특집논문-01-6-1-05

비트 플레인을 이용한 영상의 연성 워터마킹

이 혜 주*, 홍 진 우*, 김 진 웅*

Fragile Image Watermarking Using Bit Planes

Hye-Joo Lee*, Jin Woo Hong* and Jin Woong Kim*

요 약

디지털 워터마킹은 워터마크의 성질에 따라 강성 워터마킹(robust watermarking)과 연성 워터마킹(fragile watermarking)으로 분류할 수 있다. 강성 워터마킹은 저작권 보호를 위한 기법이고, 연성 워터마킹은 데이터의 인증/무결성을 위한 기법으로 데이터의 진위를 확인하는 수단으로 이용할 수 있다. 일반적으로 연성 워터마킹은 영상을 변조하거나 위조하였을 때 이전에 삽입되어 있던 워터마크를 검출할 수 없게 되면 영상이 변조나 위조되었다고 판단한다. 영상의 화소 값은 비트의 조합으로 구성되므로 영상의 변조는 비트의 변경을 의미한다고 할 수 있다. 따라서, 본 논문에서는 상위 비트 플레인(bit plane)과 하위 비트 플레인의 변조를 판단하기 위해 2개의 워터마크를 삽입하는 연성 워터마킹을 제안한다. 실험결과, 영상에 삽입된 워터마크는 시각적으로 영상 내에서 확인할 수 없으며, 영상에 변조를 가하였을 때 변조의 위치를 확인할 수 있었다.

Abstract

Digital watermarking has been proposed for copyright protection of digital data. According to the property of an embedded watermark, it is classified into two categories, robust watermarking and fragile watermarking. The former is used for copyright protection, and the latter applies to the authentication/integrity to verify the authenticity of data. If an image has been modified or forged, the embedded watermark cannot be extracted from the image. As a result, it is possible to detect the modification of the image. As pixels are represented by bits, the modification of bits corresponds to the alteration of the image. In this paper, a new fragile watermarking is proposed in which two watermarks are embedded in order to detect some modification occurred in high and low bit planes. From simulation results, the embedded watermark is invisible in a watermarked image and we can locate some places where the modification occurring

I. 서 론

멀티미디어 데이터의 사용 증가와 함께 멀티미디어 데이터를 보호하기 위한 많은 연구가 이루어지고 있다. 특히, 멀티미디어 데이터를 보호하기 위해 워터마크(watermark)라고 하는 기밀 정보를 데이터 자체에 숨겨둠으로써 데이터를 보호하는 디지털 워터마킹(digital watermarking) 기술은 1990년 이후 활발하게 연구되어 왔다[1,2,3,4]. 디지털 워터마킹 기술은 데이터의 저작권 보호(copyright protection)에 응용할 수 있을 뿐만 아니라, 데이터의 변조 여부를 확인할 수 있는 인증/무결성(authentication/integrity)에 응용 가능하다. 전자의 경우, 데이터에 대한 여러 가지 처리에도 워터마크는 충분한 견고성(robustness)을 가져야 하는 반면에, 후자는 워터마크가 변경되었음을 쉽게 발견할 수 있어야 하며, 전자와 후자를 각각 강성 워터마킹(robust

* 한국전자통신연구원 무선방송기술연구소 방송미디어부
Broadcasting Media Technology Department, Radio & Broadcasting Technology Laboratory, Electronics and Telecommunications Research Institute)

watermarking), 연성 워터마킹(fragile watermarking)이라 한다.

연성 워터마킹은 디지털 카메라와 같은 장치에 의해 생성된 디지털 데이터에 워터마크를 삽입하고, 인터넷과 같은 네트워크를 이용하여 배포한 후 누군가에 의해 데이터의 내용이 변경되었는가를 검증할 수 있는 것으로 데이터의 진위(authenticity)를 확인하는 데 응용될 수 있다[5,6,7,8]. 일반적으로 연성 워터마킹은 암호학적 해쉬값(cryptographic hash value)이나 랜덤 비트와 같은 검증 데이터를 멀티미디어 데이터 내에 삽입한 후에 멀티미디어 데이터의 변조를 확인하게 된다. 이러한 연성 워터마킹 기술을 세분하면 완전 연성 워터마킹(complete fragile watermarking)과 준 연성 워터마킹(semi-fragile watermarking)으로 분류할 수 있다. 완전 연성 워터마킹은 변조된 멀티미디어 데이터에 대해서는 완벽하게 변조를 확인해야 하는 반면, 준 연성 워터마킹은 특정한 처리를 허용하는 것으로 예를 들어 영상에 대한 JPEG 압축과 같은 처리는 어느 정도 사용자가 이용할 수 있도록 허용되어야 한다. 즉, 준 연성 워터마킹은 특정 처리에 대해서는 강성 워터마킹과 같은 견고성(robustness)을 필요조건으로 한다.

본 논문에서는 영상의 비트 플레인을 워터마크를 삽입하기 위한 정보로써 이용하는 연성 워터마킹 기법을 제안하며, 그 구성은 다음과 같다. 먼저, 연성 워터마킹에 관한 개념 및 기존의 방법들을 2장에서 살펴보고, 3장에서는 제안방식에 의한 워터마크 삽입 및 변조의 확인 방법에 대해 기술한다. 4장에서는 시뮬레이션을 통하여 제안 방식에 대한 효율성을 확인하고, 마지막으로 5장에서는 결론과 향후의 과제에 대하여 기술한다.

