Agent 기반 불법 복제 방지 DRM모델

이덕규[0] 박희운 이임영
순천향대학교 정보기술공학부
(hbrhcdbr, heeun)@sec-cse.sch.ac.kr, imylee@sch.ac.kr

A DRM Model for Illegal Copyrights Protection based on Agent

Duk-Kyu Lee[0] Hee-Un Park Im-Yeong Lee
Division of Information Technology Engineering , SoonChunHyang University

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 보호 기술 중에서 컨텐츠에 대한 유통/서비스에 해당하는 기술을 만족하는 프로토콜을 제시할 것이다. 이를 위해 컨텐츠 불법복제 및 불법사용을 방지할 수 있도록 Agent를 이용한다. Agent는 특별한 설치가 필요 없이 컨텐츠 내에 내포되어 있게 된다. 내포된 Agent는 불법복제 및 불법사용에 대해 체크함으로써 불법복제의 사용을 차단할 수 있도록 한다.

1. 서 론

전자 상거래를 통해서 디지털 컨텐츠 판매가 활성화 되기 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 방법 들로 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.

DRM이란 디지털 컨텐츠 출판, 유통 및 사용에 필요한 관리 및 보호체계로 정의한다. 관리로는 통일된 컨텐츠 관리 체계를 구축하기 위한 기반 구조 기술을 말하는데 DOI, INDECS 등의 범 국가적인 컨텐츠 관리 기반 Infra 기술이며, 보호체계로는 컨텐츠를 안전하게 보호하기 위한 응용 기술을 말한다.

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 기술등이 있다

본 고에서는 이중에서 디지털 창작물에 대한 유통/서비스과정에서의 컨텐츠를 위한 보호를 제시할 것이다. 유통 혹은 서비스 단계 에서 발생할 수 있는 불법복제를 차단함으로써 더 나아가는 저작권보호 및 사용권 보호를 이룰 수 있을 것으로 생각된다.

기존에 제시되었던 모델에서는 전용 브라우저, smartcard

3. 요구 사항

본 모델에서는 다음과 같은 기본적인 요구사항이 필요하다.

및 프로그램 Install을 이용하였다. 이러한 모델에서의 문제점은 특별한 개체가 필요하다는 것이다. 이러한 문제점을 해결하고자 다음과 같은 불법복제를 방지할 수 있는 DRM모델을 제시하고자 한다. 본 고에서는 이전에 제시되었던 전용브라우저나 smartcard의 이용 없이 컨텐츠 안에 포함된 Agent를 이용하여 컨텐츠의 불법복제를 방지하고자 한다.

2. Agent 개요

이동 Agent는 독립적이고 자율적으로 원하는 정보를 찾아 네트워크를 이동하면서 여러 서비스를 수행하도록 구현 된다. 다음 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 이전하여 이전과 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.

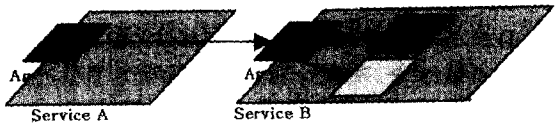


그림 1 이동 Agent의 동작

컨텐츠 구매를 원하는 자로써 컨텐츠에 대한 지불 및 사용권을 갖는다. CP(Contents Provider) Master Server와 함께 컨텐츠를 제공 받기 위한 키를 생성한다.

3.1 Agent가 가지는 요구 사항

Agent는 다음과 같은 요구 사항을 필요로 한다.

- Agent는 컨텐츠 내부에 존재한다.

컨텐츠 내부에 존재하게 되며 Agent를 사용자 임의 대로 삭제시킬 수 없다. 만약 Agent 삭제 시에는 컨텐츠도 함께 삭제된다. (Virus와 같이 존재한다.)

- Agent는 컨텐츠 제공 후 실행한다.

컨텐츠에 포함되어 있는 Agent는 컨텐츠 제공과 함께 전달되며 사용자 컴퓨터 상에서 컨텐츠를 실행함과 동시에 로드 된다.

- Agent는 Boot시 항상 로드 된다.

컴퓨터의 OS가 구동된 후 컨텐츠 불법복제 방지를 위한 Agent는 항상 로드 된다.

- Agent는 인자를 포함한다.

컨텐츠 불법복제를 방지하기 위한 인자를 가지며 인자에는 ID와 키 값은 반드시 포함되어야 한다.

3.2 컨텐츠에 대한 불법복제

- 사용자가 권한이 없는 상태에서 복사한 경우에 해당한다. 또는 사용자가 권한 획득 없이 복사한 경우에 해당한다.
- 통신로 상에서 불법 취득한 컨텐츠로 한다.

4. 제안 방식

본 고에서는 Agent를 이용하여 불법복제를 방지하고자 한다. 전체적인 모델에서 초기 컨텐츠에 대한 워터마크 삽입과 지불에 관한 부분은 기존의 시스템을 이용하도록 한다.

