MPEG-4 기반의 인터넷 방송을 위한DRM 솔루션의 설계 및 구현

김준일*, 김용빈*, 신동일*, 신동규*, 박지현**, 김정현**
세종대학교 컴퓨터공학과*
한국 전자통신 연구원 컴퓨터 소프트웨어 연구소**
e-mail: {junil, kimybin, dshin, shindk}@gce.sejong.ac.kr,
{iunhyun, bonobono}@etri.re.kr

Design and Implementation of the DRM Solution for MPEG-4 based Internet Broadcasting.

Jun-il Kim*, Young-bin Kim*, Dong-il Shin*, Dong-kyoo Shin*,
Ji-hyun Park**, Jung-hyun Kim**
Dept of Computer Science and Engineering, Sejong University*
Electronic and Telecommunications Research Institute**

요 약

본 연구는 MPEG-4 시스템 파일 포맷인 MP4 파일 포맷을 분석하여 I-VOP(Intra - Video Object Plane)의 추출·암호화를 통한 DRM 솔루션을 설계 및 구현하였다. 또한, 구현을 통해 암호화 정보를 포함한 DRM 정보를 MPEG-4 데이터 내부에 삽입하여 스트리밍 서비스에 DRM을 적용시키는 방안을 제시하였다. I-VOP의 암호화는 가장 효율적인 데이터 암호화 방안으로 전체 데이터를 암/복호화 하는데서 생기는 시스템 부하를 최소화 시킬 수 있다. 플레이어는 스트리밍 패킷을 받음과 동시에 데이터의 암호화 유·무를 확인하고, DRM 정보를 이용하여 복호화 시킴으로써 인터넷 방송용 MPEG-4 스트리밍 데이터의 저작권 보호를 실현한다.

1. 서론

인터넷과 통신 기술의 발전으로 인해 기존 다운로드방식의 디지털 정보는 실시간 스트리밍 형태의 서비스로 변화하고 있다. 디지털 정보의 편리성은 정보 소비자의 디지털 콘텐츠에 대한 수요를 더욱더 증가시키고 있고, 디지털 정보는 제작, 유통 상의 용이함으로 인해 정보 제공자의 디지털 콘텐츠 제작 또한 급증하고 있다 [1].

그러나 디지털 콘텐츠는 복제, 변형, 유포 등이 용이하고, 안전하지 않은 인터넷을 통해 유통되고 있어, 보안과 저작권 문제가 중요한 쟁점으로 대두되고 있다. 접근제어 위주의 보안대책과 함께 콘텐츠의 사용권한 제어 및 통제를 지속적으로 보호, 관리할 수 있는 새로운 기술에 대한 요구가 증가하고 있다.

본 연구는 개방된 인터넷 환경에 노출되어있는 인터넷 방송용 MPEG-4 데이터의 암호화를 통한 DRM 솔루션을 개발함으로써, 저작권 문제로 인한 온라인 콘텐츠 산업 및 오프라인 콘텐츠 산업의 위축을 방지하는 것을 목적으로 한다.

2. 인터넷 방송용 DRM 기술개요

멀티미디어 데이터에 DRM을 적용하는 방법으로는 Download DRM 과 Streaming DRM으로 구분될 수 있다.

2.1 Download DRM 기술

Download DRM 솔루션은 인증된 사용자에게 파일 서버에 저장되어 있는 컨텐츠의 복사를 허용함으로써 온라인, 오프라인에 관계없이 사용자가 해당 컨텐츠를 사용하도록 하며 다운로드한 컨텐츠를 불법 복제 및 불법유통으로부터 보호하는 방법이다. [그림1]은 일반적인 다운로드형 DRM 서비스 흐름도이다 [13].

