멀티미디어 콘텐츠 보호를 위한 보완된 프레임워크 설계
Supplemented Framework Design for Multimedia Contents

경태원[a], 이찬우[b], 김상국[c]

[a]경희대학교 산업공학과
[a]경희대학교 컴퓨터공학과
[c] 경희대학교 산업공학과 교수

초록

네트워크 기술의 발달과 컴퓨터 성능의 향상으로 영화, 음악, 게임, 도서 등과 같은 다양한 형태의 디지털 콘텐츠 산업이 발전하였다. 그러나 P2P 기술을 이용한 파일 공유 서비스는 디지털 콘텐츠의 불법적 사용을 부추기고 있다. 이러한 디지털 콘텐츠 불법 복제와 무단 배포는 창작자의 저작권 침해와 유통질서를 혼란에 빠지게 한다. 따라서 디지털 자원에 대한 지적 재산권 보호문제가 새로운 이슈로 떠오르게 되었다. 현재 디지털 콘텐츠에 대한 저작권 보호를 위해 암호화, 워터마킹, 그리고 CPSA(Content Protection System Architecture) 등과 같은 기술들이 개발되고 있다. 즉, 저작권 보호를 위한 기술은 소프트웨어적인 방법과 하드웨어적인 방법으로 양분되어 발전되고 있다. 그러나 이처럼 서로 다른 방식으로 개발된 기술들은 호환성과 상호 연계성 측면에서 문제점을 드러내고 있다. 따라서 본 연구에서는 하드웨어와 소프트웨어 접근 기술들의 특성과 문제점들에 대해 살펴보고 효과적인 멀티미디어 콘텐츠 보호를 위해 이 두 가지 기술을 제시하고자 한다.

1. 서론

수 년 내에 컴퓨터 하드웨어는 4GHz 대의 마이크로프로세서, 4GB 메모리, 수백 GB의 하드디스크 용량 등을 기본 사양이 될 것으로 예상된다. 그리고 네트워크 기술은 더욱 향상되어 수백 MBps의 속도로 데이터를 전송하게 될 것이다. 이처럼 놀라울 정도로 빠르게 발전하고 있는 하드웨어 기술이 우리의 생활에 어떻게 영향을 미칠지는 예측하기 어렵다. 그러나 이러한 하드웨어의 발달을 통해 멀티미디어 콘텐츠 시대가 올 것은 분명한 사실이다. 현재 영화, 음악, 게임, 도서 등과 같은 다양한 형태의 디지털 콘텐츠 산업이 발전하고 있다. 또한 조직의 정보자산, 도서관, 지리정보 등 우리 주변에 존재하는 수 많은 콘텐츠들이 디지털 형태로 서비스되는 이른바 멀티미디어 콘텐츠 시대로 패러다임이 변화하고 있다.

멀티미디어 콘텐츠의 수요 증가와 더불어 요구되는 것은 이러한 콘텐츠들의 보호 방법이다. 복제 기술의 발달로 디지털 콘텐츠는 CD-RW와 같은 컴퓨터 주변 기기만 갖추면 아주 짧은 시간에, 적은 비용으로 간단하게 원본과 동일한 복제품을 만들 수 있으며, 아무리 많은 복사를 하더라도 멀티미디어 콘텐츠의 품질에는 변화가 없다. 그러므로 이러한 P2P 기술을 이용한 파일 공유 서비스는 멀티미디어 콘텐츠의 불법 복제를 부추기고 있다. 이러한 멀티미디어 콘텐츠의 무단 복제와 배포는 디지털 시대의 질서를 어지럽히는 심각한 사회 문제가 되었다. 따라서 건전한 디지털 사회를 구축하기 위해서는 멀티미디어 콘텐츠 보호를 위한 기술 개발이 절실히 필요한 상태이다.

