멀티미디어 데이터 보호를 위한 랜덤 대칭키 기반 부분 암호화 시스템

정용훈° 김정재 전문석
숭실대학교 대학원 컴퓨터학과
jyh0178@hotmail.com°, argniss@yahoo.co.kr, mjun@computing.ssu.ac.kr

A Random Symmetric key based Partial Encryption System for Multimedia Data Protection

Younghoon Jung° JungJae Kim MoonSeog Jun
Dept. of Computing in Soongsil Univ.

요 약

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 하지만 디지털 저작물은 품질에 대한 손상이 없이 복제가 가능하기 때문에 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다. 본 논문에서는 기존의 암호화 방법보다 다양한 키를 생성하는 알고리즘을 제안하며, 키 생성 알고리즘을 통해 각각 생성된 랜덤 대칭키를 서버에 저장하지 않는 기존의 시스템보다 보안성이 높은 암호화 방법을 제안한다.

1. 서 론

DRM은 저작권 보호기술을 이용하여 허가되지 않은 사용자로부터 디지털 저작물을 안전하게 보호함으로써 저작권자의 권리 및 이익을 지속적으로 보호하고 관리하는 기술이다[3]. DRM 기술을 통해 디지털 저작물에 대한 지적재산권 침해사례로부터 저작권을 보호하고, 유통과정을 관리하기 위한 종합적인 대책이 추진되어 저작물에 대한 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[6]. 하지만 기존의 DRM 시스템에서는 하나의 키로만 암호화하기 때문에 그 키가 유출되면 더이상 안전을 보장받지 못한다. 본 논문에서는 디지털 콘텐츠 사용자 인증에 있어서 사용자에 의한 비밀키의 노출을 막기 위하여 여러개의 비밀키를 서버의 시큐리티 모듈에 의해 부분적으로 암호화하는 기법을 제안하여 하나의 비밀키가 노출 되더라도 저작물 전체에 대한 복호화를 할 수 없는 방법을 제안하며, 실행시 사용자에게 지연시간이 없는 실시간 복호화 및 재생을 할 수 있도록 하는 통합적인 DRM 시스템을 제안한다.
본 논문의 구성으로, 2장에서는 기존의 DRM 시스템에 대해서 언급을 하고, 3장에서는 온라인에서 동영상 데이터에 적용 가능한 보안이 향상된 새로운 부분 암호화 DRM 시스템을 제안하며, 4장에서는 결론으로 기술한다.

2. 관련 연구

2.1 기존의 DRM 시스템

2.1.1 InterTrust의 DRM 시스템

InterTrust 사의 DRM 솔루션 특징은 저작물의 보호를 위해서 암호기술과 워터마킹을 사용하며 저작물 사용규칙을 지정하여 사용내역의 수집 및 기록, 과금 처리를 수행하는 것이다. 사용자 컴퓨터에 에이전트를 실행하여 라이선스와 과금 처리, 저작물의 실행을 에이전트를 통하여 처리하도록 하였다. 저작물은 사전에 암호화되어 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 라이선스 에이전트가 라이선스를 확인하고 지불정보를 전송하여 거래를 체결하도록 하였다. 그러므로 신용카드나 전자 화폐 등의 결제 방식을 이용하여 거래할 수 있다[1, 2, 4]. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistribution)를 실현하였다[3].

2.1.2 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단 간(end-to-end) DRM 시스템이다[5]. 핵심 제어 부분은 WMRM(Windows Media Rights Manager)으로서 WMRM의 Rights Manager는 저작물 제공자에게 인터넷 상에서 암호화된 파일 형식으로 보호된 음악, 비디오 등의 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. 인증서 취소목록은 마이크로소프트사의 웹사이트를 통해 배포된다. 키는 라이선스에 포함되고, 라이선스와 저작물은 분리되어

