

# 디지털 방송과 콘텐츠 복제방지 표준활동

김형중  
강원대학교 제어계측공학과 교수

최근 국내에서 SDM-WG (Secure Digital Multimedia Working Group) 출범이 있었다. 대한전자공학회 산하에 멀티미디어콘텐츠보호기술규격위원회가 설립되었다. 국제적인 활동도 활발해서 이미 MPEG IPMP, OPIMA, SDMI 등 많은 국제활동이 전개되고 있다.

## 디지털 방송의 특성과 불법복제

한국도 디지털 방송 시대에 들어서고 있다. 아직은 시형 방송 단계이기 때문에 콘텐츠 불법복제에 대해서는 언급하고 싶어하지 않는다. 시형방송 자체도 힘든 일이기 때문이다. 그러나 디지털방송이 정착되면 이 문제가 전면에 부상하게 될 것이다.

디지털 방송은 MPEG-2로 압축된 디지털 데이터를 내보낸다. 여기서 디지털 데이터의 특성 때문에 불법복제 문제가 심각히 대두된다. 디지털 데이터는 완벽한 복제가 가능하고, 혹시 오류가 발생해도 복구가 가능하다. 게다가 디지털 데이터는 편집이 쉬워 원본보다 더 좋은 품질을 지닌 콘텐츠로 둔갑시킬 수도 있다. 대량 배포도 매우 쉽다. 이런 점 때문에 대항할 수 있는 고급 기술이 필요하다.

디지털 방송 콘텐츠를 보호하는 기술은 제한접근(Conditional Access), 즉 CA 외에 별다른 현재는 별다른 대안이 없다. 그래서 다양한 기술을 개발하고 표준화하려는 움직임이 대두되고 있다. 앞으로 디지털방송 콘텐츠에 스크램블링 기술 적용 여부를 논의하게 될 것이다. 공익을 우선하는 방송은 스크램블링 기술을 적용하지 않을 것이다. 그러나 영리를 목적으로 하는 방송은 대부분 스크램블링 기술을 적용하지 않을 수 없다.

그런데 디지털방송 스크램블링에서 가장 문제가 되는 것은 이 시스템이 기지평문공격(Known Plan-Text Attack) 환경에 고스란히 노출되어 있다는 점이다. 풀리기 전 콘텐츠와 풀린 후의 콘텐츠를 모두 가지고 있기 때문에 공격자는 시간적 여유만 있으면 키를 찾을 수 있다.

디지털방송은 비디오 및 오디오를 전송하고 부가서비스로 데이터를 전송하게 된다. 일반적으로 비디오는 데이터 양이 방대해서 전송에 시간이 많이 걸린다. 그래서 불법복제

전문가들도 일단은 양이 적은 오디오를 주로 공격한다. 디지털방송에서 제공되는 고급 오디오를 녹음해서 파는 길이 훨씬 쉽기 때문이다. 데이터는 주로 T-Commerce와 관련된 상품거래 정보들이기 때문에 복제방지보다는 개인의 사생활 정보보호 차원에서 접근해야 한다.

공격에 견디기 위해서는 두 가지 접근법이 있다. 하나는 키를 자주 바꾸는 방법이다. 현재는 DVD를 비롯한 많은 시스템에서 키를 바꾸는 방법을 적용하고 있다. 둘째는 키를 길게 하는 방법이다. 그런데 이 방법은 계산에 시간이 많이 소요되어 당분간 적용하기 어렵다. 멀티미디어 속성 때문에 키를 다 풀어놓고 나중에 천천히 즐기게 하는 것은 상품성이 없다. 멀티미디어는 리얼타임 처리가 가능할 때 상품성이 극대화된다.

## 콘텐츠 복제방지의 중요성

에디슨이 축음기를 발명한 이래 음악을 저장하는 전통적 매체는 레코드였다. 80년대 초까지도 LP 판의 독무대였다. 테이프가 레코드 시장의 일부를 잠식하거나 대체했지만 역시 레코드는 가장 훌륭한 저장 수단이었다.

