변환키 비대칭 워터마킹 시스템의 강인성 분석 및 개선☆

Robustness Analysis and Improvement on Transformed-key Asymmetric Watermarking System

김 남 진* 최 두 섭** 송 원 석*** 최 혁**** 김 태 정*****
Namjin Kim Dooseop Choi Wonseok Song Hyuk Choi Taejeong Kim

요 약

본 논문은 변환키 비대칭 워터마킹 시스템의 강인성을 분석하고 이에 대한 개선을 제안한다. 먼저 비대칭 워터마킹 시스템의 공개 검출을 불가능하게 하는 빼기공격의 상황을 가정하고 변환키 비대칭 워터마킹 시스템의 검출성능에 대한 척도를 제안한다. 다음으로 빼기공격에 강인하기 위하여 변환키 비대칭 워터마킹 시스템이 갖추어야 할 최적의 조건을 분석한다. 또한 변환키 비대칭 워터마킹 시스템 전체의 검출 성능을 개선하기 위하여 새로운 비공개 검출 방법을 제안한다. 제안하는 개선된 방식은 빼기공격 뿐만이 아니라 Wu의 공격에도 강인함을 보인다.

ABSTRACT

In this paper, we analyze the robustness of transformed-key asymmetric watermarking system and show its improvement by proposing a new detection method. Based on the assumption that the transformed-key asymmetric watermarking system is under the threat of subtraction attack, we first propose the criterion for the detection performance of the watermarking system and analyze the optimum condition on the system. Next, a new detection method is proposed to improve the detection performance of the system based on the criterion. The proposed improvement makes the system robust to not only subtraction attack but also Wu's attack.

☞ KeyWords : Asymmetric Watermarking(비대칭 워터마킹), TKW, Robustness analysis(강인성 분석), Detection Key(검출키)

1. 서 론

디지털 워터마킹은 디지털 멀티미디어에 사람이 인지하지 못하는 정보를 삽입하는 기술로써 저작권 보호 등에 사용된다 [1]. 많은 디지털 워터마킹 기술들은 워터마크의 삽입과 추출을 위하여 같은 키를 사용한다는 측면에 있어서 대칭적이다. 하지만 이러한 방식은 일반 사용자가 워터마크의 추출을 위한 키에 접근이 가능한 경우 삽입된 워터마크를 너무도 쉽게 제거할 수 있다는 문제점을 가지고 있다 [2][3].

민감도 공격은 그러한 예를 잘 보여주고 있다. 멀티미디어 콘텐츠의 불법 복제를 제한하는 복사방지 기술의 경우, 일반적으로 워터마크 검출기가 블랙박스 형태로 일반인들에게 공개된다. 이 때 공격자들은 워터마크가 삽입된 멀티미디어 콘텐츠에 임의의 신호를 삽입하고 워터마크 추출기의 반응을 살핌으로써 실제 삽입된 워터마크를 예측하게 된다. 이렇게 예측된 워터마크를 멀티미디어 콘텐츠로부터 제거함으로써 공격자들은 워터마크가 검출되지 않는 새로운 멀티미디어 콘텐츠를

* 정 회 원 : KT 중앙연구소 연구원
nkim@kt.com
** 정 회 원 : 서울대학교 대학원 전기컴퓨터공학부
박사과정 dschoi@infolab.snu.ac.kr(교신저자)
*** 정 회 원 : 서울대학교 대학원 전기컴퓨터공학부
박사과정 metro@infolab.snu.ac.kr
**** 정 회 원 : 서울시립대학교 컴퓨터과학부 교수
chyuk@venus.uos.ac.kr
***** 정 회 원 : 서울대학교 전기컴퓨터공학부 교수
tjkim@infolab.snu.ac.kr
[2010/08/30 투고 - 2010/09/06 심사 - 2010/10/06 심사완료]
☆ 본 연구는 문화체육관광부 및 한국문화콘텐츠진흥원의 2009년도 문화콘텐츠산업기술지원사업의 연구결과로 수행되었음.

