

디지털 저작권 보호를 위한 라이선스 에이전트의 설계

이광형, 이근왕, 김희숙*

청운대학교, 아산정보기능대학*

요 약

디지털 저작물의 전송환경이 빠른 속도로 바뀔에 따라서 디지털 저작물의 저작권 보호가 중요한 이슈로 부각되고 있다. DRM(Digital Right Management)은 디지털 저작자나 출판업자, 그리고 인터넷 서비스 제공자들에게 디지털 저작물을 접근하고 사용하는데 있어서 신뢰할수 있는 환경을 만들 수 있는 관심있는 분야이다. 본 논문에서는 라이선스 에이전트를 이용하여 기존의 DRM 기법이 가지고 있는 정적인 DRM이나 온라인환경에 제한된 어플리케이션의 단점을 개선한 디지털 저작물의 보호 기법에 대하여 제안한다. 제안된 논문은 동적인 DRM기법으로 동적인 요구 제어 기술을 바탕으로 라이선스 에이전트를 이용하여 온라인과 오프라인 환경에서 동시에 모니터링과 추적을 수행한다. 제안된 시스템은 PKI 보안 환경에서 사용자의 행동이나 데이터 보안을 실시간으로 감시하여 불법적인 접근과 사용을 막는다.

The Design of License Agent Rights Protection

Kwang-Hyoung Lee, Keun-Wang Lee, Hee-Sook Kim*

Chungwoon University, Asan Information Polytechnic College*

ABSTRACT

As the logistic environment of digital contents is rapidly changing, the protection of the digital rights for digital content has been recognized as one of critical issues. Digital Right Management(DRM) has taken much interest Internet Service Provider(ISP), authors and publishers of digital content as an interested approach to create a trusted environment for access and use of digital resources. This paper propose an interested digital rights protection scheme using license agent to address problems facing contemporary DRM approached : static digital rights management, and limited application to on-line environment. We introduce a dynamic mission control technology to realize dynamic digital rights management. And we incorporate license agent to on- and off-line monitoring and tracking. The proposed system prevent illegal access and use by using PKI security method, real time action monitoring for user, data security for itself.

1. 서 론

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 디지털자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 이러한 디지털 콘텐츠는 품질의 손상 없이 복제가 가능하기 때문에 이의 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다. 콘텐츠 보호와 관리를 위해서는 안정성, 보안성 확보를 위한 정보보호 기술과 저작권을 관리하고 콘텐츠 유통 전반을 감시, 추적하는 디지털 저작권 관리(DRM: Digital Right Management) 기술이 필요하다(James et al., 1998; Jai, 1997). DRM은 저작권 보호기술을 이용하여 허가되지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호함으로써 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 관리 기술로 정의할 수 있다(Dubl, 2001).

기존의 DRM은 사용자의 프라이버시 보호가 저작권 보호에 직접적으로 필요하지 않다는 이유로 사용자의 프라이버시 보호에 대해서는 고려하지 않았다. 이러한 영향으로 라이선스 발급시의 사용자 인증과 콘텐츠의 불법 사용 감시를 위한 사용내역 보고 과정에서 사용자 정보가 유출되는 문제점이 발생하였고, 이로 인해 사용자 프라이버시 침해 문제가 발생하게 되었다(Vora et al, 2001).

본 논문에서는 라이선스 에이전트를 이용하여 온라인과 오프라인 상에서 멀티미디어 콘텐츠에 대한 사용자 인증과 원 데이터 자체의 암호화를 통해 불법적인 실행, 복사, 이동을 방지할 수 있는 통합적인 DRM 시

스템을 설계하고자 한다.

2. 관련연구

2.1 정보 보호 기술

암호화는 전자서명 및 정보보호를 위한 기본적인 기술이라고 할 수 있다. 암호화란 어떤 자료나 정보에 대하여 타인이 식별할 수 없도록 기술적 조치를 취하여 암호문으로 바꾼 것으로, 데이터를 암호화하는 방식은 대칭 암호화방식과 비대칭 암호화 방식의 두 가지 기본적인 형태가 있다(Diffie et al., 1996).

