정규논문 (Regular Paper)
방송공학회논문지 제18권 제2호, 2013년 3월 (JBE Vol. 18, No. 2, March 2013)
http://dx.doi.org/10.5909/JBE.2013.18.2.196
ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

포렌식마크 기술 평가 및 인증 기술

오 원 근[a)‡]

Technologies for Forensic Marking Certification

Weon - Geun Oh[a)‡]

요 약

본 논문에서는 국내 디지털 저작권 보호 업체 혹은 대학 및 연구소에서 개발하고 생산하는 포렌식마크 기술의 품질을 객관적으로 평가할 수 있는 평가절차와 평가지표를 정량적으로 제시하였다. 포렌식마크 기술을 객관적으로 평가하기 위해서 본 논문에서는 우선, 구매자 정보가 삽입된 테스트 영상의 공격 항목과 수준을 정하고, 포렌식마크 정보의 추출 성능을 평가하기 위한 평가절차로서 평가항목, 평가기준, 평가절차를, 그리고 인증을 위해서는 포렌식마크 기술의 신뢰성에 대한 통계정보를 포함하는 인증서를 생성하기 위한 인증절차를 포함하였다. 이러한 포렌식마크 기술의 평가 및 인증 기술은 기술 개발자에게는 자신들이 개발한 포렌식마크 기술에 대한 객관적인 평가결과를 미리 알아볼 수 있어서 기술의 상품성을 점검할 수 있고 소비자 입장에서는 객관적이고 보편타당성 있는 평가결과에 대한 신뢰를 가질 수 있다. 평가자 입장에서는 기술 평가를 통해 객관적이고 정량적인 평가 결과를 얻을 수 있어서 상대적인 우열을 가리기가 용이해지는 편리성을 얻을 수 있다. 이를 통하여 포렌식마크 기술의 발전과 디지털 저작권 보호 시장의 활성화에 일조를 할 수 있을 것으로 사료된다.

Abstract

The importance of Digital Rights Protection technologies, especially the forensic marking, is getting larger and larger as the demand for the digital contents is increased. But the technologies for the evaluation of forensic marking is not set up properly due to the conflicts between interested parties and technical difficulties. Therefore to evaluate the performance of forensic marking objectively, image and video modification items/levels and evaluation criteria are essential. This paper suggests the quantitative system for evaluating the performance of forensic marking objectively. By providing the opportunity to evaluate the Digital Rights Protection product in objective and quantitative manner, forensic marking industry can expedite its technology development and consumer can get objective and universally validated performance result. It is expected this technology could help revitalizing the related industries and help expediting the development of forensic mark technologies.

Keyword : Forensic Marking, DRM, Evaluation, Certification

a) 한국전자통신연구원 (Creative Content Research Laboratory, ETRI)
‡ Corresponding Author : 오원근 (Weon-Geun Oh)
E-mail: owg@etri.re.kr
Tel: +82-42-860-5572 Fax: +82-42-860-1121
※ 본 연구는 지식경제부 정보통신표준화 및 인증지원사업의 일환으로 수행하였음. [2012-PM10-04, 디지털 콘텐츠 핑거프린팅 표준개발].
· Manuscript received August 30, 2012 Revised January 14, 2013 Accepted February 5, 2013.

I. 서 론

디지털 콘텐츠는, 그 특성상 내용의 손실 없이 무한복제가 가능하기 때문에 인터넷 상에서 불법복제 및 유통의 가능성이 매우 높다. 실제적으로 2011년 한 해 동안 우리나라 국민 10명 중 3명 이상이 온·오프라인 상에서 불법복제물을 이용했으며 국민 1인당 한 달 평균 4.35개를 이용하여 약 874원(1년 평균 약 10,488원)의 불법복제물을 구입하거나 이용한 것으로 조사되었다[1]. 이러한 디지털 콘텐츠 불법 복제/유통의 근본적인 해결책은 콘텐츠 사용자의 의식의 변환과 함께 이들 콘텐츠가 인터넷 상에서 불법으로 유통되는 것을 근본적으로 차단하는 디지털 콘텐츠 저작권 보호 기술의 개발이다.

