라이선스 기반 디지털 저작권 보호 방안

A Protection Protocol for License-based Digital Rights

신 원
동명정보대학교 정보보호학과
Shin Weon(shinweon@tit.ac.kr)

요약

인터넷 기술의 발달에 힘입어 누구나 다양한 멀티미디어 정보를 접근할 수 있게 되었으나, 이로 인해 멀티미디어 콘텐츠 저작권의 침해라는 새로운 문제가 발생하게 되었다. 최근 이러한 저작권 문제를 해결하기 위한 방안으로 디지털 저작권 관리가 활발히 연구되고 있다. 본 논문에서는 라이선스에 기반하여 멀티미디어 콘텐츠의 저작권을 보호할 수 있는 방안을 제안한다. 제안 방안은 콘텐츠의 한정 배포와 재배포(Superdistribution)를 제공하고 사용 규칙에 따른 콘텐츠의 안전한 사용을 보장한다.

■ 중심어 : | 디지털 저작권 | 라이선스 | Superdistribution | DRM | 멀티미디어 보안 |

Abstract

The Internet technologies allows anybody who has connect a network to access various multimedia information. But, it brings new issues about the violation of intellectual property and copyright of multimedia contents. Digital right managements have been actively studied as approaches to solve them. In this paper, we propose license-based schemes for the protection of contents and its rights on digital right management. The proposed schemes provide limited distribution and superdistribution of contents, and guarantee to securely use contents by usage rules.

■ keyword : | Digital Night | License | Superdistribution | DRM | Multimedia Security |

I. 서 론

미디어 기술과 컴퓨터 네트워크의 결합은 새로운 가능성을 제시하였고, 다양한 미디어의 융합을 통하여 새로운 멀티미디어 세상이 전개되기 시작했다. 쇼핑, 강의, 진료, 회의 등이 가상 세계에서 가능하게 되었으며 다양한 음악, 영화, 게임 등을 인터넷을 통하여 실시간으로 즐길 수 있게 되었다. 즉, 네트워크를 통하여 텍스트, 이미지, 사운드, 동영상 등을 기반으로 하는 멀티미디어 콘텐츠를 누구나 쉽게 얻을 수 있고 이를 다시 복제, 배포할 수 있는 환경이 되었다. 이는 모든 미디어가 컴퓨터가 처리 가능한 디지털 데이터로 가공됨으로써 더 이상 원본과 복사본의 구분이 불가능하다는 것을 의미한다. 원본과 똑같은 품질을 가진 콘텐츠를 거의 무한정으로 복제가 가능하고 네트워크를 통하여 빠른 시간에 배포가 가능하다는 것은 정보화 사회에서

접수번호 : #050519-003
접수일자 : 2005년 05월 19일
심사완료일 : 2005년 08월 05일
교신저자 : 신원, e-mail : shinweon@tit.ac.kr

의 가장 큰 장점인 동시에 멀티미디어 콘텐츠에 대한 저작권에 있어 새로운 위협이 되고 있다. 얼마 전 국내의 소리바다 판결, 저작권법 개정안에 대한 논쟁은 이런 문제점을 극명하게 보여주는 실례로 볼 수 있으며 근본적인 대처 방안이 등장하지 않는 한 앞으로도 이와 같은 문제가 얼마든지 발생할 수 있는 가능성이 존재한다.

현재 멀티미디어 콘텐츠의 저작권 보호를 위한 대표적인 기술로는 DRM(Digital Rights Management)과 워터마킹(Watermarking)을 들 수 있다. DRM은 콘텐츠의 복제는 허용하도록 하고 사용 권한에 제한을 두어 원작자의 권리를 사전에 보호하는 방식임에 비해, 워터마킹은 콘텐츠에 삽입되어 있는 특정 정보를 추적하여 원작자 또는 불법 배포자를 가려내는 사후 검출 방식이다[1][2]. 즉, 텍스트, 이미지, 오디오, 비디오 등에 멀티미디어 콘텐츠에 특정 저작권 정보를 사람의 시각 및 청각으로 구별할 수 없도록 삽입하는 기술이 바로 워터마킹이다[1]. 이를 이용하여 소유권 분쟁 발생시 이미 삽입된 워터마킹을 검색, 추출하여 원작자를 찾을 수 있도록 한다. 이러한 워터마킹에 대한 연구는 이미 국내외적으로 광범위하게 진행되어져 오고 있으며 이를 응용한 다양한 제품들도 출시되고 있다.

본 논문에서는 위에서 언급한 DRM에 대하여 살펴보고, 안전한 콘텐츠 배포와 정당한 사용에 대하여 논의하도록 한다. 먼저 2장에서는 관련 연구로써 기존 DRM 시스템을 살펴보고, 3장에서는 DRM 시스템의 구성과 동작에 대하여 설명한다. 4장에서는 현재 DRM 시스템에서 동작 가능한 라이선스 기반 저작권 보호 방안을 제안하고 5장에서 안전성 분석과 개선 방안에 대해 논의한 후 마지막 6장에서 결론을 맺는다.

