情 報 保 護 學 會 誌
第 12 券 第 1 號, 2002. 2

비대칭 워터마킹 시스템에 관한 연구

최 혁*, 김 태 정*

요 약

디지털 데이터의 저작권 보호를 위해 사용되는 워터마킹은 키의 대칭성 측면으로 볼 때 대칭 방식과 비대칭 방식으로 나눌 수 있다. 기존의 연구들은 거의 모두가 대칭 워터마킹의 형태로 이루어져 왔으나 공개적인 검출이 필요한 워터마킹의 특성상 삽입키와 검출키가 같은 대칭 형태에서는 검출기에서 유출되는 정보에 의해 삽입키가 제거될 수 있는 안전성 문제를 가지고 있다. 이를 해결하기 위해 검출키와 삽입키가 다른 비대칭 워터마킹 방식이 대두되었다. 본 논문은 최근에 2세대 워터마킹 방식으로 주목을 받고 있는 비대칭 워터마킹의 개념과 기존의 연구들을 소개하고 그들의 성능을 비교, 분석하였다.

Ⅰ. 서 론

최근 디지털 신호는 오디오, 비디오, 정지 영상 등에서 아날로그 신호를 대체하고 있다. 아날로그 신호는 원래의 신호를 정확하게 표현할 수 있다는 장점이 있지만, 미세한 잡음에도 쉽게 영향을 받아 원래의 신호가 변경되기가 쉽다. 이에 반해 디지털 신호는 잡음에 대해서 강인할 뿐만 아니라 복제 후에도 원본과 완전히 동일한 신호를 갖는다. 그러나 복제된 신호가 원본과 동일하기 때문에 불법적으로 복제된 복사본들이 원본의 가치를 떨어뜨리고 지적 재산권(intellectual property right, IPR)을 침해할 수도 있다. 또한, 디지털로 저장, 전송되는 비중이 커지면서 디지털 신호에 대한 저작권(copyright)의 보호는 중요한 문제로 제기되고 있으며 이를 위한 효율적인 방법이 요구되고 있다.

디지털 워터마킹(watermarking)은 디지털 신호에 특정한 정보를 담고있는 워터마크를 사용자가 인식할 수 없도록 삽입하는 것을 말하며 삽입된 정보를 이용하여 디지털 신호의 소유권을 보호한다[1].

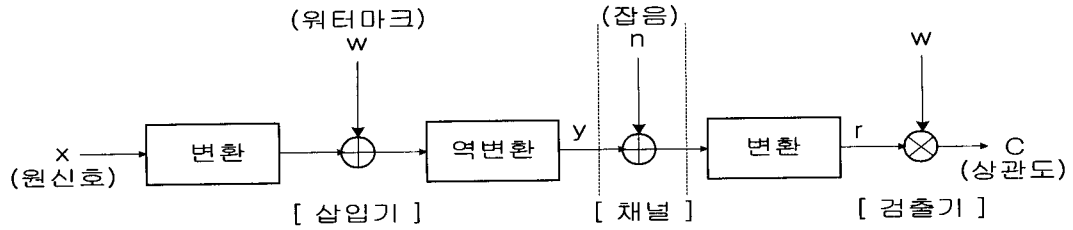
워터마크는 소유권이외에도 디지털 신호의 원본의 진위, 판매경로 등을 확인하는 경우에 사용될 수 있다. 이밖에도 광역 모니터링, 인증, 복사 방지 등의 활용에 사용되기도 한다.

일반적으로 워터마킹에 요구되는 요건들에는 인간 지각에 거슬리지 않게 워터마크를 삽입하는 투명성, 다양한 변형 뒤에도 워터마크를 검출할 수 있는 강인성, 삽입되는 정보의 양, 의도적인 공격에 대한 안전성 등이 고려되고 있다. 그러나, 이들 요건들은 서로 상충적인 특성을 가지고 있어 각기 활용에 따라 적절하게 타협되어 시스템 구현에 적용된다.

기존의 워터마킹에 대한 연구들은 소유권 정보를 제공하는 경우를 고려하여 워터마크가 쉽게 지워지지 않도록 강인성에 초점을 맞춘 알고리듬의 개발에 주력해 왔다. 그러나, 실제적인 환경에서 워터마킹을 사용하는 경우 다양한 의도적 공격, 즉, 삽입된 워터마킹을 제거하거나 검출이 불가능하도록 만들려는 공격들에 대한 안전성이 보장되어야 한다. 특히, 실제적인 워터마킹의 응용환경이 일반 사용자가 검출기를 통해 쉽고 자유롭게 워터마크 정보를 확인하는 상황에서 안전성에 대한 문제는 더욱더 중요하고 어려운 문제라고 할 수 있다.

