MPEG-4 비디오 스트림의 암호화 기법 연구

김광호, 최순용, 김건희, 신동규, 신동일
세종대학교 컴퓨터 공학과
E-mail: {mis2010, artjian, ghkim, shindk, dshin }@gce.sejong.ac.kr

A Research on the Encryption Techniques of MPEG-4 Video Streams

Kwangho Kim, Soonyong Choi, Gunhee Kim, Dongkyoo Shin, Dongil Shin
Department of Computer Science and Engineering, Sejong University

요 약

본 논문에서는 MPEG-4 스트림의 디지털 저작권 관리(DRM)를 위한 암호화 방법을 제안한다. MPEG-4는 멀티미디어 스트리밍을 위한 표준이며 MPEG-4 파일 포맷에 따라 저장된다. 인가된 사용자들만 접근이 가능하도록 MPEG-4 파일 포맷으로부터 추출된 I-VOP, P-VOP의 매크로 블록(MB)들과 모션 벡터(MV)들을 암호화 하는 3가지 방법을 설계하였고, MPEG-4 데이터의 암호화에는 DES(Data Encryption Standard)를 사용하였다. 이러한 암호화 방법을 기반으로 MPEG-4 데이터 스트리밍을 위한 인터넷 방송 서비스용 DRM 솔루션을 구현하고, 최적의 암호화 방법을 선택하기 위해 복호화 속도 및 영상의 품질을 비교하였다.

1. 서론

오늘날의 통신 시스템은 유무선 환경을 통합하고, 디지털 컨텐츠 배포를 위한 고품질의 서비스를 제공한다. MPEG-4[1]를 사용한 스트리밍 서비스는 유무선 모두에 적합한 양질의 방송 솔루션 중의 하나이다.

본 논문에서는 MPEG-4를 사용하는 멀티미디어 서비스의 저작권 관리(DRM)를 위하여 디지털 컨텐츠를 암호화하는 방법을 적용하며, DES(Data Encryption Standard)[2,3]를 사용하여 MPEG-4 데이터를 암호화 하였다. 이를 위하여 MPEG-4 파일 포맷에서 추출한 매크로 블록(MB, Macro Block), I-VOP(Video Object Plane), P-VOP의 모션 벡터(MV, Motion Vector)를 암호화하는 3가지 암호화 방법을 제안하였다. 또한 이 3가지 방법을 기반으로, MPEG-4 데이터 스트리밍을 위한 인터넷 방송 서비스용 DRM 솔루션을 설계하고 구현하였다.

2. 배 경

MPEG-4 표준에서 하나의 장면(Scene)내의 동일한 물리적 객체에 해당하는 연속적인 VOP들을 비디오 객체(VO, Video Object)라 부르며, 이것은 임의의 모양과 위치를 갖는 VOP들의 시퀀스(Sequence)이다. 동일한 비디오 객체에 해당하는 VOP들의 모양과 움직임, 텍스쳐 정보는 인코딩되고 전송되거나, 코드화된다. MPEG-1과 MPEG-2처럼, I-VOP, P-VOP, B-VOP은 VOP의 기본 타입이고, 각각의 VOP은 매크로 블럭들로 분해되고, 매크로 블럭은 다시 6개의 블럭들로 나누어지며, 그 블럭 내에서 DCT(Discrete Cosine Transform)가 적용된다 [4,5].

2.1 전통적인 MPEG 비디오 암호화 기법

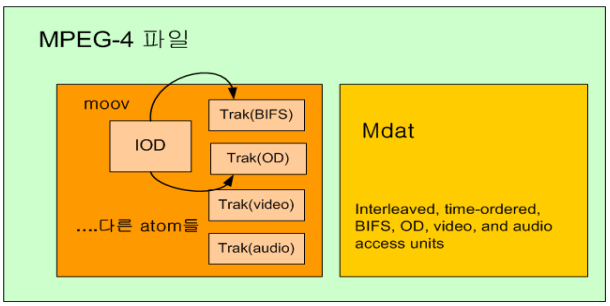
전통적으로 MPEG-1과 MPEG-2는 인증되지 않은 사용자가 스크램블하여 비디오 프로그램을 디코딩하지 못하도록 비디오 암호화 알고리즘을 사용한다 [6,7]. 일반적으로 평문으로 불리는 비디오 스트림 S에 비가역적 형 변환 E_{kl}을 적용하여, 비트스트림

