

디지털 콘텐츠 저작권 보호기술

박 남 제*, 송 유 진**

요 약

인터넷의 발전과 대량의 디지털 정보를 활용할 수 있는 기반이 성숙됨에 따라 디지털 정보가 인터넷 환경에서 이용 가능한 디지털 형태로 제작되어 활발하게 유통되고 있다. 향후 디지털 콘텐츠의 유통 및 사용이 일반화 될 것이며, 콘텐츠 유통시스템 구축이 매우 중요하게 될 것이다. 그러나 현재의 디지털 콘텐츠 유통 체계는 저작권 및 콘텐츠 사용권, 불법재생 및 복제에 대해 무방비 상태에 있다고 해도 과언이 아니다. 디지털 콘텐츠 유통에 있어서, 개별적인 콘텐츠를 보호할 수 있는 기술이 필수적으로 요구되고, 디지털 콘텐츠 저작권 보호기술의 개발을 위하여 국내외 여러 단체들이 활발히 활동중이다.

본 논문에서는 이러한 배경으로부터 디지털 콘텐츠의 개념, 저작권 보호기술의 목적 및 분류체계에 대하여 검토하고, 콘텐츠 보호기술 및 표준화 동향을 살펴본다. 또한 저작권 보호서비스 사례를 분석함으로써 저작권 보호기술의 응용 분야와 향후 전망에 대해 논한다.

1. 서 론

최근 정보통신 기술 환경이 급속도로 변화를 겪으며, 지식과 정보가 궁극적인 경쟁력의 유일한 원천이 되고 있고, 기업의 성공과 실패를 가름하는 중심적인 역할을 하게 되었다.

컴퓨터 등의 정보기술 발달로 다양한 지식과 정보들이 디지털화되고 있고, WWW(World Wide Web)의 등장으로 인터넷은 대중에게 보다 친숙한 환경을 제공함으로써, 인터넷을 통한 정보의 유통을 활성화시키는 계기가 되었다. 이 모든 것들은 처음에는 광고를 위해서 정보를 무료로 발신하는 형식에서 광고료 형태로 수입을 얻는 정보 제공 비즈니스나 정보 그 자체를 유료로 판매하는 정보 판매 비즈니스로 발전하고 있다. 전자상거래가 인터넷 비즈니스로서 주목받고 있고 인터넷상에서 거래되는 주요 디지털 콘텐츠는 SW, 서적, 비디오, 음악, 전자출판 등 정보를 상품으로 하는 것이 많다. 이와 같이 컴퓨터 네트워크와 멀티미디어 기술이 급격하게 발전함에 따라, 인터넷에서 거래 및 유통되는 자료가 점차 음악, 사진, 동영상 같이 멀티미디어화 되어가고 있는

것이다.

전자상거래 분야에 있어서 기존에는 물리적인 형태를 지니는 상품들에 대한 상거래가 주를 이루어 왔지만, 최근 들어 컴퓨터 및 인터넷 관련 기술의 급속한 발전으로 멀티미디어 자료(동영상, 정지영상, MP3 음악 등)들의 유통(콘텐츠 제공자에서 개인으로, 개인들 간으로)에 대한 요구가 급속히 증가하고 있다. 디지털 콘텐츠는 처리 과정의 단순함과 사용의 편리함 그리고 디지털 통신을 통한 대량 배포의 용이함 등의 장점이 있는 반면 데이터가 갖고 있는 내용의 무결성을 보장하기가 어렵다는 단점이 있다. 디지털 데이터 형식이 다양한 매체에 널리 적용됨에 따라, 허가받지 않은 접근에 의한 대량 복제나 저작권자와 상관없는 무단 변형 등으로 콘텐츠 소유자들의 저작권을 보장하지 못하고 있는 상황이다. 따라서 디지털 콘텐츠 제공자는 자신의 노력에 대한 정당한 대가를 받을 수 있으면서 허가되지 않은 사용, 저작권 침해를 방지할 수 있는 기술적, 제도적 환경을 요구하고 있으며, 이러한 환경의 조성은 고급 콘텐츠 생산을 유도하기 위해 필수적이다.

현재 투명한 유통 환경을 확립하고, 저작권과 관

* 성균관대학교 정보통신대학원 정보보호학과 (njpark@mail.skku.ac.kr)

** 동국대학교 정보산업학과 (song@mail.dongguk.ac.kr)

련하여 정당한 분배가 이루어 질 수 있는 멀티미디어 프레임워크를 구성하려는 노력들이 이루어지고 있으나, 그 활동들은 요소 분야들에 대한 산발적인 활동만이 존재할 뿐, 디지털 콘텐츠의 제작에서부터 소비에 이르기까지의 전체 프레임워크에 대한 통합 작업이 이루어지지 못한 상황이다

이에, 본 논문에서는 2장에서 디지털 콘텐츠 유통 형태를 살펴본 다음 저작권 보호기술의 분류체계를 점검하고, 3장에서 분류체계에 근거한 디지털 콘텐츠 저작권 보호기술의 종류 및 내용을 분석하며, 4장에서 저작권 보호기술의 현황 및 표준화 동향을 기술한다. 5장에서 국내외 저작권 보호제품 및 서비스를 살펴본 다음, 저작권 보호기술 적용시 고려사항들을 분석해 본다. 마지막으로 6장에서는 본 연구에 대한 결론을 내리고, 현재의 문제점을 진단함과 동시에 앞으로 개선되어야 할 연구방향을 기술한다.

II. 디지털 콘텐츠 보호기술 개요

디지털 콘텐츠란 의미적으로 분석하면, 멀티미디어로 구성된 정보내용이라고 볼 수 있다. 즉, 다양한 매체형태로 구성되고, 또한 일체화된 정보형태라고 할 수 있을 것이다. 이 때문에 디지털 콘텐츠에 대한 정의 개념은 명확하게 확립되어 있지 않고, 또한 멀티미디어를 논하는 사람의 목적에 따라 달리 해석되어지는 경우도 많다. 이미 정보에 대한 정의는 실제 현상으로서 여러 가지 변화를 통하여 이루어지는 법적 성질 또는 경제성을 지닌 개념으로 규정하였다. 그리고 이러한 정보가 바로 디지털화되고 다양한 매체의 집합 내지 일체화된 형태로서 디지털 콘텐츠를 구성하게 되는 것이다.

디지털 콘텐츠에 대하여 IMO(Information Market Observatory)^[5]에서는 "정보 콘텐츠 또는 비디오, 음악 등을 막론하고, 멀티미디어 상품이나 서비스를 형성하는 지적재산권을 지칭한다"고 정의하고 있으며, 소프트웨어 종합육성계획의 '98년 자료^[2]에서는 디지털 콘텐츠를 "문자·음성·영상 등의 다양한 정보형태가 통합되어 생성·전달·처리되도록 하는 시스템 및 서비스에서 활용되어지는 정보서비스 내용물"로 규정하고 있다. 그리고, 정보통신부의 『정보화 백서』^[6]에서 디지털 콘텐츠에 대한 정의를 "정보 콘텐츠를 디지털화하여 정보기기에 의해 생산, 유통, 소비되는 정보콘텐츠와 쌍방향성이 추가되어 광대역 정보통신망 또는 방송망을 통해 송수신되는 정보컨

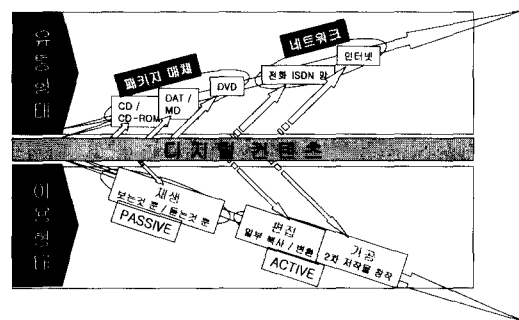
텐츠"로 정의하고 있다.

본 논문에서 디지털 정보라 함은 정보자체가 디지털 형태로 구성되거나 저장된 상태로서, 현대 지식 정보사회에서 중요하게 거론되고 있는 것은 전자상거래와 많은 관계가 있기 때문이다. 즉, 정보의 유통에 있어서 디지털화된 저작물은 그 범위 및 시간적인 면에서 차원을 달리하기 때문에 디지털화의 과정에서부터 유통까지 중요하게 다루어지고 있는 것이다.

디지털 정보의 특성은 원본과 완전히 똑같이 간단하고 또한 순식간에 복사가 가능하고, 정보의 편집·가공 조작성이 용이하며, 네트워크 경유로 직접 콘텐츠에 접근이 가능한 것이다.

2.1 디지털 콘텐츠의 유통 형태

아래 그림 1은 디지털 정보의 유통/이용형태의 변천상황을 나타낸다. 우선, 유통형태는 CD(Compact Disc), DAT(Digital Audio Tape), 최근의 DVD(Digital Versatile Disc) 등의 패키지 매체 유통에서 시작해서 ISDN(Integrated Service Digital Network)은 이미 인터넷 등의 네트워크 경유와 같이 계속해서 새로운 유통형태로 확대되고 있다. 또한, 이용형태는 최초에는 보는 것 뿐/듣는 것 뿐(재생)이던 수동적 이용에서 시작해서 일부복사/변환(편집)을 하기도 하고, 최종적으로는 새로운 2차 저작물을 창작(가공)하는 것으로 계속 변화해 오고 있다. 이러한 디지털 정보의 유통/이용형태의 변천은 예술활동과 콘텐츠 비즈니스 형태로 큰 변혁을 초래할 것으로 예상된다.



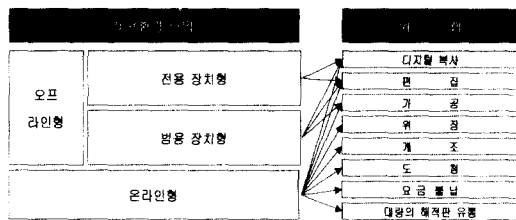
(그림 1) 디지털 정보의 유통/이용형태의 변천

전자상거래에서의 상품판매는 상품의 배송은 기존 유통 채널을 이용할 필요가 있는데, 콘텐츠 판매에

서는 발주나 결제뿐만 아니라 배송도 네트워크 상에서 이루어지기 때문에 원격지라도 즉시 정보 상품을 구입할 수 있어서 편리성이 높다. 또한, 판매자에게도 상점을 개설하는 비용이 들지 않는 것, 재고가 불필요한 것, 유통 채널을 필요로 하지 않는 것 등 콘텐츠 판매의 이점은 크다. 따라서 향후 전자상거래에서는 멀티미디어 디지털 상품을 판매하는 콘텐츠 유통이 중심이 될 전망이다.

