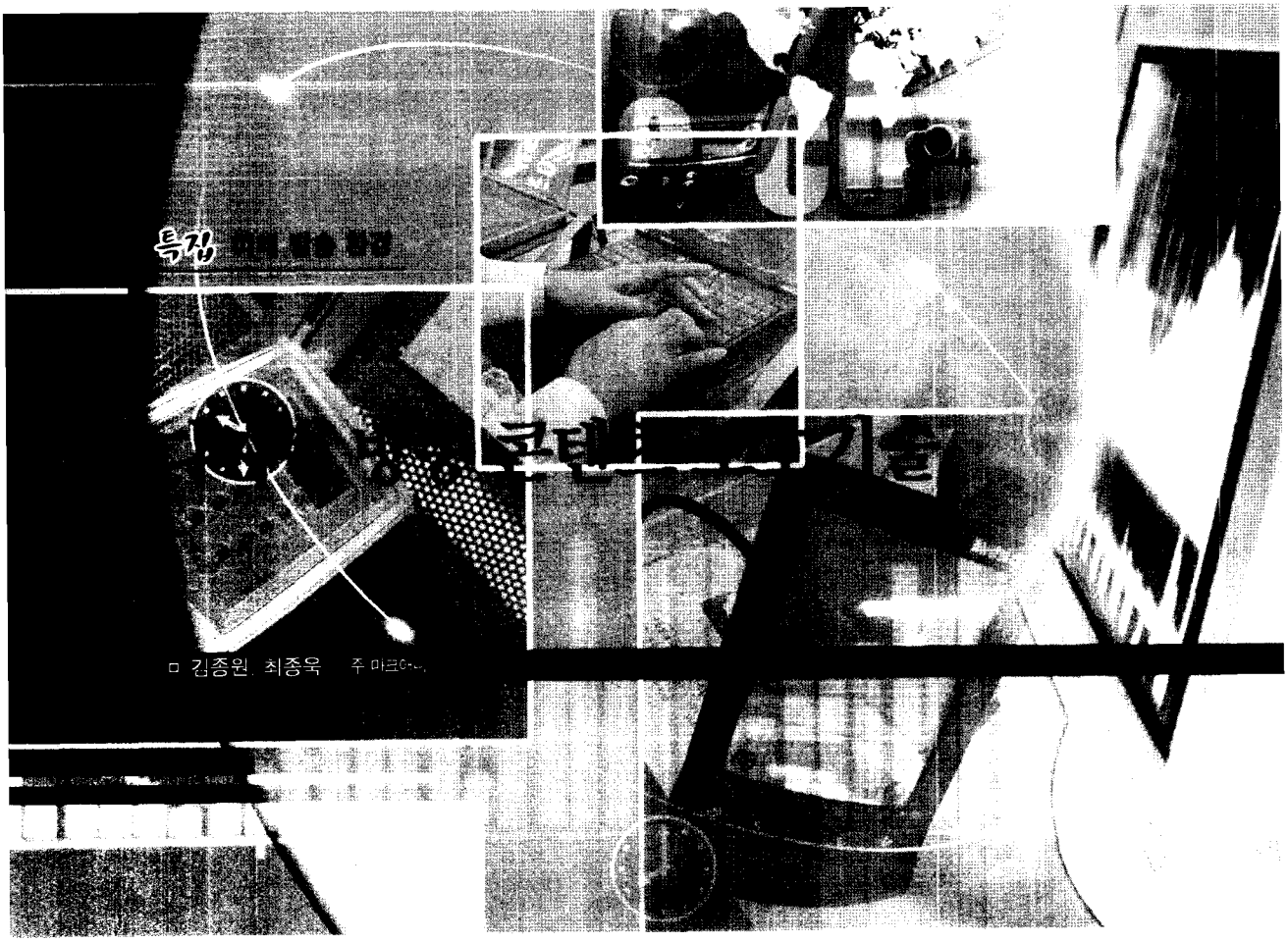


□ 김종원, 최종욱 주 마르○○

Ⅰ. 서 론

1894년 마르코니에 의해서 무선전신이 발명되면서 무선 송수신 장치에 대한 기틀이 마련되었으며, 이는 라디오 방송이나 텔레비전 방송의 초석이 되었다. 1912년 타이타닉호의 침몰사건으로 무선통신의 위력이 전세계에 알려지게 되었으며, 미 의회에서는 "라디오 법"을 통과시켰다. 이 때부터 방송이라는 의미는 미 해군에 의해서 "명령을 무선으로 한번에 여러 군함에 보낸다"는 의미로 사용되게 되었다[1].

1920년 미국에서 콜사인 KDKA로 첫 고정 라디오 방송국이 탄생하였으며, 1928년에는 독일에서 세계최초로 텔레비전 방송을 실시하였으며, 영국의 BBC는 전자식의 405주사선, 초당 25 프레임의 텔레비전 방송을 시작하였다. 이후, 1953년 북미표준인 NTSC(National Television System Committee) 방식이 개발되었으며, 1961년에는 프랑스에서 SECAM(Sequentoel Couleur A Memorie)시스템을 소개하였고, 1963년에는 PAL방식이 제안되었으며, 1967년부터 유럽에서 사용되기 시작하였다. 1972년 일본이 CCIR에 HDTV를 제안하고, 1977년에는 아날로그 방식의 HDTV개발에 박차를 가하면서 TV 기술에 새로운 전기가 마련된다. 고품질의 콘텐츠를 재생할 수 있는 HDTV에 있어서는 일본이 선두주자였으나 대역폭의 문제가 심각하게 걸려 있었고, MUSE라는 방식의 압축에 의해 절반이하로 낮추었으나 여전히 기존의 채널에 비해서 매우 높은 대역폭을 요구하고 있었다. 이런 와중에 미국은 1987년 디지털 방식의 HDTV를 제안하면서 독자적인 행보를 걷기 시작하였고, 1990년에는 지금은 잘 알려진 MPEG 그룹에서 15Mbps로 HDTV의 화질을 전송하는 방식인 디지사이퍼 방식이 발표되었다. 이 방식에 의하면 현재 텔레비전 방송방

식에 대해서 동일 품질로 4배의 전송이 가능한 방식이다.