Ⅱ. 연성 워터마킹 기술

디지털 영상을 대상으로 하는 연성 워터마킹은 데이터를 조작함으로써 데이터의 진위를 의심하게 하거나 제3자를 모함할 수 있다는 점에서 그 중요성을 논의할 수 있다. 연성 워터마킹의 필요조건은

1) 작은 영역에 대한 처리에도 데이터의 변조를 검출 가능해야 한다.
2) 영상에서 변조된 위치를 지정할 수 있어야 한다.
3) 원 영상 데이터 I와 워터마크 W에 대해서 워터마크가 삽입된 영상 I'로부터 I에 대한 정보 없이도 워터마크의 추출이 가능하여야 한다.
4) 워터마크는 비가시적이어야 한다.

여기서 1)과 2)의 조건은 연성 워터마킹의 특징이며, 이러한 필요조건에 준 연성 워터마킹에 적용하기 위해서는 특정 처리에 대한 견고성이 추가되기도 한다.

지금까지 제안되어 있는 연성 워터마킹 중에서 Wolfgang 등에 의해 제안된 방법[5]은 의사 랜덤 이진 계열인 M-계열의 워터마크 W를 삽입하기 위해 블록 b에

$$Y(b) = X(b) + W(b) \tag{1}$$

와 같이 삽입한다. 워터마크 삽입 영상 Y로부터 변조 여부를 확인하기 위해서

$$\delta(b) = Y(b) \cdot W(b) - Z(b) \cdot W(b) \tag{2}$$

와 같이 계산한다. 이때, Z는 Y로부터 변조된 가능성이 있는 영상으로, 주어진 임계값 T에 대해 $\delta > T$인 경우 영상 Z는 변조되었다고 판단하게 된다. 이 방법에서는 변조 여부를 확인할 때 원 영상이 요구되지 않지만, 식 (2)에서 알 수 있는 바와 같이 원래의 워터마크가 삽입된 영상 Y가 필요하게 되며, 이것은 변조확인 시에 원 영상이 요구되는 것과 동일하다. 이 방법 외에도 블록의 해쉬(hash) 값을 이용하여 변조 여부를 판단하는 BBHF (block-based hash function) 기법[5]은 블록의 해쉬 값을 계산하여 저장한 다음에 변조의 여부를 확인할 때 영상으로부터 블록에 대한 해쉬 값을 재계산하고 저장된 해쉬 값과 비교하여 변조 여부를 판단하게 된다. 그러나, 이 방법은 블록의 해쉬 값을 저장하고 있어야 하는 결점이 있다.

Kundur에 의한 제안 방법[8]은 L-레벨의 이산 웨이블렛 분해(discrete wavelet decomposition)을 이용하여 워터마크를 삽입한다. 길이 N인 이진 워터마크 $w(i)$, $i=1, \cdots, N$는 키 $ckey(i)$에 의해 랜덤하게 선택된 웨이블렛 계수 $f_{k,l}$에 다음과 같이 삽입되어진다.

1) $Q(f_{k,l}(m,n)) = w(i)$이면, 계수 값은 변경되지 않는다.
2) $Q(f_{k,l}(m,n)) \neq w(i)$이면, 계수 값은 아래와 같이 양자화된다.

$$f_{k,l}'(m,n) = \begin{cases} f_{k,l}(m,n) + \triangle, \text{ if } f_{k,l}(m,n) \leq 0 \\ f_{k,l}(m,n) - \triangle, \text{ if } f_{k,l}(m,n) > 0 \end{cases} \tag{3}$$

이때, 함수 Q는 다음과 같이 정의된다.

$$Q(f)=\begin{cases} 0, \text{if } r\triangle \le f < (r+1)\triangle \text{ for } r=0,\pm2,\pm4,\cdots \\ 1, \text{if } r\triangle \le f < (r+1)\triangle \text{ for } r=\pm1,\pm3,\pm5,\cdots \end{cases} \quad (4)$$

여기서 수식에서의 k와 l은 웨이블렛 변환에서의 수직 및 수평 부분, (m,n)은 각 부분에서의 위치를 의미한다. 새롭게 변경된 웨이블렛 계수 $f'_{k,l}$를 역 웨이블렛 변환을 수행함으로써 워터마크가 삽입된 영상을 얻게 된다.

영상의 변조를 검출하기 위해서는 먼저 웨이블렛 계수 값으로부터 식(4)의 함수 Q의 조건에 따라 $\varpi(i)$를 추출한다. 변조 여부는 원래의 워터마크와 추출된 워터마크로부터 다음과 같이 변조 평가 함수(tamper assessment function, TAF)를 이용한다.

$$TAF(w,\varpi)=\frac{1}{N}\sum_{i=1}^{N} w(i)\oplus\varpi(i), \quad \oplus:\text{XOR} \quad (5)$$

이때 변조 평가 함수의 값과 임계값 T를 비교하여, 만일 $0\le T\le 1$에 대해서 $TAF(w,\varpi)\ge T$이면 변조되었다고 판단하게 된다. 즉, Kundur의 방법은 양자화 단위 $\triangle$를 이용하여 계수 값을 양자화하는 방법으로, 실제 양자화 단위인 $\triangle$보다 작은 $\triangle'$를 이용하여 영상을 변조하는 경우에는 변조 여부를 확인할 수 없는 가능성이 있다.

