디지털 컨텐츠 저작권 보안기술 동향

고 은 주* 성 경** 최 용 락***

◈ 목 차 ◈

1. 서 론

디지털 미디어와 그 유통이 활발하게 이루어지면서 콘텐츠 제작자에게 디지털의 완벽한 복제 특성은 심각한 걱정거리로 불거졌다. 이렇게 인터넷과 멀티미디어 기술의 급속한 발전으로 디지털 컨텐츠(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 점차 중요한 위치를 차지해 가고 있다.

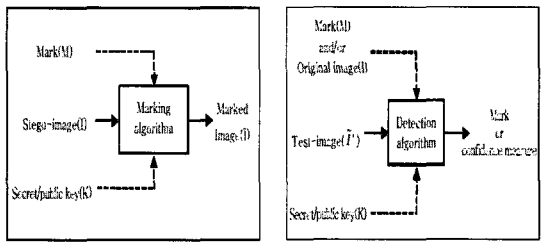
이런 기술들 중 워터마크(watermark)기술은 디지털 콘텐츠의 저작권 보호를 목적으로 사람의 눈이나 귀를 통해 감지하기 어렵도록 디지털 이미지, 오디오, 비디오 신호에 저작권 정보를 삽입하여 멀티미디어 데이터에 대한 소유권을 보호할 수 있으며 무분별한 데이터의 불법 복제도 방지할 수 있는 기술로 연구되고 있다.

본 논문에서는 워터마크 기술이란 무엇이며 이와 관련된 국내외의 기술동향과 전망에 대해서 알아보고자 한다.

2. 디지털 워터마킹 기술

2.1 디지털 워터마킹 정의

디지털 워터마크는 네트워크상에서 사용 가능한 상



(그림 1) 디지털 워터마킹 과정

태로 널리 분포, 유통될 수 있는 멀티미디어 데이터 및 출판물과 같이 지적 재산권 보호 대상 성격을 지니는 자료에 대해 원 데이터에 권리자 및 인증과 같은 추가적이 정보를 삽입하여 데이터에 대한 지적재산권을 보호하기 위한 기법이다. 즉, 워터마킹 저작권 보호 기술의 일종으로서 영상, 비디오, 오디오 등의 멀티미디어 데이터에 소유주만이 아는 신호를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 불법 복제하여 유통할 경우는 정밀한 검사를 하여 저작권을 입증할 수 있다. 따라서 영상, 음향, 비디오 등의 자료에 그림 1과 같이 저작자 고유의 신호를 넣고, 후에 사용자들에 의해 데이터가 불법적으로 복제 유통되었을 때 제작자의 신호를 추출, 검지하는 기술을 의미한다.

2.2 디지털 워터마킹 기술 활용분야

2.2.1 저작권 보호

디지털 콘텐츠의 소유관계를 주장하기 위한 방법으로 콘텐츠에 워터마크를 삽입하는 것이다. 즉, 지적재

* 대전대학교 대학원 컴퓨터공학과 박사과정
** 동해대학교 컴퓨터공학과 조교수
*** 대전대학교 컴퓨터공학부 교수

산권의 보호를 위해서 콘텐츠 소유자가 자신의 콘텐츠에 저작권 정보를 위해서 콘텐츠 정보를 나타내는 워터마크를 삽입하고 누가 자신의 저작권을 침해하거나, 불법으로 사용했을 때 법정에서 자신의 소유권임을 증명할 수 있는 정보로 사용할 수 있다. 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 콘텐츠를 사고 파는 콘텐츠 몰이나 귀중한 텍스트, 오디오파일, 이미지파일, 비디오파일 등의 저작권 주장에 주로 적용된다.

2.2.2 저작권 제어

멀티미디어 콘텐츠를 복사하거나 재생하는데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 콘텐츠에 삽입되어 콘텐츠를 복사할 수 있는 횟수 등을 제어하는데 사용하는 것이다. 즉, 디지털 콘텐츠에 삽입하는 워터마크를 복제와 관련된 정보에 삽입하게 되면 복사 횟수의 제한 및 복사의 권한, 복제 방지 등으로 활용이 가능하고, 재생의 횟수 역시 제한할 수 있다. 이 방법의 경우 복사를 할 때마다 하드웨어가 워터마크를 수정하게 되므로 어느 제한 이상 복사할 수 없게 된다.

