Journal of Korea Multimedia Society Vol. 14, No. 3, March 2011(pp. 403-413)

DCT영역에서 스크램블된 이진 위상 컴퓨터형성홀로그램을 이용한 디지털 영상 워터마킹 기술

김 철 수†

요 약

본 논문에서는 DCT영역에서 스크램블된 이진 위상 컴퓨터형성홀로그램을 이용한 디지털 영상 워터마킹 기술을 제안하였다. 워터마크 삽입과정은 워터마크로 사용되는 은닉영상 대신 은닉영상을 손실 없이 재생할 수 있는 이진 위상 컴퓨터홀로그램을 생성하고 이를 스크램블기법으로 암호화 하여 워터마크로 사용한다. 그리고 암호화된 워터마크에 가중치 함수를 곱하고 호스트영상의 DCT영역에서 DC성분에 삽입한 후 IDCT를 수행한다. 워터마크의 추출은 워터마킹된 영상과 원래의 호스트영상의 DCT계수 차이를 구하고, 삽입시 적용한 가중치 함수를 나눈 후 디스크램블링 하여 복호화 한다. 그리고 복호화된 워터마크를 역푸리에 변환하여 은닉영상을 재생한다. 마지막으로 원래의 은닉영상과 복호화된 은닉영상과의 상관을 통해 워터마크의 존재여부를 결정한다. 제안된 워터마킹 기술은 이진 값으로 구성된 은닉영상의 홀로그램정보를 이용하고 스크램블링 암호화 기법을 활용하였음으로 기존의 어떠한 워터마킹 기술보다 압축, 잡음 및 절단과 같은 다양한 외부공격에 안전하고 견실한 특징을 가지고 있음을 컴퓨터시뮬레이션을 통해 그 장점들을 확인하였다.

Digital Image Watermarking Technique using Scrambled Binary Phase Computer Generated Hologram in Discrete Cosine Transform Domain

Cheol-Su Kim†

ABSTRACT

In this paper, we proposed a digital image watermarking technique using scrambled 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 encrypt it through the scramble operation. 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 descramble operation. 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 scramble encryption technique so it is very secure and robust to the various 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(이산 코사인 변환), Binary Phase Computer Generated Hologram (이진 위상 컴퓨터형성홀로그램), Watermark(워터마크), Hidden Image(은닉 영상), Host Image(호스트 영상)

※ 교신저자(Corresponding Author) : 김철수, 주소 : 대구광역시 북구 산격동 1307(702-701), 전화 : 053)940-8815, FAX : 053)950-5505, E-mail : kcs6694@hanmail.net

접수일 : 2010년 4월 12일, 수정일 : 2010년 10월 11일
완료일 : 2011년 1월 7일

† 정회원, 경북대학교 IT대학 연구원

1. 서 론

현대 정보화 사회에서는 컴퓨터의 보급 및 초고속 네트워크의 구축 등으로 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 창작의욕 및 경제적 손실을 초래하므로 불법적인 복제를 막고, 저작권을 효과적으로 보호하기 위한 콘텐츠 보호 기술이 요구되고 있다. 일반적으로 정보 보호 방법에는 통신 시에 정보가 인증된 사람이 아닌 제 3자에게 누설되지 않도록 하는 암호화/복호화(encryption/decryption) 기술과[1,2] 각종 멀티미디어 저작물에 지적 소유권자의 마크를 삽입함으로써 불법 복제 및 추적을 통해 저작권(copyright)을 보호하려는 워터마킹기술이 있다[3-17]. 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 비시각성(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[3-6]. 그리고 디지털 콘텐츠의 소유권을 증명하기 위해 워터마크로 사용되는 기존의 랜덤잡음이나 로고(logo) 대신 로고의 디지털 홀로그램을 워터마크로 사용하여 워터마크 자체에 외부공격에 대한 강인성을 부여하는 연구들이 많이 진행되고 있다[7-8], [11-14]. 최근 들어 홀로그램을 이용한 워터마킹 기술의 적용영역을 확대하고, 콘텐츠의 불법유통을 추적하고자 하는 방향으로 연구가 진행되고 있는 추세이다[13-14]. 워터마킹 기술은 그 응용과 목적에 따라 그 요구사항이 약간씩 다르지만 공통적인 요구사항은 비시각성과 견실성이다[15-17]. 그러나 워터마크의 정보량에 따라 비시각성과 견실성 사이에는 상호보완적(trade-off) 관계가 있다. 즉 정보량이 적어지면 비시각성은 개선되지만 데이터의 압축, 필터링 등과 같은 공격에 약하며, 정보량이 많아지면 공격에 대한 견실성은 개선되지만 비시각성이 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 의문시되는 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 비시각성과 견실성을 동시에 만족시킬 수 있으리라 기대된다. 또한 홀로그램을 스크램블 연산을 통해 암호화하여 워터마크로 사용함으로써 외부공격 및 정보보호 기능을 더 강화하고자 한다. 홀로그램을 워터마크로 사용하기 위해서는 먼저 은닉영상을 완벽하게 재생할 수 있는 최적의 이진 위상 컴퓨터형성홀로그램(binary phase computer generated hologram; BPCGH)을 설계하는 과정, 암호화과정, 비시각성과 견실성을 동시에 만족하는 적절한 가중치 함수를 통해 호스트영상에 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 워터마크를 암호화하고, 다양한 외부 공