현재 일반적으로 사용되어지고 있는 디지털 콘텐츠의 저작권 보호기술 중 대표적인 기술이 디지털 저작권 관리 기술인데, 이 중에서도 포렌식마크 기술은, 디지털 콘텐츠에 디지털 콘텐츠를 구매한 사용자의 정보를 삽입함으로써 이후에 발생하게 될 콘텐츠의 불법 배포자를 추적하는 데 사용되는 기술이다[7][8][9]. 즉 디지털 워터마킹을 사용하였을 때는 판매되는 모든 콘텐츠에 삽입되는 정보(저작권 정보)가 동일한 반면, 포렌식마크 기술을 사용하였을 때는 판매되는 콘텐츠가 구매한 사용자들마다 조금씩 다른 정보를 가지므로 만약 콘텐츠가 불법적으로 재배포가 된다면 해당 콘텐츠 내에서 포렌식마크 정보를 추출하여 어떤 구매자에게 판매된 콘텐츠임을 식별할 수 있게 되어 법적인 조치를 가할 수 있게 된다. 따라서 일반적인 구매자들로 하여금 불법적인 재분배에 대한 의욕을 저하시키고, 생산자들의 창작의욕을 고취시켜 디지털 콘텐츠 산업의 발전에 좋은 영향을 줄 수 있을 거라 기대된다.

이러한 배경으로 국내외 산업체에서는 다양한 기술을 활용하여 VOD 스트리밍을 보호하고[3], 공유 콘텐츠에 대한 저작권 침해사항을 감시하거나[4], 콘텐츠의 중복여부의 판별[5] 및 동일 콘텐츠 제공 서비스[6] 등을 하고 있다. 그러나 비디오 포렌식 마크의 삽입속도가 아직 느리고(1.5Mbps 스트리밍의 경우 300ms의 지연), 일부 공격(캡쳐후 재인코딩의 경우)이 가해진 파일에서는 포렌식 마크의 검출성능이 90% 정도로 실시간성과 정확성이 떨어져 지속적인 기술개발이 필요한 상황이다.

한편, 포렌식마크 기술을 평가하는 방법에 대한 기술은 업계의 이해관계와 기술적인 어려움 때문에 아직 잘 정비되어 있지 못하다. 현재는 여러 다른 기관에서 각기 자기들 나름대로 평가해서 사용하고 있으나 그들이 어떤 식으로 포렌식마크 기술을 평가하는지에 대한 내용은 알려져 있지 않고, 공모공격에 대한 평가모델[11]이 일부 보고되고 있을 뿐이다.

포렌식마크 기술의 평가 및 인증을 위해서는 다양한 포렌식마크 기술에 대한 평가 절차를 반복하여야 하며, 평가 결과에 대한 안정성과 신뢰성을 확보하기 위해서는 같은 포렌식마크 기술에 대해서도 성능 테스트를 여러 차례 실행하는 것이 바람직하다. 이렇게 함으로써 포렌식마크 기술이나 기술의 평가 및 인증이 객관적으로 이루어 질 수 있어, 평가 결과를 상호 신뢰할 수 있게 되기 때문이다. 이를 위해서는 포렌식마크 기술 평가 및 인증절차를 자동화하는 것이 효율적이며, 이를 위해 인증기관에 설치된 평가 및 인증 엔진에 연구실의 연구, 개발자나 산업체의 기술 개발자 및 수요자가 인터넷을 통해 쉽게 접근하고 평가를 받을 수 있도록 하는 방식이 필요하다.

II. 포렌식마크 기술의 개요

포렌식마크 기술(forensic marking)은 콘텐츠 관련 정보를 디지털 콘텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하다고 볼 수 있으나, 저작권자나 판매자의 정보가 아닌 디지털 콘텐츠를 구매한 사용자의 정보(이하 포렌식마크라 함)를 삽입함으로써 이후에 발생하게 될 콘텐츠 불법 배포자를 추적하는 데 사용되는 기술이다.

포렌식마크 기술은 워터마킹의 확장 기술로 콘텐츠의 상거래 시 소유자의 정보뿐만 아니라 구매자의 정보도 포함하는 정보를 콘텐츠에 삽입하여 후에 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 저작권 보호 기술이다[14][15][16]. 즉 디지털 워터마킹을 사용하였을 때는 판매되는 모든 콘텐츠에 삽입되는 정보가 동일한 반면, 포렌식마크를 사용하였을 때는 판매되는 콘텐츠가

