情報保護學會論文誌
第15券 第2號, 2005. 4

이미지 인증을 위한 DWT 계수기반 다중 워터마킹*

이 혜 란,† 이 경 현‡
부경대학교

Multi-Watermarking for Image Authentication Based on DWT Coefficients

Hye-Ran Lee,† kyung-Hyune Rhee‡
Pukyong National University

요 약

본 논문에서는 악의적인 공격에는 워터마크가 쉽게 깨어지고 비악의적인 공격에는 워터마크가 쉽게 깨어지지 않도록 하는 두 가지 목적을 동시에 만족시키기 위한 다중 워터마킹 알고리즘을 제안한다. Discrete Wavelet Transform(DWT)의 계수를 이용해 이미지를 인증하는 기법으로, 워터마크로 사용될 이진 이미지와 LL3 영역에서 추출된 특징을 조합하여 이미지에 삽입될 정보를 생성한다. 이미지의 공간영역과 주파수영역에 정보를 다중으로 삽입하여 공간영역에서 일어날 수 있는 악의적인 공격에 대응할 뿐만 아니라 주파수영역에서의 blurring, sharpening 및 JPEG 압축과 같은 비 악의적인 공격을 허용하는 기법이다. 공간영역에서는 이미지 블록의 모든 픽셀의 Least Significant Bit(LSB)에 정보를 삽입하고, 주파수영역에서는 삽입할 정보에 따라 LH2와 HL2의 계수를 조절하므로 정보를 삽입하게 된다.

ABSTRACT

In this paper, we propose a multi-watermarking algorithm to satisfy two purposes: fragility against malicious attacks and robustness against non-malicious attacks. The algorithm can be used for image authentication using coefficients of Discrete Wavelet Transform(DWT). In the proposed method, watermarks are generated by combining binary image with some features extracted from the subband LL3, and then they are embedded into both the spatial and frequency domain. That is, on the spatial domain they are embedded into the Least Significant Bit(LSB) of all pixels of image blocks, and on the frequency domain the coefficients of the subband LH2 and HL2 are adjusted according to the watermarks. Thus the algorithm not only resists malicious attack but also permits non-malicious attacks such as blurring, sharpening, and JPEG compression.

Keywords : *Semi-fragile Watermarking, dual-watermark, DWT, Authentication*

Ⅰ. 서 론

이미지에 대한 디지털 워터마킹은 시각적으로 인지할 수 없는 정보인 디지털 워터마크를 디지털 이미지에 삽입하는 기술[1]로서 사용용도에 따라 크게 두 분야 즉, 견고한 워터마킹(robust watermar-

접수일 : 2005년 3월 26일 ; 채택일 : 2005년 4월 13일
* 본 연구는 대학 IT 연구센터(ITRC) 육성지원사업의 지원으로 수행되었음.
† 주저자 : 9helen@hanmail.net
‡ 교신저자 : khrhee@pknu.ac.kr

king)과 연성 워터마킹(fragile watermarking)으로 분류할 수 있다. 견고한 워터마킹은 일반적으로 저작권 보호 및 소유권 증명에 사용하고 연성 워터마킹은 인증과 무결성의 증명을 목적으로 사용한다. 연성 워터마크는 이미지가 정당한 소유자에게서 왔고, 변조되지 않았다는 것을 증명할 수 있어야 한다. 많은 연성 워터마킹 기법들[2-5]이 제안되어져 왔으며, 특히 Wong[6]은 공개키 암호 방식을 이용한 디지털 서명 기반의 블록별 인증 워터마킹 기법을 제안하였다. Wong의 기법은 이미지를 블록으로 나누고 각 블록별로 서명을 생성한 후 각 블록 픽셀의 least significant bit(LSB)에 서명을 삽입한다. 만약 불법적인 변조가 발생한 경우에는 블록의 서명 값이 달라지므로 변조된 곳의 위치를 측정할 수 있게 된다. 하지만 블록별로 독립적으로 워터마킹을 수행하는 Wong의 기법은 블록 cut-and-paste 공격 및 Holliman과 Memon의 counterfeiting 공격[7]에 대해 취약하다는 문제점을 가지고 있다. Wong 기법의 문제점을 보완하기 위해 이웃블록을 사용하는 Li 등[8]의 기법이 제안되었으나 역시 이러한 공격에 견디지 못하였고, 변조 위치의 정확성도 떨어졌다. Barreto 등[9]은 그림 1과 같이 contextual 정보를 이용함으로써 블록별로 독립적으로 워터마킹을 수행하는 기법의 취약점을 피하려고 시도하였으나, transplantation 공격에 안전하지 못하였다. Chien 등[10]은 웨이블릿 변환을 기반으로 하는 연성 워터마킹을 제안하였는데, 3단계 웨이블릿 변환 후 각 서브이미지 블록의 핑거프린트를 생성한다. 블록의 핑거프린트는 블록과 이웃 블록, 저주파수의 정보의 값을 입력으로 하는 해쉬함수에 의해 생성한다. 생성한 핑거프린트는 암호화 한 후 블록의 LSB에 삽입한다. Chien 등의 기법은 공간 영역에서의 변조 및 웨이블릿 계수 변조의 유무를 확인할 수 있으며 이웃 블록과 저주파수의 정보를 사용하여 여러 공격에 견뎌 낼 수 있다. 하지만, 이미지가 변경되었을 경우에는 블록의 핑거프린트 자체를 생성할 수 없어 변경의 유무를 파악하는 시도조차 할 수 없는 심각한 문제가 발생된다.