키의 대칭성 측면에서 워터마킹 방식을 분류해 보면 거의 모든 방식이 삽입기와 검출기 측에서 같은 워터마크를 사용하는 대칭 워터마킹이다. 이러한 경우에, 일반 사용자가 공개적으로 검출기를 이용하여 워터마크 정보를 확인하는 환경에서는 공개된 검출기가 공격이나 실수에 의해 내부 키 정보가 유출되는 경우 유출된 정보가 삽입기의 정보와 동일하기 때문에 시스템 전체의 안전성에 위협이 되게 된다. 이를 막기 위해서는 삽입기와 검출기의 워터마크를 다르게 사용하는 비대칭 워터마킹 방식이 필요하다.

* 서울대학교 전기컴퓨터공학부 정보시스템 연구실 (camel@infolab.snu.ac.kr, tkim@snu.ac.kr)



〔그림 1〕 일반적인 워터마킹 과정

비대칭 워터마킹은 비대칭 암호화의 개념과 매우 유사한데 삽입기와 검출기에서 서로 다른 키를 이용함으로써 검출기에서 내부 키 정보가 유출되어도 삽입키의 정보는 안전하게 보존됨으로써 전체 시스템의 안전성을 향상시킬 수 있다.

본 논문에서는 비대칭 워터마킹 방식의 개념을 암호화의 경우와 비교하여 살펴보고 최근에 제안된 비대칭 방식들의 내용을 소개한다. 또, 각 방식들의 특성들을 살펴보고 그들의 성능을 분석한다.

Ⅱ. 암호화와 워터마킹

1. 대칭 시스템

디지털 워터마킹의 과정은 워터마크의 생성, 삽입, 검출의 세가지 과정으로 이루어져 있으며 일반적으로 워터마크가 삽입된 신호가 전송되어 검출되는 과정을 도시해보면 그림 1과 같다.

워터마크의 생성은 삽입하고자 하는 정보를 생성자만이 알고 있는 비밀키에 의해 변조하여 사용하는데 이진 m-수열, 가우시안 랜덤 수열 등이 워터마크로 많이 사용된다.

$\mathbf{x}$를 커버 데이터라고 부르고 워터마크가 삽입될 디지털 컨텐츠 신호라 할 때, 생성된 워터마크 $\mathbf{w}$는 다음과 같이 커버 데이터에 더해진다.

$$\mathbf{y} = \mathbf{x} + \alpha\,\mathbf{w} \tag{1}$$

이때, $\mathbf{y}$는 워터마크가 삽입된 데이터를 말하며, α는 삽입된 워터마크가 인간 지각에 거슬리지 않을 정도의 크기를 갖도록 조절하는 상수이다. 워터마크가 삽입되는 영역은 영상의 공간 영역이나 음성의 시간축 영역 등 원신호에 그대로 더해지는 경우도 있지만 커버 데이터를 DFT, DCT, DWT 등과 같은 변환을 거친 후에 변환 영역에 삽입할 수도 있다. 일반적으로 변환 영역에 워터마크를 삽입하는 경우가 일반적인 신호처리 변형에 더 강인하다고 알려져 있다.

전송 과정에서 채널 잡음 등이 더해진 뒤 검출단에서는 삽입되어 있는 워터마크와 같은 기준 수열 $\mathbf{w}$를 이용하여 상관도 검출을 행한다. 즉, 워터마크가 삽입되어 있으면 전송된 신호와 기준 수열의 상관도가 기준값 보다 커서 워터마크가 삽입되어 있음을 알 수 있으며 그렇지 않은 경우는 워터마크가 삽입되어 있지 않다고 판단한다.

워터마킹의 삽입과 검출 과정은 암호화, 복호화 과정과 유사하다. 대칭 암호화 (또는 비밀키 암호화)에서 암호화 과정은 다음과 같다[2].

$$c = E_K(m) \tag{2}$$

$E_K(\cdot)$는 키 K를 사용하는 암호화 함수를 말하며, m은 메시지를, c는 암호문을 말한다. 암호문은 같은 키를 사용하는 복호화 함수 $D_K(\cdot)$에 의해 복호화된다.

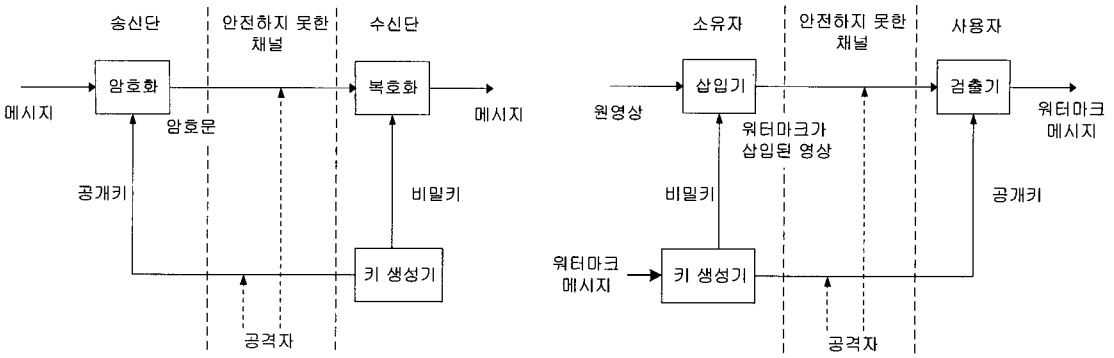
$$m = D_K(c) \tag{3}$$

워터마킹에서도 삽입과정을 다음과 같이 표현할 수 있다.