따라서, 원 영상 혹은 원래의 워터마크가 삽입된 영상을 요구하지 않으면서 양자화 방법을 기반으로 하지 않는 방법을 본 논문에서 제안한다. 제안 방식은 비트 플레인 정보를 이용하여 대역확산 기반 워터마킹으로 워터마크를 삽입하여 영상의 변조/위조 여부를 확인하는 연성 워터마킹으로 다음 장에서 기술한다.

Ⅲ. 비트 플레인을 이용한 대역확산 기반 워터마킹

3.1 워터마크의 삽입

영상은 비트 플레인들의 비트 값의 조합으로 구성되어진다. 따라서, 영상의 변조는 결국 비트 플레인을 구성하는 비트 값들의 변화를 의미한다. 제안방식은 영상을 블록으로 분할하여 워터마크 비트를 삽입하는 것으로, 그림 1은 하나의 블록에 대한 워터마크 한 비트의 삽입 과정

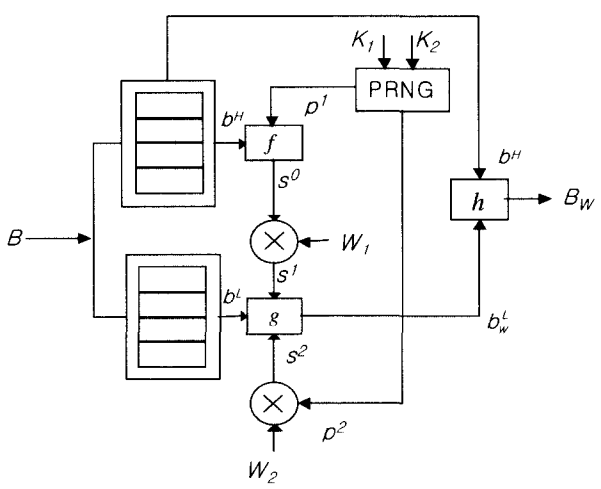


그림 1. 워터마킹 과정
Fig. 1. Watermarking Procedure

을 나타내고 있다.

워터마크를 삽입하기 위해 먼저, 크기 $N\times M$이고 256 레벨 그레이 영상 I를 크기 m인 n개의 블록 B로 분할한다. 하나의 블록 B에 대하여 1차원 배열로 $B=(b_1,\cdots,b_m)$, $0\le b_j\le 255$로 나타낼 때, 블록 B를 구성하는 i번째 비트 플레인을 $b^i=(b_1^i,\cdots,b_m^i)$, $b_j^i=\{0,1\}, 1\le j\le m$, $1\le i\le 8$로 표기한다. 여기서 i는 비트 플레인, j는 1차원 배열에서의 위치를 나타내는 기호이다. 또한, 상위 비트 플레인의 집합은 $b^H=\{b^i \mid i=8,7,6,5\}$, 하위 비트 플레인의 집합은 $b^L=\{b^i \mid i=4,3,2,1\}$로 나타낸다.

제안 방식은 영상의 변조를 확인하기 위해 이중 워터마킹을 수행한다. 첫 번째 워터마크 W_1은 상위 비트 플레인에 발생된 변화를, 두 번째 워터마크 W_2는 하위 비트 플레인에 발생된 변화를 확인하기 위해 이용된다. 길이 n인 워터마크 $W_1=(w_1^1,\cdots,w_1^n)$ 중 k번째 블록에 삽입되는 워터마크 비트 $w_1^k=\{-1,1\}$, $1\le k\le n$에 대하여 상위 비트 플레인으로부터 계열 s^0를 구하게 된다. 계열 s^0는 K_1을 키로 하는 이진 의사랜덤 계열(binary pseudorandom sequence) p^1을 이용하여 그림 2와 같은 함수 f에 의해

$$s^0=f(b^H,p^1)=(s_1^0,\cdots s_m^0) \quad (6)$$

와 같이 계산된다.

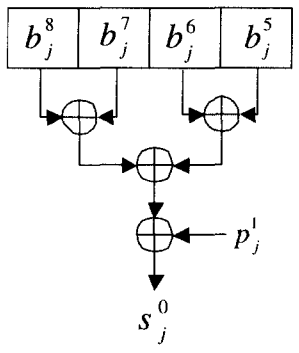


그림 2. 함수 $f(\oplus$: XOR)
Fig. 2. Function $f(\oplus$: XOR)

이때, $s_j^0=\{0,1\}$의 값은 워터마크 삽입을 위해 0과 1은 각각 -1과 1로 대응시키고, 계열 s^0와 워터마크 한 비트 w_1^k를 다음과 같이 계산한다.

$$s^1=w_1^k\cdot s^0=(w_1^k\cdot s_1^k,\cdots w_1^k\cdot s_m^0) \tag{7}$$

워터마크 $W_2=(w_2^1,\cdots,w_2^n)$는 K_2를 키로 하는 이진 의사랜덤 계열 p^2를 이용하여 식(7)과 동일하게 k번째 블록에 워터마크 한 비트 w_2^k를 계산한다.