(Bitstream)인 암호문 C를 생성하는 방법이 사용된다($C = E_{k1}(S)$). 비밀키 $k2$를 가진 인증된 사용자는 $D_{k2} = E_{k1}^{-1}$을 이용해 암호화된 비디오 스트림을 복호화할 수 있다. 복호화 과정은 다음과 같으며, 인자 $k1$은 암호화 키, $k2$는 복호화 키이다.

$$D_{k2}(C) = E_{k1}^{-1}(C) = E_{k1}^{-1}(E_{k1}(S)) = S$$

2.2 MPEG-4 파일 포맷

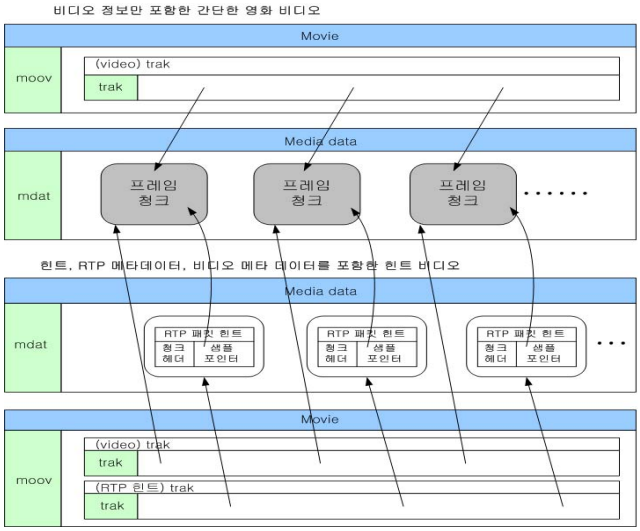
MPEG-4는 현재 ISO의 MPEG(Moving Picture Experts Group)에 의해 정의된 디지털 미디어 표준이다. MPEG-4 파일 포맷 표준을 채용함으로써, 모든 디지털 미디어 컨텐츠는 실시간 비디오와 오디오 스트리밍까지 지원하는 하나의 공통 파일 포맷으로 저작될 수 있게 된다 [1].



(그림 1) MPEG-4 파일 포맷의 예

MPEG-4 파일 포맷은 atom이라 불리는 객체 기반 구조로 구성되어 있다. 대부분의 atom들은 메타데이터의 계층구조로 이루어져 있고, movie(MOOV) atom내에 포함되어 있다. (그림 1)은 3개의 스트림을 포함한 간단한 교환 파일의 예이다 [1].

MPEG-4 파일 포맷은 힌트 트랙(hint track)인 메타데이터가 특정한 전송 프로토콜을 통해 미디어 데이터가 전달되는 방법을 서버 어플리케이션에게 알려줌으로써 스트리밍을 용이하게 해준다 [8,9].

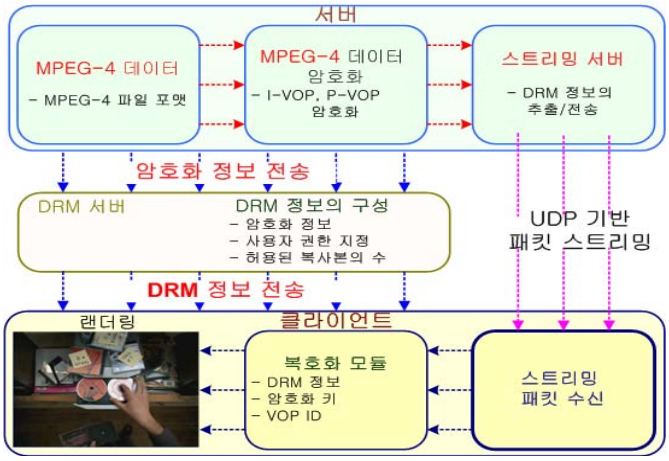


(그림 2) 비디오 스트림용 RTP 프로토콜 힌트 트랙들의 관계

(그림 2)는 간단한 비디오 스트림용 RTP 프로토콜 힌트 트랙들의 포함관계를 보여준다. 파일내의 메타데이터는 MPEG-4 파일 포맷이 컨텐츠의 스트리밍, 편집, 재생, 및 교환을 가능하게 해준다 [1,11].

3. DRM을 적용한 인터넷 방송 시스템의 설계 및 구현

본 논문에서는 MPEG-4 데이터 스트리밍이 가능한 인터넷 방송 서비스용 DRM 솔루션을 설계 및 구현하였다. 시스템의 전체 구조는 (그림 3)에 나타내었다.



