디지털 워터마킹 기술동향 및 전망

The Trend of Digital Watermarking Technology for Digital Rights Management

오병택(B.T. Oh) 정보유통연구팀 연구원
문병주(B.J. Moon) 정보유통연구팀 선임연구원, 팀장
이동일(D.I. Lee) 정보유통연구팀 책임연구원

최근 인터넷 환경의 빠른 성장과 함께 더욱 다양하고 많은 콘텐츠들이 개발되고 있다. 반면에 디지털 데이터의 특성상 복제가 쉽고 또한, 불법적으로 복제된 콘텐츠가 인터넷을 통해 빠르게 배포되고 있다. 이에 멀티미디어 데이터에 대한 소유권 문제와 이를 효율적으로 보호하고, 디지털화된 콘텐츠의 불법 복제를 제한하기 위한 방법이 요구되고 있다. 본 고에서는 워터마크 기술이란 어떤 것이며 이와 관련된 국내외의 기술동향과 전망에 대해서 알아본다.

I. 서 론

인터넷과 멀티미디어 기술의 급속한 발전으로 디지털 콘텐츠(digital contents)의 제작 및 유통에 대한 사회적 요구가 증가함에 따라 콘텐츠 저작자의 저작권 보호에 대한 요청이 날로 증가하고 있으며, 디지털 콘텐츠의 불법복제 및 유통을 방지하기 위해 멀티미디어 저작물의 저작권을 보호하기 위한 기술이 연구되고 있다.

그 중 워터마크(watermark) 기술은 디지털 콘텐츠의 저작권 보호를 목적으로 사람의 눈이나 귀를 통해 쉽게 감지하기 어렵게 디지털 이미지, 오디오, 비디오 신호에 저작권 정보를 삽입하여 멀티미디어 데이터에 대한 소유권을 보호할 수 있으며 무분별한 데이터의 불법 복제도 방지할 수 있는 기술로 알려져 있다.

본 고에서는 워터마크 기술이란 어떤 것이며 이와 관련된 국내외의 기술동향과 전망에 대해서 알아보고자 한다.

II. 워터마크 기술의 분류

1. 활용도에 따른 분류

디지털 워터마킹(digital watermarking) 기술은 용도에 따라 크게 강성(robust), 연성(fragile), 핑거프린팅(fingerprinting), 스테가노그래피(steganography) 등 네 가지로 분류할 수 있으며, 이들 중 가장 기본적인 기술은 강성 워터마킹 기술이다(<표 1> 참조).

강성 워터마킹 기술은 특정인이 콘텐츠를 불법으로 이용할 목적으로 워터마크를 고의로 훼손하거나 변형하려는 시도를 막는 데 사용되는 기술이며, 이를 위해서 원본 워터마킹을 변조하려는 외부의 시도가 있을 때 데이터의 품질이 심각하게 훼손되기 전에는 워터마크가 깨지지 않도록 설계한 워터마킹 기술이다.

강성 워터마킹 기법을 활용하면 각종 민원 서류를 포함한 다양한 증명서의 온라인 발급 업무도 가능해질 뿐 아니라, 인터넷 서명의 복제나 위조로 인한 사고를 사전에 막을 수도 있다. 또한 각종 온라인

티켓이나 상품권 등으로 적용 범위를 확장할 경우 다양한 실시간 인증 처리에도 이용될 수 있을 것으로 기대된다.

연성 워터마킹 개념은 병원의 임상 사진 이미지나 관공서의 문서, 군사 기밀 문서 등의 원본 텍스트와 같이 파일의 외부 유출을 막아야 하는 경우에 사용된다. 즉 데이터에 변형을 가하면 쉽게 워터마크가 깨지면서 원본 콘텐츠도 동시에 훼손되도록 설계한 워터마킹으로, 변형여부를 검사하여 인증과 무결성을 제공하기 위한 방법으로 사용된다.

