디지털 컨텐트 저작권 보호 기술 동향

동덕여자대학교 배민오*
Fasoo.com 조규곤

1. 서 론

아날로그에서 디지털시대로의 이동이 빠르게 진행되고 있지만 저자나 출판사같은 컨텐트 소유자는 디지털 정보를 배포하는 것에 조심스럽지 않을 수 없다. 파일 하나를 순식간에 복사하여 배포하는 인터넷이 있기 때문이다. 그럼에도 불구하고 디지털 컨텐트가 인터넷을 통해 전자적으로 거래되어야 하는 것은 시대적 흐름이라 할 수 있다. 따라서 디지털 컨텐트 저작권 보호 기술에 관심이 모아지고 있다. 또한 많은 컨텐트 소유자들이 컨텐트 유료화에 관심을 보임에 따라서 저작권을 보호할 뿐만 아니라 인터넷을 통하여 안정된 수익 모델을 촉진할 수 있는 법적이며 기술적 장치에 대한 관심이 높아지고 있다.

디지털 컨텐트 저작권 보호 기술은 1)저작권의 원 소유자가 누구였는지를 추적할 수 있게 하는 디지털 워터마킹[1], DOI[2] 및 INDECS[3]와 같은 저작권 추적 기술과, 2)사용 권한(use rights)을 획득하지 못한 사람에게는 컨텐트를 사용하지 못하게 하는 저작권 관리 기술들로 대별될 수 있다. 저작권 추적 기술의 디지털 워터마킹 적용은 간단한 반면 저작권을 적극적으로 보호하지는 못하는 단점이 있다.

암호화 기술을 응용한 저작권 관리 기술들은 저작권자가 대가를 지불한 사용자에게만 사용권한을 줄 수 있어 좀 더 적극적인 저작권 보호 기술이다. 하지만 이런 암호화 기술들은 암호화 키(key)의 관리를 어떻게 하느냐에 따라 보안성이 떨어지기도 하여, 암호화 키를 안전하게 저장하기 위한 기술을 덧붙인 기술들이 개발되어 왔다. 다른 한편으로는 이런 기술들이 전자상거래에서 활용되기 위해서는 사용권한을 좀 더 다양한 방법으로 제어할 필요가 있으며, 이를 위한 기술들도 개발되고 있다. 초기에는 특정 사용자에게 컨텐트를 사용할 수 있는 모든 권한을 부여하는 단순한 방식에서 최근에는 컨텐트를 볼(view) 수는 있으나 인쇄(print)는 못하게 한다든지, 사용할 수 있는 기간이나 횟수를 제어 할 수 있도록 하는 등 실 상거래에서 발생할 수 있는 다양한 방식의 사용권한 제어를 시도하려는 DRM(Digital Rights Management) 기술이 개발 상용화 되고 있다.

2. 저작권 추적 기술

특정마크나 고유번호를 삽입, 컨텐트를 식별해 법적 분쟁시 소유권을 입증할 수 있는 기법이다. 디지털 컨텐트는 복사본이 원본과 동일하기 때문에 대량으로 복사되어도 소유자를 가려낼 수 없는 단점을 보완하기 위해 사용되는 기술은 워터마킹과 DOI, INDECS가 있다.

2.1 워터마킹

디지털 컨텐트가 컴퓨터를 이용해서 인쇄, 연주되는 경우, 컨텐트 보호 기술만으로는 디지털 컨텐트를 완전하게 보호하는 것은 불가능하다. 인쇄·연주에 의해 생성된 디지털 데이터 유출을 완전히 방지하는 것은 현재의 컴퓨터 구조를 전제로 하는 한 불가능하다. 따라서 유출된 컨텐트가 대량으로 유통되는 것을 억제하는 것을 목적

* 정회원

으로 하여 컨텐트에 저작권 정보 등의 추적정보를 삽입하는 기술로서는 디지털 워터마킹 기법이 알려져 있다. 디지털 워터마킹은 인지할 수 없거나, 또는 간신히 인지할 수 있게 한 디지털 데이터의 변형이다. 대부분의 경우 이 디지털 데이터는 디지털 멀티미디어 데이터인 경우가 많다. 이러한 워터마크가 디지털 이미지에만 응용되는 것처럼 언급되지만 비디오, 음악과 같은 다른 형태의 디지털 데이터에도 사용할 수 있다.

보이지 않는 워터마크란 인지되지는 않지만 나중에 전산적 처리에 의해 추출할 수 있는 워터마크이다. 이렇게 전산적 처리중 인증된 경우에만 워터마크 추출을 허용하기 위해 암호를 요구할 수도 있다. 이런 암호를 워터마크 키(key)라고 하지만 이것은 암호화 키(encryption key)와는 상당히 다르고 목적도 다르다. 만약 보이지 않는 워터마크가 자체내에 데이터를 가지고 있다면 데이터 감추기(data hiding)를 하는 것이 된다.