본 논문에서는 웨이블릿 변환[11]을 수행하여 이미지의 특징을 추출하고, 추출한 특징을 이용해 이중 워터마크를 삽입하여 이미지를 인증하는 연성 워터마킹기법을 제안한다. 먼저, 3단계 웨이블릿 변환을 수행하여 웨이블릿 계수가 가장 견고한 핵심 정보인 LL3을 이미지의 특징으로 사용하며, 워터마크 이미지와 조합하여 이미지에 삽입할 정보로 사용한다. 워터마크는 공간 영역에서 한 번 삽입되고, 주파수 영역에서 한 번 더 삽입된다. 주파수 영역에서는 중간 주파 계수를 조절하므로 워터마크를 삽입하고, 공간 영역에서는 각 블록 픽셀의 LSB에 워터마크를 삽입한다. 이미지의 특징을 이용함으로써 블록 cut-and-paste 공격 및 counterfeiting 공격, transplantation 공격에 강건하며, 웨이블릿 변환 후 중간 주파수에 워터마크를 삽입함으로써 blurring, sharpening, JPEG 압축과 같은 비 악의적인 변환은 허용하는 기법이다.

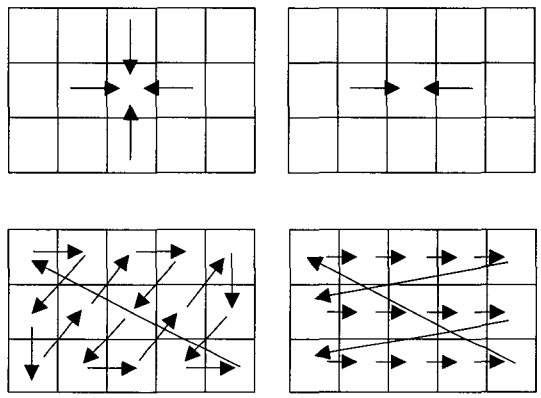

그림 1. contextual 정보 이용 예

본 논문은 먼저 관련 연구에 대해 설명하고, 3장에서 DWT 계수기반의 이중워터마킹을 제안한 후, 4장에서 실험결과를 논하는 순서로 구성되어진다.

II. 관련연구

2.1 Wong의 기법[6]

Wong의 기법은 그레이 레벨 이미지를 위한 공개키 인증 워터마킹으로 $M \times N$ 크기의 이미지 $x_{m,n}$에 이진 워터마크 이미지 $b_{m,n}$을 삽입하여 워터마크된 이미지 $y_{m,n}$을 얻는다. 워터마크의 삽입은 블록별로 독립적으로 이루어지며 삽입 과정은 다음과 같다.

단계 1. 이미지 $x_{m,n}$의 r번째 $I \times J$크기의 블록을 X_r이라 하고, X_r의 LSB를 0으로 바꾼 것을 $\tilde{X}_r$이라 한다.

단계 2. $H(\cdot)$는 MD5와 같은 암호학적인 해쉬 함수로 다음과 같이 계산한다.

$$H(M, N, \mathcal{X}_r) = (p^r_1, p^r_2, \cdots, p^r_s)$$

s는 해쉬 함수의 결과 비트수이다. $IJ \leq s$되기 위해 블록의 크기를 고려해야할 필요가 있다. P_r은 다음과 같이 나타낸다.

$$P_r = (p^r_1, p^r_2, \cdots, p^r_{IJ})$$

단계 3. P_r과 $b_{m,n}$의 블록 B_r을 조합하여 아래와 같이 W_r을 생성한다.

$$W_r = P_r \oplus B_r$$

단계 4. 공개키 암호 시스템으로 W_r을 암호화하며, K는 개인키이다.

$$C_r = E_K(W_r)$$

단계 5. 이진 블록 C_r은 $\mathcal{X}_r$의 LSB에 삽입되어 워터마크된 블록 Y_r가 만들어 진다.

워터마크 검증 알고리즘은 다음과 같다.

단계 1. 검증하려고 하는 블록 Z_r에서 LSB를 여전히 포함하고 있는 G_r과 LSB를 0으로 바꾼 $\mathcal{Z}_r$로 구분하고, 먼저 워터마크 삽입 시에 사용한 개인키 K에 대응하는 공개키 K로 다음과 같이 G_r을 복호화한다

$$U_r = D_K(G_r)$$

단계 2. M, N과 $\mathcal{Z}_r$를 입력으로 하는 해쉬함수를 수행하여 결과 Q_r을 얻는다.

