디지털 도서관에서의 저작권보호 기술

숭실대학교 신용태*
(주)디지탭 오성흔

1. 서 론

디지털 도서관은 나날이 늘어나는 도서관 자료에 대한 관리자의 과중한 업무를 줄여주고 사무능률을 개선하여 보다 신속하고 편리한 업무처리를 가능하게 하며, 이용자에게는 고정 단말기 또는 이동 단말기를 통해 원하는 자료를 빠르게 검색하고 멀티미디어 수준의 자료를 제공함으로써 도서관 자료 이용률과 경영·관리 효율을 극대화시키고 이용자의 정보이용 환경을 획기적으로 향상시킬 수 있는 시스템이다.

디지털 도서관을 통해 이용자는 단순 문서 형태로부터 음악, 동영상, 애니메이션 등과 같은 멀티미디어 형태까지 원하는 콘텐츠에 대해 회사, 학교, 집에서 다양한 단말기를 통해 무료 또는 유료로 서비스 받을 수 있다. 디지털 도서관은 다양한 형태와 수준을 갖는 수많은 디지털 콘텐츠를 보유·저장하고 효율적인 검색 서비스를 제공하는 디지털 보관소(Digital Archive)와 같은 형태를 띨 것이다. 디지털 도서관은 이용자에게 쉽고 정확하게 원하는 자료를 검색할 수 있도록 해야 하고 좋은 품질의 콘텐츠를 충분하게 보유하고 있어야 한다. 이를 위해 디지털 도서관은 무료 콘텐츠뿐만 아니라 보다 좋은 품질과 전문적인 내용을 담고 있는 유료 콘텐츠 또한 보유하게 될 것이다. 이러한 유료 콘텐츠를 개발하는 전문 디지털 콘텐츠 저작자들은 자신의 디지털 콘텐츠가 디지털 도서관뿐만 아니라 여러 유통 시장에서 활발하게 유통되기를 원하는 동시에 콘텐츠의 저작권이 보호되어 지속적인 수입 확보가 유지될 수 있기를 원한다. 그러나 디지털의 완벽한 복제 특성은 저작권자들에게 심각한 위협거리로 대두되었고 불법 복제물의 유통은 저작권자들에게 심각한 경제적 손실을 끼쳤다. 예를 들어 IIPA(International Intellectual Property Alliance)는 미국 영화산업과 음반산업의 불법 유통에 의한 손실이 각각 연간 13억과 17억 달러 수준에 이른다고 추정하였다.

정보 및 통신 기술의 발달, 초고속 정보통신망의 구축, 멀티미디어 기술의 발전으로 인해 도서관 자료의 디지털 콘텐츠화가 매우 빠르게 이루어지고 있지만 여전히 콘텐츠의 저작권 문제를 해결하기 위한 시도는 매우 제한적으로 이루어지고 있다. 저작권 문제에 대해 충분히 안전하다고 평가되는 해결책들이 거의 없기 때문에 다량의 콘텐츠를 보유하고 있는 저작자 및 저작권자, 서비스 제공자들은 콘텐츠의 디지털화 및 온라인 서비스를 두려워하고 있으며 여전히 많은 초기투자비용과 물류비용을 발생시키는 물리적인 유통 구조를 이용하여 콘텐츠를 유통시키고 있다. 저작권 보호 문제를 해결하여 신뢰성 있는 디지털 콘텐츠 전자상거래 환경을 구축하기 위한 대안으로써 디지털 저작권 관리(Digital Rights Management 또는 DRM) 시스템 기술이 부각되고 있다. DRM 관련 기술에 대한 연구와 표준화가 국내외적으로 활발하게 이루어지고 있으며 이미 일부 동영상, 음악, 문서 콘텐츠에 DRM이 적용되어 서비스가 제공되고 있다.

본 고에서는 국회전자도서관의 DRM 구축 사례를 들어 디지털 도서관에 DRM이 적용되는 방법과 그 실효성에 대해 살펴보고자 한다. 2장에서는 디지털 저작권 관리에 대한 개요와 기술 동향을 살펴본다. 3장에서는 국회전자도서관의 DRM 구축사례를 설명하고 4장에서 맺음말로 본 고를 마치고자 한다.

2. DRM 개요 및 기술 현황

멀티미디어 및 정보 처리 기술의 발달과 고도화된 유·무선 인터넷 환경, 이용자들의 새로운 정보형태

* 종신회원

의 추구와 기대치가 높아짐에 따라 디지털 콘텐츠의 전자상거래 유통 시장의 급속한 성장이 예측되고 있다. 사회·경제·문화 등 많은 분야의 기존 정보들이 디지털화 되어 가고 있으며 앞으로 2005년까지 콘텐츠의 60% 이상이 디지털화 되어 갈 것으로 예측된다. 이미 MP3, 비디오 스트리밍, e-Book과 같은 디지털 콘텐츠는 우리 주위에서 서비스가 제공되고 있다. 그러나 정보의 디지털화는 불법 복제와 배포, 조작 및 유통을 가능하게 함으로써 저작권자에게 심각한 경제적 손실을 끼치고 더 나아가 디지털 콘텐츠 유통시장의 활성화를 저해하는 원인이 되고 있다. 이에 대한 대안책으로 디지털 저작권 관리(DRM) 시스템 기술을 이용한 디지털 콘텐츠의 저작권 보호에 대한 연구와 개발, 상업화가 이루어 지고 있다.

