화상 데이터의 저작권 보호를 위한 디지털 워터마킹

이혜주, 박지환
부경대학교 전자계산학과

Digital Watermarking for Copyright Protection of Image Data

Hye-Joo Lee, Ji-Hwan Park
Dept. of Computer Science, PuKyong Nat'l University

요 약

디지털 데이터의 저작권 보호를 위하여 최근 디지털 워터마킹에 관하여 많은 연구가 이루어지고 있다. 디지털 워터마킹이란 인간의 시각이나 청각이 인지할 수 없는 범위 내에서 디지털 데이터의 값을 약간 변경함에 따라 워터마크라고 하는 저작권 정보를 몰래 삽입하는 방법이다. 본 논문에서는 주변 화소와의 차가 정해진 임계값을 넘는 화소에 워터마크를 집어넣은 후, 유사성을 측정하여 워터마크를 검출하는 공간 영역 기반(spatial domain based) 워터마킹을 제안한다.

1. 서론

컴퓨터의 보급에 따라 디지털 데이터의 사용이 증가되고, 특히 데이터 압축 기술의 발달로 인하여 화상, 오디오, 비디오와 같은 많은 저장 공간을 필요로 하는 디지털 데이터의 사용이 일반화되고 있다. 또한 디지털 데이터의 복사는 아날로그 데이터의 복사와 달리 여러 번의 복사를 수행하여도 데이터의 품질이 손상되지 않으며, 인터넷과 같은 컴퓨터 네트워크를 통한 디지털 데이터의 복사는 전파의 속도가 빠를 뿐만 아니라 그 범위도 매우 넓고, 누구든지 동일한 품질의 디지털 데이터를 이용할 수 있다는 장점을 가지게 된다. 그러나, 이러한 복사의 용이성은 저작권 보호의 관점에서 볼 때 문제가 발생한다. 즉, 많은 시간과 노력을 투자하여 제작한 화상, 오디오, 비디오 디지털 데이터가 저작자의 허가 또는 적절한 대가의 지불 없이 불법적으로 복사되어짐에 따라 저작권이 보호받지 못하는 경우가 발생하게 되고, 결국 저작자는 자신의 저작물을 공개하기를 꺼리는 바람직하지 못한 결과를 초래하게 된다.

본 연구는 한국과학재단 핵심전문 연구과제(과제번호:981-0928-493-2) 연구비에 의해 연구되었음

이와 같이 컴퓨터 네트워크 상에서 디지털 데이터의 저작권을 보호하기 위한 기본적인 방법은 암호(cryptography)를 이용하는 것으로 데이터를 암호화(encryption)하여 올바른 복호 키를 가진 사용자, 즉 허가나 대가를 지불한 정당한 사용자만이 데이터를 복호할 수 있도록 하는 것이다. 그러나, 이 방법은 복호된 디지털 데이터를 복사할 수 있어 역시 저작권 보호를 위한 해결책이 될 수 없다. 따라서, 이것을 해결하기 위한 방법으로써 먼저, 디지털 데이터와 분리될 수 없도록 저작권 정보를 디지털 데이터에 미리 숨겨 놓고 암호화하여 사용자에게 배포한다. 그리고, 배포된 데이터를 복호한 경우에도 저작권 정보는 복호된 디지털 데이터 내에 계속 존재하게 되어 저작권 보호가 가능하다. 이러한 개념을 도입한 것이 디지털 워터마킹(digital watermarking)으로 현재 많은 연구가 이루어지고 있다[1-3].

일반적으로 디지털 워터마킹은 문서 화상, 오디오 등 모든 종류의 디지털 데이터에 대하여 연구가 이루어지고 있으나, 본 논문에서는 화상 데이터에 대해서 논의한다. 본 논문의 구성은 다음과 같다. 먼저, 2장에서는 디지털 워터마킹의 개념과 기존의 제안되어 있는 기법들에 대해서 기술하고 3장에서는 간단한 방

법으로 화상 데이터에 대하여 워터마크를 집어넣는 방법을 제안한다. 그리고, 4장에서는 제안한 워터마킹 기법에 대하여 시뮬레이션하여 그 유효성을 보인다. 마지막으로 5장의 결론에서는 향후의 연구과제를 제시한다.