격들이 동시에 발생하더라고 이에 견실하게 대응할 수 있는 기술로서 전체 구성은 워터마크 생성, 암호화 및 삽입과정과 워터마크의 추출, 복호화 및 검증과정으로 분류된다. 워터마크의 삽입과정은 먼저 simulated annealing(SA)알고리듬을 이용하여 은닉영상의 BPCGH를 설계하여 워터마크를 생성하고, 열 방향 및 행 방향 랜덤 키 정보를 이용한 스크램블 연산을 통해 암호화한다. 그리고 암호화된 워터마크를 DCT영역에서 가중치 함수를 곱한 후, 호스트영상의 DC성분에 삽입하고, IDCT를 수행함으로써 호스트영상에 삽입한다. 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.

2.1 워터마크의 설계

홀로그래피(Holography)는 빛의 간섭성을 이용하여 물체에 의해 산란된 물체파와 기준파의 간섭세기 정보를 기록하고 재생하는 방법을 의미하며, 홀로그램은 그 기술로 기록하고 재생된 3차원 입체영상을 가리킨다. 이에 반해 컴퓨터형성홀로그램(computer generated hologram; CGH)는 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[1,12]. 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. 생성하려는 은닉영상 함수 $h(x,y)$는 SA 알고리듬을 통해 설계된 BPCGH 함수 $H(u,v)$을 푸리에 변환함으로써 얻을 수 있다. 각 함수는 $N\times N$ 화소들로 구성되어 있으며, 이들의 이산적인 표현은

$$h_{mn} = \frac{1}{N^2}\sum_{k=-N/2}^{N/2-1}\sum_{l=-N/2}^{N/2-1} H_{kl} \times \exp\left(j2\pi\left(\frac{km}{N}+\frac{ln}{N}\right)\right) \tag{1}$$

와 같다. 여기서 H_{kl}는 $H(u,v)$의 (k,l)번째 표본화 값이며, h_{mn}는 $h(x,y)$의 (m,n)번째 표본화 값이다.

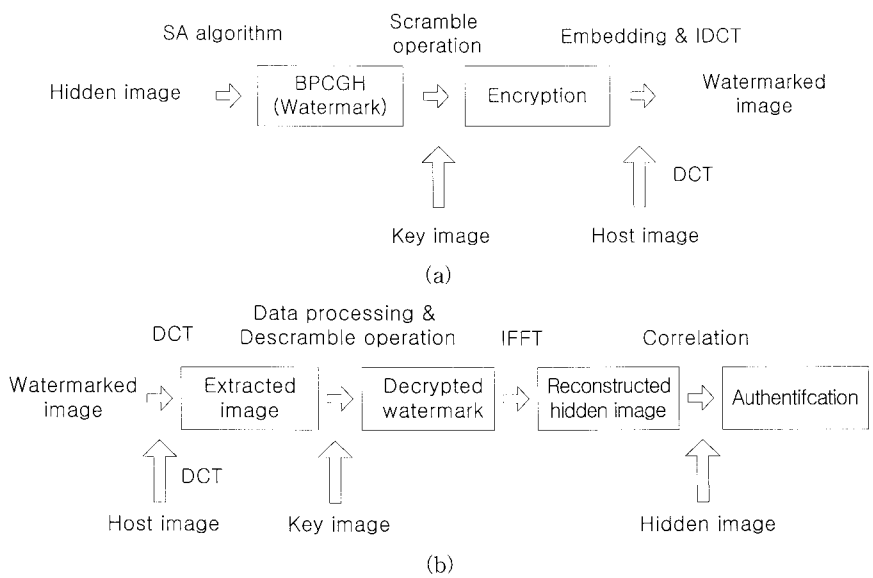


그림 1. 제안한 디지털 영상 워터마킹 기술
(a) 워터마크 생성, 부호화 및 삽입, (b) 워터마크 추출, 복호화 및 검증

SA 알고리듬에서 비용함수는 생성하려는 영상에 따라 다르며, 이진영상이나 명암도영상 생성을 위한 비용함수는 은닉영상내 제한된 영역에 위치하고 있는 목표영상과 재생된 영상 사이의 평균자승오차 E로 정의한다.

$$E=\frac{1}{AB}\sum_{m=m_0}^{A-1}\sum_{n=n_0}^{B-1}\left||f'_{mn}|^2-|h_{mn}|^2\right|^2 \tag{2-a}$$

$$c\sum_{m=-N/2}^{N/2-1}\sum_{n=-N/2}^{N/2-1}|f_{mn}|^2=\eta_t \tag{2-b}$$

$$|f'_{mn}|^2=c|f_{mn}|^2 \tag{2-c}$$

여기서 η_t는 목표효율을 나타내고, A와 B는 각각 목표영상의 가로 및 세로의 크기를 나타낸다. c는 목표영상 f'_{mn}의 전체 에너지가 η_t가 되도록 하는 제어상수이며, 전처리 과정에서 영상에 따라 달라진다. 이 비용함수는 제한된 영역내에서 목표영상을 찾아가도록 함으로써 관심영역 밖의 배경잡음을 줄여 더욱 높은 효율을 가질 수 있게 한다. BPCGH의 최적 설계를 위한 SA 알고리듬의 순서도는 그림 2와 같으며, 수행과정은 다음과 같다[1].

