

디지털 워터마킹 기술

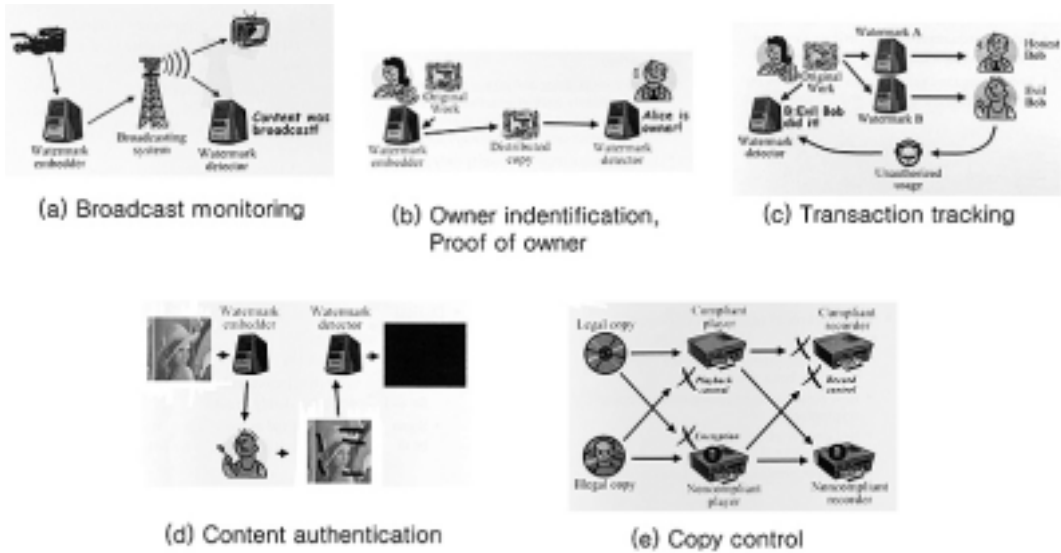
디지털 방송의 본격적인 실시와 PVR(Personal Video Recorder) 등 단말 기술의 발달에 따라 고화질 디지털 콘텐츠의 불법적인 복제나 배포에 따른 원본 소유주를 밝히는 저작권 문제가 대두될 것이 예상된다. 이런 상황에서 이에 대처 할 수 있는 강력한 솔루션이 없는 것이 현실이며, 디지털 콘텐츠의 특성상 원본과 동일성을 가지는 복사본의 창출을 제어한다는 것은 종래의 기술로서는 거의 불가능하다는 것이 현재 기술적인 상황이다. 따라서, 새로운 기술에 대한 연구가 진행되고 있으며 이 중에서 디지털 워터마킹(watermarking) 기술이 대표적인 기술이라 할 수 있다. 디지털 워터마킹 기술은 디지털 영상, 음성 등의 데이터에 인지되지 않는 정보를 은닉시켜 배포한 후에 불법 사용이 적발되었을 경우 그 불법 데이터에서 워터마크를 추출하여 저작권을 주장할 수 있는 방법이다.

1. 서론

디지털 방송 콘텐츠의 저작권 보호를 위하여 디지털 콘텐츠에 인증 기능을 부여함으로써 불법 복제 및 배포를 방지하고 제작자의 저작권과 관련된 권리를 주장할 수 있게 하는 기술이 디지털 워터마킹 기술이다. 워터마크란 700년 전 이태리의 여러 제지 제조업자들이 각자 자신들이 제조한 종이를 구분하기 위하여 눈에 잘 띄지 않게 자신들만의 문자나 기호 등을 삽입한 표시를 뜻한다. 이와 같이 디지털 영상 및 음성 등의 데이터에 디지털 기술을 이용하여 인지되지 않는 정보를 은닉시키는 기술을 디지털 워터마킹이라 한다. 인지되는 않는 정보로서 저작권, 소유자, 사용 제한 등의 내용을 워터마크로 사용하여 아래의 <그림 1>과 같이 방송 모니터링(broadcast monitoring),

소유권 확인 및 증명(owner identification and proof of owner), 유통 추적(transaction tracking), 콘텐츠 내용 인증(content authentication), 복제 제어(copy control) 등의 용도로 활용할 수 있다.