급속한 디지털화와 네트워크로 복사에 필요한 장치와 장비의 가격이 많이 저렴해졌다. 게다가 복사본은 원본과 거의 똑같은 품질이라고 하는 이점도 있다. 그런 이유로 불법복사와 개조 등의 불법이용이 무제한 상태가 되어 저작권 관리는 당사자의 지적 양심에 달려있게 되었다.

다음 그림 2는 디지털 콘텐츠의 유통/이용형태의 다양화에 따른 이용 환경의 분류와 예상되는 저작권 침해의 위협 종류를 나타낸다.



(그림 2) 이용환경과 위협의 종류

이러한 정보 유통 환경 하에서 우수한 창작품을 공개하려는 의욕을 저해할 뿐만 아니라 정당한 상거래도 성립할 수 없게 된다. 따라서 디지털 콘텐츠의 지적재산권을 보증하고, 적합한 사용료를 징수하는 시스템의 구축과 동시에 콘텐츠 자체의 유통관리도 가능하게 하는 기술개발이 절실하게 요청되어 각종의 콘텐츠 보호기술이 등장하고 있다.

안전한 디지털 콘텐츠 유통을 위한 콘텐츠 저작권 보호기술의 요구사항을 살펴보면 다음과 같다. 우선, 디지털 콘텐츠에 저작권 정보를 안전하게 표기할 수 있어야 한다. 둘째, 이러한 저작권 표기정보는 유일하게 식별되어야 하며, 암호화하여 관리되어야 한다. 셋째, 여러 저작권 범규에 맞는 저작권 정보관리기술이 포함되어야 한다. 넷째, 암호기반의 불법복제에 대한 대책이 있어야 한다. 다섯째, 저작권 정보가 안전하게 삽입/검출/검증되어야 한다. 여섯째, 저작권 침해/공격에 따른 대응되는 대책이 있어야 한다.

일곱째, 저작권 및 소유자 정보가 관리되어야 한다.

이러한 저작권 보호기술의 요구사항들을 만족시키는 보호기술들의 분류 체계를 살펴보면 2.2절과 같다.

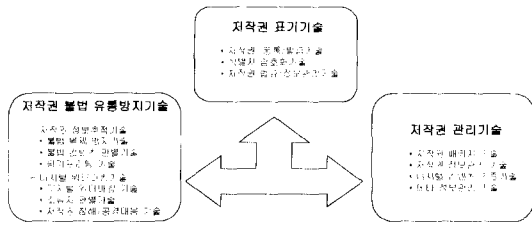
2.2 디지털 콘텐츠 저작권 보호기술 분류체계

저작권이란 '인간의 독창적인 생각을 시각, 청각 또는 시청각을 통하여 지각할 수 있도록 독창적으로 표현한 것(Expressive information), 즉 저작물에 대하여 부여한 독점적이고 배타적인 권리이다. 특히가 새로운 발명이란 아이디어 그 자체를 보호하는 권리라고 한다면, 저작권은 아이디어의 표현(Expression of Idea)을 보호해주는 점에서 차이가 있다. 따라서 타인의 저작물과 동일한 내용이라도 표현이 상이한 경우에는 저작권법의 보호를 받을 수 있다.

이러한 디지털 콘텐츠의 정의에 따른 유통에 있어서 저작권자 권리 보호기술은 다음 기능을 제공하는 것을 목적으로 한다¹⁾.

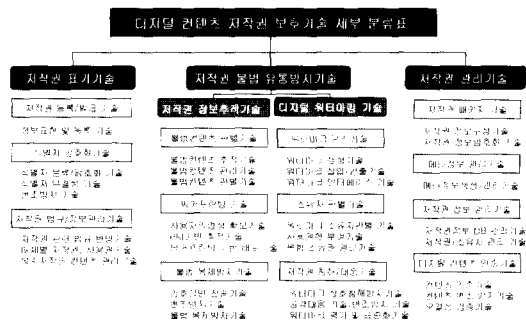
- ① 불법 복제 및 재생을 차단하고, 변경 및 해킹이 불가능한 체계의 저작자가 원하는 사용자와 원하지 않는 사용자를 식별해서, 전자에게만 선택적으로 효용성을 제공한다.
- ② 콘텐츠를 화면을 통해 보거나, 출력, 복사, 전송, 수정하는 등의 다양한 조작성 권한에 따라 가능하고 여러 단계에서 대한 소유 권한에 대한 제어가 가능해야 한다. 뿐만 아니라, 불법 행위의 경우 사용권을 취소하는 기법이 필요하다.
- ③ 멀티미디어의 음악, 그림, 영화, 게임 등 각각의 전달되는 콘텐츠의 특성에 적합한 저작권자 권한 보호가 이루어져야 한다.
- ④ 콘텐츠가 재유통 가능한 디지털 형식으로 누설되는 것을 방지 또는 억제한다.
- ⑤ 콘텐츠의 유통에도 효율적이고, 간단하게 할 수 있도록 지원해야 한다.
- ⑥ 콘텐츠 배포 및 홍보가 용이하도록 하며, 이용자 관리 등 다양한 기능을 제공해야 한다.

이의 목적에 부합되는 유통에 따른 저작권 보호기술을 분류하면 그림 3과 같다.



(그림 3) 디지털 콘텐츠 저작권 보호기술 개념도

저작권 보호기술의 세부 분류는 저작권 보호 대상에 따라 3개 분야로 구분하고 각 분야별 주요 세부 기술은 아래의 그림 4와 같이 나타낼 수 있다.



(그림 4) 주요 디지털콘텐츠 저작권 보호기술의 세부 분류

본 논문에서는 디지털 콘텐츠의 유통에 따른 저작권의 보호 기술을 크게 저작권 표기 기술, 암호기술을 사용한 저작권 정보 추적기술 및 워터마크 중심의 저작권 삽입/검출/검증기술인 디지털 워터마킹 기술 그리고, 표기 체계에 해당하는 XrML/DRM 중심의 저작권 관리기술로 구분된다. 세부 기술영역으로는 저작권 표기기술은 저작권 등록/발급기술, 식별자 암호화기술, 저작권 법규/정보관리 기술로 분류되며, 저작권 불법 유통방지 기술은 크게 저작권 정보추적기술과 디지털 워터마킹 기술로 나누어진다. 이 중 정보추적 기술은 불법 콘텐츠를 판별하는 추적 및 판별, 관리기술과 사용자의 정보를 삽입하는 핑거프린팅 기술 그리고 암호기반 기술을 이용한 불법 복제방지 기술로 이루어진다. 디지털 워터마킹 기술은 워터마크 관리기술과 워터마크 소유자 판별기술, 워터마크의 변조에 따른 방지기술로 구성된다. 마지막으로 저작권 관리기술에는 저작권에 관련된 정보의 암호화 기술 및 저작권/소유자 정보관리 기술, 디지털 콘텐츠 인증기술로 분류되어진다. 지금까지의 여러 콘텐츠 저작권 보호기술들은 상호

연관적인 관계로 구성되어지며, 종합적인 기능으로 구현된다.

III. 디지털 콘텐츠 저작권 보호기술

디지털 콘텐츠 저작권 보호기술은 저작권의 소유자를 추적할 수 있게 하는 디지털 워터마킹, DOI(Digital Object Identifier), INDECS (Interoperability of Data in E-Commerce System)와 같은 저작권 추적기술과 사용권한을 제한하는 저작권 관리기술들로 대별될 수 있다. 저작권 추적기술의 디지털 워터마킹 적용은 간단한 반면 저작권을 적극적으로 보호하지는 못하는 단점이 있다. 이에 반해 암호화 기술을 응용한 저작권 관리기술들은 사용료를 지불한 이용자에게만 사용권한을 줄 수 있어 좀 더 적극적인 저작권 보호기술이다.

전자상거래에서의 활용을 위해 초기에는 특정 사용자에게 콘텐츠를 사용할 수 있는 모든 권한을 부여하는 단순한 방식에서 최근에는 콘텐츠를 볼 수는 있지만 인쇄는 못하게 한다든지, 사용할 수 있는 기간이나 횟수를 제어하는 등의 실 상거래에서 발생할 수 있는 다양한 방식의 사용권한 제어를 시도하려는 DRM(Digital Rights Management) 기술이 개발 상용화되고 있다.

3.1 저작권 표기 기술

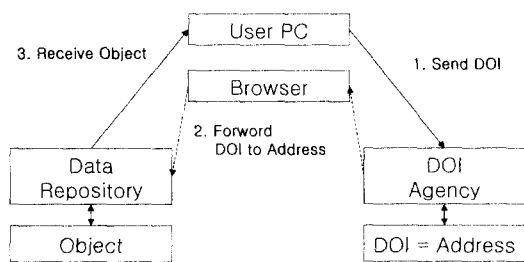
3.1.1 DOI 기반 저작권 표기/등록

저작권 표기 기술은 DOI에 기반한 저작권 표기/등록에 관한 사항으로서 DOI 등록/발급에 관한 부분과 식별자에 대한 전반적인 암호화 기술 및 저작권 법규와 저작권 정보를 관리하는 기술로 나눌 수 있다. DOI 등록 및 발급은 DOI 기반 인터페이스, DB 구축 및 표준화와 관련되는 내용으로 구성되며, 식별자에 대한 디지털 서명, 암호화 및 무결성을 확보할 수 있는 기술이 필요하다. 저작권 법규 부분은 전반적인 저작권 사항과 저작권 정보관리 기술에 대한 사항을 다루게 된다.

디지털 환경에서 저작권 관리를 가능하게 하는 틀을 개발하려는 미국 출판협회인 AAP(Association of American Publishers)의 노력으로부터 발전하여 DOI가 되었다.

DOI는 URN의 특성을 간직하고 있으며, 기존의 식별자 체계를 포함할 수 있기 때문에 그 어떤 식별

자 체계보다 현재 우월하다. DOI가 가지는 최소 기능은 디지털 저작물의 식별자를 부여하는 URN (Uniform Resource Name)의 규격을 만족시키는 것이지만, 다른 큰 장점은 개방적이라는 것이다. URN은 IETF가 URL의 단점을 보완하고 신뢰성 있는 웹 문서를 찾기 위하여 제안한 웹 주소 체계로, 포괄적인 범위, 유일성, 영구성, 규모성(Scalability), 기존의 명명 시스템 지원, 확장성, 독립성을 갖추고 있다. DOI는 URN의 조건에 추가적인 저작권 처리를 위한 기능을 갖추고 있으며, 변환(Resolution)을 통하여 최종적으로 URL로 사상하는 기능을 하게 된다. DOI 처리 과정은 그림 5와 같다¹²²⁾.