2.1.1 워터마킹의 다양한 응용들

워터마킹의 중요한 목적중의 하나는 소유자 정보를 전달하기 위함이다. 그리고 이런 소유자의 개념도 원 소유자와 수신자(최종사용자, 도서판과 같은) 두 가지가 있다. 또한 보이게 하는 방법 및 보이지 않게 하는 방법도 있다.

수신자를 워터마킹하는 방법이 가장 중요한 워터마킹 응용이다. 수신자를 워터마킹한다면 개인의 사생활 침해한다고 생각하기 쉽겠지만, 그렇지 않다. 예를 들면 어떤 수신자가 불법적으로 워터마킹된 저작물을 웹에 올려놓는다면 자신의 아이디를 노출시키는 위험은 감수해야 한다.

소유자를 워터마킹하는 이유는 좀 더 자세한 설명이 필요하다. 먼저 보이는 워터마크는 광고나 제한으로써 역할을 할 수 있다. 즉 소유자가 정기적으로 웹을 검사하여 남용을 찾아 내기 위함이라고 할 수 있다. 만약 조금이라도 변화가 있다면 워터마크를 찾아 낼 수 있어야 하겠다. 컨텐트의 원본입증을 위해 소유자 워터마킹을 이용할 수는 있겠다 대부분의 보이지 않는 워터마크는 강건해야 한다. 즉 워터마킹된 컨텐트를 변화시켜도 워터마크는 그대로 살아 있어야 하겠다. 하지만 원본입증을 위한 워터마크는 보이지 않지만 잘 깨어지는 성질이 필요하다. 즉 컨텐트를 조금만 수정하려고 시도하여도 워터마크가 쉽게 깨어져야 한다. 이러한 응용을 위한 중요한 준비는 워터마크 탐지기가 어떻게 동작하게 하는지 준비하는 것이다. 만약 모든 사용자가 탐지기가 있어야 한다면 이 워터마크에 역공학을 적용하여 비밀스런 깨어지기 쉬운 워터마크를 만들 수 있게 된다. 이런 비밀을 보장하기 위해 탐지기는 보통은 안전 서버에 두는 것이 안전하다.

캡셔닝(captioning)이란 컨텐트의 이름, 저자, 날짜 및 연락처 등을 보이지 않는 워터마크에 함께 두는 기법이다. 여기에 있는 정보는 관계된 모든 이에게 유용하다. 예를 들면, 라디오에서 방송되는 노래가 될 수 있다. 노래 소유자나 라디오 방송국 소유주는 방송되는 노래의 정확한 회수에 관심이 있을 것이다. 들을 수 없는 옴으로 워터마킹되었다면, 각 대도시 지역에서 "라디오 청취 프로그램" 자동적으로 방송국을 모니터하여 위의 일이 가능하게 할 수 있다.

위성방송이나 DVD 매체의 디지털 영화를 제작하는 영화사는 워터마크에 많은 관심을 표명하고 있다. 영화사는 보이지는 않지만 강건한 "never copy", "copy once", "no more copy" 워터마크를 영화에 삽입하려고 한다. 이렇게 하려면 모든 기록장치가 워터마크를 검출할 수 있어야 하고, 워터마크가 허용하지 않는 복사는 되지 않도록 지원되어야 한다.

2.2 DOI(Digital Object Identifier)

디지털 환경에서 저작권관리를 가능하게 하는 툴을 개발하려는 AAP(Association of American Publishers)의 노력으로부터 발전하여 DOI가 되었다. 무엇을 보호하기 위해서는 먼저 보호하려는 객체가 무엇인지를 혼동함이 없이 분명히 나타낼 수 있어야 한다. 따라서 DOI는 지속적인 이름을 가진 개체 그 자체를 관리하는 도구를 충분히 구현하는 첫 단계로써 DOI가 시작되었으며 지속적(persistent)이고 유일한 작명의 실용적 시도라 할 수 있겠다. 아주 간략히 언급한다면 DOI는 다음을 제공하는 것으로 설명할 수 있다.

- 지적자산의 지속적인 식별자(persistent identifier)
- 이 식별자를 유용한 정보나 서비스로 변환하기 위한 방안

두 번째 것에 의해 식별자를 어떠한 특정 정보와 연관지을 수 있다. 출판사의 웹 사이트와 연결하는 것이 쉬운 방법 중의 하나이다. 하지만 식별자의 연관을 이렇게 사용하는 것만으로 제한하는 것은 가능하지도 생산적이지 못하기 때문에 이것이 DOI의 의도는 아니다. DOI는 많은 응용과 국지적 사용을 위해 공개적 식별자로 사용되는 것이 원 의도이다. 또한 다른 정보 식별자와 같이 DOI는 특정 응용에 대해 독립적이어야 한다. 많은 사용자에 의해서 자유롭게 사용되는 경우가 많이 있어야 한다.

