DCT 영역에서 암호화된 이진 위상 컴퓨터형성 홀로그램을 이용한 반복적 디지털 영상 워터마킹 기술†

(An Iterative Digital Image Watermarking Technique using Encrypted Binary Phase Computer Generated Hologram in the DCT Domain)

김 철 수*
(Cheol-Su Kim)

요 약 본 논문에서는 DCT영역에서 암호화된 이진 위상 컴퓨터형성홀로그램을 이용한 반복적 디지털 영상 워터마킹 기술을 제안하였다. 워터마크 삽입과정은 워터마크로 사용되는 은닉영상 대신 은닉영상을 손실없이 재생할 수 있는 이진 위상 컴퓨터형성홀로그램을 생성하고, 반복적으로 표현한 후, 이를 랜덤하게 발생시킨 이진 위상성분을 가지는 키 영상과의 XOR 연산을 통해 암호화하여 워터마크로 사용한다. 그리고 이 암호화된 워터마크에 가중치 함수를 곱하고, 호스트영상의 DCT 영역에서 DC 성분에 삽입한 후, IDCT를 수행한다. 워터마크의 추출은 워터마킹된 영상과 호스트영상의 DCT 계수 차이를 구하고, 삽입시 적용한 가중치 함수를 나눈 후, 키 영상과의 XOR 연산을 이용하여 복호화한다. 그리고 복호화된 워터마크를 역푸리에 변환하여 은닉 영상을 재생한다. 마지막으로 원래의 은닉영상과 복호화된 은닉영상과의 상관을 통해 워터마크의 존재여부를 결정한다. 제안한 방법은 워터마킹 기술은 이진 값으로 구성된 은닉 영상의 홀로그램 정보를 이용하고, 암호화 기법을 활용하였으므로 기존의 어떠한 워터마킹 기술보다 외부 공격에 안전하고, 견실한 특징을 가지고 있으며, 컴퓨터 시뮬레이션을 통해 그 장점들을 확인하였다.

핵심주제어 : DCT, 이진 위상 컴퓨터형성홀로그램, 워터마크, 은닉영상, 호스트영상

Abstract In this paper, we proposed an iterative digital image watermarking technique using encrypted binary phase computer generated hologram in the discrete cosine transform(DCT) domain. For the embedding process of watermark, using simulated annealing algorithm, we would generate a binary phase computer generated hologram(BPCGH) which can reconstruct hidden image perfectly instead of hidden image and repeat the hologram and encrypt it through the XOR operation with key image that is ramdomly generated binary phase components. We multiply the encrypted watermark by the weight function and embed it into the DC coefficients in the DCT domain of host image and an inverse DCT is performed. For the extracting process of watermark, we compare the DC coefficients of watermarked image and original host image in the DCT domain and dividing it by the weight function and decrypt it using XOR operation with key image. And we recover the hidden image by inverse Fourier transforming the decrypted watermark. Finally, we compute the correlation between the original hidden image and recovered hidden image to determine if a watermark exits in the host image. The proposed watermarking technique use the hologram information of hidden image which consist of binary values and encryption technique so it is very secure and robust to the external attacks such as compression, noises and cropping. We confirmed the advantages of the proposed watermarking technique through the computer simulations.

Key Words : discrete cosine transform, binary phase computer generated hologram, watermark, hidden image, host image

† 이 논문은 2008년도 경주대학교 연구년 지원에 의하여 이루어졌음.

