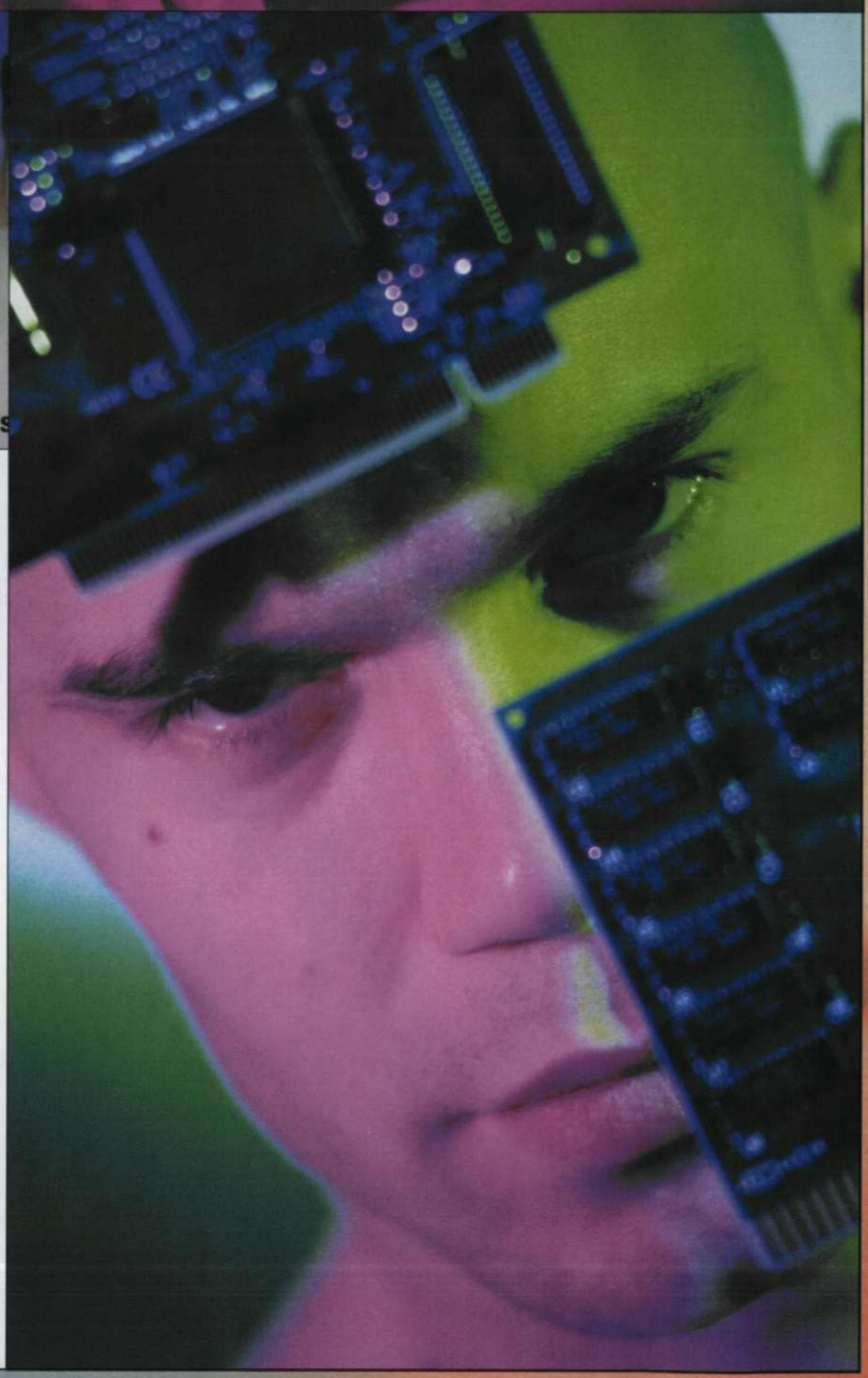
디지털 워터마킹(Digital Watermarking)

"이미지, 영상, 음악 등 디지털 콘텐츠 저작권 보호기술로 떠올라"

김진영 실트로닉테크놀로지 신사업기획팀장



연재순서

어린 시절 방학 숙제용으로 제작된 노란색 표지의 '탐구생활'을 기억하시는 분들이 많이 계실 줄 안다. 그 중에서 '과일즙으로 글씨 쓰기'란 것이 있었는데 실제 글씨를 쓰고 말리면 아무 표시가 없다가 불을 쬐면 글씨가 나타나는 신기한 경험을 한 적이 있음을 필자는 떠올리곤 한다. 지금과 같은 시대에서는 단순한 놀이에 불과하게 생각되는 이 방식은 고대부터 전쟁이나 위급한 상황에서 적을 속여 중요한 정보를 전달하기 위해서 널리 사용해 왔었다.

