹인 PDWG (Portable Device Working Group)을 만들어 세계 각 정보통신 업체들로부터 제안서를 받아 규격을 제정하였다. SDMI는 PDWG에서 제정하는 규격이 SDMI 전체의 목적에 부합되어야 한다는 규정을 두어 PDWG의 결과를 그대로 SDMI 전체 시스템에도 적용 가능케 하였다.

그림 1은 PDWG 표준 모델(Reference Model)이다. SDMI PDWG 표준 모델은 Licensed SDMI-Compliant Module(LCM), SDMI Portable Device (PD), 그리고 SDMI-Compliant Storage Media로 구성되어 있다. LCM은 CD, DVD와 그 밖의 입력원으로부터 저작권 보호가 필요한 *content*와 저작권 보호의 규칙인 *rules*를 받아서 이를 SDMI-Compliant Storage Media및 SDMI PD와의 안전한 통신을 하게 된다. *rules*는 LCM의 *content* 관

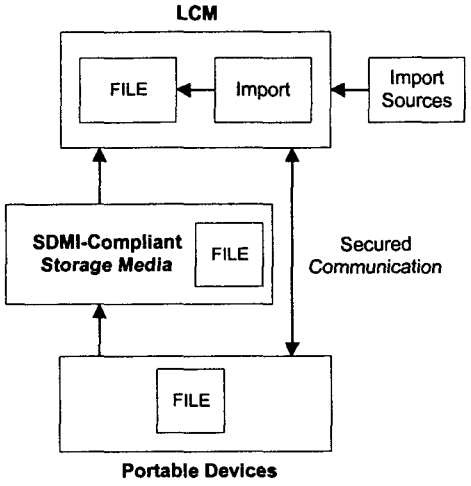

그림 1. SDMI PDWG 표준 모델

리, 저작권 보호, 그리고 SDMI-Compliant Storage Media와 SDMI PD 간의 데이터 송수신 방식 등을 결정한다.

SDMI에서 요구하는 기능 요구사항(functional requirement)을 각 부분별로 정리하면 다음과 같다.

2.2.1 LCM의 요구사항

- LCM은 SDMI 음악을 보안성 없는 디지털 음악으로 변환하지 않아야 한다.
- LCM은 컨텐츠 관리를 위해 안전하고 보안성이 있는 환경을 제공해야 한다.
- LCM은 SDMI-Compliant Storage Media 또는 PD 등과 통신할 때 안전한 통신을 제공해야 한다.

2.2.2 SDMI PD의 요구사항

- PD는 SDMI 음악을 보안성 없는 디지털 음악으로 바꾸지 않아야 한다.
- PD는 마이크로폰 입력을 제공할 수 있다.
- PD는 아날로그 입력, 출력 보안을 제공할 수 있다.

2.2.3 LCM/PD Interaction의 요구사항

- LCM은 *rules*에 부합하여 보안성이 있는 컨텐츠를 재생해야 한다.
- PD는 LCM에 의해 처리된 적당한 규칙에 따라서 보안성이 있는 컨텐츠를 재생해야 한다.
- LCM과 PD는 온라인 및 오프라인으로 동작할 수 있어야 한다.

3. 저작권 보호 시스템의 조사 분석

대표적인 오디오 저작권 보호 시스템은 삼성전자의 SecuMAX, AT&T A2B Music의 PolicyMaker, NTT & KOBELCO의 전자 Sukashi, 그리고 Liquid Audio 사의 Liquidfier Pro 등이 있다. 이들의 주요 특징 및 기능은 다음과 같다.

