

상관도 검출기반의 안전한 비대칭 워터마킹

이 덕[†] · 김 종 원^{**} · 최 종 욱^{***}

요 약

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

본 논문에서는 선형 연립방정식의 해집합을 이용하여 개인 키의 탐색 공간을 효과적으로 확장하였다. 또한 공개 키로부터 개인 키를 유출할 수 없도록 하기 위하여 공개 키의 생성은 안전한 선형변환 방식에 기초하였으며 높은 상관도 검출이 가능하도록 구성되었다. 실험결과 워터마크가 삽입된 영상에서 1bit의 정보 뿐만 아니라, 멀티 bit의 정보에 대한 공개 키 상관도 검출이 정확히 이루어짐을 확인할 수 있었으며 JPEG 압축 후에도 높은 상관도 검출이 가능한 것으로 나타났다.

키워드 : 개인 키, 공개 키, 상관도검출, 비대칭

Secure Asymmetric Watermarking Based on Correlation Detection

De Li[†] · JongWeon Kim^{**} · JongUk Choi^{***}

ABSTRACT

Traditional watermarking technologies are symmetric method which embedding and detection keys are same. Although the symmetric watermarking method is easy to detect the watermark, this method has weakness against to malicious attacks to 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 several researchers as a next generation watermarking technology.

In this paper, we have expanded search space of secret key using the solution set of linear simultaneous equations. Secret key is generated by secure linear transformation method to prevent of guessing secret key from public key, and the correlation value between secret key and public key is high. At the results, the multi bits information can be embedded and high correlation value was detected after JPEG compression.

Key Words : Private Key, Public Key, Correlation Detection, Asymmetric

1. 서 론

최근 디지털 미디어의 보편화와 전자출판, 컴퓨터, 통신, 멀티미디어 등 산업의 급격하고 광범위한 성장, 그리고 다양한 멀티미디어 콘텐츠의 디지털화, 인터넷과 같은 디지털 통신망의 급속한 발전으로 멀티미디어 데이터가 매우 빠르고 쉽게 배포되고 있다. 미디어에 대한 디지털화 추세는 편집,

전송 및 저장시의 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 대하여 원 데이터에 관리 및 인증을 위한 추가적인 정보를 삽입하여

※ 과학기술부 국제공동연구 지원사업

† 준 회 원 : 상명대학교 컴퓨터과학과 박사과정

** 정 회 원 : 상명대학교 디지털저작권보호연구센터 책임연구원

*** 종신회원 : 상명대학교 소프트웨어대학 교수

논문접수 : 2005년 3월 4일, 심사완료 : 2005년 5월 6일

멀티미디어에 대한 지적 재산권을 보호하기 위한 기법이다.

기존의 워터마킹 방식에는 삽입된 워터마크를 제거하거나 검출이 불가능하도록 하는 공격들이 존재한다. 이러한 공격이 가능한 원인은 기존의 워터마킹 방식이 삽입기와 검출기에서 동일한 비밀키를 사용하는 대칭키 방식이기 때문이다. 대칭키 방식의 워터마킹 시스템에서는 삽입과 검출에서 동일한 키를 사용하는 관계로 검증자가 검출기에서 워터마크 정보를 검출하여 삽입된 워터마크 정보를 제거하거나 위,변조시킬 수 있다. 이러한 공격에 대응하기 위해서는 워터마크의 삽입과 검출 시 서로 다른 키를 사용하는 비대칭 워터마킹 기술이 필요하다. 본 논문에서는 공개 키 암호시스템과 유사한 개념을 적용하여 비대칭 워터마킹 시스템을 구성하였으며, 삽입 시 사용하는 키를 개인 키라고 하고 검출 시 사용하는 키를 공개 키라고 한다.

본 논문에서는 상관도 검출기반의 안전성이 높고 검출 성능이 우수한 비대칭 워터마킹 방식을 제안한다. 우선 개인 키의 큰 탐색공간을 확보하기 위하여 선형연립방정식의 해 집합을 이용하였으며, 개인 키 및 공개 키의 생성과정에서는 높은 상관도 검출이 가능하고 공개 키로부터 개인 키 정보를 검출해 낼 수 없도록 안전한 선형변환 및 특수행렬을 이용하여 구성하였다. 본 논문의 제안 방식은 1bit의 정보 뿐만 아니라 멀티 bit의 정보를 삽입하고 신뢰성 있게 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 비교분석하며, 3장에서는 제안하는 비대칭 워터마킹 방식을 소개하며, 4장에서는 본 제안된 방식의 실험결과를 분석하며, 5장은 결론에 대해 기술한다.

