임베디드 컴퓨팅 환경에서 은닉 에이전트를 이용한 불법복사 방지 모델에 관한 연구

이덕규* · 한종욱* · 정교일*

*한국전자통신연구원

A Study on a Illegal Copy Protection Model using Hidden Agent in Embedded Computing Environment

Deok Gyu Lee* · Jong Wook Han* · Kyo Il Chung*

*Electronics and Telecommunications Research Institute

E-mail : deokgyulee@etri.re.kr

요 약

최근 디지털 컨텐츠의 지적 재산권 보호를 위한 디지털 워터마킹 기술 및 핑거프린팅의 연구가 활발히 진행되고 있다. DRM(Digital Rights Management)는 디지털 콘텐츠 지적 재산권 보호뿐만 아니라 콘텐츠에 대한 출판, 유통 및 사용에 필요한 관리와 보호체계이다. 본 논문에서는 콘텐츠 유통 과정에서 발생할 수 있는 불법 복사와 같은 불법 행동에 대해 콘텐츠를 안전하게 보호하며 사용자에게 편의성을 제공 할 수 있는 프로토콜을 제시할 것이다. 이를 위해 콘텐츠 불법복사 및 불법사용을 방지할 수 있도록 은닉 에이전트(Hidden Agent)를 이용한다. 이 은닉 에이전트는 특별한 설치가 필요 없이 콘텐츠 내에 내포되어 있어 불법복사 및 불법사용에 대해 체크함으로써 불법복사의 사용을 차단할 수 있도록 한다. 또한 사용자들에게 숨겨져 있기 때문에 워터마킹의 역할 또한 대신할 수 있다.

ABSTRACT

There have been researches into digital Watermarking technology or Fingerprinting vigorously to safeguard Protective rights for knowledge and poverty for digital contents. DRM(Digital Rights Management) is not only Protective rights for knowledge and poverty, but also management and systems that are necessary to put out, circulate and use for contents. This paper proposes two kinds of ideas. One is protecting contents from illegal acts such as illegal copies when the contents are in the process of circulation. The other is the protocol that can give users convenience. Hidden Agents are used so that contents are protected from illegal copies and illegal use in the contents and cuts off those illegal acts. The Agent will be installed without any special setup. In addition, it can replace roles of Watermarking as a protection. Therefore, this paper shows the solution of illegal copies that happens frequently.

키워드

Embedded Computing, Hidden Agent, Illegal Copy Protection

Ⅰ. 서 론

전자 상거래를 통해서 디지털 콘텐츠 판매가 활성화되기 위해서는 지적 재산권 보호에 대한 연구가 선행되어야 한다. 디지털 콘텐츠는 일반적인 오프라인 콘텐츠와는 달리 쉽게 복사 및 배포가 가능하다는 특성이 있다. 따라서 합법적인 구매자가 판매자로부터 디지털 콘텐츠를 구입한 후, 이것의 불법적인 재분배(redistribution)를 막을 수 있는 방법이 고려되어야 한다.

디지털 콘텐츠를 안전하게 보호하기 위한 응용기술로는 디지털 콘텐츠 유통/서비스를 위한 저작

권 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 콘텐츠를 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. 이러한 모델에서의 문제점은 특별한 개체가 필요하다는 것이다. 이러한 문제점을 해결하고자 다음과 같은 불법복사를 방지할 수 있는 DRM모델을 제시하고자 한다. 본고에서는 이전에 제시되었던 전용플레이어나 스마트카드의 이용 없이 콘텐츠 안에 포함된 에이전트를 이용하여 컨텐츠의 불법복사를 방지하고자 한다.

II. 제안 방식

본고에서는 은닉 에이전트를 이용하여 불법복사를 방지하고자 한다. 전체적인 모델에서 초기 콘텐츠에 대한 워터마크 삽입과 지불에 관한 부분은 기존의 시스템을 이용하도록 한다.

1. 제안 방식에서의 은닉 에이전트 요구사항

은닉 에이전트는 다음과 같은 요구 사항을 필요로 한다.

(1) 은닉 에이전트는 콘텐츠 내부에 존재한다.

(2) 은닉 에이전트는 콘텐츠 제공 후 실행한다.

(3) 은닉 에이전트는 Boot시 항상 로드된다.

(4) 은닉 에이전트는 생성인자와 제공인자를 포함한다.

(5) 은닉 에이전트 내부에 존재하는 T는 COPY 명령시에 변하게 된다.