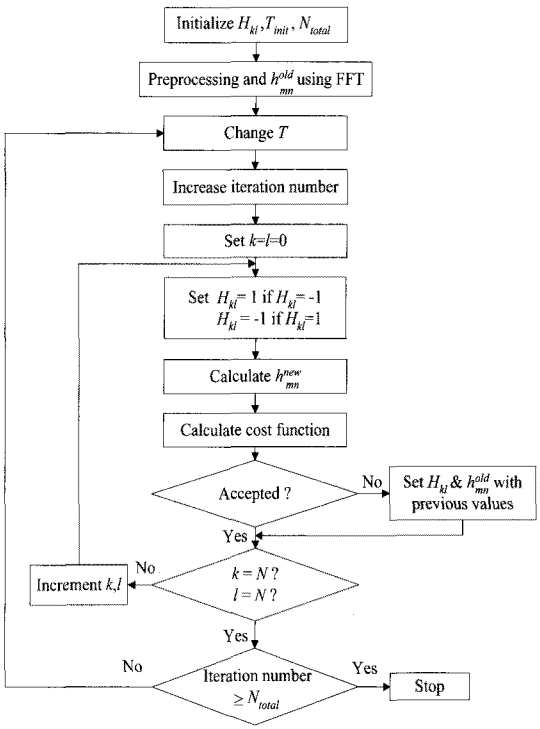


그림 2. 이진 위상 컴퓨터형성홀로그램의 최적 설계를 위한 SA 알고리듬의 순서도

① BPCGHC의 초기 투과함수 H_{kl}을 2단계의 값으로 무작위 선정하고, 비용함수 E^{old}를 계산한다.

② 초기온도, 온도의 냉각속도, 그리고 반복횟수를 경험적으로 결정한다.

③ BPCGH의 투과함수의 한 화소 값을 바꾼 후, 비용함수 E^{new}를 계산하고, 아래의 조건을 판단하여 수용여부를 결정한다.

$$\begin{array}{ll}\Delta E= & E^{old}-E^{new}\\ \Delta E<0, & \text{무조건수용}\\ \Delta E\geq 0, & \text{조건부수용}\end{array} \tag{3}$$

④ 투과함수의 인접한 화소를 바꾸고, 반복횟수만큼 ③의 과정을 반복한다.

과정 ③에서 비용함수의 변화량이 양수일 때에도 조건부 수용을 하여 국소 최적 해에 빠지지 않도록 하였다. 수용여부는 아래와 같이 표현되는 볼쯔만 확률분포(Boltzman probability distribution)와 무작위로 발생된 0~1 사이의 값과 비교하여 결정하였다.

$$P(\Delta E)=\exp(-\Delta E/T_n),\quad T_n=(D_t)^n\ T_{init} \tag{4}$$

여기서 P는 수용 확률을 나타내고, ΔE는 비용함수의 변화량을 나타낸다. 그리고 T_n는 n번째 반복과정에서의 온도를 나타내는 변수이고, T_{init}는 초기온도를 나타내는 변수이다. 식 (4)에서 확률 $P(\Delta E)$는 온도와 비용함수의 변화량의 함수이며, 반복과정의 초기에는 거의 1에 가깝게 두어 조건부 수용을 받아들이고, 말기에는 배제하도록 초기온도와 반복횟수를 결정하였다. 그리고 투과함수 H_{kl}의 한 화소가 바뀔 때마다 재생된 영상함수 값의 변화는 푸리에 역변환 대신 그 순간의 변화량만을 가감하여 많은 시간을 절감하였다. 이를 수식으로 나타내면

$$h_{mn}^{new}=h_{mn}^{old}-tH_{kl}\exp\left(j2\pi\left(\frac{km}{N}+\frac{\ln}{N}\right)\right) \tag{5}$$

이다. 여기서 t는 현재 H_{kl}의 값과 다음에 나올 H_{kl}의 값에 따라 결정되며, m,n,k 그리고 l은 각각 $0,1,\cdots,N-1$ 범위의 값을 가지는 정수이며, $km+\ln$은 $2(N^2-2N+1)$의 범위를 갖는 정수이다. 그리고 지수함수는 사인함수와 코사인함수의 합으로 표시되므로 주기 N인 삼각함수를 미리 계산하여 N개의 배열에 저장시켜 반복과정 중 호출하여 사용함으로써 계산시간을 절감했다. 이와 같이 구한 투고함수 H_{kl}

이 워터마크 함수가 되며 $W(k,l)$로 표현한다.