$$s^2=w_2^k\cdot p^2 \tag{8}$$

이와 같이 계산된 s^1과 s^2를

$$b_W^L=g(b^L,s^1,s^2)=(\tilde{b}^L+s^1+s^2) \tag{9}$$

와 같이 계산한다. 이때 하위 2비트만으로 이루어진 값에 가산하며 이것은 큰 값에 의한 영향을 최소화하기 위한 것이다. 식(9)와 같이 워터마크가 삽입된 하위 비트값 b_W^L은 0과 15의 범위를 넘지 않도록 음수의 값이 되는 경우는 0으로, 16이상의 값이 되는 경우는 15로 설정한다. 이 결과를 다음과 같이 b_W^L와 상위 비트 플레인 b^H를 결합한다.

$$b_w=h(b^H,b_W^L)=(b^H\| b_W^L) \tag{10}$$

여기서 기호 $\|$는 두 요소간의 연접(concatenation)을 의미한다. 최종적으로 b_W를 2차원 배열로 재구성하면 워터마크가 삽입된 블록 B_W를 얻게 된다. 전체 블록에 대하여 이 과정을 수행하면 영상에 워터마크가 삽입되어진다.

위의 과정에 나타난 바와 같이 각각의 워터마크를 삽입할 때 비트 플레인의 정보를 이용하기 때문에 어떤 처리에 의해 상위 비트가 변경이 되면 실제 삽입시 이용된 계열과 다르기 때문에 정확한 워터마크 추출이 가능하지 않게 된다.

3.2 변조의 확인

연성 워터마킹에 있어서 변조 여부의 확인은 삽입된 워터마크를 추출하여 원 워터마크와 비교하여 서로 다른 값을 가진 경우에 변조 여부를 확인할 수 있다. 따라서, 먼저 삽입된 워터마크를 추출하여야 한다. 워터마크 추출은 대역확산 기반 워터마킹과 동일하게 워터마크와 워터마크가 삽입된 블록 간의 상관을 이용하여 워터마크를 검출하게 된다. 대역확산 기반 워터마킹은 원 영상 없이 워터마크 추출이 가능한 방법으로 많은 워터마킹 기법들이 이러한 대역확산 기법을 기반으로 하고 있다[9,10]. 그림 3은 하나의 블록에 대하여 한 비트의 워터마크 추출 과정을 나타낸 블록도이다.

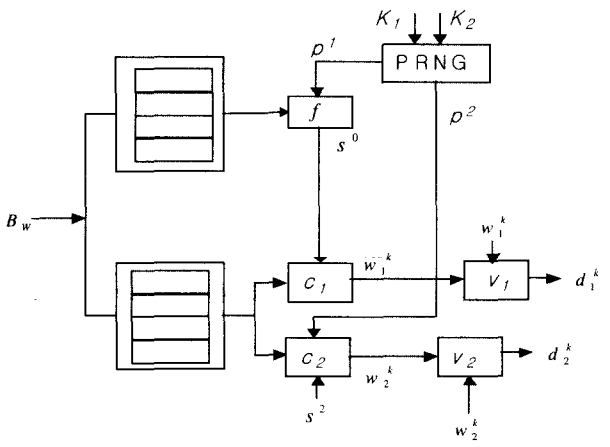


그림 3. 워터마크 추출 및 변조 확인
Fig. 3. Watermark Extraction and Verification of Modification

워터마크를 추출하기 위해 삽입 시와 마찬가지로 영상을 블록으로 분할하고 각각을 $\overline{b}^H$와 $\overline{b}^L$로 분리한다. 워터마크 W_1을 추출하기 위해 삽입 시와 동일한 함수 f를 이용한다. 키 K_1에 의해 생성된 계열 p^1와 상위 비트 플레인 $\overline{b}^H$로부터

$$\bar{s}^0 = f(\bar{b}^H, p^1) \tag{11}$$

를 계산한다. 그림 3에서 함수 c_1은 $\bar{s}^0$와 $\bar{b}^L$을 입력으로 하여 상관을 계산하고 블록에 삽입된 비트를 추출하는 함수로 그림 4의 과정에 의해 k번째 블록의 $\bar{b}^L$에 삽입된 워터마크 한 비트 $\bar{w}_1^k$를 추출한다.

