情 報 保 護 學 會 誌
第 11 券 第 5 號, 2001. 10

Watermarking Product Status

김 현 태*, 배 익 성*, 김 정 현*, 최 창 렬*, 정 제 창**

1. 상용 기술의 정의

디지털 워터마크 제품의 개발에 있어서 알고리즘 개발이 가장 중요한 부분이라 할 수 있다. 하지만 알고리즘 개발시 상용 제품의 적용분야가 어떤 것인가에 따른 문제 역시 중요하다. 적용분야에 따라서는 알고리즘의 수정이 불가피 한 경우가 발생할 수 밖에 없기 때문이다. 가령 예를 들어 이미지 워터마킹 제품의 알고리즘이 아무리 강인성과 화질에 있어서 사용자들의 요구를 충족한다 할지라도 이 알고리즘을 똑같은 방식으로 동영상 컨텐츠에 적용할 수 없을 수도 있을 것이다. 그것은 동영상 컨텐츠의 경우 이미지 컨텐츠와 비교할 때 워터마크 삽입 과정을 처리하는 데 필요한 시간의 차이가 너무도 크기 때문이다. 초당 한 장을 처리할 수 있는 알고리즘에서 동영상 컨텐츠를 처리 할 경우 일반적으로 24장에서 많게는 30장 정도를 처리해야 하기 때문에 동영상의 경우 실시간 워터마크 삽입 과정의 처리 속도가 무엇보다도 필요하기 때문이다. 이처럼 알고리즘 개발과정에서는 고려해야 하는 요소의 적용 분야가 어떠한 것인가에 대한 고려도 상당히 중요하게 된다. 따라서 상용 기술은 적용되는 분야와 그 기술을 사용하게 될 사용자에게 얼마나 적합한지를 우선적으로 고려해야 한다.

2. 상용 기술에 대한 요구

실제적으로 시장에서의 디지털 워터마크의 상용기술에 대한 요구는 워터마크가 삽입된 컨텐츠에 대한 공격 시 공격한 컨텐츠가 상용화 가치가 있는가 혹은 저작권자가 어느 정도까지의 컨텐츠를 보호하려 하는가에 따라 조금씩 달라질 것이다. 디지털 워터마크 기술의 적용분야를 저작권 보호를 위해서만 사용되어 지는 것은 아니다. 인증(Authentication)을 위한 워터마크 기술도 현재 상용화되어 사용되고 있다. 위에서 언급한 내용들과는 반대로 컨텐츠의 변형에 대해 감지하여 컨텐츠의 진위 및 훼손, 조작 여부를 판단하는 방법으로도 유용하게 사용되어 지고 있다. 이 경우 실질적으로 컨텐츠에 대해서 워터마크를 검출할 수 있어야 하며 변형을 가한 영상에 워터마크를 다시 삽입할 경우 변형한 사람의 정보를 포함하게 하여 변형 자체를 막을 수 있어야 한다. 이러한 기술은 현재 문서 형태의 컨텐츠와 의료 영상과 같은 컨텐츠의 위조를 막아야 하는 분야에서 사용되어 지고 있다. 또한 고려해야 할 사항은 알고리즘에 대한 reverse-engineering이 어느 정도의 시간(computation-time)이 소요되는 가에 대한 문제를 들 수 있다. 어느 기술에서나 reverse-engineering이 가능할 수 있는 면이 있기 때문이다. 이러한 문제들에 관련되어 저작권보호를 위한 분야의 오디오 워터마크 기법에 대한 강인성의 요구를 IFPI(International Federation for the Phonographic Industry)에서 제안했다[1]. IFP에서 요구한 강인성은 다음과 같다.

- 워터마크 삽입 알고리즘과 구현 후 소리의 recoding 시 sonic quality에 영향을 주지 않아야 한다.
- 삽입 정보는 다양한 공격에 강인하게 추출되어져야 한다. 필터링(filtering)과 같은 일반적인 신호처리뿐만 아니라 D/A 와 A/D 변환과 압축(MPEG Compression)과 10%정도의 time expansion 등의 공격, 노이즈(noise)의 삽입, 동일한 시스템 내에서의 워터마크 삽입, 15dB의 정도의 주파수 응답 왜곡(frequency

* (주) 실트로닉 연구소 ({kimht, isbae, petrucci, deneb} @sealtronic.com)
** 한양대학교 전자공학과 교수, (주) 실트로닉 기술이사 (jjeong@icsp2.hanyang.ac.kr)

response distortion), group delay distortion 과 notch filter 공격

- 귀에 거슬리는 음질 왜곡 없이 삽입된 정보에 대한 변경이나 제거가 불가능해야 한다.
- 주어진 signal-to-noise 레벨이 20dB 이상일 경우 에러 보정(error correction)후 20 bps 의 대역폭을 가져야 하고, 신호의 레벨이나 타입(classical, pop, speech)등에 영향을 받지 않아야 한다.

