# 상관도와 임계치 방식을 이용한 다중검출 비대칭 워터마킹

정회원 이 덕*, 김 종 원**, 최 종 욱***

# Hybrid Asymmetric Watermarking using Correlation and Critical Criteria

De Li*, Jong-Weon Kim**, Jong-Uk Choi*** *Reguler Member*

요 약

기존의 워터마킹 기술은 대부분 삽입과 검출에서 동일한 키를 사용하는 대칭 키 방식이다. 이러한 대칭 키 워터마킹 방식은 검출을 쉽게 할 수 있는 반면에 공격자에 의하여 검출기의 비밀키 정보가 유출될 경우 삽입 정보가 제거되거나 변조되는 치명적인 공격을 받을 수 있다. 따라서 최근에는 삽입기에서 비밀키를 사용하여 삽입하고 검출기에서 공개키를 이용하여 검출하는 비대칭 워터마킹(Asymmetric Watermarking) 방식이 차세대 워터마킹 기술로 주목을 받고 있다.

본 논문에서 제안하는 상관도와 임계치 방식은 각기 단일 방식으로 사용할 수 있는 방식이며 결합하여 다중검출 방식으로도 사용할 수 있다. 다중 검출방식으로 사용할 경우 동일한 공개키를 이용하여 검출기에서 상관도 방식과 임계치 방식으로 상호 보완적이며 신뢰성이 있는 검출을 할 수 있다. 키 생성과정에서는 안전한 선형 변환방식과 특수행렬을 이용하여 개인키와 공개키를 생성하였고 높은 상관도 검출이 가능하도록 구성되었다.

실험결과 공개키 검출 성능 및 대칭 키 방식과의 검출 성능 비교 등을 통하여 다양한 측면에서 제안 방식의 정확성을 확인하였다. 또한 워터마크가 삽입된 영상에서 1bit의 정보뿐만 아니라, 멀티 bit의 삽입정보에 대한 공개키 상관도 검출과 임계치 검출이 정확히 이루어짐을 확인할 수 있었으며 JPEG 및 JPEG200 압축에도 강인함을 보였다.

**Key Words :** 상관도 검출(correlation detection), 임계치 검출(critical criteria), 다중검출(hybrid detection), 공개키(public key), 비대칭(asymmetric)

ABSTRACT

Traditional watermarking technologies are symmetric method which embedding and detection keys are the same. Although the symmetric watermarking method is easy to detect the watermark, this method has weakness against to malicious attacks remove or modify the watermark information when the symmetric key is disclosure. Recently, the asymmetric watermarking method that has different keys to embed and detect is watched by severalresearchers as a next generation watermarking technology.

In this paper, hybrid asymmetric watermarking algorithm is proposed. This algorithm is composed of correlation detection method and critical criteria method. Each method can be individually used to detect

* 상명대학교 디지털저작권보호연구센터 연구원 (lide!smu.ac.kr)
** 상명대학교 디지털저작권보호연구센터 책임연구원
*** 상명대학교 소프트웨어대학 교수
논문번호 : KICS2005-05-200, 접수일자 : 2005년 5월 17일
※ 본 논문은 과학기술부 국제공동연구 지원사업에 의하여 연구되었음.

watermark from a watermarked content. Hybrid asymmetric detection is complement between two methods, and more feasible than when each method is used respectively. Private key and public key are generated by secure linear transformation and specific matrix.

As a result, we have proved the proposed algorithm is secured than symmetric watermarking algorithms. This algorithm can expand to multi bits embedding watermark system and is robust to JPEG and JPEG2000 compression.

## Ⅰ. 서 론

최근 다양한 멀티미디어 콘텐츠의 디지털화, 인터넷과 같은 디지털 통신망의 급속한 발전으로 멀티미디어 데이터가 매우 빠르고 쉽게 배포되고 있다. 미디어에 대한 디지털화 추세는 편집, 전송 및 저장 시의 편리함으로 더욱 가속화되고 있으며 문헌, 영상, 음성 등이 디지털화 되면서 누구나 손쉽게 그 매체들이 저장되어 있는 시스템을 이용하여 복사할 수 있게 되었다. 그러므로 사용하고자 하는 정보의 전송 문제, 사용자가 그 정보를 사용하는데 필요한 허가와 보상의 문제와 제한의 문제, 그리고 그 정보를 소유하고 있는 기관의 권리 등 다양한 문제가 발생할 수 있다. 이러한 문제들의 해결책의 하나로 디지털 워터마킹 기술이 주목을 받고 있다. 이 기술은 네트워크 상에서 널리 배포, 유통될 수 있는 멀티미디어 데이터 및 출판물과 같이 지적 재산권 보호 대상 성격을 지니는 자료에 대해 원 데이터에 관리 및 인증을 위한 추가적인 정보를 삽입하여 멀티미디어에 대한 지적 재산권을 보호하기 위한 기법이다.

