韓國 컴퓨터情報學會 論文誌
第13卷 第7號, 2008. 12.

2008-13-7-3-5

공개키 공격에 안전한 비대칭 워터마킹

이 덕*, 김 종 원**, 최 종 욱***

A Secure Asymmetric Watermarking to the Public Key Attack

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

요 약

본 논문에서는 공개키 공격에 안전한 비대칭 워터마킹 시스템을 구성하기 위하여 효과적인 공개 키 및 개인 키 생성 알고리즘을 제안한다. 공개 키와 개인 키의 생성은 특수행렬을 이용한 선형변환 방식에 기초하였으며 높은 상관도 검출이 가능하도록 구성되었다. 또 공개 키 공격에 대한 검증과 검출을 위한 공개 키를 추가로 생성하여 분배하는 방안을 제안하여 특정된 환경에서 공개 키 공격에 효과적으로 대응하도록 하였다.

실험결과 워터마크가 삽입된 영상에서 공개 키 및 개인 키를 이용하여 효과적으로 높은 상관도 검출을 할 수 있었으며 공개 키 공격을 받은 영상에서 추가로 발급된 검증용 공개 키를 이용하여 효과적으로 상관도 검출을 할 수 있음을 확인하였다.

Abstract

In this paper, we proposed an algorithm for an effective public key and private key generation to implement a secure asymmetric watermarking system against the public key attack. The public key and private key generation is based on the linear transformation using a special matrix and the keys are designed to be able to have high correlation value. We also proposed a counter plan of public key attack. This method uses a multiple public key generation and distribution.

As the results, the correlation value between the public key and the private key is high in the watermarked image. After the public key attack, this can detect the correlation by using other public key.

▸ Keyword : 상관도검출(correlation detection), 비대칭(asymmetric), 공개키(public key), 공개키 공격(public key attack)

• 제1저자 : 이 덕
• 접수일 : 2008. 10. 16, 심사일 : 2008. 11. 20, 심사완료일 : 2008. 12. 24.
* 연변대학교 공과대학 부교수 ** 상명대학교 디지털저작권보호연구센터 연구교수
*** 상명대학교 소프트웨어대학 교수

Ⅰ. 서 론

디지털 워터마킹 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 멀티미디어 콘텐츠에 대한 지적 재산권을 보호하기 위한 기법이다. 특히 최근 애플사의 스티브 잡스가 음반사들에 DRM Free를 요구하고 나서 워터마킹 기술[1-9]과 콘텐츠 인식기술[10-12]에 대한 수요가 더욱 확대되고 있는 실정이다.

기존의 워터마킹 방식은 삽입기와 검출기에서 동일한 비밀키를 사용하는 대칭키 방식이다. 대칭키 방식의 워터마킹 시스템에서는 삽입과 검출에서 동일한 키를 사용하는 관계로 검증자가 검출기에서 워터마크 정보를 검출하여 삽입된 워터마크 정보를 제거할 수 있게 된다. 따라서 이러한 공격에 대응하기 위해서는 워터마크의 삽입과 검출 시 서로 다른 키를 사용하는 비대칭 워터마킹 기술이 필요하다.

본 논문에서는 상관도 검출기반의 안전성이 높고 검출성능이 우수한 비대칭 워터마킹 방식을 제안한다. 공개 키와 개인키의 생성과정에서는 높은 상관도 검출이 가능하고, 공개 키로부터 개인키 정보를 유추해 낼 수 없도록 직교행렬과 전치행렬에 기반한 안전한 선형변환 방식을 이용하여 공개 키를 구성하였다. 또한 기존의 모든 비대칭 워터미킹 기법에서 공개 키 검출로 인하여 보편적으로 존재하는 공개 키 공격에 효과적으로 대응하기 위하여 공개 키 공격 검증 및 상관도 검출용 공개 키를 추가로 생성하여 분배하는 방식을 제안하였으며 특정된 환경에서 공개 키 공격에 효과적으로 대응하도록 하였다. 본 논문의 실험에서는 이미지에 개인 키를 이용하여 워터마크 정보를 삽입하고 공개 키를 이용하여 상관도 방식으로 정확하게 검출할 수 있음을 확인하였으며 JPEG압축에도 강인한 것으로 검증되었다. 또한 공개 키 공격을 받았을 경우 추가로 발급 받은 공개 키를 이용하여 공격에 대한 판단 및 상관도 검출을 할 수 있음을 보여준다.

