韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-1-15

상관도 검출기반의 비대칭 공개 키 워터마킹

이 덕*, 김 종 원**, 최 종 욱***

Asymmetric public-key watermarking based on correlation method

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

요 약

기존의 디지털 워터마킹 기술은 대부분 삽입과 검출에서 동일한 키를 사용하는 대칭키 방식이다. 이러한 대칭키 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 1비트의 정보 뿐만 아니라, 멀티 비트의 정보에 대한 공개 키 상관도 검출이 정확히 이루어짐을 확인할 수 있었으며 JPEG압축 후에도 높은 상관도 검출이 가능한 것으로 나타났다.

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 theresults, the multi bits information can be embedded and high correlation value was detected after JPEG compression.

▸ Keyword : 개인 키(private key), 공개 키(public key), 상관도검출(correlation detection), 비대칭(asymmetric)

• 제1저자 : 이 덕
• 접수일 : 2005.06.05, 심사완료일 : 2005.07.01
* 상명대학교 컴퓨터과학과 박사과정, ** 상명대학교 디지털저작권보호연구센터 책임연구원
*** 상명대학교 소프트웨어대학 교수
※ 산업자원부 공통핵심기술개발사업

Ⅰ. 서 론

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[1-11] 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 검출이 불가능하도록 하는 공격들이 존재한다. 이러한 공격 원인중의 하나는 기존의 워터마킹 시스템이 삽입기와 검출기에서 동일한 키를 사용하는 대칭키 방식을 사용하기 때문이다. 대칭키 방식의 경우 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 키를 사용하는 비대칭 워터마킹 기술이 필요하다.

본 논문에서는 상관도 검출기반의 안전하며 검출성능이 우수한 비대칭 워터마킹 방식을 제안한다. 우선 개인 키의 큰 탐색공간을 확보하기 위하여 선형연립방정식의 해 집합을 이용하였으며, 공개 키의 생성과정에서는 높은 상관도 검출이 가능하고 개인 키 정보를 추출할 수 없도록 안전한 선형변환을 이용하여 공개 키를 구성하였다. 본 논문의 제안방식은 1비트 뿐만 아니라 멀티비트의 정보를 삽입하고 정확하게 검출될 수 있도록 구성 되었으며, JPEG압축에도 강인한 것으로 검증되었다.

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 공개 키 검출방식으로, 공개 키 암호 시스템과 유사하게 워터마크 삽입기에서 개인 키와 공개 키를 생성하여 정보 삽입에 개인 키를 사용하고 검증자가 검출 시에 공개 키를 사용하여 워터마크의 삽입여부를 검증하는 방식이다. 개인 키와 공개 키의 생성은 다양한 방법이 있을 수 있으나 어떠한 경우에서든지 공개 키 또는 공개 키와 개인 키가 삽입된 삽입 본으로부터 개인 키 정보를 추출해 낼 수 없어야 하며, 공개 키로부터 개인 키의 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 구현하였는데 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 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 표시되므로 공개 키를 이용하여 워터마크의 검출이 가능하게 된다. 이 방식에서는 공개 키 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 비밀 키를 M공간으로 압축시킨다. 이는 암호에서와 유사하게 하

나의 공개 키에 대하여 (N-M)차원 만큼의 비밀 키가 존재하므로 비밀 키의 탐색이 가능하지 않도록 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 선형 이외에 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 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 공개 키의 구성 및 검출형식으로 인한 문제점으로 다양한 공격에 대하여 적절하게 대응할 수 없는 단점을 안고 있다. Schyndel[1] 방식에서는 생성 가능한 Legendre 수열이 제한적인 관계로 탐색공간이 현저히 줄어들게 되며 공격자가 삽입된 수열을 쉽게 찾아 낼 수 있는 단점을 안고 있다. 또 Smith[4]와 Schyndel[1] 방식은 전송된 신호와 그 신호를 변환시킨 신호와의 상관도를 이용하는 형태로 검출하기에 워터마크의 존재 여부만을 확인할 수 있어 제한적인 활용에 국한적으로 사용되게 된다. Furon[5]의 경우에는 워터마크가 삽입되어 있는 신호에 전력 밀도 스펙트럼의 모양을 평평하게 만드는 필터 처리를 이용한 공격이 가능하다. Craver[6,7], Adelsbach[8,9]와 같이 암호화 프로토콜을 이용한 경우는 보안적인 측면이 강화될 수는 있는 반면에 상관도 검출과 같이 신뢰성 있는 검출은 기대하기 어렵다.

