컬러 영상을 위한 하이브리드 워터마킹

A Hybrid Watermarking Scheme for Color Images

이 현 석* 비비 옥타비아** 김 미 애*** 이 원 형****
Hyun-Suk Lee Vivi Oktavia Mi-Ae Kim Won-Hyung Lee

요 약

본 논문에서는 컬러 영상을 위한 하이브리드(hybrid) 디지털 워터마킹 기법을 제안한다. 즉, 두 개의 워터마크가 주파수 영역과 공간 영역 상에 각각 삽입된다. 첫 번째 워터마크는 영상 데이터를 DWT(discrete wavelet transform)를 사용하여 주파수 공간으로 변환한 후, 인간의 시각이 밝기에 민감하지 않다는 사실을 이용하여 컬러 영상의 밝기(luminance) 성분에 대역확산(spread-spectrum) 방법으로 워터마크를 삽입한다. 삽입되는 워터마크는 유사난수 패턴(pseudo-random pattern)을 사용하며 워터마크 검출시에는 상관도(correlation)를 이용하여 워터마크를 추출한다. 두 번째 워터마크는 첫 번째 워터마크가 클로핑(cropping)과 같은 기하학적 공격(geometrical attack)에 취약한 점을 보완하기 위해 삽입한다. 영상의 공간 영역에서 블루 채널 상에 두 번째 워터마크가 삽입되며, 이때 영상의 특징점의 픽셀값을 입력 값으로 하여 해쉬함수의 출력값을 구한다. 따라서 두 번째 워터마크는 영상의 위·변조를 판별할 수 있는 tamper detection의 기능을 한다.

Abstract

This paper presents a hybrid digital watermarking scheme for color images. We insert two watermarks in the DWT domain using spread-spectrum correlation-based watermarking in luminance component of the color image and in spatial domain using pixel-value substitution of blue channel of color image. The objectives of this paper are to have the watermark robust to common signal processing and to detect any changes on the watermarked image for tamper detection at the same time. This watermark scheme will have the robustness characteristic as typical in frequency domain watermark, and also ability to detect any changes on the image (tamper detection).

Keyword : Hybrid Watermarking, Color Image, Tamper detection, Copyright protection

1. 서 론

최근 컴퓨터 기술의 급속한 발달과 인터넷의 확산으로 사운드, 이미지, 비디오와 같은 멀티미디어 데이터들이 디지털화 되고 있으며 이로 인해 디지털 컨텐츠의 유통 및 이용이 증가하고 있다. 디지털 컨텐츠를 위한 유무선 전송 환경이 갖추어지고 여기에 적합한 새로운 형태의 시장이 형성됨에 따라 기존의 오프라인에서 제공되던 음반, 영화, 책, 방송 등이 온라인에까지 영역을 넓혀가고 있으며 앞으로 전자상거래 시스템이 정착되면 디지털 컨텐츠 시장은 더욱 성장할 것으로 전망된다.

이렇게 네트워크 환경이 발전함에 따라 사용자들은 더욱 다양하고 질 높은 디지털 컨텐츠 서비스를 원하게 되었다. 그리고 디지털 형태의 데이터는 기존의 아날로그 데이터들과 비교하여 데이터의 저장과 편집이 용이한 장점을 가지고 있다. 하지만 이러한 장점은 데이터의 훼손 없이 대량 복사가 가능하고 빠르고 광범위한 배포가 가능하다는 단점이 되기도 한다. 특히, 디지털화된 데이

* 준 회 원 : LG전자 정보통신
hslee9392@lge.com(제 1저자)
** 준 회 원 : 중앙대학교 첨단영상대학원 영상공학과(석사)
vivi_o@hotmail.com(공동저자)
*** 정 회 원 : 중앙대학교 첨단영상대학원 영상공학과(석사)
kimma@dreameiz.com(공동저자)
**** 종신회원 : 중앙대학교 첨단영상대학원 영상공학과 교수
한국컴퓨터게임학회 부회장
whlee@cau.ac.kr(공동저자)

터는 원본과 복사본의 구분이 불가능하여 소유권 보호 문제가 생길 수가 있다. 따라서 디지털 컨텐츠를 소유한 사람들은 디지털이 가지는 완벽한 복제 특성 때문에 사업화에 많은 어려움을 겪고 있다.

따라서, 인터넷과 통신을 이용하여 디지털 컨텐츠를 유통하는데 있어서 정보의 보안성이 중요한 문제점으로 대두되었고, 이를 위해 암호화 방법이 연구되고 있다. 암호화 방법이란 평범한 사람이 이해할 수 있는 내용을 특정한 사람을 제외하고 이해할 수 없는 형태로의 변형과 특정한 사람을 제외하면 이해할 수 없는 형태를 이해할 수 있는 형태로 바꾸는 방법을 말한다[1]. 그러나 상대의 정보를 가로채려는 노력, 즉 암호해독(cryptanalysis)으로 인해 암호화된 디지털 데이터는 불법적으로 유통될 수 있다. 따라서 디지털 컨텐츠의 불법적인 유통으로부터 소유주 또는 저작자의 권리를 보호하기 위해 디지털 워터마킹(watermarking) 기술이 제안되고 있다. 워터마킹 기술은 디지털 컨텐츠에 사람의 시각이나 청각으로 구별할 수 없는 저작권 정보를 삽입하여 불법적인 복제로부터 저작권을 증명할 수 있는 기술이다. 이러한 워터마킹 기술의 연구는 디지털 데이터의 손실을 최소화하면서 좀 더 강인한 워터마킹 알고리즘을 개발하는데 목적이 있다.

본 논문에서 제안한 워터마킹 방법은 몇 가지 특징을 가지고 있다. 첫째, 다양한 공격에 대해서 강인성을 보이며, 취약한 공격에 대해서는 tamper detection 기능을 추가하여 영상의 조작 부분을 밝혀 낼 수 있도록 하였다. 두 번째, 워터마크 검출시에 원본 영상을 필요로 하지 않는 블라인드(blind) 워터마킹 방법이다. 세 번째, 상충관계에 있는 강인성과 비가시성을 최대한 만족할 수 있도록 하였다. 네 번째, 컬러 영상을 대상으로 색상이 가지는 특성을 활용하였다. 인간의 시각에 덜 민감한 성분에 워터마크를 삽입함으로써 워터마크가 삽입된 영상의 품질이 보다 좋도록 하였다.

