情報保護學會論文誌
第19卷 第2號, 2009. 4

H.264 콘텐츠 스트리밍을 위한 효율적인 DRM 시스템의 설계 및 구현

정 윤 현,† 오 수 현‡
호서대학교

Design and Implementation of Efficient DRM System for Contents Streaming based on H.264

Yoon-Hyun Jung,† Soo-Hyun Oh‡
Hoseo University

요 약

멀티미디어 기기와 인터넷의 발달로 디지털 콘텐츠의 제작과 유통이 일반화 되면서 스트리밍 방식의 DRM 시스템이 중요한 위치를 차지하게 되었다. 기존의 스트리밍 방식의 DRM 시스템은 콘텐츠의 모든 데이터를 암호화함으로써 시스템에 많은 부하를 가져왔다. 본 논문에서는 데이터의 일부만을 암호화하여 시스템 성능을 극대화하고, 암호화된 콘텐츠를 네트워크 프로토콜에 독립적으로 전송할 수 있는 스트리밍 방식의 DRM 시스템을 제안하고, 제안하는 시스템을 구현하여 성능 분석한 결과를 제시한다.

ABSTRACT

DRM system with streaming scheme has obtained it's priority due to generalized production and distribution of digital contents by development of multimedia device and internet. Previous DRM system with streaming scheme over-burdened the system by encrypting every data of the contents. This paper presents DRM system with new streaming scheme that is able to independently transmit encrypted contents to network protocol and maximize system function by encrypting only certain parts of data. Also, performance is analyzed through designing and implementing the proposed system.

Keywords: DRM, streaming, H.264

I. 서 론

오늘날 멀티미디어 기기의 발달로 디지털 콘텐츠(Digital Contents)를 쉽게 제작할 수 있게 되어서 텍스트, 이미지, 오디오, 비디오, 게임 등 다양한 콘텐츠(Contents)의 생산이 증가하고 있다. 또한 네트워크 기술의 발달로 디지털 콘텐츠의 배포가 일반화 되고 있으며, 각 가정에 까지 실시간으로 콘텐츠를 스트리밍(Streaming) 할 수 있는 단계에 이르렀다.

접수일(2008년 10월 20일), 수정일(2009년 1월 14일), 게재확정일(2009년 2월 3일)
† 주저자, jyh2554@empal.com
‡ 교신저자, shoh@hoseo.edu

이로 인하여 디지털 콘텐츠에 대한 보호의 필요성이 대두 되었다. DRM(Digital Right Management)은 디지털 콘텐츠를 저작권자와 제공자로부터 고객에게 정확하고 안전하게 전달하며, 디지털 콘텐츠와 관련된 주체들의 권리를 보호하고 불법적인 유통 및 재배포를 방지하는 기술이다[1,2]. 디지털 콘텐츠는 다운로드(Download)방식과 스트리밍 방식에 따라서 DRM 구현이 상이하다. 다운로드 방식의 디지털 콘텐츠에 대한 보호는 콘텐츠 전체를 암호화 하고 사용자 인증을 통한 라이선스 발급으로 콘텐츠의 안전한 유통을 보장한다. 그러나 스트리밍 방식의 디지털 콘텐츠는 스트리밍 서버(Streaming Server)가 스트리밍 시 패킷(Packet) 전체를 암호화 한다면 서버

에 과중한 부하를 일으켜서 현실적으로 서비스를 제공하기 힘들다[3].

본 논문에서는 스트리밍 서버와 스트리밍 프로토콜에 최소한의 영향을 주면서 효율성과 안전성 요구 사항을 동시에 만족하는 H.264 콘텐츠 스트리밍 방식의 개선된 DRM 시스템을 제안한다.

