멀티미디어 콘텐츠 보호를 위한 해쉬체인 기반의 DRM 시스템 설계

이영구° 박찬길* 김정재* 이경석** 전문석***
숭실대학교 일반대학원, 산업연구원**
{ad3927°, ckpark*, argniss*}@ssu.ac.kr, kslee@kiet.re.kr**, mjun@computing.ssu.ac.kr***

Design of DRM System Based on Hash-Chain for Multimedia Contents Protection

Young-Gu Lee°, Chan-Kil Park*, Jung-Jae Kim*, Kyung-Seok Lee**, Moon-Seog Jun***
SoongSil University, Information Management Div. KIET

요 약

컴퓨터통신기술과 정보처리기술의 발전으로 멀티미디어 콘텐츠의 활성화를 촉진하였다. 정보화시대 국가경쟁 사업으로 정부차원에서도 문화 콘텐츠 개발을 국제적 경쟁력을 가진 고품질의 문화콘텐츠를 제작 공급할 수 있는 핵심 성장기반을 조성하기 위하여 국가사업으로 확대하고 있다.

본 논문에서는 멀티미디어 콘텐츠 보호를 위하여 해쉬체인 알고리즘을 이용한 멀티미디어 데이터의 암호화 기법을 제안하였으며, 인가된 사용자 확인을 위하여 사용자인증 및 키 전송 알고리즘을 이용하여 사용자인증 및 키전송 프로토콜을 설계하였으며, 복호화시 재생 지연시간을 줄이기 위하여 이중버퍼를 구성 효율적인 버퍼 스케줄을 이용하여 멀티미디어 콘텐츠의 실시간 복호화 방법을 제안한다.

1. 서 론

컴퓨터기술의 발전과 통신기술의 발전은 정보화 사회를 가속화 시켰으며 컴퓨터 간 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화하면서 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 디지털 저작물은 품질에 대한 손상이 없이 복제가 가능하기 때문에 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다. 디지털 저작물 보호를 위해서는 안정성과 보안성 확보를 위하여 정보보호 기술이 요구되고, 디지털 저작권과 저작물 유통의 전반을 감시하고 추적하기 위한 디지털 저작권 관리(DRM : Digital Rights Management) 기술이 필요하게 되었다.

DRM 시스템에서의 사용자 인증 방식으로 제공되는 인증기법은 사용자가 데이터를 불법 복제하여 유통할 수 있기 때문에 유통되는 데이터를 완전히 보호할 수 없는 단점이 존재한다. 이에 반하여 데이터 자체에 대한 보호는 저작물 자체에 암호화를 수행하여 저작물에 대한 사용자의 접근을 제한하는 방식이다.

본 논문에서는 디지털 콘텐츠 사용자 인증에 있어서 사용자에 의한 비밀키의 노출을 막기 위하여 사용자 인증번호를 무선으로 제공하고 제공된 인증번호를 입력하여 유선으로 비밀키를 제공받는 방법을 제안하였으며, 저작물을 해쉬체인 알고리즘을 이용하여 암호화하는 방법을 제안함으로써 멀티미디어 콘텐츠의 안전하게 제공할 수 있는 방법을 연구하였다.

2. 관련연구

2.1 기존의 DRM 시스템

디지털 저작물의 유통을 위해서는 상용화된 전자상거래 시스템들과 상호 연결을 통해서 저작물 유통과 결재가 가능하도록 표준화된 분류 체계와 식별체계가 갖추어져야한다. 저작권 보호와 관리를 위해서는 저작물에 대하여 온라인 환경과 오프라인 환경에서 저작권 이용에 대한 위법 여부를 판단할 수 있도록 저작권 사용 내역을 자동으로 감시하고 추적할 수 있는 기능과 저작권 사용에 대한 자동 통계 기능 및 분석 기능이 제공되어야 하며 원 저작물의 데이터 보호와 인증을 위해 기존의 저작물에 대한 단순한 사용권한 제한이나 패스워드 인증 방식이 아닌 공개키 기법을 이용한 사용자 인증과 데이터 암호화를 이용하여 동영상 데이터를 보호해야 한다[1].