본 논문의 구성은 2장에서는 비대칭 워터마킹 기술과 기존 연구들을 비교 분석하고, 3장에서는 제안하는 비대칭 워터마킹 알고리즘 및 공개키 공격 대응방안을 논의하며, 4장에서는 본 제안방식의 실험결과를 분석하고, 5장은 결론에 대해 기술한다.

Ⅱ. 비대칭 워터마킹 기술

비대칭 워터마킹 방식은 공개키 검출방식으로, 공개키 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 소개하도록 한다.

Choi[1]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 변환 행렬이 상쇄되고 결과적으로 원시 키의 상관도로 표현되므로 공개 키를 이용하여 워터마크의 검출이 가능하게 된다.

Picard[2]는 신경망 함수를 이용한 비대칭 워터마킹 방식을 제안하였다. 이 방식은 N크기의 입력을 받아 M크기로 출력하는 선형 신경망 함수를 이용하여 N공간의 비밀 키를 M공간으로 압축시킨다. 워터마크의 삽입은 원본 데이터에 비밀키를 삽입하고, 검출 과정에서는 워터마크가 삽입된 신호를 같은 방식으로 신경망 함수에 입력하여 얻은 값과 공개 키와의 상관도를 구하게 된다.

Smith[3]는 같은 워터마크를 두 번 삽입하여 두 부분의 상관도를 계산하여 검출하는 간단한 형태의 방식을 제안하였고, Furon[4]은 전력 밀도 스펙트럼방식을 이용하여 스펙트럼의 모양으로 워터마크의 삽입 여부를 검증하는 비대칭 워터마킹 방식을 제안하였다.

이외에도 최근에는 보다 안전한 비대칭 알고리즘들이 제안되고 있는데 Fu[5]는 소유권자의 정보와 구매자의 정보를 가증합의 형태로 원본에 삽입하고 대칭 및 비대칭 검출방식으로 하는 방안을 제안하였다. 또 Tzeng[6]은 특정 공간분해를 이용한 비대칭 워터마킹 방안을 제안하였는데 원본 이미지의 특정 분해공간에 워터마크를 삽입하고 특정 매트릭스로 검출하는 방안으로 워터마크의 제거를 어렵게 하는 특징을 갖고 있다. 이외에도 기존의 방안에 대한 분석[7]과 보다 기타 진보

적인 방안[8-9]들이 제안되고 있다.

이러한 기존의 방식들 사이에는 차이점과 유사성이 존재하고 있으며 대부분 다양한 공격에 대하여 적절하게 대응할 수 없는 단점을 안고 있다. Smith의 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. 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 신호간섭으로 검출 성능은 떨어지게 된다. 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. 또한 기존의 모든 비대칭 워터마킹 방식들이 공동으로 안고 있는 공개 키 공격에 대한 문제를 일부 해결할 수 있는 방안을 제안함으로써 앞으로 공개 키 공격을 효과적으로 차단할 수 있는 가능성을 제시하였다.

III. 제안한 비대칭 워터마킹 알고리즘 및 공개 키 공격 대응방안

3.1 개인 키와 공개 키의 생성

제안하는 비대칭 워터마킹 방식은 공개키 암호시스템과 유사하게 개인 키와 공개키로 구성된다. Sr는 대칭 키 워터마킹 시스템에서 단일 키로 사용되는 비밀 키와 동일한 개념의 비밀 키이며, 개인 키와 공개 키는 비밀 키 Sr로부터 생성되게 된다. 대칭과 비대칭 워터마킹 시스템을 상호 비교하고 분석하기 위하여 이들 키들을 명확히 구분하는 것이 바람직하다.

