

영상압축에 강인한 변질검증 워터마킹에 관한 연구

정희원 안성철*, 이경학**, 박화범**, 고희화**

A Study on Semi-Fragile Watermarking for Robust Authentication on Image Compression

Sung-cheol Ahn*, Kyoung-hak Lee**, Hwa-bum Park**, Hyung-hwa Ko** *Regular Members*

요 약

소프트웨어의 발전으로 인해 디지털 콘텐츠에 대한 복사, 변경이 손쉽게 일반인들에 의해서도 가능하게 되어 콘텐츠의 제작자는 소유권 주장이나 내용의 변질에 대한 인증과 검증을 필요로 하게 되었다. 변질검증(Fragile) 워터마킹 기법은 워터마크가 삽입된 영상의 변질 및 훼손 여부를 판별할 수 있지만, 고의적이지 않은 표준화된 영상압축 등에서도 워터마크가 사라지는 문제점이 있다. 본 논문에서 JPEG 압축과 같은 영상처리에서는 강인하지만 변질에는 약한 Semi-Fragile 워터마킹 방법을 제안하였다. 제안한 방법은 블록간의 상관관계를 이용하여 워터마크를 생성하고, DCT(Discrete Cosine Transform)수행 후에 계수 값들의 양자화를 이용하여 HVS(Human Visual System)에 둔감한 부분의 계수 값에 삽입하는 방법을 제안하였다. 실험결과 공간영역 상에서 미세한 변화에도 변질여부의 검출 정도가 뛰어났으며, 변질된 부분을 블록별로 검출할 수 있어 공간상의 어떤 위치의 픽셀들이 변화하였는지를 시각적으로 확인할 수 있었다.

Key Words : Watermarking, DCT, Semi-fragile, Block-reordering, JPEG

ABSTRACT

The rapid progress of the software has enabled individuals to copy and remark digital contents, which was only done by professionals. As a solution for the problems, contents producer needs to have certification and inspection of its contents and hold the proprietary right. A fragile watermarking method is able to detect the distortion and damage of watermarked image, but the watermark is also fragile on standardized image compression. That is the problem of fragile watermarking technique. We propose semi-fragile watermarking technique that is robust in the image processing such as JPEG compression used on computer, but it is fragile on the addition of noise and other attacks.

In the proposed method, we can generate the watermarks of an image from the relationship between two block coefficients, also the generated watermark is inserted into insensible part of HVS(Human Visual System) after processing DCT(Discrete Cosine Transform) and using quantization. As a result, on the spatial domain, high detection of distortion has been possible even in slight changes, and could detect the corrupted blocks on image. Therefore, it is simple to judge the pixels at which some location has been changed in the space.

1. 서론

오늘날 정보화 사회에서 멀티미디어 콘텐츠의

유통은 막대한 정보를 공유하고 있으며, 각 분야의 사용자가 공동으로 이용할 수 있게 되었다. 하지만 이러한 멀티미디어 콘텐츠들은 개인 창작의

* (주)디티브이인터랙티브(sungb612@dtvinteractive.com), ** 광운대학교 전자통신공학과 영상처리연구소(goldbug15@kw.ac.kr)
논문번호 : KICS2006-01-020, 접수일자 : 2006년 1월 20일, 최종게재논문통보일자 : 2006년 11월 15일

산물로 그 저작권을 보호받아야 하며, 콘텐츠의 변질여부가 판단되어야 하는 응용분야에서는 무결성이 검증되어야 한다. 지적재산권 보호를 위해 사용되는 방법은 디지털 미디어 자체에 접근을 통제하는 방화벽(Firewall)과 암호화 방식을 사용하여 키를 소유한 사람만이 내용을 볼 수 있게 하는 방법이 있다[1]. 그러나 위의 방법은 일단 인증된 사용자에게 의해 접근되어 사용되고 난 후에는 어떠한 효력도 존재하지 않게 되며, 소유권의 주장이나 변질 검증이 필요한 용도에서는 효과적인 방법이 못된다. 디지털 저작물 소유권에 대한 인증과 불법적인 복제, 변조 등의 문제해결을 위한 방법으로 디지털 워터마킹(Digital Watermarking)방법이 있다^[2-3]. 디지털 워터마킹은 데이터 내부에 임의의 정보를 은닉시켜 저작물의 소유권과 무결성의 검증을 받을 수 있도록 하는 기술이다.