1956년 5월 12일 국내에 처음으로 텔레비전 방송이 시작된 이후로 컬러 텔레비전 시대를 거쳐서 디지털 방송 시대에 접어들고 있는 시점에서 방송 콘텐츠의 중요성이 그 어느 때보다 강조되고 있다. 기존의 아날로그 방송을 위해서 제작되는 콘텐츠와 고품질의 디지털 방송을 위해서 제작되는 콘텐츠의 품질이 갖는 차이에서부터, 제작에 투입되는 장비와 비용의 모든 측면에서 매우 막대한 투자를 필요로 하고있다. 이와 같이 막대한 투자를 통해서 제작된 디지털 방송 콘텐츠는 디지털로 전송되고 수신되는 특성상, 한번 복제가 일어나면 불법적인 유통을 제어할 수 없는 문제를 안고 있다.

아날로그로 제작된 콘텐츠는 VCR을 통해서 녹화를 하더라도 방송 품질의 절반이하의 해상도로 저장되며, 마그네틱 테잎의 특성상, 반복적인 사용에 의해서 품질이 저하되며, 대량으로 복제할 때는 원본보다 품질이 저하되는 특성을 가지고 있다. 그러나, 디지털로 제작된 콘텐츠는 열화가 일어나지 않으며, 무제한의 복제가 가능하고 네트웍을 통해서 손쉽게 전달이 가능하다는 장점이자 단점을 보유하고 있다.

우리나라는 올해 초고속 통신망 가입자가 1000만을 넘어섰으며, 따라서 대부분의 가정이 ADSL이나 케이블 모뎀과 같은 초고속 통신망을 사용하고 있다는 것이다. 이러한 초고속 통신망 사용자는 콘텐츠의 공유나 배포이서 매우 유리한 입장에 서있으며, 따라서, 콘텐츠를 제작하는 방송사나 기타 콘텐츠 서비스 사업자들에게는 불법유통으로 인한 저작권 침해를 우려하지 않을 수 없는 것이 현실이다.

본격적인 디지털 방송시대를 앞두고, 고품질 디지털 방송 콘텐츠를 불법복제나 유통으로부터 방어하기 위해서는 기술적으로나 법적인 제재조치가 필요하며, 다양한 분야에서 이러한 방송 콘텐츠를 보호할 수 있는 기술이 개발되거나 적용되고 있다. 본고에서는 디지털 방송 콘텐츠 보호기술에 대한 소개와 관련 법안에 대한 소개를 하기로 하겠다.

Ⅱ. 콘텐츠와 저작권

대량복제의 시작은 출판기술의 발달로부터 유래되었다고 할 수 있다. 목판이나 금속활자와 같은 대량복제를 위한 기구들이 발명되기 이전에는 필사본이 유통되었기 때문에 당시의 콘텐츠라고 할 수 있는 서적은 매우 희귀한 자료가 되었다. 그러나 인쇄술의 발달로 대량복제, 대량유통의 시대가 열리면서 저작권에 대한 관심이 높아지기 시작하였으며, 미국이나 유럽을 시작으로 저작권을 보호하기 위한 법제화가 추진되기 시작하였다.

최초의 저작권 관련 분쟁사례로는 1908년 미국에서 음악 출판사인 화이트 스미스 뮤직 퍼블리싱사가 자동피아노 두루말이 제작업체인 아폴로사에 저작권 위반으로 제소한 사례를 들 수 있다. 미국 대법원은 이 사건에 대해서 공평이용의 원칙에 따라서 아폴로사에게 승소판결을 내렸으며, 미국 의회는 1년뒤 두루말이와 녹음을 저작권 보호대상에 포함을 시켰다.

지금은 거의 대부분의 가정에서 사용되고 있는 VCR이 소니사에 의해서 처음 출시되었던 1975년도에 월트 디즈니와 유니버설 스튜디오는 이 VCR의 저작권 침해이유로 판매금지 청구소송을 제기하였다. 1984년 미국 대법원은 VCR의 저작권 침해 가능성은 인정되지만 개인적 용도로 활용하는 것은 문제가 없다는 것으로 소니에게 승소 판결을 내렸

다. 이후, 1992년도에는 녹음테잎이나 복제장치를 생산하는 업체가 음악가에게 지불할 로열티 기금 납부를 의무화하였으며, 디지털 저작물의 불법복제 행위가 심각해지면서 1998년도에는 DMCA (Digital Millennium Copyright Act)에서 디지털 저작물의 보호를 법제화했다.

아날로그 방송이 진행되고, 오프라인을 통해서 콘텐츠들이 공급되던 시절이라고 해도 콘텐츠의 저작권 침해사례가 빈번하게 일어났었다. 단지 오프라인이라는 상황에서는 전달매개체가 사람이나 택배, 우편과 같은 방법을 이용하기 때문에 전달과정이 오래 걸리고 불법유통 단속을 통해서 제재를 가할 수 있기 때문에 심각한 영향을 미치지는 않았다. 아날로그 방송 콘텐츠가 비록 불법복제나 유통이 활성화되지 않더라도 콘텐츠 제작자인 헐리우드의 영화제작사나 음반협회에서는 끊임없이 불법복제나 유통에 대한 근절책을 마련하기 위해서 고민해오고 있었으며, 기술적 혹은 법적인 제재를 가하기 위해서 노력해왔다.

아날로그 콘텐츠에서도 성행했던 불법복제와 불법유통이 디지털 시대에서 더욱 심각하게 문제시되는 것은 디지털 콘텐츠의 특성이 원본과 복제본의 품질차이가 없으며, 무제한 적으로 복제가 가능하다는 것이며, 또 한가지는 그 유통구조가 오프라인처럼 사람과 사람이 만나야하는 것이 아니라 네트웍에만 연결되어 있으면 불법유통이 가능하다는 취약성을 가지고 있기 때문이다. 네트웍을 통한 유통구조는 중간 유통이라는 과정을 생략함으로써 콘텐츠 창작자나 서비스 제공자, 사용자에게 긍정적인 수익분배를 가져올 수 있는 구조로 활용할 수 있으나 오히려, 불법유통의 매개체로 사용되기 때문에 콘텐츠 유통시장에 악영향을 미치고 있는 것이다.

마찬가지로 디지털 방송 콘텐츠에 있어서도 개인용 디지털 녹화장치인 PVR(Personal Video Recorder)에 의해서 쉽게 저장되고, DVD 기록장치를 통해서 유포되거나 인터넷을 통해서 급속히 확산될 수 있다. 고품질의 방송 콘텐츠를 만들기 위한 노력이 점점 증가하고, 비용도 함께 증가하고 있는 추세에서 오히려, 불법유통에 의한 저작권의 침해는 새로운 고품질 방송 콘텐츠를 만들기 위한 투자여력을 손상시키게 될 것이며, 따라서 기술적인 조치나 법적인 조치에 의해서 방송 콘텐츠를 보호하기 위한 노력이 필요한 것이다.

