제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

MPEG-4 IPMPX 를 적용한 MP3 플레이어

최범석, 석종원, 홍진우
한국전자통신연구원
e-mail : bschoi@etri.re.kr, jwseok@etri.re.kr, jwhong@etri.re.kr

MP3 player with MPEG-4 IPMPX

Bum Suk Choi, Jong Won Seok, Jin Woo Hong
ETRI

요 약

현재 MPEG 국제 표준화 기구에서는 MPEG-4 IPMPX(Extensions of Intellectual Property Management and Protection system) 분야를 통하여 다양한 벤더(vendor)들에 의하여 개발된 서로 다른 보호 툴들이 하나의 사용자 단말 시스템에서 적용될 수 있도록 그 구조를 정의하고 있다. 이 기술은 각 툴을 유일하게 식별하도록 하는 툴 ID 와, 단말 시스템과 툴 사이, 또는 툴과 툴 사이에 의사소통을 위한 공통된 메시지 클래스에 기반을 두고 있다. 본 논문은 현재 표준화가 진행되고 있는 MPEG-4 IPMPX 규격[1]에 정의된 IPMPX 메시지를 통하여 동작할 수 있는 오디오 워터마킹 툴의 구현과 구현된 툴과 IPMP 시스템과의 연동에 관한 것이다. 구현된 툴이 실제 IPMPX 단말 시스템과 이상 없이 동작하는 것을 확인하기 위하여 IPMPX 규격에 정의된 Message Router 와 Tool Manager 를 MP3 플레이어에 적용한 단말 시스템에 기존의 복호화 툴과 구현된 워터마킹 툴을 연동하였으며, 암호화되어 입력된 MP3 파일이 복호화, 디코딩, 워터마크 추출 과정을 통과하여 이상 없이 재생됨을 확인하였다

1. 서론

최근까지 양질의 디지털 콘텐츠를 보호하기 위한 다양한 알고리즘들이 여러 벤더들에 의하여 개발 되었다. 이러한 알고리즘들은 그 안전성 면에서는 지속적인 검증을 통하여 발전되고 있으나 범용성에 있어서는 아직 그 중요성에 대한 인식이 부족하다. 디지털 방송이 실현된다면 이를 시청하고자 하는 사용자들은 모두 셋톱 형태의 단말기를 가지고 있어야 한다. 만일 콘텐츠를 보호하기 위한 알고리즘들이 범용성이 없다면 새로운 알고리즘의 추가나, 교체가 필요할 경우, 단말 시스템 자체에 큰 영향을 줄 수 있다. 방송 환경과 같이 단말 소유자가 수백만 이상일 경우에 이는 곧 엄청난 비용을 의미하게 된다. 따라서 이러한 알고리즘들이 기계의 부속품과 같이 하나의 툴로 시스템 안의 다른 모듈들에 큰 영향을 주지 않고도 추가, 제거, 교체되어 사용될 수 있는 환경을 제공하는 것이 필요하다. MPEG-4 IPMPX 에서는 각 콘텐츠 보호 알고리즘을 보호 툴(tool)의 개념으로 보고 다양한 보호 툴들을 식별할 수 있는 툴 ID 를 기반으로하는 툴 호출과 이들간의 정보 교환을 위한 공통된 메시지 클래스를 정의하고 있다. 또한 단말에서 툴을 관리하기 위한 TM(Tool Manager)과 툴 과 툴 사이, 또는 툴과 단말 시스템 사이의 메시지 전달을 위한 MR(Message Router)을 정의하고 있다[2].

본 연구의 최종 목표는 MPEG-4 IPMPX 시스템과 MPEG-4 참조 소프트웨어(IM1 player)와의 정합 및 다양한 콘텐츠 보호 툴들과의 연동이다. 이를 위하여 먼저 MPEG IPMP 시스템을 간단한 MP3 플레이어에 구현하고 본 시스템을 사용하여 MPEG IPMP 규격을 따르는 보호 툴들과의 연동 시험을 한 후, 마지막으로 MPEG-4 참조 소프트웨어와 IPMPX 시스템을 정합하는 것이다. 본 논문은 그 중간 결과로, MPEG-4 IPMPX 시스템을 간단하 MP3 플레이어에 구현하고 MPEG-4 IPMPX 규격에서 정의하고 있는 메시지 클레스와 자체 정의한 메시지 클래스에 의하여 작동할 수 있는 다양한 보호 툴과의 연동에 대한 것이다.