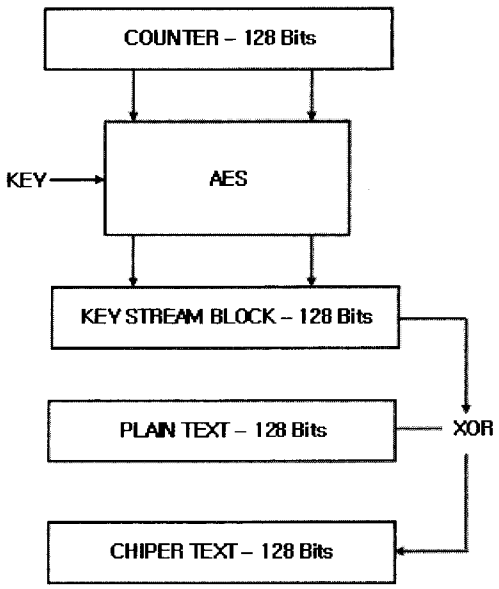
본 논문의 구성은 다음과 같다. 먼저 제 2장에서는 대표적인 DRM 시스템에 대해 설명하고, 제 3장에서 H.264에 대하여 간략히 기술한다. 다음으로 제 4장에서는 제안하는 DRM 시스템에서 사용하는 H.264 NAL(Network Abstract Layer) 암호화 방법 및 전체적인 시스템 구조에 대하여 자세히 설명하고 제 5장에서 제안하는 시스템을 실제로 구현하여 성능 분석한 결과를 제시한다. 그리고 마지막으로 6장에서는 결론을 맺는다.

II. 관련 연구

2.1 ISMA

ISMA(Internet Streaming Media Alliance)[4]는 스트리밍 미디어(Streaming Media)의 채택을 가속화하기 위하여 2000년에 결성된 단체로 오디오 및 비디오 스트리밍의 안전한 전송을 위한 하나의 프레임 워크이다. 스트리밍 방식의 콘텐츠 암호화를 위하여 대칭키 암호 알고리즘을 사용하며 전송을 위해 RTP 프로토콜을 UDP 레이어에서 적용한다[5-8]. 대칭키 암호 알고리즘으로는 DES, 3DES, AES등 다양한 알고리즘이 적용 가능하다. 또한 긴 미디어 데이터를 암호화하기 위하여 카운터 모드(Counter Mode)를 사용하고 있다.

[그림 1]은 AES 알고리즘을 이용하여 128비트 카운터 모드로 콘텐츠를 암호화 하는 과정을 보여준다. AES는 128비트(16바이트) 단위로 동작하며 카운트 모드에 사용하는 카운터 값 역시 128비트 이다. 카운트 값을 1씩 증가 하면서 키를 이용하여 AES로 암호화 한 후, 생성된 128비트의 각 키 스트림을 해당 콘텐츠의 128비트 단위로 XOR 연산을 수행하면 암호화가 완료된다. 복호화도 동일한 방식으로 수행된다. 지원하는 형식은 ISMA Spec1.0에서는 MPEG4 파일 포맷만 지원하였으나 ISMA Spec2.0은 ISO 미디어 파일 전체를 지원한다. ISMA는 ISO 미디어 파일에 대한 범용적인 DRM 시스템으로 콘텐츠 전체를 암호화 한다.



[그림 1] AES 128비트 카운터 모드의 암호화 과정

2.2 Microsoft의DRM 시스템

Microsoft의 DRM시스템은 저작물 제공자에게 인터넷상에서 암호화를 통하여 음악이나 비디오 파일에 대해 보호된 콘텐츠를 제공한다. 각각의 서버 또는 클라이언트들은 개인화 과정을 통하여 키 쌍을 할당받으며 서버 또는 클라이언트가 안전하지 않다고 판단되면 인증서 취소 목록을 이용하여 서비스 대상에서 제외시킨다. 키는 라이선스에 포함되고 라이선스와 콘텐츠는 분리되어 제공된다. 이 시스템은 음악, 비디오 등의 범용적인 DRM 시스템으로, 콘텐츠 전체를 암호화 한다.

2.3 InterTrust의 DRM 시스템

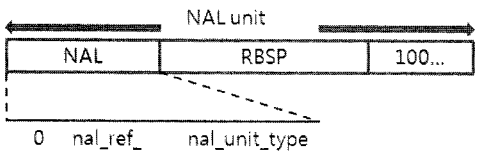
InterTrust의 DRM 시스템은 암호 기술과 워터마킹 기술을 이용하여 콘텐츠를 보호하며 콘텐츠 사용 규칙을 지정하여 사용 내역의 수집 및 기록, 과금 처리를 수행 한다. 콘텐츠는 사용 전 에 암호화 되며 사용 하는 시점에 라이선스 에이전트가 라이선스를 확인하고, 지불정보를 전송하여 거래가 진행된다. 또한 콘텐츠가 암호화 되어 있으므로 사용자들 사이에 암호화된 콘텐츠를 주고받을 수 있는 콘텐츠 재분배를 실현하였다.