DRM이란 콘텐츠의 지적 재산권이 디지털 방식에 의해서 안전하게 보호·유지되도록 하여 디지털 콘텐츠가 창작에서부터 소비에까지 이르는 모든 유통 시점에서 거래 규칙과 사용 규칙이 적법하게 성취되도록 하는 기술이다. 보다 자세히 말하면 DRM은 디지털 콘텐츠의 표현 및 식별, 디지털 콘텐츠 유통 시장의 다양한 주체들의 이용 및 거래·과금 규칙의 정의, 의도한 규칙들에 따른 디지털 콘텐츠의 사용 제어, 콘텐츠 분배를 위한 암호화 및 인증·키 관리, 워터마킹, 불법복제 추적 기술, 콘텐츠의 투명한 전자상거래를 위한 거래 내역의 관리 및 보고 등을 가능하도록 하는 디지털 저작권 관리에 관한 하드웨어 및 소프트웨어 기술, 절차, 처리, 알고리즘 등을 의미한다. 즉, DRM은 불법 복제를 효과적으로 방지하고 거래 당사자들이 적법하게 콘텐츠를 이용하고 수익을 확보할 수 있는 신뢰성 있는 유통 환경을 마련함으로써 디지털 콘텐츠 산업의 발전을 도모할 수 있는 기반을 제공한다.

DRM이 제공하는 일반적인 기능은 크게 (1) 디지털 콘텐츠의 식별체계, (2) 불법적인 접근 및 사용, 복제 방지, (3) 저작권 및 사용 규칙의 정의·표현, (4) 과금 및 거래 내역 관리로 구분할 수 있다.

(1) 디지털 콘텐츠의 식별 체계

다양한 형태와 폭발적으로 증가하는 디지털 콘텐츠들의 체계적인 관리 및 통제, 접근, 이용효율성을 위해 대상물을 식별할 수 있는 체계가 요구된다. 예를 들어 기존 아날로그 콘텐츠의 식별 체계로는 국제표준도서번호(ISBN, ISO2108), 국제표준연속간행물번호(ISSN, ISO3297) 등이 있다. 기존 URL(Uniform Resource Locator)와 달리 디지털 콘텐츠의 위치정보에 상관없이 해당 디지털 콘텐츠에 고유한 이름체계를 제공해 주는 URN(Uniform Resource Name)이 제안되었으며 이를 구체적으로 실현하기 위해 응용의 일종으로 DOI(Digital Object Identifier), CID (Content ID), MPEG-21 Part3 DII&D(Digital Item Identification & Description) 등이 개발, 제안되었다. DOI는 디지털 콘텐츠에 대한 고유번호(식별자)를 부여하는 기능뿐만 아니라 URN Resolver와 같은 시스템을 이용한 DOI-URN 변환 기능을 제공함으로써 인터넷 상의 해당 디지털 콘텐츠를 추적할 수 있는 기능을 제공한다. MPEG-21 Part3 DII&D는 디지털 아이템의 속성, 타입, 구조적 형태 등에 관계없이 디지털 객체에 대한 식별과 기술을 할 수 있는 표준 프레임워크를 제공하며 다양한 식별체계(DOI, CID, URL 등)의 상호운용성을 위한 연구로써 RSS (Resolution System Switcher) 모델을 제안하고 있다. 디지털 콘텐츠에 대한 고유식별번호를 발급하고 관리하는 기관을 식별번호 등록관리기관이라고 부르는데 아직 유통 환경 내에서 독립적인 주체로 정착되어 있지는 않지만 식별 체계에 대한 요구의 증가에 의해 독립적인 주체로 정착될 것이다.

(2) 불법적인 접근 및 사용, 복제 방지

이 기능은 디지털 콘텐츠의 저작권 보호를 위한 DRM의 핵심 기능이다. 이 기능은 라이센스를 얻은 이용자 만이 허용된 규칙에 따라 디지털 콘텐츠를 사용하도록 하는 보호 측면에서의 요구사항을 가질 뿐만 아니라 보호 기능으로 인해 디지털 콘텐츠 이용에 불편함이 없도록 투명한 사용을 가능케 하는 편이성의 요구사항을 갖는다. 이 기능을 위해 적용되는 요소기술은 다음과 같이 내용제어(Content Control), 사용제어(Usage Control), 접근제어(Access Control)로 나눌 수 있다.

