Journal of Korea Multimedia Society Vol. 7, No. 8, August 2004(pp. 1107-1119)

전자화폐 시스템을 적용한 DRM 모델에 관한 연구

이덕규[†], 오형근[††], 이임영[†††]

요 약

전자상거래에서 중요한 지불 수단으로서 전자화폐 시스템이 있는데 전자화폐의 요구사항에는 독립성, 양도성, 분할성 등이 있다. 이는 컨텐츠에도 동일한 요구사항으로써 컨텐츠를 제공하는 데 있어 DRM에서 필요한 요구사항이 된다. 전자화폐의 요구사항이 컨텐츠 요구사항으로 이관될 수 있는 것은 컨텐츠 자체가 금전적 개념으로 볼 수 있기 때문이다. 컨텐츠에 대한 복제 및 복사, 익명 사용자의 접근 등 여러 관계에서 동일하게 적용시킬 수 있다. 본 논문에서는 전자화폐와 컨텐츠에 대해 동일한 가치로 두고, 전자화폐의 요구사항과 DRM의 요구사항을 살펴본 뒤 이를 통해 전자화폐의 개념을 적용하여 DRM 모델을 제시하고자 한다. 본 논문에서 사용되는 개념은 계층적 트리구조를 이용하여 복사 사용 권한을 두었으며 익명 사용자를 위해 컨텐츠에 대한 익명성과 사용자에 대한 익명성을 부여하였다. 마지막으로 제안된 여러 가지 방식들을 살펴보고 비교, 분석해 본다.

A Study on DRM Model Using Electronic Cash System

Deok-Gyu Lee[†], Hyung-Geun Oh[††], Im-Yeong Lee[†††]

ABSTRACT

There is Electronic-cash system as important payment means in Electronic-commerce and the requirement of electronic cash is independence, transferability, divisibility etc. This is important requirement in DRM to provide contents as a same requirement to contents. Because contents itself can see that requirement of Electronic-cash can be transferred the control of to contents requirement as monetary concept. Can apply equally in reproduction and copy for contents, anonymity user's access etc, and several relations. In this paper, wish to put by value that is equal about Electronic-cash and contents, and apply concept of Electronic-cash through this and present DRM model after examine requirement of Electronic-cash and DRM's requirement. Concept used in this paper left copy use authority to use hierarchic tree structure and endowed anonymity for contents and anonymity about user for anonymous user. Finally, examines and compares and analyzes proposed existing methods.

Key words: DRM, Contents Protection(컨텐츠 보호), Electronic Cash(전자화폐)

1. 서 론

전자상거래를 통해서 디지털 컨텐츠 판매가 활성화되기 위해서는 지적 재산권 보호에 대한 연구가 선행되어야 한다. 디지털 컨텐츠는 일반적인 오프라인 컨텐츠와는 달리 쉽게 복사 및 배포가 가능하다는 특성이 있다. 따라서 합법적인 구매자가 판매자로부터 디지털 컨텐츠를 구입한 후, 이것의 불법적인 재분배(Redistribution)를 막을 수 있는 방법이 고려되어야 한다. 이러한 방법들로 최근 디지털 컨텐츠의

※ 교신저자(Corresponding Author) : 이덕규, 주소 : 충남 아산시 신창면 읍내리 646(336-745), 전화 : 041)542-8819, FAX : 041)530-1548, E-mail : hbrhcdbr@sch.ac.kr
접수일 : 2003년 11월 4일, 완료일 : 2004년 1월 10일
[†] 준회원, 순천향대학교 정보기술공학부
[††] 준회원, 국가보안기술연구소 (E-mail : hgoh@etri.re.kr)
[†††] 종신회원, 순천향대학교 정보기술공학부 (E-mail : imylee@sch.ac.kr)
※ 본 연구는 한국과학재단 목적기초연구(R05-2003-000-12019-0)지원으로 수행되었음.

지적 재산권 보호를 위한 디지털 워터마킹 기술 및 핑거프린팅의 연구가 활발히 진행되고 있다. 이러한 원천 기술들을 이용하여 많은 DRM(Digital Rights Management)모델 들이 제시되어 왔으며 현재 널리 활용되고 있다.

또한 디지털 컨텐츠를 안전하게 보호하기 위한 응용기술로는 디지털 컨텐츠 유통/서비스를 위한 저작권 보호기술, 디지털 창작물에 대한 저작권/소유권/사용권을 제어하는 기술 및 암호기술 그리고 디지털 워터마킹 기술 등이 있다[7,9,12,14].

이와 연관하여 전자화폐는 실물 화폐의 기능을 사이버 공간에서 수행하기 위해 구성된 디지털 데이터이다. 전자화폐는 기존의 실물 화폐가 가지고 있는 기능뿐만 아니라 분할성, 추적성 등과 같은 새로운 기능을 추가시킴으로서 그 유용성을 증대시킬 수가 있다. 이러한 기능들은 컨텐츠 자체에 대해 유통 상에서 일어날 수 있는 위험 요소를 제거할 수 있다.

본 논문에서는 에서는 앞서 언급된 전자화폐의 특성을 적용함으로써 디지털 창작물에 대한 유통/서비스과정에서 컨텐츠를 보호할 수 있는 방안을 제시할 것이다. 더 나아가서는 유통 혹은 서비스 단계에서 발생할 수 있는 불법복사를 차단함으로써 저작권보호 및 사용권 보호를 이룰 수 있을 것으로 사료된다.

이를 위해 기존 전자화폐 및 DRM의 요구사항을 분석하고 이를 통해 전자화폐 시스템을 적용한 새로운 DRM 모델을 제시하고자 한다. 또한 [19]에 제시되었던 전용플레이어나 스마트카드 모두에서 사용이 가능하고 유무선 환경에 제한 없이 사용 가능하도록 설계하고자 한다.

2. DRM의 요구사항

저작권이란 '인간의 독창적인 생각을 시각, 청각 또는 시청각을 통하여 지각할 수 있도록 독창적으로 표현한 것(Expressive information)이다. 즉, 저작물에 대하여 부여한 독점적이고 배타적인 권리이다. 특허가 새로운 발명이란 아이디어 그 자체를 보호하는 권리라고 한다면, 저작권은 아이디어의 표현(Expression of Idea)을 보호해주는 점에서 차이가 있다. 따라서 타인의 저작물과 동일한 내용이라도 표현이 상이한 경우에는 저작권법의 보호를 받을 수 있다[7,9,13].

이러한 디지털 컨텐츠의 정의에 따른 유통에 있어서 저작권자 권리 보호기술은 다음 기능을 제공하는 것을 목적으로 한다.

(1) 불법 복제 및 불법 재생을 차단하고, 변경 및 해킹에 대비하여 저작자가 사용을 원하는 사용자와 원하지 않는 사용자를 식별해서, 원하는 사용자에게만 선택적으로 효용성을 제공한다.

- 이것은 전자화폐의 요구사항에 있어 분할성(Dividability)에 해당할 수 있을 것이다. 분할성은 일정한 가치를 가지고 있는 전자화폐는 그 가치만큼 자유롭게 분할 사용 할 수 있어야 한다.

컨텐츠에 대한 복사 권한을 부여받았을 경우 사용자는 컨텐츠에 복사 권한에 대하여 자유롭게 사용할 수 있어야 하는 의미와 같이 볼 수 있다.

(2) 컨텐츠를 화면을 통해 보거나, 출력, 복사, 전송, 수정 등의 다양한 조작이 권한에 따라 가능하고 조작시 소유 권한에 대한 제어가 가능해야 한다. 뿐만 아니라, 불법 행위의 경우 사용권을 취소하는 기법이 필요하다.

