SDRM: PKI기반의 스테가노그래피를 이용한 Secure DRM 시스템 설계 및 분석

SDRM: The Design and Analysis of Secure DRM Systems Based on PKI using Steganography

도경화(Kyoung-Hwa Do)*, 전문석(Moon-Seog Jun)**

초 록

인터넷의 발전과 더불어 멀티미디어 콘텐츠 제품도 많이 활성화되고 있다. 이는 인터넷을 통하여 배포되는 멀티미디어 콘텐츠가 상업성을 갖게되는 발판이 되었다. 그러나, 이러한 멀티미디어 컨텐츠는 복사가 자유롭기 때문에 워터마킹 기법만 사용하는 경우에는 상업적으로 사용되기에 많은 취약성을 가지고 있다. 따라서 본 논문에서는 공개키기반구조(PKI)를 이용하고 스테가노그래피 기법을 활용하여 멀티미디어 콘텐츠를 보호하기 위한 Secure DRM 시스템을 제안한다. SDRM 시스템은 워터마킹 기술과 스테가노그래피 기술의 특이점을 보강하여 일반적인 DRM 시스템보다 더 강력하다. 따라서, SDRM을 통하여 사용자 인증 뿐만 아니라 멀티미디어 콘텐츠의 불법복제 및 불법도용을 방지할 수 있다.

ABSTRACT

The contents for multimedia are very activated along to revolution of Internet. So this fact allows the contents for multimedia to be commercialized. These contents, however, included much vulnerability that it is difficult to be commercialized because attackers easily reproduce that. Many developers want to use watermarking method as the technique to protect the contents for multimedia, but it is very vulnerable to use only one method. This paper proposes the Secure DRM system which protects the contents for multimedia using Public Key Infrastructure and steganography methods. The SDRM system is more powerful than general DRM systems in that it has the special feature of watermarking and steganography techniques. We can prevent the attackers from reproducing and stealing the contents illegally, and authenticating users through SDRM systems.

키워드 : DRM, 정보은닉, 스테가노그래피, 정보보안, 네트웍보안

DRM, Information Hiding, Steganograppy, Information Security, Network Security

* 숭실대학교 통신연구실

** 숭실대학교 정보과학대학교

1. 서 론

인터넷의 발전으로 멀티미디어 저작에 대한 분야의 발전도 활발해졌다. 이렇게 제작된 멀티미디어 컨텐츠는 인터넷으로 쉽게 배포할 수 있으며, 인터넷을 이용하여 상업적인 목적으로 멀티미디어 컨텐츠를 제공하기도 한다. 그러나 이러한 멀티미디어 컨텐츠는 디지털미디어의 특성상 저작자의 동의 없이 복제가 가능하기 때문에 상업적으로 사용하는데 많은 허점을 가지고 있다. 따라서 이러한 불법 복제와 도용을 방지하기 위하여 DRM(Digital Right Management) 시스템의 개발이 활발히 이루어지고 있다.

멀티미디어 콘텐츠를 보호하기 위한 기술은 크게 사용자 및 저작자의 인증과 멀티미디어 콘텐츠에 대한 보호 등 두 가지로 분류될 수 있다. 사용자 및 저작자의 인증은 사용자에 대한 인증을 통하여 접근을 통제하는 것이고 멀티미디어 콘텐츠에 대한 보호는 콘텐츠 재생과 복제 등에 대한 권한에 따른 콘텐츠의 보호이다.

사용자 및 저작자 인증의 경우, 일반적으로 멀티미디어 콘텐츠를 제공하는 사이트에서 멀티미디어 콘텐츠에 대한 라이선스를 제공하는 경우인데, 이때 콘텐츠를 제공하는 사이트에서 발행하는 라이선스를 사용하는 것 이외에 멀티미디어 콘텐츠의 보호를 위하여 사용자에 대한 인증이 필요하다. 멀티미디어 콘텐츠 보호의 경우, 현재 멀티미디어 콘텐츠의 재생 자체를 보호하기 위하여 대다수 워터마킹 기술을 이용한다. 즉, 멀티미디어 컨텐츠에 저작자나 배포자의 특징을 의미하는 특정 마크를 삽입함으로써 불법 복제나 도용에 대한 보안을 강화하는 것이다. 그러나 기본적인 워터마킹 기술인 멀티미디어 콘텐츠에 저작자나 식별자의 특정 마크를 삽입하는 것은 본 논문 2.2절 워터마킹과 스테가노그래피에서 설명 되었듯이 콘텐츠에 삽입된 워터마크 데이터에 대한 여러 크래킹기술[1]에 의하여 불법 도용이 되는 경우가 많기 때문에, 이에 대한 추가보안이 필요하다.

따라서 본 논문에서는 멀티미디어 콘텐츠를 보호하기 위하여 사용자 및 저작자 인증과 멀티미디어 콘텐츠 보호를 위하여 다음과 같은 SDRM 시스템을 설계하고 분석한다. 멀티미디어 콘텐츠 저작자와 사용자의 보호를 위한 인증의 경우는 인증서 발급이 필요한데 이을 위하여 공개키기반구조(PKI)를 이용한다. 이때 발행된 인증서는 라이선스의 역할을 수행하게 된다. 또한 콘텐츠 보호를 위하여 일반적으로 DRM에서 사용하고 있는 도용방지 추적 알고리즘인 워터마킹 알고리즘에 대한 보안성을 강화하기 위하여 스테가노그래피 알고리즘을 추가하여 복호화키를 전송함으로서 저작권을 보호하는 Secure DRM 시스템을 제안하고 설계한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 통하여 공개키기반구조를 사용한 안전한 키관리 기술과 기존 DRM(Digital Right Managements) 체계 그리고 워터마킹과 스테가노그래피 알고리즘에 대해 알아보고 3장에서는 제안한 Secure DRM 시스템의 구성요소에 대한 고려사항에 대해 설명한다. 4장에서는 스테가노그래피를 이용한 SDRM 시스템를 설계하고 5장에서는 이에 대한 기

본적인 분석을 수행하며 마지막 6장에서 결론을 내린다.