(그림 5) DOI를 통한 자료 획득과정

3.1.2 INDECS

INDECS는 디지털 콘텐츠의 전자상거래를 위한 기반 마련과 지적재산권 관리를 위한 메타데이터가 필요하다는 인식하에 시작된 프로젝트로서 1998년 유럽 연합이 지원하는 Info2000프로젝트의 지원을 받아 시작되었다. INDECS의 목표는 상이한 메타데이터 스키마가 상호 호환되고 특정 분야에서 개발된 메타데이터가 다른 분야에서도 이용가능 하도록 하는데 있다. INDECS는 전통적인 메타데이터인 더블린코어와 같은 자원기술 원소를 가지고 있으나 인간과 지적재산권 계약, 그리고 이들 사이에 연결요소를 추가적으로 포함하고 있다. INDECS는 유럽에서, DOI는 미국에서 앞장서 추진중인 국제적인 활동으로 WIPO, NISO, W3C에서 이미 감증을 거쳤으며, ISO와 연계 활동을 추진하고 있다.

INDECS는 지금 등장하는 여러 스킴에 대한 대안을 제공하는 것이 아니고 이들 여러 스킴들이 협력할 수 있는 방법을 제공한다. INDECS 메타스키마는 권리와 표시하는 메타 데이터를 합성할 수 있게 설계되어 있다. 이것은 먼저 고 수준에서 광범위한 멀티미디어 메타데이터 모델을 장시간에 걸쳐서 개발함으로써 시도한다. 지적재산은 물론이고 그 무

엇이라도 기술하는 방법이 하나뿐인 경우는 없다. INDECS 스키마는 최대한으로 광범위한 응용들을 지원할 수 있게 설계된다. 그렇게 한 다음 현실의 데이터원소를 이 모델에 넣어 이를 데이터끼리 연관되는 방법을 조심스럽게 고안함으로써 저 수준에서 접근할 수 있다. 마지막으로 INDECS 스키마는 권리와 내용이 모든 네트워크와 시스템에 걸쳐 인지되게 하기 위해 서로 상이한 스키마를 함께 매핑하는 수단을 제공한다.

3.2 저작권 정보추적기술

디지털 콘텐츠는 디지털 기반의 파일로 되어 있기 때문에 쉽게 불법 유통시키거나 복사할 수 있다. 따라서 불법 콘텐츠에 대해 추적하거나 관리할 수 있는 기술이 필요하며 암호학적 기법 등을 사용하여 이를 판별하거나 방지할 수 있는 기술들이 필요하다. 특히 핑거프린팅 기술과 PKI 기반 기술을 접목하여 불법적 콘텐츠에 대해 추적할 수 있는 기능으로 구성된다. 또한, 콘텐츠 이용의 보호는 안전한 H/W·디바이스를 어느 정도 가정하는가에 따라 방법은 달라진다. 통상 PC상에서 동작하는 소프트웨어에 의해 멀티미디어 콘텐츠의 이용이 제공된다. 안전상 가장 엄격한 케이스에 초점을 맞추는 것으로 해서 소프트웨어의 보호기능을 제공하는 Tamper Resistant 소프트웨어 기술이 있다.

암호화된 멀티미디어 콘텐츠는 반드시 복호된 뒤에 이용되어야 한다. 암호를 해독하는 행위는 곤란하게 되어 있기 때문에 공격자는 암호화된 멀티미디어 콘텐츠가 복호화된 상태 혹은 그 복호화 과정을 공격해서 평문 콘텐츠를 꺼내는 것으로, 해독 가능성을 찾아내려고 할 것이다. Tamper Resistant 소프트웨어 기술은 콘텐츠를 복호하는 소프트웨어 프로그램이나 복호된 콘텐츠를 처리하는 소프트웨어 프로그램을 공격자에 의한 해식행위로부터 보호하기 위한 기술이다.

3.2.1 핑거프린팅(Fingerprinting)

핑거프린팅은 불법으로 유통되는 복사본들을 감시하거나 추적할 때 유용한 방법으로 제품마다 서로 다른 유일한 코드를 부여하여 구매자의 정보를 표시한다.

즉, 디지털 워터마킹에서는 콘텐츠 내부에 소유권자나 판매권자의 정보가 삽입되는 반면에 이 기술은

구매자의 정보가 삽입되는 것이다. 따라서, 핑거프린팅을 이용하면 불법적으로 콘텐츠를 재분배한 구매자가 누구인지 밝혀낼 수 있기 때문에, 구매자들로 하여금 불법적인 재분배를 방지할 수 있다.

핑거프린팅에 필요한 요구사항으로는 콘텐츠 품질 보장성, 강건성(Robustness), 비대칭성(Asymmetry), 익명성(Anonymity), 조건부 추적성(Conditional Traceability) 등을 들 수 있다.

핑거프린팅은 어떠한 암호 알고리즘을 사용하였는가에 따라서 대칭(Symmetric) 핑거프린팅과 비대칭(Asymmetric) 핑거프린팅으로 나누어지고 익명성 보장을 위한 Anonymous 핑거프린팅과 여러 사용자들이 공모하여 공격할 수 없도록 안전성을 제공하는 Collusion Secure 핑거프린팅을 적용한 Traitor Tracing도 핑거프린팅의 한 부분으로 간주된다^[20].

3.2.2 DTCP 기술

DTCP란 Digital Transmission Content Protection의 약자로 셋탑에 내장되는 칩 세트로 구성된다. Hitachi, Intel, Mastushita, Sony, Toshiba가 제안하였고, 기본적으로 IEEE 1394 위에서 동작한다. 현재 DTCP기술이 업계에서는 가장 참고할 가치가 높다. 이 기술이 업계에서 큰 영향력을 행사하는 5개 기업에 의해 결정되었다는 점과, 현재까지 우리가 상상할 수 있는 주요 기술을 망라하고 있다는 점에서 주목을 받고 있다. 이 표준은 다음 세 가지 기준을 염두에 두고 결정되었다.

- (1) 어떻게 하면 저작권을 소유한 콘텐츠 및 기타 중요한 가치를 지닌 콘텐츠를 불법복제로부터 보호할 수 있나?
- (2) 어떻게 하면 사용자를 불편하게 하지 않으면서 PC와 가전 메이커들이 효율적으로 콘텐츠를 보호할 수 있나?
- (3) 어떻게 하면 (IEEE 1394 같은) 디지털 포트들을 PC와 가전제품 사이에 현실적으로 구현할 수 있나?

이 기준에 따라 DTCP는 복제제어정보, 인증 및 키 교환, 콘텐츠 스크램블링, 시스템 정보갱신의 네 기술을 활용하고 있다. 인증 및 키 교환에서는 공개키 방식의 DSA (Digital Signature Algorithm) 및 Diffie-Hellman 키 교환방식을 사용하는데, 여기에

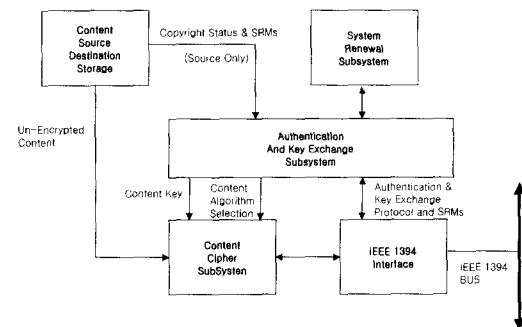
타원곡선암호 ECC (Elliptic Curve Cryptography) 방식을 함께 사용한다.

콘텐츠 스크램블링에는 기반 암호 알고리즘으로 Hitachi의 비밀키 방식의 M6가 사용된다. 이런 알고리즘은 쉽게 크래커의 공격을 받을 수 있기 때문에 30초에 한 번씩 키를 바꾼다. 선택적으로 스크램블링에 Modified Blowfish와 DES (Data Encryption Standard) 두 가지가 사용될 수 있다. 선택적 알고리즘은 인증할 때 협상에 의해 결정할 수 있다. 모든 방식은 안전성을 위해 C-CBC (Converted Cipher Block Chaining) 모드로 운용한다. 모든 알고리즘은 MPEG-2 대역폭을 충분히 만족할 수 있는 성능을 제공할 수 있어야 한다.

키 교환은 기기 사이의 1394 비동기 패킷을 통해 이루어진다. 그런데 이들은 IEC-61883과 IEEE AV/C Digital Interface Command Set 표준을 준수해야 한다.

복제 제어정보는 “자유복제” “일회복제” “추가복제불가” “복제불가” 와 같은 네 종류가 있다. “자유복제”에서는 복제를 금하지 않는다. “일회복제”는 한 번에 한해 복제가 가능하지만 “추가복제불가” 상태가 되어 더 이상의 복제는 불가능해진다. “복제불가”는 디스플레이만 가능하고 복제는 아예 불가능한 콘텐츠 상태를 말한다.

해킹을 시도한 기기의 일련번호는 SRM (System Renewability Message) 리스트에 저장되어 해당 기기가 접속을 시도할 때 거절할 수 있도록 한다. 이 SRM은 계속해서 갱신되어 복제방지에 활용된다.



[그림 6] DTCP의 개념도

3.3 디지털 워터마킹 기술

디지털 콘텐츠가 PC를 이용해서 인쇄·연주되는 경우, 콘텐츠 보호만으로는 디지털 콘텐츠를 완전히

게 보호하는 것은 불가능하다.

예를 들면, 디지털 콘텐츠를 범용 프린터로 인쇄하는 것을 허용한 경우, 프린터 드라이버 경유해서 인쇄 데이터를 파일로 출력하는 행위를 금지하는 수단은 없다. 마찬가지로 음악 데이터는 사운드 보드에 의해 D/A변환되어 연주되지만 사운드 보드로 입력되는 디지털 데이터가 유출되는 가능성을 배제할 수는 없다.

이와 같이 인쇄·연주로 인해 생성된 디지털 데이터의 유출을 완전하게 방지하는 것은, 현 상태의 PC 아키텍처를 전제로 하는 한 불가능하다. 그리고 유출된 콘텐츠가 대량으로 유통되는 것을 억제하는 것을 목적으로 콘텐츠에 저작권 정보 등의 추적 정보를 삽입하는 기술로써 디지털 워터마킹 기술이 알려져 있다.

디지털 워터마킹(Digital Watermarking)은 저작권 정보를 디지털 콘텐츠 속에 삽입시켜 소유자의 저작권을 보호하는 것을 목적으로 하는 기술로서, 콘텐츠에 대한 소유권 등을 판별할 수 있는 기술에 해당된다. 저작권 보호를 위한 디지털 워터마킹 기법의 안전성을 보장하기 위해서, 삽입 정보의 위치를 결정할 때 워터마킹 공격에 대한 견고성과 육안적 비구별성을 동시에 추구해야 하고, 워터마킹 알고리즘의 은닉성 대신 키의 은닉성이 보장되어야 하며, 키의 사용으로 허가받지 않은 사용자의 워터마크 검출을 방지할 수 있어야 한다.