2. 비대칭 워터마킹 기술

비대칭 워터마킹 방식은 공개 키 검출방식으로, 공개 키 암호 시스템과 유사하게 콘텐츠의 저작권 소유주가 개인 키와 공개 키를 생성하여 정보 삽입에 개인 키를 사용하고, 검증자가 검출 시에 공개 키를 사용하여 개인정보의 삽입여부를 검증하는 방식이다. 개인 키와 공개 키는 다양한 방법으로 생성될 수 있으나 어떠한 경우에서든지 공개 키로부터 개인 키 정보는 추출해 낼 수 없어야 하며, 공개 키와 워터마크가 삽입된 삽입본으로부터 워터마크의 존재여부를 정확히 검증해 낼 수 있어야 한다.

최근에 여러 가지 방식의 비대칭 워터마킹 방식들이 제안되었는데, 그 중 몇 가지 대표적인 방식들에 대해 소개하고 비교 분석한다.

Van Schyndel[1]은 Legendre 수열의 변환을 이용하여 비대칭 워터마킹을 구현하였는데 이 방식은 Legendre 수열은 이산 푸리에 변환을 하면 같은 수열의 켈레 형태를 얻을 수 있다는 특성을 이용하였다. 이 방식에서는 상관도 값이 Legendre 수열의 상관도 값으로 표현되므로 Legendre 길이

만을 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 비밀 키와 공개 키를 생성해 내게 된다. 검출기에서는 공개 키를 이용하여 상관도 검출을 하게 되는데 상관도 계산 과정에서 비밀 키와 공개 키의 변환행렬이 상쇄되고 결과적으로 원시 키의 상관도로 표현되므로 공개 키를 이용하여 워터마크의 검출이 가능하게 된다. 이 방식에서는 공개 키만 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 비밀 키를 M공간으로 압축시킨다. 이는 암호화에서와 유사하게 하나의 공개 키에 대하여 (N-M)차원 만큼의 비밀 키가 존재하므로 비밀 키의 탐색이 어려워지도록 하는데 목적을 두고 있다. 워터마크의 삽입은 원본 데이터에 비밀 키를 삽입하고, 검출 과정에서는 워터마크가 삽입된 신호를 같은 방식으로 신경망 함수에 입력하여 얻은 값과 공개 키와의 상관도를 구하게 된다. 신경망 함수는 선형이외에 비 선형을 사용할 수 있으며 다단계 층을 거칠 수도 있으나 비선형에 가까워질수록 안전은 제고되지만 검출 성능은 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 전력 밀도 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 방식들 사이에는 차이점과 유사성이 존재하고 있으며 대부분 효과적이고 신뢰성 있는 검출에 다소 한계가 있으며 다양한 유형의 공격에도 적절하게 대응할 수 없는 단점을 안고 있다. Schyndel 방식에서는 생성 가능한 Legendre 수열이 제한적인 관계로 탐색공간이 현저히 줄어들게 되며 공격자가 삽입된 수열을 쉽게 찾아 낼 수 있는 단점을 안고 있다. 또 Smith와 Schyndel 방식은 전송된 신호와 그 신호를 변환시킨 신호와의 상관도를 이용하는 형태로 검출하기에 워터마크의 존재 여부만을 확인할 수 있어 제한적인 활용에 국한적으로 사용되게 된다. Furon의 경우에는 워터마크가 삽입되어 있는 신호에 전력 밀도 스펙트럼의 모양을 평평하게 만드는 필터 처리를 이용한 공격이 가능하다. Craver, Adelsbach와 같이 암호화 프로토콜을 이용한 경우는 보안적인 측면이 강화될 수는 있는 반면에 상관도 검출과 같이 신뢰성 있는 검출은 기대하기 어렵다. Picard 방식은 신경망을 이용한 방식으로 검출과정에서 커버 신호 자체를 변환시켜 검출을 행하며 신경망 층에 선형 및 비선형 함수를 이용할 수 있다. 비 선형함수를 이용할 경우에는 안전성 측면에서 개선될 수 있겠으나 신호간섭으