Choi[2], Picard[3] 방식은 본 제안방식과 유사한 변환방식을 이용하지만 효율적인 키 탐색공간의 확보, 신뢰성 있는 검출 및 공격 가능성 등에 대하여 일부 문제점을 안고 있다.

Choi[2] 방식은 변환키 방식으로 신호간섭을 줄여 효과적으로 상관도 검출을 할 수 있는 반면에 비밀 키 탐색공간 확보를 위한 안전한 방안이 제기되지 않았다. Picard[3] 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 신호간섭으로 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 검출함으로 신뢰성 있는 높은 상관도 검출이 가능하게 한다.

본 논문에서 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 검출 신뢰성이 높은 공개 키 검출이 가능하도록 하였다.

III. 제안한 비대칭 워터마킹 방식

3.1 연립방정식의 해 집합을 이용한 비밀 키 탐색 공간

제안하는 비대칭 워터마킹 방식은 공개 키 암호시스템과 유사하게 개인 키와 공개 키로 구성되는데 공개 키와 개인 키는 비밀 키 Sr로부터 생성되게 된다. 대칭과 비대칭 워터마킹 시스템을 상호 비교하고 분석하기 위하여 이들 키들을 명확히 구분하는 것이 바람직하다.

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

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

$$A_{mn}=\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{vmatrix}, \quad x=\begin{vmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{vmatrix}, \quad b=\begin{vmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{vmatrix} \quad \cdots\cdots (2)$$

식(2)로부터 연립방정식(1)은 행렬식 Ax=b의 형태로 표시된다. 여기서 rank(A) = rank(A:b) 〈 n (n은 미지수의 개수)의 조건을 만족할 경우 x는 무수히 많은 해를 가질 수 있게 된다. 이와 같은 결과를 비대칭 워터마킹 시스템에 적용하기 위하여 아래와 같은 방법으로 비밀 키를 이용하여 공개 키 구성에 필요한 V를 생성한다.

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

U는 n*n행렬이고 Sr은 n*n행렬로 이루어진 비밀 키이다.

여기서 rank(U) = rank(U:V) 〈 n 의 조건을 만족하는 U와 V를 선택하여 사용하면, 무수히 많은 비밀 키 Sr를 생성할 수 있게 되므로 비밀 키 및 개인 키의 탐색공간이 증가하게 되어 시스템의 안전성을 효과적으로 제고하게 된다. Sr은 무수히 많은 해의 집합에서 선형독립인 해들로만 이루어진 비밀 키 집합의 한 원소이며, 비밀 키의 공간은 U에 의하여 결정된다.

3.2 개인 키 및 공개 키 구성

비대칭 워터마킹 시스템의 개인 키와 공개 키는 비밀 키를 이용하여 아래와 같이 구성된다. 여기서 Q는 임의 행렬의 QR행렬분해에 의해 생성된 직교 행렬이다.

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

$$P = QU^tUS_r \quad \cdots\cdots (5)$$

식(5)에서의 U는 rank(U) = rank(U:V) 〈 n 을 만족하는 행렬이다. 여기서 직교행렬 Q를 사용하는 목적은 공개 키를 이용한 개인 키의 계산 복잡도를 높여 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 m은 삽입 비트 정보로서 m∈{-1,1}의 값을 취하며 m이 1일 경우는 비트 1을 m이 1일 경우는 비트 0가 삽입됨을 의미한다. α 는 워터마크 삽입 강도이며 S는 식(4)에서 생성된 개인 키이다.

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

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

워터마크의 삽입은 식(7)과 같이 n*n의 정보삽입 블록에 워터마크를 삽입하게 된다. Ii와 Ii(w)는 정보 삽입블록과 워터마크가 삽입된 블록이다. Wi는 하나의 블록에 삽입되는 워터마크신호이다. 검출 시에 하나의 n*n 블록에서 1비트의 정보를 검출하게 된다.

3.4 공개 키를 이용한 상관도 검출

공개 키 P와 워터마크가 삽입된 신호 I(w)를 이용하여 상관도 일반식으로 상관도를 계산하는 과정은 아래와 같다.

$$\begin{aligned} C = P^tI(w) &= (S_r^tU^tUQ^t)I + (S_r^tU^tUQ^t)N \\ &\quad + \alpha m(S_r^tU^tUQ^t)QS_r \\ &= (S_r^tU^tUQ^t)I + (S_r^tU^tUQ^t)N \\ &\quad + \alpha mVV \end{aligned} \quad \cdots\cdots (8)$$

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 거의 상관도가 발생하지 않으므로 그 값은 상대적으로 세 번째 항에 비해 아주 작은 값으로 나타나게 되어 V의 상관도 값만으로 개인 키의 삽입 여부를 판단할 수 있게 된다. 이렇게 되어 상관도 검출과정에서 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.