활용 분야는 온라인 티켓, 성적증명서, 주민등록 등본 등의 전자문서 발급시 횟수제한 등이 있다. 그리고 MP3 플레이어, PDA, 모바일폰 등의 휴대용 기기나 DVD 플레이어에 워터마크 디코더를 장착하여 오디오, 비디오 등의 불법 사용을 방지할 수 있다.

2.2.3 방송모니터링

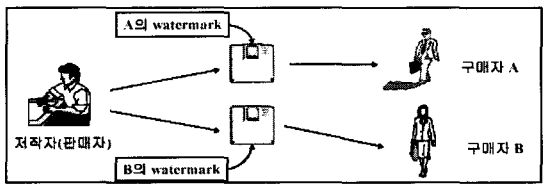
상업 광고 속에 워터마크를 삽입한 후 자동화된 모니터링 시스템에 의해 광고가 계약대로 방송되고 있는지를 확인할 수 있다. 현재 이런 모니터링은 사람이 직접 방송물을 보면서 그 횟수와 시간을 측정하고 있다. 광고뿐 아니라 TV 프로그램도 이러한 방법으로 보호될 수 있다. 실시간 방송감시 시스템은 모든 방송 채널을 체크할 수 있고 발견여부에 따라서 TV 방송국에서 과금할 수 있다. 또한, 시청률과 관련된 정보 역시 워터마크를 사용하여 자동적으로 안정적인 조사가 가능하다.

2.2.4 불법복제추적(핑거프린팅)

인터넷상에서 불법으로 유통되고 있는 디지털 콘텐츠를 발견했을 때, 디지털 워터마킹 기법이 적용된 콘텐츠라면 그 콘텐츠의 원래 저작자가 누구인지는 알아 낼 수 있지만, 불법적으로 배포한 사람은 확인 할 수 없다. 이를 해결하기 위해서 워터마크로서 삽입하는 정보를 저작권자나 판매자가 아닌 구매자의 정보를 삽입하게되는데, 이를 핑거프린트라고 부른다.

만약 불법으로 유통되고 있는 콘텐츠에서 핑거프린트 정보를 추출하게 되면, 그 콘텐츠가 어떤 구매자에게 판매된 콘텐츠인지를 식별(Identification) 할 수 있게 되어 법적인 조치를 가할 수 있게 된다. 이처럼 지적재산권의 보호를 위해서 콘텐츠 소유자가 핑거프린팅 기술을 이용하여 콘텐츠를 공급받는 사용자마다 ID나 일련번호와 같은 다른 워터마크를 삽입함으로써 라이선스 계약을 위반하고 불법 배포한 사용자를 찾아내는데 사용할 수 있다. 또한, 소비자의 소비 형태와 유통의 경로에 대한 정보 역시 획득할 수 있다.

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



(그림 2) 핑거프린팅의 적용 사례

2.2.5 온라인상의 콘텐츠 위변조 판별

보통 연성 워터마킹 기술을 이용하며 온라인이

나 오프라인 상에서 편집이나 수정시, 워터마킹된 부분이 깨지게 되므로 이를 통해 문서의 진위여부를 판별하는 것이다. 예를 들면 다른 사람이 워터마킹이된 문서를 사용하여 일부를 수정한 후에 이를 사용하려고 할 때 원 저작권자는 이 파일을 검사하여 이 파일이 원본인지 아니면 변조된 것인지 확인한다.

각종 계약서류, 사진이나 그림 등의 작품, 그리고 동영상이 디지털로 되어 있다면 디지털의 특성상 여러 가지 프로그램을 사용하여 누구나 쉽게 위조나 변조를 가할 수 있다. 이런 일들을 방지하기 위해 디지털 콘텐츠에 아주 작은 공격에도 쉽게 깨지지는 워터마크를 삽입하여, 위조나 변조를 시도하면 원본이 아니라는 것을 증명해줌과 동시에 변조된 위치를 파악할 수 있다.

대표적으로 DVR(Digital Video Recorder) 및 감시 시스템에서 위·변조 방지를 위한 워터마크의 수요가 급격히 증가하고 잇다. 암호 기법과의 차이점은 워터마크의 특성상 부가적인 데이터가 필요없다는 점과 위치 파악이 가능하다는 점이다. 또한, 인증된 콘텐츠의 경우 의료 영상 등과 같이 특수한 목적에 따라서는 워터마크가 삽입되기 이전의 콘텐츠를 다시 만들 수 있는 경우도 있다.

