디지털 콘텐츠 유통 프레임워크에서 DRM적용방법 설계+

*전진영° *박진홍 *신용태 **이혜주 **홍진우
*숭실대학교 컴퓨터학과
**한국 전자 통신 연구원 전파방송연구소 방송미디어부
{nurnadly, elzk, shin}@cherry.ssu.ac.kr, {hyejoo, jwhong}@etri.re.kr

A Design of DRM Solution in a Distribution Framework of the Digital Content

Jinyoung Jeon°* Jinhong Park* Youngtae Shin* Hyejoo Lee** Jinwoo Hong**
*Dept. of Computing, Soongsil University
**Dept. of Broadcasting Media, Electronics & Telecommunications Research Institute

요 약

정부의 초고속 인터넷 환경을 구축하려는 적극적인 노력과 폭발적인 인터넷 사용자의 증가로 디지털 콘텐츠의 수요는 매우 커지고 있다. 앞으로 고부가가치 산업으로 발전이 예상되는 디지털 콘텐츠 사업에서 콘텐츠의 기밀성을 보장하고 저작권을 보호할 수 있는 유통 구조는 매우 중요한 것으로 판단된다. 본 논문은 현재 논의 되고 있는 디지털 콘텐츠 유통에 관련해 MPEG-21과 DRM 기술에 대해 개략 적으로 살펴본 후 콘텐츠 제공자, 유통 업자, DRM 서버, 이용자 시스템으로 이루어진 DRM 기반의 디지털 콘텐츠 유통 모델을 제안한다. 그리고 제시된 유통 구조에서 이용될 수 있는 유통 개체 간의 키 교환 기법을 제안한다.

1.서 론

최근 정부의 초고속 인터넷 환경을 구축하려는 적극적인 노력과 인터넷 사용자의 폭발적인 증가를 바탕으로 정보 통신 분야는 괄목할만한 성장을 거두었다. 이러한 성장을 바탕으로 디지털 콘텐츠의 수요는 매우 증가하고 있으며 여러 분야에서 다양한 요구가 발생하고 있다. 그러나 불법 소프트웨어 복제로 인한 무분별한 콘텐츠 불법 유통은 소프트웨어 산업 발전의 큰 저해요소로 자리 잡고 있다. 따라서 디지털 콘텐츠 산업의 성공적인 상용화를 위해서 디지털 콘텐츠의 기밀성을 유지하고 저작권을 보호할 수 있는 유통 프레임워크가 매우 절실히 요구되고 있다.

이미 디지털 콘텐츠의 저작권을 보호하기 위한 기술로 DRM(Digital Rights Management) 기술이 시장에서는 각광받고 있고, 이를 위해 워터 마킹을 비롯하여 다양한 보안 기술들이 국내 및 국외에서 지속적으로 연구 개발 중이다. 본 논문은 범용적인 DRM 기반의 디지털 콘텐츠 유통 구조와 이 유통 구조에서 요구되는 키 관리 기법을 제안한다.

본 논문은 2장에서 MPEG-21의 디지털 콘텐츠 유통 프레임워크와 DRM 기술을 살펴본 후 3장에서는 DRM 기반의 유통 프레임 워크와 키 관리 메커니즘을 제안한다. 마지막으로 4장은 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2.1. MPEG-21

MPEG은 디지털 오디오 및 비디오 관련 기술의 표준화 기구로 5개의 하위 워킹 그룹을 운용하고 있다. MPEG-21[1]은 하위 워킹 그룹의 하나로서 MPEG 기술을 바탕으로 멀티미디어 유통 프레임 워크에 대한 표준화를 추진하는 그룹이다. MPEG-21 프레임 워크는 DID, Content Representation, DII&D, Content Management & Usage, IPMP, Terminals & Networks, Event Reporting으로 구성된다. 여기서 IPMP는 Intellectual Property Management & Protection의 약자로 디지털 콘텐츠 유통의 보호 및 관리 수단을 의미하는 구성 요소이다. 이 안에는 암호화, 거래 인증, 워터 마킹 등의 기술들이 논의 되고 있으며, 현재 시장에서 크게 각광 받고 있는 DRM 기술 체계와 흡사하다.

2.2. DRM(Digital Rights Management)

DRM은 여러 가지 정의가 있을 수 있지만 대체적으로 온라인을 통해 디지털 콘텐츠를 유통시키는 데 있어 콘텐츠의 기밀성을 유지하고, 불법적인 재배포를 봉쇄하며, 콘텐츠에 대한 저작권을 유지·보호 하는 기술로 알려 지고 있다. 이를 위해 다양한 H/W, S/W 보안 기술들이 연구되고 있으며, 저작권을 정의하기 위한 XrML이나 ODRL 언어들이 표준화 과정 중에 있다. 콘텐츠의 암호화를 위해 가장 중요시 되는 키 관리 시스템과, 유통 구조에서 빼 놓을 수 없는 지불 연계 시스템, 저작권이나 사용 규칙을 안전하게 보관 및 관리 할 수 있는 시스템들은 많은 회사들이 자사의 기술을 표준으로 삼기 위해 경쟁하고 있는 기술들이다.