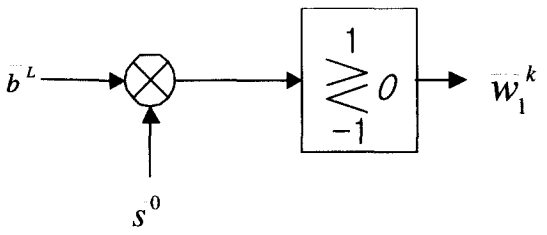


그림 4. 함수 c_1
Fig. 4. Function c_1

그림 4에서 기호 ⊗는 상관 계산을 의미하는 것으로, $\bar{w}_1^k$의 추출을 위해 $\bar{b}^L$에

$$\begin{aligned} r_1 &= \langle \bar{b}^L, \bar{s}^0 \rangle \\ &= \langle b^L + s^1 + s^2, \bar{s}^0 \rangle \\ &= \langle b^L, \bar{s}^0 \rangle + \langle s^1, \bar{s}^0 \rangle + \langle s^2, \bar{s}^0 \rangle \end{aligned} \tag{12}$$

와 같은 계산을 수행한다. 식(12)의 두 번째 항은

$$\langle s^1, \bar{s}^0 \rangle = \langle w_1^k s^0, \bar{s}^0 \rangle \tag{13}$$

이므로 만일 상위 비트 플레인의 값들이 변하지 않았을 경우, 즉 $s^o = \bar{s}^0$이면 식 (13)의 값은 $w_1^k \sum_{j=1}^{m} (s_j^0)^2 = w_1^k m$이 된다. 따라서, 나머지 항들이 0에 가까운 값이 된다고 가정하면, 식(12)로부터

$$w_1^k = \begin{cases} 1, \text{if } r_1 > 0 \\ -1, otherwise \end{cases} \tag{14}$$

와 같이 결정한다. 이러한 과정을 n개의 블록에 대하여 수행하면 워터마크 $\bar{W}_1$을 구성하게 된다.

영상의 변조 여부를 확인하기 위해 추출된 워터마크 $\bar{W}_1$의 값 1과 -1은 각각 1과 0으로 대응시키고, 원래의 워터마크 W_1(1과 -1을 1과 0으로 대응)과 비교하여 변조 평가 값 t_1을 다음 식으로 계산한다.

$$t_1 = \frac{1}{n} \sum_{k=1}^{n} d_1^k \tag{15}$$

여기서, d_1^k은 함수 v_1에 의해 $d_1^k = v_1(w_1^k, \bar{w}_1^k) = = w_1^k \oplus \bar{w}_1^k$으로 계산되며, ⊕은 XOR연산을 의미한다. 이때 변조 평가 값 $t_1 \neq 0$이면 변조의 발생 여부를 확인하게 되고, $d_1^k = 1$이 되는 부분들을 영상의 변조가 발생된 곳으로 지정한다.

워터마크 $\bar{W}_2$도 $\bar{b}^L$과 p^2를 입력으로 하여 위와 유사한 과정에 의해 추출한 t_2와 d_2를 계산하여 변조의 여부를 결정하고 변조의 위치를 지정하게 된다.

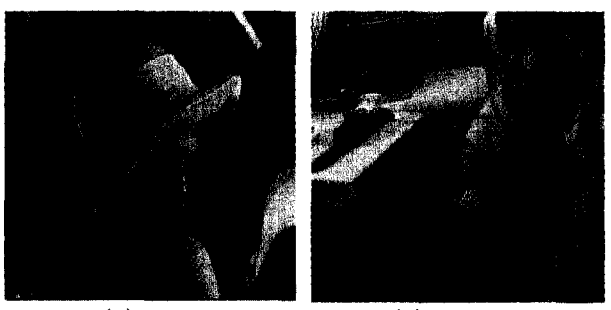
IV. 시뮬레이션 및 결과

4.1 실험 내용

제안 방식의 유효성을 측정하기 위해 Lena, Barbara (256×256, 8bits/pixel)의 그레이 영상을 이용하여 다음과 같이 실험하였다. 8×8블록으로 영상을 분할하여 총 1024개의 블록에 워터마크를 삽입하였다($m=64$, $n=1024$). 이때, 워터마크는 하위 비트들을 변경시켜 삽입되기 때문에 그림 5와 같이 시각적으로 워터마크의 삽입에 의해 영상의 화질은 저하되지 않음을 알 수 있다.

그림 5의 워터마크 삽입 영상에 대하여 어떤 처리도 하지 않은 경우에 제안 방식에 의해 변조 여부를 확인한 결과, 명확하게 변조가 되지 않았음을 확인하였다.

영상을 변경함에 있어서 크게 2가지의 형태로 수행될 수 있다. 첫 번째 방식은 영상의 컨텐츠는 그대로 유지하면서 변경시키는 것으로 압축이나 화질 향상을 위한 처리



(a) Lena (b) Barbara

그림 5. 워터마크 삽입 영상
Fig. 5. Watermarked Image

등을 예로 들 수 있다. 다른 하나는 영상 내의 컨텐츠를 제거하거나 추가함으로써 영상을 실질적으로 위조하는 것으로 이것은 영상이 전달하고자 하는 정보가 변경되는 경우이다.

표 1은 워터마크를 삽입한 후 품질 계수(quality factor) q를 75, 50, 25로 JPEG 압축을 수행한 후 영상의 변조 여부를 확인한 결과이며, 표 2는 영상의 밝기를 조절한 후 영상의 변조 여부를 확인한 것이다. 표1과 표2에서 t_1, t_2는 각각 식(15)에 의해 계산된 2개의 워터마크에 대한 변조 평가 값으로 모두 0이상의 값을 가지고 있다. 검출률은 상위 비트 플레인과 하위 비트 플레인에서의 변조 검출수를 전체 블록 수로 나눈 것이다.