2.2 워터마크의 암호화

은닉영상의 홀로그램정보인 워터마크함수 $W(k,l)$를 호스트영상에 삽입하기 전에, 암호화 과정을 수행한다. 워터마크 함수는 64×64개의 1 또는 '-1'의 이진값을 가진다. 워터마크로 사용되는 홀로그램은 그 정보의 일부를 잃어도 은닉영상을 복원할 수 있는 성질이 있으므로 정보의 전송과정에서 생길 수 있는 각종 잡음 및 외부 공격 등에 상당히 견실하다. 이를 암호화하기 위하여 랜덤하게 발생시킨 행 방향 키를 이용하여 BPCGH를 1차 스크램블 연산을 한 뒤, 랜덤하게 발생시킨 열 방향 키를 이용하여 2차 스크램블한다. 두 번의 스크램블 연산을 하게 되면 원래 영상의 형태와 전혀 다른 암호화된 새로운 영상을 구할 수 있다. 스크램블 연산을 통한 암호화 과정을 그림 3에 나타내었다. 그림 3의 예에서는 테스트 영상을 가로 및 세로 방향으로 5개의 블록으로 나눈 후, 이에 대한 행 방향 및 열 방향 랜덤 키 정보를 발생시켜 스크램블 연산을 함으로써 홀로그램 정보를 암호화 시켰다. 이를 수식으로 표현하면 다음과 같다.

$$W_E(k,l) = Scramble_{xy}oper.[W(k,l)], \quad 1 \le k,l \le K,L \tag{6}$$

여기서 K과 L은 가로 및 세로 방향의 블록 수를 의미한다.

이때 행 방향 키 정보와 열 방향 키 정보는 워터마크의 복호화 과정에서 반드시 필요하게 된다.

2.3 워터마크의 삽입

암호화된 워터마크 $W_E(k,l)$는 호스트영상 $f(x,y)$의 DCT영역에서 적절한 가중치를 가지고 삽입된다. 이를 위해 먼저 호스트영상을 겹치지 않는 8×8블록으로 분리한 후 DCT를 취한다. 이를 표현하면 다음과 같다[4].

$$f(x,y) = \bigcup_{k=1}^{K}\bigcup_{l=1}^{L} f_{kl}(x',y'),\ 1 \le x',y' \le 8 \tag{7}$$

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

여기서 매개변수 k,l은 전체영상에서 가로 및 세로 방향의 블록 위치를 의미하고, K,L은 가로 및 세로 방향의 블록의 수를 의미한다. x',y'은 공간영역에서의 블록 내 매개변수를 의미하고, u,v는 DCT 영역 내의 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.

$$F_{kl}^{w}(u,v) = \begin{cases} F_{kl}(0,0) + \delta_{kl} \times W_E(k,l), & \text{if } u=v=0 \\ F_{kl}(u,v), & otherwise \end{cases} \tag{9}$$

$$\delta_{kl} = weight \times F_{kl}(0,0)$$

$$f^{w}(x,y) = \bigcup_{k=1}^{K}\bigcup_{l=1}^{L} IDCT[F_{kl}^{w}(u,v)] \tag{10}$$

여기서 $F_{kl}^{w}(u,v)$는 암호화된 워터마크가 삽입된 영상의 (k,l)번째 8x8 블록 크기의 DCT 함수를 의미하고, δ_{kl}는 그 블록의 DC성분을 고려한 가중치 함수를 의미하며, 변수 $weight$값에 의해 워터마크의 정보량이 결정된다. 그리고 $f^{w}(x,y)$는 워터마크가 삽입된 호스트영상을 의미한다. 제안하는 방법은 워터마크로 사용되는 은닉영상의 BPCGH정보를 반복하여 사

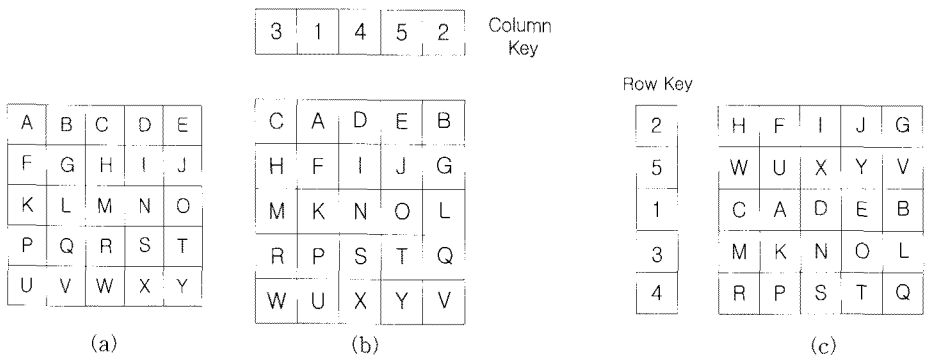


그림 3. 스크램블 기법을 이용한 암호화 과정
(a) 테스트 영상, (b) 열 방향 스크램블된 영상, (c) 열 방향 및 행 방향 스크램블된 영상

용하고, 암호화함으로써 절단과 같은 외부공격에 더 강한 성질을 가질 뿐만 아니라 정보보호 기능이 더 강화된 특징이 있다.