레코드나 테이프와 같은 아날로그 매체에서도 복제는 있었다. 그러나 디지털 매체처럼 위협적이지 않았다. 아날로그 방식으로 대량 복제하려면 고속복사기와 테이프가 필요하다. 우선 돈이 있어야 복사도 한다는 의미이다. 게다가 시간도 필요하고, 장소도 필요하다. 또, 복사된 테이프는 일단 포장한 다음 저장하거나 운반해야 한다. 어찌 되었든 노동력도 필요하다. 불법복제 단속이 시행되면 물건을 숨기거나 버려야 했다. 아무튼 아날로그 시대에는 복제품이 물리적인 실체로 존재했다.

디지털시대에 들어서면서 양상이 사뭇 달라졌다. 우선 복제품의 물리적 실체가 존재하지 않는다. 다만 파일 형태로 존재할 뿐이다. 그래서 인터넷에서는 복제도 아주 간단하다. 마우스 클릭 한 번으로 모든 것이 복제된다. 물리적 실체가 존재하지 않기 때문에 테이프도, 포장도, 운반도 필요하지 않다. 수천 수만 카피가 순식간에 복제되어 세계 구석구석에 전송될 수 있다.

아날로그 복제에서는 품질이 떨어지는 것을 감수해야 했지만 디지털에서는 품질 열화도 발생하지 않는다. 오히려 품질을 개선할 수도 있다.

그래서 디지털 복제가 두려운 것이다. 손가락만 움직일 수 있다면 누구라도 불법복제를 할 수 있다.

디지털 시대에서는 디지털 콘텐츠가 중요하다고 외쳐댄다. 맞는 말이다. 그렇지만 이처럼 불법복제가 쉬운데 과연 누가 비싼 돈 들여 콘텐츠를 만들려 하겠는가? 차라리 자신하는 셈치면 모를까.

디지털 방송에서도 마찬가지이다. 방송 이전 단계에 먼저 콘텐츠에 대해 그 비용을 충분히 쳐주거나 아니면 복제가 어렵게 해 줄 필요가 있다. 그래서 스크램블링 기술 외에도 별도로 디지털 콘텐츠의 복제방지에 대한 요구가 있을 것이다.

### 콘텐츠 복제방지 주요활동

디지털방송에서 복제방지가 이렇게 조미의 관심사이지만 아직도 이 분야에 대한 대비가 국내에서는 거의 없는 형편이다. 이 분야를 전담해서 표준을 정하려는 움직임도 아직은 없다.

유럽에서는 디지털방송에 대비해 ACTS의 일환으로 TALISMAN이라는 프로젝트를 수행한 바 있다. 이 프로젝트는 유럽연합 서비스 제공자에게 대규모 상업적 해적행위와 불법복제로부터 디지털 상품을 보호할 수 있는 표준 저작권 메커니즘을 제공하는 것이 목표였다. 디지털 형태로 저장된 정보가 증가하고 새로운 미디어 방송 서비스가 개발되면서 보안 솔루션에 대한 요구가 매우 시급해졌다.

새로운 서비스의 수용 여부는 정보제공자의 이익을 보호할 수 있는 적절한 기술의 가용성에 따라 달라진다. 디지털 형태로 저장된 데이터의 저작권 보호를 어떻게 실현할 것인지에 대한 해답은 아직 찾지 못했다.

그래서 비디오 콘텐츠 보호용 계층적 솔루션을 만들기 위해 제작자 단체, 콘텐츠 제공자, 방송사업자의 요구사항에 기반을 두고 진화하는 개방형 프레임워크를 개발하려는 것이 TALISMAN 프로젝트의 목표가 되었다.

솔루션의 종류는 다양해서 비트 스트림 헤더에 정보를 심는 방식에서부터 워터마크처럼 제거되지 않고 콘텐츠에 파묻은 정보를 이용하는 방법까지 다양하다. 이런 기술을 활용하는 하드웨어를 적절한 가격에 구입할 수 있게 하기 위한 조치들도 강구했다.

유럽에서는 그 이후로도 OCTALIS 등 다양한 프로젝트가 이어져 최근의 OCCAM까지 유럽연합 프로젝트가 이어지고 있다.

