論文
5-2-12

라이선스 에이전트를 이용한 디지털 저작권 보호를 위한 멀티미디어 데이터 관리 및 감시 시스템의 설계

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

박재표(Jae-Pyo Park)[1] 이광형(Kwang-Hyoung lee)[2]
김 원 (Won Kim)[3] 전 문 석(Moon-Seok Jeon)[4]

요 약

디지털 저작물의 전송환경이 빠른 속도로 바뀜에 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 신뢰할 수 있는 환경을 만들 수 있는 관심 있는 분야이다. 본 논문에서는 라이선스 에이전트를 이용하여 기존의 DRM 기법이 가지고 있는 정적인 DRM이나 온라인 환경에 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.

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.

키워드 : DRM(Digital Right Management), PKI(Public Key Infrastructure), 에이전트(agent)

1) 정회원 : 숭실대학교 정보과학대학 컴퓨터학과 박사과정
2) 정회원 : 숭실대학교 정보과학대학 컴퓨터학과 박사과정
3) 정회원 : 기전여자대학 교수
4) 정회원 : 숭실대학교 정보과학대학 컴퓨터학과 교수

논문접수 : 2004. 2. 5.
심사완료 : 2004. 2. 12.

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 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. 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[6]. 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[8].

DRM 기술을 통해 디지털 콘텐츠에 대한 지적재산권 침해사례로부터 저작권을 보호하고 유통과정을 관리하기 위한 종합적인 대책의 일환으로 추진되고 있으며 저작권에 대한 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[10].

기존의 DRM은 사용자의 프라이버시 보호가 저작권 보호에 직접적으로 필요하지 않는다는 이유로 사용자의 프라이버시 보호에 대해서는 고려하지 않았다. 이러한 영향으로 라이선스 발급 시의 사용자 인증과 콘텐츠의 불법 사용 감시를 위한 사용내역 보고 과정에서 사용자 정보가 유출되는 문제점이 발생하였고, 이로 인해 사용자 프라이버시 침해 문제가 발생하게 되었다[12].

DRM 솔루션의 경우 InterTrust사, ContentGuard사 등 외국 업체와 국내의 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다. 그러나 기존 DRM 기술의 경우 콘텐츠에 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. 따라서 온라인 및 오프라인 환경에서 모든 콘텐츠 유형에 적용가능하면서 동적인 저작권 관리와 실시간 감시 및 추적을 가능하게 하는 디지털저작권관리 기술의 개발이 필요한 실정이다[3].

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 라이선스 에이전트를 이용하여 온라인과 오프라인 상에서 멀티미디어 콘텐츠에 대한 사용자 인증과 원 데

이터 자체의 암호화를 통해 불법적인 실행, 복사, 이동을 방지할 수 있는 통합적인 DRM 시스템을 설계하고자 한다.

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[6]. 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[9].

DRM 기술을 통해 디지털 콘텐츠에 대한 지적재산권 침해사례로부터 저작권을 보호하고 유통과정을 관리하기 위한 종합적인 대책의 일환으로 추진되고 있으며 저작권에 대한 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[10].

기존의 DRM은 사용자의 프라이버시 보호가 저작권 보호에 직접적으로 필요하지 않는다는 이유로 사용자의 프라이버시 보호에 대해서는 고려하지 않았다. 이러한 영향으로 라이선스 발급 시의 사용자 인증과 콘텐츠의 불법 사용 감시를 위한 사용내역 보고 과정에서 사용자 정보가 유출되는 문제점이 발생하였고, 이로 인해 사용자 프라이버시 침해 문제가 발생하게 되었다[12].

DRM 솔루션의 경우 InterTrust사, ContentGuard사 등 외국 업체와 국내의 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다. 그러나 기존 DRM 기술의 경우 콘텐츠에 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. 따라서 온라인 및 오프라인 환경에서 모든 콘텐츠 유형에 적용가능하면서 동적인 저작권 관리와 실시간 감시 및 추적을 가능하게 하는 디지털저작권관리 기술의 개발이 필요한 실정이다[3].

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 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 시스템을 설계하고자 한다.