2. 관련 연구

본 논문의 기본구조는 공개키기반구조를 사용하여 멀티미디어 콘텐츠를 사용하는 사용자에 대한 인증을 수행하고 이 인증을 통하여 획득된 인증서 혹은 라이선스를 통하여 과금이나 재생 등을 행하는 DRM 시스템이다. 멀티미디어 콘텐츠를 보호하기 위하여 invisible 워터마킹을 수행하고 이에 보안성을 강화하기 위하여 스테가노그래피 방식을 사용한다.

다시 말해, 본 논문에서 저작권 보호 및 복제 방지를 위하여 워터마킹과 스테가노그래피를 모두 사용하고 있는데 이에 대한 차이점은 사용목적에 따라 다르다고 볼 수 있다[1]. 워터마크는 커버데이터의 저작권, 라이선스, 출판권 등을 특성에 따라 인식할 수 있다. 그러나 스테가노그래피는 삽입된 메시지가 중요성을 갖게 되므로 커버데이터가 주요성이 덜하다는 것이다. 따라서, 본 논문에서는 워터마킹을 수행한 멀티미디어 콘테츠에 스테가노그래피를 수행하여 멀티미디어를 재생시킬 수 있는 중요키를 삽입시켜서 보안성을 강화시킨다.

또한, 현재 공개키기반구조로 사용자를 인증하고 워터마크 기법을 사용하여 만화나 소설등의 콘텐츠를 다운 받을 수 있도록 하는 기술이 연구되고 실제 진행되고 있다. 그러나, 본 논문과 같이 각 항목들이 전부 연동되는 기술은 아직 연구중이다.

2.1 공개키기반구조(PKI)와 DRM(Digital Right Management)

기존에 공개키기반구조는 인증 및 지불과 관련되는 많은 분야에서 응용되고 있다. DRM에서도 공개키 기반구조의 인증서를 사용하여 개인의 인증이나 비밀성을 지킬 수 있도록 하고 있다[2]. 다음에서 기존의 공개키 기반구조와 DRM에 대해 설명한다.

공개키 기반구조는 공개키 암호기술이 안전하게 적용될 수 있는 기반 구조로 키와 인증서를 안전하게 관리해 주는 서비스를 제공한다. 즉 공개키 암호를 기반으로 하고 있는 전자서명 응용계층에서 무결성, 인증, 송수신 부인방지 등의 보안이 효율적이고 안정적으로 제공될 수 있도록 함을 목적으로 한다.

PKI를 구성하는 객체들은 인증기관(CA: Certification Authority), 등록기관(RA: Registration Authority), 디렉토리(Directory), 사용자(User)이며, PKI 시스템의 주요 기능에는 인증서관리, 키관리, 암호화, 전자서명이 있다[3,4].

DRM 서비스의 기본요소는 지불과 콘텐츠 인증을 담당하는 클리어링하우스, 지불시스템, 사용자와 클리어링하우스를 연결시키는 중간업자, 그리고 패키저와 사용자이다[4].

DRM 시스템의 수행 절차를 보면 〈그림 1〉과 같다. 먼저 사용자는 중간업자를 통하여 클리어링하우스에 인증을 요구하고 클리어링하우스는 인증확인에 대한 확인메시지를 보낸다. 중간업자는 패키저를 통하여 사용자에

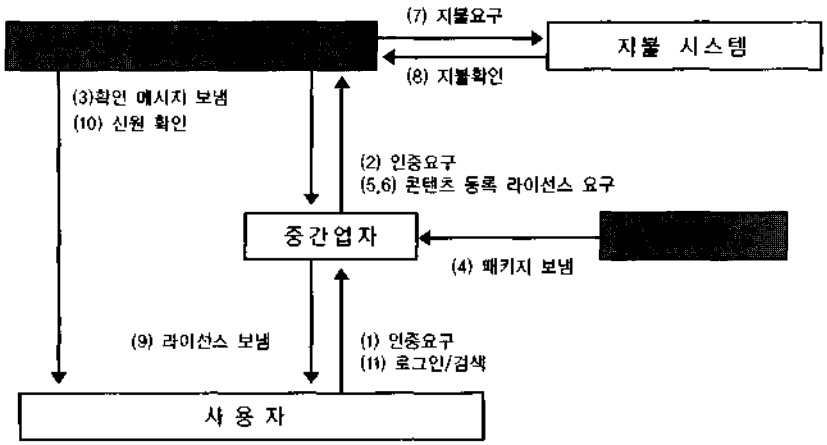
게 패키지를 보내고 사용자는 중간업자를 통하여 콘텐츠를 등록하거나 원하는 콘텐츠를 재생하기 위하여 라이선스를 요구한다. 클리어링하우스는 지불시스템을 통하여 사용자에게 지불을 요구하고 이에 대한 지불내역을 확인한 후 중간업자를 통하여 사용자에게 라이선스를 제공한다. 사용자는 이 라이선스를 통하여 로그인을 하여 원하는 콘텐츠를 검색하고 재생한다.