이와 유사한 표준화로 작업으로 알려진 것이 SDMI(Secure Digital Music Initiative)이고 RIAA라는 미국 은반 협회에서 주관하는 인터넷 음반업계의 컨소시엄을 말한다. 정지영상이나 디지털 비디오 나 일반적인 멀티미디어의 워터마크 삽입 조건도 유사한 요구 사항을 가진다[2].

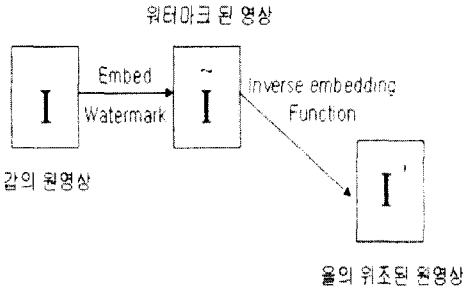
워터마크 시스템에서 공격자는 시스템의 가장 취약한 부분만을 공격할 수 있으므로 컨텐츠 소유자나 워터마킹 소프트웨어의 시스템 측면에서 모든 과정이 기밀성(security)을 유지해야 한다. 현재까지 워터마크 시스템은 각각의 다른 과정에서 공격받고 있다. 따라서 기존의 워터마크의 제거나 손상의 측면에서의 공격만큼이나 다양하게 연구되어 지고 있다. 일반적으로 워터마크 시스템의 공격에 대해서 크게 네 가지 종류로 구분 할 수 있다[3].

- Robustness attack : 일반적인 신호 처리와 압축과 같은 환경에서의 공격으로 워터마크 삽입 정보의 제거를 목적으로 한다.
- Presentation attack : 여기서는 검출기 측면에서 워터마크를 찾을 수 없게 하는 것이다. 예를 들어 워터마크가 삽입된 컨텐츠임에도 불구하고 검출기(detector)에서 워터마크 검출할 수 없게 함이다.
- Interpretation attack : counterfeiting 인해 실제 워터마크 삽입자를 결정할 수 없게 하는 공격으로 이 경우 실제 원래의 마크가 아무런 효력을 발생하지 못한다.
- legal attack : 이 공격은 법적인 문제나 기반 시스템에 관련된 공격이라 할 수 있다.

위에서 언급한 내용 중에 몇 가지를 예를 들어 설명하면, 초기에 워터마크 개발자나 공격자들이 가장 고려한 공격은 아마도 워터마크를 제거하는 공격이었을 것이다. 따라서 일반적인 신호처리나 압축 등이 다양하게 공격으로 응용되어 졌다. Public Watermark(Blind Watermarking 과는 개념이 다름)를 사용하는 Digimarc 사의 PictureMarc의 경우 공개적인 해킹 툴이 존재하기도 한다[4]. 또한 의도적인 공격을 위하여 공격 툴(Tool)이 특별히 디자인되기도 한다. SS(Spread Spectrum) 기법의 모든 워터마크 알고리즘을 공격하기 위한 비선형 필터링(Nonlinear Filtering) 기법이 있다. Langelaar, Lagendijk, Biemond[5]등이 이러한 기법을 설명하고 있다. 검출기 측면에서의 공격으로 워터마크의 검출을 할 수 없게 하는 공격은 일반적으로 잘 알려진 공격이 기하학적인 변형일 것이다. 현재 StirMark[6] 라는 프로그램이 이러한 공격에 대한 테스트를 할 수 있는 툴로써 잘 알려져 있고 이것을 적용하여 알고리즘이나 상용제품이 테스트되기도 한다. 기하학적인 변형에는 RSC (Rotation, Scaling, Crop)뿐만 아니라 Random Geometric Distortion 이라는 변형이 있다. 영상을 예로 들어 설명하면 RSC와 같은 변형은 영상 전체에 대하여 변형이 일정하게 일어나지만 Random Geometric Distortion의 경우 영상 국부적으로 변형이 가해지므로 원 영상에 대한 정보를 가지고 있지 않은 경우 워터마크를 검출하기에 어려운 변형이다. 특히 이러한 공격 중 Cropping과 같은 변형은 일반적으로 가장 빈번하게 일어나는 변형이라고 할 수 있다. 인터넷을 통해 홈페이지를 이미지를 사용하여 디자인하는 경우 홈페이지가 제공되는 네트워크의 전송률에 따라 영상을 분할하여 디자인하는 경우가 빈번하다. 이런 경우 Tracker가 Tracking 중에 이러한 영상을 인식할 경우 분할된 영상에서도 워터마크를 검출해야 한다. Cropping에 관해서 어느 정도 성능을 갖추는 가에 따라서 상용제품이 평가 되어 지기도 한다. 세 번째로 Interpretation Attack의 경우 Private Watermark에 중점적으로 초점이 맞추어진 공격이라고 할 수 있다. Protocol 공격의 경우 공격자에 의하여 Private Watermark 알고리즘 자체가 저작권 보호를 위해 적용되지 못하게 될 수 있다. 이 알고리즘의 기본적 이론은 다음과 같다.