워터마킹의 유래

원래 워터마크(Watermark)란 고대 이집트에서 파피루스(종이)를 만드는 과정에서 섬유질을 물에 풀었다가 물을 압착하기 위해 틀을 사용하는 과정에서 나온 마크를 말한다. 중세에는 작전명령서 같은 기밀문서의 안전한 배송을 위해, 또는 연애편지와 같은 개인적인 메시지 전달을 위해 사용되기도 했었고, 제지업자들은 자신들의 고유 상품임을 증명하기 위해 종이에 마크를 삽입하기도 했었다.

현대에 와서는 지폐를 제조하는 과정에서 종이가 젖어 있을 때 인쇄를 하고 말린 후 양면에 인쇄를 하면 빛을 통해서만 확인할 수 있는 그림이 들어가 있는데, 이것을 워터마크라 한다. 이는 위조지폐를 확인하기 위한 방법으로 흔히 쓰이는데 우리나라 지폐권에 쓰이고 있으며, 미 항공우주국(NASA)를 비롯해 미 연방수사국(FBI) 등에서 보안 기술 중의 하나로 활용되고 있다.

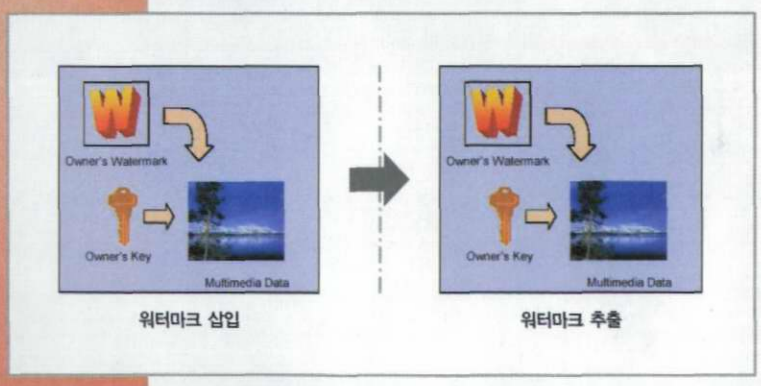
오늘날 디지털 멀티미디어의 발달에 따라 디지털 워터마크라는 개념이 등장하게 되었고, 기존의 오프라인 성격과는 다른 온라인에 적용되기 시작하면서 그 개념이 확산일로에 있다. 또한 단순 저작자 표시 이외에 관련 정보(입력 시간, 입력자, 입력 장소 등)을 다양하게 삽입할 수도 있다.

〈그림1〉 워터마크는 우리의 일상 생활 가까이 있다

디지털 워터마킹의 정의와 일반적 특성

디지털 워터마킹이란 이미지, 영상, 음악 등의 디지털 저작물의 저작권을 보호하거나 위 · 변조를 감별하고 추적하기 위해서 특수한 형태의 워터마크를 삽입하고(Embedding), 추후 검출(Detecting)하는 기술적 방법을 뜻한다. 저작물 데이터의 전부를 바꾸는 암호화와는 달리 워터마크 삽이 후에도 원본 신호를 유지하는 것을 특징으로 한다.

〈그림2〉 워터마크 삽입/추출 개념도



이전 연재에서 살펴본 DRM은 암호화가 근간 기술을 이룬다. 암호화의 기본 특성은 권한이 없는 사람들의 데이터에 대한 접근 권한을 제한함으로써 복제 방지나 기타 보안을 유지하는 것이었다. 이는 저작물에 대해서 지불/결재 과정을 거치지 않은 일반 사용자들의 접근 자체를 봉쇄하는 것이며, 개념적으로는 암호화가 풀린 이후의 상황에서는 콘텐츠 보호가 어려운 상황이 초래될 수 있다.

