MPEG-4 스트리밍 미디어 보호를 위한 시스템 설계 및 구현

김정현, 박지현, 윤기송
한국전자통신연구원 인터넷컴퓨팅연구부

Design and Implementations of Protection System for MPEG-4 Streaming Media

Jeonghyun Kim, Jihyun Park, Kisong Yoon
Internet Computing Research Department
Electronics and Telecommunications Research Institute
E-mail : bonobono@etri.re.kr

Abstract

In this paper, we propose a DRM(Digital Rights Management) system for streaming media which can not only protect streamed MPEG-4 content but be easily integrated with existing MPEG-4 streaming system. To protect MPEG-4 media more effectively and more securely, encryption should be considered on encoding phase and also streaming server should be designed to support DRM. However that means it cannot support existing streaming system. Our approach is to design a DRM system independent to the streaming server. So, we used an encryption method which can be applied to compressed MPEG-4. The processing time of decryption in client system must be minimized to guarantee the QoS of streaming service. To satisfy this requirement, it is essential to analyze the effect of DRM on performance. We made some performance test and present the result. Also, we apply proposed system to ISMA(The Inter net Streaming Media Alliance) streaming system which is open standard for MPEG-4 media streaming.

I. 서론

스트리밍 기술은 로컬 시스템에 컨텐츠를 저장하지 않고 실시간으로 데이터를 전송하여 재생이 가능하도록 한다. 따라서 VOD 와 같은 대용량 컨텐츠의 경우 컨텐츠의 특성상 그리고 컨텐츠의 저작권 보호를 위한 보안상의 이유로 스트리밍 방식으로 서비스를 하고 있다. 그러나 스트리밍 URL 을 캡처하여 서버로부터 직접 스트림을 받아 저장하는 툴이 나오면서 스트리밍 컨텐츠를 로컬 시스템에 저장할 수 있게 되었다. 로컬 시스템에 저장된 스트리밍 컨텐츠는 아무런 제약 없이 불법 복제 및 배포가 가능하다.

위와 같은 문제점을 해결하기 위해 본 논문에서는 스트리밍 미디어의 저작권 보호를 위한 시스템을 제안한다. 스트리밍 서버는 미리 암호화하여 저장된 컨텐츠를 스트리밍 하고 클라이언트는 실시간으로 암호화된 스트림을 복호화 하여 재생 함으로써 네트워크 상의 공격으로부터 안전할 수 있다. 또한 스트리밍 데이터를 로컬시스템에 저장하여 유포한다 할지라도 암호화된 데이터 이므로 정당한 라이센스를 갖지 않은 사용자는 사용할 수 없다. 제안 시스템은 인터넷 스트리밍 미디어 연합(The Internet Streaming Media Alliance: ISMA)에서 제안한 MPEG-4 미디어의 스트리밍을 위한 공개 표준을 따르는 스트리밍 시스템을 지원하도록 구현되었다.

본 논문의 구성은 다음과 같다. 2 장에서는 디지털 ISMA 스펙 및 MPEG-4 표준 파일 포맷인 MP4 파일 포맷에 관해 설명하고 3 장에서는 제안 시스템에 대해 기술한다. 4 장에서는 제안 시스템의 성능 실험에 대한 결과를 설명하고 마지막으로 5 장에서 결론을 맺는다.

II. 관련연구

2.1 ISMA

비영리 단체인 ISMA 는 인터넷을 통한 스트리밍 미디어용 공개표준의 시장 채택을 가속화하기 위해 출범된 단체로 2001 년 9 월 MPEG-4 미디어의 스트리밍을 위한 표준 규격인 ISMA 1.0 을 발표하였다[1]. 이 규격은 기존의 MPEG-4 비디오/오디오 압축 기술과 IETF 스트리밍 기술을 조합하여 구성한 것으로 그림 1 은 IETF 스트리밍 모델을 보여준다.