3.1 PolicyMaker

PolicyMaker는 AT&T사가 개발한 오디오 저작권 보호 시스템으로서 적용 가능한 파일 형식은 MP4이다. MP4는 AT&T, 톰슨, Fraunhofer 등의 업체가 공동으로 만든 규격으로 MP3에 비해 음질이 우수하고 압축률이 높다. MPEG-1 Layer-2에 비해서는 2배, MP3에 비해서는 1.4배의 압축률을 갖는 오디오 형식이며, Twin VQ와 함께 차세대 오디오 파일 형식으로 많이 사용되어 질 것으로 예상된다. MP4에 사용되는 대표적인 기술로는 허프만 부호화, 양자화 및 스캐일링, 역방향 적응적 예측, temporal noise shaping (TNS), 그리고 변형된 DCT 등이 있다. 그리고 대표적인 MP4 플레이어는 Homeboy AAC, BitAAC, Astrid/Quartex AAC, 그리고 AT&T의 A2B 등이 있다. A2B는 AT&T Proprietary 압축 알고리즘, CryptoLib Security Library, 그리고 PolicyMaker의 세 부분으로 구성되어 있다. AT&T Proprietary 압축 알고리즘은 MP3에 비해서 성능이 월등히 우수하며, 음질에 큰 손실이 없이 최대 20:1의 압축률을 가질 수 있다. 그리고 이러한 압축 알고리즘에 의해서 압축된 오디오 파일이 인터넷을 통하여 유통되기 위해서는 보안 알고리즘이 필요한데, CryptoLib Security Library가 RSA와 DES를 비롯한 많은 보안 알고리즘을 제공한다.

PolicyMaker는 다른 방식들과는 달리 중앙집중식 인증 관리에서 탈피하여 Public Key와 Secret Key를 PGP와 X.509의 적용원리를 통해 인증하는 복제방지 시스템이다[8]. 그림 2는 PolicyMaker의 구조를 나타낸다. 사용자의 요구(signature)가 있으면 데이터베이스 내의 License

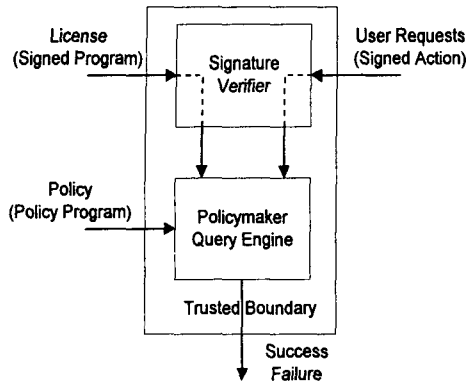

그림 2. PolicyMaker의 구조

와의 비교를 통해 사용자 요구에 대한 검증을 한 다음, PolicyMaker에서 인증 여부를 결정하는 구조이다. 지금까지 나와있는 대부분의 보안 알고리즘은 중앙 집중식 관리 방식인데 A2B는 여기에서 탈피하여 Public Key와 Private Key를 이용하여 오디오의 안전한 관리를 가능하게 한다. 그림 3은 A2B의 오디오 관리 개념을 보여 주고 있다.

3.2 SecuMAX

삼성전자는 국내 최초로 PC용 소프트웨어 오디오 플레이어 Music driver로 1999년부터 MP3 음악파일에 대한 상용 서비스를 시작하고 있다. Music driver에는 복제방지 시스템인 SecuMAX가 탑재되어 MP3와 MP4 오디오 파일의 안전한 유통을 가능하게 한다.

SecuMAX는 그림 4와 같이 사용자 인증서비스를 하는 서버와 디지털 파일의 암호화 및 전송을 담당하는 클라이언트로 나뉘어져 있다. SecuMAX 서버는 고객의 ID, 패스워드 및 주민등록번호를 확인하여 그 고객에게 부여된 암호 해독키를 제공하며, 검증된 보안모드와 암호화 과정의 수시 변경을 통해 안정성을 확보한다. 그리고 SecuMAX 클라이언트는 준비된 컨텐츠가 다운로드될 때 on-the-fly 방식으로 암호화가 되어 디지털 컨텐츠 서비스업자(CP)가 데이터 변환 없이 사용할 수 있으며, 컨텐츠 서비스업자가 설치를 원할 경우 저작권 소유자로부터 승인을 받으면 설치가 가능하다.

SecuMAX는 암호화 알고리즘으로 Block Cipher SNAKE를 사용하고 있으며, 키 생성 방법으로서 Block Chained Hashing 알고리즘인 MD5를 적용하고 있다.