2. 디지털 워터마킹

저작권을 보호하기 위하여 디지털 데이터를 암호화하는 경우에는 복호 키를 가진 정당한 사용자에 의한 복호된 데이터의 불법적인 2차 배포를 방지할 수 없다는 문제점이 있다. 따라서, 2차 배포를 방지하기 위해 디지털 데이터와 분리할 수 없도록 저작권 정보를 데이터 내에 숨겨둔 후 암호화하여 사용자에게 전송한다. 이때 불법적으로 2차 배포된 디지털 데이터로부터 저작권 정보를 추출함으로써 자신의 저작물임을 증명함과 동시에 저작권 정보에 사용자 정보를 포함시키는 경우에 누가 불법적으로 배포하였는가도 함께 지적할 수 있다. 이것은 디지털 데이터의 암호화만으로는 저작권 보호가 미흡하기 때문에 보완책으로 이용하는 것으로 어떤 디지털 데이터 내에 2차적인 데이터를 몰래 숨겨 놓는 경우를 심층암호(steganography)[4-5]라 한다. 심층암호의 응용은 그림1과 같이 데이터 은닉(data hiding, data embedding) 기법과 저작권 보호를 위한 기법으로 나눌 수 있고, 후자는 다시 디지털 워터마킹(digital watermarking)과 fingerprinting으로 분류되지만 저작권 보호를 위한 기법을 통칭 디지털 워터표시이라고 한다.

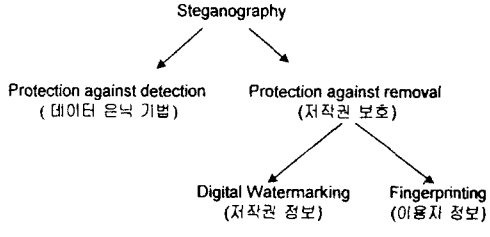


그림 1. 심층암호의 분류

데이터 은닉 기법의 목적은 제3자가 알아 차릴 수 없도록 비밀 데이터를 다른 데이터에 몰래 숨겨서 전송하기 위한 것이기 때문에 이 기법은 비밀 데이터의 존재 여부의 검출(detection)에 대하여 견고하게 숨길 수 있도록 설계되어야 한다. 데이터 은닉 기법은 화상, 오디오, 비디오와 같은 데이터뿐만이 아니라 네트워크 상의 패킷과 같은 일시적으로 발생하는 데이터들 내에 비밀 데이터를 숨겨두는 경우도 포함하고 있다. 이러한 데이터 은닉 기법을 기반으로 디지털 워터마킹은 워터마크(watermark)라는 저작권 정보를 디지털 데이터 내에 숨겨 두어 저작권을 보호하고자 하는 특수한 목적으로 이용한다. 두 방법의 차이점을 Simmon의 '죄수의 문제(Prisoner's Problem)'으로 설명하면, 데이터 은닉 기법은 Alice와 Bob의 탈출 계획이 간수 Eve에 의해 탄로되지 않도록 서신을 주고받는 것이 목적이며, 디지털 워터마킹은 Alice와 Bob의 서신이 Eve에 의해 변경되지 않도록 함을 목적으로 한다. 그러나, 두 방법 모두 인간이 인지할 수 없는 범위 내에서 디지털 데이터의 값을 변경하여 정보를 숨겨 두는 것으로 데이터 은닉 기법들을 확장하여 디지털 워터마킹에 응용할 수 있기 때문에 데이터 은닉 기법이 좀더 넓은 분야라 볼 수 있다. 그러나, 디지털 워터마킹은 저작권 보호를 위한 법적 증거물로써 이용될 수 있는 만큼 데이터 은닉 기법보다는 아래와 같은 조건을 만족하는 견고한 방법으로 설계되어야 한다[6].

◆ 디지털 워터마킹의 조건

(1) 워터마크는 헤더부나 특정 영역에 집중되지 않고 디지털 데이터의 전 영역으로 분산시켜 숨겨 놓아야 한다.