1비트의 정보를 삽입할 경우와 멀티비트를 삽입할 경우 워터마크가 삽입된 상관도 검출용 신호 $I(w)_d$ 는 서로 다른 방식으로 처리하게 된다.

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

식 (9)는 1비트의 정보만 삽입하고 검출할 경우인데 동일한 워터마크 W를 정보삽입 블록 Ii에 반복적을 삽입하여 $I(w)_d$ 를 계산하게 된다.

$$I(w)_d = I(w) = I_i + W_i \quad \cdots\cdots (10)$$

식(10)는 멀티비트를 삽입하고 검출할 경우로서 각각의 블록에 서로 다른 Wi를 삽입하여 매개의 블록에서 상관도를 계산함으로써 서로 다른 비트 정보를 검출하게 된다.

이와 같이 본 제안방식은 신뢰성과 안전성 측면에서 합리적인 방안을 제공한다.

Ⅳ. 실험결과 및 고찰

본 논문은 MATLAB을 사용하여 구현하였으며 JPEG2000 압축과 변환에는 Elecard J2k_Compressor를 사용하였다. 알고리즘 구현과정에서는 512*512의 "lena" 이미지를 사용하여 공간영역에 삽입하였으며 추가로 Baboon, Peppers 등 표준 영상들도 사용하였다. 1비트의 정보의 삽입 시에는 정보삽입 블록으로 128*128블록을 사용하였으며, 멀티비트의 삽입에는 64*64의 블록을 사용하였다. 행렬 Q도 두 경우에 각각 128*128와 64*64 행렬을 사용하였다.

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

$$C = R(IFFT(FFT(I(w)) \bullet CONJ(FFT(P)))) \quad \cdots\cdots (11)$$

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

전체 영상에 1비트의 정보만 삽입하였을 경우 PSNR=40.8db로, 멀티비트 삽입 시에는 PSNR=40.1db로 나타났다.

(그림 1)은 개인 키와 공개 키의 상관도 값을 정규화 한 검출결과로서 위쪽이 개인 키 검출 결과(Cmax=0.9875, Csnd=0.0524)이고 아래쪽이 공개 키 검출결과(Cmax=0.9833, Csnd=0.0605)이다. 여기서 Cmax와 Csnd는 각각 가장 큰 값인 상관도 Peak값과 상관도 값 중 Peak값을 제외한 두 번째로 큰 값이다.

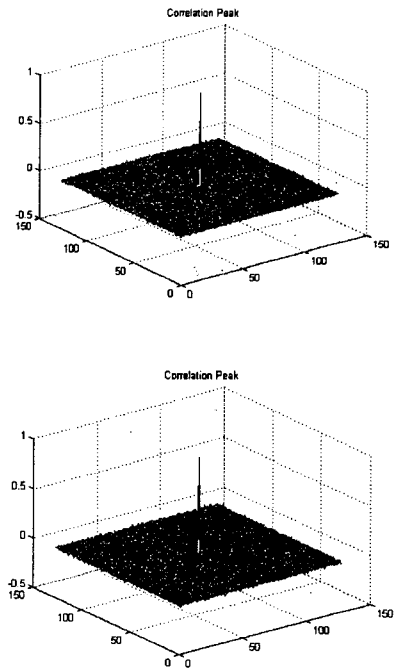

그림 1. 개인 키와 공개 키의 상관도 검출 (정규화)
Fig 1. Correlation detection of private key and public key (normalization)

(그림 2)는 JPEG압축 후의 개인 키와 공개 키의 상관도 검출결과로서 정규화를 하지 않은 값이다. 위쪽이 개인 키 검출 결과(Cmax=905.4, Csnd=299.6)이고 아래쪽이 공개 키 검출결과(Cmax=399.3, Csnd=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 실험에서 나타난 Peak값으로부터 문제없이 검출할 수 있었으며 압축 후에도 비교적 우수한 검출 성능을 보여주고 있다.