SDRM 시스템에서 PKI는 콘텐츠에 대한 등록과 사용자에 대한 인증을 인증·지불서버를 통하여 수행하게 된다. 위에 설명된 요소를 본 SDRM 시스템의 요소와 비교하면, 인증기관은 인증·지불서버로 볼 수 있으며 등록기관은 콘텐츠등록·암호화서버로 대체된다〈그림 2〉. 사용자는 SDRM 프로그램을 사용하여 인증서 및 라이선스를 확인하고 멀티미디어 콘텐츠를 재생하게 된다.

2.2 워터마킹(Watermarking)과 스테가노그래피(Steganography)

SDRM 시스템에서 기본적으로 DRM시스템의 형식을 따르고 있으며, 저작권보호와 불법복제에 대한 기본적인 해결방법으로 워터마킹을 이용하고 추가적으로 스테가노그래피를 사용하여 중요키를 전송하는데 사용하여 비도를 높인다. SDRM 시스템은 특징적인 식별자를 워터마킹 알고리즘을 사용하여 멀티미디어 콘텐츠에 삽입하고, 이렇게 삽입된 워터마크는 사용자 인증서를 사용하여 검출하는 방식으로 확인된다. 다음은 워터마킹과 스테가노그래피에 대한 정의와 기존에 워터마킹의 문제점에 대해 알아본다.

워터마킹이란 오디오, 정지영상, 비디오 신호 등의 멀티미디어 데이터에 귀나 눈으로 식별하지 못하도록 데이터의 소유권 정보를 삽입하는 과정으로, 일단 워터마킹된 데이터는 권한이 없는 사용자에게 통계적으로 소유권



〈그림 1〉 DRM 기반 상거래 체계

정보의 검출이 불가능해야 하며, 신호처리 필터링이나 정보압축 동작에 의해 신호가 변형되더라도 소유자에 의해서는 소유권 정보의 검출이 가능해야 한다[6].

그러나, 워터마크는 데이터가 압축되어 손실되거나 위치추적을 통한 추출(워터마크 크래킹: Watermarking Cracking), 워터마크를 디텍터를 통하여 마크의 선명도를 약화시키기(워터마크 세척: Watermarking washing), 잘 알려진 워터마크 위조(Counterfeit marking) 그리고 상업적으로 인정이 되는 사용자가 인증을 한 후 디텍터를 사용하여 복제하는 방식(마크 디텍터 사용: use of mark detector) 등의 공격 기법들에 의해 안전하지 못하다[1]. 따라서 다른 보안요소가 요구된다.

스테가노그래피란 정보은닉[7]의 또 다른 종류로서 통신의 유무를 비밀로 하는 것을 말한다. 다시 말해, 현재 보내고 있는 데이터의 내부에 은닉 데이터를 숨기게 된다. 이때, 암호화와의 차이점은 암호화는 데이터가 암호화되어 있다는 것을 제3자가 알게 되나 스테가노그래피는 암호화된 데이터가 숨겨져 있다는 것을 제3자가 눈치채지 못하는 것을 말한다. 다시말해 은닉데이터 자체가 더욱 중요한 요소가 되는 것이다.

스테가노그래피의 구성요소는 커버 메시지와 삽입 메시지로 구분된다. 커버 메시지는 제3자에게 아무런 의심없이 전달되는 실제적인 의미가 없는 메시지 즉, 삽입 메시지를 숨기고 있는 데이터이다. 삽입 메시지는 두집단간에 비밀스럽게 전달되는 실질적인 메시지이다. 또한 커버 메시지에 삽입 메시지를 숨기는 과정에서 메시지 검출을 제한시키기 위해 키를 설정하는데 이것을 스테고키(Stego Key)라고 한다. 이렇게 커버 메시지와 삽입 메시지가 혼합되어 실질적으로 전달되는 데이터를 스테고데이터(Stego Data)라고 한다. 즉, 스테가노그래피는 암호화된 메시지를 동영상, 이미지, 음악화일 등 다른 데이터 안에 혼합하여 제 3자가 내부에 숨겨진 데이터 자체를 알아차리지 못하도록 숨기고 전달시키는 방법이다[8].

3. SDRM 시스템의 구성요소에 대한 고려사항

SDRM 시스템은 몇 가지 고려사항을 갖는다. 첫째, 멀티미디어 콘텐츠의 접근에 대한 권한이 그 멀티미디어를 저작한 소유자로부터 획득 되어야 한다는 것이다. 이는 멀티미디어 컨텐츠 제공자가 자신이 저작한 디지털 자산을 자신의 소유로 보호하길 원하기 때문이다. 이러한 저작권을 보호하면서 영상과 오디오 같은 멀티미디어 콘텐츠를 사용자들이 사용할 수 있도록 다음과 같은 요소를 고려해야한다.

- 콘텐츠 보호를 위한 공개키기반구조의 고려사항
- 사용추적에 대한 고려사항
- 강력한 콘텐츠 보호를 위한 고려사항

콘텐츠 보호를 위해 공개키기반구조에 적용하기 위하여 디지털 멀티미디어 컨텐츠는 DRM 기술로 암호된 후 사용자단 기기 및 소

프트웨어에서 재생 시 라이선스 클리어링하우스로부터 복호키를 받아 암호화된 디지털 컨테츠를 복호하여 플레이어에게 이를 재생케 한다. 따라서, 암호키와 복호키의 보관 및 관리, 분배 체계가 DRM 시스템 속성상 중요한 역할을 하게되며, 이를 안전하게 그리고 효율적으로 키를 관리해야 한다[2,9].