2.2.1 지속적 식별

가. 균일 자원 이름(URN:Uniform Resource Name)

DOI는 자원이나 개체의 지속적 식별자를 제공한다. 웹에서 사용되는 URL은 인스턴스가 있는 위치를 표시하는데 반해서, DOI에서는 개체를 직접 표시하는 것이 가능하다. 따라서 DOI에서는 위치와 독립적으로 디지털 객체를 관리하는 기반 구조가 가능하다. 인터넷이 발전하던 도중에도 지속적 이름에 대한 요구는 인지되기 시작한 것은 오래되었다. 위와 같은 요구를 다음과 같은 DOI 원칙으로 정리할 수 있다.

- 전역범위: 이름은 위치적인 의미가 아닌 전역적 범위를 갖는다. 따라서 어느 곳에서나 동일한 의미를 갖는다.
- 유일성: 동일한 URN이 두 개의 상이한 자원에 할당이 되지 않는다.
- 지속성: 어느 URN이 할당되었다면 이 URN의 생명은 무한하다. 즉 이 URN은 전역 적으로 영원히 유일하며 이것이 식별하는 자원 또는 이름과 유관한 어느 기관의 생명보다 더 오래 동안 자원의 참조로써 사용 가능하다.
- Scalability: 네트워크 상에 개념적으로라도 존재할 수 있는 어떠한(크던 작던 간에) 자원에도 할당 가능하다
- 기존 시스템 지원: 기존의 작명 시스템이 다른 요건을 충족한다면 이 기존 시스템도 지원해야 한다.
- 확장성: URN 스킴은 미래의 확장에 대비해야 한다.
- 독립성: 이름 부여 조건은 전적으로 작명기관의 책임이다.

URN의 일반적 형태는 urn: nid: nss이다. 여기서, nid는 정의된 이름공간 식별자(예 doi)이고, nss는 nid 내의 이름공간에 따라 달라지는 글자열이다. 개념적으로 URN에 urn:si:nid:nss 처럼 특정한 스킴 식별자(si)가 포함될 수 있다. 위의 두 가지 경우 모두 왼쪽에서 오른쪽으로 읽음에 따라서 계층적 이름 공간을 따라 내려오는 것에 해당된다. urn:doi:10.1000/123456789에서 nid는 doi이며, nss는 10.1000/123456789이다. 문맥상 혼동할 이유가 없다면 nss만 표현하고 이것을 DOI로 사용한다. 위의 예에서 DOI는 '/'에 의해 두 부분으로 나누어져 있다. '/'의 앞부분 즉 10.1000은 prefix라 하고 DOI를 생성관리하는 기관에 의해 유지된다. 이들 기관은 다시 DOI 등록 기관(현재는 IDF)에 의해 지정된다. 정보의 유일성 개념은 웹 또는 인터넷 기반에만 있는 것은 아니다. 이런 식별자는 여러 가지 경우에 이용할 수 있다. 예를 들면, URN framework은 전화번호나 책의 ISBN 등에도 적용 가능하다. IETF와 W3C는 표시된 이름 공간 내에서 유일한 식별자를 표준화하는 전반적인 스킴으로 URI(Uniform Resource Identifier)라는 용어를 사용한다. URI는 URL과 URN을 포함한다. URI는 추상적 객체를 가지고 있는 자원들을 식별할 수 있다고 여겨진다. DOI는 URN과 URI의 요구조건과도 일치한다.

나. DOI 해결(Resolution)

DOI는 URN 요구사항을 따르므로, 지속적 식별자 구현을 방해하는 문제를 해결할 수 있는 능력이 있다. DOI는 지속적 이름을 제공하고, 핸들 시스템 기술을 이용하는 해결시스템이다. 이 핸들 시스템도 URN 순응한다고 여겨진다. 이 핸들 시스템은 DOI에 없는 여러 가능성 및 특성을 포함한다. 핸들은 다중 해결할 수 있는 능력을 보유하고 있다. 하지만 DOI 개념이 처음 생겼을 때는 DOI 핸들 구현을 한 개의 DOI가 한 개의 URL으로 해결되는 단일 해결로 제한하는 것이 좋겠다고 여겨졌다. 이렇게 한 이유는 잠재적 사

용자에게는 위에서 언급한 여러 문제들이 알려져 있지 않았고 위에서 언급한 것처럼 단일 해결로 하는 것이 논리적 시작점이라고 생각했기 때문이다. 핸들의 능력을 충분히 확장하는 것은 곧 바람직한 개발방향이라고 여겨지게 되어 DOI의 장기적 목표가 되었다. 우리는 IDF가 장래에는 다중해결을 이용하는 어떤 특정한 응용개발을 지원할 것으로 보고 있다. 핸들을 지원하기 위한 브라우저 플러그인이 있기는 하지만 사용자에 의해 설치되어야 한다. 이런 조건이 웹에서 사용될 때는 사용요건이 될 수 없기 때문에 DOI에서 URN으로 해결은 기존 프로토콜을 이용할 수밖에 없다. 핸들개발자와 IDF는 브라우저 제조업자가 핸들 프로토콜을 지원하도록 협력하고 장려한다. 한편 프락시 서버는 http로 대부분의 세계와 통신할 수 있고 또한 핸들 프로토콜을 사용하여 핸들 시스템과도 통신가능하다. 따라서 외부 세계에서 보면 현 DOI 문법(예, 10.1000/123456789)은 곧바로 http://dx.doi.org/10.1000/123456789와 같은 http로 번역되는 것처럼 보인다.