[그림 1] 다운로드형 DRM 서비스 흐름도

2.2 Streaming DRM 기술

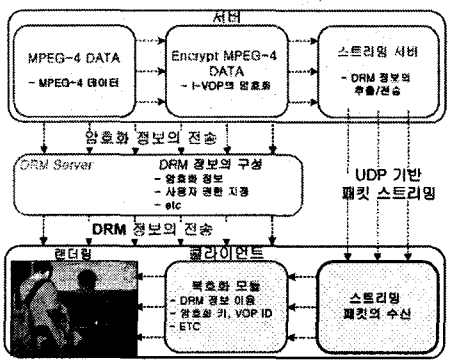
Streaming DRM 솔루션은 기존의 Download DRM 방식의 단점을 보완하여 실시간 서비스 적용가능한 방식이다. 사용자 인증시 발생한 사용자 키를 암호

화하여 세션을 유지하고 컨텐츠의 종료시 암호에 대한 효력을 상실하게 함으로써 컨텐츠에 대한 보안을 유지하는 방법이다. [그림2]는 스트리밍 DRM 솔루션의 서비스 흐름도이다 [13].

[그림 2] 스트리밍형 DRM 서비스 흐름도

3. 인터넷 방송용 DRM 솔루션의 설계 및 구현

본 논문에서는 MPEG-4를 이용한 다운로드 및 스트리밍 서비스에 모두 적용 가능한 DRM 솔루션을 구현하였다. 설계 및 구현에 대한 전반적인 구조는 [그림3]과 같다.



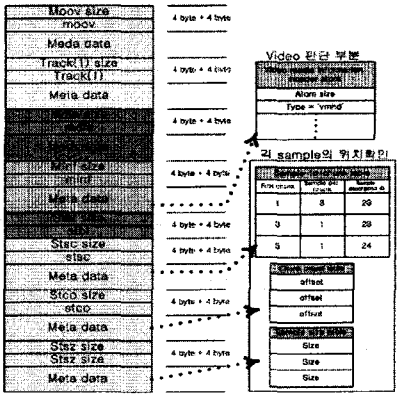
[그림 3] 인터넷 방송용 DRM 솔루션

본 논문에서는 MPEG-4의 압축특성을 이용하여 비디오 데이터 중 가장 중요도가 높은 I-VOP를 이용한 DRM 솔루션을 제안한다. 본 논문에서 구현한 I-VOP 추출 알고리즘을 이용하여 I-VOP를 추출/암호화한 후, 암호화에 관련된 정보를 MPEG-4 데이터 내부에 삽입함으로써 DRM 솔루션의 적용이 가능하다. 데이터 내부에 삽입된 암호화 정보는 스트리밍 서버에 의해 DRM 서버로 전송되고, DRM 서버는 인증된 사용자에게 사용자 규칙 등을 포함한 DRM 정보를 전송하게 된다, DRM 서버는 암호화와 관련된 DRM 정보에 사용자 규칙 등의 정보를 포함하여 사용자에게 전송하고, 사용자의 플레이어 내부에 삽입된 복호화 모듈을 이용하여 VOP를 실시간 복호화한다. 사용자는 암호화된 데이터를 전송받지만, 플레이어 내부의 복호화 모듈을 이용하여 원활한 서비스를 이용가능하다.

3.1 비디오 프레임 추출 알고리즘

MPEG-4의 시스템 포맷은 MP4 파일 포맷을 따른다. I-VOP를 추출하기 위해서는 전체 비디오 프레임(I, B, P -VOP)의 추출이 필수적이다. 비디오 프레임을 추출하는 방법으로 MP4 파일의 메타데이터를 파싱하여 각 비디오 프레임의 옵셋을 추출한다 [5,8].

MP4 파일은 실제 데이터를 가지고 있는 mdat Atom 과 실제 데이터의 기술정보를 가지고 있는 메타데이터로 나눠진다. 메타데이터는 Atom이라는 기본 데이터 유닛으로 구분되는데, 메타데이터의 가장 상위에는 Movie Atom이 존재한다. [그림4]은 MPEG-4의 전체 구조 및 내부에 존재하는 메타데이터를 파싱하여 비디오 프레임을 추출하는 개요도이다 [4,7].



[그림 4] 전체구조 및 Meta Data의 추출

비디오 샘플을 추출하기 위한 순서는 다음과 같다.