* 경주대학교 컴퓨터멀티미디어공학부

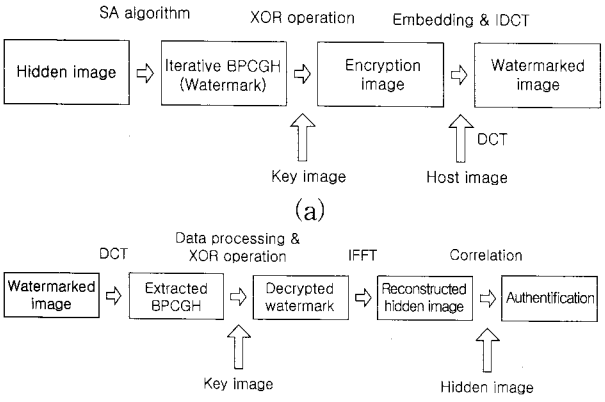
1. 서 론

최근 컴퓨터의 급속한 보급과 인터넷과 같은 정보통신의 발달로 인해 엄청난 양의 디지털 멀티미디어 정보들이 쉽게 생성되고, 시공간을 초월하여 상호 정보교환이 이루어지고 있다. 모든 멀티미디어 매체들이 디지털화 되어가면서 저장이나 전송 등에는 상당한 이점을 제공해 주지만 디지털 콘텐츠의 불법적인 복제나 유통은 콘텐츠 제작자의 창작 의욕 및 경제적 손실을 초래하므로 불법적인 복제를 막고, 저작권을 효과적으로 보호하기 위한 콘텐츠 보호 기술이 요구되고 있다. 일반적으로 정보 보호 방법에는 통신 시에 정보가 제3자에게 누설되지 않도록 하는 암호화/복호화(encryption/decryption) 기술과[1-2] 멀티미디어와 같은 저작물에 지적 소유권자의 마크를 삽입함으로써 불법 복제 및 저작권(copyright)을 보호하려는 워터마킹기술이 있다[3-9]. 암호화 방법은 정보를 이용하기 위해서 먼저 암호화가 풀려야 하고, 암호화가 풀린 디지털 정보에 접근하게 되면 복제와 유통이 자유롭고, 저작권 정보를 파악할 수 없는 반면에 워터마킹 기술은 정보자체에 저작권 정보를 눈에 보이지 않게 삽입시키는 방법으로 불법유통의 추적이나 복제를 방지하는데 유용하게 활용할 수 있는 방식이다. 일반적으로 워터마크 기법이 효과적으로 사용되기 위해 갖추어야 할 기본요건에는 비가시성(invisibility), 견실성(robustness), 삽입될 수 있는 적절한 정보량, 낮은 에러확률이 있으며, 공간적 영역보다는 주파수 영역에서 워터마크를 삽입하는 것이 다양한 공격에 보다 견실한 특성을 가진다고 알려져 있다[3-4]. 워터마킹 기술은 그 응용과 목적에 따라 그 요구사항이 약간씩 다르지만 공통적인 요구사항은 비지각성과 견실성이다. 그러나 워터마크의 정보량에 따라 비지각성과 견실성 사이에는 trade-off 관계가 있다. 즉 정보량이 적어지면 비지각성은 개선되지만 데이터의 압축, 필터링 등과 같은 공격에 약하며, 정보량이 많아지면 공격에 대한 견실성은 개선되지만 비지각성이 떨어진다. 또한 각종 다양한 외부공격이 동시에 들어올 경우에 대한 연구는 많이 이루어지고 있지 않으며, 그 결과도 좋지 않다. 그러므로 일반적으로 적용할 수 있는 워터마킹 기술은 아직까지 개발된 사례가 없어 표준화에 많은 어려움이 있는 실정이다. 그리고 워터마크 기술과 관련된 프로그램의 대부분이 단순한 형태를 하고 있어, 프로그래밍을 어느 정도 공부한 사람이면 콘텐츠에서 워터마크를 손쉽게 제거할 수 있고, 워터마크가 제거된 콘텐츠는 불법적으로 유통되고 있는 것이 현실이며, 현재까지 연구소 또는 학교에서 발표되고 있는 논문이나 학술대회에서 제안되는 기술들이 그 적용 영역이 매우 좁아 그 실용성이 의문시 되는 경우가 많은 실정이다.

본 논문에서는 현재까지 발표되거나 연구되고 있는 방법의 문제점을 해결하여 디지털 콘텐츠 및 서비스 시장에 실제로 활용 가능성이 있는 홀로그램 정보를 암호화하여 워터마크로 이용하는 새로운 디지털 워터마킹 기술을 제안하고자 한다. 홀로그램은 그 정보량이 일부 손실되더라도 원래의 영상을 복원할 수 있는 특징이 있기 때문에 이를 워터마크로 사용할 수 있다면 워터마킹 기술에서 가장 문제가 되고 있는 비지각성과 견실성을 동시에 만족시킬 수 있으리라 기대된다. 또한 홀로그램을 반복 표현하고, 암호화하여 워터마크로 사용함으로써 외부공격 및 정보보호 기능을 더 강화하고자 한다. 홀로그램을 워터마크로 사용하기 위해서는 먼저 은둔영상을 완벽하게 재생할 수 있는 최적의 이진 위상 컴퓨터형성홀로그램(binary phase computer gernerated hologram; BPCGH)을 설계하는 과정, 반복표현 및 암호화과정, 비지각성과 강인성을 동시에 만족하는 적절한 가중치 함수를 통해 호스트 영상에 삽입하는 과정, 워터마크의 추출 및 복호화 과정, 그리고 추출된 워터마크의 진위 여부를 검증하는 과정이 필요하다.

