2007년도 대한전기학회 하계학술대회 논문집 2007. 7. 18 - 20

라이센스 에이전트를 이용한 멀티미디어 데이터관리 및 감시 시스템 설계

조현섭, 유인호*
청운대학교 전자공학과, 국립익산대학 전기과*

The Design of a Multimedia Data Management and Monitoring System for using License Agent

Hyun-Seob Cho, In-Ho Ryu*
Dept of Electronic Engineering Chungwoon University, *Dept of Electrical Engineering Iksan National 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 컴퓨터간 상호연결성의 증대로 디지털자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 컨텐츠 보호와 관리를 위해서는 안정성, 보안성 확보를 위한 정보보호 기술과 저작권을 관리하고 컨텐츠 츄통 전반을 감시, 추적하는 디지털 저작권 관리(DRM:Dititial Right Management) 기술이 필요하다(James et al., 1998: Jai, 1997).

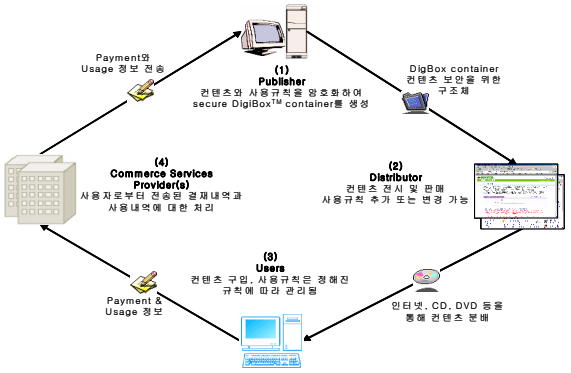
DRM 솔루션의 경우 InterTrust사, ContentGuard사 등 외국 업체와 국내의 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다. 그러나, 기존 DRM 기술의 경우 컨텐츠에 보호조건, 저작관리 등을 삽입하여 패키징하는 정적인 저작권 관리를 하기 때문에 저작권에 대한 동적인 제어가 어려울 뿐 아니라, 감시 및 추적 기능의 제약으로 불법적인 복제 등 지적재산권 침해 발생 시 불법행위 입증에 필요한 자료 확보의 어려움 등 해결해야 할 많은 과제를 가지고 있다. 사용자 프라이버시 침해는 사용자의 동의나 인가를 받지 않은 상태에서 한 개인의 정보를 수집하고, 인증에 필요한 정보 외에 개인을 식별할 수 있는 불필요한 정보를 수집한다든지 혹은 정보 이용에 대한 충분한 동의나 사전인지 없이 이를 사용하거나, 저장된 정보를 무단으로 공개하는 것으로 인해 발생한다. 최근 스팸 메일등과 같은 여러 피해사례가 높아짐에 따라 사용자 프라이버시에 침해에 대한 인식이 증가하고 있다. 이에 따라 DRM에서도 기존의 저작권 보호뿐만 아니라 사용자의 프라이버시 보호가 DRM 분야의 새로운 연구 과제가 되고 있다. 본 논문에서는 라이센스 에이전트를 이용하여 온라인과 오프라인 상에서 멀티미디어 컨텐프에 대한 사용자 인증과 원 데이터 자체의 암호화를 통해 불법적인 실행, 복사, 이동을 방지할 수 있는 통합적인 DRM 시스템을 설계하고자 한다.

2. 관련연구

2.1 정보 보호 기술

WMRM의 Rights Manager는 컨텐츠 제공자에게 인터넷 상에서 암호화된 파일 형식으로 보호된 음악, 비디오 등의 미디어를 배달한다. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(Indivisualization)과정을 통해 키 쌍을 할당받게 된며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스들에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 MS의 웹사이트를 통해 배포된다. 키는 라이센스에 포함되고, 라이센스와 컨텐츠는 분리되어 분배된다.