암호화 방식의 경우 일단 암호화된 데이터의 평문을 얻은 이용자는 원래의 소유권자와 동일한 능력을 갖게 되어 데이터의 저작권과 소유권을 알 수 없기 때문에 이를 무단으로 복사하여 배포하는 것을 막을 수가 없다. 따라서, 암호화를 이용한 방법은 정보보호를 위한 주요 수단이지는 하나 디지털 저작물에 대한 저작권 침해를 방지하기 위한 감시 및 추적 기능의 제공 등 근본적인 해결책의 제공에 한계가 있다(한효영 외, 2000).

2.2 디지털 저작권 관리 기술

DRM은 디지털저작물을 저작한 저작자로부터 유통업체 및 소비자들에게 법적인 문제없이 안전하고 신뢰할 수 있는 조건하에 유통될 수 있도록 해주는 일관된 관리체계이다. DRM 시스템은 여러 단계의 발전과정을 거쳐 다음과 같은 기술적인 문제점들을 해결해 왔다.

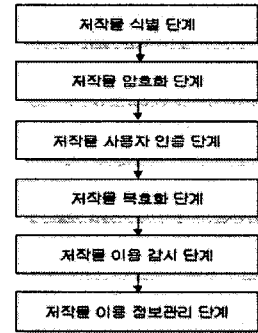
- (1) 콘텐츠에 대한 무결성과 신뢰성의 확보
- (2) 저작권에 대한 기술 (Rights Specification)
- (3) 저작권 획득 방법
- (4) 저작권 사용 추적
- (5) 저작권 취득, 기술 및 허용(granting)

이 가운데 콘텐츠의 무결성과 신뢰성 확보를 위하여 암호화 기술을 중심으로 발전하여 왔으며 저작권에 대한 내용을 명시하기 위하여 XrML 기반으로 표준화가 진전되고 있으며 식별자 부여를 위하여 DOI를 적극 활용해 나가는 추세이다. 그리고 DRM은 전자상거래시스템과 결합해서 다양한 형태의 조건에 따른 디지털콘텐츠의 유통을 일체화된 방식으로 제공할 수 있는 다양한 솔루션들이 등장하고 있다(황대준 외, 2001).

3. LA를 이용한 DRM 시스템 설계

3.1 시스템 모형

제안하는 시스템에 대한 시스템 모형은 다음과 같다. 디지털 저작물에 대한 저작권 보호와 저작물의 유통에 따른 저작권을 체계적으로 관리하기 위해서는 하나의 종합적인 시스템으로 설계되고 구현되어야 한다. 디지털 저작권 관리에 요구되는 식별, 저작권 정보, 저작물 이용 감시 및 저작권 이용 현황 등을 일련의 통합된 프로세스로 관리하기 위한 시스템 구성을 가져야 한다. 제안하는 디지털 저작권 보호 시스템의 모형은 <그림 3-1>과 같다.



<그림 3-1> 시스템 모형

첫째, 저작물 식별 단계에서는 호환성 확보 및 표준화를 위하여 DOI(Digital Object Identifier) 분류체계와 메타데이터 관리 표준인 Dublin Core 및 저작권 기술언어로 XrML을 적용한다.

둘째, 저작물 암호화 단계에서는 원 저작물의 데이터 보호를 위해 PKI(Public Key Infrastructure)기반 암호화 기법을 이용하여 공개키를 원 저작물에 삽입하는 컨테이너 방식을 이용한다.

셋째, 저작물 사용자 인증 단계에서는 사용자가 저작물에 대한 사용을 원할 때 인증된 사용자인지에 대한 여부를 판단하는 단계로서 인증되지 않은 사용자 일 경우에는 안내 메시지와 함께 저작물에 대한 사용을 할 수 없도록 제한한다.

넷째, 저작물 복호화 단계에서는 저작물 암호화 단계에서 컨테이너 방식으로 삽입된 암호를 해제하는 단계로서 앞 단계인 저작물 사용자 인증 단계에서 인증된 사용자가 저작물에 대한 사용을 위해 프로그램을 가

동시킬 때 복호화 작업을 병행하면서 저작물에 대한 사용이 이루어 질 수 있도록 복호화 작업을 수행한다.