원 영상을 I, 워터마크를 W, 워터마크 된 영상을 I′ 라고 할 때 I′가 배포되었을 경우 워터마크 검출

은 유사도 함수(Correlation Function) C와 관련되는데 C(w, x)는 원래의 워터마크 W와 검출된 워터마크 X사이의 유사도 측정하게 된다. 본질적으로 이러한 알고리즘에서는 원본과 워터마크가 삽입된 영상간의 차이를 이용하여 워터마크를 검출하는 것이다. 이러한 알고리즘의 특성을 역이용하여 공격하는 것이 Protocol 공격이다[7]. 이것을 그림 1과 같이 표현 하였다. 그림에서 갑이 컨텐츠의 생산자이면 워터마크 W를 삽입하여 인터넷을 통해 유포했다고 하면, 을은 이 컨텐츠에 대해서 아무런 대가도 지불하지 않고 컨텐츠를 사용하기 위해서 을의 워터마크를 삽입하는 것이 아니라 "빼(subtract)"게 된다. 따라서 을은 I" = I - x = I + w -x 가 되는 영상을 획득 할 수 있다. 을 I자신의 영상이라고 저작권 보호를 요청하게 되고 갑과 어떤 영상이 원본인가에 대한 비교에 들어가게 된다.



〔그림 1〕 위조된 원 영상을 만드는 과정

이때

$$I'-I=w-x,\ c(w-x,\ w) = 1 \quad (1)$$
$$I-I'=x-w,\ c(x-w,\ x) = 1 \quad (2)$$

(1)과 (2)와 같은 결과가 나타나게 되면 과연 누구의 저작권을 인정할 수 있을 것인가? 결론적으로 이 공격은 저작권 자체를 무력화시키는 공격이 되는 것이다. 이러한 공격에 대해서는 [8]에 설명되어 있다. 또한 DVD와 같은 제품에서 사용하는 워터마크 방식에 대한 공격은 워터마크 삽입 방식에 대한 정보를 공격자가 알지 않아도 되는 공격으로 "Oracle attack"이라고 불려진다. 컨텐츠의 열화를 최소화하면서 워터마크 검출기에서 워터마크가 검출되지 않을 때까지 변형을 가하는 것이다[9],[10]. 이러한 공격은 Public Watermarking 기법에서만 사용되는 것은 아니다. "Custom-tailored oracle attack"이라는 기법은 Private Watermarking에서도 적용될 수 있다[21]. 이 공격에서는 공격자가 워터마크 삽입과 추출 알고리즘을 알고 있어야 한다. 지금까지는 신호 처리에 기초 워터마크 기술의 상용화 시 요구되는 조건들이라면 다음에 논의하는 것은 실제적으로 상용화되어질 시스템의 디자인 관점에서 논의한다.