III. H.264 NAL

ITU-T 와 ISO/IEC가 함께 JVT(Joint Video Team)을 구성하여 기존의 MPEG-2, H.263, MPEG-4 비디오 압축 표준보다 압축 성능이 향상된 H.264/AVC 비디오 부호화 표준을 제정하였다 [8-11]. 이렇게 향상된 압축 성능을 통하여 H.264/AVC 방식은 현재 전 세계적인 차세대 동영상 압축 기술로 평가받고 있다.

3.1 NAL

H.264/AVC의 특징 중 하나가 Video Coding Layer(VLC)와 Network Abstract Layer(NAL)를 분리 한 것이다. VLC는 인코딩(Encoding)을 수행하며, 독립적으로 네트워크를 통하여 NAL 전송이 가능하도록 VLC의 데이터를 NAL Units이라는 단위로 캡슐화(Encapsulation)를 수행한다. NAL Unit은 [그림 2]와 같이 1 Bytes의 헤더와 RBSP(Raw Bytes Sequence Payload)와 트레일링 비트(Trailing Bits)들로 구성되어 있다. NAL Header는 1 Bit(Forbidden), 엔코딩 된 데이터를 나타내는 2 Bits (nal_ref_idc) 그리고 NAL Unit의 타입(Type)을 나타내는 5 Bits (nal_unit_type)로 구성된다. RBSP는 픽쳐 슬라이스(Picture Slices)와 파라미터 세트(Parameter Set)가 존재한다. 트레일링 비트는 페이로드(payload)의 끝을 알리기 위해 사용한다.



[그림 2] NAL Unit

3.2 NAL Unit Types

NAL Unit의 타입의 정보는 [표 1]과 같다. NAL Unit 타입은 현재 1~12 까지만 정의 되어 있다. 1~5, 12번 NAL Unit은 엔코딩 된 데이터인 VCL NAL Units 이며 나머지 NAL Unit은 파라미터 등의 부가 정보를 나타내는 엔코딩 되지 않은 비 VCL NAL Unit이다. 여러 NAL 타입 중 IDR, SPS, PPS, SEI는 디코딩을 하기 위해서 가장 필수적인 정보들이다. NAL이 0이거나 24~31사이의 값을 가질 때는 복호화 과정이 없는 것으로 정의되어있다.

또한 복호화기는 Extend(보류) NAL Unit 타입의 모든 NAL 내용은 처리하지 않는다. IDR (Instantaneous Decoding Refresh) 픽쳐는 비디오 시퀀스(Video Sequence)의 선두 픽쳐로서 참조 픽쳐 버퍼의 상태와 프레임 번호, POC등 픽쳐 비트열을 복호하기 위해 필요한 모든 상태를 초기화한다. SPS(Sequence Parameter Sets)은 하나의 비디오 시퀀스에 포함된 모든 NAL Unit에 적용되는 중요한 헤더 정보로서 프로파일ID나 래벨, 참조 프레임의 개수, 화면 크기 등의 정보가 포함된다.

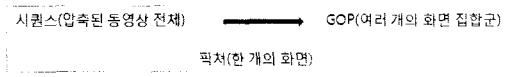
[표 1] NAL Unit 타입

Type	Name
0	[Unspecified]
1	Coded Slices
2	Data Partition A
3	Data Partition B
4	Data Partition C
5	IDR
6	SEI
7	SPS
8	PPS
9	Access Unit Delimiter
10	EoS (End of Sequence)
11	EoS (End of Stream)
12	Filler Data
13 - 23	[Extended]
24 - 31	[Unspecified]

PPS(Picture Parameter Sets)은 비디오 시퀀스내의 여러 픽쳐에 적용되는 중요한 헤더 정보로서 엔트로피 부호화 방법, 슬라이스 그룹 개수, 가중치 예측 방법, 디블록킹 필터 사용 여부, 8x8 변환 모드 사용 여부 등의 정보가 포함된다. SEI(Supplemental Enhancement Information)은 복호화 된 데이터의 화면 표현과 관련된 시간 정보 및 부가정보를 포함한다.

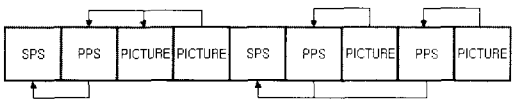
3.3 NAL 비트 열

하나의 시퀀스는 [그림 3]과 같은 계층 구조로 정해져 있기 때문에, 비트열에서 정보를 정렬하는 순서도 이러한 계층 구조를 따른다.