Client가 패키징 되어 보호된 컨텐츠를 실행시키면 player는 Licence Server에 라이센스를 요청한다. Server는 라이센스 요청에 대해 사용자의 인증과 지불여부를 확인한 후에 라이센스를 발생한다. 서버는 라이센스 발생 후 라이센스를 client 의 player에 전송한다. player는 서버에서 전송받은 라이센스를 확인한 후 사용규칙에 따라 컨텐츠를 실행한다. MS WMRM의 경우 Key ID와 Key seed를 결합하여 컨텐츠 암호화 키를 생성하는데, Key ID는 컨텐츠 해더에 포함되어 컨텐츠와 함께 패키징 되어 배포되고, Key seed는 클리어링하우스에 저장되어 관리된다. 복호화 키를 생성하기 위해서는 컨텐츠에 포함되어있는 Key ID와 서버가 관리하는 Key seed가 필요하다. MS의 WMRM 은 윈도우미디어플레이어에 탑재되어 널리 사용되지만, 동적변화변경에 제한적이고 윈도우미디어플레이어에만 적용되어 다양한 파일 형식을 지원하지 못한다. 그리고 라이센스를 발급 받기 위한 그림 1의 2와 3단계의 인증단계에서 특정한 보호기술 없이 사용자를 인증하여 사용자 ID나 전자우편 주소와 같은 사용자정보가 유출된다. Intertrust의 DRM은 컨텐츠의 보호를 위한 암호화 및 복호화, 컨텐츠의 사용규칙, 사용내역 기록 및 수집, 그리고 과금체계에 대한 지원이 이루어지고 있고, Superdistribution(Brd, 1996)을 실현하였으며, 사용자의 컴퓨터에서 컨텐츠를 사용하는 시점에서 거래를 체결하도록 하여 신용카드나 전자 화폐 등의 결제 방식을 이용하도록 하였다(박복녕 외, 2003: 이용효 외, 2001). Intertrust DRM의 서비스 흐름도는 그림 2-1에서 나타낸다.



[그림 2-1] Interust DRM 흐름도

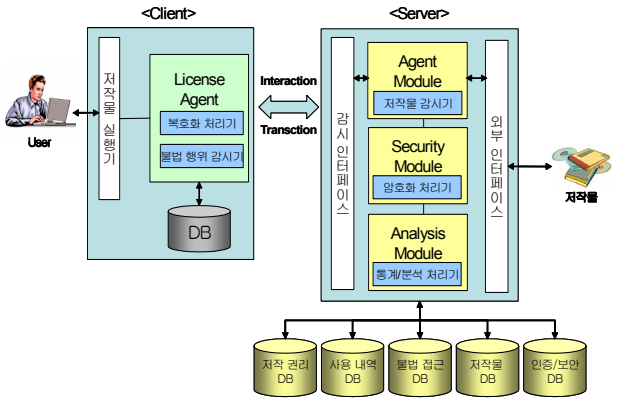
Intertrust의 DRM 기술은 다음과 같은 요소로 구성되었다. 첫째, InterRight Point는 Intertrust 구조의 핵심구조로 사용자의 컴퓨터와 서버의 MetaUtility 내에서 동작하도록 한다. 둘째, DigiBox® Container는 암호화된 컨텐츠와 사용 규칙 전송을 탑재하게 된다. 셋째, 사용 규칙은 가격, 결재 방법, 재생, 프린트, 복사, 저장, superdistibution 등에 관한 규칙으로 DigiBox에 탑재되어 있다. 넷째, 거래 승인(Transaction Authority) 프레임워크는 컨텐츠의 사용 내역이나 과금 내역 등의 정보를 처리하도록

한다. Intertrust에서 라이센스 획득 방법은 다른 방식들과 다르게 이용자의 컴퓨터에 설치된 라이센스 관리자를 통하여 라이센스를 획득한다. 이 방식이 가능하기 위해서는 오프라인 상태에서도 가능한 지불수단이 존재하여야 한다. Intertrust DRM은 그림 1의 (4)와 (1)사이의 사용내역 전송과정에서 평문 상태로 Payment와 Usage정보를 전달하기 때문에 사용자의 Payment Usage정보가 노출되어 이로 인한 사용자 정보 유출로 사용자의 프라이버시 침해 문제가 발생할 수 있다.