워터마크 프로그램을 포함하는 시스템을 사용하는 사용자는 워터마크 삽입 알고리즘의 이해나 기술적인 메커니즘에 대해서 제한적으로 알고 있게 된다. 따라서 워터마킹 알고리즘은 하나의 블랙 박스(black-box)로 만들어 져야 하고 어떤 특정 사용자도 이러한 알고리즘의 상세한 이해를 원하는 것도 아니다. 통상 컨텐츠를 제작하는 예술가나 디자이너들이 이러한 저작권 보호 기술이 필요할 것이다. 그러나 이러한 컨텐츠 제작자들은 자신의 컨텐츠가 워터마크의 삽입으로 인한 컨텐츠의 열화를 좋아하지 않는다. 결국 때에 따라서는 열화가 심한 컨텐츠에 대한 저작권 보호를 요구하지 않을 수 있다. 따라서 응용 분야에 따른 여러 가지 형태의 제품을 상용화시키거나 일반적인 trade-off 이상의 워터마크 알고리즘을 개발하는가에 대한 고민이 필요할 것이다. 이와 더불어 사용자 환경에 대한 문제도 야기된다. 상용화 된 PictureMark의 경우 Adobe Photoshop이라는 이미지 처리 프로그램에 존재한다. 이때 PictureMark를 사용하여 워터마크를 삽입하고 Photoshop을 이용하여 영상을 재구성할 경우 사용자는 자신도 모르는 사이에 결과적으로 영상을 변형하여 워터마크의 강인성을 떨어뜨리는 경우가 발생할 수 있다. 따라서 이 경우 재구성된 영상에 대해서 마지막에 워터마크를 삽입하는 것이 현명할 것이다. 이러한 사실을 사용자에게 인식시키거나 사용자 환경을 구성할 때 이러한 점을 고려하는 것이 좋을 것이다.

위에서 언급한 내용들을 살펴보면 현존하는 대부분의 공격은 삽입 과정보다는 검출 과정에 초점이 맞추어진 공격이다. 이러한 공격들이나 요구조건을 자세히 분석하면 저작권 보호를 위한 워터마크 알고리즘이나 이를 상용할 때 발생하는 문제점들을 최소화시킬 수 있다. 현재 상용화되어진 제품이나 혹은 상용화 준비중인 제품들은 기하학적인 변형이나 D/A,

A/D(이 경우 다양한 변형이 동시에 이루어 짐)와 같은 변형에 대한 강인성은 현재 충족되어지고 있다.

3. 상용 기술의 업체 및 제품 현황

현재 전 세계의 많은 기업들이 각각 보유하고 있는 고유의 알고리즘을 응용하여 워터마킹 제품을 선보이고 있다. 국내에서는 지난 SDMI에 두개의 기업이 참가를 하며 초기 시장을 선도하고 활발한 시장 형성을 하고 있으며 해외에서는 주로 이미지 워터마킹을 중심으로 특정 기업의 주도 하에 시장의 주류가 형성되고 있다.

우선 국내에서의 개발 회사 제품 현황을 살펴보면

a. ㈜실트로닉 테크놀로지

➡ 현재 오디오, 이미지, 비디오 워터마킹의 분야와 위/변조 인증 분야에서 제품을 보유하고 있다. MagicTag 이라는 상품명으로 저작권 보호 및 관리 제품을 출시하고 있으며 최근 삼성계열 및 일본 시장, 유럽 시장, 북미 시장에 진출하며 활발한 판매활동을 펼치고 있다. 지난 2000년 초 SDMI에 오디오 워터마킹 기술을 제안하며 시장에 진입하게 되었으며 이후 이미지 워터마킹과 비디오 워터마킹, 이외 문서 및 의료 영상의 위/변조 인증용 워터마킹 기술도 개발하였다. 특징적인 사항은 현재 원본이 없는 검출 방식으로 Stirmark에 대응이 되는 이미지 워터마킹 기술을 국내에서 유일하게 개발하였으며 소형의 여권사진 등에도 다량의 데이터를 삽입하여 안정적인 검출률을 보이는 등 해외의 유수 기업과의 기술 경쟁에 뒤지지 않고 있다. 또한 MPEG 전용 압축 방식에 적용되는 비디오 워터마킹 기술을 개발, 상용화하여 국산 신기술을 받는 등 국내 기술력의 향상에 주도적인 역할을 하고 있다.