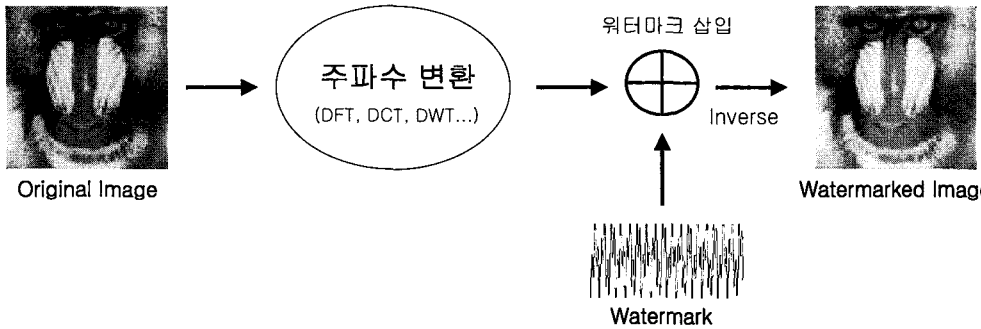
2. 관련 연구

2.1 디지털 워터마킹(digital watermarking)

디지털 워터마킹은 디지털 컨텐츠에 사람의 지각으로 판별할 수 없는 저작권 정보(워터마크)를 삽입하는 기술이다. 이렇게 저작권 정보인 워터마크를 삽입함으로써 디지털 컨텐츠의 유통과정에서 지적 재산권 분쟁이 발생했을 경우 디지털 컨텐츠에 대한 소유권을 주장할 수 있다. 이러한 워터마킹 기술은 비가시성(Invisibility), 강인성(Robustness), 안정성(Security),삽입될 수 있는 정보의 양(Data Payload), 워터마크 검출시 원영상의 사용여부, 워터마크의 빠른 검출, 다중성(Multiplex), 복잡성(Complexity), 낮은 오차 확률 같은 특성을 만족해야 한다. 그리고 워터마킹 기술은 소유권 증명(Owner Identification & Proof of Ownership), 컨텐츠 인증(Content Authentication), 불법 배포자의 확인(Fingerprinting for Traitor Tracking), 복사와 기기 제어(Copy & Device Control), 방송 모니터링(Broadcast Monitoring), 디지털 컨텐츠 저작권 관리(DRM)에 응용될 수 있다. 디지털 워터마킹 기술은 관점에 따라 다양한 방법으로 나눌 수 있다. 여기에서는 강인성, 워터마크 삽입 영역, 삽입 및 검출 방식, 가시성에 따라 분류하였다[2].

(1) 강인성에 의한 분류

- Fragile 워터마킹 : 영상 데이터의 변경을 막는 목적보다는 워터마크가 삽입된 데이터의 변경시도(공격)를 감지하는데 사용된다.
- Semi-Fragile 워터마킹 : 사용자가 한계치를 규정하여 한계치 이상의 변경시도(공격)에 대해서는 워터마크가 손상되도록 한다.
- Robust 워터마킹 : 가능한 모든 변경시도(공격)가 이루어져도 워터마크가 손상되지 않고 검출될 수 있도록 한다.



〈그림 1〉 주파수 영역에서의 워터마크 삽입 과정

(2) 워터마크 삽입영역에 의한 분류

- Spatial 워터마킹 : 공간 영역에서의 워터마킹으로 이미지 화소(pixel) 자체를 조작하는 방법이다. 주로 시각적으로 영향을 적게 미치는 화소의 하위 비트에 워터마크를 삽입한다. Spatial 워터마킹은 알고리즘 자체가 간단하기 때문에 적은 계산량으로 워터마크를 삽입할 수 있는 장점이 있다. 그러나 잡음(noise)과 신호처리 등에는 강인하지 못하다.
- Spectral(or Frequency) 워터마킹 : 주파수 영역에 워터마크를 삽입하는 방법이다. 즉, 영상을 고속 푸리에 변환(FFT : Fast Fourier Transform), 이산 코사인 변환(DCT : Discrete Cosine Transform), 웨이블릿 변환(Wavelet Transform) 등을 이용하여 주파수 영역으로 변환한 후에 워터마크를 삽입하는 방법이다.

(3) 워터마크 삽입 및 검출 방식에 따른 분류

- Private 워터마킹(non-blind 워터마킹)
- Semi-Private 워터마킹
- Public 워터마킹(blind or oblivious 워터마킹)
- Public Key 워터마킹

(4) 가시성에 따른 분류

- Visible 워터마킹
- Invisible 워터마킹

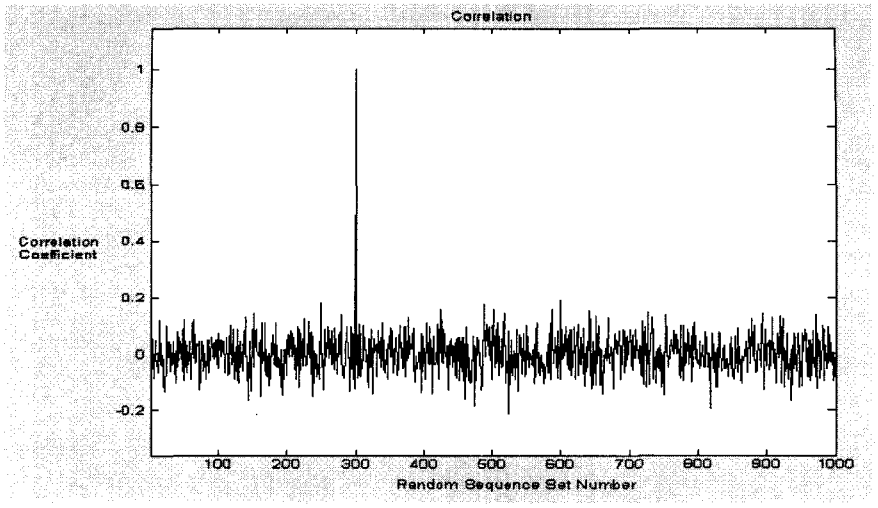
2.2 상관도 측정기반 워터마킹(correlation-based Watermarking)[4-12]

공간 영역(spatial domain)에서 영상에 워터마크를 삽입하는 가장 간단한 방법은 영상의 각 픽셀들의 밝기값(luminance value)에 유사난수 패턴을 더하는 것이다. 워터마크가 삽입된 영상 $I_W(x,y)$를 만들기 위해서 유사난수 패턴 $W(x,y)$에 이득요소(gain factor) k를 곱하고 원본 영상 $I(x,y)$에 더한다.

$$I_W(x,y) = I(x,y) + k \cdot W(x,y) \qquad \text{(식 1)}$$

워터마크가 삽입되었을지 모르는 어떤 영상 $I_W(x,y)$에서 워터마크를 검출하기 위해서 영상 $I_W(x,y)$와 유사난수 패턴 사이의 상관도를 계산한다. 정확한 키를 가지고 생성된 유사난수 패턴과의 상관도는 높지만 서로 다른 키를 사용하여 발생된 유사난수 패턴들은 낮은 상관도를 갖는다. 따라서, 워터마크의 존재 여부를 결정하기 위해서 임계값(threshold) T를 정한다. 만일 상관계수가 어떤 임계값 T를 초과한다면, 영상 $I_W(x,y)$는 워터마크 $W(x,y)$를 가지고 있는 것이다.

$$R_{I_W(x,y)W(x,y)} > T \rightarrow W(x,y) \ extracted$$
$$< T \rightarrow No \ W(x,y) \ extracted \qquad \text{(식 2)}$$



〈그림 2〉 시드키가 300일 때 생성된 유사난수 패턴과 1000개의 시드키로 각각 생성된 유사난수 패턴과의 상관도

그림 2는 1000개의 시드키 중에서 하나를 사용하여 유사난수 패턴을 생성하고, 이 패턴과 각각의 시드키를 사용한 유사난수 패턴과의 상관도를 나타낸다. 여기에서는 시드키 300을 사용하여 유사난수 패턴을 생성하였음을 알 수 있다. 그리고 정확한 시드키가 아닐 경우는 상관도가 0.2 보다 작은 값을 가지고 있다.