비대칭 워터마킹 시스템의 개인 키와 공개키는 비밀 키를 이용하여 아래와 같이 구성된다. 여기서U는 랜덤 생성 행렬이며 Q는 임의의 랜덤 행렬의 행렬분해에 의해 생성된 직교행렬이다.

$$S = QS_r \quad \cdots\cdots (1)$$

$$P = QU^t US_r \quad \cdots\cdots (2)$$

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. 이와 같이 공개 키와 개인 키를 구성하는 또 다른 이유는 공개 키 생성기가 임의의 랜덤행렬 U를 변경함으로써 공개 키 공격이 발생하였을 경우 쉽게 추가 검증용 공개 키를 생성할 수 있도록 하기 위함이다.

3.2 워터마크의 생성 및 삽입 방식

워터마크는 아래의 식(3)에서와 같이 생성되는데 여기서 m은 삽입 비트 정보로서 m∈{-1,1}의 값을 취하며 m이 -1일 경우는 bit 1을 m이 1일 경우는 bit 0가 삽입됨을 의미한다. S는 식(1)에서 생성된 개인 키이다.

$$W = m \cdot S \quad \cdots\cdots (3)$$

$$I_i(w) = I_i + W_i \quad \cdots\cdots (4)$$

워터마크의 삽입은 식(4)과 같이 n*n의 정보삽입 블록에 워터마크를 삽입하게 된다. I_i와 $I_i(w)$는 정보 삽입블록과 워터마크가 삽입된 블록이다. W_i는 하나의 정보 삽입블록에 삽입되는 워터마크신호이다. 검출 시에 하나의 n*n 블록에서 1bit의 정보를 추출하게 된다.

이외에 전체 이미지에 1bit의 정보만 삽입할 경우, 즉 정보의 삽입 여부만 판단하는 경우의 응용에서는 JPEG압축에 강인하게 하도록 설계 하기 위하여 특정 8*8 DCT 블록 패턴에 워터마크를 삽입하게 된다. 즉 n*n 개인 키 중의 몇 bit (본 논문의 실험에서는 4bit 만을 취함)씩만을 취하여 8*8 DCT 특정 블록에 반복적으로 삽입하는 방식으로 전체 개인 키를 하나의 이미지에 삽입할 수 있도록 한다. 이 경우 개인 키를 하나의 DCT 블록에 삽입하는 과정을 식 (5)와 같이 표시할 수 있다.

$$I_i(w) = I_{DCT(i)} + S_{B(i)} \quad \cdots\cdots (5)$$

3.3 공개 키를 이용한 워터마크 검출

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

$$C=P^{t}I(w)=(S_r^{t}U^{t}UQ^{t})I+(S_r^{t}U^{t}UQ^{t})N+m(S_r^{t}U^{t}UQ^{t})QS_r$$
$$=(S_r^{t}U^{t}UQ^{t})I+(S_r^{t}U^{t}UQ^{t})N+mV^{t}V \quad \cdots\cdots (6)$$

식(6)의 세 번째 항에서는 직교행렬의 전치행렬은 역 행렬과 같다는 특성을 이용하여 계산과정에서 Q가 상쇄되며 결과적으로 V=USr 의 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 값만으로 개인 키의 삽입 여부를 판단할 수 있게 된다. 이렇게 되어 상관도 검출과정에서비밀 키나 개인키 정보를 직접 사용하지 않고 공개 키 정보만을 이용하여 검출이 가능하며, 공개키 정보로부터 개인 키 정보나 비밀 키 정보를 계산하는 것은 매우 어렵게 된다.