II. 관련 연구

DRM은 콘텐츠의 지속적인 보호, 콘텐츠 사용 규칙과 권리에 대한 표현 방식, 사용규칙의 강제적 통제를 포함하는 광범위한 규약이지만, 협의의 의미에서 DRM은 암호화 기술을 이용하여 허가된 사용자가 허가된 권한 범위 내에서만 콘텐츠의 이용이 가능하도록 통제하는 기술로 정의할 수 있다[2].

최근 많은 업체에서 DRM 시스템을 구축하고 있는데, Intertrust DRM[3]과 Microsoft WMRM[4], MPEG-21[5]이 가장 대표적이다. 본 장에서는 그 중 DRM의 표준화를 주도하고 있는 MPEG-21[5]을 살펴보고, 기제안된 다른 방안을 살펴본다.

1. MPEG-21

MPEG-21[5]은 국제표준화기구인 MPEG에서 멀티미디어 영역에서 사용자가 사용하는 다양한 유형과 유통 방식을 지원하기 위한 멀티미디어 프레임워크이며, 여러 표준화 단체에서 개발해온 표준화 도구들을 통합하여 이루어지고 있다. 이를 위해 다양한 네트워크와 장치에서 멀티미디어 자원의 투명하고 부가적 사용을 지원한 7개의 구성요소를 두고 있다[5].

가. 디지털 항목 선언(Digital Item Declaration)
나. 콘텐츠 표현(Contents Representation)
다. 디지털 항목 식별과 기술(Digital Item Identification and Description)
라. 컨텐트 운영과 사용(Content Management and Usage)
마. 지적재산권 운영과 보호(Intellectual Property Management and Protection)
바. 터미널과 네트워크(Terminals and Networks)
사. 사건 보고기능(Event Reporting)

[그림 1]은 MPEG-21에서 구성된 요소와 그 요소들 간에 발생되는 반응들에 대해 표시한 것이다. MPEG-21에서 정의되는 User는 기존의 디지털 콘텐츠의 사용자만을 지칭하는 것이 아니라, 콘텐츠 생산자, 제공자, 소비자, 재가공 판매자 등 모두를 포함하여 지칭한다.

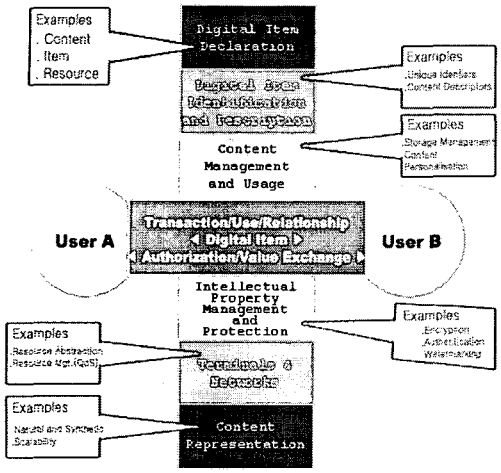

그림 1. MPEG-21의 구성 요소

2. LDRM(License-based DRM)

정연정 등[6]은 창조자, 유통업자, 구매자, 클리어링하우스가 참여하는 유통 모델에서 디지털 콘텐츠의 안전한 유통을 위하여 라이선스에 기반한 디지털 저작권 보호 시스템을 제안하였다. 이를 위해 메타데이터, Secure Container, 라이선스, DRM 클라이언트, 유통서버, 클리어링하우스 등을 설계하였다.

LDRM에서는 사용자가 원하는 콘텐츠를 선택하고 해당하는 사용규칙을 요청하면, 클리어링하우스는 콘텐츠와 사용자에 따른 적절한 라이선스를 발급한다. 사용자는 발급된 라이선스 범위 내에서 콘텐츠를 사용할 수 있다. 또한, 콘텐츠 패키저를 이용하여 데이터 구조, 데이터 무결성, 암복호화 방법, 인코딩/디코딩 방법 등을 정의하고 콘텐츠에 대한 비밀성과 무결성을 보장한다. 이를 위해 암호화키를 생성한 후 콘텐츠에 대해 암호화를 수행하고 라이선스를 발행하는 형태로 구성하였다. [그림 2]는 LDRM에서 사용하는 암호화키의 전달 방식을 보여준다.

LDRM은 특별히 라이선스 보호를 위해 필터 드라이브를 이용한 보호 방법을 제공한다. 그러나, 사용자 하드웨어 바인딩을 이용한 콘텐츠 사용을 지원하지 않

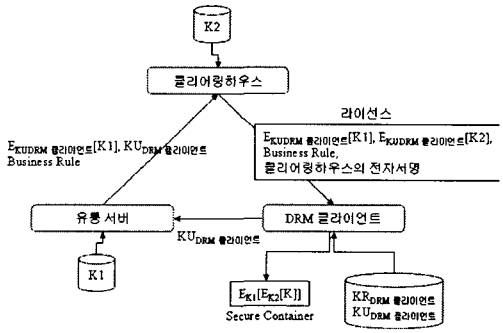

그림 2. LDRM의 암호화키 전달

고 Superdistribution을 제공하지 않는다.