현재 진행중인 멀티미디어 콘텐츠 보호 기술은 크게 소프트웨어적 방법과 하드웨어적 방법으로 나누어져 있다. 소프트웨어 측면의 대표적 콘텐츠 보호 기술에는 암호화(Cryptography), 워터마킹(Watermarking) 그리고 DRM(Digital Rights Management) 이 있다. 그리고 하드웨어 측면의 콘텐츠 보호 기술에는 인증을 통해 DVD 콘텐츠를 보호하는 스크램블 기술, 디지털 장치들간 안전한 콘텐츠 전송을 고려하는 DTCP(Digital Transmission Content Protection) 기술, 그리고 DVI(Digital Visual Interface) 기술 등이 있다. 또한, 최근에는 Intel, International Business Machines Corporation, Matsushita Electronic Industrial Co., Ltd, Toshiba Corporation의 4개 회사가 연합하여 CPSA(Content Protection System Architecture)라는 기술을 새롭게 제시하였다.

현재 멀티미디어 콘텐츠 보호를 위해 소프트웨어와 하드웨어 기술을 이용한 연구들이 활발히 이루어지고 있지만, 기존 기술을 이용한 멀티미디어 콘텐츠 보호에는 몇 가지 문제점들이 지적되고 있다. 첫째, 다양한 인증 기술 및 복사 방지 기술의 난립이다. 즉, 현재 콘텐츠에 대한 인증 과정이 구현된 시스템마다 모두 다르기 때문에 이와 같이 서로 다른 방식과 체계가 적용된 시스템은 멀티미디어 콘텐츠 보호에 대한 효율을 떨어트리고 있다. 둘째, 표준화의 문제이다. 소프트웨어를 이용한 대표적 보호 기술인 DRM의 경우, 모델 구조에 대한 비표준화가 문제되고 있다. 현재 연구, 발표된 시스템들은 각기 서로 다른 방식과 소프트웨어를 사용자에게 제공하고 있다. 따라서 호환성 측면과 상호 연계측면에서 많은 문제점을 보이고 있다. 셋째, 비용과 사용상의 불편함 문제이다. 하드웨어적인 보호 기술은 소프트웨어적인 방법 보다 안정적이긴 하지만, 개발 비용이 상대적으로 높아 고가의 소프트웨어 제품에만 주로 사용된다. 또한, 모든 소프트웨어마다 새로운 하드웨어 락을 PC에 설치해야 한다는 것 자체가 비합리적인 부분으로 지적된다. 따라서 본 연구에서는 이러한 문제점들을 인식하고 하드웨어적 방법과 소프트웨어적 방법을 함께 고려하여 멀티미디어 콘테츠를 보호를 위한 보다 안전한 프레임워크를 설계하고자 하였다.

2. 기존 멀티미디어 콘텐츠 보호 기법

2.1 암호화(Cryptography)

암호화(Cryptography)는 전자서명 및 정보보호를 위한 기본적인 기술로써 어떤 자료나 정보에 대하여 타인이 식별할 수 없도록 기술적 조치를 취하여 암호문으로 바꾼 것이다. 데이터를 암호화하는 방식은 크게 대칭 암호화 방식과 비대칭 암호화 방식으로 나눌 수 있다.
일반 암호화 방식의 경우 일단 암호화된 데이터 평문을 받은 이용자는 원래의 소유권자와 동일한 능력을 갖게 되어 이를 무단으로 복사하여 배포하는 것을 막을 수가 없다. 따라서 암호화를 이용한 방법은 정보보호를 위한 주요 수단이기는 하나, 디지털 콘텐츠에 대한 저작권 침해 방지를 위한 감시 및 추적 기능 제공 등에는 한계가 있다.