표 1. 품질 계수 q에 따른 t_1, t_2의 값

Table 1. Value of t_1, t_2 according to quality factor q

영상 \ q		75	50	25
Lena	t_1	0.4082	0.4746	0.4844
	t_2	0.4746	0.5039	0.5107
	검출률	0.6865	0.7422	0.7480
Barbara	t_1	0.4141	0.4756	0.5166
	t_2	0.4854	0.4971	0.4980
	검출률	0.7070	0.7441	0.7441

표 1의 결과를 보면, 품질 계수가 작을수록 영상에 대한 변조가 많이 일어나므로 t_1, t_2의 값은 전반적으로 증가하고 있음을 알 수 있다.

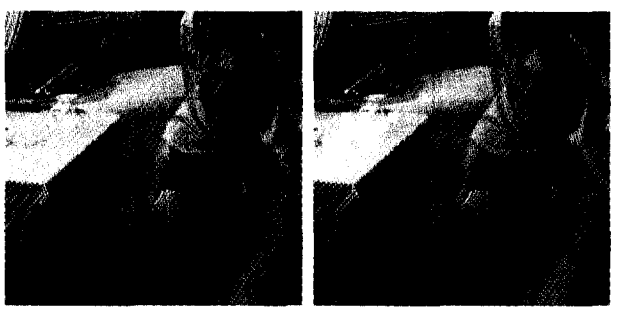
표 2. 영상의 밝기 조절에 따른 t_1, t_2의 값

Table 2. Value of t_1, t_2 according to brightness adjustment

영상 \ β		0.1	0.3	-0.1	-0.3
Lena	t_1	0.4316	0.7471	0.2959	0.4121
	t_2	0.2705	0.3203	0.7305	0.5820
	검출률	0.4775	0.8878	0.8213	0.7666
Barbara	t_1	0.4268	0.7227	0.2217	0.4150
	t_2	0.2090	0.3320	0.7451	0.6162
	검출률	0.4619	0.8438	0.8174	0.8115

표 2에서 β는 밝기를 조절하는 파라메터로 $0 \le \beta \le 1$인 경우에는 영상이 밝아지고, $-1.0 \le \beta < 0$인 경우에는 영상이 어두워진다. 영상의 밝기를 밝게 하거나 어둡게 할수록 t_1과 t_2의 값이 증가함을 알 수 있다.

이러한 영상 전체를 변경시키는 것 이외에 영상의 일부분을 조작하는 두 번째 경우에 대한 실험으로 그림 6과 같이 Barbara 영상에서 테이블 위의 물건을 제거하는 조작을 수행하였다. 이것은 그래픽 편집 툴의 복사 브러쉬 기능을 이용하면 손쉽게 조작이 가능하다. 이 영상에 대해서 제안 방식에 의해 변조 확인 및 위치를 지정하면 그림 6(b)와 같은 결과를 얻을 수 있었다.



(a) modified image (b) location of modification

그림 6. 영상의 위조 및 위치

Fig. 6. Forgery of image and location

그림 6(b)에서 백색부분이 변조가 이루어져 있음을 나타내는 것으로 변조 위치를 대부분 명확하게 지정하고 있다.

변조 여부를 판단함에 있어서 2개의 오류가 발생한다. 첫번째 오류는 변조가 일어나지 않았으나 변조가 있다고 판단하는 경우로 이것은 검출기의 비트 에러 확률과 같다. 즉, 식(12)의 값은 다음과 같이 표시할 수 있다.

$$r_1 = \underbrace{< b^L, s^0 > + < s^2, s^0 >}_{\sum_1} + \underbrace{< s^1, s^0 >}_{\sum_2} \tag{16}$$

이때, 비트 에러 확률은

$$\begin{aligned} BER_1 &= \Pr(\textstyle\sum_1 > m \\ &= \frac{1}{\sqrt{2\pi}\sigma_{\sum_1}} \int_n^{\infty} \exp\left(\frac{-t^2}{2\sigma^2_{\sum_1}}\right) dt \\ &= \frac{1}{2}\, erfc\left(\frac{m}{\sqrt{2}\sigma_{\sum_1}}\right) \end{aligned} \tag{17}$$

가 된다. 단, $\sigma_{\sum 1} = \sigma_{s^0}\sqrt{\sigma^2_{b^L} + \mu^2_{b^L} + \sigma^2_{s^2} + \mu^2_{s^2}}$이다.

두 번째의 오류는 변조가 발생하였으나 변조를 판단

하지 못하는 경우로 연성 워터마킹에서는 이 확률이 가능한 최소가 되어야 한다. 변조 δ에 의해 식 (16)과 같은 형태로 다음과 같이 계산된다.

$$r_1' = \underbrace{<\bar{b}^L, s^0>}_{r_1} + \underbrace{<\delta, s^0>}_{\sum_2} \tag{18}$$