다섯째, 저작물 이용 감시 단계에서는 저작물에 대한 사용자의 사용권한 범위를 초과하거나 저작물에 대한 복사 및 이동 등 허가되지 않은 불법적인 사용 행위를 시도할 경우 이를 봉쇄하도록 저작물에 대한 지속적인 모니터링을 하는 단계이다.

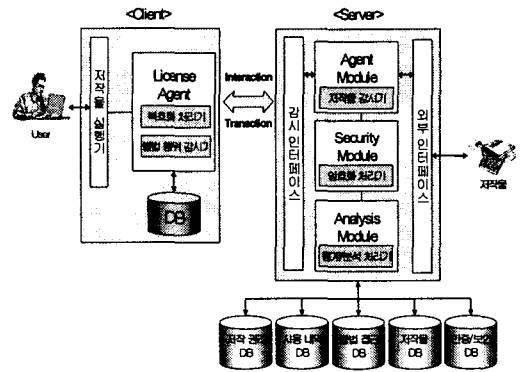
여섯째, 저작물 이용 정보관리 단계에서는 원 저작물 이용에 대한 전반적인 분석을 통해 통계를 계산하는 단계로서 어떤 사용자가 어떤 저작물에 대해 정상적인 사용 및 불법적인 사용을 몇 회나 시도 했는지, 또한, 사용권한 범위가 어느 정도인지 등 저작권 위배사례 수집 및 분석을 통하여 사용자에 대한 블랙리스트 관리와 각종 통계 정보를 계산하여 그 정보를 갱신 및 유지하는 작업을 수행한다.

시스템 모형에서 제시된 각 단계는 모두 시스템 서버에서 클라이언트로 이동되어 데몬으로 활성화된 라이선스 에이전트에 의해 자동으로 수행된다. 모든 정보는 시스템 서버에 있는 데이터베이스에 저장 및 관리되며, 라이선스 에이전트에게 필요한 정보는 클라이언트에 전송되어 클라이언트 데이터베이스에 저장된다. 시스템 서버에 있는 데이터베이스의 정보는 수시로 업데이트 됨과 동시에 클라이언트에 있는 데이터베이스도 수시로 업데이트가 되어 항상 최신의 정보를 유지하게 된다. 이는 네트워크의 에러 발생으로 인한 네트워크 단절시 시스템 서버의 정보를 이용할 수 없게 되므로 클라이언트에 있는 데이터베이스를 이용하기 위함

이다. 따라서, 제안하는 시스템은 온라인과 오프라인 상에서 모두 수행될 수 있도록 설계하였다.

3.2 시스템 구조

라이선스 에이전트는 원 저작물의 데이터 보호와 인증을 위해 기존의 저작물에 대한 단순한 사용권한 제한이나 패스워드 인증 방식이 아닌 PKI 기법을 이용한 사용자 인증과 데이터 암호화를 이용하여 원 저작물에 삽입하여 데이터를 보호해야 한다. 제안하는 시스템은 클라이언트/서버로 구성되어 운용되며 <그림 3-2>는 전체 구조도를 나타낸다.



<그림 3-2> 제안 시스템 구성도

시스템 서버는 외부 인터페이스를 통해 저작물이 등록되면 에이전트 모듈에 의해 저작물 감시에 대한 처리가 이루어지고 저작물에 대한 암호화 과정이 수행된다. 사용자의 저작물에 대한 사용 행위가 이루어지면 서버에서 파견된 라이선스 에이전트에 의해 사용자 인증 과정을 거친 후 인증된

사용자라면 저작물이 응용 프로그램에 의해 실행되고 인증되지 않은 사용자라면 경고 메시지를 보내게 된다.

