Journal of Korea Multimedia Society Vol. 10, No. 5, May 2007(pp. 569-582)

Buyer-Seller 워터마킹 프로토콜 상에서 POCS 기반의 디지털 워터마킹

권성근[†], 이지혜[††], 이석환[†††], 권기룡[††††]

요 약

디지털 콘텐츠의 저작권 보호와 불법 복제 및 배포 방지를 위한 기법인 디지털 워터마킹 기술은 'Buyer-Seller 워터마킹 프로토콜'과 같은 암호학적인 프로토콜과의 결합을 통해 전자상거래 상에서 구매자와 판매자 모두에게 신뢰할 만한 계약절차를 제공할 수 있다. 최근 워터마킹 기법의 이용을 전제로 한 여러 암호학적 프로토콜들이 연구되고 있으나, 프로토콜 내 워터마킹 기법의 실제 적용 및 구현 방법에 대해서는 언급이 전무한 실정이다. 본 논문에서는 Buyer-Seller 워터마킹 프로토콜 상에서 POCS 기반의 워터마크 삽입 방법을 제안한다. 제안한 방법에서는 EZW에 기반한 견고성 볼록 집합과 PSNR 비가 우수한 비가시성 볼록 집합을 정의한 후 이들 두 집합으로 수렴조건을 만족할 때 까지 반복 투영시킨다. 실험결과로부터 제안한 방법이 기존의 방법에 비하여 다양한 공격에 대한 BER이 0.02-0.10정도 낮음을 확인하였다.

POCS Based Digital Watermarking in Buyer-Seller Watermarking Protocal

Seong-Geun Kwon[†], Ji-Hye Lee[††], Suk-Hwan Lee[†††], Ki-Ryong Kwon[††††]

ABSTRACT

Digital watermarking technique for copyright protection and prevention of illegal copy and distribution can provide the reliable transaction to both buyer and seller in e-commerce through the cryptographic protocol such as 'Buyer-seller watermarking protocol'. Recently there has been researched about some cryptographic protocols for watermarking system but there has no yet mentioned about the implementation of practical watermarking technique in protocol. This paper presents the watermark embedding technique based on POCS in buyer-seller watermarking protocol. The proposed method designs the robust convex set based on EZW and the invisible convex set using PSNR and then projects into two sets until the convergence condition is satisfied. Experimental results verified that BER of watermark that is embedded by the proposed method has lower 0.02-0.10 than BER of the conventional method.

Key words: Digital Watermarking(디지털 워터마킹), Buyer-Seller Watermarking Protocol(판매자-구매자 워터마킹 프로토콜), POCS(POCS)

※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산시 남구 대연3동 599-1 부경대학교(608-737), 전화 : 051)620-6495, FAX : 051)620-6390,
E-mail : krkwon@pknu.ac.kr
접수일 : 2007년 1월 18일, 완료일 : 2007년 3월 20일
[†] 정회원, 삼성전자 무선사업부
(E-mail : seonggeunkwon@hanmail.net)
[††] 부산외국어대학교 전자컴퓨터공학과
(E-mail : queenka1025@yahoo.co.kr)
[†††] 정회원, 동명대학교 정보보호학과
(E-mail : skylee@tit.ac.kr)
[††††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부
※ 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10260-0) 및 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음

1. 서 론

디지털 워터마킹은 소유권자 혹은, 저자의 정보를 음악 파일, 이미지, 동영상과 같은 디지털 콘텐츠 내에 은닉함으로써 콘텐츠의 정상적인 배포 후 합법적 사용자에 의한 불법 복제물이 발견될 때, 해당 콘텐츠 내에 삽입된 소유권자 혹은 저자 정보 추출 과정을 통해 저작권을 보호하는 기법이다[1-3]. 이와 같은 디지털 워터마킹과 더불어 실제 전자상거래 상에서 구매자와 판매자 서로가 신뢰할 수 있는 계약절차를 제공하는 암호학적 프로토콜 또한 함께 연구되어 왔다. 초창기 대칭형 핑거프린팅 프로토콜[4]에서는 구매자와 판매자 모두 핑거프린팅된 콘텐츠에 접근이 가능하므로 불법 배포자가 구매자인지 아니면 판매자인지를 명확히 가려낼 수 없는 문제점(customer's right problem)을 가지고 있다. 따라서, 이러한 문제점을 해결하고자 비대칭형 프로토콜이 제안되었다[5-7]. 이 기법들은 핑거프린팅된 콘텐츠를 오직 구매자만이 접근할 수 있도록 설계하여 대칭형 프로토콜에서 문제되었던 불법 배포에 대한 책임소재를 분명히 가려낼 수 있다. 하지만 이 기법 역시 원본 콘텐츠와 불법 배포 콘텐츠와의 비교를 통해 구매자가 핑거프린팅 정보 획득이 가능하며, 판매자가 불법 배포의 책임이 있는 구매자의 또 다른 콘텐츠에 추출된 핑거프린팅 정보를 삽입할 수 있는 문제점 (unbinding problem)을 가지고 있다. Lei 등[8]은 판매자가 불법 배포 콘텐츠에서 핑거프린팅 정보를 획득하더라도 이를 사용하지 못하도록 구매자의 익명성을 보장하는 익명인증기관과 일회용 공개키 기반의 Buyer-Seller 워터마킹 프로토콜을 설계하였다.

위에서 언급한 암호학적 프로토콜들은 구매자의 정보를 해당 콘텐츠와 결합시키기 위해 디지털 워터마킹 기법을 이용하고 있다. 여기서 암호학적 프로토콜 상에서의 디지털 워터마킹 기법은 기존의 워터마킹 기법과는 달리 공개키 기반의 암호 시스템 상에서 콘텐츠와 워터마크의 암호화 처리 후, '준동형 특성(homomorphic property)'을 이용하여 결합 과정이 수행되어야만 한다. 즉, 정수의 대수적 특성에 기초하여 이루어지는 암·복호화 과정을 만족하기 위하여 콘텐츠와 워터마크를 정수 형태로 각각 암호화하여 이들을 결합하여야 한다. 기존의 워터마킹 기법에서는 견고성 및 비가시성 등의 요구사항들을 고려하여 공간 영역 상에서의 화소값보다 DCT, DFT 및 DWT 등의 주파수 계수에 워터마크를 삽입한다. 그러나 주파수 계수는 실수 형태로 존재하므로, 이를 암호화 영역 내에서 연산하기에는 적절하지 못하다.

본 논문에서는 공개키 기반의 Buyer-Seller 워터마킹 프로토콜 상에서 암호화 영역 내에서 암호화된 콘텐츠와 워터마크 정보를 삽입하는 방법을 제안한다. 제안한 워터마크 삽입 방법은 EZW (Embedded Zerotree Wavelet)에 기반한 견고성 볼록 집합과 PSNR 비가 우수한 비가시성 볼록 집합을 정의한 후 이들 두 집합으로 각각 투영시키는 POCS (Projection onto Convex Sets)에 기반한다. 여기서 견고성 볼록 집합은 암호화 영역 내에서의 준동형 특성을 만족하고 또한 EZW의 비중요 계수들이 다양한 공격에 강인하도록 정의된다. 그리고 비가시성 볼록 집합은 원하는 PSNR비를 가지도록 공간 영역 상에서 화소값들의 변경 제한 범위로 정의된다. 실험 결과로부터 제안한 방법이 기존의 방법에 비하여 삽입되는 워터마크 비트수가 많으므로 PSNR 측면에서 0-9dB 정도 낮았으나, 다양한 공격 실험에서 BER이 0.02-0.10정도 높음을 확인하였다.

본 논문의 구성을 살펴보면, 2장에서는 Buyer-Seller 워터마킹 프로토콜의 일반적인 구조와 해당 프로토콜의 기반이 되는 공개키 암호화 시스템의 특성 그리고 POCS에 대하여 간략히 살펴본다. 그리고 3장에서는 제안한 Buyer-Seller 워터마킹 프로토콜 상에서의 POCS 기반의 워터마크 삽입 방법을 살펴보고, 4장에서는 제안한 방법의 비가시성과 견고성에 대한 실험 결과 및 고찰을, 그리고 5장에서는 본 논문의 결론을 맺는다.

