워터마크 공격 및 평가 기술 동향

Technical Trends on the Attack and Evaluation for Watermarking Algorithms

김진호(J.H. Kim) 콘텐츠보호연구팀 선임연구원
서영호(Y.H. Seo) 콘텐츠보호연구팀 책임연구원, 팀장
이흥규(H.K. Lee) KAIST 전산학과 교수

네트워크 환경의 발전과 디지털 미디어 저작툴의 발전으로 이미지, 오디오, 비디오, 전자 문서 등의 멀티미디어 데이터는 시공간적 차이 없이 인터넷에서 빠르게 배포되고 있다. 품질의 손실 없이 무한 복제가 가능한 디지털 콘텐츠의 특성 및 저작권에 대한 의식의 부족 때문에 이들 데이터의 불법 복제 및 무단 배포가 일어나고 있다. 이와 동시에 디지털 콘텐츠의 저작권 정보를 보호하기 위한 워터마킹 기술도 연구개발이 활발하게 진행되고 있다. 또한 워터마킹 기술의 취약성을 밝히는 워터마크 공격 기술도 워터마킹 기술의 발전과 더불어 개발되고 있는 상황이다. 본 고에서는 다양한 워터마킹 기술들의 성능을 검증하기 위해 어떠한 워터마크 공격 기술과 워터마크 평가 기술이 있는지 동향을 파악하고 이러한 기술의 내용을 살펴본다. 또한 워터마크 공격 기술과 평가 기술에 관련된 최근의 국제 표준화 현황도 살펴본다.

I. 서 론

1995년 최초로 디지털 워터마킹이라는 개념이 소개된 이후 이러한 기술을 이용하여 저작권자 확인, 불법유통 추적, 방송 모니터링, 접근 제어 등 다양한 응용분야에의 활용가능성이 제기되고 실제로 점차 많은 분야에서 저작권자의 권리를 보호하기 위하여 사용되고 있다[1]. 그러나 이와 동시에 이러한 기술을 무력화시키는 기술들도 또한 다양한 방법으로 제기되고 있다. 디지털 워터마킹 기술을 개발하는 연구기관이나 개인들이 이러한 기술을 이용하여 디지털 워터마킹 기술을 무력화시키는 기술을 선보이기도 한다. 또한 보다 심오한 이론연구를 위하여 디지털 워터마크를 제거하거나 검출이 불가능하게 하는 연구들을 수행하고 있다. 현재 정지영상, 동영상, 오디오 등의 매체별로 저작권을 보호하기 위한 기술들이 가장 활발하게 연구되고 활용되고 있으며 공격기술도 역시 이러한 매체에 집중되고 있다.

디지털 워터마킹 기술에 대한 평가는 그 기술의 성능을 객관적으로 입증한다는 점에서 그 기대효과는 매우 크다[2],[3]. 또한 대부분 논문이나 학술대회에서 제안되는 기술들이 그 적용 도메인이 매우 좁아 그 실용성이 의문시 되는 경우가 많다. 따라서 디지털 워터마킹 기술의 잠재적인 고객인 콘텐츠 보유자, 콘텐츠 서비스 기관, 서비스 관련 각종 솔루션 기술 개발 기관 등에서 어떠한 기술을 채택하여만 그들의 권리를 보호 받을 수 있을지 결정하지 못하여 결과적으로 디지털 콘텐츠 및 그 서비스 시장의 확대를 가로막는 주요한 요인이 되고 있다. 따라서 2000년대부터는 동영상, 오디오 등을 주요 매체로 하여 기술평가 시도 및 사실상의 표준으로 추진하려는 움직임이 커지고 있다.