단계 3. U_r과 Q_r을 다음과 같이 계산하여 워터마크를 추출한다.

$$O_r = Q_r \oplus U_r$$

2.2 블록 cut-and-paste 공격과 counterfeiting 공격

블록단위로 독립적으로 워터마킹을 수행하는 기법들의 문제점은 블록 cut-and-paste 공격에 취약하다는 것이다. 블록 cut-and-paste 공격이란 크기가 같은 이미지에 동일한 워터마크가 삽입되어 있다면 해당 이미지의 블록 또는 다른 이미지의 블록을 잘라 붙여 불법적인 변조를 발생시킨다하더라도 정당한 워터마크가 추출되어 마치 변조되지 않은 것처럼 인증이 이루어지는 공격이다. 블록 cut-and-paste 공격을 위해 공격자는 동일한 크기의 이미지에 동일한 워터마크가 삽입된 합법적인 이미지를 수집한다. 워터마크가 삽입될 때에 이미지 고유의 특징이 전혀 고려되지 않으므로 이미지만 충분히 수집한다면 공격자는 성공적으로 공격을 수행할 수 있게 된다. 그림 2는 블록 cut-and-paste 공격의 예를 보여준다. Holliman과 Memon의 counterfeiting 공격은 블록 cut-and-paste 공격을 이미지 전체에 반복적으로 실행하여 위조된 워터마크된 이미지를 생성하는 것이다. 이미지 전체가 위조되었지만, 실제로 새

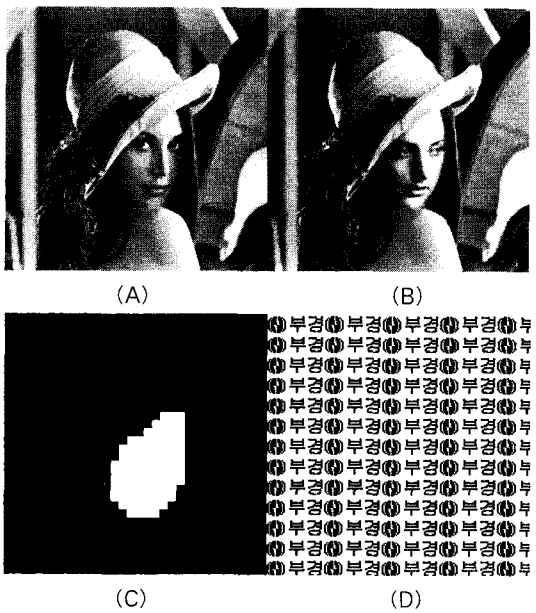

그림 2. (A)워터마크된 영상 (B)동일하게 워터마크된 다른 이미지로부터 얼굴부분을 cut-and-paste 한 영상 (C)실제로 변조된 영역 (D)변조후에도 정상적으로 정상적으로 추출된 워터마크

롭게 구성된 이미지에서 워터마크를 추출하면 성공적으로 워터마크 추출이 가능하게 되는 공격이다.

블록별로 독립적으로 워터마킹을 수행하는 Wong의 기법은 위에서 설명한 블록 cut-and-paste 공격과 counterfeiting 공격에 취약하게 되고, 이웃

블록의 정보를 사용하는 Li 등의 기법도 두 이웃블록으로부터 블록의 반의 LSB를 0으로 바꾼 후 복사하여 붙여 넣고, 그것들의 서명값을 계산하여 삽입하므로 위의 공격이 가능하게 된다.

2.3 Barreto 등의 기법[9]

Barreto 등은 블록 cut-and-paste 공격 및 counterfeiting 공격을 막기 위해 그림 1처럼 이미지의 contextual 정보를 이용하였다. contextual 정보를 많이 이용하면 할수록 이미지의 의존도가 높아져 공격에는 강해질 수 있지만, 의존도만큼의 위치측정의 정확도는 떨어지게 된다. 다음은 contextual 정보를 이웃 블록 한 개를 사용한 블록의 해쉬값을 구하는 식이다.

$$H_t \equiv H(M, N, Z_t^*, Z_{(t-1) \bmod n}^*, t)$$

M, N은 이미지의 크기이며 Z_t^*는 LSB를 0으로 바꾼 해당 블록의 값이고, $Z_{(t-1) \bmod n}^*$는 LSB를 0으로 바꾼 해당 블록의 이전 블록이며, t는 블록의 인덱스이다. Barreto 등의 기법에서는 이전의 블록값을 계속적으로 연결하여 해당 해쉬값을 구하고 있으므로 더 이상 블록 cut-and-paste 공격과 counterfeiting 공격을 행할 수 없게 된다. 하지만, Barreto 등의 기법은 다음에서 소개될 transplantation 공격에는 취약함을 볼 수 있다.

2.4 Transplantation 공격[9]

X'와 $\overline{X}'$는 Barreto 등의 기법으로 워터마크된 이미지라고 할 때, 아래의 $X'_A \rightarrow X'_B$는 블록 X'_B가 블록 X'_A에 의존됨을 나타낸다고 간주하고, 이미지 $\overline{X}'$와 X'가 아래와 같이 주어진다.

$$X' : \cdots \rightarrow X'_A \rightarrow X'_D \rightarrow X'_B \rightarrow X'_C \rightarrow \cdots$$
$$\overline{X}' : \cdots \rightarrow \overline{X}'_A \rightarrow \overline{X}'_E \rightarrow \overline{X}'_B \rightarrow \overline{X}'_C \rightarrow \cdots$$

$$X_A^* = \overline{X}_A^*,\ X_B^* = \overline{X}_B^*,\ X_C^* = \overline{X}_C^*,\ X_D^* \neq \overline{X}_E^*$$