2.2 워터마킹(Watermarking)

디지털 워터마크는 디지털 정보나 기존의 아날로그 형태의 정보를 디지털화할 때, 첨가시키는 일종의 저작권 관리 정보로서 개인의 식별 기호나 부호라고 정의할 수 있다. 즉, 워터마크는 디지털 콘텐츠, 콘텐츠 저작자 및 콘텐츠 권리자를 식별하는 정보 또는 콘텐츠 이용 조건에 관한 정보 및 그러한 정보를 나타내는 숫자나 부호로서, 콘텐츠가 불법 복사될 때 이들 정보의 어느 항목이 콘텐츠의 복제물에 부착되어 나타나도록 되어 있다. 워터마크 기술은 불법 복제에 대해서는 매우 소극적 방어 수단이지만 다른 저작권 보호 수단이 모두 제거된 후에도 저작권자가 소유권을 주장할 수 있는 마지막 보루로서의 근거를 남긴다는 측면에서 중요성이 높아지고 있다.
디지털 워터마킹 기술은 1990년대에 중점적으로 연구되기 시작하였다. 그러나 그 가치가 제대로 인정되기 시작한 것은 멀티미디어 콘텐츠에 대한 저작권 보호를 위한 모임인 SDMI가 출범하면서부터라고 볼 수 있다. SDMI는 1999년 7월 저작권 보호를 위한 기술 기준안인 PDWG 규격 1.0을 발표했고, 그 해 9월에 이에 대한 수정안에 합의하였다. 이 규격에 다양한 개념과 기술들이 도입되었지만 대부분이 선언적 수준에 머무르고 있다. 디지털 워터마크에 대해서도 ARIS의 기술을 채택한다는 정도로 서술하고 있으며 아직 워터마크 기술에 대한 세계 표준화는 이루어지지 않고 있다.

2.3 CPSA(Content Protection System Architecture)

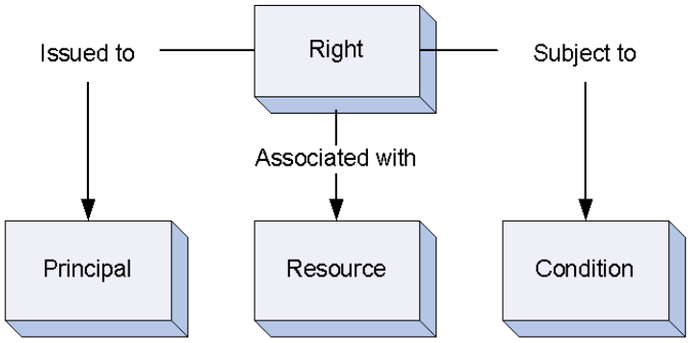
CPSA(Content Protection System Architecture)는 Intel, International Business Machines Corporation, Matsushita Electronic Industrial Co., Ltd, 그리고 Toshiba Corporation의 4개 회사가 연합하여 멀티미디어 콘텐츠 보호를 위한 프레임워크로 제시되었으며, 하드웨어적 콘텐츠 보호 기술이다. CPSA의 출현 배경을 살펴보면, 디지털 시대로 접어들면서 일반 정보 디바이스(PC, DVD-Player and Recorder, Set-top box, Digital TV)들 간 정보 이동이 활발해짐과 더불어 콘텐츠를 보호를 위한 노력이 증가하게 되었다. 암호화와 워터마킹 기술을 이용한 CPSA는 오디오와 비디오 형식의 아날로그 및 디지털 콘텐츠 보호를 위한 프레임워크를 제시하였다. 그러나 CPSA 기술은 개별 장치들에 적용되는 것으로서 콘텐츠 보호를 위한 전체 프레임을 형성할 수가 없었다. 또한 다양한 형태의 멀티미디어 콘텐츠를 전송하기 위해 사용된 장치들간에 호환성이 부족하게 되었다. 따라서 콘텐츠 보호를 위해서는 서비스되는 제품마다 모두 별도의 보안 기술을 적용시켜야 한다는 번거로움이 발생하였다.

3. 멀티미디어 콘텐츠 보호를 위한 프레임워크 설계

프레임워크는 크게 두 부분으로 나눌 수 있다. 첫째, 멀티미디어 콘테츠 저작권 보호를 위해 XrML을 이용한 DRM기술 적용 부분, 둘째 소프트웨어와 하드웨어 기술을 적용한 불법 복제 방지 부분이다.