기존의 워터마킹 방식들에는 삽입된 워터마크를 제거하거나 위, 변조하는 등 다양한 형태의 공격들이 존재한다. 이러한 공격의 원인중의 하나는 기존의 워터마킹 시스템이 삽입기와 검출기에서 동일한 키 정보를 사용하는 대칭키 방식을 사용하기 때문이다. 대칭키 방식의 워터마킹 시스템에서 워터마크에 대한 검증자가 검출기에서 워터마크 정보를 유출하여 삽입된 워터마크 정보를 제거하려는 공격을 할 수 있다. 이러한 공격에 대응하기 위해서는 워터마크의 삽입과 추출 시 서로 다른 정보를 사용하는 비대칭 워터마킹 기술이 필요하다.

본 논문에서는 각기 단일 방식으로 사용할 수 있는 상관도 검출 방식과 임계치 검출 방식을 제안하며, 또 동일한 공개키를 이용하여 상관도 검출과 임계치 검출을 동시에 진행할 수 있는 상호 보완적인 다중 검출 방안을 제안한다. 키의 생성과정에서는 높은 상관도 검출과 임계치 검출이 가능하도록 안전한 선형변환방식과 특수행렬을 사용하여 구성하였으며, 안전성 측면에서 공개키로부터 개인키 정보의 유출이 어렵게 하였다. 또한 두 가지 검출 방식을 동시에 진행 할 수 있어 신뢰성 있는 검출을 할 수 있으며 부분적인 공격 노출에 효과적으로 대처할 수 있게 된다. 본 방식은 1bit의 정보 뿐만 아니라 멀티 bit의 정보를 삽입하고 정확하게 검출될 수 있도록 구성 되었으며, JPEG압축에도 강인한 것으로 나타났다. 또한 본 제안 방식은 다양한 멀티미디어 콘텐츠에 적용 가능한 원천 기술이다.

본 논문의 구성은 2장에서는 비대칭 워터마킹 기술과 기존 연구들을 살펴보며, 3장에서는 제안하는 비대칭 워터마킹 방식을 소개하며, 4장에서는 본 제안된 방식의 실험결과를 보여주며, 5장은 결론에 대해 기술한다.

## Ⅱ. 비대칭 워터마킹 기술

비대칭 워터마킹 방식은 공개키 검출방식으로, 공개키 암호 시스템과 유사하게 콘텐츠의 저작권 소유주가 개인키와 공개키를 생성하여 정보 삽입에 개인키를 사용하고, 검증자가 검출 시에 공개키를 사용하여 비밀키의 삽입여부를 검증하는 방식이다. 개인키와 공개키의 생성은 다양한 방법이 있을 수 있으나 어떠한 경우에서든지 공개키 또는 공개키와 개인키가 삽입된 신호로부터 개인키 정보를 추출해 낼 수 없어야 하며, 공개키로부터 개인키의 삽입여부를 정확히 검증해 낼 수 있어야 한다.

최근에 여러 가지 방식의 비대칭 워터마킹 방식들이 제안되었는데, 그 중 몇 가지 대표적인 방식들에 대해 소개하도록 한다.

Van Schyndel[1]은 Legendre 수열의 변환을 이용하여 비대칭 워터마킹을 구현하였다. 이 방식은 Legendre 수열은 이산 푸리에 변환을 하면 같은 수열의 켤레 형태를 얻을 수 있다는 특성을 이용하였다. 이 방식에서는 상관도 값이 Legendre 수열의 상관도 값으로 표현되므로 Legendre 길이만을 이용하여 워터마크 검출이 가능하게 된다.

Choi[2]는 선형변환을 이용한 비대칭 워터마킹 방식을 제안하였다. 이 방식에서는 하나의 원시 키를 먼저 생성한 뒤 선형 랜덤 변환 행렬을 이용하여 비밀키와 공개키를 생성해 내게 된다. 검출기에서는 공개키를 이용하여 상관도 검출을 하게 되는데 상관도 계산 과정에서 비밀키와 공개키의 변환 행렬이 상쇄되고 결과적으로 원시 키의 상관도로 표시되므로 공개키를 이용하여 워터마크의 검출이 가능하게 된다. 이 방식에서는 공개키 만 공개되며 선형변환 행렬과 원시 키는 공개되지 않는다.

Picard[3]는 신경망 함수를 이용한 비대칭 워터마킹 방식을 제안하였다. 이 방식은 N크기의 입력을 받아 M크기로 출력하는 선형 신경망 함수를 이용하여 N공간의 비밀키를 M공간으로 압축시킨다. 이는 암호에서와 유사하게 하나의 공개키에 대하여 (N-M)차원 만큼의 비밀키가 존재하므로 비밀키의 탐색이 가능하지 않도록 하는데 목적을 두고 있다. 워터마크의 삽입은 원본 데이터에 비밀키를 삽입하고, 검출 과정에서는 워터마크가 삽입된 신호를 같은 방식으로 신경망 함수에 입력하여 얻은 값과 공개키와의 상관도를 구하게 된다. 신경망 함수는 선형이외에 비 선형을 사용할 수 있으며 다단계 층을 거칠 수 도 있으나 비선형에 가까워질수록 안전성이 강화되지만 검출 성능이 떨어지게 된다. 따라서 안전성과 검출 성능 사이에 조절이 필요하다.