핑거프린팅은 현재 사용되고 있는 '바코드'와 유사한 개념으로, 고유번호나 식별자를 콘텐츠에 삽입하는 것이다. 이 기술을 적용하면 누구에게 배포되었는지 알 수 있으므로 물류 사업에서 제품을 분류하는 데 활용되거나 전송 경로를 확인할 수 있다. 또한 불법적인 유통이 이루어질 경우 배포자를 추적할 수 있다[1].

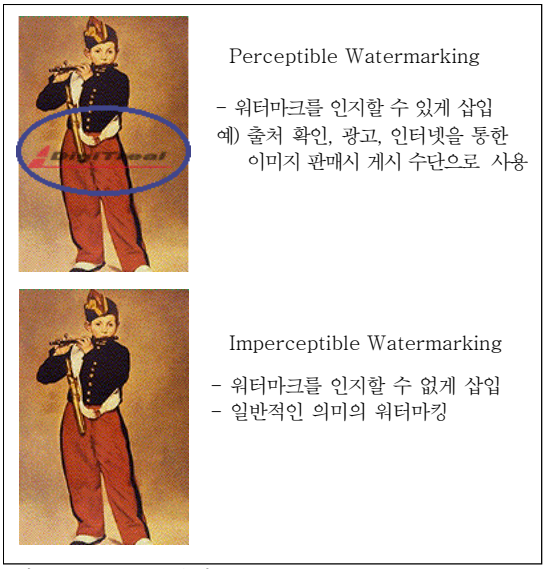
<표 1> 워터마크 기술의 용도에 따른 분류

강성(robust) 워터마킹	• 원본 이미지에 저작자 고유의 표식으로 워터마크를 삽입하여 저작권 증명 및 보호에 사용 • 삽입된 워터마크를 지우거나 무력화 시키려는 공격에 견딜 수 있는 내성(robustness)이 가장 중요 • 현 모든 공격에 대해 강성을 제공하기는 어려움
연성(fragile) 워터마킹	• 원본과 조금이라도 다르면 워터마크가 깨어지며 원본 이미지가 손상되게 설계 • 강성 워터마킹 기술과는 반대로 워터마크가 얼마나 잘 깨어질 수 있느냐가 척도가 됨 • 복제되어서는 안되는 데이터의 보호를 위해서 유용하게 사용됨 • 은행이나 관공서의 문서, 법률 문서, 병원의 각종 임상 사진 등의 '원본 보호 및 증명'에 많이 사용됨
핑거프린팅 (fingerprinting)	• '지문'과 같은 고유한 정보를 파일에 삽입하고, 그 삽입된 정보를 다양하게 활용할 수 있도록 함 • 바 코드(bar code) 대체, 정보의 전송 경로/배포 경로 확인, 물류 사업에서 제품의 분류작업에도 이용 가능
스테가노그래피 (steganography)	• 정보를 은닉하거나 다른 형태로 위장하여 주고 받을 수 있게 하는 기능을 가지며 주로 군사적인 목적으로 쓰임 • 암호화(encryption) 형태보다 한층 진보된 '암호 통신' 예) 중요한 암호나 비밀 문서를 음악 파일의 형태로 위장하여 아군에게 전달

스테가노그래피는 '감추어져 있다'는 뜻의 그리스어인 'stergano'와 '통신하다'라는 뜻의 'graphos'가 결합된 용어로, 정보를 숨기거나 다른 형태로 위장하여 주고받을 때 사용할 수 있는 일종의 '암호통신'기술이다. 음악 파일을 문서 파일처럼 가장할 수 있음은 물론, 그림 파일 속에 음악 파일을 은닉하는 것도 가능하다.