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

2.2.6 기 타

이밖에도 여권이나 주민등록증의 사용자 신원카드에 내재된 워터마킹을 인식하여 신원확인을 하거나, 인증을 하는 경우, 혹은 저작권 정보의 추적기술, 장치의 사용권 제한 등 여러 분야에 사용될 수 있다. 최근에는 깨진 부분을 복구할 수 있는 워터마크 기법과 압축이나 일반적인 처리에는 반응하지 않고, 「오리기&붙이기」와 같은 의도적인 공격에만 반응하는 기법이 활발히 연구되고 있으며, 일부상용제품이 나와 있다. 이외에도 응용방법에 따라 그 활용분야와 파생범위는 확대될 것이다.

표 1은 디지털 워터마킹 적용분야를 요약하여 나타낸 것이다.

(표 1) 디지털 워터마킹 적용 분야

분야	내용
저작권증명	▪ 저작권이 등록되지 않은 컨텐츠에 대한 저작권 증명 ▪ 인터넷에 공개된 특종기사의 사진
모니터링정보	▪ 특정 컨텐츠에 대한 불법 복사본을 감시하기 위해 모니터링정보 ▪ DigMarc사의 mark Spider(웹에서 특정 워터마킹이 삽입된 컨텐츠 검색)
복사제어정보	▪ 워터마크를 컨텐츠의 복사 및 사용을 제어하는 제어정보로 사용 ▪ OTWG Data Hiding Subgroup의 워터마킹 기술(DVD 플레이어에 적용)
핑거프린팅	▪ 컨텐츠 판매시 구매자 정보를 컨텐츠에 핑거프린팅하여 불법 복제본 발견시 부정행위자 추적 ▪ 실시간 구매자 정보 핑거프린팅
출력물 복사방지	▪ 깨지기 쉬운 워터마킹을 사진, 그림 등에 삽입하여 출력물이 복사되는 경우 워터마크가 깨지도록함 ▪ 여권, 증명서(행정문서)등의 위변조방지

2.3 디지털 워터마킹 공격 방법

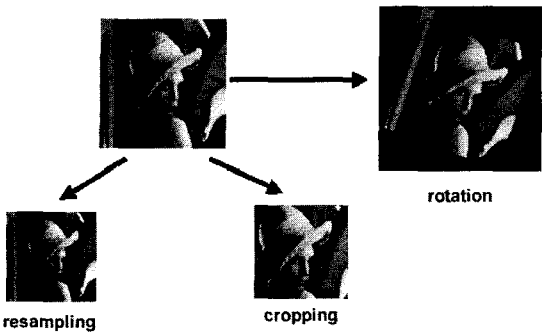
마크를 삽입한 정당한 사용자가 마크로 검출할 수 없도록 삽입된 워터마크를 제거하거나 수정하려고 하는 일련의 행위를 공격이 라고 정의를 한다면, 여러 가지 다양한 방법의 워터마크에 대한 공격방법이 존재한다.

2.3.1 신호 감쇄 공격

여러 가지 워터마크에 대한 공격방법들 중에서 강인성에 대한 공격으로 가장 직관적이고 명백한 공격이다. 이는 워터마크된 이미지 또는 데이터에서 그 워터마크 신호를 감쇄시켜 워터마크를 파괴하는 다양한 공격 방법이 존재한다. 공격 방법에는 노이즈 추가, 중복 마킹, 필터링, 재양자화, 리샘플링, 칼라 모델 변환, 압축 공격, 평균 공격이 있다.

2.3.2 검출 실패

워터 마크된 이미지 또는 데이터에서 워터마크를 찾는 것을 방해하는 방법이다. 이는 워터마킹의 위치를 바꾼다거나 숨겨지도록 하는 방법으로서 신호를



(그림 3) 기하학적인 변형

감쇄시키는 방법과는 차이가 있다. 공격 방법에는 Jitter 공격, 기하학적인 변형, 모자이크 공격 등이 있다.

2.3.3 위조 공격

주로 공격자가 소유권 주장을 못하도록 막는 방법이다. 워터마크를 추출해내는 방법 등이다. 공격 방법에는 Marking Copy 공격, Watermarking inversion이 있다.

2.3.4 IBM Attack

SWICO(Single Watermarked Image Couterfeit 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.

2.3.5 Template attack

일종의 synchronization attack이다. 많은 워터마킹 기술들이 관계 변환 과정에도 불구하고 워터마크를 검출할 수 있도록 하기 위해 메시지 외에도 기준으로 삼는 패턴을 삽입한다. 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.