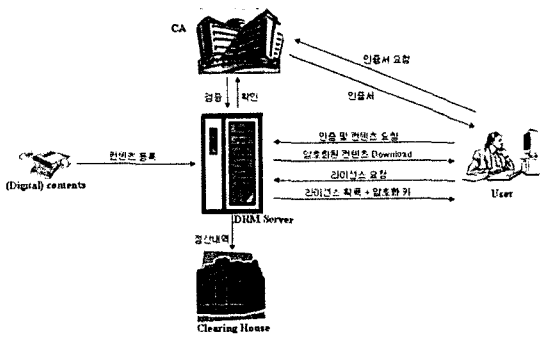

그림 1 DRM 시스템 구성도

DRM 시스템은 <그림 1>과 같이 인증기관과 저작물 공급업자, 사용자, 그리고 클리어링하우스(Clearing house)로 구성된다. 저작물이 작가에 의하여 창작되어 출판업자에게 넘겨지면 출판업자는 저작물에 대한 가격, 유통기한, 사용조건 등을 명시하여 분배업자에게 전송한다. 분배업자는 저작물을 암호화하여 사용자에게 분배하면 사용자는 저작물에 대하여 사용 금액을 지불한 후 라이선스를 발급받아 사용할 수 있다.

2.2 기존 DRM 시스템 분석

멀티미디어 데이터를 암호화하는 방법에는 크게 공개키 암호화 알고리즘을 사용하는 기법과 대칭키 암호화 알고리즘을 이용하는 방법으로 크게 나눌 수 있다. 공개키 암호화를 사용하면 암호화시 사용자마다 대용량 데이터를 암호화함으로서 실시간 다운로드가 불가능해 지며, 서버의 오버헤드 발생으로 시스템에 많은 부하가 발생하며 복호화시 클라이언트에서 많은 계산량으로 속도 저하 및 부하가 가중된다. 반면에 대칭키 알고리즘을 사용하면 단일 대칭키를 사용하므로 키 노출시 보안 취약하다. 또한 영상데이터에서 I-Frame 만을 암호화 하기위한 I-Frame 추출 알고리즘 사용해야 하며 다양한 멀티미디어 포맷을 지원하지 못하는 문제점이 있다.[2]

디지털 저작권 관리에 요구되는 식별, 저작권 정보, 저작물 이용 감시 및 저작권 이용 현황 등을 통합된 프로세스로 관리하기 위한 시스템을 <그림 2>와 같이 단계별로 구성하고 있다.

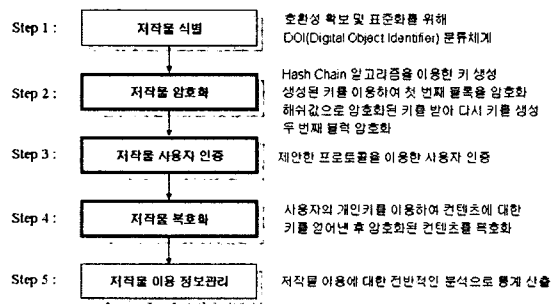

그림 2 저작물 처리 단계

3. 제안하는 멀티미디어 데이터 암호화 기법

3.1 멀티미디어 데이터 분할 (Block Slice) 기법

멀티미디어데이터를 암호화하기 전에 RAW Data를 블록으로 나누어 각각의 블록을 암호화 할 수 있도록 전처리 작업을 수행한다. 전처리작업 수행시 첫 번째 암호화 블록은 원 데이터가 시작되기 전에 지연시간(TI:Time Interval) 만큼을 첫 번째 블록크기로 정하고 두 번째 블록의 크기는 이전 블록크기의 100~200% 내에서 블록으로 나누어 처리한다.

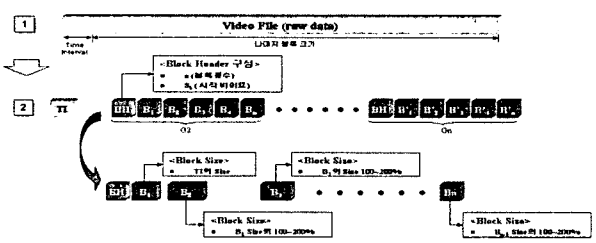

그림 3 멀티미디어 데이터 블록 분할 처리

몇 개의 블록을 묶어 하나의 그룹으로 나타내고, 하나의 그룹은 첫 번째 블록의 1500% 내에서 하나의 그룹으로 묶는다. 두 번째 그룹에서 마지막 그룹까지 같은 방법으로 그룹화 한다. 블록을 몇 개의 그룹으로 그룹화하는 것은 암호화 또는 복호화시 보상이중버퍼를 이용하여 암/복호화시 처리속도를 향상시켜 DRM 시스템의 효율성을 제공할 수 있기 위해서이다.