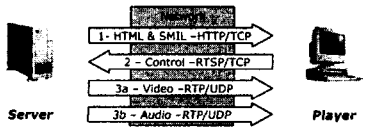

그림 1. IETF 스트리밍 모델

ISMA 스펙에서 미디어 전송과 관련하여 비디오/오디오 데이터 전송은 RFC 1889 (Real Time Protocol/ Real Time Control Protocol: RTP/RTCP), RFC 1890(Audio Video Protocol: AVP), RFC 768(User Datagram Protocol: UDP)을, MPEG-4 비디오/오디오 데이터를 RTP 패킷의 유료부하에 담기 위해 패킷화하는 부분은 RFC 3016 및 RFC Configuration of Generic MPEG-4 Systems 을 이용하고 미디어 제어와 관련하여 RFC 2326(Real Time Streaming Protocol: RTSP)을, 미디어 공고(announcement) 부분은 RFC 2327(Session Description Protocol: SDP)을 이용한다[2]. 스트리밍 포맷으로는 MPEG-4 Part 1 의 MP4 파일 포맷[3]과 ISMA 의 hint track 규격을 이용한다.

ISMA 1.0 의 규격은 두 프로파일로 나누어 지는데 '프로파일 0'은 화면 크기나 오디오 성능이 제한된 휴대폰이나 PDA 등의 장비를 통해 모바일 스트리밍 오디오와 비디오를 전송하기 위한 것이며, 브로드밴드 네트워크를 기반으로 고안된 '프로파일 1' 은 일반 PC 나 셋탑박스 등의 성능이 보다 뛰어난 장비를 위한 규격이다. 각 프로파일의 규격은 표 1 과 같다.

표 1. ISMA Profile 규격

	Profile 0	Profile 1
Video	* MPEG-4 ISO/IEC 14496-2, Simple Profile@Level 1 * QCIF(176X144) * Maximum bitrate 64Kbps	* MPEG-4 ISO/IEC 14496-2, Advanced Simple Profile @Level 3 * CIF(352X288) * Maximum bitrate 1.5Mbps
Audio	* MPEG-4 ISO/IEC 14496-3, High Quality Audio Profile @Level 2 * CELP, L/C ACC	* MPEG-4 ISO/IEC 14496-3, High Quality Audio Profile @Level 2 * CELP, L/C ACC

2.2 MP4 File Format

MPEG-4 Part 1 에서는 MPEG-4 미디어의 상호 교환, 관리, 편집, 화면 재생 등을 수월하게 할 수 있도록 MP4 파일 포맷을 설계하였다. MP4 파일은 atom 이라는 단위로 구성되는데 메타데이터를 담고 있는 movie atom 과 실제 미디어 데이터를 담고 있는 media data atom 으로 구성되어 있다. Atom 은 다시 여러 개의 track 으로 구성되고, video track, audio track, OD(Object Descriptor) track, BIFS(Binary Format for Scene) track, hint track 등이 포함된다.

MP4 파일의 스트리밍 방식은 기존의 스트리밍 미디어 포맷과 차이가 있다. 기존의 스트리밍 미디어 포맷은 미디어 자체를 패킷화하여 파일로 저장된 스트림을 전송 하는 반면 MP4 파일의 경우 미디어 데이터는 자체는 그대로 두고 패킷화하는 방법을 기술한 hint track 정보를 이용해 전송시 미디어 데이터를 패킷화 하여 전송하게 된다. 즉, 로컬 시스템에 저장된 파일과 스트리밍 할 파일의 형태가 동일하다. 따라서 MP4 파일을 스트리밍 하기 위해서는 video, audio track 에 대한 각각의 hint track 이 있어야 한다.

III. 제안 시스템

3.1 시스템 구조

제안 시스템의 구조는 그림 2 와 같다. 그림 2 에서 패키저는 MP4 파일을 암호화 하여 암호화된 파일을 스트리밍 서버로 전송하고 키 및 복호화 할 때 필요한 정보를 라이센스 서버로 보낸다. 사용자가 웹 페이지에서 서비스 받기를 원하는 컨텐츠를 선택하고 사용규칙을 선택 한 후 지불이 끝나면 클라이언트의 공개키가 웹 서버로 전송되고 웹 서버는 다시 사용자가 선택한 컨텐츠의 ID 와 사용규칙, 그리고 클라이언트의 공개키 정보를 라이센스 서버로 보낸다. 라이센스 서버는 복호화 할 때 필요한 정보 및 사용규칙 정보를 포함한 라이센스를 생성하고 이것을 웹 서버로부터 받은 클라이언트의 공개키로 암호화하여 클라이언트에 전송한다. 클라이언트는 이 라이센스 정보를 이용해 암호화된 스트림을 실시간으로 복호화 하여 재생하고 사용규칙에 따라 컨텐츠의 사용을 제어한다.