2. 제안한 디지털 영상 워터마킹 기술

제안한 방법은 기존에 발표된 디지털 워터마킹 기술과는 달리 다양한 외부 공격들이 동시에 발생하더라고 이에 견실하게 대응할 수 있는 기술로서 전체 구성은 워터마크 생성, 암호화 및 삽입과정과 워터마크의 추출, 복호화 및 검증과정으로 분류된다. 워터마크 생성은 simulated annealing(SA)알고리듬을 이용한 은닉영상의 BPCGH설계 및 반복표현으로 이루어진다. 그리고, 랜덤하게 발생시킨 키 영상과 XOR 논리연산을 통해 암호화되며, DCT 영역에서 가중치 함수를 곱한 후, 호스트영상의 DC성분에 삽입하고, IDCT를 수행함으로써 호스트영상에 워터마크가 삽입된다. 워터마크의 추출, 복호화 및 검증은 DCT 및 가중치 함수와의 연산을 통한 워터마크의 추출, 암호화된 워터마크의 복호화, 역푸리에 변환 및 상관연산을 통한 워터마크의 검증과정으로 구성된다. 이 과정들을 그림 1에 나타내었다.



(그림 1) 제안한 디지털 영상 워터마킹 기술
(a) 워터마크 생성, 부호화 및 삽입, (b) 워터마크 추출, 복호화 및 검증

2.1 워터마크의 설계

홀로그램이란 물체에 의해 산란된 파면의 크기와 위상정보를 기준파와 간섭을 통하여 세기의 형태로 기록한 것이며, 이를 통하여 입체 영상 정보를 충실히 재현할 수 있는 기술이다. 이에 반해 CGH는 회절이론에 의한 수학적인 연산을 통해 이상적인 간섭 파면을 계산하여 기록한 것이며, 존재하지 않는 물체의 경우에도 사용할 수 있어 광통신소자 및 신호처리의 많은 분야에 사용되고 있다. 일반적으로 연속정보의 CGH 제작은 기록소자의 해상도 제한, 정보의 저장 및 전송에서 많은 문제점이 있으므로 정보의 이진화가 요구된다. 그러나 연속정보를 이진화하면 정보의 손실이 발생하고, 영상 재생 시 양자화 잡음으로 나타난다. 이를 해결하는 여러 방법들 중 최적의 해를 구할 수 있는 대표적인 방법이 SA 알고리듬이다[2],[9]. 통계열역학에서 비롯된 SA 알고리듬은 복잡한 최적 해를 풀기 위하나 반복적인 알고리듬으로써 국소 최적해에서 벗어날 수 있는 반면 많은 반복과정을 수행해야 하므로 시간이 많이 소요된다. 본 논문에서는 SA 알고리듬을 이용하여 워터마크로 사용할 은닉영상에 대한 최적의 BPCGH를 설계하였다. SA알고리듬에서는 사용되는 매개변수들의 값들에 의해 그 성능이 결정되는데, 본 논문에서는 32x32 크기의 은닉영상에 대한 최적의 BPCGH를 설계하기 위해 초기온도 T_{init}는 1.0, 냉각속도D_t는 0.91, 그리고 반복 횟수 N는 80회로 하였다. 설계된 32x32 크기의 BPCGH는 반복 표현하여 64x64크기로 만든 후, 워터마크로 사용하였다.

2.2 워터마크의 암호화

은닉 영상의 홀로그램정보를 반복표현한 워터마크함수 $W(k,l)$를 호스트영상에 삽입하기 전에, 암호화 과정을 수행한다. 워터마크 함수는 64x64개의 1 또는 '-1'의 이진 값을 가지며 $W(k,l)=1$ 또는 -1, $1 \le k,l \le K,L$로 표현된다. 워터마크로 사용되는 홀로그램은 그 정보의 일부를 잃어도 은닉 영상을 복원할 수 있는 성질이 있으므로 정보의 전송과정에서 생길 수 있는 각종 잡음 및 외부 공격 등에 상당히 견실하다. 이를 암호화하기 위하여 랜덤하게 발생시킨 이진 위상영상을 암호 키 $Key(k,l)$으로 정하고, 이를 표 1의 규칙을 적용한 XOR 연산을 하면 암호화 된 워터마크 영상 $W_E(k,l)$을 구할 수 있다. 이를 식으로 표현하면 다음과 같다.