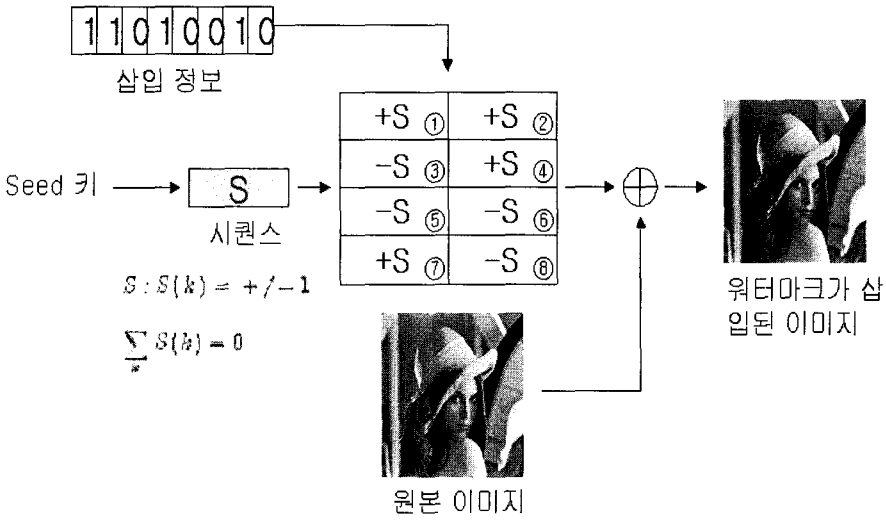
2.3 대역확산 기법을 이용한 워터마킹(watermarking using spread spectrum)

대역확산 통신기술은 1960년대부터 군사용으로 주로 사용되어 왔다. 적에게 도청이 되지 않고, 적의 방해전파에도 강한 통신방식을 구현하고자 했기 때문에 대역확산 통신방식은 꾸준히 발달해 왔다. 확산코드에 의한 통신방식은 송신 데이터에 확산코드를 곱해주고 이렇게 곱해진 원래의 송신 데이터는 확산코드와 같은 속도의 확산신호가 된다. 이 확산신호를 전자파를 실어서 송신을 하고, 수신 쪽에서는 이 확산신호에 다시 송신 쪽에서 사용한 동일한 확산 코드를 곱해주면 원래 송신하고자 했던 데이터를 얻을 수 있다.

CDMA(Code Division Multiple Access) 같은 대역확산 기법을 이용한 워터마킹 방법은 많은 장점을 가지고 있다[4-12]. [3]에서 제안한 Cox의 방법은 워터마킹 알고리즘을 공개할 수 있고, 워터마크가 유사난수 잡음과 같은 특징을 가지고 있으며, 시각적으로 중요한 부분에 워터마크를 삽입한다는 특징을 가지고 있다.

그림 3은 대역확산 기법을 이용한 워터마킹 방법의 한 예이다. 먼저, 영상을 같은 크기의 블록으로 나눈다. 이때 블록의 수는 영상 안에 삽입하려는 정보의 비트수로 결정된다. 다음으로 시드키를 사용해서 평균이 0이고 {-1}과 {+1}로 구성되는 유사 순열 'S'를 발생시킨다. 원본 영상에 삽입될 워터마크는 +S 또는 -S 같은 블록의 연속으로 구성된다. 만일 삽입정보 비트가 +1이면 +S, 그렇지 않으면 -S이며, 그림 3과 같이 원본 영상에 삽입된다.

워터마크가 삽입된 영상에서 워터마크를 추출하기 위해 S와 워터마크가 삽입된 영상의 각 블록 사이의 상관계수를 계산한다. 만일 결과가 0보다 크면 삽입정보 비트가 1이고, 반대의 경우는 0이다.



〈그림 3〉 대역확산 기법을 이용한 워터마킹 삽입 알고리즘

2.4 Fragile 워터마킹

Fragile 워터마킹은 디지털 컨텐츠의 인증 및 무결성의 검정을 목적으로 한다. Fragile 워터마크가 삽입된 영상을 변형할 경우 쉽게 워터마크 정보가 폐기되는 특성을 이용하면 변형 여부를 쉽게 알아낼 수 있으므로 원본 증명과 같은 분야에 응용할 수가 있다. 예를 들어, 원본 증명이 필요한 문서를 출력하여 배포하는 경우를 살펴보면 출력시 인쇄물에 fragile 워터마크 정보를 삽입하고 배포를 하게 되면 이를 복사기로 복사하는 과정에서 워터마크 정보에 손실이 발생하게 된다. 따라서, 워터마크 정보의 존재 여부를 판별함으로써 원본 문서의 진위를 가릴 수 있게 되는 것이다.

Yeung & Mintzer의 방법[13]은 LUT(look-up table)을 이용하며 워터마크를 표시하기 위해서 LSB를 변형한다. 이 방법의 문제점은 LUT와 로고(워터마크)가 다양한 영상에 다시 사용될 경우 위조되기 쉽다는 것이다. Wong의 방법[14]은 영상을 블록들로 나누고 LSB에 해쉬함수와 public key를 사용하여 워터마크를 삽입한다. 이 방법은 변경된 위치측정(localization)이 제한되고, 알고리즘이 느리다는 단점을 가지고 있다.

