구매자-판매자 워터마킹 프로토콜상에서 DCT 기반의 방향성 적응 워터마킹

성택영[†], 권기창^{††}, 이석환^{***}, 권기룡^{****}, 우종호^{*****}

A Direction-Adaptive Watermarking Technique Based on 2DCT in the Buyer-Seller Watermarking Protocol

Teak-Young Seong[†], Ki-Chang Kwon^{††}, Suk-Hwan Lee^{***},
Ki-Ryong Kwon^{****}, Chong-Ho Woo^{*****}

ABSTRACT

Buyer-seller watermarking protocol is one of the copyright protection techniques which combine a cryptographic protocol used in electronic commerce with a digital watermarking scheme aiming at proving the ownership of multimedia contents and preventing the illegal reproduction and redistribution of digital contents. In this paper, it is proposed a new watermarking scheme in an encrypted domain in an image that is based on the block-DCT framework. In order to implement watermarking scheme in a public-key cryptosystem, it is divided that frequency coefficients exist as real number into integer and decimal layer. And the decimal layer is modified integer type through integral-processing. Also, for robustness and invisibility required in watermarking scheme, it is designed a direction-adaptive watermarking scheme based on locally edge-properties of each block in an image through analyzing distribution property of the frequency coefficients in a block using JND threshold.

Key words: Buyer-Seller Watermarking Protocol, DCT Transform, Direction-Adaptive Watermarking

1. 서 론

최근 디지털 워터마킹 기법과 더불어 전자상거래 상에서 이용되는 암호학적 기법과 구매자 및 판매자 정보를 디지털 콘텐츠 내에 함께 삽입하는 핑거프린팅 기법을 결합한 암호학적 프로토콜이 연구되고 있다. 암호학적 프로토콜은 전자상거래 상에서 구매자

와 판매자가 서로 신뢰할 수 있는 계약절차를 제공하며, 차후 불법 유통이 의심되는 콘텐츠의 발견시, 콘텐츠 내에 삽입된 구매자 정보를 추출함으로써 불법 복제 및 배포의 책임 소재를 밝혀낸다. 이 프로토콜은 판매자가 핑거프린팅된 콘텐츠에 접근할 수 있는 지 없는지에 따라 대칭형[1]과 비대칭형[2]으로 구분된다.

※ Corresponding Author : Chong-Ho Woo, Address: (608-737) 599-1 Daeyeon-Dong, Namgu, Busan, Korea, TEL : +82-51-629-6250, FAX : +82-51-629-6264, E-mail : chwoo@pknu.ac.kr

Receipt date : May. 7, 2014, Revision date : Jun. 21, 2014
Approval date : Jun. 23, 2014

[†] Interdisciplinary Program of Information Security, Pukyong National Univ.
(E-mail : theage76@pknu.ac.kr)

^{††} Dept. of IT Cooperative System, Gyeongbuk Provincial College (E-mail : kwon0819@daum.net)

^{***} Dept. of Information Security, Tongmyong University
(E-mail : skylee@tu.ac.kr)

^{****} Interdisciplinary Program of Information Security, Pukyong National Univ.

(E-mail : krkwon@pknu.ac.kr)

^{*****} Dept. of Computer Engineering, Pukyong National Univ.

※ This work was supported by a Research Grant of Pukyong National University(2013Year)

Pfitzmann 등[1]이 제안한 대칭형 핑거프린팅 프로토콜에서는 핑거프린팅 프로토콜과 구매자 판별 프로토콜의 하부 프로토콜과 구매기록 저장을 위한 데이터베이스로 구성되어 있다. 그러나 하부 프로토콜에서는 구매자뿐만 아니라 판매자도 핑거프린팅된 콘텐츠에 접근이 가능하므로, 불법 복제를 통해 유출된 콘텐츠의 적발시, 불법 배포자가 구매자인지 아니면 판매자인지를 명확히 가려낼 수 없는 소비자 권리 문제(customer's right problem)이 야기된다. 이러한 문제점을 해결하기 위하여 비대칭형 프로토콜들이 제안되어 왔다.

비대칭형 프로토콜[2]은 핑거프린팅된 콘텐츠를 오직 구매자만이 접근할 수 있도록 구매자와 판매자의 2자(2-party)간, 혹은 인증기관을 포함한 3자(3-party)간 프로토콜로 설계된다. 따라서 판매자는 해당 콘텐츠의 매매시, 핑거프린팅된 콘텐츠에 대한 접근이 불가능하므로, 불법 배포에 대한 책임소재로부터 자유로울 수 있다. 그러나 판매자가 원본 콘텐츠와 불법 배포 콘텐츠와의 비교를 통하여 불법 배포 콘텐츠 내의 핑거프린팅 정보를 획득할 수 있다. 그러므로 이 프로토콜에서는 판매자가 추출된 핑거프린팅 정보를 불법 배포의 책임이 있는 구매자의 다른 구매 콘텐츠에 삽입할 수 있는 비결합 문제(unbinding problem)이 존재한다. Lei 등[3]은 비결합 문제를 해결하기 위하여 구매자의 익명성을 보장하는 익명인증기관을 두는 일회용 공개키 기반의 암호 프로토콜을 제안하였다. 이 프로토콜에서는 판매자가 불법 유통 콘텐츠에서 핑거프린팅 정보를 획득하더라도 이를 무용지물로 만든다.

