다중 랜덤 대칭키를 사용한 DRM 보안 시스템에 관한 연구

이광형[0], 정용훈, 김정재, 이경석, 전문석
dreamace@seoil.ac.kr, jyh0178@empal.com, argniss@yahoo.co.kr, mjun@computing.ssu.ac.kr

A Study on DRM Security System Using Multi-Random Symmetric Key

요 약

본 논문에서는 기존의 암호화 방법보다 다양한 키를 생성하는 알고리즘을 제안하고, 키 생성 알고리즘을 통해 각각 생성된 대칭키를 서버에 저장하지 않는 기존의 시스템보다 보안성이 높은 암호화 방법을 제안한다. 제안한 시스템을 설계하고 구현한 후 성능 평가를 위해 다양한 크기의 비디오 데이터 파일을 이용하여 실험을 수행하여 제안한 시스템이 기존 시스템에 비해 비디오 데이터 파일 재생 시 암호화 복호화 시간을 포함한 지연시간을 줄어 든 것을 검증하였다.

1. 서론

인터넷의 확산과 컴퓨터 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 디지털 저작물은 품질의 손상 없이 복제가 가능하기 때문에 디지털 저작권 관리(DRM: Digital Rights Management) 기술이 필요하다. 이러한 DRM 기술을 이용하여 InterTrust사와 Microsoft사 등의 외국 업체와 Digicap와 같은 국내 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다[3].

하지만 기존 DRM 솔루션들은 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보장하지 못하는 단점이 있다.

기존의 DRM은 이 문제를 해결하기 위해서 여러 개의 대칭키를 사용하여 암호화하는 기법을 제안하며, 암호화 및 복호화 속도를 개선하기 위하여 동영상 전체가 아닌 부분적으로 암호화 하는 방법을 제안한다. 또한 동영상 재생 시 대용량의 복호화를 수행하기 위해서 많은 시간이 필요하므로 원활한 동영상의 재생을 위하여 효율적인 보상 이중 버퍼 스케줄링을 사용하여 사용자에게 실시간, 복호화 및 재생을 할 수 있도록 시스템을 제안한다.

2. 관련 연구

2.1 기존의 DRM 시스템

2.1.1 InterTrust의 DRM 시스템

InterTrust사의 DRM 솔루션은 사전에 암호화되어 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 라이선스 에이전트가 라이선스를 확인하고 지불정보를 전송하여 거래를 체결하도록 하였다[6, 7, 8]. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistribution)를 실현하였다[2].

하지만 InterTrust사의 DRM 시스템의 복호화는 복호화가 끝난 후에 재생이 가능한 점, 1개의 키로만 암호화하기 때문에 키가 유출이 될 경우 더 이상 보호를 받지 못한다는 점, 파일 전체를 암호화하기 때문에 암호화/복호화 하는데 시간이 오래 걸리는 단점이 있다.

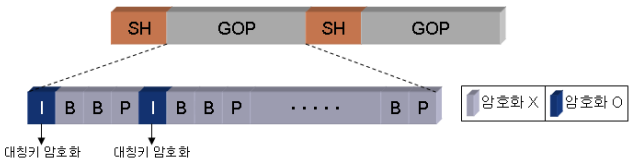
2.1.2 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 WMRM (Windows Media Rights Manager)으로서 저작물 제공자에게 인터넷상에서 암호화된 파일 형식으로 미디어를 배달한다. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(indivisualization)과정을 통해 키쌍을 할당받게 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다.

하지만 Microsoft사의 DRM 시스템의 경우는 자사의 WMV와 WMA의 파일 포맷만을 지원하기 때문에 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

2.2.3 I-Frame DRM 시스템

I-Frame DRM 시스템은 (그림 1)과 같이 동영상 GOP(Group Of Picture)의 I-Frame을 대칭키를 이용하여 AES 알고리즘이나 SEED 알고리즘 중에서 하나를 선택하여 암호화한 후 해당 콘텐츠의 ID(CID)와 대칭키의 값을 서버의 데이터베이스에 저장한다[1].



(그림 1) I-Frame DRM 시스템의 암호화 방법

I-Frame DRM 시스템은 전체 동영상의 복호화가 끝나기 전에 해당 파일을 재생할 수 있는 이중 버퍼 알고리즘을 사용한다. 이 I-Frame DRM 시스템은 I-Frame만을 암호화하기 때문에 부분 암호화 시스템에 속한다.

