# IPTV에서 H.264/AVC 콘텐츠 재생을 위한 DRM 시스템 연구 및 설계

신영록*, 나상호*, 허의남*
*경희대학교 컴퓨터공학과
e-mail : {ekseldw, shna, johnhuh}@khu.ac.kr

# A Study and Design of IPTV DRM System for Playback of H.264/AVC Contents

Young-Rok Shin*, Sang-Ho Na*, Eui-Nam Huh*
*Dept of Computer Engineering, KyungHee University

요 약

멀티미디어 기기의 발달과 인터넷의 확산 등의 영향으로 디지털 콘텐츠의 제작 및 유통이 일반화되면서 시장 활성화가 되었지만 불법복제로 인한 시장에 악영향도 미치고 있다. 그리하여 DRM이란 정보보호 기술이 일반화되고 그 기능이 중요하게 되었다. 본 논문에서는 기존의 데이터 전체를 암호화하는 방식의 DRM 시스템과는 달리 H.264/AVC의 특성을 이용하여 콘텐츠의 일부만을 암호화하여 서버에 최소한의 영향을 주면서 영상을 전송할 수 있는 효과적인 DRM 시스템을 제안하였다.

## 1. 서론

멀티미디어 기기의 발달로 인해 오늘날에는 디지털 콘텐츠를 쉽게 제작할 수 있게 되었다. 그에 많은 오디오, 비디오 등의 디지털 콘텐츠의 생산율이 크게 증가했다. 또, 인터넷의 발전은 디지털 콘텐츠의 유통을 쉽게 만들었고, 디지털 콘텐츠가 짧은 시간 안에 배포될 수 있게 되었고 일반화되었다. 하지만 그에 비하여 디지털 콘텐츠의 수정 및 복사는 너무 간단하며, 원본과 복사본은 크게 차이가 없다는 특징을 가지고 있다. 이러한 디지털화의 특징은 디지털 콘텐츠 시장의 활성화라는 이점을 가져오기도 하였지만 불법복제로 인한 저작권 문제를 낳기도 하였다.

그리하여 제작자의 디지털 콘텐츠의 보호를 요구하게 되었고, DRM(Digital Right Management)이란 정보보호 기술이 사용되기 시작하였다. DRM은 콘텐츠의 불법복제를 방지하고 지정된 사용자에게 허가된 범위 내에서 디지털 콘텐츠를 사용하게 하여 디지털 콘텐츠의 안전하고 투명한 유통을 가능하게 하는 기술이다. 본 논문에서는 서버에 최소한의 영향을 주면서 효율적으로 H.264/AVC 형식의 콘텐츠를 재생할 수 있는 DRM 시스템을 제안한다.

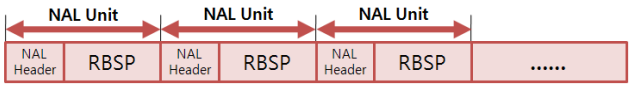
## 2. 관련연구

### 2.1. H.264/AVC

H.264는 매우 높은 데이터 압축률을 가지는 디지털 비디오 코덱 표준으로 MPEG-4 파트 10 또는 AVC(Advanced Video Coding)라 부르기도 한다. 이 표준은 ITU-T의 VCEG(Video Coding Experts Group)와 ISO/IEC의 MPEG(Moving Picture Experts Group)이 공동으로 JVT(Joint Video Team)를 구성하고 표준화를 진행한 결과물로 나온 것이다.

### 2.2. NAL(Network Abstract Layer)

H.264는 시작 단계부터 네트워크 전송을 목적으로 개발되어졌다. 따라서 동영상 부호화 처리 그 자체를 다루는 VCL(Video Coding Layer)가 부호화된 정보를 전송하고 저장하는 하위 시스템과의 사이에 있는 NAL(Network Abstract Layer이라는 계층이 정의되어 있어서 VCL과 NAL이 분리된 구조로 구성되어 있는 것이 특징이다. NAL Unit은 다음 그림과 같이 NAL Unit Header와 RBSP(Raw Bytes Sequence Payload)로 구성되어 있다.




(그림 1) H.264 Stream과 NAL Unit

NAL Unit Header는 1바이트로 1비트의 forbidden_zero-bit, 인코딩된 데이터를 나타내는 2비트의 nal_ref_idc, 5비트의 nal_unit_type으로 이루어져 있다. NAL Unit의 타입의 정보는 <표 1>과 같다.