2. MPEG-4 IPMPX 시스템

MPEG-4 IPMPX 규격서에 정의된 항목 중, 다음 항

목들이 본 시스템에서 구현되었다.

- IPMP 툴들 간, 또는 IPMP 툴과 단말 시스템 간의 메시지 전달 역할을 하는 MR
- 필요한 툴들이 단말에 존재 하는가를 조사하고 그 툴을 작동시키는 역할을 하는 TM
- MPEG-4 IPMPX 규격서에 정의된 메시지들
- IPMPX 콤포넌트들과(MR 과 TM) 미디어 스트림 처리 시스템(예: IM1 플레이어) 사이의 인터페이스

다음과 같은 역할을 하는 IPMP 툴들이 구현 되었다.

- Rights Management(RM) 툴: 간단히 사용자의 Username 과 Password 를 물어보는 툴
- 복호화 툴: AES 알고리즘을 사용하여 암호화된 콘텐츠를 복호화 하는 툴
- 워터마킹 툴: 대역확산을 이용하여 raw 오디오 데이터로부터 워터마크를 추출하는 툴

덧붙여, Rights Management 툴과 단말 시스템 간의 상호 인증이 구현되었다.

그림 1 은 구현된 단말 시스템의 기능을 보여준다 [7].

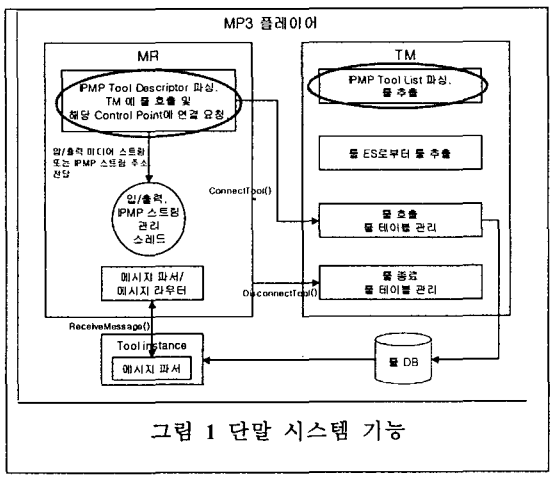

그림 1 단말 시스템 기능

이러한 단말 시스템은 MR 과 TM 을 구동 시키고, 사용자와의 간단한 인터페이스를 제공하며, 입력 데이터로부터 콘텐츠를 추출하고 파싱한다. 또한 IPMP 툴들과의 상호인증을 제공하고 IPMP 툴들과의 메시지 교환을 가능하게 하며, MP3 오디오 디코딩과 랜더링을 수행한다.

본 단말 시스템의 대상이 MPEG-4 콘텐츠가 아닌 MP3 오디오 데이터이므로 MPEG-4 파일 시스템의 IOD(Initial Object Decriptor)로부터 Tool list 를 추출하여 파싱하는 부분과 OD(Object Decriptor)로부터 IPMP Tool Descriptor 를 추출하여 파싱하는 부분(원으로 표시)은 구현되어 있지 않다.

그림 2 는 위에서 언급한 콤포넌트들이 stand-alone 플레이어 구조 상에서 어떻게 구성되어 있는가를 보여준다.

