DRM 기반 MP4 스트리밍을 위한 비디오 암호화 알고리즘에 관한 연구

김 정 현, 윤 기 송, 전 경 표
한국전자통신연구원

A Study on Video Encryption Algorithm for DRM-based MP4 Streaming

Kim jeong-hyun, Yoon ki-song, Jeon kyung-pyo
Electronics and Telecommunications Research Institute
E-mail : bonobono@etri.re.kr

요 약

Internet의 발달로 사람들은 정보를 쉽게 얻을 수 있을 뿐만 아니라 교환하고 유통할 수 있게 됨에 따라 컨텐츠 불법복제 문제를 야기 시키고 이로 인해 저작권 보호에 대한 관심이 높아지고 있다. VOD(Video On Demand)와 인터넷 방송과 같은 멀티미디어 상거래 또한 사용 권리를 가진 사용자만이 컨텐츠에 접근하고 이용할 수 있어야 한다. 본 논문에서는 MP4 기반 스트리밍 서비스 모델에 적용할 수 있는 DRM(Digital Rights Management) 시스템을 제시하여 이 DRM 시스템에 적용할 수 있는 MP4 암호화 알고리즘을 제안한다.

Abstract

Internet has made it easer to get information, also distribute and exchange it among people. It brings about issues regarding intelligent property and copyright threats. In a multimedia commerce such as video-on-demand, Internet broadcasting services, only users who have rights for use of these services should be able to access and watch those video or movies. In this paper, we propose DRM(Digital Right Management) system for MP4 -based streaming and MP4 encryption algorithm for proposed DRM system.

I. 서론

인터넷이 보편화되고 디지털 기술이 발전하면서 누구나 쉽게 디지털 컨텐츠를 사용하고 배포할 수 있게 되었다. 이로 인해 불법복제와 같은 문제들이 대두되고 있다. VOD, 인터넷 방송과 같은 스트리밍 멀티미디어 또한 불법 다운로드 및 불법 사용으로 인한 문제가 심각한 상황이다.

본 논문에서는 MP4 기반 스트리밍 서비스 모델에 적용할 수 있는 DRM 시스템을 제안하고 이 DRM 시스템에 적용할 수 있는 MP4 파일에 대한 암호화 알고리즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 컨텐츠 보호 및 권리 보호를 위한 유통모델을 제시한다. 또한 MP4 파일 포맷 표준에 대한 설명과 기존의 MPEG 비디오 암호화 알고리즘 및 문제점을 기술한다. 3장에서는 DRM 시스템과 MP4 스트리밍 모델에 적용할 수 있는 암호화 알고리즘을 제안하고, 마지막으로 4장에서는 정리 및 향후과제를 결론을 맺는다.

II. 관련연구

1. 컨텐츠 보호 및 권리 보호를 위한 유통 모델

컨텐츠를 보호하고 저작권자 및 유통 주체들의 권리를 보호하기 위해서 컨텐츠 유통모델을 좀더 연구할 필요가 있다. 우리는 MPEG-21[1]에서 채택하고 있는 European Commission IMPRIMATUR Business Model[2]을 참고하였다. IMPRIMATUR Business Model은 ERMS(Electronic Rights Management System), 즉 DRM시스템 개발에 관한 개념적인 프레임웍을 보여주고 있다. 이것은 컨텐츠를 만들고 유통시키는데 관련된 역할(role) 및 이러한 역할들 간의 관계를 정의하고 있다. 그림 1은 IMPRIMATUR Business Model에서 Media Distributor(유통업자)를 통해 수익(royalty)분배가 이루어짐으로서 발생할 수 있는 유통 주체들 간의 수익분배 문제를 해결하기 위해 기존의 모니터링 서버 대신 클리어링하우스로 대체함으로써 모니터링 역할뿐만 아니라 수익 분배가 올바르게 이루어지는지 관여할 수 있도록 수정한 모델이다.

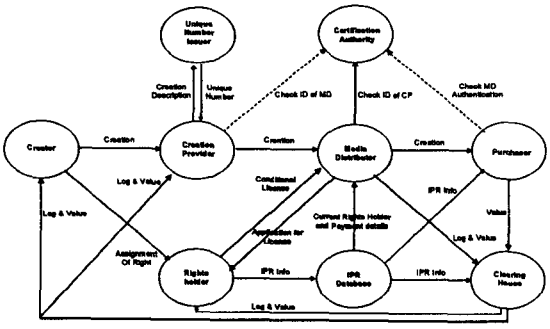

그림 1. 수정된 IMPRIMATUR Business Model

2. MP4 파일 포맷 표준

MP4 파일 포맷은 MPEG-4 미디어의 상호 교환, 관리, 편집, 화면 재생 등을 수월하게 할 수 있도록 유연하고 확장 가능한 형식으로 설계된 파일 포맷 이다[3].