2. 관련연구

2.1 정보 보호 기술

2.1.1 암호화

암호화는 전자서명 및 정보보호를 위한 기본적인 기술이라고 할 수 있다. 암호화란 어떤 자료나 정보에 대하여 타인이 식별할 수 없도록 기술적 조치를 취하여 암호문으

로 바꾼 것으로, 데이터를 암호화하는 방식은 대칭 암호화방식과 비대칭 암호화 방식의 두 가지 기본적인 형태가 있다[13].

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 수단이기는 하나 디지털 저작물에 대한 저작권 침해를 방지하기 위한 감시 및 추적 기능의 제공 등 근본적인 해결책의 제공에 한계가 있다[4].

2.1.2 침입탐지시스템

침입탐지시스템(IDS : Intrusion Detection System)은 단순한 접근 제어 기능이 아닌 침입의 패턴 데이터베이스와 전문가시스템(Expert System)을 이용해서 네트워크나 시스템의 사용을 실시간으로 모니터링하고 침입을 탐지하는 보안시스템이다[14]. 침입탐지시스템은 침입차단시스템이 단순한 규칙에 따라 불법 침입을 차단하는데 따른 보안상의 한계점을 보완한다. 그러나 침입담지시스템은 적용범위가 시스템 내부에 국한되는 특징이 있어 온라인 및 오프라인을 통하여 유통되고 있는 디지털 콘텐츠에 대한 지적재산권 보호에 활용되기에는 저작권 침해를 입증할 수 있는 감시 및 추적 기능의 부재 등 많은 한계를 가지고 있다.

2.1.3 디지털워터마킹

디지털워터마킹(Digital Watermarking) 기술은 디지털 데이터를 보호하기 위해 이용되는 암호화 기술과는 달리, 디지털 콘텐츠 내에 저작자 정보, 또는 이용자 정보를 분리할 수 없는 방법으로 부가정보를 삽입하여 원본과 사본을 구별할 수 있는 기능 제공을 통하여 저작권과 소유권을 보호하는 방법으로 데이터에 일정한 패턴이나 코드를 숨겨서 부호화하는 과정이다[15]. 이러한 디지털 워터마킹은 영상, 이미지, 음악자료 등의 다양한 디지털 콘텐츠에 적용가능하며, 문서자료에 적용될 수도 있다. 디지털워터마킹 기술은 지적재산권 보호뿐만 아니라, 불법 유통을 감시할 수 있는 디지털 지문(finger printing), 디지털데이터 인증(authentication) 및 무결성(integrity)과 레이블링(labeling) 분야에도 응용될 수 있다. 디지털 워터마킹 기술은 초기에는 간단한 방법으로 저작권을 보호할 수 있는 기술로 관심을 받으면서 급격한 기술적 발전이 이루어졌다. 디지털워터마킹 기술은 지적재산권 보호문제를 기술적으로 해결하기 위한 대안의 하나로 제시되고 있다. 그러나 디지털워터마킹 기술의 경우 콘텐츠에 삽입되는 정적인 저작권 관리 및 추적기능 제공의 한계로 저작권을 적극적으로 보호하지 못하는 단점이 있다.

2.2 디지털 저작권 관리 기술

2.2.1 DRM 기술 동향

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)

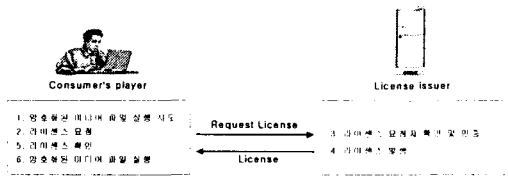
이 가운데 콘텐츠의 무결성과 신뢰성 확보를 위하여 암호화 기술을 중심으로 발전하여 왔으며 저작권에 대한 내용을 명시하기 위하여 XrML 기반으로 표준화가 진전되고 있으며 식별자 부여를 위하여 DOI를 적극 활용해 나가는 추세이다. 그리고 DRM은 전자상거래시스템과 결합해서 다양한 형태의 조건에 따른 디지털 콘텐츠의 유통을 일체화된 방식으로 제공할 수 있는 다양한 솔루션들이 등장하고 있다[5].

2.2.2 기존의 DRM 솔루션

1) Microsoft

Microsoft 의 WMRM(Windows Media Rights Manager)는 콘텐츠 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단 간(end-to-end) DRM 시스템이다[1].