① 내용제어

워터마킹 기술을 이용하여 디지털 콘텐츠 내용 내에 저작권 보호 및 추적을 위한 정보를 비가시적 또는 가시적으로 삽입함으로써 불법 복제 및 배포, 재판매와 같은 행위에 대한 역추적 및 신원확인을 가능하게 하고 원저작자의 소유권 주장 등을 가능하게 한다. 내용제어 자체만으로는 불법 복사를 방지할 수 없지만 불법행위에 대한 추적을 가능하게 한다. 워터마킹 기술이 가져야 할 기본 특성으로는 디지털 콘텐츠의 품질에 인식할만한 손상이 없어야 하는 비인지

성, 정식으로 허가 받은 상태에서만 워터마크의 접근이 가능해야 하는 안전성, 워터마크를 제거하려는 악의적인 공격에도 남을 수 있는 강인성 등이 있다. 워터마킹 기술은 크게 삽입 기술과 검출 기술로 나눌 수 있다. 삽입 기술은 공간 영역 또는 주파수 영역에서의 워터마크 삽입 기술이 있다. 검출 기술은 원본 콘텐츠의 필요 유무에 따라 공개, 비공개 검출 기술이 있다. 오디오 워터마킹 관련 표준활동으로는 SDMI(Secure Digital Music Initiative), STEP2000 등이 있다. 비디오 워터마킹 관련 표준 활동으로는 CPTWG(Copy Protection Technical Working Group)과 TALISMAN 등이 있다. 워터마크의 중요성과 잠재된 개발성 때문에 많은 단체에서 워터마킹 연구와 표준화를 활발히 진행하고 있다. 그러나 현재의 워터마킹 기술은 암호화 기술 정도의 안전성을 가지지 못하며 강인성과 정보량, 품질에 대한 trade-off 문제 때문에 활발한 적용은 힘들며 제한적인 조건 내에서 사용되고 있다.

② 사용제어

디지털 콘텐츠 내에 또는 해당 디지털 콘텐츠와 같이 발급되는 라이센스에 명시된 사용 규칙에 따라 디지털 콘텐츠가 사용되도록 함으로써 이용자의 정당하지 않은 디지털 콘텐츠의 사용을 방지하는 것이다. 디지털 콘텐츠의 사용 규칙으로는 copy · transfer · loan · play · print · export · view · extract · edit · embed 등과 같은 사용유형규칙, folder · directory · delete · backup과 같은 파일관리규칙, 사용기간 · 사용개시일 · 사용만료일 등과 같은 사용시간규칙, 그리고 기타 사용요금 · 사용횟수 · 사용장소 · 접근조건 등과 같은 항목들이 있다. 주로 이용되는 방법은 암호화 키나 디지털 서명 등을 이용하여 콘텐츠의 사용행위를 제어하거나 복제조절정보(Copy Control Information)를 워터마크로 삽입하여 사용시 워터마크를 검출하여 play를 방지하거나 scrambling을 동작시킨다.

③ 접근제어

인증 기술을 이용하여 라이센스를 가지지 않은 이용자가 디지털 콘텐츠에 접근하지 못하도록 방지하는 기술이다. 그러나 인증키가 풀린 디지털 콘텐츠에 대한 불법 접근에 대한 제어는 불가능해진다. 이용자는 디지털 콘텐츠를 사용하기 위하여 적합한 절차에 의해 라이센스를 받는다. 라이센스에는 콘텐츠를 복호화할 수 있는 키(주로 대칭키)와 사용규칙이 명시되어 있으며 부가적으로 디지털 콘텐츠에 대한 설명, 저작자 정보, 발급자 정보, 이용자 정보 등이 포함된다. 라이센스의 불법 유출 및 변경, 손상을 방지하기 위해 안전하게 보관 · 관리할 수 있는 암호 및 인증 기술이 사용된다. 이용자의 운영체제 내에 포함된 라이센스 관리자 또는 클리어링하우스(Clearing House)나 콘텐츠 제공자로부터 다운로드 받은 라이센스 관리자라는 클라이언트 프로그램을 통해 이용자는 보유한 라이센스들을 관리한다. 라이센스 관리자는 해당 라이센스의 유효성을 검증하고 디지털 콘텐츠 사용 시 콘텐츠 복호화를 수행하고 사용규칙에 따른 디지털 콘텐츠의 사용제어 등을 수행한다. 클리어링하우스와 같은 라이센스 발급자는 라이센스의 안전한 전송을 위해 주로 비대칭키 암호화 방식의 공개키를 통해 라이센스를 암호화하여 전송함으로써 불법 이용자가 라이센스를 취득 · 이용하는 것을 방지한다.