〔그림 3〕 시퀀스 구성

〔그림 4〕와 같이 H.264/AVC는 하나의 비트 열에 여러 개의 시퀀스로 구성될 수 있다. 시퀀스를 식별하기 위해서 SPS안에는 SPS번호가 있고, PPS안에서 SPS번호를 지정하여 어느 시퀀스에 속하는지를 식별한다. 또한 PPS에도 번호가 있는데 픽쳐 헤더 안에 PPS번호를 지정함으로써 어느 PPS를 사용하는가를 식별한다.



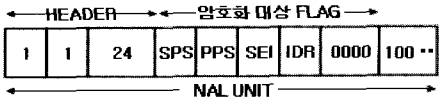
〔그림 4〕 SPS & PPS & 픽쳐의 관계

IV. 제안하는 H.264 콘텐츠 스트리밍 방식의 DRM 시스템

본 장에서는 제안하는 H.264 콘텐츠 스트리밍 방식의 DRM 시스템에 대해 기술한다. 제안하는 DRM 시스템은 H.264 비트열 중 SPS, PPS, IDR과 같은 특정 NAL 타입만을 암호화하여 압축 성능을 높였으며 암/복호화 모듈을 시스템에 독립적으로 설계하였다.

4.1 제안하는 H.264 콘텐츠 암호화 방식

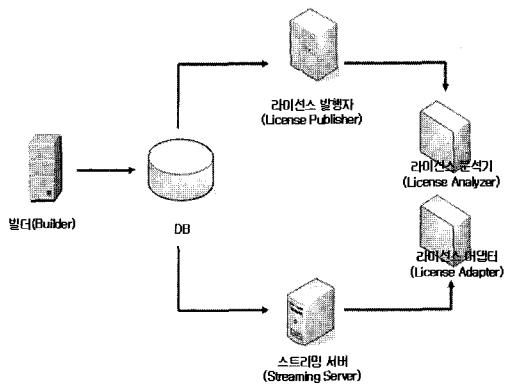
제안하는 H.264 콘텐츠 암호화 방식은 SPS, PPS, IDR과 같은 세 가지의 NAL 타입을 암호화 한다. 암호화 대상 NAL 타입은 ISMA의 디폴트 암호화 방식인 AES 128비트 카운터 모드로 암/복호화를 수행한다. AES 128비트 카운터 모드 암호화 방식은 2.1절에서 설명하였다. 이들의 암호화 우선순위는 SPS, PPS, IDR 순이다. SPS는 비트열의 각 시퀀스에 필요한 정보 즉 프로파일 ID나 참조 프레임의 개수 등의 필수 정보를 가지고 있기 때문에 암호화 하였을 경우 가장 큰 효과를 볼 수 있다. PPS는 SPS의 픽쳐 정보로서 실제 픽쳐를 디코딩 하는 방법을 정의하였으므로 2번째 우선순위를 갖는다. 마지막으로 IDR은 영상 시퀀스의 선두 픽쳐로서 가장 낮은 우선순위를 갖고 암호화 한다. 어떤 NAL 타입이 암호화 되었는지는24번의 NAL 타입을 이용하여서 클라이언트에게 전달하는 방법을 사용한다. 앞에서 설명한 NAL 타입 중 NAL이 0이거나 24~31 사이의 값을 가질 때는 복호화 과정이 없는 것으로 정의 되었다. 그러므로 24~31까지의 NAL 타입은 응용에 따라 선택적으로 사용할 수 있음을 의미하며, 24번 NAL 타입을 이용함으로써 암호화 되지 않은 H. 264파일과도 호환성을 유지 할 수 있다. 〔그림 5〕는 보류 타입인 24번째 NAL 타입의 구조이다. NAL Unit헤더의 nal_unit_type 을 24로 지정하며, RBSP는 1 Byte로 구성되며 각 1비트를 암호화 대상 플래그(SPS, PPS, IDR) 로 설정하여 암호화 대상 NAL 타입을 지정한다.