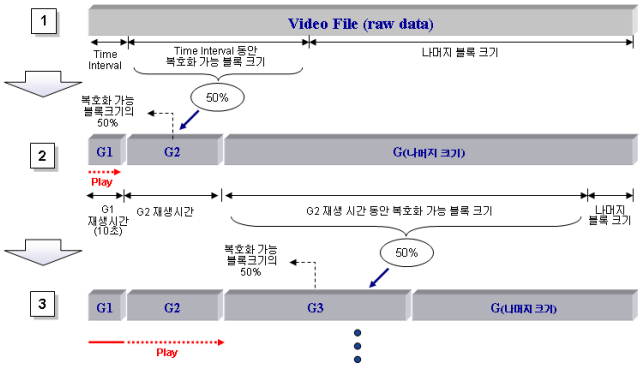
하지만 I-Frame을 추출하기 위하여 GOP(Group of Picture) 그룹의 모든 헤더의 내용을 읽은 다음 I-Frame의 크기를 계산하기 때문에 모든 GOP 헤더를 읽는데 시간이 많이 소비된다. 기존의 시스템과 같이 한 개의 키 만을 사용하며, 재생 시 처음 블록을 복호화 하는데 걸리는 재생 지연시간이 발생한다.

3. 제안하는 시스템

3.1 제안하는 DRM 시스템 암호화 방법

암호화를 시작하기 이전에 먼저 시작하는 작업은 슬라이스 레이어로 나누어 주는 작업이다. 이 슬라이스 레이어 작업은 서버에서 받은 해당 저작물에 대한 시간과 화면 사이즈를 획득한 후, Time Interval 값과 해당되는 동영상 파일의 크기를 먼저 계산한 후, 이 Time Interval 부분이 재생과 동시에 다음 블록이 복호화 되는 사이즈 크기의 50%~95% 양을 구하게 된다. 이러한 방법의 연속으로 다음 동영상이 재생되는 동안 다음 프레임은 복호화를 할 수 있다. 다음 (그림 2)는 총 4개로 분할된 동영상을 볼 수 있다.

슬라이스 레이어 작업을 거친 다음 암호화 작업으로 넘어간다. 암호화 조건은 연속적으로 암호화를 시키지 않는 블록은 없어야 하며, 전체 암호화된 블록은 50% 이상이어야 한다.

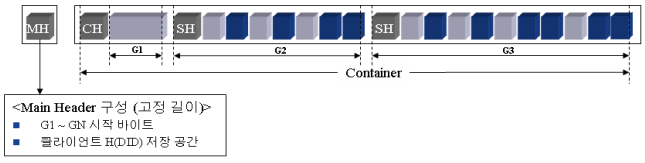


(그림 2) 제안하는 동영상의 슬라이스 레이어

G2 슬라이스 레이어 헤더에는 랜덤수(n), 즉 블록의 개수와 암호화 시킬 블록(0101011), 세분화된 블록 시작 바이트(S_b)를 담고 있으며, 슬라이스 헤더(SH)는 CID 값으로 다시 암호화 시켜 열어볼 수 없도록 만들어 둔다. 다음 슬라이스 레이어에서 나누어 놓은 부분 슬라이스 레이어 중 1로 매핑된 블록을 암호화 하는데, 암호화 키는 (식 1)과 같이 생성한다.

$$KEY = H(CID \| S_b \| n \| EB) \qquad \text{(식 1)}$$

암호화 과정이 끝나면 슬라이스 레이어의 모든 블록을 하나로 합치는 과정을 거치게 된다.



(그림 3) 제안하는 시스템의 암호화 파일 구성

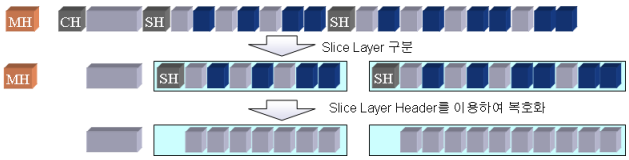
LAU에는 라이선스를 획득할 수 있는 URL이 들어가 있으며, 암호화된 컨텐츠를 재생시킬 때 해당 컨텐츠의 2차 ID의 값으로 해당 LAU로 가서 라이선스가 있는지 확인을 하고, 만약 라이선스가 없다면 라이선스를 받을 수 있는 웹페이지 URL로 이동하기 위하여 넣어둔 값이며, 컨테이너 헤더는 암호화를 시키지 않는다. 클라이언트에서 LAU를 통하여 라이선스를 획득한 다음 동영상을 복호화 하기 위해서는 각각의 슬라이어 레이어가 몇 바이트인지 알아야 하므로, 메인 헤더(MH)를 따로 구성을 해야 하

는데, (그림 3)와 같이 메인 헤더(MH)는 클라이언트의 DID를 해쉬한 값을 저장할 공간과 각각의 $G_1 \sim G_n$의 시작 바이트를 기록해 놓은 파일이다.