3.4 공개 키 공격 분석

공개 키의 상관도 검출 시에는 공개 키를 이용한 공격이 항상 존재하게 된다. 식(7)과 같이 워터마크가 삽입된 신호에 적당한 강도로 공개 키를 빼주면 음의 공개 키가 상관도를 떨어뜨리게 되어 워터마크가 검출되지 않게 할 수 있다. 여기서 $I(w)'$은 공개키 공격을 받은 후의 신호이고 β는 공개키 공격 강도이다.

$$C_{at}=P^{t}I(w)'$$
$$=P^{t}(I(w)-\beta P)\ll P^{t}I(w) \quad \cdots\cdots (7)$$

이와 같이 공개 키 공격이 성공하는 이유는 비대칭 워터마킹 시스템의 특징상 검출기에서 공개 키를 공개하고 공개 키와 워터마크가 삽입된 신호를 이용하여 검출하도록 하기 때문이다. 공개 키 공격이 성공하는 경우 공격된 신호와 공격하기 전의 신호와의 왜곡 정도를 평가해 비대칭 방식들의 성능을 평가하는데 대부분의 방식이 변형 정도가 2~3dB 정도로 높지 않아 이러한 공격이 충분히 가능하다고 할 수 있다.

공개 키 공격은 공격자가 검증자인지 아니면 이미 외부로부터 공격 받은 신호를 검증자가 검증하는 경우인지에 따라 내부자 공격과 외부자 공격으로 나누어 볼 수 있다. 내부 공격은 워터마크 검증자가 공개 키를 이용하여 워터마크가 삽입된 신호에 대하여 공개 키 공격을 가하고 워터마크가 삽입되어 있지 않다고 주장하는 경우이며, 외부 공격은 워터마크가 삽입된 신호가 다른 공격자에 의해 이미 공격을 받았고 워터마크 검증자는 공격을 받은 신호로 검출을 하여 워터마크 신호를 검출할 수 없게 되는 경우를 의미한다. 비대칭 워터마킹 시스템의 특징상 내부 공격은 원천적으로 막기가 어렵다. 본 제안 방식에서는 검증 및 추가 검출용 공개 키의 생성으로 외부 공격과 내부 공격을 판단하는 기준을 제공하며, 일부 공격에 효과적으로 대응하도록 구성하였다.

3.5 공개 키 공격 대응 방안

공개키 공격에 대한 대응책으로 개인 키로 검출하는 방식이 있으나 개인 키로 검출할 경우 비대칭 시스템의 특성상 개인 키를 검증자에게 전달하여 검출하도록 할 수는 없고 증명자가 공격을 받은 콘텐츠를 검증자로부터 받아서 개인 키로 워터마크를 검출하여 그 결과를 검증자에게 확인시켜야 한다. 하지만 이와 같이 검증자가 검증하여야 하는 부분을 증명자가 대신 하게 되면 신뢰성 문제가 발생하게 될 우려가 있고 더욱 중요한 것은 비대칭 시스템의 의미를 상실하여 대칭 방식의 검출과 별다를 바가 없게 된다는 것이다.

따라서 본 논문에서는 증명자가 공개 키를 추가로 재발급하는 방법을 제안한다. 공개 키 공격을 받았을 경우 증명자는 검증자에게 아래와 같이 식(8)을 이용하여 검증 및 검출용 공개 키 PVD를 추가로 발급하게 된다.

$$P_{VD}=QU_{VD}^{t}U_{VD}S_r \quad \cdots\cdots (8)$$

이 식에서 UVD는 기존의 공격에 사용된 공개 키 P의 생성시 사용된 U와 Orthogonal 관계의 랜덤 행렬이며 Q와 Sr은 P의 생성에 사용된 직교행렬과 비밀키 그대로 사용한다. 이렇게 함으로써 PVD가 기존의 개인 키와 상관관계를 발생하도록 하여 상관도 검출이 용이하도록 구성하였다. 식(9)는 PVD가 공개 키 P에 의해 공격 받은 신호에서 상관도 검출을 하는 과정을 보여준다. 여기서 β는 P의 공격 강도이다.