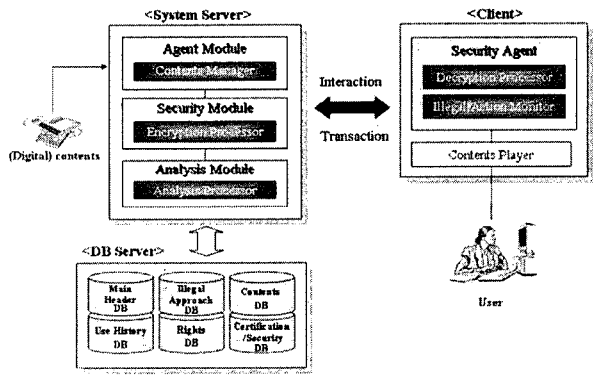
분배된다.

2.2 기존의 DRM 시스템 분석

두 제품 모두 저작물에 저작권 정보를 삽입하는 방식이므로 패키징 작업이 끝난 후에 는 보호 조건의 변경이 필요한 경우 변경할 수 없으므로 필요시 재 패키징을 해야 하는 문제점이 있으며, DRM 솔루션에 적용된 주요기술 역시 적법한 사용자가 플레이어를 통하여 평문을 획득했을 경우, 이를 무단으로 복사하여 배포하는 것을 막을 수가 없는 문제점이 있다. 즉 두 시스템 모두 사용자가 키를 노출했을 경우에는 심각한 보안 위협이 된다.

3. 제안하는 시스템

3.1 제안하는 DRM 시스템 구성도

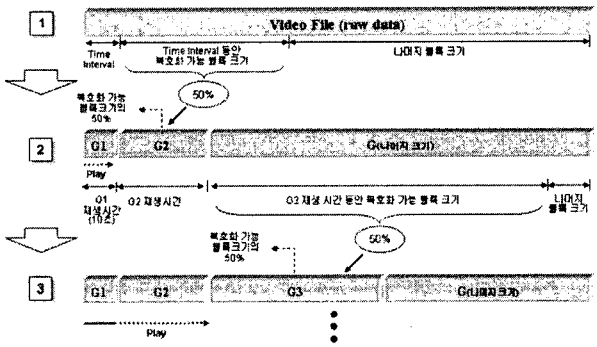


[그림 3-1] 제안하는 DRM 시스템 구성도

① 에이전트 모듈 : 클라이언트에서 넘어온 데이터와 컨텐츠를 등록하기 위해 일어나는 일련의 모든 처리과정을 각각의 모듈에게 분배하는 모듈
② 암호화 모듈 : 저작물을 각각의 다른 비밀키(RKs)를 사용하여 AES 알고리즘으로 암호화하고 해당 저작물과 키 유추에 관한 정보를 저작물 데이터베이스와 메인 헤더 데이터베이스에 저장하는 모듈
③ 분석 모듈 : 통계분석 처리기는 클라이언트에서 발생하는 모든 상황을 감시할 뿐만 아니라 서버에서 암호화 되는 모든 행위에 대한 내용을 각각의 데이터베이스에게 저장하는 역할을 담당하는 모듈
④ 시큐리티 에이전트 : 클라이언트에 위치하며, 동영상을 복호화 및 재생을 담당하며, 이에 필요한 모든 행위를 서버의 에이전트 모듈에 전송하는 기능

3.2 제안하는 DRM 시스템 암호화 방법

암호화를 시작할 때 가장 먼저 시작하는 작업은 슬라이스 레이어로 나주어 주는 작업이다. 이 슬라이스 레이어 작업은 서버에서 받은 해당 저작물에 대한 시간과 화면 사이즈를 획득한 후, 10초 즉 Time Interval 값에 해당되는 동영상 파일의 크기를 먼저 계산한 후, 이 타임 인터벌 부분이 재생됨과 동시에 다음 블록이 복호화 될 수 있는 사이즈 크기의 50% ~ 95% 양을 구하게 된다. 이 이유는 복호화만 시킬때 100%라고 가정을 하고, 이 과정은 이전 블록이 재생됨과 동시에 복호화를 해야 하기 때문에 비중을 CPU 사용율을 고려하여 최대 복호화 양의 일부분으로 정하게 된다. 이러한 방법으로 이 다음 동영상 데이터가 플레이 되는 동안, 해당 동영상 파일의 복호화 할 수 있는 동영상의 사이즈를 구하는 작업을 반복하게 된다. 이러한 방법으로 해당 동영상의 그룹을 n개로 나누어 저장을 하게 된다. 이 아래의 [그림 3-2]는 4개로 분할된 그룹을 볼 수가 있다.