3.4 제안하는 DRM 복호화 방법

동영상 컨테이너를 다운로드 받은 클라이언트에서 컨테이너를 실행시키면 CH에 있는 LAU를 통하여 라이선스를 확인한 후에 클라이언트의 DID의 해쉬 값을 보내주면, 서버의 에이전트에서 해당 DID 해쉬 값을 해당 컨테이너의 MH에 포함하여 사용자의 공개키로 암호화 하여 클라이언트로 전송해 준다. 클라이언트 에이전트는 사용자의 인증서로 컨텐츠의 메인 헤더파일 복호화 작업을 수행한다. MH를 복호화 한 후, CID 값을 얻기 위해서는 서버에서 SSL을 통해 클라이언트 세션 ID값과 컨텐츠 헤더 파일을 XOR한 값, 즉 Temp ID(임시 ID)값을 전송 해 주게 되며, 클라이언트에서는 Temp ID값을 다시 Session ID와 XOR 시켜 CID값을 추출하게 된다.

나머지 과정은 암호화 기법의 역순으로 진행이 된다(그림 4).



(그림 4) 제안하는 시스템의 복호화 과정

4. 실험 평가

4.1 기존 시스템과의 비교 분석

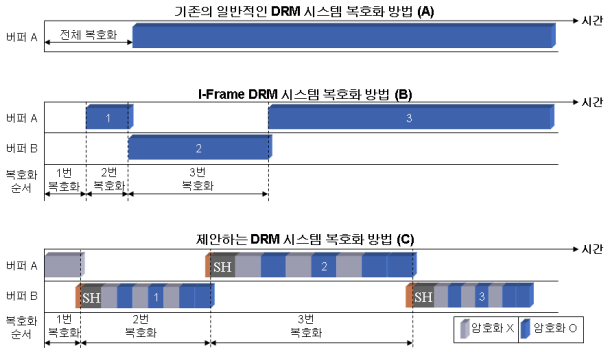
DRM시스템에서 가장 많은 시간을 소요하는 것은 저작물에 대한 암호화와 복호화 시간이므로 암호화 및 복호화 방식에 대한 시간과 시스템 사양별로 인한 재생시간을 분석한다.

암호화에 대한 비교분석은 [표 1]과 같이 암호화 기법과 키의 노출 가능성, 동영상 자체의 암호화 방식과 적용파일에 대하여 비교해볼 수 있다. 암호화 방법은 대칭키 암호화 방식을 사용한다.

[표 1] 기존 DRM 시스템과의 암호화에 대한 분석

비교 항목	기존의 DRM 시스템	제안하는 개선된 DRM 시스템
암호화 기법	한 개의 대칭키	복수개의 대칭키
키의 노출 가능성	높음	낮음
동영상 자체 암호화 방식	파일의 전체나 일부분	파일의 일부분

기존의 DRM 시스템의 기법과 제안하는 DRM 시스템 기법의 차이는 (그림 5)와 같다.



(그림 5) 기존 시스템과 제안하는 시스템의 복호화 기법

사용자가 동영상을 실행하면 에이전트는 해당 저작물에 대한 라이선스의 유효성을 서버에 접속하여 검증하여 정당한 사용자인 경우 복호화를 수행하여 해당 저작물을 재생한다. 복호화 과정을 수행을 하기 때문에 (A), (B), (C) 3개의 방법이 모두 동일하다.

그러나 기존의 일반적인 DRM 시스템 복호화 방법(A)은 전체 동영상에 대한 복호화가 끝난 후에 재생을 수행하므로 사용자는 복호화가 끝날 때 까지 긴 시간을 기다려야 하므로 대용량 동영상 파일인 경우 복호화에 많은 시간이 소요되므로 실시간적인 서비스를 제공할 수 없다. I-Frame DRM 시스템 복호화 방법(B)의 경우 이중 버퍼 알고리즘을 사용하였지만 동영상의 모든 프레임이 암호화 되어 있기 때문에 바로 시작하지 못한다는 단점이 있다.

제안하는 DRM 시스템 복호화 방법(C)에서는 재생시 지연시간이 없도록 개선하여 실시간적인 서비스를 가능하게 하였다.