(그림 3) 인터넷 방송을 위한 DRM 솔루션의 전반적인 구조

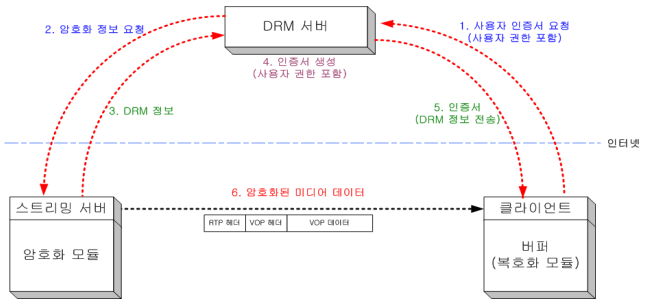
먼저 MPEG-4 파일에서 비디오 데이터를 추출하고, 여기에 3가지 종류의 암호화 방법을 적용하였다.

1) I-VOP 내의 매크로 블록(MB)들의 암호화 (*방법-1*)
2) P-VOP 내의 MB들과 모션 벡터(MV)들의 암호화 (*방법-2*)
3) I-VOP 내의 MB들과 P-VOP 내의 MB와 MV를 모두 암호화 (*방법-3*)

암호화 알고리즘으로는 DES(Data Encryption Standard)[2,3]를 사용했으며, 본 연구의 목표는 이러한 3가지 방법을 구현하고 테스트하여 DRM 솔루션을 위한 최적의 암호화 기법을 찾는 것이다.

본 연구에서는 각각의 VOP에 대한 MB와 MV를 추출하기 위해 MPEG-4 파일 포맷 내의 MPEG 데이터에 직접 접근을 시도하였고, 이미 암호화된 MPEG-4 파일의 효율적인 관리를 위해 MPEG 데이터 파일에 DRM 정보를 삽입하였다.

암호화된 MPEG-4 데이터는 DRM 서버가 제공한 DRM 정보(복호화 키와 사용자 인증 정보)와 함께 클라이언트에 전송된다. 클라이언트는 복호화 모듈을 사용해서 실시간으로 전송된 미디어 데이터를 복호화하고, 복호화된 미디어 데이터를 렌더링(rendering)한다. (그림 4)는 클라이언트와 스트리밍 서버 사이에서 DRM 서버가 DRM 정보를 전송하는 구조를 보여준다.



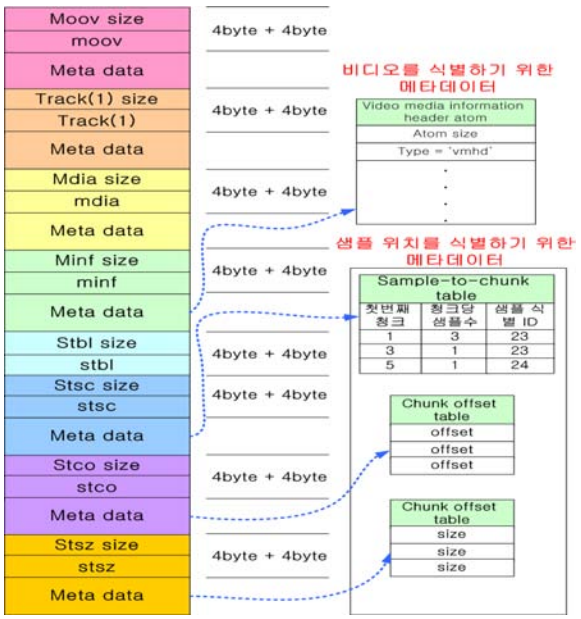
(그림 4) 클라이언트와 서버 간의 DRM 정보 전송

3.1 비디오 프레임 추출 알고리즘

MPEG-4 파일 포맷은 atom들로 구성되어 있으며, 크게 메타데이터(moov atom)와 실제 데이터(mdat atom)의 두 부분으로 나뉘어 진다 [1,10].