2. 워터마킹의 인지가능 여부에 따른 분류

워터마킹 기술은 가시성에 따라 (그림 1)에서와 같이 인지할 수 있는 워터마킹(perceptible watermarking)과 인지할 수 없는 워터마킹(imperceptible watermarking)으로 분류할 수 있다. 인지할 수 없는 워터마킹은 원저작물에 워터마킹이 나타나지 않게 하여 원저작물 자체를 훼손하지 않은 상태로 워터마킹을 삽입하여 저작권을 보호할 수 있는 방법이다. 현재 빠른 속도로 증가하고 있는 멀티미디어 저작물들과 저작권을 동시에 보호하기 위해 저작물 원상태를 거의 훼손하지 않고 워터마크를 삽입하여 저작권을 보호할 수 있는 기술로 활발한 연구가 진행되고 있다. 일반적인 의미의 워터마킹은 인지할 수 없는 워터마크를 삽입하는 것을 말한다.



<자료>: DigiTreal, 수정

(그림 1) 인지가능 여부에 따른 분류

III. 워터마킹 기술

1. 워터마킹 기술 적용분야

워터마킹 기술을 구현하기 위해 워터마킹 기술을 단독으로 사용한 경우도 있으며, 다른 기술과의 접목으로 구현하는 방법들도 있는데 현재까지 잘 알려진 적용분야의 예로는 다음과 같은 것들이 있다[2],[3].

가. 저작권 주장

디지털 콘텐츠의 소유관계를 주장하기 위한 방법으로 콘텐츠에 워터마크를 삽입하는 것이다. 먼저 콘텐츠를 만드는 저작자는 프로그램을 사용해서 워터마크를 생성한 뒤 그것을 원본 콘텐츠에 삽입한다. 그런 뒤 저작자는 워터마크가 삽입된 이미지를 공개한다. 워터마크가 가시적으로 나타난 경우는 다른 사람들이 이것을 보고 복사하지 않을 것이고, 비가시적인 경우는 다른 사람이 콘텐츠의 소유를 주장하면 원래 콘텐츠를 생성한 저작자는 소유를 주장하는 사람의 이미지에 자신이 삽입한 워터마크가 있음을 보여주어 자신의 소유권을 증명하면 되는 것이다. 하지만 이런 방법이 동작하기 위해서는 이미지에 대한 압축, 확대, 축소 등과 같은 연산을 수행해도 워터마크가 없어지지 않고 남아 있어야 한다.

이 기술은 텍스트, 오디오파일, 비디오파일, 이미지파일, 벡터파일 등의 저작권 주장에 주로 사용된다.

나. 온라인상의 콘텐츠 위변조 판별

보통 연성 워터마킹 기술을 이용하며 온라인이나 오프라인 상에서 편집이나 수정시, 워터마킹된 부분이 깨지게 되므로 이를 통해 문서의 진위여부를 판별하는 것이다. 예를 들면 다른 사람이 워터마킹이 된 문서를 사용하여 일부를 수정한 후에 이를 사용하려고 할 때 원 저작권자는 이 파일을 검사하여 이 파일이 원본인지 아니면 변조된 것인지 확인한다.

주로 온라인 티켓, 보험증서, 성적증명서, 의료기록 등 온라인 혹은 오프라인상으로 전송되는 파일들의 위변조 확인에 활용된다.

다. 무단 배포 방지(복사 제어)

워터마킹 기술을 사용해서 콘텐츠에 대한 추가적인 정보를 제공하는 것이다. 한 예로 이미지를 만드는 경우 이 이미지가 만들어진 시간, 창작자 등과 같은 정보나 복사된 것이라는 표시를 워터마크로 만들어서 이미지에 삽입한다.

주로 각종 서류나 문서, 유가증권 등의 복사기를 통한 복사방지에 적용된다.

라. 사용자 제어

멀티미디어 콘텐츠를 복사하거나 재생하는 데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 콘텐츠에 삽입되어 콘텐츠를 복사할 수 있는 횟수 등을 제어하는 데 사용하는 것이다. 이 방법의 경우 복사를 할 때마다 하드웨어가 워터마크를 수정하게 되므로 어느 제한 이상 복사할 수 없게 된다.