2. 기존 연구

2.1 Buyer-Seller 워터마킹 프로토콜

Buyer-Seller 워터마킹 프로토콜[8]에서는 그림 1에서와 같이 '구매자(buyer)'와 '판매자(seller)', 그리고 '워터마크 인증기관(watermark certification authority)'으로 구성된 3자의 프로토콜을 이루고 있다. 계약과정에서 각 구성원 간에 일어나는 일련의 절차들을 살펴보면 다음과 같다. 먼저 판매자의 보유 콘텐츠에 대한 구매 의사를 가진 구매자는 '공개키(pk_B)'와 '비밀키(sk_B)' 한 쌍을 생성한 후, pk_B를 인증

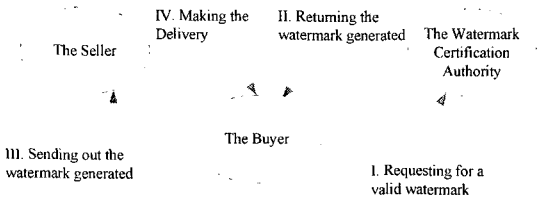


그림 1. Buyer-Seller 워터마킹 프로토콜 상에서의 구매절차

기관에 전달하며 워터마크의 생성을 요청한다(Ⅰ). 인증기관은 생성한 워터마크 w를 pk_B를 이용해 암호화 한 후, 암호화된 워터마크 $pk_B(w)$와 $pk_B(w)$의 유효성을 입증하는 '인증서명($Cert_{WCA}(pk_B)$)'을 구매자에게 제공한다(Ⅱ). 구매자는 전달받은 $pk_B(w)$와 $Cert_{WCA}(pk_B)$ 및 pk_B를 구매리스트와 함께 판매자에게 전송한다(Ⅲ). 판매자는 우선 $Cert_{WCA}(pk_B)$를 통해 $pk_B(w)$의 인증확인을 거친 후 워터마크의 유효함이 인정되면 구매리스트의 구매 콘텐츠를 pk_B를 이용해 암호화된 콘텐츠 $pk_B(contents)$를 생성한다. 그 후, $pk_B(contents)$와 $pk_B(w)$를 결합시킨 $pk_B(contents \cdot w)$를 구매자에게 전달하게 되고(Ⅳ), 이를 전달받은 구매자는 비밀키 sk_B를 이용해 $pk_B(contents \cdot w)$를 복호화함으로써 최종적으로 워터마크가 삽입된 콘텐츠를 획득한다. 이와 같은 일련의 구매절차에서는 오직 구매자만이 복호화 과정을 거친 워터마크 삽입 콘텐츠에는 접근할 수 있다. 따라서 불법으로 유통되는 콘텐츠의 적발시, 판매자는 불법 배포의 책임 추궁으로부터 자유로울 수 있다.

Buyer-Seller 워터마킹 프로토콜은 프로토콜의 진행 흐름에 따라 워터마크 생성 프로토콜과 워터마크 삽입 프로토콜, 분쟁 해결 프로토콜로 나뉘어진다. 여기서 워터마크 삽입 프로토콜은 워터마크와 콘텐츠간의 결합과 관련되며, 이의 흐름은 그림 2에서와 같다. 먼저, 구매자 측에서는 암·복호화 키 pk_B 및 sk_B를 생성한 후 삽입할 워터마크 w를 암호화 $E_{pk_B}(w)$한다. 판매자는 암호화된 워터마크 $E_{pk_B}(w)$와 pk_B를 구매자에게 전달받은 다음, 판매할 콘텐츠 영상 Im을 pk_B에 의하여 $E_{pk_B}(Im)$를 생성한다. 그리고 이를 공개키 암호화시스템의 준동형 (Homomorphic) 특성 ($E_{pk_B}(Im)+E_{pk_B}(w)=E_{pk_B}(Im+w)$)을 이용하여 선형 결합 $E_{pk_B}(Im+w)$한 후 구매자에게 전송한다. 암호화된 영상 $E_{pk_B}(Im+w)$를 전달받은 구매자는 이를 복호화 함수 $D_{sk_B}()$에 의하여 워터마크가 삽입된 콘텐츠를 획득하게 된다.

2.2 기존의 워터마킹

기존의 워터마킹 기법 중 먼저 Buyer-Seller 워터마크 프로토콜 상에서의 워터마크 삽입 방법을 살펴보기로 한다. Kuribayashi 등[9]은 Buyer-Seller 워터마크 프로토콜 상에서 처음으로 워터마크 삽입 방법을 제안하였다. 이 방법에서는 영상을 매크로 블록(16×16) 단위의 DCT를 수행한 후, 기존의 8×8 크기의 양자화 테이블을 보간하여 확장시킨 16×16 크기의 양자화 테이블을 이용하여 양자화한다. 이 때 양자화 DCT 계수를 워터마크 비트가 '1'인 경우에 최근접 홀수 값으로 변경하고, 워터마크 비트가 0인 경우에 최근접 짝수 값으로 변경한다. 이 방법은 양자화 과정을 거쳐 정수화된 주파수 계수를 사용하므로 암호화 영역 상에서 워터마크를 삽입할 수 있다. 그러나 재양자화 과정에 의하여 양자화 계수가 원래 값의 최근접 짝 또는 홀수로 변경되므로 일반적인 JPEG 압축공격 및 양자화 계수의 간단한 변경만으

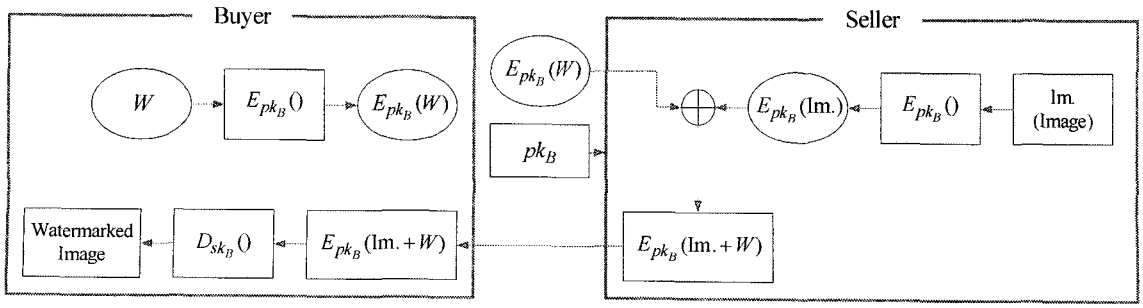


그림 2. 워터마크 삽입 프로토콜의 블록도

로도 쉽게 워터마크가 제거되는 단점이 있다.

본 논문에서는 Buyer-Seller 워터마크 프로토콜 상에서 강인하고 비가시성이 우수한 워터마크를 삽입하기 위하여 EZW [10]상에서 POCS 기반의 워터마크 삽입 방법을 제안한다. 우선 기존의 EZW 상에서의 워터마킹 기법을 간략히 살펴보기로 한다. Inoue 등[11]은 DWT 상의 EZW 알고리즘에 정의된 제로트리에 의해 비중요 계수와 중요 계수로 웨이브릿 계수를 분류한 후 워터마크를 비중요 계수 또는 중요 계수에 삽입한다. 비중요 계수에 대한 워터마크 삽입 방법으로는 우선 LH, HL, HH 중 임의의 방향 대역 내의 1,2,3 레벨을 선택하여 문턱치 $T=\alpha C_{\max}$을 계산한다. 여기서 $C_{\max}$은 선택된 대역 내의 최대 계수치를 나타내고, α는 $0.01<\alpha<0.1$이다. 문턱치 T에 의하여 워터마크 삽입 비트수만큼 제로트리 집합 $Z_1, Z_2, \cdots, Z_N$를 구한 다음 워터마크 비트 $w(k)_{k=1,2,\cdots,N}$가 0일 때, 제로트리 Z_k 내의 모든 계수값들을 $-m$으로, 워터마크 비트 $w(k)$가 1일 때 m로 변경한다. 중요 계수에 대한 워터마크 삽입 방법으로는 최상위 레벨의 LH, HL, HH 중 임의의 대역 내에서 중요계수를 $T_1<|C_k|<T_2$, $T_2>T_1>\alpha C_{\max}$에 의하여 찾는다. 워터마크 비트 $w(k)$가 0이면 $|C_k|=T_2$, 1이면 $|C_k|=T_1$로 한다. 이 방법은 실수 연산에 의하여 워터마크를 삽입하므로 암호화 영역 내에서는 적용되지 못한다.