$$W_E(k,l) = Key(k,l) \oplus W(k,l), \quad 1 \le k,l \le K,L \tag{1}$$

<표 1> XOR 연산을 이용한 워터마크의 암호화 위상(크기)값

Encrypted watermark	Key image	Watermark
π(-1)	0(1)	π(-1)
	π(-1)	0(1)
0(1)	0(1)	0(1)
	π(-1)	π(-1)

이때 위상 값을 크기로 표현하면 'π'의 위상은 '-1'로 표현되고, '0'위상은 '+1'로 표현된다.

2.3 워터마크의 삽입

암호화된 워터마크 $W_E(k,l)$는 호스트영상 $f(x,y)$의 DCT 영역에서 적절한 가중치를 가지고 삽입된다. 이를 위해 먼저 호스트영상을 겹치지 않는 8x8블록으로 분리한 후 DCT를 취한다. 이를 표현하면 다음과 같다.

$$f(x,y) = \bigcup_{k=1}^{K} \bigcup_{l=1}^{L} f_{kl}(x',y'),\ 1 \le x',y' \le 8 \tag{2}$$

$$F_{kl}(u,v) = DCT[f_{kl}(x',y')],\ 1 \le u,v \le 8 \tag{3}$$

여기서 매개변수 k,l은 가로 및 세로 방향의 블록 크기를 의미하며, x',y'은 블록내 매개변수를 의미한다. 그리고 u,v는 DCT 영역내의 매개변수를 나타낸다. 암호화된 워터마크는 각 블록의 DC 계수를 고려한 가중치와 곱해진 후, 각 블록의 DC 계수에 더해지고, 마지막으로 IDCT를 취함으로써

워터마크가 삽입된 호스트영상이 구해진다. 이와 같은 과정을 수식으로 표현하면 다음과 같다.

$$f^w(x,y)=\bigcup_{k=1}^{K}\bigcup_{l=1}^{L} IDCT[F_{kl}^w(u,v)] \quad (4)$$

$$F_{kl}^w(u,v)=\begin{cases}F_{kl}(u,v)+\delta\times W_E(k,l), & \text{if } u=v=0\\ F_{kl}(u,v) & otherwise\end{cases}$$

$$\delta(k,l)=weight\times F_{kl}(0,0)$$

여기서 $F_{kl}^w(u,v)$는 암호화된 워터마크가 삽입된 영상의 DCT 함수를 의미하고, $F_{kl}(u,v)$는 (k,l)번째 8x8 블록의 DCT 함수를 의미하며, $\delta(k,l)$는 그 블록의 DC성분을 고려한 가중치 함수를 의미하며, 변수 $weight$값에 의해 워터마크의 정보량이 결정된다. 제안하는 방법은 워터마크로 사용되는 은닉영상의 BPCGH정보를 반복하여 사용하고, 암호화함으로써 절단과 같은 외부공격에 더 강한 성질을 가질 뿐만 아니라 정보보호 기능이 더 강화된 특징이 있다[9].

2.4 워터마크의 추출 및 복호화

워터마킹된 호스트영상은 여러 외부의 공격을 받을 수 있고, 이로 인해 워터마크 추출이 어려워 불법복제 및 유통의 추적이 불가능할 수 있다. 본 논문에서 최종 삽입되는 워터마크의 값들이 암호화된 홀로그램 정보이고, 이진 값으로 구성되어 있으므로 외부공격에 매우 견실하다. 워터마크의 추출은 삽입과정의 역순이며, DCT 영역에서 이루어진다. 그러므로 워터마킹된 호스트영상 $f^w(x,y)$와 원래 호스트영상인 $f(x,y)$의 DCT 결과의 차를 구한 후, 삽입전의 가중치 함수의 역수를 곱하면 된다. 이를 수식으로 표현하면 아래와 같다.

$$W'_E(k,l)=[F_{kl}^w(0,0)-F_{kl}(0,0)]\times\frac{1}{\delta(k,l)} \quad (5)$$

추출된 결과는 다시 한번 키 영상과의 XOR연산을 통해 복호화 과정을 거치게 되며 아래 식으로 표현된다.

$$W_D(k,l)=W'_E(k,l)\oplus Key(k,l) \quad (6)$$

복호화된 워터마크는 은닉영상의 BPCGH 정보이므로 추출 및 복호화과정에서 정보의 손실이 다소 있더라도 역푸리에 변환을 하면 은닉영상을 재생할 수 있다.