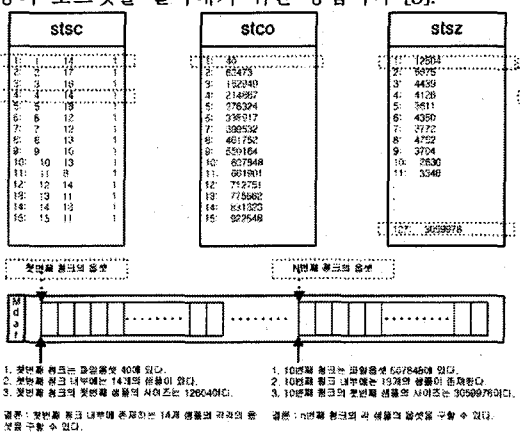
i. Video media Information header Atom의 존재 확인을 통해 비디오 트랙이 맞는지 확인한다.

ii 비디오 트랙 내에 Sample Table Atoms의 데이터를 추출한다.

- Sample Table Atoms에는 실제 데이터의 위치 정보와 Description 정보를 포함한 메타데이터가 들어있다.

iii. Sample Table Atoms 내에 있는 Sample to Chunk(stco), Sample per Chunk(stsc), Sample Size Atom(stsz)의 각 Table 정보를 얻어온다.

위의 세 단계를 이용하여, 비디오 트랙인지를 확인하고, 비디오 트랙내의 샘플 테이블을 얻어온 후, 각 샘플의 위치정보를 얻어올 수 있다. [그림5]는 얻어온 샘플의 위치정보를 이용하여 실제 데이터의 파일상의 오프셋을 알아내기 위한 방법이다 [5].



[그림 5] 실제 샘플의 오프셋 알아내기

3.2 I-VOP 추출 암호화

이전에 추출한 비디오 프레임을 이용하여 I-VOP를 찾아내고, 찾아낸 I-VOP의 상위 64bit를 블록암호화 한다. 본 과제에서 사용하는 블록 암호화방식은 DES 방식으로, 입력값과 출력값이 동일한 크기를 가지므로, 암호화된 데이터는 파일크기의 변화를 주지 않는다. 만약, 암호화에 입력값과 출력값이 동일하지 않은 암호화 알고리즘을 사용할 경우, Padding bit이 발생하여, 전체 sample의 파일옵셋이 변경되기 때문에 이런 피해를 최소화하기 위한 방안으로 블록 암호화 알고리즘인 DES를 이용했다. 또한, 64bit의 배수를 입력값으로 지정하여 DES 알고리즘상의 패딩이 일어나지 못하도록 예방하였다 [1,3].

비디오 샘플 중에서 I-VOP을 추출하는 방법으로는 MPEG-4 Visual Part 표준문서의 일부를 참조한다 [2]. 각 비디오 객체는 vop_start_code를 가지고 있다. 위에서 언급한 I, B, P-VOP의 실제 데이터에는 모두 스타트코드가 존재하는데, 그 Start_code는 4Byte (32bit)값으로 x00 00 01 B6(16진수)으로 정의된다. 또한 각 비디오 객체의 vop_start_code (4byte) 이후 2bit는 vop_coding_type을 나타내는데, 이 부분에서 I, B, P-VOP를 구분할 수 있다.

```
VideoObjectPlane()      {        No.      of      bits
Mnemonic
        vop_start_code      32      bslbf
        vop_coding_type     2       uimsbf
        do {
                modulo_time_base    1       bslbf
        }   while   (modulo_time_base   !=   '0')

        marker_bit 1        bslbf
        vop_time_increment  1-16    uimsbf
        marker_bit 1        bslbf
.....
}
```

[그림 6] MPEG-4 Visual Structure

다음 표는 vop_coding_type을 나타낸다. vop_coding_type을 알아내기 위한 방법으로 vop_start_code 이후 상위 2bit를 읽어온다. 읽어온 상위 2bit와 [표1]을 비교하여, vop의 coding type을 알아낸다 [2,7,9,10].

vop_coding_type	coding method
00	Intra-coded(I-VOP)
01	Predictive-coded(P-VOP)
10	Bidirectionally-Predictive-coded(B-VOP)
11	Sprite

[표1] VOP CODING TYPE

[그림7]은 위 과정에서 구현된 Encrypt Module을 이용해 I-VOP를 암호화한 데이터(우)와 실제 데이터(좌)의 비교화면이다.