[그림 3-2] 제안하는 동영상의 슬라이스 레이어

슬라이스 레이어 작업을 거친 다음 암호화 작업으로 넘어간다. 이 암호화 작업시 G1 그룹 즉 타임 인터벌에 해당되는 블록은 암호화를 하지 않고, 다음 G2 블록부터 암호화 작업을 시킨다. 이유는 동영상 플레이시 초기재생시간을 확보하기 위해서이며, 플레이시 바로 실행이 가능하다는 장점이 있다. 다음 G2의 슬라이스 레이어 블록부터 랜덤수 5 ~ 15까지 발행한 후, 해당 수만큼 그 동영상을 다시 나누게 된다. 만약 해당 랜덤수가 7이 나왔을 경우, 동일한 사이즈로 7등분으로 나누어 주며, 암호화 시킬 블록과 그렇지 않은 블록을 나누어 주어야 한다. 암호화 시킬 블록의 조건은 연속적으로 암호화를 시키지 않는 블록은 없어야 하며, 전체 암호화 블록은 50% 이상이어야 한다. [그림 3-3]에서 처럼 암호화 할 슬라이스 레이어 블록 부분을 1로 매핑을 시키고, 암호화 하지 않을 슬라이스 레이어 부분을 0으로 매핑 시켜 EB(Encoding Block : 예 0101011)을 구한다. G2 슬라이스 레이어 해더를 만들고 이 헤더에는 랜덤수, 즉 블록의 개수와 암호화 시킬 블록, 세분화된 블록 시작 바이트를 담고 있다. 이 헤더파일은 다시 CID(Content ID) 값으로 다시 암호화 시켜 열어볼 수 없도록 만들어 둔다. 마지막으로 슬라이스 레이어에서 나누어 놓은 부분 슬라이스 레이어를 각각 암호화 시키기 위해 각각의 키를 생성시켜야 한다. 해당 키는 (수식 3.1)과 같이 생성한다.

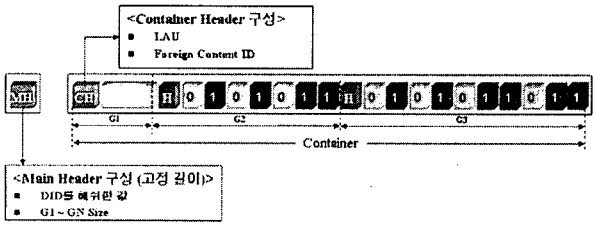
$$KEY = H(CID \| S_b \| n \| EB) \qquad \text{(수식 3.1)}$$

이 n개의 그룹 파일에 헤더를 각각 붙인 후, 각각의 그

룹이 시작되는 바이트의 위치를 전체의 동영상 헤더파일로 기록해 둔다. 위에서 발행한 해당 난수의 크기로 나누어진 파일에 대한 정보 즉 슬라이스 레이어의 헤더에 각각의 해당 블록의 Byte 사이즈와 암호화 블록의 코드, 암호화 되어 있는 EB를 기록한다. [그림 3-3]에서 처럼 헤더의 정보와 CID로 해쉬한 값을 부분 슬라이스 레이어의 1에 해당되는 부분만을 (수식 3.1)의 키값으로 대칭키 암호화방법으로 암호화를 시킨다. 여기서 해쉬 함수는 128Bit MD5를 사용하고, 암호화는 Rinjdael 암호화 방법을 사용한다.