2.5 워터마크의 검증

워터마크의 존재여부는 최종 복호화된 워터마크인 BPCGH 정보를 역푸리에 변환하여 은닉영상을 재생한 다음, 삽입전의 BPCGH로부터 재생한 은닉영상과의 상관을 통해 검증할 수 있다. 그 상관첨두치가 적절히 정한 문턱치 값 이상이면 워터마크가 존재하고, 미만이면 존재하지 않는 것으로 판단한다. 이를 수식으로 표현하면 다음과 같다.

$$c(x,y)=IFT\{W(k,l)\}\otimes IFT\{W_D(k,l)\} \quad (7)$$

$$\begin{cases}\text{워터마크가 존재}, & \text{if } c(x,y)_{\max}\geq T_{th}\\ \text{워터마크가 부재}, & otherwise\end{cases}$$

여기서 $\otimes$는 상관연산자를 의미하며, 문턱치 T_{th}는 최대 상관첨두치의 50%로 둔다.

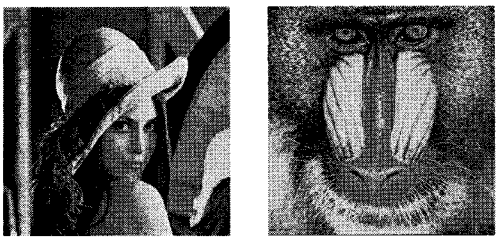
3. 컴퓨터시뮬레이션 결과 및 고찰

본 논문에서 제안한 디지털 워터마킹 기술의 성능 측정을 위해 사용한 호스트영상은 512x512화소를 가지는 Lena와 Baboon 영상이며, 워터마크는 32x32 크기의 은닉영상인 영문자 'T'에 대해 설계한 BPCGH를 반복 표현한 64x64 크기의 홀로그램 패턴이다. 제안된 방법의 성능 측정을 위해 JPEG 압축, 가우시안 잡음 및 절단과 같은 외부공격에 대한 견실성을 측정하였다. 그리고 워터마크가 삽입된 영상의 비가시성을 측정하기 위해 PSNR(Peak Signal to Noise Ratio)을 이용하였다.

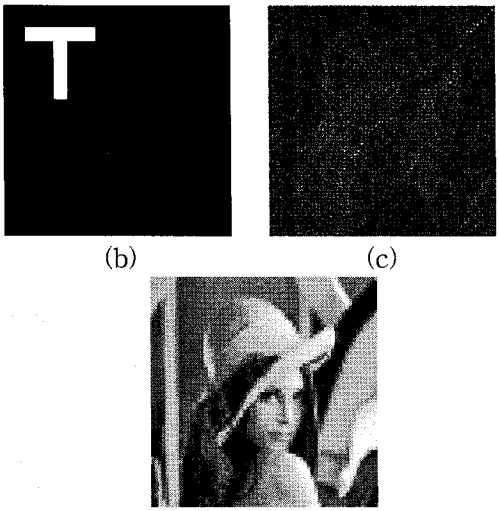
$$PSNR=20\log_{10}(255/RMSE) \quad (8)$$

$$RMSE=\sqrt{\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[f^w(x,y)-f(x,y)]^2}$$

여기서 M, N은 호스트영상의 x축 및 y축의 크기를 나타낸다. 그림 2는 성능 측정에 사용된 두 개의 호스트영상, 은닉영상, Lena 영상에 대한 8x8 블록 DCT 영상 및 DC 성분을 나타낸다. 그림 2(d)와 같은 DCT의 DC 성분에 암호화된 워터마크 정보를 삽입한다.