- 전자화폐의 요구사항 중에서 독립성(Independence)에 해당할 수 있다. 전자화폐의 보안은 어떠한 물리적인 상태들에 의존해서는 안 된다. 이것은 복사 방지를 위해서 사용되는 복사 방지 인쇄 기술이나 또는 변경 불가능한 디바이스(Tamper Resister Device)와 같이 데이터를 보호하기 위한 외부적인 요소들에 의해 그 보안성이 결정되어서는 안 된다.

(3) 멀티미디어의 음악, 그림, 영화, 게임 등 전달되는 컨텐츠의 특성에 적합한 저작권자 권한 보호가 이루어져야 한다.

- 전자화폐의 요구 사항 중에서 불추적성(Untraceability)에 해당할 수 있다. 전자화폐의 지불과정에서 물품 구입 내용과 사용자와의 관계가 어느 누구에 의해서도 추적 불가능해야 한다.

저작권의 권한 보호뿐만 아니라 사용자 사용에 대한 권한도 보장받아야 하는데 이러한 것은 전자화폐의 불추적성을 기초로 해결될 수 있다.

(4) 컨텐츠가 재유통 가능한 디지털 형식으로 누

설되는 것을 방지 또는 억제해야 한다.

(5) 컨텐츠의 유통 시 효율성, 편리성 및 안전성을 고려해야 한다.

- 전자화폐의 요구 사항 중에서 보안성(Security)에 해당할 수 있다. 복사와 위조의 위험성은 예방이 되어야 한다. 즉, 화폐 가치가 복사되더라도 사용될 수가 없어야 하며, 불법 사용자는 즉시 판별 가능해야 한다.

컨텐츠 유통 시 효율성과 편리성을 고려해야 하며 유통과정에서 발생할 수 있는 위협행위에 대해 쉽고 빠르게 대처가 가능하도록 안전성을 고려해야 한다.

(6) 컨텐츠 배포 및 홍보가 용이하도록 하며, 이용자 관리 등 다양한 기능을 제공해야 한다.

- 전자화폐의 요구 사항 중에서 양도성(Transferability)에 해당할 수 있다. 전자화폐는 다른 사람에게 이전할 수 있어야 한다.

다른 사용자에게 복사 권한을 가지고 있는 사용자가 쉽게 복사해 줄 수 있어야 한다.

3. DRM 모델에 대한 연구 동향

DRM은 여러 가지 기술들이 조합되어 이루어진 커다란 개념이며 저작권 '관리기술'과 저작권 '보호기술'로 구별될 수 있다.

저작권 관리 기술은 범세계적으로 통일된 일련의 디지털 저작물 관리 체계를 마련하기 위한 것으로, 저작권 관련 단체들을 중심으로 컨텐츠 식별자(DOI: Digital Object Identifier), 컨텐츠 메타데이터(INDECS: INteroperability of Data in E-Commerce System), 컨텐츠 권리명세언어와 같은 기술 표준화 작업이 진행 중이며, 관련 제품들도 출시되고 있다.

저작권 보호기술은 관리기술에서 정의하는 일련의 원칙과 시나리오들을 강제화(Enforcement)하는 기술로 이해할 수 있다. 시장에 등장한 대부분의 DRM제품들은 저작권 보호기술을 상품화한 것이며, 주요 업체들은 자사의 솔루션에 표준화 작업이 진행되고 있는 표준 관리기술을 수용하려는 노력을 기울이고 있다. 안전한 저작권 보호기술을 위해 암호요소기술, 키 분배 및 관리, TRM(Tamper Resistant Module)과 같은 세부 기술들이 요구된다.

다음은 DRM 전체적인 구성요소와 흐름에 대해 살펴본 후, 기존 제품들에 대한 분석을 통하여 복사에 대한 권한과 복사자에 대한 추적 등 여러 가지 기능을 가지는 DRM 모델을 제안한다.

3.1 DRM 구성 요소

디지털 컨텐츠는 저작자의 창작물로서 생성, 유통/판매, 소비의 단계를 거치게 된다. 디지털 정보를 보호하기 위해서는 위의 매 단계마다 DRM기능을 추가하여야 한다. 생성 및 유통 준비단계에서는 컨텐츠를 암호/보호하는데 필요한 패키지(Package)가, 유통/판매 단계에서는 라이선스 발급과 금융을 각각 담당하는 라이선스와 금융 클리어링하우스가 필요하다. 그리고 소비단계에서는 복호화와 사용권리(Usage Rights)에 따라 재생을 통제하는 DRM Agent가 필요하다. 이와 같은 DRM 주요 구성 요소는 아래 그림 1과 같다. 패키지는 암호화를 통해 컨텐츠를 보호하는 기능을 한다. 컨텐츠에 대한 암호화 시 암호화키와 복호화 키를 생성하여 암호화 키는 컨텐츠를 암호화하는데 사용하며 복호화 키는 암호화된 컨텐츠의 이용을 위해 라이선스는 클리어링하우스로 전달된다.

패키징된 컨텐츠는 유통망(온라인 쇼핑몰, CD, E-mail등)을 통해 금융결재를 마친 구매자에게 전달된다(그림 1의 2, 3 단계 참조). 이 때 구매자는 컨텐츠와 함께 라이선스를 받게 된다(그림 1의 4 단계 참조). 라이선스(Licence)에는 컨텐츠를 사용할 수 있는 권리정보와 암호화된 파일을 풀 수 있는 복호화 키를 담고 있는데 보관되어있는 복호화 키를 이용하

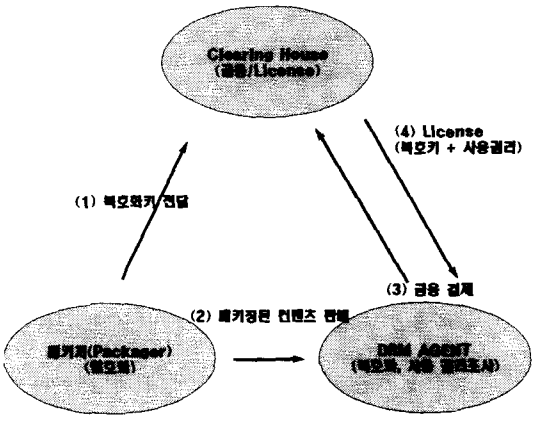


그림 1. DRM 주요 구성 요소

여 컨텐츠의 암호를 풀고, 사용 권리에 의거 컨텐츠를 재생한다.

사용 권리에는 컨텐츠의 사용 횟수, 사용기간, 라이선스 유효기간, 다른 기기에로의 전송, 다른 저장매체로의 이동 등이 있다.

클리어링하우스(Clearing House : 결제 센터)는 금융과 라이선스 클리어링하우스로 나누어지며, 금융 클리어링하우스는 컨텐츠의 상거래(구매/판매/유통)시에 필요한 금융결재 및 이에 연관된 판매금액의 정산에 필요한 작업을 행한다. 라이선스 클리어링하우스는 앞서 언급한 라이선스 발행서버를 가리키는 보다 포괄적인 용어로서, 암호 컨텐츠의 해독에 필요한 라이선스를 발급해 주는 기능을 한다. IMPRIMATUR와 MPEG(Moving Picture Experts Group) 비즈니스 모델에서는 감독 기관(Monitoring Authority)라는 용어를 사용한다[4,5,7,9].