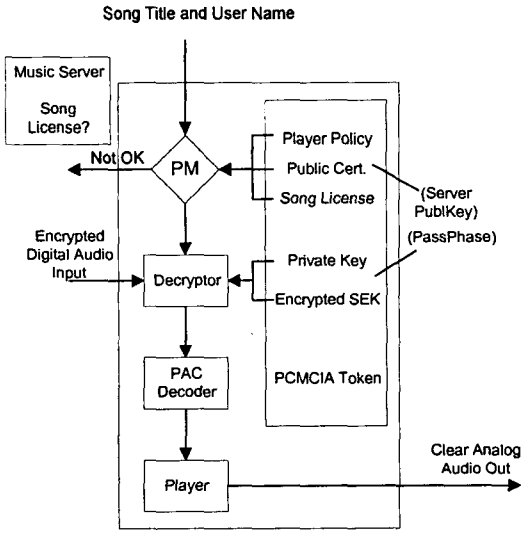

그림 3. A2B의 안전한 음악 파일 관리 도구

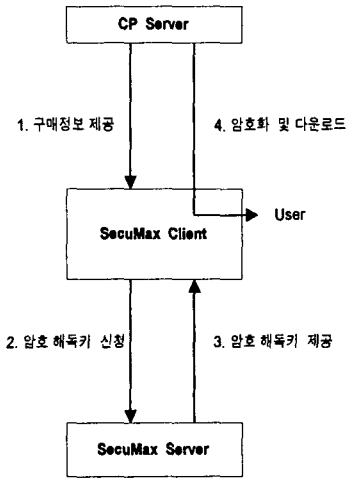

그림 4. SecuMAX의 개념도

3.3 그 외의 저작권 보호 시스템

3.3.1 Liquidfier Pro

Liquid Audio사에서 개발된 Liquidfier Pro는 극장과 TV 등의 일반 미디어 사운드 시스템에서 사용되고 있다. 지원하는 입력 파일 형태는 Dolby digital AC3와 MPEG-2 AAC이다. Liquidfier Pro에 사용된 암호화 알고리즘의 특징은 다음과 같다.

- RSA 인증 암호화 알고리즘을 채택
- Multi-layer security 방식의 워터마킹 기법 사용
- Liquidfier Pro로 자체 인코딩
- Liquid Music Server로 상거래 지원
- RSA알고리즘을 적용한 MusicPassport는 Liquid Track이라는 부가정보를 담고있는 음악파일 형태를 구입하여 합법적인 재생을 가능하게 함

3.3.2 InterTrust

InterTrust Technology사에서 개발되었으며, 정보보안 및 거래, 암호화 키 관리 시스템으로 안전한 프로토콜(secure protocol)인 NNCP를 통해 DigiBox라는 컨텐츠 컨테이너를 교환하여 오디오 파일을 거래한다. InterTrust에서는 InterRights Point가 데이터에 암호화와 정보 캡슐링을 하고, Business Rules/Cryptographic key 생성 등의 작업 및 곡에 대한 다양한 정보의 입력을 가능하게 한다. 지원 파일 형태로는 MPEG, DVD, AVI, PDF, HTML 등의 멀티미디어 컨텐츠 파일이다. 여기에 사용된 암호화 알고리즘은 다음과 같다.

- InterRightsPoint에 의한 데이터 암호화 및 정보 캡슐링
- InterRightsPont에 의한 Business Rules 및 Cryptographic key 생성

3.3.3 전자 Sukashi

일본의 NTT와 Kobelco사에서 개발하였으며, MP3 및 TwinVQ audio를 입력 파일로 지원한다. 음악의 경우 연속적인 미디어이므로 시간축 방향의 스크램블이 효과적이며 스크램블 해제 시 재생력이 좋다는 점을 이용한다.

전자 Sukashi는 SolidAudio라는 하드웨어 플레이어를 지원하고 있지만 소프트웨어의 지원은 없다. 다음은 전자 Sukashi에서 사용하고 있는 암호화 방식이다.

- TwinVQ 스펙 채용
- 압축과 스크램블링으로 워터마킹을 적용한 배포시스템
- Pitch, gain, LSP, Forward Envelope, MDCT 등 5종의 음악 데이터 파라미터에 스크램블을 거는 방식

3.3.4 GMO MP4 방식

Secure Computer Communications사에서 개발한 시스템으로서, 인스톨된 디코더를 이용하여 오디오 파일을 재생하는 다른 시스템과는 달리 오디오 파일 내에 디코더 프로그램이 내장되어 있는 방식이다. 따라서 이 시스템은 여러 파일을 순서적으로 듣는 플레이 리스트를 이용할 수 없고, 다른 시스템과의 호환성도 문제가 된다.