(3) 저작권 및 사용 규칙의 정의 · 표현

디지털 콘텐츠 유통 시장이 거대해지고 활발해 짐에 따라 다양한 비즈니스 모델, 콘텐츠 판매 및 배포 방식, 과금 방식, 콘텐츠 이용 방식이 존재하게 될 것이다. 이를 위해 디지털 콘텐츠의 저작권 정보, 사용규칙, 조건, 거래 규칙 등을 정의 및 표현할 수 있는 저작권 메타데이터의 정의 및 권리표현언어가 필요하다. 이 정의 및 언어는 저작자, 저작권자, 콘텐츠 배급자, 판매자, 이용자로 구성되는 콘텐츠 유통 가치사슬을 명확히 정의하고 이들 각각이 요구하는 비즈니스 규칙을 쉽게 적용, 표현할 수 있도록 유연성과 확장성을 지녀야 한다. 디지털 콘텐츠 유통에 있어서 메타데이터 요소에 대한 표준화 문제는 상호운용성 확보를 위한 주요한 이슈로 다루어지고 있다. 메타데이터 요소 표준화와 관련하여 많은 활동들이 있으며 대표적으로 더블린 코어(Dublin Core)와 MPEG-7, INDECS, MPEG-21 RDD를 꼽을 수 있다.

현재 메타데이터를 기술하기 위한 언어로써 XML이 많이 사용되고 있다. XML은 W3C의 SGML 워킹그룹에서 제안한 것으로써 SGML의 복잡성과 이용률을 최소화하면서 HTML이 반영하지 못하는 문헌의 구조화를 지원해 주는 마크업 언어이다. MPEG21에서는 디지털 콘텐츠 유통에 관여하는 메타데이터 기술언어를 표준화하기 위한 활동으로 REL(Rights Expression Language)을 추진 중에 있다. 일반적으로 메타데이터 기술언어는 각각의 유통 시스템에서

개별적으로 개발하고 비밀화하여 사용하여 왔지만 다른 시스템 및 서비스 간의 상호운용성, 영속성, 신뢰성 등을 효과적으로 확보하기 위하여 표준화된 메타데이터 기술언어를 개발하고 있다. 2001년 12월 MPEG 회의에서 REL로서 ContentGuard가 XrML (eXtensible Rights Markup Language)을, 그리고 호주의 IPR Systems사가 ODRL을 제안하였고 XrML이 채택되어 현재 지속적으로 보완, 검토 중에 있다. XrML은 1.0 버전을 거쳐 현재 2.0 버전까지 나와 있으며 공개 스펙으로써 로열티 없이 누구나 사용 가능하다. 마이크로소프트를 비롯하여 국내의 다수 DRM 업체가 XrML을 권리기술언어로써 활용하고 있다.

(4) 과금 및 거래 내역 관리

디지털 콘텐츠의 분배 및 거래, 사용에 대한 내용을 수집, 보고함으로써 유통 가치 사슬에 관련되어 있는 각 주체들이 정당하게 수입을 확보하고 전자상거래의 투명성을 제공하기 위한 기술이다. 클리어링하우스는 이 기능을 위한 DRM 환경의 중요한 요소인데 콘텐츠 제공자가 디지털 콘텐츠를 패키징(디지털 콘텐츠의 불법복제를 막고 적법한 라이센스 절차에 의해 디지털 콘텐츠를 이용할 수 있도록 암호화하는 절차)할 수 있는 기술을 제공하고 콘텐츠 제공자로부터 특정 디지털 콘텐츠의 암호화 키 및 관련 정보들을 수집, 관리한다. 또한 디지털 콘텐츠를 사용하려는 이용자에게 라이센스를 생성, 발급하고 이에 대한 거래 내역을 관리·보고 기능을 수행한다. 어떤 클리어링하우스에서는 과금 처리를 동시에 처리하기도 한다. 전자상거래의 대부분의 거래내역 정보가 몇몇의 클리어링하우스에 집중되기 때문에 이들로부터 필요한 정보를 수집하는 제3의 통제기관인 디지털 클리어링센터(Digital Clearing Center 또는 DCC)의 필요성이 요구되고 있다. DCC는 클리어링하우스로부터 거래내역 정보를 보고 받고 다시 저작자나 저작권자에게 이를 알림으로써 저작자(저작권자)와 유통업자 사이의 신뢰성 있는 환경을 제공한다. 또한 DCC는 수집한 정보를 통해 전자상거래 관세 자료 및 다양한 통계자료로 활용한다.

3. 국회도서관의 DRM 구축 사례

국회도서관에서는 1985년 입법자료 및 도서관 자료에 대한 전산화를 위해 전산담당관실을 신설함으로써 입법부의 정보화 사업을 시작하였다. 1997년부터는 국가전자도서관의 표준모델을 제시하기 위한 '국가전자도서관 기본계획'을 수립하고 이를 기반으로 전자도서관 구축사업을 꾸준히 추진해 오고 있다. 2000년까지 정부간행물, 사회과학분야학위논문, 학술지 등 약 2,660만 페이지 분량의 원문자료를 디지털화하였다. 저작권 침해가 되지 않는 원문 자료들에 대해서 국회도서관의 인터넷 접속을 통하여 일반 국민들에게 제공하고 있다. 또한 국회의원들의 입법 및 의정활동 지원을 위해 입법 및 정책수립에 관련된 원문 정보 및 전문 정보들을 디지털화 하고 통합 DB로 제공하고 있다. 국회도서관은 원문 DB의 폭발적인 증가와 폭넓은 서비스 제공, 안전하고 지속적인 서비스 제공을 위해 S/W, H/W적으로 기능과 성능을 확장하고 있다. 이러한 확장의 일환으로 국회도서관에서는 DRM을 이용한 원문 DB 서비스의 저작권 보호 기능을 추가하였다. 본 장에서는 국회도서관에서 원문 DB 서비스에 대한 DRM 구축 사례를 살펴본다.