3.2 DRM 흐름

DRM(Digital Rights Management: 디지털 관리 기술) 기술은 디지털 컨텐츠 유통 과정에서 발생하는 에이전트 권리와 신뢰성, 컨텐츠의 안전성 및 재활용성, 유통의 투명성을 보장하는 종합적인 구조로 정의할 수 있다. 그러므로 DRM은 암호화기술, 워터마킹 기술, 변조방지 기술을 포함하고 컨텐츠의 가치사슬(유통에서의 컨텐츠 고유의 특징)을 지원하여야 한다. 또한 저작권자, 컨텐츠 제공자, 소비자 사이에 신뢰를 제공하지만, 근본적으로 요소기술이 아니기 때문에, 특정 시스템이 DRM 체계를 갖추었는지 구별하기 쉽지 않다[12,14,20].

이에 따라 디지털 컨텐츠 상거래 시스템이 DRM 체계를 갖추었는지는 다음과 같은 관점에서 판명할 수 있다.

- 저작권자와 컨텐츠 제공자 사이에서의 상호 신뢰성 지원체계 지원 여부
- 컨텐츠 제공자와 소비자 사이 간 컨텐츠의 안전한 전송과 사용의 보장 여부
- Superdistribution의 지원 여부[1)]

위와 같은 구조를 지원하는 전형적인 형태는 그림 2와 같다.

1) Superdistribution이란 컨텐츠를 타인에게 제공(복사 및 대여)하였을 때, 타인이 합법적으로 해당 컨텐츠를 사용할 수 있게 하는 구조이다.

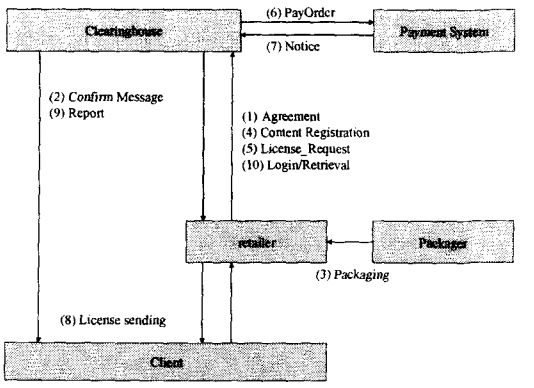


그림 2. 일반적인 DRM 흐름도

- Clearing House: 클리어링하우스, 거래의 투명성을 보장하는 기능을 하는 것으로 retailer가 라이선스 발급을 요청하면, 해당 라이선스를 발급하여 소비자에게 제공한다.
- Packager: 패키지
- Retailer: 컨텐츠 제공자

그림 2를 기반으로 유통 과정을 설명하면 다음과 같다.

(1) 클리어링하우스와 컨텐츠 제공자간에 라이선스 서비스를 계약한다.
(2) 클리어링하우스는 계약의 결과로 패키지를 포함하는 툴을 사용자에게 제공한다.
(3) 컨텐츠 제공자는 DRM 서비스를 하기 위하여 패키지를 이용하여 컨텐츠를 암호화한다.
(4) 패키징 결과 정보를 클리어링하우스에 등록한다.
(5) 컨텐츠 제공자는 컨텐츠를 소비자에게 판매하고, 소비자가 특정 컨텐츠 구매 시 해당 컨텐츠에 대한 위한 라이선스 발급을 클리어링하우스에 요청한다.
(6)~(7) 해당 컨텐츠의 지불 처리를 한다.
(8) 지불 처리가 완료되면 소비자에게 클리어링하우스는 라이선스를 제공한다.
(9) 클리어링하우스는 주기적으로 발급한 라이선스에 대한 정보를 유통 업자에게 제공한다.
(10) 필요시 유통업자는 거래 정보의 자세한 것을 클리어링하우스에 들어와서 볼 수 있다.

위와 같은 클리어링하우스와 유통업자가 분리된

DRM 모델에서는 유통업자의 판매 내역을 클리어링 하우스가 가지고 있어 거래 내역을 속일 수 없기 때문에 저작권자와 유통업자간에 신뢰성을 제공할 수 있다.

3.3 기존 방식

디지털 컨텐츠 유통 시장에 필수적 인프라인 DRM 기술은 현재 저작권을 가진 컨텐츠 소유자와 무료로 사용하기를 원하는 인터넷 사용자로 인해 더딘 진행을 보이고 있다. 초기 한국의 DRM 업체들은 인터넷 유료화 시장을 목표로 했으나, 별다른 성과를 못 내고 최근에는 전자메일, 전자문서, 소프트웨어 유통 등 다양한 시장으로 제품을 개발하고 있다. 또한 사업 모델로서는 판매 방식 측면에서 기존의 솔루션 판매 방식과 DRM ASP서비스 모델을 채택하고 있다[20-24].

DRM 전체 운용과정에는 2가지 방식이 있다. 운용 방식 측면에서는 라이선스 서버만 운용하는 사업모델과 라이선스 서버와 빌링시스템을 연동한 과금시스템(Financial Clearing House)을 운용하는 사업모델을 선보이고 있다. 표 1은 기존 업체에 특징 및 장점에 대해 설명하고 있다.

국내 DRM 솔루션의 종류는 크게 3가지로 인터트러스트(Intertrust) 기반 솔루션, MS 기반 솔루션, 그리고 국내 독자 개발 솔루션으로 분류할 수 있다.

첫째로 인터트러스트 솔루션을 채택하고 있는 회사로는 P사와 T사가 있는데, P사는 인터트러스트사에서 제공되는 API를 이용하여 다단계 보안 알고리즘을 채용한 E-Book, A/V(Audio/Video) 컨텐츠 솔루션과 과금시스템(Financial Clearing House)을 통한 유통 과금 처리 서비스를 제공한다. 그리고 T사는 기업을 대상으로 문서 보안 및 전자메일 솔루션을 제공하며 라이선스 서버만 운영한다. E-Book, 오디오, 비디오, 이미지 등 각각의 미디어마다 별도의 전용 클라이언트 S/W를 추가로 설치해야 한다.

둘째로 MS 기반 DRM 솔루션을 제공하는 회사로는 D사가 있는데, 소규모 A/V 엔터테인먼트 시장에 컨텐츠 솔루션을 제공하고 암호화된 컨텐츠에 대해 라이선스 인증을 해주는 라이선스 서버를 통해 수수료를 받고 있지만, 아직 라이선스와 연동된 과금시스템을 제공하지 못하고 있다.

이 솔루션은 MS의 WM(Window Media) Player를 클라이언트 S/W로 사용하므로 A/V 컨텐츠에 대해 별도의 S/W가 필요 없으나, E-Book에 대해서는 전용의 클라이언트 S/W가 필요하다.

셋째로 국내 자체 개발 DRM 솔루션 업체들은 워터마킹 기술을 기반으로 DRM 솔루션을 제공하는 M사 등의 업체와 암호전문업체로서 PKI(Public Key Infrastructure)기반 DRM 솔루션을 제공하는 C사와 같은 업체들이 있다.