3.1. XrML을 이용한 DRM 모델

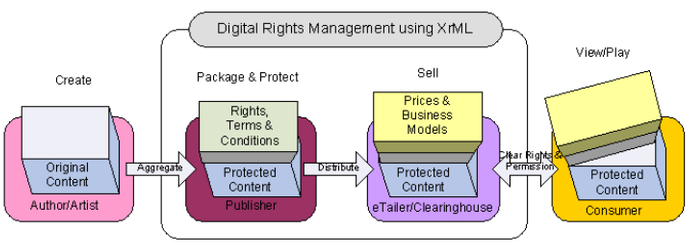
DRM(Digital Rights Management)이란 콘텐츠 제작단계의 암호화(Encryption) 및 콘텐츠 사용단계의 사용 인증 지원, 사용 범위 관리, 유료 사용을 위한 과금 관리 지원 등을 포함하는 일련의 시스템을 의미한다. 이러한 DRM 시스템을 이용하면 디지털 음악, 영화, 교육, 게임 기타 여러 목적으로 제작된 디지털 콘텐츠의 불법적인 유통을 방지할 수 있다. 즉, 복제 방지, 사용 횟수 제한, 재생 장치 제한 등을 통해 정상적 절차를 통해 구입한 사용자만이 콘텐츠를 재생, 이용할 수 있다. 일반적으로 DRM은 디지털 콘텐츠를 암호화하여 인증된 사용자만이 파일에 접근할 수 있는 복호화 키를 갖도록 하는 기술이다. 그러나 이것만 가지고는 DRM이 기존 PKI 시스템과 별반 차이가 없을 것이다. 두 기술의 본질적 차이는 궁극적으로 허가된 사용자의 『공격을 방지』(Tamper Proofing, Tamper Resistance)할 수 있는 가의 여부에 있다. 즉, 콘텐츠를 복호화 할 수 있는 인증된 사용자가 그것을 재배포하는 경우 PKI 기술로는 추적/제어 할 수 있는 방법이 부족하지만, DRM은 허가된 사용자의 공격(재배포)을 막고, 배포시킨 사용자를 추적할 수 있는 기능을 지니고 있다는 점에서 가장 큰 차이가 있다.
DRM은 저작권 패키지 기술, 메타정보 관리 기술, 저작권 정보 관리 기술, 그리고 디지털 콘텐츠 인증 기술로 나눌 수 있다. 그 중에서 디지털 콘테츠에 대한 식별 정보, 내용 정보, 특성 정보, 저작권 정보 등의 요소를 정의하고 기술하기 위해 XrML을 사용하였다.
XrML(eXtensible rights Markup Language)은 디지털 콘텐츠 및 웹 서비스와 관련된 권리와 조건들을 표현하고, 저작권자, 콘텐츠 제공자, 사용자간에 권리항목들의 표준을 제정하기 위한 목적에서 시작되었다. 즉, XrML은 멀티미디어 콘텐츠에 대한 저작권 및 소유권 정보 등을 포괄적으로 정의할 수 있는 확장된 저작권 표시 언어라고 정의할 수 있다.
콘텐츠 제공자는 XrML을 이용하여 사용자에게 특정 권한을 부여할 수 있으며, 이러한 모든 권한에 대해서 사용기간과 조건을 명시할 수 있다. 또한 사용기간과 사용 권한에 따른 과금 부과가 가능하다.



[그림 1] XrML 데이터 모델

그림 1은 XrML의 네 가지 요소를 보여주고 있다.
예를 들어, 일반 사용자가 어떤 콘텐츠를 사용하기를 원한다 하자. 만약 그 콘텐츠가 저장된 사이트가 사용자가 회원으로 가입된 사이트라면 사용자는 웹 인증을 통해 로그인할 것이다. 이것이 사용자 확인(Principal)이고 로그인이 되었다는 것은 권리(Right)를 얻었다는 것이다. 사용자는 자기가 원하는 콘텐츠를 찾고 다운로드 메뉴를 누른다. 다운로드를 누르면 조건(Condition)을 체크해서 그것을 다운로드 할 수 있는 회원인지 묻는다. 인증과정을 마치면 사용자의 PC에 다운로드 된다. 이때 사용자가 다운로드 한 것이 자원(Resource)이다.