이러한 관련 연구를 바탕으로 본 논문은 좀 더 범용적인 DRM 기반의 디지털 콘텐츠 유통 모델을 제시하고자 한다.

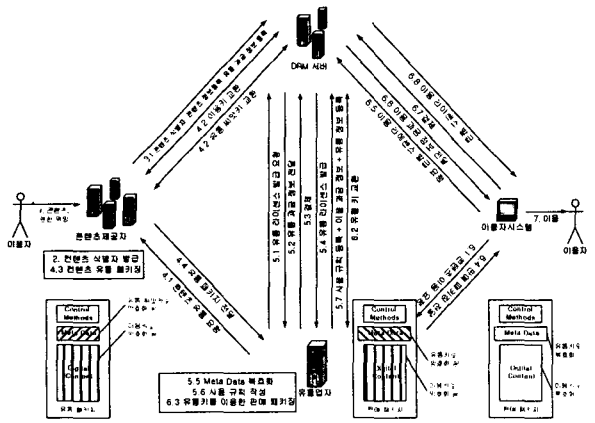
3.제안 시스템

+ 본 연구는 2003년 한국전자통신연구원 위탁과제의 지원으로 수행되고 있습니다.

이 논문에서는 범용적인 디지털 콘텐츠의 기밀성을 보장하고 저작권을 보호할 수 있는 DRM 기반의 유통 모델을 제시한다. 또한 이 모델에서 기밀성 보장을 위해 사용될 키 관리 기법을 제안하고자 한다. 각 유통 개체의 정의는 다음과 같다.

- 생성자 : 디지털 콘텐츠를 창작하고 콘텐츠 제공자에게 저작권을 위임하는 개체
- 콘텐츠 제공자 : 콘텐츠에 식별자를 부여하고 유통 패키지를 생성하는 개체
- 유통 업자 : 유통 패키지를 구매하여 비즈니스 모델을 적용한 후 판매 패키지를 생성
- DRM 서버 : 콘텐츠 접근·이용 제어, 유통 과정 모니터링, 과금 처리, 유통 개체 인증
- 이용자 시스템 (이용자) : 디지털 콘텐츠의 수요자
- 유통 패키지 : 콘텐츠 제공자가 유통을 위해 생성하는 패키지, 두개의 키로 암호화 됨
- 판매 패키지 : 유통 업자가 판매를 위해 생성하는 패키지, 비즈니스 모델이 적용 됨

3.1. 제안하는 DRM 기반의 디지털 콘텐츠 유통 모델



[그림 1] DRM 기반의 디지털 콘텐츠 유통 모델

[그림 1]과 같이 제안된 DRM 기반의 디지털 콘텐츠 유통 모델은 4개의 개체로 이루어져 있고 크게는 DRM 서버와 특화된 DRM 클라이언트들로 이루어진 서버/클라이언트 구조이다. 콘텐츠를 유통 시키는 개체들은 콘텐츠를 메타 정보 및 제어 함수들과 함께 암호화 시켜 패키지로 유통 하고 이 정보들을 DRM 서버에 저장한다. 콘텐츠를 이용하는 개체는 암호화된 패키지를 유통 개체들로부터 전달 받고 DRM 서버가 발급하는 라이선스를 구매하여 콘텐츠를 이용할 수 있다. 이 유통 구조는 유통키와 이용키를 이용해 콘텐츠 유통과 이용에 대한 접근을 따로 제어하기 때문에 유통 과정 중 각 개체 내부에서 디지털 콘텐츠가 유출 될 수 있는 위험을 감소시킨다. 비록 유통 업자라 하더라도 유통 패키지 안에 있는 디지털 콘텐츠를 직접 이용할 수 없기 때문에 콘텐츠 제공자는 유통 패키지를 만들면서 메타 데이터에 진열(Display) 정보를 추가해야 한다. 유통 업자는 이 진열 정보가 들어 있는 메타 데이터를 처리하여 디지털 콘텐츠에 직접 접근하지 않고도 콘텐츠를 광고 하고 유통시킬 수 있다. 이러한 유통 모델을 위해 라이선스도 유통 라이선스와 이용 라이선스 두 가지 종류가 있어야 한다.