3.1 개 요

본 사례는 국회전자도서관의 원문 DB 서비스에서 제공하는 원문 자료의 불법 복제 및 불법 유통을 방지하기 위하여 기존 전자도서관 서비스에 DRM 시스템을 구축한 것이다. 국회전자도서관의 이용은 국회도서관내 또는 외부기관에 설치된 단말기를 이용하거나 인터넷 접속을 통해서 이용할 수 있다. 관내 설치 단말기 이용은 관내 국회 종사자, 국회의원 및 보좌관, 또는 도서 열람실 이용자를 통해 이루어 지며 IP 주소를 통한 인증 후 원문 DB에 대한 검색 및 열람이 가능하다. 외부기관 설치 단말기 이용의 경우 단말기의 NIC의 MAC 주소를 통한 인증을 통하여 사용이 가능하다. 인터넷 접속을 통해 열람을 하는 일반 이용자는 이용자 ID와 패스워드 입력을 통해 이용자 인증을 수행하며 저작권 문제가 해결된 문서에 대해서만 열람이 가능하다. 이용자는 이미지화 된 원문 자료들을 국회전자도서관에서 제공하는 이미지 뷰어를 통해 열람할 수 있다.

국회전자도서관의 원문 DB 서비스에 DRM을 적용함으로써 얻어지는 기능 및 장점은 다음과 같다.

- 기존 네트워크 보안 시스템의 성능 향상을 위한 추가적 기능
  - 관내외 접속 로그 분석을 통한 클리어링하우스

시스템 도입
- IP 주소, MAC 주소, 이용자 ID 등 서버 접속 및 열람 자료에 대한 제반 근거 확보
- 유사시 백도어 등과 같은 해킹 통로 추적 및 비정상적 접속 시도에 대한 근거자료 확보

· DRM 서버 확충을 통한 콘텐츠의 저작권 보호 방안 마련
- 인증 이용자의 접속 경로에 따라 콘텐츠의 공개 수준 결정 근거 마련 및 불법적인 데이터 유출시 유통 차단
- 워터마킹 엔진을 이용한 원시 콘텐츠의 보호 기능 추가
- 콘텐츠 저장소의 해킹에 대비한 콘텐츠의 암호화 저장 기능
- 인증 이용자 외에 어느 누구도 콘텐츠를 사용할 수 없도록 하는 암호화 통신 기능

· 뷰어의 이용자 인터페이스 유지
- 기존 이용자 뷰어에 DRM 모듈을 Plug-in 형태로 추가

타기관 제공 콘텐츠의 복호화 모듈 추가를 위한 인터페이스 마련

3.2 서비스 구성도

DRM이 적용된 국회전자도서관 시스템은 클라이언트, 웹 서버, 원문 DB 서버로 구성된다. 웹 서버는 원문 DB 서비스를 사용하기 위한 이용자 인증을 담당하고 원문 DB 서버는 인증된 이용자가 요청한 원문 자료를 암호화하여 전송해주는 작업을 담당한다. 그림 1은 원문 DB 서비스의 흐름도를 보여 준다.

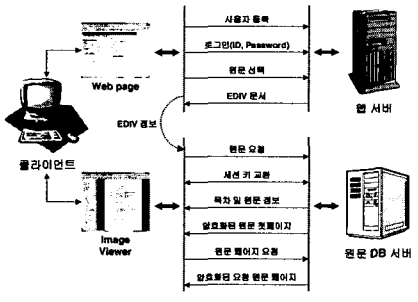


그림 1 국회전자도서관의 원문 DB 서비스 흐름도

클라이언트는 국회도서관 홈페이지(http://www.nanet.go.kr/)의 '전자도서관' 서비스를 통해 원문 DB 서비스를 받을 수 있다. 이용자는 전자도서관 서비스를 받기 위해서 먼저 이용자 등록을 해야 한다. 등록된 이용자는 이용자 ID와 패스워드를 통해 로그인 함으로써 국회도서관의 자료를 검색할 수 있다. 제공되는 질의 방식에 따라 이용자는 원하는 원문 DB 문서를 검색한다. 검색된 항목에 대해서 이용자가 원문 보기를 선택하면 웹 서버는 해당 원문에 대한 EDIV 문서를 클라이언트에게 전달한다. EDIV 문서에는 이용자가 원하는 원문 자료를 보유한 원문 DB 서버 정보와 원문 정보, 이용자 정보, 암호화를 위한 정보 등을 가지고 있다. 클라이언트의 웹 브라우저는 EDIV 문서를 처리할 수 있는 뷰어 프로그램을 실행시킨 후 다운로드한 EDIV 문서를 전달한다. 클라이언트의 뷰어 프로그램은 EDIV 문서에서 얻은 정보를 통해 해당 원문 DB 서버에 서비스를 요청한다. 원문 DB 서버는 요청에 대한 세션 정보를 구성하고 이용자와 공유할 세션 키를 생성한다. 이 세션 키는 대칭 키이며 원문 DB 서버와 클라이언트 간에 전송되는 원문을 암호화하고 복호화 하기 위해 사용된다. 이 세션 키는 RSA 또는 Diffie-Hellman과 같은 키 교환 알고리즘을 이용하여 교환된다. 세션 키의 교환이 이루어 진 후 원문 DB 서버는 해당 원문에 대한 목차와 세션 키로 암호화된 원문 첫 페이지를 전송한다. 그림 2는 뷰어 프로그램을 통한 원문 보기 화면을 보여 준다. 좌측 목차의 해당 페이지를 선택할 때마다 원문 DB 서버는 해당 이미지를 실시간으로 암호화하여 전송해주고 클라이언트는 이를 복호화 하여 우측에 원문 이미지를 보여 준다.