3. LAP(License Administration Protocol)

박복녕 등[7]은 디지털 저작권 보호에서 사용자의 프라이버시 보호를 제공하는 라이선스 보호 프로토콜을 제안하였다. 임시 ID와 토큰을 사용하여 사용자 식별 정보 노출을 방지함으로써 익명성을 보장하고, 암호화를 적용하여 콘텐츠에 대한 비밀성을 제공한다.

LAP에서 라이선스에 대한 부분은 라이선스 에이전트를 두어 관리한다. 라이선스 에이전트는 콘텐츠 제공자로부터 암호화된 콘텐츠를 다운로드 받은 후 사용계약을 체결하고 라이선스를 획득한다. 라이선스 에이전트는 이 라이선스를 이용하여 클리어링하우스로부터 인증 받은 후 콘텐츠 복호화키를 제공받아 복호화한 후 콘텐츠를 실행한다. [그림 3]은 LAP의 구성 요소인 라이선스 에이전트의 동작을 보여준다.

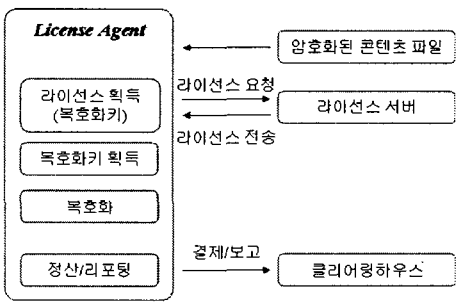

그림 3. LAP의 라이선스 에이전트 동작

LAP는 사용자 하드웨어 바인딩을 이용한 콘텐츠 사용 및 Superdistribution을 제공하고 사용자 프라이버시를 강조한 방안이다. 그러나 프라이버시를 제공하기 위해 프로토콜이 상당히 복잡하고, 키를 분산 처리함으로써 통신량이 많은 단점을 가진다.

III. DRM 시스템의 동작

DRM 시스템의 핵심은 멀티미디어 콘텐츠의 복제 및 배포는 얼마든지 허용하지만, 그 사용 및 열람에 있어서는 인증받은 사용자에게만 허가하도록 하여 불법적인 사용을 제한하는 것이다[2]. 이를 위해서는 디지털 콘텐츠 보호 기술, 안전한 디지털 배포 기술, DRM 모듈 보호 기술 등이 필수적으로 구현되어야 한다. 즉, DRM 시스템의 목적을 이루기 위해서는 다양한 정보 보호 기술 적용이 필수적인데, 대표적인 것이 데이터 암호화, 인증 및 서명 기술이다.

본 장에서는 디지털 저작권 보호 방안을 적용할 DRM 시스템과 DRM 모듈, 라이선스 구조에 대하여 기술한다.

1. 시스템 구성

DRM이 적용된 멀티미디어 콘텐츠는 일정 금액의 사용료를 지불하여 정당한 사용 권한을 획득한 사용자에게만 콘텐츠 사용을 허가하도록 함으로써 디지털 콘텐츠의 무제한 사용을 차단하는 것이다. 실제적으로는 디지털 콘텐츠에 대한 무제한의 복제가 가능하지만 그 사용 권한에는 특정한 제약을 두어 원작자의 권리를 보장하기 위한 방법이다.

DRM 시스템을 통한 콘텐츠 배포 및 사용은 다음과 같은 과정으로 이루어진다.

(1) **디지털 콘텐츠의 생성** : 콘텐츠 제공자는 다양한 장비, 소프트웨어 등을 이용하여 디지털 콘텐츠를 제작하고 배포자에게 전달한다.

(2) **디지털 콘텐츠의 배포** : 배포자는 특정키를 생성하여 콘텐츠를 암호화하고 인터넷 또는 CD-ROM, 디스켓 등과 같은 온라인 및 오프라인 매체를 통해 자유롭게 복제, 배포한다.

(3) **디지털 콘텐츠의 사용과 재배포** : 콘텐츠에 대한 사용 권한은 사용자가 정당한 사용료를 지불한 후에 사용자 인증 과정을 거쳐 라이선스를 부여받을 수 있으며 인증된 후에는 원할 때 얼마든지 사용할 수 있는 권한을 가진다. 또한, 암호화된 콘텐츠는 누구나 복제 및 재배포가 얼마든지 가능하지만 인증받지 못한 불법 사용자의 사용은 원천적으로 차단한다.

(4) **사용 내역 확인** : DRM 시스템은 콘텐츠 제공자에게 사용자가 사용한 디지털 콘텐츠에 대한 내역을 제공함으로써 전자화폐, 신용카드, 자동이체 등 다양한 방법을 사용하여 사용료를 결제할 수 있도록 한다.