디지털 워터마킹을 이용한 방송 모니터링은 디지털 워터마크를 삽입하여 TV 또는 라디오 방송 채널을 통하여 콘텐츠가 방송된 시간이나 방송 여부를 자동적으로 모니터링 할 수 있어, 광고주나 방송국에서 시청률 조사 및 해적 방송 모니터링 등에 쓰일 수 있다. 디지털 워터마킹에 의한 소유자 확인 및 증명은 디지털 콘텐츠에 삽입된 워터마크로서 정당한 콘텐츠 사용자는 콘텐츠의 소유자를 확인하면서 사용할 수 있으며, 콘텐츠에 대한 지적 재산권에 관한 법적 문제가 발생하였을 때, 소유권 증명으로도 쓰일 수 있다. 디지털 워터마킹을 이용한 유통

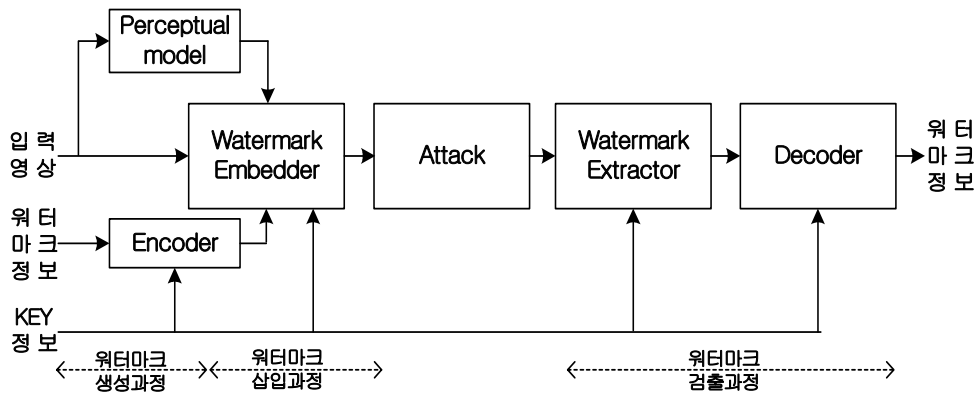


<그림 1> 워터마킹 기술 활용

추적 기능은 콘텐츠의 유통과정에서 콘텐츠의 구매자를 구분할 수 있게 워터마크를 넣는 기술을 의미한다. 이러한 기능을 이용하여 불법적인 복제 콘텐츠가 유통되었을 때 그 콘텐츠의 최초 구매자를 추적하여 불법 복제의 유통을 막을 수 있다는 기대를 할 수 있다. 디지털 워터마킹을 이용한 콘텐츠 내용 인증 기능은 원본 콘텐츠에 워터마크로 삽입하여 콘텐츠에 불법적 또는 인위적인 변형이 가해졌을 때 변형된 부분은 검출해낼 수 있어 원본 콘텐츠의 불법적인 변형을 방지할 수 있다. 디지털 워터마킹에 의한 복제 제어는 디지털 콘텐츠를 사용할 수 있는 장비나 기기와 연계하여 삽입되어 있는 워터마크에 의해 복사를 제어하거나 재생을 제어하는 기술을 의미한다.

디지털 워터마킹 기술은 워터마크 생성 (generation), 삽입(embedding) 및 검출 (detecting) 단계 기술로 크게 구분되며, 다양한 목적에 맞는 다양한 방식의 기술이 제

안되고 있으나 공통적으로 4가지 고려해야 할 사항이 항상 뒤따르게 된다. 첫 번째, 비지각성(imperceptibility)으로 디지털 워터마크는 원본 콘텐츠의 품질에 영향을 미치지 않도록 삽입되어야 하는데 이 한계가 인간의 시각이나 청각에 최대한 인식되지 않는 정도이다. 두 번째, 강인성(robustness)으로 디지털 콘텐츠에 어떠한 조작이나 위조가 가해진다고 하더라도 워터마크는 검출하는 조건이다. 세 번째, 보안성(security)으로 워터마크의 삽입과 검출 알고리즘이 알려져도 워터마크의 존재를 검출하거나 제거하는데 도움을 줄 수 없도록 기술을 개발해야 한다. 마지막 네 번째로 원본의 사용여부로 워터마크 검출 시에 원본을 사용할 것인지 사용하지 않을 것인지를 고려해야 한다. 특별히 디지털 워터마킹 알고리즘 분류 중에 원본을 가지고 검출하는 기술은 널블라인드(non-blind) 워터마킹 방식이라 하고 원본 없이 검출하는 기술을 블라인드(blind) 워터



<그림 2> 워터마킹 과정

마킹 방식이라 한다. 두 가지 방식 중에 난 블라인드 워터마킹 방식이 강인성 면에서 우수하나 원본을 보유하기 위해서는 많은 용량의 데이터베이스가 구축되어 있어야 하는 단점이 있어 최근의 연구는 블라인드 워터마킹 방식으로 치우쳐지고 있다.

