지불정보를 이용한 Hidden Agent 컨텐츠 불법 복사 방지에 관한 연구

이덕규*, 오형근**, 이임영*
* 순천향대학교 정보기술공학부
** 국가보안기술연구소

A Study on Contents Illegal Copy Protection in Hidden Agent Using Payment Information

Deok-Gyu Lee*, Hyung-Geun Oh**, Im-Yeong Lee*
* Division of Information Technology Engineering, Soonchunhyang University
** National Security Research Institute
E-mail : hbrhcdbr@catholic.or.kr, hgoh@etri.re.kr, imylee@sch.ac.kr

요 약

디지털 컨텐츠의 지적 재산권 보호를 위한 디지털 워터마킹 기술 및 핑거프린팅의 연구가 활발히 진행되고 있다. DRM(Digital Rights Management)는 디지털 컨텐츠 지적 재산권 보호뿐만 아니라 컨텐츠에 대한 출판, 유통 및 사용에 필요한 관리와 보호체계이다. 본 논문에서는 컨텐츠 유통과정에서 발생할 수 있는 불법 복사와 같은 불법 행동에 대해 컨텐츠를 안전하게 보호하며 사용자에게 편의성을 제공 할 수 있는 프로토콜을 제시할 것이며 또한 지불의 효율적 사용을 위해 분할성 기능과 함께 화폐 추적과 사용자 추적 기능을 Hidden Agent에 포함하여 제안한다. 이 Hidden Agent는 특별한 설치가 필요 없이 컨텐츠 내에 내포되어 있어 컨텐츠에 대한 지불, 불법복사 및 불법사용에 대해 체크함으로써 불법복사의 사용을 차단할 수 있도록 한다. 또한 사용자들에게 숨겨져 있기 때문에 워터마킹의 역할 또한 대신할 수 있다. 따라서 본 논문에서는 유통과정에서 가장 빈번하게 나타날 수 있는 지불과 불법 복사에 대하여 Hidden Agent를 이용하여 해결하였다.

1. 서론

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.[1]

DRM이란 디지털 컨텐츠 출판, 유통 및 사용에 필요한 관리 및 보호체계로 정의한다. 관리로는 통일된 컨텐츠 관리 체계를 구축하기 위한 기반 구조 기술을 말하는데 DOI(Digital Object Identifier), INDECS (INteroperability of Data in E-Commerce Systems) 등의 범 국가적인 컨텐츠 관리 기반 인프라 기술이며, 보호체계로는 컨텐츠를 안전하게 보호하기 위한 응용 기술을 말한다.[6]

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.

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

본 논문에서는 이중에서 디지털 창작물에 대한 유통/서비스과정에서의 컨텐츠를 위한 보호를 제시할 것이다. 유통 혹은 서비스 단계에서 발생할 수 있는 불법복사를 차단함으로써 더 나아가는 저작권보호 및 사용권 보호를 이룰 수 있을 것으로 사료된다.

기존에 제시되었던 모델에서는 전용 플레이어, 스마트카드 및 프로그램 인스톨을 이용하였다. 두 모델에서의 문제점은 특별한 개체가 필요하다는 것이다. 이러한 문제점을 해결하고자 다음과 같은 불법복사를 방지할 수 있는 DRM모델을 제시하고자 한다. 본 고에서는 이전에 제시되었던 전용플레이어나 스마트카드의 이용 없이 컨텐츠 안에 포함된 Agent를 이용하여 컨텐츠의 불법복사를 방지하고 Hidden Agent 내에 전자 화폐를 포함함으로써 지불을 할 수 있는 방식을 제안한다.

2. Agent 개요

2.1 이동 Agent

이동 Agent는 독립적이고 자율적으로 원하는 정보를 찾아 네트워크를 이동하면서 여러 서비스를 수행하도록 구현된다. 그림 1은 이동 Agent의 동작 모습을 개략적으로 나타낸

것으로 로컬에서 리모트 호스트로 이동한 후 작업을 수행하는 모습을 보여주고 있다. Agent는 호스트 A에서 B로 이동하여 이미 정의된 인터페이스를 통하여 B의 서비스 및 자원에 접근하여 원하는 정보를 얻어 원래의 서버 A로 전송한다.
원하는 정보를 얻은 후 Agent는 또 다른 서버로 이전(移轉)하여 이전(以前)과 같은 동작을 수행한다. 이동 Agent는 사용자를 위해 자동적으로 행동하는 프로세스이며, 수행을 시작하면 자신이 생성된 시스템을 벗어나 네트워크를 통하여 한 장소에서 또 다른 장소로 옮겨 다니며 원하는 정보를 수집한다.

