□신기술해설□

전자상거래에서의 디지털 컨텐츠 저작권 보호를 위한 데이터 은닉과 디지털 워터마킹 기술[1)]

조 정 석[†] 최 종 욱[††]

◈ 목 차 ◈

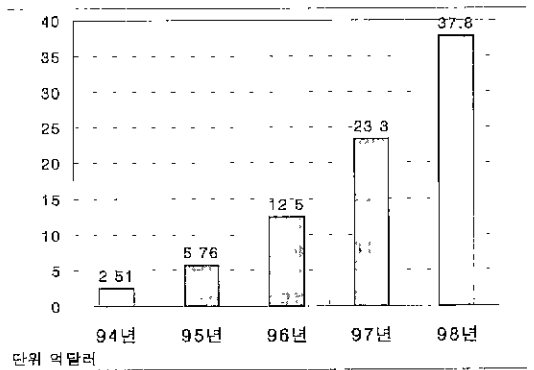
1. 서 론

1.1 멀티미디어 컨텐츠 산업의 성장

인터넷 사용자의 폭발적인 증가로 네트워크를 이용한 멀티미디어 정보의 분배 및 공유가 급속히 이루어지고 있으며, 이러한 추세는 각국이 국가적인 우선과제로서 추진하고 있는 초고속 망 사업과 빠르게 확장되고 있는 위성 네트, 그리고 최근의 무선 인터넷 망의 구축으로 가속화되고 있다.

인터넷 통계로 유명한 포레스터(Forrester)사에 의하면 미국에서 인터넷을 사용하여 물건을 사본 적이 있는 사용자는 97년 여름의 740만 명에서 98년 초 1000만 명으로 증가하였다. 불과 6개월 사이에 30%이상이 증가한 것이다. 현재 미국가정의 43%가 PC를 가지고 있으며 이들 중 반이 넘는, 전체 가정의 25%가 지속적으로 인터넷에 접속하고 있다고 한다. 이에 따라 미국에서의 인터넷 접속건수는 매 100일마다 100%씩 증가하고 있다.

인터넷 사용자 수의 증가와 함께 전자상거래(EC) 시장도 빠르게 성장하고 있다. [그림 1]에 나타난 것과 같이 96년에 8억 달러이던 EC시장은 98년에 81억 달러, 2003년에는 2조 달러 규모가 될 것으로 예측하고 있다. 전자상거래 시장에서는 부동산과 일반 소비용품, 책, 심지어 햄버거와 햄, 생선과 같은 상품들이 팔리고 있으며 음악, 영상, 비디오, 뉴스와 같은 멀티미디어 컨텐츠도 거래되고 있다.



(그림 1) 세계 전자상거래 시장성장추세와 전망
(쥬피터커뮤니케이션社)

디지털 멀티미디어 컨텐츠 시장은 급속히 성장하고 있으며, 한국 멀티미디어 컨텐츠 진흥센터에

1) 본 연구는 과학기술부 핵심소프트웨어 기술개발사업 (98-NS-01-08-A-13)의 지원에 의해서 수행되었음.
† 정회원 : 트러스텍(주)
†† 정회원 : 상명대학교 정보통신학부

의하면 향후 5년 내에 세계시장은 3조 달러에 육박할 것으로 예측하고 있다. 정보통신 연구원의 조사에 따르면 멀티미디어 컨텐츠 산업은 국내의 경우 1998년도 시장규모는 2,258억원으로 27% 성장하였다. 멀티미디어에 대한 인식이 확산됨에 따라 시장이 지속적으로 확대될 전망이어서 '99~2003까지의 평균성장률은 56%로 고속성장을 이루어 2003년에는 1조 8,237억원 규모의 시장을 형성할 전망이다. 향후에는 교육용 컨텐츠의 개발, 디지털 영상서비스 체계 구축, 게임산업의 성장으로 연평균 56%대로 높은 성장세를 보일 전망이다.

멀티미디어 컨텐츠 세계 시장의 성장은 아래 표와 같이 예측되고 있으며 앞에서 언급한 컨텐츠 시장 동향 예측 자료를 근거로 본 기술을 소프트웨어 및 인터넷 서비스 시스템으로 상용화할 경우 멀티미디어 컨텐츠 시장 규모 대비 3%의 매출을 가정할 때 본 기술의 매출액은 2001년에 세계적으로는 480억 달러, 국내 시장은 450억원 정도가 될 것으로 예상된다.

(표 1) 멀티미디어 컨텐츠 시장 전망 : 정보통신 정책연구원 '97

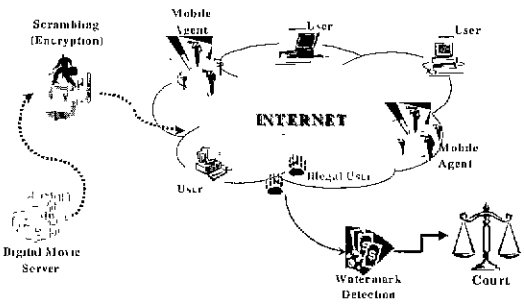
구 분	세계시장 (단위: 억 달러)			국내시장 (단위: 억원)			비고
연 도	1996	2001	성장률	1996	2001	성장률	
멀티미디어 출판	100	4,460	114%	440	2,000	35%	
디지털 영상물	346	4,470	67%	504	3,500	47%	
게임	800	7,000	54%	520	5,000	57%	
교육용 소프트웨어	14	70	38%	640	4,500	48%	
계	1,260	16,000	66%	2,104	15,000	48%	

1.2 멀티미디어 컨텐츠의 지적 재산권 보호

일반적으로 디지털 데이터를 보호하기 위한 방법에는 데이터 암호화, 특히 인증된 사용자만이 암호화된 데이터의 해독 키를 부여 받아 해독하는 방식이 일반적이다. 이러한 암호화는 영상 물 전송 시 구매자가 아닌 타인이 수취하거나 중간에서 낚아채는 경우를 예방하기 위한 방법이다. 또한 이러한 암호화 방법은 구매자로 하여금 대금을 지불해야만 정상적인 제품을 인도 받을 수 있기 때문에 사용되기도 한다.