(a)

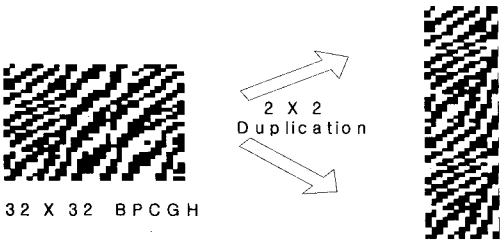


(b) (c)

(d)

(그림 2) 호스트영상, 은닉영상 및 호스트영상의 DCT 결과 영상

(a) 호스트영상(Lena, Baboon; 512x512) (b) 은닉영상(32x32) (c) Lena영상의 8x8 블록 DCT결과(512x512), (d) DCT결과의 DC 성분(64x64)



(그림 3) 워터마크 설계 과정

그림 3은 은닉영상에 대해 SA 알고리듬을 이용하여 설계한 BPCGH를 반복 표현한 워터마크 설계과정을 보여주며, 그림과 같이 반복 표현하여 사용함으로써 절단과 같은 외부공격에 좀 더 견실해질 수 있다. 최종 설계된 워터마크는 랜덤하게 발생시킨 키 영상과의 XOR 연산을 통해 암호화되며 이를 그림 4에 나타내었다. 암호화된 워터마크 영

(a) (b)

(그림 4) XOR 연산을 이용한 워터마크의 암호화

(a) 키 영상 (b) 암호화된 워터마크

상은 랜덤한 형태의 이진 위상 값을 갖는 영상으로 은닉영상의 BPCGH에 대한 정보가 나타나 있지 않으며, 키 영상이 있어야 복호화가 가능하다.

그림 2(d)와 같은 DCT의 DC 성분에 그림 4(b)의 암호화된 BPCGH정보를 적절히 삽입한 후, IDCT변환을 수행함으로써 워터마크된 호스트영상이 구해진다. 제안된 방법은 은닉영상의 BPCGH 정보를 반복 표현한 후, 이를 암호화하여 워터마크로 사용하였으므로, 각종 외부공격에 강할 뿐만 아니라 암호화과정도 포함하고 있으므로 기존에 제안된 많은 디지털 워터마킹 기술에 비해 정보보호 기능이 강화되었다고 할 수 있다. 컴퓨터 시뮬레이션을 통해 각종 공격에 대한 PSNR 값과 추출된 워터마크의 검증을 위한 상관결과 값은 표 2와 같으며, 이들 값들은 5회 반복 실험한 결과를 평균한 것이다. 그리고 이때 워터마크의 정보량을 결정하는 가중치(*weight*)값은 0.015로 두었다.

<표 2> 외부공격에 대한 PSNR측정 및 상관결과

외부공격	PSNR(dB)		정규화된 상관첨두치	
	Lena	Baboon	Lena	Baboon
워터마킹 삽입	41.883	41.219	1.000	1.000
JPEG 압축*)	34.686	27.588	0.872	0.911
JPEG 압축 + 가우시안잡음**)	29.960	26.095	0.753	0.793
JPEG 압축 + 가우시안잡음 + 절단***)	30.475	26.012	0.601	0.581

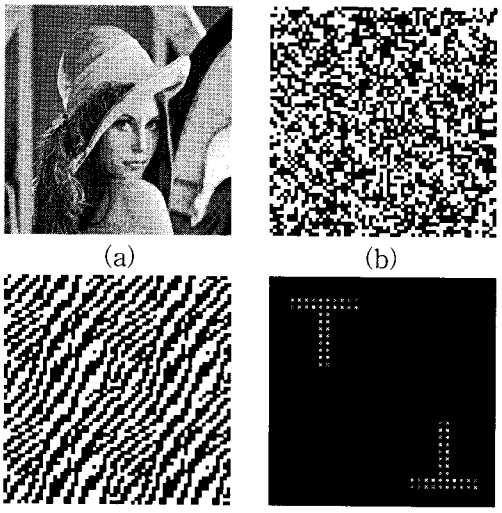
*) 압축률(Lena; 90%, Baboon; 80%)