4. 제안 방식

본 논문에서 제안하고 있는 방식은 전자화폐 시스템에서 요구하는 기본적인 기능을 DRM에서 요구하는 기능에 적용하였으며, 컨텐츠의 사용자를 추적할 수 있고 익명으로 제공된 컨텐츠에 대하여 익명성을 취소할 수 있는 부가 기능을 가지고 있다. 본 제안

표 1. 기존 방식 특징 및 장단점

업 체 명	특징 및 장단점
P사	· InterTrust DRM의 다단계 암호화 이용(Contents 암호화, 키 암호화) · 이미지, 동영상, 오디오용 독립 플레이어 필요
T사	· InterTrust DRM의 다단계 암호화 이용(Contents 암호화, 키 암호화) · Secure Doc, Secure E-mail 제품 중심
D사	· 소규모 솔루션 개발(Movie-On 서비스 참여) · WM Player 사용
C사	· PKI 방식 지원 · 인증서 방식의 접근 제어 · 독자적인 Player 제공(지속적인 upgrade 필요) · PDF, HTML, MP3, MPEG, AVI, FLASH등 모든 멀티미디어 컨텐츠를 지원가능
M사	· 워터마킹 기술을 기반 · User의 컨텐츠, 관리 툴인 AnyCap으로 미디어에 맞는 플레이어 선택 구동 · DRM SI 제공

방식에서 적용되는 암호화는 컨텐츠 전체에 행하여지는 것이 아니라 컨텐츠에 일부분에 적용하여 암호화를 진행한다. 이는 파일 전체에 하는 것이 효율성 측면에서 보다 좋은 장점을 나타내기 때문이다. 먼저 각 개체는 RSA 알고리즘을 이용하여 키를 생성하며, 해쉬 함수에 기반한 계층적 구조 테이블(Hierarchical Structure Table)을 이용한 컨텐츠에 대한 복사 권한, Schnorr의 인증 기법을 이용한 복사 권한이 없는 컨텐츠에 대한 이중 사용(Double Spending) 방지와 컨텐츠에 대한 불법 사용 시 사용자 신원 노출 등의 특성을 만족시켜 주고 있다[1,17]. 또한 이산대수 문제를 이용한 개개의 복사된 컨텐츠에 대한 추적 기능과 ElGamal 암호 기법을 이용한 사용자 추적(Owner Tracing) 기능을 제공하여 사용자의 익명성을 조절함으로써 컨텐츠 자체에 대한 불법적인 중복 사용을 방지해 주고 있다. 그리고 클리어링하우스에서의 라이선스 발행 시 컨텐츠 제공자와 사용자 인증을 위해 변형된 S/Key one-time password 방식을 사용함으로서 라이선스가 단일 항으로 구성되게 하고 있다.

그림 3은 제안 방식의 전체적인 흐름을 보여주는 그림이다. 각 단계별로 보면 컨텐츠 분배까지 총 5단계가 있으며, 후에 불법적인 사용에 대한 추적 단계가 포함된다. 우선 사용자는 클리어링하우스에서 라이선스를 발급받는다. 이때 클리어링하우스와 서비스 제공자는 라이선스를 공유한다. 라이선스를 공유하는 이유는 서비스 제공자에게 요청하는 사용자가 정당한 사용자인지 확인하게 되며, 서비스 제공자는 라이선스를 이용하여 컨텐츠와 제공함으로써 후에 불법적인 사용이 있으면 불법 컨텐츠로부터 라이선스를 추출하여 불법적인 사용자를 추적할 수 있기 때문이다. 다음 사용자는 라이선스를 발급받은 후에 컨텐츠 패키지를 요청하고 서비스 제공자로부터 패키지를 발행받는다. 발행받은 컨텐츠 패키지는 클리어링하우스에서 발급받은 라이선스를 이용하여 컨텐츠를 사용하게 된다. 불법적인 사용 혹은 복제에 악용되어 컨텐츠가 유포되면 서비스 제공자는 사용자 추적을 Trustee에 요청하게 된다. 이때 컨텐츠 및 불법 컨텐츠를 제공함으로써 클리어링하우스로부터 제공받은 정보를 이용하여 사용자 추적 및 선별할 수 있게 된다.

4.1 계층적 구조 테이블

본 방식에서는 컨텐츠의 복사 권한 제어를 위해 여러 가지 기능들 중에서 복사 권한성을 만족시켜 주기 위해 계층적 구조 테이블을 사용하고 있다. 이

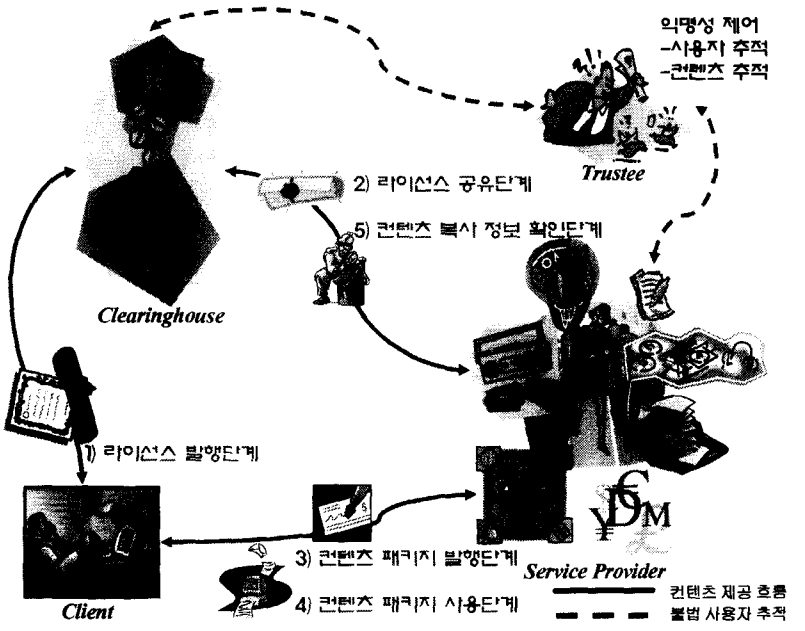


그림 3. 전체 흐름도

테이블에 의해 클라이언트는 컨텐츠 제공자로부터 제공받은 컨텐츠를 원하는 복사 횟수만큼 분할하여 사용할 수 있으며 사용된 컨텐츠들의 복사 횟수 합은 초기에 컨텐츠 제공자로부터 받은 복사 횟수와 동일하게 된다[18].

계층적 구조 테이블은 트리구조를 가지고 있고 복사 권한 정보에 해당하는 각 노드는 다음과 같은 규칙을 가진다.

a. 노드 N에 있어서 해당 복사 횟수는 자식 노드들의 합과 같다.
b. 어떤 한 노드가 사용되면, 모든 자식 노드와 부모 노드는 사용할 수 없다.
c. 어떤 노드도 한 번 이상 사용될 수 없다.

그림 4는 복사 횟수와 각 노드 값들에 대한 트리구조를 나타내고 있으며 컨텐츠 제공자로부터 받은 컨텐츠 복사 횟수 N은 루트 노드 V_{i0}에 해당한다. 루트 노드는 다시 두 개의 *Subnode*($=V_{i00}, V_{i01}$)로 나뉘게 된다. 또한 사용자가 원하는 만큼의 복사 횟수를 가질 수 있는데 이것은 사용자가 복사를 원하는 횟수의 선택에 따라 달라진다. 나눠진 자식 노드의 합은 루트노드(V_{i0})와 같게 된다. *Subnode*는 두 개의 해쉬 함수 f_1과 f_2를 사용하는데 왼쪽 노드는 f_1을 사용하고 오른쪽 노드는 f_2를 사용하여 트리를 구성한다. 각 노드의 값은 다음과 같이 상위 노드를 이용하여 하위 노드를 계산해 낸다.

$$V_{i0} = N$$
$$V_{i00} \equiv V_{i0} \cdot f_1(V_{i0} \| n) \bmod p,$$
$$V_{i01} \equiv V_{i0} \cdot f_2(V_{i0} \| V_{i0} - n) \bmod p$$
$$V_{i000} \equiv V_{i00} \cdot f_1(V_{i00} \| n) \bmod p,$$
$$V_{i001} \equiv V_{i00} \cdot f_2(V_{i00} \| V_{i00} - n) \bmod p$$
$$V_{i010} \equiv V_{i01} \cdot f_1(V_{i01} \| n) \bmod p,$$
$$V_{i011} \equiv V_{i01} \cdot f_2(V_{i01} \| V_{i01} - n) \bmod p$$
$$(2 \le n \le V_{i\,MAX} - 1)$$

4.2 시스템 파라메터

다음은 본 방식에서 사용되는 시스템 파라메터에 대해 기술한다. 각 파라메터는 구성요소에 따라 구분하고 있으며 각 구성요소가 생성하고 전달하는 파라메터에 대해 기술하고 있다.