또한 공급자로부터 제공되는 영상물이 타인에 의해 변조되거나 위조되어 제공되는 경우 구매자를 보호하기 위해, 혹은 전달된 영상물이 위 변조되어 유통되는 것을 방지하기 위해 디지털 서명 기법을 사용할 수 있다. 이는 영상 물 데이터에 첨부하여 보내지는 Hash값으로 원본이 변조되는 경우 구매자는 원문의 해쉬함수값을 계산하여 차이가 나기 때문에 변조된 것으로 판단할 수 있다. 디지털 서명 된 값을 가지고는 원문을 찾아낼 수가 없다는 성질을 이용하여 전송자의 인증기능으로 사용하고 있다.

그러나 암호화된 영상물의 전송은 전송된 이후 합법적인 또는 불법적인 제3자에 의해 복제되고 유통되는 경우 이를 방지할 방법이 없다. 전송과정에서만 데이터 보호가 가능하며 전송 이후의 문제를 해결할 수는 없다. 따라서 암호화가 해독되거나 암호코드가 변형된 파일의 불법 변조/복제 및 네트워크상에서의 불법배포, CD제작을 통한 제 3의 유통을 방지할 수 있는 기술이 필요하다. 제1차적으로는 컨텐츠 데이터를 입수한 사용자



(그림 2) 멀티미디어 서비스 시스템의 보안 체계 구성도

의 의도에 따라 데이터의 조작과 변형이 가능하지 않도록 하는 조작 방지 기술이 개발되어야 한다.

2. 본 론

2.1 저작권 보호와 데이터 은닉

디지털 이미지에 대한 데이터 은닉 연구는 상대적으로 초보적인 연구단계이며 그 성장 잠재력이 매우 높은 분야이다. 지난 5년간 컴퓨터 관련 분야의 모든 출판물의 90%이상이 디지털 이미지와 같은 형태로 출판되었다. 데이터 은닉은 여러 전문분야에 깊은 관계를 가지고 있다. 예를 들어 이미지와 신호처리와 같은 암호 학, 통신이론, 신호 압축 및 영상인식 이론 등에 적용되어 왔다. 가까운 미래에는 정지영상, 비디오 및 음악은 기존의 아날로그 형태에서 디지털 형태로 점진적으로 대체되리라 예상된다. 또한 장기적인 안목에서 미국 TV 방송은 2006년에 디지털 방송으로 전환을 목표로 하고 있다.

디지털로 신호를 표현하는 방법은 기존의 아날로그를 사용하여 표현하는 방법에 비해 다음과 같은 많은 장점을 지니고 있다[4,6,7,8].

1. 복제 및 레코딩 하는데 있어서 손실이 없다.
2. 네트워크를 통해 배포가 편리하다.
3. 편집 및 수정이 쉽다.
4. 데이터가 항구적이고 값싸며, 검색이 쉽다.

그러나, 이러한 장점들은 동시에 심각한 문제점을 가지고 있다. 즉, 저작권 침해, 불법 복제 및 배포, 합법적인 인증 문제, 손쉬운 위조 등이다. 디지털 이미지에 대한 침해는 이미 인터넷상에서는 일반적인 현상이 되었다. 현재, 디지털 이미지나 동영상에 이러한 불법행위에 대한 법적인 증거자료로서 보호 장치를 사용할 수 없다. 이는 아직까지 디지털 이미지나 불법행위를 감지하기 위한 신뢰성 있는 메커니즘이 없기 때문이다. 그러므로 디지털 저작물에 대한 데이터 은닉은 이러한 문제점들을 극복해야만 실질적으로 사용이 가능할 것이다.

이미지에 정보를 은닉하는 형태에 의존하는 것은, 적어도 두 가지이상의 데이터 은닉 구조상의 특징이 있다. 즉, 비견고성, 데이터 은닉의 비발견성, 그리고 이미지 워터마킹의 견고성이다. [13] 첫번째의 경우, 디지털 이미지는 비공개적인 메시지를 위한 저장매체로서 사용될 수 있다. 예를 들어, 암호화된 비트 열에서 각 픽셀에서 중요하지 않은 비트를 대체하거나, 전형적인 이미지 변화는 인지가 불가능하고 암화화 된 메시지는 원 이미지와 같이 보이는 이미지를 수정하게 된다. 이 방법은 통신에서 매우 실제적인 은닉이다. 메시지 삽입은 이미지 신호에 관한 지식과 에러 정정 코드를 사용하여 매우 복잡하게 만들 수 있다.

이미지 워터마킹 견고성에 대한 두 번째 적용은 짧은 메시지(워터마크)를 이미지에 견고하게 하는 방법으로서 삽입하는 방법이다[6,29,31]. 예를 들어 손실압축(lossy compression), 필터(filtering), 노이즈 삽입(noise adding), 회전과 같은 위치적인 변화(geometrical transformations) 등이다.