저작물은 라이선스 에이전트에 의해 실시간으로 불법 행위 감시를 하게 되고 모든 사용자의 불법적인 행위는 감시 인터페이스를 통해 서버의 데이터베이스에 저장된다. 인증된 사용자라 할지라도 사용권한에 따라 제한적인 사용을 위해 저작물 자체 암호화에 의해 저작물을 보호하게 된다.

서버의 에이전트 모듈과 클라이언트의 라이선스 에이전트의 기능 및 처리를 요약하면 다음과 같다.

- 저작물 실시간 감시
- 사용자의 저작물 사용 행위 실시간 감시
- 저작물 자체의 암호화/복호화
- 사용자 인증 및 사용 권한 부여
- 저작물 실행에 의한 응용프로그램 사용 시 버퍼 스케줄링
- 저작물 감시에 따른 통계 및 분석
- 사용자 불법 행위에 따른 통계 및 분석

4. 인증 및 암호화 기법

4.1 동영상 파일의 암호화 및 복호화

동영상 데이터 자체의 암호화를 위해 LA는 다음과 같은 요구사항을 필요로 한다.

첫째, Agent는 클라이언트 시스템 내부에 존재한다. 클라이언트 내부에 존재하게 되며 Agent를 사용자 임의적으로 종료하게 되면 다운로드한 동영상의 정상적인 재생을 할 수 없다.

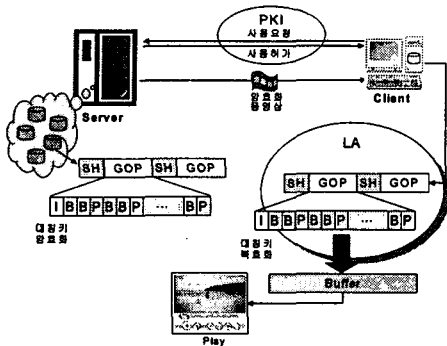
둘째, Agent는 클라이언트 사용자가 서버에 처음으로 접속하였을 때 서버로부터 다운 로드 하여 실행하며 클라이언트 시스템의 부팅과 동시에 실행되거나 사용자에게 의해 실행되어 사용한다.

셋째, Agent는 동영상의 실행 시 실행동영상의 사용자정의 데이터를 체크하여 암호화되어 있는 동영상과 일반 동영상을 구분하여 암호화되어 있는 동영상일 경우 서버에 사용요청을 수행한다. 사용요청을 받은 서버가 사용자 인증을 하게 되면 복호화에 필요한 대칭키를 사용자의 공개키로 암호화하여 클라이언트로 전송하게 되고 에이전트에 의해 암호화 되어 있는 동영상의 I 프레임은 복호화 하여 재생할 수 있도록 한다.

넷째, Agent는 사용자의 정보와 실행하고자 하는 동영상의 정보를 서버로 보내게 되고 서버는 사용자와 동영상정보를 통하여 실행 횟수 제한을 수행 할 수 있다.

서버의 동영상 데이터는 각 영상의 I 프레임을 추출하여 대칭키로 암호화 되어 있다. 사용자는 서버의 동영상을 다운로드 할 수 있으나 I 프레임이 암호화 되어 있어 정상적으로 사용할 수가 없다. 대칭키 알고리즘은 암호화와 복호화 하는 시간을 최소화 줄일 수 있기 때문에 사용하였다. 다운로드 받은 동영상을 클라이언트에서 재생 하고자 할 때 사용자는 서버에 사용 요청을 하게 되고 서버는 정상적인 사용자의 유·무를 판별하여 인증을 하여 주게 된다.

<그림 4-1>은 시스템의 저작물인 동영상 데이터의 암호화 및 복호화 과정을 나타낸 것이다.



<그림 4-1> 암호화/복호화 과정

이 인증절차는 PKI 알고리즘을 사용한다. 사용자의 공개키로 요청하는 동영상의 대칭키를 암호화 하여 클라이언트에 넘겨준다. 클라이언트의 에이전트는 사용자의 개인키로 복호화 하여 플레이 되는 동영상의 I 프레임과 B, P 프레임과 함께 버퍼에 저장하여 플레이 한다. 버퍼에는 전체 동영상이 플레이 되는 동안 지연되는 프레임의 계산을 하여 초기에 버퍼 사이즈를 결정한 후 플레이 하도록 한다.