$$\mathbf{y} = \varepsilon_K(\mathbf{x}, m) \tag{4}$$

$\varepsilon_K(\cdot)$는 삽입 함수이고, 메시지 m은 키 K에 의해 워터마크 $\mathbf{w}$로 만들어져 커버 데이터에 삽입된다. 삽입된 메시지는 검출 함수 $d_K(\cdot)$에 의해 다음과 같이 검출된다.

$$m = d_K(\mathbf{y}) \tag{5}$$



(a) 비대칭 암호화 (b) 비대칭 워터마킹

〔그림 2〕 비대칭 시스템 비교

식 (2)-(5)를 비교해보면 워터마킹 과정과 암호화 과정이 매우 유사한 형태를 가짐을 알 수 있다. 이러한 유사성은 비대칭 암호화와 비대칭 워터마킹의 개념에서도 찾아볼 수 있다.

2. 비대칭 시스템

2.1 비대칭 암호화

암호화에서도 대칭 암호화 방식이 먼저 개발되어 오랫동안 사용되어 왔다. 대칭 암호화의 장점은 빠른 처리 속도와 오랫동안 검증되어 온 안전성 등을 생각해 볼 수 있지만 키의 관리 문제에서 약점을 가지고 있다. 즉, 두 사람이 안전하게 암호화를 통해 메시지를 주고 받기 위해서는 서로 같은 키를 가지고 있어야 하는데 키를 안전하게 전달하고 보존하는 것은 매우 어려운 문제이다. 특히 다자간에 메시지 교환을 하기 위해서는 각각의 전송시에 서로 다른 키가 요구되기 때문에 키의 분배 문제 또한 매우 중요한 문제로 작용한다. 그래서 이러한 키의 분배 및 관리 문제를 해결하기 위해 비대칭 암호화가 개발되었는데 비대칭 암호화는 암호화와 복호화에서 서로 다른 키를 사용함으로써 이러한 문제를 해결하였다. 즉, 비밀키와 공개키를 쌍으로 생성한 뒤 공개키 만을 공개해 두면 수신자에게 메시지를 전달하고 싶은 송신자는 수신자의 공개키를 이용하여 메시지를 암호화한 뒤 암호문을 전송한다. 물론 두 키 사이에는 수학적인 관계가 있고, 공개키에 의해서는 비밀키를 찾아내기가 불가능 해야한다. 수신자는 자신만이 알고 있는 비밀키를 이용하여 암호문을 복호화하고 메시지를 확인하게 된다. 비대칭 암호화의 방식은 그림 2 (a)와 같이 도시할 수 있다.

2.1 비대칭 워터마킹

대칭 워터마킹 시스템은 암호화와 마찬가지로 키가 안전하게 보존된다는 가정 하에서 시스템의 안전성이 보장된다. 그러나 이러한 키의 안전한 관리는 매우 어려운 일이며 안전성 문제가 존재한다. 이를 해결하기 위해 암호화와 유사하게 비대칭 워터마킹 시스템을 생각해 볼 수 있으며 그림 2 (b)와 같이 도시해 볼 수 있다.

워터마킹과 암호과정에는 차이점도 존재한다. 워터마킹은 송신자에 의해 워터마크 키가 생성되며 검출 방식도 유사성을 비교하는 상관도 검출을 하기 때문에 암호화에서처럼 메시지와 암호문이 일대일 관계를 가지지 않고 일대다 관계를 가지게 된다. 또한 암호화된 메시지는 그 자체로의 의미는 부여되지 않으며 복호기에 전송되는 암호문이 변경되지 않음을 가정하고 있다. 이와는 달리 워터마킹은 워터마크가 삽입된 데이터는 원본과 크게 다르지 않아야 하며 일반적인 신호처리 뿐 아니라 고의적인 공격에도 강인해야 하므로 암호화의 이론 및 기법을 비대칭 워터마킹에 그대로 적용하는 것은 적절하지 못하다.

Ⅲ. 비대칭 워터마킹 기술

우리는 2절에서 언급된 비대칭 암호화와 비대칭 워터마킹의 개념 비교를 바탕으로 선형 랜덤 변환을 이용한 비대칭 워터마킹 방식을 제안하였다[3]. 본

절에서는 제안된 변환키 방식과 함께 최근까지 여러 가지 방식으로 제안되어 온 비대칭 방식들을 발표된 순서대로 간단히 정리해 본다.

