전자화폐 시스템을 적용한 DRM 모델에 관한 연구

이덕규[0]
순천향대학교 정보기술공학부
hbrhcdbr@catholic.or.kr[0]

오형근
국가보안기술연구소
hgoh@etri.re.kr

이임영
순천향대학교 정보기술공학부
imylee@sch.ac.kr

A Study on DRM Model using Electronic Cash System

Deok-Gyu Lee[0]
Soonchunhyang University
Division of Information Engineering

Hyung-Gn Oh
National Security
Research Institute

Im-Yeong Lee
Soonchunhyang University
Division of Information Engineering

요 약

전자상거래에서 중요한 지불 수단으로서 전자화폐 시스템이 있다. 이러한 전자화폐의 요구사항을 살펴보면 독립성, 양도성, 분할성 등이 요구된다. 각각은 컨텐츠를 제공하는데 있어 DRM에서 필요한 요구사항이 된다. 컨텐츠 자체가 금전적 개념으로 볼 수 있기 때문이다. 컨텐츠 자체에 대한 복제 및 복사, 익명사용자등 여러 관계에서 동일하게 적용시킬 수 있다. 본 논문에서는 이러한 의미를 가지고 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. 또한 사용자로 하여금 원하는 복사의 수만큼 복사할 수 있는 권한을 제공함으로써 사용하기에 편리하도록 하였다.

1. 서 론

전자 상거래를 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 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. 하지만 컨텐츠를 제작하는 과정에서보다는 컨텐츠를 제공하고, 유통시키는 과정에서 불법적인 복사가 일어날 수 있으므로 컨텐츠를 유통과정에서의 보안에 대해 살펴봄으로써 좀 더 안전한 DRM 모델을 제시하려 한다.

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.

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.[2]

본 논문에서는 이중에서 디지털 창작물에 대한 유통/서비스 과정에서의 컨텐츠 보호를 제시할 것이다. 유통 혹은 서비스 단계에서 발생할 수 있는 불법복사를 차단함으로써 더 나아가서는 저작권보호 및 사용권 보호를 이룰 수 있을 것으로 사료된다. 전자화폐의 요구사항을 분석하고 이를 통해 DRM 요구사항을 살펴 본 뒤 이를 통해 전자화폐 시스템을 적용한 새로운 모델을 제시하고자 한다. 전자화폐가 갖는 분할성, 이중 사용방지 등 여러 부분들이 DRM의 컨텐츠 제공에 있어 많은 부분 수용할 수 있다. 이미 많은 연구가 진행되어있는 전자화폐 시스템을 이용함으로써 보다 발전적인 방향으로 나아갈 수 있을 것이라 생각된다. 이에 본 고에서는 이전에 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.

이러한 디지털 컨텐츠의 정의에 따른 유통에 있어서 저작권자 권리 보호기술은 다음 기능을 제공하는 것을 목적으로 한다.[1][2][3]

(1) 불법 복제 및 재생을 차단하고, 변경 및 해킹이 불가능한 체계의 저작자가 원하는 사용자와 원하지 않는 사용자를 식별해서, 전자에게만 선택적으로 효용성을 제공한다.

- 이것은 전자화폐의 요구사항에 있어 분할성(Divisibility)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, 수정하는 등의 다양한 조작이 권한에 따라 가능하고 소유 권한에 대한 제어가 가능해야 한다. 뿐만 아니라, 불법 행위의 경우 사용권을 취소하는 기법이 필요하다.

- 전자 화폐의 요구사항 중에서 독립성(Independence)에 해당할 수 있다. 전자화폐의 보안성(Security)는 어떠한 물리적인 상태들에 의존해서는 안 된다. 이것은 복사 방지를 위해서 사용되는 복사 방지 인쇄 기술이나 또는 tamper resistance device와 같이 데이터를 보호하기 위한 외부적인 요소들에 의해 그 보안성이 결정되어서는 안 된다.

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

- 전자 화폐의 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 사용자의 사용에 있어서의 권한도 보장받아야 하는데 이러한 것은 전자화폐의 불추적성을 기초로 해결할 수 있다.

(4) 컨텐츠가 재유통 가능한 디지털 형식으로 누설되는 것을 방지 또는 억제해야 한다.