4.2 라이선스 인증 기법

저작물 저작자는 창작한 저작물을 콘텐츠 출판업자에게 전송한다. 그러면 콘텐츠 출판업자는 해당 저작물을 임의의 대칭키 Ks 로 암호화하여 암호화된 저작물 C를 콘텐츠 제공자에게 전송하여 콘텐츠 제공자의 서버에 저장한다.

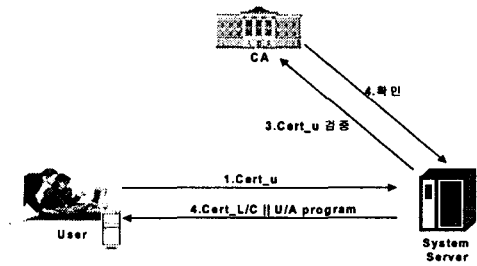
$$C = EKs[data]$$

사용자는 원하는 저작물을 콘텐츠 제공자

의 서버에서 다운로드 받아서 사용할 수 있다. 그러나 다운로드 된 콘텐츠는 암호화 되어 있으므로 사용자가 임의로 실행할 수 없다. 그러므로 다음의 단계를 거쳐서 사용할 수 있다.

1) Step 1 : 사용자 등록 프로토콜

사용자는 콘텐츠를 사용하기 위하여 우선 사용자 등록을 한다. 사용자 등록 과정은 <그림 4-2>과 같다.



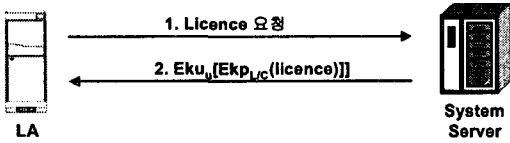
<그림 4-2> 사용자 등록 프로토콜

사용자는 라이선스 서버 기능을 갖는 시스템 서버에 접속하여 자신의 인증서 cert_u 를 전송한다. 시스템 서버는 사용자의 인증서 cert u를 인증경로를 통하여 검증하고 올바른 인증서이면 사용자 에이전트 프로그램과 클리어링 하우스의 인증서를 전송한다.

2) Step 2 : 라이선스 발급 프로토콜

사용자는 라이선스 에이전트(LA) 프로그램을 설치하고 라이선스 에이전트를 실행한다. 사용자의 PC에 탑재된 라이선스 에이전트는 사용자가 암호화된 저작물을 실행하면

<그림 4-3>과 같이 시스템 서버에 접속하여 라이선스를 발급받는다.



<그림 4-3> 라이선스 발급 프로토콜

라이선스 에이전트는 시스템 서버에 접속하여 원하는 저작물에 대한 라이선스를 요청한다. 시스템 서버는 라이선스 ID, 사용자 ID, 저작물 ID, 권한 등이 담긴 라이선스를 발급한다. 이때 라이선스의 구조는 <그림 4-4>와 같다.

Licence ID
user ID = certID
저작물 ID
date
권한
확장영역

<그림 4-4> 라이선스 구조

이 때, 보안을 위하여 다음과 같이 사용자의 공개키로 암호화하고 자신의 개인키로 서명하여 전송한다.

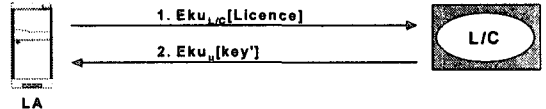
$$Eku_u[EkpL/C(licence)]$$

여기서 ku는 공개키를 나타내고 kp는 개인키를 나타낸다. 그러므로 kuu는 사용자(user)의 공개키이고 kpL/C는 L/C의 개인

키이다.

3) Step 3 : 라이선스 인증 프로토콜

라이선스 에이전트는 사용자가 암호화된 저작물을 실행하면 라이선스가 있는지 확인한다. 만약 라이선스가 없다면 위의 step 2에 따라서 라이선스를 발급받고 라이선스가 있다면 다음 그림과 같이 해당 라이선스에 대한 인증을 시스템 서버에 탑재된 라이선스 클리어링 하우스(L/H)에 요청한다.