여러 종류의 콘텐츠 중 영상 콘텐츠에 관련된 디지털 워터마킹 기술과 KBS의 지적 재산권을 보호하기 위해 개발한 워터마킹 기술에 대해 간략히 소개하고자 한다.

2. 디지털 이미지/동영상

워터마킹 삽입 및 검출 기술

디지털 이미지/동영상 워터마킹 기술은 1990년대 초에 처음 소개되어 1990년대 중반부터 활발히 연구되어 현재까지 짧은 시간 사이에 많은 방법들이 개발되고 있으며 발전하고 있다. 디지털 이미지/동영상 워터마킹 과정은 대체적으로 <그림 2>와 같이 나타내며 아래의 식과 같이 표현할 수 있다.

워터마크 생성과정은 삽입하고자 하는 워터마크를 어떤 형태로 대상 콘텐츠에 삽입

할 것인지 결정하는 방법이다. 워터마크는 이진(binary) 영상, 키(key) 값에 의해 변환된 이진 영상, 키 정보에 의해 암호화된 문자열 또는 유사잡음(pseudonoise) 신호등이 사용된다. 이러한 워터마크는 워터마크의 유무 정보뿐만 아니라 저작권, 소유자, 콘텐츠 내용 등을 포함할 수 있으며, 이렇게 워터마크에 삽입되는 내용을 워터마크 페이로드(payload)라 정의한다.

$$I_w(x) = I(x) + k(I(x)) \cdot W(x)$$

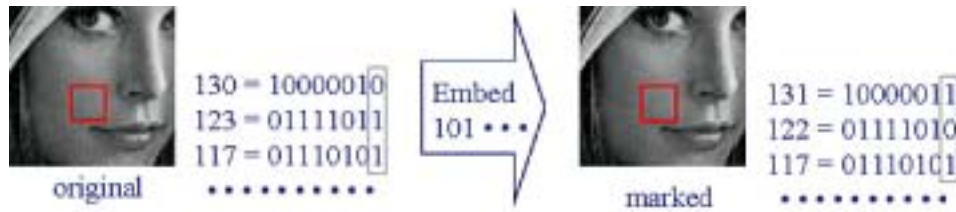
$I(x)$: 원본 콘텐츠

$I_w(x)$: 워터마크 삽입 콘텐츠

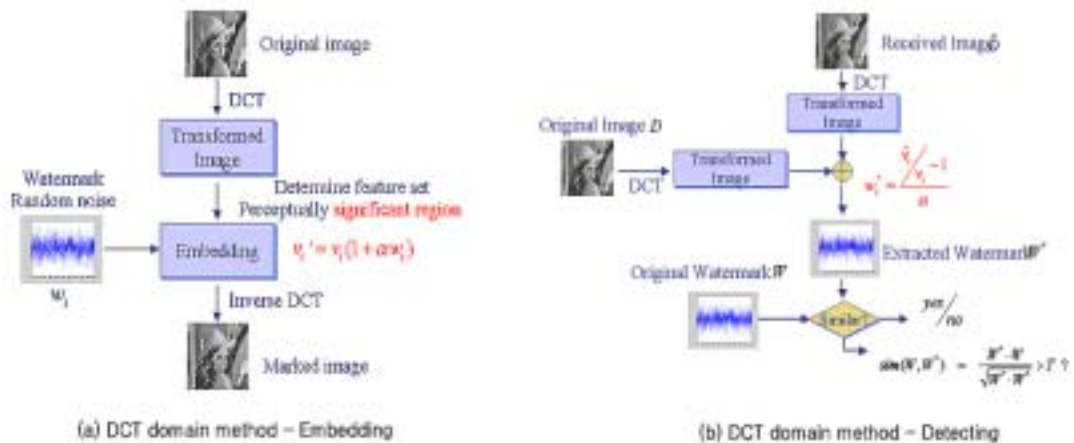
$W(x)$: 워터마크

$k(I(x))$: 워터마크 강도

워터마크 삽입과정은 생성된 워터마크를 어떻게 원본 영상에 삽입할 것인지 결정하는 과정으로 대부분이 공간 도메인(spatial domain) 또는 변환 도메인(transform domain)에서 인간시각시스템(human visual system)을 참조한 삽입강도를 정하여 더하는 방식을 사용한다. 여기서 변환 도메인으