암호학적 프로토콜에서는 핑거프린팅 정보들이 디지털 워터마킹 기법에 의하여 해당 콘텐츠와 결합된다. 그러나 공개키 기반의 암호 시스템이 가지는 '준동형 특성(homomorphic property)'을 기반으로 결합 과정이 수행되어야만 암호학적 프로토콜이 요구하는 비대칭 속성을 만족시킬 수 있다. 다시 말하면 정수의 대수적 특성에 기초하여 이루어지는 암호화 과정에서는 콘텐츠 및 워터마크가 정수 형태로 존재하여 이를 각각 암호화된 후 결합되어야 한다.

기존의 buyer-seller 워터마킹 프로토콜들에서는 구매자 및 판매자 정보와 디지털 콘텐츠 간의 결합을 위하여 워터마킹 기법이 필수적이다[4,11]. 하지만, 프로토콜상의 공개키 암호 시스템은 정수의 대수적

특성을 기반으로 하는데 비해 연산대상이 되는 콘텐츠는 일반적으로 주파수 영역 상에서 실수형태로 존재하므로 암호화 영역 내에서 삼입정보와 주파수 계수를 직접적으로 결합시키는 데에는 어려움이 따른다.

본 논문에서는 공개키 기반의 구매자-판매자 워터마킹 프로토콜상에서 블록 DCT를 기반으로 블록 내 AC계수들의 분포특성을 고려한 방향성 적응 워터마킹 기법을 제안한다. 제안한 기법에서는 각 블록을 AC계수들의 분별역치(JND: just noticeable difference) 특성을 이용하여 방향 성분별로 분류한 후, 이 성분에 따라 삼입 대상 계수를 선정한다. 그리고 각 블록이 가지는 국부적 에지 특성의 방향에 따라 워터마킹이 수행된다[5,6]. 이 때 삼입 대상 계수가 실수형태로 존재하므로 이를 정수부와 소수부로 분할 한 뒤 소수부를 정수화하여 이들 각각에 워터마크를 결합한다. 따라서 제안한 방법은 기존의 방법과는 달리 양자화 과정을 통한 계수 정보의 손실 없이 공개키 기반의 암호 시스템에서 워터마킹이 가능하다. 제안한 방법의 비가시성과 강인성을 평가하기 위하여 PSNR 비교 및 서로 다른 특성을 가지는 실험 영상들에 대하여 quality factor 'q'의 조절에 따른 JPEG 압축 실험을 행하였다.

본 논문의 구성을 살펴보면, 먼저 2장에서는 구매자-판매자 워터마킹 프로토콜의 일반적인 구조와 해당 프로토콜의 기반이 되는 공개키 암호화 시스템의 특성에 대해 서술한다. 3장에서는 제안한 구매자-판매자 워터마킹 프로토콜 상에서의 방향성 적응 워터마킹 기법에 대해 기술하고, 4장에서는 제안한 방법의 비가시성과 강인성에 대한 실험 결과 및 고찰에 대하여 살펴본다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

2. 구매자-판매자 워터마킹 프로토콜

2.1 구매자-판매자 워터마킹 프로토콜

구매자-판매자 워터마킹 프로토콜은 프로토콜의 진행 흐름에 따라 워터마크 생성 프로토콜, 워터마킹 프로토콜, 그리고 분쟁해결 프로토콜로 나누어진다[7,8]. 이 중 워터마킹 프로토콜은 워터마크와 콘텐츠 간의 결합과 관련된 프로토콜로 이의 흐름은 그림 1에서와 같다. 그림에서 보는 바와 같이 워터마크와

Fig. 1. Block diagram of watermarking protocol.

콘텐츠는 $E_{pk_B}()$ 에 의하여 각각 암호화 된 후에 이들을 선형 결합한다. 그리고 $D_{sk_B}()$ 를 이용해 워터마크가 삽입된 콘텐츠로 복호화 됨을 알 수 있다.