<그림 4-5> 라이선스 구조

라이선스 클리어링 하우스는 라이선스 에이전트로부터 라이선스에 대한 인증 요청을 받으면 라이선스 저장 목록에서 권한을 확인한 후 인증을 하게 된다. 라이선스 저장 목록은 [표 4-1]과 같다.

[표 4-1] 라이선스 저장 목록

Licence ID	user ID	저작물 ID	권한	권한 값	key
1	11111	s11111	1	10	12345678
2	22222	a11111	2	04-3-12	87654321
3	33333	k11111	1	5	33333333
.
.

사용자의 라이선스가 특정일까지의 시간 라이선스이면 해당 시간이 경과 되었는지

확인하고 사용횟수에 대한 라이선스라면 횟수를 하나 줄인 후 해당 키 값을 다음과 같이 사용자의 ID와 연산하여 이를 사용자의 공개키로 암호화하여 전송한다.

$$E_{kuu}[key'] \quad (\text{where } key' = Ks \oplus userID)$$

암호화된 키를 받은 사용자 에이전트는 해당 암호화된 키를 사용자의 개인키로 복호화하여 key'을 추출하고 이를 사용자의 라이선스에 있는 user ID와 연산하여 키를 얻어서 암호화된 저작물을 복호화하여 사용자에게 보여준다.

5. 결론 및 향후 연구방향

본 논문에서는 라이선스 에이전트를 이용한 디지털 저작권 보호를 위한 멀티미디어 데이터 관리 및 감시 시스템에 대해 제안하고 설계하였다. 라이선스 에이전트는 PKI 기법을 이용하여 사용자 인증을 하며, 컨테이너 기법을 이용하여 시스템 서버에서 데이터 자체의 암호화를 한 후 클라이언트에서 버퍼 스케줄링에 의해 복호화를 하는 멀티미디어 데이터에 대한 저작권을 보호하는 기능을 수행한다.

앞으로 시스템 설계에 있어서 멀티미디어 데이터를 사용자가 실행할 때 버퍼 관리 스케줄링에 대한 구체적인 설계가 요구되며, 현재 설계를 기반으로 한 시스템 구현이 진행중에 있다.

참 고 문 헌

- [1]박복녕, 김태운, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이선스 관리 프로토콜", 한국정보과학회 논문지 I, 제30권, 제2호 pp.189-0198, 2003.
- [2]이용효, 황대준, "에이전트 기반의 동적 디지털저작권관리 시스템 설계 및 구현", 한국정보처리학회 논문지 D, 제8-D권, 제5호, pp.613-622, 2001.
- [3]한효영, 박복녕, 김태운, "Software Aging을 이용한 소프트웨어 저작권 보호 시스템", 정보과학회 2002년 추계학술대회, 제29권, 제2호, 2002.
- [4]황대준, 이용효, "에이전트 기반의 동적 디지털저작권관리 시스템 설계 및 구현", 한국정보처리학회논문지, 제8권, 제5호, pp. 613-622, 2001.
- [5]James Cannady, Jay Harrell, "A Comparative Analysis of Current Intrusion Detection Technologies", http://iw.gtri.gatech.edu/Papers/ids_rev.html, Feb., 1998.
- [6]Jai Sundar B., Spafford E., "Software Agents for Intrusion Detection," Technical Report, Department of Computer Science, Purdue University, 1997.
- [7]J.Dubl,"Digital Rights Management: A Defination", IDC 2001.
- [8]J.Dubl, S.Kevorkian, "Understanding DRM system: An IDC White paper", IDC, 2001.
- [9]Kentaro Endo, "The Building up of national Regional and International Registers for works and objects of related rights," Proc. pf International Conference on WIPO, Seoul, Korea October 25-27, 2000.
- [10]V.K Gupta, "Technological measures of protection," "Proc. of International Conference on WIPO, Seoul, Korea October 28-29, 2000.