구체적으로 워터마크 관리 기술과 소유자 판별 기술 및 저작권 침해와 공격에 대응할 수 있는 기술로 나뉜다. 워터마크 관리 기술은 삽입, 추출 및 관리 기능을 제공하며, 소유자를 검증하고 사용권한을 검증할 수 있는 체계에 해당된다. 또한 워터마크에 대한 상호 침해 방지 기술을 제공하고 안전성을 평가할 수 있는 기준을 제공한다. 현재까지 개발됐거나 개발이 진행중인 워터마킹 기술은 워터마크가 삽입되는 매체에 따라 오디오/이미지/비디오/텍스트 워터마킹 등으로 크게 구분된다.

워터마킹은 비소유권자의 불법적인 조작을 막고 저작권 보호(Copyright Protection), 데이터 인증(Data Authentication), 소유권 증명(Ownership Identification)을 효율적인 방안으로 제공해 준다.

한편, 안전한 디지털 워터마킹을 위한 요구 조건을 살펴보면 다음과 같다.

- ① 원본 이미지와 워터마크가 삽입된 이미지의 화

질이 육안으로 구별되지 않아야 한다.

- ② 허가받지 않은 사용자는 워터마크를 검출할 수 없어야 한다.
- ③ 워터마크를 검출하는데 원본 이미지나 워터마크 삽입 이미지를 사용하지 않아야 한다.
- ④ 워터마크 데이터는 삽입될 이미지를 적절한 수준에서 손상시키는 이미지 처리에 견고해야 한다.
- ⑤ 워터마킹 기법 알고리즘은 공개되어야 하고, 오직 개인키의 은닉성이 이미지 저작권을 보호할 수 있어야 한다.

3.4 저작권 관리기술

XML 방식으로 디지털 콘텐츠를 전송하는 체계가 표준으로 정착되면서 콘텐츠에 대한 저작권을 표기하고 저작권을 관리하기 위한 기술이 필요하게 되었으며, XrML로 대표되는 저작권 표기 방식이 제시되어 종합적인 측면에서 개선된 저작권 관리기능을 제공할 수 있다. 따라서 콘텐츠에 대한 저작권 보호기술로서 XrML에 기반한 저작권 표기 및 관리 기술을 중심으로 DRM 저작권 정보관리 및 인증기술로 구성된다.

콘텐츠 저작권 관리기술은 앞의 추적기술에 비해 좀더 적극적인 방안을 제시한 기술로 암호화 기술을 이용하여 디지털 콘텐츠를 안전하게 보호함으로써 콘텐츠 제작자의 권리 및 이익을 지속적으로 보호 및 관리하는 기술이다. 이러한 기술은 DRM이라는 대중적인 용어로 사용되는데, DRM은 디지털 콘텐츠의 안전한 유통(Trusted Digital Content Commerce)이라고 간략화할 수 있다. 즉, 디지털 콘텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다. 디지털 콘텐츠는 저작권자가 지정한 규칙과 함께 패키징되어 암호화되며, 콘텐츠를 이용하고자 하는 사용자는 동봉된 규칙을 만족해야만 이용이 가능한 것이다.

DRM은 소프트웨어와 e메일, 디지털문서 등 디지털 자산뿐만 아니라 음악 영상 출판물 등 각종 온라인 콘텐츠의 저작권을 안전하게 보호하고 관리할 수 있는 기술이다. 또한 콘텐츠의 보안과 저작권 보호뿐만 아니라, 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통 관리까지를 일괄 지원하는 기술이다. 여기에는 적법한 사용자만 콘텐츠를 사용하고

적절한 요금을 지불하도록 만드는 디지털 저작권 관리기술, 저작권 승인과 집행을 위한 소프트웨어 및 보안 기술, 지불 결제기술이 모두 포함된다.

컨텐츠의 저작권 침해를 근본적으로 차단하기 위한 저작권 관리(DRM) 기술들은 다음과 같은 기능들을 기본으로 한다.^[15]

① 암호화 및 키 관리 기능

DRM 기술은 기본적으로 암호화 기술들을 응용하고 있다. 암호화 된 콘텐츠를 배포하여, 복호화키가 없는 사람은 암호화된 콘텐츠를 사용할 수 없도록 한다. 이 복호화 키를 어떤 방법으로 관리하느냐에 따라 여러 방안들이 있다. 다음은 대표적인 암호화 방법이다.

- 대칭키 암호(Symmetric Key Encryption) : 양측에서 똑같은 키를 갖고 있어서 데이터에 접근하려면 이 키가 있어야 한다. 대표적인 알고리즘으로 DES(Data Encryption Standard), IDEA, Blowfish 등이 있고 대칭키 암호는 빠르다는 장점을 가지고 있다.
- 공개키 암호(Public Key Encryption) : 2개의 키가 하나는 암호화를 할 때, 또 하나는 복호화를 할 때 쓰인다. 대칭키와 다른 점은 암/복호화 키가 다르다는 것이다.
- 해쉬함수 (Hash Function) : 큰 화일을 입력받아 작은 수를 생성한다. 즉, 각각이 다른 길이의 입력을 받아 고정된 길이의 출력을 생성한다.

② 콘텐츠의 지속적 보호 기능

사용권한을 가지고 있는 사람이 암호화되어 있는 콘텐츠로부터 암호화되지 않은 콘텐츠를 쉽게 만들 수 있다면 여전히 저작권 보호는 미흡하다. 따라서 항상 사용할 때 이외에는 콘텐츠가 암호화된 상태로 존재하도록 하여야 하며, 사용 중에도 복호화된 콘텐츠의 추출을 어렵게 하는 기술이 필요하다.

③ 사용 규칙 정의 및 제어

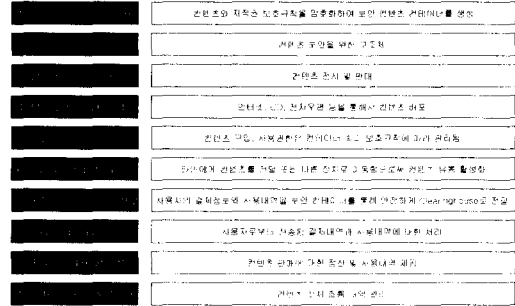
저작권의 관리방법 즉, 콘텐츠의 사용규칙을 정의하는 방법 및 그 정의대로 보호되도록 제어하는 일련의 기술들이 필요하다.

④ 사용내용 측정

저작권을 보호하는 근본적인 목적은 제작자에게 경제적인 이득을 보장해 주는 일이다. 이에 사용내

역을 측정할 수 있는 기능이 필요하다. 이 정보를 근거로 과금을 할 수 있게 되며 금융 결제처리를 자동화할 수 있도록 발전되어 왔다.

DRM을 이용한 디지털 콘텐츠 유통 플랫폼으로서의 세부적인 절차를 살펴보면 다음과 같다.^[14]



(그림 7) DRM을 이용한 디지털 콘텐츠의 유통 흐름도

① 콘텐츠와 사용규정의 패키징

콘텐츠 제작자는 판매할 콘텐츠와 적용될 규정을 함께 암호화하여 Secure Content Container로 패키징한다. 규정은 사용자가 콘텐츠를 사용하는 시점에 적용될 사용규칙 및 조건으로 사용료 및 사용권한, 사용기록 내역조회 방법, 사용료 부과방법 등의 정보를 담고 있다.

② 콘텐츠 배포

패키징된 콘텐츠는 최종 사용자에게 전달될 때까지 Secure Content Container에 의해 안전하게 보호된다. 이는 인터넷이나 CD-ROM 또는 E-Mail을 통해서 전달되어 진다.

③ 콘텐츠 구입 및 사용

이용자가 콘텐츠를 사용하는 시점에 콘텐츠와 함께 패키징된 규정에서 정의한 사용 규칙 및 조건이 이용자에게 제시된다. 이용자는 제시된 규정에 대하여 동의를 함으로서 콘텐츠의 사용권한을 부여 받는다.

④ Superdistribution

콘텐츠 사용자는 이 콘텐츠를 친구에게 전달할 수 있다. 비록 구매한 이용자가 콘텐츠에 대해 사용권한을 취득한 상태라고 하더라도 전달받은 친구가 사용규정을 만족해야만 사용권한을 부여받을 수 있다.

⑤ 결제정보 및 사용내역 관리

이용자가 사용한 콘텐츠의 결제정보 및 사용내역

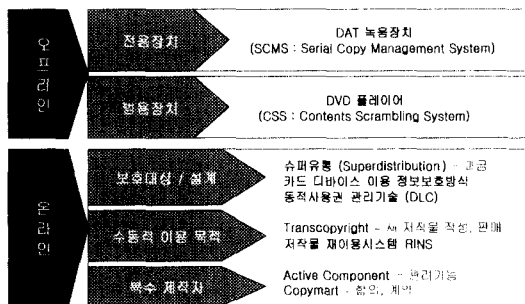
은 Clearinghouse로 전송된다. Clearinghouse는 전송된 결제정보 및 사용내역을 처리해서 콘텐츠 소유자와 콘텐츠 유통업자에게 정산 금액 및 판매내역을 제공한다.

IV. 저작권 보호기술 동향

본 장에서는 이용환경과 표준화에 따라 보호기술 동향을 분석하고, 이를 근거로 주요 콘텐츠 저작권 보호기술과 서비스 사례를 알아본다.

4.1 이용환경에 따른 저작권 보호기술 동향

오프 라인·전용장치형, 오프 라인·범용장치형 및 온라인형의 각 이용환경에 있어서 저작권 보호 기술의 동향에 대해 실제적인 예를 기반으로 살펴보면 그림 8과 같다^[2].



(그림 8) 이용환경에 따른 저작권 보호기술의 동향

4.1.1 오프라인·전용장치형

오디오 분야 최초의 디지털 녹음기인 DAT녹음장치(Digital Audio Taperecorder)는 해적판을 유통시키는 온상이 되고 있었다. 판매 초기에는 디지털 복사가 불가능한 구조였다. 그 결과, 디지털 녹음기에 대한 호응도가 반감하여 이용자로부터 관심이 멀어졌다. 그 후 콘텐츠 제공자 측과 이용자 측의 절충안으로 디지털 입출력 인터페이스를 설치하는 대신에 SCMS(Serial Copy Management System)방식이라고 하는 복사제한 기구를 의무적으로 포함시켜 판매하게 되었다.

이 방식은 매체의 특정영역에 원본(1회 복사가능), 1세대 복사 끝남(복사 불가) 등의 플래그를 설치, 다른 DAT로의 복사시에 복사원의 플래그정보를 파악해서 복사 가능여부를 판단하는 방법이다.