브라우저가 바로 지원되거나 또는 플러그인을 통해 간접적인 방법으로 지원된다면, 해결기는 적절한 해결 시스템으로 유도되어야 한다. 해결 시스템과 그 안에 있는 특정 이름 공간의 등록은 DOI주관 기관이 자세히 모니터하는 또 다른 인터넷 영역이다. 상업적으로 중요한 URN이나 이름 공간은 도메인 작명 기관과 유사한 통치 구조를 요구할 수도 있다.

현재는 DOI가 단일 해결시스템으로 취급되고 또한 http 프락시를 사용하므로 현재의 DOI의 많은 기능은 PURL(Persistent URL)과 같은 재유도 도구에 의해 수행 가능하다. 현재는 이렇게 하지만 이렇게 하는 것이 장기적인 목적은 아니다. 즉,

- 핸들은 직접 프로토콜인데 비해 PURL은 또 다른 차원의 간접적인 방법을 사용하는 재 유도 서버이다.
- 핸들은 다중 해결 능력을 가지고 있으므로 지능형 클라이언트를 만들 수 있다. 즉, DOI입력에 의해서 한 개 이상의 해결 결과를 많은 리스트로부터 돌려 줄 수 있는 클라이언트 기구를 정의할 수 있다. DOI를 이용하여 이런 기구의 원형이 구축되었고, 다른 핸들 구현에 리파지터리 기능을 이용한 유사한 기능성이 있다.
- 핸들은 scalable하다.
- DOI는 URN조건을 충족시키기 때문에 URN이고 정보식별자, 지속적 이름으로 웹 이외의 다른 문맥에서도 유용하게 사용될 수 있다.
- PURL은 지역적 구현이기 때문에 지역적 기술 지원이 필요한 반면 핸들은 전역 적으로 관리된다.

2.3 INDECS(Interoperability of Data in E-Commerce System)

INDECS는 전통적인 메타데이터인 더블린 코어와 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 검증을 거쳤으며 ISO와 연계 활동을 추진하고 있다. 선진국에 비해 디지털 컨텐트가 양적, 질적으로 부족한 우리 나라는 DOI와 INDECS 같은 보호기술로 새로운 기회를 제공받을 수 있다.

과거에는 지적자산을 위한 국제적 메타 데이터 주관기관은 컨텐트를 찾거나 주문과 송장과 같은 극히 특정한 메시지를 교환하는데 도움을 주기 위함이었다. 메타 데이터의 용도가 상대적으로 단순하거나 폐쇄된 네트워크내의 인간에 의해 조정될 수 있었기 때문에 상이한 시스템에 저장된 메타 데이터들은 아주 많이 깊이 협력할 필요가 없었다. 하지만 컨텐트를 네트워크를 통해 분배함에 따라 전통적으로 다르고 분리된 분야에 있던 것들의 비즈니스 모델이 수렴하게 되었다. 각 전통적인 분야에서 국제적 메타 데이터 스킴이 등장하고 있다. 이들 끼리는 유사한 요구 사항을 가지고 있다. 멀티미디어 컨텐트, 다 언어, 다양한 기술적 플랫폼, 상세함에 있어 다양함, 그리고 무엇보다도 발견, 자산과 권리관리, 워크플로우, 아카이빙 등과 같은 다중기능을 포함한다.

지적자산 거래의 복잡성과 양을 생각해 보면 컴퓨터가 아니면 이러한 일들이 제어되는 것은 불가능하다는 것을 알 수 있다. 지적자산의 전자

상거래가 활성화되고 여러 메타 데이터 표준들간의 장벽이 제거되기 원한다면 지적자산이 식별되고 기술되는 표준이 필수적임을 알 수 있다. INDECS의 목적은 바로 이것이라고 할 수 있다.

INDECS는 지금 등장하는 여러 스킴에 대한 대안을 제공하는 것은 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 거쳐서 개발함으로서 시도한다. 지적자산은 물론이고 그 무엇이라도 기술하는 방법이 하나뿐인 경우는 없다. INDECS 스키마는 최대한으로 광범위한 응용들을 지원할 수 있게 설계된다. 그렇게 한 다음 현실의 데이터원소를 이 모델에 넣어 이들 데이터끼리 연관되는 방법을 조심스럽게 고안함으로서 저 수준에서 접근할 수 있다. 마지막으로 INDECS 스키마는 권리와 내용이 모든 네트워크와 시스템에 걸쳐 인지되게 하기 위해 서로 상이한 스키마들을 함께 매핑하는 수단을 제공한다.