로 검출 성능은 떨어지게 된다. 신경망 함수를 사용함으로써 비밀 키 탐색공간을 확보할 수는 있겠으나 검출 특성상 신경망 함수자체를 공개해야 하므로 이에 따른 공격의 위험이 존재하게 된다. 즉 변환행렬의 공개로 검출 상관도 값을 떨어뜨리는 잡음을 추가하는 공격이 가능하다. 본 제안방식은 이러한 문제점을 극복하고자 변환행렬을 공개하지 않으면서 특수행렬과 변환행렬을 이용하여 공개 키를 효과적으로 구성하여 신호간섭을 최소화하여 높은 상관도 검출이 가능케 하였다. 또한 커버신호 자체를 변환시켜 검출하는 것과 달리 직접 공개 키와 전송된 신호를 이용하여 검출함으로써 신뢰성 있는 높은 상관도 검출이 가능하게 한다. Choi 방식은 변환키 방식으로 신호간섭을 줄이고 높은 상관도 검출을 할 수 있는 반면에 비밀 키 탐색공간 확보를 위한 방안이 제기되지 않고 있다.

제안한 비대칭 워터마킹 방식은 특정한 조건을 만족하는 연립방정식의 해집합을 기반으로 개인 키를 구성함으로써 공개 키를 이용한 개인 키의 탐색공간을 효율적으로 증가시켜 공개 키로부터 개인 키를 탐색하려는 공격에 효과적으로 대처할 수 있다. 또한 특수 행렬과 선형 변환방식을 이용하여 신뢰성 높은 공개 키 검출이 가능하도록 하였다.

3. 제안한 비대칭 워터마킹 방식

3.1 연립방정식 해의 집합을 이용한 개인 키 탐색공간

본 제안방식에서는 아래와 같은 1차 연립방정식의 해의 집합을 이용하여 개인 키의 탐색 공간을 구성하게 된다.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned} \quad (1)$$

$$A_{m \times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \quad (2)$$

식(2)로부터 연립방정식 (1)은 행렬식 $Ax = b$ 의 형태로 표시된다. 여기서 $\text{rank}(A) = \text{rank}(A:b) < n$ (n 은 미지수의 개수)의 조건을 만족할 경우 x 는 무수히 많은 해를 가질 수 있게 된다. 이와 같은 결과를 비대칭 워터마킹 시스템에 적용하기 위하여 아래와 같은 방법으로 V 및 U 를 구성한다. U 는 공개 키 생성시에 사용되며 V 는 상관도 검출에 사용된다.

$$US_r = V \quad (3)$$

제안하는 비대칭 워터마킹 방식은 공개 키 암호시스템과

유사하게 개인 키와 공개 키를 생성하게 된다. S_r 는 대칭 키 워터마킹 시스템에서 단일 키로 사용되는 비밀 키와 동일한 개념의 비밀 키이며, 개인 키는 비밀 키 S_r 로부터 생성되게 된다. 대칭과 비대칭 워터마킹 시스템을 상호 비교하고 분석하기 위하여 이들 키들을 명확히 구분하는 것이 바람직하다.

U 는 $n \times n$ 의 변환 행렬이고 S_r 은 $n \times n$ 행렬로 이루어진 비밀 키이다. $\text{rank}(U) = \text{rank}(U:V) < n$ 의 조건을 만족하는 U 와 V 를 선택하여 사용하면, 무수히 많은 비밀 키 S_r 를 생성할 수 있게 되므로 비밀 키 및 개인 키의 탐색공간이 늘어나게 되어 시스템의 안전성을 효과적으로 제고하게 된다. S_r 는 무수히 많은 해의 집합에서 선형독립인 해들로만 이루어진 비밀 키 집합의 한 원소이며, 비밀 키의 공간은 U 에 의하여 결정된다.

3.2 개인 키 키와 공개 키의 구성

비대칭 워터마킹 시스템의 개인 키와 공개 키는 비밀 키를 이용하여 아래와 같이 구성된다. 여기서 Q 는 임의의 랜덤 행렬의 행렬분해에 의해 생성된 직교 행렬이다.

$$S = QS_r \quad (4)$$

$$P = QU'US_r \quad (5)$$

식(5)에서의 U 는 $\text{rank}(U) = \text{rank}(U:V) < n$ 을 만족하는 행렬이다. 여기서 직교행렬 Q 를 사용하는 목적은 공개 키를 이용한 개인 키의 계산 복잡도를 높이고 안전성을 제고하여 공격을 어렵고 하기 위함이다. 또 상관도 계산에서는 직교행렬의 전치행렬은 역 행렬과 같다는 특성을 이용하여 높은 상관도 검출이 가능하게 한다.