1. Hartung 방식

Hartung과 Girod는 삽입기에서 사용하는 워터마크 키와 일부만 같은 검출키를 사용하는 매우 간단한 형태의 비대칭 방식을 제안하였다[4]. 즉, 삽입기에서 사용하는 워터마크 수열이 $\mathbf{w}$일 때 삽입워터마크와 일부가 같은 검출 워터마크 $\mathbf{w}_p$를 생성한다. $\mathbf{w}_p$의 나머지 부분은 임의로 발생시킨다. 예를 들어, $\mathbf{w}$와 $1/n$만큼 같은 $\mathbf{w}_p$를 생성하는 경우 검출기에서 상관도 값은 $1/n$만큼 떨어지지만 이 값이 검출기의 기준값 이상이면 여전히 검출이 가능하다. 이때 검출 워터마크의 $n-1/n$은 안전하다고 말할 수 있다.

이 방식은 비대칭 워터마킹의 개념을 처음으로 언급한 것에 의미가 있지만, 신뢰성 있는 검출을 위해서는 삽입 워터마크의 많은 부분을 공개하여야 하며 공개된 검출 워터마크를 이용하여 삽입된 워터마크의 검출을 막을 수 있다. 공개키를 이용한 공격은 4절에서 다시 언급된다.

2. Van Schyndel 방식

Van Schyndel 외 저자들은 Legendre 수열을 이용한 워터마킹 시스템을 제안하였다[5]. Legendre 수열은 다음과 같은 특성을 가지고 있다.

$$\mathbf{Fa} = \mathbf{a}_{DFT} = c\,\mathbf{a}^* \tag{6}$$

이때 $\mathbf{F}$는 이산 푸리에 변환 행렬을 말하며 c는 상수를 $\mathbf{a}^*$는 켤레 복소수 수열을 말한다. 즉, Legendre 수열은 그 수열을 푸리에 변환하면 같은 수열의 켤레 형태를 얻을 수 있다. Van Schyndel은 이러한 특성을 이용하여, Legendre 수열 $\mathbf{a}$를 워터마크 $\mathbf{w}$로 사용하여 워터마크가 삽입된 커버 데이터 $\mathbf{y} = \mathbf{x} + \mathbf{a}$을 얻었다.

전송된 신호 $\mathbf{y}$에서 워터마크를 검출하기 위해서는 전송된 신호와 전송된 신호의 푸리에 변환된 신호와의 상관도를 이용하였다.

$$C = \frac{\mathbf{y}^t(\mathbf{Fy})}{N} \approx \frac{c\,\mathbf{a}^h\mathbf{a}}{N} \tag{7}$$

이때, t는 전치(transpose)를, h는 켤레 전치를 말한다. 검출기에서는 삽입된 Legendre 수열에 대한 정보를 사용하지 않으며 삽입된 수열의 길이만 주어진다. 그러나, 식 (7)에서 알 수 있듯이 상관도의 값이 삽입된 Legendre 수열의 상관도의 값으로 표현되므로 워터마크의 삽입 여부를 판단할 수 있다.

3. Egger 방식

Legendre 워터마킹의 핵심 개념은 이산 푸리에 변환이 Legendre 수열을 그 자신으로 다시 사상시킨다는 것을 이용하였다. Egger 외 저자들은 이러한 접근과 유사한 방식으로 선형 변환의 고유 벡터를 이용한 비대칭 방식을 제안하였다[6].

$N\times N$ 변환 행렬 $\mathbf{G}$는 행렬의 고유 벡터 $\mathbf{w}$와 일치하는 고유값 λ_0사이에 $\mathbf{Gw} = \lambda_0\,\mathbf{w}$의 관계를 가진다. 고유 벡터를 워터마크로 이용하여 커버 데이터에 삽입하면, Legendre 워터마킹과 유사한 형태로 전송된 신호와 전송된 신호를 주어진 변환 행렬에 의해 변환시킨 신호 사이의 상관도를 통해 삽입된 워터마크를 검출할 수 있다. 즉,

$$C = \mathbf{y}^h\,\mathbf{Gy}/N \approx \lambda_0\,\mathbf{w}^h\,\mathbf{w}/N \tag{8}$$

이 되고 상관도값을 기준값과 비교하여 삽입된 워터마크를 검출한다. 즉, 변환 행렬 $\mathbf{G}$는 공개키로써 검출 시에 사용되며, 고유 벡터 $\mathbf{w}$는 비밀키로써 삽입되는 워터마크로 사용되지만 검출기에서는 그 정보를 사용하지 않고 검출이 이루어진다.

4. Smith 방식

Smith와 Dodge는 매우 간단한 형태의 비대칭 방식을 제안하였다[7]. 삽입 과정은 단순히 같은 워터마크를 두 번 반복해서 삽입하며 검출과정은 두 번 삽입된 워터마크의 상관도를 이용하여 검출한다. 즉, 길이 N의 커버 데이터에 길이 $N/2$인 워터마크 $\mathbf{w}$를 두 번 삽입하면 워터마크가 삽입된 신호는 $y(n) = x(n) + w(\mathrm{mod}(n, N/2)),\ \forall n \in 0,\ldots,N-1$이 된다. 이때, mod(,)는 모듈로 함수를 말한다.