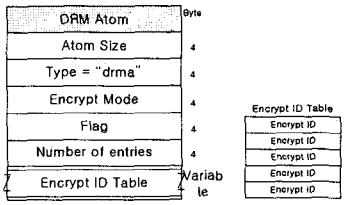
[그림 7] 암호화된 MPEG-4 의 비교

I-VOP를 암호화한 결과(우) 원본 파일(좌)과 비교했을때 Description 정보가 완전히 뒤바뀐 모습을 확인할 수 있다. 암호화시 VOP 단위로 암호화했기 때문에 재생에 있어 어떠한 에러도 출력하지 않는다. 하지만, I, P, B-VOP의 참조 위치가 변하게 됨으로 원본파일과는 전혀 다른 영상을 재생한다.

3.3 DRM MetaDATA의 생성

본 장에서는 MPEG-4 파일 내부에 DRM의 기본정보인 암호화 정보와 같은 DRM정보의 삽입을 위한 방법을 기술한다. DRM 정보를 MPEG-4 파일 내부에 넣음으로써, 유기적인 파일관리가 가능해지고, 실시간 스트리밍 서비스로의 확장이 용이하게 된다.

우선, 기존에 MPEG-4로 엔코딩된 데이터의 I-VOP를 암호화하게 되면, 디코더 측에 복호화 키와 I-VOP의 고유 ID를 전달해야 한다. 모든 비디오 (I, B, P-VOP)샘플은 고유 ID를 가지고 있는데, 가장 첫 번째 VOP 샘플에서부터 순차적으로 번호가 주어진다. 각 각의 MPEG-4 마다 I-VOP의 위치 및 고유 ID가 다르므로 서버는 클라이언트에게 I-VOP의 고유 ID를 알리는 것이 필수적이다. I-VOP의 고유 ID의 기술은 선택적 I-VOP의 암호화를 가능하게 한다. 본 연구에서는 DRM 솔루션에 이용 가능한 [그림8]과 같은 DRM Atom의 새로운 구조를 제안한다.



[그림 8] DRM Atom의 구조

본 DRM Atom의 형식은 MP4 파일포멧과 동일한 형식의 정의이다. 가장 상위의 4byte는 DRM Atom의 크기를 규정한다. Type은 'drma'로 규정하고, Encrypt Mode 필드는 암호화 방법을 기술한다. Flag 필드는 모든 VOP를 암호화 하였을 경우, 암호화 VOP Number, 즉 Number of entries와 Encrypt ID Table을 기술할 필요가 없기 때문에 1로 셋팅되었을 경우에는 Number of entries의 값이 NULL이라는 것을 나타낸다. 선택적 I-VOP를 암호화 하였을 경우에만, I-VOP ID의 entries를 나열하면 된다. [표2]는 DRM Atom의 Encrypt Mode에 대한 정의이다.

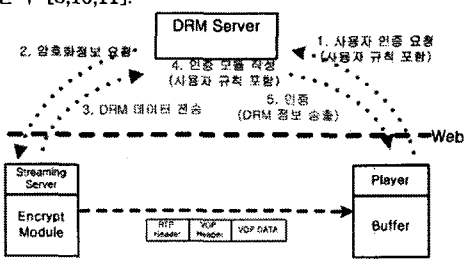
	Encrypt Mode	비 고
00	Whole VOP	64bit
01	Whole VOP	all bit
10	I VOP	64bit
11	I VOP	all bit

[표 2] Encrypt Mode

3.4 복호화 솔루션

복호화의 방법으로는 스트리밍 패킷의 내부를 감시하는 방법을 이용한다. RFC3016의 패킷타이징 기법에 따라 각 패킷의 내부는 VOP의 단편들로 구성되어있고, 각 VOP는 vop_start_coded를 가지고 있다 [6,12]. 본 논문에서는 플레이어의 버퍼 내부에 존재하는 VOP 데이터의 Start Code의 확인을 통한 복호화 방법을 이용한다.