워터마킹 기법을 사용 목적에 따라 구분하면, 미세한 변질여부까지 검출할 수 있는 프래질 워터마킹(Fragile Watermarking)^[4-5]과 압축에 의한 변질은 검출하지 않는 세미 프래질(Semi-fragile) 워터마킹 [6-7]으로 나뉘어 질수 있다. 일반적으로 영상의 변질여부를 위한 방법에는 워터마크의 생성과 워터마크의 삽입, 검출 과정, 검출된 워터마크에 의한 변질 여부의 검증 과정으로 이루어진다. 영상의 변질여부는 추출된 워터마크와 원 워터마크간의 유사도를 비교하여 변질여부를 판단하는 것이 일반적인 방법이다.

워터마킹은 워터마크의 삽입·검출과정의 적용 영역에 따라 공간영역과 주파수영역에서의 워터마킹 방법의 두 분야로 구분된다[8]. 공간영역에서의 워터마킹은 영상의 특정위치에 직접 변화시켜 워터마크를 삽입하는 것으로 계산량이 비교적 적고 단순하지만 잡음에 강인하지 못하고, JPEG 등과 같은 영상압축에 적용하기 어려운 단점이 있다. 반면, 주파수 영역의 방법은 원영상에 DCT, DFT, DWT 등을 적용한 후 적당한 주파수 대역에 워터마크를 삽입하는 방법으로 추가적인 연산이 필요하지만 압축 및 잡음에서 비교적 견고한 특성을 갖는다.

본 논문에서는 DCT를 통하여 랜덤하게 재배열된 후의 주파수 영역에서 각 블록간의 상관관계를 이용하여 워터마크를 생성한다. 각 블록마다 생성된 워터마크에 의해서 대처 값이 결정되고 그 값에 의해서 양자화된 특정 계수에 삽입하는 방법을 제안하였다.

II. 디지털 워터마킹

2.1 사용 목적에 따른 디지털 워터마킹의 분류

2.1.1 소유권 주장

창작자의 디지털 미디어 콘텐츠에 대한 소유를 주장하기 위해서 창작자는 공개키나 비밀키를 사용하여 워터마크를 생성한 뒤 그것을 원본 콘텐츠에 삽입하고 워터마크가 삽입된 이미지를 공개한다. 다른 사람이 공개된 콘텐츠의 소유를 주장하면 창작자는 소유를 주장하는 다른 사람의 이미지에 자신이 삽입한 워터마크가 있음을 보여주면 되는 것이다. 이러한 방법은 이미지에 대한 압축, 확대, 축소 등을 수행해도 워터마크가 없어지지 않고 남아 있어야 한다.

2.1.2 영상의 변질 검증

멀티미디어 콘텐츠가 법 또는 의학적인 용도, 상업적인 용도로 사용되는 경우에 훼손되거나 수정되지 않았다는 것을 확인하는 것이다. 워터마킹 방법을 사용하면 콘텐츠에 대한 인증을 수행하는 부분이 콘텐츠에 포함이 되어 데이터를 처리하는 문제를 간단히 할 수 있게 된다. 이 방법은 영상의 변형에 대해서 확인 가능한 장치가 있어야 한다.

2.2 영상 변질 검증을 위한 워터마킹의 요구사항

2.2.1 비가시성(Invisibility)

워터마크를 삽입하였을 경우, 그 결과물이 시각적으로 인지되어서는 안 된다. 이것은 불법적인 사용자들에게 검출될 경우 워터마크에 대한 공격의 대상이 될 수도 있기 때문이다. 따라서 사람의 시각적으로 인지되지 않도록 워터마크를 삽입해야 한다.

2.2.2 변질된 부분의 지역화(Localization)

이미지의 어떤 부분이 정확히 변질되었는지를 시각적으로 명백하게 판단할 수 있는 방법이 필요하게 되며, 변환된 영역에서 변질된 부분이 블록별로 혹은 픽셀단위로 표시될 수 있어야 한다.

2.2.3 부가정보 불필요성(No additional information)

기존의 데이터 인증을 위한 암호화적인 방법은 데이터의 무결성을 판단하기 위해서 부가적인 정보의 추가 및 암호화 키 또한 필요하며, 이러한 단점을 보완하기 위해서 부가적 정보가 필요 없는 워터마킹 방법이 요구된다.

