# 저작권 보호를 위한 안전한 DRM 메커니즘 설계

유성진°, 김성열*, 정일용°
조선대학교 전자계산학과°, 울산과학대학 컴퓨터정보학부*

# Design of Secure DRM(Digital Rights Management) Mechanism for Copyright Protection

Seong-Jin Yoo°, Seong-Yeol Kim*, Il-Young Chung°
Dept. of Computer Science, Chosun University°
School of Computer Information, Ulsan College*

**요 약**

인터넷의 확산과 더불어 디지털 컨텐츠의 유통도 확산되었다. 그러나 디지털 컨텐츠들은 쉽게 원본과 똑같은 품질로 복제할 수 있으며, 인터넷을 통해 빠르게 이동이 가능하고 사용자들은 얼마든지 불법으로 이용할 수 있다는 것이다. 최근 국내·외에서 이러한 문제를 해결하기 위해 디지털 컨텐츠들을 보호하고 관리할 수 있는 DRM 기술이 활발히 연구 중이다. DRM 기술은 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호하고 디지털 컨텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리 할 수 있는 기술이다. 본 논문에서는 저작권 보호를 위해 안전한 DRM 메커니즘을 제안한다.

## 1. 서론

인터넷의 확산과 더불어 각종 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 텍스트, 동영상, 음악, 전자북등 멀티미디어 자료에 대한 수요가 급격히 증가하고 있다. 그러나 디지털 자원은 품질의 손상 없이 쉽게 복제가 가능하고 이렇게 복제된 디지털 자원은 인터넷을 통하여 쉽게 유통된다. 그러므로 디지털 자원에 대한 보호가 필요하다. 디지털 컨텐츠의 보호와 관리를 위해서는 정보보호기술과 디지털저작권을 관리하고 컨텐츠 유통 전반을 감시, 추적하는 디지털저작권 관리 (DRM : Digital Rights Management) 기술이 필요하다.

정보보호기술의 경우 암호화 기술, 디지털워터마킹 기술에 관한 연구를 통하여 인증된 많은 기술들이 등장하고 있다[1].

DRM 기술의 경우, 디지털 컨텐츠에 대한 지적 재산권 침해사례로부터 저작권을 보호하고 유통과정을 관리하기 위한 종합적인 대책의 일환으로 추진되고 있으며 저작물에 대한 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어 질수 있도록 하는 다양한 연구가 진행 중에 있다[2,3].

본 논문에서는 정보보호 기술을 이용하여 안전한 DRM 메커니즘을 설계 한다. 2장에서는 관련 기술들에 대하여 기술하고, 3장에서는 안전한 DRM 메커니즘을 제안하였다. 마지막으로 4장에서는 결론을 내리고자 한다.

## 2. 관련 연구

### 2.1 암호화 기술

암호화 기술은 비밀키(대칭키) 방식과 공개키 방식이 있는데 비밀키 방식은 암호화 할 때의 키와 복호화 할 때의 키가 같고, 키는 통신 당자만 알고 있도록 비밀을 유지해야 한다. 공개키(비대칭) 방식은 암호화 할 때의 키와 복호화 할 때의 키가 서로 다르다. 암호화 할 때의 키를 공개키라고 하고 복호화 할 때의 키를 개인키라고 한다. 공개키는 공개를 하고 개인키는 개인만 알고 있도록 비밀을 유지해야 한다. 그리고 개인키를 이용하여 전자서명을 수행 할 수 있다. 비밀키 방식과 공개키 방식은 둘 다 기밀성, 무결성, 인증을 제공한다. 하지만 비밀키 방식은 전자 서명 기능을 수행할 수 없고 공개키 방식에서만 전자 서명을 수행

할 수 있다. 전자 서명은 개인키 이용하여 생성하고 공개키를 이용하여 전자서명을 검증한다[4].

### 2.2 디지털 워터마킹

디지털 워터마킹 기법은 디지털 컨텐츠에 저작자의 고유한 정보를 삽입하여 지적재산권 및 저작권을 보호하고 소유권을 주장할 수 있는 근거를 제시 할 수 있도록 하는 기술이다. [그림 1]은 디지털 워터마크 기술을 나타낸 것이다.