이전 블록 사이즈가 100~200%인 이유는 블록 사이즈의 비율이 50%로 계속 나온다면 최악의 경우 1500%까지 도달을 못하며, 200% 이상이 되면 최악의 경우 해당그룹의 블록 개수가 3개밖에 나오질 않기 때문에 100~200%의 수치를 정하였다. 또한 그룹의 크기는 초기 블록사이즈의 1500%가 나온 이유는 재생시 복호화할 수 있는 사이즈가 1522%라는 시뮬레이션 수치가 나왔으며 1522% 이상이 된다면, 해당블록이 다 재생이 된 후에도 아직 복호화를 하기 때문에 그룹과 그룹이 바뀌어 재생이 될 때 지연시간이 발생하게 된다.

3.2 Hash Chain 기법을 이용한 암호화 Key 생성

분할된 블록을 암호화 하기위하여 <그림 4>와 같이 서로 다른 두개의 해쉬함수를 사용하여 사용자 인증번호로 첫 번째 해쉬함수 $H_1()$에서 키를 생성하고, 생성된 키를 이용하여 첫 번째 블록을 암호화한다. 첫 번째 생성된 키를 받아서 두 번째 해쉬함수(H2)로 두 번째 키를 생성하며, 생성된 두 번째 키를 이용하여 두 번째 블록을 암호화 한다. H2에서 생성한 키를 다시 H1함수로 보내어 세 번째 키를 생성하고 생성된 키를 이용하여 세 번째 블록을 암호화한다. 반복하여 모든 블록이 암호화 될 때까지 반복하여 이중해쉬 함수를 이용하여 키를 생성하고 암호화를 진행한다. 두개의 해쉬함수를 이용하여 멀티미디어 데이터를 암호화함으로써 암호화의 안전성을 높일 수 있으며 하나의 키가 유출되어도 해쉬함수 알고리즘을 알 수 없으므로 다른 블록들을 복호화 할 수 없도록 하였다.

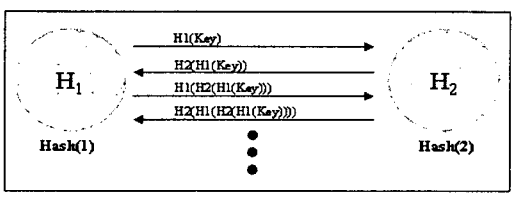

그림 4 이중 해쉬 프로토콜

본 논문에서는 분할 알고리즘을 이용 데이터를 해쉬 알고리즘을 이용하여 키를 생성하고 생성된 키를 이용하여 각각의 블록을 암호화 한다. 암호화시 그룹 내의 블록의 위치주소 및 크기정보를 가지는 BH(Block Header)와 전체그룹을 제어하는 정보는 LAU(License Acquisition URL)와 Content ID로 이루어진 CH(Container Header)로 구성되어 있으며, MH(Main Header)는 그룹의 크기와 DID를 해쉬한 값을 가지고 있다.

3.3 사용자 인증 및 키 전송 기법

정보유출 및 사용자 확인을 위하여 서버는 무선으로

사용자 인증번호를 제공하고 사용자는 인증번호를 키값으로 입력하여 복호화 키를 요청하게 한다. 사용자 인증값을 확인한 에이전트는 OTP(One Time Password)로 복호화키를 생성한다. 생성된 키는 키 분할 알고리즘을 이용하여 키를 K_a, K_b로 분할 한 후 에이전트를 이용하여 키 a를 세션증가 값과 사용자 인증값으로 해쉬한후 사용자에게 전송하고, 전송받은 사용자는 사용자 인증번호와 키a를 랜덤 값으로 해쉬한 후 서버로 보내면 K_a를 받은 것으로 인식하여 다시 분할 키 b를 사용자 인증번호와 랜덤 값과 해쉬하여 사용자에게 전송하는 절차를 거쳐 키 값을 전송한다.

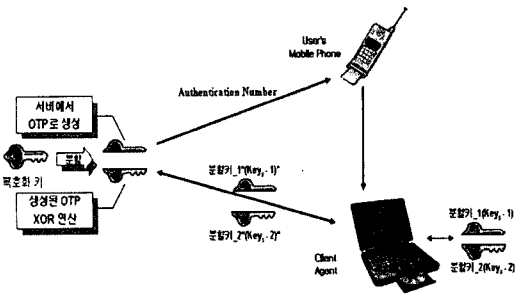

그림 5 키 전송 기법

3.4 멀티미디어 데이터 복호화 기법

동영상 복호화 과정은 Container의 Content ID와 동일한 라이선스 유/무 확인한다. 라이선스가 없을 때는 Container Header의 LAU로 이동하여 라이선스 취득하고 사용자의 DID (CPU Serial Number) 의 해쉬값으로 저장한다.

라이선스 획득시에는 사용자 인증 과정과 복호화에 필요한 암호키 수신한다. Content ID로 해당 동영상 MH 요청하고 MH에 사용자의 해쉬한 DID값과 MH를 사용자 공개키로 전송한다. 개인키로 메인헤더 복호화 후 자신의 컴퓨터와 MH에 포함된 해쉬값과 같은지 확인 후 재생한다.