4.1 전체 시스템 모델

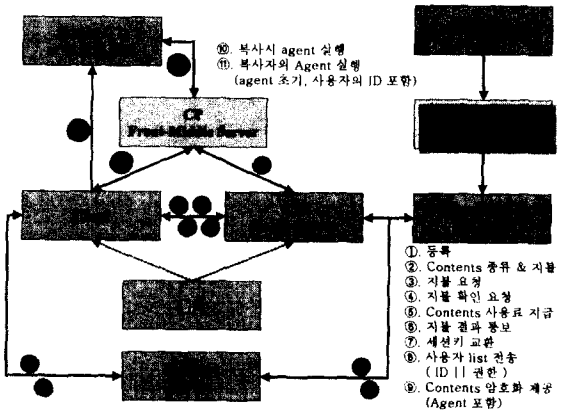


그림 2 전체 시스템 모델

4.2 구성 요소

다음은 본 시스템에서 구성하는 개체에 대하여 설명한다.

User :
과정을 진행한다.

CP Master Server :
User의 등록을 맡으며 컨텐츠에 대한 소유권을 갖는다. User와 같이 컨텐츠 제공을 위한 키를 생성한다.

CP Front-Middle Server :
불법 복제 방지를 위하여 컨텐츠 속에 제공된 Agent와의 통신을 한다. 본 개체에는 CP Master Server로부터 User의 자료를 전송 받는다. Agent로부터 수신된 User의 정보를 바탕으로 User에게 복사할 수 있는 권한을 부여한다.

Payment Server :
지불을 위한 개체로써 User와 CP Master Server 사이에 위치하게 된다.

Contents DataBase :
저작권자로부터 Watermarking된 컨텐츠를 제공 받게 된다. Contents DataBase는 저작권자가 CP인 경우, CP가 저작권을 갖게 되며, 반대로 저작권자가 다르게 존재할 경우 Contents DataBase가 저작권을 갖는다.

CA(Certificate Authentication) :
서명값을 이용하기 위해 구성되며, 후에 지불시스템과 Contents DataBase 등에 활용될 수 있다.

4.3 시스템 계수

다음은 본 논문에서 컨텐츠 제공을 위한 키 교환과 Agent에 필요한 시스템 계수에 대해 설명한다.

- **ID :** User의 Identify
- **K :** 컨텐츠 제공을 위한 암호화 키
- **KA :** Agent에서 사용되는 암호화 키
- **Sig :** 키 교환에서 무결성을 위한 서명값
  - **user :** 사용자의 서명값
  - **MS :** CP Master Server의 서명값
- **D :** 권한 종류(복사 횟수 권한, 사용 횟수 권한등)
- **L :** 해쉬값
- **T :** Time-Stamp
- **S :** 컨텐츠 종류
- **M :** 지불가

4.4 단계별 프로토콜 설명

다음은 본 고에서의 각 단계별 프로토콜에 대하여 기술한다. 총 3단계로 구성되며 컨텐츠 제공단계, 컨텐츠 지불 단계, 컨텐츠 불법 복사 확인 단계로 이루어 진다. 이 중에서 컨텐츠 지불 단계는 제외하며 지불에 관한 사항은 기존 시스템을 따르는 것으로 한다. 다음은 각 단계별로 자세히 기술한 내용이다.

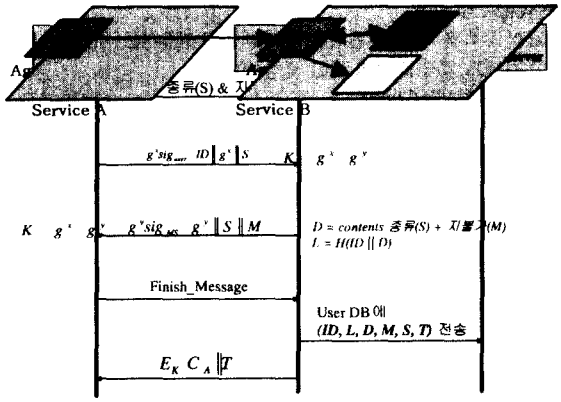
4.4.1 컨텐츠 제공 단계

다음은 컨텐츠를 제공하는 단계로서 User, CP Master Server 그리고 CP Front-Middle Server간의 키 교환 및 사용자 정보 제공하는 과정에 대해 설명한다.

처음 사용자가 이미 등록하였다고 가정하며, 등록 이후의

Phase 1. User의 컴퓨터 상에서 COPY 명령이 실행될 경우 자동으로 Agent는 수행되며, S, M, T에 대하여 암호화 후 Front-Middle Server에 전송한다.

- $E_{KA}(ID \| S \| M \| T)$



Phase 1. 사용자는 원하는 컨텐츠에 대한 종류(S)와 지불에 대한 지불가(M)를 CP Master 서버에 전송한다.