견고한 워터마크는 저작권 보호, 무결성 검지, 인증, 등에서 결정적으로 사용할 수 있다. 이러한 점은 암호적인 인증 프로토콜이 해결할 수 없는 인증과 관련된 모든 문제를 중점적으로 강조한다. 암호에 기반 하는 인증은 불완전한 보안 채널을 통하는 메시지의 전달자에 대한 인증과 같은 역할을 한다. 그러나 이러한 메시지(이미지) 암호화가 해독될 때에는 불법적인 복제나 배포에 대해 보호할 수 없게 된다. 전통적인 이미지와 달리, 디지털 예술작업은 단지 비트의 조합으로 구성되기 때문에 이러한 이미지 원본에 대한 인증을 하기위해서는 정교한 실험적인 기술에 대하여 연구하여야 한다. 그러므로, 디지털 워터마킹은 부가

적인 정보를 이미지 자체에 직접적으로 가지고 있는 것보다는 삽입에 의한 방법으로 구현하고 있다. 삽입된 정보는 인간의 눈에는 투명하게 보이지 않지만, 암호화된 키를 통한 복잡한 알고리즘을 사용하여 감지가 가능하게 된다[18,20].

2.2 데이터 은닉

암호화의 목적은 메시지를 비밀 키를 소지하지 못한 사람은 원문으로 복구할 수 없도록 인지할 수 없게 만 든다. 때때로, 이러한 방법은 보안과 사적인 요구에 의해 매우 실제적인 정보의 통신을 대신하여 암호화된 메시지를 교환한다. 이 방법의 문제는 은닉하는 방법에 있을 수 있다.

현재, 이진코드형식의 파일들은 비정상적이고 데이터를 숨기는데 있어서 쓸모없는 정도를 확인하는데 사용한다. 디지털 이미지, 비디오 및 오디오 트랙들은 이러한 목적에 대해 이상적이다. 그러나 은닉된 메시지는 이미지 전달과 관계없이 삽입되며, 또는 메시지가 이미지 전달에 관한 중요한 정보를 가지고 있어야 한다.

1) 데이터 삽입 알고리즘
2) 데이터 은닉 감지 기능

데이터 삽입 알고리즘은 비밀 메시지를 전달하는 문서 내에 은닉하는 사용하다. 이러한 삽입 처리는 비밀 키에 의해서 이 키를 소유하고 있는 상대방에 의해서만 은닉된 메시지에 접근이 가능하도록 보호되어야 한다. 데이터 은닉 감지 기능은 수정이 가능한 전달 문서에 적용하여 은닉된 비밀 메시지를 얻을 수 있다. 각각의 데이터 은닉 기술은 의도하고 있는 응용에 있어서 지시하고 있는 명확한 특성이 있다[20,21].

2.3 디지털 워터마킹

워터마크의 중요한 특성은 데이터 왜곡에 대한 견고성이다. 이것은 워터마크가 일반적인 이미지 조작을 받은 이미지로부터 읽을 수 있어야 하는 것이다. 예를 들어 필터링, 스케일링, 노이즈 추가, 크로핑 등이다. 워터마크는 저작권 보호, 핑거프린팅, 또는 접근 조작에 대해 안전한 형태로 삽입되어야 한다. 이것은 비밀 키를 제외한 삽입알고리즘의 세부사항을 을 모두 알고 있는 공격자가 워터마크에 대한 공격을 하지 못하도록 해야 한다. 이러한 응용의 경우, 워터마킹 구조는 동기적인 암호화 방법으로 비밀 키 방법을 예로 들을 수 있다.

다른 특성으로서 삽입이나 추출과정에서의 계산적인 복잡함이다. 이와 같은 것은 삽입과정이 단순하고 빠른 것을 요구하는 응용에서는 삽입 및 추출에 대해 더 시간을 소비하게 되는 단점이 있다. 예를 들어, 디지털 카메라의 일련번호를 삽입하는 처리와 같은 것이다. 또 다른 응용으로서 추출 속도가 절대적으로 중요한 분야로서 디지털 영화 상영과 같은 응용이다.

그러므로 이러한 디지털 워터마킹의 특성은 다음과 같다.[6][15][19]

1) 견고성
2) 보안성
3) 비가시성
4) 삽입/추출의 계산적인 복잡성 제한

대부분의 워터마킹 기술들은 대략적으로 두 가지로 분류할 수 있다. 어떤 변환에 의한 계수의 변화이거나 직접적인 픽셀 값의 변환이다. 일련의 기술들은, 인간의 시각기관의 특성을 고려하여 거의 보이지 않는 왜곡으로 워터마크를 하는 경우이다. 변환에 기반 한 기술들은 대부분 DCT, DFT, Wavelet , 또는 키 값을 이용한다.

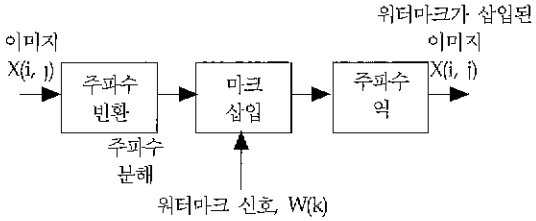
또한 워터마크를 삽입하는 방법이나 응용기술에 따라 데이터를 공간적 관점에서 삽입하는 방

법(Spatial Method), 주파수 영역에서 삽입하는 방법(Frequency Domain Method), 워터마크를 추출하는 방법과 감지하는 방법으로 나눌 수 있다.

2.3.1 공간영역에 의한 워터마킹 기술과 주파수 영역에 의한 워터마킹 기술

공간영역에서의 방법은 이미지와 같은 데이터를 공간적 측면으로 분석하여 삽입하려는 정보를 공간상에서 흩어 버려서 쉽게 구별을 할 수 없도록 하는 방법으로, 일반적으로 화면 화소 값(YIQ)에 미세한 변화를 워터마크로 사용하는 방법이다[11,28]. 이 방법은 워터마크의 삽입은 쉽지만, 손실압축(JPEG)이나 필터링과 같은 이미지 처리에 약하다는 면이 있다.