가. 사용자(U)

- p : 사용자가 발생한 소수
- g_1, g_2, g_3 : GF(p)상의 원시원
- (n_u, e_u, d_u) : 사용자의 RSA 파라메터로서, n_u, e_u는 공개키이고 d_u는 비밀키이다.
- ID_u : 사용자가 생성한 식별자로서 클리어링 하우스와 연계되는 값
  $ID_u \equiv g_1^{d_u} \bmod p$
- $S : ID_u \| response \| (H(ID_u \| response))^{d_u} \bmod n_A$,
  $response = E_R(H_N(ID_u))$
- $I \equiv g_1^s \bmod p$
- H, f_1, f_2 : 일방향 해쉬 함수(One-way hash function)로서 H는 라이선스 발행 시 사용되며 f_1과 f_2는 계층적 구조 테이블에서 노드 구성 시 사용된다.
- *CHLC*(Clearing House License Candidate) : 라이선스를 발급 받기 위해 사용자가 생성하

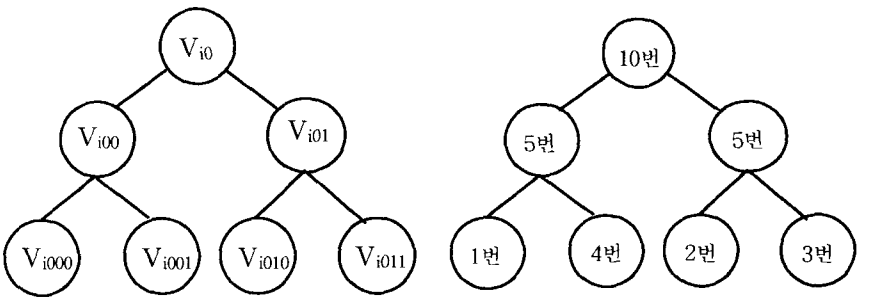


그림 4. 계층적 구조 테이블

여 보내는 라이선스 후보

$CHLC \equiv r_1^{e_B} \cdot H(I \| X_N) \bmod n_B$, 여기서 r_1은 랜덤 하게 선택

나. 클리어링하우스(*CH*) 및 컨텐츠 제공자(*SP*)

- *C*(Contents) : 컨텐츠 인자 - 실제 컨텐츠로 사용자에게 패키지로 전달될 때에는 데이터 부분과 암호화되는 부분으로 구성된다.
- $C = M + D$: 메타 데이터와 실제 데이터
- *CP*(Contents Package) : 컨텐츠 제공자가 생성하는 컨텐츠 인자 *C*를 사용하여 컨텐츠 패키지(*CP*)를 구성한다. $CP = \{ C \| A_1' \| A_2' \| sign_u(C \| A_1' \| A_2') \}$
- (n_B, e_B, d_B) : 클리어링하우스의 라이선스용 RSA 파라메터로서, n_B, e_B는 공개키이고 d_B는 비밀키이다.
- (n_B', e_B', d_B'), (n_B'', e_B'', d_B''), . . . : 클리어링하우스는 각 복사권한에 해당하는 RSA 파라메터를 생성한다. 예를 들어 (n_B', e_B', d_B')은 1번에 해당하고 (n_B'', e_B'', d_B'')는 9번에 해당한다.

다. Trustee(T)

- (D_T, N_T, X_T) : Trustee의 RSA 파라메터로서, D_T, N_T는 공개키이고 X_T는 비밀키이다.
- y_T : 수탁기관의 공개 정보, $y_T \equiv g_2^{X_T} \bmod p$

4.3 라이선스 발행 단계

컨텐츠 패키지를 발행 받기 전에 사용자는 라이선스를 발행 받아야 한다. 이때 라이선스는 라이선스 서비스 요구 시에 발급 받아 컨텐츠 패키지 발급 시 인자로서 사용하며 사용자가 원하면 새로운 라이선스를 발행 받아 사용할 수 있다. 라이선스 발행 단계에서는 변형된 S/Key one-time password를 사용하여 클리어링하우스와 사용자측이 상호 인증을 하게 되며 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다. 또한 제안 방식에서의 라이선스는 단일메시지로 구성된다.

사용자와 클리어링하우스는 상호 인증을 위한 초기화 단계를 수행한다. 먼저 사용자와 클리어링하우스는 해쉬함수를 적용할 횟수 N을 결정한다. 이를 이용하여 서버 측에 저장할 사용자의 비밀 정보를 생성해 낸다.

step 1 : 사용자는 해쉬 함수 H와 ID_u 그리고 N을 선택하고 이를 클리어링하우스에 전송한다.

step 2 : 클리어링하우스는 사용자의 비밀정보 X_{N+1}을 생성하고 X_{N+1}과 $N+1$만을 저장한다.

$X_1 = H(ID_u)$, $X_2 = H(X_1)$, ..., $X_{N+1} = H(X_N)$

step 3 : 클리어링하우스는 난수 R을 통하여 *challenge* 값을 생성하여 사용자에게 전송한다.

$challenge = (N \| R \oplus X_{N+1} \| E_R(X_{N+1}))$

step 4 : 사용자는 $H_N(ID_u)$와 $H_{N+1}(ID_u)$ 그리고 R'을 계산하고 클리어링하우스 인증 과정을 수행한다.

$R' = (H_{N+1}(ID_u) \oplus R \oplus X_{N+1})$

$D_{R'}(E_R(X_{N+1})) \stackrel{?}{\equiv} H_{N+1}(ID_u)$

클리어링하우스의 인증 과정이 성립되면 *response*, *S*, *I*와 라이선스 후보 *CHLC* 값을 계산하여 *I*값은 공개하고 *response*와 *CHLC*를 클리어링하우스에 전송한다.

step 5 : 클리어링하우스는 사용자 인증 과정을 수행하고 사용자 관련 저장 정보를 $N+1$에서 N으로, X_{N+1}을 $X_N = H_N(p)$로 갱신한다. 그리고 *CHLC*에 클리어링하우스의 서명을 하여 사용자에게 전송한다.

$D_{R'}(E_{R'}(H_N(ID_u)) \stackrel{?}{\equiv} H_N(ID_u)$

$H(H_N(ID_u)) \stackrel{?}{\equiv} X_{N+1}(ID_u)$

step 6 : 사용자는 클리어링하우스가 서명한 *CHLC*로부터 라이선스 *CHL*을 추출한다.