일 때, Barreto 알고리즘의 검출 없이 (X'_D, X'_B) 블록쌍은 $(\overline{X}'_E, \overline{X}'_B)$로 변경될 수 있다.

$$\cdots \rightarrow X'_A \rightarrow \overline{X}'_E \rightarrow \overline{X}'_B \rightarrow X'_C \rightarrow \cdots$$
$$\cdots \rightarrow \overline{X}'_A \rightarrow X'_D \rightarrow X'_B \rightarrow \overline{X}'_C \rightarrow \cdots$$

문서 이미지는 일반적으로 바탕이 되는 흰색 영역을 많이 가지고 있으므로 transplantation 공격에 취약하게 된다. 앞에서 소개한 Barreto 등의 기법도 문서 이미지에 적용될 때 transplantation 공격에 취약한 문제점이 발생한다.

2.5 Chien 등의 기법[10]

Chien 등은 웨이블릿 변환을 기반으로 하는 연성 워터마킹 기법을 제안하였는데 워터마킹 수행과정은 다음과 같다.

단계 1. 3단계 웨이블릿 변환을 수행한다.

단계 2. 고주파 통과 서브이미지를 블록으로 나누어 그 영역을 HRs라고 하고, 저주파 통과 서브이미지 전체를 영역 LR이라고 한다. L은 저주파 통과 서브이미지의 coarse approximation이며, C는 contextual 정보로서 HR의 이웃블록이다. 선택된 영역에 다음 단계를 수행하여 워터마크를 삽입한다.

단계 3. 고주파 통과 서브이미지의 각 블록의 핑거프린트를 다음과 같이 생성한다.

$$HF = H(HR^*, C^*, L^*, N_{i,j})$$

H는 해쉬함수이고, $*$는 LSB를 0으로 바꾼 것이며, $N_{i,j}$는 서브이미지의 번호이다.

단계 4. 저주파 통과 서브이미지의 핑거프린트는 $LF = H(LR^*)$로 생성한다.

단계 5. 개인키 kl로 암호화하여 다음과 같은 서명을 얻는다.

$$HS = E_{kl}(HF)$$
$$LS = E_{kl}(LF)$$

단계 6. HR^*, LR^*의 LSB에 생성한 서명 HS, LS을 삽입한다.

단계 7. 블록에 반복적으로 수행하여 워터마크된 이미지 W를 얻게 된다.

Chien 등은 웨이블릿 변환을 이용하여 공간 영역에서의 픽셀의 변조뿐만 아니라 주파수 영역에서의 계수의 변조를 검출하는 방법을 제안하였고, 이미지의 핵심이 되는 L성분을 서명값의 입력으로 사

용하여 블록의 cut-and-paste 공격 및 counterfeiting 공격에 대응하였다. 하지만 Chien 등의 기법은 이미지의 변조가 심할 경우 L성분의 값이 변경되기 때문에 서명값 생성에 문제가 발생하게 되며, 특정 블록이 변조되었을 경우에도 이미지 전체가 변경된 것으로 나타나므로 위치 측정의 문제도 발생한다.

Ⅲ. DWT 계수기반 이중 워터마킹

본 제안기법은 웨이블릿 변환을 수행하여 이미지의 핵심정보가 되는 저주파 영역을 특징으로 선택한다. 저주파 영역을 아무런 처리 없이 사용할 경우에는 Chien 등의 기법처럼 이미지 변조가 발생할 경우 서명값을 생성할 수 없는 문제가 발생하므로 저주파 영역의 계수들의 관계를 비교하여 특징맵을 생성한다. 생성된 특징맵과 워터마크 이미지가 조합되어 이미지의 삽입 정보로 사용된다. 삽입 정보는 웨이블릿 변환에서의 중간 주파 계수를 조절하므로 주파수 영역에서 삽입되어지고, 서명값을 만들어 공간영역에서 삽입되어 진다. 웨이블릿 변환, 특징 맵 추출, 계수 조절에 대해 간단히 설명한 뒤 워터마크 삽입 및 인증에 대해 기술한다.

3.1 Discrete Wavelet Transform

2차원 이미지를 위한 DWT의 기본 개념은 먼저 이미지를 부대역 필터를 사용하여 수평과 수직의 고주파, 중간주파, 저주파의 4부분으로 나눈다. 고주파 통과 필터와 저주파 통과 필터의 다른 조합으로 이미지는 low-low(LL), low-high(LH), high-low (HL), high-high(HH) 대역으로 나눌 수 있다. 1단계 웨이블릿 변환 이후를 LL1, LH1, HL1, HH1으로 표현하고, LL1대역은 다시 2단계 웨이블릿 변환을 위해 사용된다. 그림 3은 2단계 웨이블릿을 나타낸 것이다. DWT 계수로부터 원이미지를 얻기 위해서는 inverse DWT(IDWT)를 거쳐야 한다.