주파수를 이용한 방법은 멀티미디어 데이터를 주파수 성분의 아날로그 신호로 변환하고 삽입하려는 워터마크를 동일하게 아날로그 신호로 변환하여 삽입하는 방법이다. 일반적으로 데이터를 변환하는 방법으로 이산 코사인 변환(DCT)[10,22,27], 고속 푸리에 변환(FFT) 그리고 웨이브렛 변환(Wavelet Transform)[30,17]등을 이용하여 변환한다[26]. 이 방법은 아래 그림에서 보는 바와 같이 영상의 압축이나 전송과정에서 견고성을 유지한다는 데 장점이 있다. 일반적으로 주파수를 이용한 방법은 공간적 분석을 통한 워터마킹보다 여러 가지 장점을 가지고 있으며, [그림 3]은 주파수 영역에서의 워터마킹의 일반적인 절차를 보여준다.



(그림 3) 주파수 영역에서의 워터마킹 알고리즘

이 방법은 삽입하려는 워터마크 계수(데이터)들이 원 데이터의 전 영역에 분포하게 되며 한번 삽입된 워터마크는 삭제가 어려운 장점이 있어 많이 사용되나, 계수 값에 따라 얼룩이나 찌그러짐과 같은 이미지 손실이 생기는 단점이 있다.

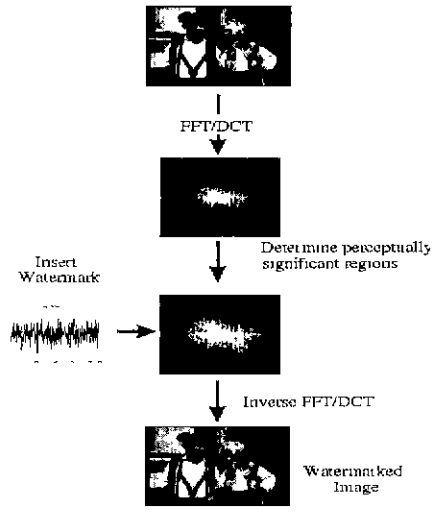
2.3.2 추출 워터터마킹 vs. 감지 워터마킹

워터마킹 구조는 원 이미지가 워터마크의 추출 과정에서 필요한 방법과 필요 없이 감지하는 방법으로 나눌 수 있다. 일반적으로 전자의 경우, 원 이미지가 필요 없는 구조보다 더 견고하다. 그러나 원 이미지가 반드시 필요하다는 단점이 실시간 처리와 같은 일부 어플리케이션에서는 문제가 될 수 있다[19].

2.4 디지털 워터마킹 알고리즘

2.4.1 Cox's Algorithm

Cox의 방법은 가장 널리 알려진 방법 중의 하나로써 N×N 이산 코사인 변환 계수 중 가장 높은 n개의 이산 코사인 변환 계수에 함수에 의한 순열(sequence)을 삽입하는 방법을 제안하였다[13].



[그림 4] Cox's Algorithm

또한, Cox의 방법과 비슷한 접근방법으로 Boland [29]는 이미지를 블록으로 나누고 이 블록내의 각 픽셀 값에 대한 편차를 구하며, 그 편차를 -127에서 127까지 정규화(normalize)를 시킨 다음 주파수 공간에서 계수들을 '1' 또는 '0'을 삽입하는 방법을 제안하였다.

일반적으로 워터마킹을 삽입하는 데 있어서 여러 방법이 연구되고 있으나 그 중에서 가장 널리 알려진 Cox의 방법은 다음과 같은 식을 이용하여 워터마크를 삽입한다.

$$v_k' = v_k(1 + \alpha w_k) \tag{1}$$

여기서, V={v_1, v_2, ..., v_n} : 원 이미지를 이산 코사인 변환이나 고속 푸리에 변환으로 변형한 값이다.

X={x_1, x_2, ..., x_n} : 워터마킹 순열SIM N(0,1)

V~ '={v_1, v_2', ..., v_n'} : 조절 순열

alpha : 스케일링 파라메터

영상에 워터마크가 삽입이 되었는지 여부를 확인하기 위한 일반적인 방법으로 상관관계를 구하여 확인한다. 또한 다음의 식을 이용하여 상관관계를 구하였다.

$$sim(w, w') = \frac{w \cdot w'}{\sqrt{w' \cdot w'}} \tag{2}$$

w' : 변형된 영상에서 추출한 워터마크

w : 원래의 워터마크

2.4.3 Podilchuk and Zeng's Algorithm[28]

인간의 시각기관 구조의 특징을 이용한Podilchuk와 Zeng방법은 어느 정도 개선된 방법이다. 이 방법은 먼저 이미지를 정사각형의 블록으로 나누고 이를 각각 블록 b로 정의 한다. 그리고 각각 DCT 주파수 (r, s)로 정의 한다. 그리고 가시적인 변화 요인이 없는 수정을 하는 DCT 계수에 의해 JND(b, r, s)를 계산한다. 이 JNDs가 Watson에 의해 설명된 주파수 마스킹 모델을 사용하는데 계산된다. 이 모델은 저작물의 높은 압축 율에 의한 손실압축 구조 형태를 기반으로 한다. 이 방법은 다음과 같은 공식으로 표현된다.

$$v_k' = v_k + JND(b, r, s) \cdot \eta_k \text{ if } v_k(b, r, s) > JND(b, r, s)'$$
$$v_k = v_k \quad otherwise \tag{3}$$

여기서 순열 η_k 는 가우시안 N(0,1)을 나타낸다. 이 방법은 종종 JNDs의 계산치 보다 크게 수정되는 경우가 있다. 그러나 저작자가 이 방법을 이용할 경우 가시적인 변화로 인해 사용하기 어렵다. 또한 워터마크 감지의 경우 삽입방법과 정확히 일치하는 과정을 통해서만 추출이 가능하다. 그러므로 저작자는 원본의 구조와 비교하여 견고성 결과가 약간 더 좋은 결과를 얻는 방법이다.