이때, δ에 의해 변조가 발생하였으나 변조를 판단하지 못할 확률은 변조를 판단할 확률로부터 계산한다. 즉, 삽입된 워터마크가 $w=1$일 때, 식 (18)의 결과가 $r_1' = m + \sum_2 < 0$으로 되거나 $w=0$일 때, $r_1' = -m + \sum_2 > 0$이 될 때, 변조를 확인할 수 있다. 이것은 $w=1$일 때 발생되는 비트 에러 확률과 같으므로

$$\begin{aligned} BER_2 &= \Pr(\sum_2 > m) \\ &= 1/\sqrt{2\pi}\sigma_{\sum 2} \int_m^{\infty} \exp\left(\frac{-t^2}{2\sigma^2_{\sum_2}}\right)^{dt} \\ &= \frac{1}{2} erfc\left(\frac{m}{\sqrt{2}\sigma_{s^0}\sqrt{\sigma_\delta + \mu_\delta}}\right) \end{aligned} \tag{19}$$

가 된다. 따라서, 식 (19)로부터 변조를 확인하지 못할 확률은

$$BER_3 = 1 - BER_2 \tag{20}$$

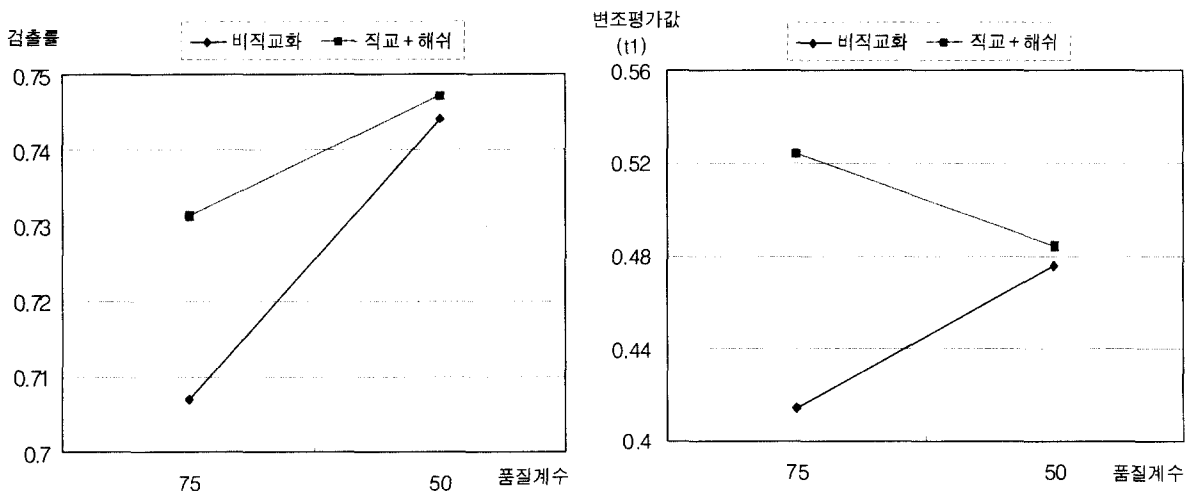
가 된다.

4.2 실험 결과 고찰

실험결과 본 논문에서 제안한 방식의 경우 2가지의 문제점이 야기될 수 있음을 확인하였다. 첫 번째, 제안 방식에서의 문제점은 함수 f의 구조이다. 함수 f는 그림 3과 같이 비트 s_j^0를 구성하기 위해 상위 4비트에 대하여 XOR 연산을 수행한다. 이때, 4개의 상위 비트에서 2개의 비트 값이 동시에 변경되는 경우에는 상위 비트가 변경됨에도 불구하고 s_j^0의 값은 변경되지 않기 때문에 변조의 여부를 확인할 수 없게 된다. 이 문제를 해결하기 위한 방법으로 암호학적 해쉬 함수를 이용하여 함수 f를 설계함으로써 상위 비트 플레인에서 한 비트가 변경되어도 전체 s^0가 변경될 수 있도록 할 수 있을 것이다.

두 번째 문제로써 하위 비트 값에 2개의 워터마크를 삽입하기 때문에 추출시 워터마크 간의 간섭이 발생될 수 있다. 이것은 워터마크 간의 간섭이 최소가 되도록 직교성(orthogonality)을 갖는 2개의 워터마크를 이용해야 한다.

암호학적 해쉬 방법 중 하나인 MD5 방식[11]과 Gram-Schmidt 직교화 방식[12]를 이용하여 해쉬 및 직교성을 적용한 결과와 표 1에서 영상 Barbara와의 검출률을 비교한 결과를 그림 7에 나타내었다. 여기서, 해쉬 함수를 이용하는 경우에는 한 블록의 상위 비트 플레인들을 입력으로 하여 MD5를 수행하면 128비트가 출력되어 이 중에서 64비트만을 이용하였다. 또한 해쉬 함수를 적용한 결과와 두번째 워터마크를 직교화하였다. 그림 7(a)는 워터마



(a) 직교화 (b) 직교화 및 해쉬 함수

그림 7. 직교화 및 해쉬 함수의 이용

Fig. 7. Use of orthogonalization and Hash function

크간의 직교성을 제공하여 변조를 검출한 결과를 표 1에서 영상 Barbara와의 검출률과 비교한 것이며, 그림 7(b)는 직교성과 해쉬 함수를 동시에 이용하여 상위 비트에 대한 변조 평가 값 t_1을 각각 나타낸 것으로 검출률이 증가됨을 알 수 있다.