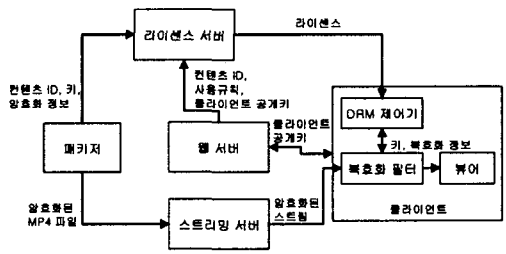

그림 2. 시스템 구조

패키저에서 암호화된 MP4 파일 또한 표준 MP4 파일 포맷을 따르도록 하여 스트리밍 서버가 암호화된 MP4 파일을 스트리밍 할 때도 암호화가 되지 않은 원본 파일과 똑 같은 방식으로 스트리밍 하게 된다. 스트리밍 서버와 독립적으로 설계함으로써 기존의 스트리밍 서버에 대한 수정 없이 제안 시스템의 적용이 가능하다.

3.2 MP4 암호화

그림 3 은 원본 MP4 파일에서 암호화된 MP4 파일을 생성하는 과정을 나타낸 것이다. 원본 MP4 파일은 Scene Description track, Object Description track, Video track, Audio track 으로 이루어져있다. 이중 실제 MPEG-4 비디오와 오디오 데이터를 담고 있는 비디오와 오디오 track 만을 암호화 하고 각각에 대한 Hint track 을 생성한다. 또, 암호화 정보 및 기타 메타데이터 정보를 담은 Meta-Info track 과 이것에 대한 Hint track 을 추가하여 암호화된 MP4 파일을 생성하게 된다. 이렇게 암호화된 파일 또한 MP4 포맷을 따른다.

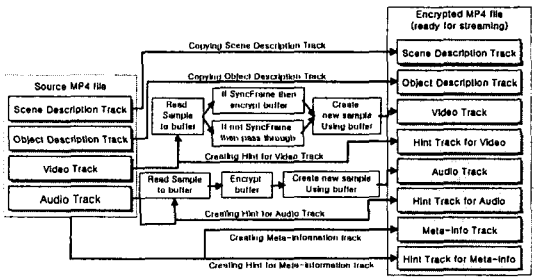

그림 3. 암호화된 MP4 파일 생성

비디오와 오디오 track 에는 각각 MPEG-4 비디오, 오디오의 Elementary stream[4,5]이 샘플 단위로 저장되어 있으며 이때 샘플은 비디오와 오디오의 프레임에 해당한다. 스트리밍의 경우 실시간으로 데이터를 전송 받아 재생해야 하므로 압축 스트림의 디코딩 작업 외에 복호화 과정이 추가되어 클라이언트의 성능에 영향을 미칠 수 있다. 이러한 영향을 최소화하기 위해 비디오의 경우 MPEG-4 압축 특성을 이용하여 I-프레임만을 암호화 함으로써 암호화되는 데이터 량을 줄인다. 그림 4 는 MPEG-4 비디오 샘플의 암호화된 결과를 보여준다. 샘플의 헤더부분 중 복호화 할 때 I-프레임인지를 확인하기 위해 VOP(Video Object Plan) start code 가 포함되어 있는 상위 32 바이트를 암호화 하지 않는다. 또한, 블록 암호화 알고리즘을 이용할 경우 암호화할 데이터가 블록의 크기보다 작을 경우 패딩을 하게 되므로 암호화된 후 샘플 크기가 변하지 않도록 Tail 부분도 암호화 하지 않는다.