II. 워터마크 공격 및 평가 기술 동향

1. 워터마크 공격 기술

영상, 동영상, 오디오 등 멀티미디어 데이터 이외에 DNA, 파쇄문서, 소프트웨어, 데이터베이스 등 non-media를 포함하여 다양한 디지털 콘텐츠에 대

한 저작권을 보호하기 위하여 디지털 워터마킹 기술이 존재한다. 이러한 기술의 성능평가를 위하여 공격기술 또한 필연적인 것으로 공격기술과 평가기술을 분리하여 설명하기는 어려운 실정이다. 본 보고서에서는 Stirmark, Checkmark 등 정지영상에 대한 각종 평가도구들은 공격기술에서 설명하고 그 이외의 기술들은 평가기술에서 설명하기로 한다.

가. Stirmark

Stirmark는 정지영상에 대한 디지털 워터마킹 알고리듬을 평가하기 위한 방법으로 1997년 v.1.0이 발표되었다. 그 후 계속 수정되면서 현재 오디오, 동영상 워터마킹 알고리듬으로 확장 가능한 Stirmark v.4.0이 나와 있다[4]. Stirmark는 벤치마킹 방법들 중에서 가장 대표적인 것으로 강인성에 주안점을 둔 벤치마킹 방법이다. Stirmark v.4.0의 특징을 보면 워터마킹 기술은 서로 다른 목적으로 많은 응용 분야에 적용되기 때문에 벤치마킹 전에 사용 목적과 대상을 선택하도록 하고 있다. 즉, 영상의 품질 계수, 강인성, 공격의 강도 등을 적용하여 벤치마킹을 실시한다. Stirmark는 벤치마킹을 이용한 애플리케이션이 나오지 않고 있으며, 척도로 이용되는 PSNR은 시각적인 척도로는 부적합하다. 또한, 공격 기법이 기하학적 변환에 많은 비중을 두고 있다. 그리고, 삽입・추출에 걸리는 시간을 고려하지 않고, 이미지의 사전 정보를 고려하지 않은 문제점들을 가지고 있다.

나. Checkmark

Checkmark는 Stirmark의 여러 가지 문제점을 개선하기 위해 만들어졌다[5]. 크게 Martin Kutter의 공격 분류기준에서 제네바대학교의 Sviatoslav Voloshynovskiy의 분류로 변경되면서 새로운 공격들이 추가되었다. 기존의 JPEG 압축만을 고려하던 부분이 JPEG2000에서 사용되는 웨이블릿 압축을 포함하고 있으며, 이전에 워터마크가 삽입된 영상으로부터 워터마크를 추출하여 그 정보를 공격할 데이터에 다시 삽입하는 복사공격이 새로이 추가되었다. 이 외에도 여러 가지 신호처리적 공격들이 새롭게 포함되어 워터마킹 알고리듬의 강인성 테스트를 실시한다. Checkmark는 이러한 공격 유형뿐만 아니라 새로운 화질 평가방법으로 weighted PSNR과 Watson metric을 도입하고 있다. 그리고, 출력 양식을 XML 포맷으로 나타내며, 결과 테이블은 HTML로 작성한다. 소스는 Stirmark와 달리 Matlab으로 작성되어 일반 사용자가 다루기 쉽게 되어 있다.

다. Optimark

기존의 벤치마킹 도구를 보완하기 위해 데살로니키(Thessaloniki) 아리스토텔레스 대학(Aristotle Univ.)에서 2001년도에 Optimark를 제시했으며 기존의 벤치마킹 기법에 복잡성, 제한된 데이터와 주어진 비트오류율(Bit Error Rate: BER)에 얼마나 많은 비트의 은닉정보를 삽입할 수 있는지를 나타내는 정보량(payload), 알고리듬이 공격에 대응하여 얼마나 강인한지를 나타내는 파손한계(breakdown limit) 등을 평가할 수 있는 도구를 제시했다[6]. 또한 각 영역에서의 강인성을 종합적으로 평가하여 수치적으로 나타낼 수 있는 스코어(overall score)를 제시했다.

라. JEWELS

JEWELS는 일본 전자정보기술산업협회(JEITA)에서 워터마크 평가 지원 시스템(JEWELS)으로 개발하여, 정지영상의 저작권 보호 및 이용자의 이용범위에 대한 가이드라인 설정을 목적으로 디지털 워터마킹 기술의 안전성 평가를 위한 벤치마킹 프로그램이다[7]. JEWELS는 전체적으로 11개 항목의 내성평가와 15가지의 영상 변환공격을 포함하고 있다. 각 항목들은 여러 개의 매개변수를 가지면서 다양한 공격이 가능하도록 구성되어 있다.