3.3 워터마크의 생성 및 삽입

워터마크는 아래의 식(6)에서와 같이 생성되는데 여기서 m 은 삽입 비트 정보로서 $m \in \{-1, 1\}$ 의 값을 취하며 m 이 -1일 경우는 bit 1을 m 이 1일 경우는 bit 0가 삽입됨을 의미한다. α 워터마크 삽입강도이며 S 는 식(4)에서 생성된 개인 키이다.

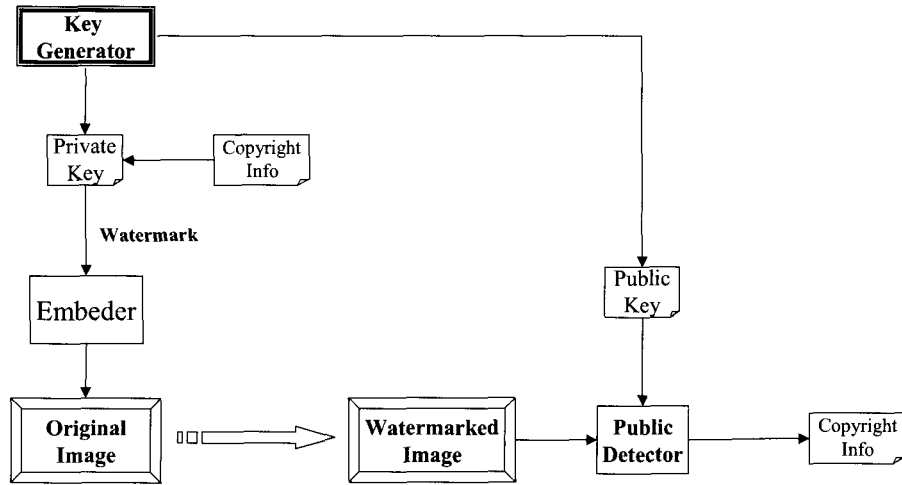
$$W = \alpha \cdot m \cdot S \quad (6)$$

$$I_i(w) = I_i + W_i \quad (7)$$

워터마크의 삽입은 식(7)과 같이 $n \times n$ 의 정보삽입 블록에 워터마크를 삽입하게 된다. I_i 와 $I_i(w)$ 는 정보 삽입블록과 워터마크가 삽입된 블록이다. W_i 는 하나의 정보 삽입블록에 삽입되는 워터마크 신호이다. 검출 시에 하나의 $n \times n$ 블록에서 1bit의 정보를 추출하게 된다.

3.4 공개 키를 이용한 상관도 검출

공개 키 P 와 워터마크가 삽입된 신호 $I(w)$ 를 이용하여 상관도 일반적으로 상관도를 계산하는 과정은 아래와 같다.



(그림 1) 제안 비대칭 워터마킹 시스템 흐름도

$$\begin{aligned}
 C &= P^t I(w) \\
 &= (S, 'U'UQ')I + (S, 'U'UQ')N \\
 &\quad + am(S, 'U'UQ')QS, \\
 &= (S, 'U'UQ')I + (S, 'U'UQ')N \\
 &\quad + amV'V
 \end{aligned} \tag{8}$$

식(8)의 세 번째 항에서는 직교행렬의 전치행렬은 역 행렬과 같다는 특성을 이용하여 계산과정에서 Q가 상쇄되며 결과적으로 V의 상관도 값으로 나타나게 된다. 첫 번째와 두 번째 항의 원본 신호와 노이즈 신호는 공개 키와 아주 작은 상관도가 발생하게 되므로 그 값은 상대적으로 세 번째 항에 비해 아주 작은 값으로 나타나게 되어 V의 상관도 값 만으로 개인 키의 삽입 여부를 판단할 수 있게 된다. 이렇게 되어 상관도 검출과정에서 비밀 키나 개인 키 정보를 직접 사용하지 않고 공개 키 정보만을 이용하여 검출이 가능하며, 공개 키 정보로부터 개인 키 정보나 비밀 키 정보를 계산하는 것은 매우 어렵게 된다.