획득하게 된다.

이처럼 대칭형 워터마킹 방식의 보안문제가 두드러지면서 이에 대한 해결책으로 비대칭 워터마킹 방식이 제안되었다. 비대칭 워터마킹 방식은 워터마크의 삽입을 위한 키(개인키)와 워터마크의 추출을 위한 키(공개키)를 서로 다르게 설계함으로써 멀티미디어에 삽입된 워터마크를 제거할 수 없도록 한다. 따라서 비대칭 워터마킹 방식은 대칭형 워터마킹 방식에 비해 보안성이 더욱 강화된 워터마킹 방식이라 할 수 있다.

많은 연구자들이 비대칭 워터마킹 방식들을 제안해 왔다 [4-7]. 그중에서도 변환키 비대칭 워터마킹 시스템 (transformed-key asymmetric watermarking system, TKW) [7] 은 매우 안전하면서도 강인한 비대칭 워터마킹 방식으로 알려져 있다. 이 시스템은 개인키와 공개키를 생성하기 위해 원시키 $\boldsymbol{u}$에 각각 선형 변환 $\boldsymbol{A}$와 $\boldsymbol{A}^{-t}$를 적용한다. 여기서 $-t$는 역전치를 의미한다. 선형 변환으로부터 생성된 개인키 $\boldsymbol{Au}$는 워터마크의 삽입을 위하여 사용되고 공개키 $\boldsymbol{A}^{-t}\boldsymbol{u}$는 워터마크의 검출을 위하여 사용된다. 이때 워터마킹 알고리즘과 공개키를 일반인들에게 공개한다.

변환키 워터마킹 방식의 가장 큰 장점은 빼기공격에 강인하다는 것이다. 빼기공격은 임의의 상수가 곱해진 공개키 $\beta\boldsymbol{A}^{-t}\boldsymbol{u}$를 워터마크가 삽입된 신호로부터 뺌으로써 공개 검출을 불가능하게 하는 공격이다. 변환키 워터마킹 방식은 개인키와 공개키 간의 상관도 계수 ρ, $(0 \le \rho \le 1)$ 를 적절히 조절함으로써 빼기공격이 일어난 후에도 권한이 있는 사용자에 의해 개인키를 이용한 워터마크 검출을 가능 하게 한다 [7]. 이 때 ρ가 클수록 빼기공격이 발생하지 않은 경우의 공개 검출 성능은 높아지며 반대로 빼기공격이 발생한 경우의 비공개 검출 성능은 줄어들게 된다. 따라서 적절한 ρ를 선택하여 시스템 전체의 검출 성능을 최대화 할 필요가 있다. 참고로 [7]에서 제안하는 상관도 계수 값은 $\rho = 0.5$이며 우리는 이 값이 변환키 시스템의 전체 검출 성능을 최대화 하지 않음을 보일 것이다.

본 논문에서는 먼저 변환키 비대칭 워터마킹 시스템의 검출 성능에 대한 척도를 제시한다. 제안하는 척도는 빼기공격이 발생하지 않은 경우의 공개 검출 성능과 빼기공격이 발생한 경우의 비공개 검출 성능을 모두 반영하도록 정의된다. 따라서 변환키 비대칭 워터마킹 시스템 전체의 검출 성능을 나타낸다. 다음으로, 제안하는 척도로부터 변환키 시스템의 검출 성능을 최대로 하는 ρ를 분석한다. 또한 새로운 비공개 검출 방식을 제안함으로써 변환키 비대칭 워터마킹 시스템의 전체 검출 성능을 한 단계 더 높이고자 한다.