- 사용자 확인(Principal) : 누가 권한을 부여 받았는지 여부에 관한 정보를 포함하고 있다. 각 주체들은 유일한 정보(Primary Key)를 갖고 있다. 이 정보의 확인을 통해 그 주체가 누구인지를 알 수 있다.
- 권리(Right) : 주체가 어떤 리소스를 특정 조건 하에서 실행할 수 있도록 권한을 부여 받는 것이다. 전형적으로 권리는 동작 또는 동작의 종류를 주체가 연결된 디지털 리소스에 실행 가능하도록 하는 것이다.
- 자원(Resource) : 콘텐츠를 말한다. 자원은 디지털 파일들(전자책, 오디오, 비디오, 파일 또는 이미지)과 서비스(e-mail 서비스, B2B 트랜잭션 서비스) 또는 주체에 의해 소유된 정보를 말한다.
- 조건(Condition) : 실행할 수 있는 권리에 대한 제약으로서 사용 기간, 사용 조건, 그리고 그 밖의 다양한 요구사항들이다. 간단한 조건의 예로는 자원을 실행할 수 있는 기간 제한, 횟수 제한 등이 있다.



[그림 2] DRM using XrML

그림 2는 멀티미디어 콘텐츠가 콘텐츠 생성자로부터 최종 사용자에게 제공되는 과정을 보여주고 있다. 서비스 과정 중, 콘텐츠의 사용권, 소유권, 지불 조건 등을 XrML을 이용하여 DRM 시스템을 구축하게 된다.
사용 예제를 소개하면 다음과 같다.

[리스트 1] XrML 2.0 기반의 라이센스 사용 예제

```
<license>
    <grant>
        <keyHolder>     // principal
            <info>
                <dsig:keyValue>
                    <dsig:RSAKeyValue>

<dsig:Modulus>Fa7wo6NYfmvGqy4ACSWcNmuQfbejSZx7aCibIg

kYswUeTCrmS0h27GJrA15SS7TYZzSfaS0xR9lZdUEF0ThO4w==
                    </dsig:Modus>
                    <dsig:Exponent>AQABAA==</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>
        </info>
    </keyHolder>
    <cx:print/>             // right
    <cx:digitalWork>        // resource
        <cx:locator>
            <nonSecureIndirect
URL="http://www.contentguard.com/sampleBook.spd"/>
        </cx:locator>
    </cx:digitalWork>
    <validityInterval>      // condition
        <nonAfter>2004-12-24T23:59:59</notAfter>
    </validityInterval>
    </grant>
</license>
```

[리스트 1]은 XrML의 예제 코드이다. 권리(License)는 앞서 설명한 대로 권한부여(Grant)를 포함하고 있다. keyHolder는 사용자 확인(Principal)으로 공개키 알고리즘의 하나인 RSA를 사용하며, 모듈러스 값과 익스포넨셜 값으로 전기한 값을 사용한다. Print는 right로 이것이 정하고 있는 디지털 리소스는 프린트 가능이라는 정보를 나타내며, dititalWork는 자원(Resource)로 위의 URL에 있는 디지털 자원을 사용하라는 것이다. validityInterval은 조건(Condition)으로서 사용 기간을 나타내고 있다. '2004-12-24일 23시 59분 59초'까지 사용 가능하다는 것을 나타낸다. 이런 형태로 XrML은 구성되어 있다.