3.2 특징 맵 추출

이미지의 특징은 3단계 웨이블릿 변환 후 LL3 대역으로 잡는다. 이미지의 특징은 블록 cut-and-paste 공격 및 counterfeiting 공격, transplantation 공격 등을 막기 위한 contextual 정보로 사용하기 때문에 이미지의 어떠한 변경에도 변경되지 않고 강인성을 유지하는 것이 중요하다. 이미지가 변경되면 LL3 대역값이 변경될 수 있으므로 LL3 대역값을 조절할 필요가 있다. 특징 맵은 다음의 식과 같이 해당 계수와 이웃 계수의 차이가 양수이면 '1'로 기록하고, 그렇지 않으면 '0'으로 기록하여 구성한다. 그림 4는 특징 맵을 표현한 것이다.

$$e_{31}(m,n) > e_{31}(m,n+1) : '1'$$
$$e_{31}(m,n) < e_{31}(m,n+1) : '0'$$

$e_{31}(m,n)$에서 e는 웨이블릿 계수를 나타내고, e_{31}에서 인덱스 $_3$은 웨이브릿 변환의 3단계 영역을 나타내는 것이고, 인덱스 $_1$은 3단계에서의 LL성

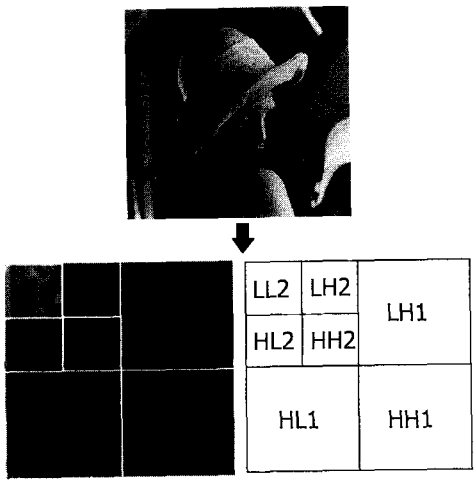

그림 3. 2단계 웨이블릿 변환

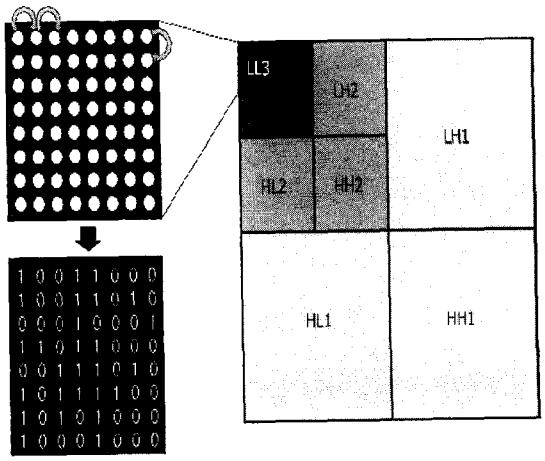

그림 4. 특징 맵

분, 즉 LL3를 나타낸다. e_{32}는 3단계의 LH영역을 나타내고, e_{33}은 3단계의 HH영역, e_{34}는 HL영역, (m, n)은 각 영역의 계수의 위치를 나타낸다.

LL3 대역값을 그대로 사용하지 않고 특징 맵을 이용하면 blurring, sharpening과 같은 비 악의적인 공격에도 효과적이다. 계수의 전체적인 변경이 있어도 특징 맵을 추출할 수 있도록 계수와 그 이웃 계수와의 차이를 이용해 특징 맵을 추출한다.

3.3 계수 조절

주파수 영역 워터마킹에서 워터마크를 저주파 대역에 삽입하면 이미지의 화질에 크게 영향을 주게 되며, 반면 고주파 대역에 워터마크를 삽입하면 이미지의 화질 저하는 줄일 수 있지만 삽입된 워터마크가 이미지 압축 등에 쉽게 깨어져 워터마크를 제대로 검출할 수 없게 된다. 이러한 이유로 워터마크는 보통 중간주파수 대역에 삽입하게 된다. 제안 기법에서도 중간주파수 대역인 LH2와 HL2 대역의 계수를 조절하는 것으로 워터마크를 삽입하게 된다. 만약 워터마터마크 비트가 '1'이면 그림 5와 같이 동일한 위치의 LH2의 계수값과 HL2 계수값을 비교하여 큰 계수값을 가장 근접한 홀수로 조절하고, 워터마크 비트가 '0'인 경우에는 가장 근접한 짝수로 조절한다.

만약 LH2와 HL2의 계수값의 차이가 t보다 작을 경우에는 식 (1)과 같이 최소한 t만큼의 차이를 준다. t값이 커지면 워터마크는 강인해지지만 화질의 열화가 발생할 수 있기 때문에 응용에 따라 t의 값을 조절할 수 있다.

$$\begin{aligned} &|e_{22}(m,n)-e_{24}(m,n)|=d \\ &\qquad d<t\text{이면}, \\ &e_{22}(m,n)\geq e_{24}(m,n) : e_{22}(m,n)+(t-d) \\ &e_{22}(m,n)<e_{24}(m,n) : e_{24}(m,n)+(t-d) \end{aligned} \quad (1)$$

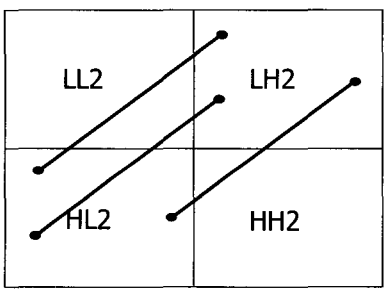

그림 5. 동일한 위치의 LH2계수와 HL2 계수

3.4 워터마크 삽입

워터마크가 삽입될 원이미지 X는 $N\times M$이고, 시각적으로 의미를 가진 이진이미지 B를 워터마크로 사용한다. 워터마크의 삽입과정은 다음 단계와 같이 이루어진다.