3. LA를 이용한 DRM 시스템 설계

3.1 시스템 구조

디지털 컨텐츠의 유통을 위해서는 상용화된 전자상거래 시스템들과 상호 연결을 통해서 저작물 유통과 결재가 가능하도록 표준화된 분류 체계와 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 한다. 특히, 법적인 문제 발생 시 저작권 위법 사례에 대하여 이를 입증할 수 있는 객관적인 자료의 유지 및 제공 기능이 저작권 보호 및 관리 시스템의 설계 요소로서 고려되어야 한다. 시스템 서버에 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 라이센스 에이전트에 의해 사용자 인증 과정을 거친 후 인증된 사용자라면 저작물이 응용 프로그램에 의해 실행되고 인증되지 않은 사용자라면 경고 메시지를 보내게 된다. 저작물은 라이센스 에이전트에 의해 실시간으로 불법 행위 감시를 하게 되고 모든 사용자의 불법적인 행위는 감시 인터페이스를 통해 서버의 데이터베이스에 저장된다.



[그림 3-1] 제안 시스템 구성도

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.

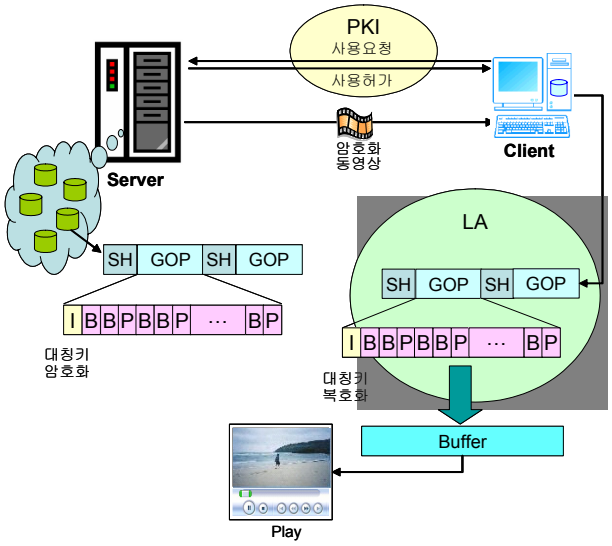
둘째, Agent는 클라이언트 사용자가 서버에 처음으로 접속하였을 때 서버로부터 다운 로드 하여 실행하며 클라이언트 시스템의 부팅과 동시에 실행되거나 사용자에 의해 실행되어 사용한다.

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 암호화 하여 클라이언트로 전송하게 되고 에이전트에 의해 암호화 되어 있는 동영상의 I 프레임을 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 최소로 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 4-1은 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 프레임을 추출하여 대칭키로 복호화를 수행한 후 B, P 프레임과 함께 버퍼에 저장하여 플레이 한다. 버퍼에는 전체 동영상이 플레이 되는 동안 지연되는 프레임을 계산하여 초기에 버퍼 사이즈를 결정한 후 플레이 하도록 한다.

4.2 라이센스 인증 기법

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

$$C = EKs[data]$$

사용자는 원하는 저작물을 컨텐츠 제공자의 서버에서 다운로드 받아서 사용할 수 있다. 그러나 다운로드 된 컨텐츠는 암호화되어 있으므로 사용자가 임의로 실행할 수 없다. 그러므로 다음의 단계를 거쳐서 사용할 수 있다.

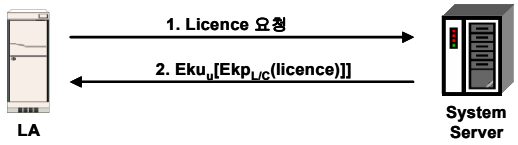
1) Step 1 : 사용자 등록 프로토콜

사용자는 컨텐츠를 사용하기 위하여 우선 사용자 등록을 한다. 사용자는 라이센스 서버 기능을 갖는 시스템 서버에 접속하여 자신의 인증서 cert_u를 전송한다. 시스템 서버는 사용자의 인증서 cert u를 인증경로를 통하여 검증하고 올바른 인증서이면 사용자 에이전트 프로그램과 클리어링 하우스의 인증서를 전송한다.