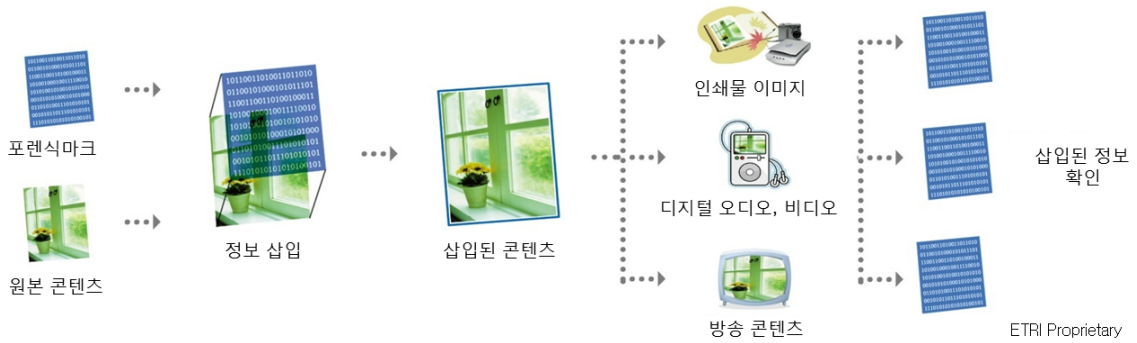

그림 1. 포렌식마크 기술의 개념
Fig. 1 Forensic Marking

구매한 사용자들마다 조금씩 다른 정보를 가지므로 만약 콘텐츠가 불법적으로 재배포가 된다면 해당 콘텐츠 내에서 포렌식마크를 추출하여 어떤 구매자에게 판매된 콘텐츠임을 식별할 수 있게 되어 법적인 조치를 가할 수 있게 된다. 따라서 일반적인 구매자들로 하여금 불법적인 재분배에 대한 의욕을 저하시키고, 생산자들의 창작의욕을 고취시켜 디지털 콘텐츠 산업의 발전에 좋은 영향을 줄 수 있다.

이러한 포렌식마크 기술은 소유권에 대한 인증뿐만 아니라 개인 식별 기능까지 제공해야 하므로 기존의 워터마킹이 갖추어야 할 요구사항인 비가시성, 견고성, 유일성과 더불어 공모 허용, 비대칭성, 익명성, 조건부 추적성 등이 부가적으로 필요하다.

III. 포렌식마크 기술의 성능 평가 모델

워터마킹 기술은 불법복제 콘텐츠로부터 소유자의 워터마크를 추출함으로써 소유권을 명확히 해주는 기능을 하지만 불법 행위자를 가려낼 수는 없다. 반면에 포렌식마크 기술은 콘텐츠 내에 소유자 정보와 구매자 정보를 함께 포함하는 포렌식마크 정보를 삽입하여 후에 불법으로 배포된 콘텐츠로부터 배포자가 누구인지를 역추적할 수 있도록 해주는 기술이다. 불법 배포자를 추적할 수 있다는 관점에서 포렌식마크 기술은 부정자 추적(traitor tracing) 기술로도 논의될 수 있다. 포렌식마크 기술에서는 콘텐츠에 관한 정보가 삽입된 디지털 콘텐츠를 조작하여 삽입정보 신호를

표 1. 포렌식마크 기술의 요구사항
Table 1. Requirements of Forensic Marking

요구사항	설 명	비 고
강인성 (Robustness)	포렌식마크가 삽입된 콘텐츠의 변환, 재샘플링, 재양자화, 압축 등과 같은 일반적인 신호 처리뿐만 아니라 회전, 이동 등 기하학적 영상 변환에도 삽입정보가 유지되어야 한다.	워터마크 기술의 요구사항과 동일
비가시성 (Imperceptibility)	콘텐츠의 가치를 그대로 유지함과 동시에 삽입 정보가 인간의 시각이나 감각에 의해 감지될 수 없어야 한다.	
유일성 (Uniqueness)	검출된 삽입정보는 저작자/구매자를 명확하게 특정할 수 있어야 한다.	
공모허용성 (Collusion tolerance)	포렌식마크가 삽입된 콘텐츠는 삽입되는 내용이 구매자마다 다르므로 다수의 구매자들이 자신의 콘텐츠를 비교하여 삽입 정보를 삭제하거나 다른 사용자의 정보를 삽입한 콘텐츠로 위조하여 배포할 수 있으므로, 이와 같은 공격에 견고하기 위해 아무리 많은 콘텐츠가 주어지더라도 포렌식마크를 찾거나 삭제할 수 없어야 하고 새로운 포렌식마크를 생성할 수 없어야 한다.	포렌식마크 기술의 요구사항
비대칭성 (Asymmetry)	포렌식마크가 삽입된 콘텐츠는 판매자는 알지 못하고, 구매자만이 알아야 한다.	
익명성(Anonymity)	구매자의 익명성을 보장해야 한다.	
조건부 추적성 (Conditional Traceability)	정직한 구매자는 익명으로 유지되는 반면, 불법 배포한 부정자는 반드시 추적할 수 있다.	

제거하거나, 삽입정보 신호를 검출할 수 없게 만드는 강인성에 대한 공격(attack)과, 여러 명의 악의적인 구매자들이 콘텐츠간의 상이성을 이용하여 포렌식마크 정보를 지우거나 공모자 이외의 다른 구매자의 정보를 포함한 새로운 콘텐츠를 생성할 수 있는 공모 공격(collision attack)[10][12][13] 이 있다.