유일 식별자는 오래 전부터 컴퓨터 시스템간에 상호연동을 위한 핵심적인 키로 인식되었다. 최근에는 식별자에 강건한 메타 데이터를 추가할 필요성이 점점 더 분명해진다. DOI와 ISWC와 같은 지적자산을 위한 새로이 구현된 식별자들은 관련된 메타 데이터 구조를 정의한다. 따라서 유일적 식별은 INDECS 스키마에서의 핵심이라 할 수 있다. 유일적 식별 원칙은 여러 다른 차원에서 동작한다. 먼저, 그 어떤 것이 식별되어야 한다. 즉, 지적자산과 연관된 사람과 합의들이 유일적으로 구분되어야 한다. INDECS는 ISBN이나 ISRC와 같은 기존의 식별 시스템을 이용한다. 다음, 모든 것들이 자기 자신의 도메인(또는 이름공간)에서 유일하게 식별되어야 한다. 0-297-84261-7이라는 숫자가 ISBN이지 전화번호가 아니라는 사실을 안다면 이 번호가 참조하는 책의 식별은 확실한 것이다. 세 번째, 메타 데이터 구조 자체도 유일 식별자를 사용한다는 점이 INDECS에서는 아주 중요한 점이다. INDECS에서 사용되는 모든 용어들은 구조화된 데이터 사전에서 조심스럽게 정의되어 있다. 정의 자체도 유일 식별 형태로 하고 있고 또 이 정의에 의해 한 용어가 다른 것과 구분될 수 있다. INDECS 메타 데이터 사전내의 용어들은 iid 수자(INDECS identification number)에 의해 유일하게 식별된다.

INDECS에서는 언어가 아닌 유일 식별성에 의해 상호 운용성을 지원하는데 있어 위와 같은 식별 시스템은 중심적 역할을 한다. 다른 메타 데이터 스킴은 그 무엇에 대한 그들만의 이름과 메시지 구조를 사용한다. iid 구조가 이들 이름과 메시지 구조를 INDECS iid를 공통분모로 이용하여 서로 매핑되게 한다

INDECS 모델의 범위에 의해 모든 수렴 평면들간의 다대다 매핑을 할 수 있다. iid만 본다면 간단하고 단순한 수일뿐이지만, INDECS 모델 내에서의 위치에 의해 상이한 문맥과 여러 가지의 상세한 정도로 사용되는 메타 데이터 간의 훨씬 더 복잡한 번역을 개발하는 것이 가능해 진다. 이것이 바로 미래의 스키마의 중요개발이다

INDECS의 목표는 상이한 스킴이 상호운용 가능하게 하는 것뿐만 아니고, 한 분야에서 개발된 메타데이터가 서로의 이익을 위해 타 분야에서도 사용 가능하게 하는 것도 있다. 예를 들면, 인쇄소가 음향 및 영상 업계로 확장하거나, 녹음된 음악이 멀티미디어화 한다면, 새로운 메타 데이터와 표준을 개발하기보다는 이미 개발된 것을 이용하는 것이 효과적일 것이다.

3. 디지털 저작권 관리 기술 (DRM)

3.1 DRM의 기본 기능

디지털 컨텐트의 저작권 침해를 근본적으로 차단하기 위한 저작권 관리(DRM) 기술들은 여러 단계의 발전 과정을 거쳐오면서 다음과 같은 기술적인 문제들을 해결해 왔다.

- 암호화 및 키 관리
- 디지털 컨텐트의 지속적 보호
- 사용 규칙 정의 및 제어
- 사용 내역 측정

암호화 및 키 관리: DRM 기술은 기본적으로 암호화 기술들을 응용하고 있다. 암호화 된 디지털 컨텐트를 배포하여, 복호화 키가 없는 사람은

암호화 된 디지털 컨텐트를 사용할 수 없도록 한다. 이 복호화 키를 어떤 방법으로 관리하느냐에 따라 여러 가지의 기술들이 개발되고 있으며 이에 따라 해당 기술의 보안성이 크게 좌우된다.

디지털 컨텐트의 지속적 보호: 물론 이것만으로 저작권이 충분히 보호되지 않는다. 저작권은 디지털 컨텐트의 전 유통 과정에서 지속적으로 보호되어야 한다. 사용권한을 가지고 있는 사람이 암호화되어 있는 디지털 컨텐트로부터 암호화되지 않은 디지털 컨텐트를 쉽게 만들 수 있다면 여전히 저작권 보호는 사용자의 양심에 의존할 방법 밖에는 없을 것이다. 따라서 항상 사용할 때 이외에는 디지털 컨텐트가 암호화된 상태로 존재하도록 하여야 하며, 사용 중에도 복호화된 디지털 컨텐트를 추출하기 어렵게 하는 기술이 필요하다.