$$C_V=(P_{VD})^{t}(I(w)-\beta P)$$
$$=P_{VD}^{t}I(w)-\beta P_{VD}^{t}P \quad \cdots\cdots (9)$$

PVD는 개인 키와 공개 키 P와 모두 상관관계를 발생하므로 이 식의 첫 번째 항과 두 번째 항 모두 상관도 값이 발생하나 두 번째 항의 PVD와 P의 상관도는 자기 상관 보다 작은

값이고 또 β는 P의 공격 강도이므로 첫 번째 항에서 발생된 상관도 값 전체를 떨어뜨리지는 못한다. 하여 CV는 여전히 어느 정도의 상관도 값으로 나타나게 된다. 따라서 검증자의 공격이 가해지지 않는 외부 공격의 경우에는 이와 같은 방법으로 공개 키를 추가로 발급하여 상관도 검출을 효과적으로 수행할 수 있게 된다.

하지만 검증자가 공개 키 공격을 하는 내부 공격의 경우 검증자는 워터마크가 삽입된 신호에서 자신이 공개 키 공격에 사용했던 공개 키 P를 제거하고 새로 발급 받은 공개 키 PVD를 이용하여 식(9)와 유사하게 재차 공격하게 된다. 이 경우에는 식(10)과 같이 다시 원래의 공개 키 P로 검출이 가능하다.

$$C=(P)^t(I(w)-\beta_{VD}P_{VD}) \\ =P^tI(w)-\beta_{VD}P^tP_{VD} \quad \cdots\cdots (10)$$

이외에도 검증자는 기존의 공개 키 P와 새로 발급받은 공개 키 PVD를 모두 사용하여 식(11),(12)와 같이 공격을 할 수 있다. 이 경우에는 두 공개 키의 공격 강도에 따라 공격의 공격 유형을 비대칭형 공격과 대칭형 공격으로 나눌 수 있다. 비대칭형 공격은 두 개의 공개 키의 공격 강도가 서로 다른 경우를 말하는데 이 경우에는 단일 공개 키 공격에 대한 방어와 유사하게 공개 키 P로 검출이 불가능하도록 공격한 신호에 대해 PVD를 이용하여 검출하고 PVD로 검출이 불가능하도록 공격한 신호에 대해 P를 이용하여 상관도 검출이 가능하다.

$$C_1=(P)^t(I(w)-\beta_1P-\beta_{VD1}P_{VD}) \\ =P^tI(w)-\beta_1P^tP-\beta_{VD1}P^tP_{VD} \quad \cdots\cdots (11)$$

$$C_2=(P_{VD})^t(I(w)-\beta_2P-\beta_{VD2}P_{VD}) \\ =P_{VD}{}^tI(w)-\beta_2P_{VD}{}^tP-\beta_{VD2}P_{VD}{}^tP_{VD} \quad \cdots\cdots (12)$$

하지만 두 공개 키의 공격 강도가 서로 같은 대칭형 공격의 경우 적당한 공격 강도를 취하면 식(13),(14)에서와 같이 어느 하나의 공개 키를 이용하여도 상관도 검출을 할 수 없게 된다. 이러한 공격은 어떠한 방법으로든 방어를 하기가 어려우므로 이런 공격은 탐지하여 적발하는 것이 필요하다.

$$C_{31}=(P)^t(I(w)-\beta_3P-\beta_3P_{VD}) \\ =P^tI(w)-\beta_3P^tP-\beta_3P^tP_{VD} \quad \cdots\cdots (13) \\ \ll P^tI(w)$$

$$C_{32}=(P_{VD})^t(I(w)-\beta_3P-\beta_3P_{VD}) \\ =P_{VD}{}^tI(w)-\beta_3P_{VD}{}^tP-\beta_3P_{VD}{}^tP_{VD} \quad \cdots\cdots (14) \\ \ll P_{VD}{}^tI(w)$$