(2) 편집, 압축, 전송 등 여러 가지 처리에 대해서 변경 또는 제거되지 않아야 한다. 특히, 화상과 같은 디지털 데이터의 일부분을 추출하여 이용하는 경우에도 워터마크 정보를 복원할 수 있어야 한다.

(3) 워터마크의 수정이나 소거 등의 공격에 견고해야 한다.

(4) 정규로 입수한 복수의 디지털 데이터의 워터마크 정보를 부정하게 해독하여 정당한 사용자를 부정하게 모함하는 결탁공격(collusion attack)에 강해야 한다.

위의 조건들은 워터마킹의 응용 분야에 따라 약간 달라지게 된다. 예를 들어, 워터마크를 디지털 데이터의 무결성과 인증에 이용하는 경우에는 (3)항은 만족하지 않아도 된다. 즉, 디지털 데이터를 획득한 후, 이 데이터의 변경 유무를 판단하기 위해서는 약간의 변경에도 워터마크의 변화가 발생되는 것이 바람직하다. 또한, 위의 조건을 모두 만족하는 디지털 워터

마킹을 설계하는 것은 매우 어려운 문제이다.

3. 디지털 워터마킹의 제안

기존의 디지털 워터마킹 기법들을 분류하면 크게 공간 영역(spatial domain) 기반 워터마킹[7-8]과 주파수 영역(frequency domain) 기반 워터마킹[9-10]으로 나눌 수 있다. 일반적으로 공간 영역 기반 워터마킹보다는 후자가 필터링, 압축, cropping 등에 견고하다는 것이 많은 연구에 의해서 알려져 있다. 그러나, 주파수 영역 기반 워터마킹은 주파수 변환을 수행하여 워터마크를 삽입하고 다시 공간 영역으로 변환해야 하기 때문에 처리시간이 다소 소요된다. 따라서, 빠른 워터마크 삽입 처리 시간을 요구하는 응용 분야에는 적합하지 않게 되기 때문에 공간 영역 기반 워터마킹에 대한 연구가 필요하다. 일반적으로 공간 영역 기반 워터마킹은 화소의 통계적 성질을 이용한다. 예를 들어, Bender 등[7]에 의해 제안된 'Patchwork 알고리즘'은 동일한 레벨의 화소 값 a, b를 선택하게 된다. 이때, $s=a-b$라 하고 이 과정을 n번을 반복한다. i번째의 화소의 차를 $s_i=a_i-b_i$라 하면 기대값 $S=\sum_{i=1}^{n}s_i$는 0이 된다. 여기서 화상에 워터마킹하기 위해서는 고정된 값을 각각 가산하거나 감산하면 S는 0이 되지 않게 된다. 이와 같이 S의 값이 0이 되는 경우에는 워터마크가 없는 화상으로 판단하고, 그 반대의 경우에는 워터마크가 되어 있는 화상으로 판단할 수 있게 된다. 이 방법의 단점은 동일한 레벨의 화소 쌍을 찾기가 어렵고, 압축과 같은 처리에 견고하지 못하는 단점이 있다.

또한 Pitas[8] 등에 의해 제안된 'superposition 알고리즘'은 $N\times M$ 화상 $X=\{x_{mn}\}$에 대해서, 비밀 정보 E를 0과 1의 개수가 같은 이진 패턴

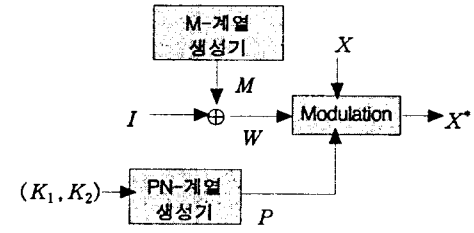
$$E=\{e_{mn}, n\in\{0,\ldots,N-1\}, m\in\{0,\ldots,M-1\}\},$$

이라 할 때, X를 2개의 부집합

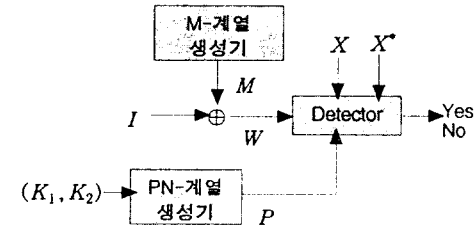
$$A=\{x_{mn}\in X, e_{mn}=1\},\quad B=\{x_{mn}\in X, e_{mn}=0\}$$