MP4 파일은 atom이라는 단위로 구성되어 있고 그림 2와 같이 메타데이터를 담고 있는 movie atom과 실제 미디어 데이터를 담고 있는 media data atom으로 구성되어 있다. 그림 2에서 moov는 movie atom의 타입이고 mdat는 media data atom의 타입을 나타낸다.

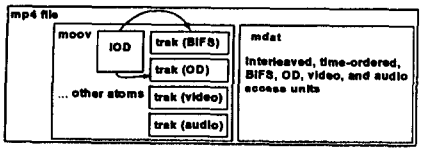

그림 2. MP4 파일 구조

Atom은 다시 여러 개의 track으로 구성되는데 video track, audio track, OD(Object Descriptor) track, BIFS(Binary Format for Scene) track 등이 있다. 그림 3은 Atom의 계층적 구조를 자세히 보여주고 있다.

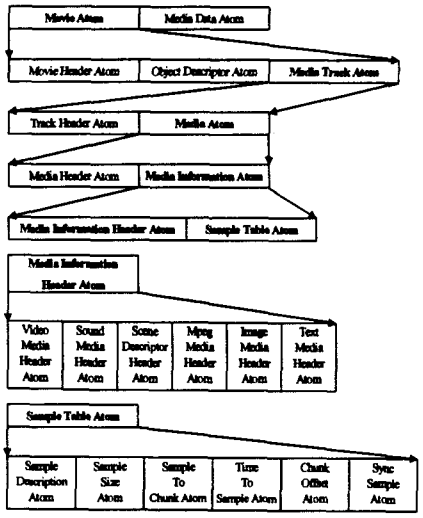

그림 3. Atom의 계층적 구조

MP4 파일 안의 실제 미디어 데이터는 그림 4와 같이 비디오와 오디오 프레임으로 구성된 video chunk와 audio chunk가 연속된 형태로 되어 있다. 그림 3의 sample table atom은 비디오와 오디오의 chunk와 프레임 정보를 나타내고 여기에 있는 offset 정보를 이용해 media data atom의 실제 데이터에 접근할 수 있다. 이때 sample은 frame을 의미한다.

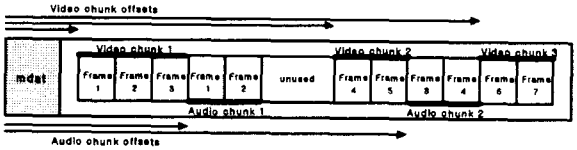

그림 4. Media Data Atom 구조

MP4 파일의 스트리밍 방법은 기존의 스트리밍 미디어 포맷과 차이가 있다. 기존의 스트리밍 미디어 포맷은 미디어 자체를 패킷화하여 스트리밍이 가능하도록 하는 반면 MP4 파일의 경우 미디어 데이터 자체는 그대로 두고 미디어 데이터의 패킷화하는 방법과 타임정보 등과 같은 스트리밍에 필요한 정보들을 기술한 hint track을 이용한다. 따라서 MP4 파일 안의 video data와 audio data를 스트리밍하기 위해서는 video track에 대한 hint track과 audio track에 대한 hint track을 추가하면 된다. 그림 5는 video track에 대한 hint track과 참조 관계를 보여주고 있다.

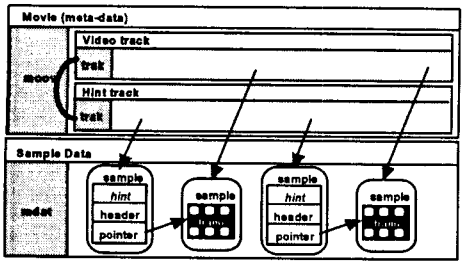

그림 5. MP4 파일의 hint track을 포함한 구조

3. MPEG 비디오 암호화 알고리즘

3.1 전체 암호화 방법

비디오 암호화 방법의 가장 간단한 방법은 DES[4]나 AES[5]와 같은 표준 암호화 알고리즘을 이용해 MPEG 비디오 스트림 전체를 암호화 하는 것이다. 이 방법은 가장 안전할 수는 있지만 스트리밍에 적용하기에는 속도나 계산량에 따른 오버헤드 면에서 제약이 따른다.