2. 전체 시스템 모델

본 모델에서는 크게 4단계로 나누어 볼 수 있다. 콘텐츠 생성 단계, 콘텐츠 제공 단계, 콘텐츠 지불 단계, 콘텐츠 불법 복사 확인 단계로 이뤄졌다. 각 단계에 대해 간략히 살펴보면 다음과 같다. 콘텐츠 생성 단계는 원본 데이터 처리를 통해 저작권이 포함된 콘텐츠를 제작하는 단계이며, 콘텐츠 지불 단계, 콘텐츠 제공 단계, 콘텐츠 불법 복사 확인 단계는 불법적인 복사자 혹은 정당한 복사자를 대상으로 하는 단계로 구성된다.

3. 구성 요소

다음은 본 시스템에서 구성하는 개체에 대하여 설명한다.

(1) 사용자(User) : 콘텐츠 구매를 원하는 자로써 콘텐츠에 대한 지불 및 사용권을 갖는다. CP(Contents Provider) Master Server와 함께 콘텐츠를 제공받기 위한 키를 생성한다.

(2) CP Master Server : 사용자(User)의 등록을 맡으며 콘텐츠에 대한 소유권을 갖는다. 사용자(User)와 같이 콘텐츠 제공을 위한 키를 생성한다.

(3) CP Front-Middle Server : 불법 복사 방지를 위하여 콘텐츠 속에 제공된 은닉 에이전트와의 통신을 한다. 본 개체에는 CP Master Server로부터 사용자(User)의 자료를 전송 받는다. 은닉 에이전트로부터 수신된 사용자(User)의 정보를 바탕으로 사용자(User)에게 복사할 수 있는 권한을 부여한다.

(4) Payment Server : 지불을 위한 개체로써 사용자(User)와 CP Master Server 사이에 위치하게 된다.

(5) Contents Database : 저작권자로부터 Watermarking된 콘텐츠를 제공받게 된다. Contents Database는 저작권자가 CP인 경우, CP가 저작권을 갖게 되며, 반대로 저작권자가 다르게 존재할 경우 Contents Database가 저작권을 갖는다.

(6) CA(Certificate Authentication) : 서명 값을 이용하기 위해 구성되며, 후에 지불시스템과 Contents Database 등에 활용될 수 있다.

5. 시스템 계수

다음은 본 논문에서 콘텐츠 제공을 위한 키 교환과 은닉 에이전트에 필요한 시스템 계수에 대해 설명한다.

- U : 사용자(User)
- MS : CP Master Server
- FS : CP Front-Middle Server
- ID : 사용자의 ID
- L : Hash Value. : $L = H(ID \| D)$
- K_A :은닉에이전트에서 사용되는 암호화 키
- T : Time-Stamp
- Sig_{user} : 사용자의 서명값
- Sig_{MS} : CP Master Server의 서명값
- A : 은닉 에이전트
- D : 권한종류(복사횟수, 사용 횟수 권한 등)
- p : 사용자가 공개한 소수(Prime Number)
- g : 사용자가 공개한 GF(P)의 원시근
- Y^*, X^* : *의 공개키와 개인키
- K : 콘텐츠 제공을 위한 암호화 키
- S : 콘텐츠 종류 (Contents Class)
- M : 지불가 (Payment Value)
- R: 은닉 에이전트 생성값
- C : 제공되는 콘텐츠(Contents)

6. 제안 프로토콜

본 방식에서 사용되는 은닉 에이전트가 콘텐츠(Contents)에 포함되어 제공되고 있다. 은닉 에이전트는 복사 시 자신의 생성인자와 제공인자를

통하여 불법복사에 대한 권한을 제한한다. 다음은 각 단계에 대하여 자세히 기술한 것이다.

DRM은 총 4단계로 구성되며 콘텐츠 생성단계, 콘텐츠 제공단계, 콘텐츠 지불 단계, 콘텐츠 불법 복사 확인 단계로 이루어진다. 이 중에서 콘텐츠 지불 단계는 제외하며 지불에 관한 사항은 기존 시스템을 따르는 것으로 한다. 또한 제안방식에서는 콘텐츠 제공단계와 콘텐츠 불법 복사 확인 단계를 중점으로 기술한다. 다음은 각 단계별로 자세히 기술한 내용이다.

6.1 콘텐츠 제공 단계

다음은 콘텐츠를 제공하는 단계로서 사용자(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 과정을 진행한다.