Ⅲ. 디지털 콘텐츠를 위한 법안 활동

냅스터와 같은 P2P 서비스를 기반으로하는 사이트가 콘텐츠의 불법유통을 조장한다는 이유로 소송에 걸리면서 폐쇄 결정이 내려졌고, 우리나라에서도 소리바다의 P2P 서버의 폐쇄 결정이 내려졌다. 콘텐츠를 소유하고 있는 음반사나 영화사들은 인터넷을 통한 불법 콘텐츠의 유통으로부터 자신들의 권리를 지켜내기 위한 노력의 일환으로 기술적 조치를 강구하려는 시도를 해왔다. DVD 포럼 산하에서는 CptWG(Copy Protection Technical Working Group)가[2] 활동을 하면서 DVD의 불법복제 방지 기술에 대한 논의가 이루어지고 있으며, 미국음반산업협회인 RIAA(Recording Industry Association of America)의 주도하에 음반에 대한 저작권 보호기술의 채택을 위해서 SDMI(Secure Digital Music Initiative)[3]라는 조직을 구성하였으나 여러 가지 논쟁만 남기고 무위로 끝나버리고 말았다.

SDMI와 같은 활동이 업체간의 이견으로 합의를 도출하지 못하게되자 미국 음반산업협회나 MPAA(The Motion Picture Association of

America)와 같은 콘텐츠 사업자들은 법적인 조치를 강구하기 위해서 정치권을 움직이기 시작하였다.

1. SSSCA

음반 업계에서 꾸준한 디지털 저작권보호에 대한 로비의 결과, 1998년 DMCA(디지털 밀레니엄 저작권 법률)를 탄생시키고, 그의 연장선에서 이번 Security Systems Standards and Certification Act : SSSCA의 Draft안이 8월에 어니스트 홀링스(사우스 캐롤라이나 상원의원-Commerce Committee 의장)에 의해 제기되고, 이는 2001년 9월 말 경에 법안으로 소개될 예정이었다. SSSCA는 1998년 법안이 통과된 DMCA의 확장 혹은 확대라고 간주되고 있는데, 이는 모든 종류의 상호작용이 가능한, 즉 디지털 형식의 복제 정보를 저장, 제어, 전송 등의 기능을 가진 모든 하드웨어(디바이스)나 소프트웨어는 반드시 그 속에 저작권을 보호할 수 있는 기술이 내장되어 있어야 한다는 법안이다. 이 법안에서는 산업계가 보안 표준에 대해서 의견의 일치를 볼 수 있도록 약 1년간의 유예기간을 가지게 될 것이고, 상무위원회에서 참가하여 하나의 표준을 만들 것이라고 알려졌다.

산업계와 정부가 디지털 저작물을 보호하기 위하여 인증된 보안기술을 사용하도록 위임함으로써, 인터넷 환경을 Pay-to-Pay 시스템으로 전환하려는 목적으로 일반적인 Fair Use(영화의 VHS 테이프에 저장하는 행위, 친구에게 책을 빌려주는 행위, 소프트웨어의 backup copy 등)의 개념을 축소시켜, 단지 Time-shifting(개인이 나중에 보기 위해 저장 혹은 복제하는 행위로 생각이 됨)을 위한 복제만을 Fair Use로 간주한다. 이 결과, 법령의 위반시 5년간의 징역과 50만달러의 벌금형 항목이 추가될 것으로 알려졌다.

또한, 미국 자체의 네트워크나 데이터 보호 능력의 향상 목적으로 미국은 클린턴 행정부시절에 보안 연구소 및 정보보호프로그램에 투자하기 위해서 약 6억 달러를 비축해 놓은 상태이다. 전체적으로 보면, 디지털 콘텐츠 소유권자와 제공자, 프로그래머, 오픈소스 옹호자들로 나뉘어져 상호 공방을 하고 있는 것으로 파악되고 있다. 이 법안에 대해서 드러난 지지자는 지난 8월 처음으로 이 법안의 Draft를 내 놓은 상무위원회 위원장인 어니스트 홀링스 상원의원, 꾸준한 로비활동을 펼치고 있는 Walt Disney 등 Hollywood 진영의 인사이다. 현재, Intel, IBM 등의 하드웨어 제조업자들은 자발적으로 자신들의 미래 제품에 이러한 디지털 저작권 보호기술을 넣으려는 작업을 진행해 오고 있다.

2. CBDTPA

SSSCA 법안상정이 IT업계나 기타 사용자들의 반발에 부딪치자, 2002년 3월 어니스트 홀링스 상원의원은 이를 약간 축소하여 '소비자 광대역 및 디지털 텔레비전 촉진법안' (CBDTPA; Consumer Broadband and Digital Television Promotion Act)을 상정하는 전략으로 선회했다. CBDTPA에 따르면 PC · 휴대폰 · CD플레이어 등 각종 디지털 하드웨어와 소프트웨어 개발회사들은 앞으로 정부가 지정하는 복제방지 기술을 제품에 반드시 포함시켜야 한다. 이와함께 연방통신위원회(FCC)의해 저작권물을 재생산할 수 있는 능력을 가진 것으로 평가된 소프트웨어는 미국내에서 일절 판매가 금지된다. 또, 무료로 프로그램 코드를 시중에 제공하는 프로그래머들도 정부가 인정하는 기술범위 내에서

만 새로운 버전을 발표할 수 있다. 만일 이를 위반하고 불법복제 프로그램을 판매할 경우에는 최고 5년의 징역과 50만달러의 벌금을 물게 된다.

어니스트 홀링스 의원은 법안 상정 배경에 대해 "인터넷 및 디지털 TV 산업은 컨텐츠의 저작권이 지켜지는 가운데 발전할 수 있다"며 "나는 민간의 토의를 통해 저작권 문제가 해결될 수 있다고 믿지만, 지금까지의 과정을 볼 때 해결을 촉진하기 위한 매개체가 필요하다고 본다"고 설명했다. 이는 그동안 영화, 음반 등 엔터테인먼트 업체들이 요청해온 불법복제 콘텐츠 근절방안 마련을 정치권이 전폭 수용한 결과로 풀이된다.