2.4.4 Zhao & Koch's Algorithm (비가시적 워터마킹)[24]

Zhao와 Koch가 제안한 방법으로 이 방법은 이산 코사인 변환(Discrete Cosine Transform)계수에 비트 열을 삽입하는 방법으로 JPEG압축방법과 같이 이미지를 8×8블록으로 나눈 다음 이 블록에 대하여 이산 코사인 변환 계수를 계산한다. 이 계수를 이미지의 질을 결정하는 Q-factor와 JPEG의 표준 양자화 행렬(standard quantization matrix)로 양자화를 하고, 양자화 된 3개의 블록을 비교하는 데 세 번째 블록의 계수가 다른 두 개의 블록의 계수보다 작을 경우에는 블록을 '1'로 부호화 한다.

그러므로 이러한 방법으로 주파수에 마스킹 하는 것과 같은 현상을 얻는 방법은 각각의 블록이 DCT 변환되어 위에서 언급한 주파수 마스킹 모델을 이용하여 DCT 주파수 계수각각에 허용 가능한 최대치 변화를 계산하여 사용한다. 그러므로

다른 제 3자가 보기에 워터마크가 삽입되어 있는지 거의 알지 못하도록 원 데이터의 주파수와 거의 같은 주파수를 삽입하여 보이지 않도록 구조화하는 방법이다. 예를 들어, 주파수 f의 사인함수회절과 차이 c는 사인함수 변화가 주파수 f와 가까워 지면서 감지 임계 값은 증가한다. 그러므로 사인함수 회절에 대한 차이 c는 다음 식과 같이 표현된다.

$$U(x,\ y)U+Ap(x\cos\theta-y\sin\theta) \tag{4}$$

그러므로 c=A/U로 정의한다. 또한 대조 감응도 H(f)는 주파수 f=(f_x, f_y)의 회절 함수로서 다음과 같다.

$$c_0(f^{-1})=H(f)=(0.31+0.69f)e^{-0.29f},\ f=\sqrt{f^2x+f^2y} \tag{5}$$

함수 f로서 주파수 f의 임계 값 차이는, 마스킹 주파수 f_m과 마스킹 차이c_m 이며 다음의 공식으로 표현된다.

$$c(f.fm)=c_0(f)Max\left\{1,[f(\frac{f}{f_m})c_m]^a\right\} \tag{6}$$

여기에서 $c_0(f)$는 주파수 f에 대한 감지 임계치이다. 주파수 f에서 감지 임계 치 c(f)를 찾기 위해서는 근접해있는 주파수f_m으로 알 수 있다. 또한 Minkowski norm을 사용하여 기여도의 합계는 파라메터 β=4로 하여 다음의 식으로 구할 수 있다.

$$c(f)=[\sum_{fm}c(f,f_m)^{\beta}]^{1/\beta} \tag{7}$$

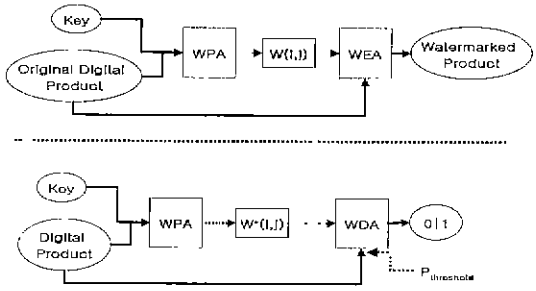
여기에서 의미하는 합계는 DCT 행렬에서 9개의 인접한 행렬의 주파수들에 대한 합이다. 이 방법은M_{ij} 에 의해서 생성되는 pseudo-noise sequence를 저작자의 ID로서 사용하여 보안성을 유지하는 구조이다. 또한 원 이미지로부터 마스킹 행렬Mij 과pseudo-noise sequence를 재 생성하는 것을 통해 저작자의 ID를 감지한다. pseudo-noise sequence를 측정하는 방법으로서 원래의 배열 S와의 상관관계를 측정한다. 상관관계를 측정하기 위한 공식은 다음과 같다.

$$\begin{aligned} H_0&: X=R-S=N \quad (No\,watermark)\\ H_1&: X=R-S=W+N \quad (Watermark) \end{aligned} \tag{10}$$

위의 식에서 R은 원 손실 또는 조작을 통해 변형된 신호, W'은 조작 또는 손실을 통해 변형된 워터마크 이다. 또한 N은 노이즈이다. 이 방식은 이미지에 대한 모든 종류의 왜곡 조작에 강하다는 것이 특징이다. 저작자의 기록인 워터마크는 매우 심하게 노이즈가 삽입되거나, JPEG손실압축(10%), 또는 전 이미지의 15%을 삭제하여도 감지가 되는 장점이 있다.

2.4.5 Fridrich's Algorithm [20]

삽입하고자 하는 워터마크 신호를 패턴에 의한 키 발생 방법에 의존하는 방법은 생성되는 워터마크신호가 패턴의 형태로서 삽입 및 추출되며, 이러한 패턴의 생성은 의사난수(Pseudo Random Number) 발생함수를 이용한다. 이 알고리즘은 다른 공간분석 방법들 보다 워터마크가 비교적 견고하며, 이미지의 밝기차이에 의한 워터마크 신호의 공간적인 분포나 이미지의 전 영역에 대한 고른 분포를 하는 기존의 방법들이 받을 수 있는 공격에 대해 강하다.