〔그림 5〕 NAL TYPE 24의 구성도

4.2 제안하는 스트리밍 방식의 DRM 시스템

제안하는 스트리밍 방식의 DRM 시스템은 4.1절에서 설명한 암호화 방식을 사용하여 콘텐츠를 실시간으로 전송하도록 빌더(Builder), 라이선스 발행자(License Publisher), 스트리밍 서버(Streaming Server), 라이선스 분석기(License Analyzer), 네트워크 어댑터(Network Adapter)로 구성되어 있다. 〔그림 6〕은 제안하는 시스템의 구성 요소들을 나타낸다. 시스템을 구성하는 각 하위 시스템은 다음과 같은 기능을 가진다. 먼저 빌더는 128 비트 AES 카



〔그림 6〕 제안하는 시스템의 구성

운터 모드에서 사용할 암호화 키와 카운터 값을 생성하여 데이터베이스에 저장하는 역할을 한다. 암호화 키와 카운터 값은 난수생성기를 사용하여 생성하며, 생성된 정보는 라이선스 정보로 패키징(Packaging)하여 데이터베이스에 저장한다. 라이선스 정보로는 암호화 키, 카운터 값, 콘텐츠URL로 구성된다. 라이선스 발행자는 라이선스 정보를 클라이언트에게 안전하게 전송하는 역할을 한다. 라이선스 정보는 RSA 공개키 암호 알고리즘을 사용하여 클라이언트의 공개키로 암호화함으로써, 라이선스의 기밀성을 보장한다.

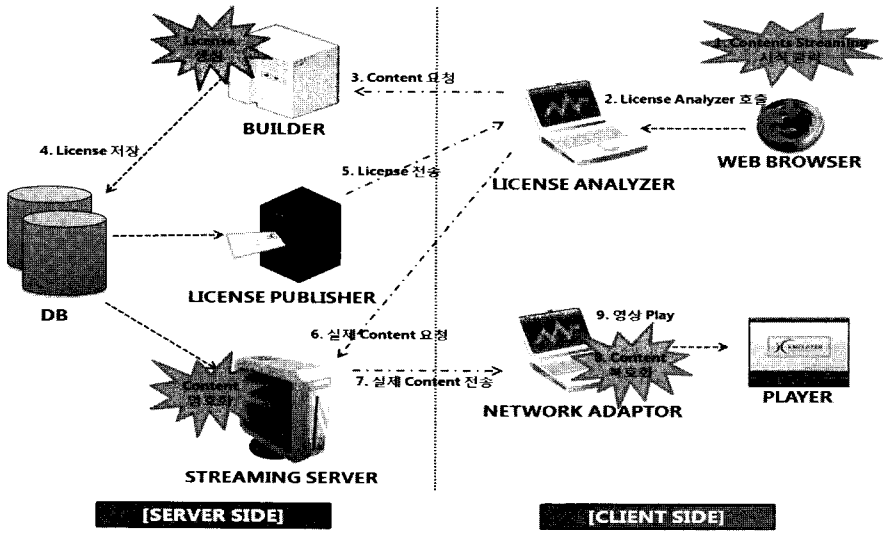
스트리밍 서버는 콘텐츠를 128비트 AES 카운터 모드로 암호화 하여 클라이언트에게 전송하는 역할을 한다. 라이선스 분석기는 라이선스 정보를 분석하여 해당하는 콘텐츠를 스트리밍 서버에 요청하는 역할을 한다. 라이선스 발행자를 통하여 전송 받은 라이선스를 클라이언트의 비밀키로 복호화 하여 콘텐츠 URL을 추출한 후 스트리밍 서버에 콘텐츠를 요청한다. 네트워크 어댑터는 스트리밍 서버로부터 전송된 암호화된 콘텐츠를 IP 레이어에서 복호화 하는 역할을 한다. 네트워크 어댑터는 동영상 플레이어 같은 응용 어플리케이션 보다 먼저 스트리밍 서버에서의 전송된 패킷을 검사하며, 암호화 된 데이터가 발견되었을 경우128 비트 AES 카운터 모드로 복호화 한다. 네트워크 어댑터는 해당하는 스트리밍 서버에 대한 패킷만을 복호화하기 때문에 클라이언트에 큰 부하가 없으며 IP 레이어에서 동작하므로 실제 응용 어플리케이션과는 독립적으로 동작한다. 제안하는 시스템의 구성요소 및 기능은 [표 2]와 같으며, 전체 동작 과정은 다음과 같다.