**) 가우시안 잡음: 20%(zero mean one variance)

***) 절단율: 25%

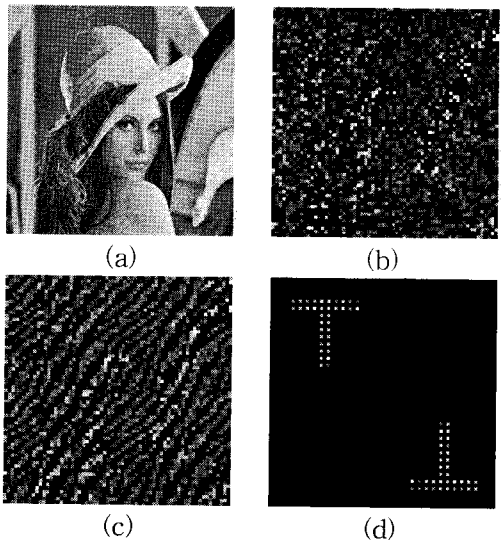
표 2의 결과를 보면 압축, 잡음 및 절단과 같은 외부 공격들이 누적되어 들어오더라도 정규화된 상관첨두치에 문턱치(0.5)를 적절히 적용하면 워터마크의 존재여부를 판별할 수 있음을 알 수 있다. 그림 5는 워터마킹이 삽입된 호스트영상, 추출된 워터마크영상, 복호화된 워터마크영상, 그리고 최종적으로 재생된 은닉영상의 결과를 보여준다. 32x32 크기의 BPCGH를 반복적으로 나타내어 64x64 크기로 확대하였으므로 재생되는 은닉영상의 형태는 그림 2(b)와는 차이가 남을 확인할 수 있다. 그리고 외부공격이 없었으므로 최종 복호화된 워터마크 영상은 그림 3의 반복 표현된 BPCGH 패턴과 동일함을 알 수 있다. 그림 6, 7, 8에서는 외부의 다양한 공격들이 누적되어 들어왔을 경우 제안한 디지털 워터마킹 기술이 워터마크의 추출 및 존재여부를 검증할 수 있음을 보여준

다. 다양한 외부 공격으로 인해 추출 및 복호화된 워터마크 영상과 원래의 워터마크 영상에 다소 차이점이 있지만 이들이 홀로그램 정보이므로 재생되는 은닉영상은 거의 비슷함을 알 수 있다. 이와 같이 본 논문에서 제안하는 워터마킹 기술에서는 워터마크가 홀로그램의 정보를 지니고 있으므로 압축, 잡음 및 절단과 같은 외부잡음에 강인할 수 있다. 또한 암호화 과정을 거쳤으므로 키 정보가 없으면 워터마크의 복호화가 불가능하므로 정보보호 기능이 강화된 장점이 있다. 그리고 워터마크의 정보량인 *weight*값을 조정하면 비가시성 및 워터마크 검증에 좀 더 유연하게 대응할 수 있다.



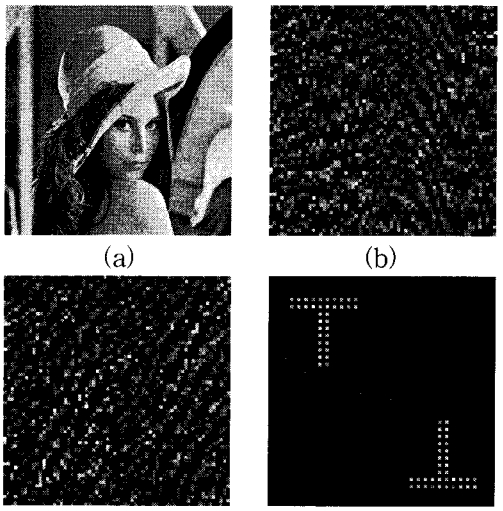
(a) (b) (c) (d)

(그림 5) 워터마크 추출결과
(a) 워터마크 삽입된 호스트영상(512x512), (b) 추출된 워터마크(64x64), (c) 복호화된 워터마크(64x64), (d) 재생된 은닉영상(64x64)



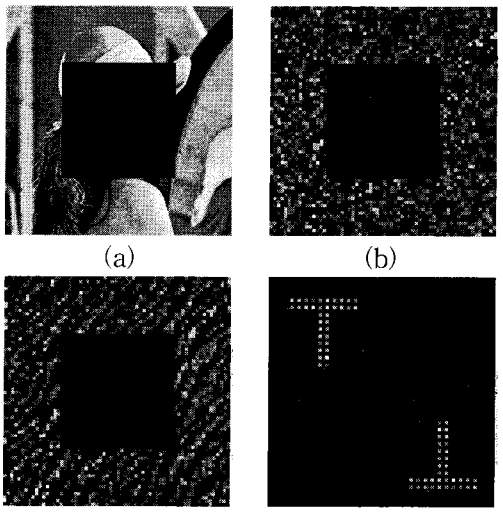
(a) (b) (c) (d)