SDRM 시스템은 위에서 개발한 기술을 통합한 시스템으로 각종 과금 연동 모듈, 인증·지불서버, 콘텐츠제공서버·사이트, 콘텐츠등록·암호화서버, 사용자 인터페이스(SDRM 프로그램) 등의 구축요소로 이루어지며, 약간의 인터페이스 변경으로 상용 사이트에 적용 운용이 가능하다.

사용추적에 대한 고려사항은 웹을 사용하면서 정보의 고리가 저장되는데 주안점을 둘 수 있다. 웹을 사용하여 인터넷거래를 하는 사용자에 대한 정보가 분실 될 수 있다. 이런 문제점은 SSL(Secure Sockets Layer)을 사용하는 CA 서버의 공개키기반구조를 통해 해결될 수 있다. 일단 SSL 기술에 의해 암호화 처리가 된 문서는 정보를 보내는 사람과 정보를 받는 사람 외에는 아무도 해독할 수 없기 때문에 전자문서가 전송되는 도중에 해커가 가로챈다고 해도 정보의 내용을 절대로 알 수 없으며 정보를 암호화, 복호화시 인증서로 설정된 라이선스가 필요하기 때문에 정보유출의 가능성은 그만큼 더 적어지게 된다. 따라서 SSL을 이용한 서버 및 사용자 인증서는 인터넷상의 전자상거래에서 안전하게 이용될 수 있다.

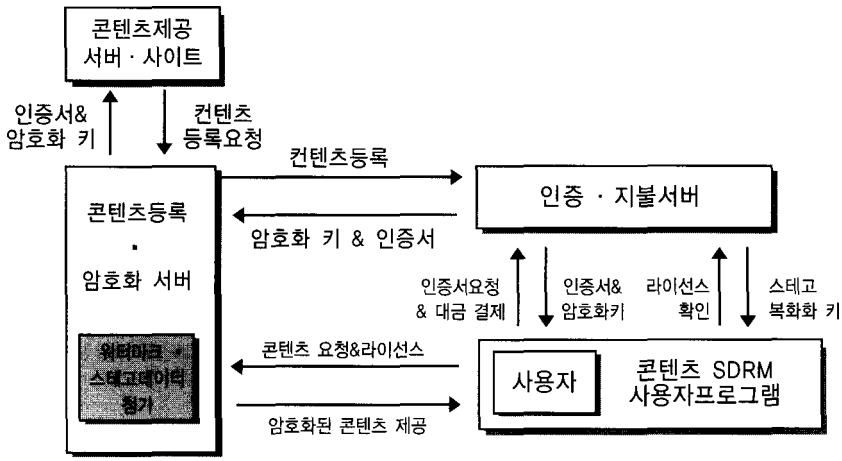
강력한 콘텐츠 보호를 위해서는 워터마킹 기법에 보안 요소를 추가 하여야한다. 워터마킹은 외부로부터의 변형에 강한 인식장치가 기기의 내부나 콘텐츠에 포함되어 있어 복사, 부분복제, 변형등을 할 수 없도록 하는 기술이다. 이는 대부분 콘텐츠의 일부분에 탑재하여 라이센스(인증키)를 통하여 복제방지를 할 수 없도록 한다. 그러나, 이러한 방식도 워터마킹을 공격하는 프로그램에 의해 위험성이 대두되고 있다. SDRM 시스템에서는 워터마킹 기법에 스테가노그래피 기법을 이용하여, 인증서와 라이센스를 통하여 콘텐츠에 공개키나 라이선스 등의 스테고데이터를 삽입함으로서 복제방지에 대한 보호를 한층 강화한다.

4. SDRM 시스템 구조

SDRM 시스템은 콘텐츠 및 사용자 인증을 위하여 공개키 기반구조를 기반으로 있다. 콘텐츠 제공자는 콘텐츠를 제공하기 전에 저작권에 대한 인증을 거치고 콘텐츠제공자의 공개키나 비밀정보를 스테고데이터로 변경하여 콘텐츠에 삽입한다. 이렇게 함으로서 워터마킹의 크랙킹으로부터 야기되는 취약성을 보강할 수 있다.

〈그림 2〉는 시스템 전체 구성도를 나타낸다. 시스템의 구성요소는 콘텐츠제공 서버·사이트, 콘텐츠등록·암호화서버, 인증·지불서버, 콘텐츠 SDRM 사용자프로그램, 그리고 사용자이다.

콘텐츠 제공서버와 사이트는 인증·지불서버에 콘텐츠를 인증받기위하여 콘텐츠등록·암호화서버에 컨텐츠 등록을 요청한다. 그러



〈그림 2〉 SDRM(Secure DRM) 구조

면, 콘텐츠등록 · 암호화서버는 인증 · 지불서버에 콘텐츠를 등록하고, 등록된 해당 콘텐츠에 맞추어 암호화키와 인증서를 부여한다. 이렇게 부여된 암호화키와 인증서는 라이선스화 되어 콘텐츠제공 서버 · 사이트에 저장된다. 이때, 사용자는 미리 콘텐츠등록?암호화 서버에서 받은 콘텐츠 SDRM 사용자 프로그램을 설치하고 인증 · 지불서버에 사용자 인증을 및 해당 콘텐츠 인증서를 요청하고 대금을 결제하면, 인증서와 암호화키를 발급받는다. 그런 후에, 콘텐츠를 요청하면서 라이선스화된 인증서를 콘텐츠등록 · 암호화서버로 보내면, 암호화된 콘텐츠를 제공한다. 이때, 콘텐츠는 워터마킹 뿐만 아니라, 스테고데이터가 삽입되어있기 때문에 콘텐츠 SDRM 사용자 프로그램에 저장된 라이선스를 통하여 재생할 수 있다〈그림 2〉.