SCMS방식은 1세대까지의 디지털 녹음은 가능하지만 2세대 이후의 디지털 녹음은 금지하는 방식이다. 복사 조작 후, 이전 복사 매체 플래그는 『1세대 복사 끝남(복사 불가)』이 된다. 단, 복사 매체 플래그는 변화하지 않는다. 즉 하나의 부모 DAT에서 복수의 자식 DAT로의 Parallel 복사는 가능하지만 기하급수식 계산식으로 복사수가 급증하는 자식 →손자→...의 시리얼 복사를 금지하는 것을 설계 방침으로 한다. 그 후에 상품화된 MD(Mini Disc)에도 마찬가지로 기구를 포함시키는 것이 의무화되었다. 역시 콘텐츠 제공자 측으로의 담보로써 DAT/MD 등의 매체 및 녹음기에 일정 비율의 저작권료를 추가해서 판매되고 음악관계의 저작권 단체로 환원되는 구조가 설계되었다.

4.1.2 오프라인·범용장치형

고밀도 기록 기술, 화상 부호화 기술 등의 발달에 의해 CD와 같은 직경의 디스크에 133분의 영화(4.7MB의 디지털 동화상 및 음성 추적 가능)등이 상용 TV만큼의 품질로 재생 가능한 DVD(Digital Versatile Disc)가 1996년부터 발매되었다. 당초에는 DVD전용 플레이어 장치로써 발매되어 TV 모니터에 접속해서 영화감상 등을 하는 것이 주요한 이용 형태였다. 최근에는 대용량이며 또한 멀티미디어 정보의 Random Access가 가능하다는 특징을 살려 CD-ROM 장치에 대신하는 기억장치로써, PC내장의 DVD장치가 발매되기 시작했다. PC기능을 이용해서 대화형으로 영화를 재생하는 것뿐만 아니라 앞으로 OS와 대용량 응용 소프트웨어의 공급 매체로서도 주목되었다.

범용PC와 대용량 디지털 콘텐츠 기록 매체가 불법복사 또는 부정 편집·가공된 해적판 저작물의 유통에 의한 저작권자의 권리침해문제는 심각한 것으로 예상된다. 그래서 영화, 민생전자기기, 컴퓨터 산업계에서 구성되는 단체 CPTWG(Copy Protection Technical Working Group)에서 DVD의 저작권 보호방식이 검토되고 있다. CPTWG에서 상정하고 있는 것은 일반 소비자에 의한 불법복사이다. 전문가의 해적판 작성행위까지 방지하는 것은 불가능하다. DVD장치의 구비요건은 다음 4가지이다.

① 암호화된 영상과 오디오 데이터를 해독하는 것 :

콘텐츠 암호화에는 Master Key(키 관리기구 관리), Disc Key, Title Key(저작권자가 관리)의

세 개의 암호키를 계층적으로 이용하고 있다. DVD 내용을 그대로 다른 매체에 기록해도 재생 불가능하다.

② 지역설계정보에 의한 재생 제한에 대응 가능한 것 : 전 세계를 6분할해서 같은 지역에서 구입한 DVD매체와 플레이어의 조합으로 밖에 재생이 불가능하다.

③ 아날로그 VTR등으로의 복사 제한을 설계하는 것 : 아날로그 VTR 등에 복사할 때 이전 복사의 영상이 흐트러지고, 사용할 수 없게 된다.

④ PC의 버스를 통과하는 데이터의 복사방지를 하기 위해서 버스 인증 기능을 구비하는 것

암호를 사용해서 일반적으로 실현하고 있는 Challenge Response방식에 의해 DVD장치와 PC의 DVD 데이터 복호화부와의 사이에서 상호인증을 하고, 서로가 인증을 받은 DVD모듈인 것을 확인한다. 인증에 성공한 후, 데이터 전송 그 때마다 변하는 키(Bus Key)에 의해 Disc Key와 Title Key를 암호화해서 DVD장치에서 PC로 보낸다. PC측에서 데이터를 복호하는 구조를 채용하고 있다. PC측의 복호처리부는 암호해제용 전용 LSI등 하드웨어에 의해 처음에는 실현했지만, 최근에는 'Tamper Resistant Software'라고 불리는 Debugger를 등에서도 내부가 해석되기 어려운 소프트웨어에 의한 실현 형태도 출현하고 있다. 역시, 최근의 CPTWG의 움직임으로서 복사 가능회수정보를 전자 워터마킹기술을 이용해서 콘텐츠 내에 삽입하는 것에 의해 복사 가능한 회수를 제한하는 방법을 검토하고 있는 중이다.

4.1.3 온라인형

PC와 네트워크를 연결시켜서 온라인형 이용환경에서의 콘텐츠 보호기술은 그 보호대상, 설계 아이디어에 의해 여러 가지 방식이 제안되고 있다.³⁾⁽¹⁴⁾⁽¹⁵⁾

① 슈퍼유통(Superdistribution)

슈퍼유통이라는 것은 PC용 프로그램 소프트웨어를 중심으로 하는 디지털 지적재산권을 소유가 아닌 이용을 전제로 한 것에 의해 유통시켜 네트워크를 통해서 적정하게 과금한다는 개념이다. Tamper Resistant기구에 의해 구성되는 슈퍼유통 컴퓨터에 소프트웨어의 사용상황을 기록하는 구조를 부여한다. 또, 소프트웨어 본체는 식별 코드, 암호키 정보

와 과금정보 등을 포함하는 슈퍼유통 소프트웨어로써 구성된다. 소프트웨어의 입수경로는 네트워크, 패키지 매체, 위성방송, 더욱이 타인으로서의 양도 등 한정하고 있지 않다. 소프트웨어를 사용할 때마다 사용 기록이 관리되고 그것을 회수하는 것에 의해 요금을 징수해 수입을 재분배하는 시스템으로서 제안되고 있다

② 카드 디바이스 이용 정보보호방식

암호·인증·디지털 서명의 암호기술 및 카드 디바이스 기술을 이용한 VOD(Video On Demand) 서비스를 위해 저작권 보호기술이 제안되고 있다. 이용자 개인을 인증하고 암호화 콘텐츠를 복호하는 키를 저장하는 휴대 가능한 카드 디바이스를 도입해 디지털 콘텐츠를 서버에서 사용자 장치까지 배송하는 것부터 이용하는 것까지 정규 이용자 외에 액세스 불가능한 구성으로 되어 있다. 게다가 정규 이용자라도 암호화되어 있지 않은 디지털 데이터의 입수는 불가능하다.

③ 동적 사용권 관리기술(DLC : Dynamic License Control)

DLC는 사용자와 컴퓨터 기반의 사용권 관리를 기본으로 한다. 보조적으로 지정된 사람을 사용권의 기본으로 하는 경우는 사용자 기반(UBL)이라고 하고, 지정된 컴퓨터를 사용권의 기본으로 하는 경우는 컴퓨터 기반(CBL)이라고 한다. 콘텐츠의 종류에 따라 사용권 관리가 다를 수 있다. DLC서버는 DLC 서버가 발행한 신분증을 이용하여 사용자를 식별할 수 있다. 컴퓨터의 식별은 사용자가 제공한 컴퓨터의 정보를 이용한다. 따라서 현재의 사용권 관리 상황은 사용자의 완벽한 식별이 가능하며, 컴퓨터를 식별하는 경우 제한적이다. 그러나 앞으로 CPU가 ID 제공한다면 사용자가 별도의 정보제공 없이도 완벽한 컴퓨터의 식별이 가능하다. 사용권의 종류는 영구 사용권과 일정기간 사용권 지원으로 구분할 수 있다. 사용료 지불 종류는 무료, 유료, 기준, 사용자수 기준, 업그레이드, 학생, 일반 등으로 나눌 수 있다. 사용권을 불법적으로 남용하는 경우 사용권의 취소 행위에 해당된다. 이에 따라서 사용권 또는 신분증 갱신시 거부할 수 있다.

다음의 두 가지 방식은 주로 수동적 이용을 목적으로 한 저작권 보호방식이고 또한 Tamper Resistant적인 하드웨어 기구를 필요로 하는 것이 공통점이다.

④ Transcopyright

제 3자가 다른 권리자 저작물의 일부를 참조해서 새로운 저작물을 작성·발매할 때 권리 허락절차를 Transcopyright로써 제안한다. WWW에서 유통하는 저작물의 HTML 기술 내에 저작권 관리정보를 기입해 두고, 제 3자가 참조해서 자신의 콘텐츠 내에 붙일 때, 그 콘텐츠의 권리정보가 부가되는 구조이다.

⑤ 저작물 재이용 시스템 RINS

이 시스템은 저작물의 부정이용을 방지하면서 재이용을 가능하게 하기 위한 구조를 제안하고 있다. 데이터를 실체(암호화된 데이터)와 사용권(복호기)으로 분산하고, 사용권은 IC카드 등의 Tamper Resistant적인 디바이스 등에서 안전하게 관리한다. 데이터의 이용시는 OS가 복호, 표시, 외부기억장치 등으로의 출력 등을 관리·제한해서 데이터를 보호한다. 또, 콘텐츠 2가 내장된 콘텐츠 1의 이용시 콘텐츠 2의 사용권을 소유하지 않은 이용자는 콘텐츠 1내의 콘텐츠 2부분을 이용 불가능한 구조를 제안하고 있다.

다음 두 가지 방식은 주로 복수의 저작권자의 소재를 합성해서 새로운 콘텐츠를 작성할 때의 권리처리 및 액세스권 관리의 구조를 중심으로 제안하고 있다.

⑥ Active Component

인터넷에 의한 멀티미디어 정보의 유통시, Active Component라고 불리는 콘텐츠의 관리기능을 분담하는 부분을 사용자 장치 내에 설계하는 방식이 제안되고 있다. 우선, 콘텐츠 제공 서비스를 받기 전에 사용자 장치를 한결같이 특정하기 위해서 머신 ID를 Component Server라 불리는 서버에 등록하고, 복호키 등을 포함 Active Component를 발행받은 사용자 장치에 저장한다. 머신ID를 예를 들어 OS버전, 메모리사이즈, 외부기억장치종류, 제조번호, 디렉토리·파일 구성 등의 보조변수에 의해 계산된다. 이후는 Web서버에서 콘텐츠를 다운로드할 때, 사용자 장치의 Active Component와 서버 사이에서 인증·암호통신이 이루어지고 콘텐츠가 보호된다. 이것은 공개키 암호를 이용한 인증 방식으로 유추할 수 있다. (증명서 발행기관이 Component Server이고 공개키 증명서가 Active Component에 상당한다.)