활용분야로는 온라인 티켓, 성적증명서, 주민등록 등본 등의 전자문서 발급시 횟수제한 등이 있다.

마. 기타

이 밖에도 여권이나 주민등록증의 사용자 신원카드에 내재된 워터마킹을 인식하여 신원확인을 하거나, 인증을 하는 경우, 혹은 저작권 정보의 추적기술, 장치의 사용권 제한 등 여러 분야에 사용될 수가 있다. 이 외에도 응용방법에 따라 그 활용분야와 파생범위는 확대될 것이다.

2. 워터마킹 공격 방법

워터마킹을 무효화 시키는 공격 기술에는 rotation, scale, translation, JPEG(MPEG) compression 등과 같은 기본적인 신호처리부터 복합적인 기술 등 여러 가지 공격기술이 있으며[3], Anti-watermarking 제품(StirMark, UnZign 등)에 이와 같은 공격 기능들이 포함되어 있다.

Digimarc사의 경우(PictureMarc, Media Commerce) 이들 공격에 의해 상당한 타격을 입은 경우

가 있으며, 공격 기술은 워터마킹 기술의 시험, 평가에도 사용되고 있고, 다양한 공격에 대한 강성이 기술의 척도로 자리 잡는 계기를 마련하고 있다.

본 장에서는 대표적인 공격 기술에 대해서 알아보고자 한다[4].

가. Filtering Attack

실제 많은 워터마크 신호는 spread spectrum 기술을 이용하여 노이즈(noise)와 비슷한 형태를 띈다. Filtering attack은 lowpass filtering으로 노이즈를 없애듯이 워터마크 정보를 없애는 공격 방법이며, 간단한 lowpass filter에서부터 wiener filter까지 다양한 방법들이 사용된다.

Wiener filter 방법에 대한 해결책은 워터마킹의 power spectrum이 cover signal의 power spectrum과 상수와의 곱이 될 때 가장 안전하게 된다고 한다. 또 다른 공격으로 median filtering이 있는데, 이 역시 노이즈를 없애는 데 많이 사용되며, 워터마크 정보를 무력화시키긴 하지만 콘텐츠의 품질이 떨어지는 결과를 얻는다.

나. Copy Attack

워터마크가 삽입된 신호에서 wiener filtering과 같은 방법을 통해 삽입된 워터마크를 측정하고, 측정된 워터마크를 워터마킹 되지 않은 임의의 신호에 더함으로써 워터마크 검출기(watermark detector)가 자신이 마크한 신호가 아닌 신호에서도 워터마크를 검출할 수 있게 하여 가성 양성률(false positive rate)을 높이는 기술이며, 애플리케이션에 따라 매우 심각한 타격을 받을 수 있다. 해결책으로 또 하나의 워터마크를 삽입한 것과 원 신호에 의존적인 워터마크를 삽입하는 방법이 있지만, 무엇보다 워터마크가 쉽게 측정되지 않게 하는 것이 우선일 것이다.

다. Mosaic Attack

워터마크가 검출되기 전에 먼저 워터마크된 신호를 워터마크가 검출되지 않을 정도로 작게 조각낸 후, 검출기를 지난 후에 다시 조각을 맞추는 방법이다. 이는 워터마킹이 일정 크기 이상의 신호를 요구하는 특성을 역으로 이용한 것이다. 하지만, 이미 프린트된 이미지의 경우에는 적용할 수 없는 방법이다.

라. IBM Attack

SWICO(Single Watermarked Image Counterfeit Original) attack으로도 불리워지는 공격인데, 타인 소유의 워터마크가 삽입된 이미지나 오디오에 랜덤 노이즈(random noise)와 비슷한 자신의 워터마크를 삽입하여, 각자의 검출기에서 각자의 워터마크를 검출할 수 있게 하여 소유권 분쟁을 일으키는 방법이다. 양자 모두 자신의 워터마크를 검출할 수 있는데 이 방법은 구현하기가 매우 쉬우며, 이에 대한 완벽한 해결책을 찾기는 쉽지 않다.