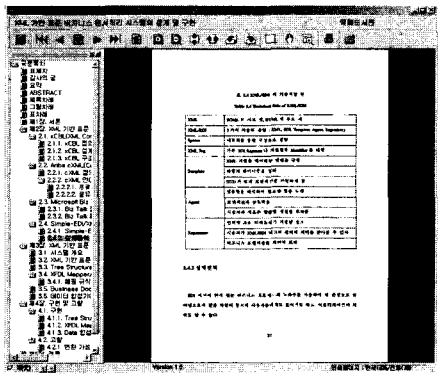


그림 2 뷰어를 통한 원문 보기 예제

3.3 적용된 기술 분석

그림 3은 국회전자도서관 DRM의 작업 흐름을 보여 준다. DRM의 운영은 두 단계로 나누어 지는데 첫 번째 단계(그림 3에서의 점선 참조)는 서비스를 위한 전처리 과정으로 원문저작자의 소유권 주장 및 확인을 가능하게 하기 위한 워터마킹 처리와 원문 DB 서버에서의 원문 기밀성을 보장하기 위한 1차 DRM 암호화 처리로 이루어 진다. 두번째 단계(그림 3에서의 실선 참조)는 서비스 시 이루어지는 것으로 클라이언트의 인증 처리와 안전한 기밀 통신을 위한 원문의 2차 DRM 암호화 처리로 이루어 진다.

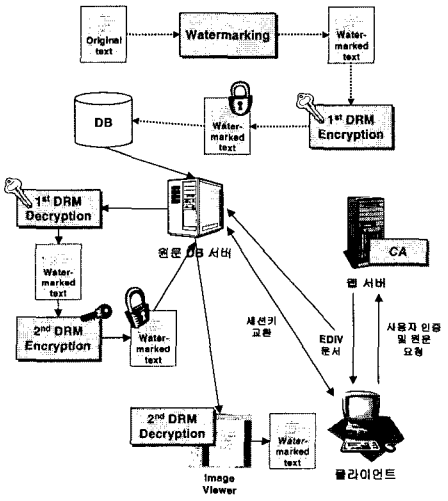


그림 3 DRM 작업 흐름

(1) 서비스 전처리 단계

이 단계에서는 원문 저작자의 소유권 주장과 확인을 위한 워터마킹 기술과 원문 DB 서버의 해킹 등으로 인한 불법적인 원문 유출 방지를 위한 1차적인 DRM 암호화 기술이 사용된다. 사용된 기술에 대한 설명은 다음과 같다.

· 워터마킹

제공되는 원문은 JPEG와 TIFF 형식의 이미지로 보관되어 있지만 사용된 워터마킹 방식은 특정 정지영상 파일 형식에 상관없이 적용될 수 있다. 워터마킹 방식은 정지영상 파일에 소유자를 확인할 수 있는 로고 정보를 삽입하여 소유권을 확인할 수 있도록 고안되었으며, 도서관 같은 대규모의 데이터 베이스 환경에서 관리자가 쉽게 이용할 수 있는데 초점을 맞추어 개발되었다. 이를 위해 빠른 속도로 처리하면서도 일반 이용자들의 사용 환경에서 발생할 수 있는 문제인 압축과 크로핑(cropping)에 강인하도록 설계하여 이러한 영상 변형에 강인한 워터마킹이 유지되도록 하였다. 여기서는 속도가 빠른 하르 변환(Haar transform) 필터를 이용한 웨이블렛 변환(wavelet transform)을 사용하였는데 웨이블렛 변환 방식은 공간 영역과 주파수 영역의 성분을 동시에 가지기 때문에 워터마크의 국부적 검출을 가능하게 하고 압축과 같은 변형에 강인한 성질을 갖는다. 워터마크 삽입은 주파수 영역 기반의 양자화 워터마킹(Quantization watermarking) 방식을 이용하였다. 관리자는 삽입할 워터마크 이미지를 선택한 후 대화식 또는 배치방식으로 워터마크를 삽입할 수 있다. 또한 워터마킹된 원문의 확인을 위해 검출 프로그램을 사용하는데 대상 이미지에서 특정 관리자가 삽입한 워터마크 이미지가 검출되는지를 확인한다. 이 프로그램은 삽입과정과 같은 방식으로 진행하며 크로핑을 고려하여 자동으로 워터마크 정보의 위치를 확인하는 동기화 기능을 가지고 있다.