Ⅳ. 디지털 TV의 보안을 위한 기술

미국을 중심으로 디지털 콘텐츠를 보호하기위한 기술적 조치를 법적인 강제조치에 의해서 멀티미디어 재생기에의 채택을 의무화하는 움직임이 일어나면서, 업체내에서도 자발적으로 보안 표준을 위한 합종연횡이 일어나고 있다. 이 가운데 가장 활발히 움직이고 있는 곳으로는 케이블 TV 연합체인 오픈 케이블(OpenCable™)이라는 조직과, 가전제품을 생산하는 업체들을 중심으로하는 기술적 활동들이 있다.

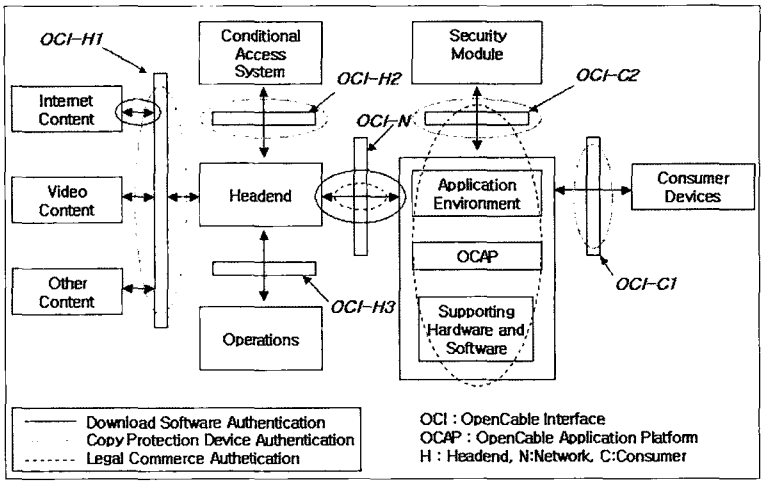
1. 오픈케이블의 저작권 보호[5]

오픈케이블 기술표준은 2005년부터 미국의 차세대 디지털 케이블 방송 표준 규격으로 적용될 예정이며, 우리나라도 디지털 유선 방송 표준으로 채택되었다. 오픈케이블의 기술표준에서는 디지털 콘텐츠의 복제방지 기술을 적용하도록 되어있으며, 2001년 6월 ANSI SCTE 41/formerly DVS 301(POD Copy Protection System)에 기술표준 규격으로 제정되었다. 이를 기반으로 2002년 5월 복제방지 기술에 관한 규격으로 발표된 것이 OC-SP-PODCP-IF-I07-020524 (OpenCable™ POD Copy Protection System)[6]이다.

이 기술표준에서 복제방지를 위해서 적용된 기술들을 살펴보면 〈표 1〉과 같다[7].

〈표 1〉 방송 콘텐츠 불법복제 방지 기술표준에 포함된 정보보호 기술

기술명칭	용 도	비 고
DES-ECB	수신제한장치(POD)에서 셋톱 박스로 전송하는 콘텐츠 암호화	- 64bits 블록 암호화 - 56bits 암호화 키 적용 - MPEG2 TS payload에만 적용
DFAST	DES-ECB 암호화 키 발생	- US patent 5054067 - US patent 4860353
SHA-1	-키정보 압축, 발생 -인증서 정보 압축	-FIPS PUB 180-1/186-1 compliance -CCI 채널 인증 정보 발생
Diffie -Hellman algorithm	- 장치 인증용 비밀정보 생성 -암호화 키 공유	- FIPS PUB 140-1 compliance - 1024bits public key
ITU X.509 version 3	-장치인증 -공개키 교환	- IETF PKIX RFC2459 compliance - Public key type : F4 - 2048bits modulus RSA signature - 3 level chain
CRL	수신제한 장치에 대한 서비스 권한 부여 및 제한	- IETF PKIX RFC2459 compliance -EMM generation
Challenge & Response	CCI 무결성 보장	- SHA-1, FIPS PUB 140-1 - One second time limit



〈그림 1〉 오픈케이블의 시스템 구조

오픈케이블의 불법복제 방지를 위한 기술에서는 콘텐츠가 셋톱박스와 수신제한장치(POD) 사이에서 원본 형태로 출력되지 못하도록 콘텐츠를 DES-ECB(Data Encryption Standard-Electronic CodeBook mode) 방식에 의해 암호화하도록 규정하고 있으며, 암호화를 위해 필요한 키 정보의 교환을 위해 Diffie-Hellman 공개키 기반 키교환 알고리즘을 도입하고 있다. 또한, 키 교환시 해당 장치간의 제 3자공격을 방지하기 위해서 ITU-T X.509r3 인증서를 통해 키정보의 무결성과 장치의 적법성을 인증하도록 규정하고 있다. 키 정보의 압축을 위해서는 SHA-1(Secure Hash Algorithm)을 사용하고 있으며, 최종 암호화 키 수열 생성을 위해서는 DFAST(Dynamic Feedback Arrangement Scrambling Technique) 알고리즘을 케이블랩스를 통해 라이센스하여 이용하도록 권고하고 있다.

또한, 서비스를 개시하는 시점과 서비스 중에도 수신 장치의 서비스 권한과 범위를 제어하기 위해 인증서 폐지 목록(CRL : Certificate Revocation List)을 적용하도록 권고하고 있으며, 복제방지를 위한 제어의 기준은 복제제어 정보(CCI : Copy Control Information)를 기준으로 하고 있다.

만일 CCI가 00이 아닌 콘텐츠에 대해서 CA 스크램블이 Off되어 있는 경우에는 POD CP는 스크램블을 하지 않는다. 이는 서비스 제공자가 일차적으로 CA를 통해 보호하지 않는 콘텐츠에 대해서는 POD가 복제 금지에 대한 책임을 지지 않는다는 것이다.

이러한 오픈케이블의 구조를 〈그림 1〉에 나타내었다.

〈표 2〉 CCI 정보에 대한 복제방지 제어 의미와 용도

CCI bits	디지털 콘텐츠	아날로그 콘텐츠	CA	POD CP
00	복제 허용	복제 허용	Off	Off
01	이후의 복제 금지	AGC On, Split bust Off	On	On
10	한번의 복제 허용	AGC On, 2 Line Split bust On	On	On
11	복제 불허	AGC On, 4 Line Split bust On	On	On

2. HDMI(High Definition Multimedia Interface)

HDMI는 미국의 DMCA법안이나 SSSCA법안, CBDTPA법안의 통과를 고려한 대책 마련을 위해서 히타치, 마쓰시다(파나소닉), 소니, 도시바, 필립스, 실리콘 이미지 그리고 톰슨사가 연합하여 멀티미디어 콘텐츠의 불법복제 방지를

위한 기술 표준안을 만들고자하는 조직이다. HDMI에서는 모든 콘텐츠를 3가지로 구분하여, 무제한 복제가능(Copy free)과 1회 복제(Copy once), 복제 불가(Do not Copy)의 CCI를 사용한다. 따라서 소비자들에게 CCI에 기반하여 녹화나 재생에 대한 저작권 사용료를 징수하는 것으로 방향을 잡고 있다.