다른 한편에서는 오디오의 복제방지를 위한 기술이 개발되었다. 레코드나 테이프의 아날로그 매체 이후 디지털 시대로 넘어가면서 디지털 오디오 테이프 DAT가 출현했다. 불행하게도 DAT는 시장 진입에 실패했다. 주된 이유는 복제

방지에 대한 충분한 대비책을 마련하지 못했기 때문이다.

CD가 DAT 뒤를 이었는데, 같은 디지털 매체이면서도 CD는 시장진입에 성공해 레코드를 몰아냈다. 그 이유는 CD 복제가 비교적 어려웠기 때문이다. CD를 복제하려면 CD-R이 필요했으나, 당시 가격이 비싸 아무나 그것을 살 수 없었기 때문이다. 그런데 지금은 CD-R이 대중화됨에 따라 누구나 하나씩 가질 수 있게 되었다. 이제는 CD도 불법복제 위협을 받고 있다.

그런데 CD 시장에서 더 위협적인 존재는 MP3 압축 기술이다. MP3로 압축하면 용량은 10배 이상 줄어들면서 음악 품질은 거의 훼손되지 않는다. 게다가 인터넷의 급속한 발전으로 세계 구석구석이 거미줄처럼 연결되고 ADSL과 같이 전송용량이 큰 모델이 속속 개발되면서 불법복제는 콘텐츠 업자에게 치명적 위협을 가하고 있다.

멀티미디어 시대를 앞당긴 것은 압축기술 덕분이라고 해도 과언이 아니다. 그런데 불법복제가 기승을 부리도록 한 것도 압축기술 때문이라니 아이러니가 아닐 수 없다. CD 수준의 곡을 10배 이상 압축하면 저장용량도 10배 줄고, 전송 속도도 10배 빠르다. 그러나 불법복제 유혹도 그 정도로 커진다 할 수 있다.

특히 DVD는 CD보다 용량이 더 크기 때문에 고화질의 영화도 저장할 수 있다. 그렇지만 비디오는 압축했음에도 불구하고 800 MB 이상의 용량을 지닌다. 대역용량이 1 Mbps 정도의 고속 모뎀으로도 6,400초가 걸린다. 아직도 전송시간이 길다. 그래서 비디오가 오디오에 비해 덜 위협적이다. 그렇지만 최근 DivX의 출현으로 이야기가 달라지기 시작했다.

아무튼 DVD 보호 분야의 기수는 소위 5C이다. 5개의 회사가 모였어서 5C인데 그 멤버는 히타치, 인텔, 마쓰시다, 소니, 도시바. 5C는 DVD를 보호하기 위해 CSS라는 기술을 개발했다. CSS는 복제방지 기술의 교과서다. 그런데 최근 CSS 기술을 무력화시킬 수 있는 DeCSS가 출현하면서 복제방지에는 역시 영원한 승자가 없다는 것을 확인시켜 주었다.

### SDMI

1998년 미국 음반시장에 비상이 걸렸다. 미국음반협회 RIAA가 음반판매량을 조사해보니 젊은 고객층 중심으로 판매량이 격감한 것이다. 그 원인을 추정해 본 결과 MP3 플레이어 출현이 주범이라는 결론에 이르렀다. MP3 플레이어 메이커를 상대로 RIAA가 소송을 걸었으나 결과는 RIAA의 패소로 끝났다. 기존의 아날로그 시대 법률 관점에서 볼 때 디지털 복제는 불법이 아니라는 것이 판결의 요지였다.

이로 인해 위협을 느낀 미국, 일본, 독일의 음반협회들이 뭉쳤다. 98년 12월 이들은 기술인력을 모아 황급히 SDMI를 결성하고 불법복제에 대한 대비책을 마련하기 시작했다. 만일 이를 좌시한다면 음반 제작업계는 몰락할 수 밖에 없고,

연쇄적으로 아티스트에게도 치명적인 타격을 줄 것이며, 결국 그 피해는 좋은 음악을 듣고 싶어하는 고객에게 돌아갈 것이라는 절박감 때문이었다.