Phase 2. 컨텐츠 제공을 위한 키 교환이 이루어지는 단계중 사용자 키 전송 과정이다.

- g^x, $sig_{user}(ID \| g^x \| S)$
- D = S + M
- L = H(ID ‖ D)

Phase 3. 사용자로부터 받은 값을 이용하여 키 값을 만들고 서버 키 전송을 한다.

- $K = g^x + g^y$
- g^y, $sig_{MS}(g^x \| S \| M)$

Phase 4. 서버로부터 받은 값을 이용하여 키 값을 만들고 키 교환 종료 메시지를 전송한다.

- $K = g^x + g^y$
- Finish_Message

Phase 5. Master Server에서 생성한 인자들을 Front-Middle Server로 전송한다.

- (ID, L, D, M, S, T)

Phase 6. Master Server는 컨텐츠에 대해 사용자에 알맞은 Agent를 삽입한 후 전송한다.

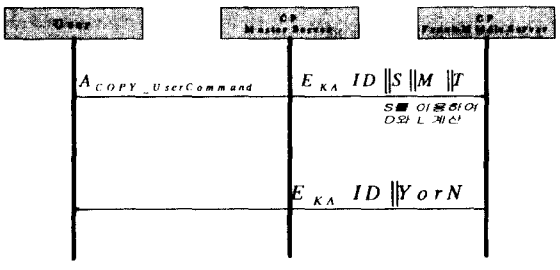
- $E_K(C_{(A)} \| T)$

4.4.2 컨텐츠 불법 복사 확인 단계

다음은 컨텐츠에 대해 사용자가 복사를 원하거나 불법 복사가 이루어졌을 경우 Agent의 동작에 대해 기술한다.

앞에서의 설명과 같이 Agent는 컨텐츠 제공과 함께 동작된다. 사용자가 OS상에서 COPY, MOVE와 같은 명령이 동작할 경우 Agent가 동작하게 되며 서버로부터 받은 키를 이용하여 ID, S, M을 암호화하여 Front-Middle Server에게 전송한다. Front-Middle Sever는 Agent와의 작업만 하게 된다.

만약 Agent가 서버와 연결할 수 없다면 복사 권한은 부여 되지 않는다.



Phase 2. Front-Middle Server는 받은 ID, S, M을 이용하여 D와 L을 계산 후, 자신이 가지고 있는 DB의 내용과 비교하여 복사 권한을 부여한다.

- D = S + M
- L = H(ID ‖ D)
- E_{KA}(ID ‖ YorN)

5. 제안 시스템 고찰

본 고에서는 Agent를 이용하여 불법 복제를 방지하려 하였다. 컨텐츠 내부에 Agent를 포함시킴으로써 사용자로부터는 컨텐츠에 사용권에 대해 권한을 제약(일부 사용권 부여)하였고, CP로부터는 소유권을 부여하였으며, 원본제작자로부터는 저작권을 부여하였다.

불법 복사자로부터 컨텐츠 보호의 경우에 사용자에게 있는 S, M값이 없으므로 불법적으로 복사를 하였다 하더라도 Agent와 Front-Middle Server에서 생성하는 D와 L을 계산할 수 없으므로 승인을 받을 수 없다. 또한 사용자가 정당한 방법으로 복사를 시도할 경우 Agent가 Front-Middle Sever에 복사 권한을 가지고 있기 때문에 불법적으로 복사할 수 없다. 다른 경우는 오프라인에서 복사를 시도할 경우 Agent 내에 Front-Middle Server의 권한이 없으면 그 컨텐츠에 대해 복사 실행을 주지 않으므로 컨텐츠에 대한 불법 복사를 없앨 수 있다. 불법 복사가 행해져 파일이 유통되는 경우에는 컨텐츠 내부에 Agent가 ID값을 가지고 있으므로 컨텐츠에 대한 책임을 확인 할 수 있다.

6. 결 론

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

본 논문은 Agent를 이용한 불법 복제 방지 DRM 모델을 제시하였다. 기존 시스템에 변경 없이 사용할 수 있고, 사용자가 Agent의 여부를 알지 못한다. 또한 Agent는 별도의 설치 없이 컨텐츠 내에 위치하도록 하였다. 이러한 Agent를 이용하여 불법복제를 방지함으로써 전체적인 DRM모델에 쉽게 접근할 수 있을 것이다.

참고 문헌

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

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

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

[4] N. R. Wagner, "Fingerprinting:, IEEE Symposium on Security and Privacy, 1983

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

[7] http://www.uspto.gov

[8] http://www.metarights.com

[4] G, Vigna, "Cryptographic traces for Mobile Agents", In:G.Vigna(Ed.), Mobile Agents and Security, Springer-Verlag, Lecure Note in Computer Science 1419, pp 137-153, 1998