(5) 컨텐츠의 유통에도 효율적(Efficiency)이고, 간단(Simply)하게 할 수 있도록 지원해야 한다.

- 전자 화폐의 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. 유통에서는 효율적이고 간단해야하며 유통과정에서 발생할 수 있는 위협행위에 대해 쉽고 빠르게 대처가 가능해야 한다.

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

- 전자 화폐의 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. 제안 방식

본 논문에서 제안하고 있는 방식은 전자화폐 시스템에서 요구하는 기본적인 기능을 이용하여 DRM에서 요구하는 기능으로 적용하였으며, 컨텐츠의 사용자를 추적할 수 있고 익명으로 제공된 컨텐츠에 대하여 익명성을 취소할 수 있는 부가 기능을 가지고 있다. 먼저 각 개체는 RSA 알고리즘을 이용하여 키를 생성하며, 해시 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. 또한 이산 대수 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 복사에 대한 사용을 방지해 주고 있다. 그리고 클리어링 하우스에서의 라이선스 발행 시 컨텐츠 제공자와 사용자 인증을 위해 변형된 S/Key one-time password 방식을 사용함으로서 라이선스가 단일 항으로 구성되게 하고 있다. [5][11][12][13]

그림 1은 제안 방식의 전체적인 흐름을 보여준다.

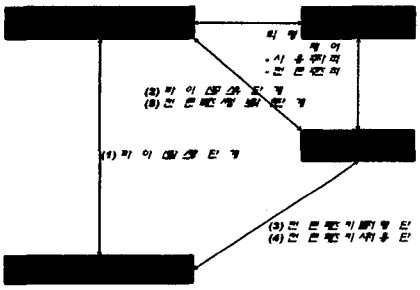

그림 1 전체 흐름도

3.1 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 테이블에 의해 컨텐츠 제공자에서 제공받은 컨텐츠를 원하는 복사 횟수만큼 분할하여 사용할 수 있으며 분할된 복사들의 합은 초기에 컨텐츠 제공자로부터 받은 복사 횟수와 동일하게 된다. 계층적 구조 테이블은 트리구조를 가지고 있고 각 노드는 복사 권한 정보에 해당하며 다음과 같은 규칙을 가진다.

a. 노드 N에 있어서 해당 복사 횟수는 자기 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.

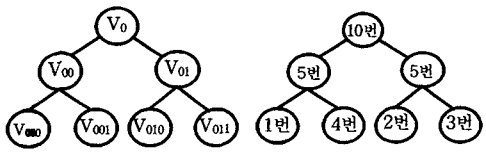

그림 2 계층적 구조 테이블

그림 2는 복사 횟수와 각 노드들의 값에 대한 트리구조를 나타내고 있으며 컨텐츠 제공자로부터 받은 컨텐츠 복사 횟수 N은 루트 노드 V_0에 해당한다. 루트 노드는 다시 두 개의 subnode(=V_{00}, V_{01})로 나뉘어지게 된다. 또한 사용자가 원하는 만큼의 복사횟수를 가질 수 있는데 이것은 사용자가 복사를 원하는 횟수의 선택에 따라 달라지게 된다. 나눠진 자식 노드의 합은 루트노드(V0)와 같게 된다. subnode는 두 개의 해시 함수 f1과 f2를 사용하는데 왼쪽 노드는 f1을 사용하고 오른쪽 노드는 f2를 사용하여 트리를 구성한다. 각 노드의 값은 다음과 같이 상위 노드를 이용하여 하위 노드를 계산해 낸다.