2.2 공개키 암호화 시스템

Diffie와 Hellman에 의하여 처음 제시된 공개키 암호 시스템은 하나의 비밀키 만을 공동의 이용자가 사용하는 관용 방식에서 발생하는 키 관리의 문제점으로 지적되던 키 분배 방식을 획기적으로 해결한 암호 방식으로 암호 · 복호화에 사용되는 키를 두개로 나누어 하나는 암호화 키로, 다른 하나는 복호화 키로 사용한다[9]. 이때, 암호화 키는 공개 목록에 등록 · 공개하므로 ‘공개키(public key)’라고 부르며, 복호화 키는 개인이 비밀리에 보관하므로 ‘비밀키(secret key)’ 또는 ‘개인키(private key)’라고 부른다. 공개키 암호의 특징 중 하나는 암호화 키를 이용하여 메시지 M 을 암호화 시킬 경우, $D_{sk}(E_{pk}(M))=M$ 또는, $E_{pk}(D_{sk}(M))=M$ 이 성립한다는 것이며 두 가지 모두가 성립하는 경우도 있다.

이러한 트랩도어 역할을 수행하는 pk 를 구하기 위해 이용하는 수학적 근간에 따라 각각 특색 있는 공개키 암호 시스템들이 나타났는데 그중 가장 대표적인 예로 RSA 암호 방식을 꼽을 수 있다. Rivest, Shamir, Adleman에 의해 제안된 RSA 암호 방식은 합성수의 소인수 분해의 어려움에 기인하여 실현하였는데 RSA의 시스템 설정 및 암호 · 복호화 과정은 다음과 같다.

1. 충분히 크고 크기가 비슷한 두 개의 소수 p 와

q 를 선택한다.

2. $n=pq$ 와 $\phi(n)=(p-1)(q-1)$ 을 계산한다.

3. $\gcd(\phi(n),e)=1$ 인 랜덤한 정수 $e(1 < e < \phi(n))$ 를 선택한다.

4. 확장 유클리드 알고리즘을 이용하여

$ed=1 \bmod \phi(n)$ 인 $d(1 < d < \phi(n))$ 를 계산한다.

위의 과정에서 생성된 공개키는 (e,n) 이며, 비밀키는 (p,q,d) 이다. 이때, B가 A에게 암호문을 전송하고 A는 B로부터 받은 암호문을 복호화 하는 과정은 다음과 같다.

암호화:

1. B는 A의 공개키 (e,n) 를 얻는다.
2. 메시지 m 을 $[0, n-1]$ 사이의 수로 표현한다.
3. $c=m^e \bmod n$ 을 계산한다.
4. 암호문 c 를 계산한다.

복호화:

A는 자신의 비밀키 d 를 이용하여 $m=c^d \bmod n$ 을 복원한다.

(증명)

$$\begin{aligned} m^{ed} &= m^{1+k\phi(n)} \bmod n \\ &= m(m^{\phi(n)})^k \bmod n \\ &= m \bmod n \end{aligned}$$

위의 과정을 통해 메시지 m_1, m_2 가 각각 c_1, c_2 로 암호화 되었을 때, $(m_1 m_2)^e = c_1 c_2 \bmod n$ 이기 때문에 $E_e(m_1)E_e(m_2) = E_e(m_1 m_2)$ 가 성립하고 이를 복호화 함수를 이용해 복호화 시키면 $D_d(E_e(m_1 m_2)) = m_1 m_2$

이 된다. 이러한 성질을 준동형 특성이라고 하는데, buyer-seller 워터마킹 프로토콜에서는 이러한 특성을 이용하여 암호화 영역 내에서 워터마크와 콘텐츠를 서로 결합시킨다. 하지만 RSA의 경우 곱의 준동형 특성(multiplicative homomorphic property)이 성립하므로 워터마크와 콘텐츠가 합의 형태로 결합하는 일반적인 워터마킹 기법에는 적용하기가 어렵다. 따라서 본 논문에서는 합의 준동형 특성(additive homomorphic property)을 가지는 Okamoto-Uchiyama 암호화 기법[10]을 적용하여 암호화 영역 내의 워터마킹을 수행한다.

Okamoto-Uchiyama 암호화 기법에서의 준동형 특성은 다음과 같다.

1. $E(m, r)$ 을 암호화 함수로 둔다. 이때 m 은 메시지이고 r 은 임의의 수이다.
2. 법 $n = p^2q$ 이며, 이때 p 와 q 는 큰 소수이다.
3. 본 암호 방식은 다음과 같은 준동형 특성을 만족한다.

$$E_e(m_1, r_1) \cdot E_e(m_2, r_2) = E_e(m_1 + m_2, r_1 + r_2) \pmod{n} \quad (1)$$