2.3.6 특정한 환경에 대한 공격 방법

신호를 없애는 공격이나 워터마크를 못 찾게 하는 공격 외에도 특정 환경에서만 사용되는 공격 방법이 있다. 아래에서 언급되고 있는 두 가지 경우가 아주 좋은 예라고 할 수 있으며, 이는 제시된 워터마크 방법에서만 적용 가능한 공격 방법이다. 주로 Twin peaks는 색상 정보가 적은 이미지에 워터마크를 삽입하였을 때 나타나며, 에코 숨김은 오디오 데이터에 주로 사용하는 기법이다. 공격 방법에는 Twin peaks 공격, Echo hiding에 대한 공격이 있다.

2.3.7 기타 공격 방법

기타 공격 방법에는 주로 법정에서 문제가 되는 경우가 이에 속하며, 워터마크에 사용된 키를 찾기 위하여 전수공격을 하는 방법도 포함되어 있다. 워터마크는 비밀키를 사용하기 때문에 키의 관리가 중요하다. 공격 방법에는 키에 대한 전수 공격, Foreign server 공격, Spoofing 공격, Oracle 공격이 있다.

2.4 디지털 워터마킹 요구 조건

워터마킹 방법은 표 2와 같이 기본적인 요구 조건을 만족해야 한다.

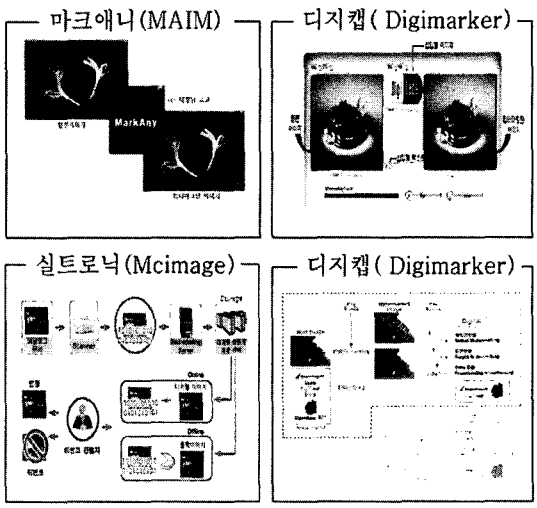
따라서, 원본 영상에 삽입된 워터마크는 시각적으로 보이지 않고, 오직 소유권자만이 Watermark Key를 가짐으로써 워터마크를 삽입, 추출, 제거할 수 있고, 삽입된 워터마크는 일반적인 영상 처리 등의 영상 변형(손실 압축, 필터링, 잡음 첨가, 리샘플링 등) 후에도 남아 있어 워터마크의 강인함을 보여준다.

3. 국내외 제품 동향

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 알아보도록 하겠다.

(표 2) 워터마킹의 요구 조건

요구조건	내용
관련된키 (associated Key)	• Watermark Key라고 부르는 ID번호와 관계가 있음 • 워터마크를 삽입하고, 추출하고, 제거하는데 사용 • 개인적 소유권의 합법성을 확인하는데 사용
지각의 비가시성 (Perceptual Invisibility)	• 인간의 시각에 감지되지 않아야함 • 영상 데이터의 경우 원본 영상과 워터마크가 삽입된 영상처리를 분간할 수 없도록 함 • 원본 영상은 합법적인 소유자에게만 접근이 가능하고, 그런 차이가 관찰자에 의해서는 인식되지 않게 남아 있어야함
신뢰할 수 있는 추출 (Trustworthy Detection)	• 어떤 특정 영상에 대한 확실한 소유권 증명을 해야함 • 워터마크 추출 실패는 나타나지 않아야 하지만 만약에 나타나면 드물게 나타나야함
자동화된 추출과 검색 (Automated Detection and Search)	• 한소유권자의 생산물의 불법적인 파괴에 대하여 네트워크 환경에서 공동으로 접근할 수 있는 영역을 조사하는 검색 절차와 쉽게 결합되어야함
다중 워터마킹 (Multiple Watermarking)	• 같은 이미지에서 다른 워터마크를 충분히 많이 첨가할 수 있어야 함 • 워터마크는 유일한 키를 사용하여 추출할 수 있어야함 • 이미 워터마크된 영상을 다른 사람이 다시 워터마킹하는 것을 막을 수 없기 때문에 필요하다 • 저작권 소유가 한 소유자로부터 다른 소유자로 이동된 경우에 편리하다
강인성(Robustness)	• 워터마크가 내장된 디지털 영상은 고의든 고의가 아니든 수정될 수 있음 • 일반적인 영상처리 등의 영상 변형(압축, 필터링, 잡음첨가, 회전스케일링 등)후에 남아있어야함
통계적인 비가시성 (Statistical Invisibility)	• 통계적 방법을 사용하여 복구 되어서는 안됨 • 다량의 워터마크가 내장된 디지털 영상들의 소유는 같은 키를 이용하여 통계적인 방법을 적용함으로써 워터마크를 배치해서는 안됨 • 워터마크는 이미지에 의존적 이어야함