2002년 5월 발표에 의하면 HDMI는 "broadcast flag"라는 것을 이용하여 콘텐츠 내에 CCI 정보를 숨기는 워터마킹 기술을 활용할 것으로 예상되고 있으며, 유사한 활동인 DTCP(Digital Transmission Content Protection)이나 HTDP(High-bandwidth Digital Content Protection)과의 연합이 이루어질 것이다. DTCP는 디지털 콘텐츠의 전송채널에서의 복제제어 정보, 인증 및 키 교환, 콘텐츠 스크램블링, 시스템 정보갱신 등의 기술을 활용하는 것으로 오픈 케이블과 유사한 기술표준체계를 가지고 있다. 여기서 복제제어 정보로는 워터마킹을 이용하며, 자유복제, 일회복제, 추가복제불가, 복제불가의 네 종류를 사용한다.

이밖에도 CptWG산하에 BPDG(Broadcasting Protection Discussion Group)가 개설되어 방송 콘텐츠 보호기술에 대한 논의가 이루어지고 있으며, 2002년 6월 HDMI 사양 0.9 버전이 제안되었다.

Ⅴ. 워터마킹과 DRM

디지털 콘텐츠의 저작권 보호에 대한 관심이 높아지면서 디지털 콘텐츠의 복제를 방지하거나 보호할 수 있는 기술들이 등장하고 있다. 그 가운데 가장 효과적으로 활용되고 있는 기술이 디지털 워터마킹 기술과 DRM(Digital Rights Management) 기술이다.

1. 디지털 워터마킹 알고리즘

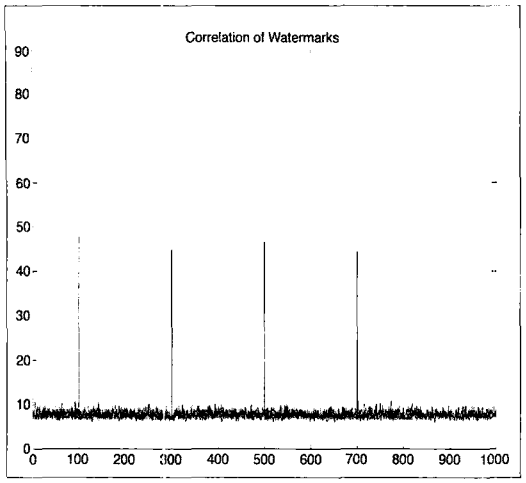
디지털 워터마킹 알고리즘은 매우 다양한 형태의 알고리즘들이 개발되고 있으나 그 기본적인 형태에 있어서는 큰 변화가 없기 때문에 여기서는 가장 기본적인 형태의 워터마킹 알고리즘에 대해서 설명하도록 한다.

하위비트 코딩 : 디지털 콘텐츠의 매 샘플에서 최하위 비트를 원하는 정보인 워터마크로 대치하는 방법이다. 이 방법은 구현이 매우 용이하고, 처리시간이 빠르지만 외부의 공격에 의해서 손쉽게 워터마크가 제거되기 때문에 연약한(fragile) 워터마크라고 한다.

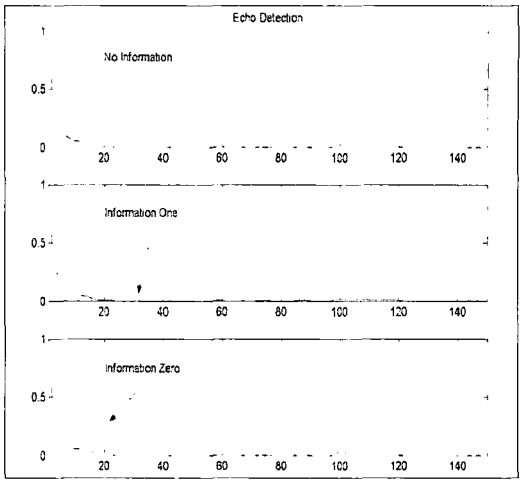
패치웍 알고리즘 : 이는 통계적인 방법을 이용해서 랜덤하게 선택된 두 영역의 평균값은 동일하다는 가정하에 수행된다. 선택된 두 영역 중에서 한 영역은 평균값을 높이고, 다른 영역은 평균값을 낮춤으로써 전체적인 평균값은 변화가 없게 만들고, 랜덤하게 선택된 순서를 알지 못하면 그 변화를 감지할 수 없도록 만드는 방법이다. 워터마크를 검출할 때는 랜덤 순서에 의해서 선택된 두 영역의 샘플 값의 차이를 식(1)과 같이 구함으로써 워터마크의 존재 여부를 확인할 수 있다.

$$S = \sum_{i=1}^{n} (\tilde{a}_i - \tilde{b}_i) \qquad (1)$$

확산대역 알고리즘 : 이 방식은 NEC 연구소의 I. J. Cox[8]에 의해서 제시된 방법으로 워터마크 정보를 확산대역의 특성을 갖는 랜덤 수열로 생성함으로써 워터마크의 보안성을 높일 뿐만 아니라, 주파수 전대역에 걸쳐서 워터마크 정보가 잔류함으로



〈그림 2〉 키 값에 따른 랜덤 수열의 상관도



〈그림 3〉 켑스트럼에 의한 에코 검출

써 외부공격에 의해서 일부가 소실되더라도 워터마크 정보를 복원할 수 있다는 장점을 가지고 있다. 또한, 랜덤 수열을 생성하는 키 값에 따라서 서로 다른 랜덤 수열의 생성이 가능하며, 생성된 수열들 간에는 상관성이 매우 낮기 때문에 워터마크 검출에 있어서 오류가 일어나는 것을 최소화 할 수 있다. 〈그림 2〉에서 보는 바와 같이 자신의 키 값과 동일한 키 값에 의해서 생성된 랜덤 수열과는 매우 높은 상관도를 보이지만 다른 키 값에 의해서 생성된 랜덤 수열과의 상관도는 상대적으로 매우 낮다는 것을 알 수 있다.