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

3.2 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수에 대해 기술한다. 각 계수는 구성요소에 따라 구분하고 있으며 각 구성요소가 생성하고 전달하는 계수에 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 계수로서, n_u, e_u는 공개키이고 d_u는 비밀키이다.
·ID_u : 사용자가 생성한 식별자로서 클리어링 하우스와 연계
$ID_u \equiv g_1^{d_U} \bmod p$
·S : $ID_u \| response \| (H(ID_u \| response))^{d_A} \bmod n_A$, $response = E_R(H_N(ID_u))$
·I ≡ $g_1^s \bmod p$
·H, f1, f2 : 일방향 해시 함수(One-way hash function)로서 H는 라이선스 발행 시 사용되며 f1과 f2는 계층적 구조 테이블에서 노드 구성 시 사용된다.
·CHLC(Clearing House License Candidate) : 라이선스를 발급 받기 위해 사용자가 생성하여 보내는 라이선스 후보
CHLC ≡ $r_1^{e_B} \cdot H(I \| X_N) \bmod n_B$, 여기서 r_1은 랜덤 하게 선택

나. 클리어링 하우스(CH) 및 컨텐츠 제공자(SP)

·CP(Contents Packager) : 컨텐츠 제공자가 생성하는 컨텐츠 인자 C를 사용하여 컨텐츠패키저(CP)를 구성한다. CP = {C ‖ A_1' ‖ A_2' ‖ $sign_u(C \| A_1' \| A_2')$}
·C : Contnets 파일
·(n_B, e_B, d_B) : 클리어링 하우스의 라이선스용 RSA 계수로서, n_B, e_B는 공개키이고 d_B는 비밀키이다.
·(n_B', e_B', d_B'), (n_B'', e_B'', d_B''), . . . : 클리어링 하우스는 각 복사권한에 해당하는 RSA 계수를 생성한다. 예를 들어 (n_B', e_B', d_B')은 1번에 해당하고 (n_B'', e_B'', d_B'')는 10번에 해당한다.

다. Trustee(T)

·(DT, NT, XT) : Trustee의 RSA 계수로서, DT, NT는 공개키이고 XT는 비밀키이다.
·y_T : 수탁기관의 공개 정보, $y_T \equiv g_2^{X_T} \bmod p$

3.3 라이선스 발행 단계

컨텐츠 패키저를 발행 받기 전에 사용자는 라이선스를 발행 받아야 한다. 이때 라이선스는 라이선스 서비스 요구 시에 발급 받아 컨텐츠 패키저 발급 시 인자로서 사용하며 사용자가 원하면 새로운 라이선스를 발행 받아 사용할 수 있다. 라이선스 발행 단계에서는 변형된 S/Key one-time password를 사용하여 클리어링 하우스와 사용자측이 상호 인증을 하게 되며 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다. 또한 제안 방식에서의 라이선스는 단일 항으로 구성된다. [6]

사용자클리어링 하우스는 상호 인증을 위한 초기화 단계를 수행한다. 먼저 사용자와 클리어링 하우스는 해시 함수를 적용할 횟수 N을 결정한다. 이를 이용하여 서버 측에 저장할 사용자의 비밀 정보를 생성해 낸다.

step 1 : 사용자는 hash function H와 ID_u 그리고 N을 선택하고 이를 클리어링 하우스에 전송한다.

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

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

step 3 : 클리어링 하우스는 난수 R과 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 클리어링 하우스 인증 과정을 수행한다.

$R' = (H_{N+1}(ID_u) \oplus R \oplus X_{N+1}),\ D_R(E_R(X_{N+1})) \stackrel{?}{\equiv} H_{N+1}(ID_u)$

클리어링 하우스의 인증 과정이 성립되면 response, S, I와 라이선스

후보 CHLC 값을 계산하여 I값은 공개하고 response와 CHLC를 클리어링 하우스에 전송한다.

step 5 : 클리어링 하우스는 사용자 인증 과정을 수행하고 사용자 관련 저장 정보를 N+1에서 N으로, X_{N+1}을 $X_N = H_N(ID_U)$로 갱신한다. 그리고 CHLC에 클리어링 하우스의 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 클리어링 하우스가 서명한 CHLC로부터 라이선스 CHL을 추출한다.

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

3.4 컨텐츠 패키저 발행 단계

클리어링 하우스가 발행한 라이선스를 이용하여 컨텐츠 제공자로부터 컨텐츠 패키저를 발행 받는 과정이다. 컨텐츠 패키저를 발행 받는 동안에 컨텐츠를 추적할 수 있는 인자 A_1'이 생성되며 이것은 컨텐츠 추적 단계에서 trustee를 거치면서 컨텐츠 추적을 위해 사용된다.

step 1 : 사용자는 v∈{1, . . . , 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 A1', A2'를 올바르게 생성하였는지 확인한 뒤 w∈{1, . . . , 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 r2는 랜덤한 정수이며 사용자가 컨텐츠 패키저를 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.