4.1 SDRM 시스템의 전체 데이터 흐름도

다음 데이터 흐름도는 사용자가 해당 콘텐츠를 제공받기 위하여 인증 지불서버에 콘텐츠 사용자 인증을 받고 결제를 한후 SDRM 프로그램을 다운받아 인증서와 암호화키로 생성된 라이선스를 통하여 스테가노그래피가 삽입되어 있는 콘텐츠를 복호화하여 재생하는 절차이다〈그림 3〉.

[콘텐츠 등록·인증부]

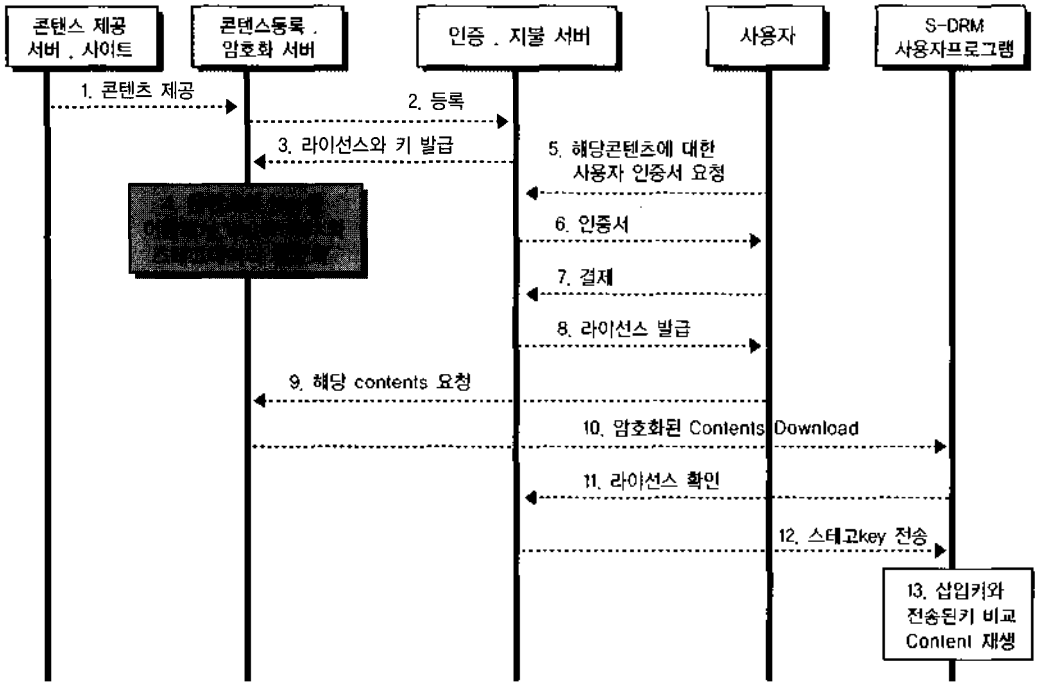
1. 콘텐츠제공 서버·사이트를 통하여 콘텐츠등록·암호화 서버에 콘텐츠 등록 요청
2. 콘텐츠등록·암호화 서버로 등록 요청된 컨텐츠를 인증·지불 서버에 등록요청
3. 인증·지불 서버에서 라이선스와 키 발급
4. 발급받은 라이선스와 발급받은 키를 통하여 워터마크와 스테고데이터를 암호화하여 콘텐츠에 삽입

[사용자 콘텐츠 제공요청 및 인증부]

5. 사용자는 인증·지불서버에 해당 콘텐츠에 대한 사용자 인증서 요청
6. 인증·지불서버는 해당콘텐츠에 대한 사용자 인증서를 사용자에게 제공
7. 사용자는 해당 콘텐츠에 대한 결제 수행
8. 인증·지불서버에서 해당 콘텐츠에 대한 라이선스를 사용자에게 발급

[콘텐츠 복호화 및 재생]

9. 사용자는 콘텐츠등록·암호화 서버에 해당 콘텐츠를 요청
10. SDRM 사용자 프로그램을 통하여 콘텐츠등록·암호화 서버로부터 암호화된 콘텐츠 다운로드
11. SDRM 사용자 프로그램을 통하여 인증·지불 서버를 통하여 발급받은 라이선스 확인
12. 인증·지불 서버는 콘텐츠에 삽입된 스테고데이터를 복호화하기 위한 스테고키를 SDRM 사용자 프로그램에 전송
13. 발급받은 스테고키를 통하여 해당 콘텐츠에 스테고데이터를 복호화하고 복호화된 스테고데이터 내의 삽입데이터인 스테고키와 발급받은 스테고키 비교