1bit의 정보를 삽입할 경우와 멀티 bit를 삽입할 경우 워터마크가 삽입된 상관도 검출용 신호 $I(w)_d$ 는 서로 방식으로 처리하게 된다.

$$I(w)_d = \sum_{i=1}^e (I_i + W) \tag{9}$$

식 (9)는 1bit의 정보만 삽입하고 검출할 경우인데 동일한 워터마크 W를 정보삽입 블록 I_i 에 반복적으로 삽입하여 $I(w)_d$ 를 계산하게 된다.

$$I(w)_d = I(w) = I_i + W_i \tag{10}$$

식 (10)는 멀티 bit를 삽입하고 검출할 경우로서 각각의 블록에 서로 다른 W_i 를 삽입하여 매개의 블록에서 상관도를 계산함으로써 서로 다른 bit 정보를 검출하게 된다.

(그림 1)은 제안한 비대칭 워터마킹 시스템 흐름도를 보여 준다. 그림에서 Copyright info는 식(6)에서의 삽입 정보 m이며, 이는 저작권 정보와 같은 인증정보 일 수 있다. 키 생성기에서는 개인 키와 공개 키를 생성하고, 개인 키와 저작권 정보는 워터마크를 구성하며 워터마크는 삽입기에 의하여 원본 이미지에 삽입 된다. 키 생성기에서 생성된 공개 키는 워터마크가 삽입된 이미지와 함께 검출기에 전달되며 검출기에서는 이 공개 키를 이용하여 상관도 검출을 진행하게 된다.

4. 실험결과 및 고찰

본 알고리즘의 구현과정에서 512*512의 "lena" 이미지를 사용하여 공간영역에 삽입하였다. 1bit의 정보의 삽입 시에는 정보삽입 블록(n*n)으로 128*128블록을 사용하였으며, 멀티bit의 삽입에는 64*64의 블록을 사용하였다. QR분해로 생성된 행렬 Q도 두 경우에 각각 128*128와 64*64의 행렬을 사용하였다.

실험에서 상관도 값의 계산과정은 아래의 식(11)에서와 같이 푸리에 변환을 사용하여 고속으로 진행하게 된다.

$$C = R(IFFT(FFT(I(w))*CONJ(FFT(P)))) \tag{11}$$

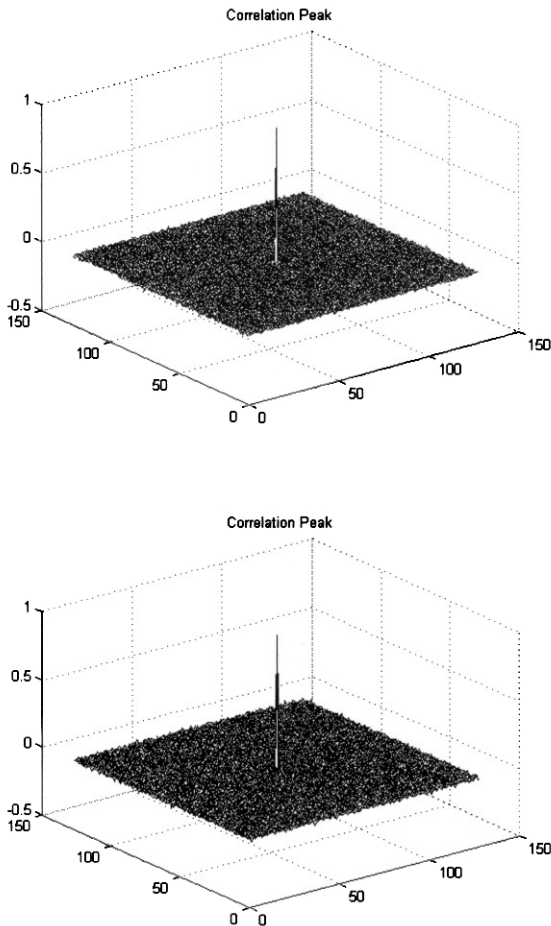
여기서 FFT와 IFFT는 푸리에 변환과 역 푸리에 변환을 의미하며 CONJ는 Conjugation을 의미한다. R은 실수를 취함을 나타내고 "*"는 행렬의 원소 대 원소의 곱셈을 표시한다.