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

Phase 2. 콘텐츠를 제공받기 위하여 콘텐츠를 암호화할 수 있는 키를 먼저 교환하여야 한다. 이를 위해 사용자는 g,p를 공개하고 사용자의 비밀값 X_{user}를 이용하여 다음 Y_A를 계산한 후, 사용자의 ID, Y_A, S값을 서명하여 전송한다.

$$U:\ Y_A \equiv g^{X_{user}} \bmod p$$

$$U \rightarrow MS:\ Y_A \parallel Sig_{user}(ID \parallel Y_A \parallel S)$$

$$MS:\ D = S + M,\quad L = H(ID \parallel D)$$

Phase 3. CP 서버는 사용자로부터 받은 값을 이용하여 서버의 비밀값 X_{MS}를 이용하여 K를 계산한다. 다음 서버의 비밀값 X_{MS}를 이용하여 Y_B를 계산한 후 서버는 사용자에게 Y_B값과 함께 서버의 Y_B, S, M을 서명하여 전송한다.

$$MS:\ K \equiv \left(g^{X_{user}}\right)^{X_{MS}} \bmod p = Y_A^{X_{MS}} \bmod p = Y_B^{X_{user}} \bmod p$$

$$MS:\ Y_B \equiv g^{X_{MS}} \bmod p$$

$$MS \rightarrow U:\ Y_B \parallel Sign_{MS}(Y_B \parallel S \parallel M)$$

Phase 4. 사용자는 *CP* 서버로부터 받은 Y_B를 이용하여 키 값 K를 계산하고 키 교환 종료 메시지를 전송한다.

$$U:\ K \equiv \left(g^{X_{MS}}\right)^{X_{user}} \bmod p = Y_B^{X_{user}} \bmod p = Y_A^{X_{MS}} \bmod p$$

$$U \rightarrow MS:\ Finish\_Message$$

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

$$MS \rightarrow FS:\ (ID,\ L,\ D,\ M,\ S,\ T)$$

Phase 6. Master Server는 콘텐츠에 대해 사용자에 알맞은 은닉 에이전트를 삽입한 후 전송한다. 이때 T는 복사되는 시점을 가지는 것으로 만약 COPY 시 T 값은 변화하게 된다. 콘텐츠 내에 에이전트(Agent)와 Time Stamp값(T)이 포함되어 전송되어진다.

$$MS \rightarrow U:\ E_K(C_{(A \parallel T)})$$

6.2 콘텐츠 불법 복사 확인 단계

다음은 콘텐츠에 대해 사용자가 복사를 원하거나 불법 복사가 이루어졌을 경우 은닉 에이전트의 동작에 대해 기술한다.

앞에서의 설명과 같이 은닉 에이전트는 콘텐츠 제공과 함께 동작된다. 사용자가 OS상에서 COPY, MOVE와 같은 명령이 동작할 경우 은닉 에이전트가 동작하게 되며 서버로부터 받은 키를 이용하여 ID, S, M, L을 암호화하여 Front-Mid dle Server에게 전송한다.

이때 은닉 에이전트 내부에 있는 T값은 초기 T값을 의미한다. 또한 Front-Middle Sever는 은닉 에이전트와의 작업만 하게 된다.

만약 은닉 에이전트가 서버와 연결할 수 없다면 복사 권한은 부여되지 않는다.

Phase 1. 사용자(User)의 컴퓨터상에서 COPY 명령이 실행될 경우 자동으로 은닉 에이전트는 수행되며, S, M, T(은닉 에이전트의 내부인자)에 대하여 암호화 후 Front-Middle Server에 전송한다.

$$U \rightarrow FS:\ E_{K_A}(ID \parallel S \parallel M \parallel L \parallel T)$$

Phase 2. Front-Middle Server는 받은 ID, S, M을 이용하여 D와 L을 계산 후, 자신이 가지고 있는 DB의 내용과 비교하여 복사 권한을 부여한다. 은닉 에이전트와 CP Front Middle Server에 있는 T값을 비교하여 불법적인 복사가 이루어졌는지 확인한다.

$$FS:\ Compute\ \ D = S + M$$
$$L = H(ID \parallel D)$$

$$Compare\ \ T\ \ T',\ Compare\ \ D\ \ D',\ Compare\ \ L\ \ L'$$

$$FS \rightarrow U:\ E_{K_A}(ID \parallel Yes \text{ or } No)$$

III. 제안 시스템 고찰

본고에서는 은닉 에이전트를 이용하여 불법 복사를 방지하였다. 콘텐츠 내부에 은닉 에이전트를 포함시킴으로써 사용자로부터는 컨텐츠의 사용권에 대해 권한을 제약(일부 사용권 부여)하였고, CP로부터는 소유권을 부여하였으며, 원본 제작자로부터는 저작권을 부여하였다.