<그림 3> LSB 방식 워터마킹



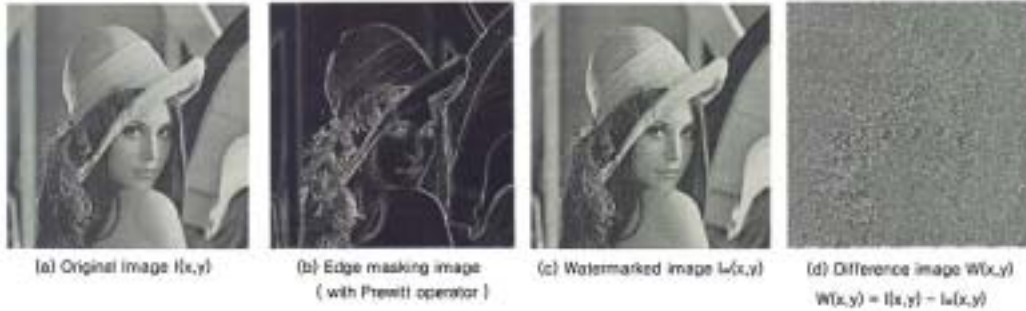
<그림 4> DCT를 이용한 워터마킹 방식

로는 이산 푸리에 변환(DFT : Discrete Fourier Transform), 이산 코사인 변환(DCT : Discrete Cosine Transform), 이산 웨이블릿 변환(DWT : Discrete Wavelet Transform), 푸리에-멜른 변환(FMT : Fourier-Mellin Transform)등이 사용목적에 따라 다양하게 사용된다. 공간 도메인을 이용한 방법 중 대표적인 방법은 <그림 3>과 같이 이미지/동영상 콘텐츠 내의 임의의 여러 픽셀을 선택하여 각각의 픽셀 이진 값의 마지막 비트를 워터마킹 삽입 위치로 하여 삽입 및 검출하는 LSB(Least Significant Bit) 방식이 있다. 이 방법은 간단하고 빠른

방법이지만 간단한 공격에도 워터마크를 잃어버릴 수 있는 단점이 있다.

변환 도메인을 이용한 방법 중 대표적인 방법이자 가장 많이 참조되는 <그림 4>에 표현된 J. Cox가 제안한 이산 코사인 변환 도메인을 사용한 방법이다. 이 방법은 이미지/동영상의 압축이 대부분 이산 코사인 변환을 이용하므로 압축 이미지/동영상에 바로 적용할 수 있으며 간단한 공격에 공간 도메인보다 강하다는 장점이 있다 하지만 의도적으로 가해될 수 있는 기하학적 공격 등에는 약한 단점이 있다.

대부분의 디지털 이미지/동영상 워터마



<그림 5> 윤곽선 정보를 이용한 HVS 워터마킹 방식

킹에서 워터마크의 비가시성(invisibility)를 위하여 인간시각시스템의 특성을 고려한 모델을 적용하여 삽입하게 된다. 인간시각시스템을 고려한 방법으론 이미지/동영상의 색상 성분 중 시각에 덜 민감한 B(blue) 성분에 워터마크를 삽입하는 방법, 이산 코사인 변환 도메인 또는 이산 웨이블릿 변환 도메인에서 주파수 영역을 이용하여 고주파수 영역 또는 <그림 5>와 같이 영상의 윤곽선(edge) 영역에 삽입하는 방법이 있으며, 확률적인 방법을 적용한 NVF(Noise Visibility Function)을 이용하는 방법 등이 있다.