(그림 2)는 원본 영상과 워터마크가 삽입된 영상으로 PSNR = 40.8db로 나타났다. 멀티bit(64bit) 삽입 시에는 PSNR = 40.1db로 나타났다.



(그림 2) 원본 영상(좌)와 워터마크가 삽입된 영상(우)

(그림 3)은 개인 키와 공개 키의 상관도 값을 정규화 한 검출결과로서 위쪽이 개인 키 검출 결과($C_{max} = 0.9875$, $C_{snd} = 0.0524$)이고 아래쪽이 공개 키 검출결과($C_{max} = 0.9833$, $C_{snd} = 0.0605$)이다. 여기서 C_{max} 와 C_{snd} 는 각각 가장 큰 값인 상관도 Peak값과 상관도 값 중 Peak값 다음으로 큰 값이다.



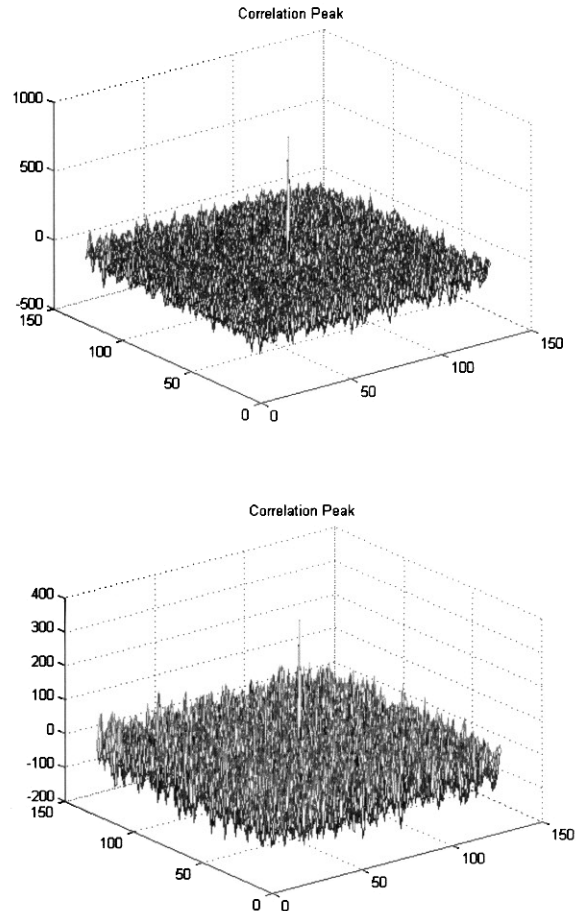
(그림 3) 개인 키와 공개 키의 상관도 검출(정규화)

(그림 4)는 JPEG압축 후의 개인 키와 공개 키의 상관도 검출결과로서 정규화를 하지 않은 값이다. 위쪽이 개인 키 검출 결과($C_{max} = 905.4$, $C_{snd} = 299.6$)이고 아래쪽이 공개 키 검출결과 ($C_{max} = 399.3$, $C_{snd} = 161.2$)이다. 이 실험에서 JPEG압축 QF

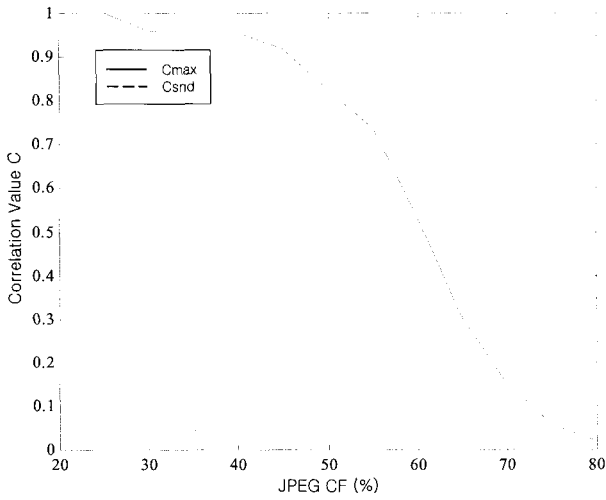
(Quality Factor)는 65%를 사용하였다. 수치적으로 볼 때 공개 키 상관도 검출이 개인 키 상관도 검출에 비해 다소 적은 값들로 나타났으나 Peak값으로부터 문제없이 검출할 수 있으며 압축 후에도 비교적 우수한 검출 성능을 보여주고 있다.