클라이언트는 더블버퍼링(Double Buffering)구조를 가지고 있다. 첫 번째 버퍼는 패킷으로 나뉘어 들어오는 비디오 데이터를 하나의 완전한 VOP가 이루어질 때까지 저장하고 있다가, 하나의 VOP를 이루게 되면 랜더링 버퍼로 전송하는데, 이때, 두 번째 버퍼로 이동하는 메시지를 훅킹하여, 비디오 데이터의 스타트코드를 확인한다. 확인된 데이터의 상위 4byte를 감시하여, 그 패킷에 존재하는 데이터의 유형을 구분한다.(VOP 데이터, Audio 데이터의 구분) 전송받은 데이터가 VOP 데이터일 때, DRM 서버로부터 전송받은 DRM 정보를 이용하여 복호화한다. 플레이어의 복호화 방법으로는, VOP start code가 존재할 때마다, 프레임 인덱스를 부여하고, DRM 모듈로부터 전송받은 고유 ID와 일치하는 VOP 패킷에 vop_start_coded 부분을 제외한 하위 64bit*n을 복호화하게 된다. 복호화된 VOP 정보는 두 번째 버퍼를 거치고 사용자에게 랜더링 되게된다. 다음 [그림7]은 서버와 클라이언트간의 DRM 정보교환을 나타낸다 [3,10,11].



[그림 9] 서버와 클라이언트의 DRM 정보교환

처음 사용자는 웹 서버를 통해서 스트리밍 서비스의 인증을 요청하게 된다. 서버는 사용자의 요청을 허락할 경우 스트리밍 서버에 암호화 정보를 요청하고 스트리밍 서버는 암호화 정보를 DRM 서버로 전송한다. DRM 서버는 사용자 규칙을 포함한 DRM 정보를 플레이어에 전송함으로써 인증과정을 마치게 된다. 모든 인증과정이 끝나면 DRM 서버로부터 전송받은 DRM 정보를 기반으로 RTP로부터 전송받은 각 VOP를 복호화한 후 사용자 화면에 출력하도록 하였다. [그림10]은 암호화된 인터넷 방송용 MPEG-4 스트리밍 데이터를 실시간 복호화하여 재생하는 화면이다.

[그림 10] 실시간 복호화 장면

4. 결론 및 향후연구

본 연구에서는 인터넷 방송용 스트리밍 데이터의 암호화를 통해 강력한 저작권 보호를 실현했다. 스트리밍 데이터인 MPEG-4의 압축특성을 이용하여, 비디오 객체 데이터가 들어있는 I-VOP를 암호화하고, 복호화에 필요한 복호화키와 I-VOP 고유 ID를 DRM 정보에 삽입함으로써 인터넷 방송용 MPEG-4 DRM 솔루션을 구현했다. 기존에는 세션 연결단계의 보안유지를 통한 DRM 솔루션이 주류를 이루고 있다. 인터넷 방송용 MPEG-4 스트리밍 데이터 자체의 암호화를 통한 DRM 솔루션은 증가하는 디지털 콘텐츠시장의 새로운 해결방안이다 [1].

하지만, 본 연구는 MPEG-4 스트리밍 서비스에만 적용가능하다는 문제점을 가지고 있다. 현재 스트리밍을 위한 기술로는 MPEG-4 뿐만 아니라, RM, ASF 등 다양한 기술이 존재한다. 추후에는 모든 스트리밍 기술에 적용 가능한 DRM 기술의 개발이 이루어져야 할 것이다.

참고문헌

[1] Joshua Duhl "Understanding DRM Systems"
[2] "ISO/IEC FCD 14496-2 Visual" ISO/IEC
[3] "QuickTime Streaming Server Modules" Apple computer.inc, 2002
[4] "ISO/IEC JTC1/SC29/WG11N3506" 2000 July
[5] "QTFileFormat" Apple Computer 2000
[6] "RTP Payload Format for MPEG-4 Audio/Visual Stream" 2000, November
[7] *"The MPEG-4 video standard verification model"* Thomas Sikora
[8] "ISO/IEC FCD 14496-1 System" ISO/IEC
[9] "ISO/IEC 14496-1:2000" ISO/IEC
[10] " http://www.mpeg4ip.org " MPEG4IP
[11] http://www.applecomputer.com
[12] "Transmission of MPEG-4 video over the Internet" Sieven Gringeri, Sami Iren
[13] "Digital rights management and watermarking of multimedia content for m-commerce applications" Ericsson Research