(그림 4) 국내 제품 솔루션

3.1 국내의 제품 동향

마크애니(MarkAny)는 1999년 2월에 설립한 트러스텍이라는 회사로 출발하였으며 다수의 특허 및 상표 등록을 하고 있다. 국내 회사로 유일하게 STEP2000에서 5개업체 중 2위(1위는 IBM), SDMI phase 1에서 4개 업체 중 하나로 선정된 바 있다. 마크애니는 SDMI 4강에 진출하였으며 STEP2001에서도 다시 선정되었다. 주요제품으로는 MAIM(이미지 워터마킹), MAO(오디오 워터마킹), MAVI(비디오 워터마킹), MAVEC(벡터 워터마킹), Document SAFER, Content SAFER, Web SAFER, 문서 위변조 방지 등이 있다.

실트로닉은 1999년 9월 설립한 회사로 자체개발기술과 한국전자통신연구원의 기술과 출원과 특허를 토대로 워터마킹 솔루션을 내놓고 있다. 워터마크 알고리즘을 이용한 멀티미디어 콘텐츠의 저작권 보호 솔루션으로 RIGHTS@fer Multimedia, RIGHT@fer Document, MagiCheck, Magic tag 등이 출시되어 있다.

그림 4는 현재 국내 제품 솔루션을 보여주고 있다.

디지트리얼은 1997년 (주)한국메디컴시스템이라는 의료관련 솔루션제공업체로 출발하여 2000년 3월 국내 출원 중인 특허 "대역분할 방식을 사용한 디지털 정지영상의 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 4.0, WaterStamp-Print, WSDVR 등의 제품이 출시되고 있다.

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

디지털 이노텍은 2000년 5월 설립하였으며 인터넷 상에서 사용되는 각종 멀티미디어의 저작권보호를 위하여 설립된 연구개발 중심의 회사이며 일반 영상에 워터마크를 삽입하는 방식의 보안용 바코드 솔루션을 개발했다.

3.2 외국의 제품 동향

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

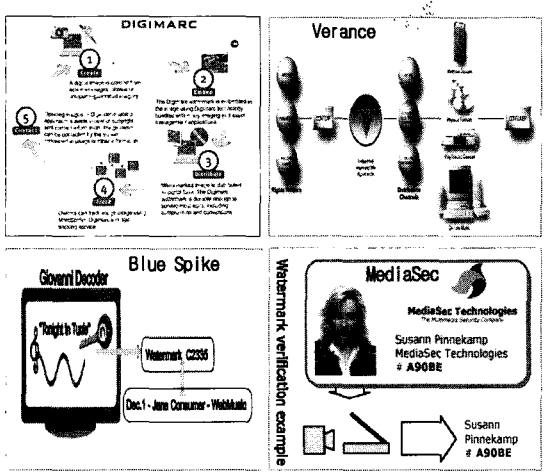
Verance은 1999년 10월 Solena와 Aris와의 합병으로 설립된 회사로 주로 오디오 워터마킹 쪽에 강하다. Musicode, Mediacode 등을 출시하였으며 20여 개의 특허를 기초 SDMI와 DVD 오디오 등의 표준화 작업에 참여하고 있다. 현재는 Verance audio Watermark detector 등의 제품을 판매하고 있다.