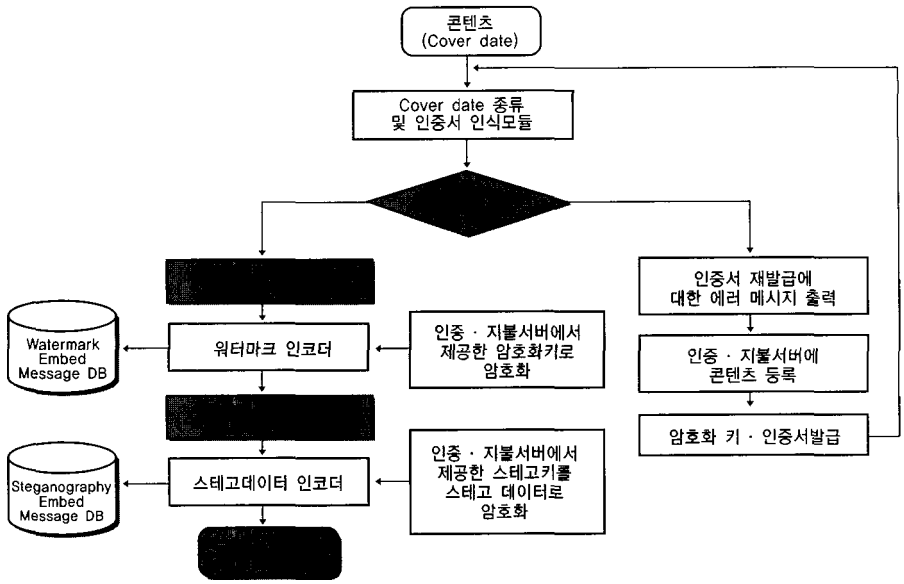


〈그림 3〉 SDRM 데이터 흐름도

4.2 불법복제 및 도용방지를 위한 워터마킹 및 스테고데이터 삽입 모듈 설계

인터넷을 통한 콘텐츠 및 전자문서는 위·변조 및 불법 복제 등의 확인 여부가 불가능하다는 문제가 있다. 따라서, 본 논문에서는 도용방지를 위해 멀티미디어 콘텐츠에 워터마킹 기술을 사용해서 보호하고 스테고그래피 기술을 사용하여 스테고데이터를 스테고키를 사용하여 콘텐츠에 삽입하여 도용방지 및 불법 복제를 강화한다.

본 논문에서 콘텐츠는 워터마킹과 스테가노그래피의 커버데이터이다. 불법 복제 및 도용에 대한 방지를 위하여 콘텐츠등록 암호화 서버에서는 아래 순서도와 같은 방법을 수행한다〈그림 4〉. 입력이 요청된 콘텐츠에 커버데이터(콘텐츠)의 종류와 인증서에 대한 정보를 인식하고 인증서의 기간을 검사한다. 인증서 기간이 허용이 될 경우, 워터마크 삽입모듈을 통하여 워터마크를 삽입한다. 워터마킹 삽입 메시지 데이터베이스를 통하여 입력될 메시지를 선정하고 인증·지불서버에서 제공한 암호화키를 통하여 워터마크를 삽입(인코딩)한다. 보안을 강화하기 위하여 스테고데이터를 삽입한다. 스테가노그래피 삽입 메시지 데이터베이스에서 삽입 메시지를 추출하여 인증·지불서버에서 제공한 스테고키



〈그림 4〉 불법복제 및 불법도용을 위한 워터마킹 및 스테고데이터 삽입 모듈

로 암호화하여 삽입(인코딩)한다.

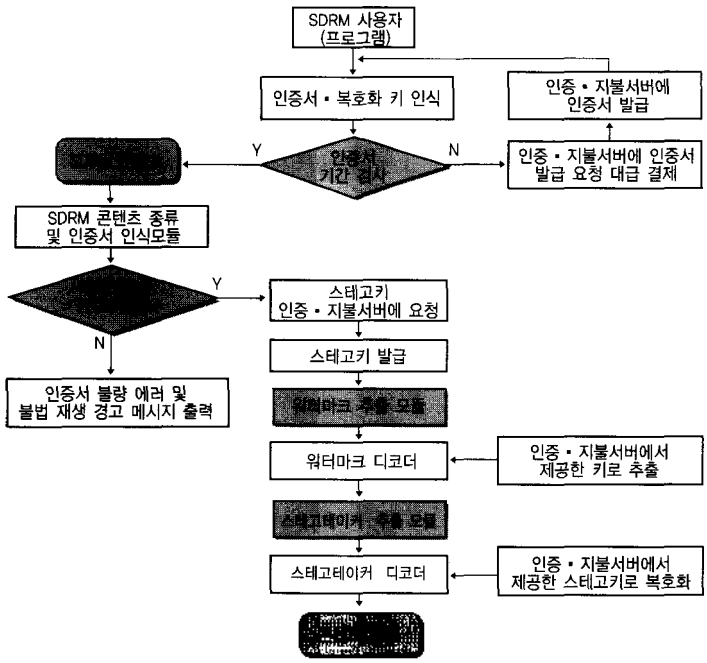
만일, 인증서 기간을 검사하였는데, 인증서 기간이 만료되었거나, 인증서가 인식되지 않을 경우, 인증서 발급에 대한 에러메시지를 출력하고 인증 · 지불서버에 콘텐츠를 등록하고 암호화키와 인증서를 발급받는다.

4.3 불법복제 및 도용방지를 위한 워터마킹 및 스테고데이터 추출 모듈 설계

4.2절에서는 불법복제 및 불법도용을 위한 워터마킹 및 스테고데이터 삽입 모듈을 통하여 SDRM 콘텐츠가 생성되었다. 생성된 SDRM 콘텐츠는 불법복제 및 도용방지를 위하여 사용자 인증을 거친 인증서와 암호화 키를 사용한 워터마킹 및 스테고데이터가 삽입되어 있다.

워터마킹 및 스테고데이터 추출 모듈에서는 SDRM 콘텐츠를 사용자 프로그램을 통하여 인증서를 검사한 후 콘텐츠를 재생한다 〈그림 5〉.