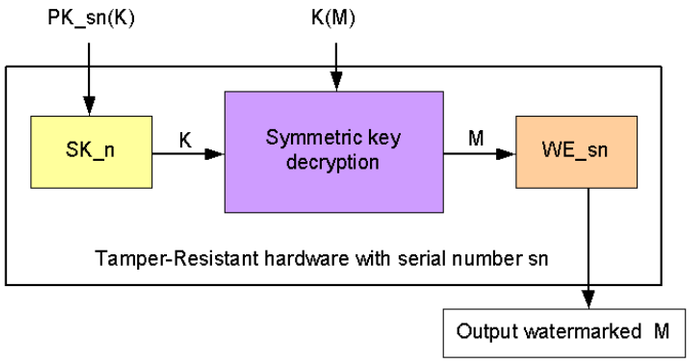
3.2 Tamper-Resistant H/W를 이용한 콘텐츠 암호화

소프트웨어적 보안 기술은 사용자에게 편리성을 제공해 주지만, 오브젝트 코드를 소스 코드로 변화하여 프로그램의 기능과 해법을 추출하는 리버스 엔지니어링(Reverse Engineering) 공격에 약하다는 결점이 있다. 따라서 이러한 약점을 보완하기 위한 하드웨어적 기술이 필요하게 되었다.

소프트웨어적으로 워터마크를 삽입하는 기존의 방법을 하드웨어에서 실행하게 하고 그 하드웨어에서만 가질 수 있는 정보를 워터마크로 삽입하게 하는 방법이다. 기존의 방법에서는 워터마크를 콘텐츠의 소유자가 소프트웨어적 방법으로 삽입하였다. 그러나 제안하는 방법에서는 Tamper-Resistant H/W가 이 일을 대신 하도록 하는 것이다. 여기서 Tamper-Resistant H/W는 워터마크를 삽입하고 복호화 할 수 있는 디바이스를 말한다. 그리고 하드웨어 디바이스에 의해 삽입된 워터마크는 하드웨어의 유일한 공개키(Public Key)와 개인키(Private Key)에 관계되는 암호를 나타낸다.

초기 Tamper-Resistant 기술은 소프트웨어의 변조 및 관찰을 막기 위하여 연구되었다. 본 연구에서는 tamper-resistant를 콘텐츠 보호를 위한 도구로 사용하였다. 특히, 공개키 암호체계 중에서 개인키는 암호문을

해독하는데 적용하였다.



[그림 3] Tamper-Resistant Hardware Function

Tamper-Resistant는 시리얼 번호 sn과 개인키 SK_sn, 그리고 디지털 콘텐츠에 시리얼 번호 sn을 삽입하기 위한 워터마킹 프로세스 WE_sn으로 구성된다. WE_sn은 디지털 콘텐츠에 워터마킹을 삽입하는 것뿐만 아니라, 워터마크된 콘텐츠에 삽입된 시리얼 번호 sn을 검색하기도 한다. M은 디지털 콘텐츠를 의미하고, K는 디지털 콘텐츠 M을 암호화하기 위한 대칭키 이다. K(M)은 비밀키 K를 가지고 있는 M의 암호이다. PK_sn(K)는 공개키 PK_sn을 가지고 있는 K의 암호문을 의미한다.
예를 들어, 사용자는 멀티미디어 콘텐츠(M)를 사용하기 위해 콘텐츠 제공자에게 사용자의 공개키(PK_sn)과 시리얼 번호(sn), 그리고 인증서(ID)를 전송해야 한다. PK_sn이 정당하게 취득되었을 경우, 콘텐츠 제공자는 사용자에게 PK_sn에 의해 암호화된 K와 암호문을 전송하게 된다.
암호화 기술 측면에서 볼 때 멀티미디어 콘텐츠를 배포하기 전에 파일이 암호화되어 있고 키가 공개키로 암호화되는 것은 동일하다. 그러나 Tamper-Resistant H/W에 그 공개키에 대응되는 개인키를 유지시키는 것이 다르다. 따라서 멀티미디어 콘텐츠를 사용하려는 사람은 암호화된 파일과 키를 Tamper-Resistant H/W에 입력하는 것이 필요하다. 그리고 하드웨어로부터 출력을 내 보내기 전에 그 파일은 Tamper-Resistant H/W에 의해 워터마크가 삽입된다.