3. 제안한 워터마킹 알고리즘

3.1 Robust 워터마킹

3.1.1 유사난수 패턴 생성(pseudo-random pattern generation)

확산코드는 대역확산을 효과적으로 하기 위해서 각각의 확산코드 사이에 상호연관(cross-correlation)이 없어야 한다. 즉, 랜덤잡음(random noise) 또는 백색 잡음(white noise)과 같은 특성을 가지고 있어야 한다. 대역확산 통신방식에서 두 확산 신호 사이에 상호연관이 있으면, 두 확산코드 사이에 이 양만큼 상호간섭을 주게 되어 통화품질 저하 및 채널용량이 감소하게 된다. 이와 같은 특성을 수학적으로 표현하면 다음과 같다.

$$\frac{1}{N}\int_0^T p_i(t)p_j(t)dt = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases} \qquad \text{(식 3)}$$

즉, 임의의 시간 T 동안에 각각의 확산코드를 곱했을 때 같은 확산코드를 곱해준 경우에만 1이 되고, 다른 확산코드를 곱하면 0이 되어 신호가 나타나지 않아야 한다. 이와 같은 특성을 잘 만족하

는 신호는 반복주기가 무한히 긴 랜덤잡음(random noise) 또는 백색 잡음(white noise)이다. 디지털 신호의 경우에는 랜덤 시퀀스(random sequence)를 사용하며 신호를 재생하기 위해서는 송신할 때 곱한 확산코드와 동일한 확산코드를 곱해야 하므로 재생이 가능한 랜덤 시퀀스를 사용해야 한다. 따라서, 유사난수잡음(pseudo-random noise)을 주로 사용하며, 다음과 같은 특징을 갖는다.

- 반복주기가 충분히 길다.
- 한 주기 속에 각 시퀀스 간에 상호연관이 매우 작다.
- 한 주기 속에 0과 1의 개수가 비슷하다.
- 시퀀스의 일부를 가지고 전체 시퀀스를 재생할 수 없다.
- 적절한 방법으로 다시 재생 가능해야 한다.

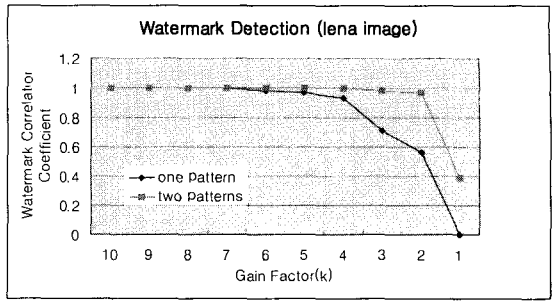
본 논문에서는 이러한 대역확산 통신기술에서 사용하는 확산코드의 특성을 이용하여 삽입하고자 하는 정보 0과 1을 대신해서 표현할 워터마크로서 두 개의 유사난수 패턴을 생성한다. 본 논문에서는 시드키를 사용하여 4x4크기의 유사난수 패턴 하나를 먼저 생성한다. 이때 만들어진 유사난수 패턴은 {-1}과 {1}로 구성되고 각 성분의 합은 0이다. 그리고 이 패턴의 부호를 바꿈으로써 상관도가 -1인 또 다른 패턴을 만들었다. 그림 4는 실험에서 사용한 두 개의 유사난수 패턴이다.

-1	1	-1	1
1	-1	-1	1
-1	1	-1	1
1	1	-1	-1

1	-1	1	-1
-1	1	1	-1
1	-1	1	-1
-1	-1	1	1

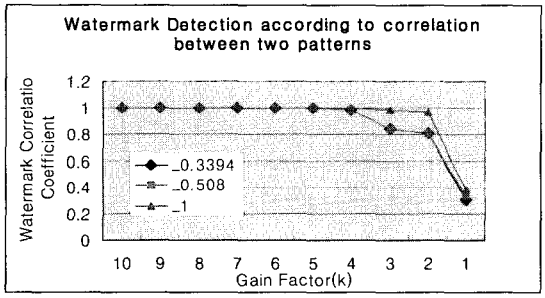
〈그림 4〉 본 논문에서 실험에 사용한 상관도가 -1인 두개의 유사난수 패턴

그림 5에서는 삽입 정보 0과 1을 표현하기 위



〈그림 5〉 하나의 패턴을 사용할 경우와 두 개의 패턴을 사용할 경우의 워터마크 검출 성능 비교

해서 한 개의 패턴을 사용하는 것과 두 개의 패턴을 사용하는 것을 비교하였다. 결과에서 알 수 있듯이 두 개의 패턴을 사용하는 것이 보다 좋은 워터마크 검출 성능을 보여 주었다.



〈그림 6〉 상관도에 따른 워터마크 검출 성능 비교

두 개의 패턴으로 삽입 정보를 표현할 경우 기존의 논문에서는 상관도가 적은 두 개의 유사난수 패턴을 사용하였다. 그러나 본 논문에서는 처음 만든 유사난수 패턴의 부호를 변경함으로써 상관도가 -1인 두 개의 유사난수 패턴을 이용하여 삽입 정보 0과 1을 표현하였다. 상관도가 -1이라는 의미는 수학적으로 상관도가 높은 것이지만, {-1}과 {1} 사이의 관계는 실제적으로는 가장 차이가 크기 때문에 워터마크 검출시에 상관도 비교에서 유리할 수 있다. 그림 6에서 보듯이 본 논문에서 제안한 방식으로 유사난수 패턴을 생성했을 경우 워터마크 검출시에 보다 좋은 성능을 보여 주었다.

3.1.2 워터마크 삽입(watermark embedding) 알고리즘

워터마크를 삽입하기 위한 첫 번째 단계는 MxN 크기의 컬러 영상에서 밝기(luminance) 성분을 추출하는 것이다. 인간의 시각은 밝기 성분에 덜 민감하기 때문에 이러한 성질을 이용하여 컬러 영상의 밝기 성분에 워터마크를 삽입한다. 만약 컬러 영상의 포맷이 RGB라면 밝기 성분을 얻기 위해 YUV 색상 공간으로 바꾸어야 한다. 그리고 2단계 DWT를 사용하여 각 서브밴드를 구성한다. 이렇게 구해진 HL2, LH2, HH2 서브밴드는 유사난수 패턴을 삽입하기 위해 4x4 크기의 블록으로 나누어진다. 각 블록은 삽입하고자 하는 워터마크 비트에 따라 유사난수 패턴을 삽입한다. 삽입 방법은 다음의 공식에 따라 웨이블릿 계수(wavelet coefficient)를 변형한다.

$$I_{DY'}(i) = I_{DY'}(i) + k \cdot pattern \qquad \text{(식 4)}$$

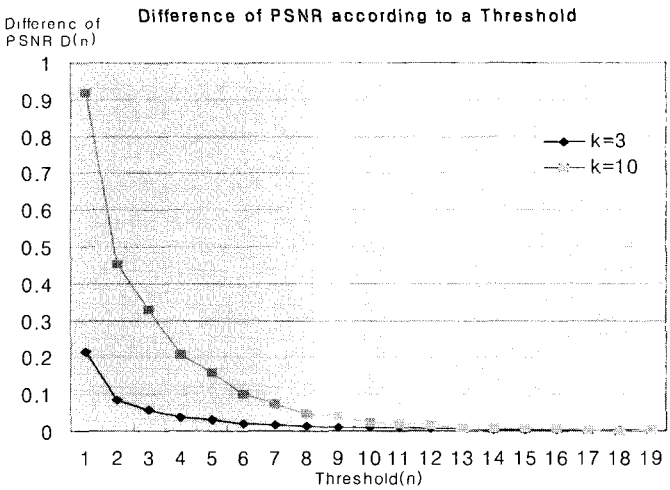
$I_{DY'}(i)$는 크기 4x4인 블록 i의 밝기 성분 $I_{Y'}$의 웨이블릿 계수이다. k는 이득요소(gain factor)로서 워터마크 삽입 강도(strength)를 조절한다. $pattern$은 앞에서 생성한 두 개의 4x4 유사난수 패턴을 의미한다. 만일 워터마크 비트가 0일 경우 첫 번째 유사난수 패턴이 삽입되고, 그렇지 않으면(워터마크 비트가 1일 경우) 두 번째 유사난수 패턴을 삽입한다.