마. Template Attack

일종의 synchronization attack이다. 많은 워터마킹 기술들이 관계 변환(affine transformation) 과정에도 불구하고 워터마크를 검출할 수 있도록 하기 위해 메시지 외에도 기준으로 삼는 패턴을 삽입하는데, 이 공격은 그러한 패턴을 파괴함으로써 검출기를 혼란시켜 워터마크 검출을 불가능하게 하는 방법이다. 삽입 과정에 대한 약간의 정보만으로도 패턴을 찾을 수 있으며 다른 패턴을 추가하여 혼란을 일으키든지, 또는 기존의 패턴을 약화시켜 워터마크를 검출하지 못하게 할 수 있는 것이 현실이다. 물론 결과 신호의 품질은 패턴 측정의 정확도와 삽입된 워터마크의 강도에 따라 달라진다.

3. 벤치마킹 툴

가. Stirmark

이미지 워터마킹 기술의 강성을 테스트하기 위해 1997년 11월에 버전 1.0이 개발되었으며, 간단한

기하학적 변환(simple geometric transformations)으로 이미지 크기변환(scaling), 자르기(cropping), 회전(rotations), X/Y-절단(X/Y-shearing), 컬럼, 라인 제거(column & line removal)와 함께 압축(compression) 등의 과정을 통해 워터마킹 기술의 내성을 측정하는 툴이다. 현재는 Stirmark 4.0 version이 공개되어 있다.

나. Checkmark
(http://watermarking.unige.ch/Checkmark/)

Stirmark 보다는 좀더 향상된 이미지 워터마킹 벤치마킹 툴이다. Wavelet-based compression, 복사 공격(copy attack), 템플릿 제거 공격(template removal attack) 등이 포함되어 있으며, 이미지 품질을 측정하는 metric도 포함되어 있어 좀더 객관적인 평가를 할 수 있게 하였다. 유럽의 DCT 사와 University of Geneva 그룹의 멤버들이 개발하였으며, 2001년 12월에 Checkmark 1.2 version이 공개되었다.

다. CertiMark(www.certimark.org)

European project에서 대학 및 산업체 15개가 참가하여 2000년 5월에 디지털 워터마킹의 벤치마킹을 위한 CertiMark(CERTIfication for water-MARKing technology) 프로젝트를 출범하였다. 이의 주된 목적은 디지털 워터마킹 기술에 적합한 벤치마크를 설계하고 개발하여 디지털 워터마킹 전문가 및 기관에 제공하는 것이다.

4. 디지털 워터마크 관련 시장동향

국내 디지털 콘텐츠 산업은 2000년 이후 연평균 50% 이상의 높은 성장률을 보이면서 2005년 약 33억 달러 이상의 생산규모를 형성할 것으로 예상된다(자료: 한국소프트웨어진흥원).

정보 보안 시장도 더불어 매년 50% 이상 고속 성장하고 있고 향후에는 저작권 보호 관련 시장 추세와 비슷할 것으로 예상되고 있으며, 디지털 워터마크 관련 회사인 Digimarc의 매출은 매년 100~200% 이상 고속 성장하고 있다.

디지털 워터마크 관련 시장이 성장하면서 새로운 파생 시장으로 인터넷 우표 사업(2000년 세계 시장 규모 총 2억 달러, 2003년 6억 달러, 자료: IDC), 인터넷 이미지 판매 사업, 인터넷 티켓 판매 사업, 문서 보안 관련 사업 등이 창출되고 있다.

5. 국내외 제품동향

이렇게 다양한 워터마킹에 대한 기술개발과 상품화는 국내외 기업들에 의해 시도되고 있으며 이러한 회사의 제품을 통해 워터마킹에 대한 현재의 기술동향을 평가할 수 있을 것이다. 여기서는 국내외 대표적인 회사들과 이들이 현재 출시한 제품들을 설명하도록 하겠다.