• 사용 규칙 정의 및 제어: 저작권 보호 기술이 보안성만 중요한 것은 물론 아니다. 저작권이 어떤 방식으로 관리되기를 정의하는, 즉 디지털 컨텐트의 사용규칙을 정의하는 방법이 필요하고, 그 정의대로 보호되도록 제어하는 일련의 기술들이 필요하게 된다.

• 사용 내역 측정: 저작권을 보호하는 좀 더 근원적인 목적은 저작권자에게 경제적인 이득을 보장해 주는 일일 것이다. 그러기 위해서는 디지털 컨텐트를 얼마나 사용했는지를 계측할 수 있는 기능을 필요로 한다. 그 정보를 근거로 과금(billing)할 수 있게 되며 금융 결제 처리를 자동화 할 수 있도록 발전되어 왔다.

3.2 DRM 기술 비교

본 보고서에서는 무수히 많은 저작권 관리 기술 중에서 최소한 위에서 언급한 기능들을 대체로 구현하고 있다고 판단되는 다음의 세 회사에서 만든 기술들을 주로 분석하였다. 비교된 기술들도 계속 변형 발전되고 있는 중이고 공개되는 기술 내용에는 많은 제약이 있어 비교 분석에 한계가 있다.

- InterTrust Technology[4]
- RightsMarket.com[5]
- ContentGuard[6]

위의 세 회사의 DRM 기술들은 대체로 다음과 같은 컨텐트의 생성에서부터 사용에 이르는 절차를 따르고 있다.

1 컨텐트 사용 규칙 정의
2. 컨텐트 암호화
3. 암호화된 컨텐트의 전달
4. 사용규칙 해석
5 암호화된 컨텐트의 복호화
6. 사용규칙에 따른 컨텐트 활용 제어
7 사용 내역 기록
8. 사용 내역 수집

위의 절차적 단계별로 기술적인 사항들을 비교 검토하여 보기로 하자. 컨텐트 사용 규칙의 정의는 사용 규칙을 얼마나 다양하게 제어할 수 있는가 하는 것이 중요한 문제이기도 하다. 현재 나와 있는 기술들은 대부분 사용회수 사용기간 사용개시일 사용만료일, 사용자의 상태, 예를 들어 특정 회원권의 소유 여부, 사용자의 나이 등에 따라 컨텐트를 보거나(view), 인쇄(print), 저장(save), 잘라 붙이기(cut-and-paste) 등을 허용하는 컨텐트의 사용 규칙을 정할 수 있다. 이 부분에서 특징적인 동향은 InterTrust와 Content Guard에서는 사용규칙을 정의하기 위한 언어로 XML을 사용하고 있으며 ContentGuard에서는 자신들의 XML 판 사용규칙언어인 XrML (Extensible Rights Markup Language)[7]기술을 공개하여 표준화를 추진하고 있다. 사용 규칙의 정의가 표준화 된다면 사용 규칙을 작성하는 도구 및 컨텐트 응용 시스템의 상호 호환성을 보장 받을 수 있을 것으로 기대가 된다.

컨텐트의 암호화 방식은 전체 시스템의 특성에 많은 영향을 주게 된다. 가장 손쉽게 생각할 수 있는 방식이 비대칭 암호화 기술을 응용하여 인가된 사용자의 공개키로 암호화하는 방식이다. 그러면 인가된 사용자 외에는 복호화 할 수 없으므로 저작권 보호는 잘 된다고 볼 수 있다. 그러나 이 방법은 컨텐트를 받을 사람을 미리 알아야 한다는 제약이 있다. 따라서 디지털 컨텐트의 전자상거래를 구현하고자 할 때 미리 암호화를 해 놓을 수 없어 불특정 다수에게 배포를 할 수 없다. 대칭키를 이용하여 암호화 하게 되면 미리

암호화를 해 놓을 수 있으나 암호화 키의 전달, 저장, 변경 등 키 관리가 복잡해지는 단점이 있다. InterTrust나 RightsMarket.com에서는 이 방식을 원용하여 쓴다. 기술적으로 어려워지기는 하나 이 방식을 채택할 경우 같은 디지털 컨텐트는 암호화 된 방식이 같으므로 사용자가 다른 사용자에게 암호화된 컨텐트를 전달할 수 있어서 이른바 superdistribution[8]이 실현될 수 있는 큰 장점이 있다.