4. 결론

컴퓨터의 소형화, 고성능화, 그리고 네트워크 기술의 고속화는 IT 분야의 새로운 혁신을 초래하고 있다. 이러한 기술의 지속적 발달은 영화, 음악, 도서 등과 같은 콘텐츠를 디지털화시켜 제공할 수 있게 하였고, 더 나아가 지도나 도서관 까지도 디지털화된 제품으로써 사용자에게 서비스되고 있다. 하지만 컴퓨터 기술의 발달로 멀티미디어 콘테츠는 불법 복제나 무단 배포의 위험에 노출 되었고, 이로 인한 저작권 침해문제가 심각한 사회문제로 대두 되었다.
멀티미디어 콘테츠 보호를 위해 콘텐츠 공급자 별로 다양한 보안기술이 적용되었다. 그러나 이러한 다양한 기술의 적용은 사용자에게 혼란을 가중시켰고, 동일한 데이터 일지라도 서비스되는 방식과 보호기술의 차이로 인해 호환 되지 않는 문제점이 발생하게 되었다. 이처럼 법률적 제도나 기술적 표준화 없이 개발된 기술이나 제품들은 멀티미디어 콘테츠 활성화에 커다란 걸림돌이 되고 있다.
본 연구에서는 멀티미디어 콘테츠 보호를 위해 개발된 기존 방법들의 문제점들을 살펴 보고, 소프트웨어적인 방법과 하드웨어적인 방법을 결합시킴으로써 새롭게 보완된 프레임워크를 제시하고자 하였다.
XrML을 이용하여 설계된 DRM 시스템은 콘텐츠 저작권, 소유권, 사용자 권한, 그리고 사용조건 등을 기술함으로써 멀티미디어 콘텐츠의 사용 권리(Usage Rights) 및 확인을 통한 상호 운용성을 강화시켰다. 또한 멀티미디어 콘텐츠와 권리(Right), 조건(Condition), 그리고 요금(Fee) 부분에서 사용자와 콘텐츠 소유자 모두에게 신뢰를 제공하고 있다.
Tamper-resistant H/W는 멀티미디어 콘텐츠의 불법 복제나 무단 배포로 인해 발생되는 피해를 감소시킬 수 있게 되었다.
향후 디지털 방송 콘텐츠나 모바일 콘텐츠와 같이 멀티미디어 콘텐츠의 종류가 다양해지고 복잡해짐에 따라 콘텐츠 보호 기술 또한 정교해지고, 표준화를 통해 콘텐츠간 호환성을 높여야 할 것이다. 또한 멀티미디어 콘텐츠 유통 과정에서 공급자와 사용자간의 신뢰 구축을 위해 인증 기술의 보안이 지속적으로 이루어져야 할 것이며, 사용자의 정보 보호를 위한 체계적인 법적, 제도적 노력이 강화되어야 할 것이다.

참고문헌

[1] http://www.wipro.com/dwlphp/Download.php3 "Digital Transmission Content Protection"
[2] http://www.ddwg.org/if/data/0830991.pdf, “DDWG members meeting, Palm Spring CA” 1999. 8. 30.
[3] http://data.dt.co.kr/special_report/board.asp, “공개키 암호화 기술”
[4] 강호갑, “DRM vs. Watermarking”, 2002, Fasoo.com R&D Center.
[5] http://www.4centity.com/tech/index.html#CPSA, "Content Protection System Architecture: A Comprehensive Framework for Content Protection".
[6] Feng Bao, Kent Ridge Ditial Labs, Singapore, "Multimedia Content Protection Cryptography and Watermarking in Tamper-resistant Hardware".
[7]www.fcc.gov/oet/tac/april26-02-docs/Digital-Content-Protection3.ppt, "Digital Content Protection Overview". April 26, 2002.
[8] Qiong Liu, “Digital Rights Management for Content Distribution”, Australasian Information Security Workshop 2003.
[9] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard “Digital Rights Management for Content Distribution”, Australasian Information Security Workshop 2003