2. 워터마크 평가 기술

가. Certimark

Certimark 프로젝트는 2000년 5월부터 2002년 7월까지 유럽에서 수행된 대규모 프로젝트로 그 연

구비 규모는 약 600만 달러에 달한다. 제네바 대학교 등의 학계를 주축으로 Thomson, Philips 등 15개 산업체 및 학계의 연구기관이 모여 컨소시엄을 구성하여 수행하였다. 그 목적은 디지털 워터마킹 기술을 위한 완벽한 벤치마킹 도구, 참조도구 개발, 워터마킹 알고리듬의 인증절차 마련 및 관련 핵심기술의 개발이다. 이러한 목적을 달성하기 위하여 각종 응용시나리오 내에서 영상 워터마킹 기술을 평가하기 위하여 기술의 공급자와 사용자 모두가 사용할 수 있는 안전한 체계를 개발하고 기술의 성숙도를 높이기 위하여 새로운 공격기법들이 연구되었다.

앞에서 기술한 Stirmark, Checkmark가 주로 평가 도구의 구현에 치중한 반면에 European task force로서 워터마킹 기술을 보급하기 위한 Certimark는 워터마킹 기술을 응용 시나리오와 함께 워터마킹 기술을 평가하는 것을 특징으로 한다[8]. 즉, 워터마킹 기술은 응용에 따라 만족해야 하는 요구 사항들이 달라진다는 점에 주목하여 워터마킹 기술의 응용 시나리오를 포함시켜 평가한다. Certimark의 목적은 좀 더 공정한 워터마킹 평가를 수행하여 워터마킹 기술의 사용자는 자신의 요구에 맞는 적합한 기술을 선택할 수 있도록 하고, 개발자는 자신이 개발하는 워터마킹 기술의 완성도를 향상시키는 데 이용할 수 있도록 하기 위함이다. 이에 따라서 Certimark는 시나리오 파라미터, 컨트롤 파라미터의 정의, 그리고 워터마킹의 강인성을 평가하기 위한 공격의 종류(정지 영상 및 동영상), 평가를 위한 출력 파라미터(시각적 품질, 용량, 검출 및 false alarm probability, BER, complexity), 그리고 평가에 대한 결과보고 절차 등을 정의한다. 현재 Certimark가 공개한 문서들은 <표 1>과 같다.

<표 1> Certimark 문서

번호	제목	내용
D 2.1	Watermarking application and requirements for benchmarking	워터마킹 기술의 응용에 대한 검토와 성능 척도에 관한 파라미터를 고려
D 2.2	Benchmark metrics and parameters	워터마킹 시스템의 벤치마킹에 포함되는 파라미터들에 대한 기술
D 3.1	Benchmark architecture	벤치마킹 툴에 대한 기본구조를 제시
D 4.1	Common data processing and intentional attacks	공통적인 처리와 의도적인 공격에 대한 리스트를 제시
D 5.3	New media type	새로운 미디어 형식에 대한 벤치마킹 구조에의 영향 및 가능 변경 등을 기술
D 5.4	Channel capacity	대부분의 응용 시나리오 시에 다른 알고리듬의 데이터 저장 한계를 확증하기 위한 채널 용량을 검토

Certimark는 워터마킹 응용으로서 소유권 증명(proof of ownership), 방송 모니터링, 핑거프린팅, 무결성 체크, 식별 및 인증, 사용 제어, 정보 부가 채널(information side channel)로 분류하고, 각각에 대한 요구사항들을 제시하고 있다. Certimark에서는 동영상 워터마킹에 대한 시나리오는 모니터링과 디지털 시네마(digital cinema)를 예로 들고 있다.