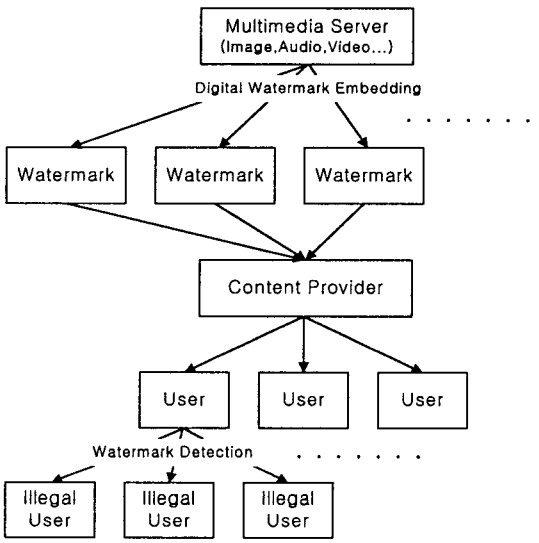


그림 1. 디지털 워터마크 기술

이러한 디지털 워터마킹은 다음과 같은 다양한 특성 및 요구조건을 만족해야 한다. 먼저 워터마크를 삽입 하였을 때 컨텐츠의 원본과 워터마크가 삽입된 컨텐츠의 구별이 어렵고 품질을 유지해야 하는 비가시성, 여러 가지 형태의 변형이나 공격에도 추출이 가능해야 하는 강인성, 추출된 워터마크가 확실한 소유권을 주장할 수 있어야 되는 명확성, 관련 키값 등을 알고 있을 경우에만 워터마크의 확인이 가능한 보안성, 그리고 원본 컨텐츠 없이 워터마킹된 컨텐츠만으로 워터마크를 검출 할 수 있는 블라인더 기법이 요구되고 있다[5,6].

### 2.3 DRM 기술

DRM은 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 컨텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템이다. 즉, 디지털 컨텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다[7,8].

DRM 시스템에 있어 가장 중요한 기술은 암호화 기술로서 고객의 비밀번호 혹은 고객 컴퓨터의 고유번호를 암호 키로 사용하여 컨텐츠를 암호화하여 전달하기 때문에 이를 복사하여 제 3자가에게 전달하여도 키가 없이 풀리지 않도록 하는 점이 중요하다. 또한 컨텐츠의 전파가 물론 이외에도 컨텐츠 사용규칙, 제어기술, 과금 결제를 위한 기술 등의 부대적인 기술들이 필요하다[9].

## 3. 안전한 DRM 메커니즘

### 3.1 Notation

표기법은 [표 1]을 따른다.

<표 1> 제안된 프로토콜 표기법

| 표기 | 설명 |
|---|---|
| CP | 컨텐츠 제공자 |
| C | 사용자 고객 |
| S | 상서래 서버 |
| PG | 지불 게이트웨이 |
| Auth | 인증기관 |
| DRM | Digital Rights Management 서버 |
| Cons | 컨텐츠 |
| S/W | 디지털 컨텐츠를 사용 할 수 있는 전용 Software |
| Req(i) | i를 요청 |
| Pay | 지불 |
| ConsInfo | 컨텐츠 정보(가격, 규칙 등) |
| KeyInfo | 컨텐츠 암호화키 생성 정보 |
| PayInfo | 지불 정보 |
| $PayRe_i$ | i를 위한 지불 결과 |
| $PK_i$ | i의 공개키 |
| $SK_i$ | i의 개인키 |
| $Cert_i$ | i의 인증서 정보 |
| $K_{cs}$ | C와 S의 공유된 세션키 |
| $K_s$ | 컨텐츠 암호화 키 |
| A \|\| B | A와 B 데이터의 연접 |
| $E_k[m]$ | k를 이용하여 m을 암호화 |
| h{m} | m을 해쉬 함수로 수행 |
| Time | 타임스탬프 |

### 3.2 컨텐츠 등록

컨텐츠 제공자는 컨텐츠에 대한 저작물 관리, 고객 과금 처리, 저작물 사용권 이전, 컨텐츠를 암호화할 키 등과 같은 내용들을 합의하고 DRM Server에 등록한다. DRM Server는 등록에 관한 보고를 한다. 이 등록, 보고 과정은 오프라인 또는 온라인으로 안전하게 수행된다고 가정한다. 컨텐츠 등록은 [그림 2]와 같이 수행된다.