2.4 워터마크의 추출 및 복호화

워터마킹된 호스트영상은 여러 외부의 공격을 받을 수 있고, 이로 인해 워터마크 추출이 어려워 불법 복제 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.

$$W'_E(k,l) = [F^w_{kl}(0,0) - F_{kl}(0,0)] \times \frac{1}{\delta_{kl}} \tag{11}$$

추출된 결과는 다시 두 개의 키 정보를 이용하여 디스크램블 연산을 하여 복호화 한다.

$$W_D(k,l) = Descramble_{xy}oper.[W'_E(k,l)] \tag{12}$$

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.

$$c(x,y) = IFT\{W(k,l)\} \otimes IFT\{W_D(k,l)\} \tag{13}$$

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

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 512×512화소를 가지는 Lena, Baboon 및 Barbara 영상이며, 워터마크는 64x64 크기의 은닉영상인 영문자 'GJU'에 대해 설계한 BPCGH 패턴이다. 제안된 방법의 성능 측정을 위해 JPEG압축, 가우시안 잡음 및 절단과 같은 외부공격에 대한 견실성을 상관을 통해 측정하였다. 그리고 워터마크가 삽입된 영상의 비가시성을 측정하기 위해 PSNR(Peak Signal to Noise Ratio)을 이용하였다.

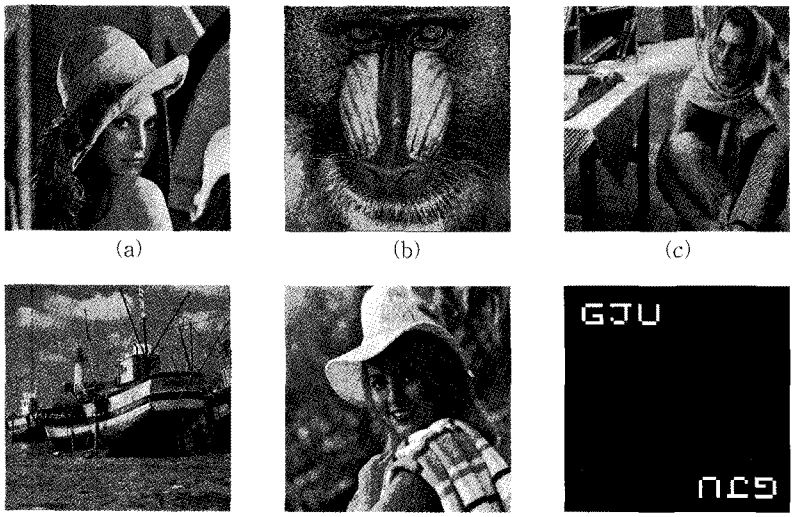
$$PSNR = 20\log_{10}(255/RMSE) \tag{14}$$

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

여기서 M, N은 호스트영상의 x축 및 y축의 크기를 나타낸다. 그림 4는 성능 측정에 사용된 세 개의 호스트영상과 은닉영상을 나타낸다. 그림 5는 Lena 영상에 대한 8×8 블록 DCT 영상 및 DC 성분을 나타낸다. 그림 5(b)와 같은 DCT의 DC 성분에 암호화된 워터마크 정보를 삽입한다.

본 논문에서는 은닉영상에 대한 최적의 BPCGH를 설계하기 위해 SA 알고리듬을 이용하였다. SA알고리듬에서는 비용함수와 사용되는 매개변수들의 값들에 의해 그 성능이 결정되는데, 비용함수는 반복횟수의 초기에는 일시적으로 증가할 수 있지만, 반복횟수의 증가에 따라 그 값이 감소하여야 한다. SA 알고리듬에서 사용된 매개변수인 초기온도 T_{init}는 1.0, 냉각속도D_t는 0.91, 그리고 반복 횟수 N는 100회로 하였다. 그림 6은 반복횟수의 증가에 따라 비용함수가 변화하는 모양과 SA 알고리듬에 의해 설계된 최적의 BPCGH 패턴을 나타낸다.

은닉영상에 대한 BPCGH는 스크램블 연산에 의해 다시 암호화 되며 이를 그림 7에 나타내었다. 그림 7(a)는 BPCGH를 열 방향으로 8개의 블록으로 나눈 후, 스크램블한 결과 영상을 나타내고, 그림 7(b)는 그림 7(a)을 다시 행 방향으로 8개의 블록으로 나눈 후, 스크램블 연산을 통해 구한 결과 영상을 나타낸다. 즉 그림 7(b) 영상이 BPCGH에 대해 최종적으로 암호화된 영상을 의미한다. 암호화된 영상은 원래의 BPCGH와는 전혀 다른 형태의 영상이며, 스크램블

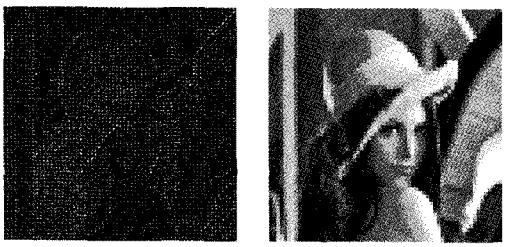


(a) (b) (c)

(d) (e) (f)