불법 복제 추적을 위해서는 공모한 구매자를 찾아내는 것이 목적이고 공모자 입장에서는 자신의 신분을 보호하는 것이 목적이다. 포렌식마크 기술은 불법 복제에 대한 방지 기술이기보다는 불법 복제에 대한 검출과 증명과정을 통한 수동적인 불법 복제 억제기술이라 할 수 있다. 최근에는 포렌식마크 기술과 웹 검색 기술을 함께 활용하여 능동적으로 웹상에서 불법 복제 콘텐츠를 검색해주는 불법 복제 콘텐츠 추적기술에 대한 연구가 진행중에 있다. 이러한 포렌식 마크 기술은 그 목적에 따라 다양한 기술적 요구사항이 제기되는데 표 1은 포렌식마크 기술에서 불법 배포자를 추적하기 위한 요구 사항이다.

IV. 기술평가 항목

포렌식마크 기술의 성능을 평가하기 위해서는 콘텐츠에 삽입된 포렌식마크에 대한 공격이 필요한데, 워터마킹과는 달리 구매자 정보를 동일 콘텐츠에 삽입하는 포렌식마크 기술에 대한 공격의 종류는 크게 포렌식마크 기술의 강인성에 대한 공격과 포렌식마크의 위조에 관한 공모공격이 있다(표 2 참조).

표 2. 공격의 종류 및 내용
Table 2. Type of Attacks

공격의 종류	공격내용	대상 콘텐츠
강인성 공격	콘텐츠에 관한 정보가 삽입된 디지털 콘텐츠를 조작하여 삽입정보 신호를 제거하거나, 삽입정보 신호를 검출할 수 없게 만들거나, 또는 위조된 삽입정보를 만들어 삽입한 사람이 저작권 및 소유권을 주장할 수 없도록 하는 것과 같은 강인성에 대한 공격	정지영상
		동영상
공모공격	공격자는 여러 개의 콘텐츠를 서로 비교하여 구매자 정보를 제거하거나 혹은 유추하여 다른 구매자 정보를 삽입하는 공격	정지/동영상 공통

1. 공격 항목

1.1 정지영상(image)에 대한 강인성 공격

공격 항목	공격방법
회전공격	영상을 다음의 각도로 회전을 실시한다. 1도, 4도, 7도, 15도, 16도, 30도, 37도, 45도
이동공격	영상을 다음의 픽셀만큼 이동한다. 0.1픽셀, 0.2픽셀, 0.3픽셀, 0.4픽셀, 0.5픽셀
업샘플링	영상을 다음과 같은 비율로 업 샘플링을 각각 적용한다. 1:1.1, 1:1.4, 1:1.5, 1:1.6, 1:2, 1:3, 1:4
다운 샘플링	영상을 다음의 비율의 다운 샘플링을 각각 적용한다. 1:0.9, 1:0.8, 1:0.7, 1:0.5, 1:0.4, 1:0.2, 1:0.1
필터링	영상에 smoothing, sharpening, median filtering을 적용한다. Median filtering은 3×3, 4×4, 5×5의 윈도우 사이즈를 사용한다. gaussian filter와 sharpening filter는 다음의 마스크를 사용한다. gaussian filter, $h=\begin{bmatrix}1&2&1\\2&4&2\\1&2&1\end{bmatrix}$, sharpening filter, $h=\begin{bmatrix}0&-1&0\\-1&5&-1\\0&-1&0\end{bmatrix}$
클립핑	영상의 가장자리를 전체 영상에서 가로, 세로 1/10, 2/10, 3/10, 4/10, 5/10를 제거한다.
D/A와 A/D 변환	디지털(Digital) 정지영상을 아날로그(Analog)로 변환하고, 재차 디지털로 변환한다.
압축	JPEG 압축으로서 QP 4, 6, 7, 10, 15, 20에 대하여 압축을 한다.
화면율(aspect ratio) 변형	영상의 수평/수직 스케일 요소를 다르게 적용하여 변형한다.
수평 플립	영상을 좌우 방향으로 플립한다.
쉬어링(shearing)	영상을 X축 및 Y축으로 (0, 1), (0, 5), (1, 0), (5, 0), (1, 1), (5, 5) 만큼 변형한다. (x, y) 괄호안의 파라미터는 각각 X축 및 Y축을 가리키며 X축으로 x% 만큼을, Y축으로 y% 만큼을 이동한다.
선형기하 변형	영상을 아래 선형 기하변형식을 사용, 각각의 계수 (a, b, c, d)에 대해 다음의 값들을 취해 선형 기하변형을 시킨다. (1.010, 0.013, 0.009, 1.011), (1.007, 0.010, 0.010, 1.012), (1.013, 0.008, 0.011, 1.008), $x' = ax + by$ $y' = cx + dy$
복합변형 (클립핑, 이동, 다운샘플링)	원 영상을, 클립핑->이동->다운샘플링의 순서로 다음과 같은 3개의 비율로 순차적으로 변형한다. (1/10, 0.1픽셀, 1:0.9), (2/10, 0.3픽셀, 1:0.7), (3/10, 0.5픽셀, 1:0.5)