이외에도 Smith[4]는 같은 워터마크를 두 번 삽입하여 두 부분의 상관도를 계산하여 검출하는 간단한 형태의 방식을 제안하였고, Furon[5]은 전력밀도 스펙트럼방식을 이용하여 스펙트럼의 모양으로 워터마크의 삽입 여부를 검증하는 비대칭 워터마킹 방식을 제안하였다. 그 외에도 Craver S[6,7], Adelsbach A[8,9] 등은 암호학적인 프로토콜을 이용한 비대칭 워터마킹 시스템을 제안하였다. 이러한 기존의 방식은 대부분 효과적이며 신뢰성 있는 검출에 다소 한계가 있으며 다양한 유형의 공격에도 적절하게 대응할 수 없는 단점을 안고 있다.

## Ⅲ. 제안한 비대칭 워터마킹 방식

### 3.1 개인키 및 워터마크 생성

개인키 S는 식(1)과 같이 선형변환을 이용하여 비밀키 Sr로부터 생성되는데 의사 랜덤수열의 자기상관특성을 이용하기 위하여 Sr은 n*n 랜덤 행렬을 사용한다. 즉 $S_{r,j}{}^{t}S_{r,i} = \delta_{ij}$ 이고 $\delta_{ij}$는 Kronecker delta이다.

$$S = QS_r \tag{1}$$

여기서 계산 복잡도와 안전성을 위하여 직교행렬 Q를 사용하게 되는데 상관도 값 계산 시에 직교행렬의 전치행렬은 역 행렬과 같다는 특성을 이용하게 된다.

워터마크는 아래의 식(2)에서와 같이 생성되는데 여기서 m은 삽입 비트 정보로서 m∈{-1,1}의 값을 취하며 m이 1일 경우는 bit 1이, m이 1일 경우는 bit 0이 삽입됨을 의미한다. $\alpha$는 워터마크 삽입 강도이며 S는 개인키이다.

$$W = \alpha m S \tag{2}$$

$$I_i(w) = I_i + W_i \tag{3}$$

워터마크의 삽입은 식(3)과 같이 n*n의 정보삽입 블록에 워터마크를 삽입하게 된다. Ii와 Ii(w)는 정보 삽입블록과 워터마크가 삽입된 블록이다. Wi는 하나의 정보삽입 블록에 삽입되는 워터마크 신호이다. 검출 시 하나의 n*n 블록에서 1bit의 정보를 검출하게 된다.

### 3.2 공개키의 구성

비대칭 워터마킹 시스템의 공개키 P는 아래의 식(4)에서와 같이 지수 함수식을 이용하여 구성하게 된다.

$$P_i = r^{H_i} \cdot g^{K_i} \tag{4}$$

$$H = QU^{t}US_r \tag{5}$$

여기서 r과 g는 임의의 큰 양수이고 Ki는 n*n 임의의 랜덤 행렬의 한 원소이다. H는 식(5)에서와 같이 생성되며, U는 임의의 랜덤 행렬이다. Q는 식(1)에서 사용된 직교행렬이고 Sr은 비밀키이다. P는 n*n 행렬이며 식(4)는 행렬 P의 한 원소를 구하는 계산식이 된다.

### 3.3 공개키를 이용한 상관도 방식의 검출

공개키를 이용한 상관도 검출 방식에서는 공개키 P의 로그 값을 취하여 워터마크가 삽입된 신호와의 상관도를 구하게 되는데 그 계산과정은 아래와 같다.

$$\begin{aligned} C &= (\log P)^{t} I(w) = (H\log r + K\log g)^{t} I(w) \\ &= ((\log r)^{t} S_r{}^{t} U^{t} U Q^{t} + (\log g)^{t} K^{t}) I \\ &\quad + ((\log r)^{t} S_r{}^{t} U^{t} U Q^{t} + (\log g)^{t} K^{t}) N \end{aligned}$$

$$+\alpha m(\log g)' K' S_r + \alpha m(\log r)' S_r' U' U Q' Q S_r$$
$$\approx \alpha m \log r(S_r' U' U S_r) = \alpha m \log r(U S_r)' U S_r \quad (6)$$

식(6)의 네 번째 항에서 직교행렬 Q의 전치행렬은 역 행렬과 같으므로 QtQ=Q-1Q=1이 되어 결과적으로 USr 의 상관도 값으로 나타나게 된다. 그 외의 항들에선 거의 상관도가 발생하지 않으며 상대적으로 네 번째 항에 비해 아주 작은 값으로 나타나게 되어 상관도 값 C는 근사하게 네 번째 항의 값으로 표현가능하며, USr의 상관도 값 만으로 워터마크의 삽입 여부를 판단할 수 있게 된다. 이렇게 되어 상관도 검출과정에서 개인키 정보를 직접 사용하지 않고 공개키 정보만을 이용하여 검출이 가능하며, 공개키 정보로부터 개인키 정보를 계산하는 것은 매우 어렵게 된다.