3.3.5 캡슐 오디오

LG 인터넷, LG 전자, BR 네트콤 등 3사가 공동으로 개발한 캡슐 오디오는 보안/인증 패키지인 캡슐 시스템의 한 부분으로 디지털 오디오에 캡슐의 기술을 적용시킨 제품이며, MP3에 대해 음악 전문 사이트인 MPNETS(www.mpnets.com)에서 서비스 중이다. 캡슐 오디오에서 사용하고 있는 암호화 알고리즘은 다음과 같다.

- 암호화 방식에 Blow Fish 알고리즘을 채택

- 사용자 인증 방식은 가변형 개인 키 형태인 토큰을 사용
- 스마트 카드를 지원하는 off-line에서의 사용자 인증 기능

3.3.6 Fraunhofer IIS-A Audio & Multimedia

독일의 Fraunhofer사에서 개발되었으며 MP3와 MP4 방식의 오디오 파일 뿐만 아니라, MPEG-4와 ITU-T H.263 등과 같은 비디오 파일에 대해서도 적용 가능하다. 또한 실시간 처리를 위한 DSP 솔루션을 제공하고 있으며, 현재 멀티미디어 컨텐츠에 대한 저작권 보호 알고리즘을 개발 중에 있다.

4. 결 론

최근에 오디오 저작권 보호의 필요성이 대두되면서 각국의 정보통신 업체들은 보다 우수한 성능의 오디오 저작권 보호 시스템을 개발 중에 있으며, 여러 국가 단체에서는 이를 표준화하기 위한 작업을 활발히 진행 중에 있다. 대표적인 오디오 저작권 보호 시스템은 삼성전자의 SecuMAX, AT&T A2B Music의 PolicyMaker, NTT & KOBELCO의 전자 Sukashi, 그리고 Liquid Audio사의 Liquidfier Pro 등이 있다. 그리고 대표적인 표준화 단체로는 미국음반협회를 중심으로 한 SDMI가 있다. 국내에서도 여러 관련 단체들을 중심으로 표준화 작업에 많은 노력을 기울이고 있지만 여러 업체들 간의 이해관계로 인해 계속 연기되고 있는 실정이다. 따라서 빠른 시일 내에 국내 표준을 정하여 서비스를 통일함으로써 사용자에게는 편리하고 안전한 사용을 돕고, 저작권자에게는 저작권의 보호를 가져올 수 있을 것이다.

참 고 문 헌

[1] http://www.a2bmusic.com
[2] http://www.m4you.com
[3] http://www.riaa.com/tech/sdmiinfo.htm
[4] http://www.sdmi.org/
[5] http://www.aes.org/
[6] http://iis.fhg.de/amm/
[7] http://www.brnetcomm.co.kr/item/capsuleAudio/newversion/conc.html
[8] M. Blaze, J. Feigenbaum, and Jack Lacy, "Decentralized Trust management," *in Proc. IEEE Conference on Security and Privacy*, Oakland, CA, May 1996.
[9] http://www.globalmusic.com
[10] http://www.kisa.or.kr/

최 재 각

- 1984년 2월 경북대학교 전자공학과 졸업 (공학사)
- 1987년 2월 한국과학기술원 전기 및 전자공학과 졸업(공학석사)
- 1997년 8월 한국과학기술원 전기 및 전자공학과 졸업(공학박사)
- 1987년 2월~1998년 2월 한국전자통신연구원 선임연구원
- 1998년 3월~2001년 8월 경일대학교 제어계측공학과 조교수
- 2001년 9월~현재 동의대학교 컴퓨터공학과 조교수
- 관심분야 : 영상처리, 영상 및 멀티미디어 통신, 워터마킹 등
- E-mail : cjg@deu.ac.kr

김 지 홍

- 1986년 2월 경북대학교 전자공학과 졸업(공학사)
- 1988년 2월 경북대학교 대학원 전자공학과 졸업(공학석사)
- 1996년 8월 포항공과대학교 대학원 전자전기공학과 졸업(공학박사)
- 1988년 2월~1997년 2월 한국전자통신연구원 선임연구원
- 1997년 3월~2002년 2월 부산외국어대학교 컴퓨터공학과 조교수
- 2002년 3월~현재 동의대학교 영화영상공학과 조교수
- 관심분야 : 영상처리, 컴퓨터그래픽스, 워터마킹 등