WMRM의 Rights Manager는 콘텐츠 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 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스들에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 MS의 웹사이트를 통해 배포된다. 키는 라이선스에 포함되고, 라이선스와 콘텐츠는 분리되어 분배된다. 그림 1은 WMRM에서 라이선스 획득 단계를 나타낸다.



[그림 112] 라이선스 획득 단계

Client가 패키징되어 보호된 콘텐츠를 실행시키면 player는 Licence Server에 라이선스를 요청한다. Server는 라이선스 요청에 대해 사용자의 인증과 지불여부를 확인한 후에 라이선스를 발생한다. 서버는 라이선스 발생 후 라이선스를 client 의 player에 전송한다. player는 서버에서 전송받은 라이선스를 확인한 후 사용규칙에 따라 콘텐츠를 실행한다.

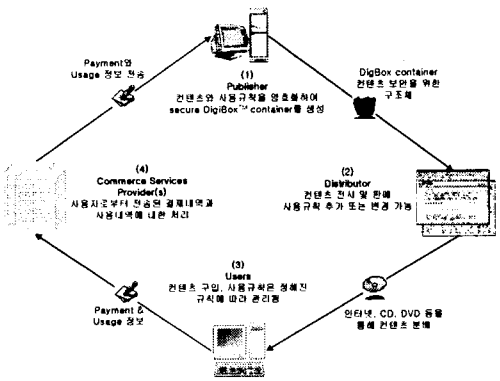
MS WMRM의 경우 Key ID와 Key seed를 결합하여 콘텐츠 암호화키를 생성하는데, Key ID는 콘텐츠 헤더에 포함되어 콘텐츠와 함께 패키징되어 배포되고, Key seed는 클리어링하우스에 저장되어 관리된다. 복호화 키를 생성하기 위해서는 콘텐츠에 포함되어있는 Key ID와 서버가 관리하는 Key seed가 필요하다.

MS의 WMRM 은 윈도우미디어플레이어에 탑재되어 널리 사용되지만, 동적변화변경에 제한적이고 윈도우미디어플레이어에만 적용되어 다양한 파일 형식을 지원하지 못한다. 그리고 라이선스를 발급 받기 위한 그림 1의 2와 3단계의 인증단계에서 특정한 보호기술 없이 사용자를 인증하여 사용자 ID나 전자우편 주소와 같은 사용자정보가 유출된다.

2) InterTrust

InterTrust의 DRM은 콘텐츠의 보호를 위한 암호화 및 복호화, 콘텐츠의 사용규칙, 사용내역 기록 및 수집, 그리고 과금체계에 대한 지원이 이루어지고 있고, Superdistribution[16]을 실현하였으며, 사용

자의 컴퓨터에서 콘텐츠를 사용하는 시점에서 거래를 체결하도록 하여 신용카드나 전자 화폐 등의 결제 방식을 이용하도록 하였다[1][2]. InterTrust DRM의 서비스 흐름도는 그림 2에서 나타낸다.



[그림 113] 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 콘텐츠와 사용 규칙 전송을 탑재하게 된다. 셋째, 사용 규칙은 가격, 결재 방법, 재생, 프린트, 복사, 저장, superdistribution 등에 관한 규칙으로 DigiBox에 탑재되어 있다. 넷째, 거래 승인(Transaction Authority) 프레임워크는 콘텐츠의 사용 내역이나 과금 내역 등의 정보를 처리하도록 한다.

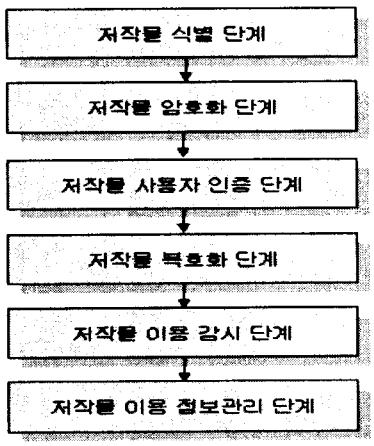
InterTrust에서 라이선스 획득 방법은 다른 방식들과 다르게 이용자의 컴퓨터에 설치된 라이선스 관리자를 통하여 라이선스를 획득한다. 이 방식이 가능하기 위해서는 오프라인 상태에서도 가능한 지불수단이 존재하여야 한다.