SDMI에 내노라 하는 업체는 다 회원사로 가입했다. 음반회사를 안심시킬 수 있는 기술적 조치를 마련하면 원음을 제공하겠다는 것이다. 그 결과 스크램블링, 디지털 서명, 디지털 워터마크 등이 제안되었다. 앞으로 어떤 기상천외한 기술이 나오지 모르겠지만 현재 기술만으로 복제방지를 원천적으로 봉쇄하기는 어렵다. 공격자도 내노라 하는 전문가들이기 때문이다.

그래서 RIAA가 복제방지 기술을 꾸준히 개발하면서 한편으로는 법정싸움을 병행하고 있다. 최근 MP3.COM이나 NAPSTER.COM을 제소한 것이 좋은 예이다. 이런 일련의 과정을 통해 추구하는 목표는 단 하나다. 바로 "선량한 사람을 선량한 사람으로 남게 한다 (Keep honest people honest)"는 것.

아무리 기술을 개발하고 법적 소송을 벌여도 해적은 근절할 수 없으니 제돈 내고 사는 사람의 수를 늘리는 수밖에 없다는 것이 결론이다. 그러자면 고객을 고대한 인격자나 부자로 만들어야 한다. 그렇지만 음반협회가 그런 일을 할 수는 없다. 그래서 우선 복제를 기술적으로 매우 어렵게 만들고, 그럼에도 불구하고 불법이 저질러지면 법률을 동원하겠다는 것이다. 그래서 많은 해적 후보들을 미수범으로 만들겠다는 것이 그들의 계산이다.

SDMI가 1999년 페이스 1 워터마크를 선정했는데 여기서 Ars Technologies의 워터마크가 채택되었다. 그런데 2000년 들어 다시 페이스 2 워터마크를 선정하기 위한 작업이 진행되고 있다. 여기에 국내에서는 실트로닉과 마크에니가 각각 워터마크를 제안한 바 있다.

현재 마지막까지 남아 평가를 받고 있는 것은 압축 여부를 알아낼 수 있게 설계된 네 종류의 워터마크와 특정 환경에서는 원본 CD가 없을 때 앨범의 개별 트랙을 전송할 수 없게 하는 두 종류의 별도 기술이 포함되어 있다.

이들 기술은 <http://www.hacksdmi.org>에서 공개적으로 테스트를 받았다. 이 일이 앞으로 복제방지 기술 개발에 참조모델로 사용될 가능성이 있다. 객관적 평가를 위해 평가기준을 정하지만 중요한 것은 해커들의 공격에 살아남는지 보이는 것이 더 바람직할 수도 있다는 점이다.

SDMI는 앞으로도 오랜 기간 활동할 것으로 보인다. 그런데 SDMI의 규격화 작업에 대한 시장의 반응은 다양하다. SDMI의 규격을 따르는 것이 반드시 필요하다는 주장도 있다. SDMI는 다양한 시장의 요구를 다 반영하려 해서 오히려 업체가 수용할 수 없는 규격을 만들고 있다는 비난도 있다. 어찌 되었든 SDMI 규격은 자발적 규격 (Voluntary Spec) 이상도 이하도 아니다. 다시 말해 강제규정이 아니기 때문에 지켜도 그만이고 지키지 않아도 그만이다.

SDMI 규격의 핵심은 결코 워터마크가 아니다. 그럼에도 불구하고 한국에서 두 회사가 페이스 2 워터마크를 제안하면서 마치 SDMI는 워터마크만 다루는 기구처럼 인식되어 버렸는데 실제로는 복제방지를 위한 다양한 솔루션을 규격화하고 개발하는데 앞장서고 있다.

## 국제표준

복제방지에 눈을 돌린 최초의 국제표준이 MPEG IPMP이다. IPMP는 사용규정 (Usage Rule) 개념과 IPMP API에 대해 논의했다. 암호 방식의 다양성을 인정해 구현방법은 규격에 규정하지 않고, 호환성을 위해 인터페이스만 정했다. MPEG에서도 반드시 IPMP를 채택해야 한다는 강제규정은 없다.