### 3.4 공개키를 이용한 임계치 방식의 검출

상관도 검출에서 사용된 공개키 P를 이용하여 임계치 방식으로도 검출할 수 있는데 우선 공개키 P와 워터마크가 삽입된 신호 I(w)를 이용하여 다음과 같은 방식으로 임계치 검증 값 V를 계산하게 된다.

$$V = r^{C_0} \cdot g^a = \prod_{i=1}^{n \times n} (p_i^{I(w)_i}) \quad (7)$$

여기서 식(7)의 좌측의 $V = r^{C_0} \cdot g^a$ 값은 우측의 공개키와 워터마크가 삽입된 신호의 함수 값으로 표현 된다. 이렇게 함으로써 공개된 정보만으로 V 값을 구성할 수 있게 된다.

$$C_0 = \sum_{i=1}^{n \times n} H_i \cdot I(w)_i, \quad a = \sum_{i=1}^{n \times n} k_i \cdot I(w)_i \quad (8)$$

식(7)에서의 C0와 a는 식(8)에서와 같이 표현된다. 식(8)로부터 C0는 H의 상관도 값으로 표현됨을 알 수 있으며, C0는또 다음과 같이 표현할 수 있다.

$$\begin{aligned} C_0 &= (H)' I(w) = (QU' U S_r)' I(w) \\ &= (S_r' U' U Q') I + (S_r' U' U Q') N \\ &\quad + \alpha m(S_r' U' U Q' Q S_r) \\ &\approx \alpha m(S_r' U' U S_r) \\ &= \alpha m(U S_r)' U S_r = \alpha m \sum_{i=1}^{n \times n} (U S_r)^2 \end{aligned} \quad (9)$$

식(9)는 식(6)과 유사하게 세 번째 항에서 직교행렬 Q의 전치행렬은 역 행렬과 같으므로 QtQ=Q-1Q=1

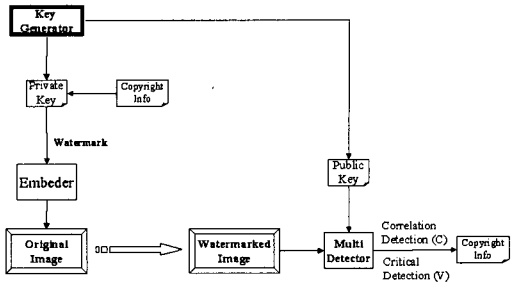



그림 1. 다중 검출 비대칭 워터마킹 시스템 구성도

이 되어 결과적으로 USr 의 상관도 값으로 나타나게 된다. 그 외의 항들에선 거의 상관도가 발생하지 않으며 상대적으로 세 번째 항에 비해 아주 작은 값으로 나타나게 되어 상관도 값 C는 근사하게 세 번째 항의 값으로 표현 가능하다. 또 m∈{-1,1}이므로 삽입된 bit가 1bit의 경우 C0는 아주 큰 양수, 0bit의 경우에는 아주 작은 음수 값을 가지게 되며 워터마크가 삽입되지 않았을 경우에는 영에 가까운 아주 작은 양수 값을 가지게 됨을 알 수 있다.

따라서 식(9)을 이용하면 삽입된 bit에 따라 식(7)로부터 계산된 V값이 현저한 차이를 보여 V값으로 워터마크의 삽입여부와 삽입 bit를 판단할 수 있게 된다. 식(7)로부터 실제로 V값은 공개키와 워터마크가 삽입된 신호만으로 계산 가능하므로 개인키 정보를 직접 사용하지 않고도 검출이 가능하게 된다.

본 논문에서 제안하는 상관도 검출 방식과 임계치 검출 방식은 각기 단독으로 사용 가능한 방식이며 결합하여 하나의 다중 검출 방식으로도 사용 가능하다. 다중 검출 방식으로 사용될 경우 이중으로 검출 할 수 있게 되어 상호 보완적인 방식으로 사용될 수 있으며 신뢰성 있는 검출을 진행할 수 있게 된다.

그림 1은 다중 검출 비대칭 워터마킹 시스템 구성도로서 삽입기에서 개인키와 공개키를 생성하고, 또 개인키와 저작권 정보를 이용하여 워터마크를 생성하며 워터마크는 원본 이미지에 삽입 된다. 삽입기에서 생성된 공개키는 워터마크가 삽입된 이미지와 함께 검출기에 전달되며 검출기에서는 이 공개키를 이용하여 상관도 검출 또는 임계치 검출을 진행하게 된다.

## Ⅳ. 실험 결과

본 제안 방식의 구현과정에서 512*512의 "lena" 이미지를 사용하여 공간영역에 삽입하였다. 1bit의

그림 2. 원본 영상(left)와 워터마크가 삽입된 영상(right)

정보의 삽입 시에는 정보삽입 블록으로 128*128블록을 사용하였으며, 멀티bit의 삽입에는 64*64의 블록을 사용하였다. 삽입 영상의 PSNR값은 그림 2에서와 같이 44.93으로 나타났다.

실험에서 상관도 값의 계산과정은 아래의 식(10)에서와 같이 푸리에 변환을 사용하여 고속으로 진행하게 된다.

$$C = R(IFFT(FFT(I(w)) * CONJ(FFT(P)))) \quad (10)$$

여기서 FFT와 IFFT는 푸리에 변환과 역 푸리에 변환을 의미하며 CONJ는 Conjugation을 의미한다. R은 실수를 취함을 나타내고 "*"는 행렬의 원소 대 원소의 곱셈을 표시한다.

그림 3은 개인키와 공개키의 상관도 값을 정규화한 검출결과로서 위쪽이 개인키 검출 결과(Cmax=0.99, Csnd=0.04)이고 아래쪽이 공개키 검출결과(Cmax=0.98, Csnd=0.06)이다.