InterTrust DRM은 그림 2의 (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 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 암호와 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 가동시킬 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 업데이트됨과 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 위함이다. 따라서 제안하는 시스템은 온라인과 오프라인 상에서 모두 수행될 수 있도록 설계하였다.

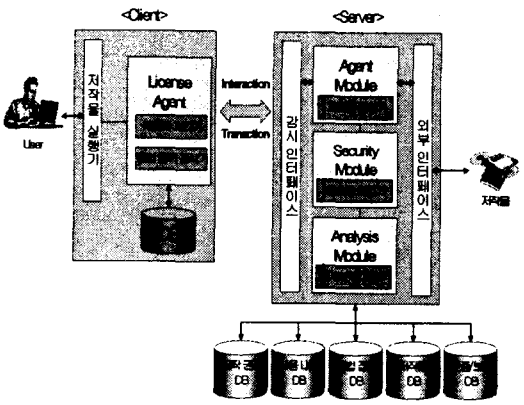
3.2 시스템 구조

디지털 콘텐츠의 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.

또한, 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.

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 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.



<그림 3-2> 제안 시스템 구성도

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.

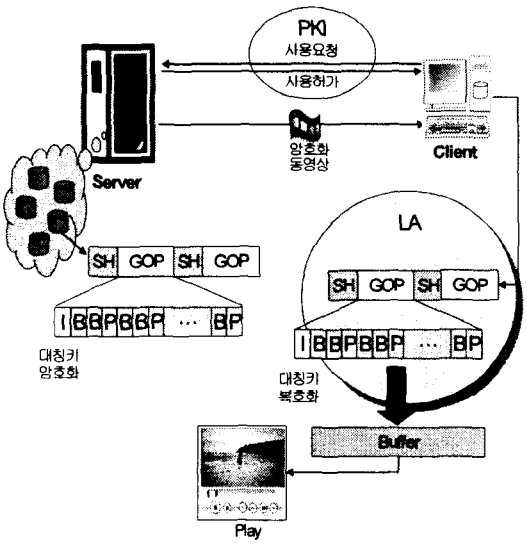
둘째, Agent는 클라이언트 사용자가 서버에 처음으로 접속하였을 때 서버로부터 다운 로드 하여 실행하며 클라이언트 시스템의 부팅과 동시에 실행되거나 사용자에 의해 실행되어 사용한다.

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 4-1>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 암호와 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 라이선스 인증 기법

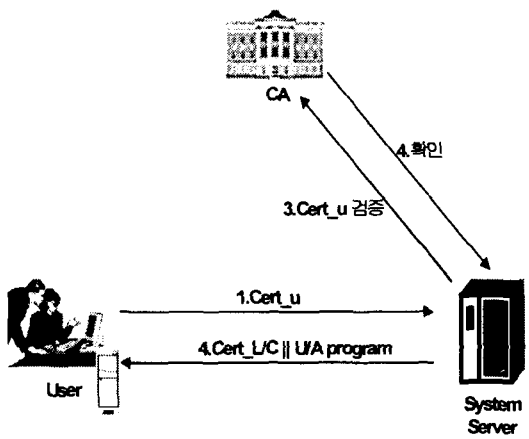
저작물 저작자는 창작한 저작물을 콘텐츠 출판업자에게 전송한다. 그러면 콘텐츠 출판업자는 해당 저작물을 임의의 대칭키 Ks로 암호화하여 암호화된 저작물 C를 콘텐츠 제공자에게 전송하여 콘텐츠 제공자의 서버에 저장한다.

$$C = EKs[data]$$

사용자는 원하는 저작물을 콘텐츠 제공자의 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.

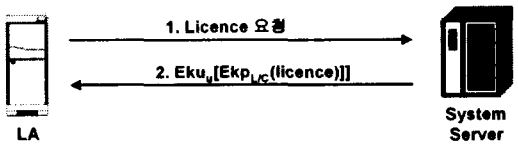


<그림 4-2> 사용자 등록 프로토콜

사용자는 라이선스 서버 기능을 갖는 시스템 서버에 접속하여 자신의 인증서 cert_u를 전송한다. 시스템 서버는 사용자의 인증서 cert u를 인증경로를 통하여 검증하고 올바른 인증서이면 사용자 에이전트 프로그램과 클리어링하우스의 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

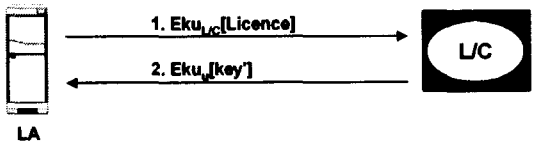
이 때, 보안을 위하여 다음과 같이 사용자의 공개키로 암호화하고 자신의 개인키로 서명하여 전송한다.