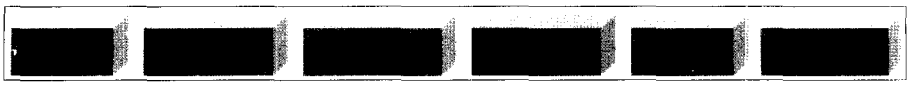
위상코딩 알고리즘 : 위상코딩은 이미지보다는 오디오 워터마킹 기술에서 많이 활용되는 기술이다. 오디오 신호의 세그먼트를 주파수 영역으로 변환하고, 여기서 얻어지는 위상성분을 변형함으로써 워터마크 정보를 은닉하는 기술이다. 위상코딩 방식은 외부공격에 매우 강인하지만 워터마크의 삽입도 그만큼 어려운 기술에 해당된다.

에코코딩 : 사람의 청각은 매우 짧은 신호의 지연에 대해서는 감지할 수 없기 때문에 본 방식은 원 오디오 신호에 짧은 시간지연을 갖는 오디오 신호를 더함으로써 워터마크 정보를 삽입하는 방법이다. 이는 식(2)와 같이 나타낼 수 있으며, 워터마크

$$y_0(t) = x(t) + x(t-\delta_0)$$
$$y_1(t) = x(t) + x(t-\delta_1) \qquad (2)$$

의 검출에는 〈그림 3〉과 같이 켑스트럼을 이용하여 검출할 수 있다.

심리음향 모델 : 오디오 워터마킹에서는 인체의 청각의 주파수 특성을 이용하여 워터마크 신호를 생성하고, 오디오에 삽입하는 방식이 많이 이용되고 있다. 심리음향 모델은 매우 짧은 시간 윈도우 내에서 두 개의 음이 존재할 때 큰 음에 의해서 작은 음이 마스킹되는 효과(temporal masking)나 인접 주파수 대역에서 존재하는 음은 에너지가 큰 음에 의해서 작은 음이 마스킹 되는 효과(frequency masking)를 이용하여 효과적으로 워터마크를 삽입하고 검출할 수 있다.



〈그림 4〉 콘텐츠 가치사슬 (IDC, 2001)

이와 같이 디지털 워터마킹 기술은 콘텐츠 자체에 특정한 정보를 은닉하고, 외부의 공격에 강인하게 설계되었기 때문에 콘텐츠에 항상 붙어 다니는 정보로서 활용가치를 가지고 있다. 비록 오픈케이블이나 DTCP에서 전송 채널에서의 암호화 기술에 의해서 원본 콘텐츠의 노출을 회피하려고 하고 있으나, 최종적으로 사용자가 콘텐츠를 이용하는 경우에는 복호화된 원본 콘텐츠가 노출될 수밖에 없다. 이렇게 노출된 콘텐츠는 스크린 캡춰나 녹음에 의해서 원본에 가까운 품질의 콘텐츠를 획득할 수 있으며, 비디오 영상과 같은 경우에는 메모리에서 콘텐츠 데이터를 가져오는 등의 방법에 의해서 유출될 수 있는 것이다.

그러나, 디지털 워터마크는 콘텐츠에 은닉되어 있어서 상기와 같은 방법에 의해서 콘텐츠가 유출되었을 때도 워터마크 정보가 콘텐츠에 잔류하게되며, 이 정보를 이용하여 재생기기를 제어하는 정보로 활용한다면 매우 효과적이다. HDMI의 "broadcasting flag"와 같은 것이 워터마크 정보로 은닉되었을 때 활용할 수 있는 방법이다.

2. 디지털 저작권 관리기술

초창기 콘텐츠 서비스 사업자의 저작권 보호는 회원에게 사용자명과 비밀번호를 부여함으로써 인증된 사용자만이 콘텐츠에 접근하겠다는 정책을 사용하였다. 그러나 웹을 통해 서비스되는 콘텐츠의 특성상 콘텐츠가 존재하는 경로가 노출되면, 사용자명과 비밀번호를 입력하지 않더라도 콘텐츠에 접근할 수 있다는 취약점이 있다. 따라서, 사용자의 콘텐츠 사용권한 제어나 유통, 과금결제, 저작권 사용현황, 사용자의 인증과 콘텐츠의 보호를 종합적으로 다룰 수 있는 기술을 필요로하게 되었다.

DRM 기술은 디지털 콘텐츠의 이용권한을 관장하고 콘텐츠의 전체 라이프사이클에 걸쳐서 콘텐츠의 이용 결과를 관리하는 하드웨어와 소프트웨어 서비스와 기술이다. 콘텐츠의 가치사슬은 〈그림 4〉와 같이 나타낼 수 있다.

〈그림 4〉는 콘텐츠 가치사슬에 참여하는 많은 회사들에 의해서 수행되는 중요한 역할을 설명한다. 콘텐츠 유통을 위한 모든 비즈니스 모델이 콘텐츠 가치사슬의 콘텐츠 생산자와 콘텐츠 사용자 사이의 모든 구성이 다 들어가는 것은 아니다. 즉, 하나의 회사가 다중 역할을 수행할 수도 있다.

대부분의 기술업체들은 다음과 같은 두 가지의 기본적 목적을 가지고 DRM을 구현한다.

상거래를 위한 DRM : 디지털 콘텐츠를 유료화하기 위해서는 적법한 절차를 거친 사용자만이 이용이 가능하도록 해야하며, 이와 같은 적법한 사용에 대해서 과금을 하고, 불법적인 사용으로부터 콘텐츠를 보호함으로써 디지털 콘텐츠의 상업적 가치를 보호하기 위하여 DRM을 이용하는 것이다.

기밀성을 위한 DRM : 개인 정보보호를 위해서 정보의 기밀성을 유지하는 목적으로 DRM을 이용하는 것이다. 디지털 콘텐츠의 상거래에 있어서 그 거래내역 - 어떤 콘텐츠를 언제 얼마만큼 사용을 했는지 등 - 은 개인의 사생활과 관련된 부분이며, 이러

한 정보의 불법적 사용으로부터 보호는 매우 중요한 것이다. 정보의 기밀성을 위한 DRM은 기업의 기밀이나 정책관리에 적용할 수 있다.

3. DRM의 요소기술

DRM 기술은 콘텐츠의 생성에서부터 사용자에 이르기까지의 라이프사이클에 관계해서, 불법유통을 방지하고 권한관리와 과금결제, 사용내역관리 등을 포함한 디지털 저작권 관리기술이다. 그러나 DRM은 콘텐츠 서비스 사업자의 사업모델에 따라서 다양한 정책을 가질 수 있으며, 이러한 다양한 정책에 따라서 다양한 시스템으로 구성될수 있다.