$CHL \equiv [r_1 \cdot H(I \| X_N)^{d_B} \bmod n_B] / r_1$

$\equiv H(I \| X_N)^{d_B} \bmod n_B$

4.4 컨텐츠 패키지 발행 단계

클리어링하우스가 발행한 라이선스를 이용하여 컨텐츠 제공자로부터 컨텐츠 패키지를 발행 받는 과정이다. 컨텐츠 패키지를 발행 받는 동안에 컨텐츠를 추적할 수 있는 인자 A_1'이 생성되며 이 A_1'은 컨텐츠 추적 단계에서 trustee를 거치면서 컨텐츠 추적을

위해 사용된다.

step 1 : 사용자는 $v \in 1, \ldots, p-1$ 을 랜덤 하게 선택하고 A_1'과 A_2'를 생성하여 컨텐츠 제공자에게 전송한다.

$$A_1' \equiv y_T^v \bmod p,\ A_2' \equiv Ig_2 g_3^{v^{-1}} \bmod p$$

step 2 : 컨텐츠 제공자는 A_1', A_2'를 올바르게 생성하였는지 확인한 뒤 $w \in 1, \ldots, p-1$ 을 랜덤 하게 선택하여 사용자에게 전송한다.

$$\log_{g_3}(A_2'/Ig_2) \stackrel{?}{\equiv} \log_{A_1' y_T}$$

step 3 : 사용자는 랜덤 넘버 b를 선택하여 Z를 계산한다. 또한 r'값을 계산하여 Z와 함께 컨텐츠 제공자에게 전송한다. 이때 r_2는 랜덤한 정수이며 사용자가 컨텐츠 패키지를 전송 받기 위해 생성한 데이터를 은닉시킨다.

$$Z \equiv r_2^{e_B'} \cdot H(CHL \| b) \bmod n_B',\ r' \equiv Zw + v \bmod p$$

step 4 : 컨텐츠 제공자는 Z에 서명을 해 주기 전에 Z가 사용자 A에 의해 올바르게 생성되었는지 확인한 후, Z에 서명한 값 Z'을 사용자에게 전송한다.

$$g_2^{r'} \stackrel{?}{\equiv} (a')^Z \cdot (A_1')^{X_T^{-1}}$$

$$Z' \equiv Z^{d_B'} \equiv (r_2^{e_B'} \cdot H(CHL \| b) \bmod n_B')^{d_B'}$$

$$\equiv r_2 \cdot (H(CHL \| b))^{d_B'} \bmod n_B'$$

(단, $a' \equiv g_2^w \bmod p$)

step 5 : 사용자는 Z'으로부터 C를 추출해 낸다.

$$C \equiv Z'/r_2$$

$$\equiv (H(CHL \| b))^{d_B'} \bmod n_B'$$

이때, 실제 컨텐츠 패키지(CP)는 $\{C \| A_1' \| A_2' \| sign_u(C \| A_1' \| A_2')\}$으로 구성되어 있다.

4.5 컨텐츠 패키지 사용 단계

컨텐츠 패키지 사용 단계로서 컨텐츠 제공자로부터 컨텐츠를 제공받은 후 사용자는 클리어링하우스로부터 생성된 라이선스와 계층적 구조 테이블을 이용하여 컨텐츠 제공자에게 원하는 사용횟수를 알려준다. 즉 10번 중 9번을 사용하기 원한다면 노드 값 V_{i00}을 계산하고 이와 관련된 Y_{i00}을 계산하여 컨텐츠 제공자에 전송함으로써 컨텐츠 패키지에 대한 유효성을 검사한다.

step 1 : 사용자는 컨텐츠를 사용하기 원하는 복사에 대한 노드 값(V_{i00}, n)과 (X_{i00})를 계산한 뒤 CP, CHL, A, A_1, A_2, (A_3)와 함께 컨텐츠 제공자에 전송한다.

$$A \equiv (A_2')^v \bmod p,\ A_1 \equiv g_2^v \bmod p,\ A_2 \equiv g_1^{ts} \bmod p$$

$$V_{i00} \equiv V_{i0} \cdot f_1(V_{i0} \| n) \bmod p$$

$$X_{00} = g_1^{V_{i00}} \bmod p$$

step 2 : 컨텐츠 제공자는 컨텐츠 패키지 CP에 있는 사용자 서명을 확인한 뒤 V_{i00}과 A, A_1, A_2를 확인한다.

$$V_{i00} \stackrel{?}{\equiv} V_{i0} \cdot f_1(V_{i0} \| n) \bmod p$$

$$A \stackrel{?}{\equiv} A_1 \cdot A_2 \cdot g_3 \bmod p$$

그리고 나서 난수 $R_{i00} \in 1, \ldots, p-2$를 생성하여 사용자에게 전송한다.

step 3 : R_{i00}을 이용하여 사용자는 다음의 Y_{i00}를 계산하여 컨텐츠 제공자에게 전송한다.

$$Y_{i00} \equiv V_{i00} + R_{i00} \cdot S \bmod p-1$$

step 4 : 컨텐츠 제공자는 Y_{i00}에 대한 다음 식이 성립하는지 확인하여, 만족하면 V_{i00}를 인증하여 컨텐츠 복사에 대한 권한 9번을 받아들인다.

$$g_1^{Y_{i00}} \equiv X_{i00} \cdot (I)^{R_{i00}} \bmod p$$

4.6 컨텐츠 복사 정보 확인 단계

사용자가 사용한 컨텐츠 패키지 CP를 전송하기 위해서 컨텐츠 제공자는 복사 권한 확인서를 클리어링하우스에 전송한다. 클리어링하우스가 H를 전송받으면 컨텐츠 패키지 및 라이선스의 유효성을 확인하고 클리어링하우스의 DB를 이용하여 복사 여부를 확인한다.

$$H = I,\ p,\ g_1,\ g_2,\ g_3,\ V_{i00}$$

$$R_{i00},\ Y_{i00},\ O_A(=(A_1, A_3)),\ CHL,\ CP$$

이때, O_A는 사용자 및 컨텐츠 추적인자 A_1, A_3로 구성된 데이터로서 선택적으로 사용할 수 있다.

5. 제안 방식의 고찰

5.1 컨텐츠 복사 권한에 대한 안전성

컨텐츠 패키지는 디지털 데이터가 가지는 특징으

로 인해 대량으로 복사가 가능하기 때문에 이를 방지하기 위한 대책이 수립되어 있어야 한다. 이를 위해 본 제안 방식에서는 계층적 구조 테이블을 구성하기 위해 필요한 규칙들을 만족시키고 있다.

같은 컨텐츠의 이중 사용에 관한 해결책으로는 중복 사용된 같은 노드를 컨텐츠 제공자에 사용하였을 경우, 컨텐츠 제공자에서는 즉시 이중 사용 여부를 검출할 수 있어야 한다. 즉 V_{i00}이 두 번 사용되었을 경우 Y_{i00}과 Y_{i00}'으로부터 사용자의 ID_u를 검출 할 수 있어야 한다.

컨텐츠 제공자는 사용자가 보내온 V_{i00}, Y_{i00}, Y_{i00}', X_{i00}, X_{i00}'으로부터

$$Y_{i00} - Y_{i00}' \equiv (R_{i00} - R_{i00}') \cdot S \bmod p - 1$$

$$\therefore S \equiv (Y_{i00} - Y_{i00}')/(R_{i00} - R_{i00}') \bmod p - 1$$

위의 수식과 같이 S가 구해지고 이로부터 ID_u가 구해진다.

5.2 익명성 제어

익명성 제어는 익명성 조절 파라메터에 의해 제공되며 선택적으로 익명성을 취소할 수 있다. 즉, 어떠한 전자화폐의 익명성은 취소가 되고 어떠한 컨텐츠 패키지들은 계속해서 익명성을 유지시킬 수가 있다는 것을 의미한다. 익명성 취소는 크게 두 개의 모델로 구분해 볼 수가 있는데, 하나는 컨텐츠 패키지의 소유자를 식별하는 소유자 추적(Owner Tracing)과 클리어링하우스로부터의 컨텐츠 불법 복사를 제어하기 위한 불법 복사 컨텐츠 추적이 있을 수 있다. 소유자 추적에 있어서 익명성 제어 파라메터는 trustee가 컨텐츠에 대한 사용이 이루어지고 난 후, 컨텐츠의 소유자를 판별해 낼 수 있도록 해준다.