로 나눌 수 있다. 이때 화상의 열화를 초래하지 않을 정도의 작은 값 d를 각각 2개의 부집합에 가산하거나 감산한다. 그리고, 워터마크를 검출하기 위해서는 각 집합의 평균 $\bar{a}$, $\bar{b}$를 계산하여, 이 평균의 차가 $2d$에 가깝게 되면 워터마크된 화상이고 워터마크되지 않은 화상이라면 0에 가깝게 된다. 그러나, 압축이나 저역 통과 필터링과 같은 처리에 견고하지 못하다는 단점이 있다. 이러한 방법 외에도 간단하게 LSB의 비트를 워터마크와 대체시키거나, M-계열을 이용하여 워터마크 정보를 숨기는 방법들이 제안되어있다.

위의 방법들은 화상의 통계적 성질을 고려할 뿐 인간의 시각 성질을 이용하지 않는다. 따라서, 본 논문에서는 위의 방법들과 달리 주변 화소의 밝기를 고려하여 워터마크 정보를 집어넣는 방법을 이용한다. 이것은 인간의 시각 특성 중에서 주변 화소와의 밝기 차이가 큰 경우 주목 화소의 값의 변화를 인식하기 어렵다는 마스킹 성질을 이용하는 것으로 그림2와 같이 워터마킹과 워터마크 검출을 수행한다.



(a) 워터마킹 과정



(b) 워터마크 검출

그림2. 워터마크의 삽입과 검출 과정

먼저, 워터마크를 숨기기 위하여 $N\times M$ 크기의 원 화상 X의 각 화소 값 x_{ij}, $0\le i<N$, $0\le j<M$에 대해서 주변 화소 값과의 밝기 차 v_{ij}를 식(1)과 같이 계산한다.

$$v_{ij}=\left(\sum_{k=i-1}^{i+1}\sum_{l=j-1}^{j+1}|x_{ij}-x_{kl}|\right)/8 \qquad (1)$$

이와 같이 계산된 v_{ij}로부터 워터마크가 삽입될 위치를 지시하는 T_{ij}는 주어진 임계값 Th에 대해서,

$$T_{ij}=\begin{cases}1, & v_{ij}\ge Th\\ 0, & \text{otherwise}\end{cases} \qquad (2)$$

와 같이 설정된다. 이때, 워터마크 길이 l은 $T_{ij}=1$

의 개수가 된다.

워터마크 $W=\{w_l \mid 1,0\}$은 식(3)과 같이 최대주기를 가지는 M-계열과 길이 q비트인 저작자의 ID I와 exclusive-OR 연산을 수행하여 구한다.

$$W=I \oplus M \tag{3}$$

이때, $q \ll l$이므로 저작자 ID를 반복하여 W를 구성한다. 그리고, 2개의 키 (K_1, K_2)를 입력으로 하는 의사 랜덤 계열 $P=\{p_l \mid 0<p_l<1\}$를 이용하여 x_{ij}의 값을 아래와 같이 변경함으로서 워터마킹을 수행하게 된다.

$$x_{ij}^{*}=\begin{cases} x_{ij}+\alpha \cdot (p_l+w_l), & \text{if } T_{ij}=1 \\ x_{ij}, & \text{if } T_{ij}=0 \end{cases} \tag{4}$$

여기서, α는 변환 인수로써 원 화소 값의 변화되는 양을 조정한다.

한편, 워터마크는 원래의 화상 X, 워터마크된 X^{*}, 그리고 키 (K_1, K_2)에 의해 생성된 의사 랜덤 계열 P를 입력으로 하여 워터마크된 화상으로부터 재계산된 P^{*}와의 유사성을 식(5)와 같이 측정하여 검출한다.

$$SIM(P, P^{*})=\frac{P \cdot P^{*}}{\sqrt{P^{*} \cdot P^{*}}} \tag{5}$$

원 화상은 저작자만이 소유하고 실제 제안한 워터마킹 기법은 워터마크 검출 시 원 화상을 필요로 하기 때문에 저작자만이 소유하는 원 화상은 키의 역할을 하게 된다.