2.3 POCS 이론

워터마킹 시스템의 필요 조건에는 견고성, 비가시성 및 용량성 등이 있다. 이들 조건들은 서로 상호 교환 (trade-off)적이다. 기존의 워터마킹 방법에서는 이들 조건을 만족하기 위하여 공간 영역 또는 변환 영역 상에서 견고성이 우수한 계수에 비가시적으로 워터마크를 삽입한다. 그러나 이 두 성질을 만족하는 조건들이 상호 의존적이다. Lee 등[12]은 POCS에 기반한 3D 메쉬 모델 워터마킹 기법을 제안하였다. 이 방법에서는 3D 메쉬 모델의 꼭지점 밀도에 대한 견고성 집합과 각 꼭지점의 이동 범위에 대한 비가시성 집합을 각각 독립적으로 설계한 후, 반복 투영 과정에 의하여 이 두 조건을 동시에 만족하는 하나의 수렴점을 찾는다.

본 논문에서는 위의 방법들을 이용하여 Buyer-Seller 워터마킹 프로토콜 상에서의 워터마킹 기법을 제안한다. 본 절에서는 POCS 이론에 대하여 간략히 살펴본다. $NH\times NV$ 크기의 영상 $\boldsymbol{f}$은 $NH\times NV$ 길이의 벡터로 표현되며, 이는 힐버트 공간 $\mathbf{H}$ 상에서의 원소라 가정한다. $\mathbf{H}$상에서 m 개의 닫힌 볼록 집합 (Closed convex set) $C_i\,(i=1,2,\cdots,m)$이 정의되어지고 이들 집합으로 n회 투영된 영상 $\boldsymbol{f}_n$은

$$\boldsymbol{f}_n=P_nP_{n-1}\cdots P_1\boldsymbol{f}_{n-1},\ n=1,2,\cdots \tag{1}$$

이다. 여기서 초기 벡터 $\boldsymbol{f}_0$은 원 영상 $\boldsymbol{f}$이고, 볼록 집합 C_i은 서로 공집합이 아니다. 임의의 집합 C_i 상으로의 투영기 P_i는

$$\|\boldsymbol{f}-P_i\boldsymbol{f}\|=\min_{g\in C_i}\|\boldsymbol{f}-\boldsymbol{g}\| \tag{2}$$

와 같이 정의되며, $\boldsymbol{g}$는 $\boldsymbol{f}$의 투영된 영상이다. 이들 집합으로 반복 교대 투영 과정에 의하여 $\boldsymbol{f}$은 교집합 $C_0=\cap_{i=1}^{m}C_i$의 한 원소로 수렴한다. POCS에 기반한 워터마킹에서 가장 주요한 사항은 원하는 워터마크된 영상의 모든 특성을 닫혀진 볼록 집합으로 표현하는 것이다. 제안한 방법에서는 두 개의 닫힌 볼록 집합인 견고성 집합 C_R 및 비가시성 집합 C_I을 각각 정의한 후, 수렴 조건을 만족할 때까지 영상 $\boldsymbol{f}$를 두 집합으로 반복 투영한다. 위의 과정에 의하여 최종 수렴되는 벡터는 이들 집합의 교집합 성분인 $\boldsymbol{f}^*$이며, 이는 워터마크가 삽입된 영상이다. 여기서 원 영상 $\boldsymbol{f}$은 비가시성 볼록 집합 C_I에 속해 있으므로, 투영 순서는 $\boldsymbol{f}_n=P_IP_R\boldsymbol{f}_{n-1}$이다.

3. 제안한 워터마킹 알고리즘

3.1 POCS 기반의 워터마크 삽입 개요

본 논문에서는 Buyer-Seller 워터마킹 프로토콜 상에서 EZW 구조의 웨이브릿 변환을 이용한 POCS 기반의 워터마크 삽입 방법을 제안한다. 제안한 워터마크 삽입 과정에서는 우선 비가시성 볼록 집합 C_I 및 견고성 볼록 집합 C_R를 정의한 다음, 그림 3에서와 같이 판매자 단에서 구매자로부터 전달된 암호화된 워터마크 $E_{pk_B}(W)$를 견고성 볼록 집합 내에 투영함으로써 삽입한다. 즉, 수렴 조건을 만족할 때까지 두 볼록 집합으로 반복 투영함으로써 워터마크가 삽입된 영상 $Im.+E_{pk_B}(W)$을 획득한 후, 이를 키 pk_B에

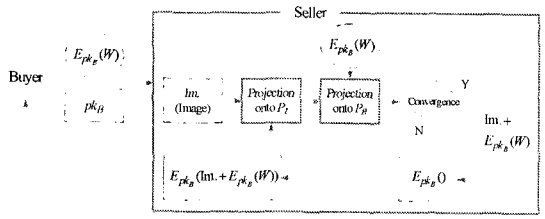


그림 3. 판매자단에서 제안한 워터마크 삽입 과정

의하여 암호화 $E_{pk_B}(Im.+E_{pk_B}(W))$하여 구매자에게 전달한다. 이 때 비가시성 볼록 집합 C_I은 사용자가 원하는 PSNR를 만족하도록 설계된다. 그리고 견고성 볼록 집합 C_H은 EZW 상에서 비중요 계수 (Insignificant Coefficients)가 워터마크 $E_{pk_B}(W)$에 따라 견고성을 가지는 범위 내에 변경되도록 설계되어진다. 이 때 암호화 영역에서 정수 연산이 가능하도록 ISC 계수를 양자화 과정을 수행한 후, 이를 워터마크 $E_{pk_B}(W)$에 따라 변경한다. 영상 f를 제안한 방법에 의하여 정의된 C_I 및 C_H 집합으로 투영 과정은 다음과 같다.

1) 초기 벡터 f_0는 원 영상 f으로 한다.

2) 매 회 투영되는 벡터 f_n를 계산한다.

$$f_n = P_I P_H f_{n-1},\ n \geq 1$$

3) 수렴 조건을 만족할 때까지 2) 번을 반복 수행한다. 이 때 수렴 조건으로는 n회 투영된 벡터 f_n와 이전 투영된 벡터 f_{n-1}와의

$$MSE = \sqrt{\frac{1}{NV \cdot NH}\sum_{i=0}^{NV}\sum_{j=0}^{NH}(f_n(i,j)-f_{n-1}(i,j))^2} \leq 10^{-1}$$

이다.

다음 절에서는 EZW 상에서의 비중요 계수 선택에 대하여 살펴본 후, 이 계수에 워터마크를 삽입하기 위한 견고성 볼록 집합 및 PSNR에 따른 비가시성 볼록 집합을 차례로 살펴보기로 한다.