b. 마크애니

➡ SDMI에 삼성과의 공동 제안을 통하여 시장에 진입하게 되었다. 제품은 오디오, 이미지, 비디오 분야에서 개발이 되었으며 현재 MAO, MAIM, MAV라는 상품명으로 판매하고 있다. 주로 원본을 이용한 로고 삽입 방식이 주류를 이루고 있어 Counterfeit 공격에 노출이 되고 있으며 그에 대한 보완으로 Key 삽입 방식을 추가하였으나 1bit 삽입을 통한 워터마크의 삽입 유무만을 식별할 수 있도록 하고 있다. 가장 특징적인 사항은 지난 해 STEP2000에 참가하여 오디오 워터마킹 분야에서 5개의 후보군 중 한 개의 회사로 선발된 경력을 지니고 있다.

c. 컨텐츠 코리아

➡ 이미지 워터마킹의 출시를 통하여 워터마킹 시장에 진입하였으며 Contents Guardian이라는 이름으로 제품을 판매하고 있다. 주로 ASP 형태로 서비스를 하고 있으며 Stand-alone의 형태로도 판매전략을 갖고 있다. 최근에는 ETRI로부터의 기술 이전을 통하여 오디오 상용 제품을 출시하고 두 분야로 시장을 확대하고 있다. 이미지 워터마킹에 있어서는 지금까지 원본이 필요한 기술을 바탕으로 적용하였으나 최근 원본이 없는 기술을 개발하여 신분증 등에 적용하기 위한 기술을 개발중이다.

d. 디지트리얼

➡ 최초 설립 시, 의료 영상의 압축 전송 기술을 중심으로 사업을 시작하였으며 최근 워터마킹 시장에 진입하게 된 후발 주자이다. 제품의 이름은 Waterstamp라는 이름으로 판매를 하고 있으며 검출시 원본을 필요로 하는 기술을 바탕으로 하고 있다. 이외에 Water Certificate라는 제품으로 위/변조 방지 기술을 개발하고 BMP 파일 대상의 이미지 인증 시장에 진입하고 있다.

지금부터는 현재 해외에서 활발하게 상용 서비스를 하고 있는 업체를 중심으로 설명하기로 한다. 우선 크게 분야를 나누어 세 가지 부류로 나누어 오디오 워터마킹 개발 회사를 소개하면

1. 오디오

a. Verance

➡ SDMI Phase I 에서 오디오 워터마킹 기술

이 채택되면서 주목받았던 기업으로 Aris Technology라는 회사를 합병하면서 새롭게 사명을 바꾸었다. Phase II에서도 좋은 성적을 거두어 신규 투자를 유치하였으나 SDMI 단체의 활동 중단으로 인하여 수익 모델의 부재로 고심하고 있다. 최근 오디오 워터마킹 기술을 바탕으로 한 모니터링 시스템(Confir Media) 등 응용 기술의 확충을 꾀하며 새로운 도약을 준비중이다.

b. Blue Spike

➡ SDMI에 워터마킹을 제안한 업체로 Giovanni라는 상품으로 오디오 워터마킹 기술을 판매하고 있다. SDMI에 제안한 업체 중 공격에 대한 내성이 가장 취약한 결과를 보였으며 시장에서는 아직 별다른 호응을 얻지 못하고 있는 실정이다.

c. Cognicity

➡ Ahmed Tewfik이라는 Minnesota University 출신의 개발자로 구성된 벤처기업으로 오디오 워터마킹의 초기 시장에서 주목받았던 기업이었다. 또한 SDMI에 참가, 경쟁을 하였으나 Plenary Group과의 마찰로 참가 포기를 하였다. 이후 AudioKey라는 제품으로 판매를 지속하였으나 최근 추가 펀딩의 실패로 IP의 판매를 마지막으로 사이트를 내리고 청산 절차를 진행중이다.

d. CRL

➡ 초기 EMI의 투자 기업이었으나 독립하여 다양한 연구 활동을 하고 있는 영국계의 Research 기관이다. 완성된 제품을 판매하는 형태가 아닌 연구 기술을 라이센스하여 로열티를 징수하는 형태로 사업을 하고 있는 업체이다. 또한 SDMI에 참가하여 경쟁을 하기도 하였다.