가. 국내의 제품 동향

1) 마크애니(MarkAny, http://www.markany.com)

1999년 2월 상명대 최종욱교수가 설립한 트러스텍이라는 회사로 출발하였다. 현재 국내 28건, 국제 8건의 특허를 기초로 각종 워터마킹 제품을 출시하고 있다. 국내회사로 유일하게 STEP2000에서 5개 업체 중 2위(1위는 IBM), SDMI phase 1에서 4개 업체 중 하나로 선정된 바 있다[2]. 마크애니는 SDMI 4강에 진출하였으며 STEP 2001에서도 다시 선정되었다. 주요제품으로는 MAVI(비디오 워터마킹) MAO(오디오 워터마킹), MAIM(이미지 워터마킹), MAVEC(벡터 워터마킹), Document SAFER, Content SAFER, Web SAFER 등이 있다.

2) 실트로닉(http://www.sealtronic.com)

1999년 9월 설립한 회사로 자체개발기술과 ETRI(한국전자통신연구원)의 기술과 출원된 특허를 토대로 워터마킹 솔루션을 내놓고 있다. 워터마크 알고리듬을 이용한 멀티미디어 콘텐츠의 저작권 보호 솔루션으로 RIGHTS@fer Multimedia, Magi-Check, Magic tag가 출시되어 있다.

3) 디지트리얼(http://www.digitreal.com)

1997년 (주)한국메디컴시스템이라는 의료관련 솔루션제공업체로 출발하여 2000년 3월 국내출원 중인 특허 "저작권 보호를 위한 비가시성 디지털 직인 삽입 방법"을 기초로 2001년 2월 키워드 방식의 디지털 이미지 워터마킹 솔루션 WaterStamp Version 1.0(일반용)을 내놓았으며 현재는 WaterStamp Version 3.0, WaterStamp-Print, WS-DVR 등의 제품이 출시되고 있다.

4) 콘텐츠 코리아(http://www.contents.co.kr)

1997년 1월 인포머셜컨설팅이라는 회사로 출발하여 주로 콘텐츠 관련사업과 이에 관련한 워터마킹 제품을 출시하고 있다. 주요 워터마킹 제품으로는 콘텐츠 가디언(contents guardian 1.0), 발권 시스템 등이 있는데 이는 디지털 콘텐츠 보호기술로서 암호화 알고리듬을 이용한 디지털 워터마킹 기술을 적용한 제품이다.

5) 디지털 이노텍
(http://www.digital-innotech.com)

KAIST 전산학과 교수인 이흥규 박사가 2000년 5월 설립하였으며 인터넷상에서 사용되는 각종 멀티미디어의 저작권보호를 위하여 설립된 연구개발 중심의 회사이며 일반 영상에 워터마크를 삽입하는 방식의 보안용 바코드 솔루션을 개발했다.

이흥규 박사는 현재 정보통신부, 한국전자통신연구원이 후원하는 'DRM 포럼 보호 기술분과위원장'으로 활동하고 있다.

나. 외국의 제품동향[2]

1) Digimarc(http://www.digimarc.com)

1996년 최초로 워터마킹 관련제품을 출시하였으며 20여 개가 넘는 특허를 출원하였다. 특히 이미지 워터마킹제품이 우수하다. Picture mark, Batch-marcpro, Mediabridge(이미지 워터마킹 응용), Mediaommerce(이미지, 음악, 비디오) 등을 내놓았다. 특히 이 회사는 Adobe사의 포토샵에 플러그인 형태로 제품을 제공하고 있으며 툴 키트도 제공하고 있다.

2) Verance(http://www.verance.com)

1999년 10월 Solena와 Aris와의 합병으로 설립된 회사로 주로 오디오 워터마킹 쪽에 강하다. Musicode, Mediacode 등을 출시하였으며 20여 개의 특허를 기초로 SDMI와 DVD 오디오 등의 표준화 작업에 참여하고 있다. 현재는 Verance audio watermark detector 등의 제품을 판매하고 있다.