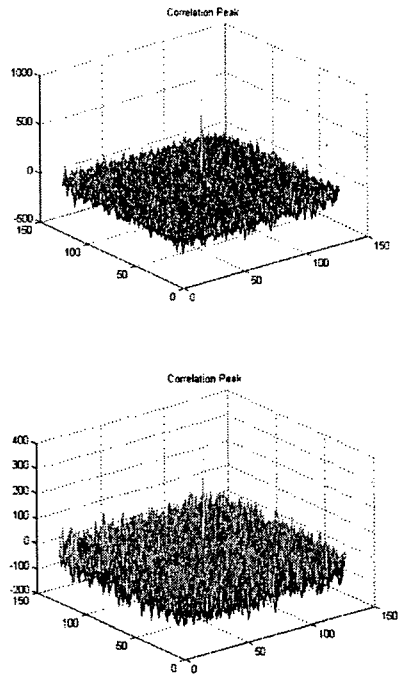

그림 2. JPEG압축에 따른 개인 키와 공개 키의 상관도 검출 (QF=65%)
Fig 2. Correlation detection of private key and public key with JPEG compression (QF=65%)

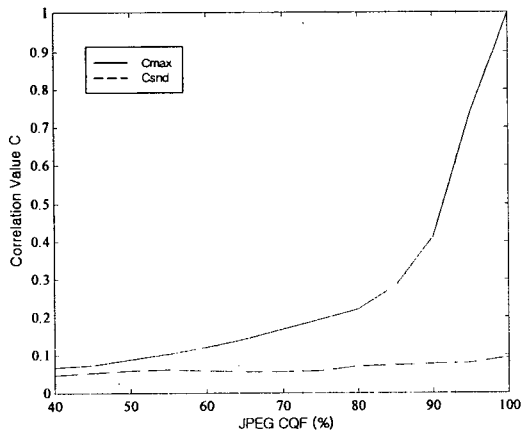

그림 3. QF에 따른 공개 키의 검출 성능
Fig 3. Detection performance of public key with quality factor

(그림 3)은 JPEG압축의 QF(Quality factor)에 따른 공개 키의 검출 결과를 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 4)는 JPEG2000압축의 CF(Compress factor)에 따른 공개 키의 검출 결과를 보여준다. 그림에서 실선으로 표시된 부분이 Cmax이고 점선으로 표시된 부분이 Csnd이다. 여기서 CF의 증가에 따라 Cmax와 Csnd의 사이가 점차 축소되고 있어 검출 성능이 떨어지며, QF=55% 정도의 지점에서는 이 차이이가 급격이 작아지고 있음을 알 수 있다. 이 그래프에서 CF=25% 일 경우에 CR(Compress Ratio) = 1:4 이고, CF=80% 일 경우에 CR(Compress Ratio) = 1:46 이다. CF=80% 이상일 경우에는 압축율이 현저히 높아져 이지미가 상당히 왜곡되어 있으며 그래프에서 보다시피 공개 키 검출도 이 경우에는 어렵게 된다. (이 그래프에서는 상관도 계산 값을 정규화 하여 얻을 결과를 적용하였음.)

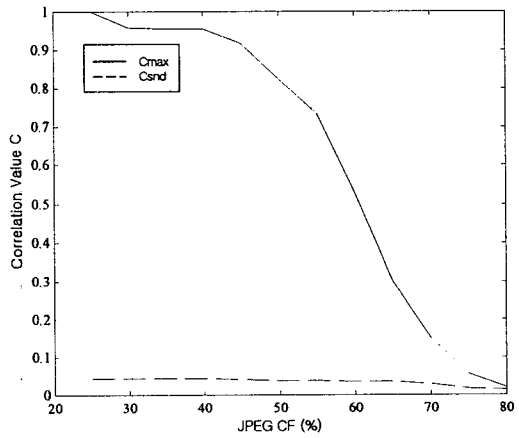

그림 4. JPEG2000 compress factor에 따른 공개 키의 검출 성능
Fig 4. Detection performance of public key with JPEG2000 compress facto

(그림 5)는 JPEG압축의 QF(Quality Factor)에 따른 비밀 키(실선), 개인 키(굵은점선), 공개 키(가는점선)의 Cmax을 보여줌으로써 QF에 따른 대칭 및 비대칭 워터마킹 시스템의 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.)

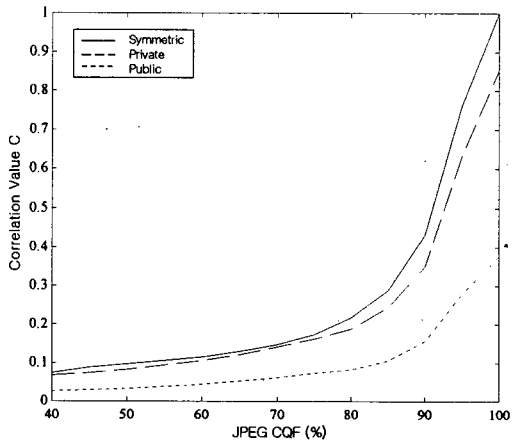

그림 5. QF에 따른 대칭 및 비대칭 시스템 검출 성능비교
Fig 5. Comparison of detection performance of symmetric and asymmetric system with quality factor

〈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 1. 삽입강도에 따른 공개 키 검출 성능
Table 1. Detection performance of public key with embedding intensity

α	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 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 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.