이러한 DRM은 원래의 목적에 맞게 동작하기 위해서는 다음과 같은 요구 사항을 만족해야만 한다. 첫째, DRM 시스템은 우연한 사고뿐만 아니라 악의적인 변조에 대해서도 멀티미디어 콘텐츠를 보호할 수 있어야 한다[8]. 만약 변조가 가능하다면 공격자는 사용 회수, 지불 방식 등을 수정하여 콘텐츠를 자유롭게 배포할 수 있는 취약성이 존재한다. 둘째, 불법적인 읽기에 대하여 보호되어야 한다[8]. 공격자는 콘텐츠 복호화 키나 DRM 액세스 코드와 같은 비밀 정보를 보고 DRM 시스템에 적용하여 공격할 수 있으므로 불법적인 읽기 공격에 대해서도 보호되어야 한다. 무엇보다도 공격자 입장에서는 오프라인에서 하드웨어 장치를 이용한 변조 및 읽기 공격도 수행할 수 있으므로 이러한 공격에도 견딜 수 있도록 강건하게 설계되어야 한다.

2. DRM 모듈의 동작

콘텐츠와 라이선스 배포를 중심으로 DRM을 살펴보면, 참여자인 콘텐츠 배포자(Contents Distributor), 라이선스 클리어링하우스(License Clearinghouse), 사용자 클라이언트(User's Client)들의 상호 동작으로 나타낼 수 있다. [그림 4]는 DRM의 동작을 개략적으로 보여준다.

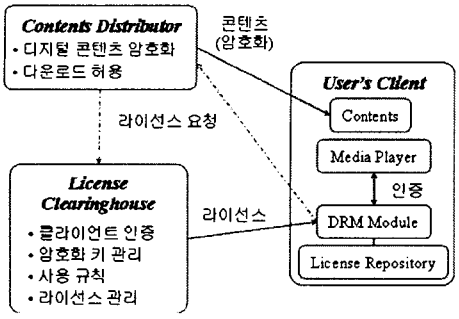

그림 4. DRM 시스템의 동작

DRM 모듈을 중심으로 시스템의 세부 동작을 살펴보면 먼저 ① 콘텐츠 배포자와 라이선스 클리어링하우스 사이에 각 콘텐츠를 암호화할 때 사용한 비밀 정보를 공유한다. ② 콘텐츠 배포자는 각 콘텐츠를 암호화할 때 사용한 비밀 정보를 이용하여 적절한 암호 기술을 사용하여 암호화하고 일반 사용자들이 다운로드받을 수 있도록 웹사이트 등을 통하여 공개한다. ③ 일반 사용자는 자신의 원하는 콘텐츠를 검색하고 암호화된 상태의 콘텐츠를 다운로드 받는데, 이를 다시 복제하거나 배포하는 것은 가능하지만 사용하거나 열람할 수는 없다. 사용자가 암호화된 콘텐츠를 사용하려면 DRM 모듈이 동작하면서 정당한 허가를 위해 라이선스를 요청한다. ④ 라이선스 클리어링하우스는 클라이언트를 인증하고 사용 규칙이 포함된 라이선스를 전송한다. 이 때 DRM 모듈은 라이선스를 안전한 장소에 보관한다. 미디어 플레이어는 콘텐츠 사용을 위해 저장소에 저장된 라이선스 정보를 얻기 위해 DRM 모듈에 요청하는데, 콘텐츠에 대해 정당한 라이선스 정보라면 사용 및 열람을 허가하고 라이선스 정보가 정당하지 않거나 없다면 허가하지 않는다.

DRM 모듈은 DRM 시스템에서 콘텐츠 사용자를 대행하는 에이전트로 볼 수 있으며 라이선스를 관리하고 콘텐츠의 복호화 등을 담당하는 매우 중요한 역할을 수행하므로, DRM 모듈은 DRM 시스템에서 안전하게 보호되어야 한다. 이를 위해 DRM 모듈은 TRS (Tamper Resistant Software)[9]를 사용하여 구현한다.

3. 라이선스의 사용

라이선스는 사용자에게 전달되는 콘텐츠에 대한 권한(Permission), 조건(Condition), 키(Key) 정보 등을 포함하는 권리 인증서로, 라이선스 클리어링하우스가 라이선스 일련번호, 사용자 및 하드웨어의 바인딩 정보, 발행 일자, 콘텐츠 사용 규칙 등이 포함하여 발행한다.

사용자는 콘텐츠를 전송 받는 것은 얼마든지 가능하지만 콘텐츠를 사용하기 위해서는 반드시 라이선스의 발급을 받아야만 한다. 이를 통하여 해당 콘텐츠를 복호화하고 사용 규칙에 따라 콘텐츠 사용이 가능하며 결재 시스템을 통해 사용료를 지불하게 된다.

Ⅳ. 라이선스 기반 디지털 저작권 보호 방안

본 논문에서 사용되는 표기법은 다음과 같다.

CD : Contents Distributor

LCH : License Clearinghouse

sn : 라이선스의 일련번호

usage : 콘텐츠의 사용 규칙을 기술, 사용자가 콘텐츠를 사용하는데 있어서 콘텐츠 타입, 사용 회수, 장비 환경, 사용 방법(view, play, print, save, execute 등)을 통제

dd : download descriptor, 콘텐츠의 위치를 지정하는 URL 또는 URI로 구성

dt : date & time, 라이선스의 발급 날짜와 시간

제안 방안은 다양한 암호 기법이 사용되는데, 그 표기는 다음과 같다.