IPMP는 암호엔진을 말한다. 구현은 알아서 하라고 했기 때문에 얼마나 많은 IPMP 엔진이 존재할 지 알 수 없는 일이다. 서로 다른 IPMP들끼리 대화는 가능하다. API를 공유하기 때문이다. 그러나 단말을 만드는 사람 입장에서는 여간 골치 아프지 않다. 수많은 IPMP를 제한된 단말에 다 구현할 수 없기 때문이다.

이런 문제를 해결한 것이 바로 OPIMA VM이다. SDMI의 LCM도 마찬가지이다. OPIMA VM이나 SDMI LCM은 서로 다른 IPMP 엔진 사이의 통역을 담당한다.

현재 OPIMA는 표준화활동이 잠정적으로 중단된 상태이다. SDMI는 주로 디지털 뮤직 규격화에 앞장서고 있다. MPEG-4에서부터는 IPMP가 중요한 이유로 부상해서 MPEG-21에서는 가장 중요한 이슈 가운데 하나가 되었다.

이 가운데 주목할 필요가 있는 것은 OPIMA와 MPEG-21이다. OPIMA는 차세대 복제방지 솔루션이 될 가능성이 충분히 있다. 2년 넘게 전문가들이 논의해서 만든 규격을 바탕으로 현재 유럽연합에서 OCCAMM이라는 프로젝트를 통해 OPIMA VM을 개발하고 있다. OCCAMM에는 여러 기관이 참여하고 있으나 가장 핵심멤버는 필립스이다. MPEG-21은 기존의 MPEG-4 IPMP, MPEG-7 IPMP 이후 새로운 멀티미디어 프레임워크에 걸맞는 새로운 솔루션을 찾고 있다.

다양한 국제활동이 이루어지고 있기는 하지만 여전히 복제방지에 대한 논란은 끊이지 않고 있다. 카피라이트와 카피레프트 논쟁도 그렇고, 완벽한 복제방지가 현재로는 어려운 것도 해결해야 할 과제이다. 그래서 방송에 대한 논의는 한 발짝도 진전되지 않고 있는 양상이다.

방송과 관련된 표준은 ATSC나 DVB에서 정하고 있다. 그러나 이들은 주로 제한접근 기술인 CA에 한정되고 있다. 예를 들면 ATSC 문서 A/70이 좋은 예이다. 그러나 CA는 방송접근을 제한할 뿐이지 수신한 콘텐츠의 불법복제를 막는 기술은 아니다. 이런 점에서 콘텐츠 불법복제를 방지할 표준이 필요하다는 것이다.

## 국내표준

국내에서는 DMC가 최초로 표준과 관련된 활동을 하기 위해 회원을 규합하고 몇 차례 모임을 가졌으나 주로 정지 작업을 하는 선에서 막을 내렸다. 처음에는 MP3 단말을 만드는 업체에게 SDMI 동향을 소개하고 대응책을 마련하며 우선 내수시장을 여는 방법을 모색했다. 그러나 권리단체에 대한 난맥상으로 인해 좌절을 맛보고 말았다. 또 SDMI가 지지부진한 진도를 보인 것도 중요한 걸림돌이었다. 그렇지만 DMC의 노력을 과소평가해서는 곤란하다. DMC는 IPMP의 중요성을 각인시키는 일에 큰 기여를 했다.

산업자원부가 나서 이 분야 표준을 주도하기 위해 SDM-WG를 설립했다. 주축은 DMC 연장선상에 있지만 시범사업을 통해 표준화를 달성한다는 새로운 접근법을 채택하고 있다. 시장에서 막강한 영향력을 행사할 수 있는 가수를 동원해서 신곡을 MP3로만 우선 판매하겠다는 것이다. 곡에는 일련번호를 워터마크로 삽입한 다음 스크램블링 기술을 걸어 시장에 내보내겠다는 것이다. 이러한 온라인 판매방식이 시범사업의 골자이지만 이를 통해 DRM 기술과 워터마크 기술의 표준을 정하고 비즈니스 모델을 파악하겠다는 내부 목표를 정했다. 이를 통해 자연스럽게 국내시장의 사실상 표준이 정해질 것이며 국내 기술시장 보호가 가능하다는 낙관적 견해를 가지고 시범사업을 추진하고 있다.