이와는 달리 워터마킹 기술은 데이터에 대해 접근 제한을 두지 않으며, 워터마크는 항상 저작물 자체에 존재하므로 언제든지 검출할 수 있다. 또한 워터마킹(별도의 언급이 없는

〈그림3〉 가시적 워터마크의 대표적인 사례

한 디지털 워터마킹으로 총칭함)은 사전적 의미의 보호시스템인 DRM과는 달리 사후적 의미의 저작권 보호 관리 툴이라고 할 수 있다. 즉 특정 이미지의 저작권자가 이미지를 생성해 온라인으로 배포함에 앞서 워터마크를 삽입한 후에 불법적인 사용 사실을 인지하게 되면 그 이미지를 회수해 추출을 하게 되는데 이때 검출된 워터마크를 증빙자료로 불법 사용자에게 법적인 압력을 행사할 수 있게 된다.

이런 과정을 가능케 하는 것은 바로 워터마킹 기술의 '비가시성'이다. 워터마킹 기술은 워터마크를 삽입한 후에도 화질이나, 음질, 이미지에 변화가 없이 인간의 시각이나 청각으로 감지하지 못하도록 아주 미세하게 삽입해 워터마크 삽입여부를 알 수 없게 하는 것을 기본적이고 중요한 특성으로 한다. 이런 워터마크를 'Imperceptible 워터마크'라고 한다. 만일 저작권 정보를 담고 있는 워터마크에 쉽게 접근할 수 있다면 마크를 변형해 없애는 공격이 가능하기 때문에 저작권 보호라는 본래의 목적을 달성하기 어려울 것이다.

물론 비인지성과는 달리 뚜렷하게 워터마크를 표시해 디지털 저작물의 복제 및 불법 사용 및 위·변조를 억제하는 효과를 가질 수도 있는데 이를 'Perceptible 워터마킹'이라고 한다. 방송사나 음반사들이 주로 사용하는 방식으로 원래 사후적 툴인 워터마킹을 사전에 심리적으로나마 불법 행위에 대한 부담감을 지우려는 의도로 사용되기도 한다.

특성에 따른 워터마킹 기술 분류

가시성과 관련해 구분하는 방법 외에도 그 응용 분야 및 용도에 따라 크게 Robust 워터마킹과 Fragile 워터마킹으로 구분할 수 있다. 저작물에 대한 불법 행위에 대해 워터마크가 얼마만큼의 강인성을 제공하는가가 중요한 기준이 된다.

Robust 워터마크

우선 삽입되는 정보로 인해 원래의 저작물이 사람이 인지할 수 있을 만큼의 손상 및 품질 저하가 있어서는 안되며, 저작권 정보가 되도록 여러 가지 공격(JPEG/MPEG 압축, 회전, 크기 조절, 부분 절단 등)시에도 검출돼야 하며, 인쇄나 스캐닝 시의 '디지털 → 아날로그, 아날로그 → 디지털' 변환에도 견딜 수 있어야 한다. 이렇게 저작권 정보를 끝까지 검출하게 보장함으로서 저작물에 대한 권리 표시를 할 가치 있는 콘텐츠에 적용된다. 이를테면 방송사의 방송물이나 음반물에 적용될 수 있

워터마크의 분류기준

분류기준	방식	비고
마크의 인지가능 여부	Perceptible 워터마킹	대부분 fragile 워터마킹
	Imperceptible 워터마킹	강인성 제공위한 조건
강인성 제공여부	Robust 워터마킹	저작권 보호 제공
	Fragile 워터마킹	인증/무결성 제공
삽입/검출 방식	Private marking	검출시 원본 필요
	Public marking	검출시 원본 불필요
	Public key marking	공개키 워터마킹
마크의 삽입 영역	Spatial Domain	신호처리에 약한 특성
	Frequency Domain	HVS 특성 고려

겠다.

하지만 아직까지 전 세계적으로 완벽하게 상기 기술한 외부공격에 100% 완벽한 방어를 할 수 있는 워터마킹 기술은 개발되지 못했다. 학계를 중심으로 많은 연구가 진행되고 있으며, 관련 업계들도 연구작업을 진행중이나 아직은 기술적 수준이 상업화를 충분히 지원할 수 있을 정도는 아니다.