표 2. 영상 및 압축에 따른 공개 키 검출 성능
Table 2. Detection performance of public key with Image and Compression

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

〈표 1〉과 〈표 2〉에서 jpg는 QF=65%를 사용하였고 〈표 2〉에서의 j2k는 CF=65%를 사용하였다.

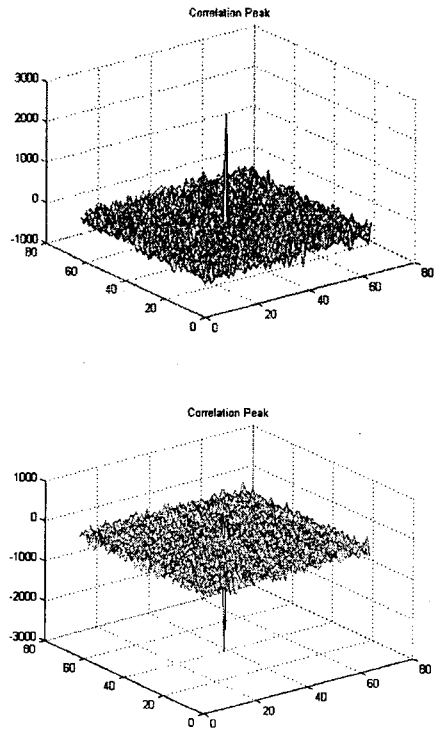

그림 6. 멀티비트 공개 키 상관도 검출
Fig 6. Correlation detection of public key at the multi-bits system

(그림 6)은 멀티비트 검출 시 64*64블록에서 공개 키의 상관도 검출한 결과로서 1비트(왼쪽, Cmax=2716.8, Csnd=482.8)와 0비트(오른쪽, Cmax=-2766.8, Csnd=-408.7)의 임의의 두 블록을 선택하여 그 결과를 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 비트정보를 삽입하였으므로 64비트의 정보를 삽입하고 추출할 수 있게 된다.

V. 결 론

기존의 대부분의 워터마킹 방식은 삽입기와 검출기에서 같은 비밀 키 정보를 사용하는 대칭키 방식을 사용하고 있다. 하지만 이러한 관용 방식은 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 해집합을 이용하여 개인 키의 탐색공간을 대폭 확대하였으며, 공개 키의 생성과정에서는 변환행렬과 특수행렬을 이용하여 높은 상관도 검출이 가능하도록 효과적으로 공개 키를 생성하였으며 공개 키로부터 개인 키를 추출할 수 없도록 안전하게 구성하였다. 실험결과 JPEG압축에도 강인한 것으로 나타났으며 1비트의 정보 뿐만 아니라 멀티비트의 개인 키 정보를 삽입하고 공개 키로 검출을 할 수 있었으며 높은 검출 성능을 보여주었다. 또한 공개 키의 검출 성능 및 대칭 방식의 워터마킹 시스템과의 비교를 통하여 제안 방식의 정확성을 검증하였다.

참고문헌

[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.

[10] 한수영, 이두수, "PIM을 이용한 웨이블릿 패킷 기반 워터마킹", 한국컴퓨터정보학회 논문지 제8권 제3호, 2003.

[11] 송상주, 이두성, "에지와 대역가산기술을 이용한 디지털 워터마킹", 한국컴퓨터정보학회 논문지 제9권 제4호, 2004.

저 자 소 개

이 덕

1996년(중) 할빈이공대학교 전기공학과 졸업 (공학사)
2001년 상명대학교 전자계산학과 졸업 (이학석사)
2000년~현재 상명대학교 컴퓨터과학과 박사과정
〈관심분야〉 디지털워터마킹, 저작권 관리기술, 디지털신호처리, 컴퓨터시스템 및 네트워크 보안

김 종 원

1989년 서울시립대학교 전자공학과 졸업(공학사)
1991년 서울시립대학교 전자공학과 졸업(공학석사)
1995년 서울시립대학교 전자공학과 졸업(공학박사)
1996~2000년 주성대학 정보통신학과 조교수
2000~2004년 (주)마크애니 부설 연구소장
2005~현재 상명대학교 디지털저작권보호연구센터 책임연구원
〈관심분야〉 디지털워터마킹, 저작권 보호 및 관리기술, 디지털신호처리

최 종 욱

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