그림 4. 호스트영상과 은닉영상

(a) 호스트영상(Lena; 512×512), (b) 호스트영상(Baboon; 512×512), (c) 호스트영상(Barbara; 512×512), (d) 호스트영상(Boat; 512×512), (e) 호스트영상(Elaine; 512×512), (f) 은닉영상(이진영상; 64×64)

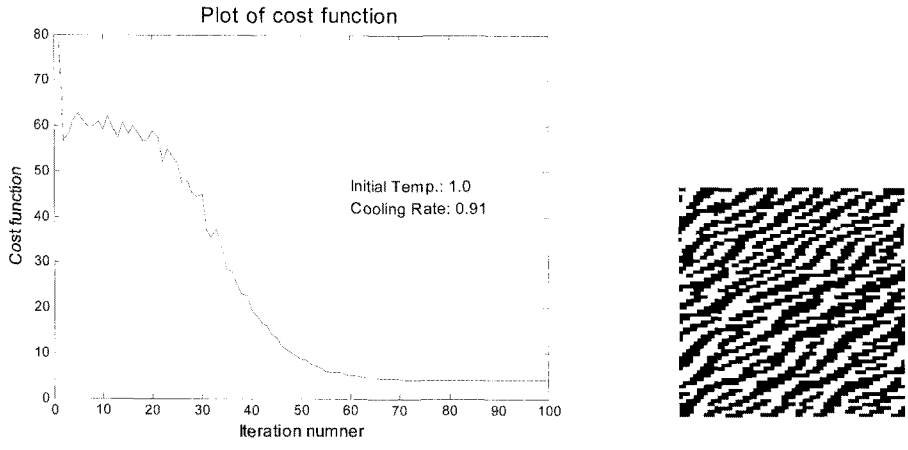


(a) (b)

그림 5. 호스트영상의 DCT 결과 영상

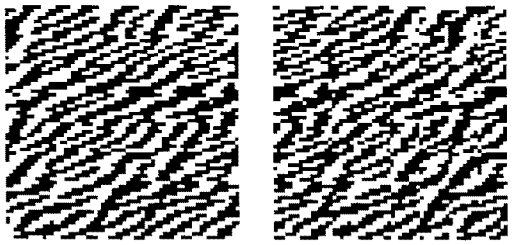
(a) Lena영상의 8×8 블록 DCT결과(512×512), (b) DCT 결과의 DC 성분(64×64)

연산에 사용된 열 방향 및 행 방향의 키 정보가 없으면 복원할 수 없다. 그림 5(b)와 같은 DCT의 DC 성분에 그림 7(b)의 암호화된 BPCGH정보를 적절히 삽입한 후, IDCT변환을 수행함으로써 워터마크된 호스트영상이 구해진다. 제안된 방법은 은닉영상의 BPCGH정보를 암호화하여 워터마크로 사용하였으므로, 각종 외부공격에 강할 뿐만 아니라 암호화과정도 포함하고 있으므로 기존에 제안된 많은 디지털 워터마킹 기술에 비해 정보보호기능이 강화되었다고 할 수 있다.



(a) (b)

그림 6. 비용함수 및 BPCGH (a) 비용함수, (b) BPCGH



(a) (b)

그림 7. 스크램블 암호화 과정
(a) 열 방향 키 정보에 의해 스크램블된 BPCGH, (b) 열 방향 및 행 방향 키 정보에 의해 스크램블된 BPCGH(암호화된 BPCGH)

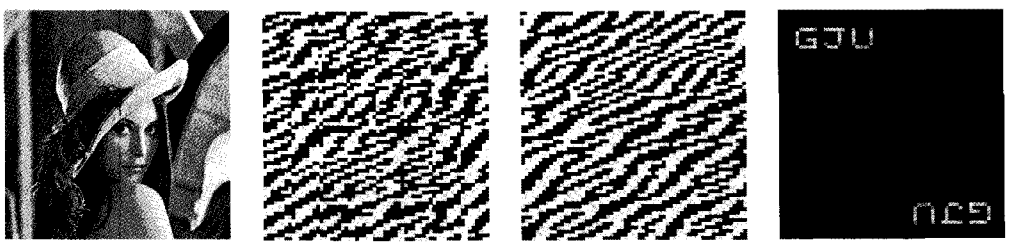
컴퓨터 시뮬레이션을 통해 각종 공격에 대한 PSNR 값과 추출된 워터마크의 검증을 위한 상관결과 값은 표 1과 같으며, 이들 값들은 5회 반복 실험한 결과를 평균한 것이다. 이는 스크램블 암호화과정에서 랜덤하게 발생시킨 키 정보의 평균을 얻기 위해서이다. 그리고 이때 워터마크의 정보량을 결정하는 가중치(*weight*)값은 워터마킹된 호스트영상의 화질이 비교적 양호하면서 PSNR 값이 40이상 유지되도록 하기위해 0.015로 두었다.