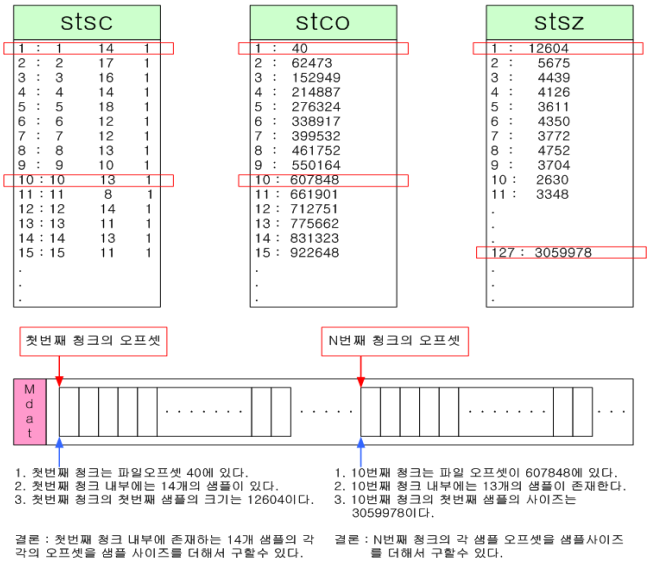
MPEG-4 파일 포맷의 비디오 데이터를 암호화하기 위해서 MPEG-4 파일의 메타데이터를 파싱(parsing)해야만 하고, I-VOP, P-VOP, B-VOP과 같은 비디오 프레임들을 추출해야 한다. (그림 5)는 비디오 데이터를 추출하기 위해서 MPEG-4 파일 포맷의 메타데이터를 해석하는 방법을 보여준다.

비디오 샘플을 추출하기 위해 비디오 트랙의 stbl(sample table atom), stco(sample to chunk), stsc(sample per chunk), stsz(sample size) atom 테이블 정보(table information)를 획득한다.



(그림 5) MPEG-4 파일 포맷의 메타데이터 해석

위의 기술된 절차에 따라, 비디오 트랙 내의 sample 테이블과 각 샘플의 위치 정보를 얻는다. (그림 6)은 각 샘플의 위치정보를 이용하여 오프셋(offset)을 계산하여 mdat atom으로부터 실제 데이터를 획득하는 방법을 보여준다 [1,10].



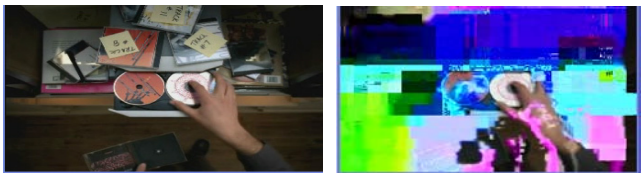
(그림 6) 오프셋을 계산하여 비디오 데이터를 획득

3.2 I-VOP의 매크로 블록 추출 및 암호화 (방법-1)

I-VOP을 비디오 데이터에서 추출하고, DES를 I-VOP에 적용한다. DES는 블록 암호화 알고리즘이며, 입출력 데이터의 크기에는 영향을 주지 않는다.

MPEG-4 비디오 표준[5]을 따라 비디오 데이터에서 I-VOP을 추출하였다. 각 VOP은 하나의 video_start_code와 vop_coding_type으로 I-VOP, P-VOP, B-VOP들의 VOP타입을 식별한다.

(그림 7)은 I-VOP 내의 매크로 블록들을 암호화한 결과를 보여준다.



(그림 7) I-VOP 내의 매크로 블록을 암호화한 결과

3.3 P-VOP 내의 매크로 블록들과 모션 벡터들의 암호화 (방법-2)

P-VOP 내의 인트라 코딩된 매크로 블록(MB)들과 모션 벡터(MV)들을 암호화하며 결과는 (그림 8)와 같다. I-VOP의 인트라 코딩된 매크로 블럭들이 많은 정보를 가지고 있기 때문에, 스트리밍되는 동안 몇몇 완전한 정지 영상들이 나타나게 된다. 만약, 비디오 시퀀스 내에 I-VOP의 비율이 크지 않다면, P-VOP 암호화는 효율적인 방법이 될 수 있다.

(그림 8) P-VOP 내의 매크로 블록과 모션벡터 암호화 결과

3.4 I-VOP 내의 매크로 블럭과 P-VOP 내의 모션 벡터 동시 암호화 (방법-3)

인트라 코딩된 매크로 블록들이 많은 코딩 정보들을 가지고 있기 때문에 *방법-1*과 *방법-2*는 둘 다 만족할 만한 결과를 제공해 주지는 않는다. 이 문제를 해결방안으로 I-VOP 내의 매크로 블록들과, P-VOP 내의 모션 벡터들을 함께 암호화 한다. (그림 9)은 그 결과를 보여주며, 이것은 3가지 방법 중에 가장 강력한 암호화 방법이지만, 암호화를 위해 처리해야할 데이터량이 증가하여, 스트리밍 시퀀스를 재생하는 클라이언트의 수행능력이 감소되었다.