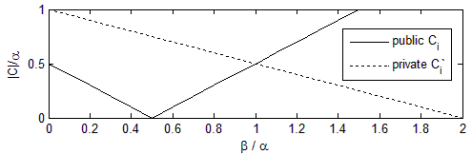
변환키 비대칭 워터마킹 시스템의 신호처리 공격, 예를 들어 JPEG 압축 등, 에 대한 강인성은 삽입된 워터마크의 파워 및 워터마크가 삽입된 도메인 등 에 의해 결정되며 그 결과는 [7]로부터 확인할 수 있다. 따라서 본 논문은 오직 ρ에 따른 변환키 비대칭 워터마킹 시스템의 빼기공격에 대한 강인성 분석 및 그 개선에 초점을 맞춘다.

2. 변환키 비대칭 워터마킹 시스템

일반적인 워터마킹 시스템에서 워터마크 셋 $\{w_i, i = 1,..,k\}$은 원본신호 x에 삽입되는 정규화 된 직교 시퀀스 들이다. 워터마크 삽입기는 다음의 수식을 통하여 워터마크를 삽입한다: $y = x + \alpha w_i$. 여기서 α는 워터마크의 비인지성을 결정하는 상수이다. 워터마크 추출기는 수신된 신호 r과 워터마크 w_j 사이의 상관도 값을 다음과 같이 구한다. $C_j = w_j^t r = w_j^t \hat{x} + \alpha w_j^t w_i$. 이 때 $\hat{x} = x + n$이고 n은 공격 노이즈를 나타낸다. 만약 워터마킹 시스템이 $w_j^t \hat{x} \approx 0$와 $w_j^t w_i = \delta_{ij}$를 만족하도록 설계된다면, 미리 정해놓은 기준치 T와 $|C_j|$을 비교하여 특정 워터마크의 존재 유무를 파악할 수 있게 된다. 다음은 변환키 비대칭 워터마킹 시스템을 설명한다.

• *비대칭 워터마크의 생성과 삽입* : 원시키

$\{\boldsymbol{u_i}, i=1,..,k\}$와 $\boldsymbol{A}$를 각각 길이가 n인 정규화된 직교 시퀀스와 크기가 $n\times n$인, 역함수가



(그림 1) 빼기공격에 대한 공개 및 비공개 검출

존재하는 행렬이라 정의하자. 변환키 시스템의 정규화 된 개인키 $\boldsymbol{w_s}$와 공개키 $\boldsymbol{w_p}$는 다음과 같이 정의된다.

$$\boldsymbol{w_{s,i}} = \frac{\boldsymbol{Au_i}}{\|\boldsymbol{Au_i}\|} = \gamma_s \boldsymbol{Au_i}$$

$$\boldsymbol{w_{p,i}} = \frac{\boldsymbol{A^{-t}u_i}}{\|\boldsymbol{A^{-t}u_i}\|} = \gamma_p \boldsymbol{A^{-t}u_i} \quad (1)$$

워터마크의 삽입은 $\boldsymbol{y} = \boldsymbol{x} + \alpha \boldsymbol{w_{s,i}} = \boldsymbol{x} + \alpha\gamma_s \boldsymbol{Au_i}$에 의해 이루어지며 오직 $\boldsymbol{A^{-t}u_i}$와 워터마킹 알고리즘만이 공개된다.

• *비대칭 워터마크의 추출* : 워터마크의 추출 과정은 추출기 입력 $\boldsymbol{r}$과 공개키 사이의 상관도 측정을 통하여 이루어진다.

$$C_j = \boldsymbol{w_{p,j}^t r} = \gamma_p \boldsymbol{u_j^t A^{-1}\hat{x}} + \gamma_p \boldsymbol{u_j^t A^{-1}} \alpha\gamma_s \boldsymbol{Au_i} \quad (2)$$
$$= \gamma_p \boldsymbol{u_j^t A^{-1}\hat{x}} + \alpha\gamma_p\gamma_s \boldsymbol{u_j^t u_i}.$$

만약 변환키 비대칭 워터마킹 시스템이 $\boldsymbol{u_j^t} A^{-1}\hat{x} \approx 0, j=1,...,k$을 만족하도록 설계된다면 $\boldsymbol{u_i}$의 직교성으로부터 $C_j \ll C_i, j=1,...,k, j\neq i$이 성립되며 최종적으로 C_j를 기준치 T와 비교함으로써 워터마크의 유무를 판단한다. 끝으로 권한이 부여된 그룹은 개인키 $\boldsymbol{w_{s,i}}$를 이용하여 삽입된 워터마크를 추출할 수 있음을 언급한다.