가. 불법 사용에 대한 컨텐츠 추적

컨텐츠 추적 기능을 통해 사용자가 컨텐츠 패키지를 사용하기 전에 trustee에 의해 컨텐츠 제공자에 추적 기능을 부여 할 수가 있다. 즉, 컨텐츠 패키지 발행 단계에서 사용자가 컨텐츠 제공자에 전송한 복사 권한 사본 중 A_1'으로부터 trustee는 A_1을 생성하고 이를 컨텐츠 제공자에 재전송해 줌으로써 컨텐츠 제공자 측에서는 사용한 컨텐츠를 확인하고 복사할 수 있는 컨텐츠와 복사 가능한 컨텐츠를 연결함으로써 컨텐츠 자체에 대해 추적할 수가 있다. 컨텐츠 패키지 발행 단계에서는 다음 과정을 수행시킴으로서 컨텐츠 추적 기능을 제공한다.

step 1 : 컨텐츠 제공자는 사용자가 제시한 복사 권한 사본 중 A_1'을 trustee에게 제공한다.

step 2 : trustee는 A_1'로부터 A_1을 계산해낸다.

$$(A_1')^{X_T^{-1}} \equiv (y_T^v)^{x_T^{-1}}$$

$$\equiv g_2^{X_T \cdot v \cdot X_T^{-1}} \equiv g_2^v \equiv A_1$$

step 3 : trustee는 A_1을 컨텐츠 제공자에게 전송한다.

이때 trustee가 전송해 준 A_1을 사용자가 생성하여 컨텐츠 사용 단계에서 컨텐츠 제공자에 제공하는 A_1과 연결시킨다.

나. 사용자 추적

사용자 추적 단계는 컨텐츠 사용이이 이루어지고 난 후에 사용자를 판별하는 방법으로서 합법적인 컨텐츠에 대한 제공이 이루어지고 난 후에 추적을 가능케 한다. 이는 컨텐츠의 부정사용에 관련된 것들에 기반하기보다는 사용자가 구입한 물품들에 대한 혐의가 주어질 경우에 그 컨텐츠의 사용자를 추적하게 된다. 이 단계는 컨텐츠 복사 정보 확인 단계에 추가하여 구성되며 사용자가 컨텐츠 제공자에 상점에 컨텐츠 패키지 사용 시 $A_3(= ID_u \cdot (y_T)^v \bmod p)$이 추가된다.

step 1 : 클리어링하우스는 컨텐츠 제공자가 복사 권한 확인서로부터 A_3을 trustee에 전송한다.

step 2 : trustee는 A_3로부터 $A_3' \equiv ID_u^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하여 클리어링하우스에 전송한다.

$$A_3' \equiv A_3^{X_T^{-1}} \bmod p$$

$$\equiv ID_u^{X_T^{-1}} \cdot g_2^v \bmod p$$

step 3 : 클리어링하우스는 trustee가 전송한 A_3'로부터 ID_u를 계산해 낸다.

$$A_3'/A_2 \bmod p \equiv ID_u^{X_T^{-1}} \cdot g_2^v/g_2^v \bmod p$$

$$\equiv ID_u^{X_T^{-1}} \bmod p$$

$$\therefore \quad ID_u = (ID_u^{X_T^{-1}})^{D_T^{-1}} \bmod p$$

5.3 비교분석

본 절에서는 제안한 방식과 기존 시스템과의 비교

분석하여 평가한다.

표 2에서 제안한 방식과 기존의 시스템의 성능을 비교 분석한 것이다. 기존의 몇몇 시스템은 MP3의 불법복사는 막을 수 있지만 정식으로 구매한 사용자가 악의적으로 MP3 데이터나 키를 유포할 시에 방지할 수 있는 대책이 미비하였다. 하지만 제안한 시스템에서는 컨텐츠가 제 3자에게 배포 시에 Agent와 CP Front- Middle Server의 키 값이 포함되도록 하고 있다. 또한 Hidden Agent 내부적으로 생성되는 R값이 있기 때문에 MP3 데이터의 불법 유통을 방지할 수 있다.

기존의 시스템인 P사, D사와 M사의 경우 독립적인 플레이어를 사용함으로써 무선으로의 확장이 어려울 뿐만 아니라 여러 단계의 암호화로 인해 원본 컨텐츠에 대한 강건성이 떨어질 수 있다.

또한 본 방식에서는 Agent를 이용하여 복사에 대한 권한만 제한하고 있지만 기존 시스템에서는 매 컨텐츠에 대하여 인증을 통과해야만 컨텐츠에 대한 플레이가 가능하다. 처음 컨텐츠에 대한 구입 완료 후에 매번 사용자 인증을 받아야 함으로써 사용자에게 많은 불편을 줄 수 있다. 하지만 제안한 방식은 단지 복사와 이동명령에 대한 제한을 하고 있기 때문에 사용자는 일반적인 컨텐츠를 사용하는 방식과 같이 사용할 수 있다.

각 항목에 대하여 자세히 살펴보면 컨텐츠 불법 유통 방지에 대해 본 방식에서는 사용자가 발생한 값과 이를 바탕으로 클리어링하우스에서 발급되는 라이선스를 가지고 있고 최종적으로 컨텐츠 제공자의 값을 포함하고 사용자에게 제공되기 때문에 3개체의 모든 값을 아는 사용자만이 컨텐츠에 대한 접근을 허용하게 되므로 컨텐츠의 불법 유통을 방지할 수 있다.

컨텐츠 전송 시 노출 위험은 기존방식에서는 컨텐츠 전체를 암호화하는 방식이거나 컨텐츠는 그대로 전송되고 플레이어에서 컨텐츠에 대한 라이선스를 확인하는 방식을 취하고 있기 때문에 전송로 상에서 컨텐츠 취득시 이용하여 원본 컨텐츠를 획득할 수 있었다. 하지만 제안 방식에서는 컨텐츠 전체에 대한 암호화가 아니가 컨텐츠의 헤더 부분에 대하여 암호화하여 전송하기 때문에 전송되는 데이터를 취득한다하더라도 데이터 헤더 부분을 획득하지 못함으로 전송로 상에서도 안전하게 컨텐츠를 유통시킬 수 있다.

본 제안 방식은 헤더를 통한 암호화로 컨텐츠 이동의 어려움을 제거하였고 이로써 나타날 수 있는 문제점은 최초 컨텐츠 제공시 사용자가 획득하게 되는 복사 권한을 제한하도록 함으로써 해결하였다. 컨텐츠가 복사된다 할지라도 복사 권한을 불법 사용자 임의로 제어하지 못하게 됨으로 인해 사용자의 컨텐츠에서 권한이 제외된 컨텐츠를 획득할 수 없도록 하고 있다.

이중 사용 방지에 대해 기존 방식에서는 컨텐츠가 유통된 후에 사용자가 컨텐츠를 획득하여 컨텐츠 원본을 추출한 뒤 유통한다 해도 사용에 대한 권한은 사용자에게 있으므로 이중 사용이 가능하였다. 그러나 제안방식에서는 최초 컨텐츠를 받기 전에 사용 횟수를 제한하고 사용이 있을 때마다 접속하여 자신의 사용횟수를 줄이면서 사용하거나 최초 컨텐츠 내부에 있는 횟수를 줄이면서 사용하기 때문에 자신의 사용횟수를 모두 사용하게 되면 이후에는 복제가 이뤄질 수 없도록 되어있다.