검출기에서는 전송된 신호 $\mathbf{y}$를 반으로 잘라서 두 부분 수열의 상관도를 구한다.

$$C=\frac{\mathbf{y}_1^{\,t}\,\mathbf{y}_2}{N/2}\approx\frac{\mathbf{w}^{t}\,\mathbf{w}}{N/2} \tag{9}$$

상관도 값에서 삽입된 워터마크 수열을 사용하지 않고 삽입된 워터마크의 검출이 가능함을 알 수 있다.

5. Furon 방식

Furon과 Duhamel은 전력 밀도 스펙트럼(PDS)을 이용한 비대칭 워터마킹 방식을 제안하였다[8]. 워터마킹 과정을 정리해보면 다음과 같다.

먼저, 커버 신호를 치환시켜서 신호간의 상관을 없앤다. 치환된 신호의 전력 밀도 스펙트럼은 평평하다고 가정한다. 다음에, 특정 모양을 갖는 잡음 신호를 치환된 커버 신호에 삽입한다. 이러한 신호를 만들기 위해 백색 잡음 신호에 특정 모양을 갖게 하는 필터 처리를 한 뒤 나오는 신호를 워터마크로 사용한다. 즉, 백색 잡음 신호 $\mathbf{z}$의 전력 P_z은 평평한 모양을 갖지만 $H(\Omega)$를 선택된 필터의 주파수 응답이라고 할 때 필터를 통과한 신호 $\mathbf{w}$의 전력 밀도 스펙트럼은 $\Phi_{ww}(\Omega)=P_z|H(\Omega)|^2$이 된다.

생성된 워터마크 신호 $\mathbf{w}$와 치환된 커버 신호 $\mathbf{x}'$는 서로 독립이라고 할 수 있으므로 워터마크가 삽입된 치환된 신호의 전력 밀도 스펙트럼은 $\Phi_{yy}(\Omega)=P_{x'}+P_z|H(\Omega)|^2$으로 볼 수 있으며 워터마크의 스펙트럼과 비슷한 모양을 갖게 된다.

검출 과정은 전송된 신호를 삽입 과정과 같은 방법으로 치환시킨 뒤에 치환된 신호 $\mathbf{y}'$의 전력 밀도 스펙트럼 $\Phi_{y'y'}(\Omega)$을 구하고 워터마크 전력밀도 스펙트럼과의 유사성을 측정한다. 즉, 치환된 신호의 전력 밀도 스펙트럼의 모양이 워터마크의 모양과 매우 유사할 경우에 워터마크가 삽입되어 있다고 판단하며, 치환된 신호가 평평한 모양이면 워터마크가 없다고 판단한다.

이 방식에서는 워터마크 신호의 전력 밀도 스펙트럼 모양이 공개키가 된다. 저자들은 스펙트럼 모양만으로는 워터마크 신호의 위상 성분을 알 수 없어 워터마크의 추정이 가능하지 않다고 주장하였다.

6. 변환키 방식

우리는 선형 변환을 이용한 비대칭 워터마킹 방식을 제안하였다[3]. 즉, 원시키 $\mathbf{u}$를 먼저 생성한 뒤 선형 랜덤 변환 행렬 $\mathbf{A}$를 이용하여 비밀키 $\mathbf{s}=\mathbf{Au}$와 공개키 $\mathbf{p}=\mathbf{A}^{-t}\mathbf{u}$를 구하였다. 비밀키는 삽입기에서 커버 데이터에 삽입되어 워터마크 신호 $\mathbf{y}=\mathbf{x}+\mathbf{s}$를 만든다.

검출기에서는 공개키를 이용하여 상관도 검출을 하게 되는데 이 과정에서 비밀키와 공개키의 변환 행렬이 서로 상쇄되고 원시키의 상관도를 구할 수 있게 되어 삽입된 워터마크의 검출이 가능해진다.

$$\begin{aligned} C &= \mathbf{p}^{t}\,\mathbf{y}=\mathbf{u}^{t}\,\mathbf{A}^{-1}\mathbf{x}+\mathbf{u}^{t}\,\mathbf{A}^{-1}\mathbf{A}\,\mathbf{u} \\ &= \mathbf{u}^{t}\,\mathbf{A}^{-1}\mathbf{x}+\mathbf{u}^{t}\,\mathbf{u} \end{aligned} \tag{10}$$

제안된 방식에서 공개되는 것은 공개키 $\mathbf{p}$이며 선형 변환 $\mathbf{A}$나 원시키 $\mathbf{u}$는 공개되지 않는다. 이때 공개키를 이용해서 삽입되어 있는 비밀키를 추측하는 것은 배낭 문제(knapsack problem)와 같은 형태로써 매우 어려운 문제가 되어 이러한 공격에 대해 안전함이 보여졌다[3].