콘텐츠의 암호화 : 이는 콘텐츠의 포맷에 관계없이 사용자 이외의 파일사용을 방지하는 디지털 콘텐츠의 금고 역할을 수행한다. 암호화는 디지털 콘텐츠를 포장하여 전달하는 것과 같은 의미에서 패키징이라고 불리우기도 한다. 암호화의 형태로는 공개키 방식을 사용하는 것과 대칭키 방식의 알고리즘을 이용하는 방법이 있다. 공개키 방식은 대용량의 콘텐츠를 암호화하기에는 연산량이 너무 많기 때문에 비효율적이고, 콘텐츠 제공 서버의 부담을 가중시키는 문제가 있다. 이에 반해 대칭키 방식은 대용량의 콘텐츠를 암호화하는데 용이하지만 키를 분배하는데 보안상의 어려움이 존재한다. 최근에는 이를 효과적으로 해결하기 위해서 콘텐츠의 암호화는 대칭키 방식으로 하고, 대칭키의 전송에는 공개키를 이용하는 방식이 활용되고 있다.

콘텐츠의 전송 : 암호화된 콘텐츠는 온라인 상에서 안전하게 사용자에게 전달되어야 한다. 콘텐츠의 전송은 암호화와 연계된 방법을 사용하여 전송하는 것이 일반적이다. 전송방법으로는 원본 콘텐츠를 일괄적으로 서버에서 관리하면서 필요에 따라서 스트리밍으로 전송하는 방법과 개인 사용자에게 콘텐츠를 다운로드 시켜서 분산하여 관리하고, 서버에서는 사용규칙이나 암복호화만을 제어하는 방법으로 구분할 수 있다.

콘텐츠의 유통 및 과금 : 콘텐츠의 유통과 과금은 콘텐츠 서비스 사업자의 비즈니스 모델에 따라서 다양한 형태를 가질 수 있다. 콘텐츠의 유통에서는 사용자의 콘텐츠 사용 이외에도 다른 사용자에 의한 추가적인 전송여부의 허용 등, 전체적인 콘텐츠의 사용에 관한 규칙을 정의하고, 그에 따른 과금과 결제가 이루어지는 것이다. 콘텐츠의 사용에 있어서는 일회성 사용이나 영구사용, 보관용 등에 따라서 권한이 달라지며, 권한에 따른 비용지불도 달라지게 된다. 과금과 결제에 있어서는 사이버 머니를

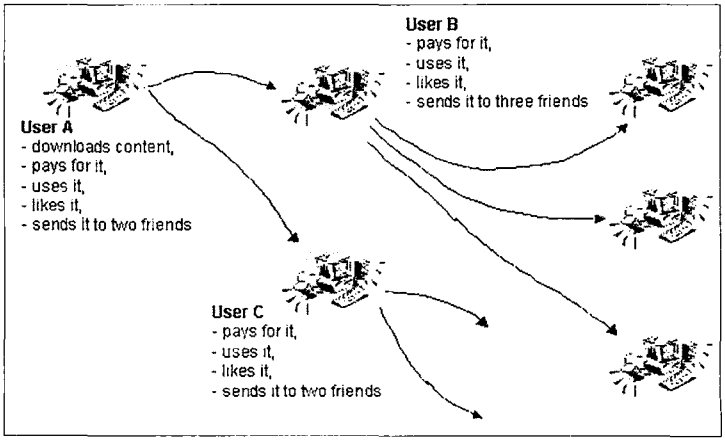


그림 5. 콘텐츠의 양도(Superdistribution)

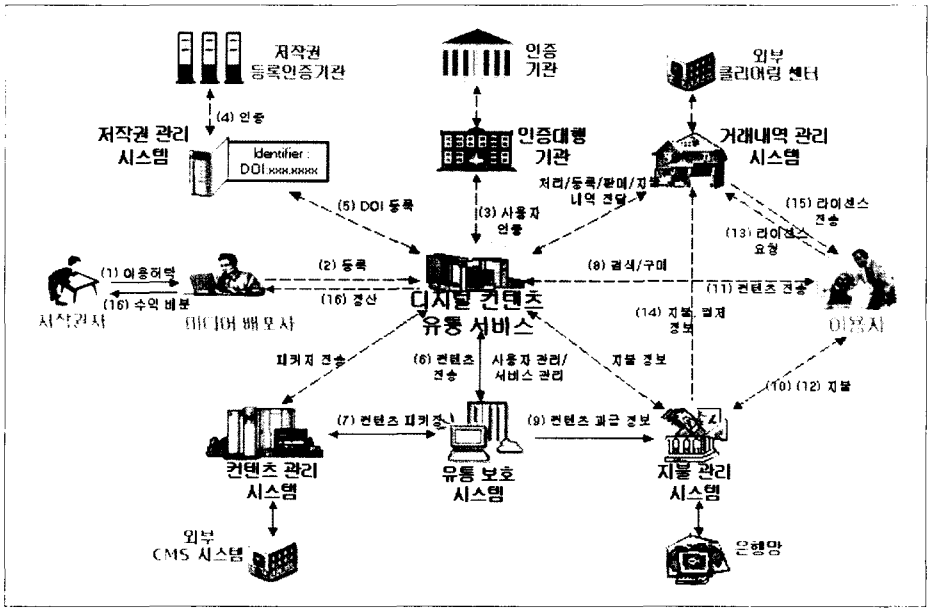
활용하는 방법에서부터 무선단말기를 통한 결제, 은행이나 카드사를 통한 결제 등 다양한 방법에 의해서 과금과 결제가 이루어질 수 있다. 특히, 콘텐츠의 특성상 B2B(Business to Businuss)보다는 B2C(Business to Customer) 거래가 많이 이루어지며, 따라서 소액결제가 많이 이루어지기 때문에 소액결제 지원에 대한 부분을 많이 다루게 된다.

콘텐츠의 정보추적 : 만일 다른 사용자에 의한 콘텐츠의 유통이 발생한 경우 이 콘텐츠를 제어하기 위한 정보의 추적여부를 고려한다. 정보 추적은 로그분석을 통하여 콘텐츠의 이동 및 복제여부를 확인하는 방법과 이를 이용하여 개별적인 콘텐츠의 사용을 제한하도록 하는 방법 등이 있다.