⑦ Copymart

저작물 판매를 위해 합의·계약에 기초해서 저작권 시장 Copymart의 개념이 제안되어 있다. 이 개념은 저작권자의 의지로 자기의 저작물의 이용 조건을 결정해서 정보를 제공하는 것이 가능, 이용자는 그 조건으로 대가를 지불해서 찾는 데이터를 입수할 수 있다. 저작권 체제, 기술, 비즈니스 3자의 공존을 고려한 시스템이라고 말할 수 있다.

4.2 저작권 보호기술 표준화동향

디지털 통신이 활성화되면서 멀티미디어 콘텐츠 보호가 초미의 관심사로 대두되고 있다. 한번의 클릭으로 디지털 콘텐츠가 무한 복제되어 유포될 수 있지만 콘텐츠의 질에는 전혀 성능저하가 발생하지 않는다. 따라서, 디지털 콘텐츠의 복제방지가 효율적으로 이루어지지 않을 경우 멀티미디어 콘텐츠 산업은 활성화되기 어렵다. MP3나 DVD 산업이 부상하고 있고, 2000년대에는 본격적으로 디지털 TV 방송이 개시될 상황이지만, 멀티미디어 콘텐츠 보호는 이제 겨우 태동단계에 있다. 유럽에서는 위성방송 수신을 위한 CA(Conditional Access) 스마트카드가 도입되었다. 최근 OPIMA, SDMI, DVD Forum의 CPTWG, MPEG의 IPMP 등이 이 분야 표준화를 위해 노력하고 있다. 국내에서도 DMC가 결성되어 표준화 노력을 경주하고 있다¹⁷⁾.

멀티미디어 콘텐츠 보호를 위해 활발히 움직이고 있는 표준화 기구는 표 1과 같다. OPIMA는 포괄적인 디지털 콘텐츠 복제보호를 위한 표준을 정하고 있다. SDMI는 MP3 음악을 1차 대상으로 표준을 정하고 있다. DVD Forum의 CPTWG는 DVD 콘텐츠 복제방지가 주요 관심사이다. MPEG은 IPMP(Intellectual Property Management and Protection)를 규정하고 있다. 이 표준화 모임은 음반 산업을 대표하는 미국 레코드 업계 조합인 RIAA(Recording Industry Association of America), 영화 산업을 대표하는 MPAA(Motion Picture Association of America), 가전제품 메이커를 대표하는 CEMA(Consumer Electronics Manufacturers Association) 등과 관심 기업들이 주축을 이루어 각종 표준을 정하고 있다. 국내에서는 전자부품연구원이 주축이 되어 DMC(Digital Music Consortium)를 결성해서 MP3 위주로 표준화를 진행하고 있으며, 디지털 콘텐츠 보호표준안

마련을 목표로 설립한 'SDM표준화 워킹그룹'을 통해 표준화활동을 선도해 왔다. 최근에는 정통부 산하의 디지털 콘텐츠포럼, (사)한국디지털콘텐츠 학회 등이 활동하고, '디지털음악표준화그룹(DMSG)'도 출범하여 활동을 하고 있다.

(표 1) 주요 표준화 기구

OPIMA	Open Plat form Initiative for Multimedia Access (http://drogo.cselst.stet.it/ufv)
CPTWG	Copy Protection Technical Working Group DTDG (Digital Transmission Discussion Group) DHSG (Data Hiding Sub-Group) (http://www.dvcc.com/dhsg/)
MPEG	Moving Picture Experts Group (http://drogo.cselst.stet.it/mpeg/) IPMP (Intellectual Property Management and Protection)
SDMI	Secure Digital Music Initiative (http://www.sdmi.org/)
DMC	Digital Music Consortium (http://www.kdmc.or.kr/)

4.2.1 SDMI (Secure Digital Music Initiative)

SDMI는 디지털 음악파일의 포맷 표준개발을 추진하기위한 음반업체의 컨소시엄을 뜻한다. 인터넷을 통한 음악파일의 안전한 유통을 위해 전세계 주요 음반사들과 관련 단체와 업체들이 모여 결성하였으며, 음악의 저작권을 보호하고 불법 복제를 방지하기 위한 기술개발을 목표로 한다^[21].

4.2.2 STEP 2000

STEP2000은 "디지털 워터마킹" 기술을 기반으로 디지털 음악 유통의 성공적인 실현을 위한 국제평가 프로젝트로서, 일본 저작권 협회와 국제 저작권 관리 단체인 프랑스의 CISAC와 BIEM에 의해 실시되는 것으로 워터마킹 기술의 능력을 인정하고, 향후 기술의 이용증진에 목적을 준 프로젝트이다^[21].

4.2.3 MPEG(Motion Picture Expert Group)

멀티미디어를 인터넷과 디지털 저장의 효율적인 응용을 위해 부호화 방법을 체계적으로 연구하고 표준화 작업을 하기위한 ISO/IEC의 기술자문위원회 산하 전문가 그룹(SC29 WG11)을 말한다. MPEG

표준화 작업은 MPEG1, MPEG2, MPEG4, MPEG7, MPEG21으로 진행중이다^[21].

4.2.4 IDF(International DOI Foundation)

DOI 식별 체계의 규격화 활동을 진행중인 IDF는 1997년 10월에 미국 출판 협회(Association of American Publishers)의 기술 위원회(Enabling Technologies Committee)에 의하여 공식적으로 시작되어, 초기에는 DOI 식별자를 서적 관련 분야에 적용시키는 것을 중심으로 진행하였고, 이후 DOI를 인터넷 상에서의 멀티미디어 콘텐츠를 식별하기 위한 식별자로서 구성하는 것으로 발전되어 왔다. IDF에서는 DOI 부문의 시스템 구성 및 기구의 구성에 대하여 연구, 검토되어지고 있다^[22].

4.2.5 cIDf(Content Identification Forum)

cIDf는 일본 내에서 디지털 콘텐츠의 유통에 대한 프레임워크를 구성하기 위하여 동경대의 Hiroshi Yasuda 교수를 의장으로 NTT, 교토 Digital Archive Organization, Dentsu, Hitachi, Matsusita 전기 공업, Sharp, PDC 가 중심이 되어 1999년 8월에 설립된, 디지털 콘텐츠에 삽입되어 저작권 보호 및 인증에 이용될 수 있는 "Content ID"의 표준화를 목적으로 하고 있다. cIDf에서는 워터마킹을 이용하여 콘텐츠마다 "content ID"라는 것을 삽입하여 콘텐츠의 저작권 정보를 명확히 하고, 콘텐츠의 유통을 통하여 발생하는 이익을 보장하며, 바코드와 같은 기능을 디지털 콘텐츠에 제공함으로써 디지털 콘텐츠 유통 관리 및 분석을 가능하게 하고, 불법적인 복제에 대한 감시 기능을 확립하며, 다양한 데이터 베이스로부터 콘텐츠를 획득하거나 탐색할 수 있는 서비스를 제공하려 한다.

V. 국내외 저작권 보호제품/서비스 동향

5.1 국내 동향

5.1.1 BR Netcomm사의 Digicap

Digicap은 통신상의 디지털 콘텐츠 유통시대를 맞아 저작권 보호를 통한 저작권자의 권리를 지키고 소비자들에게 합법적으로 편리한 콘텐츠 제공방법을 마련하기 위해 개발되었다. Digicap은 보안에 관련한 암호화 방식에 BolwFish 알고리즘을 사용하고, 사용자 인증방식은 가변형 개인 Key 형태인 Token

을 사용한다. 완벽한 보안 구조를 갖추어 Key의 복제나 변조가 불가능하며, 사용자가 ID를 공유하는 경우에도 중복 생성을 제한하거나 허용할 수가 있다. 서비스의 제공업체는 이와 더불어 발급하는 Key에 다양한 부가 사항을 함께 적용할 수 있도록 설계되었다. Digicap은 Smart Card를 지원하므로 Off-Line에서의 사용자 인증을 가능케하며, 앞으로 전자지갑을 이용한 전자상거래 시장이 활성화 될 경우 추가투자 없이 콘텐츠 사업을 본격화할 수 있다는 점이 장점이다.¹³⁾

5.1.2 삼성의 secuMAX

secuMAX는 1999년 1월 1일부터 상용화가 시작된 삼성의 MP3 미디어 데이터 유통 기술로서, SNAKE 알고리즘을 바탕으로 한 순수 국내기술로 개발되었다. 사용자는 우선 MP3 디지털 콘텐츠 서비스 사이트에서 회원등록을 하게 된다. 회원 등록 시 사용자의 ID, Password, 주민등록번호를 secuMAX 서버에 등록하게 되는데, 이것은 사용자 인증 역할을 수행하는 기초 자료로 활용된다. 회원 등록을 마친 후 암호 해독키와 전용 플레이어를 다운로드받는데, secuMAX 복호화 모듈이 내장된 Music Drive가 들어 있다. 암호 해독키는 music drive를 설치하는 과정에 등록하도록 되어 있으며, secuMAX를 이용하는 MP3 디지털 콘텐츠 음악 서비스 사이트로부터 다운로드받은 음악 파일을 재생할 수 있게 된다.¹²⁾

5.1.3 MarkAny

국내 회사로 유일하게 STEP2000에서 5개 업체 중 2위, SDMI phase 1에서 4개 업체중의 하나로 선정된 바 있다. 주요 제품으로는 MAVI(비디오 워터마킹), MAO(오디오 워터마킹), MAIM(이미지 워터마킹), MAVEC(벡터 워터마킹), MPACS(전자 의료영상 위변조 방지), MEDI(전자문서 위변조 방지) 등이 있다.

MAIM (MarkAny-Image)는 기존의 제품이 사용자 정보를 48개 정도의 바이너리 키(0110의 숫자열) 조합으로 삽입, 추출하므로 이미지의 변형, 압축 등에 쉽게 깨지는 단점을 가지고 있어 이런 제품들의 단점을 극복하고자 이미지 형태의 데이터를 원본 이미지에 삽입, 복원할 수 있도록 구성되었다. MAO(Mark Any-Audio)는 사용자가 저작한 음원 파일(wave)에 저작권을 기존의 PSN(Pseudo

-Random Noise)형태로 삽입하는 것이 아니라 로고 등의 이미지 형태로 삽입할 수 있으므로 삽입 정보량이 많고 여러 공격에 대해서도 확실하게 육안으로 저작권 정보를 확인할 수 있는 장점을 가지고 있다. MAIC(MarkAny-Identification Card)는 자동으로 디바이스에서 사용자 신원 카드에 내재되어 있는 워터마킹 및 카드정보를 인식하고 이를 외부 장치 핸들 및 서버와 연동하여 신원 관리 목적으로 사용할 수 있으며, 중요 카드 또는 문서의 위조 및 변조를 적발할 수 있다.¹⁷⁾

5.1.4 실트로닉

1999년 후반 설립된 회사로 자체 기술개발과 한국전자통신연구원의 기술과 출원된 특허를 기반으로 워터마킹 솔루션을 보유하고 있다. 워터마크 알고리즘을 이용한 멀티미디어 콘텐츠의 저작권 보호 솔루션으로 Magic Tag 오디오, Magic Tag 이미지, Magic Tag 등이 출시되어 있다.