3) Blue Spike(http://bluespike.com)

Step2000에서 5위를 하여 알려진 업체로 오디오 워터마킹에 강하다. 워터마킹 기술과 DRM 솔루션과의 연계제품을 내놓고 있다. 주요 제품으로는 Giovanni가 있다.

4) Signum Technologies
(www.signumtech.com)

1997년 7월 설립된 회사로 Suresign과 Veridata라고 하는 일련의 제품군을 판매하고 있다. 특히, 이 회사는 워터마크 관련 개발 툴 키트를 함께 판매하고 있다.

6. 워터마킹 관련 표준화 동향

이렇게 다양한 기술을 실제 적용 가능하게 하기 위해서는 무엇보다도 세계적으로 워터마크에 대한 표준화가 진행되어야 한다. 이러한 워터마크 기술의 표준화 작업은 MP3 등으로 막대한 피해를 입어 온 세계 주요 음반사들의 저작권을 보호하기 위한 노력으로 주로 오디오를 중심으로 진행되어 왔다.

세계적으로 추진되고 있는 표준화활동은 다음과 같다.

가. SDMI

SDMI(Secure Digital Music Initiative)는 세계 주요 음반 및 전자, 정보통신 분야의 175개 업체들이 1999년 2월 디지털 오디오 콘텐츠 보호를 위해 결성한 컨소시엄으로, 음악의 판권을 보호하고 불법 복제를 방지하기 위한 기술 개발을 목표로 하고 있다.

SDMI 프로젝트에는 BMG 뮤직, 소니뮤직, EMI, 워너뮤직, 유니버설뮤직 등 세계 5대 음반사들과 AT&T, IBM, 소니, 마쓰시타 등 세계적인 첨단 정보통신 업체들이 참여하고 있으며 주요 음반사들이 저작권 보호를 강화할 수 있는 새로운 방식의 표준안을 채택하기 위해 첨단 기술 업체들과 제휴해 만든 일종의 음반산업 자구책이라 할 수 있다. Phase 1에서는 4개사(Verance, CRL, Markany, Blue Spike)가 선정되었다. SDMI에서는 디지털 음악을 재생하는 휴대형 장치가 갖춰야 할 규격을 애플리케이션 레이어(application layer), 드라이버 또는 LCM(Licensed Compliant Module) 레이어, 휴대형 장치 레이어 등 세 가지 분야로 나누어 제시하고 있다.

나. STEP2000/STEP2001

STEP2000/2001은 디지털 워터마킹 기술을 기반으로 본격적인 디지털 음악 유통의 성공적인 실현을 위한 국제 평가 프로젝트로서 사단법인 일본 저작권 협회(JASRAC)와 국제 저작권 관리 단체 국제조직인 프랑스의 CISAC와 BIEM에 의해 실시되는 것으로 디지털 워터마킹 기술의 능력을 인정하고, 향후 기술의 이용 증진에 목적을 둔 프로젝트이다.

STEP2000 평가 결과로 IBM, 마그애니(한국), Victor Company of Japan, Signum, Blue Spike 등의 회사가 선정되었으며, 마크애니는 STEP2001에서도 선정되었다.

다. MPEG

여기에서의 MPEG(Motion Picture Expert Group)은 멀티미디어에 대한 사용자들의 다양한 요구를 충족시키기 위해 인터넷과 디지털 저장, 커뮤니케이션 등의 효율적 응용을 위해서 멀티미디어 소스에 대한 부호화 방법을 체계적으로 연구하고 표준화하기 위한 ISO/IEC의 기술자문위원회(Joint Technical Committee: JTC) 산하 전문가 그룹(SC29 WG11) 을 말한다. MPEG 표준화 작업은 MPEG1, MPEG2, MPEG4, MPEG7 및 MPEG21으로 진행중이며 현재 MPEG4와 MPEG7이 활발하게 활동중에 있다.