나. EBU

EBU(European Broadcasting Union)에서는 3개의 워터마크를 필요로 한다[9]. 첫번째는 모든 IPR 관련 데이터가 있는 데이터베이스의 링크로서 이용되는 식별자, 두번째는 배포 경로를 식별하기 위한 것으로 수신 측에서 삽입되는 것이다. 그리고 세번째는 end-user의 터미널을 식별하기 위한 것이다. 이러한 워터마크는 식별을 위한 응용분야가 된다. EBU의 워터마킹 평가는 품질 평가와 강인성 평가로 나누어진다. 품질 평가는 ITU-R Rec. BT. 500의 방법을 이용하거나, <표 2>와 같이 비교 실험을 수행한다.

응용에 따른 사용자 요구사항에 대해 <표 3>과 같이 워터마크의 비인지성을 포함한 총 7개의 항목으로 분류되고 각각의 항목에 대해 필수 항목과 권고 사항으로 구분된다.

<표 2> EBU의 품질평가 척도의 예

A much worse than B	100%
A worse than B	67%
A slightly worse than B	33%
A equal to B	0%
B slightly worse than A	33%
B worse than A	67%
B much worse than A	100%

<표 3> EBU 동영상 워터마킹의 요구사항

Requirements: **M**: Mandatory, **R**: Recommended, **TBD**: To Be Decided		
1. 워터마크의 가시성	스튜디오 조건에서 원본과의 비교 시 식별 불가능	**M**
2. 페이로드	워터마크 최소 세그먼트(WMS)	1 sec for W1 5 sec for W2
	Data capacity	64bits/WMS
	Detection probability per WMS	> 95%
	False positive probability per WMS	$< 10^{-8}$
	Probability for (bit) error-free payload per WMS	$> 1-10^{-8}$
3. 워터마크의 목적	Identification	
4. 안전성	예측하기 어렵고 암호학적으로 강함 이용 가능한 워터마크 키의 수 워터마크 키 관리	**M** 충분한 수 **M**
5. 워터마크 검출 및 페이로드 추출		**M**
6. 원본 및 워터마크가 삽입된 신호의 형태		ITU-T Rec. BT 656
7. 강인성	1) 압축 - MJPEG(20Mb/s) - ISO/MPEG-1(<1Mb/s) - ISO/MPEG-2(2 to 6Mb/s MP@ML) - Panasonic/DV or JVC/Digital-S, Sony/DV, Sony/Beta-SX - MPEG-2 4:2:2 - 50Mb/s recorder(Sony IMX)	 **M** **M** **M** **M** **M**
	2) PAL 코딩 및 아날로그 녹화 - Sony/Beta-SP(with PAL input) - VHS	 **M** **M**
	3) 디지털 및 아날로그 필터링 - Resampling, e.g. D/A ↔ A/D 변환 - Sampling-rate 변환, up and down 변환 - Picture aspect-ratio, e.g. 4:3 ↔ 16:9 - Frame-rate 변환, e.g. 24Hz ↔ 25Hz ↔ 30Hz - Line-scan 변환: progressive ↔ interface - Motion-compensation noise reduction - Added white noise(at -30dB) - Color-space 변환: color ↔ gray-scale - Slow motion 3:1	 **M** **M** **M** **M** **M** **M** **M** **M**

III. 워터마크 공격 및 평가 기술 내용

1. 영상 공격 기술

영상의 경우 아래와 같이 워터마크에 대한 제거 공격, 기하학적 공격, 프로토콜 공격, 암호학적 공격 등 크게 4가지의 공격기술이 존재한다.

가. 제거 공격

제거 공격의 공격 목적은 워터마킹 알고리듬의 안정성을 깨지 않고, 워터마킹된 데이터에서 워터마크 정보를 완전히 제거하는 것이다. 즉 이러한 형태의 공격은 어떠한 방법으로도 공격 받은 데이터에서 워터마크 정보를 복원할 수 없게 하는 치명적인 결과를 초래한다. 일반적으로 정교한 제거 공격이라 함은 공격 받은 영상의 화질은 충분히 유지하면서도 삽입된 워터마크를 최대한 효율적으로 손상시키는 공격을 말한다. 이 모든 공격이 워터마크를 완벽히 제거할 수 있으리라는 것은 보장할 수는 없으나, 이러한 공격을 토대로 데이터에 삽입된 워터마크는 최대한 손상시킬 수 있다.