또 다른 기술적인 이슈 중에 하나는 키(사용권한)를 어디에 저장하느냐 하는 문제가 있다. 서버에 두는 것이 키 관리의 문제를 간단하게 만들기는 하나 사용자는 항상 서버와 온라인 상태를 유지해야만 한다는 단점이 있다. 사용자 기계에 두려면 키가 쉽게 복사되어도 안되며 쉽게 훼손되어서도 안 된다. 사용자 기계에 두었을 때 또 다른 문제점 중에 하나는 사용자가 원래 사용권한을 받았던 곳이 아닌 다른 기계에서는 컨텐트를 사용 할 수 없다는 점이다. 이 문제를 해결하기 위해서는 smart card 같은 곳에 사용권한을 저장하는 방법이 한 가지 해결책이기는 하나 smart card reader의 보급에 따른 비용, smart card의 표준 문제 등으로 인하여 아직은 현실적인 대안이 되지 못하고 있다.

디지털 컨텐트의 상거래를 지원하기 위하여서는 사용 내역을 기록하는 기능은 필수적이다. 사용 내역을 어디에선가 기록을 하고 있어야 컨텐트의 사용에 따른 과금과 결제가 일어 날 수 있다. 사용 기록을 사용자의 기계에 남길 수도 있고 네트워크로 연결된 서버에 남길 수도 있다. 사용자의 기계에 남길 경우 기록이 변경되거나 삭제될 수 있으므로 tamper resistance를 적절한 수준으로 보장되어야 하며 또한 저장된 기록의 수집이 자동화되어야 한다. 반면 서버에 남길 경우 그 때 마다 네트워크에 연결되어 있어야 한다는 부담이 있다. InterTrust와RightsMarket.com의 경우는 사용자 기계에 남기고 있다. 상거래 지원을 하기 위하여 결제 기능을 추가하여야 한다. ContentGuard와 RightsMarket.com의 기술은 직접적으로 결제 처리를 위한 기능은 없으나 서버에서 사용내역에 따라 과금을 하고 일괄 결제를 하도록 구현할 수 있다. ContentGuard와 Reciprocal[9]에서는 출판물의 상거래를 위한 결제 기능을 할 수 있는 ePCS[10]라는 서비스를 제공하고 있다. 반면 InterTrust의 경우는 거래체결은 사용자의 기계에서 컨텐트를 사용하는 순간에 일어나도록 되어 있어 필요에 따라 신용카드를 이용한 즉시 결제나 전자화폐 등을 이용한 다양한 결제 방식을 구현하기 쉽도록 되어 있다.

그 외에도 위에서 언급한 여러 기능 중 일부만을 구현하고 있는 여러 기술들이 있으며 그 중 다음 것들은 검토가 필요하다.

- Preview Systems[11]
- SoftLock.com[12]
- Liquid Audio[13]
- Wave Systems[14]
- IBM (Madison Project)

3.3 DRM 표준화

위에서 보듯이 여러 다양한 기술들이 주로 기업들이 주도하에 개발되고 있다. 각각의 기술들은 서로 상호 호환성이 없으며 확장성에도 많은 제약이 있다. 많은 초기 기술들은 특정 디지털 컨텐트 예를 들어서 음악이나 software만을 위한 것들이 많았으나 점차 일반화 되어 어떤 디지털 컨텐트에든 적용할 수 있도록 발전되고 있다. 모든 디지털 컨텐트에 공통으로 적용할 수 있는 기술들이 사용 기반을 넓히는데 매우 유리할 것이다. ContentGuard의 XrML을 공개 표준으로 하려는 움직임도 관련된 많은 소프트웨어 중 일부라도 서로 상호운용 되도록 만들어 보자는 노력을 일환이다.

또 다른 움직임 중에 관심을 가져야 할 것은 미국 음반협회인 RIAA(Recording Industry Association of America)에서 주도하고 있는 SDMI(Secure Digital Music Initiatives)[15]의 표준화 움직임일 것이다. 물론 SDMI에서는 디지털 음악의 저작권 보호 기술에 초점이 맞추어져 있지만 다른 분야에도 적용 가능한 표준이 선정될 것으로 보이며 많은 영향을 미칠 것으로 보인다

PC 외에도 MP3 player, eBook, set-top box, digital TV, DVD player, mobile phone, PDA 등 디지털 컨텐트를 사용할 수 있는 다양한 device들이 출현함에 따라 저작권 보호 기술

도 이런 다양한 플랫폼에서도 일관된 방법으로 적용될 수 있도록 개발되고 있는 추세이다.

4. 결 론

디지털 컨텐트의 적절할 수준의 저작권 보호는 이제는 디지털 경제가 앞으로 나아가기 위하여 필요조건이다. 많은 인터넷 무료 정보 제공 기업들이 더 이상 광고 수입에 의존하기는 어려운 상황에 와 있다. 사용자들은 좀 더 양질의 고급 컨텐트를 원하고 있으나 컨텐트 소유자들은 불법 사용이 염려되어 자신들의 컨텐트를 내 놓지 않고 있다. 그렇다고 현재의 저작권 보호 기술들이 완벽한 상태는 아니므로 필요 이상 저작권 보호를 강제로 적용하는 것은 사용자들에게 불편을 초래하여 바람직하다고 볼 수 없다.