2.3 기존의 워터마킹 기법

2.3.1 공간영역에서의 디지털 워터마킹

신호 그 자체의 도메인에서 작업하는 것을 공간 영역에서의 디지털 워터마킹이라고 하며, 가장 간단한 방법은 LSB를 바꾸는 것인데[9-10] 매우 간단한 신호처리에 의해서도 손쉽게 손상되기 때문에, 강인성을 요구하는 경우에는 거의 사용되지 않고 있지만, 원본이 어떠한 형태로든 변형된 경우 워터마크를 검출할 수 없게 하는 인증의 목적으로 사용되는 워터마킹용으로 널리 사용되고 있다. 하지만 워터마킹 정보에 대한 통계적인 추측이 용이하고 압축이나 영상의 변형에도 비교적 약하여 주파수영역의 워터마킹 방법과 병행 사용되는 것이 일반적이다.

2.3.2 주파수영역에서의 디지털 워터마킹

워터마크의 삽입 및 추출을 변환 영역에서 하는 것을 말하는데, 단일 주파수 성분을 변화시킴으로써 변환 블록내의 밝기 값 전체에 영향을 미치고, 따라서 불법적인 공격에 강한 워터마크를 만들 수 있다. 영상 데이터를 주파수 형태로 변형했을 때 가질 수 있는 통신 채널이라고 가정한다면, 워터마크는 그 통신 채널로 통과하는 신호라고 볼 수 있다. 그 신호가 잡음, 필터링, 압축전송 등에 영향을 받지 않고 효과적으로 전송이 될 수 있도록 대역확산통신(Spread Spectrum)방식을 도입한다^[11]. 특정 주파수 대역의 에너지는 감지할 수 없을 정도로 작지만 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 분산되어 있는 주파수 성분을 모으면 높은 신호대 잡음비로 신호를 검출할 수 있다. 워터마크를 영상이 갖고 있는 여러 주파수영역으로 확산시킴으로써 특정 주파수 대역의 에너지를 감지하기 어렵게 한다. 영상의 변화를 감지 못하도록 하면서 시각적으로 중요한 영역에 정보를 삽입하는 알고리즘은 시각적 변형과 JPEG 압축, 그 외 영상 처리 기술에 대하여 장단점을 고려하여 삽입하고자 하는 주파수 영역을 선택하여 워터마크를 삽입한다. 이러한 방법들은 워터마크로 일반 영상을 사용하지 않고 정상 분포를 갖는 가우시안 잡음(Gaussian Noise)나, 의사 잡음(PN:Pseudo Noise)코드를 워터마크로 사용하는 방법이다.

2.3.3 기존 변질검증 워터마킹 방법

P.W.Wong[12]은 원본 영상을 8×8블록으로 분할하고 블록내 각 픽셀의 LSB를 떼어내고, 나머지

MSB(Most Significant Bit)와 영상의 크기정보, 사용자의 비밀키를 모두 해쉬함수의 입력으로 한다. 디지털 서명을 생성하고 이를 원본 영상의 LSB에 삽입함으로써 워터마킹된 이미지를 생성하는 것이다. 이 방법은 영상의 조작여부 및 블록단위의 조작 위치 확인이 가능하고 크기변화 등에 의한 영상의 변화검출이 가능하다, 일반적인 영상처리나 영상압축 등에서도 삽입된 워터마크가 사라지게 되는 문제점이 발생한다.

2.3.4 기존의 Semi-Fragile 워터마킹 방법

M. Wu^[13]가 제안한 방법은 사용자에게 의해 생성된 일련의 LUT(Look-Up Table)과 이진 영상 패턴으로 구성된 워터마크를 DCT 영역에 삽입하여 압축에 강인한 인증 알고리즘을 제안하였다. 이 방법은 블록간의 교환은 검출할 수 없고, 사용자에게 의해 정의된 LUT를 워터마크의 삽입과 추출할 때 부가적으로 공유하고 있어야 한다는 단점이 있다.

C.Y. Lin[14]은 영상의 DCT 블록간의 상관관계에 의해서 워터마크가 생성되고, 생성된 워터마크는 또 다른 이웃하지 않은 블록의 특정 계수 LSB에 삽입한다. 추출시 별도의 부가적인 정보가 필요하지 않고 다중 블록을 이용하기에 보안성이 유지된다. 그러나 자신만의 변형된 양자화를 사용하고 삽입되는 과정에서 연산이 복잡하다는 단점이 있다.