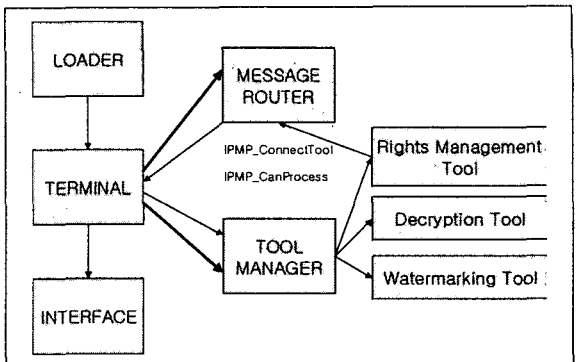

그림 2 소프트웨어 모듈 구조

단말 시스템 소프트웨어는 사용자에게 원하는 MP3 곡의 파일 이름을 묻고 해당 MP3 파일을 열며 단말 시스템을 구동시키는 LOADER 모듈, Tool List 를 IOD 로부터 가져오고 MR 과 TM 을 구동시키며 TM 이 RM 툴을 로딩하도록 요청하는 역할을 하는 TERMINAL 모듈, 그리고 사용자에게 Username 과 Password 를 묻는 INTERFACE 모듈로 이루어져 있다. 툴들간 또는 툴과 TERMINAL 모듈간 메시지를 전달해 주는 역할을 하는 MESSAGE ROUTER 와, IPMP 툴들을 로딩시키는 역할을 하는 TOOL MANAGER 모듈은 모두 TERMINAL 모듈에 의하여 구동된다. 마지막으로 TOOL MANAGER 모듈에 의하여 구동되는 IPMP 툴들로 Rights Management 툴, 복호화 툴 그리고 워터마킹 툴이 DLL 형태로 구현되어 있다.

3. 콘텐츠 재생 과정

그림 3 은 단말 시스템에서 컨텐츠가 재생 되기까지의 일련의 처리 과정을 보여준다. 회색 객체는 IPMPX 단말 시스템 콤포넌트를 나타내고 투명한 사각형 객체는 IPMP 툴들을 나타낸다. 단말 시스템의 입력으로는 MP3 콘텐트와 함께 IPMPX 관련 정보가 들어간다.

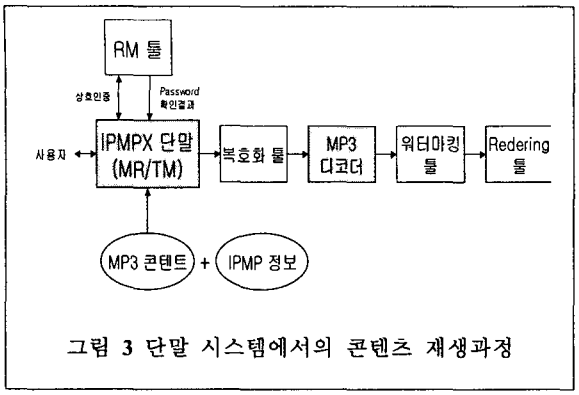

그림 3 단말 시스템에서의 콘텐츠 재생과정

단말 시스템이 셋업되고 MR 과 TM 이 작동되면, 단말 시스템은 재생 가능한 MP3 파일 목록을 사용자에게 보여주고, 사용자는 원하는 MP3 파일 하나를 선택한다. 사용자가 원하는 MP3 파일을 선택하면, Rights Management 툴이 로딩 되고 단말 시스템과의 상호 인증이 이루어진다. 구현된 시스템의 상호 인증은 XML 형식의 공개키 인증서를 상호간에 교환함으로 이루어 지며, 현재는 RM 툴과 터미널 사이에서만 인증이 이루어진다. 다음 버전에서는 challenge-response 과정과 세션키 교환을 사용하여 더욱 견고한 인증을 구현할 계획이다. 상호 인증이 끝나면, 사용자 username 과 password 를 묻게되게 되고 입력된 두 정보를 바탕으로 해쉬 알고리즘을 수행하여 128-bit 키를 생성한다.(해쉬 결과 값의 나머지 값은 절삭 된다) 만일 username 이 옳다면, 다른 툴들이 단말 시스템에 로딩된다.(복호화 툴, 워터마킹 툴이 MP3 디코더와 함께 로딩되고 렌더링 툴이 IPMP 툴로서 로딩된다.) 만일 username 이 옳지 않다면, 에러 메시지가 출력 된다.

만일 입력된 password 가 맞다면, 생성된 키로서 MP3 파일의 복호화를 시작한다. Password 가 틀리다면, 복호화가 되지 않는다.

여기서 컨텐츠는 MP3 파일과 MP3 파일을 재생하는데 필요한 IPMP 툴들에 대한 IPMP Tool list 이다.