3.2 프레임 기반 선택적 암호화 방법

위와 같은 문제를 해결하기위한 하나의 방법으로 선택적 암호화 방법이 나오게 되었다. 선택적 암호화 방법은 암호화할 부분의 선택 방법에 따라 크게 다음과 같이 나눌 수 있다.

1) I-프레임 암호화

MPEG video 스트림은 시간적 상관관계를 이용한 압축을 이용하기 때문에 완전한 영상 정보를 담고 있는 I-프레임과 I-프레임을 참조하여 하나의 프레임 영상을 복원할 수 있는 P-프레임과 B-프레임으로 구성되어 있다. 이러한 특성을 이용해 Spanos와 Maples[6][7]는 I-프레임만을 암호화 하는 방법을 제안하였다. 그러나 이 방법을 이용해 암호화 했을 경우 P/B-프레임에 포함된 인트라 블록에 의해 영상의 주요 부분들이 여전히 화면에 나타나는 것을 Agi와 Gong[8]은 보여주고 있다. P/B-프레임에 포함된 인트라 블록은 I-프레임을 참조하지 않고 독립적으로 디코딩이 가능하기 때문이다.

2) I-프레임과 P/B-프레임의 인트라 블록 암호화

위와 같은 문제를 해결하기 위해 Agi와 Gong[8]은 I-프레임 전체와 P/B-프레임에 포함된 인트라 블록을 모두 암호화 하는 방법을 제안하였다. 그러나 이 방법 또한 문제점을 야기 시킨다. 전체 MPEG 스트림 중에서 I-프레임이 차지하는 비율이 높고 영상의 종류에 따라 전체가 I-프레임으로 구성되어 있을 수도 있다. 또한 P/B-프레임에 포함된 인트라 블록을 찾기 위해서는 MPEG 스트림을 비트 단위로 찾아야하는 부담이 있다[9].

3.3 DCT 계수의 선택적 암호화

I-프레임과 P/B-프레임의 인트라 코딩된 블록은 DCT 계수로 구성되어있다. 따라서 인트라 코딩된 블록 전체를 암호화 하는 것이 아니라 DCT 계수의 일부를 암호화 하는 방법들이 나오게 되었다. 이러한 방법들은 DC 계수와 하위 AC 계수들에 대부분의 에너지가 집중되어 있다는 사실을 기반으로 하고 있다.

1) Zig-Zag Permutation 알고리즘

Tang[10]은 DC 계수를 암호화 하고 AC 계수를 스크램블링 하는 방법을 제안하였다. 이 방법에서는 8x8의 DCT 계수들을 읽을 때 zig-zag scan order 방식 대신 이 논문에서 제안한 random permutation list를 이용하였다. 이 방법은 매우 빠르기는 하지만 암호화 후 데이터의 크기가 증가하고 보안상 문제점이 있다. DCT 계수 분포의 확률성을 변형시킴으로서 Huffman Table의 효율을 떨어뜨림으로써 압축율 또한 낮아지기 때문이다. Qiao와 Nahrstedt[11][12]는 실험을 통해 이 방법이 알려진 평문 공격과 암호문 공격에 취약함을 보이고 있다.

2) DCT 계수와 움직임 벡터의 sign bit 암호화

Shi와 Bhargava[13][14][15]는 선택된 DCT 계수의 sign bit와 모든 움직임벡터의 sign bit를 암호화 한다. 이 방법은 AC 계수 전체를 암호화 하는 것이 아니기 때문에 계산량에 대한 오버헤드면에서 효율적인 방법이 될 수 있다. 그러나 Chung-Ping Wu와 C.-C Jay Juo[16]는 실험을 통해 sign bit만을 암호화 하는 방법이 효과적이지 못함을 보여주고 있다.

3.4 무작위 선택적 암호화

Qiao와 Nahrstedt[11][15]는 엔트로피 코딩이 끝난 후 적용할 수 있는 암호화 방법을 제안하였다. 이 방법은 전체 MPEG 스트림 중에서 절반만을 암호화 하는 것으로 전체를 암호화하는 것에 비해 약 47% 정도 계산량을 감소시킨다. 그림 6은 이 알고리즘을 보여준다.