3.2. 디지털 콘텐츠 유통 과정

3.1 절에 제시된 DRM 기반의 디지털 콘텐츠 유통 프레임워크에서 디지털 콘텐츠가 유통되는 과정을 살펴보자. 이 장에서는 전체적인 흐름을 설명하면서 [그림 1]에 나타난 유통 과정에 부합하는 설명 뒤에는 진한 색으로 과정 번호를 나타내었다. 유통 과정은 크게 콘텐츠 제공자와 유통 업자 사이에 일어나는 유통 과정과 유통업자와 이용자 사이에 일어나는 이용 과정으로 나눌 수 있다.

- 유통 과정

창작자는 자신이 생성한 콘텐츠를 저작권과 함께 콘텐츠 제공자에게 위임한다(1). 콘텐츠 제공자는 창작자로부터 받은 콘텐츠에 대해 콘텐츠 식별 자를 발급하고(2), DRM 서버에 콘텐츠 식별 자, 콘텐츠 기술 정보(제목, 장르 등), 진열 정보(요약 콘텐츠, 인덱스 등), 유통 과금 정보 등을 등록한다(3.1). 유통 업자는 콘텐츠 서버가 제공하는 콘텐츠 리스트 중에서 자신의 비즈니스 성향에 맞는 콘텐츠에 대해 유통 요청을 한다(4.1). 콘텐츠 제공자는 메타 데이터와 콘텐츠 암호화를 위해 사용될 유통 씨앗 키와 유통키를 DRM 서버와 교환한 후(4.2) 유통 씨앗 키로 메타 데이터를, 이용키로는 콘텐츠를 암호화 하여 유통 패키지를 생성한다(4.3). 이렇게 생성한 유통 패키지는 콘텐츠 제공자가 유통 업자에게 전달한다(4.4).

- 이용 과정

유통 업자는 콘텐츠 제공자로부터 받은 유통 패키지에 대해 유통 라이선스 유/무를 확인한 후 없을 경우는 DRM 서버에 유통 라이선스 발급 요청을 하게 된다(5.1). 유통 라이선스 발급 요청을 받은 DRM 서버는 유통 과금 정보를 유통 업자에게 전달하고(5.2) 유통 업자가 과금 정보에 따라 결제한 것이 확인되면(5.3) 등록된 유통 씨앗 키를 포함하는 유통 라이선스를 발급하게 된다(5.4). 유통 라이선스를 획득한 유통 업자는 유통 라이선스를 이용해 유통 패키지 내 진열 정보 등의 메타 정보를 추출(5.5)할 수 있고 유통 업자만의 비즈니스 모델에 맞게 콘텐츠 사용 규칙(이용 기간, 이용 횟수 등)을 작성한다(5.6). 유통 업자는 이렇게 작성한 사용 규칙을 비롯해 이용 과금 정보, 유통 정보를 DRM 서버에 등록하게 된다(5.7). 이용자는 유통업자가 진열한 콘텐츠 중에서 이용 하고자 하는 콘텐츠에 대해 콘텐츠 이용 요청을 하게 되고(6.1) 유통 업자는 판매 패키지 생성을 위해 DRM 서버와 유통키를 교환하게 된다(6.2). 유통 업자는 교환한 유통키를 이용해 자신의 비즈니스 모델이 첨가된 메타 데이터를 암호화 하여 판매 패키지를 생성하고(6.3) 이 패키지를 이용자에게 전달한다(6.4). 이용자는 자신에게 판매 패키지에 대한 이용 라이선스 유/무를 확인한 후 없을 경우 DRM 서버에 이용 라이선스 발급 요청(6.5)을 한다. DRM 서버

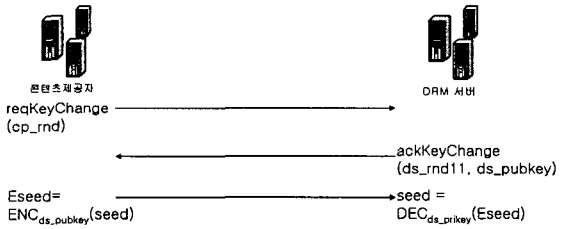
는 이 용청에 대해 이용 과금 정보를 이용자에게 전달하고(6.6) 이용자는 이 정보에 따라 결제한다(6.7). 결제가 확인 되면 DRM 서버는 등록된 유통키와 이용키를 포함하는 이용 라이선스를 발급하고(6.8) 이용자는 이 라이선스를 통해 콘텐츠를 이용할 수 있다(7).

3.3. 제안하는 키 관리 시스템

제안하는 키 관리 기법은 디지털 콘텐츠의 불법적인 유통을 막기 위해 제안된 유통 모델에서 사용된다. 수식에 대한 정의는 다음과 같다.