오디오 시장이 다소 SDMI에 의존하여 시장 형성에 실패한 반면 이미지 워터마킹 분야는 다양한 응용 기술을 바탕으로 업체들의 수익에 기여를 하고 있다.

a. Digimarc

➡ 현재 워터마킹 회사로서 Nasdaq에 상장되어 있는 유일한 기업이다. 주로 이미지 워터마킹만을 중심으로 사업권을 영위하여 왔으며 지적 재산권의 확보 또한 또 다른 사업의 일환으로 진행하고 있다. 최근에는 필립스와 비디오 워터마킹 시장에 진입을 하였으며 DVD 관련한 시장에서도 주도적인 역할을 하고 있다. 일반적인 이미지 워터마킹 제품은 Image Bridge라는 상품명으로 판매을 하고 있으며 온라인과 오프라인 연동의 광고 상품인 MediaBridge라는 제품으로 수익기반을 확보하고 있다. 특징적인 사항은 Stirmark에 대응이 되는 기술을 보유하고 Adobe에 기본 옵션으로 장착이 됨으로 경쟁력 확보에 유리한 장점을 가지고 있다.

b. Mediasec

➡ 독일의 Fraunhofer라는 연구기관으로부터 독점 라이센스를 취득하며 이미지 워터마킹 기술을 기반으로 글로벌 마케팅을 진행하고 있다. 제품의 종류를 지속적으로 확대하며 시장 진입을 하고 있으며 Syscop이라는 이름으로 활발히 움직하고 있다. 이외에도 비디오 및 문서 등 다양한 분야의 진출을 꾀하며 시장 진입을 서두르고 있으나 국제 표준 제안에 참가를 하지 않음으로 대외적인 인지도 취약이라는 단점을 가지고 있다.

c. Signum Technology

➡ 1997년에 영국을 중심으로 워터마킹 개발을 시작한 유럽 지역의 선두 주자이다. 제품의 이름은 Suresign과 Veridata라는 이름으로 제품의 판매를 하고 있으며 회사의 이름보다는 상품명이 오히려 더 잘 알려진 특이한 업체이다.
워터마킹 제품 뿐 만 아닌 PKI나 Information Hiding 기술을 포함한 제품을 선보이고 있다.

d. IBM

➡ 미국의 R&D Center와 일본의 연구소 양측에서 각각 개발을 하고 있다. 최근 유명한 워터마킹 기술진들을 상당수 영입하여 기술 기반을 다지고 있으며, 현재 공급하고 있는 제품은 TigerMark로 비가시적인 워터마킹을 제공하는 타 업체와는 달리 가시적인 워터마킹

으로 시장에서 판매하고 있다. 또한 지난 STEP2000에서 오디오 워터마킹 분야에서 가장 좋은 성적을 거둔 업체이기도 하다. 하지만 제품화하여 판매하는 사례는 아직 없는 것으로 알려져 있다.

e. DCT

➡ 스위스의 제네바 대학과 공동 개발을 하여 독점 라이센스 권리를 취득하고 있는 업체이다. 현재 스위스와 독일에 기반을 두고 있으며 후발 주자에 속한다. 따라서 아직까지는 시장에서 두드러진 두각을 보이고 있지 않는 실정이다.

f. Mken

➡ 일본의 초기 워터마킹 시장을 주도해온 업체로 꾸준한 시장 점유율을 보유하고 있다. 상품명은 Acuaporta라는 이름으로 판매를 하고 있으며 주로 이미지 워터마킹을 중심으로 하고 있다. 제공되는 주요 분야는 출력물에 대한 저작권 보호이며 일본내에서의 인지도를 바탕으로 적극적인 시장 진입을 하고 있다.

마지막으로 비디오 워터마킹과 관련된 업체들의 동향을 살펴보기로 한다.

a. Phillips

➡ 디지마크로부터 라이센스한 이미지 워터마킹 기술을 기반으로 비디오 워터마킹 기술을 개발하여 방송용 모니터링이 가능한 시스템을 하드웨어 기반으로 구축하였다. 또한 DVD-CCA에 관련하여 디지마크사와 공동으로 기술 표준 제안을 하고 있다.

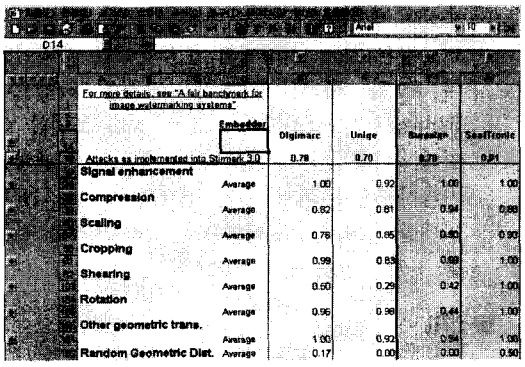
b. Sony

➡ 실제 제품의 개발보다는 향후 시장에 대한 방어의 수단으로 상당수의 특허 출원을 하고 있다. 현재 200여개의 출원 가운데 약 40개 정도의 특허가 등록되어 있을 정도로 향후 시장에 대응하기 위한 노력을 하고 있다.