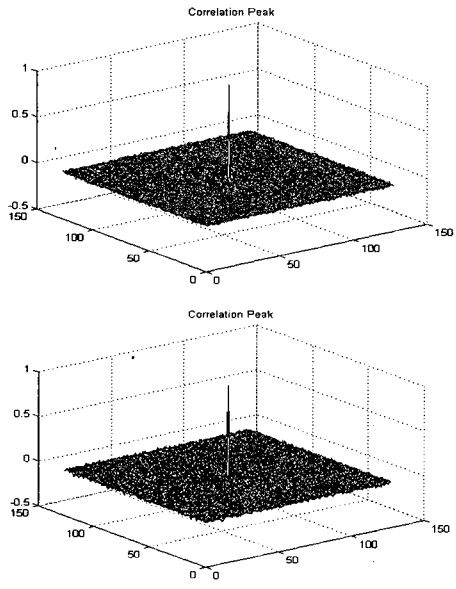



그림 3. 개인키와 공개키의 상관도 검출 (정규화)

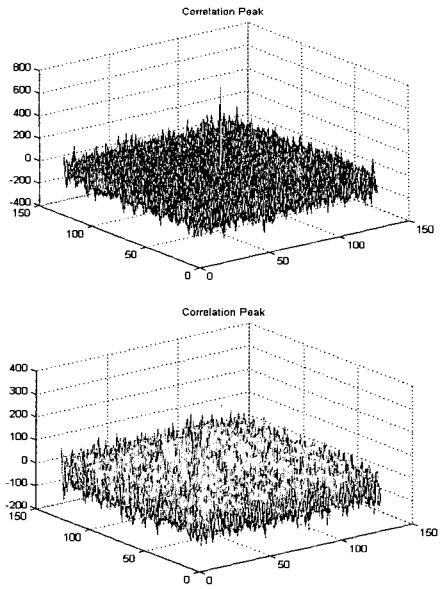



그림 4. JPEG압축에 따른 개인키와 공개키의 상관도 검출 (QF=65%)

그림 4는 JPEG압축 후의 개인키와 공개키의 상관도 검출결과로서 정규화를 하지 않은 값이다. 위쪽이 개인키 검출 결과(Cmax=777.7, Csnd=235.2)이고 아래쪽이 공개키 검출결과(Cmax=314.6, Csnd=165.87)이다. 여기서 Cmax와 Csnd는 각각 가장 큰 값인 상관도 Peak값과 상관도 값 중 두 번째로 큰 값이다. 이 실험에서 JPEG압축 QF(Quality Factor)는 65%를 사용하였다. 수치적으로 볼 때 공개키 상관도 검출이 개인키 상관도 검출에 비해 다소 적은 값들로 나타났으나 Peak값으로부터 문제없이 검출할 수 있으며 압축 후에도 비교적 우수한 검출 성능을 보여주고 있다.

그림 5는 JPEG압축의 QF(Quality Factor)에 따른 공개키의 검출 성능을 보여준다. 그림에서 실선으로 표시된 부분이 Cmax이고 점선으로 표시된 부분이 Csnd이다. 여기서 QF의 감소에 따라 Cmax와 Csnd의 사이가 점차 축소되고 있어 검출 성능이 떨어지며, QF=90% 정도의 지점에서는 이 차이이가 급격이 작아지고 있음을 알 수 있다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)

그림 6은 JPEG압축의 QF(Quality Factor)에 따른 비밀키(실선), 개인키(굵은점선), 공개키(가는점선)의 Cmax을 보여줌으로써 QF에 따른 대칭 및 비 대칭 워터마킹 시스템의 검출 성능을 비교하였다. 여기서 알 수 있듯이 비 대칭 방식의 개인키 검출이 대칭

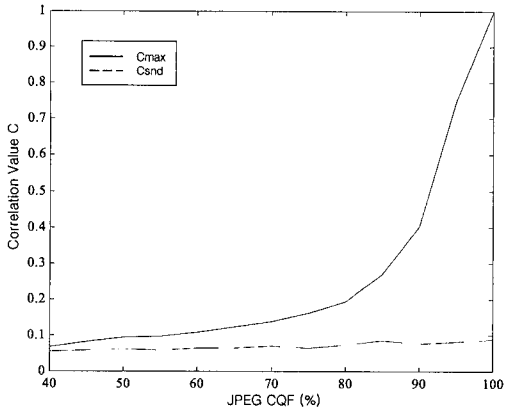



그림 5. QF에 따른 공개키의 상관도 검출 성능

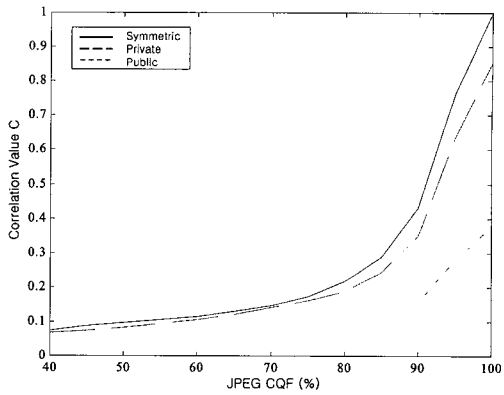



그림 6. QF에 따른 대칭 및 비대칭 워터마킹 시스템의 상관도 검출성능

방식의 비밀키 검출에 근사하게 접근하고 있으며 공개키 검출은 비밀키와 개인키 검출 값 보다는 다소 낮은 값으로 나타났다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)

표 1은 삽입강도에 따른 PSNR값과 공개키 검출 결과를 보여준다. $\alpha$값이 작아지면 전반적으로 검출 성능이 떨어지게 되며, 특히 JPEG압축의 경우에는 $\alpha$값이 3보다 작을 경우 공개키 검출이 어려워지게 됨을 알 수 있다.