2) Step 2 : 라이센스 발급 프로토콜

사용자는 라이센스 에이전트(LA) 프로그램을 설치하고 라이센스 에이전트를 실행한다. 사용자의 PC에 탑재된 라이센스 에이

전트는 사용자가 암호화된 저작물을 실행하면 그림 4-2과 같이 시스템 서버에 접속하여 라이센스를 발급받는다.



[그림 4-2] 라이센스 발급 프로토콜

라이센스 에이전트는 시스템 서버에 접속하여 원하는 저작물에 대한 라이센스를 요청한다. 시스템 서버는 라이센스 ID, 사용자 ID, 저작물 ID, 권한 등이 담긴 라이센스를 발급한다. 이때 라이센스의 구조는 그림 4-3와 같다.

Licence ID
user ID = certID
저작물 ID
date
권한
확장영역

[그림 4-3] 라이센스 구조

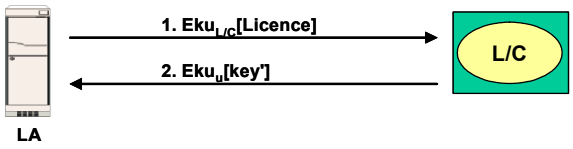
이 때, 보안을 위하여 다음과 같이 사용자의 공개키로 암호화하고 자신의 개인키로 서명하여 전송한다.

Ekuu[EkpL/C(licence)]]

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

3) Step 3 : 라이센스 인증 프로토콜

라이센스 에이전트는 사용자가 암호화된 저작물을 실행하면 라이센스가 있는지 확인한다. 만약 라이센스가 없다면 위의 step 2에 따라서 라이센스를 발급받고 라이센스가 있다면 다음 그림 4-4와 같이 해당 라이센스에 대한 인증을 시스템 서버에 탑재된 라이센스 클리어링 하우스(L/H)에 요청한다.



[그림 4-4] 라이센스 구조

라이센스 클리어링 하우스는 라이센스 에이전트로부터 라이센스에 대한 인증 요청을 받으면 라이센스 저장 목록에서 권한을 확인한 후 인증을 하게 된다. 라이센스 저장 목록은 [표 4-1]과 같다. 사용자의 라이센스가 특정일까지의 시간 라이센스이면 해당 시간이 경과 되었는지 확인하고 사용횟수에 대한 라이센스라면 횟수를 하나 줄인 후 해당 키 값을 다음과 같이 사용자의 ID와 연산하여 이를 사용자의 공개키로 암호화하여 전송한다.

Ekuu[key′] (where *key′=Ks⊕userID*)

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

[표 4-1] 라이센스 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
. . .	. . .	. . .	. . .	. . .	. . .

5. 결론 및 향후 연구방향

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

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

[참 고 문 헌]

[1] James Cannady, Jay Harrell, "A Comparative Analysis of Current Intrusion Detection Technologies," http://iw.gtri.gatech.edu/Papers/ids_rev.html, Feb., 1998.
[2] Jai Sundar B., Spafford E., "Software Agents for Intrusion Detection," Technical Report, Department of Computer Science, Purdue University, 1997.
[3] J.Dubl,"Digital Rights Management: A Defination", IDC 2001.
[4] J.Dubl, S.Kevorkian, "Understanding DRM system: An IDC White paper", IDC, 2001.
[5] 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.
[6] V.K Gupta, "Technological measures of protection, "Proc. of International Conference on WIPO, Seoul, Korea October 28-29, 2000.
[7] P.Vora, D, Reynolds, L.Dickinson,J.Erickson, D.Banks, "Privacy and Digital Rights Managements", A Position paper for the W3C Workshop on Digital Rights Management, January 2001.
[8] W. Diffie and M. E. Hellman, "New Directions in Cryptography, " IEEE Transaction on information theory, Vol. 1T-22, No.6, Nov. 1976.
[9] Frank J., "Artificial Intelligence and Intrusion Detection : Current and Future Directions, " NSA URP MDA904-93-C-4085, June, 1994.
[10] S. Craver, N. Memon, Boon-Lock Y대 and M.Yeung, "Can invisible watermarks resolve rightful ownerships," Proc. of IS&P/SPIE Conference, San Jose, CA, USA, Feb. 13-14, 1997.