4. 워터마킹 툴

워터마킹 툴은 외부로부터 입력되는 메시지들을 분리하는 Message wrapper 부분과 입력된 메시지에 따라 해당 기능을 수행하는 모듈들로 이루어져 있다. 그림 4 는 구현된 워터마킹 툴의 구조도를 보여준다.

다음 메시지들이 워터마킹 툴에 사용되었다.

- 워터마킹 툴을 초기화(sampling rate, bit rate, channel number 등) 하고, 디코딩 툴로부터 PCM 데이터를 받거나 rendering 툴로 워터마크 추출 처리가 끝난 PCM 데이터를 전달하기 위하여 IPMP_ProcessData 메시지를 사용하였다.
- 워터마킹 추출 후 PCM 데이터를 Rendering 툴로 전달하기 위한 link point 를 셋팅하기 위하여 IPMP_ProcessDataInitialize 가 사용되었다.
- 워터마킹 툴을 종료시기키 위하여 IPMP_UnloadMessage 가 사용되었다.

다음 버전에서는 워터마킹 툴을 초기화 시키기 위하여 IPMP_AudioWatermarkingInit 메시지를 사용하고 재생 제어를 위하여 추출된 워터마크를 터미널에 전달하기 위하여 IPMP_SendAudioWatermark 메시지를 사용할 계획이다.

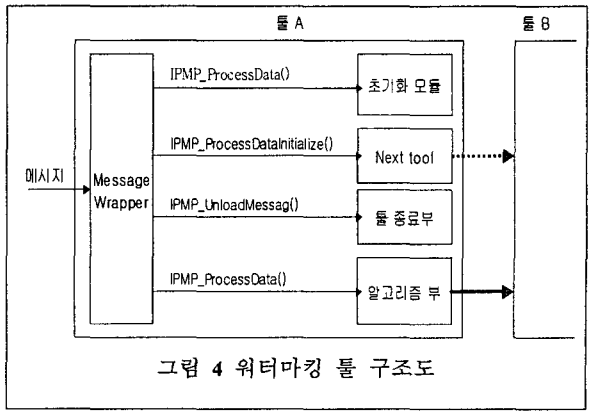

그림 4 워터마킹 툴 구조도

워터마크는 SDMI Phase II screen functionality[8]에 의거하여 삽입되었다. Phase II screen 은 오디오 콘텐츠의 불법 배포를 막기 위한 완전한 해결책으로 제시된 것이다. 디지털 오디오 콘텐츠가 통신 채널과 인터넷과 같은 네트워크를 통하여 배포될 때, 전송의 효율을 높이기 위하여 콘텐츠를 압축하여 콘텐츠 사이즈를 줄여서 전송하게 된다. 이 때, 콘텐츠의 음질을 크게 저하시켜서는 안된다. 따라서, 압축을 여부를 탐지하는 것은 콘텐츠가 불법적으로 배포된 것인가를 검사할 수 있는 효과적인 방법이다. Phase II Screen 에서는 콘텐츠로부터 다음의 워터마크가 추출되는가를 판단한다.

- "no more copies"(NMC bit)
- "do not copy if it has been compressed"(ASSERT bit)

Phase II screen 의 기능은 그림 5 와 같다. Phase II Screen 은 Robust 와 Fragile 워터마크를 미리 정의된 요구사항을 만족하도록 오디오 시그널에 삽입하여 구현한다. 입력된 오디오 신호의 Robust 워터마크를 먼저 추출하여 NMC bit 과 ASSERT bit 을 검사한다. 만일 NMC bit 이 On 이라면 REJECT 하고 Off 라면 ASSERT bit 을 검사한다. ASSERT bit 이 Off 라면 ACCEPT 되고 On 이라면 Fragile 워터마크를 검사한다. 만일 Fragile 워터마크가 살아 있다면 ACCEPT 되

고 그렇지 않다면 REJECT 된다.