워터마크의 추출을 위한 공개키는 워터마킹 알고리즘과 함께 공개되기 때문에 공격자는 적당히 상수가 곱해진 공개키 $\beta\boldsymbol{w_{p,i}}$를 워터마크가

삽입된 신호로부터 뺌으로써 공개 검출을 불가능하게 할 수 있다: $\hat{\boldsymbol{y}} = \boldsymbol{x} + \alpha\boldsymbol{w_{s,i}} - \beta\boldsymbol{w_{p,i}}$. 여기서 β는 임의의 상수이다. 따라서 공개키를 이용한 검출 결과는 다음과 같다: $C_j = \boldsymbol{w_{p,j}^t}\hat{\boldsymbol{y}} = \boldsymbol{w_{p,j}^t}(\hat{\boldsymbol{x}} + \alpha\boldsymbol{w_{s,i}} - \beta\boldsymbol{w_{p,i}})$. 잘 설계된 변환 행렬 $\boldsymbol{A}$는 서로 다른 개인키 사이의 상관도 값과 서로 다른 공개키 사이의 상관도 값을 각각 $\epsilon_s \approx 0$와 $\epsilon_p \approx 0$로 만든다고 가정한다. 또한 $\boldsymbol{w_{p,j}^t w_{s,i}} = \rho\delta_{i,j}$임을 가정하자. 여기서 ρ는 $\boldsymbol{w_{p,i}}$와 $\boldsymbol{w_{s,i}}$ 사이의 상관도 계수 이다. 마지막으로 원본 신호와 워터마크 사이의 상관도 값이 매우 작다고 가정한다면, 워터마크 추출기의 결과는 다음과 같다.

$$C_j = \begin{cases} \boldsymbol{w_{p,j}^t x} + \alpha\rho - \beta \approx \alpha\rho - \beta, & \text{if } j = i \\ \boldsymbol{w_{p,j}^t x} - \beta\epsilon_p \approx -\beta\epsilon_p, & \text{if } j \neq i \end{cases} \quad (3)$$

만약 β의 값이 $\alpha\rho - \beta < T$을 만족하도록 정해진다면 빼기공격에 의해 공개 검출이 불가능해진다. 변환키 비대칭 워터마킹 시스템의 장점은 빼기공격이 일어난 후에도 개인키를 이용하여 삽입된 워터마크를 추출할 수 있다는 것이다. 개인키를 이용한 워터마크의 검출 결과는 다음과 같다.

$$C_j^{'} = \begin{cases} \boldsymbol{w_{s,j}^t x} + \alpha - \beta\rho \approx \alpha - \beta\rho, & \text{if } j = i \\ \boldsymbol{w_{s,j}^t x} - \alpha\epsilon_s \approx -\alpha\epsilon_s, & \text{if } j \neq i \end{cases}. \quad (4)$$