(그림 5) 키 값을 이용한 워터마킹 삽입 및 추출 구조[20]

Fridrich의 알고리즘의 경우 기존 방법의 단점을 보완하기 위해서 워터마크의 패턴을 이미지 데이터에 겹치게 하는 방법을 사용하여 이를 극복하였다.그러나 이러한 방법을 사용할 경우 이미지가 손상될 위험이 있기 때문에 극히 미세한 양의 워터마크신호를 삽입해야 하며 이러한 워터마크 생성과 삽입을 위해서 의사난수와 픽셀 단위로 계산을 해서 임계 값을 넘지 않도록 조절한다. 그러나 이러한 방법은 너무나 계산량이 많아 비효율적이며 워터마크신호가 단순한 패턴에 의한 의사난수이기 때문에 추출할 경우 임계값이 낮은 워터마크신호에 대한 판별이 어려운 단점이 있다.

또한 직교 패턴(orthogonal pattern)을 이용하여 워터마크를 삽입하였다. 이것은 원래 이미지 I와 워터마크가 삽입된 이미지 또한 워터마크가 삽입된 이미지를 타인에 의하여 수정된 이미지는 다음의 식과 같다.

$$I_m = \sum_{i=1}^{I} c_i'' f_i + g' \quad c_i'' = \langle f_i,\ I_m \rangle \tag{11-1}$$

$$I_w = \sum_{i=1}^{I} c_i' f_i + g \quad c_i' = \langle f_i,\ I_w \rangle = (1+\alpha_i) c_i \tag{11-2}$$

$$I = \sum_{i=1}^{I} c_i f_i + g \quad c_i = \langle f_i,\ I \rangle \tag{11-3}$$

여기서, 는 워터마크의 시각성(visibility)과 견고성(robustness)을 나타내는 계수이고, 는 두 함수의 내적(inner product)을 의미한다. 이러한 과정을 통해 측정된 워터마크 계수를 측정하기 위해서는 교차-상호관계 "corr" c''-c 와 c'-c를 통해서 다음과 같은 공식을 이용해 측정한다.

$$corr = \frac{(c'' - c)(c' - c)}{\|c'' - d\|\|c' - d\|} \tag{12}$$

위의 식을 이용하여 워터마크의 존재를 결정하는 임계 값을 비교하여 워터마크 유무를 판별하게 된다. 그러나 이러한 방법은 N×N이미지 전체에 대해서 워터마크를 삽입하기 때문에 J개의 워터마크를 하기 위해서JN^2 byte의 메모리가 필요하며, 이때 계산 복잡도(computational complexity)는 $O(j^2 N^2)$이 된다. 따라서 계산 복잡도를 줄이기 위해서 Fridrich는 N×N 이미지를 몇 개의 블록으로 나누어 삽입하였다.

또 다른 단점으로서 워터마크를 삽입하기 위해서 영상을 이산 코사인 변환이나 고속 푸리에 변환으로 변형하였을 경우 원점에 있는 계수는 이산 코사인 성분을 나타내므로 이 원점을 피해야 하는 문제가 있다.

2.4.6 패치워크(Patchwork)[10,11]

공간 분석 방법의 응용의 대표적인 예로서 패치워크가 있다. 이 방법은 이미지에서 n개의 쌍을 임의로 선정한 (a_i, b_i)에서a_i는 명암 값을 하나씩 더해 주고, b_i는 명암 값을 하나씩 빼 줌으로써 공간상에 디지털 워터마크가 삽입하도록 구현하였다. 그러나 이 방법은 인간이 눈으로 보는 이미지의 질을 저하시키는 단점이 있다.

패치워크와 유사한 방법으로Pitas와 Kaskalis가 제안하는 방법은 이미지를 두 개의 동등한 크기의 부분집합으로 나누어 그중 하나의 부분집합에 있는 픽셀에 대하여 양의 정수인 *k-factor*를 더함으로써 표시하는 방법으로 다음의 식으로 표현할 수 있다.

$$S = \{s_{nm},\ n \in \{0, \ldots, N-1\},\ m \in \{0, \ldots M-1\}\} where\ s_{nm} \in \{0,1\}$$

$$I = \{x_{nm},\ n \in \{0, \ldots, N-1\},\ m \in \{0, \ldots, M-1\}\} where\ x_{nm} \in \{0, \ldots L-1\} \tag{13}$$

여기서 S는 삽입하려는 디지털 워터마크를 나타내며, 크기가 N×M인 원 이미지는 I이다. 또한 s와 x는 각각의 배열에서의 픽셀이며, L은 픽셀의 명암에 대한 단계를 나타낸다. 위의 식들은 다시 다음의 식들로 나타낼 수 있다.

$$A=\{x_{nm} \in I, \quad s_{nm}=1\} \tag{14-1}$$

$$B=\{x_{nm} \in I, \quad s_{nm}=0\} \tag{14-2}$$

$$|A|=|B|=\frac{|I|}{2}=\frac{N\times M}{2}, \quad I=A\bigcup B \tag{14-3}$$

$$C=\{x_{nm} \otimes k, \quad x_{nm} \in A\} \tag{14-4}$$

여기서 (식 14-4)의 *k-factor*는 두 개의 부분집합의 분산(variance)으로 계산된다. 그러나 이미지의 각 픽셀의 명암을 모두 계산하기 때문에 데이터가 작은 흑백이미지에서도 비효율적인 방법으로 데이터의 양이 매우 많은 칼라이미지에 적용하기에는 불가능하다.