1.2 동영상(video)에 대한 강인성 공격

공격 항목	공격방법
H.264 압축	H.264 압축으로서 QP 36, 28, 18에 대하여 압축한다. 여기서 H.264는 JVT 동영상 표준화 그룹에서 제정한 동영상을 위해서 만들어진 손실 압축 방법 표준이다. 또, QP(Quantization Parameter)는 동영상의 품질을 제어하는 변수이다.
H.264 칼라 포맷 변경	입력 동영상의 칼라 포맷을 4:4:4, 4:2:2, 4:2:0로 변경시킨다. 4:4:4는 3개의 칼라 성분이 같은 해상도를 갖고, 4:2:2는 밝기 성분에 대해 색 성분이 2:1의 저 해상도를 갖는다. 4:2:0는 밝기 성분에 대해 색 성분이 4:1의 저 해상도를 갖는다.
H.264 비트 깊이 변형	입력된 10 비트(bit)의 동영상을 8 비트로 변화 시킨다.
동영상 압축 포맷 변형	H.264로 부호화된 동영상을 MPEG-4 심플 프로파일의 포맷으로 변형한다.
H.264 동영상 크기 변형	입력된 비디오 동영상의 크기를 CIF(Common Intermediate Format) 영상 크기와 QCIF(Quarter Common Intermediate Format) 영상크기로 변형한다.
H.264 프레임율 변형	입력된 비디오 동영상의 프레임율(frame rate)을 1/2, 4/1, 1/8로 낮춘다. 프레임율은 비디오 동영상을 구성하는 1초간 정지영상의 개수이다.
H.264 랜덤 패킷 손실율	비디오 동영상의 전송 단위인 패킷의 손실율을 20%, 10%, 5%로 변화시킨다.
H.264 클립핑	비디오 동영상을 구성하는 영상의 주변 정보를 10%, 20%, 30% 삭제하여 90%, 80%, 70%의 영상으로 구성되는 동영상으로 변화시킨다.
밝기 변환	입력된 비디오 동영상의 밝기를 다음의 비율로 변화시킨다. ±20%, ±10%, ±5%
색상/흑백 변환	입력 비디오 동영상으로부터 밝기 성분만을 가진 동영상을 생성한다.
복합변형 I (Capturing on camera (at SD resolution)	SD 해상도를 기준으로 동영상 화면이외의 영역이 0%, 5%, 10%이 되도록 카메라로 비디오 영상을 촬영한다.
복합변형 II (Analog VCR recording & recapturing)	디지털->아날로그->VCR 촬영의 반복횟수를 각각 1회, 2회, 3회 시행한다,

1.3 공모공격

공격 항목	공격방법
평균화 공격	다수공모자가 포렌식마크가 삽입된 다수의 콘텐츠를 서로 평균하여 새로운 콘텐츠를 생성하는 공격법. 테스트 콘텐츠수를 다음과 같이 평균공격을 실시한다. 5, 7, 10, 15, 20 $d_j' = d_j + \frac{1}{K}\sum_k w_{kj}$ 여기서, d_j'는 공모된 콘텐츠, d_j는 콘텐츠의 계수값이고, w_{kj} 포렌식마크정보, K는 테스트 공격에 사용된 콘텐츠 수이다.
최대최소공격	포렌식마크가 삽입된 콘텐츠에서 최소값과 최대값을 구한 후 그 평균값으로 새로운 콘텐츠를 생성하는 공격법. 테스트 콘텐츠의 최소값과 최대값을 구한 후 그 평균값으로 공격을 실시한다. $d_j' = d_j + (w_{j,\max} + w_{j,\min})/2$ 여기서, $w_{j,\max}$는 콘텐츠의 계수 중 최대값이고, $w_{j,\min}$ 는 최소값이다.
상관계수 음수화 공격	상관계수를 이용하여 포렌식마크 정보를 추출할 경우, 상관계수의 값을 음수로 만들어 공모자의 추출을 어렵게 만드는 공격. 테스트 콘텐츠의 상관계수의 값을 음수로 만들어 공격을 실시한다. $d_j' = d_j + \begin{cases} w_{j,\max}, \text{if } w_{j,med} \le (1-\alpha)w_{j,\max} + \alpha w_{j,\min} \\ w_{j,\min} \quad Ohterwise \end{cases}$ 여기서, max(*), min(*), med(*)은 각각 최대값, 최소값, 중간값이고, α는 max(*)와 min(*)값을 조정하는 계수로 일반적으로 0.5의 값을 갖는다.
상관계수 제로화 공격	상관계수 음수화 공격이 상관계수를 음수로 유도하지만 포렌식마크 정보가 지워졌다는 의미는 아닌 반면, 제로화 공격은 상관계수를 0에 가깝게 유도하여 포렌식마크 정보의 검출이 불가능하도록 만드는 공격. 테스트콘텐츠의 상관계수의 값을 0으로 만들어 공격을 실시한다. $d_j' = d_j + \begin{cases} w_{j,\max}, \text{if } w_{T,j} \le \frac{1}{2}(w_{j,\max} + w_{j,\min}) \\ w_{j,\min} \quad Ohterwise \end{cases}$ 여기서, $w_{T,j}$는 다수의 테스트 콘텐츠 중 하나로 다른 콘텐츠와 극성이 반대되는 콘텐츠이다.
모자익 공격	다수공모자가 공모에 참여한 콘텐츠의 최대, 최소값을 이용하여 상관계수의 값을 작게 만드는 공격과는 달리 포렌식마크가 삽입된 콘텐츠를 기하학적 모양으로 작게 나누어 새로운 콘텐츠를 생성하는 공격. 테스트 콘텐츠수를 다음과 같이 모자익 공격을 실시한다. 2, 4, 6, 8, 16