J. Fridrich^[15]은 두 개의 Invertible 워터마킹 방법을 제안했다. 양자화된 DCT 계수로부터 영상압축의 비트 스트림을 얻는 방법과 DCT 계수마다 적은 손실을 위해 1 bit의 삽입을 할 수 있게 양자화 테이블 값을 수정하는 방법으로 처리속도가 빠르지만, 압축할 때마다 새로운 인증코드를 삽입해야하고 변질위치를 검증할 수는 없다는 단점이 있다.

III. 제안한 Semi-Fragile 워터마킹 알고리즘

제안한 워터마킹 알고리즘은 원영상에 DCT를 수행하고, 블록의 재배열을 한 후 재배열된 각 블록 특징의 상관관계에 의해서 Feature code를 생성하며, Feature code와 사용자에게 의해 정의된 비밀키로 워터마크가 생성된다. DCT 영상의 재배열된 각 블록을 양자화한 후 특정 계수 값이 워터마크에 의해 특정한 위치의 인접한 대치 값으로 삽입하게 된다. 단, JPEG 압축정도에 따른 강인성과 비가시성을 최대화하기 위하여 양자화의 QF(Quality Factor)를 JPEG 압축률과 동일하게 사용한다. 즉, 워터마크

삽입시 사용한 QF에 따라 압축에 대한 강인성의 정도가 결정된다. 이렇게 워터마크가 삽입된 양자화 계수들을 역 양자화를 취하고 IDCT를 수행한 후 삽입할 때와 동일한 방법으로 영상을 재배열하여 워터마크가 삽입된 영상이 생성된다. 그림 1은 제안한 워터마킹 방법에 대한 기본적인 구성도이다.

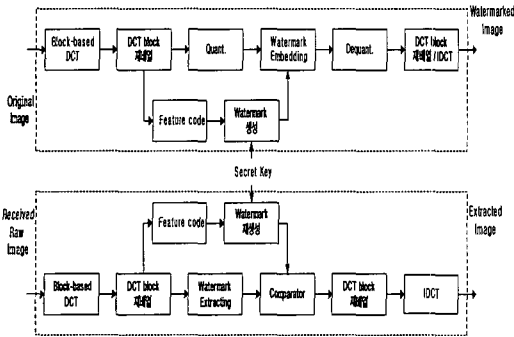


그림 1. 제안한 알고리즘 구조
Fig. 1. Structure of proposed algorithm.

3.1 워터마크 삽입 알고리즘

3.1.1 워터마크 생성

원영상에 삽입시킬 워터마크를 생성하기 위한 절차는 다음과 같다.

Step 1. 원영상을 8×8 DCT 변환

Step 2. 8×8 DCT블록을 랜덤하게 재배열(그림 2)

24×24 블록으로 매크로 블록을 형성

Step 3. 매크로 블록 내에서의 블록 순서에 따른 각 블록의 DC값 비교하여 Feature code 생성 (그림 3)

$$F = \begin{cases} 1, & X_i(0,0) - X_{i+1}(0,0) \geq 0 \\ 0, & X_i(0,0) - X_{i+1}(0,0) < 0 \end{cases} \quad (3.1)$$

$X(u,v)$: DCT 계수, $i = \{0, 1, \dots, 8\}$

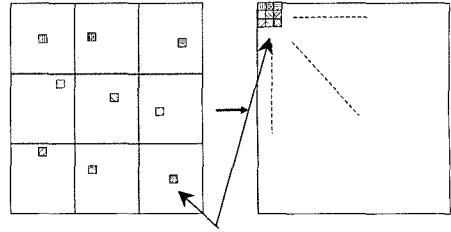
Step 4. 비밀키에 의해 의사난수 발생

Step 5. Feature code와 step 4에서 생성된 의사난수의 XOR (Exclusive OR)로 워터마크 생성

$$\text{Watermark} = F \text{ code} \oplus S \text{ code} \quad (3.2)$$

Where, S code : 의사난수

그림 2는 Step 2의 과정에서 DCT 수행 후 비밀키에 의해 랜덤하게 재배열을 하고, 9개의 블록 단위를 하나의 매크로 블록으로 형성한다.



8×8 DCT 블록

그림 2. 블록 재배열
Fig. 2. Block reordering.