5.1.5 콘텐츠코리아

콘텐츠코리아의 솔루션은 워터마크 자체에 암호화 알고리즘을 구현함과 동시에 콘텐츠 복제시 전자상거래 보안 인증시스템 기술을 적용했다. 또한 국내 처음으로 자신의 콘텐츠가 어디서 어떻게 사용되고 있는지를 실시간으로 추적할 수 있는 기능을 제공하고 있다.

대표적인 솔루션은 콘텐츠 보호를 위한 워터마킹 시스템인 '콘텐츠가디안 V.1.5' 로, 이 제품은 스탠드얼론형과 ASP형, 그리고 서버형 등 3가지로 구성됐다. '@스탠드얼론'은 개인용 컴퓨터에 설치 후 이미지나 오디오 또는 비디오에 대한 워터마크 삽입이 가능한 제품이며, '@ASP'는 중소기업체나 일반인을 위한 웹 서비스로 이 회사의 워터마킹 사이트에 회원으로 가입하면 웹 상에서 디지털 콘텐츠에 워터마크를 삽입하거나 추출할 수 있다. '@Server'는 대용량 서버 탑재형 제품으로 역추적 기능이 내장돼 있다.

5.2 국외 동향

5.2.1 InterTrust사의 DRM

InterTrust DRM(Digital Rights Management)은 전통적인 컴퓨팅 환경에 기본적인 새로운 기능성을 추가하는 소유권 소프트웨어와 기술을 기반으로

로 한다. InterTrust DRM 플랫폼은 InterRight Point', 'DigiBox Container', 'Usage Rules', 'Transaction Authority'의 4가지 요소로 구성된다. 'InterRights Point'는 InterTrust 구조의 핵심 구성요소로 각 당사자의 디지털 권리를 원격으로 관리하는 안전한 가상머신의 역할을 한다. InterTrust 시스템에 의해 보호된 정보는 'DigiBox container'라 불리는 형식으로 암호화되어 저장되며, 'DigiBox Container'에서 그 정보가 안전하지 못한 통신망으로 유출되더라도 하나의 'InterRights Point'를 통해서만 접근할 수 있으므로 지속적인 제어가 가능하다. 콘텐츠는 'Usage Rules'에 의해 관리되고, 이러한 규칙 또한 'DigiBox Container'에 저장되어 배포된다. 'Transaction Authority' 프레임워크는 'InterRights Points'를 InterTrust 파트너의 데이터 센터와 연결하는 통신제어 시스템이다^[11].

5.2.2 일본 NTT연구소의 Infoket

Infoket은 일본의 NTT연구소에서 개발한 인터넷 경유로 디지털 화상 콘텐츠를 안전하고 확실하게 구입할 수 있는 콘텐츠 정보를 정보 서버상에서 암호화한 후에 부가정보와 함께 인터넷 상에 유통시키고, 최종적으로 정보를 참조한 사용자로부터 그 요금을 회수하는 플랫폼이다. 여기서는 네트워크 상에서 도건을 막기 위해 콘텐츠를 암호화한 것 외에, 개조, 위장을 막기 위해 전자서명을 붙이는 정보의 캡슐화 기술, 안전한 복호키 배송기술 및 전자 쿠폰이라 불리는 소액 결제기술에 의해 개발된 네트워크 상에서 안전하고 확실하게 정보를 구입할 수가 있다. 콘텐츠 유통 문제에 대응 가능한 정보의 캡슐화 기술을 이용한 정보유통 모델기술인 Infoket은 대규모의 특정 조직만이 아니라 일반 사용자가 정보등록 서버에서 간단하고 쉽게 정보상품을 등록하는 것이 가능하다. 이는 정보상품을 판매정보와 함께 암호화함과 동시에 캡슐화해서 개조를 방지하는 것뿐만 아니라 자유롭게 네트워크 상을 유통시킨다. 사용자가 정보 상품으로의 접근을 하기 위해서는 네트워크상의 복호키를 배송하는 서버에 접근해서 결제 절차 후 복호키를 입수해서 복호한다. 키 배송은 안전한 키 배송 프로토콜을 정의해서 이용한다^[2].

5.2.3 Digimarc사의 MarcCenter

디지털 워터마크에 관해 가장 주목 받을만한 제품

을 내놓고 있는 곳으로 Digimarc사가 있다. Adobe PhotoShop, PhotoPaint and CorelDRAW과 같은 그래픽 패키지와의 플러그인 기능을 제공한다. 또한 워터마킹 디지털 이미지를 만들 수 있을 뿐만 아니라, 추적도 가능하다. 가장 대표적인 PictureMarc를 비롯해 BatchMarc Pro, MarcCenter, Marc Spider Service, 워터마크 SDK 툴킷 등이 Digimarc사가 제공하고 있는 워터마크 관련 제품들이다^[9].

5.2.4 SysCoP(Digital Watermarking System)

프런트퍼 컴퓨터 그래픽스 연구소의 중국계 미국인 학자 지안 차오(Jian Zhao)가 주도하는 디지털 워터마크를 위한 시스템이다. Digimarc에 비해 학술적인 내용들을 많이 찾아볼 수 있다. 멀티미디어 정보의 저작권을 보호하고자 하는 취지는 여타의 디지털 워터마크 관련 사이트와 기본적으로 같다. 여기에 Syscop의 강점으로 들 수 있는 사항은, 인터넷을 통해 전송되는 워터마크된 자료가 전송되는 모든 과정을 추적할 수 있는 수단을 제공한다는 것이다. 아울러 단지 이미지뿐만 아니라, 메일 형태로 전송되는 뉴스정보, CD, CD-ROM, CD-I, 지리 정보시스템의 자료, VOD(Video on Demand) 자료, 정형화된 텍스트(마이크로소프트 워드 문서 같은 것) 등 여러 가지 형태의 멀티미디어 정보를 대상으로 하고 있다는 점이 독특하다^[10].

5.2.5 다이사사의 아젠트(Argent)

Argent는 분산된 디지털 파일에 대한 추적뿐만 아니라 컴퓨터 네트워크상의 저작권 보호를 위한 방법을 제공하고 있다. Argent 시스템은 워터마크 프로세스에 "Key"를 사용하여, 여타 다른 디지털 워터마킹 시스템과 차별화를 두고 있다.

아젠트 파이오니어(Argent Pioneer) 워터마크 프로그램은 오디오 파일에 워터마크를 할 수 있는 매킨토시용 소프트웨어이다^[15].

5.2.6 리퀴파이어 프로

Liquid Audio사에서 제공하는 음악 배포 시스템인 리퀴파이어 프로는 스트리밍이 가능한 것이 특징이며, 다운 로드가 끝나면 파일을 저장할 수도 있는 장점이 있다. 저작권 보호 기능인 디지털 음악 워터마킹을 내재시켜 레코딩의 최하단의 복제 고유 신호를 부여하는 구조로 불법 유통을 방지시킬 수 있다. 인코딩시 들을 수 없는 신호를 음악 내에 삽

입시켜서 재생시 그 신호를 확인할 수 있다. 플레이어는 Liquid Music Player를 사용하는데, 상용 음악 배포 시스템이므로 엔코더는 일반 사용자는 입수할 수 없다. 현재까지 MP3 다음으로 인터넷상에 가장 많이 보급된 것이 이 Liquid Audio 형식이다¹⁶⁾.

5.2.7 기 타

이외에도 Verance, Cognicity, Blue Spike, IBM, 일본의 Victor, 영국의 CRL 등의 회사들이 저작권 보호와 관련된 제품들을 내놓고 있다.

5.3 저작권 보호기술 적용시 고려사항

앞절에서 소개된 저작권 보호의 각 제품 및 서비스별 동향을 살펴보면, 콘텐츠 형태에 따라 적용할 수 있는 보호기술은 각각 다를 수 있다. 반복사용여부, 복제사용 여부, 사용자와 소유자의 일치여부 등의 구분이 있을 수 있다¹⁴⁾.

본 논문에서는 콘텐츠 파일형태의 각 요소에 따라 콘텐츠에 적용되는 기술이 다양해 질 것으로 예상되며, 현재의 적용 현황을 다음의 표 2로서 정리 요약한다.

콘텐츠 형태 내용	동영상 파일	음악 파일	이미지 파일	문서 파일
파일양식	mpg, dat, rm 등	wma, sm3, lqt 등	gif, bmp, jpeg 등	hwp, doc, pdf 등
가격	중	저	저	저
제작자와 사용자 일치여부	일치	일치	다를 수 있다.	다를 수 있다.
제사용여부	적다	빈번	빈번	빈번
주요 적용 가능 복제방지 기술	watermarking DTCP	watermarking DTCP	watermarking (fingerprinting)	watermarking (fingerprinting)
주요 적용 보호기술	Infoket InterTrust DRM CSS MarkAny	Digicap, secuMAX, Liquid Audio, InterTrust DRM, Argent MarkAny	syscop, DWS, Argent, MarkAny	fingerprinting, syscop, DWS,
기타	실행 제어이 름	단일 상품수로는 가장 많이 사용	사용자의 원본관점 필요성 있음	사용자 원본관점 필요성 있음

동영상 파일 또는 음악 파일인 경우 디지털 데이터의 수행결과를 재생할 수 있다. 즉, 동영상의 경우엔 카메라로 녹화 재생할 수가 있고, 음악인 경우 녹음기로 녹음 재생이 가능하다. 이러한 무단 복제의 방법으로는 워터마킹의 이용 삽입하는 방법이 있으나, 문서파일일 경우엔 이 기법을 적용하기가 어렵고, 사용자가 구매 후 원본의 편집이 필요한 경우가 있으므로 무단 복제를 막기가 힘들다. 이에 핑거프린팅의 보호기술이 대두되고 있다. 동영상의 자료, 음악파일은 컴퓨터 자원이 많이 할당되어 사용되어 지므로 수행 능력을 고려한 시스템 성능을 갖추어야 한다. 이를 회피하는 방법으로 하드웨어 형태로 서비스를 제공하는 기술 경향도 있다.

이러한 콘텐츠 형태에 맞는 저작권 보호기술을 정리하면, 각각의 요소에 적합한 기술로서 이뤄지고 있으나 앞으로의 디지털 콘텐츠의 종합적인 형태로의 지원을 갖춘 저작권 보호기술 시스템에 관한 연구가 필요하다.