$E_K(m)$: 키 K를 이용하여 메시지 m을 암호화

$Sig_X(m)$: 메시지 m에 대한 X의 전자서명

$Enc_X(m)$: X의 공개키로 메시지 m을 암호화

$H(m)$: 메시지 m에 대한 해쉬값

제안 방안을 적용하기 위한 가정은 다음과 같다.

첫째, 제안 방안에서 사용하는 해쉬 알고리즘(Hash

Algorithm, 예를 들어 HAS-160, SHA-1), 비밀키 암호 시스템(Secret Key Cryptosystem, 예를 들어 SEED, Rijndael), 공개키 암호 시스템(Public Key Cryptosystem, 예를 들어 RSA), 전자 서명 알고리즘(Digital Signature Algorithm, 예를 들어 KCDSA, DSA)은 이미 안전하다고 알려진 알고리즘들을 사용한다. 둘째, 각 참여자들은 서로의 공개키(Public Key)를 알고 있고 개인키(Private Key)를 안전한 장소에 보관한다. 즉, 개인키는 사용자 본인 또는 DRM 모듈만이 접근 가능하다.

본 장에서는 암호 기술을 사용한 라이선스 기반 저작권 보호 방안 2가지를 제안하는데, "한정 배포 방안"과 "Superdistribution 가능 방안"으로 나누어 제안한다.

1. 한정 배포 방안

특정 사용자에게 암호화된 콘텐츠를 배포하고 그 사용자만 해당 콘텐츠를 사용하도록 하는 방식으로 다음과 같이 동작한다.

A. 콘텐츠 다운로드 요청

① $DM_A \rightarrow CD$: $Enc_{CD}((CID_n, UID_A, DID_A), Sig_A(CID_n, UID_A, DID_A))$

사용자는 콘텐츠 배포자에 접속하여 콘텐츠를 선택하고 다운로드를 요청하면, DRM 모듈 DM_A은 사용자 A를 대신해서 해당 콘텐츠 ID CID_n, 사용자 ID UID_A, 사용자 장치 번호 ID DID_A를 서명값과 함께 CD의 공개키로 암호화하여 전송한다.

② $CD \rightarrow DM_A$: $(CID_n, usage, dd)$

콘텐츠 배포자는 해당 콘텐츠의 CID_n와 콘텐츠 사용 규칙 *usage*와 콘텐츠 위치를 나타내는 *download descriptor*(예를 들어 URL 또는 URI)를 알려준다.

B. 콘텐츠 배포

③ CD: $K = H(K_1, K_2)$
$K_1 = H(ID_{CD}, CID_n, r_{CD})$
$K_2 = H(CID_n, DID_A)$

콘텐츠 배포자는 자신의 ID ID_{CD}, 콘텐츠의 CID_n, 자신이 생성한 임의의 난수 r_{CD}와 콘텐츠의 CID_n, 사용자 장치 번호 DID_A를 사용하여 암호화키 K를 생성하고 비밀키 암호 시스템을 이용하여 콘텐츠 C_n을 암호화한다. $\rightarrow E_K(C_n)$

④ $CD \rightarrow DM_A$: $(CID_n, E_K(C_n))$

DRM 모듈은 콘텐츠의 CID_n와 해당하는 암호화된 콘텐츠 $E_K(C_n)$을 다운로드한다.

C. 라이선스 발급

⑤

$DM_A \rightarrow LCH$: $Enc_{LCH}((UID_A, DID_A, CID_n), Sig_A(UID_A, DID_A, CID_n))$

암호화된 콘텐츠를 사용하기 위해 라이선스를 발급받아야 하는데, DRM 모듈은 라이선스 클리어링하우스에 라이선스를 신청하기 위한 정보인 사용자의 UID_A, 콘텐츠의 CID_n, 사용자 장치 번호 DID_A와 함께 서명값을 LCH의 공개키로 암호화하여 전송한다.

⑥ $LCH \rightarrow DM_A$: $Enc_A(L_A(C_n))$

라이선스 클리어링하우스는 콘텐츠 C_n에 대한 A의 라이선스 $L_A(C_n)$을 생성하고 A의 공개키로 암호화한 뒤에 전송한다.

⑦ $DM_A \rightarrow LCH$: $Sig_A(H(L_A(C_n)))$

DRM 모듈은 라이선스 전송에 대한 응답으로 해쉬값을 생성하여 전자서명한 후 전송한다.

한정 배포 방안에서 사용되는 라이선스의 구조는 다음과 같다.

$L_A(C_n) = (ID_{LCH}, UID_A, DID_A, CID_n, K_1, sn, usage, dt), Sig_{LCH}(H(ID_{LCH}, UID_A, DID_A, CID_n, K_1, sn, usage, dt))$

한정 배포 방안에서 DRM 모듈은 라이선스에 포함된 K_1과 사용자 장치 번호에 기반하는 K_2를 이용

하여 $K(=H(K_1, K_2))$를 계산하고 $E_K(C_n)$를 복호화하여 C_n을 사용한다. 여기서, K_2는 사용자 A 컴퓨터의 고유한 장치 번호 DID_A에 의존하여 DRM 모듈이 계산하므로 다른 컴퓨터에서는 암호화키 K를 계산할 수 없다. 즉, 한정 배포 방안은 특정한 수신자만이 복호화하여 동작 가능하므로 재배포하더라도 복호화할 수 없다.