단계 1. 이미지 X의 모든 픽셀의 LSB를 제거하여 X^*를 얻는다.

단계 2. X^*에 3단계 웨이블릿 변환을 적용한다.

단계 3. LL3 영역에 식 (1)을 적용하여 특징 맵 F를 추출한다.

단계 4. 특징 맵 F와 워터마크 이진이미지 B에 XOR 연산을 수행하여 이미지에 실제로 삽입될 삽입 정보 C를 얻는다.

$$C=F\oplus B$$

단계 5. 삽입 정보 C로 LH2와 HL2의 계수를 식 (2)와 같이 조절한다. 만약 LH2와 HL2의 계수값의 차이가 t보다 작을 경우에는 위의 식 (1)와 같이 최소한 t만큼의 차이를 준다.

$$\begin{aligned} C(m,n)=1 &\begin{cases} e_{22}(m,n)\geq e_{24}(m,n) & , e_{22}(m,n)\text{: 근접한 홀수} \\ e_{24}(m,n)>e_{22}(m,n) & , e_{24}(m,n)\text{: 근접한 홀수} \end{cases} \\ C(m,n)=0 &\begin{cases} e_{22}(m,n)\geq e_{24}(m,n) & , e_{22}(m,n)\text{: 근접한 짝수} \\ e_{24}(m,n)>e_{22}(m,n) & , e_{24}(m,n)\text{: 근접한 짝수} \end{cases} \end{aligned} \quad (2)$$

단계 6. IDWT를 적용하여 주파수 영역에서 워터마크가 삽입된 $\mathcal{X}$를 얻는다.

단계 7. $\mathcal{X}$는 8×8의 n개의 $\mathcal{X}_r(0\leq r<n)$블록 으로 나눈다.

단계 8. 해쉬 함수 H를 사용하여 블록의 핑거프린트 $H_r=H(M,N,\mathcal{X}_r,F)$을 계산한다.

단계 9. H_r과 B_r을 XOR 연산을 수행하여 E_r을 얻는다.

단계 10. 개인키로 E_r을 암호화하여 디지털 서명 S_r을 생성한다.

단계 11. $\mathcal{X}_r$의 LSB에 S_r을 삽입하여 워터마크된 블록 X'_r을 얻는다.

모든 블록에 단계 8부터 단계11까지를 반복 수행한다. 그림 6의 블록도는 워터마크 삽입 과정을 나타낸 것이다.

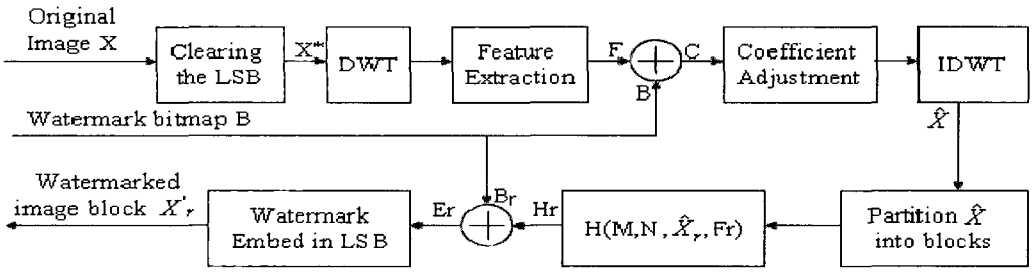

그림 6. 워터마크 삽입 과정

3.5 인증

수신된 이미지 Z를 인증하기 위하여, 먼저 이미지를 블록으로 나눈 후 블록별로 LSB를 추출하여 그 결과를 Z라 두고 LSB를 0으로 제거한 이미지를 Z^*라 한다. 특징 맵을 생성하기 위해 먼저 LSB가 제거된 이미지에 3단계 웨이블릿 변환을 수행한다. 삽입 시와 동일하게 특징 맵 F를 추출하고 특징 맵과 워터마크 이미지를 연산하여 삽입 정보 C'를 얻는다. LH2와 HL2의 계수값을 비교하여 값이 큰 계수가 짝수인지 홀수인지를 비교하므로 C를 얻는다. C'와 C를 비교하여 이미지의 변조 유무를 확인할 수 있다. 다음으로 역웨이블릿 변환을 수행하여 공간 영역상의 이미지로 복원한 다음 특징 맵 F를 이용하여 삽입시와 동일한 방법으로 블록의 서명 S_r을 생성한다. 생성된 S_r와 블록의 LSB에서 추출한 Z를 비교하여 해당 블록의 변조 유무를 확인할 수 있다.