- ENC : 암호화, Rijndael 대칭키 암호화알고리즘을 사용 [2]
- DEC : 복호화, Rijndael 대칭키 암호화알고리즘을 사용
- MD5 : MD5 해쉬 함수 [3]
- SHA1 : SHA1 해쉬 함수 [4]
- UKF(Use-Key Function) : 이용키 함수
- DFK(Distribute-Key Function) : 유통 씨앗 키 함수
- || : byte concatenation, XOR : exclusive OR

3.3.1 콘텐츠 제공자와 DRM 서버간의 키 교환



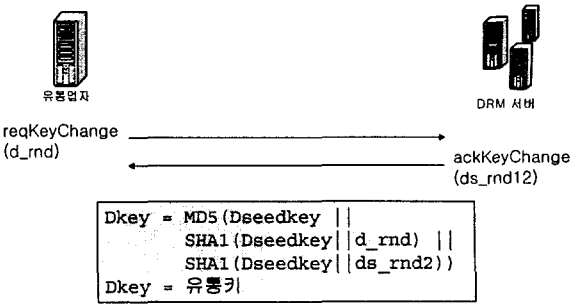

```
UKF(a, b, c, d) = MD5(a || MD5(b || c)) XOR MD5(a || MD5(b || d))
DKF(a, b, c, d) = MD5(a || SHA1(b || c)) XOR MD5(a || SHA1(b || d))

seekKey = MD5(seed || MD5(seed || cp_rnd) ||
                      MD5(seed || ds_rnd1))
useKey= MD5(seedKey || UKF(seedKey, seed, ds_rnd1, cp_rnd))
DseedKey= MD5(seedKey || DKF(seedKey, seed, ds_rnd1, cp_rnd))
useKey = 이용키, DseedKey = 유통 씨앗 키
```

[그림 2] 이용키, 유통 씨앗 키 교환

[그림 2]는 콘텐츠 제공자와 DRM 서버 사이에 유통 씨앗 키와 이용키를 교환하는 방법을 보여주고 있다. 콘텐츠 제공자는 DRM 서버에 키 교환을 요청하면서 자신이 생성한 임의의 값(cp_rnd)을 전달한다. DRM 서버는 이에 대한 응답으로 임의 값(ds_rnd1)과 함께 자신의 공용키(ds_pubkey)를 콘텐츠 제공자에게 전달한다. 콘텐츠 제공자는 모든 키 값의 씨앗 값이 되는 임의의 값(seed)을 생성하여 이를 ds_pubkey로 암호화 하여 DRM 서버에 전달한다. 콘텐츠 서버와 DRM 서버는 이렇게 cp_rnd, ds_rnd, seed 값을 공유한 후 [그림 2]에 제시되어 있는 연산 식에 따라 이용키와 유통 씨앗 키를 각각 생성한다.

3.3.2 유통 업자와 DRM 서버간의 키 교환



[그림 3] 유통키 교환

[그림 3]은 유통업자와 DRM 서버 사이에 유통키를 교환하는 과정을 보여주고 있다. 유통 업자는 DRM 서버에 키 교환을 요청하면서 자신이 생성한 임의 값(d_rnd)을 전달한다. DRM 서버는 새로 생성한 임의 값(ds_rnd2)을 응답으로서 보낸다. 이렇게 임의 값을 교환 한 후 서로 보관하고 있는 유통 씨앗 키와 함께 [그림 3]에서 제시한 연산 식에 따라 유통키를 생성한다.

4. 결론 및 향후연구 방향

본 논문에서는 고 부가가치 산업으로 발전이 예상되는 디지털 콘텐츠 산업을 위해 디지털 콘텐츠를 안전하게 유통하고, 이에 대한 저작권을 유지할 수 있는 유통 프레임 워크를 제안하였다. 또한 이 유통 구조에서 이용될 수 있는 유통 개체 간에 키 교환 메커니즘을 제안하였다. 제안된 유통 구조는 콘텐츠 유통과 이용에 대한 제어를 분리함으로써 유통의 안정성을 높이고, 유통업자가 자신의 비즈니스 모델을 적용할 수 있는 장점이 있다.

제안된 유통 모델에서 DRM 서버의 과부하를 줄일 수 있도록 분산 DRM 서버 구성이 필요하고, 유통 라이선스와 이용 라이선스를 효율적으로 관리하기 위한 라이선스 관리 기술과 함께 콘텐츠 재배포를 위한 기술들이 필요하다고 판단된다. 향후 위에서 언급한 기술들을 고려하여 본 논문에서 제안한 유통 모델을 구현할 예정이다.

참고 문헌

[1] http://www.chiariglione.org/mpeg/standards.htm

[2] Joan Daemen and Vincent Rijmen, "The Rijndael Block Cipher", September 2003 http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf

[3] Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321, April 1992.

[4] D. Eastlake 3rd, P. Jones., "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001