4. 시뮬레이션 및 결과

그림3의 5개의 화상 girl, lenna, aerial, barbara, boat(256×256, 8 bits/pixel)을 대상으로 각 화상에 워터마킹을 수행하였다.

제안 방식에 의해 워터마크된 화상은 그림3의 우측에 나타냈으며, 시각적으로 원래의 화상과 화질의 차이는 거의 인식할 수 없음을 알 수 있다. 또한, α의 값은 $v_{ij}/2$로 설정하였기 때문에 v_{ij}가 10인 경우에는 최대 5만큼의 화소 값만 변경되므로 워터마크된 화상의 화질은 그다지 열화되지 않게 된다. 따라서, α의 값을 적절하게 설정하는 경우에 워터마크된 화상의 화질은 원 화상과 차이가 있지만, 시각적으로 차이를 구별할 수 없는 워터마크된 화상을 얻을 수 있다.

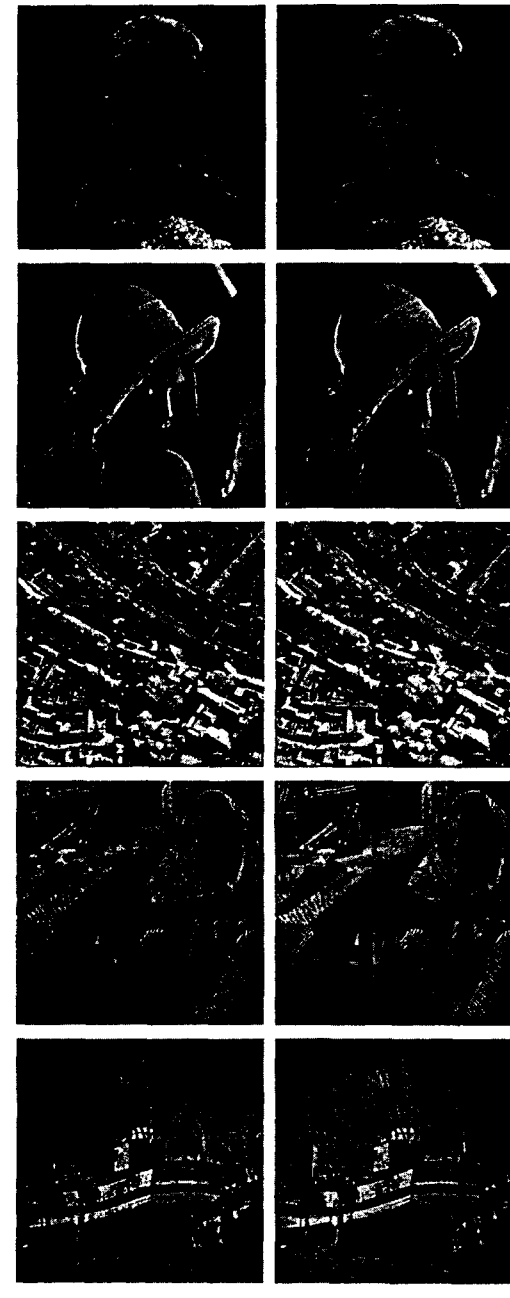


그림3. 원 화상(좌측)과 워터마크된 화상(우측)

워터마크는 마스킹 값이 $5 \le v_{ij} \le 10$을 만족하는 위치에 삽입하였다. 마스킹 값의 분포는 화상마다 달라지기 때문에 워터마크를 삽입될 위치는 화상에 의존되

어진다. 또한, 마스킹 값은 원 화상으로부터 계산되어지기 때문에 원 화상을 가지고 있지 않은 사용자는 정확하게 워터마크가 삽입되어 있는 위치를 알 수 없게 된다. 각 화상에 대하여 마스킹 값에 의해 워터마크가 삽입될 위치를 그림4에 나타내고 있다. 각 대상 화일에 삽입되는 워터마크의 길이는 표1에 나타낸다.