[그림 3-3] 암호화 한 슬라이스 레이어

이와 같은 방법으로 각 슬라이스 레이어의 난수로 발생된 블록을 모두 암호화 하는 방법으로 모든 슬라이스 레이어를 암호화 한 다음, [그림 3-4]의 슬라이스 레이어의 모든 블록을 하나로 합치는 과정을 거치게 된다.

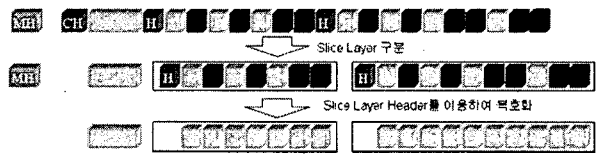


[그림 3-4] 제안하는 시스템의 암호화 파일 구성

하나로 합쳐진 블록에 CH(Container 헤더)를 구성하게 되는데 이 CH는 LAU(License Acquisition URL)와 컨텐츠의 2차 ID(Foreign Content ID)로 구성이 되어 있으며 이 컨테이너는 웹사이트를 통해서 사용자가 받아갈 수가 있다. 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 첫 페이지를 띄워 주기 위해서 넣어둔 값이며, 컨테이너 헤더는 암호화를 시키지 않는다. MH(Main 헤더)는 G1~Gn의 사이즈를 기록한 값과 클라이언트의 DID(Device ID)를 저장한 상태이며, 각각의 사용자가 동영상 실행시 이 파일을 전송시킬때 사용자의 공개키로 암호화 시켜서 보내주게 된다.

3.3 제안하는 DRM 시스템 복호화 방법

복호화 작업을 시작하기 전에 CID 값을 얻기 위해서는 SSL을 통해 얻어진 세션 아이디 값과 컨텐츠 헤더 파일을 XOR한 값, 즉 Temp ID(임시 ID)값을 전송받게 되며, 클라이언트에서 다시 Temp ID값을 Session ID와 XOR 시켜 컨텐츠의 CID값을 추출하고, 각 헤더에 있는 값을 읽어들여 복호화하게 된다.



[그림 3-5] 제안하는 시스템의 복호화 과정

이때 사용자의 개인키로 복호화된 MH를 통해서 클라이언트의 DID값과 비교를 한 후, DID값이 맞지 않는다면 복호화 작업을 중단하고, 새로운 MH를 부여 받도록 한다. 다음 컨텐츠를 실행시 각각의 슬라이스 레이어로 구분을 나눈 후, CID로 슬라이스 레이어의 헤더파일을 복호화 한 후, 이 헤더를 이용하여 각각의 슬라이스 조각 레이어의 키를 생성하여 암호화된 블록을 복호화 시킨다.

4. 결 론

본 논문에서는 시큐리티 에이전트를 이용한 멀티미디어 데이터 보호를 위한 랜덤 대칭키 기반 부분 암호화 시스템에 대하여 제안하였다. 디지털 콘텐츠 사용자 인증에 있어서 사용자에 의한 비밀키의 노출을 막기 위하여 여러개의 비밀키를 암호화 모듈에 의해 부분적으로 암호화하는 기법을 제안하여 하나의 비밀키가 노출 되더라도 저작물 전체에 대한 복호화를 할 수 없는 방법을 제안 하였으며, 암호화 속도 역시 파일 전체가 아닌 부분적이기 때문에 다른 기존의 시스템보다 향상 된 새로운 기법을 제안하였다. 또한 복호화 과정에서 클라이언트의 시큐리티 에이전트는 동영상 실행 시 복호화와 실시간 실행을 위하여 Time Interval 값을 주어 가능토록 하였다.

5. 참고 문헌

[1] Joshua Duhl and Susan Kevorkian, "Unde rstanding DRM system: An IDC White paper," IDC, 2001.

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

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

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

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

[6] 이용호 : 이용효, 황대준, "에이전트 기반의 동적 디지털 저작권관리 시스템 설계 및 구현," 한국정보처리학회 논문지 D, 제8-D권, 제5호, pp.613-622, 2001.