3.2 EZW 상에서의 삽입 대상 계수 선택

제안한 방법에서는 영상 f을 4-레벨 웨이블릿 변환한 후 각 대역별의 웨이블릿 계수들을 암호화 영역 내에서의 정수 연수를 위하여 양자화한다.

$$q_{l,f}(u,v) = floor\left(\frac{C_{l,f}(u,v)}{\alpha \cdot Q}\right) \quad (3)$$

여기서 $C_{l,f}(u,v)$는 (l,f) 부대역 내에 (u,v) 위치의 DWT 계수이고, $q_{l,f}(u,v)$는 $C_{l,f}(u,v)$의 양자화 계수이고 l은 레벨, f는 방향성을 나타낸다. α는 양자화 스케일 인자로 α가 클 경우에 견고하게 워터마크를 삽입할 수 있으나 화질이 열화될 수 있다. 제안한 방법에서는 견고성이 우수한 α를 설정하여 견고성 볼록 집합을 설계한 다음, 임의의 PSNR이 되도록 비가시성 볼록 집합을 설계한다. 양자화 테이블 값 Q는 Watson 등[13]에 의해 4-레벨 9/7탭 DWT 상에서 제시된 값으로, 표 1에서와 같다. 표 1에서 방향 1,2,3,4는 평탄, 수평, 수직, 대각선 방향을 나타낸다.

문턱치에 의하여 중요계수 및 비중요계수로 나눈다. 이때 문턱치는 각 대역별의 JND 값이다. 워터마크 삽입 계수를 결정하기 위해 (LH4, LH3, LH2), (HL4, HL3, HL2), (HH4, HH3, HH2) 내에서 임계치(threshold)를 주어 계수의 절대치가 주어진 문턱치 Th보다 작은 경우를 비중요계수(insignificant), 반대의 경우를 중요계수(significant)로 구분한다. 또한 비중요계수로 구성된 공간트리를 제로트리로 정의한다. 그림 4에서와 같이 웨이블릿 계수의 제로트리 구조의 특성인 부모계수에서 후손계수로 내려가면 내려 갈수록 계수의 값이 감소하는 것과 부모 계수의 값이 클 경우 후손 계수들 역시 값이 클 확률이 높으며, 부모계수의 값이 작을 경우 후손 계수들 역시 값이 작을 확률이 높은 웨이블릿 분해된 영상의 자기 상관성의 특성을 이용하여 워터 마크를 삽입한다.

표 1. 4레벨 9/7탭 DWT 상에서의 양자화 테이블

Orientation	Level			
	1	2	3	4
1	14.05	11.11	11.36	14.5
2	23.03	14.68	12.71	14.16
3	58.76	28.41	19.54	17.86
4	23.03	14.69	12.71	14.16

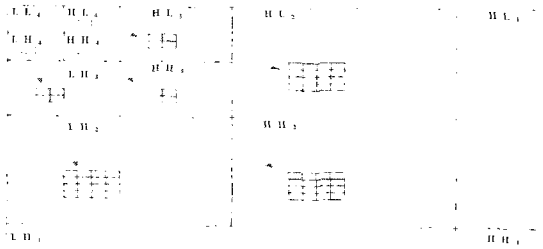


그림 4. 웨이브릿 계수의 제로트리 구조

3.2.2 견고성 볼록 집합

제안한 방법에서는 암호화된 워터마크 $E_{pk_B}(W)=\{w_i|i\in[1,N]\}$를 EZW 상에서의 양자화된 NISC 계수 트리에 삽입한다. 즉, 2,3,4 레벨의 양자화된 비중요 계수 트리 S_i는

$$S_i=\{q_{1,f}(u,v),\ q_{3,f}(2u+m,2v+n)_{m,n\in[0,1]},\ q_{2,f}(u,v)(2^2u+m,2^2v+n)_{m,n\in[0,3]}\} \quad (4)$$

와 같이 일련의 순서로 나열한다. 임의의 워터마크 비트 w_i는 19개의 계수로 구성된 비중요 계수 트리 S_i에 다음과 같이 각각 삽입된다.

IF $w_j=1$, Then $|q'_{l,f}(u,v)|=[\beta_{l,f}-\epsilon_{l,f},\beta_{l,f}+\epsilon_{l,f}]$
ELSE IF $w_j=0$,
Then $|q'_{l,f}(u,v)|=[\beta_{l,f}/2-\epsilon_{l,f},\beta_{l,f}/2+\epsilon_{l,f}]$

즉, 워터마크 비트에 따라 양자화된 계수 $q_{l,f}(u,v)$를 그림 5에서와 같이 두 영역 $[\beta_{l,f}-\epsilon_{l,f},\beta_{l,f}+\epsilon_{l,f}]$ 및 $[\beta_{l,f}/2-\epsilon_{l,f},\beta_{l,f}/2+\epsilon_{l,f}]$ 내로 변경한다. 여기서 $\epsilon_{l,f}$는 영역의 범위를 결정짓는 변수로 두 영역이 중복되지 않도록 $\beta_{l,f}/2+\epsilon_{l,f}<\alpha(\beta_{l,f}-\epsilon_{l,f})$와 $\beta_{l,f}/2-\epsilon_{l,f}>0$을 만족하도록 설정하여야 한다. 이를 전개하면

$$\beta_{l,f}/2+\epsilon_{l,f}<\alpha(\beta_{l,f}-\epsilon_{l,f}),\ \epsilon_{l,f}<\frac{\beta_{l,f}(\alpha-1/2)}{1+\alpha},\quad 1/2<\alpha<1 \quad (5)$$

$$\beta_{l,f}/2-\epsilon_{l,f}>0,\qquad \epsilon_{l,f}<\beta_{l,f}/2 \quad (6)$$

이므로, $\epsilon_{l,f}$는

$$\epsilon_{l,f}<\min\left(\frac{\beta_{l,f}(\alpha-1/2)}{1+\alpha},\beta_{l,f}/2\right)=\frac{\beta_{l,f}(\alpha-1/2)}{1+\alpha} \quad (7)$$

의 범위 내에 있다. 여기서 $\epsilon_{l,f}$의 값이 매우 작으면 견고성이 우수하나 반복 투영시 수렴되지 않을 수 있다. 따라서 제안한 방법에서는 $\epsilon_{l,f}$를 식 (7) 범위의 중간값 $\epsilon_{l,f}=\beta_{l,f}(\alpha-1/2)/(2+2\alpha)$으로 결정하였다. 이상과 같은 워터마크 삽입 조건을 만족하는 견고성 볼록 집합 C_R은

$$C_R=\{\boldsymbol{f}:|q'_{l,f}(u,v)|=[\beta_{l,f}-\epsilon_{l,f},\beta_{l,f}+\epsilon_{l,f}]\ \text{if}\ w=1,\ \text{or}\ |q'_{l,f}(u,v)|=[\beta_{l,f}/2-\epsilon_{l,f},\beta_{l,f}/2+\epsilon_{l,f}]\ \text{if}\ w=0\} \quad (8)$$

이다. $\beta_{l,f}$는 워터마크 삽입 강도로 레벨과 부대역의

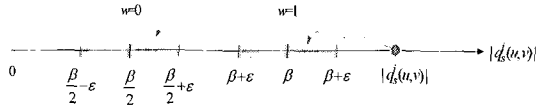


그림 5. 워터마크 삽입 조건

에너지 분포에 따라 적응적으로 결정되어야 한다. 제안한 방법에서는 $\beta_{l,f}$를 결정하기 위하여 각 대역별 분포를 구간 $S_{i\in[1,N]}$는

$$S_i=[\frac{MAX|q_{l,f}(u,v)|}{N}\times(i-1),\frac{MAX|q_{l,f}(u,v)|}{N}\times i],\quad 1\le i\le N \quad (9)$$

으로 분할한 다음, 각 구간에 속하는 웨이브릿 계수들의 개수 $n(S_i)_{i\in[1,N]}$를 구한다. 이들 구간의 개수들 중 중간값을 가지는 구간의 인덱스가 i일 때, $\beta_{l,f}$는

$$\beta_{l,f}=\frac{MAX|q_{l,f}(u,v)|}{N}\times(i+0.5) \quad (10)$$

이다. 영상 $\boldsymbol{f}$를 견고성 볼록 집합 C_R으로 투영시키는 가장 최적의 투영기 P_R

IF $w_j=1$, $|q_{l,f}(u,v)|=\beta_{l,f}$
ELSE $w_j=0$, $|q_{l,f}(u,v)|=\beta_{l,f}/2$