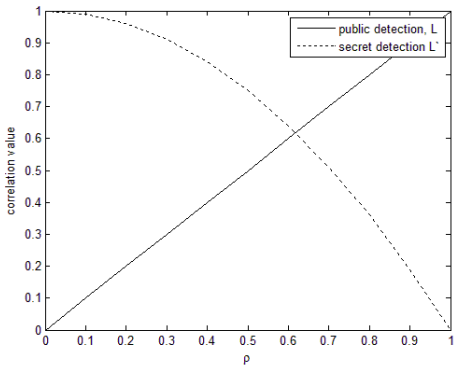
빼기공격에 강인하기 위한 변환키 비대칭 워터마킹 시스템의 조건으로 [7]에서는 $\rho = 0.5$를 제안하고 있으며 그림.1은 이때의 C_j와 $C_j^{'}$의 값을 β의 값에 따라 보여주고 있다. 그림에서 볼 수 있듯이 개인키를 이용한 검출과 공개키를 이용한 검출을 동시에 불가능하게 하는 β는 존재하지 않음을 알 수 있다. 따라서 변환키 비대칭 워터마킹 시스템은 빼기공격에 강인함을 알 수 있다.

3. 변환키 시스템의 강인성 분석 및 개선

3.1 변환키 비대칭 워터마킹 시스템의 강인성 척도

위에서 언급하였듯이 변환키 시스템의 가장 큰 장점은 빼기공격 후에도 개인키를 이용한 워터마

크 검출이 가능하다는 것에 있다. 따라서 변환키 시스템의 검출 성능에 대한 척도는 공개키와 개인키를 이용한 검출 결과를 모두 반영해야 한다. 이를 위해 우리는 검출 성능 지표 D를 다음과 같이 제안한다.



(그림 2) ρ값에 따른 검출 값의 변화

$$D = \min(\overline{D}(\boldsymbol{w}_p^t\boldsymbol{y}),\ \overline{D}(\boldsymbol{w}_s^t\hat{\boldsymbol{y}})) \quad (5)$$
$$= \min(\overline{D}(L),\ \overline{D}(L'))$$

여기서 $\overline{D}$는 검출 성능을 나타내는 어떠한 지표도 될 수 있으며, $\boldsymbol{y} = \boldsymbol{x} + \alpha\boldsymbol{w}_s$, $\hat{\boldsymbol{y}} = \boldsymbol{x} + \alpha\boldsymbol{w}_s - \beta\boldsymbol{w}_p$이다. 만약 $\boldsymbol{w}_p^t\boldsymbol{y}$와 $\boldsymbol{w}_s^t\hat{\boldsymbol{y}}$이 같은 분산을 갖는 확률 밀도의 확률 변수일 경우 검출 성능 지표 D는 다음과 같이 표현될 수 있다.

$$D = \min(E(L), E(L')) \quad (6)$$

여기서 E는 평균을 의미한다. 결국 검출 성능 지표 D는 빼기공격이 발생한 후 개인키를 이용한 검출 L'의 예측치와 빼기공격이 발생하지 않은 상황에서 공개키를 이용한 검출 L의 예측치 중에서 더욱 작은 쪽을 선택함을 의미한다. 따라서 검출 성능 지표 D를 최대화함으로써 변환키 비대칭 워터마킹 시스템 전체의 강인성을 최대화할 수 있다.

3.2 변환키 시스템의 강인성 분석

식 (3)에서 $C_j = 0$을 만족시키기 위해, 즉 변환키 시스템의 공개 검출을 불가능하게 만들기 위해 공격자는 $\beta = \alpha\rho$을 선택할 것이다. 이 경우 $L = \alpha\rho$, $L' = \alpha(1-\rho^2)$이 된다. 그림 2는 ρ값에 따른 L과 L'의 값의 변화를 보여주고 있다. 그림에서 볼 수 있듯이 검출 성능 지표 D는 L과 L'이 만나는 지점에서 최대가 된다. 즉 $\alpha\rho = \alpha(1-\rho^2)$을 만족하는 $\rho = \rho_{opt}$가 변환키 시스템의 강인성을 최대로 한다. 가정 $0 \le \rho \le 1$을 바탕으로 $\rho_{opt} = (-1+\sqrt{5})/2 \approx 0.62$이다.