4.2 성능 비교

본 논문에서 실험 평가를 하기위해 사용한 비교 DRM 시스템은 Microsoft사의 DRM 시스템과 I-Frame DRM 시스템을 가지고 비교 분석하였다. 실험 데이터 샘플은 18개의 서로 다른 파일크기를 가지고 있는 동영상 데이터를 사용하였고, Microsoft사의 DRM 시스템의 경우는 Version 1 Key ID를 사용을 하였으며, I-Frame 암호화 DRM 시스템의 경우는 AES 암호화 방법을 128비트에서 256비트로 수정하여 평가를 수행하였다. 본 논문에서 사용한

MD5 해쉬 알고리즘은 128비트이다.

암호화에 대한 시간을 비교 분석한 결과는 제안한 시스템이 [표 2]과 같이 I-Frame DRM 시스템 보다 약 1.56배 향상되었다.

[표 2] 기존 시스템과의 암호화에 대한 시간

파일크기(MB)	동영상 재생 시간 (Sec)	I-Frame 갯수	Microsoft DRM 암호화 시간 (Sec)	I-Frame DRM 암호화 시간 (Sec)	제안하는 시스템 암호화 시간 (Sec)
4.2	20	610	99.269	1.416	0.937
12.2	60	1,821	249.413	4.961	3.109
120.5	600	18,001	2122.847	47.957	30.906
717.078	5,505	139,129	9468.497	204.670	131.657

복호화에 대한 시간을 비교 분석한 결과는 [표 3]와 같이 기존의 I-Frame DRM 시스템 보다 약 1.61배 향상되었다.

[표 3] 기존 시스템과의 복호화에 대한 시간

파일크기(MB)	동영상 재생 시간 (Sec)	I-Frame 갯수	Microsoft DRM 복호화 시간 (Sec)	I-Frame DRM 복호화 시간 (Sec)	제안하는 시스템 복호화 시간 (Sec)
4.2	20	610	2.084	1.764	0.969
12.2	60	1,821	3.831	3.505	2.234
120.5	600	18,001	35.794	32.651	20.791
717.078	5,505	139,129	211.279	194.043	129.482

기존의 시스템과 제안하는 시스템과의 전반적인 사항을 비교 분석 해 보면 제안하는 시스템은 기존의 시스템과 같이 모든 동영상 파일을 지원하며 동영상 전체에 대한 암호화를 수행하지 않기 때문에 암호화 및 복호화에 대한 속도가 기존의 시스템보다 더 향상되었다.

5. 결 론

본 논문에서는 다중 랜덤 대칭키를 이용한 멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 대하여 제안하였다.

제안한 시스템은 불법적인 사용자에 의한 비밀키 유출을 막기 위하여 다수의 비밀키를 사용하여 부분적으로 암호화하는 방법을 사용하여 다른 기존의 시스템보다 암호화 및 복호화 속도를 개선하였으며, 원활한 동영상의 재생을 위해 보상 버퍼제어 방식을 제안하여 효율적인 버퍼 스케줄링을 수행하여 사용자에게 실시간 복호화 및 재생을 할 수 있도록 하였다. 시뮬레이션을 통해 클라이언트에서 대용량의 동영상 데이터 파일 재생 시 복호화 시간을 포함한 재생 지연시간을 기존 시스템에 비해 평균 약 15%이상 줄일 수 있는 것을 확인하였다.

향후 과제는 휴대폰 및 PDA와 같은 개인 이동식 휴대 단말기에서 활용할 수 있도록 시스템을 개선할 계획이다.

참고문헌

[1] 김정재 외 2명, “동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템,” 한국정보처리학회 논문지 C, VOL. 12-C NO. 02pp. 0183~0190 2005.04

[2] 정용훈 외 2명, “멀티미디어 데이터 보호를 위한 랜덤 대칭키 기반 부분 암호화 시스템,“ 한국정보과학회 한국컴퓨터종합학술대회 VOL. 00 NO. 00 pp. 0154~0156 2005. 07

[3] Brad Cox, Superdistribution : Objects As Property on the Electronic Frontier, Addision-Wesley, May 1996.

[4] Sung, J Park, "Copyrights Protection Techniques," Proceedings International Digital Content Conference, Seoul Korea, Nov. 28-29, 2000.

[5] V.K. Gupta, "Technological Measures of Protection," Proceedings of International Comference on WIPO, Seoul Korea, October 25-27, 2000.

[6] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography, " IEEE Transac tion on Information Theory, Vol.IT-22, No.6, pp.644-654, November 1976.

[7] Intertrust : http://www.intertrust.com/main/overview/drm.html

[8] Joshua Duhl and Susan Kevorkian, "Understanding DRM system: An IDC White paper," IDC, 2001.

[9] Joshua Duhl, "Digital Rights Management : A Definition," IDC 2001.

[10] Microsoft : http://www.microsoft.com/windows/windowsmedia/drm.asp