7. Picard 방식

Picard와 Robert는 신경망 함수를 이용한 비대칭 워터마킹 방식을 제안하였다[9,10]. 이 방식은 변환키 방식과 매우 유사한데, 먼저 단일층 선형 신경망의 경우를 생각해 보면 이는 선형 투사와 같다. 즉, 크기 N의 입력 공간이 선형 투사 함수 $\mathbf{G}$에 의해 크기 M의 출력 공간이 되는 경우를 생각해 보자. 이때, $\mathbf{G}$의 $N\cdot M$ 계수들 u_{ij}를 랜덤하게 발생시킨 뒤 크기 N의 비밀키 $\mathbf{s}$를 투사하면 크기 M의 공개키 $\mathbf{p}$를 얻을 수 있다.

$$p_j=\sum_{i=1}^{N}s_i\cdot u_{ij},\quad j=1,\ldots,M \tag{11}$$

삽입 과정은 커버 데이터에 비밀키를 삽입하고 ($\mathbf{y}=\mathbf{x}+\mathbf{s}$) 검출 과정에서는 전송된 신호를 같은 방식으로 투사한 뒤 ($y_j'=\sum_{i}^{N}y_i\cdot u_{ij}$) 공개키와의

상관도를 구한다.

$$C = \sum_{j=1}^{M} y_j' \cdot p_j = \sum_{j=1}^{M} p_j \cdot \left(\sum_{i=1}^{N} x_i \cdot u_{ij} \right) + \sum_{j=1}^{M} p_j^2 \quad (12)$$

즉, 상관도 값에서 공개키의 상관도 값을 구할 수 있으며 이를 통해 워터마크를 검출하게 된다. 이 방식에서는 투사 함수 **G**와 공개키 **p**가 검출기에 공개된다. 식 (11)에서 투사 함수와 공개키가 주어진 경우에도 비밀키를 추측할 수 없게 하기 위한 조건은 $M<N$이다. 저자들은 출력 공간의 차원이 입력 공간보다 작은 경우 하나의 주어진 공개키에 대해 $(N-M)$차원 만큼의 가능한 비밀키가 존재하므로 비밀키의 추측은 가능하지 않다고 주장하였다.

신경망의 내부층은 이와 같은 선형 함수 이외에도 비선형 함수를 이용할 수 있으며 다단계의 층을 거칠 수도 있다.

Ⅳ. 비대칭 워터마킹 방식의 비교

3절에서 소개된 비대칭 방식들은 각기 다른 발상에서 출발하여 차이점도 존재하지만 매우 유사한 특징들도 많이 가지고 있다. 본 절에서는 제안된 방식들의 문제점을 분석해 보고 각 방식들의 유사성과 차이점을 비교해 본다. Hartung의 방식은 비대칭 방식으로 사용하기에 안전성이 많이 떨어져서 이를 제외한 6가지 방식들에 대해 비교하였다.

먼저, Legendre 방식에서의 문제점은 생성 가능한 워터마크 키의 양(키 용량)이 작아서 공격자가 삽입된 수열을 쉽게 찾아낼 수 있다는 것이다. 길이 N인 Legendre 수열은 $N-2$개만이 존재하므로 가능한 모든 수열을 검출기 입력으로 주고 검출 결과를 확인함으로써 삽입된 수열을 찾아낼 수 있다.

고유 벡터를 이용한 워터마킹 방식은 Legendre 수열을 이용한 방식의 연장으로 볼 수 있지만, 이러한 문제에 대해서는 좀더 안전하다고 할 수 있다. 즉, 기하학적 중복도(geometric multiplicity)가 매우 큰 고유값을 갖는 고유 벡터를 워터마크로 사용하면 고유값에 해당하는 고유벡터가 유일하게 정의되지 않고 중복도에 따라 기하급수적으로 증가하게 되므로, 공격자가 시도해 보아야 할 워터마크의 수를 증가시킬 수 있고 이러한 공격에 대해서 안전성을 높일 수 있다.

다음으로 검출 과정을 분석해 보면, Smith, Schyndel, Egger 방식들은 모두 전송된 신호와 그 신호를 변환시킨 신호와의 상관도를 이용하는 형태이다. 검출단에서 필요한 정보의 양을 살펴보면 삽입된 워터마크의 길이나 변환 행렬 등 매우 적은 비용(overhead)만이 필요하므로 검출기를 매우 간단한 형태로 구현할 수 있을 것이다. 그러나 이들 방식은 검출기에서 워터마크의 존재 여부만을 알 수 있으며 어떤 워터마크가 삽입되어 있는지는 확인할 수 없다. 즉, 이들 방식에 의한 워터마킹의 용량(capacity)은 1비트로 볼 수 있으며, 이러한 작은 용량으로 가능한 매우 제한적인 활용 경우에 국한해서 사용할 수 있을 것이다.