그림 1 이동 Agent의 동작

2.2 Hidden Agent

Hidden Agent는 이동 Agent와 마찬가지로 독립적이고 자율적인 행동을 하면서 서비스를 수행한다. 그림 2는 Hidden Agent의 동작을 개략적으로 나타낸 것으로 제공자에게서 사용자에게로 이동하여 수행하는 모습을 보여주고 있다.
Hidden Agent는 Offered Serve에서 End Entity로 이동하여 이미 정의된 인터페이스를 통하여 End Entity의 명령 및 자원에 상주하여 특정한 행동에 대해 원래의 제공서버로 전송한다.
특정한 행동을 얻은 Hidden Agent는 계속적으로 상주하여 이전과 같은 동작을 수행한다. Hidden Agent는 사용자의 특정한 행동을 위해 자동적으로 행동하는 프로세스이며, 수행을 시작하면 자신이 생성된 시스템(즉, Offered Server)을 벗어나 네트워크를 통해 한 장소에 머물며 특정한 행동에 대해 기동된다.

그림 2 Hidden Agent의 동작

4. 제안 방식

본 방식에서 사용되는 Hidden Agent가 Contents에 포함되어 제공되고 있다. Hidden Agent는 복사 시 자신의 생성인자와 제공인자를 통하여 불법복사에 대한 권한을 제한한다. 다음은 각 단계에 대하여 자세히 기술한 것이다.
DRM은 총 4단계로 구성되며 컨텐츠 생성단계, 컨텐츠 제공단계, 컨텐츠 지불 단계, 컨텐츠 불법 복사 확인 단계로 이루어진다. 이 중에서 컨텐츠 지불 단계는 Hidden Agent에 포함하여 전자화폐의 기능을 제공하며 그 외의 사항은 기존 시스템을 따르는 것으로 한다. 또한 컨텐츠 제공단계에 앞서 전자화폐를 발행하고 지불하는 단계를 선행하며 마지막으로 컨텐츠 불법 복사시에 불법 복사를 제한할 수 있는 컨텐츠 불법 복사 확인 단계로 기술한다. 다음은 각 단계별로 자세히 기술한 내용이다.

4.1 계층적 구조 테이블

전자화폐의 여러 가지 기능들 중에서 분할성을 만족시켜주기 위해 계층적 구조 테이블을 사용하고 있다. 이 테이블에 의해 은행에서 발급 받은 전자화폐를 보다 작은 금액으로 분할하여 사용할 수 있으며 분할된 금액들의 합은 초기에 은행으로부터 받은 전자화폐 금액과 동일하게 된다. 계층적 구조 테이블은 트리 구조를 가지고 있고 각 노드는 화폐 금액 정보에 해당하며 다음과 같은 규칙을 가진다.

a. 노드 N에 있어서 해당 금액은 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.

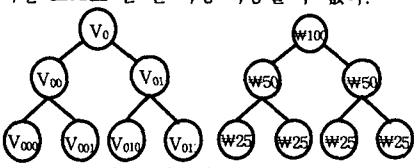

그림 3. 계층적 구조 테이블

그림 3은 화폐 금액과 각 노드들의 값에 대한 트리 구조를 나타내고 있으며 은행으로부터 받은 전자화폐 C는 루트 노드 V_0에 해당한다. 루트 노드는 다시 두 개의 subnode(=V_{00}, V_{01})로 나뉘어지며 이 때 자식 노드의 합은 루트노드(V_0)와 같게 된다. subnode는 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.

$$V_0 = C$$
$$V_{00} \equiv V_0 \cdot f_1(V_0) \bmod p, \quad V_{01} \equiv V_0 \cdot f_2(V_0) \bmod p$$
$$V_{000} \equiv V_{00} \cdot f_1(V_{00}) \bmod p, \quad V_{001} \equiv V_{00} \cdot f_2(V_{00}) \bmod p$$
$$V_{010} \equiv V_{01} \cdot f_1(V_{01}) \bmod p, \quad V_{011} \equiv V_{01} \cdot f_2(V_{01}) \bmod p$$

4.1 시스템 파라메타

다음은 본 제안방식에서 사용되는 시스템 파라메터에 대해 기술한 것이다.