한편 대한전자공학회 산하에 멀티미디어콘텐츠보호기술 규격위원회가 설립되었다. 국내의 표준이나 규격을 정하는 일에 중립적인 기관이 필요하다는 것이 위원회의 출발 동기이다. 이 분야는 업무영역으로 볼 때 문화관광부, 산업자원부, 정보통신부가 협력해야 할 부분이 많다. 이 위원회는 부처간 영역 다툼이 예상되는 것을 조정하고 기술적 해석 내지 조언을 제공하며 규격 정비에 일조를 하겠다는 원칙을 가지고 있다. MPEG-21에 대비하기 위해 정부 지원책이 준비되고 있다. 여기서 MPEG-21의 한 분야인 IPMP 기술개발이 이루어질 것으로 보인다. 아마도 이 지원책에 방송용 IPMP 기술개발이 포함되어야 할 것으로 본다.

## 맺음말

디지털방송 환경에 어울리는 복제방지 기술이 절실히 요

## 약어 표

AAC	Advanced Audio Coding
CA	Conditional Access
CSS	Content Scrambling System
CD	Compact Disc
CD-R	Compact Disc Recorder
DMC	Digital Music Consortium
DTCP	Digital Transmission Content Protection
DVD	Digital Versatile Disk
DVD-R	Digital Versatile Disk-Recorder
HDTV	High-Definition TV
IPCTV	Intelligent PC/TV
IPMP	Intellectual Property Management and Protection
LCM	Licensed Compliant Module
MPEG	Moving Picture Expert Group
MP3	MPEG Layer-3
OPIMA	Open Platform Initiative for Multimedia Access
OPIMA VM	OPIMA Virtual Machine
P2P	Peer-to-Peer
RIAA	Recording Industry Associations of America
SDMI	Secure Digital Music Initiative
SDM-WG	Secure Digital Multimedia Working Group
5C	Hitachi, Intel, Matsushita, Sony, Toshiba

구되지만 방송과 관련된 표준에 대해 거의 논의되지 않고 있어 매우 안타깝다. 국내에서도 시급히 이에 대한 대비책을 서둘러 논의하는 마당이 마련되어야 할 것으로 보인다. 선행 기술개발을 통해 방송에서의 경쟁력을 확보할 수 있는 절호의 기회를 잡을 수도 있는 시점에 우리가 놓여있다. 한국은 HDTV 과제 및 IPCTV 과제를 통해 우수한 방송기술력을 확보했기 때문에 복제방지 기술을 앞서 개발한다면 명실상부한 방송기술 선진국으로 나아갈 수도 있다. 2000년부터 시작되는 산업자원부 중기거점과제 IMS 프로젝트에서도 IPMP 개발이 이루어질 것으로 예상하고 있다. 현재 진행되고 있는 MPEG-21과 SDMI의 동향은 어떤 형태로든 방송에도 일부 영향을 미칠 것으로 보인다.

IPMP 분야에서 가장 충격적인 사건은 넵스터의 등장이라고 할 수 있다. 누구도 예상하지 못했던 넵스터의 P2P 기술은 디지털 콘텐츠 복제방지 기술 개발의 앞날이 얼마나 험난하며 기발한 발상전환을 요구하는지 짐작케 한다. 그래서 MPEG-21도 디지털 시대에 걸맞는 새로운 복제방지 기술을 간절히 고대하고 있다.

## 필자소개



### 김형중

- 1978년 서울대 전기공학과 졸업
- 1989년 서울대학교 제어계측공학과 공학박사
- 1992년~1993년 USC 방문교수
- 현 재 강원대학교 제어계측공학과 교수, OPIMA 및 MPEG 회원,  
대화형 디지털TV "IPCTV" 개발 총괄책임자, SDM-WG 기술규격위원회 위원장