3.3 새로운 검출 방식의 제안

위 절 에서는 변환키 비대칭 워터마킹 시스템의 강인성을 최대로 하는 최적의 ρ에 대하여 논의하였다. 이 절 에서는 비공개 검출 시 기존의 개인키가 아닌 새로운 비공개 검출키를 사용함으로써 변환키 시스템의 강인성을 더욱 높일 수 있음을 보여준다.

명제1 : 공개키 $\boldsymbol{w}_p$, 개인키 $\boldsymbol{w}_s$, 새로운 검출키 $\boldsymbol{w}_n$를 각각 길이가 N인 단위 벡터라 정의하고 각 검출키와 원본신호 $\boldsymbol{x}$가 서로 직교임을 가정하자. 그러면 $\max(D = \min(\boldsymbol{w}_p^t\boldsymbol{y},\ \boldsymbol{w}_n^t\hat{\boldsymbol{y}})) = \alpha\sqrt{2}/2$이고 $\boldsymbol{w}_n = \sqrt{2}\boldsymbol{w}_s - \boldsymbol{w}_p$,$\rho = \sqrt{2}/2$이다.

증명 : $\boldsymbol{w}_s$와 $\boldsymbol{w}_p$를 기저로 갖는 벡터 공간 W를 정의하자. 또한 벡터 공간 V를 W의 직교 차 공간으로 정의하자. 그렇다면 $\boldsymbol{w}_n = \lambda\boldsymbol{w}_w + \gamma\boldsymbol{w}_v$로 정의할 수 있게 된다. 여기서 $\boldsymbol{w}_w$와 $\boldsymbol{w}_v$는 $\boldsymbol{w}_n$을 각각 벡터 공간 W와 V으로 사영 시킨 결과이다. 즉 $\boldsymbol{w}_w \in W$, $\boldsymbol{w}_v \in V$ 이다. 마지막으로 $\|\boldsymbol{w}_w\| = \|\boldsymbol{w}_v\| = 1$이고, λ와 γ는 임의의 상수로서 $\lambda^2 + \gamma^2 = 1$을 만족한다.

$\boldsymbol{x}_p^t\hat{\boldsymbol{y}} = 0$을 만족하는 β는 $\alpha\rho$이므로 $\boldsymbol{w}_p^t\boldsymbol{y}$와 $\boldsymbol{w}_n^t\hat{\boldsymbol{y}}$은 각각 다음과 같음을 보일 수 있다.

$\boldsymbol{w}_p^t\boldsymbol{y} = \alpha\rho$

$$\begin{aligned} \boldsymbol{w}_n^t\hat{\boldsymbol{y}} &= \boldsymbol{w}_n^t(\boldsymbol{x}+\alpha\boldsymbol{w}_s-\beta\boldsymbol{w}_p) \\ &= (\lambda\boldsymbol{w}_w^t+\gamma\boldsymbol{w}_v^t)(\alpha\boldsymbol{w}_s-\beta\boldsymbol{w}_p) \\ &= \lambda(\alpha\boldsymbol{w}_w^t\boldsymbol{w}_s-\alpha\rho\boldsymbol{w}_w^t\boldsymbol{w}_p) \\ &= \lambda\alpha(\cos\theta_\mu-\cos\theta_\rho\cos\theta_v) \\ &\le \lambda\alpha(\cos(\theta_v-\theta_\rho)-\cos\theta_\rho\cos\theta_v) \\ &= \lambda\alpha\sin\theta_\rho\sin\theta_v \\ &= \lambda\alpha\sin\theta_v\sqrt{1-\rho^2} \le \alpha\sqrt{1-\rho^2} \end{aligned} \quad (7)$$