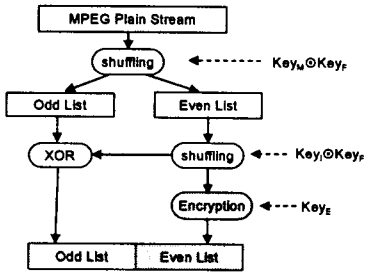

그림 6. Qiao와 Nahrstedt의 제안 알고리즘

기본 방법은 one-time pad 알고리즘의 특성을 기반으로 하고 있다. MPEG 스트림을 동일한 크기로 두 부분으로 나누어 이것을 XOR 연산을 한 후 이 중 한 부분을 DES를 이용해 암호화한다. 그림 6의 마지막 부분과 같이 XOR 연

산의 결과 값과 암호화된 결과 값이 결국 최종 값이 된다. 이때 DES 암호화를 했던 부분이 pad 역할을 하게 된다.

One-time pad 알고리즘은 pad가 랜덤하다면 안전한 방법이기 때문에 Qiao와 Nahrstedt가 제안한 방법 또한 암호화가 될 부분의 랜덤성만을 보장해 준다면 안전한 방법이 될 것이다. Qiao와 Nahrstedt는 MPEG 스트림에 대한 실험을 통한 동일한 비트 패턴이 발생하는 통계적 특성을 이용해 그 값을 랜덤하게 하고 있다.

III. 제안 시스템

1. DRM 시스템

그림 7은 위에서 설명한 유통 모델을 기반으로 설계한 DRM 시스템의 구조이다. 이 구조에는 원본 컨텐츠 생성과 관련된 부분은 제외되었다. 이 DRM 시스템은 위에서 정의한 역할을 기반으로 모듈별로 설계되어 유연성 있는 구조로 되어있기 때문에 스트리밍 서비스 모델뿐만 아니라 다운로드 방식의 컨텐츠 유통 모델에 적용하더라도 구조상 변화는 거의 없다.

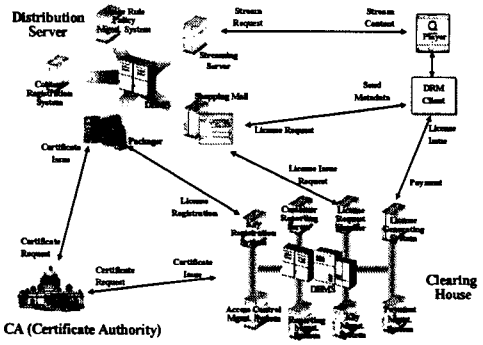

그림 7. 스트리밍 미디어를 위한 DRM 시스템 구조

2. MP4 스트리밍을 위한 비디오 암호화 알고리즘

컨텐츠 보호를 위해 컨텐츠 암호화는 DRM 시스템에서 필수 요소이다. MP4 스트리밍 모델에 DRM을 적용하기 위해서는 MP4 파일의 암호화 작업이 먼저 수행되어야하고 여기에는 다음과 같은 요구사항이 따른다.

첫째, 암호화된 MP4 파일은 표준 MP4 파일 포맷을 따라야 한다. 스트리밍 서버는 서비스할 파일의 암호화 여부에 상관없이 스트리밍이 가능해야 하기 때문이다.

둘째, 암호화는 인코딩 과정과 별도로 압축이 끝난 상태에서 적용할 수 있어야 한다. 이것은 위에서 제시한 컨텐츠 유통 모델을 지원하기 위해서 압축과정이 끝난 후 MP4 파일로 존재하는 상태에서 암호화를 할 수 있어야 함을 의미한다.

셋째, 스트리밍 미디어에 대한 기본적인 요구사항으로 여기에 적용할 암호화 방법은 실시간을 보장할 수 있어야 한다.

그림 8은 MP4 파일의 암호화에 대한 간략한 프로세스를 나타낸 것으로 암호화하기 전의 MP4 파일 구조와 암호화 후의 MP4 파일 구조를 보여준다.

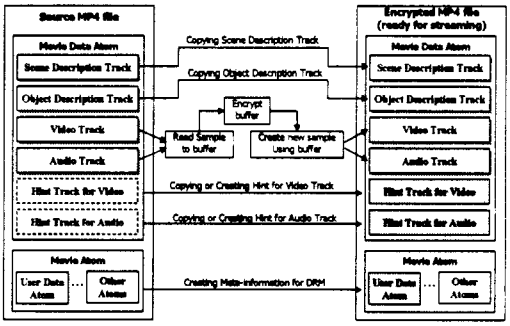

그림 8. MP4 파일의 암호화 프로세스

본 DRM 시스템에서는 위에서 설명하고 있는 Qiao와 Nahrstedt가 제안한 알고리즘을 확장하여 이용한다. Qiao와 Nahrstedt 알고리즘에서 전체 스트림 중 절반만을 암호화 함하도록 고정되어 있기 때문에 보안성 레벨을 조절 할 수 없었다. 그래서 본 논문에서는 그림 9에서 박스 안에 표시된 과정을 한번 더 수행함으로써 와 같이 전체 파일의 1/4, 1/8까지 암호화량을 조절할 수 있도록 한다. 이와 같은 과정을 수행할 때는 전체 MPEG 스트림을 128 바이트씩 나누어 수행하며 바이트 단위로 처리한다.