이때 강인성(robustness)과 비가시성(imperceptibility)의 균형을 위해서 워터마크 삽입 강도를 조절한다. 먼저 워터마크 삽입 강도를 조절하기 위한 임계값(threshold) T를 정한다. 만일 웨이블릿 계수가 임계값 T를 초과하면 워터마크 삽입 강도는 이득요소 k를 그대로 사용한다. 그러나 만일 웨이블릿 계수가 임계값 T보다 작다면 워터마크 삽입 강도는 $\frac{1}{2}k$가 된다. 이렇게 웨이블릿 계수의 크기에 따라 워터마크 삽입 강도를 조절함으로써 컬러 영상의 품질은 향상될 수 있다. 그림 7은 임계값에 따른 PSNR의 차이를 비교한 그림이다.

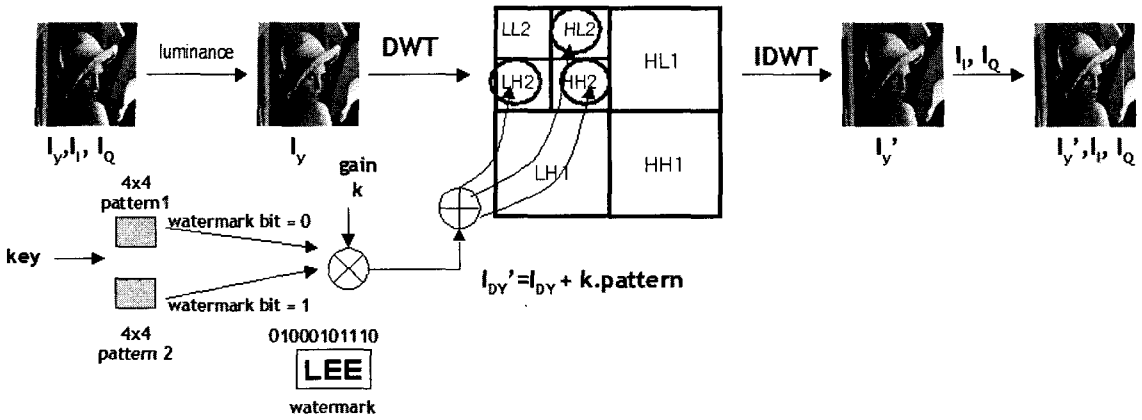
PSNR 차이 $D(n)$은 다음과 같이 표현할 수 있다.

$$D(n) = P(n+1) - P(n) \qquad \text{(식 5)}$$

$P(n)$: $T = nk$ 일 때 워터마크가 삽입된 영상의 PSNR



〈그림 7〉 임계값에 따른 PSNR의 차이



〈그림 8〉 워터마크 삽입 알고리즘

그림 7에서 알 수 있듯이 임계값이 증가할수록 워터마크가 삽입된 영상의 PSNR은 좋아진다. 그러나 임계값이 증가할수록 향상되는 PSNR의 폭은 줄어든다. 따라서, 본 논문에서는 임계값 T를 $3k$로 결정하였다.

그림 8은 본 논문에서 제안하는 워터마크 삽입 알고리즘의 다이어그램이다.

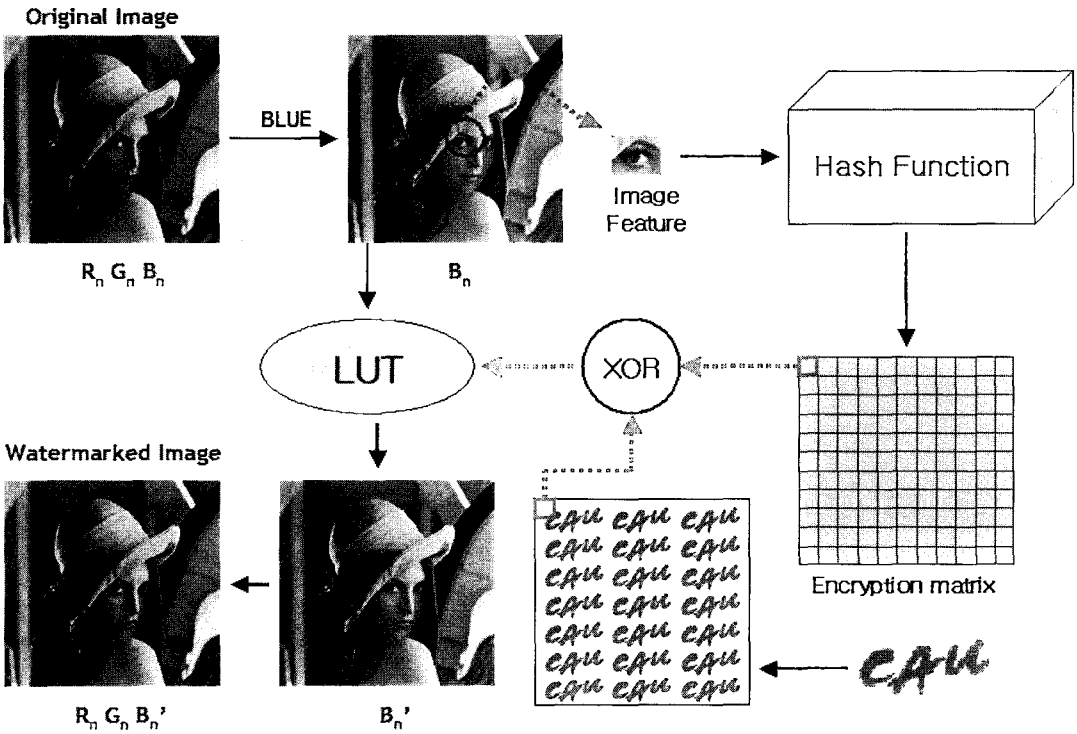
3.1.3 워터마크 검출(watermark Detection) 알고리즘

워터마크 검출 방법은 워터마크 삽입 방법과 유사하며 DWT 도메인에 삽입된 워터마크를 검출하기 위해서 상관도를 이용한다. 먼저 워터마크가 삽입된 컬러 영상의 밝기 성분을 추출한다. 그리고 2단계 DWT를 이용하여 각각의 서브밴드를 구성하고 HL2, LH2, HH2 서브밴드를 4x4 크기의 블록으로 다시 나눈다. 삽입된 워터마크 비트를 알아내기 위해서 DWT 서브밴드 각 블록과 두 개의 유사난수 패턴 사이의 상관도를 계산한다. 만일 첫 번째 유사난수 패턴과 서브밴드 블록 사이의 상관도가 두 번째 유사난수 패턴과 서브밴드 블록 사이의 상관도 보다 크다면 워터마크 비트는 0으로 판정된다. 그러나 반대로 작다면 워터마크 비트는 1이 된다. 워터마크가 모두 검출될 때 까지 이러한 과정을 각 서브밴드(HL2, LH2, HH2)의 모든 블록에서 반복한다.