(그림 5)는 JPEG2000압축의 CF(Compress factor)에 따른 공개 키의 검출 결과를 보여준다. 그림에서 실선으로 표시된 부분이 C_{max} 이고 점선으로 표시된 부분이 C_{snd} 이다. 여기서 CF의 증가에 따라 C_{max} 와 C_{snd} 의 사이가 점차 축소되고 있어 검출 성능이 떨어지며, QF = 55% 정도의 지점에서는 이 차이가 급격히 작아지고 있음을 알 수 있다. 이 그래프에서 CF = 25%일 경우에 CR(Compress Ratio) = 1:4이고, CF = 80%일 경우에 CR(Compress Ratio) = 1:46이다. CF = 80% 이상일 경우에는 압축율이 현저히 높아져 이미지가 상당히 왜곡되어 있으며 그래프에서 보다시피 공개 키 검출도 이 경우에는 어렵게 된다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)

(그림 6)은 JPEG압축의 QF(Quality Factor)에 따른 비밀 키(실선), 개인 키(굵은점선), 공개 키(가는점선)의 C_{max} 을 보여줌으로써 QF에 따른 대칭 및 비대칭 워터마킹 시스템의

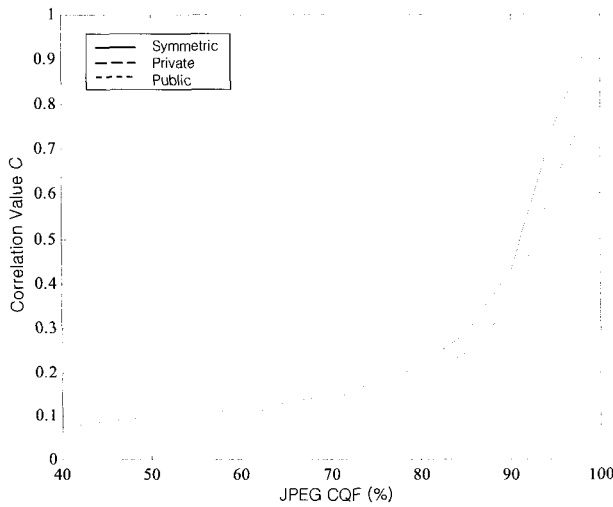


(그림 4) JPEG압축에 따른 개인 키와 공개 키의 상관도 검출 (QF = 65%)



(그림 5) JPEG2000 Compress Factor에 따른 공개 키의 검출 성능

검출 성능을 비교하였다. 여기서 알 수 있듯이 비대칭 방식의 개인 키 검출이 대칭방식의 비밀 키 검출에 근사하게 접근하고 있으며 공개 키 검출은 비밀 키와 개인 키 검출 값 보다는 다소 낮은 값으로 나타났다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)



(그림 6) QF에 따른 대칭 및 비대칭 시스템 검출 성능비교

<표 1> 삽입강도에 따른 공개 키 검출 성능

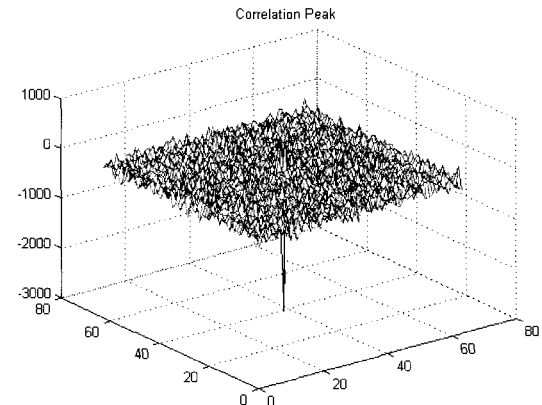
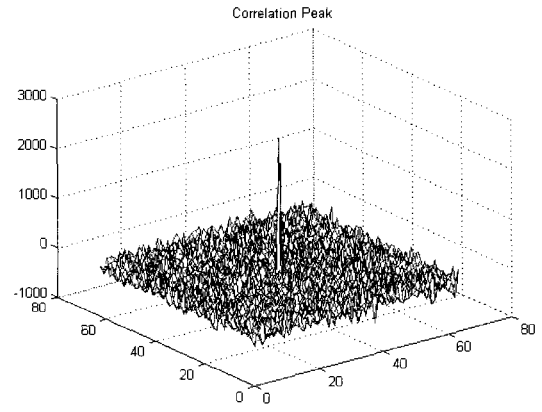
Alpha	PSNR	Lena.bmp		Lena.jpg	
		Cmax	Csnd	Cmax	Csnd
14	40.8	0.983	0.044	0.049	0.019
10	43.5	0.709	0.035	0.034	0.017
6	47.6	0.423	0.024	0.018	0.016
2	54.3	0.138	0.019	0.015	0.014