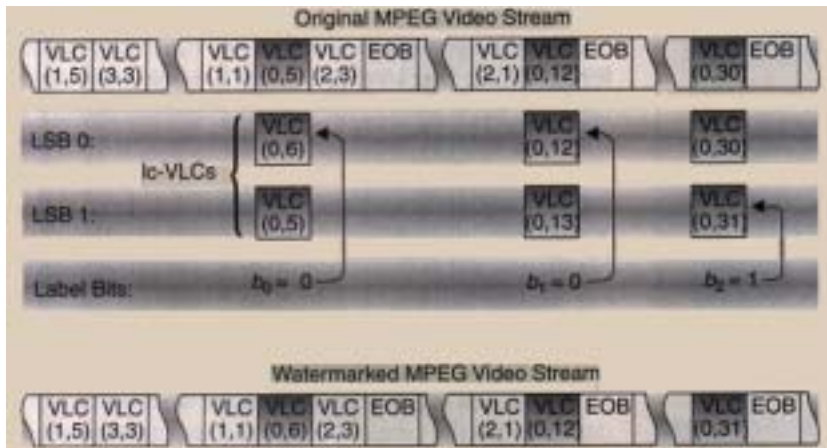
워터마크의 검출 과정은 크게 원본 콘텐츠의 사용 여부에 따라서 두가지로 나뉜다. 원본을 가지고 하는 널블라인드 검출방식으로는 원본 콘텐츠와의 차 값을 이용하는 방법과 아래의 식과 같이 원본과의 유사도를 측정하는 워터마크 검출법이 있다. 블라인드 검출방식으론 워터마크 신호의 자기상관도(autocorrelation)를 구하는 방식, 정합 필터(matched filter)을 이용한 방식 또는 확률적인 방법을 응용한 MAP(Maximum A-Posteriori)을 이용하는 방식 등이 있다.

$$sim(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X}}$$

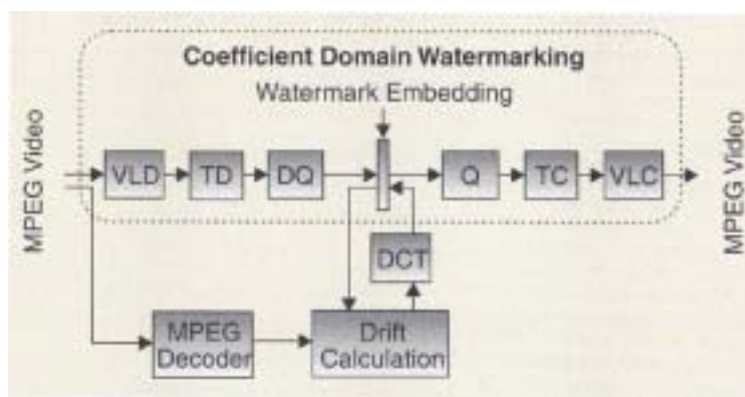
X : original image
 X^* : watermarked image

디지털 동영상 워터마킹 기술은 동영상 압축의 표준으로 자리잡고 있는 MPEG(Moving Picture Expert Group) 압축 방식에 기반하여 크게 두가지로 분류할 수 있는데 압축 도메인(compressed domain) 워터마킹 기술과 비압축 도메인(uncompressed domain) 워터마킹 기술이다.

비압축 도메인 워터마킹 기술은 위에서 설명한 이미지 워터마킹 기법과 크게 다르지 않는다. 왜냐하면, 압축되어 있는 동영상 스트림(stream)에서 동영상 압축을 제거한 한 개의 프레임(frame)은 디지털 이미지와 같기 때문이다. 따라서 비압축 도메인 동영상 워터마킹 기술은 이미지 워터마킹 기술을 그대로 사용한다. 두 번째로 압축 도메인 워터마킹 기술은 동영상 압축 기술을 응용한 방법으로 움직임 벡터(motion vector)에 워터마크를 삽입하는 방법, 동영상의 GOP(Group Of Picture) 구조에 워터마크 삽입하는 방법과 <그림 6>과 같은 동영



<그림 6> VLC의 LBS를 이용한 동영상 워터마킹 방식



<그림 7> 비압축 도메인 동영상 워터마킹 과정

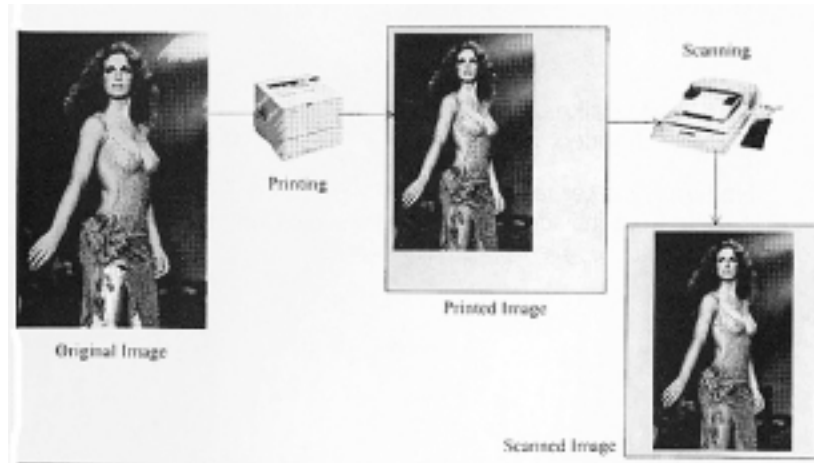
상의 VLC(Variable Length Code)의 LBS에 워터마크를 삽입하는 방법 등이 있다.