표 1의 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 7은 워터마킹이 삽입된 호스트영상, 추출된 워터마크영상, 디스크램블 연산에 의해 복호화된 워터마크영상, 그리고 최종적으로 재생된 은닉영상의 결과를 보여준다. 그림 8에서 재생된 은닉영상인 8(d)와 그림 4(d)의 원래의 은닉영상과 거의 차이가 없음을 알 수 있다. 이 두 영상의 상관을 계산하여 워터마크의

표 1. 외부공격에 대한 PSNR측정 및 상관결과

PSNR 및 상관첨두치 \ 외부공격		워터마킹 삽입	JPEG 압축*)	JPEG압축+ 가우시안 잡음**)	JPEG압축+가우시안 잡음+절단***)
PSNR (dB)	Lena	41.769	36.892	31.158	31.090
	Baboon	41.058	27.484	25.843	25.981
	Barbara	42.220	32.026	29.259	29.122
	Boat	41.915	32.936	29.816	29.793
	Elaine	41.073	32.135	29.024	29.123
정규화된 상관 첨두치	Lena	1.000	0.866	0.778	0.601
	Baboon	1.000	0.914	0.807	0.638
	Barbara	1.000	0.813	0.705	0.596
	Boat	1.000	0.772	0.713	0.571
	Elaine	1.000	0.908	0.818	0.668

*) 압축률(Lena; 88%, Baboon; 73%, Barbara; 83%, Boat; 98%, Elaine; 99%)
**) 가우시안 잡음(zero mean one variance): 20%
***) 절단율: 25%



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

그림 8. 워터마크 추출결과
(a) 워터마크 삽입된 호스트영상(512×512), (b) 추출된 워터마크(64×64), (c) 복호화된 워터마크(64×64), (d) 재생된 은닉영상(64×64)

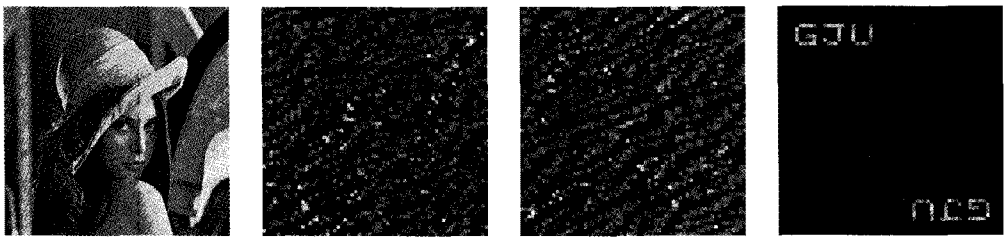
존재여부를 결정한다.

그림 9, 10, 11에서는 외부의 다양한 공격들이 누적되어 들어왔을 경우 제안한 디지털 워터마킹 기술이 워터마크의 추출 및 존재여부를 검증할 수 있음을 보여준다. 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 가중치 값을 조정하면 비가시성 및 워터마크 검증에 좀 더 유연하게 대응할 수 있다.

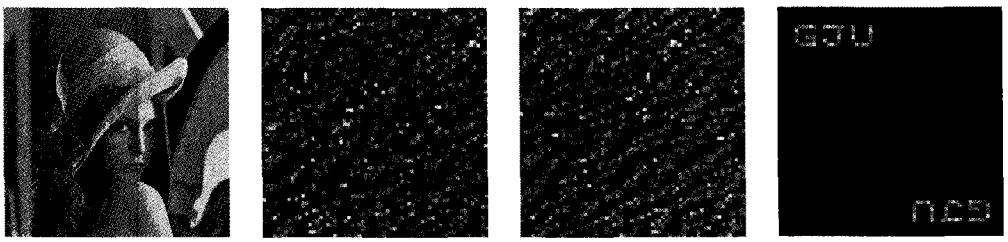
4. 결 론

본 논문에서는 홀로그램을 이용하는 디지털 워터



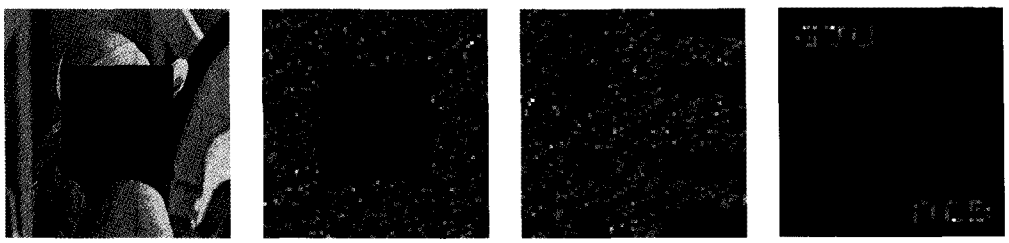
(a) (b) (c) (d)

그림 9. 압축 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(88%)된 호스트영상(512×512), (b) 추출된 워터마크(64×64), (c) 복호화된 워터마크(64×64), (d) 재생된 은닉영상(64×64)



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

그림 10. 압축 및 가우시안 잡음 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(88%) 및 가우시안 잡음(20%)이 첨가된 호스트영상(512×512), (b) 추출된 워터마크(64×64), (c) 복호화된 워터마크(64×64), (d) 재생된 은닉영상(64×64)



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

그림 11. 압축, 가우시안 잡음 및 절단 공격에 따른 워터마크 추출 결과
(a) JPEG 압축(88%), 가우시안 잡음(20%) 및 절단(25%) 호스트영상(512×512), (b) 추출된 워터마크(64×64), (c) 복호화된 워터마크(64×64), (d) 재생된 은닉영상(64×64)