라. SEDICA

디지털 콘텐츠 보호, 관리를 위한 워터마킹 기술 및 DRM 기술 개발의 국제 선도적 역할을 하며, 디지털 워터마킹 기술 및 DRM 기술 관련 산학연 협력의 장을 마련하고, 디지털 워터마킹 기술 및 DRM 기술의 국제 표준화를 유도하기 위해서 한국의 정보통신부가 추진하는 국제적 협의회이다[5]. SEDICA(Secure DIgital Content Association)는 한국과학기술원 이흥규 교수와 동의대학교 이창열 교수가 중심이 되어 워터마킹 분과, DRM 분과, 국제추진분과, 산업응용분과로 나뉘어 기술기준 설정 및 관련산업 지원 등의 다양한 사업을 펼치고 있다.

Ⅳ. 결론 및 향후 연구전망

디지털 워터마킹 기술은 초기에는 간단한 방법으로 저작권을 보호할 수 있는 기술로 관심을 받으면서 급격한 기술적 발전이 이루어졌으며, 워터마크의 강인성에 대한 체계적인 벤치마크 테스트를 수행하기 위해 워터마크 공격기법에 대한 연구도 병행하여 활발히 진행되고 있다. 디지털 워터마크 관련 시장이 성장하면서 인터넷 우표 사업, 인터넷 티켓 판매와 같은 파생, 응용 사업들이 창출되고 있다.

디지털 워터마킹에 대한 검토사항으로 호환성 및 표준화 문제에 대한 의견이 제기되어 업계와 단체가 중심이 되어 각각의 목적에 맞는 표준에 대한 논의가 진행되고 있다.

지금까지 연구된 워터마킹 기술의 경우 부분적으

로는 임의의 공격에 견딜 수 있으며 지각적으로도 양호한 결과를 보인다고 발표되고 있다. 하지만 현재까지의 모든 조건을 만족하는 강인한 워터마크 기술을 개발하기 위해서는 앞으로도 많은 연구가 진행되어야 할 것이다.

마찬가지로, 아무리 기술이 발전한다 할지라도 그에 대항하는 기술이 대응하여 발전하기 때문에 지적재산권에 관한 정책적, 문화적, 사회적 인식의 전환이 우선되어야 할 것이다.

참 고 문 헌

[1] '디지털 저작권 지키는 워터마킹,' 한국정보문화센터 웹진 '아름다운 e 세상(http://webzine.info21.or.kr/)' 2002. 2.

[2] 최종욱, '디지털 콘텐츠 보호를 위한 암호화기술-워터마킹,' E-commerce, 한국전자거래진흥원, 통권 28호, 2001. 3.

[3] '저작권 보호 위한 명약 처방「디지털 워터마킹」,' ZDNet Korea 2001. 3. 15.

[4] 김남득, '디지털 워터마킹 기술소개 및 동향보고,' KOSEN/OSTIN, 2001.

[5] SEDICA, http://www.sedica.or.kr

[6] 엄건애, 'General Watermarking Model and its Applications,' 한국과학기술원 석사학위 논문, 2000. 12.

[7] 정사라 외 2, '디지털 콘텐츠의 저작권 관리를 위한 워터마킹 기술,' 전자통신동향분석, 제 16권 제 4호, 2001. 8., pp. 41 - 53.

[8] 'DRM 포럼 기술추적 보고서,' 한국디지털콘텐츠포럼, 2002. 3.

[9] 김종원, '끝까지 숨어서 콘텐츠 보호하는 디지털 워터마킹,' 마이크로소프트웨어, 2001. 10., pp. 250 - 257.

[10] http://unicorn.pknu.ac.kr/~isl/dw.html

[11] http://www.cl.cam.ac.uk/~fapp2/watermar-king/stir-mark/

[12] DigiTreal, http://www.digitreal.co.kr