이다. 그러나 이는 비가시성 볼록 집합 C_I와의 교집합이 공집합될 수 있으므로, 이는 수렴 조건을 만족하지 않을 수도 있다. 따라서 제안한 방법에서는 $q_{l,f}(u,v)$를 워터마크 비트 w_i에 따른 목표치 X

$$X=\begin{cases}\beta_{l,f}, & \text{if}\ w_i=1\\ \beta_{l,f}/2, & \text{if}\ w_i=0\end{cases}$$

와의 선형 보간기에 의하여 아래와 같이 워터마크 삽입 범위 내 $[X-\epsilon_{l,f},X+\epsilon_{l,f}]$로 변경한다. 양자화된 계수의 절대치 $q_{l,f}(u,v)$가 목표치 X보다 클 경우에는 변경된 $q'_{l,f}(u,v)$는

$$|q'_{l,f}(u,v)|=\alpha|q_{l,f}(u,v)|+(1-\alpha)X\ ,\ |q_{l,f}(u,v)|>X \quad (11)$$

이며, $q'_{l,f}(u,v)$가 삽입 범위 $[X,X+\epsilon_{l,f}]$ 내에

$$X\le|q'_{l,f}(u,v)|=\alpha|q_{l,f}(u,v)|+(1-\alpha)X\le X+\epsilon_{l,f} \quad (12)$$

있어야 한다. 인자 α에 대하여 전개하면

$$0 \leqq \alpha \leqq \frac{\epsilon_{l,f}}{|q_{l,f}(u,v)|-X} \tag{13}$$

이다. 제안한 방법에서는 인자 α를 중간값 $\alpha=\frac{\epsilon_{l,f}}{2(|q_{l,f}(u,v)|-X)}$으로 결정하였다. 양자화된 계수의 절대치 $q_{l,f}(u,v)$가 목표치 X보다 작을 경우에는 변경된 $q'_{l,f}(u,v)$는

$$|q'_{l,f}(u,v)|=\alpha(X-\epsilon_{l,f})+(1-\alpha)|q_{l,f}(u,v)|,\quad |q_{l,f}(u,v)|<X \tag{14}$$

이며, 삽입 범위 $[X-\epsilon_{l,f}, X]$ 내에

$$X-\epsilon_{l,f} \leqq |q'_{l,f}(u,v)|=\alpha(X-\epsilon_{l,f})+(1-\alpha)|q_{l,f}(u,v)| \leqq X \tag{15}$$

있어야 하므로 이를 인자 α에 대하여 전개하면

$$\frac{X-|q_{l,f}(u,v)|-\epsilon_{l,f}}{X-|q_{l,f}(u,v)|} \leqq \alpha \leqq 1 \tag{16}$$

이다. 제안한 방법에서는 인자 α를 중간값 $\alpha=\frac{1}{2(X-|q_{l,f}(u,v)|)}$으로 결정하였다. 이를 정리하면 견고성 볼록 집합으로 투영기 P_R는

$$|q'_{l,f}(u,v)|=\begin{cases}\frac{\epsilon_{l,f}}{2(|q_{l,f}(u,v)|-X)}|q_{l,f}(u,v)|+(1-\frac{\epsilon_{l,f}}{2(|q_{l,f}(u,v)|-X)})X, & |q_{l,f}(u,v)|>X \\ \frac{1}{2(X-|q_{l,f}(u,v)|)}(X-\epsilon_{l,f})+(1-\frac{1}{2(X-|q_{l,f}(u,v)|)})|q_{l,f}(u,v)|, & |q_{l,f}(u,v)|<X\end{cases} \tag{17}$$

이다.

3.3 비가시성 집합

견고성 볼록 집합으로 투영시 워터마크의 비가시성을 고려하지 않았으므로, 화질의 열화가 발생된다. 따라서 제안한 방법에서는 비가시성 볼록 집합이 원영상 f와의 PSNR이 목표치 X[dB]

$$PSNR=10\log_{10}\frac{255^2}{MSE} \geqq X[\mathrm{dB}] \tag{18}$$

$$\text{where } MSE=\frac{1}{NH\cdot NV}\sum_{i=0}^{NH}\sum_{j=0}^{NV}\|f(i,j)-f'(i,j)\|^2$$

을 가지도록 설계한다. 우선 식 (16)을 MSE에 관하여 전개하면

$$MSE=\frac{1}{NH\cdot NV}\sum_{i=0}^{NH}\sum_{j=0}^{NV}\|f(i,j)-f'(i,j)\|^2 \leqq \frac{255^2}{10^{X/10}} \tag{19}$$

이 된다. 위 식의 조건을 만족하기 위하여 제안한 방법에서는 원 영상과 투영된 영상의 각 화소값의 차이가

$$\frac{1}{NH\cdot NV}\|f(i,j)-f'(i,j)\|^2 \leqq \frac{255^2}{10^{X/10}} \tag{20}$$

되도록 하며, 이를 다시 전개하면

$$|f(i,j)-f'(i,j)| \leqq \left(\frac{255^2\times NH\cdot NV}{10^{X/5}}\right)^{1/2} \tag{21}$$

이다. 따라서 비가시성 볼록 집합 C_I은

$$C_I=\left\{f' : |f(i,j)-f'(i,j)| \leqq \left(\frac{255^2\times NH\cdot NV}{10^{X/5}}\right)^{1/2}\right\} \tag{22}$$

이다. 여기서 $\left(\frac{255^2\times NH\cdot NV}{10^{X/5}}\right)^{1/2}=A$로 정의하기로 한다. 비가시성 볼록 집합 C_I으로 투영기 P_I는

$$f'(i,j)=\begin{cases}f(i,j)-A, & \text{if } f'(i,j)<f(i,j)-A \\ f(i,j)+A, & \text{if } f'(i,j)>f(i,j)+A \\ f(i,j), & else\end{cases} \tag{23}$$

이다.

3.4 워터마크 추출

워터마크가 삽입된 영상 $Im.+E_{pk_B}(W)$은 암호화 $E_{pk_B}(Im.+E_{pk_B}(W))$되어 구매자에게 주어진다. 구매자는 복호키를 이용하여 워터마크가 삽입된 영상을 획득하며, 이를 불법 배포되었을 때 판매자측에서는 워터마크 추출기에 의하여 암호화된 워터마크 비트 $E_{pk_B}(W)=\{w_i|i\in[1,N]\}$를 추출한다. 추출된 $E_{pk_B}(W)$는 인증 기관에 의하여 복호된다. 워터마크 추출은 견고성 볼록 집합에서 설계된 투영기 P_R 과정과 유사하다. 즉, 워터마크 비트 $\hat{w_i}$는 EZW 상에서의 식 (4)에 나타난 NISC 계수 트리 구조 내의 19개 계수값들을 $\hat{q_{l,f}}(au+m,av+n)$, $(a=1,m=n=0,\text{if } l=4,\ a=2,m,n\in[0,1],\text{if } l=3,\ a=4,m,n\in[0,3],\text{if } l=2)$ 워터마크 삽입 조건의 두 목표치 $\beta_{l,k}/2$와 $\beta_{l,k}$의 중간값 $3\beta_{l,k}/4$과 비교하여

$$\hat{w}_i=\begin{cases}1, \hat{q}_{l,f}(au+m,av+n)>3\beta_{k,l}/4\\ 0, \hat{q}_{l,f}(au+m,av+n)<3\beta_{k,l}/4\end{cases} \quad (24)$$

와 같이 추출한다. 그리고 최종 워터마크 비트 w_i^*는 총 19개의 워터마크 비트의 과반수에 의하여 추출된다.