Ⅳ. 실험 결과

본 논문에서 제안한 다중 워터마킹 기법을 검증하기 위해 Daubechies[11,12] 필터를 사용한 이산 웨이블릿을 사용하였다. 실험에 사용한 원 영상에는 256×256 크기의 Lena, Barbara, Camera 그레이 영상을, 워터마크 이진 영상으로는 32×32 크기의 학교 로고를 사용하였고 t값은 0.5로 두었다.

Transplantation 공격을 실험하기 위해 여백이 많은 로고 영상에 워터마크를 삽입하여 실험하였다. 실험은 제안한 방법에 의해 다중 워터마크가 삽입된 영상에 대한 일반적인 영상처리 기법인 blurring과 sharpening, JPEG 압축 공격 등을 실험하였고, 공간 영역에서 블록 cut-and-paste 공격, transplantation 공격 등을 실험하였다. 공간상의 변질된 영역의 위치 판단을 쉽게 하기 위해서 검은색 배경에 흰색 블록으로 변질된 영역을 표시하였다. 워터마크 삽입시 화질에 대한 객관적인 평가를 위해 원 영상과 워터마크된 영상의 MSE(Mean square Error)에 대한 평균값을 이용한 PSNR(Peak Signal-to-Noise Ratio)을 사용하였다.

$$MSE=\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f(i,j)-f'(i,j))^2$$

$$PSNR=10\log_{10}(\frac{255^2}{MSE})$$

$f(i,j)$는 원 영상이고, $f'(i,j)$는 워터마크된 영상이며, MN은 영상의 화소수를 말한다.

그림 8은 Barreto 등의 기법에서 취약했던 transplantation 공격을 제안기법에 적용한 결과로서 두 워터마크된 영상으로부터 여백을 가진 블록을 잘라 붙이기 했을 경우에도 변조된 영역으로 위치측정이 되었음을 알 수 있었다. 주파수 영역에서 워터마크를 삽입한 Chien 등의 기법과 제안기법이 3×3 필터를 이용하여 Blurring과 Sharpening처리 후에 워터마크가 제대로 추출된 것을 볼 수 있었다. 표 1는 JPEG 압축 이후에 워터마크를 추출한 결과로

표 1. JPEG 압축에 따른 워터마크 추출

JPEG 압축 (quality)	Chien 등의 기법	제안기법
70	○	○
65	×	○
60	×	○
55	×	○

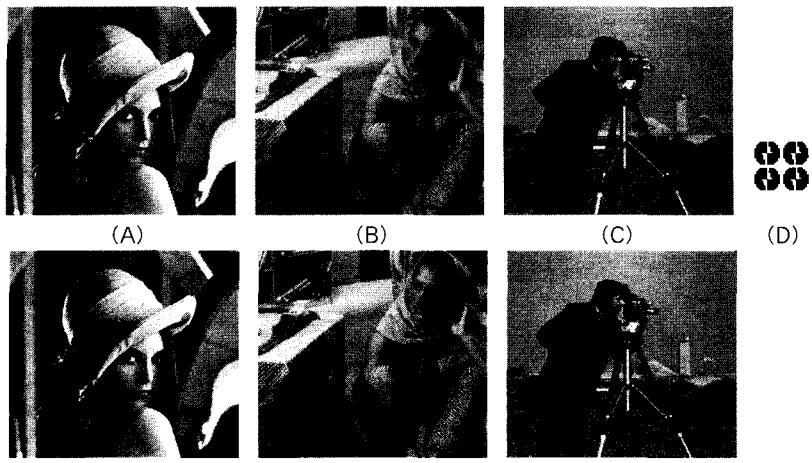

그림 7. (A)(B)(C) 원영상 (D) 워터마크 (E)(F)(G) 워터마크된 영상

서 제안기법은 JPEG quality 55%까지 워터마크가 추출된 반면, 중간주파뿐만 아니라 고주파 영역에도 워터마크를 수행한 Chien 등의 기법은 70%까지만 워터마크가 추출된 것을 확인할 수 있었다.

V. 결 론

합법적인 이미지에 불법적인 변조가 발생한 경우와 통상적인 이미지 처리와 같은 비 악의적인 변화가 발생한 경우를 동시에 만족시킬 수 있는 이미지 인증 알고리즘을 제안하였다. 본 논문은 Discrete Wavelet Transform(DWT)의 계수를 이용해 이미지를 인증하는 기법으로, 워터마크로 사용될 이진 이미지와 LL3 영역에서 추출된 특징을 조합하여 이미지에 삽입될 정보를 생성하였다. 이미지의 공간영역과 주파수영역에 정보를 다중으로 삽입하여 공간영역에서 일어날 수 있는 악의적인 공격에 대응할 뿐만 아니라 주파수영역에서의 blurring, sharpening 및 JPEG 압축과 같은 비 악의적인 공격을 허용하는 기법이다. 공간영역에서는 이미지 블록의 모든 픽셀의 Least Significant Bit(LSB)에 정보를 삽입하였고, 주파수영역에서는 삽입할 정보에