불법 복사자로부터 콘텐츠 보호의 경우에 사용자에게 있는 초기 T값이 없으므로 불법적으로 복사를 하였다 하더라도 은닉 에이전트와 Front-Middle Server에서 생성하는 D와 L을 계산할 수 없으므로 승인을 받을 수 없다. 콘텐츠 복사에 의한 불법 복사 시도 시 생성되는 T값이 변화되기 때문에 불법복사를 막을 수 있다.

또한 사용자가 정당한 방법으로 복사를 시도할 경우 은닉 에이전트가 Front-Middle Sever에 복사 권한을 가지고 있기 때문에 불법적으로 복사할

수 없다. 다른 경우는 오프라인에서 복사를 시도할 경우 은닉 에이전트 내에 Front-Middle Server의 권한이 없으면 그 콘텐츠에 대해 복사 실행을 주지 않으므로 콘텐츠에 대한 불법 복사를 없앨 수 있다. 불법 복사가 행해져 파일이 유통되는 경우에는 콘텐츠 내부에 은닉 에이전트가 *ID*값을 가지고 있으므로 콘텐츠에 대한 책임을 확인 할 수 있다.

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 제 3자에게 배포시에 은닉 에이전트와 CP Front-Middle Server의 키 값이 있다. 또한 은닉 에이전트 내부적으로 생성되는 *R*값이 있기 때문에 MP3 데이터의 불법 유통을 방지할 수 있다. 또한 본 방식에서는 에이전트를 이용하여 복사에 대한 권한만 제한하고 있지만 기존 시스템에서는 매 콘텐츠에 대하여 인증을 통과해야만 콘텐츠에 대한 플레이가 가능하다. 처음 콘텐츠에 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 콘텐츠를 사용하는 방식과 같이 사용할 수 있다.

Ⅳ. 결 론

현재 DRM에 관하여 많은 연구가 진행 중에 있다. DRM모델에서 유통과 관리부분 중 콘텐츠에 대한 보호는 전체 모델에서 가장 핵심적인 부분이라 할 수 있다. 기존에 사용되었던 전용 플레이어를 이용한 방식, 스마트카드를 이용한 방식 등이 가지고 있었던 문제점을 해결하려 하였으며, 사용자에게 불편을 주는 매번 인증을 통한 콘텐츠 제공방식을 해결하려 노력하였다. 본 논문은 은닉 에이전트를 이용한 불법 복사 방지 DRM 모델을 제시하였다. 기존 시스템에 변경 없이 사용할 수 있고, 사용자가 은닉 에이전트의 여부를 알지 못한다. 전용 플레이어를 통한 제공이 아니기 때문에 향후 유·무선 분야에서 사용될 수 있으리라 본다. 또한 은닉 에이전트는 별도의 설치 없이 콘텐츠 내에 위치하도록 하였다. 이러한 은닉 에이전트를 이용하여 불법복사를 방지함으로써 전체적인 DRM모델에 쉽게 접근할 수 있을 것이다. 또한, 은닉 에이전트는 콘텐츠와 연관되어 실행되지만 사용자와는 무관하게 동작되고 사용자에게는 에이전트의 실행이 보이지 않기 때문에 사용자마다 은닉 에이전트를 생성할 때 사용자 정보를 삽입하거나 제공자 정보를 삽입한다면 후에 불법 복제 등 여러 가지 문제가 발생하였을 경우에는 이 정보를 확인하여 불법 사용자를 확인할 수 있다. 이와 같은 방법으로 은닉 에이전트는 워터마킹의 역할로서 사후의 보안을 담당할 수 있을 것이다.

향후 연구 과제로는 원본 콘텐츠에 대한 소유권과 지불을 적용한 방식, 익명 사용자를 위한 콘텐츠 제공 등을 포함하여야 할 것으로 본다. 이러한 DRM 기술이 연예/오락용 디지털 콘텐츠의 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]Microsoft Windows Media Rights Manager SDK(Software Development Kit) Manual

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

[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 콘텐츠 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

[9]http://www.dreaminitech.com

[10]http://www.fasoo.com

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

[12]http://www.markany.com

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

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

[15]임채덕, 김홍남, 박승민, 김두헌, 김선자, 김채규, 임기욱, "임베디드 소프트웨어 기술동향 및 산업발전 동향", 정보통신연구진흥지, 4권 3호, 2002

[16]권오혁, "Embedded System, RTOS", 삼성 SDS IT Review, 2003

[17]장정숙, 전용희, "임베디드 시스템 보안", 한국정보통신학회지, 22권 8호, pp 81-97, 2005