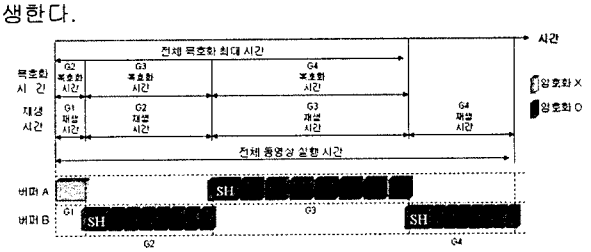

그림 6 동영상 실행을 위한 보상 이중버퍼 시스템

MH는 사용자의 공개키를 사용하여 전송하며 사용자의 개인키로 MH를 복호화한다. BH의 위치 획득 후 사용자 인증 기법을 통해 키를 획득하며 BH의 내용을 Key로 Gk(B1 ~ Bn)* 의 내용을 복호화한다. 복호화시 보상 이중 버퍼 알고리즘을 사용하여 재생하며 버퍼에는 전체 동영상이 재생되는 동안 지연되는 프레임을 계산하여 초기에 버퍼 사이즈를 결정한 후 재생 하도록 한다. 이를 위해서 <그림 6>과 같이 2개의 버퍼를 사용하는 보상 이중버퍼 시스템을 사용한다.

복호화를 위하여 초기에는 G1(타임 인터벌 값) 10초 분량의 프레임을 먼저 재생하기 위해 버퍼 A에 저장하여 실행한다. 그리고 동영상이 실행되는 10초 동안에 슬라이스 레이어 G2 분량의 데이터를 복호화하여 버퍼 B에 저장한다. 버퍼 A에서 실행이 끝나면 에이전트는 버퍼 B의 데이터가 이어서 실행될 수 있도록 버퍼 B의 메모리 참조 값을 저장한다. 실질적으로 버퍼 A에서 버퍼 B로 바뀔 때 화면의 끈김현상이 발생하는데 이는 해당 G2의 프레임이 완전치 않은 프레임이기 때문이다. 이를 방지하기 위해서 G1의 마지막 프레임의 값을 버퍼 B에 붙여서 완전한 프레임으로 바꿔주기 위한 작업이 필요하다. 따라서 전체적으로 화면이 끊기는 현상이 발생하지 않으면서 동영상을 실행할 수 있다.

4. 결론

제안된 해쉬체인 기반의 DRM 시스템에서는 멀티미디어 콘텐츠 암호화의 안전성 향상을 위하여 이중 해쉬체인 기법을 제안하였다. 암호화는 공개키 기법을 이용하여 MH로 전송하여 해당 저작물을 파일로 독립 관리하였으며, 서버에는 컨텐츠에 대한 각각의 키가 저장되고 시큐리티 에이전트가 연산과정을 통해 n개의 대칭키를 생성하여 각각의 키를 이용하여 블록단위로 암호화 하였다. 사용자 인증시 사용자 인증 프로토콜을 사용하여 키 획득 및 사용자 인증하도록 하였으며, 이전의 세션ID 값과 현재 세션 ID값을 가지고 연산하기 때문에 외부 공격에 강하며 유/무선을 같이 사용하여 인증하므로 보다 안전하게 키전송을 할 수 있게 하였다. 한번 계산한 블록키는 키 관리 에이전트를 두어 재계산 필요 없이 사용자 인증만 받은 후 사용할 수 있도록 연구하였다.

참고문헌

[1] 박재표, 이광형, 김정재, 전문석, "라이센스 에이전트를 이용한 디지털 저작권 보호 및 감시 시스템의 설계," 한국산업정보보안학회 논문지, 제4권, 제1호, pp.15-24, 2004.

[2] 김정재, 박재표, 전문석, "멀티미디어 데이터 보호를 위한 공유 키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지, 제12-C권, 제2호, 2005.

[3] Russ Housley and Tim Polk, "Planning for PKI," John Wiley & Sons, 2002.

[4] Barbara L. Fox Brian A. LaMacchia, "Encouraging Recognition of Fair uses in DRM Systems," Communications of The ACM, VOL. 46 NO. 04 pp. 61 ~ 63 2003. 04

[5] John S. Erickson, "Fair use, DRM, and trusted computing," Communications of the ACM, VOL.46 NO.04 pp. 34 ~ 39 2003. 04

[6] Gildas Avoine and Philippe Oechslin, "RFID Traceability: A Multilayer Problem," EPFL Lausanne, Switzerland, 2005