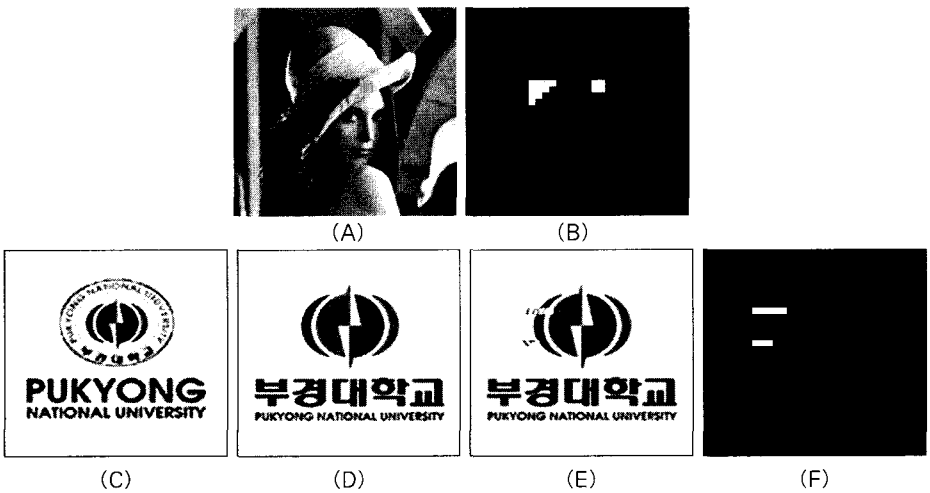

그림 8. (A) 블록 cut-and-paste 공격 (B) 블록 cut-and-paste 공격 후 변조 위치 측정 (C)(D) 워터마크된 영상 (C) transplantation 공격 (F) transplantation 공격 후 변조 위치 측정

따라 LH2와 HL2의 계수를 조절하므로 정보를 삽입하였다. 실험을 통해 제안기법의 성능을 확인하였다. 제안 알고리즘의 적용분야로는 위·변조 등의 변조여부를 판별하면서 통상적인 이미지 처리가 가능한 의료 영상, 법적인 문서 등에 적용이 가능하다. 향후 연구 과제로서 더 다양한 이미지 처리에 강인하면서 이미지를 인증할 수 있는 기법으로의 향상이 필요할 것이다.

참 고 문 헌

[1] 김종원, 신동환, 신승원, 최종욱, "디지털 워터마킹 기술의 산업적 응용" 한국정보보호학회, 정보보호학회지, 12권 1호 pp.11-18, 2002

[1] M. M. Yeung, and F. Mintzer, "An invisible watermarking technique for image verification" *Proceedings of IEEE Int. Conf. Image Processing*, pp. 680-683, 1997

[2] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," *Int. Conf. Multimedia Computing and systems*, pp. 209-213, 1999

[3] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Processing*, Vol. 11, No. 6, pp. 585-595, 2002

[4] J. Fridrich, M. Goljan, and A. C. Baldoza, "New fragile authentication watermark for images," *Proc. IEEE Int. Conf. Image Processing, Vancouver, BC, Canada*, Sept. 10-13, 2000

[5] P. W. Wong, "A watermark for image integrity and ownership verification," *Proceedings of IEEE Int. Conf. Image Processing*, pp. 455-459, 1998

[6] M. Holliman, and N. Memon, "Counterfeiting attacks on oblivious blockwise independent invisible watermarking schemes", *IEEE Trans. Image Processing*, pp.432-441, 2000

[7] C. T. Li, D. C. Lou, and T. H. Chen, "Image authentication and integrity verification via content-based watermarks and a public key cryptosystem," *Proceedings of IEEE Int. Conf. Image Processing*, pp. 694-697, 2000

[8] P. S. L. M. Barreto, H. Y. Kim and V. Rijmen, "Toward secure public-key blockwise fragile authentication watermarking," *IEE Proc.-Vis. Image Signal Processing*, Vol. 149, No. 2, pp.57-62, 2002

[9] C. C. Chien, K. C. Fan, and S. W. Wang, "A wavelet-based public key image authentication watermarking" *Proceedings of IEEE 37th Annual 2003 Int. Carnahan Conf.* pp. 321-324, 2003

[10] R. M. Rao, A. S. Bopardikar, *Wavelet transforms introduction to theory and applications*, Addison-Wesley, 1998

[11] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Trans. signal Processing*, Vol. 41, No. 12, pp.3444-34 63, Dec. 1993

〈著者紹介〉

이 혜 란 (Hye-Ran Lee) 학생회원

1998년 한국방송통신대학교 전자계산학과 학사
2002년 부경대학교 전자계산학과 석사
2005년 부경대학교 전자계산학과 박사과정
〈관심분야〉 Digital Watermarking, DRM, 이미지 인증, 멀티미디어 정보보호

이 경 현 (Kyung-Hyune Rhee) 정회원

1982년 경북대학교 수학교육과 졸업(이학사)
1985년 한국과학기술원 응용수학과(이학석사)
1992년 한국과학기술원 수학과(이학박사)
1985년~1993년 한국전자통신연구소 연구원, 선임연구원
1993년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
1995년~1996년 Univ. of Adelaide, 응용수학과, Australia 방문 교수
1999년 Univ. of Tokyo, 객원 연구원
1997년~현재 한국멀티미디어학회 재무이사, 논문지 편집위원
2001년~현재 한국통신정보보호학회 논문지 편집위원
〈관심분야〉 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론