2. Superdistribution 가능 방안

임의의 암호화키를 사용하여 암호화된 콘텐츠를 자유롭게 배포하고 사용자 인증을 통해 라이선스를 부여받은 사용자만이 복호화할 수 있도록 하여 콘텐츠를 사용하는 방식이다.

A. 콘텐츠 다운로드 요청

① $DM_A \rightarrow CD$: (CID_n)

사용자는 콘텐츠 배포자에 접속하여 콘텐츠를 선택하고 다운로드를 요청한다.

② $CD \rightarrow DM_A$: $(CID_n, usage, dd)$

콘텐츠 배포자는 해당 콘텐츠의 CID_n와 사용규칙 *usage*와 콘텐츠 위치를 나타내는 *download descriptor*를 알려준다.

B. 콘텐츠 배포

③ CD: $K = H(ID_{CD}, CID_n, r_{CD})$

콘텐츠 배포자는 자신의 ID_{CD}, 콘텐츠의 CID_n, 임의의 난수 r_{CD}를 사용하여 암호화키 K를 생성하고 비밀키 암호 시스템을 이용하여 콘텐츠 C_n을 암호화한다.

④ $CD \rightarrow DM_A$: $(CID_n, E_K(C_n))$

DRM 모듈은 콘텐츠의 CID_n와 해당하는 암호화된 콘텐츠 C_n을 다운로드한다.

C. 라이선스 발급

⑤

$$DM_A \rightarrow LCH: \; Enc_{LCH}((UID_A, DID_A, CID_n), Sig_A(UID_A, DID_A, CID_n))$$

DRM 모듈은 라이선스 클리어링하우스에 라이선스를 신청하기 위한 정보인 사용자의 UID_A, 콘텐츠의 CID_n, 사용자 장치 번호 DID_A와 함께 서명값을 LCH의 공개키로 암호화하여 전송한다.

⑥ $LCH \rightarrow DM_A$: $Enc_A(L_A(C_n))$

라이선스 클리어링하우스는 콘텐츠 C_n에 대한 A의 라이선스 $L_A(C_n)$을 생성하고 A의 공개키로 암호화한 뒤에 전송한다.

⑦ $DM_A \rightarrow LCH$: $Sig_A(H(L_A(C_n)))$

DRM 모듈은 라이선스 전송에 대한 응답으로 해쉬값을 생성하여 전자서명한 후 전송한다.

D. 콘텐츠 재배포

⑧ $A \rightarrow B, \cdots, X$: $(CID_n, E_K(C_n))$

사용자 A는 또 다른 사용자인 $B, \cdots, X$에게 암호화된 콘텐츠를 재배포(Superdistribution)할 수 있다. 사용자 $B, \cdots, X$가 콘텐츠 C_n을 사용하기 위해서는 사용자 A와 마찬가지로 앞에서 설명한 라이선스 발급 절차를 거쳐야 한다.

Superdistribution 가능 방안에서 사용되는 라이선스의 구조는 다음과 같다.

$$L_A(C_n) = (ID_{LCH}, UID_A, DID_A, CID_n, K, sn, usage, dt), \; Sig_{LCH}(H(ID_{LCH}, UID_A, DID_A, CID_n, K, sn, usage, dt))$$

Superdistribution 방안에서 DRM 모듈은 라이선스에 포함된 암호화키 K를 이용하여 $E_K(C_n)$를 복호화하여 콘텐츠 C_n을 사용할 수 있다. 여기서, K는 특정 사용자에 의존하지 않고 정당한 라이선스만 발급받으면 누구나 얻을 수 있으므로 $E_K(C_n)$의 재배포가 가능하다. 단, $L_A(C_n)$는 안전하게 보관되어

DRM 모듈만 접근할 수 있다. 만약, $E_K(C_n)$의 복호화를 시도하려면 복호화키 K를 얻어야 하고, 이를 위해서는 $L_A(C_n)$를 안전하게 보관하고 있는 DRM 모듈 DM_A에 대한 공격이 성공하여야 한다.

V. 안전성 분석 및 개선 방안

본 장에서는 제안 방안에 대한 안전성을 분석하고 개선 방안에 대하여 논의한다.

1. 안전성 분석

제안 방안에 대한 안전성 분석 내용은 다음과 같다.

첫째, 제안 방안은 콘텐츠의 안전한 배포를 보장한다. 제안 방안에서 콘텐츠는 콘텐츠 배포자가 생성한 임의의 암호화키 K를 사용하여 암호화하여 $E_K(C_n)$을 전송한다. 여기서 K를 생성하기 위해서는 r_{CD}를 알아내면 되는데, 만약 r_{CD}가 i비트라면, 정확히 예측할 수 있는 확률은 $1/2^i$이다. i를 충분히 크게 하면 ($\geq$128), 예측할 수 있는 확률은 거의 0에 가까우므로 현실적으로 불가능하다.