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 파라메타로서, n_u, e_u는 공개키이고 d_u는 비밀키이다.
- ID_u : 사용자가 생성한 식별자로서 은행의 계좌 번호와 연계, $ID_u \equiv g_1^{d_U} \bmod p$
- S : $ID_U \| response \| (H(ID_U \| response))^{d_U} \bmod n_A$
  $response = E_K(H_N(ID_u))$
- $I \equiv g_1^s \bmod p$
- H, f_1, f_2 : 일방향 해쉬 함수(One-way hash function)로서 H는 전자면허 발행시 사용되며 f_1과 f_2는 계층적 구조 테이블에서 노드 구성시 사용된다.
- BLC(Bank License Candidate) : 전자면허를 발급 받기 위해 사용자가 생성하여 보내는 전자면허 후보
  BLC $\equiv r_1^{e_B} \cdot H(I \| X_N) \bmod n_B$, 여기서 r_1은 랜덤하게 선택
- EC(Electronic Cash) : 은행이 발행하는 전자화폐 인자 C를 사용하여 전자화폐(EC)를 구성한다.
  EC = $\{C \| A_1' \| A_2' \| sign_u(C \| A_1' \| A_2')\}$

나. 은행(B)

- (n_B, e_B, d_B) : 은행의 전자면허용 RSA 파라메타로서, n_B, e_B는 공개키이고 d_B는 비밀키이다.
- (n_B', e_B', d_B'), (n_B'', e_B'', d_B''), . . . : 은행은 각 금액에 해당하는 RSA 파라메타를 생성한다. 예를 들어 (n_B', e_B', d_B')은 ₩100에 해당하고 (n_B'', e_B'', d_B'')은 ₩1000에 해당한다.

다. 수탁기관(N)

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

라. 상점(M)

- S : 컨텐츠 종류
- D : 컨텐츠 복사 횟수
- T : 컨텐츠 내에 삽입되는 Time-Stamp
- (n_m, e_m, d_m) : 상점의 RSA 파라메타로서, n_m, e_m는 공개키이고 d_m는 비밀키이다.
- ID_m : 상점이 생성한 식별자, $ID_m \equiv g_1^{d_m} \bmod p$

4.2 전자면허 발행 단계

전자화폐를 발행 받기 전에 사용자는 전자면허를 발행 받아야 한다. 이때 전자면허는 계좌 개설시에 발급 받아 전자화폐 발급시 인자로서 사용하며 사용자가 원하면 새로운 전자면허를 발행 받아 사용할 수 있다. 전자면허 발행 단계에서는 변형된 S/Key one-time password를 사용하여 은행과 사용자측이 상호 인증을 하게 되며 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다.

사용자와 은행은 상호 인증을 위한 초기화 단계를 수행한다. 먼저 사용자와 은행은 해쉬함수를 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 은행에 전송한다.

step 2. 은행은 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. 은행은 난수 R과 challenge 값을 생성하여 사용자에게 전송한다.

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

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

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

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

은행의 인증 과정이 성립되면 response, S, I와 전자면허 후보 BLC 값을 계산하여 I값은 공개하고 response와 BLC를 은행에 전송한다.

step 5. 계층적 구조 테이블 은행은 사용자 인증 과정을 수행하고 사용자 관련 저장 정보를 N+1에서 N으로, X_{N+1}을 $X_N = H_N(p)$로 갱신한다. 그리고 BLC에 은행의 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 은행이 서명한 BLC로부터 전자면허 BL을 추출한다.

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

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

4.3 전자화폐 발행 단계

은행이 발행한 전자면허를 이용하여 은행으로부터 전자화폐를 발행 받는 과정이다. 전자화폐를 발행 받는 동안에 화폐를 추적할 수 있는 인자 A_1'이 생성되며 이 A_1'은 화폐 추적 단계에서 trustee를 거치면서 화폐 추적을 위해 사용된다.

step 1. 사용자는 $v \in \{1, \ldots, p-1\}$를 랜덤하게 선택하고 A_1'과 A_2'를 생성하여 은행에 전송한다.

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

step 2. 은행은 A_1', A_2'를 올바르게 생성하였는지 확인한 뒤 $w \in \{1, \ldots, p-1\}$를 랜덤하게 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 은행에 전송한다. 이때 r_2는 랜덤한 정수이며 사용자가 화폐를 전송받기 위해 생성한 데이터를 은닉시킨다.