표1. 워터마크 길이(마스킹 값 $5 \le v_{ij} \le 10$인 경우)

대상화상	girl	lenna	aerial	barbara	boat
워터마크의 길이	7551	10474	19787	13590	10535

그림4에서와 같이 삽입 위치들은 화상의 윤곽선 부분으로써 일반적으로 인간의 시각은 복잡한 부분에서의 변화는 인식하기 어렵다는 성질을 고려할 때, 본 논문에서의 주변 화소와의 평균 밝기 차를 이용하는 제안 방법은 적절하다고 여겨진다.

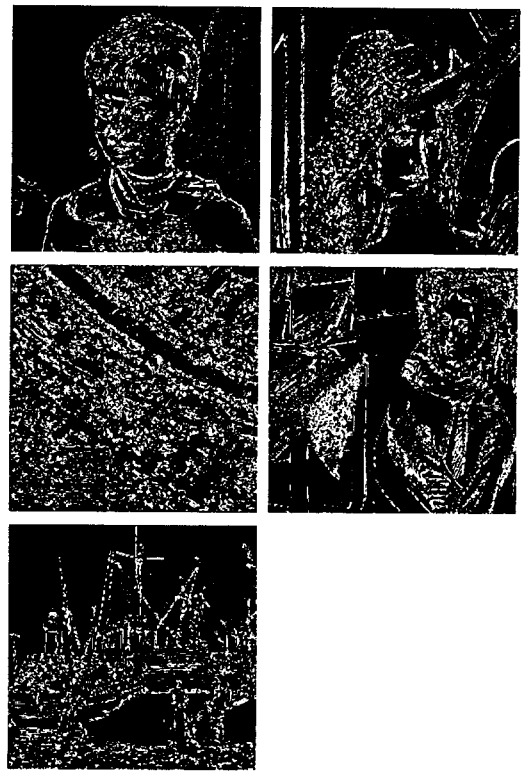


그림4. 워터마크 삽입 위치

그림3의 워터마크된 화상으로부터 워터마크의 유사성을 측정한 결과를 그림5에 나타내고 있다. 그 결과 높은 유사성을 가지고 있음을 알 수 있다.

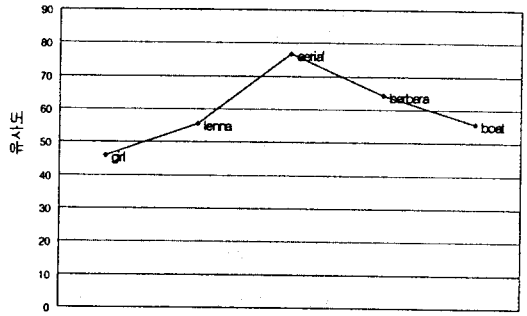


그림5. 유사성 측정

워터마킹에서 가장 중요한 문제는 압축, 필터링, cropping과 같은 화상 처리에의 견고성 문제이다. 예를 들어, 워터마크된 화상을 JPEG 압축한 후 복호화상으로부터 워터마크를 검출할 수 있어야 한다. 그러나, JPEG 압축과 같은 손실 압축은 화상 데이터의 중복성(redundancy)을 대폭으로 제거하기 때문에 데이터가 소실되어진다. 따라서, 압축후 복호된 화상은 워터마크된 화상과 달라지게 되어 유사성의 값이 떨어지게 된다. 그림7은 각각 품질 계수(quality factor)를 80%, 50%, 5%로 JPEG 압축한 후 유사성을 측정한 결과이다.

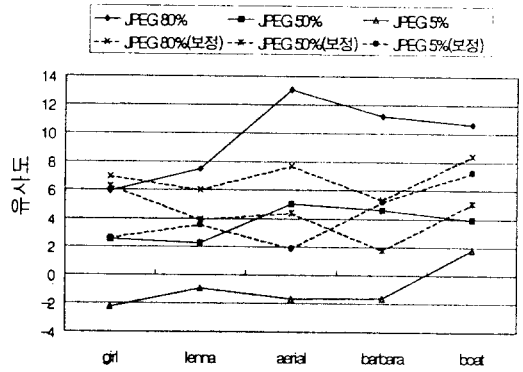


그림6. JPEG 압축 후의 유사성 측정

그림5와 그림6을 비교하면 유사성의 차이가 많이 남을 알 수 있다. 이것은 제안 방식의 워터마크 삽입 위치가 대부분이 윤곽선 부분으로 결정되고, 이 부분들의 화소 값들은 화상의 고주파 성분을 제거하여 압축을 수행하는 JPEG 압축에 의해 다른 부분들보다