이러한 제거 공격의 종류에는 잡음제거, 손실압축, 재변조, 양자화, 공모, 동기제거(템플릿 제거, 모자이크) 등의 기술들이 있다.

나. 기하학적 공격

삽입된 워터마크를 제거하거나 에너지를 낮추는 제거 공격과는 달리, 기하학적 공격은 워터마크가 삽입된 정지영상의 공간적 변형을 통해 워터마크 검출기와 워터마크 사이의 동기를 왜곡시켜 워터마크가 발견되지 않도록 하는 공격형태이다. 이 공격은 워터마크 검출을 막는 효과적인 방법이라는 점 이외에도 시중의 영상편집 도구들을 이용하여 누구나 손쉽게 가할 수 있는 공격의 형태라는 점에서 주요 연구 과제가 되어 왔다.

기하학적 공격은 영상의 변형 영역에 따라 크게 두 가지 범주로 나눌 수 있다. 하나는 영상 전체에 작용하는 변형으로 일반적인 영상 편집에 사용되는 회전, 이동, 자르기 등과 같은 변형을 말한다. 대부분의 경우 이는 수학적으로 쉽게 모델링 될 수 있으며, 이 공격에 강인한 워터마킹 기법들에 대한 많은 연구가 나와 있다. 다른 하나는 영상의 부분적인 지역에 작용하는 변형으로 주요한 시각적 왜곡 없이 효과적으로 동기를 제거하는 공격형태이다. Stirmark에서 제공하는 랜덤 밴딩 공격이 대표적이다. 근래 이 공격에 대해 강인한 워터마킹 기법에 대한 연구들이 나오고 있으나 여전히 여러 워터마킹 기법들에 대해 효과적인 공격 방법이 되고 있다.

다. 프로토콜 공격

디지털 정지영상 데이터는 인터넷의 발달로 불법적인 복제와 불법 유포의 부작용이 아주 쉽게 발생한다. 이러한 불법적인 복제와 유포를 막기 위하여 디지털 워터마크 방법이 도입되었다. 즉 정지영상에 소유주만이 알 수 있는 디지털 워터마크를 삽입하여 인터넷에 유포한 후 불법적인 사용이 발생했을 경우 디지털 워터마크를 통하여 소유권을 주장할 수 있다. 프로토콜 공격은 워터마크를 삽입하여 소유를 주장하고자 하는 응용을 공격하는 것을 목적으로 하고 있다. 즉 워터마크가 삽입된 정지영상에 공격자의 워터마크가 삽입된 복제 정지영상을 만들어 소유권 주장을 못하도록 하는 것이다. 프로토콜 공격에는 크게 가역 워터마크 공격(invertible watermark attack) 방법과 복제 공격 방법이 있다.

라. 암호학적 공격

암호학적 공격 방법의 주된 목적은 워터마킹 방법에서 암호학적 요소를 공격하여 삽입된 워터마크를 제거하는 것이다. 암호학적 공격 방법에는 전수키 조사(exhaustive key search) 방법과 오라클 공격 방법이 있다.

2. 오디오 공격 기술

SDMI(Secure Digital Music Initiative)에서 사용된 공격 기술들을 나열하면 다음과 같다[10].