2. 성능평가 항목

성능평가 항목	성능 평가 방법
강인성	강인성은 각 시험 공격에 대해 삽입된 포렌식마크와 검출된 포렌식마크의 비율의 통계를 사용하여 평가한다. 다음의 세가지 방식의 성능 측정치를 사용한다. - 비트 정보 손실율 : 검출 포렌식마크 비트 수/삽입된 포렌식마크 비트수 - 바이트 정보 손실율 : 검출 포렌식마크 비트 수/삽입된 포렌식마크 바이트수 - 무손실 포렌식마크 정보 검출율 : 에러가 전혀 없으면 1로, 그렇지 않으면 0으로 한다.
공모 허용성	공모허용성은 포렌식마크가 삽입된 영상에 대해 공모공격 후 추출이 가능한 공모자수를 공모허용성으로 함.

삽입 정보량	삽입 정보량은 각 테스트 공격 후에도 90% 이상 추출이 가능한 워터마크 비트수를 삽입정보량으로 한다
비가시성	비가시성은 포렌식마크가 삽입된 영상에 대해 임의로 선정된 5명의 전문가로부터 가시성을 1부터 3까지 (1: 눈에 띔, 2: 중간 3: 눈에 뛰지 않음)의 등급을 받고 이의 통계치를 사용한다.
기술의 복잡성	기술의 복잡성은, 포렌식마크 기술의 포렌식마크 정보의 삽입/검출의 성능을 나타내며 다음과 같이 두 개로 나눌 수 있다. - 삽입 계산 복잡성 : 인증 대상의 포렌식마크 기술의 포렌식마크 삽입 계산속도와 사용 메모리 양 - 검출 계산 복잡성: 인증 대상의 포렌식마크 기술의 포렌식마크 검출의 계산 속도와 사용 메모리 양

V. 인증

1. 인증신청 및 성능평가

포렌식마크 기술의 성능평가 및 인증절차는 그림 2과 같다.

먼저 포렌식마크 기술 소유자는 포렌식마크 기술과 표 3과 같이 인증기관 정보, 인증신청자 정보, 포렌식마크 기술의 일반정보를 포함한 인증신청서를 이메일이나 웹페이지 등의 전자적 방법을 사용하여 인증기관에 제출한다. 인증기관은 제출된 포렌식마크 기술을 앞의 4절의 기술평가를 통하여 성능평가 과정을 수행한다.

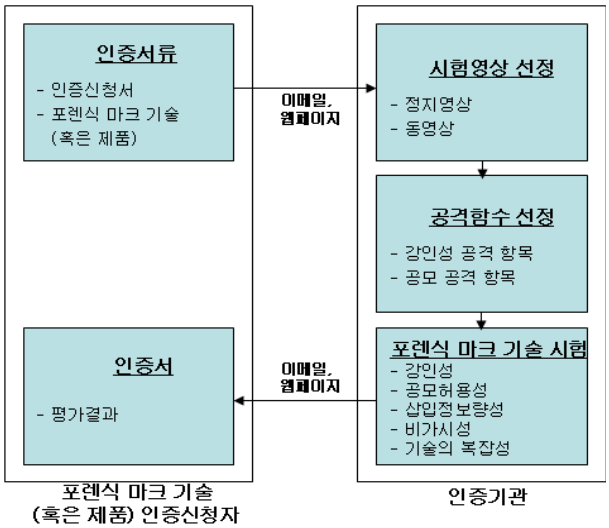

그림 2. 포렌식마크 기술 평가 및 인증 절차
Fig. 2. Procedures of Forensic Marking Evaluation and Certification