4 실험 결과 및 고찰

Buyer-Seller 워터마킹 프로토콜 상에서 제안한 POCS 기반의 워터마킹 방법의 성능 평가를 위하여 본 실험에서는 512×512 크기의 Barbara, Lena, Baboon 영상을 사용하였다. 본 실험에서 사용된 워터마크는 영문 알파벳과 숫자들의 조합으로 이루어진 35문자를 8비트 확장 ASCII 코드의 이진 비트열로 변환시킨 후 각 비트들을 스크램블링함으로써 암호화된 280비트 길이의 스트림이다. 제안한 방법의 성능 평가를 위하여 워터마크의 비가시성 척도로 원영상과 워터마크가 은닉된 영상 사이의 PSNR을 사용하였고, JPEG 압축 및 다양한 영상처리 공격 실험을 통해 견고성을 평가하였다. 실험에 사용된 삽입 계수 결정하는 문턱치 Th는 JND 값으로 레벨 및 방향에 따라 Th_{LH4}= 23.03, Th_{LH3}=14.68, Th_{LH2}=12.71, Th_{HL4}=23.03, Th_{HL3}=14.69, Th_{HL2}=12.71, Th_{HH4}=58.76, Th_{HH3}=28.41, Th_{HH2}=19.54으로 사용하였다. 표 2, 3, 4를 살펴보면, (LH4,LH3,LH2) 영역 내에 삽입 가능한 워터마크 비트수는 Barbara일 경우 224 비트, Lena일 경우 291 비트, 그리고 Baboon일 경우 30 비트이다. 기존의 방법에 비하여 제안한 방법이 삽입되는 워터마크 비트수가 2-3배 정도 많음을 알 수 있다.

4.1 비가시성 실험

제안한 방법의 비가시성를 평가하기 위하여 기존의 방법과 PSNR을 비교하였다. 먼저 비가시성 볼록 집합에서 원하는 PSNR 비 X를 46 dB로 설정하여

표 2. Barbara영상의 각 밴드별 삽입 비트수 및 PSNR

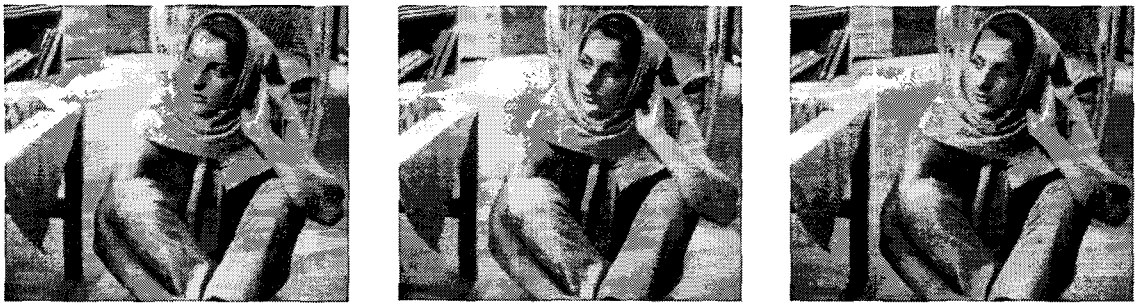
밴드	영상(Barbara)			
	H. INOUE Method		Proposed Method	
	비트수[bits]	PSNR[dB]	비트수[bits]	PSNR[dB]
(LH4,LH3,LH2)	84	54.77	231	48.36
(HL4,HL3,HL2)	105	51.21	273	46.38
(HH4,HH3,HH2)	168	50.39	336	49.08

표 3. Lena 영상의 각 밴드별 삽입 비트수 및 PSNR

밴드	영상(Lena)			
	H. INOUE Method		Proposed Method	
	비트수[bits]	PSNR[dB]	비트수[bits]	PSNR[dB]
(LH4,LH3,LH2)	210	50.70	294	48.66
(HL4,HL3,HL2)	336	48.68	315	50.38
(HH4,HH3,HH2)	378	49.15	483	49.84

표 4. Baboon 영상의 각 밴드별 삽입 비트수 및 PSNR

밴드	영상(Baboon)			
	H. INOUE Method		Proposed Method	
	비트수[bits]	PSNR[dB]	비트수[bits]	PSNR[dB]
(LH4,LH3,LH2)	21	67.72	105	58.28
(HL4,HL3,HL2)	42	63.82	147	53.79
(HH4,HH3,HH2)	126	54.42	168	51.64



(a) (b) (c)

그림 6. (a) Barbara 원 영상 (b) Inoue 방법의 워터마킹 영상 (c) 제안한 방법의 워터마킹 영상

(a) (b) (c)

그림 7. (a) Lena 원 영상 (b) Inoue 방법의 워터마킹 영상 (c) 제안한 방법의 워터마킹 영상

(a) (b) (c)

그림 8. (a) Baboon 원 영상 (b) Inoue 방법의 워터마킹 영상 (c) 제안한 방법의 워터마킹 영상

(a) (b) (c)

그림 9. (a) Barbara 영상의 삽입 가능 블록 (HL4,HL3,HL2), (b) Lena 영상의 삽입 가능 블록 (LH4,LH3,LH2), (c) Baboon 영상의 삽입 가능 블록 (HH4,HH3,HH2)

실험을 수행하였다. 이는 수렴 조건을 만족하기 위한 값이다. 표 2, 3, 4를 살펴보면, Babara 영상일 경우 기존의 방법은 50.39-54.77 dB이며 제안한 방법은 46.38-49.08 dB이다. Lena 영상일 경우 기존의 방법은 48.68-50.70 dB이나, 제안한 방법은 48.66-49.84 dB이다. 그리고 Baboon 영상일 경우 기존의 방법은 54.42-67.72 dB이나 제안한 방법은 51.64-58.28 dB이다. 즉 제안한 방법이 기존의 방법에 비하여 약 0-9 dB 정도 낮음을 알 수 있다. 이는 제안한 방법에 의하여 삽입된 워터마크 비트수가 기존의 방법에 비하여 2-3배 정도 많기 때문이다. 그리고 비가시성 볼록 집합의 설정 PSNR X를 46 dB 이상일 경우에 견고성 볼록 집합과의 수렴 조건을 만족하지 않는다. 기존의 방법 및 제안한 방법에 의하여 워터마크가 삽입된 Babara, Lena 및 Baboon 영상은 그림 6, 7, 8에서와 같다. 이 그림들을 살펴보면 원 영상과의 차이가 거의 없으므로, 워터마크가 비지각적으로 삽입됨을 볼 수 있다. 그림 9는 Babara, Lena 및 Baboon 영상에서 비중요 계수의 제로 트리 구조에 해당되는 위치의 블록을 나타내고 있다. 이 그림을 살펴보면, 고주파 성분이 많은 Baboon 영상에서는 Babara 및 Lena 영상에 비하여 워터마크가 삽입되는 블록이 많지 않음을 알 수 있다. 중요 계수 및 비중요 계수를 분류하는 문턱값은 영상에 따라 적절히 조절하면 삽입되는 워터마크수를 조절할 수 있을 것이다. 향후 본 연구에서는 X가 46 dB 이상일 때 수렴 조건을 만족하는 볼록 집합 설계가 필요하다.