SPS(Sequence Parameter Set)는 프로파일, 레벨 등 시퀀스 전체의 부호화에 걸쳐있는 정보가 포함되어 있는 헤더 정보로 sequence parameter set ID, profile and level, number of reference frames 등을 포함하고 있다. 이 정보들은 영상 디코딩을 위하여 필수적인 정보들이다. 또한, PPS(Picture Parameter Set)는 픽쳐 전체의 부호화 모드, 예를 들어 엔트로피 부호화 모드, 픽쳐 단위의 양자화 파

라미터 초기 값 등을 나타내는 헤더 정보이다. picture parameter ID, sequence parameter ID 등의 파라미터가 저장되며, 이 정보들은 각 픽쳐의 디코딩을 위해 필수적인 정보들이다. NAL 타입이 0 또는 24~31인 경우 디코딩 과정이 필요 없다. 즉, 24~31까지의 NAL 타입은 선택적 사용이 가능하다. RBSP에는 SPS, PPS 등의 정보를 알려주는 parameter set과 VCL에 해당하는 Slice 데이터가 포함될 수 있다.

<표 1> NAL Unit Type

| 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] |

## 3. 제안하는 암호화 방식 및 DRM 시스템

### 3.1 제안하는 콘텐츠 암호화 방식

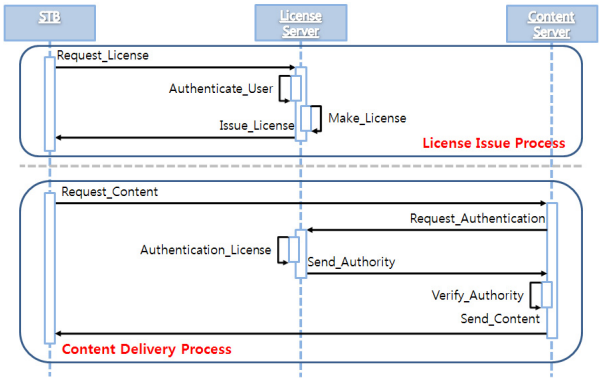
제안하는 콘텐츠 암호화 방식은 콘텐츠의 전체를 암호화하는 것이 아닌 일부 NAL 타입만을 암호화하는 것이다. 즉, 디코딩을 위하여 필수적인 정보라고 언급했던 NAL 타입인 SPS, PPS 만을 암호화한다. NAL 전체를 암호화 하는 방식은 암호화 강도 측면에서 장점이 있지만, 전체적으로 암호화를 위한 오버헤드가 증가하여 효율성이 크게 떨어진다. 그래서 오버헤드를 줄이고 효율성을 높일 수 있는 NAL 일부만을 암호화하는 방식을 택한다.

### 3.2 제안하는 인증서 방식의 DRM 시스템

제안하는 DRM 시스템은 인증서 방식을 택한다. 따라서 사용자가 STB를 통하여 최초로 서비스를 요청할 때 라이센스 서버에서 인증서를 발급하고, STB와 콘텐츠 서버에서는 발급된 인증서를 이용하여 콘텐츠를 주고 받는 형태이다. 제안하는 시스템에서 라이센스 서버는 하나의 인증기관으로서 역할을 수행한다. 그림 2는 제안하는 인증서 기반의 DRM 시스템의 동작과정을 간단하게 나타낸 Sequence Diagram이다.

## 4. 결론

디지털 콘텐츠의 보호를 위한 기술로서 DRM이 사용




(그림 2) 제안하는 인증서 기반 DRM의 동작과정

되고 있다. 또한 많은 콘텐츠의 디지털화가 급증하면서 DRM의 사용은 일반화되었다. 그 중 음성 및 영상 데이터에 대한 디지털화가 가장 활발하게 이루어지고 있으며 저작권 문제로 인해 이슈가 되기도 하였다.

본 논문에서는 영상 데이터 중의 하나인 H.264/AVC의 NAL이라는 특성을 이용하여 콘텐츠를 효율적으로 암호화하고 암호화된 콘텐츠를 사용자에게 전송하기 위해 인증서 방식의 DRM 시스템을 제안하였다. AES 암호화 알고리즘을 이용하여 foreman 비디오 파일을 H.264 형식으로 인코딩 한 후 특정 NAL 타입의 내용을 암호화하여 동영상 디코딩 시 화면을 알아볼 수 없을 정도임을 확인하였으며, 그림 3을 통하여 그 정도를 확인할 수 있다.

(그림 3) SPS 암호화 후 FFPlay로 디코딩한 화면

인증서 기반의 DRM 시스템의 경우 현재 개발 중에 있다. 현재 개발 중인 DRM 시스템은 향후 서비스 될 Mobile IPTV에도 적용할 수 있을 것으로 생각된다.

## ACKNOWLEDGEMENT

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2009-(C1090-0903-0011))

## 참고문헌

[1] 최동현, 이병희, 김승주, 원동호, "DRM(Digital Right Management) 기술", 정보과학학회지, 제25권 제5호, pp. 17 ~ 21, 2007.5.

[2] 정윤현, 오수현, "H.264 콘텐츠 스트리밍을 위한 효율적인 DRM 시스템의 설계 및 구현", 정보보호학회논문지, 제19권 제2호, pp. 155 ~ 163, 2009.4.

[3] 호요성, 김승환, "H.264/AVC 표준의 소스 코드 분석", 두양사, 2007.