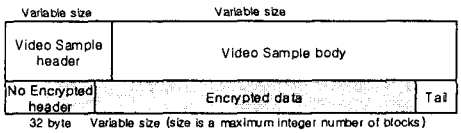

그림 4. MPEG-4 비디오 샘플 암호화

3.3 DRM 클라이언트

그림 5 는 클라이언트 프로세스의 상태 다이어그램을 보여준다. 암호화된 MP4 스트림을 재생하기 위해서 플레이어는 DRM 제어기로부터 복호화 할 때 필요한 정보를 얻어와야 한다. 플레이어로부터 복호화 정보에 대한 요청이 들어오면 DRM 제어기는 인증을 거친 후 플레이어로부터 스트리밍 세션 정보를 받고 복호화에 필요한 키 및 권리 정보 등 메타데이터를 플레이어에 넘긴다. 플레이어는 이 정보를 이용해 암호화된 스트림을 복호화한다. 암호화된 MP4 파일을 클라이언트에 저장하여 재생할 경우 플레이어는 패키저에서 추가한 Meta-Info track 정보를 이용해 이 MP4 파일이 암호화 되었는를 알 수 있고 복호화에 필요한 정보를 DRM 제어기에 요청할 수 있다.

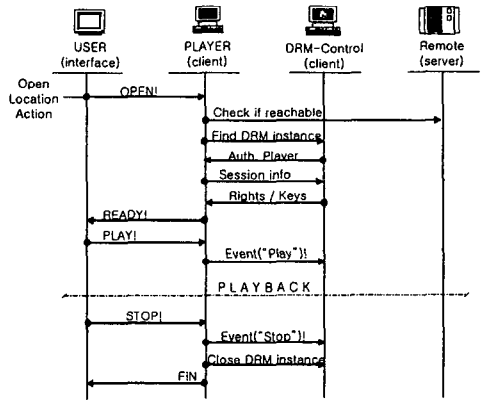

그림 5. 클라이언트 상태 다이어그램

그림 6 은 복호화 필터를 Directshow[6] 필터 그래프를 나타낸 것이다. RTP/RTSP stream source 는 스트리밍 서버로부터 RTP/RTSP 패킷을 받아서 파싱하여 복호화 필터에 MP4 파일의 MPEG-4 비디오, 오디오 샘플을 넘긴다. 복호화 필터는 데이터를 복호화 하여 암호가 풀린 원본 MPEG-4 비디오, 오디오 샘플을 MPEG-4 디코더로 넘기게 된다. 이때 비디오는 I-프레임만 암호화 되었으므로 VOP start code 를 검사하여 I-프레임일 경우에만 복호화를 수행하게 된다.

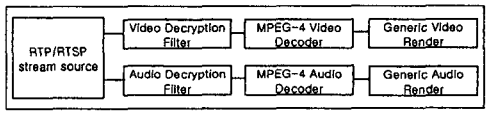

그림 6. 복호화 필터 그래프

IV. 실험 결과

실험은 DES-ECB 방식을 이용하였으며, 표 2 에서 보이는 바와 같이 3 개의 파일에 대해 실험하였다. 파일 A, B, C 에 대한 한 실험 결과는 각각 표 3, 4, 5 에 나타냈다. 실험 결과 비디오의 I-프레임만 암호화 하였을 경우 전체 비디오 프레임을 암호화 한 경우보다 암호화량을 줄임으로써 클라이언트에 미치는 영향 또한 줄일 수 있음을 알 수 있다.

표 2. 테스트 파일의 규격

	File A	File B	File C
Video track	MPEG-4, 320 x 240, 25fps, 210kbps	MPEG-4, 90 x 60, 8fps, 4kbps	MPEG-4, 320 x 240, 29.97fps, 974kbps
Audio track	MPEG-4 @ L1, 32000Hz, 56kbps	MPEG-4 @ L1, 16000Hz, 16kbps	MPEG-4 @ L1, 44000Hz, 128kbps
Duration	7405.560 sec (~124 min)	1718.976 sec (~29 min)	30.063 sec
File size	240 MB	10 MB	4 MB
Total video samples	184,139	13,752	901
I-Frame	768	5,481	23