4.2 견고성 실험

견고성 실험에서는 JPEG 압축과 일반적인 영상처리 공격에 대한 실험을 수행하였다. 다양한 화질인자 q에 대한 JPEG 공격에서 추출된 워터마크의 오류 비트수는 표 5, 6, 7에서와 같다. 표에서 나타나듯이 q가 30이상에서는 비트의 오류가 발생되지 않았음을 확인할 수 있다. Barbara 영상에 대한 기존의 Inoue 방법과 제안한 방법의 워터마크 BER (bit error rate)는 그림 10에서와 같다. 이 그림에서 살펴보듯이 제안한 방법이 기존의 방법에 비하여 0.05~0.10 정도 낮음을 알 수 있다. Lena 영상에 대한 기존의 Inoue 방법과 제안한 방법의 워터마크 BER (bit error rate)는 그림 11에서와 같다. 이 그림에서 살펴보듯이 제안한 방법이 기존의 방법에 비하여 0.02~

표 5. Barbara 영상에서 q에 대한 추출된 워터마크의 BER

q	영상(Barbara)					
	H.INOUE Method			Proposed Method		
	LH	HL	HH	LH	HL	HH
90	0	0	0	0	0	0
80	0	0	0	0	0	0
70	0	0.009	0	0	0	0
60	0.012	0.009	0.006	0	0	0.002
50	0.025	0.009	0.012	0	0	0.002
40	0.037	0.009	0.042	0	0	0.008
30	0.1	0.029	0.092	0	0	0.083
20	0.112	0.077	0.263	0.066	0.007	0.245

LH=(LH4,LH3,LH2), HL=(HL4,HL3,HL2),
HH=(HH4,HH3,HH2)

표 6. Lena 영상에서 q에 대한 추출된 워터마크의 BER

q	영상(Lena)					
	H.INOUE Method			Proposed Method		
	LH	HL	HH	LH	HL	HH
90	0	0	0	0	0	0
80	0	0	0	0	0	0
70	0	0.002	0.002	0	0	0.002
60	0.018	0.002	0.033	0	0.006	0.006
50	0.028	0.01	0.064	0.003	0.006	0.025
40	0.037	0.031	0.152	0.006	0.018	0.065
30	0.052	0.071	0.252	0.013	0.055	0.196
20	0.127	0.156	0.360	0.075	0.179	0.305

표 7. Baboon 영상에서 q에 대한 추출된 워터마크의 BER

q	영상(Barbara)					
	H.INOUE Method			Proposed Method		
	LH	HL	HH	LH	HL	HH
90	0	0	0	0	0	0
80	0	0	0	0	0	0
70	0	0	0	0	0	0
60	0	0	0	0	0	0
50	0	0	0	0	0	0
40	0	0	0	0	0	0
30	0	0	0.023	0	0	0
20	0.25	0	0.023	0.033	0	0.065

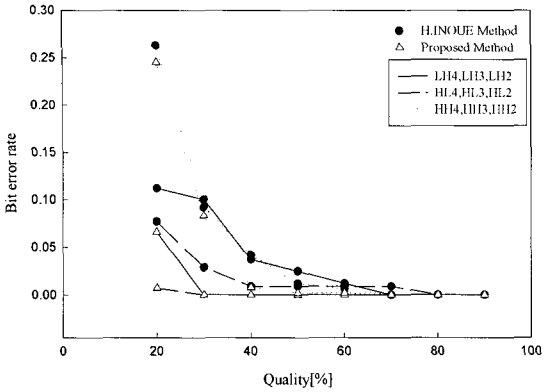


그림 10. Barbara 영상에서 q에 대한 추출된 워터마크의 BER

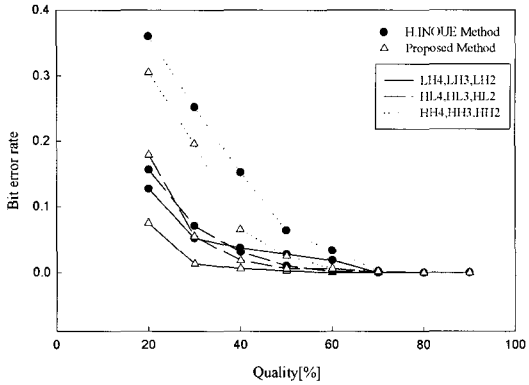


그림 11. Lena 영상에서 q에 대한 추출된 워터마크의 BER

0.03 정도 낮음을 알 수 있다. 그러나 Baboon 영상의 경우 삽입 비트수가 적어 기존의 방법과 제안한 방법 모두 비트 오류가 거의 일어나지 않았다. Gaussian, Median, Sharpening, FMLR 등의 영상처리 공격에 대한 실험 결과는 표 8, 9, 10에서와 같다. 그림 12, 그림 13, 그림 14에서 알 수 있듯이 일반적인 영상처리 공격에서도 barbara 영상의 경우 기존의 방법이 제안한 방법보다 Gaussian 공격은 0.036, Median 공격은 0.016, Sharpening 공격은 0.012, FMLR 공격은

표 8. Barbara 영상에서 각종 공격에 대한 BER

Attack	영상(Barbara)					
	H.INOUE Method			Proposed Method		
	BER			BER		
	LH	HL	HH	LH	HL	HH
No Attack	0	0	0	0	0	0
Gaussian	0.029	0.024	0	0.004	0.013	0
Sharpening	0.038	0.049	0	0.049	0.026	0.002
Median	0.019	0	0.012	0.011	0.004	0.011
FMLR	0.14	0.27	0.18	0.099	0.053	0.092

LH=(LH4,LH3,LH2), HL=(HL4,HL3,HL2), HH=(HH4,HH3,HH2)
FMLR(Frequency Mode Laplacian Removal)

표 9. Lena 영상에서 각종 공격에 대한 BER

Attack	영상(Lena)					
	H.INOUE Method			Proposed Method		
	BER			BER		
	LH	HL	HH	LH	HL	HH
No Attack	0	0	0	0	0	0
Gaussian	0.047	0.036	0.005	0.002	0.004	0
Sharpening	0.056	0.038	0.003	0.027	0.046	0
Median	0.042	0.024	0.001	0.013	0.009	0.012
FMLR	0.34	0.27	0.31	0.25	0.21	0.27

LH=(LH4,LH3,LH2), HL=(HL4,HL3,HL2), HH=(HH4,HH3,HH2)
FMLR(Frequency Mode Laplacian Removal)

표 10. Baboon 영상에서 각종 공격에 대한 BER

Attack	영상(Baboon)					
	H.INOUE Method			Proposed Method		
	BER			BER		
	LH	HL	HH	LH	HL	HH
No Attack	0	0	0	0	0	0
Gaussian	0	0	0	0.064	0	0.008
Sharpening	0.20	0	0	0.064	0	0
Median	0	0	0.023	0.032	0	0.008
FMLR	0	0	0.047	0	0	0.016

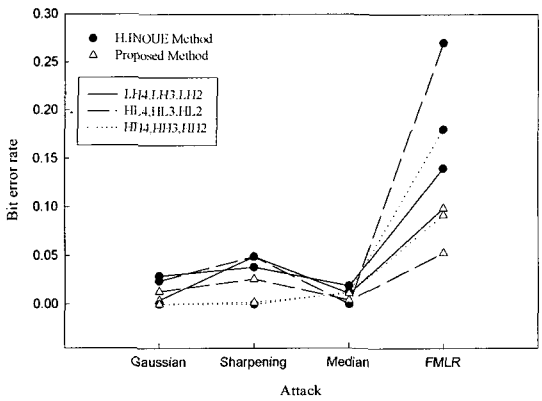


그림 12. Barbara 영상에서 각종 공격에 대한 BER

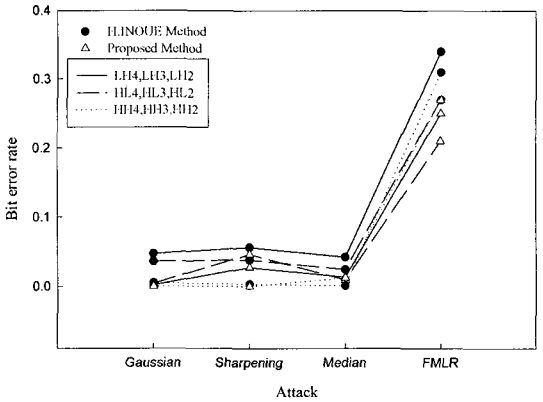


그림 13. Lena 영상에서 각종 공격에 대한 BER

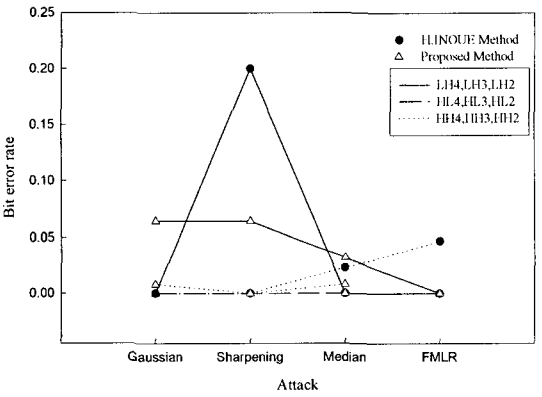


그림 14. Baboon 영상에서 각종 공격에 대한 BER

0.32 정도 낮음을 알 수 있었다. Lena 영상의 경우 기존의 방법이 제안한 방법보다 Gaussian 공격은 0.082, Median 공격은 0.033, Sharpening 공격은 0.024, FMLR 공격은 0.049 정도가 낮음을 알 수 있었다. 그리고 baboon 영상의 경우 JPEG 공격에서 뿐만 아니라 일반적인 영상처리 공격에서도 삽입 비트수가 적어 기존의 방법과 제안한 방법 모두 비트 오류가 거의 일어나지 않았다.