표 1. 삽입강도에 따른 공개키 상관도 검출 성능

| Alpha | PSNR | Lena.bmp | | Lena.jpg | |
|---|---|---|---|---|---|
| | | Cmax | Csnd | Cmax | Csnd |
| 1 | 58.91 | 1454.7 | 204.6 | 163.2 | 163.3 |
| 2 | 52.89 | 2866.0 | 295.1 | 153.7 | 153.7 |
| 3 | 49.37 | 4277.0 | 385.7 | 173.5 | 157.6 |
| 5 | 44.93 | 7099.3 | 566.9 | 314.6 | 165.9 |
| 7 | 42.01 | 9921.5 | 748.2 | 382.2 | 162.5 |
| 9 | 39.83 | 12744 | 929.7 | 482.5 | 165.9 |
| 11 | 38.08 | 15567 | 1111.3 | 662.5 | 166.7 |

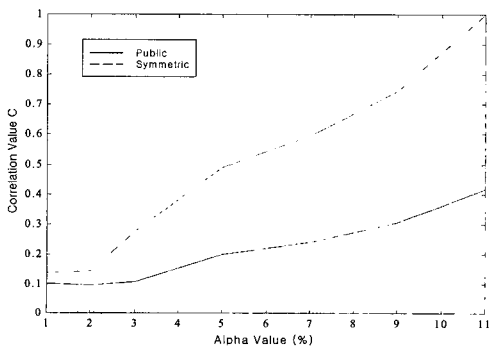



그림 7. 삽입강도에 따른 대칭 및 비대칭 워터마킹 시스템의 상관도 검출성능 (JPEG)

표 2. 영상 및 압축에 따른 공개키 검출 성능

| Format | CV | Lena | Baboon | Peppers |
|---|---|---|---|---|
| BMP | Cmax | 0.983 | 0.997 | 0.989 |
| | Csnd | 0.044 | 0.075 | 0.061 |
| JPG | Cmax | 0.049 | 0.178 | 0.062 |
| | Csnd | 0.019 | 0.065 | 0.038 |
| J2K | Cmax | 0.298 | 0.419 | 0.372 |
| | Csnd | 0.035 | 0.057 | 0.044 |

그림 7은 JPEG압축 이미지를 대상으로 삽입강도에 따른 공개키(실선)와 비밀키(점선)의 Cmax을 보여줌으로써 삽입강도에 따른 대칭 및 비대칭 워터마킹 시스템의 상관도 검출 성능을 비교하였다. 여기서 삽입강도의 증가에 따라 비밀키의 상관도 값이 공개키의 상관도 값 보다 다소 빠른 폭으로 증가하고 있음을 알 수 있다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)

표 2는 영상별로 bmp와 jpg, jpeg2000 등 포맷에 따른 공개키의 검출 성능을 보여준다. Cmax와 Csnd 차의 값을 검출 성능으로 하여 비교할 경우 우선 영상별로 보면 bmp 포맷에서는 Lena 이미지가 조금 높은 성능을 보였고, jpg와 j2k 포맷에서는 고 주파수 성분이 강한 Baboon 이지지가 가장 높은 검출 성능을 보였다. 압축에 따른 성능을 비교해 보면 bmp 포맷이 가장 높은 검출 성능을 보여주며, 다음으로 j2k, jpg의 순으로 되어있음을 확인할 수 있다.

그림 8은 멀티비트 검출 시 64*64블록에서 공개키의 상관도 검출한 결과로서 1bit(위쪽, Cmax=2335.9, Csnd=420.2)와 0bit(아래쪽, Cmax=-2318.6, Csnd=-383.7)의 임의의 두 블록을 선택하여 그 결