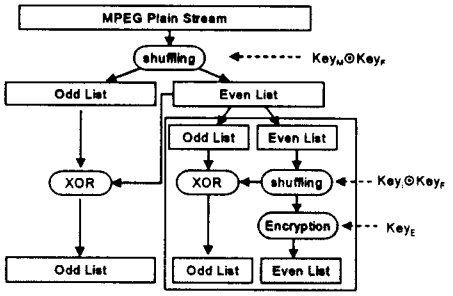

그림 9. 수정된 알고리즘

또한 표 1과 같이 I-프레임과 P/B-프레임의 암호화량을 다르게 적용함으로써 암호화 효율을 높일 수 있을 것으로 예측된다.

표 1. 암호화 모드

Encryption Mode	I-frame	P-frame	B-frame
Mode 1	1/2	1/4	1/4
Mode 2	1/2	1/8	1/8
Mode 3	1/4	1/8	1/8

IV. 결론 및 향후과제

본 논문에서는 MP4 스트리밍 서비스를 위한 DRM 시스템의 구조 및 DRM 시스템에서 이용할 수 있는 비디오 암

호화 방법에 대해 제안한다. 제안 방법은 앞에서 제시한 세 가지 요구사항을 만족하며 사용자들이 불법으로 스트리밍 데이터를 다운로드하더라도 원본컨텐츠의 유출을 막을 수 있다.

향후 실험을 통해 제안 방법에 대한 안전성 및 효율성을 보일 계획이다.

참 고 문 헌

[1] ISO/IEC JTC1/SC29/WG11/MPEG/N3939 Information technology - Multimedia framework(MPEG21) - Part1: Vision, Technlogies and Strategy, Jan. 2001

[2] IMPRIMATUR Business Model, Version 2.1, June 1999, Available at http://www.imprimatur.net

[3] ISO/IEC JTC1/SC29/WG11/MPEG/N4668 MPEG-4 Overview-(V.21.-Jeju Version)

[4] Data Encryption Standard(DES), FIPS Publication 46-2 1993

[5] Announcing the Advanced Encryption Standard(AES), FIPS Publication 197, 2001

[6] Maples T.B. and Spanos GA. Performance study of a selective encryption scheme for the security for networked real-time video, ICCC 1995

[7] Spanos G.A. and Maples T.B., Security for real-time mpeg compressed video in distributed multimedia applications, 15th IEEE International Phoenix Conference on Computers and Communications, March 1996

[8] Agi I. and Gong L., An empirical study of secure mpeg video transmission, IN NDSS 1996

[9] L.Qiao and K. Nahrsedt, A new algorithm for mpeg video encryption, Proceedings of the First International Conference on Imaging Science, System and Technology, July 1997

[10] Tang L. Methods for Encrypting and Decrypting MPEG Video Data Efficiency, ACM Multimedia 1996

[11] L.Qiao and K. Nahrsedt, and I. Tam, Is mpeg encryption by using random list instead of zigzag order secure?, IEEE International Symposium on Consumer Electronics, December 1997

[12] C. Shi and B. Bhargava, A Fast MPEG Video Encryption Algorithm, in Proc. of the sixth ACM international conference on Multimedia, September 1999

[13] C. Shi and B. Bhargava, An Efficient MPEG Video Encrytpion Algorithm, Reliable Distributed Systems, Proceedings. 17th IEEE Symposium on, October 1998

[13] C. Shi S.Y. Wang, and B. Bhargava, MPEG Video Encryption in Real-time Using Secret key Cryptography, in Proc. of PDPTA 1999

[14] Chung-Ping 쩌 and C.-C.Jay Juo, Fast Encryption Methods for Audiovisual Data Confidenciality, SPIE Vol. 4209

[15] ㅣ.Qiao and K. Nahrstedt, Compression of mpeg encryption algorithms, International Journal on Computer & Graphic, 1998