Table 3. Processing Time of File A

	Encrypt all	Decrypt all	Encrypt I-Frames	Decrypt I-Frames
Open File	0.3s [0.5%]	0.3s [0.7%]	0.3s [0.7%]	0.3s [1.0%]
Audio Processing	16.8s [30.6%]	7.5s [17.2%]	17.9s [42.8%]	7.4s [25.1%]
Video Processing	31.9s [58.1%]	29.7s [68.3%]	23.3s [55.7%]	21.4s [72.8%]
Video Crypting	5.9s [10.7%]	6.0s [13.8%]	0.3s [0.7%]	0.3s [1.0%]
Average Crypting	32μs	32μs	0.39ms	0.39ms
Total	54.9s	43.5s	41.8s	29.4s

Table 4. Processing Time of File B

	Encrypt all	Decrypt all	Encrypt I-Frames	Decrypt I-Frames
Open File	0.0s [0.0%]	0.0s [0.0%]	0.0s [0.0%]	0.0s [0.0%]
Audio Processing	1.5s [62.5%]	0.3s [25.0%]	0.7s [50.0%]	0.3s [30.0%]
Video Processing	0.7s [29.2%]	0.7s [58.3%]	0.6s [42.9%]	0.6s [60.0%]
Video Crypting	0.2s [8.3%]	0.2s [16.7%]	0.1s [7.1%]	0.1s [10.0%]
Average Crypting	14.5μs	14.5μs	18.2 μs	18.2 μs
Total	2.4s	1.2s	1.4s	1.0s

Table 5. Processing Time of File C

	Encrypt all	Decrypt all	Encrypt I-Frames	Decrypt I-Frames
Open File	0.0s [0.0%]	0.0s [0.0%]	0.0s [0.0%]	0.0s [0.0%]
Audio Processing	0.23s [30.3%]	0.12s [20.0%]	0.22s [39.3%]	0.10s [24.4%]
Video Processing	0.43s [56.6%]	0.38s [63.3%]	0.32s [57.1%]	0.29s [70.7%]
Video Crypting	0.1s [13.2%]	0.1s [16.7%]	0.02s [3.6%]	0.02s [4.9%]
Average Crypting	0.11ms	0.11ms	0.87ms	0.87ms
Total	0.76s	0.60s	0.56s	0.41s

그림 7-a 와 7-b 는 각각 암호화 된 채로 재생되는 영상과 복호화되어 재생되는 영상을 나타낸 것이다.

Fig 7-a. 암호화 영상 재생 화면

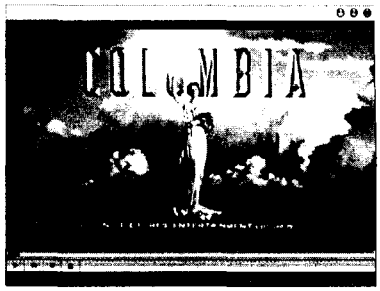

Fig 7-b. 복호화 영상 재생 화면

V. 결론

본 논문에서는 MPEG-4 스트리밍 미디어 보호를 위한 시스템을 제안하였다. 이 시스템은 MPEG-4 미디어의 스트리밍을 위한 공개 표준인 ISMA 스트리밍 시스템을 지원한다. 암호화된 파일 또한 원본 파일과 동일한 포맷을 따르도록 함으로써 기존의 스트리밍 서버의 수정 없이 제안 시스템의 적용이 가능하다. 또한 MPEG-4 비디오의 I-프레임만을 암호화함으로써 전체 프레임을 암호화 했을 때 보다 복호화 작업으로 인해 스트리밍 QoS 에 미치는 영향을 줄이고자 하였다. 향후 스트리밍 환경에 보다 적합한 암호화 방법에 대한 고려가 요구된다.

참고문헌

[1] Internet Streaming Media Alliance Implementation Spec, Ver.1.0, available at http://www.isma.tv

[2] These RFC specs are available at http://www.ietf.org

[3] ISOIIEC 14496-1 :2001/Amd.l:2001 (E) Information technology - Coding of audio-visual objects - Part 1: Systems

[4] ISO/IEC 14496-2:2001/Amd. 1 :2002(E) Information technology - Coding of audio-visual objects - Part 2: Visual

[5] ISO/IEC 14496-2:2001/Amd. 1 :2002(E) Information technology - Coding of audio-visual objects - Part 3: Audio

[6] DirectShow, available at http://www.microsoft.com/Developer/PRODINFO/directx/dxm/help/ds/c-frame.htm#default.htm