(1) 사용자가 콘텐츠 스트리밍 시작을 클릭한다.
(2) 웹 브라우저가 해당 콘텐츠 정보를 읽어 라이선스 분석기를 호출한다.
(3) 라이선스 분석기는 콘텐츠를 빌더에게 요청한다.
(4) 빌더는 암호화 키와 카운터 값을 난 수 생성기로 만든 후, 패키징을 통하여 라이선스를 만들고 데이터베이스에 저장한다.
(5) 라이선스 발행자는 데이터베이스에 저장된 라이선스를 클라이언트의 공개키로 암호화 하여 전송한다.
(6) 라이선스 분석기는 전송된 라이선스 정보를 클라이언트의 비밀키로 복호화 한 후, 라이선스의 콘텐츠 URL을 이용하여 스트리밍 서버에 콘텐츠를 요청한다.
(7) 스트리밍서버는 콘텐츠를 암호화하여 전송한다.
(8) 네트워크 아답터는 암호화된 패킷을 복호화 하여 플레이어에게 독립적으로 전달한다.
(9) 플레이어는 복호화 된 콘텐츠를 사용자에게 보여준다.

[그림 7]은 제안하는 H.264 콘텐츠 스트리밍 DRM 시스템의 전체적인 동작 과정을 나타낸다.

[표 2] 제안하는 시스템의 구성요소 및 기능

구성 요소	기능
빌더	- 암호화 키와 카운터 값의 발급(의사 난 수 생성기 사용) - 패키징 처리 - 라이선스 정보를 데이터베이스에 저장
라이선스 발행자	- 라이선스 정보 데이터베이스로부터 추출 - 클라이언트의 공개키를 이용하여 암호화 키, 콘텐츠 정보와 같은 라이선스 정보를 RSA 공개키 암호 알고리즘으로 암호화 - 클라이언트에게 전송
스트리밍 서버	- 콘텐츠 암호화(128비트 AES 카운터모드 사용) - 클라이언트에게 전송
라이선스 분석기	- 라이선스 요청 - 라이선스를 클라이언트 비밀키로 복호화 - 스트리밍 서버에 콘텐츠 요청
네트워크 어댑터	- IP 레이어에서 패킷을 모니터링 - 콘텐츠 복호화(128 비트 AES 카운터 모드사용)



〔그림 7〕 제안하는 시스템의 동작 과정

V. 제안하는 시스템의 성능 분석

제안하는 H.264 콘텐츠 스트리밍 DRM 시스템의 성능을 측정하기 위해서, 애리조나 대학교에서 제공하는 2개의 테스트 비디오 시퀀스(foreman, mobile)를 사용하였다. 비디오 시퀀스는 352 x 288 해상도에 300 프레임 4:2:0 YUV로 구성되어 있다. 테스트 환경은 〔표 3〕과 같다[12-14].

본 장에서는 다음과 같은 테스트 환경에서 제안하는 암호화 방법의 효율성 및 안전성을 분석하였다.

〔표 3〕 테스트 환경

Processor	Intel® Core™ Processor Duo
L2 Cache	2MB
System Bus	667MHz
Memory	1024MB (On 512MB + 512MB)
Operating System	Windows XP
Compiler	Microsoft Visual C++ 6.0
Bit rate(kb/s)	43.96kbps
Profile Type	Main Profile
Frame rate	30
No. frames coded	299
Encoding reference software	H.264 JM 13.0
Decoding reference software	FFMpeg

5.1 효율성 분석

암/복호화 모듈은 전체 시스템에 독립된 한 모듈로서 구현되었기 때문에, 전체 수행시간 중 해당 파일의 암/복호화 수행 시간을 측정하였다.

측정결과는 〔표 4〕와 같다. 테스트 결과, 전체 NAL Unit 수행 시간 대비 SPS, PPS, IDR 수행 시간이 크게 줄어드는 것을 확인 하였다.

테스트 결과, ISMA 방식 대비 제안한 NAL Unit의 암호화 수행 시간은 25% 정도였다. 각각의 NAL Unit 암/복호화 수행시간을 분석해보면, SPS, PPS는 디코딩을 하기 위한 부가정보로서 비트열의 매우 작은 부분을 차지하기 때문에 암/복호화 수행시간에 거의 영향을 주지 않는다. 또한 IDR은 화면 내에서 예측을 하기 때문에 다른 프레임보다 상대적으로 큰 데이터를 갖고 있지만, 전체 300 프레임 중 10%만 차지하므로 효율적인 암/복호화를 할 수 있다.