익명성 제공에서 본 방식은 사용자의 정보를 컨텐츠 제공자에게 제공하지 않다가 불법적인 사용이 발생하게 되면 Trustee와 함께 사용자의 정보를 밝히

표 2. 제안 방식과 기존 시스템 비교 분석 (○: 가능, ×: 불가능)

비교항목 / 각 방식	컨텐츠 불법 유통 방지	컨텐츠 전송 시 노출 방지 기능	이중사용방지	익명성 제공
P사	×	○	×	×
T사	○	○	×	×
D사	○	×	×	×
C사	×	○	×	×
M사	×	×	×	×
제안 방식	○	○	○	○

게 되어 있는 구조이므로 정상적인 사용자의 정보는 알 수 없다. 독립 플레이어 사용에 대한 부분은 일부 기존 방식의 경우에는 제공하는 플레이어를 사용하여야만 컨텐츠를 획득할 수 있는데 반해 제안방식의 경우에는 다른 플레이어가 없다하더라도 기존 플레이어에서 실행되는 구조가 되도록 설계하였다.

6. 결 론

현재 DRM에 관하여 많은 연구가 진행 중에 있다. 컨텐츠 제공 및 유통 흐름 모델에서 유통과 관리부분 중 컨텐츠에 대한 보호는 전체 모델에서 가장 핵심적인 부분이라 할 수 있다.

본 논문은 전자화폐 기능을 이용하여 새로운 DRM 모델을 제시하였다. 컨텐츠 복사권한에 대한 안전성은 복사에 대해 이중 사용 및 다른 노드의 사용을 막음으로써 불법적인 컨텐츠 복사를 방지할 수 있다. 불법적인 복사가 이뤄진다 하더라도 라이선스 발행 시 혹은 컨텐츠 패키지 발행 시에 사용자 추적/컨텐츠 추적인자를 삽입함으로써 개개인에 의해 발생될 수 있는 불법 복제를 방지할 수 있다.

또한 본 논문에서 제시하고 있는 시스템은 익명 사용자를 대상으로 컨텐츠를 배포할 수 있기 때문에 구매자의 익명성을 보장해 줄 수 있다. 실제적으로 구매자들이 자신의 프라이버시를 보호받으며 컨텐츠를 구입할 수 있으므로 컨텐츠에 대한 수요를 증대시킬 수 있다.

향후 연구 과제로는 원본 컨텐츠에 대한 소유권과 지불을 적용한 방식을 위한 컨텐츠 제공 등을 포함하여야 할 것으로 본다.

이러한 DRM 기술이 언예/오락용 디지털 컨텐츠의 온라인 판매뿐만 아니라 CD 등의 오프라인 매체로 판매되는 현재의 소프트웨어 유통체계에도 많은 변화를 가지고 올 것이다.

참 고 문 헌

[1] B. von Solms and D. Naccache, "On blind signatures and perfect crimes", Computers and Security, Vol. 11, No. 6, pp581-583, 1992.

[2] C. P. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, Vol. 4, No. 3, 161-174, 1991.

[3] Hohl F., 1998, "Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts", In: G. Vigna(Ed.), Mobile Agents and Security, Springer-Verlag, Lecture Note in Computer Science 1419, pp 137-153.

[4] ISMA Report, "Internet Streaming Media Alliance DRM Task Force Report," IRTF-IDRM.52' IETF meeting, October 2001.

[5] kiyoshi Yamanaka, Hitoshi Shibagaki, Norihigo Sakurai, and Terunao Soneoka, "Trend of Digital Copyright Protection Technologies," NTT R&D Vol. 47, No. 6, 1998.

[6] kiyoshi Yamanaka, Hitoshi Shibagaki, Norihigo Sakurai, and Terunao Soneoka, "Infoket-I (Infoket-I: an Information Distribution Platform on the Internet," NTT R&D Vol. 46, No. 2, 1997.

[7] Mark Bauger, "Internet Digital Rights Management Taxonomy," IETF-51 August 6, 2001.

[8] M.Stadler, J.M.Piveteau and J.Camenisch, "Fair blind signatures", In Advances in Cryptology, Eurocrypto '95, LNCS 921, pp209-219, 1995.

[9] Paul, John D., Butler W., "Digital Rights Management Operating System," United State Patent 6,330,670, December 11, 2001, http://cryptome.org/ms-drm-os.htm

[10] Vigna A., 1998, "Cryptographic traces for Mobile Agents," In: G. Vigna (Ed.), Mobile Agents and Security, Springer-Verlag, Lecture Note in Computer Science 1419, pp 99-113.

[11] Sander T. & Tschudin, 1997, "Toward Mobile Cryptography", International Computer Security Institute (ICSI), TR-97-049.

[12] 박남제, 송유진, "디지털 컨텐츠 저작권 보호기술", 한국정보보호학회지, 제 11권 제 5호, pp1-17, 2002. 10.

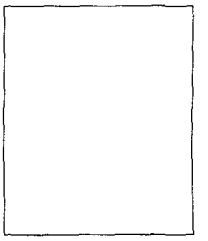
[13] 이창열, "DRM 기술", 한국정보보호학회지, 제 12권 제 1호, pp1-10, 2002. 2.

[14] 이형우, "안전한 컨텐츠 유통을 위한 방안 연구", 제 12권 제 1호, pp48-54, 2002. 2.
[15] 여상수, 윤훈기, 김성권, "디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅의 연구동향", 한국정보보호학회지, 제 11권 3호, pp90-99.
[16] 이덕규, 오형근, 이임영, "지불정보를 이용한 Hidden Agent 컨텐츠 불법 복사 방지에 관한 연구", 02' 한국멀티미디어학회 춘계학술대회, pp947-950, 2002. 5.
[17] 김기현, 은유진, 박정호, 고승철, "변형 일회용 패스워드 시스템 제안", 제 10회 정보보호와 암호에 관한 학술 대회, pp75-92, 1998.
[18] 오형근, 이임영, "새로운 추적 가능한 전자화폐 프로토콜에 관한 연구", '98, 한국정보과학회 추계학술발표회 논문집(III), pp344-pp346, 1998.
[19] 이덕규, 이임영, "Agent 기반 불법 복제 방지 DRM모델", 한국정보과학회 추계학술대회, 2001.
[20] 김종안, 임태영, 한평희, 이상홍, "국내외 DRM 솔루션 및 비즈니스 현황과 MS-DRM에 관한 연구", 한국통신 정보통신 연구, 15권, 3호, pp36-42, 2001. 9.
[21] IntertrustTM Corporation http://www.intertrust.com
[22] Markany Co. http://www.markany.com
[23] DreamInTech co. http://www.dreamintech.co.kr
[24] DigiMarc. http://www.digimac.com

이 덕 규

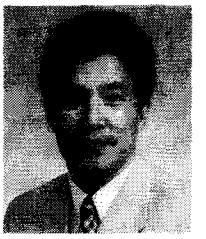
2001년 2월 순천향대학교 컴퓨터공학과 졸업
2003년 2월 순천향대학교 전산학과 석사
2003년 3월~현재 순천향대학교 전산학과 박사과정

관심분야 : Broadcast Encryption, DRM, EKE



오 형 근

2000년 2월 순천향대학교 전산학과 석사
2000년 2월~2000년 8월 한국사이버페이먼트(KCP) 선임연구원
2000년 8월~현재 국가보안기술연구소 선임연구원
2003년 9월 고려대학교 정보보호대학원 박사과정
관심분야 : 전자화폐, 악성코드, 관제시스템



이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학전공 석사
1989년 3월 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안