따라서 본 논문에서 제안하는 비대칭 워터마킹 시스템에서는 우선 키 생성 시스템에서 검증용 공개 키 PVD를 생성하여 검증자에게 보내주어 내부공격과 외부공격을 판단하게 되는데, 만일 검증자가 PVD를 이용하여 효과적으로 공격 받은 신호로부터 상관도 검출을 진행하였다면 외부 공격이라고 판단하게 된다. 그렇지 않고 검증자가 PVD나 P를 이용하여 공격 받은 신호로부터 상관도 검출을 할 수 없다고 주장한다면 검증자가 1차 공격에 이어 스스로 2차 내부 공격을 시행하였음을 확인할 수 있게 된다. 이럴 경우 증명자는 검증자가 공격자라고 지목하고 저작권 침해로 신고 할 수 있게 된다.

Ⅳ. 실험결과 및 고찰

본 알고리즘의 구현과정에서 512*512의 표준 영상을 사용하여 공간영역에 삽입하였으며, 1bit의 정보만 삽입할 경우에는 JPEG압축에 강인한 방식을 구성하기 위하여 DCT 영역에서 구현하였다. 정보 삽입 블록(n*n)과 128*128 블록을 사용하였으며, 본 논문에서 사용된 모든 키와 QR분해로 생성된 행렬 Q도 128*128 행렬을 사용하였다.

그림1은 JPG압축후 개인 키와 공개 키의 상관도 값을 정규화 한 검출결과로서 왼쪽이 개인 키 검출 결과(Cmax=0.1161, Csnd=0.0198)이고 오른쪽이 공개 키 검출결과(Cmax=0.1044, Csnd=0.0260)이다. 이과 같은 결과는 DCT 도메인에서 8*8 DCT 블록의 특정 위치에 개인 키를 삽입하고 상관도 검출을 진행한 결과이다.

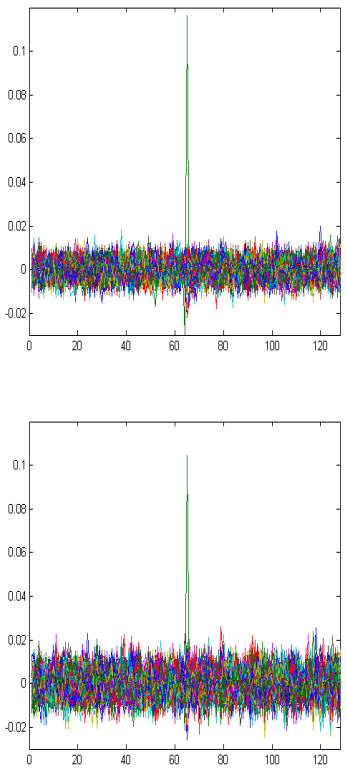

그림 1. JPG압축후의 개인 키와 공개 키의 상관도 검출 (정규화)
Fig 1. Correlation detection of private key and public key with JPEG compression (normalization)

그림2는 JPEG압축의 QF(Quality Factor)에 따른 비밀키(실선), 개인 키(굵은점선), 공개 키(가는점선)의 Cmax을 보여줌으로써 QF에 따른 대칭 및 비 대칭 워터마킹 시스템의 검출 성능을 비교하였다. 여기서 알 수 있듯이 비 대칭 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.)

그림3은 BMP를 대상으로 공격 실험을 진행한 것으로 공개 키 P로 공격 받은 후 추가 발급한 검증용 공개 키 PVD로 검출한 결과를 보여준다. 왼쪽은 공개 키 P로 공격을 받은 후 P로 상관도 검출이 불가능함을 보여주는데 공격 시 사용한 베타 값은 2.5e-4이다. 오른쪽은 공개 키 PVD로 상관도 검출을 정확히 진행한 검출결과(Cmax=0.0539, Csnd=0.004)를 보여준다.