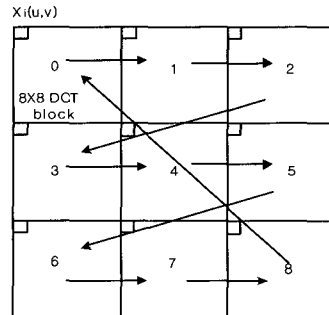


그림 3. Feature code 생성과정
Fig. 3. Feature code generation process

그림 3은 워터마크를 생성하기 전처리 과정으로 각 블록간의 상관관계에 의해 Feature code가 생성되는 과정을 나타낸다

3.1.2 워터마크 삽입

본 논문에서는 DCT계수의 의해서 구해진 워터마크로 인접한 특정 계수가 결정이 되고, 결정된 계수의 부분 양자화를 통하여 워터마크를 삽입한다. 그리고 양자화 부분의 변형 민감도를 이용하여 변질을 검출하는 방법으로 원영상을 양자화한 후 워터마크가 삽입될 계수에 3.1.1절에 의해 구해진 워터마크에 따라 인접한 특정 계수값이 삽입된다. 특정 계수 값은 변질을 검출 시 변형 민감도를 위하여 유사한 양자화 테이블 값을 갖는 계수를 선택한다.

워터마크를 삽입하는 과정은 다음과 같다.

Step 1. 워터마크 삽입 계수와 인접한 특정 계수의 부분 양자화 (그림 4)

Step 2. 인접한 특정 계수 값이 '0'의 값을 갖는지 확인하고 '0'일 경우 양자화하기 전의 부호 비트 (Sign Bits)를 확인하여 '1' 또는 '-1'을 더한다.

$$X'(u,v) = \begin{cases} x'(u,v) & , x'(u,v) \neq 0 \\ x'(u,v) + \text{sgn}(x(u,v)) & , x'(u,v) = 0 \end{cases} \quad (3.3)$$

Where, $(u, v) = \{(1,3) \text{ or } (3,1)\}$

$$x(u, v) = \frac{X(u, v)}{Q_m}$$

$$x'(u, v) = \text{Integer Round}\left(\frac{X(u, v)}{Q_m}\right)$$

$X(u, v)$: 양자화된 계수, $X(u, v)$: DCT 계수

Step 3. 인접한 특정 계수 값 선택(그림 5)

Step 4. 워터마크가 삽입될 위치에 선택된 계수 값으로 대체

$$X(2, 2) = \begin{cases} X(1, 3) & \text{if } W = 0 \\ X(3, 1) & \text{if } W = 1 \end{cases} \quad (3.4)$$

W : Watermark

$X(u, v)$

16 (DC)	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

그림 4. 양자화 테이블 (Q_m)
Fig. 4. Quantization table.

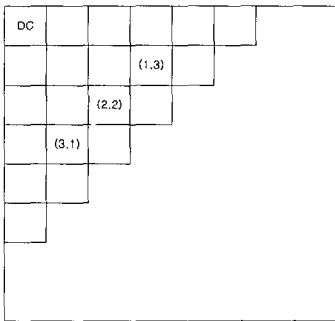


그림 5. 워터마크 삽입을 위한 인접한 값 선택
Fig. 5. The nearest value selection for watermark embedding.

그림 5는 3.1.1에서 생성된 워터마크에 의해서 특정 위치에 대체될 인접한 계수를 선택한다. 이와 같이 모두 4단계에 의해서 워터마크가 삽입이 되고, 역양자화를 거쳐 IDCT를 수행하여 JPEG 압축에서는 강인하고 그렇지 않은 의도적인 변질에서는 검증할 수 있는 워터마크된 영상을 얻을 수 있다.

3.2 워터마크 추출 알고리즘

워터마크 추출과정은 삽입알고리즘과 유사한 방법으로 추출을 한다.

Step 1. 워터마크 삽입된 영상을 8×8 DCT로 변환

Step 2. 블록 재배열(그림 2)

Step 3. 워터마크 재생성(그림 3)

3.1.1의 Step 3-5와 같이 Feature code를 생성하고 삽입할 때와 동일한 비밀키에 의해 생성된 의사난수와의 XOR에 의해 워터마크가 재생성 된다.