3.2 Tamper Detection을 위한 fragile 워터마킹

본 논문에서는 Robust 워터마크를 삽입한 후에 tamper detection을 위해서 RGB 색상 모델에서 Blue 채널을 추출하고, Blue 채널의 공간 영역 상에 fragile 워터마크를 삽입한다. 그림 9는 tamper detection을 위한 fragile 워터마크의 삽입 과정을 설명한다. 다음은 워터마크 삽입 단계이다.

1. 먼저, 원영상에서 특징점을 선택한다.
2. 영상의 특징점으로 선택한 픽셀 값들을 입력 값으로 해쉬값을 구한다. 본 논문에서는 sha256 해쉬함수를 사용하였다. 따라서, 해쉬값은 256비트이다.
3. 256 비트의 해쉬값을 반복하여 원영상과 같은 크기의 encryption matrix를 만든다.
4. 로고(logo) 또한 반복하여 원영상과 같은 크기의 워터마크를 만든다.
5. 3,4에서 만들어진 결과를 XOR한다.
6. 원영상의 블루채널에서 각 픽셀의 LUT (look-up table) 값과 5의 결과를 비교한다.
7. 같은 값이면 원영상 블루 채널의 픽셀을 그



〈그림 9〉 Tamper Detection을 위한 fragile 워터마킹 삽입 알고리즘

대로 사용하고, 다른 값일 경우 LUT에서 일치하는 가장 가까운 값으로 픽셀값을 대체한다.

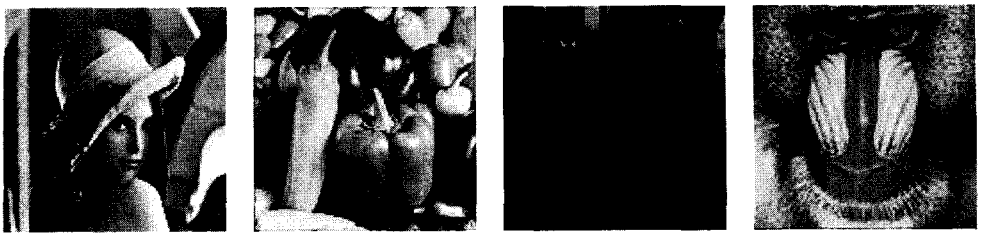
본 논문에서는 특징점을 임의로 잡아 주었다. 예를 들어 Lena 영상의 경우 오른쪽 눈을 특징점으로 하였다. 실제 응용에서는 용도에 맞는 특징점 검출 알고리즘을 사용한다. 이렇게 특징점의 해쉬값과 로고값을 XOR한 값을 LUT를 이용하여 삽입함으로써, 만일 영상의 중요한 부분에 변형이 가해지면 원본 영상이 파괴되므로 안정성이 향상되었다. 그러나 특징점으로 선택한 부분에 대해서는 워터마크를 삽입하지 않았다.

4. 실험 결과 및 고찰

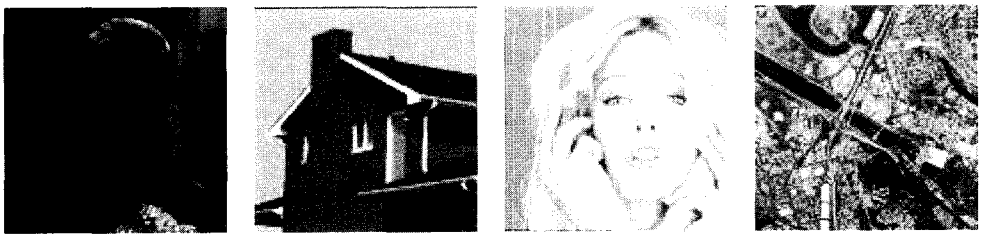
본 논문에서는 제안한 워터마킹 알고리즘은 다음의 환경에서 실험하였다.

그림 10은 실험에서 사용한 Lena, Peppers, Couple, Baboon, Girl, House, Tiffany, San Diego 컬러 영상들이다. 본 실험에서는 8가지의 512x512x24bit 컬러 영상을 사용하였고, 주파수 영역으로의 변환을 위해서 Harr 방식의 이산 웨이블릿 변환을 사용하였다. 그리고 실험을 통해서 제안한 워터마킹 알고리즘이 강인성과 비가시성을 만족하는지 여부에 중점을 두었다. 따라서, 워터마크를 삽입한 후에 영상의 PSNR을 측정하고, JPEG 압축, 잡음 첨가 등의 영상처리 후에 워터마크를 검출할 수 있는지 확인하였다.

- 컴퓨터 사양 : Pentium 4, 메모리 512램
- 운영 체제 : Microsoft Window XP
- 구현 프로그램툴 : MATLAB 6.1



(a) Lena (b) Peppers (c) Couple (d) Baboon



(e) Girl (f) House (g) Tiffany (h) San Diego

〈그림 10〉 실험에 사용한 512x512x24bit 컬러 영상들

4.1 비가시성 평가

그림 11에서는 Lena 컬러 영상에 대해서 원본 영상과 본 논문에서 제안한 워터마킹 알고리즘을 이용하여 워터마크를 삽입한 영상을 비교하였다. 본 실험에서는 워터마크 삽입 강도를 $k=5$로 정하였다.