<표 1>은 삽입강도에 따른 PSNR값과 공개 키 검출결과를 보여준다. α 값이 작아지면 전반적으로 검출성능이 떨어지게 되며, 특히 JPEG압축의 경우에는 α 값이 2까지 내려갈 경우 공개 키 검출이 어려워지게 됨을 알 수 있다.

<표 2>는 영상별로 bmp와 jpg, jpeg2000 등 포맷에 따른 공개 키의 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 고주파수 성분이 강한 Baboon 이미지가 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. <표 1>과 <표 2>에서 jpg는 QF = 65%를 사용하였고 <표 2>에서의 j2k는 CF = 65%를 사용하였다.

<표 2> 영상 및 압축에 따른 공개 키 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 7) 멀티비트 공개 키 상관도 검출

(그림 7)은 멀티비트 검출 시 64*64블록에서 공개 키의 상관도 검출한 결과로서 1bit(왼쪽, $C_{max} = 2716.8$, $C_{snd} = 482.8$)와 0bit(오른쪽, $C_{max} = -2766.8$, $C_{snd} = -408.7$)의 임의의 두 블록을 선택하여 그 결과를 보여준다. 멀티비트를 삽입할 경우 블록 size가 작아지는 관계로 C_{max} 값이 현저히 떨어지기는 하나 C_{snd} 와의 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.

<표 3>은 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.

<표 3> 워터마크 삽입 및 검출 속도 비교

삽입블록	워터마크 삽입		워터마크 검출	
	대칭	비대칭	대칭	비대칭
128*128	0.41 s	0.48 s	0.37 s	0.37 s
64*64	0.39 s	0.45 s	0.29 s	0.29 s

워터마크 삽입단계에서 비대칭 방식의 경우에는 개인 키 및 공개 키 계산 과정이 포함하게 되므로 대칭 방식에 비해 속도가 다소 떨어지게 된다. 검출단계에서는 검증자가 전송 받은 비밀 키 또는 공개 키를 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.

5. 결 론

기존의 대부분의 워터마킹 방식은 삽입기와 검출기에서 같은 비밀 키 정보를 사용하는 대칭 키 방식을 사용하고 있다. 하지만 이러한 대칭방식은 검출기에서 비밀 정보가 유출되었을 경우 워터마크의 제거나 검출 불가 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 특정된 조건하의 선형 연립방정식의 해 집합을 이용하여 비밀 키의 탐색공간을 대폭 확대하였으며, 공개 키의 생성과정에서는 선형 행렬변환과 특수행렬을 이용하

여 높은 상관도 검출이 가능하도록 공개 키를 생성하였으며 공개 키로부터 개인 키를 유출할 수 없도록 구성하였다. 본 논문의 제안방식은 이미지뿐만 아니라 다양한 멀티미디어 콘텐츠에 적용 가능한 원천 기술이다. 실험에서는 Quality Factor, 삽입강도 등에 따른 공개 키 검출 성능 및 대칭 키 방식과의 검출 성능 비교 등을 통하여 다양한 측면에서 제안 방식의 성능평가를 진행하였으며 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 강한 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), Toulouse, France, September 3-6, 2002.

이 덕



e-mail : lide@smu.ac.kr
 1996년 (중) 할빈이공대학교 전기공학과(공학사)
 2001년 상명대학교 전자계산학과(이학석사)
 2001년~현재 상명대학교 컴퓨터학과 박사과정

1999년~현재 상명대학교 디지털저작권보호연구센터 선임연구원
 관심분야: 디지털워터마킹, 저작권관리기술, 디지털신호처리, 컴퓨터시스템 및 네트워크보안

김 종 원



e-mail : jwkim@smu.ac.kr
 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



e-mail : juchoi@smu.ac.kr
 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