· 1차 DRM 암호화

워터마킹된 원문을 원문 DB서버에 저장하기 전에 서버의 해킹, 크래킹과 같은 불법 공격에 의한 원문의 불법 유출을 방지하기 위해 관리자에 의해 1차적으로 암호화 된다. 사용된 암호화 알고리즘은 대칭키 방식의 Rijndael 알고리즘이 사용되었다. 이 암호화 알고리즘은 벨기에의 Joan Daemen과 Vincent Rijmen에 의해 개발되었으며, 2000년 10월 NIST에서 AES 암호 알고리즘으로 최종 선정되었다. SPN(Substitution-Permutation Network) 구조의 가변 블록길이를 지원하는 블록암호 방식으로 지원 블록 길이는 128, 192, 256 비트이며, 각 블록 길이에 대해 128,192,256 비트의 키를 사용할 수 있다. Rijndael는 지금까지 알려진 모든 공격에 강하고, 여러 플랫폼에서 빠르고코드가 간단하며, 디자인도 단순하다. 관리자는 암호화에 사용될 키를 설정하고 이 키를 이용하여 워터마킹된 원문을 암호화 하여 원문 DB 서버에 저장한다. 모든 원문 이미지가 암호화가 적용되어야 하는 것은 아니며 관리자가 선택할 수 있다.

(2) 서비스 단계

이 단계에서는 이용자의 신원 확인과 세션 키 공유를 위한 인증 기술과 서버와 인증된 이용자 사이의 원문 기밀 전송을 위한 2차 DRM 암호화 기술이 사용된다. 사용된 기술에 대한 설명은 다음과 같다.

· 인증

국회도서관내 또는 외부기관 설치 단말기의 경우 IP 주소, MAC 주소 등과 같은 하드웨어의 고유값을 통해 인증을 수행한다. 외부 인터넷 이용자의 경우는 이용자 ID와 패스워드를 이용한 로그인을 통해 인증을 수행한다. 인증된 이용자는 웹 페이지를 이용해 원문 검색을 수행하고 원하는 원문 서비스를 웹 서버에 요청한다. 웹 서버는 해당 원문의 EDIV 문서를 클라이언트에 전달하여 뷰어 프로그램을 실행 시킨다. 뷰어 프로그램은 해당 원문을 가지고 있는 원문 DB 서버에 서비스를 요청한다. 원문 DB 서버는 요청과 함께 전송된 EDIV 문서 정보를 가지고 세션 키를 구성한다. 세션 키는 키 교환 알고리즘을 통해 클라이언트와 공유된다. 세션 키는 2차 DRM 암호화·복호화 시에 사용되며 정해진 시간 동안 그리고 세션이 유지되는 동안만 사용 가능하므로 시간이 지나거나 세션이 끊어지면 더 이상 사용할 수 없다.

· 2차 DRM 암호화

클라이언트와의 세션 키 교환이 이루진 후 원문 DB 서버는 요청한 원문 이미지를 공유된 세션 키를 가지고 실시간으로 암호화하여 클라이언트의 뷰어에 전송한다. 1차 DRM 암호화가 적용된 원문 이미지의 경우 1차 DRM 암호화에 쓰인 공유 키를 통해 먼저 복호화하여 2차 DRM 암호화를 적용한다. 2차 DRM 암호화에는 1차 DRM 암호화에서와 같이 Rijndael 알고리즘이 사용되었다. 암호화된 원문 이미지를 받은 클라이언트는 원문 DB 서버와 공유한 세션 키를 이용하여 복호화하고 이를 화면에 보여 준다.

원문 보호를 위한 DRM 기술 외에 클라이언트의 뷰어 프로그램의 버전을 자동으로 체크하고 업데이트 하는 기능을 제공한다. 현재 국회전자도서관의 원문 데이터는 이미지 파일 형식으로 되어 있지만 차후 다른 형태의 콘텐츠나 타기관의 특유 보호 방식에 의해 생성된 콘텐츠를 지원하기 위해 프로토콜 해석기가 뷰어 프로그램 내에 탑재되어 있다. 이 프로토콜 해석기는 전송 받은 콘텐츠를 처리할 수 있는 적절한 모듈을 이용하여 이용자에게 서비스한다. 뷰어 프로그램은 처리 모듈을 ocx, lib, dll 등의 형태로 보유하고 있으며 향후 추가가 가능하도록 인터페이스를 제공한다.

또한 라이센스를 발급하는 기능은 없지만 거래 내역 관리를 해주는 클리어링하우스 시스템을 지원함으로써 관내외 단말기의 접속 로그 및 각 문서의 열람횟수 등의 정보를 제공하여 사용 통계 자료를 산출할 수 있도록 하며 해킹, 크래킹 시도에 대한 단말기 추적에 대한 근거를 제공해 준다.