(그림 6) 압축 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(90%)된 호스트영상(512x512), (b) 추출된 워터마크(64x64), (c) 복호화된 워터마크(64x64), (d) 재생된 은닉영상(64x64)



(a) (b) (c) (d)

(그림 7) 압축 및 가우시안 잡음 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(90%) 및 가우시안 잡음(20%)이 첨가된 호스트영상(512x512), (b) 추출된 워터마크(64x64), (c) 복호화된 워터마크(64x64), (d) 재생된 은닉영상(64x64)



(a) (b) (c) (d)

(그림 8) 압축, 가우시안 잡음 및 절단 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(90%), 가우시안 잡음(20%) 및 절단(25%) 호스트영상(512x512), (b) 추출된 워터마크(64x64), (c) 복호화된 워터마크(64x64), (d) 재생된 은닉영상(64x64)

4. 결 론

본 논문에서는 워터마크로 사용될 은닉영상의 BPCGH를 설계하고, 반복적으로 표현한 후, 암호화하여 호스트영상의 DCT 영역에서 DC성분에 적절하게 삽입하는 디지털 워터마킹 기술을 제안하였다. 제안된 워터마킹 기술은 은닉영상의 홀로그램 정보를 반복적으로 이용하고, 암화화 과정을 거쳤으며, 이진 값을 가지므로 각종 외부공격이 동시에 누적되어 들어오더라도 워터마킹 정보를 추출하고, 검증할 수 있는 장점이 있음을 컴퓨터 시뮬레이션을 통해 확인하였다. 앞으로 제안한 디지털 워터마킹 기술이 좀 더 다양한 외부공격에 대해 어떻게 반응하는지를 점검할 예정이며, 긍정적인 결과가 도출이 되면 디지털 콘텐츠 보호, 및 지적재산권이 중요시 되는 미래 유비쿼터스 시대에서 그 활용도가 높을 것으로 예상된다.

참 고 문 헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 32, no. 7, pp. 767- 769, 1995

[2] J. Ohtsubo and A. Fujimoto "Practical image encryption and decryption by phase-coding technique for optical security systems," *Applied Optics*, vol. 41, no. 23, pp. 4848-4855, 2002

[3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio, and video," *Proc. of the IEEE. Int. conf. Image Processing*, vol 3, pp. 243-246, 1996

[4] J. Huang and Y. Q. Shi, "Adaptive image watermarking scheme based on visual masking," *Electronics Letters*, vol. 34, no. 8, pp. 748-750, 1998

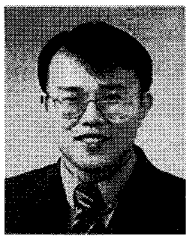
[5] 김정연, 남제호, "DCT 압축영역에서의 DC 영상 기반 다해상도 워터마킹 기법," *대한전자공학회 논문지*, 제 45권 SP편 4호, pp. 1-9, 2008

[6] X. Xia, C. G. Boncelet and G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497-511, 1998

[7] F. Ahmed, I. S. Moskowitz, "Correlation-based watermarking method for image authentification applications," *Opt. Eng.*, vol. 43, no. 8, pp. 1833-1838, 2004

[8] D. Zheng, J. Zho and A. E. Saddik, "RST-Invariant Digital Watermarking Based on Log-Polar mapping and Phase Correlation," *IEEE Trans. on Circuit and Systems for Video Techno.*, vol. 13. no. 8, pp. 753-765, 2003

[9] 김철수, "DCT 영역에서 컴퓨터형성홀로그램을 이용한 디지털 영상 워터마킹 기술", 경주대학교 정보전자기술논총, 제 7권 pp. 37-48, 2008



김 철 수 (Cheol-Su Kim)

- 종신회원
- 1989년 2월: 경북대학교 전자공학과(공학사)
- 1991년 2월: 경북대학교 대학원 전자공학과 (공학석사)
- 1997년 2월: 경북대학교 대학원 전자공학과 (공학박사)
- 1995년 3월 ~ 1998년 2월: 김천대학 전자통신과
- 2008년 2월 ~ 2009년 1월: Univ. of Connecticut 컴퓨터전자공학과 방문교수
- 1998년 3월 ~ 현재: 경주대학교 컴퓨터멀티미디어공학부 부교수
- 관심분야: 광통신, 정보보호, 광메모리 등

논문접수일 : 2009년 6월 9일
논문수정일 : 2009년 7월 27일
게재확정일 : 2009년 8월 15일