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

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

3) Step 3 : 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 클리어링하우스(L/C)에 요청한다.



<그림 4-5> 라이선스 구조

라이선스 클리어링하우스는 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.

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

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 진행 중에 있다.

참 고 문 헌

[1] 박복녕, 김태윤, "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] 이덕규, 박희운, 이임영, "Agent 기반 불법 복제 방지 DRM모델" 정보과학회 2001년 추계학술대회, 제28권, 제2호, pp. 682-684, 2001.

[4] 한효영, 박복녕, 김태윤, "Software Aging을 이용한 소프트웨어 저작권 보호 시스템", 정보과학회 2002년 추계학술대회, 제29권, 제2호, 2002.

[5] 황대준, 이용효, "에이전트 기반의 동적 디지털저작권관리 시스템 설계 및 구현", 한국정보처리학회 논문지, 제8권,. 제5호, pp. 613-622, 2001.

[6] James Cannady, Jay Harrell, "A Comparative Analysis of Current Intrusion Detection Technologies," http://iw.gtri.gatech.edu/Papers/ids_rev.html, Feb., 1998.

[7] Jai Sundar B., Spafford E., "Software Agents for Intrusion Detection," Technical Report, Department of Computer Science, Purdue University, 1997.

[8] J.Dubl,"Digital Rights Management: A Defination", IDC 2001.

[9] J.Dubl, S.Kevorkian, "Understanding DRM system: An IDC White paper", IDC, 2001.

[10] 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.

[11] V.K Gupta, "Technological measures of protection, "Proc. of International Conference on WIPO, Seoul, Korea October 28-29, 2000.
[12] 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.
[13] W. Diffie and M. E. Hellman, "New Directions in Cryptography, " IEEE Transaction on information theory, Vol. 1T-22, No.6, Nov. 1976.
[14] Frank J., "Artificial Intelligence and Intrusion Detection : Current and Future Directions, " NSA URP MDA904-93-C-4085, June, 1994.
[15] 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.
[16] Brd J.Cox,"Superdistribution : Objects As Property on the Electronic Frontier", Addision-Wesley, May 1996.

박 재 표

1996년 숭실대학교 컴퓨터학부(공학사)
1998년 숭실대학교 컴퓨터학과(공학석사)
2001년 숭실대학교 컴퓨터 학과 박사과정 수료
1998년~현재 국립 한경대학교 컴퓨터공학과 강사
관심분야 : 전자상거래 보안, 컴퓨터 통신, 영상처리, 멀티미디어 보안

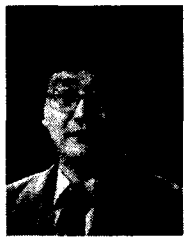
이 광 형

1998년 광주대학교 전자계산학과(공학사)
2002년 숭실대학교 컴퓨터학과(공학석사)
2002년~현재 숭실대학교 컴퓨터학과 박사과정
관심분야 : EC, S/W Agent, 영상처리, e-CRM

김 원

1988 숭실대학교 전자계산학과 공학사
1993 숭실대학교 전자계산학과 공학석사
1997 숭실대학교 전자계산학과 공학박사
1995. 3 ~ 현재 전주기전여자대학 조교수
관심분야 : 컴퓨터 통신, 보안

전 문 석



1981년 숭실대학교 전자계산학과(공학사)
1986년 University of Maryland Computer Science(공학석사)
1989년 University of Maryland Computer Science(공학박사)
1989년 3월~7월 Morgan State University 조교수
1989년~1991년 New Mexico State University Physical Science Lab 책임 연구원
1991년~현재 숭실대학교 부교수
관심분야 : 인터넷 보안, 멀티미디어 보안, 인증 시스템