- echo
- dynamic range
- equlization
- speed increase/decrease
- time scale increase/decrease
- resampling 44.1kHz~48kHz
- band pass 필터
- 노이즈 추가(-36dB~-60dB)
- wow와 flutter 추가
- MP3 코딩/디코딩
- AAC 코딩/디코딩

Ⅳ. 관련 기술 표준화 현황

1. MPEG-21 Part 11: Evaluation Tools for Persistent Association Technologies

2000년 MPEG-21의 표준화가 시작된 이후 표준화가 진행됨에 따라 초기의 7개 세부분야에서 16개의 세부분야로 확장되었고 그 중 디지털 워터마킹 기술과 직접 관련된 분야는 Part 11의 'evaluation tools for persistent association technologies'이다[11]. MPEG-21은 멀티미디어의 각종 요소들이 함께 구성되는 프레임워크 기술이다. 이 기술에서는 특히 콘텐츠의 코드화된 표현이 메타데이터 서술자(descriptor) 및 그 콘텐츠에 적용되는 IPMP(Intellectual Property Management and Protection) 보호 기술과 함께 서술된다. 따라서 MPEG-21 내에서는

콘텐츠, 메타데이터, 그리고 IPMP 요소들 사이에 어소시에이션(결합)을 생성하고 유지하는 도구에 대한 필요성이 제기된다. 디지털 워터마킹과 핑거프린팅으로 알려진 기술에 기반한 도구들은 그 결합이 콘텐츠 자체에 포함될 수 있거나 또는 콘텐츠로부터 추론될 수 있는 멀티미디어 요소들 사이에 결합을 구성하는 수단을 제공한다. 더욱이 디지털 워터마킹이나 핑거프린팅에 기초한 도구들은 콘텐츠의 적응(adaptation)에도 견고하게 그러한 기능을 유지한다. 그러한 도구들은 PAT(Persistent Association Technologies)라고 불리우며 따라서 이러한 도구들을 구현하고 평가할 필요성이 있다.

현재 가장 최근의 Working Draft(WD) 문서는 2004년 3월에 발간된 N6392 ISO/IEC PDTR 21000-11 Evaluation Tools for Persistent Association Technologies 이다. 그 이후 관련 ad-hoc 워킹 그룹을 구성하여 현재 지속적으로 작업중이다. N6392 문서에서는 오디오를 위한 디지털 워터마킹과 핑거프린팅 기술에 대한 논의가 이루어지고 있다. 오디오에 대해 압축, 신호처리, 잡음 첨가, 시간축 변화, 잘라내기 등의 다양한 공격을 가하였을 때 워터마크가 어느 정도나 추출되는지를 시험하는 안내를 하고 있다. 현재 각 기술마다의 개략적인 연구가 진행중이며 PAT의 요구사항, 해당 기술의 평가척도 및 그 규격, 관련 각종 이슈들, 현재까지의 연구결과 등에 대한 조사가 병행되고 있다. 현재는 오디오에 대하여만 표준화 작업을 진행하고 있으나 향후에는 비디오, 정지영상, 텍스트 등에도 확대될 예정이다.

2. SDMI

오디오 분야에서 대표적으로 사실상의 국제표준을 통한 저작권보호기술의 상용화를 추구하였던 단체이다. 2000년 11월에 2단계 평가를 끝마치고 실제 사용을 위하여 공개테스트를 수행하였다. 공개테스트 결과 외부의 해킹에 취약함이 드러나 2001년 6월 그 활동을 중지하였다.

3. CPTWG

CPTWG(Copy Protection Technical Working Group)은 1997년부터 활동을 시작하여 NEC, SONY, Pioneer, Hitachi, Philips, Digimarc, Macrovision 등 미국 및 유럽의 대표적인 산업체들이 참여하고 있다[12]. 이후 Galaxy 그룹(NEC, SONY, Pioneer, Hitachi)과 Millennium 그룹(Philips, Digimarc, Macrovision)으로 나뉘어 경쟁적으로 기술개발을 하였다. 최근에는 VWM이라는 하나의 그룹으로 활동하고 있다. 2001년 비디오 콘텐츠 보호기술 평가를 위한 기술 요청을 한 적이 있으며 현재도 계속 활동하고 있다.