물론 다른 시각에서 접근할 수도 있겠다. 보안 관련 제품이 거의 그렇듯 보안성이 높아지면 사용자 편의성이나 성능이 떨어지게 돼있다. Robust 워터마킹에서도 강인성을 높이기 위해 복잡한 embedding을 거치게 되면 detecting 시 많은 로드를 가지게 되는 위험성이 크다. 따라서 시장성 또는 상품성과 관련해서는 Robustness와 Complexity와의 상호 조율이 필요하다 하겠다.

Fragile 워터마크

워터마크의 강인성을 통해 소유권 주장이나 저작권과 관련된 목적으로 사용된 것이 Robust 워터마킹이었다면 워터마크 자체가 아주 작은 외부 공격에도 깨지게(검출되지 않게) 만들어 원본 여부를 감별해내는 것이 Fragile 워터마크이다. 따라서 워터마크가 검출되는 저작물은 위 · 변조가 진행되지 않은 원본임을 증명할 수 있게 해 '인증'과 '무결성'에 대한 증명을 하게 된다. 또한 워터마크 삽입기술에 따라 어느 부분이 위 · 변조되었는지 위치를 추적할 수 있게 하는 기능까지 추가할 수 있다. 대표적으로 DVR에 적용돼 녹화된 데이터에 대한 인증을 기대할 수 있게 되었다.

이밖에 Robust와 Fragile의 중간 형태로서 일정 수준 이상의 변화에만 워터마크가 손상되는 Semi-fragile 워터마크가 있는데, 압축이나 코딩 등과 같은 경우는 비의도적인 공격으로 인식해 살아 남고, Copy & Paste와 같은 의도적 공격에는 공격 위치를 확인할 수 있는 워터마크이다. 원본 필요 유무에 따라 Private 마킹, Public 마킹, Public Key 마킹 등으로 구분할 수 있다. Private 마킹은 워터마크 검출 시 원본 데이터가 필요하며, 검출 결과로 삽입되었던 마크를 출력해 입력한 마크와 삽입돼 있는 마크를 비교해 진위여부를 판별한다.

Public 마킹은 원본 없이 워터마크 삽입에 사용된 Key만으로 검출을 시행해 삽입된 워터마크를 얻을 수 있는 방법이다. 원본 없이 키에 의존해 추출하기 때문에 Private 마킹에 비해 상대적으로 설계와 구현이 어렵다. 하지만 원본이 필요 없기 때문에 관리와 사용의 편의성은 높다하겠다.

Public Key 마킹은 가장 발전한 형태로서 공개키 기반으로 삽입, 추출을 진행하는 방식이다. 즉 사용자의 비밀키로 워터마크를 삽입하며, 사용된 비밀키에 대응되는 공개키로 워터마크를 검증할 수 있다. 공개키 방식의 특성상 누구나 마크를 검증해 소유권 정보를 획득할 수 있으나 워터마크가 제거된 원본을 얻을 수 없어야 한다.

또한 워터마크가 삽입되는 공간에 따라 Spatial 영역과 Frequency 영역으로 나누어 볼 수 있다. 시간 · 공간 영역에 워터마크를 삽입하는 방식은 디지털 데이터에 직접 워터마크를 삽입하게 되는데 이럴 경우 변형이나 신호처리 기술에 의해 워터마크가 쉽게 깨지는 특성을 갖고 있기 때문에 주로 Fragile 워터마크 분야에 쓰이고 있다. 주파수 영역에 워터마크를 삽입하는 방식은 인간이 인지하기 힘든 주파수 대역으로 변환 후 변환 영역에서 삽입을 하게 된다. 시간 · 공간 영역에 워터마크를 넣는 것보다는 보다 강인한 성질의 워터마크를 특징으로 한다.

이상 간략하게 디지털 워터마킹의 정의와 워터마크의 종류에 대해 살펴보았다. 이전 연재를 꾸준히 살펴보신 독자들이시라면 DRM과는 상이한 점이 있음을 아셨으리라 생각한다. 기술적인 관점에서 보자면 근본적으로 DRM와 워터마킹은 차이점이 더 많다고 할 수 있다. 하지만 상품의 관점이나 효용의 관점에서 본다면 둘은 서로간의 보완재 역할을 할 수 있을 것으로 생각한다.

앞으로 3회의 연재를 통해 워터마킹 기술의 여러 가지 응용 분야와 관련 현황에 대해 살펴볼 예정이니 많은 관심과 기탄 없는 조언을 독자 여러분들께 요청드리는 바이다.