V. 결 론

연성 워터마킹은 데이터의 변조/위조를 확인하고 그 위치를 지정할 수 있는 것으로 데이터의 인증/무결성을 신뢰하기 위한 수단으로 이용할 수 있다. 연성 워터마킹은 약한 워터마크를 설계하여 약간의 처리에 대해서도 워터마크가 손상되거나 제거되도록 설계되어야 한다. 본 논문에서는 영상의 가장 최소 단위인 비트들의 집합, 즉 비트 플레인 정보를 이용하여 연성 워터마킹을 수행하는 방법을 제안하였다. 제안 방식은 공간 영역(spatial domain) 기반으로 DCT, 웨이블렛과 같은 복잡한 변환을 이용하지 않기 때문에 고속 수행이 가능한 장점이 있다. 그러나, 결과고찰에서 논의한 바와 같이 몇 가지의 문제점이 제기될 수 있기 때문에 실용적인 면에서 JPEG 압축과 같은 특정 처리를 허용하는 준 연성 워터마킹에 적용 가능해야 한다. 따라서, 향후에는 준 연성 워터마킹의 적용, 검출기의 오류(false alarm)에 의한 성능 분석 및 다양한 공격에 대한 연구가 필요하다.

참 고 논 문

[1] S. Katzenbeisser and F. A. P. Petitcolas etd., *Information Hiding : Techniques for Steganography and Digital Watermarking, ARTECH HOUSE*, pp.95-208, 2000

[2] I. J. Cox, J. K. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, 1997

[3] I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Model," *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, pp. 540-550, 1998

[4] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proc. of the IEEE*, Vol. 87, No. 7, pp. 1079-1107, 1999

[5] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark," *Security and Watermarking of Multimedia Contents, Proc. of SPIE*, Vol. 3657, pp. 204-213, 1999

[6] M. Wu and B. Liu, "Watermarking for Image Authentication," *Proc. of ICIP*, pp. 437-441, 1998

[7] L. Xie and G. R. Arce, "Joint Wavelet Compression and Authentication Watermarking," *Proc. of ICIP*, pp. 427-431, 1998

[8] D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," *Proc. of the IEEE*, vol. 87, No. 7, pp. 1167-1180, 1999

[9] J. R. Hernandez, M. Amado and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," *IEEE Trans. on Image Processing*, Vol. 9, No. 1, pp. 55-67, 2000

[10] M. Kutter, Digital Image Watermarking: Hiding Information in Images, Ph.D. Thesis, University of Rhode Island, USA, 1999

[11] A. J. Menezes, P. G., Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography, CRC Press*, pp. 321-382, 1997

[12] 오윤희, 이혜주, 박지환, "Gram-Schmidt 직교화를 이용한 다중 워터마킹 기법," *정보처리학회 추계학술발표대회 논문집, 제7권 2호*, pp. 153-156, 2000

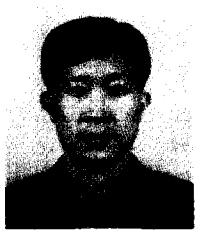
저 자 소 개

이 혜 주

1990년 3월~1994년 2월 : 부경대학교 전자계산학과 졸업 (이학사)
1994년 3월~1997년 2월 : 부경대학교 대학원 전자계산학과 졸업 (이학석사)
1997년 3월~2000년 2월 : 부경대학교 대학원 전자계산학과 졸업 (이학박사)
2000년 6월~2001년 2월 : 한국정보통신대학원대학교 박사후연구과정생
2001년 3월~현재 : 한국전자통신연구원 선임연구원(음향기술팀)
주관심분야 : 디지털 컨텐츠 보호, 디지털 워터마킹, 영상압축, 정보보호

홍 진 우

1978년 3월~1982년 2월 : 광운대학교 응용전자공학과 졸업 (공학사)
1982년 3월~1984년 2월 : 광운대학교 대학원 전자공학과 졸업 (공학석사)
1990년 3월~1993년 8월 : 광운대학교 대학원 전자계산기공학과 졸업 (공학박사)
1998년~1999년 : 독일 프라운호퍼연구소 (교환연구원)
1984년 3월~현재 : 한국전자통신연구원 음향기술연구팀장 (책임연구원)
2000년 1월~현재 : 한국음향학회 홍보이사, 뉴미디어음향 학술분과위원장, 한국방송공학회 편집위원
1993년 1월~현재 : 정보통신표준화연구단 방송기술위원회 위원
주관심분야 : 오디오 신호처리 및 부호화, 디지털 컨텐츠 보호 및 관리, 디지털 오디오 방송



김 진 웅

1981년 2월 : 서울대학교 공과대학 전자공학과 졸업 (학사)
1983년 2월 : 서울대학교 대학원 전자공학과 졸업 (석사)
1993년 8월 : Texas A&M Univ. 전기전자공학과 졸업 (박사)
1983년 3월~현재 : 한국전자통신연구원 책임연구원/방송미디어연구부장,
스웨덴 LM Ericsson사 방문연구원, 한국방송공학회 학술분과위원,
SK Telecommunications Review지 편집위원, MPEG 국제표준화회의 한국대표,
IWAIT 2001 국제 워크샵 Program Chair
주관심분야 : 디지털 VLSI 신호처리, 영상 압축, 영상 통신, 멀티미디어 데이터 방송, MPEG-4/7, 컨텐츠 보호