(그림 9) I-VOP 내의 매크로 블럭과 P-VOP 내의 모션벡터를 모두 암호화한 결과

4. 암호화 속도에 관한 모의 실험

본 연구에서는 MPEG-4 데이터를 위한 암호화 방법중 *방법-3*이 가장 뛰어난 암호화 결과를 보여주는 반면, 암호화 과정에서 처리해야하는 데이터량이 크다. 속도 증진을 위해 I-VOP의 빈도수를 조정하여 암호화에 사용될 데이터의 양을 조절할 수도 있으나, 일반적으로 I-VOP의 매크로 블럭들만 암호화하는 작업에 필요한 데이터양은 그리 크지 않다. VOP을 암호화하는 시간은 아래와 같다.

$$E(t) = DES(t) + M(t)$$

*E(t)*는 VOP의 암호화 작업을 처리하는 시간이고, *DES(t)*가 DES 암호화 작업을 처리하는 시간, *M(t)*는 전처리 시간이다.

<표 1>는 위 공식에 의하여 "CDR_Dinner.mp4"(그림 7,8,9)의 암호화 결과에서 사용된 파일)파일을 이용해 얻은 결과이다.

<표 1> 암호화 속도 측정 결과 (millisecond)

파일	VOP 개수	암호화 방법	암호화 VOP개수	평균 VOP 암호화 시간	전체 VOP 암호화 시간
CDR_Dinner.mp4	902	방법-1	23	1.5294389	35.1770958
		방법-2	879	0.2557534	224.8072710
		방법-3	902	0.2664301	240.3199226

<표 1>은 암호화의 속도가 데이터의 양에 좌우된다는 것을 보여준다. 비록 *방법-3*이 *방법-1*보다 암호화 및 복호화 작업에 7배 정도의 시간이 소요되지만, 클라이언트는 복호화, 디코딩, 렌더링 모두를 버퍼에서 처리한 후 재생하기 때문에 재생 자체에는 영향을 주지 않는다.

5. 결론

본 연구에서는 MPEG-4파일 포맷에서 비디오 데이터를 추출하고 DES를 사용하여 VOP들을 암호화하는 DRM 솔루션을 설계하고 구현하였다. VOP에서 매크로 블록(MB)과 모션 벡터(MV)를 추출하여 암호화하는 3가지의 암호화 방법을 사용하였으며, *방법-3*이 가장 좋은 암호화 결과를 보여주는 반면, 가장 많은 데이터양과 처리 시간이 요구된다. 각각의 암호화 방법은 특정한 조건 하에서 최적의 성능을 나타낼 수 있다.

향후에는 멀티미디어 스트리밍 서비스를 위해 암호화된 미디어 데이터와 결합된 DRM 정보의 관리 방법이 중점 연구될 것이다.

참 고 문 헌

[1] "Information technology - Coding of audio-visual objects - Part 1: Systems ISO/IEC 14496-1:2001", ISO/IEC/SC29/WG11, 2001.

[2] "Data Encryption Standard (DES)", FIPS PUB 46-3, Oct. 25. 1999.

[3] Stallings William , "Cryptography and Network Security : Principles and Practice", 3rd Edition, Prentice Hall, 2002.

[4] Sikora Thomas, "The MPEG-4 video standard verification model", IEEE Transactions on Circuits and Systems for Video Technology, pages 19-31, Feb. 1997.

[5] "Information Technology Coding of Audio-Visual Objects Part 2:Visual, ISO/IEC 14496-2", ISO/IEC/SC29/WG11, Nov. 1998.

[6] M. Adnan, Alattar and Al-Semari, "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams", Proceedings of 1999 International Conference on Image Processing, pages 256 -260, Oct. 1999.

[7] C. Shi and B. Bhargava, "An Efficient MPEG Video Encryption Algorithm", Proceedings of Seventeenth IEEE Symposium on Reliable Distributed Systems, pages 381 -386, Oct. 1998.

[8] "QuickTime Streaming Server Modules", Apple computer, 2002.

[9] Gringeri Sieven, Iren Sami, "Transmission of MPEG-4 video over the Internet", IEEE International Conference on Multimedia and Expo, pages1767 -1770, July. 30 - Aug. 2. 2000.

[10] "QuickTime File Format", Apple Computer, June. 2000.

[11] "RTP Payload Format for MPEG-4 Audio/Visual Stream", RFC 3016, Nov. 2000.