SDRM 사용자 프로그램은 인증 후 사용자 인증서를 발급받는다. 사용자가 재생하고자 하는 SDRM 콘텐츠를 다운로드 받아 SDRM 콘텐츠의 종류와 인증서를 구별한다. 사용자가 미리 인증받은 인증서와 콘텐츠를 다운받을 때 저장되어 있는 인증서를 비교하여 해당 인증서가 맞으면 스테고키를 인증 · 지불서버에 요청하고 발급받는다. 인증 · 지불서버로부터 제공받은 복호화키를 통하여 암호화된 콘텐츠를 복호화하고 워터마크를 비교(검출)한다. 보안을 강화하기 위하여 첨가된 스테고데이터를 검출하기 위하여, 발급받은 스테고



〈그림 5〉 불법복제 및 불법도용을 위한 워터마킹 및 스테고데이터 삽입 모듈

키로 스테고데이터를 추출하여 스테고키나 공개키를 확인한 후 콘텐츠를 재생한다.

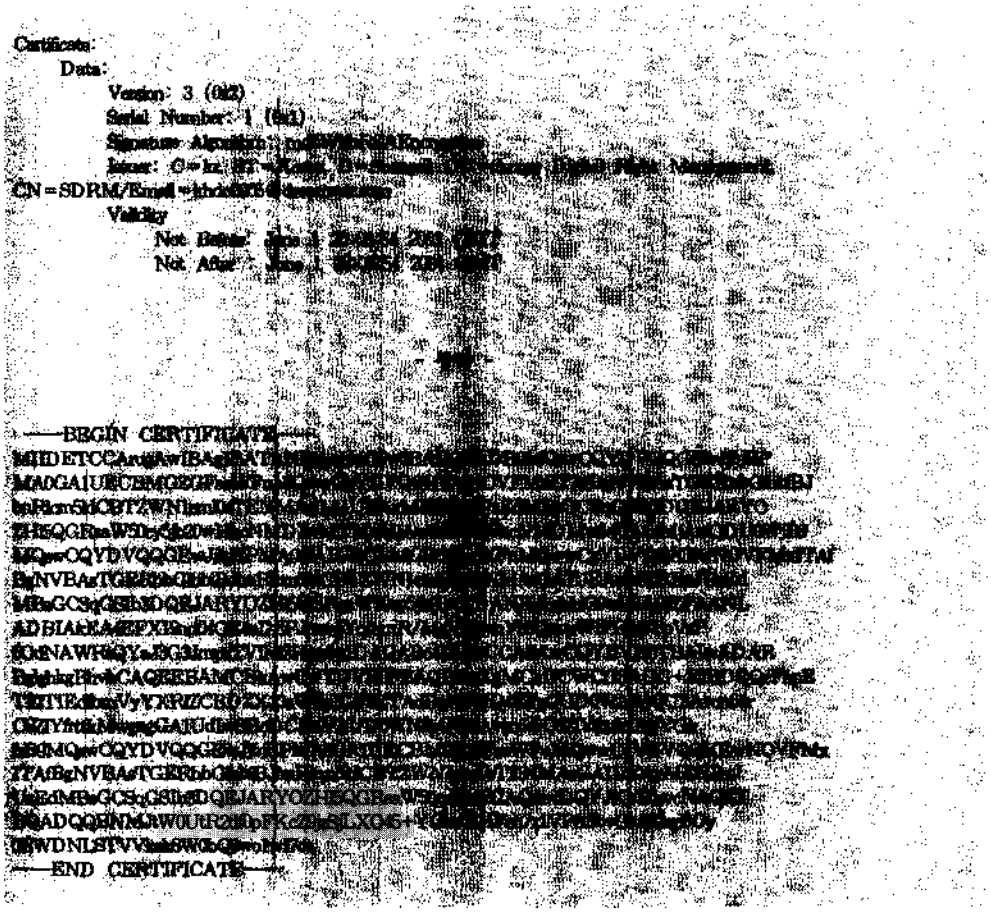
만일, 사용자 인증서와 콘텐츠 인증서가 일치하지 않을 시에는 인증서 불량 에러 메시지나 불법 재생 경고 메시지를 출력한다.

5. SDRM 시스템 분석

본 시스템은 일반 워터마킹 프로그램에 인증서와 스테가노그래피를 붙여서 불법복제 및 불법도용을 방지하는 SDRM 프로그램이다.

〈그림 6〉의 인증서는 리눅스 서버에 SSL을 이용한 인증 시스템을 사용하여 생성된 인증서로서 X.509v3를 표준으로 하고 있다. 따라서, 인증서는 인증서를 발행한 발행처로 OU = Secure Digital Right Management를 사용하였고, 공개키를 생성하는 알고리즘은 RSA, 서명키를 생성하는 알고리즘으로 MD5를 사용하였다. 또한, X.509v6 extension의 내용을 보면, 인증서 타입으로 SSL 서버를 사용한다는 것을 첨가하였고, 인증서는 Digital Signature, Non Repudiation, Key Encipherment에 사용될 것을 첨가하였다. 마지막으로 인증키값이 암호화되어 첨가되어 있다. 이는 라이선스로 사용된다.

생성된 인증서를 SDRM 프로그램에 인식하도록 하였으며, 워터마킹을 수행한 후 스테가노그래피로 공개키를 암호화하여 그 데이터를 삽입하였다. SDRM 프로그램을 통하여 생성된 데이터는 본 인증시스템이 제공하는 인증서를 보유한 사용자만이 SDRM시스템



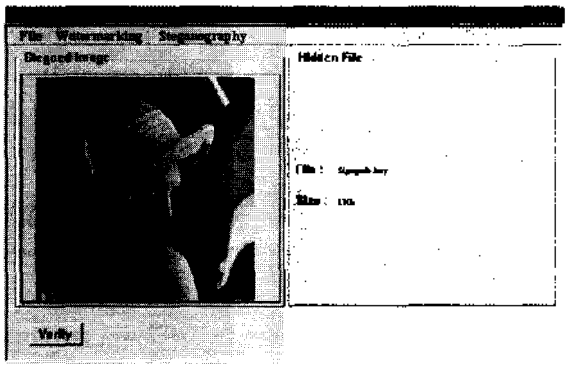
〈그림 6〉 SDRM 사용자를 위한 인증서

에서 제공하는 SDRM 뷰어를 통하여 복호화 되어야만 데이터를 재생할 수 있다.