4. 개발 기술의 평가 방법

상용 기술의 요구에 나와 있듯이 워터마크 알고리즘이 상용화되어 질 수 있는 제품으로서의 가치를 갖기 위해서는 여러 가지 요구조건을 만족 해야 한다. 영상 컨텐츠를 예를 들면 일반적으로 알고리즘 측면에서는 StirMark나 Unzign과 같은 영상 변형 툴로 평가하는 방법이 있다. 이 경우 그림 1과 같이 상용화 제품에 대한 스코어보드가 나와 있기도 하다.

[11]에서 결과를 다운로드 받을 수 있다. 따라서 [11]에 나타난 실험 영상과 공격들로 상용제품을 평가할 수 있다. 사용자 환경에 대한 평가는 역시 사용자가 얼마나 쉽고 편리하게 프로그램을 사용할 수 있게 만드는 가 예를 들어 워터마크 삽입된 영상이 어떠한 종류 포맷(bmp, jpg, gif등)을 지원하는가와 영상에 워터마크 삽입 정보량, 워터마크를 삽입할 컨텐츠에 대해 배치(batch processing)가 가능한가, 디지털 동영상의 경우 워터마크 검출 시 원본 영상에 대한 정보가 필요한가(막대한 양의 원본 데이터가 존재할 경우 워터마크 검출 시 실질적으로 원본 데이터를 찾아 비교하기가 어려우므로)등의 조건을 살펴보아야 할 것이다.



[그림 2] 상용제품의 벤치마킹 결과표

5. 향후 상용 기술의 추론

일반적으로, 상용화 된 (또는 상용화 될 만한) 워터마크 제품은 다음의 3가지 서로 상충되는 조건(비가시성, 강인성, 채널 용량)을 만족해야 한다. 비가시성(imperceptibility)은 워터마크가 삽입된 영상이 원본과 구별되지 않아야 한다는 것으로 실제 상용화하는데 있어서 상품성에 직접적인 관련이 있는 것이다. 강인성은 여러 가지 공격에 어느 정도 잘 견디는 정도를 나타내는 것으로, 대부분의 제품의 경우 여러 가지 공격을 한 후에 그 결과로서 그 제품의 성능을 재는 척도로써 많이 쓰인다. 마지막으

로, 채널 용량은 워터마크를 통해 어느 정도의 정보를 전달할 수 있는지의 여부를 나타내는 것으로, 대부분의 application 경우 약 48-128비트 정도가 필요하다.

현재의 대부분의 워터마크 제품의 경우, desynchronization (동기 신호를 잃게 만드는 공격) 공격에 대단히 취약한 단점을 갖고 있다. 물론, 몇몇 제품들의 경우 어느 정도의 내성을 갖고 있지만, 전체 영상이 아닌, 국부적인 부분에 desynchronization 공격이 (예를 들면, stirmark의 random geometric distortion) 가해졌을 경우에는 그다지 강인한 특성을 보이고 있지 못하다. Stirmark의 경우, 손쉽게 구할 수 있는 tool이므로 한 번 공격에 성공하게 되면, 사용자들이 손쉽게 따라 할 수 있는 위험성이 있게 된다. 따라서, 이것을 해결해야 하는 것은 대단히 시급한 문제라고 할 수 있다. 현재, random geometric distortion 공격의 경우, 국부적인 RST (rotation, scaling, translation) 모델링으로 어느 정도 해결의 실마리를 찾고 있다. 이 외에, projective transform공격에 대한 내성도 현재 많은 연구가 진행되고 있다. 또한, 비슷한 문제로 잘라내기 공격(cropping)을 들 수 있는데, 미래에는 보다 작은 크기의 영상이나 영상의 극히 일부분만을 가지고도 워터마크를 검출할 수 있는 방법들이 곧 등장할 것이다.