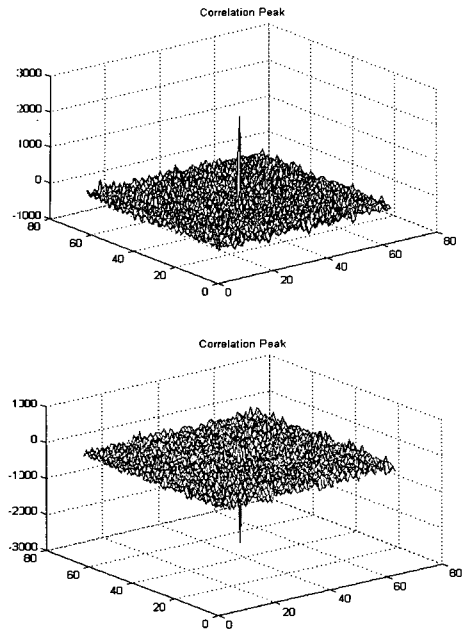



그림 8. 멀티비트 공개키 상관도 검출

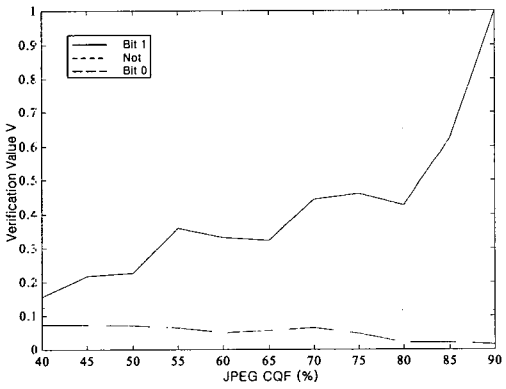



그림 9. QF에 따른 임계치 검출 성능

과를 보여준다. 멀티비트를 삽입할 경우 블록 size가 작아지는 관계로 Cmax 값이 현저히 떨어지기는 하나 Csnd와의 차이로 별 어려움 없이 검출이 가능함을 알 수 있다. 여기서는 512*512 이미지에서 64*64블록을 사용하여 bit정보를 삽입하였으므로 64bit의 정보를 삽입하고 추출할 수 있게 된다.

그림 9는 QF에 따른 1bit(실선), 0bit(굵은 점선)와 워터마크가 삽입되지 않은 경우(가는 점선)의 V값을 보여줌으로써 임계치 방식의 검출 성능을 비교하였다. 여기서 임계치 방식으로 bit의 삽입여부와 삽입 bit를 판단할 수 있음을 확인할 수 있으며 QF가 감소됨에 따라 이들의 차이가 점차 감소됨을 확인할 수 있다. 특히 QF=80% 지점에서는 그 차이가 급격히 감소됨을 알 수 있다. 하지만 워터마크가 삽입되지 않은 경우의 V값을 기준으로 적당한 임계치를 설정할 경우 정확한 검출을 할 수 있게 된다. (이 그래프에서는 V값을 정규화 하여 얻을 결과를 적용하였음.)

표 3은 삽입 강도에 따른 임계치 방식의 검출 결과(검증 값 V)로서 삽입 강도 Alpha가 1이나 2일 경우를 제외하고 워터마크의 삽입여부나 삽입 비트를 정확히 검출해 낼 수 있음을 보여준다.

표 4는 대칭 및 비대칭 워터마킹 시스템의 워터마크 삽입 및 검출 속도 비교 결과를 보여주는데 삽입과 검출속도의 측정 시 각각 1000번 삽입과 검출을 수행하여 그 평균치를 계산하였다.(상관도 검출)

워터마크 삽입단계에서 비대칭 방식의 경우에는 개인키 및 공개키 계산 과정이 포함하게 되므로 대칭 방식에 비해 속도가 다소 떨어지게 된다.

검출단계에서는 검증자가 전송 받은 비밀키 또는 공개키를 직접 이용하여 상관도 계산식으로부터 상관도 검출을 하게 되므로 대칭 및 비대칭 방식의 검출 속도에는 차이가 없게 된다. 이외에 하나의 워터마크를 삽입하는 삽입 단위인 삽입블록에 따라 결과치가 다소 차이가 있음을 알 수 있다. 삽입블록이 작으면 matrix 관련 연산이 빠르게 진행되어 삽입 또는 검출 속도가 향상되는 반면에 삽입 블록이 너무 작으면 상관도 검출 성능은 다소 떨어질 수 있다.

표 3. 삽입강도에 따른 임계치 방식의 검출 성능

| Alpha | PSNR | 1bit 삽입 | 미삽입 | 0bit 삽입 |
|---|---|---|---|---|
| 1 | 58.91 | 3.3038 | 2.1043 | 1.3348 |
| 2 | 52.89 | 2.0546 | 0.3354 | 0.0547 |
| 3 | 49.37 | 3.1786 | 0.0535 | 9.11e-04 |
| 5 | 44.93 | 114.8646 | 0.0014 | 1.65e-08 |
| 7 | 42.01 | 1.55e+05 | 3.45e-05 | 8.02e-15 |
| 9 | 39.83 | 7.94e+09 | 8.76e-07 | 1.03e-22 |
| 11 | 38.08 | 1.52e+16 | 2.22e-08 | 3.57e-32 |

표 4. 워터마크 삽입 및 검출속도 비교

| 삽입 블록 | 워터마크삽입 | | 워터마크 검출 | | |
|---|---|---|---|---|---|
| | 대칭 | 비대칭 | 대칭 | 비대칭(공) | 비대칭(개) |
| 128 | 0.17s | 0.21s | 0.15s | 0.24s | 0.18s |
| 64 | 0.15s | 0.16s | 0.06s | 0.08s | 0.07s |

## V. 결 론

기존의 대부분의 워터마킹 방식은 삽입기와 검출기에서 동일한 비밀키 정보를 사용하는 대칭 키 방식을 사용하고 있다. 하지만 이러한 대칭 방식은 검출기에서 비밀 정보가 유출되었을 경우 워터마크의 제거로 검출 불가 또는 위,변조 등의 심각한 공격으로 이어질 수 있다. 때문에 최근 워터마킹 시스템의 안전성 제고를 위하여 삽입과 검출 시에 서로 다른 키 정보를 사용하며, 또 검출 키로부터 삽입 키 정보를 추출해 낼 수 없도록 하는 비대칭 워터마킹 방식이 새롭게 주목 받고 있다.