3. 제안한 방향성 적응 워터마킹 알고리즘

3.1 제안한 구매자-판매자 워터마킹 프로토콜

본 논문에서는 공개키 암호 시스템 기반의 구매자-판매자 워터마킹 프로토콜상에서 블록 DCT를 기반으로 블록 내 AC계수들의 분포특성을 고려한 방향성 적응 워터마킹 기법을 제안한다. 인간 시각 시스템에서는 저주파 영역 내의 변화보다는 고주파 영역의 변화에 대해 둔감하게 반응한다. Watson[5]은 인간 시각에 미치는 주파수 민감도(frequency sensitivity) 및 밝기 민감도(luminance sensitivity)를 정량화한 후, 이를 이용하여 반응역치를 모델링하였다. 그리고 모델링된 JND를 DCT 기반의 영상 압축에 적용하였다. Suthaharan 등[6]은 위의 모델링된 반응역치를 문턱값으로 이용하여 이보다 더 큰 주파수 계수들에 대해서만 워터마크를 삽입하였다. 제안한 방법에서는 각 블록의 DCT 영역을 수직, 수평, 및 대각 영역으로 분할한 후 반응역치를 만족하는 주파수 계수의 수가 가장 많은 영역을 선택하여 각 블록의 방향성분을 결정한다. 그리고 각 블록의 선택된

Fig. 2. Block diagram of proposed watermarking scheme.

영역 내에서 반응역치 만족 계수들 중 임의의 계수에 워터마크를 삽입한다. 이 때, 공개키 기반 암호 시스템 상에서 구현이 가능하기 위하여 선택된 반응역치 만족 계수를 정수부와 소수부로 분할한 후, 소수부를 정수화하여 각 부분에 워터마크를 결합한다. 구매자-판매자 워터마킹 프로토콜 상에서 제안한 방향성 적응 워터마킹 기법은 그림 2에서와 같다.

3.2 삽입 방법

워터마크 삽입 방법은 블록 DCT 상에서의 워터마크 삽입 대상영역 및 계수 선정, 선정된 블록 내 주파수 계수에 대한 정수화 작업, 그리고 암호화 영역 내에서의 워터마킹으로 구성된다.

step 1. 적응적 삽입 계수 선택

적응적 삽입 계수 선택 과정에서는 정지 영상의 각 블록을 8x8 블록 DCT으로 변환한 후, 블록 내의 AC 계수 분포특성을 JND에 의하여 분석, 블록 내 에지성분의 존재 유무와 방향성을 파악하여 삽입 블록 및 삽입 계수를 결정한다. 먼저 각각의 블록들을 2차원 DCT 기저 함수의 특성을 고려하여 그림 3에서와 같이 수직, 수평, 및 대각 영역으로 분할한다. 이 때 DC 성분과 저주파 성분에 해당하는 AC1, AC2, AC4는 영역 분할에서 제외된다.

그리고 각 블록의 방향 성분을 판단하기 위하여 반응역치 문턱값을 넘는 AC 계수들의 영역별 분포 상태를 분석한다. 여기서 에지 성분의 AC 계수들을 판별하기 위한 반응역치 문턱값을 인간 시각 모델에 근거한 주파수 민감도 및 밝기 민감도를 고려하여 계산한다. 본 논문에서는 빠르고 간단한 반응역치 값

DC	AC ₁						
AC ₂	AC ₄			수 직			
수 평				대 각			

Fig. 3. Example of region partition in DCT block.

계산을 위하여 그림 4와 같이 Suthaharan 등[6]이 제안한 주파수 민감도 테이블을 사용한다. 이 주파수 민감도 값들은 JPEG 압축과정에서의 양자화 테이블 상에서의 양자화 스텝 크기 Q 의 1/2 크기를 가지며, 이는 양자화 과정에서 발생하는 오차이다. 모든 블록들에 대하여 주파수 민감도 테이블을 적용하여 식 (2) 및 (3)에 의하여 반응역치를 구한다.

$$L_{u,v,b} = F_{u,v} \left(\frac{X_{0,0,b}}{X_{0,0}} \right)^\alpha \quad (2)$$

$$J_{u,v,b} = \max \left[L_{u,v,b}, |X_{u,v,b}|^{\beta_{av}} (L_{u,v,b})^{1-\beta_{av}} \right] \quad (3)$$

여기서 $F_{u,v}$ 는 주파수 민감도이며, $L_{u,v,b}$ 는 b번째 블록 내의 밝기 민감도, $X_{0,0,b}$ 는 블록 b의 DC 값, 그리고 $X_{0,0}$ 는 각 블록별 DC 값들의 평균이다. 이때, 밝기 민감도 조절 인자 α 는 0.649이다. 블록 내 주파

Frequency Sensitivity: F								u
	8	6	7	7	9	12	25	36
	6	6	7	9	11	18	32	46
	5	7	8	11	19	28	39	48
	8	10	12	15	28	32	44	49
	12	13	20	26	34	40	52	56
	20	29	29	44	55	52	61	50
	26	30	35	40	52	57	60	52
	31	28	28	31	39	46	51	50
v								

Fig. 4. Table of frequency sensitivity.

수 계수별 반응역치 값인 $J_{u,v,b}$ 는 식 (3)에 구하여 구하여지는데, $X_{u,v,b}$ 는 블록 b의 주파수 계수 값이며 조절인자 $\beta_{u,v}$ 는 0.7을 사용한다.