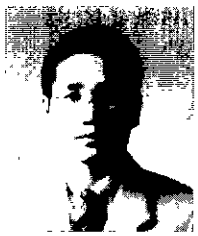
각 컨텐트의 특성에 따라 적절한 저작권 보호를 하고 거기에 맞는 기술을 선택하여야 할 것이다. 본 보고서에서 다루었던 저작권 추적 기술은 컨텐트 사용에 따르는 비용을 최종 소비자가 지불할 필요는 없지만 그 컨텐트가 원 저작자의 허락 없이 제가공 되는 것을 막으려고 하는 경우 적절한 기술이 될 것이다. 저작권 추적 기술은 또한 저작권 관리 기술과 같이 적용되어 보안성을 한 층 더 높일 수도 있을 것이다 저작권 관리 기술은 컨텐트의 사용 규칙을 어떻게 적용하느냐에 따라 저작권 보호 수준이 매우 다를 수 있는데 어떤 수준의 보호가 적절한지는 다분히 컨텐트의 유형에 따라서 결정해야 할 것이다. 예를 들어 어떤 컨텐트는 news 같아서 생성된 지 오래되면 가치가 떨어진다면 초기에는 저작권 보호를 철저히 하다가 일정 시간이 지난다면 하지 않는 것이 적절할 것이다. 또 어떤 컨텐트는 음악 같이 반복적으로 사용할 가능성이 많은 반면 어떤 것은 한 번 사용하면 다시 사용할 가능성이 적은 것도 있을 것이다 모두 이에 적절한 저작권 보호를 하는 것이 저작권자의 이익을 보호하면서 사용자의 편의성도 고려하는 방안일 것이다.

저작권 보호 기술들은 이제 막 시장에서 적용되는 단계이고 적용해야 하는 환경도 급격히 변하고 있는 상황이어서 많은 기술의 발전과 변화가 예상되고 있다 모든 컨텐트 유형에 적용 가능하고 모든 적용 환경에서 일관되게 적용될 수 있는 기술이 대세를 이룰 것으로 보이며, 본 보고서가 그런 다양한 기술들은 접근하는데 작으나마 도움이 되기를 바란다.

참고문헌

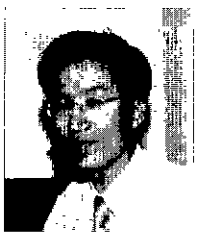
[1] Fred Mintzer, Jeffrey Lotspiech, Norishige Morimoto. Safegarding Digital Library Contents and Users: Digital Watermarking. D-Lib Magazine, December 1997.
[2] Norman Paskin. DOI: Current Status and Outlook. D-Lib Magazine, May 1999
[3] http://www.indecs.org/
[4] http://www.interturst.com
[5] http://www.rightsmarket.com
[6] http://www.contentguard.com
[7] http://www.xrml.org
[8] "Superdistribution: Objects As Property on the Electronic Frontier", Brad J. Cox, Addison-Wesley, May 1996.
[9] http://www.reciprocal.com
[10] http://www.contentguard.com/ePCS.htm
[11] http://www.previewsystems.com
[12] http://www.softlock.com
[13] http://www.liquidaudio.com
[14] http://www.wave.com
[15] http://www.sdmi.org

배 민 오



1981 서울대학교 전자공학과(학사)
1983 한국과학기술원 전산학과(석사)
1983~1986 삼성전자 종합연구소
1992 Syracuse University 전산정보학과(박사)
1992 삼성SDS 정보기술연구소
1996~현재 동덕여자대학교 전자계산학과 조교수
관심분야:논리프로그래밍, 전자상거래, XML 프로그래밍, 웹 데이터베이스
E-mail:bai@dongduk.ac.kr

조 규 곤



1981 서울대학교 전기공학 학사
1983 서울대학교 전기공학 석사
1983~1987 삼성전자
1992 미국 Rutgers University 컴퓨터공학 박사
1992~2000 삼성SDS
2000~현재 Fasoo.com 대표이사
관심분야:DRM, Software Architecture, Machine Learning, Computer Vision
E-mail:kcho@fasoo.com

• 제12회 한글 및 한국어 정보처리 학술대회 논문모집 •

- 일 자 : 2000년 10월 13 ~ 14일
- 장 소 : 성공회대학교
- 논문제출 일정
  - 논문제출 마감 : 2000년 9월 2일
  - 심사결과 통보 : 2000년 9월 10일
  - 최종논문 제출 마감 : 2000년 9월 30일
- 논문양식 : 정보과학회 논문양식(A4용지)으로 최대 8페이지로 제한
- 주 최 : 한국어정보처리연구회, 한국인지과학회
- 논문제출 및 문의처
  - 논문 업로드 : http://magics.yonsei.ac.kr/klip2000/upload.html
  - 문의 및 제출 : 연세대학교 전산학과 나동열 교수
    Tel. 033-760-2246
    E-mail:klip2000@magics.yonsei.ac.kr