또, Smith, Schyndel, Egger, Furon의 방식은 검출 형태 면에서 유사한 방식들로 볼 수 있다. 즉, 검출 형태가 대칭 워터마킹 방식일때는 1차 형태인 $\mathbf{y}^t\mathbf{w}$이지만 이들 방식에서는 2차 형태인 $\mathbf{y}^t\mathbf{A}\mathbf{y}$ 형태를 갖게 된다. Schyndel의 경우는 행렬 **A**가 이산 푸리에 변환 행렬이며 Egger의 경우에는 검출단에 주어지는 변환 행렬이다. Smith와 Furon의 경우에도 이러한 2차 형태로 검출 값을 표현할 수 있다[11].

그러나, 이러한 2차 형태의 검출 형태는 신호 간섭이 크다는 단점도 가지고 있다. 검출 상관도값을 풀어보면 다음과 같다.

$$C = Q(\mathbf{x}) + Q(\mathbf{x},\mathbf{w}) + Q(\mathbf{w},\mathbf{x}) + Q(\mathbf{w}) \quad (13)$$

이때, $Q(\mathbf{x},\mathbf{y}) = \mathbf{x}^t\mathbf{A}\mathbf{y}/N$이다. 식에서 뒤의 두 항은 대칭 방식의 상관도 값과 같은 항이지만 앞의 두 항은 2차 형태의 검출 값에서만 나타난다. 워터마킹에서 커버 데이터가 워터마크보다 매우 큰 파워를 가지고 있기 때문에 앞의 두 항, 특히 첫 항의 간섭이 검출에 큰 영향을 주게 되며, 결과적으로 검출 성능면에서 대칭 방식보다 매우 낮은 성능을 보이게 된다. 검출 성능을 평가하기 위한 척도로 워터마크가 삽입되었을 때 상관도 값의 평균값과 상관도 값의 표준편차의 비인 $D = \mathrm{E}\{C|\mathrm{H}_1\}/\mathrm{STD}\{C\}$가 많이 이용되어왔다. 이 비가 클수록 검출 에러 확률이 낮아지게 되며 바꿔 말해 검출의 신뢰성이 높다고 할 수 있다. 커버신호와 워터마크의 전력비가 20dB일 때 검출 성능을 대략적으로 평가해 보면 표 1과

〔표 1〕 비대칭 방식 비교

방식	비밀키	키 용량	공개키	검출기 비용	용량	검출 형태	신호 간섭	검출 성능	행렬 공개	공개키 공격
Schyndel	Legendre 수열	소	수열 길이	소	1	y^tAy	고	$D_{sym}/10$	공개	가능
Egger	고유 벡터	중	변환 행렬	중	1	y^tAy	고	$D_{sym}/10$	공개	가능
Smith	랜덤 수열	대	수열 길이	소	1	y^tAy	고	$D_{sym}/10$	공개	가능
Furon	잡음 수열	대	PDS 모양	대	$\log_2 N$	y^tAy	고	$D_{sym}/10$	공개	가능
Picard	랜덤 수열	대	투사 함수, 공개 수열	대	$\log_2 N$	y^tAw	저	$\leq D_{sym}/\sqrt{2}$	공개	가능
변환키	비밀 수열	대	공개 수열	대	$\log_2 N$	y^tAw	저	$D_{sym}/2$	비공개	가능

같다. 비대칭 방식은 모두 대칭 방식의 검출 성능 D_{sym}보다 낮은 결과를 보이며 특히 2차 형태의 경우가 다른 경우에 비해 커버 신호의 간섭으로 검출 성능이 더 떨어지게 된다.

검출 형태에서 나타나는 변환 행렬의 공개 여부를 살펴보면 변환키 방식을 제외하고 다른 모든 방식은 변환 행렬이 공개된다. [11]에서 분석된 것과 같이 변환 행렬이 공개된 경우 변환행렬의 고유 벡터와 고유값을 이용해 검출 상관도값을 떨어뜨리는 잡음을 추가하는 공격이 가능하므로, 변환 행렬의 공개는 안전성 측면에서 불리하다고 할 수 있다.

선형 신경망 방식은 선형 변환으로 해석될 수 있으므로 변환키 방식과 매우 유사하다고 할 수 있다. 차이점은 신경망 방식은 커버 신호 자체를 변환시켜 검출을 행하며 신경망 층에 비선형 함수를 이용할 수 있다는 것이다. 비선형 함수를 이용하는 경우에는 입력과 출력의 관계가 비선형이 되기 때문에 안전성 측면에서 개선될 수 있으나 검출 성능은 떨어지게 된다. 활용 경우를 고려하여 안전성과 검출 성능 사이의 타협이 필요하다.