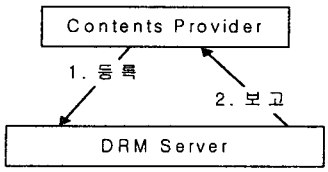


그림 2. 컨텐츠 등록

### 3.3 안전한 DRM 메커니즘

DRM 메커니즘은 등록된 컨텐츠를 안전하게 배포, 관리 하여 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리한다. 컨텐츠 제공 시스템은 [그림 3]과 같이 수행된다. 인증서의 경우 신뢰된 인증기관으로부터 발급받은 인증서이다.

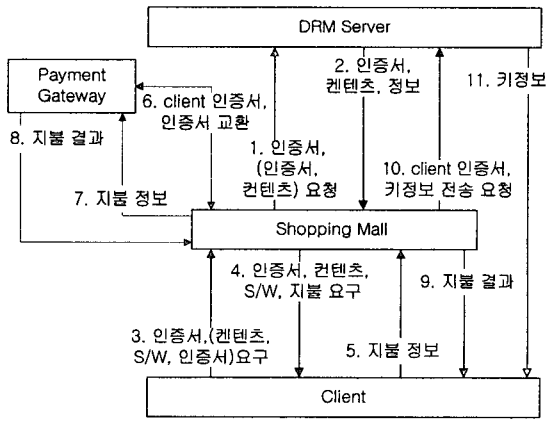


그림 3. DRM 메커니즘

1. S -----> DRM
   $SK_{Auth}[Cert_s]$, $Req(SK_{Auth}[Cert_{DRM}], Cons)$
2. DRM -----> S
   $SK_{Auth}[Cert_{DRM}]$, $E_{Ks}[Cons]$, $E_{PKs}[ConsInfo]$
3. C -----> S
   $SK_{Auth}[Cert_c]$,
   $Req(Cons, S/W, SK_{Auth}[Cert_s])$
4. S -----> C
   $SK_{Auth}[Cert_s]$, $E_{Ks}[Cons]$, S/W,
   $E_{PKc}[Req(Pay)]$
5. C -----> S
   $E_{PKs}[PayInfo, Time, Es_{Kc}h\{PayInfo, Time\}]$
6. S -----> PG
   $SK_{Auth}[Cert_c]$, $SK_{Auth}[Cert_s]$
   PG -----> S
   $SK_{Auth}[Cert_{PG}]$
7. S -----> PG
   $E_{PKPG}[PayInfo, Time,$
   $Es_{Ks}[h\{PayInfo, Time\}]]$
8. PG -----> S
   $E_{PKs}[[PayRe_s], E_{PKc}[PayRe_c], Time,$
   $E_{SKPG}[h\{[PayRe_s], E_{PKc}[PayRe_c], Time\}]]$
9. S -----> C
   $E_{PKc}[PayRe_c, Time, Es_{Ks}[h\{PayRe_c, Time\}]$
10. S -----> DRM
    $SK_{Auth}[Cert_c]$, $E_{PKDRM}[Req(KeyInfo)]$
11. DRM -----> C
    $E_{PKc}[KeyInfo]$

1. 쇼핑몰에서는 DRM Server에 자신의 인증서를 보내고, DRM Server의 인증서와 컨텐츠를 요청한다.

2. DRM Server는 자신의 인증서와 컨텐츠 제공자와 합의된 내용을 바탕으로 암호화된 컨텐츠와 정보를 전송한다. 컨텐츠는 컨텐츠 암호화키를 이용하여 암호화가 되어 있고, 컨텐츠 정보는 Shopping Mall의 공개키를 이용하여 암호화한다.

3. 고객은 자신의 인증서를 전송하고, 암호화된 컨텐츠, 컨텐츠 전용 S/W, 인증서를 요청한다.

4. Shopping Mall은 자신의 인증서, 암호화된 컨텐츠, 컨텐츠 전용 S/W를 전송하고 지불요구를 한다. 지불요구는 고객의 공개키를 이용하여 암호화한다.

5. 사용자는 지불요청서를 확인하고 지불 정보를 전송한다. 지불요청서가 올바르지 않으면 거래가 종료된다. 지불정보는 기밀성을 유지하기 위해 Shopping Mall의 공개키를 이용하여 암호화하여 전송하고 무결성, 부인봉쇄 서비스를 제공하기 위해 보내는 정보에 대한 해쉬 값을 사용자의 개인키로 서명하여 전송한

다. 또한, 타임스탬프를 포함하여 재전송 공격으로부터 안전하다.