비압축 도메인 방법은 압축 도메인 방식에 비하여 공격에 강하나 <그림 7>과 같이 동영상 압축을 모두 풀어버리고 워터마크를 삽입하고 다시 동영상 압축을 실행해야 하는 등의 복잡성과 처리 시간상의 문제점이 있다.

디지털 워터마킹에서 위에서 언급한 4가

지 요구사항인 비지각성, 강인성, 보안성, 원본의 사용여부는 상반되는 점이 있어서 동시에 모두 만족시키는 알고리즘을 개발하는 것은 불가능하다. 따라서 기존의 개발된 알고리즘들은 응용 목적 및 워터마크에 가해질 예상되는 공격에 맞게 기본 방식을 개선한 방법들이 개발되어지고 있다.

3. 워터마킹 공격 대응



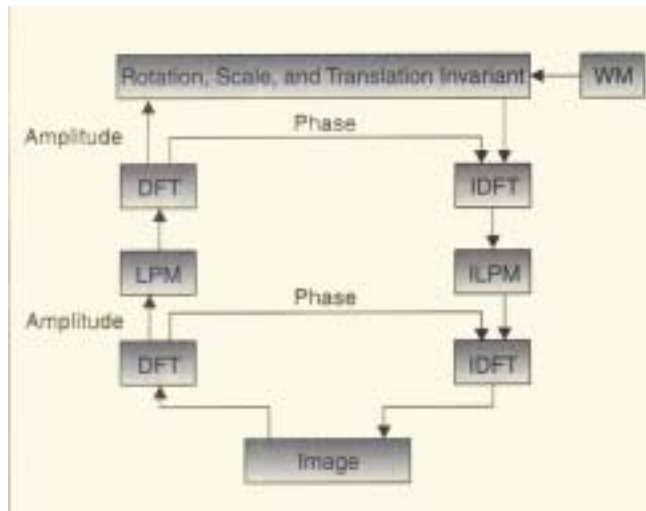
<그림 8> 프린팅 & 스캐닝 워터마킹 공격

3.1 워터마킹 공격 방법

워터마크가 삽입되어 있는 디지털 콘텐츠에 변형을 가해서 삽입된 워터마크가 검출되지 않도록 하는 것을 디지털 워터마킹 공격이라 한다. 디지털 워터마킹 공격 방법에는 여러 가지가 있으나 크게 4가지로 분류된다.

첫 번째는 제거 공격(removal attack)으로 공간 영역 또는 변환 영역에 삽입된 워터마크를 제거하기 위한 공격으로 가우시안(gaussian)/미디안(median)/평균(mean) 필터링(filtering), JPEG 또는 JPEG2000에서 사용하는 손실 압축(lossy compression)과 히스토그램 평준화(histogram equalization), <그림 8>과 같은 디지털 콘텐츠의 AD/DA 변환의 대표적인 예인 프린팅(printing) 및 스캐닝(scanning) 방법들이 있다. 두 번째는 비동기화 공격(desynchronization attack)으로 워터마크가 삽입되어있는 이미지/동영상에 변형을 가하여 워터마크를 검출하지 못하게 하는 방법으로 워터마킹된 이미지/동

영상에 주로 기하학적 변형(geometric transform)을 가하여 워터마크를 검출 못하게 하는 방법이다. 기하학적 방법에는 이동(translation), 회전(rotation), 반전(mirroring), 비례 축소(scaling), 이미지 열/행 제거, 자름(cropping), 모자이크(mosaic: 이미지를 조각으로 자름)등이 있다. 기하학적 변형 공격을 RST 공격이라고도 하고 현재 가장 힘든 공격 중에 하나로 대응책이 가장 많이 연구되고 있다. 세 번째는 암호 공격(cryptographic attack)으로 워터마킹 과정에서 사용되는 키 암호 값을 알아내는 공격으로 키 암호 값을 알아내어 워터마크를 제거한다. 네 번째는 프로토콜 공격(protocol attack)으로 이 공격은 워터마크가 삽입된 영상을 분석한 후 워터마크를 추정하거나 워터마크가 삽입되기 전의 영상을 추정하여 워터마크를 제거하거나 워터마크를 무용지물로 만드는 방법으로 복제(copy) 공격, SWICO 공격 등이 있다.