마킹 기술과 스크램블링 암호화 기법을 동시에 사용하는 정보보호 강화 방안을 제안하였다. 즉 워터마크로 사용될 은닉영상의 BPCGH를 설계하고, 스크램블 연산을 통해 암호화한 후, 호스트영상의 DCT영역에서 DC성분에 적절하게 삽입하는 디지털 워터마킹 기술이다. 제안된 워터마킹 기술은 은닉영상의 홀로그램 정보를 이용하고, 암호화 과정을 거쳤으며, 이진 값을 가지므로 각종 외부 공격이 동시에 누적되어 들어 오더도 워터마킹 정보를 추출하고, 검증할 수 있는 장점이 있음을 당양한 영상들에 대한 컴퓨터 시뮬레이션을 통해 확인하였다. 그리고 스크램블링 암호화 시에 사용된 두 개의 키 정보를 알지 못하면 워터마크 정보의 추출이 불가능하므로 정보보호 기능이 강화되었다고 할 수 있다. 앞으로 제안한 디지털 워터마킹 기술을 보완하여 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] 김철수, "이진위상 컴퓨터형성홀로그램과 다중 XOR연산을 이용한 영상 암호화의 개선,"한국산업정보학회논문지, 제13권 3호, pp. 110-116, 2008.

[2] 김승열, 유영갑, "다수의 영상에 대한 스크램블 및 디스크램블 방법," 한국콘텐츠학회논문지, Vol.6, No.6, pp. 50-55, 2006.

[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] 김영식, 권오형, 박래홍, "웨이브릿 영역에서의 디지털 영상 워터마킹 방법," 대한전자공학회논문지, 제36권, S편, 제12호, pp. 1413-1419, 1999.

[6] 김정연, 남제호, "DCT 압축영역에서의 DC 영상 기반 다해상도 워터마킹 기법," 대한전자공학회논문지, 제45권, SP편, 제4호, pp. 1-9, 2008.

[7] 김병열, 서동환, 조규보, 신창목, 김수중, 김철수, "이진 위상 홀로그램과 광학적 간섭계를 이용한 디지털 워터마킹," 한국광학회논문지, 제14권, 4호, pp. 377-382, 2003.

[8] 김규태, 김종원, 김수길, 최종욱, "비축 홀로그램을 이용한 디지털 워터마킹," 대한전자공학회논문지, 제41권, SP편 제3호, pp. 183-194, 2004.

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

[10] 이강현, "디지털 영상의 다중 하위 비트플랜에 삽입되는 워터마크," 대한전자공학회논문지, 제43권, CI편, 제6호, pp. 101-109, 2006.

[11] 조규보, 신창목, 김수중, "컴퓨터 형성 홀로그램과 광전자적 추출 알고리즘을 이용한 디지털 워터마킹 방법," 한국광학회논문지, 제17권, 1호, pp. 31-37, 2006.

[12] 김철수, "DCT영역에서 컴퓨터형성홀로그램을 이용한 디지털 영상 워터마킹 기술", 경주대학교 정보전자기술논총, 제7권, pp. 37-48, 2008.

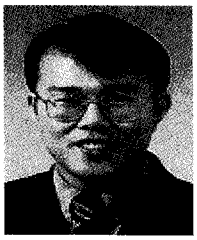
[13] 최현준, 서영호, 유지상, 김동욱, "홀로마킹: Fresnel 홀로그램을 이용한 디지털 워터마킹 기법," 한국통신학회논문지, 제34권, 6호, pp. 604-610, 2009.

[14] 이 덕, 김종원, "다단계 유통 추적을 위한 DWT-SVD 기반의 홀로그래피 포렌식마크," 한국통신학회논문지, 제35권, 2호, pp. 155-160, 2010.

[15] 김희정, 서용수, 김지홍, "POCS 이론을 이용한 인간시각시스템기반 디지털 워터마킹," 한국멀티미디어학회논문지, 제8권, 4호, pp. 516-524, 2005.

[16] 김동현, 최인호, "웨이블릿영역에서 영상융합에 의한 영상 워터마킹 기법," 한국멀티미디어학회논문지, 제11권, 4호, pp. 443-453, 2008.

[17] 배성호, "히스토그램 이동을 이용한 고용량 리버서블 워터마킹," 한국멀티미디어학회논문지, 제13권, 1호, pp. 76-82, 2010.



김 철 수

1985년 2월~1989년 2월 경북대학교 전자공학과 공학사
1989년 3월~1991년 2월 경북대학교 전자공학과 공학석사
1991년 3월~1997년 2월 경북대학교 전자공학과 공학박사
1995년 3월~1998년 2월 김천대학교 전자통신과 전임강사
1998년 3월~2010년 9월 경주대학교 컴퓨터정보공학과 교수
2008 년 2월~2009년 1월 미국 Univ. of Connecticut 방문연구교수
2010년 11월~현재 경북대학교 IT대학 연구원
관심분야 : 광신호처리, 3D 디스플레이, 광암호화, 워터마킹, 뇌-컴퓨터인터페이스 등