6. Shopping Mall과 Payment Gateway는 인증서를 서로 교환한다. 또한 Shopping Mall은 고객용 지불 결과의 안전성을 위해서 고객의 인증서도 Payment Gateway에게 전송한다.

7. Shopping Mall은 Payment Gateway에 결재 요청을 한다. 5단계처럼 기밀성, 무결성, 부인봉쇄 서비스를 제공하고 타임스탬프를 포함하여 재전송 공격으로부터 안전하다.

8. Payment Gateway는 Shopping Mall에 결재 결과를 전송한다. 5단계처럼 기밀성, 무결성, 부인봉쇄 서비스를 제공하고 타임스탬프를 포함하여 재전송 공격으로부터 안전하다. 또한 고객용 결재 결과는 고객의 공개키로 암호화함으로써 고객의 결재 정보를 Shopping Mall로부터 보호할 수 있다.

9. Shopping Mall은 Payment Gateway로부터 받은 고객용 결재 정보를 그대로 고객에게 전송한다. 기밀성, 무결성, 부인봉쇄 서비스를 제공하고 재전송 공격을 막기 위해 타임스탬프를 포함한다.

10. Shopping Mall은 DRM Server에 사용자의 인증서를 전송하고 컨텐츠 암호화키 생성정보를 고객에게 전송할 것을 요청한다.

11. DRM Server는 컨텐츠 암호화키 생성정보를 고객의 공개키로 암호화하여 전송한다.

11단계 중 인증서 교환은 처음에 한번만 이루고 지고 다음 접속에는 인증서 교환은 생략된다.

위의 단계가 끝나면 사용자는 컨텐츠 암호화키 생성정보를 복호화한다. 복호화가 되면 컨텐츠 전용 S/W는 컨텐츠 암호화키 생성정보를 이용하여 컨텐츠 암호화키를 생성하고 사용자가 볼 수 없도록 컨텐츠 암호화키를 전용 S/W에 내장시킨다.

## 4. 결론

본 논문은 정보보호 기술을 이용하여 안전한 DRM 메커니즘을 설계하고자 하였다. 제안된 메커니즘은 정보보호 기술을 이용하여 기밀성, 무결성, 인증, 부인봉쇄 서비스를 제공하고 중요한 정보에만 해쉬와 서명을 수행함으로써 불필요한 오버헤드를 갖지 않도록 하였다. 또한 컨텐츠 암호화 키는 사용자가 모르게 하여 컨텐츠를 다른 사용자에게 전송하여도 지불을 하지 않고는 디지털 컨텐츠를 사용할 수 없도록 설계하였다.

## [참고문헌]

[1] 이용호, 황대준, "에이전트 기반의 동적 디지털저작권관리 시스템 설계 및 구현," 한국정보처리학회 논문지, 제8-D권 제 5호, pp.614-622, 2001

[2] 권순홍, 김기영, 신용태, "실시간 멀티미디어 서비스의 DRM적용방법 설계," 한국정보과학회 춘계학술발표대회, 제 29권 1호, pp.481-483, 2002

[3] 장우영, 신용탁, 신동일, 신동규, "DRM시스템에서 Publisher 시스템의 설계," 한국정보과학회 추계학술발표대회, 제 28권 2호, pp.544-546, 2001

[4] W. Diffie and M. Hellman. "New Directions in Cryptography", IEEE Trans. Inform. Th., Vol.22, pp.644-654, 1976.

[5] 이혜란, 박지완 "인증과 무결성을 위한 연성 워터마킹," 한국정보처리학회 춘계학술발표대회, 제 8권 2호, pp.875-878, 2001

[6] 이형우, 김태윤, "디지털 워터마크에 대한 영지식 검증," 한국멀티미디어학회 춘계학술발표대회, 제 5권 1호, pp.877-881, 2001

[7] F.Hartung, F.Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications," IEEE Communications Magazine, VOL.38 NO.11 pp. 0078-0084, 2000

[8] 이덕규, 박희운, 이임영, "Agent 기반 불법 복제 방지 DRM모델," 한국정보과학회 춘계학술발표대회, 제 28권 1호, pp.682-684, 2001

[9] http://www.markany.com/tech02.htm