최근에 가장 문제가 되고 있는 또 하나의 강력한 공격 방법으로 워터마크 복사 공격 (copy attack)이 있다. 이것은 워터마크 신호를 없애는 공격이 아니라, 워터마크가 들어간 영상에서 워터마크를 key 없이 추출하여 다른 영상에 똑같은 워터마크를 넣음으로써 워터마크 검출기의 신뢰도를 떨어뜨리는 것을 목적으로 하는 공격이다. 이 공격 방법을 해결하기 위해서는 영상의 특성을 워터마크의 key와 연동시켜야 하는데, 이것 역시 최근에 많은 연구가 진행되고 있다.

또한, 워터마크의 채널 용량과 관련하여 상당히 많은 연구 결과가 쏟아져 나오고 있다. 특히, 워터마크 검출기에 있어서 원본 이미지를 노이즈가 아닌 부가 정보(side information)로 이용함으로써, 상당한 성능의 개선이 있었다. 그러나, 이 방법은 아직 desynchronization 공격에 대한 내성이 충분히 연구되어 있지 않아서, 이쪽에 대한 연구가 시급한 실정이다. 그러나, 현재의 연구 진행 결과로 비추어 볼 때, 1-2년 안에 충분히 실용화 할 기술이 나오리라 생각된다.

마지막으로, 검출기에서 워터마크의 동기를 찾기 위한 신호를 사용하여, 영상 및 워터마크가 겪은 공격을 분석하여 그 정보를 검출기에 보냄으로써 성능을 높이는 방법 등이 연구되어 지고 있다.

참 고 문 헌

[1] "Request for Proposals- Embedded Signaling Systems," International Federation for the Phonographic Industry, 54 Regent Street, London WIR 5PJ, 1997.

[2] kutter, M., and F. A. P. Petitcolas, "A Fair Benchmark for Image Watermarking Systems," in Proceedings of the SPIE 3657, Security and Watermarking of Multimedia Contents, 1999, pp. 226-239.

[3] Craver, S., B.-L. Yeo, and M. Yeung, "Technical Trails and Legal Tribulations," Communications of the ACM, vol. 41, no. 7, Jul. 1998, pp.44-54.

[4] Anonymous, "Learn Cracking IV-Another Weakness of PictureMarc," posted by 〈zguan.bbs@bbs.ntu.edu.tw〉 on 〈news : tw.bbs.comp.hacker〉, mirrored on 〈http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/digimarc_crack.html〉, 1997. Includes instructions to override any Digimarc watermark using PictureMarc.

[5] Langelaar, G. C., R. L. Lagendijk, and J. Biemond, "Removing Spatial Spread Spectrum Watermarks by Non-linear Filtering," in 9th European Signal Processing Conference, Island of Rhodes, Greece, 8-11 Sep. 1998, pp. 2281-2284.

[6] Petitcolas, F. A. P., R. J. Anderson, and M. G.Kuhn, "Attacks on Copyright Marking Systems," in Proceedings of the Second International Workshop on Information Hiding, vol. 1525 of Lecture Notes in Computer Science,

Springer, 1998, pp. 218-238.
[7] Craver, S., et al., "Resolving Rightful Ownerships with Invisible Watermarking Techniques : Limitations, Attacks, and Implications," IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, May 1998, pp. 573-586.
[8] Wenjun Zeng, Bede Lium, "A Statistical Watermark Detection Technique Without Using Orginal Images for Resolving Rightful Ownerships of Digital Images", IEEE Transactions on Image Processing, Vol. 8, N.11, 1999.
[9] Perrig, A., A Copyright Protection Environment for Digital Images, Diploma dissertation, Ecole Polytechnique F?d?rale de Lausanne, Lausanne, Switzerland, Feb. 1997.
[10] Linnartz, J.-P., M. G., and M. van Dijk, "Analysis of the Sensitivity Attack Against on Information Hiding, vol. 1525 of Lecture Notes in Computer Science, Springer, 1998, pp.258-272.
[11] http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/index.html

〈著 者 紹 介〉

김 현 태 (Hyuntae Kim)
본 호의 "Watermarking Technology Trend" 저자소개 참조

배 익 성 (Bae Ik Seong)
본 호의 "Watermarking Technology Trend" 저자소개 참조

김 정 현 (Jeonghyun Kim)
본 호의 "Watermarking Technology Trend" 저자소개 참조

최 창 렬 (Changryoul Choi)
본 호의 "Watermarking Technology Trend" 저자소개 참조

정 제 창(Jechang Jeong)
본 호의 "Watermarking Technology Trend" 저자소개 참조