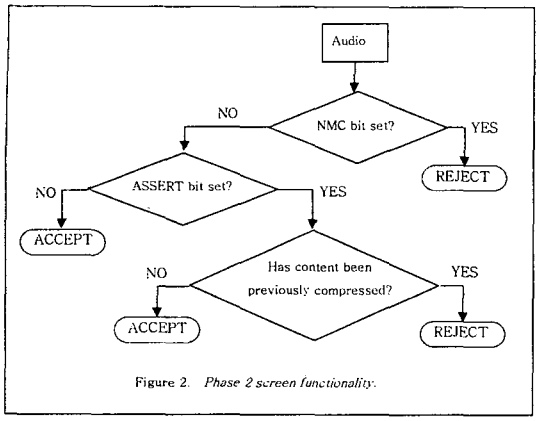

Figure 2. *Phase 2 screen functionality.*

그림 **5 Phase II screen functionality**

5. 복호화 툴

AES 복호화는 ECB 모드에서 username 과 password 를 합친 문자열을 해쉬를 돌려 얻어진 128 bit 키를 사용하여 수행된다.

복호화 툴에서 사용된 메시지들은 다음과 같다.

- 키를 초기화 시키기 위하여 IPMP_KeyData 메시지가 사용되었다.
- AES 툴과 터미널 사이에 암호문과 평문을 교환하기 위하여 IPMP_ProcessData 메시지가 사용되었다.
- 툴을 초기화 하기 위하여 툴 IPMP_ProcessDataInitialize 와 IPMP_InitializeMessage 가 사용되었다.

6. 결론

본 논문에서는 MPEG-4 IPMPX 시스템과 이를 지원하는 보호 툴간의 연동에 대하여 기술하였다. 규격서에 정의된 대부분의 메시지들과 MR 및 TM 이 구현되었으며, 보호 툴로 Rights Management 툴, AES 복호화 툴과 워터마킹 툴이 구현되었다. IPMP 시스템과 보호 툴과의 연동 시험을 통하여 암호화된 MP3 콘텐츠가 복호화, 워터마크 추출, rendering 툴을 거쳐 실시간 재생됨을 확인하였다. MPEG-4 IPMPX 는 아직 표준화 중이며 툴의 완벽한 범용성을 지원하기 위해서는 메시지 활용에 대한 명확한 정의와 메시지들 간의 프로토콜에 대한 정의가 필요하다. 워터마킹 툴을 구현하면서도 실제적으로 필요한 메시지들은 자체적으로 정의를 하여 사용해야만 했다. 무엇보다 다양한 보호 툴들은 그들만의 인터페이스적인 특성을 갖고 있는 경우가 많으므로 이러한 특성을 효과적으로 분류하여 메시지 클래스를 정의하는 것이 필요할 것으로 보여진다.

다음 과정은 현재 MPEG-4 콘텐츠 재생을 위한 참조 소프트웨어로 널리 알려져 있는 IM1 플레이어와의 총 통합이다. 이 과정은 규격서에 기술된 함수와 클래스 구현을 필요로 한다. MPEG-4 IPMP Extensions 의 완벽한 구현은 먼저 아직 구현되지 않은 규격서 상의 몇 가지 메시지들을 완성하고 이들 메시지 간의 conformance 테이스를 실시한 후, 최종적으로 TM 이 원격으로부터 툴을 가져올 수 있도록 구현될 것이다.

참고문헌

[1] ISO/IEC JTC 1/SC 29/WG11 N4850, "Study of FPDAM ISO/IEC 14496-1:2001 / AMD3", May, 2002.

[2] ISO/IEC JTC 1/SC 29/WG11 N4851, "MPEG-4 IPMP Extension (based on IM1) and MPEG-2 IPMP Reference Software Architecture", May, 2002.

[3] D3.1 Functional description of watermarking and copy protection tools, MOSES, June 2002. http://www.crl.co.uk/projects/moses

[4] N4850 Study Text of ISO/IEC 14496-1:2001/FPDAM3

[5] N4851 IPMP Reference Software Architecture and Workplan

[6] N4863 MPEG-4 System Software Status and Workplan

[7] ISO/IEC JTC1/SC29/WG11 MPEG2002/m8495, July 2002, Klagenfurt, "Current status of IST MOSES's work on MPEG-4 IPMP Extensions reference software"

[8] SDMI Portable Device Specification, Part I, Version 1.0. (http://www.sdmi.org)