Step 4. 생성된 워터마크에 의한 계수 비교

워터마크에 의해 삽입될 부분의 계수 값과 워터마크에 따른 인접한 특정 계수 값과의 유사도를 적용하는 방법을 사용한다. 재생성된 워터마크에 의한 대체값과 그에 대응하는 삽입 계수 값이 유사성을 가지지 않을 경우 해당 위치를 변질로 판별되어 기록화를 시킨다.

$$\text{If } X(2, 2) - \Delta \leq X(1, 3) \quad (3.5)$$

$$\text{or } X(3, 1) \leq X(2, 2) + \Delta$$

then, No distortion

$$\text{Where, } \Delta = \frac{Q_m}{q \times k}$$

$$q = \begin{cases} 2 - 0.02 \times QF & \text{if } QF \geq 50 \\ 50/QF & \text{otherwise} \end{cases}$$

k : variable ($2 \leq k \leq 5$)

위의 과정으로 JPEG 압축의 특성을 이용한 삽입 방법과 유사하게 추출 시에도 사용되었고 JPEG 압축에서는 삽입된 워터마크가 추출된다. 삽입된 계수 값이 특정 위치의 대체 값에 양자화 테이블과 QF에 의해 구해진 임계 값(Δ)을 더하거나 뺀 범위 안에 있으면 공간상에 위치한 해당 블록은 변질이 안 된 것이고, 포함 되지 않으면 변질이 되었음을 알 수 있다. 이것은 식(3.5)에서 알 수 있다.

IV. 실험 및 고찰

본 논문에서 제안한 알고리즘을 검증하기 위해 JPEG 압축시 워터마크의 견고성과 불법적인 변질 검증에 대한 실험을 한다. 실험에 사용한 원영상으로는 512×512 크기의 Lena, Couple, Jet 그리고 미국 화폐의 영상을 사용하였다. 변질된 부분의 위치 판단을 쉽게 하기 위해서 워터마크가 삽입된 영상

에 변질된 부분은 블록 단위로 표시하게 하였다. 워터마크 삽입시 화질에 대한 객관적인 평가 방법으로 식(4.2)과 같이 원영상과 워터마크된 영상의 MSE(Mean Square Error)에 대한 평균값을 이용한 PSNR(Peak Signal-to-Noise Ratio)을 사용하였다.

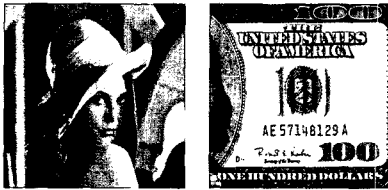
$$MSE = \frac{1}{MN} \sum_{i=0}^M \sum_{j=0}^N (f(i, j) - f'(i, j))^2 \quad (4.1)$$

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (4.2)$$

$f(i, j)$: 원영상의 화소 값

$f'(i, j)$: 워터마크된 영상의 화소 값

MN : 영상의 모든 화소 수(해상도)



(a) Lena (b) 미국 화폐

그림 6. 실험에 사용한 원영상

Fig. 6. Original image used in experiment.

실험 1) Lena의 머리핀 부분을 이웃하는 블록의 픽셀들로 대체하였을 경우 변질된 부분을 워터마크가 삽입된 영상에 검은색으로 표시한다.(그림 9)



그림 7. 워터마크된 영상 Fig. 7. Watermarked image.
 그림 8. 변질 영상 Fig. 8. Tampered image.
 그림 9. 변질검증 결과 Fig. 9. Authentication result.

실험 2) 영상의 아랫부분의 일련번호를 공격자의 의도적인 목적으로 수정하였을 경우



그림 10. 워터마크된 영상 Fig. 10. Watermarked image.
 그림 11. 변질 영상 Fig. 11. Tampered image.
 그림 12. 변질검증 결과 Fig. 12. Authentication result.

실험 3) JPEG 압축을 QF=50으로 하였을 경우(그림 14)에는 변질검증 후 JPEG 압축은 변질이 아니므로 영상에 아무런 표시를 하지 않는다.(그림 15)



그림 13. 워터마크된 영상 Fig. 13. Watermarked image.
 그림 14. JPEG (QF=50) 압축된 영상 Fig. 14. JPEG (QF=50) compressed image.
 그림 15. 변질검증 결과 Fig. 15. Authentication result.

실험 4) 영상에 가우시안 잡음(Gaussian noise) 1%를 첨가하였을 경우



그림 16. 워터마크된 영상 Fig. 16. Watermarked image.
 그림 17. 가우시안 잡음 변질영상(1%) Fig. 17. Gaussian noise tampered image(1%).
 그림 18. 변질검증 결과 Fig. 18. Authentication result.