반응역치 값인 $J_{u,v,b}$ 를 이용하여 삽입 가능한 블록을 선정하고 삽입 가능 블록 내의 삽입 대상 계수를 선정한다. 즉, 그림 4에서와 같이 식 (4), (5) 및 (6)을 통하여 b번째 블록 B_b 를 각각 수직(vertical), 수평(horizontal), 대각(diagonal)영역인 $R_{B_b,V}$, $R_{B_b,H}$, $R_{B_b,D}$ 로 분할한 뒤

$$R_{B_b,V} = \{X_{u,v,b} | X_{u,v,b} \geq J_{u,v,b}, 8 > u > 1, 2 > v \geq 0\} \quad (4)$$

$$R_{B_b,H} = \{X_{u,v,b} | X_{u,v,b} \geq J_{u,v,b}, 2 > u \geq 0, 8 > v > 1\} \quad (5)$$

$$R_{B_b,D} = \{X_{u,v,b} | X_{u,v,b} \geq J_{u,v,b}, 8 > u > 2, 8 > v > 2\} \quad (6)$$

식 (3)에 의하여 구하여진 $J_{u,v,b}$ 값에 따라 위터마크 삽입 블록을 아래와 같이 결정한다.

$$B_b = \begin{cases} 1 & n(X_{JND}) \geq Th. \\ 0 & otherwise \end{cases} \quad (7)$$

$$X_{JND} = \{X_{u,v,b} | X_{u,v,b} \in R_{B_b,V}, R_{B_b,H} \text{ and } R_{B_b,D}\} \quad (8)$$

즉, B_b 의 값이 '1'이면 위터마크 삽입 대상 블록이며, 그렇지 않으면 삽입 대상 블록에서 제외된다. 이때, $Th.$ 는 B_b 의 에지 성분의 포함 여부를 결정하기 위한 문턱값이다. B_b 가 삽입 가능 블록으로 판정되면 블록 내에 위터마크 삽입 계수 $X'_{u,v,b}$ 를 아래와 같이 결정한다.

$$X'_{u,v,b} = \begin{cases} X_{1,0,b} & n(R_{B_b,V}) = \max[n(R_{B_b,V}), n(R_{B_b,H}), n(R_{B_b,D})] \\ X_{0,1,b} & n(R_{B_b,H}) = \max[n(R_{B_b,V}), n(R_{B_b,H}), n(R_{B_b,D})] \\ X_{1,1,b} & n(R_{B_b,D}) = \max[n(R_{B_b,V}), n(R_{B_b,H}), n(R_{B_b,D})] \end{cases} \quad (9)$$

step 2. 주파수 계수의 정수부, 소수부 분할

공개키 기반 암호 시스템 상에서의 위터마킹을 고려하여 위터마크 삽입 계수들을 정수화한다. 실수 형태의 주파수 계수 값 $X_{u,v,b}$ 은

$$X_{u,v,b} = X_{u,v,b}^I + X_{u,v,b}^D \quad (10)$$

와 같이 정수(Integer)부 $X_{u,v,b}^I$ 와 소수점 이하의 유효 숫자로 이루어진 소수(Decimal)부 $X_{u,v,b}^D$ 로 이루어지므로, $X_{u,v,b}^D$ 를

$$X_{u,v,b}^{D_l} = X_{u,v,b}^D \times 10^l \quad (11)$$

와 같이 정수화시킨다. 이때 l 은 유효숫자가 차지하는 자릿수들의 길이이다.

step 3. 워터마크 삽입

위 과정에서 각각 분리된 정수부 $X_{u,v,b}^I$ 와 정수화된 소수부 $X_{u,v,b}^{D_I}$ 를 구매자로부터 전달받은 암호화된 워터마크 w_j 를 아래와 같이 결합시킨다.

if watermark $w_j = '1'$ and $X_{u,v,b} = X_{1,0,b}$, then

$$X_{1,0,b}^I = |X_{1,0,b}^I| + I[((100-q)/50 \times Q_{1,0})/2] \quad (12)$$

$$X_{1,0,b}^{D_I} = |X_{1,0,b}^{D_I}| + D_I[((100-q)/50 \times Q_{1,0})/2] \quad (13)$$

$$X_{0,1,b}^I = |X_{0,1,b}^I| - I[((100-q)/50 \times Q_{0,1})/2] \quad (14)$$

$$X_{0,1,b}^{D_I} = |X_{0,1,b}^{D_I}| - D_I[((100-q)/50 \times Q_{0,1})/2] \quad (15)$$

else if watermark $w_j = '1'$ and $X_{u,v,b} = X_{0,1,b}$, then

$$X_{0,1,b}^I = |X_{0,1,b}^I| + I[((100-q)/50 \times Q_{0,1})/2] \quad (16)$$

$$X_{0,1,b}^{D_I} = |X_{0,1,b}^{D_I}| + D_I[((100-q)/50 \times Q_{0,1})/2] \quad (17)$$