〈그림 7〉은 자바와 C++로 작성한 SDRM 프로그램을 통하여 워터마킹을 수행한 그림이다. 왼쪽의 Original Image의 그림에 KHDO@SDRM이라는 로고를 워터마킹 기법을 통하여 삽입시켰다. 이때, 원본그림에 로고표시가 나타난다. 그런후에, 스테가노그래피도 같은 방식으로 수행한다. 그러나, 스테가노그래피는 정보은닉 기술이므로 이를 수행했을 경우에는 그림에 아무런 변화가 나타나지 않는다.

〈그림 8〉은 위의 과정을 통하여 SDRM을 사용하여 생성된 데이터를 복호화한 것이다. 이때, 인증서를 받은 사용자는 사용자 인증을 수행한 후에, 패스워드를 입력하고 스테가노 데이터를 확인한 후 데이터를 확인 할 수 있다.

〈그림 7〉 원본 데이터에 워터마크를 수행



〈그림 8〉 SDRM에 의해 스테고 데이터 및 워터마크 데이터 검사

4. 결 론

인터넷의 활성화로 많은 멀티미디어 데이터들이 생성되고 있으나, 이를 불법복제 및 불법 도용하는 일이 늘어나고 있다. 따라서 DRM(Digital Right Management)이라는 저작권 보호 시스템들이 생성되고 있으나 이는 워터마킹이라는 삽입기술을 사용하고 있다. 그러나 기존에 사용하는 워터마킹 기법을 공격하는 기술의 개발로 인하여 안전성이 점점 낮아지고 있다. 따라서 본 시스템에서는 정보은닉 기법인 스테가노그래피 기법를 이용하여 멀티미디어 데이터의 불법 복제 및 불법 도용을 막는 SDRM 시스템을 설계 및 분석하였다.

현재 설계 및 구현된 SDRM 시스템은 인증서와 워터마킹 및 스테고데이터 기법을 이용하고 있다. 그러나 본 SDRM 프로그램을 이용 할때, 이러한 프로그램들을 각각 사용해야 하는 불편함을 가지고 있다. 또한, 동영상

을 제공하지 못하고 있기 때문에 많은 멀티미디어 데이터의 저작권을 보호하기는 힘들다.

따라서 향후 SDRM 시스템에는 4장에서 설계하였듯이, 인증서 설정 자동화와 워터마킹 및 스테고 데이터를 함께 설정하는 방법을 구현 및 분석하고자 한다. 또한, 동영상 등의 멀티미디어의 지원에 대한 부분을 추가하고자 한다. 이는 더욱 비도 높은 멀티미디어 저작권 보호를 수행할 수 있을 것으로 기대된다.

참 고 문 헌

[1] Henri Maitre, "Image Watermarking Why is watermarking a hard problem.", Korea-france Workshop on Multimedia, July6-9 1998.

[2] Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems", Proceedings of the ACM Workshop in Security and Privacy in DRM, 2001.

[3] Carlisle Adams, Steve Lloyd, Understanding Public-Key Infrastructure, Macmillan Technical Publishing, 1999.

[4] Hunt, R., "PKI and digital certification infrastructure", Networks, 2001. Proceedings. ninth IEEE International Conference on, October 10-12, 2001.

[5] W. Ford & M. S.Baum, "Secure Electronic Commerce", Prentice Hall PTR, 1977.

[6] Saraju P. Mohanty, "Digital Watermarking : A Tutorial Review", http://citeseer.nj.nec.com/572262.html , 1999.

[7] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding-A Survey", Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078.

[8] Lisa M. Marvel, "Image Steganography for Hidden Communication", A dissertation, Delaware Univ. 1999.

[9] Ping Wah Wong, "A Public Key Watermark for Image Verification and Authentication", Image Processing, 1998. ICIP98 Proceedings of IEEE, vol.1, 4-7 Oct. 1998.

저 자 소 개

도경화 (E-mail : khdo0905@dreamwiz.com)
1997. 건양대학교 컴퓨터공학과 졸업(학사)
1999. 숭실대학교 컴퓨터학과 졸업(석사)
2002. 숭실대학교 컴퓨터학과 수료(박사)
2001 ~ 2003. 2 숭실대학교 생산기술연구소 연구원
관심 분야 : 정보은닉, DRM, 네트워크보안, 데이터통신,
암호학 InformationHiding, DRM, Network Security,
Data Communication, Cryptography

전문석 (E-mail : mjun@computing.ssu.ac.kr)
1980. 숭실대학교 컴퓨터공학과 졸업(학사)
1986. University of Maryland 전산과 졸업(석사)
1989. University of Maryland 전산과 졸업(박사)
1989. Morgan State University 전산수학과 조교수
1989 ~ 1991. New Mexico State University 부설 Physical Science Lab.
책임연구원
1991 ~ 현재 숭실대학교 정보과학대학 정교수
관심 분야 : 네트워크보안, 컴퓨터알고리즘, 병렬처리, VLSI 설계,
암호학 Network Security, Computer Algorithm, parallel processing,
VLSI design, Cryptography