표 3. 인증신청서 양식
Table 3. Certification Application Form

인증기관 정보	인증기관 명	
	인증기관 주소	
	인증기관 일련번호	
인증신청자 정보	인증신청자 이름	
	인증신청자 주소	
	인증신청자 식별 번호	
포렌식마크 기술 일반 정보	포렌식마크 기술 식별 번호	
	특허 (선택)	
	알고리즘 설명 (선택)	
	대상 문서	
	대상 응용	

2. 인증서 교부

포렌식마크 기술의 인증기관은 포렌식마크 기술의 평가결과를 인증서에 포함하여 인증 신청기관에 보낸다. 이때, 인증기관은 인증서 데이터베이스를 구축하여 발급된 인증서들을 관리하여야 한다.

3. 인증기관 요건

인증기관은 인증 업무를 수행할 수 있는 인증시설을 구비하여야 하며, 인증업무에 대한 전담자를 두어야 한다. 여기서 인증시설은 포렌식마크 기술 소유자로부터 이 규격에서 정해진 대로 인증신청을 받아 포렌식마크 기술을 인증할 수 있는 테스트 영상 데이터베이스, 포렌식마크 데이터베이스, 공격함수 데이터베이스 및 공격 소프트웨어를 갖추고 변형 테스트를 실시하여 그 결과 성능에 대한 인증서를 발부할 수 있는 컴퓨터 하드웨어 및 소프트웨어를 말한다.

4. 인증서 양식

포렌식마크 기술평가를 위한 인증서는 다음의 항목을 포함한다.

4.1. 인증기관 정보

인증기관 정보는 인증기관 명, 인증기관 주소, 인증기관 일련번호로서 구성된다.

- 인증기관 명: 인증기관의 법인 명
- 인증기관 주소: 우편번호와 인증기관이 소속되어 있는 나라, 시/도, 동, 번지
- 인증기관 일련번호: 인증기관을 구분하기 위해 발부되는 번호

4.2. 인증신청자 정보

인증신청자 정보는 인증신청자 법인/개인명, 인증신청자 주소, 인증신청자 일련번호로서 구성된다.

- 인증신청자 이름: 포렌식마크 기술 소유자의 자연인 혹은 법인명
- 인증신청자 주소: 나라, 시/도, 동, 번지, 우편번호 등의 주소
- 인증 신청사 식별번호: 포렌식마크 기술 소유자의 신원을 확인할 수 있는 주민등록 번호/사업자 등록번호

4.3. 포렌식마크 기술 일반 정보

- 포렌식마크 기술 식별번호: 인증기관이 부여하는 각 포렌식마크 기술을 구별할 수 있는 유일한 번호
- 특허 (선택): 포렌식마크 기술에 관련된 특허 정보
- 알고리즘 (선택): 포렌식마크 기술에 관련된 알고리즘 정보
- 대상 문서: 전자 문서, 그림
- 대상 응용: 저작권 정보, 메타데이타, 복사 제어, 핑거프린팅, 로고 이미지 등

표 4. 인증서 양식
Table 4. Certification Form

인증기관 정보		인증기관 명		
		인증기관 주소		
		인증기관 일련번호		
인증신청자 정보		인증 신청자 이름		
		인증 신청자 주소		
		인증신청자 식별 번호		
포렌식마크 기술 일반정보		포렌식마크 기술 식별번호		
		특허(선택)		
		알고리즘 설명 (선택)		
		대상 문서		
		대상 응용		
포렌식마크 기술 성능	강인성 (Image)	회전	%	
		이동	%	
		샘플링	UP	%
			DOWN	%
		필터링	Gaussian	%
			Median	%
			Sharpening	%
		클립핑	%	
		D/A, A/D 변환	%	
		압축	JPEG	%
			GIF	%
		화면율	%	
		수평 플립	%	
		쉬어링	%	
		선형기하변형	%	
		복합변형	%	
	강인성 (Video)	H.264 압축	%	
		H.264 동영상 칼라 포맷변경	%	
		H.264 비트 깊이변형 (10bit → 8 bit)	%	
		동영상 압축포맷 변형 (H.264→MPEG-4 simple)	%	
		H.264 동영상 크기형	%	
		H.264 프레임율 변형	%	
		H.264 랜덤 패킷 손실율	%	
		H.264 클립핑	%	
		밝기변환	%	
		색상/흑백 변환	%	
		복합변형 I	%	
		복합변형 II	%	
	공모허용성	평균화공격	%	
		최대최소공격	%	
		상관계수 음수화공격	%	
		상관계수 제로화공격	%	
		모자익공격	%	
	삽입 정보량	Byte, bit		
	비가시성	dB		
	포렌식마크 삽입 복잡성	계산 속도	Sec/m(분)	
		사용 메모리	CPU, Memory 사용률	
	포렌식마크 검출 복잡성	계산 속도	Sec/m(분)	
		사용 메모리	CPU, Memory 사용률	