Caronni[12]는 이와 같은 방법을 사용하면서도 픽셀단위의 계산량을 줄이기 위해서 이미지를 N의 블록으로 나누어 각 이미지 블록의 밝기(luminance)의 값에 비트 열을 (bit stream) 삽입하는 방법으로 블록에 있는 픽셀의 평균값이 임계 값보다 클 경우에는 '1'로 부호화하고 임계 값보다 작을 경우에는 '0'으로 부호화 하는 방법을 제안하였다. 그러나 이 방법 또한 칼라이미지에서는 그 계산량이 많으며 블록이 클수록 이미지 조작과정에서 삽입된 워터마크가 소실되거나 원 이미지의 질을 떨어뜨리는 단점이 있다.

2.4.7 공간영역에서의 스프레드 스펙트럼 변환 (Pitas's Method)[10,19]

이 방법의 기본적인 접근 방법은 이미지의 모든 픽셀들은 기본적으로 |A|=|B|의 조건에 의해 A,B,C 집합의 형태로 나눈다. 이 집합은 pseudo-random number generator와 비밀 키 값으로 만들어진다. 흑백의 영상에서 행렬 A가 k에 의해서 gray level이 증가하면, 반대로 B의 행렬 계수들은 감소를 한다. 그러므로 C 행렬 값은 변하지 않는다. 즉, A와 B 행렬은 기본적으로 같은 분포를 가지게 되므로 이미지를 직렬화 시킨 평균값은 변하지 않는다. 또한 워터마크의 감지는 흑백이미지의 gray level에 대한 두 이미지 계수집합 A', B'가 같게 되는 다음의 식으로 표현이 가능하다.

$$\overline{a}=\sum_{A'} g_{ij} \approx \overline{b}=\sum_{B'} g_{ij}, \tag{15}$$

또한 k에 의해서 A'=A이고 B'=B로 분리가 가능하면 이것으로 워터마크를 감지하게 된다. Pitas는 다음과 같은 공식으로 워터마크의 삽입 유무를 판단한다.

$$q=\frac{\overline{w}}{\sigma_{\overline{w}}} \tag{16}$$

위의 식에서 $\overline{w}=\overline{a}-\overline{b}$ 는 A와 B 픽셀의 평균값을 뺀 값이다. 그러므로 워터마크의 삽입 유무는 다음과 같이 생각할 수 있다.

$$H_0: \textit{There is no watermark in image} \quad (\overline{w}=0)$$
$$H_1: \textit{There is no watermark in image} \quad (\overline{w}=k) \tag{17}$$

이 방법은 인간의 시각체계를 고려하여 워터마크를 은닉한다. 그러나 이 방법은 하나의 이미지에 워터마크를 여러 게 삽입할 경우 각각의 워터마크 신호들이 간섭을 일으키거나 섞여버리게 된다. 삽입되는 워터마크 신호가 고주파 영역에 존재하여 에너지가 높은 단점이 있다. 또한 gamma correction, contrast/brightness adjustment, histogram equalization)과 같은 흑백 스케일의 비선형적인 변환에 견고한 방법이지만, low-pass 나 lossy compression(JPEG 압축)과 같은 조작에 약한 단점이 있다.

3. 결 론

인터넷을 기반으로 한 멀티미디어 및 디지털 저작물에 대한 보안기술 및 저작권 보호기술 개발에 대한 필요성이 시급한 상황으로서 고 압축,

고품질의 새로운 멀티미디어 포맷의 등장과 서비스의 개발은 이러한 디지털 저작물을 관리 및 보호 기술 개발이 진행되고 있다.

초기의 비트조작이나 가시적인 방법으로 이루어진 워터마킹 기술은 주파수 공간을 이용하거나 대역확산통신기법(Spread Spectrum Communication)과 같은 응용기술을 이용하거나 디지털 워터마킹 기술을 보완하기 위한 데이터 은닉, 워터마킹을 이용한 암호화 기술 등 그 응용 방법이 매우 다양하며, 이러한 기술들의 연구 및 상호보완을 통해 디지털 저작물에 대한 저작권 보호 및 관리가 가능하리라 예상된다.

향후 디지털 워터마킹의 발전방향은 최근의 주파수 변환기법을 기반으로 저작권자의 정보를 보다 많이 삽입하면서 변형이나 조작에 강인하도록 하는 것과 DVD, MPEG-4 등과 같은 디지털 컨텐츠 플레이어(H/W, S/W)와의 연동 방법 등 다양한 응용방안이 연구되어야 할 것이다.

참고문헌

[1] 조정석, "디지털 칼라이미지의 저작권보호를 위한 디지털 워터마크 알고리즘 연구", 한국외대 석사학위 논문, 1999

[2] Anderson R. J., "Stretching the Limits of Steganography", *1st Information Hiding Workshop, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 3948, 1996.

[3] Aucsmith D., "Tamper Resistant Software: An Implementation", *1st Information Hiding Workshop, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 317333, 1996.

[4] Aura T., "Practical invisibility in digital communication", See http:// deadlock.hut.fi/ste/aura_ihw96.html. 98-03-21.

[5] Aura T., "Invisible communication", *Proc. of the HUT Seminar on Network Security '95*, Espoo, Finland, Nov 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.

[6] Bender W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", Technical report, MIT Media Lab, 1996.

[7] Berghel H. and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking", *IEEE Computer* , **29**(7), pp. 101103, 1996.

[8] Berghel, H. and L. O'GorMan, "Digital Watermarking", See http:// www.acm.org/~hlb/publications/dig_wtr/dig_watr.html. 98-03-16.