<그림 9> FMT를 이용한 워터마킹 방식



<그림 10> 로그-극 좌표 변환 영상 성질

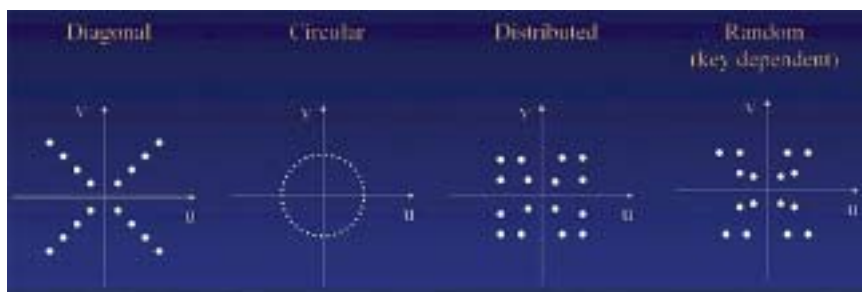
3.2 워터마킹 공격 대응

앞에서 열거한 여러 가지 공격 방법들에 대하여 전통적인 공간 도메인 또는 변환 도메인 기반의 워터마킹 방법들은 모든 공격에 다 강인한 알고리즘이 되질 못했다. 하지만 최근 몇 가지 새로운 방법들이 제안되었고, 특히 가장 대응하기 어려운 공격 방법으로 알려진 RST 공격에도 잘 대응할 수 있는 방법들이 제안되고 있다.

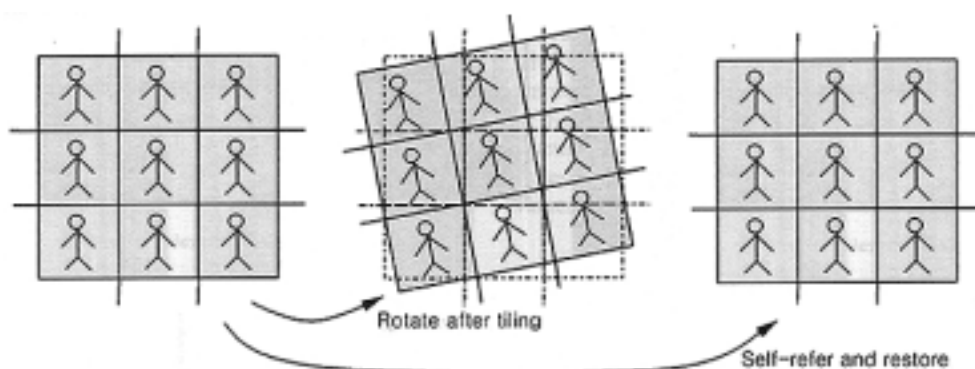
우선 FMT를 이용한 방법이다. FMT는 <그림 9>와 같이 영상을 로그(log)좌표와

극(polar)좌표계로 변환(LPM : Log-Polar Mapping)한 후 푸리에 변환하는 방식을 의미하는데, 로그-극 좌표 변환 영상은 <그림 10>과 같이 회전 및 비례 축소 공격에 불변하다는 성질을 이용한 방법으로 다른 제거 공격에도 강인하다. 하지만, 이동 공격에는 약하다는 결과가 나왔다.

다른 방법으로 템플릿(template)을 이용한 방법으로 변환 도메인에서 워터마크를 삽입할 때 워터마크 신호 이외의 규칙적인 모양을 하고 있는 템플릿 정보를 <그림 11>과 같이 여러 가지 형태로 삽입하는 방법이다.



<그림 11> 여러 가지 형태의 템플릿



<그림 12> 주기적인 워터마크 삽입

템플릿은 RST 공격 후에 워터마크 검출시에 어떤 RST 공격을 받았는지 해석할 수 있는 기능을 부여한다. 템플릿에 의해 공격 여부와 정도를 해석한 후에 워터마크를 검출한다.

또 다른 방법으로 self-reference 방법으로 템플릿과 유사한 방법이나 워터마크와 템플릿을 따로 삽입하는 방법이 아니고 <그림 12>와 같이 워터마크를 영상 전체에 주기적으로 삽입하여 워터마크 자체가 템플릿 기능도 하게 하는 방법이다. 현재까지의 검증에 의하면 템플릿 방식보다 강인한 방법으로 알려져 있고, 템플릿 방식과 self-reference 방식 모두 계산량이 많다는

것이 단점이다.