그림 11을 보면 주관적인 관점에서 원본 영상과 워터마크가 삽입된 영상의 화질 차이가 보이지 않음을 알 수 있다. 원본 영상과 워터마크가 삽입된 영상의 비가시성에 대한 좀 더 객관적인 평가를 위해서 식 6을 사용하여 PSNR(Peak Signal to Noise Ratio)을 구할 수 있다.

$$PSNR = 10 \cdot log_{10}\frac{255^2}{MSE^2} = 10 \cdot log_{10}\frac{255^2}{\sum(f(x)-f(x)')^2} \quad \text{(식 6)}$$

(a) (b)

(그림 11) (a) Lena 원본 영상 (b) 워터마크가 삽입된 영상 (c) 워터마크

$f(x)$: 원본 영상 $f(x)'$: 워터마크가 삽입된 영상

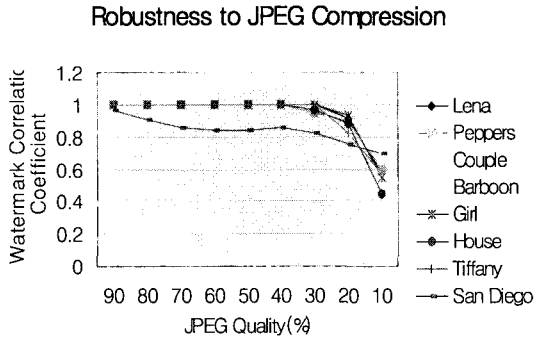
표 1은 식 6을 사용하여 원영상과 워터마크가 삽입된 영상의 PSNR을 측정한 결과이다.

〈표 1〉 각 영상에 대한 PSNR 측정 [dB]

Lena	Peppers	Couple	Baboon
52.7065	52.8301	53.5650	51.4585
Girl	House	Tiffany	San Diego
53.6780	53.6730	53.2795	50.8452

4.2 JPEG 압축에 대한 강인성(Robustness to JPEG Compression) 평가

본 실험에서는 JPEG Quality를 90%에서 10%까지 변경하면서 다양한 영상에 대해서 JPEG 압축에 대한 강인성을 평가하였다. 그림 12에서 JPEG 압축에 대해서 매우 강인함을 알 수 있다.



〈그림 12〉 JPEG 압축에 대한 강인성 평가

〈표 2〉 기타 공격에 대한 강인성 평가

Type		Lena	Peppers	Couple	Baboon
No Attack		1	1	1	0.9834
Noise Addition	5%	1	1	1	0.9834
	10%	0.9834	1	0.9834	0.9674
	15%	0.9045	0.9322	0.9370	0.8719
	20%	0.8822	0.8402	0.8767	0.7759
Blur		1	1	1	0.9190
Blur more		1	0.9834	1	0.8128
Sharpen		1	1	1	1
Sharpen more		1	1	1	1
Sharpen Edges		1	1	1	0.9674
Type		Girl	House	Tiffany	San Diego
No Attack		1	1	1	0.9519
Noise Addition	5%	1	1	1	0.9519
	10%	1	1	0.9674	0.8904
	15%	0.9674	0.9674	0.9087	0.8827
	20%	0.7876	0.7290	0.7507	0.7293
Blur		1	1	1	0.8533
Blur more		1	1	1	0.7488
Sharpen		1	1	1	0.9834
Sharpen more		1	1	1	1
Sharpen Edges		1	1	1	0.9674

4.3 기타 공격에 대한 강인성 평가

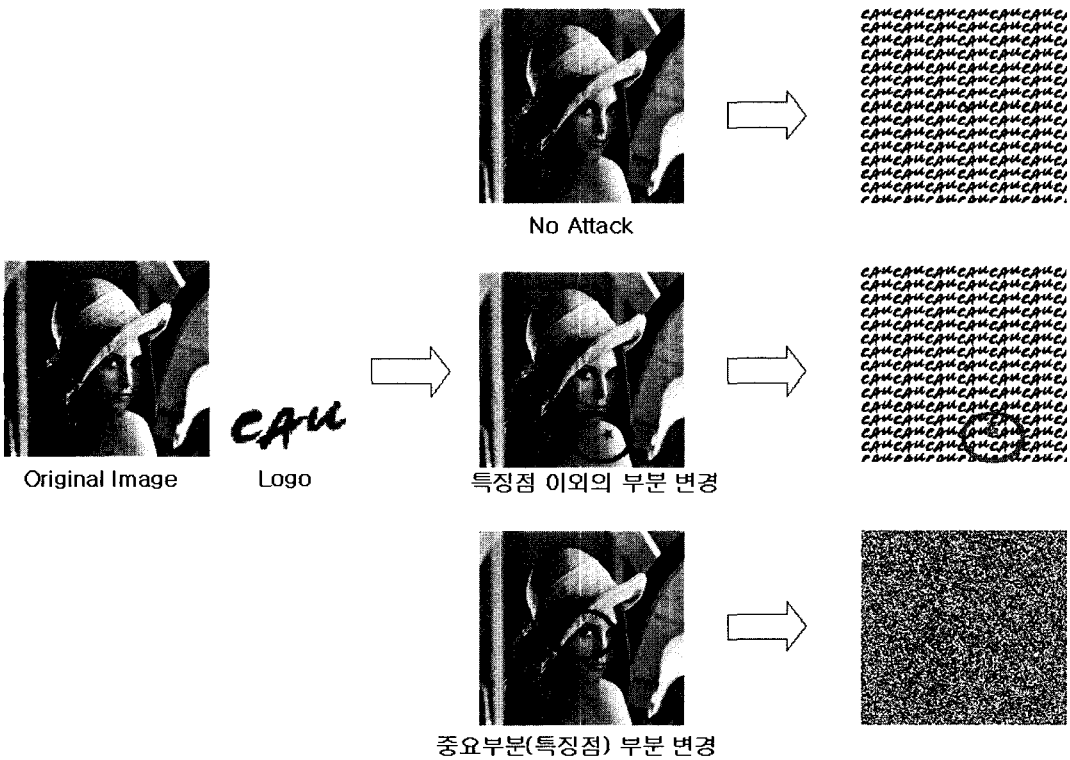
본 논문에서는 JPEG 압축 실험 이외에 잡음첨가(noise addition), blur, blur more, sharpen, sharpen more, sharpen edge 같은 공격 실험을 수행하였다. 표 2를 통해서, 본 논문에서 제안한 robust 워터마킹 알고리즘이 잡음첨가, blur, sharpen 같은 공격에 대해서도 강인함을 알 수 있다.

4.4 Tamper Detection

앞에 실험 결과에서 알 수 있듯이 본 논문에서 제안한 robust 워터마킹 알고리즘은 JPEG 압축, 잡음첨가, blur, sharpen 같은 공격에 대해서 강인한 특성을 보여 주었다. 그러나, 여전히 기하학적 공격에 대해서는 제한적인 워터마크 검출 성능을 보여 주었다. 따라서, 본 논문에서는 이러한 문제를 해결하기 위해 컬러 영상 Blue 채널의 공간 영역에 조작 여부를 감지할 수 있는 워터마크를 삽입하였다. 특히, 영상의 중요한 부분, 즉 특징점을 해쉬함수의 입력 값으로 사용함으로써 중요한 부분을 조작할 경우 원영상이 파괴되도록 워터마킹 알고리즘을 설계하였다. 그림 13에서 이러한 temper detection 과정을 설명하고 있다.