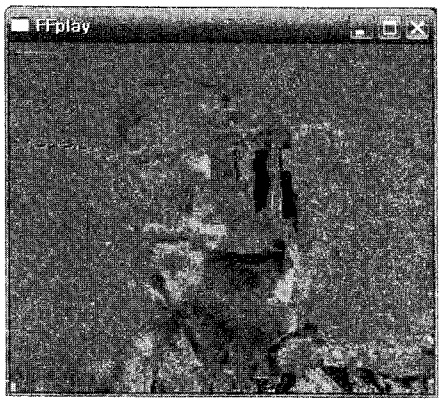
5.2 안전성 분석

〔그림 8〕은 foreman 비디오 파일을 암호화 한 후 FFMpeg으로 실행한 화면이다. SPS가 암호화된 비디오 시퀀스는 심한 노이즈의 작은 화면으로 디코딩되며, PPS가 암호화된 비디오 시퀀스는 디코딩 되지 않았다. IDR이 암호화 된 비디오 시퀀스는 심한 노이즈와 함께 윤곽선 정도만 디코딩 되었다. 실제 테스트를 통하여, 본 논문에서 제안하는 암호화 방식이 충분

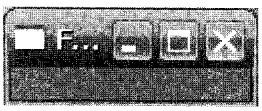
〔표 4〕 암/복호화 수행 시간

	SPS	PPS	IDR	SPS+PPS	SPS+PPS+IDR	전체(ISMA방식)
foreman	0.035ms	0.025ms	7.8ms	0.04ms	7.9ms	33.8ms
mobile	0.057ms	0.025ms	25.1ms	0.04ms	23.9ms	97.73ms
평균	0.046ms	0.025ms	16.5ms	0.04ms	15.9ms	65.6ms
모드/전체	0.07%	0.03%	25%	0.VI06%	24%	-

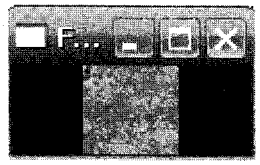
한 성능 향상 및 정당하지 않은 사용자가 콘텐츠 내용을 알 수 없도록 하는 안전성 요구사항을 만족함을 확인 할 수 있었다.



a. IDR 암호화



b. SPS+PPS+IDR암호화



c. SPS 암호화

〔그림 8〕 FFMpeg으로 실행한 화면

SPS가 암호화된 비디오 시퀀스는 심한 노이즈의 작은 화면으로 디코딩 되며, PPS가 암호화된 비디오 시퀀스는 디코딩 되지 않았다. IDR이 암호화 된 비디오 시퀀스는 심한 노이즈와 함께 윤곽선 정도만 디코딩 되었다. 실제 테스트를 통하여, 본 논문에서 제안하는 암호화 방식이 충분한 성능 향상 및 정당하지 않은 사용자가 콘텐츠 내용을 알 수 없도록 하는 안전성 요구사항을 만족함을 확인 할 수 있었다.

2절에서 설명한 Microsoft의 DRM 시스템이나 ISMA 등은 제공하는 콘텐츠의 모든 부분을 암호화하기 때문에 서버와 클라이언트에 모두 많은 부하를 주는 구조이나, 제안하는 시스템은 서버와 클라이언트의 부하를 줄이면서도 효과적인 데이터 은닉을 제공한다. 〔표 6〕은 기존의 DRM 시스템과 제안하는 시스템의 특징을 비교한 것이다.

VI. 결 론

오늘날 멀티미디어 기기의 발달로 디지털 콘텐츠를 쉽게 제작할 수 있게 되었으며 네트워크 기술의 발달로 디지털 콘텐츠의 배포가 일반화 되면서 스트리밍 방식의 DRM 시스템이 중요한 위치를 차지하게 되었다.