4. 맺음말

본 고에서는 DRM에 대한 소개와 기술 상황, 그리고 국회전자도서관의 DRM 구축 사례를 살펴보았다. 사례를 통해 알 수 있듯이 국회전자도서관의 DRM 구축 시 2장에서 언급한 DRM의 모든 기술들이 적용된 것은 아니다. 예를 들어 콘텐츠의 식별체계(물론 국회도서관 내의 자체적인 식별체계는 존재한다.), 과금 서비스 등의 기술은 적용되지 않았다. 이는 다른 이유가 있는 것이 아니라 단지 국회전자도서관의 서비스 모델이 이러한 기술들을 필요로 하지 않았기 때문이다. 일반적으로 어떠한 디지털 콘텐츠 서비스 환경이던지 간에 서비스 모델 및 유통 환경, 대상 고객, 디지털 콘텐츠의 보호정도 등에 따라 적용되어져야 하는 DRM 기술과 그 복잡도는 달라지게 된다.

디지털 콘텐츠 시장에 대한 기대가 확대되면서 DRM 기술에 대한 요구가 증가하는 추세에 있다. 이에 따라 DRM 관련 업체들이 새롭게 설립되거나 기존 디지털 콘텐츠 관련 회사들의 사업 확장이 이루어져 DRM 기술에 대한 활발한 연구와 개발이 이루어지고 있다. 그러나 디지털 콘텐츠의 유료화에 대한 사회적 인식 및 제도화가 부족하여 현재는 DRM 업체의 수익 확보가 미비하지만 디지털 콘텐츠 유통 시장의 고부가가치성 및 고성장성, 글로벌 시장이라는 기대에 따라 DRM 시장의 매우 큰 성장률이 예상되고 있다. 국외의 경우 DRM 시장의 중요성을 인식한 유수 회사들이 일찍이 연구·개발을 진행함으로써 현재 선도적인 기술적 우위를 보이고 있으며 MPEG 21, IRTF/IETF, W3C를 중심으로 DRM 기술 표준화가 진행되고 있다. 국내의 경우 아직 대기업 자체에서 DRM 시장에 대한 구체적인 접근이 보이지는 않지만 다수의 중소기업, 벤처기업 중심으로 DRM 기술 개발 및 DRM 시장이 구체화 되고 있다. 초기에는 외국회사의 DRM 핵심기술을 도입하여 서비스를 개발하였지만 최근에는 자체 DRM 핵심기술의 확보를 위한 연구 개발이 활발하게 이루어지고 있다. 또한 정부 주도하에 이루어지고 있는 디지털 콘텐츠 산업 활성화 정책과 DRM 기술 표준화 및 포럼 중심의 전문가 그룹의 결집, 업체 간의 기술 상호 교류 등이 최근에 활발하게 이루어지고 있는 실정이다. 디지털 콘

텐츠 시장은 글로벌 시장이므로 이에 대한 DRM 기술 또한 글로벌 경쟁력을 가져야 하며 국제 표준화에 부합한 경쟁 제품들이 개발되어야 한다. 지금까지 대부분의 국내 기업은 자체 특유의 기술 및 서비스 모델을 중심으로 개발해 왔지만 서서히 국제 표준화에 부합한 제품의 개발에 초점을 맞추고 있다.

참고문헌

[1] 한국소프트웨어진흥원, 디지털콘텐츠 유통 프레임워크 구축 및 기술표준 전략 수립에 관한 연구, 2002.

[2] Jan Bormans and Keith Hill, MPEG21 Overview, MPEG, 2001.

[3] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom, Digital Watermarking, Morgan-Kaufmann Publishers, 1999.

[4] Renato Iannella, Digital Rights Management(DRM) Architectures, D-Lib Magazine, Vol. 7, No. 6, June 2001.

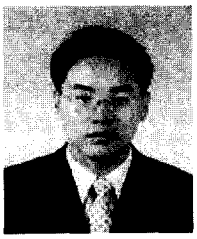
[5] S. Sun and L. Lannom, Handle System Overview, IDRM, August 2001.

[6] DOI Foundation, DOI Handbook, April 2002.

신 용 태

한양대학교산업공학(학사)
Univ.of Iowa 전산학(석사)
Univ.of Iowa 전산학(박사)
Univ.of Iowa 객원교수
Michigan State Univ. 객원교수
현재 숭실대학교 컴퓨터학부 부교수
관심분야 : DRM, 멀티캐스트 통신, 그룹 통신, 모바일 IP 등
E-mail:shin@comp.ssu.ac.kr

오 성 흔



인천대학교 정보통신공학(학사)
숭실대학교 컴퓨터학과(석사)
숭실대학교 컴퓨터학과(박사)
현재 (주)디지캡 기술연구소 선임연구원
관심분야:DRM, 암호학, 실시간 시스템, 멀티미디어 시스템 등
E-mail:honestly@digicaps.com