4. 개발 알고리즘 소개

본 연구에서는 DTV 및 패키지 미디어 콘텐츠에서 KBS의 소유권을 증명할 수 있는 워터마킹 기술 개발에 목표를 두고 최종적으로 방송용 실시간 워터마킹 삽입 및 비실시간 워터마크 검출 시스템을 개발하고자 한다.

DTV의 경우 DTV 방송 환경을 고려하여 전송 압축 규격인 MPEG-2 압축을 기본으로 하고, 이러한 압축 후에 재전송 사업자나 일반 시청자들이 MPEG-2 스트림을 저장한

후 취할 수 있는 워터마크 공격에 대해 실험을 하였다. KBS 저작권 정보 워터마크를 삽입하고, 여러 가지 환경의 공격에 대응할 수 있는 기술을 개발하였다. 각각의 개발 요소 기술로는 워터마크 생성과정의 워터마크 보안성을 위한 워터마크 메시지 엔코딩 기술, 비가시성을 위해 입력 영상의 특성을 이용한 비가시성 특징을 추출하는 기술과 워터마크 삽입과정에서 엔코딩된 워터마크 메시지와 비가시성 특성을 조합하여 입력영상에 삽입하는 기술이 있다. 워터마크 검출과정에선 공격받은 영상에서 워터마크로 가정되는 정보를 추출하는 기술과 추출된 정보를 해석하여 워터마크를 복원하는 디코딩 기술을 개발하였다.

웹 캐스팅용 워터마크의 경우 현재 서비스되고 있는 동영상의 대부분이 저비트율로 압축되어 있어, DTV 또는 패키지 미디어용 워터마킹 방법으로 워터마크를 삽입하면 강한 동영상 압축 과정에서 모두 소멸된다. 또한 저비트율로 압축된 동영상의 경우, 재압축이나 수정 등의 편집 작업에 의해 영상의 화질이 크게 저하될 수 있다. 따라서 저비트율에 맞는 웹 캐스팅 만의 다른 방법을 개발하였으며, 현재 서비스되고 있는 낮은 비트율뿐만 아니라, 앞으로의 초고속 인터넷 대역폭에 대응할 수 있도록 압축 강도(300K ~ 700Kbps)에 맞추어 실험을 하였다. 웹 캐스팅용 워터마크의 경우는 삽입 정보로 KBS의 소유권 여부를 사용하였으며 강한 압축에 의해 추가적인 공격에 대한 실험은 수행하지 않았다

5. 결론

최근 국내외의 디지털 방송은 기존의 아날로그 방송에 비해 5배 이상의 고화질과 CD 수준의 음질, 양방향 전자상거래 등의

장점을 내세우며 콘텐츠와 가전 산업의 전면으로 등장하고 있다. 또한, IT 기술 발전에 따른 인터넷 전송 대역폭 확장과 하드디스크가 장착된 셋톱박스(set-top box)인 PVR(Personal Video Recorder) 및 디지털 VHS(Video Home System) 등 디지털 단말기 제품의 발전에 따라 개인 및 재전송 방송 사업자들에 의한 고화질 디지털 콘텐츠의 불법적인 복제나 배포에 따른 저작권 문제가 대두될 것이 예상된다. KBS는 이러한 국내외 환경의 변화 속에서 방송용 콘텐츠의 저작권 보호를 위한 연구에 착수하였다.

현재까지 DTV 방송, DVD 등의 패키지 미디어, 웹 캐스팅용 미디어에 워터마크 신호를 삽입, 검출하는 기술을 각각 개발하였다. EBU에서 제안한 방송용 콘텐츠에 대한 디지털 워터마킹 기술 요구사항을 바탕으로 KBS 환경에 필요한 요구 사항 항목을 추가하여 개발된 워터마킹 알고리즘에 대하여 다양한 테스트를 수행하였으며, 우수한 성능을 확인할 수 있었다.

향후 이와 같은 연구 결과를 바탕으로 개발된 알고리즘 성능 향상 및 실시간 DTV 방송에 적용할 수 있는 하드웨어 구현 작업에 착수하여 KBS의 지적 재산권을 보호할 수 있는 기술을 지속적으로 연구하고자 한다.