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

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

(표 3) 기타 국내외 제품 동향

회사	내용
디지캡	• 1996년 10월 설립된 회사로 저작권에 대한 정보를 다양한 멀티미디어 컨텐츠의 특성에 알맞게 워터마킹하여 저작권을 보호함 • 워터마킹 제품으로 Dgicap@image가 있음 • 이 회사는 DRM 관련 개발툴을 함께 판매
외워웰닷컴	• 오디오 압축과 신호처리 기술을 적용한 워터마킹 기술 WOWDWS(WOWDigital Water-marking System) 개발 • 오디오 주파수 대역에 저작권 정보, 사용자 ID 등의 정보를 담은 워터마크를 삽입하는 형태로 디지털 아날로그와 파일 형식 변환 압축 샘플링 등 내구성이 뛰어남
트러스텍	• 영상이나 오디오에 1.2MB 정도의 정보를 삽입하고 추출할수 있는 워터마킹 기술 개발 • 인터넷 증명서 발급 기술과 온라인 티켓 발급키 등 적극 제안함
Alpha-tec	• 1989년 설립된 회사 • EIKONAMARD, AudioMa가, VideoMark, VdMark 등.
MedaSec	• 1996년 설립된 회사 • MedaSignPrint, MedaSignDigital, MedaTrust, SysCop



(그림 5) 국외 제품 솔루션

4. 결론 및 향후 연구 방향

본 논문에서는 DRM의 세부 중요 기술로 부각되고 있는 워터마크 기술의 특성을 살펴보았다. 네트워크와

미디어의 발달로 멀티미디어 데이터의 불법 유통이 급속히 확산되고 있기 때문에, 향후 전자상거래의 안정적인 발전을 위해서는 디지털 데이터의 저작권 관리와 보호가 반드시 필요하게 되었다.

많은 단체에서 저작권 관리에 대한 알고리즘을 개발하고, 표준화 작업을 진행시키고 있는데 특히 불법 복제제어와 전자 지문에 관계된 워터마크는 알고리즘의 잠재적 개발 가능성 때문에 활발한 연구가 진행되고 있다.

지금까지 연구된 워터마킹 기술의 경우 부분적으로는 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. 워터마크를 비롯한 저작권 관리와 보호에 관한 기술들은 시스템의 요구사항에 따라 적용되는 기술의 종류와 강인성이 달라지게 된다. 따라서 저작권 관리 시스템 개발을 위해서는 먼저 전체 시스템의 목적과 요구사항을 분명하게 정의하고, 필요한 기술의 최적화를 위한 연구가 진행되어야 할 것이다.

참고문헌

[1] 최종욱, "디지털 콘텐츠 보호를 위한 암호화 기술-워터마킹", E-commerce, 한국전자거래진흥원, 통권 28호, 2001.3.

[2] "저작권 보호 위한 명약 처방 「디지털 워터마킹」", ZDNetKorea, 2001.3.15.

[3] 김남득, "디지털 워터마킹 기술 소개 및 동향보고", KOSEN/OSTIN, 2001.

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

[5] "DRM 포럼 기술 추적 보고서", 한국디지털콘텐츠포럼, 2002.3.

[6] 김종원, "끝까지 숨어서 콘텐츠 보호하는 디지털 워터마킹", 마이크로소프트웨어, 2001.10. pp. 250~257.

[7] 정사라 외2, "디지털 콘텐츠의 저작권 관리를 위한 워터마킹 기술", 전자통신동향분석, 제16권 제4호, 2001.8, pp. 41~53.

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

[9] ji-Hwan Park, "Attacks and Evaluation on digitial Watermarking Techniques", 2001.03.

[10] 배익성, 김강석, 차의영, "디지털 영상의저작권 보호를 위한 워터마킹에 관한 연구", 한국정보과학회 논문집 10. 1998.

[11] 강상익, "디지털 워터마킹 국내·외 표준화 동향", TTA데이터 기술위원회, 제73호 pp. 138~145.

◐ 저 자 소 개 ◑

고 은 주

2002년 호남대학교 대학원 컴퓨터공학과(석사)
2002년~현재 : 대전대학교 대학원 컴퓨터공학과 박사과정
관심분야 : DRM, 워터마킹, 네트워크 보안

성 경

1998년 목원대학교 전자정보학과(학사)
1993년 경희대학교 전자계산학과(석사)
2000년 한남대학교 컴퓨터공학과(박사수료)
1994년~현재 : 동해대학교 컴퓨터공학과 조교수
관심분야 : 정보보호, 신경회로망

최 용 락

1989년 2월 중앙대학교 전자계산학과(박사)
1982년 3월~1986년 1일 한국전자통신연구원 선임연구원
1986년 2월~현재 : 대전대학교 터공학부 교수
1997년 3월~1999년 2월 한국정보보호학회충청지부 초대지부장
2001년 3월~2003년 3월 대전대학교 공과대학 학장
2000년 10월~현재 : 대전지검 컴퓨터수사자문위원
관심분야 : 컴퓨터통신보안, 컴퓨터 포렌식스, DRM, 보안 API