마지막으로, 모든 비대칭 방식들은 공개된 키를 이용한 공격이 가능하다는 공통된 문제점을 가지고 있다. 예를 들어, Schyndel의 경우에는 공개된 수열의 길이에 맞는 Legendre 수열을 하나 선택해서 워터마크가 삽입된 신호에 빼주게 되면 삽입되어 있는 워터마크의 상관도를 떨어뜨려 검출을 불가능하게 할 수 있다. Egger, Smith의 경우에서도 같은 형태의 공격이 가능하다. Furon의 경우에는 워터마크가 삽입되어 있는 신호에 전력 밀도 스펙트럼의 모양을 평평하게 만드는 필터 처리를 이용한 공격이 가능하다. 예를 들어, 워터마크가 삽입된 신호를 치환하고 푸리에 스펙트럼을 구한 뒤, 그 절대값들을 수정한 뒤 역푸리에 변환을 하면 삽입된 워터마크의 모양을 변경시킬 수 있다. 변환키와 Picard의 경우에도 공개키를 이용한 공격이 가능하다. 예를 들어, 변환키의 경우 비밀키가 삽입되어 있는 신호에 공개된 키를 빼주면 ($\mathbf{y}' = \mathbf{x} + \mathbf{s} - \mathbf{p}$), 공개키를 이용한 상관도 계산에서 추가된 음의 공개키가 상관도를 떨어뜨리게 되어 워터마크가 검출되지 않게 할 수 있다. 이러한 공격은 비밀키에 의한 검출[3]이나 다중 공개키 생성[9]으로 보완될 수 있지만, 공개키를 통한 공격을 완전히 막을 수는 없다.

공개키를 이용한 공격들이 성공하는 경우 공격된 신호와 공격하기 전의 신호와의 왜곡 정도를 평가해 비대칭 방식들의 성능을 평가하기도 하지만 대부분의 방식이 변형 정도가 2-3dB 정도로 높지 않아 이러한 공격이 충분히 가능하다고 할 수 있다.

최근에 비대칭 방식들에 대한 논의가 활발해 지면서 비대칭 방식을 약한 공개키 방식과 강한 공개키 방식으로 나누어 설명하기도 한다. 약한 공개키 방식은 삽입기와 검출기에서 서로 다른 키를 이용하는 방식을 말하며, 강한 공개키 방식은 다른 키를 사용한다는 조건 외에 공개된 키를 이용한 어떤 공격이나 위조가 불가능한 안전한 방식을 말한다. 지금까지 검토된 방식들은 이러한 용어로 보면 모두 약한 공개키 방식에 해당하며 강한 공개키 방식은 아니다. 실제로 강한 공개키 방식이 존재할 수 있는 지에도 많은 사람들이 의구심을 가지고 있다. 이를 해결하기 위해서는 암호화에서의 경우처럼 앞으로도 많은 이론적인 분석이 필요할 것이며 많은 검증 과

정이 요구될 것이다.

비대칭 방식들의 비교 내용을 요약해 보면 표 1과 같다.

V. 결 론

실제적인 워터마킹 사용 환경에서 일반 사용자가 자유롭게 검출기를 이용하여 워터마크를 검출할 수 있을 때 워터마크의 안전성을 보장하는 것은 매우 어려운 일이다. 특히 지금까지 제안되어온 대부분의 워터마킹 알고리듬은 삽입기와 검출기 측에서 같은 워터마크 키를 사용함으로써 검출기 측에서 유출되는 정보를 이용하여 모든 워터마크를 제거할 수 있는 위험성이 존재하였다. 이러한 문제점을 해결하기 위해 여러 가지 방식의 비대칭 워터마킹 기법들이 제안되어 왔으나 실제 사용에 있어서는 아직 해결되어야 할 문제점들을 가지고 있다. 그러나, 암호화의 경우에서와 같이 많은 연구와 충분한 검증을 통한 분석이 이루어진다면 보다 안전한 비대칭 방식이 가능할 것이며 이는 워터마킹 활용에 매우 중요한 과제라고 할 수 있다.

참 고 문 헌

[1] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking techniques," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064-1087, June 1998.

[2] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

[3] 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.

[4] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," in *Proc. of the IEEE Intl. Conf. on Image Processing*, vol. 1, pp. 528-531, Sant Barbara, CA, USA, Oct. 1997.

[5] 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.

[6] J. J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in *Proc. of European Signal Processing Conf.*, Tampere, Finland, April 2000.

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

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

[9] J. Picard and A. Robert, "On the public key watermarking issue," in *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, vol. 4314, pp. 290-299, San Jose, USA, Jan. 2001.

[10] 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.

[11] T. Furon and P. Duhamel, "An unified approach of asymmetric watermarking schemes," in *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, vol. 4314, pp. 269-279, San Jose, USA, Jan. 2001.

〈者 著 紹 介〉

최 혁 (Hyuk Choi)
1994년 : 서울대학교 전자공학과 (학사)
1996년 : 서울대학교 전자공학과 (석사)
2002년 : 서울대학교 전기컴퓨터 공학부(박사)
관심분야 : Watermarking, DRM, image signal processing

김 태 정 (Taejeong Kim)
1976년 : 서울대학교 전자공학과 (학사)
1978년 : KAIST 전자공학과(석사)
1986년 : University of Michigan 전자공학과(박사)
1978년~1981년 ETRI
1986년~1988년 AT&T Bell Lab.
1988년~현재 : 서울대학교 전기컴퓨터공학부
관심분야 : Statistical and image signal processing, source coding