$$X_{1,0,b}^I = |X_{1,0,b}^I| - I[((100-q)/50 \times Q_{1,0})/2] \quad (18)$$

$$X_{1,0,b}^{D_I} = |X_{1,0,b}^{D_I}| - D_I[((100-q)/50 \times Q_{1,0})/2] \quad (19)$$

else if watermark $w_j = '1'$ and $X_{u,v,b} = X_{1,1,b}$, then

$$X_{1,1,b}^I = |X_{1,1,b}^I| + I[((100-q)/50 \times Q_{1,1})/2] \quad (20)$$

$$X_{1,1,b}^{D_I} = |X_{1,1,b}^{D_I}| + D_I[((100-q)/50 \times Q_{1,1})/2] \quad (21)$$

$$X_{1,0,b}^I = |X_{1,0,b}^I| - I[((100-q)/50 \times Q_{1,0})/2] \quad (21)$$

$$X_{1,0,b}^{D_I} = |X_{1,0,b}^{D_I}| - D_I[((100-q)/50 \times Q_{1,0})/2] \quad (22)$$

$$X_{0,1,b}^I = |X_{0,1,b}^I| - I[((100-q)/50 \times Q_{0,1})/2] \quad (23)$$

$$X_{0,1,b}^{D_I} = |X_{0,1,b}^{D_I}| - D_I[((100-q)/50 \times Q_{0,1})/2] \quad (24)$$

else

Non-embedding.

식 (12)에서 식(24)까지 살펴보면 각 블록 내의 $R_{B_v, V}$, $R_{B_v, H}$, $R_{B_v, D}$ 세 영역 중 가장 많이 $J_{u,v,b}$ 문턱값을 넘어서는 주파수 계수를 가지는 영역을 계산하여 해당 블록의 방향 성분을 분석한 후, 선정된 삽입 계

수 $X_{u,v,b}^I$ 를 요구되는 JPEG 품질 인자 q 수준까지 영향을 압축하더라도 워터마크의 생존이 가능하도록 양자화 스텝 크기의 절반 값을 더함으로써 검출시, 워터마크의 추출이 가능하도록 설계하였다.

3.3 검출 방법

워터마크 삽입 방법은 양자화 스텝 크기 Q 의 값이 같은 계수들의 크기를 변경하여 삽입 블록의 $|X_{0,1,b}|$ 와 $|X_{1,0,b}|$ 간의 차가 $Q_{0,1}(=Q_{1,0})$ 이도록 설계되었기 때문에 검출 과정에서 두 계수간의 차 값을 통해 식 25와 같이 워터마크를 검출한다.

$$w_j = \begin{cases} '1' & \|X_{0,1,b}\| - \|X_{1,0,b}\| \geq Q_{0,1}(=Q_{1,0}) \\ '0' & otherwise \end{cases} \quad (25)$$

식 (12)에서 식 (25)까지의 삽입 수식을 살펴보면 삽입 대상 계수와 동일한 양자화 스텝 크기를 가지는 주파수 계수에는 삽입 대상 계수에 더해지는 값을 뺄으로써 요구되는 JPEG 품질 인자 q 수준까지 영향을 압축하더라도 검출시 워터마크를 추출 가능하도록 하였다.

4. 실험 결과 및 고찰

제안한 기법의 성능 평가를 위해 워터마킹 영상의 JPEG 압축 처리후 워터마킹 영상과 원영상 간의 PSNR(peak signal-to-noise ratio) 검출을 통해 비가시성을 평가하였으며, JPEG 압축 후 추출된 워터마크의 에러 비트수를 검사하여 강인성을 평가하였다. 실험 영상은 각각 저, 중, 고 주파수 성분을 포함하고 있는 표준 영상 Peppers, Lena, 및 Baboon 영상을 사용하였으며 이때 각 정지 영상의 크기는 512×512 이다. 사용한 워터마크는 이진 비트열 형태로 영문 알파벳과 숫자들의 조합으로 이루어진 35문자를 8비트 확장 ASCII 코드의 이진비트열로 변환시킨 후 각 비트들을 스캔블링 취하여 생성하였다.

실험 시 사용한 각종 인자들의 경우 삽입블록 결정 문턱값 m 는 5, quality factor $q=10$ 을 주어 낮은 품질의 q 값에도 JPEG 압축 공격시 워터마크가 강인하게 살아남게 실험하였다. Lena 영상의 경우, 표준 영상으로서 삽입 가능 블록 수는 2407개이고, PSNR은 47.21dB이다. Peppers 영상은 저주파 영상으로서 이에 대한 실험 결과, 삽입 가능한 워터마크의 블록

수는 2313개이며, 워터마크가 삽입된 영상과 원영상 간의 PSNR은 50.87dB가 나왔다. 그리고 Baboon 영상은 고주파 영상으로서 삽입 가능 블록 수는 3771개이며, PSNR 결과 값은 45.74dB로 나왔다. 그림 5에서 그림 7까지 나타난 바와 같이 각각의 영상에서 워터마크 삽입 블록들은 블록들이 가지는 국부적 에

Fig. 5. Lena images. (a) original Image, (b)potential blocks for embedding process, (c) watermarked image, and extracted watermark image

Fig. 6. Peppers images. (a) original Image, (b)potential blocks for embedding process, (c) watermarked image, and extracted watermark image.