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

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

$$\equiv r_2 \cdot (H(CHL \| b))^{d_B'} \bmod n_B'$$ 여기서 $a' \equiv g_2^w \bmod p$이다.

step 5 : 사용자는 Z'으로부터 C를 추출해 낸다.

$$C \equiv Z'/r2 \equiv (H(CHL \| b))^{d_B'} \bmod n_B'$$

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

3.5 컨텐츠 패키저 사용 단계

컨텐츠 패키저 사용 단계로서 컨텐츠 제공자로부터 컨텐츠를 제공받은 후 사용자는 클리어링 하우스로부터 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 패키저에 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, A1, A2, (A3)와 함께 컨텐츠 제공자에 전송한다.

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

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

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

step 2 : 컨텐츠 제공자는 컨텐츠 패키저 CP에 있는 사용자 서명을 확인한 뒤 V_{i00}과 A, A1, A2를 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 $R_{i00} \in \{1, . . . , p-2\}$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.

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

3.6 컨텐츠 복사 정보 확인 단계

사용자가 사용한 컨텐츠 패키저 CP를 전송하기 위해서 컨텐츠 제공자는 복사 권한 확인서를 클리어링 하우스에 전송한다. 클리어링 하우스가 H를 전송 받으면 컨텐츠 패키저 및 라이선스의 유효성을 확인하고 클리어링 하우스의 DB를 이용하여 이중 사용 여부를 확인한다.

H = I, p, g_1, g_2, g_3, V_{i00}
R_{i00}, Y_{i00}, OA(= (A_1, A_3)), CHL, CP

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

4. 결론

현재 DRM에 관하여 많은 연구가 진행 중에 있다. DRM모델에서 유통과 관리부분 중 컨텐츠에 대한 보호는 전체 모델에서 가장 핵심적인 부분이라 할 수 있다.

본 논문은 전자화폐를 이용하여 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 패키저 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 연예/오락용 디지털 컨텐츠의 온라인 판매뿐만 아니라 CD 등의 오프라인 매체로 판매되는 현재의 소프트웨어 유통체계에도 많은 변화를 가지고 올 것이다.

참고문헌

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

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

[3] 이형우, "안전한 컨텐츠 유통을 위한 방안 연구", 제 12권 제 1호, pp48-54, 2002. 2

[4] 여상수, 윤훈기, 김성권, "디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅의 연구동향", 한국정보보호학회지, 제 11권 3호, pp90-99

[5] 이덕규, 오형근, 이임영, "지불정보를 이용한 Hidden Agent 컨텐츠 불법 복사 방지에 관한 연구", 02' 한국멀티미디어학회 춘계학술대회, pp947-950, 2002. 5

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

[7] B. von Solms and D. Naccache, "On blind signatures and perfect crimes", Computers and Security, pp581-583, 1992

[8] C. P. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, 4(3), 161-174, 1991

[9] 김기현, 윤유진, 박경호, 고승철, "변형 일회용 패스워드 시스템 제안", 제 10회 정보보호와 암호에 관한 학술 대회, pp75-92, 1998

[10] 오형근, 이임영, "새로운 추적 가능한 전자화폐 프로토콜에 관한 연구", '98, 한국정보과학회 추계학술발표회 논문집(III), pp344-pp346, 1998

[11] 오형근, 이임영, "분할 가능한 전자화폐 프로토콜에 관한 고찰", '98 통신정보보호 학술 발표회 논문집(충청지부), pp97-pp112, 1998

[12] 오형근, 이임영, "익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구", '98 통신정보보호학회 종합 학술 발표회, pp109-121, 1998

[13] 이덕규, 이임영, "Agent 기반 불법 복제 방지 DRM모델", 한국정보과학회 추계학술대회, 2001

[14] 김종안, 임태영, 한평희, 이상홍, "국내외 DRM 솔루션 및 비즈니스 현황과 MS-DRM에 관한 연구", 한국통신 정보통신 연구, 15권, 3호, pp36-42, 2001. 9