[9] Boney L., A. H. Tewfik, K. N. Hamdy, "Digital Watermarks for Audio Signals", *IEEE International Conference on Multimedia Computing and Systems*, Hiroshima, Japan; pp. 473480, June 1996.

[10] Bors A. G. and I. Pitas, "Image watermarking using DCT domain constraints", *Proc. IEEE Int. Conference on Image Processing*, vol. 3, pp. 231234, 1996.

[11] Bruyndonckx, O., J.-J. Quisquater and B. Macq, "Spatial Method for Copyright Labeling of Digital Images", See http://poseidon.csd.auth.gr/Workshop/papers/p_19_2.html. 98-03-28.

[12] Caronni G., "Assuring ownership rights for digital images", *Proc. Reliable IT Systems*, VIS'95, Vieweg Publishing Company, 1995.

[13] Cox I. J, J. Kilian, T.Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video", *Proc. 1996 International Conference on Image Processing*. ICIP'96. Vol III. pp.243-246.

[14] Cox I. J. and J.-P. M. G. Linnartz, "Some

general methods for tampering with watermarks", preprint, 1998.

[15] Cox I. J. and Kazuyoshi Tanaka, "NEC data hiding proposal", Technical report, NEC Copy Protection Technical Working Group, July 1997. Response to call for proposal issued by the Data Hiding SubGroup.

[16] Cox I. J. and M. L. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling", *Proc. of the SPIE Human Vision and Electronic Imaging*, vol 3016, pp. 9299, 1997.

[17] Fridrich J., "Combining Low-frequency and Spread Spectrum Watermarking", *Proc. SPIE Int. Symposium on Optical Science, Engineering, and Instrumentation*, San Diego, July 1924, 1998.

[18] Fridrich J., "Image Watermarking for Tamper Detection", *Proc. Of '98 international Conference of Image Processing (ICIP '98)*, Chicago, Oct 1998.

[19] Fridrich J., "Applications of Data Hiding in Digital Images", *Proc. of The 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems* (ISPACS'98), Melbourne, Australia, 46 November 1998.

[20] Fridrich J., "Robust digital watermarking based on key-dependent basis functions", *The 2nd Information Hiding Workshop in Portland*, Oregon, April 1517, 1998.

[21] Hartung F. and B. Girod, "Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video", *Proc. Of European Conference on Multimedia Applications, Systems and Technologies (ECMAST 97)*, Milano, Italy, May 1997.

[22] Hartung F. and B. Girod, "Digital watermarking of raw and compressed video", In N. Ohta, editor, Digital Compression Technologies and Systems for Video Communications, *SPIE Proc. Series*, vol. 2952, pp. 205213, Oct 1996.

[23] Jack Lacy, Schuyler R. Quackenbush, Amy R. Reibman and James H. Snyder, *"Intellectual property protection systems and digital watermarking"*, *Optics Express Vol. 3, No. 12*, December 7, 1988 pp. 477-484

[24] Koch E., J. Zhao, "Towards robust and hidden image copyright labeling", *Proc. Nonlinear Signal Processing Workshop*, Thessaloniki, Greece, pp. 452455, 1995.

[25] Kundur D. and D. Hatzinakos, "A Robust Digital Image Watermarking Scheme using WaveletBased Fusion," *Proc. IEEE Int. Conf. on Image Processing*, Santa Barbara, California, vol. 1, pp. 544-547, October 1997.

[26] Kundur D. and D. Hatzinakos, "Digital Watermarking using Multi-resolution Wavelet Decomposition," *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.

[27] Piva A., M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image", *Proceedings of 4th IEEE International Conference on Image Processing (ICIP'97)*, Santa Barbara, CA, USA, October 26-29, 1997, Vol I, pp. 520-523.

[28] Podilchuk C. I. and W. Zeng, "Digital image watermarking using visual models", *Proc. of the IS&T/SPIE Conference on Human Vision and Electronic Imaging II*, San Jose, CA, USA, vol. 3016, pp. 100111, Feb 1997.

[29] Ruanaidh, J.J.K, F.M. Boland and O.Sinnen, "Watermarking Digital Images for Copyright Protection", EVA'96, See http://cuiwww.unige.ch/

~oruanaid/eva_pap .html.

[30] Wang Houng-Jyh Mike, Po-Chyi Su and C.-C. Jay Kuo, Wavelet-based digital image watermarking, *Optics Express* Vol. 3, No. 12, December 7, 1988 pp 491-498

[31] Wolfgang, R. B. and E. J. Delp, "A Watermark for Digital Images", *proceedings of the 1996 International Conference on Image processing*, Lausanne, Switzerland, Sept. 16-19, 1996, vol.3, pp219-222.

조 정 석

1997년 한국외국어대학교 자연과학대학 물리학과 (물리학 학사)
1999년 한국외국어대학교 경영정보대학원 응용전산학과 (이학 석사)
1999년-현재 상명대학교 인공지능 연구소 연구원
관심분야 : 디지털 워터마킹, 멀티미디어 저작권 보호, 데이터 은닉, 신호 처리, 인터넷 보안

최 종 욱

1982년 아주대학교 산업공학과 (산업공학 학사), 서울대학원 경영학과(석사과정)
1986년-1987년 Johns C. Smith University (Charlotte, NC) Computer System Specialist
1988년-1991년 KIST 시스템 공학센터 인공지능 연구부 지식 처리연구실
1991년-현재 상명대학교 정보통신학부 교수
관심분야 : 워터마킹, 지능형 교통 시스템, 영상인식기술, 네트워크 시스템, 보안 기술