4. EBU

EBU 산하의 N/WTM이라는 연구그룹을 만들어 활동하고 있다. 이 연구결과 방송 콘텐츠용 디지털 워터마킹 기술의 사용자 요구사항과 디지털 워터마킹의 표준화를 위한 제안서 등이 작성되었다. 2000년 5월에는 유럽차원의 방송용 콘텐츠를 위한 디지털 워터마킹 기술 공개 평가회를 가져 강인성, 안정성, 신뢰도, 각종 공격에의 회복성 등을 평가 척도로 하여 제안된 기술들을 평가하였다. 평가에 응한 기업으로는 Philips, Tektronics, Thomson, Lucent 등이었으며 EBU에서 요구한 규격을 모두 만족시킨 기술은 없었다. 그러나 기술이 실제 응용을 위하여 사용되기에 충분히 성숙하였다는 결과를 발표하였다.

Ⅴ. 결론 및 향후 전망

위에서 살펴본 바와 같이 다양한 워터마킹 기술이 개발되는 만큼 다양한 공격 및 평가 방법이 제시되고 있다. 향후 워터마킹 기술에 대한 평가는 아래와 같이 규모가 큰 국제 표준 기구 혹은 산업체의 공동 컨소시엄에 의해 제정되는 공격 및 평가 기술을 바탕으로 이루어질 것으로 예측된다.

1. MPEG

MPEG-21은 국제표준 단체 중에서 가장 규모가 크고 그 활동이 활발하다. 현재 디지털 워터마킹 분야와 관련하여서는 part-11에서 국제표준 활동이 이루어지고 있다. 아직 기술 자체에 대한 규격을 논의하는 것이 아니라 이러한 기술들의 성능평가를 어떻게 할까에 대한 평가 방법론에 대한 표준화 논의가 이루어지고 있다.

이러한 디지털 워터마킹 기술평가와 관련하여서는 이미 Stirmark, Checkmark 등이 국제적으로 널리 알려져 있고 EBU, CPTWG, SDMI 등에서 기술평가 공개테스트를 수행한 적이 있어 이러한 기술평가 규격들을 집중 연구한 후 평가방법론이 표준화 될 것으로 판단된다.

따라서 우리나라와 같은 기술 후발국에서는 디지털 워터마킹 기술 자체에 대한 연구를 지속적으로 수행하여 평가방법론에 대한 표준화가 이루어진 후에 실제 발생할 기술평가에 대비하여야 할 것이다. 현재 주요 기술로서 비디오와 오디오에 대한 디지털 워터마킹과 핑거프린팅의 두 가지 응용에 대한 기술개발이 일단 집중되어야 할 것으로 보인다.

2. 기타 관련 단체 활동

국내의 경우 DRM 포럼에서 워터마킹에 대한 평가의 표준화 활동을 하고 있다[13]. MPEG 이외의 다른 단체들은 MPEG과는 달리 공개적인 국제표준 단체들이 아니다. DVD 포럼, CPTWG 등은 모두 개별 업체들이 컨소시엄을 구성하여 사실상의 표준화 기술을 연구개발하는 단체들로서 산업체에서는 특히 이러한 단체들의 움직임도 주시하여야 한다[14].

참 고 문 헌

[1] http://www.watermarkingworld.org/

[2] 임양규, 국상진, 전종민, 원동호, "워터마킹 기술의 평가 기준에 관한 연구," 한국정보처리학회 춘계 학술논문집, Vol.8, No.1, 2001, pp.395-398.

[3] F.A.P. Petitcolas and R.J. Anderson,, "Evaluation of Copyright Marking Systems," *in IEEE Multimedia Systems*, Florence, Italy, 7-11 June 1999.

[4] http://www.petitcolas.net/fabien/watermarking/stirmark/

[5] http://watermarking.unige.ch/checkmark/

[6] http://poseidon.csd.auth.gr/optimark/

[7] http://www.jeita.or.jp/

[8] http://www.certimark.org/

[9] http://www.ebu.ch/

[10] http://www.sdmi.org/

[11] http://mpeg.nist.gov/

[12] http://www.cptwg.org/

[13] http://www.drm.or.kr/

[14] http://www.dvdforum.org/forum.shtml/