본 논문에서는 각기 단일 방식으로 사용 가능한 상관도 검출 방식과 임계치 검출 방식을 제안하며, 동일한 공개키를 이용하여 상관도와 임계치 검출이라는 서로 다른 두 가지 방식으로 워터마크를 검출할 수 있는 상호 보완적인 다중 검출방식을 제안하였다. 공개키의 생성과정에서는 선형 행렬변환과 특수행렬을 이용하여 높은 상관도 검출이 가능하도록 공개키를 생성하였으며 공개키로부터 개인키를 유출할 수 없도록 구성하였다. 또한 동일한 공개키로 상관도 검출과 임계치 검출 방식을 동시에 사용함으로써 신뢰성 있는 검출을 진행 할 수 있게 되었다. 실험결과 Quality Factor, 삽입강도 등에 따른 공개키 검출 성능 및 대칭 키 방식과의 검출 성능 비교 등을 통하여 다양한 측면에서 제안 방식의 정확성을 확인하였다. 또한 1bit의 정보와 멀티 bit 정보의 검출 시 모두 신뢰성 있는 검출을 할 수 있어 높은 검출 성능을 보여주었으며 JPEG 및 JPEG200압축 등에도 강인한 것으로 나타났다.

## 참 고 문 헌


[1] R. G. Van Schyndel, A. z. Tirkel, and I. D. Svalbe, "Key independent watermark detection,"in Proc, of the IEEE Intl. Conf, on Multimedia Computing and Systems, vol. 1, pp. 580-584, Florence, Italy, June 1999.

[2] H. Choi, K, Lee, and T. Kim, "Transformed-key asymmetric watermarking system," in Proc. of SPIE: Security and Watermarking of Multimedia Contents, vol. 4314, pp. 280-289, San Jose, USA, Jan. 2001.

[3] J. Picard and A. Robert, "Neural Networks functions for public key watermarking," in Workshop on Information Hiding, pp. 142-156, Pittsburgh, PA, USA, Apr, 2001.

[4] J. Smith and C. Dodge, "Development in steganography," in Workshop on Information Hiding, pp. 77-87, Dresden, Germany, Oct, 1999.

[5] T. Furon and P. Duhamel, "An asymmetric public detection watermarking technique," in Workshop on Information Hiding, pp. 88-100, Dresden, Germany, Oct, 1999.

[6] Craver S, Katzenbeisser S, "Copyright protection protocols based on asymmetric watermark: The ticket concept," in Proceedings of the 6th Conference on Communication and Multimedia Security (CMS'01), pp. 159-170, 2001.

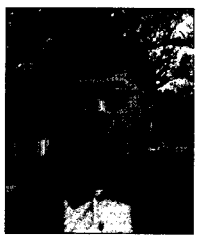
[7] Craver S, "Zero knowledge watermark detection," in International Workshop on Information Hiding (IHW'99), Lecture Notes in Computer Science 1768, pp. 101-116, 1999.

[8] Adelsbach A, Sadeghi AR, "Zero-Knowledge watermark detection and proof of ownership," in International Workshop on Information Hiding (IHW'2001) Lecture Notes in Computer Science 2137, pp. 273-288, 2001.

[9] Adelsbach A, Katzenbeisser S, Sadeghi AR, "Cryptography meets watermarking detecting watermarks with minimal or zero knowledge disclosure," in Proceedings of the European Signal Processing Conference (EUSIPCO' 2002), 2002.



이 덕(Li De) 정회원



1996년(중) 할빈이공대학교 전기공학과 (공학사)

2001년 상명대학교 전자계산학과 (이학석사)

2005년 상명대학교 컴퓨터과학과 (이학박사)

<관심분야> 디지털워터마킹, 저작권관리기술, 디지털신호처리, 컴퓨터시스템 및 네트워크보안

**김 종 원**(Jong-Weon Kim) 정회원

1989년 서울시립대학교 전자공학과(공학사)
1991년 서울시립대학교 전자공학과(공학석사)
1995년 서울시립대학교 전자공학과(공학박사)
1996년~2000년 주성대학 정보통신학과 조교수
2000년~2004년 (주)마크애니 부설연구소장
2005년~현재 상명대학교 디지털저작권보호연구센터 책임연구원
<관심분야> 디지털워터마킹, 저작권보호 및 관리기술, 디지털신호처리

**최 종 욱**(Jong-Uk Choi) 정회원

1982년 아주대학교 산업공학과(공학사)
1982년 서울대학교 경영학과(석사과정)
1986년~1987년 Johnson C. Smith University, Computer System Specialist
1988년 University of South Carolina(MIS. Ph.D)
1988년~1991년 한국과학기술연구원 시스템공학연구소 선임연구원, 실장
1991년~현재 상명대학교 소프트웨어대학 교수
2000년~현재 (주)마크애니 대표이사
<관심분야> 디지털워터마킹, 저작권보호 및 관리기술, 정보보호응용기술