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

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

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

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

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

여기서 $a' \equiv g_2^w \bmod p$이다.

step 5. 사용자는 Z'으로부터 C를 추출해 낸다.

$$C \equiv Z'/r_2 \equiv (H(BL \parallel b))^{d_B'} \bmod n_B'$$

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

4.4 컨텐츠 제공 및 대금지불 단계

컨텐츠 지불 단계로서 상점으로부터 컨텐츠를 제공받은 후 사용자는 은행으로부터 인출된 전자화폐와 계층적 구조 테이블을 이용하여 상점에게 원하는 금액을 지불한다. 즉 ₩100 중 ₩75를 지불하기 원한다면 노드 값 V_{00}, V_{010}을 계산하고 이와 관련된 Y_{00}, Y_{010}을 계산하여 상점에 전송함으로써 전자화폐에 대한 유효성을 검사한다.

step 1. 사용자는 원하는 컨텐츠에 대한 종류(S)와 사용자 ID를 서명하여 상점에 전송한다.

$$R = ID_u \parallel S \parallel sign_u(ID_U \parallel S)$$

step 2. 상점은 사용자로부터 받은 ID_u를 이용하여 컨텐츠 교환을 위한 공유 세션키 K를 계산한다. 그 후, 상점은 자신의 ID_m과 $R = ID_u \parallel S \parallel sign_u(ID_U \parallel S)$을 서명하여 사용자에게 전송한다.

$$K \equiv (ID_u)^{d_m} \bmod p$$

$$R' = ID_m \parallel R \parallel sign_m(ID_m \parallel R)$$

step 3. 사용자는 상점으로부터 받은 R'을 확인한 뒤 ID_m을 이용하여 컨텐츠 교환용 공유 세션키 K를 계산한다.

$$K \equiv (ID_m)^{d_u} \bmod p$$

step 4. 사용자와 상점의 컨텐츠 교환용 공유 세션키의 생성이 완료된 후, 사용자는 컨텐츠에 대한 지불 금액에 해당하는 노드 값(V_{00}, V_{010})과 (X_{00}, X_{010})를 계산한 뒤 EC, BL, A, A_1, A_2 (A_3)과 함께 상점에 전송한다.

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

$$V_{00} \equiv V_0 \cdot f_1(V_0) \bmod p,\ V_{010} \equiv V_{01} \cdot f_1(V_{01}) \bmod p$$

$$X_{00} = g_1^{V_{00}} \bmod p,\ X_{010} = g_1^{V_{010}} \bmod p$$

step 5. 상점은 전자화폐 EC에 있는 사용자 서명을 확인한 뒤 V_{00}, V_{010}과 A, A_1, A_2를 확인한다.

$V_{00} \stackrel{?}{=} V_0 \cdot f_1(V_0) \bmod p,\ V_{010} \stackrel{?}{=} V_{01} \cdot f_1(V_{01}) \bmod p$

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

그리고 나서 난수 R_{00}, $R_{010} \in \{1, \ldots, p-2\}$를 생성하여 사용자에게 전송한다.

step 6. R_{00}, R_{010}를 이용하여 사용자는 다음의 Y_{00}, Y_{010}를 계산하여 상점에 전송한다.

$Y_{00} \equiv V_{00} + R_{00} \cdot S \bmod p-1,\ Y_{010} \equiv V_{010} + R_{010} \cdot S \bmod p-1$

step 7. 상점은 Y_{00}와 Y_{010}에 대한 다음 식이 성립하는지 확인하여, 만족하면 V_{00}, V_{010}를 인증하여 전자화폐 ₩75을 받아들인 후 사용자가 요구한 컨텐츠에 Hidden Agent를 삽입한 후 사용자에게 전송한다. 이때 Hidden Agent(*H.A*)와 같이 삽입되는 타임스탬프 T는 발행 시점을 나타내는 시간으로 만약 사용자가 복사하게 된다면 T값은 변화하게 된다.

$g_1^{Y_{00}} \equiv X_{00} \cdot (I)^{R_{00}} \bmod p$

$g_1^{Y_{010}} \equiv X_{010} \cdot (I)^{R_{010}} \bmod p$

$E_K(Content(H.A \| T))$

step 8. 사용자는 $E_K(Content(H.A \| T))$ 값을 자신이 가지고 있는 컨텐츠 교환용 세션 키 K를 이용하여 복호화 한 뒤 사용한다.

4.5 예치단계

사용자가 지불한 전자화폐 EC를 전송하기 위해서 상점은 거래내역서 H를 은행에 전송한다. 은행이 H를 전송 받으면 전자화폐 및 전자면허의 유효성을 확인하고 은행의 DB를 이용하여 이중 사용 여부를 확인한다.