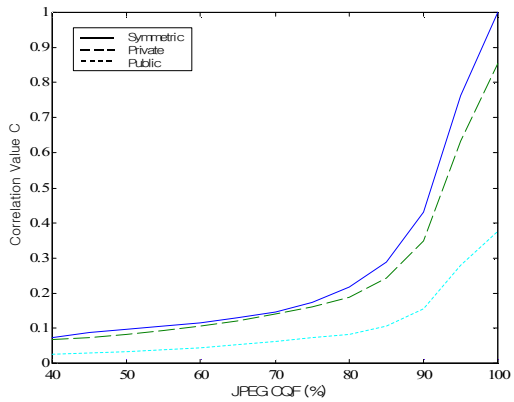

그림 2. QF에 따른 대칭 및 비 대칭 시스템 검출 성능비교
Fig 2. Comparison of detection performance of symmetric and asymmetric system with quality factor

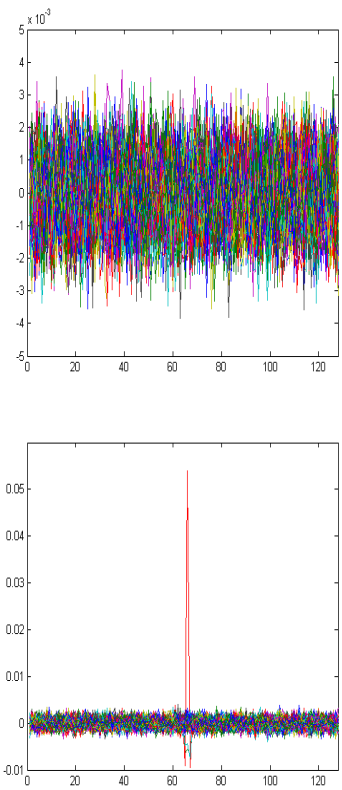

그림 3. 공개 키 공격 검증 및 검출 (BMP)
Fig 3. Public key Attack Verification & Detection (BMP)

그림4는 JPG를 대상으로 공격 실험을 진행한 것으로 공개 키 P로 공격 받은 후 추가 발급한 검증용 공개 키 PVD로 검출한 결과를 보여준다. 왼쪽은 공개 키 P로 공격을 받은 후 P로 상관도 검출이 불가능함을 보여주는데 공격 시 사용한 베타 값은 2.8e-4이다. 오른쪽은 공개 키 PVD로 상관도 검출을 정확히 진행한 검출결과(Cmax=0.6899, Csnd=0.2836)를 보여준다. 이는 DCT 도메인에서 8*8 DCT 블록의 특정 위치에 개인 키를 삽입하고 상관도 검출을 진행한 결과로서 JPEG 압축 상태에서 공개 키 공격 받았을 경우에도 여전히 상관도 검출이 가능함을 증명한다. 여기서 QF=65%를 사용하여 실험을 진행하였다.

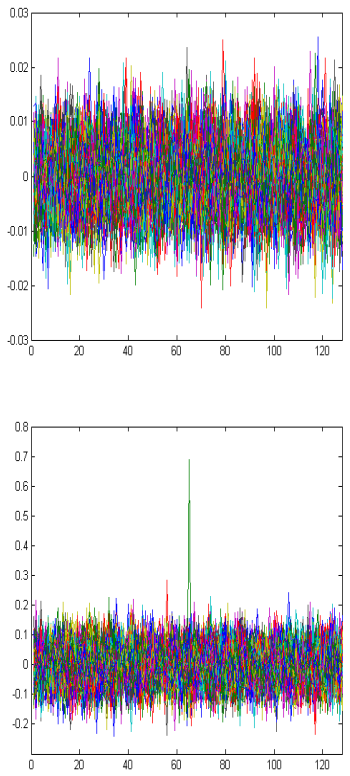

그림 4. 공개 키 공격 검증 및 검출 (JPG)
Fig 4. Public key Attack Verification & Detection (JPG)

V. 결 론

워터마크 삽입기와 검출기에서 동일한 비밀 키 정보를 사용하는 대칭 키 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 사용하는 비대칭 워터마킹 방식에 대한 연구가 다양한 측면에서 이루어지고 있다. 하지만 기존의 연구들은 비대칭 워터마킹 시스템이 안고 있는 공개키 공격에 대한 효과적인 대응방안을 제시하지 못하고 있다.