저작권 등록 및 관리 : 디지털 콘텐츠에는 저작권이 있고, 디지털 콘텐츠 생성자가 저작권을 보호받기 위해서 최초의 생성시점을 등록하고, 해당 콘텐츠에 대한 저작권자를 등록함으로써, 향후 발생할 수 있는 저작권 분쟁에 대비할 수 있는 부분이다. 특히, 해당 콘텐츠에 대한 저작권자가 등록되면 콘텐츠의 사용량에 따른 수익분배에 있어서 저작권자의 지분율에 따른 분배가 가능하며, 콘텐츠의 이용현황에 대한 로그분석 등이 가능하다. 콘텐츠의 이용현황에 대한 자료의 축적이나 통계분석 등은 콘텐츠 유통 부분에서 다루는 것이 일반적이며, 클리어링 시스템으로 분리하여 구축하기도 한다. 저작권 등록은 향후 저작권 분쟁에서 보호받기 위해서는 제도적으로 공공성을 띠고 있는 기관에서 관리운영하는 것이 적절하기 때문에 일반 콘텐츠 서비스 사업자는 저작권 등록 시스템을 운영하지 않는 경우도 많이 있다.

이러한 요소들에 의해서 구성된 DRM 시스템의 예를 〈그림 6〉에 나타내었다.

디지털 저작권 관리기술이라는 이름에서 알 수 있듯이 DRM 이라는 것은 특정한 어떤 기술을 의



〈그림 6〉 DRM 시스템의 구성 예

미한다기보다는 안전한 콘텐츠 상거래 시스템을 구성하는 구조라고 생각할 수 있다. 다만, 불법적인 사용자나 악의적으로 시스템 구조를 파헤치려는 크래커로부터 안전하게 콘텐츠를 보호하기 위해서는 시스템간에 무결성을 확인할 수 있는 tamper proofing 기술과 프로그램의 흐름에 개입하여 역공학 프로세스로 암호키를 해독하려는 시도를 무력화시키기 위한 obfuscation과 같은 기술적 조치가 필요하다.

Ⅵ. 맺음말

디지털 방송 시대를 앞두고 있는 시점에서 디지털 방송 콘텐츠의 불법유통 방지를 위한 노력이 어느 때보다도 필요한 시기이다. 과거의 아날로그 방송 콘텐츠는 저장매체가 한계를 갖고 있기 때문에 재전송에 있어서도 방송사의 품질을 넘어설 수 없는 한계를 가지고 있었지만 디지털 방송이 시작되면, 방송사나 불법적으로 재전송을 하거나 복제하여 유통을 시키는 콘텐츠의 차별성이 없어지기 때문에 많은 비용을 투입하여 디지털 방송 콘텐츠를 제작한 방송사에게는 매우 큰 위협이 될 수 있다.

얼마전 우리는 월드컵 경기를 거리의 대형 전광판에서 방영하고자 했을 때, FIFA로부터 전광판 한 대당 얼마의 비용을 지불해야된다는 이야기를 들은 적이 있었다. 또한, 케이블 TV를 비롯하여 많은 방송 콘텐츠가 유료화되어 있는데, 특히, 이와 같이 유료화가 진행되어 있는 방송 콘텐츠에 있어서는 비용을 지불한 사용자와 그렇지 않은 사용자간에 분명한 차별성이 존재해야만 많은 사용자를 끌어모을 수 있을 것이다. 따라서, 디지털 방송 콘텐츠의 불법복제나 유통을 방지하기 위한 기술이 필요한 것이며, 다양한 기술경쟁이 이루어지고 있다.

특히, 미국에서는 CBDTPA와 같은 법안을 상정함으로써, 강제적으로 멀티미디어 재생기기에 저작권 보호기술 채택을 의무화하려하고 있으며, 이에 대비해서 세계적인 기업들이 발빠른 움직임을 보이면서 HDMI와 같은 기술표준을 제안하려는 노력을 기울이고 있다. 결국 디지털 시대에 위협요소로 자리잡고 있는 불법콘텐츠의 복제나 유통을 근절시키기 위해서 법적, 기술적 조치들이 함께 진행되고 있으나 P2P와 같은 새로운 네트웍 기술의 등장은 콘텐츠 보호를 더욱 어렵게 만들어가고 있다.

기술적 조치가 강해질수록 이러한 조치를 무력화시키려는 시도가 많아지게 될 것이며, 창과 방패의 싸움은 끝없이 이어질 것이다. 그러나, 디지털화된 콘텐츠의 저작권이 보호받아야할 재산이라는 것에는 다른 이론이 있을 수 없다. 무상으로 콘텐츠를 창작하는 사람도 있지만, 오늘날 대부분의 콘텐츠 창작자는 자신들이 창작한 콘텐츠로부터 이윤을 창출하기를 원하고 있기 때문에 이들의 권리를 지켜줘야 하는 것이 또한 우리 네티즌들의 몫이 될 것이다.

참 고 문 헌

(1) 문종환, "세계방송기술사", 방송과기술 통권 80호~83호 연재, 2001
(2) http://www.dvd.org
(3) http://www.sdmi.org
(4) http://www.politechbot.com/docs/cbdtpa/
(5) http://www.opencable.com
(6) http://www.opencable.com/downloads/specs/OC-SP-PODCP-IF-I07-020524.pdf
(7) 김영화, "방송콘텐츠의 불법복제 방지를 위한 기술표준", 정보기술, 2002.
(8) I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," NEC Res. Insti., Princeton, NJ, Tech. Rep. 95-10, 1995.
(9) J. Dubl and S. Kevorkian, "Understanding DRM Systems," IDC White Paper, 2001.
(10) "DRM white paper, sonera plaza medialab," Feb., 2002.
(11) C. S. Collberg and C. Thomberson, "Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection," U. of Arizona, TR, Mar., 2000.

필 자 소 개

김 종 원

-1989년 : 서울시립대학교 공과대학 전자공학과, 공학사
-1991년 : 서울시립대학교 대학원 전자공학과, 공학석사
-1995년 : 서울시립대학교 대학원 전자공학과, 공학박사
-1995년~1996년 : 과학기술정보연구원 선임연구원
-1996년~2000년 : 주성대학 정보통신학과/음향전자기기학과 조교수
-2000년~현재 : (주)마크애니 부설연구소장
- 주관심분야 : 디지털 워터마킹, 저작권 보호기술, 디지털 신호처리

최 종 욱

-1989년 : University of South Carolina, Ph.D.
-1989년~1992년 : KIST 인공지능연구실장
-1992년~현재 : 상명대학교 정보통신학부 교수
-2000년~현재 : (주)마크애니 대표이사
- 주관심분야 : 디지털 워터마킹, DRM, 인공지능