큰 폭으로 변경되기 때문이다. 이러한 문제점을 보완하기 위하여 워터마크를 추출하기 전에 전처리(preprocessing)의 수행이 요구되어 진다. 간단한 전처리 과정으로 원 화상과 워터마크된 화상으로부터 각각 평균 밝기 차 v_{ij}, v_{ij}^*를 계산하여 x_{ij}^*를 보정한다.

$$x_{ij}' = x_{ij}^* + (v_{ij} - v_{ij}^*) \qquad (6)$$

식(6)의 x_{ij}'의 값을 x_{ij}^* 대신 이용하여 p_l^*의 값을 구하여 유사성을 계산할 수 있다. 이 결과를 그림6의 실선으로 나타내었다. 80%, 50% JPEG 압축시에는 잘못된 보정으로 인하여 유사성이 떨어지는 경우가 나타나는데, 이것은 효율적인 보정처리가 아님을 알 수 있다. 따라서, 보다 효율성이 있는 전처리 과정에 대한 연구가 필요하다.

마지막으로 P의 성질에 따른 유사성의 유효성을 판단할 수 있는 유사성의 하한에 대한 연구가 요구된다.

5. 결론

저작권 보호를 위한 디지털 워터마킹은 공간 영역에서 수행하는 경우와 주파수 영역에서 수행하는 경우로 분류되어진다. 본 논문에서는 공간 영역에서 주변 화소의 평균 밝기 차를 이용하여 워터마크 삽입 위치를 결정하고 워터마크 처리를 수행하는 방법을 제시하였다. 공간 영역 기반 워터마킹은 일반적으로 주파수 영역 기반 워터마킹보다 견고하지 못하다고 알려져 있으나, 주파수 변환을 수행할 필요가 없으며 또한 워터마크 검출 또는 추출시에 전처리 수행에 의해 성능을 향상시킬 수 있을 것이다. 본 논문에서 제안한 워터마킹 기법은 아직 JPEG 압축이나 필터링, cropping 등에 대하여 견고하지 못하기 때문에 이에 대한 후속 연구가 요구되어진다. 또한 현재의 워터마킹 기법들의 경향은 워터마크 검출 및 추출시에 원 화상을 필요로 하지 않는 방향으로 나아가고 있다. 따라서, 제안 방식을 더욱 개선하여 원 화상 없이 워터마크를 검출할 수 있도록 해야 할 것이다.

참고 문헌

[1] Proceedings of the IEEE International Conference on Image Processing 1997, 1998

[2] N. Memon, P.W.Wong, "Protecting Digital Media Content," Comm. of the ACM, Vol.41, No.7, pp.35-43, 1998

[3] M.D.Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," Proc. of the IEEE, Vol. 86, No.6, pp.1064-1087, 1998

[4] R. Anderson Ed., "Information Hiding," in Lecture Notes in Computer Science, Vol.1147, Springer, 1996

[5] R.Anderson and F.A.P.Petitcolas, "On the Limits of Stegangoraphy," IEEE JSAC, Vol. 41, No.7, pp.474-481, 1998

[6] 松井甲子雄, "電子透かしの基礎", 森北出版株式會社, 1998(in Japanese)

[7] W. Bender, D. Gruhl, N.Morimoto and A Lu, "Techniques for Data Hiding," IBM Syst. J., Vol. 35, pp.313-336, 1996

[8] N. Nikolaidis, I. Pitas, "Copyright Protection of Images Using Robust Image Signature," In proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, pp.2168-2171, 1996

[9] C. I. Podilchuk, W.Zeng, "Image-Adaptive Watermarking Using Visual Models," IEEE JSAC, Vol.16, No.4, pp.525-539, 1998

[10] I. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Specturm watermarking for Multimedia," Tech. Rep. 95-10, NEC Research Institute, 1995