그림 7. Baboon images. (a) original Image, (b)potential blocks for embedding process, (c) watermarked image, and extracted watermark image.

지 특성을 반영하여 선택됨을 알 수 있었다. 또한 반응역치 문턱값을 이용하여 블록의 방향성분을 검출할 경우, 워터마크의 용량성과 비가시성 면에서 우수한 성능을 나타냄을 알 수 있었다. 표 1은 영상별 삽입 가능 블록, 삽입비트 수 및 PSNR을 나타내었다.

표 1에서 나타난 바와 같이 워터마크 삽입 가능 블록 개수 및 삽입 비트 수는 고주파 성분이 많은 edge 및 texture에 삽입되는 양이 많게 되었다. 따라서 PSNR은 상대적으로 떨어짐을 알 수 있다. 그러나 고주파 성분이 많은 Baboon의 PSNR이 45.74[dB]이면 인간의 눈은 인지를 전혀 할 수 없다.

표 2에서 살펴보면 알 수 있듯이 50 이하의 q 값에서부터 에러 비트가 발생하였으나 워터마크 삽입과정에서 JPEG 압축 시, 원하는 q 인자 수준까지 품질을 떨어뜨리더라도 워터마크가 검출 되도록 조절 하

Table 1. Watermarking Info. for each test images.

Image	Peppers	Lena	Baboon
Embedded blocks [No.]	2313	2407	3771
Embedded bits [bits]	2313 (280×8+73)	2407 (280×8+167)	3771 (280×13+131)
PSNR[dB]	50.87	47.21	45.74
- Threshold Th.=5개, q=10			

Table 2. The number of bit error and bit error rate(BER) according to variation of q value.

q	Lena		Peppers		Baboon	
	No. of error bits	BER [%]	No. of error bits	BER [%]	No. of error bits	BER [%]
90	0/2407	0.00	0/2313	0.00	0/3771	0.00
80	0/2407	0.00	0/2313	0.00	0/3771	0.00
70	0/2407	0.00	0/2313	0.00	0/3771	0.00
60	0/2407	0.00	0/2313	0.00	0/3771	0.00
50	19/2407	0.78	11/2313	0.47	32/3771	0.85
40	38/2407	1.58	29/2313	1.25	59/3771	1.56
30	76/2407	3.16	56/2313	2.42	88/3771	2.33
20	103/2407	4.27	87/2313	3.76	126/3771	3.34
10	168/2407	6.98	113/2313	4.89	235/3771	6.23

였으나 $q=50$ 에서부터 여러 비트가 발생 하였다. 이것은, 삽입 가능 주파수 계수를 선정할 때 사용하는 $J_{u,v}$ 가 $q=50$ 일 때의 양자화 테이블 값 $Q_{u,v}/2$ 를 주파수 민감도 테이블로 사용하였기 때문에 비록, 삽입과정에서 q 값을 조절하더라도 JPEG 압축시 $q=50$ 이하에서부터 워터마크의 열화가 발생할 수 있다. 그러나, 워터마크를 중복하여 삽입하기 때문에 $q=10$ 이하에서도 워터마크를 검출할 수 있었다.

5. 결 론

암호학적 프로토콜이 가지는 정수 기반의 대수적 특성으로 인해 일반적인 주파수 영역 워터마킹 기법을 직접적으로 적용하기에는 문제점들이 있음을 2장에서 살펴보았다. 이러한 어려움을 해결하기 위한 소수의 제안 방법들 중 하나인 재양자화 과정을 통해 정수화된 주파수 계수를 손쉽게 획득할 수 있다는 이점은 있지만, 16×16 크기의 양자화 테이블 크기와 재양자화 과정 이후, 최근접 짝수 또는 홀수로 변경되는 양자화 계수로 인해 JPEG 압축 및 짝, 작은 값의 양자화 계수 변경만으로도 쉽게 워터마크가 제거되는 단점을 지니고 있었다.

본 제안 기법은 주파수 AC계수의 분포특성을 반응역치 문턱값을 이용, 블록별 방향 성분을 판정하여 워터마크를 삽입하므로 각 블록들의 국부적 에지 특성이 반영되었다. 또한, 정수의 대수적 특성에 기반

해 작동되는 공개키 기반 암호 시스템을 고려하여 실수 형태의 주파수 계수를 정수부 및 소수부로 계층을 분할하여 소수부 또한 정수화 처리하므로 암호화 영역 내에서 주파수 계수와 워터마크가 결합 가능함을 보였다. 이는 재양자화 기법과 비교해 주파수 계수 정보의 손실이 적다는 잇점도 가지고 있다. 하지만 암호화 과정을 거쳐 생성되는 일반적인 암호화 데이터양을 고려하였을 때 현재의 방법은 삽입 비트량이 적은 편이며 암호화되어 워터마크와 결합한 콘텐츠 역시 그 크기가 엄청나게 크다.