본 논문에서는 상관도 검출기반의 안전성이 높고 검출성능이 우수한 비대칭 워터마킹 방식을 제안하였다. 공개 키로부터 개인 키를 계산할 수 없도록 하기 위하여 공개 키와 개인 키의 생성은 특수행렬을 이용한 선형변환 방식에 기초하였으며 높은 상관도 검출이 가능하도록 구성되었다. 또한 기존의 모든 비대칭 워터마킹 기법들에서 보편적으로 존재하는 공개 키 공격에 효과적으로 대응하기 위하여 공개 키 공격 검증 및 검출용 공개 키를 추가로 생성하여 분배하는 방식을 제안하여 일부 공개 키 공격에 효과적으로 대응하도록 하였다.

본 논문의 제안방식은 이미지뿐만 아니라 다양한 멀티미디어 콘텐트에 적용 가능한 기술이다. 실험결과 워터마크가 삽입된 영상에서 공개 키 및 개인 키로 효과적으로 높은 상관도 검출을 할 수 있었으며 JPEG압축 후에도 높은 상관도 검출이 가능한 것으로 나타났다. 또한 공개 키 공격을 받은 영상에서 추가로 발급된 검증용 공개 키로 효과적으로 상관도 검출을 할 수 있음을 확인하였다.

참고문헌

[1] 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.

[2] 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.

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

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

Dresden, Germany, Oct, 1999.
〔5〕 Fu Y, Shen R, Shen L. A novel asymmetric watermarking scheme, Proceedings of the Third International Conference on Machine Learning and Cybernetics, Shanghai, August, 26-29, 2004
〔6〕 Tzeng J, Hwang W L, and Chen I L., An asymmetric subspace watermarking method for copyright protection, IEEE Trans. Signal Process, 53(2): 784-792, 2005
〔7〕 Chen I Te and Yeh Yi Shiung. Security analysis of transformed key asymmetric watermarking system. IEEE Signal Processing Letters, 13(4): 213-215, 2006
〔8〕 TAN Xiu-hu, LIU Guo-zhi, WANG Rui. An asymmetric watermarking robust blind watermarking algorithm. Journal of Naval University of Engineering, Vol.19 No1. 2007
〔9〕 LIU Xiang-li, DANG Lan-jun, KOU Wei-dong, WANG Zhi-guo. An Asymmetric Digital watermarking Algorithm Based on 2DFT. Journal of Sichuan University, Vol.39 No5. 2007
〔10〕 이재혁, 문호석, 박상성, 장동식, "영상의 에지 특성을 고려한 웨이블릿 기반의 적응적인 워터마킹 기법", 한국컴퓨터정보학회 논문지 제11권 제2호, 2006년
〔11〕 성보경, 정명범, 고일주, "음악 특징점간의 유사도 측정을 이용한 동일음원 인식방법", 한국컴퓨터정보학회 논문지 제13권 제3호, 2008년
〔12〕 하정요, 최미영, 최형일, "색상과 형태를 이용한 내용 기반 영상 검색", 한국컴퓨터정보학회 논문지 제13권 제1호, 2008년

저 자 소 개

이 덕 (Li De)

1996년(중) 할빈이공대학교 전기공학과 졸업 (공학사)
2001년 상명대학교 전자계산학과 졸업 (이학석사)
2000년~2005년 상명대학교 컴퓨터과학과 (컴퓨터과학박사)
2008년~현재 연변대학교 공과대학 컴퓨터과학과 부교수
관심분야: 디지털워터마킹, 저작권관리기술, 디지털신호처리, 컴퓨터시스템 및 네트워크보안

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 부설연구소장
2005~현재 상명대학교 디지털저작권보호연구센터 책임연구원
관심분야: 디지털워터마킹, 저작권보호 및 관리기술, 디지털신호처리

최 종 욱

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