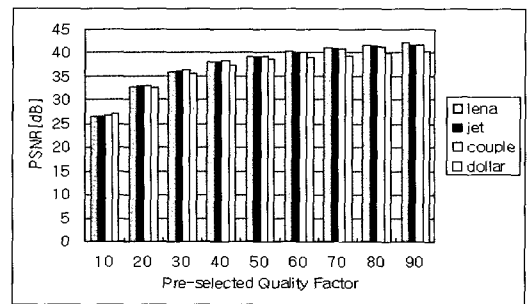


그림 19. Pre-selected QF의 변화에 따른 PSNR
 Fig. 19. PSNR by the change of pre-selected QF.

그림 19에서 워터마크 삽입시 JPEG 압축률을 따른 동일한 QF를 사용하여 워터마크를 삽입하였고 삽입된 영상의 PSNR을 비교하여 나타내었다.

제안한 방법과 C.Y.Lim[14]의 워터마크를 LSB에 삽입하는 기존 방법을 표 1과 같이 Gaussian noise 및 Brightness, Contrast의 영상변환을 비교하였다.

표 1. LSB방법과 제안한 방법의 변질검증률 비교
Table 1. Comparison of authentication probability between LSB method and proposed method for image transform.

Gaussian noise		1	2	3	4	5
Lena	제안 방법	33.4	42.4	47.3	48.4	49.1
	기존 방법	46.9	51.4	58.7	65	69.1
Jet	제안 방법	34.7	43.8	48	52.1	59.9
	기존 방법	48	56.1	63.1	66.1	69.8
Couple	제안 방법	34.8	42.4	47	47.5	49
	기존 방법	35.5	43.8	51	56.5	58.7
Brightness		60	70	80	90	100
Lena	제안 방법	14.6	17.3	19.1	22.5	27.5
	기존 방법	15.2	16.7	17.8	19.2	19.6
Jet	제안 방법	17.4	19.3	22.6	25.9	31.3
	기존 방법	16.5	18.7	19.8	23.5	28.5
Couple	제안 방법	12.4	14.1	16.6	19.8	23.9
	기존 방법	17.2	19.5	23.4	27.1	29.8
Contrast		60	70	80	90	100
Lena	제안 방법	29.4	39	52.4	66.1	77.8
	기존 방법	25.4	27.7	30.4	33.8	38.4
Jet	제안 방법	28.4	42.7	62.3	72.7	80.8
	기존 방법	25.4	28.8	33	36.4	39.9
Couple	제안 방법	27.2	38.6	50.2	59.3	70.3
	기존 방법	36.4	40.9	44.5	48.9	52

각각의 영상 변환 정도에 따라 워터마크가 삽입된 전체 영상에서의 블록화된 정도를 전체 영상에 대한 비율(Authentication Probability)로 나타내었다. 표 1에서 동일한 조건의 QF에서 워터마크를 삽입한 후 실험을 한 결과 Gaussian noise된 영상은 워터마크가 LSB에 삽입된 방법이 더 민감하지만, Brightness와 Contrast와 같은 영상변환에서는 제안한 방법에서 좋은 성능을 나타내었다.

표 2에서는 동일한 QF에서 워터마크를 삽입한 후 실험을 한 결과 PSNR은 유사하지만, 표준화된 JPEG 압축의 경우 제안한 방법(QF=50)이 기존방법(약 QF=80)보다 고압축에 강인함을 알 수 있었다.

표 2. LSB(C.Y.Lim[14]) 알고리즘과 제안한 알고리즘의 PSNR 비교 (QF=50).
Table 2. Comparison between PSNR of general algorithm and proposed algorithm (QF = 50).

구분	기존 방법	제안한 방법
Lena	39.86 dB	39.29
Jet	38.94 dB	39.19
Couple	35.70 dB	39.32
비교	The watermark can survive under maximum embed strength JPEG QF=80	The watermark can survive under maximum embed strength JPEG QF=50

V. 결론

본 논문에서는 DCT를 이용한 주파수 영역에서의 워터마크 알고리즘으로 기존의 복잡한 수식을 요구하는 방법과는 달리 원본 이미지의 DCT 계수 값들의 대치에 의해 워터마크를 삽입하는 간단한 방법을 제안하였다. 워터마크의 추출은 원본 영상을 필요로 하지 않고 워터마크가 삽입된 영상만으로도 워터마크를 추출할 수 있어 처리속도와 실용성에서 이점을 갖는 방법을 제시하였다. DCT 수행 후 블록간의 특성을 이용하여 워터마크를 삽입함으로써 DCT 기반의 JPEG 압축에 대한 강한 내성을 가지도록 하였고, QF가 50의 높은 압축률에 대한 JPEG 압축에서도 워터마크를 추출할 수 있었다.