$H = I, p, g_1, g_2, g_3, V_{00}, V_{010}$
$R_{00}, R_{010}, Y_{00}, Y_{010}, O_A(= (A_1, A_3)), EL, EC$

5. 제안 방식의 고찰

5.1 컨텐츠 불법 복사 확인

컨텐츠에 대해 사용자가 복사를 원하는 경우에 컨텐츠와 함께 제공된 Hidden Agent는 사용자가 복사 명령을 내릴 경우 동작하게 되며 에이전트가 가지고 있는 키를 이용하여 상점과 다음과 같은 단계를 수행한다. 만약 Hidden Agent가 상점과 연결되지 않는다면 복사 권한은 부여되지 않는다.

step 1. 사용자가 복사하기 원하는 컨텐츠 상에 존재하는 Hidden Agent는 복사 명령이 수행될 경우 S, T, ID_u, T 값과 지불된 금액 P를 상점에 자신의 키로 암호화하여 전송한다.

$E_{K_A}(ID_u \| S \| T \| P)$

step 2. 상점은 자신이 가지고 있는 DB의 내용과 비교하여 복사 권한을 부여한다. 만약 상점의 동의 없이 불법 복사가 되었다면 T값 대신 T'이 전송되어 상점은 복사 권한을 부여하지 않는다.

$T \stackrel{?}{=} T',\ S \stackrel{?}{=} S'$

$E_{K_A}(ID_u \| Yes or\ No)$

5.2 불법 복사 제공자 추적

불법 복사 제공자 추적 단계는 컨텐츠가 복사가 이루어진 경우 사용자를 판별하는 방법으로서 합법적인 컨텐츠 제공이 이루어지고 난 후에 추적을 가능케 한다. 이는 컨텐츠의 부정사용에 관련된 것들에 기반하기 보다는 사용자가 구입한 컨텐츠에 대한 협의가 주어질 경우에 그 컨텐츠의 사용자를 추적하게 된다. 이 단계는 예치 단계에 추가하여 구성되며 사용자가 상점에 대금 지불시 $A_3(= ID_u \cdot (y_T)^v \bmod p)$가 추가된다..

step 1. 상점은 거래 내역서로부터 A_3를 trustee에 전송한다.

step 2. trustee는 A_3로부터 $A_3' \equiv ID_u^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하여 상점에 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. 상점은 trustee가 전송한 A_3'로부터 ID_A를 계산해 낸다.

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

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

7. 결 론

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

기존에 사용되었던 전용 플레이어를 이용한 방식, 스마트카드를 이용한 방식등이 가지고 있었던 문제점을 해결하려 하였으며, 사용자에게 불편을 주는 매번 인증을 통한 컨텐츠 제공방식을 해결하려 노력하였다.

본 논문은 Hidden Agent를 이용한 불법 복사 방지 DRM 모델을 제시하였다. 기존 시스템에 변경 없이 사용할 수 있고, 사용자가 Hidden Agent의 여부를 알지 못한다. 전용 플레이어를 통한 제공이 아니기 때문에 향후 유·무선 분야에서 사용될 수 있으리라 본다. 또한 Hidden Agent는 별도의 설치 없이 컨텐츠 내에 위치하도록 하였다. 이러한 Hidden Agent를 이용하여 불법복사를 방지함으로써 전체적인 DRM모델에 쉽게 접근할 수 있을 것이다.

향후 연구 과제로는 원본 컨텐츠에 대한 소유권과 지불을 적용한 방식, 익명 사용자을 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] G, Vigna, Cryptographic traces for Mobile Agents, Mobile Agents and Security, Springer-Verlag, Lecure Note in Computer Science 1419, pp 137-153, 1998

[2] John Erickson, Principles for standardization and interoperability in web-based DRM, W3C, DRM Workshop, 2001

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

[4] 오형근, 이임영, 익명성 제어와 화폐 분할 기능을 가지는 효율적인 전자화폐 프로토콜, 한국정보과학회, Vol,26, No. 7, 1999

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

[6] 신원, 박영효, 이경현,이동 에이전트 시스템 시큐리티, 한국통신정보보호학회 종합학술발표회, pp164-171

[7] 이경현, 신원, 이동 에이전트 기반의 컨텐츠 보호 기술, 한국멀티미디어학회지, 5권, 1호, pp68-75, 2001

[8] 여상수, 윤훈기, 김성권, 디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅의 연구 동향, 한국정보보호학회지, 11권, 3호, pp90-99, 2001