그러나 기존의 스트리밍 방식의 DRM 시스템은 콘텐츠의 모든 데이터를 암호화함으로써 시스템에 많은

〔표 6〕 기존 DRM 시스템과 제안하는 시스템의 비교

	Microsoft DRM	ISMA	제안한 DRM 시스템
암호화 대상	Contents 전체	Contents 전체	특정 NAL Unit
지원 포맷	WMV File	ISO 미디어 파일	H.264
License 관리	한 파일로 관리	세션 관리로 대체	한 파일로 관리
암호화 방식	자체 암호화 방식	AES 카운터 모드	AES 카운터 모드
서비스 방법	다운로딩/스트리밍	스트리밍	스트리밍
시스템 부하	콘텐츠 전체를 암호화하므로 부하가 큼	콘텐츠 전체를 암호화하므로 부하가 큼	콘텐츠 일부를 암호화하므로 상대적으로 부하가 적음

부하를 가져왔다. 본 논문에서는 스트리밍 서버의 성능을 극대화하고, 암호화된 콘텐츠를 네트워크 프로토콜에 독립적으로 전송 할 수 있는 스트리밍 방식의 DRM 시스템을 제안하였다. 또한 라이선스 정보를 통하여 복호화 하기 때문에 패킷 캡처 툴이나 스트리밍 URL 캡처를 통한 콘텐츠 접근을 원천적으로 보호할 수 있다.

본 논문에서는 제안한 시스템의 암/복호화 모듈을 직접 구현하여 테스트를 수행하였다. 수행 결과 암/복호화 수행시간이 ISMA 방식 대비 25%정도로 축소되었으며, 정당하지 않은 사용자가 디코딩 하였을 때 화면을 알아볼 수 없을 정도로 손상되었다. 실제 테스트를 통하여 제안한 암호화 방식이 충분한 성능 향상과 안전성 요구사항을 만족함을 확인할 수 있었다.

향후 다양한 코덱과 암호화 방법에 대한 구현이 필요하며, 또한 전송 중 데이터 누수에 대한 에러 복원 기능에 대한 구현이 필요하다.

참 고 문 헌

[1] 정연정, 윤기송, 류재철, "MPEG-2 Streaming DRM 시스템 설계 및 구현," 정보보호학회지, 14(6), pp. 75-81, 2004년 12월.

[2] 박지환, 김태정, 이진홍, "컨텐츠 스트리밍을 위한 안전한 DRM 시스템 설계 및 구현," 정보보호학회 논문지, 13(4), pp. 177-185, 2003년 8월.

[3] Y. Zou, T. Huang, and W. Gao, "H.264 Video Encryption Scheme Adaptive to DRM," IEEE Transactions on Consumer Electronics, Vol. 52, No. 4, pp. 1289-1297, Nov. 2006.

[4] Internet Streaming Media Alliance, "ISMA Encryption and Authentication Specification Ver. 1.1," Dec. 2005.

[5] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP : A Transport Protocol for Real-Time Application," RFC 3550, July 2003.

[6] B. Moore, "RTP Payload Format for MPEG-4 Streams," RFC 3460, Jan. 2003.

[7] Y. Kikuchi, T. Nomura, S. Fukunaga, Y. Matsui, and H. Kimata, "RTP Payload Format for MPEG-4 Audio/-Visual Streams," RFC 3016, Nov. 2000.

[8] T. Weigand, G.J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC Video Coding Standard," IEEE Transactions on Circuits and System for Video Technology, Vol. 13, No. 7, pp. 5650-576, July 2003.

[9] ISO/IEC 14496-10:2003, Information technology- Coding of audio-visual objects-Part 10: Advanced Video Coding

[10] ISO/IEC 14496-15:2003, Information technology- Coding of audio-visual objects-Part 15: Advanced Video Coding

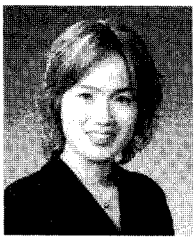
[11] ISO/IEC 14496-12:2003, Information technology- Coding of audio-visual object-Part 12: ISO Base Media File Format

[12] JVT Reference Software Version 9.5, available online at: http://iphome.hhi.de

[13] 호요성, 김 승환, H.264/AVC 표준의 소스 코드 분석, 두양사, 2007년 2월.

[14] 정제창, H.264/AVC 비디오 압축 표준, 홍릉출판사, 2005년 10월.

〈著者紹介〉



오 수 현(Soo-Hyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월 ~ 현재: 호서대학교 정보보호학과 교수
〈관심분야〉 암호 프로토콜, RFID/USN 정보보호 기술, 암호 시스템 평가 및 인증

정 윤 현(Youn-Hyun Jung) 학생회원
2007년 2월: 인하대학교 컴퓨터공학과 졸업
2009년 2월: 호서대학교 컴퓨터공학과 석사(공학석사)
2007년 2월 ~ 현재: 삼성전자 연구원
〈관심분야〉 영상 압축 DRM 시스템, 콘텐츠 보안