VI. 결 론

본 논문에서는 국내 디지털 저작권 보호 업체 혹은 대학 및 연구소에서 개발하고 생산하는 포렌식마크 기술의 품질을 객관적으로 평가할 수 있는 평가절차와 평가지표를 정량적으로 제시하였다. 포렌식마크 기술의 객관적 평가를 위한 평가 및 인증지침으로 본 논문에서는, 구매자 정보가 삽입된 테스트 영상의 공격 항목과 수준, 포렌식마크 정보의 추출 성능을 평가하기 위한 평가항목, 평가기준, 평가절차, 그리고 포렌식마크 기술의 신뢰성에 대한 통계정보를 포함하는 인증서를 생성하기 위한 인증절차를 포함하였다.

포렌식마크 기술의 평가 및 인증 기술의 목적은 기술 개발자에게는 자신들이 개발한 포렌식마크 기술에 대한 객관적인 평가결과를 제공하고, 소비자에게는 객관적이고 보편타당성 있는 평가 결과를 통해 기술(혹은 제품에) 선정에 대한 객관적인 기준을 제공하며, 기술의 평가자에게는 기술 평가를 위한 객관적이고 정량적인 기준을 제공할 수 있음으로 해서 포렌식마크 기술의 발전과 디지털 저작권 보호 시장의 활성화에 일조를 하는 것이다.

참 고 문 헌

[1] 2012 Annual Report on Copyright Protection, Korea Federation of Copyright Organization Copyright Protection Center
[2] [2010-24 Trend Analysis on Copyright Technology] Watermark/ Forensic Mark Technology, Korea Copyright Commission
[3] Verimatrix(http://www.verimatrix.com/)
[4] Vobile(http://www.vobileinc.com/)
[5] Enswers Inc.(http://www.enswers.net/)
[6] Civolution(http://www.civolution.com/)
[7] Luo Weiqi, Qu Zhenhua, Pan Feng, and Huang Jiwu,“A survey of passive technology for digital image forensics,” Front. Comput. Sci. China 2(1), pp.1－11. 2007
[8] White Paper,“Identifying and Managing Digital Media: A Technology Comparison of Digital Watermarking and Fingerprinting,” DIGIMARC, 2010
[9] Kang Hyeon RHEE,“Evaluation of Multimedia Fingerprinting Image.”Multimedia ‐ A Multidisciplinary Approach to Complex Issues, Published by InTech(www.intechopen.com), pp.141-158 March 2012
[10] Xin-Wei Li, Bao-Long Guo, and Xian-Xiang Wu.“On Collusion Attack for Digital Fingerprinting.”Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 4, pp.366-376, October 2011
[11] Hui feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and Zhengding Lu,“Collusion Attack Optimization Strategy for Digital Fingerprinting,”ACM Transactions on Multimedia Computing, Communications and Applications, Vol. 8, No. S2, Article 36, September 2012
[12] Viktor Wahadaniah, Yong Liang Guan, and Hock Chuan Chua,“A New Collusion Attack and Its Performance Evaluation,” IWDW 2002, LNCS 2613, pp.64‐80, 2003
[13] Hefei Ling, Hui Feng, Fuhao Zou, Weiqi Yan, and Zhengding Lu,“A Novel Collusion Attack Strategy for Digital Fingerprinting,” IWDW 2010, LNCS 6526, pp. 224‐238, 2011
[14] Ferdin Joe J and Vaikunda Rja T,“Enhanced Robustness for Digital Images Using Geometric Attack simulation,” International Conference on Modelling, Optimization and Computing(ICOMC-2012), Procedia 38(2012), pp.2672-2678, 2012
[15] Yong-Seok Seo, Young-Ho Su, and Chi-Jung Hwang,“DWT-based Image Fingerprinting Scheme Resistant against Geometrical Distortion and Lossy Compression.”Proceedings on ICACT 2009, pp.1321-1324, Feb. 2009
[16] Valery Korzhik, Anton Ushmotkin, and Artem Razmov.“Collusion-resistant fingerprints based on real superimposed codes,”International Journal of Computer Science and Applications, Vol. 7 No. 3, pp. 1-8, 2010

저 자 소 개

오 원 근

- 1979년 2월 : 충북대학교 전기공학과 학사
- 1981년 2월 : 영남대학교 전기공학과 석사(제어공학)
- 1988년 5월 : 일본 오오사카 대학 공학박사(시스템 공학)
- 1988년 6월 ~ 현재 : 한국전자통신연구원 연구원
- 주관심분야 : 영상처리, 컴퓨터비젼, DRM(Digital Rights Management), MVS(Mobile Visual Search)