둘째, 제안 방안은 라이선스의 위조에 대해 안전하다. 라이선스는 콘텐츠, 사용자, 배포자에 대한 여러 정보와 그 내용에 대한 전자서명으로 이루어진다. 즉, 라이선스의 위조는 기존 전자서명을 공격하여 위조 서명을 만드는 것과 동일한 어려움을 가진다. 따라서, 현실적으로 매우 어렵다.

셋째, DRM 모듈이 안전하다면, 제안 방안은 공모 공격에 안전하다. 제안 방안에서 각 암호화키와 라이선스는 DRM 모듈은 안전하게 보관하는 것으로 가정하였다. 즉, 여러 공격자가 공모하여 콘텐츠를 배포하려면 DRM 모듈을 공격하여 암호화키를 획득하여 사용하면 된다. 공모 공격에 안전하기 위해서는 DRM 모듈을 얼마나 안전하게 구현하는가에 달려있는데, TRS[9]를 적용하면 안전한 DRM 모듈 구현이 가능하다.

넷째, 제안 방안은 사용자의 컴퓨터 장치에 의존한 콘텐츠의 사용을 보장한다. 1. 한정 배포 방안에서는 콘텐츠 암호화키 자체를 사용자 장치에 의존한 값으로 암호화하여 구성하였으므로 장치에 대한 정보를 모르고서는 복호화조차 할 수 없다. 또한, 콘텐츠를 사용할 경우에는 DRM 모듈이 라이선스에 포함된 장치 정보와 실제 동작하는 컴퓨터의 장치 정보를 비교하도록 하여 사용자의 컴퓨터 장치에 의존한 사용을 보장한다. 여기서, 장치 번호 DID는 CPU의 일련번호, NIC의 MAC Address, HDD의 일련번호 등의 각종 장치들의 고유번호를 이용하여 계산한다.

2. 개선 방안과 기존 방안과의 비교

제안 방안의 개선 방안에 대해 살펴보면 다음과 같다.

첫째, 사용자 및 장치의 익명성을 보장하기 위해서는 해쉬 함수를 사용하여 UID_A대신 $H(UID_A)$를, DID_A대신 $H(DID_A)$를 사용하면 사용자의 정보가 노출되지 않으면서 라이선스를 얻어 콘텐츠를 사용할 수 있다. 결제시에는 사용자 UID_A를 요청하여 해쉬를 취한 후 라이선스에서 사용했던 $H(UID_A)$와 비교하여 일치여부를 확인한다.

둘째, DRM 모듈의 보호는 모듈을 분석하기 어지럽도록 구현하여 중요 정보를 알아내지 못하도록 하는 TRS[9] 또는 Software Obfuscation[10] 방안을 적용할 수 있다. 또한, 시스템 구현 측면에서는 하드디스크의 특정 저장소에 암호화키, 라이선스 등을 저장하고 이를 드라이버 레벨에서 암호화하여 인증 받은 DRM 모듈만이 접근하여 복호화할 수 있는 필터 드라이브를 통한 접근 제어 기술[6] 등을 사용할 수도 있다. 이를 사용하면 하드디스크를 도난당한다 하여도 암호화키, 라이선스 등은 드라이버 레벨에서 암호화되어 있으므로 복호화할 수 없다.

셋째, 제안 방안에서 콘텐츠를 암호화한 키 K_1와 K를 CD가 생성해서 LCH와 서로 공유하고 있으므로 한쪽에 문제가 생긴다 하더라도 복구할 수 있는 특성을 가진다. 그러나, 보안상의 문제로 인하여 한곳에서만 키를 관리하여야 하는 경우에는 다음과 같이 수정하면 된다. LCH가 라이선스 발급시 CD에게 키를

요청하면, CD는 암호화 키를 사용자 A의 공개키로 다시 암호화하여 LCH에게 전달하고, LCH는 이를 라이선스에 포함하여 사용자에게 전달하면 된다. 이를 통하여 암호화 키를 집중 또는 분산하여 관리할 수 있다.

넷째, 각 콘텐츠가 암호화 되어 있으므로 라이선스 없이는 그 내용을 볼 수 없다. 이에 대해 미리보기 기능을 제공하여 사용자의 편의성을 높이려면 $(CID_C, E_K(C))$를 $(CID_C, Preview, E_K(C))$로 수정하면 된다.

[표 1]은 [6]에서 제안한 LDRM 방안과 [7]에서 제안한 LAP 방안, 그리고 본 논문에서 제안한 (1) 한정 배포 방안, (2) Superdistribution 가능 방안의 특성을 비교하여 보여준다.