REFERENCE

- [1] Birgit Pfitzmann, "Trials of Traced Traitors," *Proceedings of the First International Workshop on Information Hiding*, pp. 49-64, May 30-June 01, 1996.
- [2] B. Pfitzmann and M. Schunter, "Asymmetric Fingerprinting," *Advances in Cryptology-EUROCRYPT '96, LNCS 1070, Springer-Verlag*, pp. 84-95, 1996.
- [3] C. L. Lei and M. H. Chan, "An Efficient Anonymous Buyer-Seller Watermarking Protocol," *IEEE Trans. Image Processing*, Vol. 13, No. 12, pp. 1618-1626, Dec. 2004.
- [4] N. Memon and P. W. Wong, "A Buyer-seller Watermarking Protocol," *IEEE Trans. Image Processing*, Vol. 10, No. 4, pp. 643-649, Apr. 2001.
- [5] A. B. Watson, "DCT quantization matrices visually optimized for individual images," in *Proc. SPIE Conf Human Vision, Visual Processing, and Digital Display IV*, Vol. 1913, pp. 202-216, Feb. 1993.
- [6] S. Suthaharan, S. W. Kim, H. K. Lee, and S. Sathananthan, "Perceptually tuned robust watermarking scheme for digital images," *Pattern Recognition Letters*, Vol. 21, Issue 2, pp. 145-149, 2000.
- [7] S.G. Kwon, J.H. Lee, S.H. Lee, and K.R. Kwon, "POCS Based Digital Watermarking In Buyer-Seller Watermarking Protocol," *Journal*

of Korea Multimedia Society, Vol. 10, No. 6, pp. 569-582, June 2007.

- [8] S.H. Lee, S.G. Kwon, and K.R. Kwon, "Geometric Multiple Watermarking Scheme for Mobile 3D Content Based on Anonymous Buyer-Seller Watermarking Protocol," *Journal of Korea Multimedia Society*, Vol. 12, No. 2, pp.244-256, Feb. 2009..
- [9] J.S. Kang, J.H. Kim, S.W. Park, C.S. Park, S.T. Jee, G.C. Ha, et al., *Modern Cryptography*, Kyungmoon publisher, 2002.
- [10] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," *Proc. of EUROCRYPT'98*, LNCS 1403, pp. 308-318, 1998.
- [11] Terelius, B., "Towards transferable watermarks in buyer-seller watermarking protocols," *Proceedings of the 2013 IEEE International Workshop on Information Forensics and Security*, pp. 197-202, 2013.

성택영

2004년 부산외국어대학교 전자공학과 학사 졸업(공학사)
2006년 부산외국어대학교 전자컴퓨터공학과 석사 졸업(공학석사)
2007년~현재 부경대학교 정보보호협동과정 박사과정

관심분야: 멀티미디어 신호처리, 워터마킹

권기창

1985년 안동대학교 행정학과 행정학사
1993년 대구대학교 사회개발대학원 지역개발학과 전자정보처리전공 경영학석사
2000년 영남대학교 대학원 통계학과 계산학전공 이학박사

1987년~1997년 안동대학교 전자계산소
1993년~1997년 안동과학대학 사무자동화과 교수
1998년~현재 경북도립대학 IT특약과 교수
관심분야: 멀티미디어 전자상거래, 행정정보화

이석환

1999년 경북대학교 전자공학과 학사 졸업(공학사)
2001년 경북대학교 전자공학과 석사 졸업(공학석사)
2004년 경북대학교 전자공학과 박사 졸업(공학박사)

2005년~현재 동명대학교 정보보호학과 조교수
관심분야: 워터마킹, DRM, 영상신호처리

권기룡

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)
2006년~현재 부경대학교 IT융합응용공학과 교수

2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2011년~2012년 Colorado State University, Visiting Scholar
2014년~현재 한국멀티미디어학회 수석부회장
관심분야: 멀티미디어정보보호, 영상처리, 멀티미디어 통신 및 신호처리

우종호

1978년 경북대학교 학사(공학사)
1981년 경북대학교 전자공학과 석사(공학석사)
1990년 경북대학교 전자공학과 박사(공학박사)
1981년~현재 부경대학교 컴퓨터공학과 교수

1987년~1988 Dept of CS RPI USA, Visiting Scholar
2001년~2002년 Dept of EECE LSU, Visiting Professor
2008년~2009년 CUNY USA, Visiting Professor
관심분야: Embedded System, Image Recognition, VLS Array Processing