지금까지의 콘텐츠 보호기술과 사례분석을 통해 콘텐츠 저작권 보호기술 및 제품/서비스를 바탕으로 인터넷 상에서 유통될 디지털 콘텐츠의 불법적인 이용, 재생산, 조작, 분배, 인쇄나 상영 등으로부터 소유자의 권한을 보호해 주고, 콘텐츠의 무결성을 보장하여 콘텐츠 소유자의 권한을 적극적으로 관리할 수 있는 저작권 보호 기술의 고려사항을 검토하면 다음과 같다

먼저, 디지털 정보의 특성을 반영하여 콘텐츠 저작권 보호기술에서 고려되어야 하는 사항들을 살펴 보도록 한다.

첫째, 다양한 종류의 정보보호가 이루어져야 한다.

디지털문서, 음악, 그림, 영화, 게임 등 각각의 경우 전달되는 정보의 특성에 알맞은 소유자 권한 보호가 이루어 져야 한다. 이때 각 콘텐츠의 보호는 일반적으로 유통되는 정보 보호 수준을 보장할 수 있어야 한다. 예를 들어, 디지털 문서의 경우 현재 사용되는 인쇄물의 저작권 보호 수준을 생각할 수 있을 것이다¹⁸⁾.

둘째, 다단계 정보의 제어 권한을 사용할 수 있어야 한다.

콘텐츠를 화면을 통해 보거나, 출력, 복사, 전송, 수정하는 등의 다양한 조적이 권한에 따라 가능 또는 불가능하게 해야 한다. 콘텐츠를 보거나 출력, 수정하는 등에 사용되는 툴이나 장치는 표준화되어 있거나 범용화 되어 있는 것을 사용하여야 한다.

셋째, 권한 관리를 위한 인터페이스가 제공되어야 한다.

권한 관리를 위한 모든 동작은 실시간에 처리되어야 하고, 사용자나 공급자 모두에게 편리한 인터페이스를 제공할 수 있어야 한다¹¹⁸⁾.

넷째, 콘텐츠 사용 지불 방법이 다양해야 한다.

콘텐츠에 접근하는 권한은 협상 절차에 의해서 정하게 되는데, 이 경우 정보를 최소한의 단위로 분리하여 사용자의 선택을 다양화할 수 있어야 한다. 또한 지불하는 수단도 신용카드, 스마트 카드, 전자화폐 등 다양하게 지원할 수 있어야 한다.

다섯째, 시스템의 신뢰성이 있어야 한다.

가치있는 콘텐츠를 사용하기 위해서 사용자는 자신의 신원을 확실하게 할 수 있는 증명서를 콘텐츠 제공자에게 제시하여야 하고, 콘텐츠는 신뢰성이 제공되는 시스템에 보관되어야 하며, 신뢰성이 제공되는 시스템간에만 전달되도록 해야 한다.

여섯째, 다양한 플랫폼이 지원되어야 한다.

콘텐츠 사용자가 사용하는 시스템의 종류에 관계없이 모든 시스템에서 동일한 서비스를 지원할 수 있어야 한다.

일곱째, 관리 시스템의 확장성이 있어야 한다.

콘텐츠 저작권 보호시스템은 현재 지원하는 서비스 이외에 차후에 발생할 서비스를 위하여 관리 기능의 추가가 가능하도록 구성하여야 한다.

이와 같이 콘텐츠 저작권 보호기술의 고려사항은 인터넷상에서 등록된 정보를 암호화함과 동시에 캡슐화에 의해 보호해서 자유롭게 배포하고, 사용자가 필요할 때에 복호키를 취득하는 것에 의해 정보를 구매하는 유통 보호서비스를 기본으로 한다.

암호화되고 캡슐화된 정보는 인터넷상에서 자유롭게 배포되는 것이므로 다음과 같은 기능을 가질 필요가 있다. 첫째, 정규 유통 센터에서 작성된 것임을 증명 가능해야 한다. 둘째, 캡슐이 제 3자에 의해 개조되지 않은 것이 증명 가능해야 한다. 셋째, 특정함수의 접근에서만 의미있는 정보를 추출하는 것이어야 한다. 즉, 정보의 은폐, 보호, 표준화된 인터페이스를 제공해야 한다는 것이다.

V. 결론과 전망

미래의 콘텐츠 제공은 과연 어떠한 방식으로 이뤄질 것인가. 현재 가정의 거실은 오디오 기기와 텔레비전이 중심이 되고 있다. 미래의 가정에서는 오디오

기기는 디지털로 대체된다. 인터넷이 콘텐츠 제공에 있어서 중심적인 위치를 차지할 것이라는 데는 이견이 없다.

앞으로의 1세기 후를 예측한다는 것은 서기 1000년에 살던 사람에게서 서기 2000년의 세계를 예측하라는 것과 같이 어려운 문제이다. 현재 우리는 10년 뒤를 예측하기도 어려운 실정이다. 그러나 콘텐츠의 중요성이 커진다는 것에 대해서는 자신있게 예측할 수 있다. 또한 지금까지 사용되어 오던 비즈니스 모델에 커다란 변화가 일어날 것이다.

디지털 콘텐츠 분야는 21세기의 시작부터 우리에게 새로운 변화를 보여주고 있다. 이미 PC통신이나 인터넷상에서는 다양한 콘텐츠 유통이 이루어지고 있다. 현재 콘텐츠 유통의 최대 특징은 인터넷 홈페이지와 같이 누구나 자유롭게 정보에 액세스할 수 있는 「공개형」 콘텐츠가 증가하고 있다.

이러한 추세는 디지털 콘텐츠가 보호 차원에서 중요해진다는 것을 의미한다. 따라서 안전한 콘텐츠 유통을 실현하기 위한 신기술의 콘텐츠 보호기술의 진전이 이루어지고 있다. 이러한 기술이 활용되기 위해서는 사회적, 제도적인 환경정비도 같이 이루어져야 하는데 앞으로 정보의 중요성이 커지므로 자연스럽게 디지털 콘텐츠의 중요성과 기술 연구가 이루어질 것으로 본다.

본 논문에서는 디지털 콘텐츠 보호기술의 개요, 유통/이용형태에 따른 콘텐츠 보호기술의 동향을 분석하였고, 콘텐츠 보호기술의 요소 기술과 그 응용 분야에 대해 살펴보았다. 그리고, 이의 내용을 반영해 콘텐츠 저작권 보호기술의 고려사항을 기술했다.

향후 본 고에서의 저작권 보호기술의 고려사항들을 근거로 콘텐츠 저작권 보호 시스템 관점에서 보완 및 콘텐츠 저작권 보호 메커니즘 구현이 필요하다. 본 논문을 통해, 디지털 콘텐츠의 중요성이 부각되고 있는 디지털화 시대에 정보가 정당한 사용자에게 안전하게 전달되어야 한다는 건전한 유통의 중요성이 인식되고, 디지털 콘텐츠를 안전하고 유용하게 적용할 수 있는 방향제시가 되기를 바란다.

참고 문헌

- [1] 申 吉浩·青沼英一, 디지털 콘텐츠의 권리보호와 유통, *IPSJ Magazine* Vol.40 No.5 May.1999
- [2] 山中 喜義(Kiyoshi YAMANAKA)·紫垣 齊

(Hitoshi SHIBAGAKI) · 櫻井 紀彦(Norihiko SAKURAI) · 曾根岡 昭直(Terunao SONEOKA), 디지털 저작권 보호 기술의 동향 (Trend of Digital Copyright Protection Technologies), NTT R&D Vol.47 No.6 1998

[3] 明石 修 · 森保 健治 · 寺内 敦, 인터넷을 이용한 정보유통 플랫폼 : Infoket-I(Infoket-I: an Information Distribution Platform on the Internet), NTT R&D Vol.46 No.2 1997

[4] 松井 甲子雄, 전자워터마킹 기술의 최신동향, IPSJ Magazine Vol.40 No.2 Feb.1999

[5] "The Role of the Content Sector in the Emerging Information Society", Working Paper, IMO (Information Market Observatory), 1995.9.

[6] 정보통신부, 국가정보화백서, p.510, 1998.

[7] <http://multimedia.kangwon.ac.kr/ismc/>

[8] <http://www.dvcc.com/dhsg/>

[9] DigiMarc, <http://www.digimarc.com/>

[10] Syscop, <http://www.crcg.edu/syscop/>

[11] InterTrust Technologies Corporation, <http://www.intertrust.com/>

[12] secuMAX, <http://www.secumax.com>

[13] Capsule Audio, <http://digicap.brnetcomm.co.kr/>

[14] 강호갑, "DRM을 이용한 콘텐츠 불법사용방지 시스템 구축방안", *E-Commerce*, PP.19-27, 2000. 2.

[15] 배민오, 조규근, "디지털 콘텐츠 저작권 보호 기술 동향", 정보과학회지, 2000. 7.

[16] <http://www.liguidaudio.co.kr>

[17] MarkAny, <http://www.trustech.co.kr>

[18] Gary N.Griswold, "Method for Protecting Copyright on Networks"

[19] 산업자원부, "e-Book 기술개발 저작권 보호

기술개발 종합계획(안)", 2001. 8.

[20] 김영준, 이성민, 이진호, 김태운, "멀티미디어 데이터를 위한 저작권 보호기법에 대한 고찰", *한국정보처리학회 추계 학술발표논문집* 제7권 제2호, 2000.

[21] 최중욱, "디지털 콘텐츠 보호를 위한 암호화 기술", *E-Commerce*, PP.28-33, 2001. 3.

[22] 김옥중, 김문철, 김진용 "콘텐츠 식별 기술개발동향", *주간기술동향* 980호, 2001. 1. 16.

〈著者紹介〉



박 남 제 (Nam-Je Park)

학생회원

2000년 8월 : 동국대학교 정보산업학과 졸업

2001년 3월~현재 : 성균관대학교 정보통신대학원 정보보호학과 석사

과정

2000년 5월~현재 : (주)뉴레카 정보통신연구소 선임연구원

관심분야 : 전자상거래 보안, 무선인터넷 보안, 전자지불시스템



송 유 진 (You-Jin Song)

정회원

1982년 2월 : 한국항공대학교 전자공학과 졸업

1986년 2월 : 경북대학교 정보시스템 전공 (석사)

1995년 2월 : 일본 동경공업대학 정보보호 전공 (박사)

1988년 2월~1996년 2월 : 한국전자통신연구원 선임연구원

1996년 3월~현재 : 동국대학교 정보산업학과 교수
관심분야 : 암호이론, 전자상거래 보안, 무선인터넷 보안, 스마트카드 보안, 전자화폐