5. 결론 및 향후 연구

본 논문에서는 두 가지 워터마크를 주파수 영역과 공간 영역에 삽입하는 하이브리드 워터마킹 방법을 제안하였다. 먼저, 원영상을 Harr 방식의 DWT 변환으로 주파수 영역으로 변환한 후 밝기 성분에 robust 워터마크를 삽입하였다. 공간영역에서는 원영상의 blue 채널 상에 tamper detection을 위한 fragile 워터마크를 삽입하였다.



〈그림 13〉 Tamper Detection 실험 결과

실험 결과 주파수영역에 삽입된 robust 워터마크의 경우 JPEG 압축, 잡음첨가, blur, sharpen 등 일반적인 신호처리 공격에 강인함을 알 수 있었다. 공간영역에 삽입된 fragile 워터마크의 경우에도 영상의 조작이 있을 경우, 우수한 tamper detection 성능을 보여 주었고, 또한 영상의 중요한 부분을 해쉬함수의 입력 값으로 설정함에 의해 불법적인 사용자가 영상을 조작할 경우 원본 영상이 파괴되도록 하였다.

지금까지 연구된 워터마킹 기술의 경우 부분적으로 임의의 공격에 견딜 수 있으며 인지적으로도 양호한 결과를 보인다고 발표되고 있다. 하지만 현재까지 모든 조건을 만족하는 강인한 워터마크 알고리즘은 많은 기술적인 발전이 있어야 가능할 것으로 보인다. 따라서, 워터마킹 기술은 DRM, Tracking System과 같은 솔루션과 상호보완적인 기술로서 연구되고 있다. 그리고 본 논문에서 제시한 방법과 같이 서로 다른 특징을 갖는 워터마크를 동시에 삽입함으로써 상호 보완할 수 있는 하이브리드 워터마킹 방법 또한 좋은 연구 방향이 되고 있다.

향후 연구 과제는 보다 다양한 공격에 대해서 강인할 수 있도록 워터마킹 알고리즘을 개선하는 것이다. 예를 들어, 클로핑 같은 공격에 대해서 단순히 tamper detection하는 것이 아니라 기하학적인 공격에 대해서도 강인할 수 있도록 연구할 계획이다. 아울러, DRM이나 워터마킹 Tracking System과 같은 솔루션에 응용할 수 있도록 워터마킹 알고리즘을 개선시키려고 한다.

감사의 글

본 논문은 2002년도 중앙대학교 학술연구비 지원에 의한 것임.

참 고 문 헌

[1] 이민섭, "현대암호학", pp. 2, 교우사, 2001.

[2] 우찬일, 신인철, "인증과 무결성을 위한 비밀키 워터마킹", 한국정보처리학회 논문지, 제 7권 제 11호, pp. 3576-3583, 2000.11.

[3] Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T., "Secure spread spectrum watermarking for multimedia", Image Processing, IEEE Transactions on, Vol. 6, pp. 30-37, 1997.

[4] 이현석, 장성갑, 이원형, "CDMA를 이용한 Correlation 기반 워터마킹 기법", 한국인터넷정보학회 춘계학술발표대회논문집, 제 4권 제 1호, pp. 3-11, 2003.5.

[5] 이현석, 장성갑, 이원형, "대역확산기법을 이용한 상관도 측정기반 워터마킹 방법에 관한 연구", 한국통신학회 하계학술발표대회논문집, vol.27, 2003.6.

[6] 옥타비아 비비, 이현석, 이원형, "컬러영상을 위한 하이브리드 워터마킹", 한국인터넷정보학회 추계학술대회논문집, 제 4권 제 2호, pp. 385-388, 2003.11.

[7] 이현석, 옥타비아 비비, 이원형, "Wavelet-based Watermarking using Correlation Comparison", 대한전자공학회 추계학술대회논문집, 제 26권 제 2호, pp. 217-220, 2003.11.

[8] Langelaar, G.C., Setyawan, I., Lagendijk, R.L., "Watermarking digital image and video data. A state-of-the-art overview", IEEE Signal Processing Magazine, Vol.17, pp. 20-46, 2000.

[9] Miyazaki, A., Okamoto, A., "Analysis and improvement of correlation-based watermarking methods for digital images", Circuits and Systems, ISCAS 2002, IEEE International Symposium on, Vol. 3, III-213-III-216, 2002.

[10] Vassaux, B., Bas, P., Chassery, J.-M., "A new CDMA technique for digital image watermarking, enhancing capacity of insertion and robustness", Image Processing, Proceedings. 2001 International Conference on, Vol. 3, pp.983-986, 2001.

[11] Kohda, T., Ookubo, Y., Shinokura, K., "Digital watermarking through CDMA channels using spread spectrum techniques", Spread Spectrum Techniques and Applications, 2000 IEEE Sixth International Symposium on, Vol. 2, pp.671-674, 2000

[12] Silvestre, G.C.M., Dowling, W.J., "Embedding data in digital images using CDMA techniques", Image Processing, Proceedings. 2000 International Conference on, Vol. 1, pp. 589-592, 2000

[13] M. Yeung, F. Mintzer, "An Invisible Watermarking Technique for Image Verification", Proc. ICIP'97, 1997.

[14] P.W. Wong, "A Public Key Watermark for Image Verification and Authentication", In Proceeding of ICIP, Oct. 1998.

◐ 저 자 소 개 ◑

이 현 석(HyunSuk Lee)
2002년 중앙대학교 전자전기공학부 졸업(학사)
2004년 중앙대학교 첨단영상대학원 영상공학과 졸업(석사)
2004년~현재 : LG전자 정보통신
관심분야 : 영상처리, 3D 솔루션, 모바일 차세대 플랫폼
E-mail : hslee9392@lge.com

비비 옥타비아(Vivi Oktavia)
2000년 Bandung Institute of Technology 대학교 Electrical Engineering 학과 졸업(학사)
2000~2003 년 IBM Indonesia, Storage Specialist
2003~현재 : 중앙대학교 첨단영상대학원 영상공학과 (석사)
관심분야 : Storage solution (SAN), 영상처리, Watermarking
E-mail : vivi_o@hotmail.com

김 미 애(Mi-Ae Kim)
2001년 숭실대학교 정보과학대학원 졸업(석사)
2004년 중앙대학교 첨단영상대학원 영상공학과 수료(박사)
관심분야 : Watermarking. Image Authentication, Information Hiding
E-mail : kimma@dreamwiz.com

이 원 형(Won-Hyung Lee)
현재 중앙대학교 첨단영상대학원 영상공학과 교수, 한국컴퓨터게임학회 부회장
관심분야 : Digital Contents Protection, Computer Game, Digital Media Art
E-mail : whlee@cau.ac.kr