참고 문헌

- [1] R.J. Anderson and F. Petitcolas, "On the Limits of Steganography," IEEE J. Select Areas Commun., Vol. 16, pp. 474-481, May 1998.
- [2] N. F. Johnson, Z. Duric and S. Jajodia, "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures," Kluwer Academic Publishers, pp.22-29, 2001.
- [3] Nikolaidis, N., and Pitas, I., "Digital Image Watermarking : An Overview," IEEE IICMCS, Florence, Italy, 1999.
- [4] P.S.M. Barreto, H.Y. Kim, and V. Rijmen, "Toward Secure Public-key Blockwise Fragile Authentication Watermarking," in IEEE Proc. V.I.S.P, Vol. 148, No.2, pp.57-62, April 2002.
- [5] Gary L. Friedman, "The Trustworthy Digital Camera : Restoring Credibility to the Photographic Image," IEEE Trans. on Consumer Electronics, Vol. 39, No. 4, November 1993.
- [6] D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," Proc. of the IEEE Identification and Protection of Multimedia Information, Vol. 87(7), pp. 1167-1180, July 1999.
- [7] C.K. Ho and C.T. Li, "Semi-fragile Watermarking Scheme for Authentication of JPEG Image," in Proc. IEEE ICIT LV, USA,

April 2004.

- [8] J.J.K. O Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking Digital Images for Copyright Protection," IEE Proc. vis. Image Signal Process. Vol. 143, No.4, pp.250-256, August 1996.
- [9] I.J. Cox and M.L. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling," Proc. SPIE Conf. on H.V. Electronic Imaging II, Vol. 3-16, pp. 92-99, February 1997.
- [10] R.B. Wolfgang and E.J. Delp, "A Watermarking Technique for Digital Imagery : Further Studies," Video and Imaging Processing Laboratory, Proceeding of the International Conf. on Imaging Science, pp.279-287, 1997.
- [11] I.J. Cox, J. Kilian, T. Leighton and T. Shamon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. on Image Processing, Vol. 6, No. 12, pp. 1673-1687, December 1997.
- [12] P.W. Wong "A Public Key Watermark for Image Authentication," ICIP 98. Proceedings Vol. 2, pp.437-441.
- [13] M. Wu and B. Liu, "Watermarking for Image Authentication," IEEE National Conf. on Image Processing, 1998.
- [14] C.Y. Lin and S.F. Chang, "Semi-Fragile Watermarking for Authentication JPEG Visual Content," SPIE ICSQMCII, Vol. 3971, No. 13, EI '00, 2000.
- [15] J. Fridrich, M. Goljan and R. Du, "Invertible Authentication," in Proc. SPIE, San Jose CA, January 23-26, 2001.

안 성 철 (Sung-cheol Ahn)

정회원



2000년 2월 서울산업대학교 전자공학과(학사)
 2005년 8월 광운대학교 전자통신공학과(석사)
 2006년 4월~현재
 (주)DTVinteractive 연구원
 <관심분야> Watermarking,

MPEG2, H.222, DVB

이 경 학 (Kyoung-hak Lee)

정회원



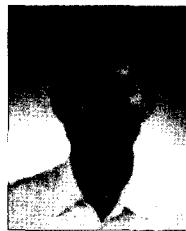
1992년 2월 광운대학교 전자통신공학과(학사)
 1994년 2월 광운대학교 전자통신공학과(석사)
 2000년 3월~현재 광운대학교 전자통신공학과 박사과정
 1994년 4월~현재 한국산업기술

평가원 선임연구원

<관심분야> 영상 압축, 통신신호처리, DSP

박 화 범 (Hwa-bum Park)

정회원



1992년 2월 호서대학교 전자통신공학과(학사)
 1994년 2월 광운대학교 전자통신공학과(석사)
 2004년 3월~현재 광운대학교 전자통신공학과 박사과정
 2000년 3월~현재 남서울대학교

강사

<관심분야> 영상 압축, Watermarking

고 형 화 (Hyung-hwa Ko)

정회원



1979년 2월 서울대학교 전자공학과(학사)
 1982년 2월 서울대학교 전자공학과(석사)
 1989년 2월 서울대학교 전자공학과(박사)
 1985년 3월~현재 광운대학교 전

자통신공학과 교수

<관심분야> 영상통신, 2진문서 압축, Wavelet부호화, 임베디드 시스템