따라서, JPEG 압축뿐만 아니라 일반적인 영상처리 공격에서도 제안한 방법이 기존의 H.INOUE 방법과 비교해 볼 때 보다 우수함을 알 수 있었다.

5. 결 론

Buyer-Seller 워터마킹 프로토콜 상에서는 암호학적 프로토콜이 가지는 정수 기반의 대수적 특성으로 인하여 기존의 워터마킹 기법을 적용하지 못함을 2장에서 살펴보았다. 이러한 어려움을 해결하기 위하여 Kuribayashi 등은 16×16 블록 크기의 주파수 계수를 재양자화 과정을 통해 정수화한 후, 워터마크 비트에 따라 최근접 짝수 또는 홀수로 변경하는 방법을 제안하였다. 그러나 이 방법은 8×8 블록 크기의 JPEG 압축 및 양자화 테이블 변경 등에 의하여 쉽게 워터마크가 제거되는 단점을 가지고 있다. Inoue 등[11]은 DWT 상의 EZW 알고리즘에 정의된 제로트

리에 의해 비중요 계수와 중요 계수로 웨이브릿 계수를 분류한 후 비중요 계수를 설정된 두 개의 값으로 변경함으로써 워터마크 비트를 삽입한다. 그러나 이 방법은 실수 연산에 의하여 워터마크를 삽입하므로 암호화 영역 내에서는 적용되지 못한다. 본 논문에서는 Buyer-Seller 워터마킹 프로토콜 상에서 공개키 기반의 암호화 영역 내에 POCS 기반의 워터마크 삽입 방법을 제안한다. 제안한 방법에서는 워터마크 삽입 계수를 결정하기 위해 (LH4, LH3, LH2), (HL4, HL3, HL2), (HH4, HH3, HH2) 상에서 계수의 절대치가 주어진 문턱치보다 작은 경우를 비 중요계수를 구한다. 그리고 각 레벨에 대한 비중요 계수들의 제로트리 상에서 워터마크를 삽입한다. 이 때 워터마크 삽입 과정은 암호화 영역 내에서 준동형 특성을 만족하고, 다양한 공격에 견고하도록 설계된 견고성 볼록 집합으로 투영함으로써 수행된다. 그리고 공간 영역 상에서 화소값들의 변경 제한 범위로 설계된 비가시성 볼록 집합으로 투영함으로써 워터마크의 비가시성을 획득한다. 암호화 과정을 거쳐 생성되는 일반적인 데이터양을 고려한 비교 실험에서 제안한 방법이 기존의 방법에 비하여 삽입되는 워터마크 비트수가 2-3배 정도 많으며, PSNR이 0-9dB정도 낮았으나, JPEG 및 다양한 공격에서 0.02-0.10 정도 BER이 낮음을 확인하였다. 향후 연구 과제로는 암호학적 영역 내에 기하학적 공격에 대한 견고성 볼록 집합 설계이며, 비가시성 및 견고성 볼록 집합 뿐만 아니라 용량성에 대한 볼록 집합 설계와 이들 집합으로 반복 투영시 수렴 조건을 만족하도록 설계하는 것이다.

참 고 문 헌

[1] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, Vol. 86, No. 6, pp. 1064-1087, June 1998.

[2] I.J. Cox, J. Kilian, 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] C.I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Select. Areas Commun.*, Vol. 16, pp. 525-539, May 1998.

[4] N.R. Wanger, "Fingerprinting," *IEEE Symposium on Security and Privacy*. 1983.

[5] B. Pfitzmann and M. Schunter, "Asymmetric Fingerprinting," *Journal of the ACM*, Vol. 33, pp. 792-807, 1986.

[6] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting," *Proc. of EUROCRYPT.97, Lecture Notes in Computer Science*, Vol. 1233, pp. 88-102, 1997.

[7] J.Domingo-Ferrer, "Anonymous Fingerprinting of electronic information with automatic identification of redistributors," *Electronics Letters*, Vol. 34, No. 13. 1998.

[8] C.L. Lei, P.L. Yu, P.L. Tsai, and M.H. Chan, "An Efficient and Anonymous Buyer-Seller Watermarking Protocal," *IEEE Trans. on Image Processing*, Vol. 13, No. 12, pp. 1618-1626, Dec. 2004.

[9] M. Kuribayashi and H. Tanaka, "A watermarking scheme applicable for fingerprinting protocol," *Proc. of International Workshop on Digital Watermarking, IWDW2003, LNCS 2939*, pp. 532-543, 2004.

[10] J.M. Shapiro, "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," *IEEE Trans. on Signal Processing*, Vol. 41, No. 12, pp. 3445-3462, Dec. 1993.

[11] H. Inoue, A. Miyazaki, and T. Kataura, "A Digital Watermark Technique Based on the Wavelet Transform and Its Robustness on Image Compression and Transformation," *IEICE Trans. Fundamentals*, Vol. E82-A, No. 1, Jan. 1999.

[12] S.-H. Lee, T.-S. Kim, S.-J. Kim, Y. Huh, K.-R. Kwon, and K.-I Lee, "3D mesh watermarking using projection onto convex sets," *IEEE International Conference on Image Processing*, Vol. 3, pp. 1577-1580, Oct. 2004.

[13] A.B. Watson, G.Y. Yang, J.A. Solomon, and

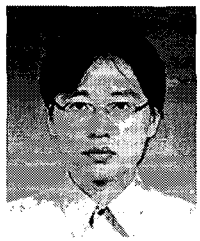
J. Villasenor, "Visibility of Wavelet Quantization Noise," *IEEE Trans. on signal Proc.* Vol. 6, No. 8, pp. 1164-1175, Aug. 1997.

권 성 근

1996년 경북대학교 전자공학과 졸업 (공학사)
1998년 경북대학교 전자공학과 졸업 (공학석사)
2002년 경북대학교 전자공학과 졸업 (공학박사)
2002년~현재 삼성전자 무선통신 사업부 연구원
관심분야 : 영상처리, 영상통신, 정보보호

이 지 혜

2005년 부산외국어대학교 정보통신과 졸업 (공학사)
2007년 부산외국어대학교 전자컴퓨터공학과 졸업 (공학석사)
관심분야 : 디지털 워터마킹, 멀티미디어영상처리



이 석 환

1999년 경북대학교 전자공학과 졸업 (공학사)
2001년 경북대학교 전자공학과 졸업 (공학석사)
2004년 경북대학교 전자공학과 졸업 (공학박사)
2005년~현재 동명대학교 정보보호학과 조교수
관심분야 : 워터마킹, DRM, 영상신호처리

권 기 룡

1986년 경북대학교 전자공학과 학사 졸업 (공학사)
1990년 경북대학교 전자공학과 석사 졸업 (공학석사)
1994년 경북대학교 전자공학과 박사 졸업 (공학박사)
2000년~2001년 Univ. of Minnesota, Post-Doc
1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
2005년~현재 한국멀티미디어학회 논문지 편집위원장
관심분야 : 멀티미디어정보보호, 멀티미디어영상처리