표 1. 제안 방안과의 비교

	LDRM	LAP	제안 방안	
			(1)	(2)
Superdistribution	×	O	×	O
한정 배포	O	×	O	×
라이선스 보호	필터 드라이브 사용	TRS 사용	TRS 사용	TRS 사용
라이선스 분배	단순	복잡	단순	단순
H/W 바인딩	×	O	O	O
콘텐츠 암호화	O	O	O	O
익명성 제공	×	O	O	O
암호화키 관리	분산처리	분산처리	분산처리/중앙집중	

제안 방안은 DRM에 직접 적용할 수 있으며, 암호 기술에 기반하여 비밀성, 인증성, 무결성, 익명성을 제공한다. 또한, 라이선스의 발급과 확인을 단순화하여 네트워크를 통한 통신량을 줄였고, 사용자의 하드웨어 장치에 의존하여 정당한 콘텐츠 사용이 가능하도록 하였다. 특히, 어플리케이션에 따라 2가지 방안을 각각 또는 함께 사용할 수도 있다.

VI. 결 론

본 논문에서는 DRM 시스템의 기본 동작을 살펴보고 DRM에 직접 적용할 수 있는 디지털 콘텐츠 보호를 위한 방안을 제안하였다. 또한, 제안 방안을 평가하고 개선방안에 대하여 논의하였다. 제안 방안은 DRM 환경에서 한정 배포와 Superdistribution이 필요한 환경에 적용할 수 있다.

최근 디지털 콘텐츠에 대한 저작권 보호라는 새로운 문제가 발생하고 있으며 이를 보호하기 위한 다양한 기술이 선보이고 있다. 그 중 DRM 시스템은 정당한 라이선스를 획득한 사람만이 콘텐츠를 사용하도록 허용하는 시스템으로써 네트워크 기술, 매체 기술, 암호화 기술 등이 복합된 멀티미디어 콘텐츠 보호 기술이다. 이를 위하여 본 논문에서는 특정 사용자만이 라이선스에 따라 콘텐츠를 사용할 수 있게 하는 "한정 배포 방안"과 콘텐츠의 배포는 누구나 가능하지만 라이선스를 취득해야만 콘텐츠를 사용할 수 있는 "Superdistribution 가능 방안"을 각각 제안하였다. 제안 방안을 통하여 DRM 시스템에서 배포 정책 및 비즈니스 모델에 따라 각각의 방안을 적용할 수 있으며, 보다 작은 통신량으로 라이선스를 배포·관리할 수 있다. 또한, 약간의 수정으로 사용자의 익명성을 보장하여 프라이버시를 보호할 수 있으며, 암복호화 키를 분산 또는 집중시켜 보안 정책에 유연하게 적용할 수 있다. 본 연구는 다양한 방법으로 가공·처리되어 인터넷으로 배포되고 있는 멀티미디어 콘텐츠를 정당하고 안전하게 사용할 수 있는 환경을 조성하는데 보탬이 되리라 예상된다.

참 고 문 헌

[1] 김현곤, 원동호, 정준원, *지적재산권 보호를 위한 정보은닉 기술 및 표준화 연구*, 한국전산원, 2000.

[2] 강호갑, *DRM 최신 국제표준 기술사양분석 및 세계 유명제품 동향과 전망에 관한 연구*, 한국소프트웨어진흥원, 2004.

[3] http://www.intertrust.com/

[4] http://www.microsoft.com/windows/ window

smedia/drm/default.aspx
[5] http://mpeg.nist.gov/
[6] 정연정, 윤기송, 류재철, "라이센스 기반 디지털 저작권 보호 시스템 설계 및 구현", 한국정보처리학회 논문지 C, Vol.11, No.1, pp.55-62, 2004.
[7] 박복령, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜", 한국정보과학회논문지, Vol.30, No.2, pp.189-198, 2003.
[8] 신원, 이경현, "이동 에이전트 기반의 콘텐츠 보호 기술", 한국멀티미디어학회지, Vol.5, No.1, pp.68-75, 2001.
[9] D. Aucsmith, "Tamper Resistant Software: An Implementation", Proceedings of the First International Workshop on Information Hiding, LNCS 1174, pp.317-333, 1996.
[10] http://www.cloakware.com/
[11] 주학수, 김대엽, 장기식, 김승주, "디지털 저작권 관리 시스템(DRM)의 개발현황", 정보보호학회지, Vol.13, No.2, pp.81-91, 2003.
[12] 노철균, 정연기, 임성운, 배상욱, 구본호, "멀티미디어 저작권 보호를 위한 디지털 워터마킹 기술의 현황", 한국멀티미디어학회지, Vol.4, No.1, pp.50-59, 2000.
[13] K. I. Lee, K. Sakurai, J. S. Lee, and J. C. Ryou, "A DRM Framework for Secure Distribution of Mobile Contents", Information Networking: Networking Technologies for Broadband and Mobile Networks International Conference ICOIN 2004, LNCS 3090, pp.905-914, 2004.

저 자 소 개

신 원(Shin Weon) 정회원

- 1996년 2월 : 부경대학교 전자계산학과(이학사)
- 1998년 2월 : 부경대학교 전자계산학과(이학석사)
- 2001년 8월 : 부경대학교 전자계산학과(이학박사)
- 2002년 3월~2005년 1월 : (주)안철수연구소 선임연구원
- 2005년 3월~현재 : 동명정보대학교 정보보호학과 전임강사

<관심분야> : 소프트웨어 보안, 악성코드 확산, 이동 에이전트 시스템, 암호 프로토콜 응용