여기서 θ_μ는 $\boldsymbol{w}_w$와 $\boldsymbol{w}_s$사이의 각도를, θ_v는 $\boldsymbol{w}_w$와 $\boldsymbol{w}_p$사이의 각도를, θ_ρ는 $\boldsymbol{w}_p$와 $\boldsymbol{w}_s$사이의 각도를 나타낸다. 위의 식으로부터 $\lambda=1, \theta_v=\pi/2$일 때 $\boldsymbol{w}_n^t\hat{\boldsymbol{y}}$은 최대 값 $\alpha\sqrt{1-\rho^2}$을 갖음을 알 수 있다. 따라서 $\rho=\sqrt{2}/2$일 때

$$\begin{aligned} \max(D) &= \max(\min(\boldsymbol{w}_p^t\boldsymbol{y}, \boldsymbol{w}_n^t\hat{\boldsymbol{y}})) \\ &= \max(\min(\alpha\rho, \alpha\sqrt{1-\rho^2})) \\ &= \alpha\sqrt{2}/2 \end{aligned} \quad (8)$$

임을 알 수 있다.

다음으로, 위에서 $\lambda=1$이므로 $\boldsymbol{w}_n \in W$이고 따라서 $\boldsymbol{w}_n=\zeta\boldsymbol{w}_s+\xi\boldsymbol{w}_p$로 표현이 가능하다. 여기서 ζ, ξ는 임의의 상수이다. 두 상수 ζ, ξ을 얻기 위해 $\boldsymbol{w}_n=\zeta\boldsymbol{w}_s+\xi\boldsymbol{w}_p$의 양 변에 각각 $\boldsymbol{w}_s$와 $\boldsymbol{w}_p$를 곱하면 다음의 연립 방정식을 얻게 되며

$$\begin{cases} \dfrac{\sqrt{2}}{2} = \zeta + \dfrac{\sqrt{2}}{2}\xi \\ 0 = \dfrac{\sqrt{2}}{2}\zeta + \xi \end{cases} \quad (9)$$

이 연립방정식의 해는 $\zeta=\sqrt{2}$, $\xi=-1$임을 쉽게 알 수 있다. 따라서 $\boldsymbol{w}_n=\sqrt{2}\boldsymbol{w}_s-\boldsymbol{w}_p$ 이다.

■ 변환키 시스템의 검출 성능 지표 D_{TKW}와 개선된 변환키 시스템의 검출 성능 지표 D_{ITKW}를 비교해 보면 $D_{KW}=\alpha\sqrt{2}/2 > \alpha(-1+\sqrt{5})/2 = D_{TKW}$ 로 새로운 검출키의 제안이 변환키 시스템의 검출성능을 높이고 있음을 알 수 있다.

(표 1) 공격에 따른 검출 성능 비교

		[7]	제안1	제안2
공격 없음	공개	0.500	0.618	0.707
	비공개	1.000	1.000	0.707
빼기 공격	공개	≈0	≈0	≈0
	비공개	0.750	0.618	0.707
Wu의 공격	공개	≈0	≈0	≈0
	비공개	≈0	≈0	0.707
검출 성능 지표		0.500	0.618	0.707

4. 검출 성능의 비교

4.1 Wu의 공격

Wu [8] 는 변환키 비대칭 워터마킹 시스템을 고려하여 공개 검출 뿐만이 아니라 비공개 검출도 불가능하게 하는 새로운 공격을 제안하였다. Wu의 공격은 다음과 같이 이루어 진다: $\bar{\boldsymbol{y}}=\boldsymbol{x}+\alpha\boldsymbol{w}_s-\alpha/\rho\boldsymbol{w}_p+\lambda I$. 여기서 λ는 상수이며 I는 다음과 같이 정의 된다.

$$I=(i(1),i(2),\ldots,i(N)),$$
$$i(k)=\begin{cases} 1 \text{ if } w_p(k)>0 \\ 0 \quad otherwise \end{cases} \quad (10)$$

Wu의 공격 후 공개키를 이용한 검출 결과는 다음과 같다.

$$\begin{aligned} |C_{wu}^p| &= \boldsymbol{w}_p^t\bar{\boldsymbol{y}} = \boldsymbol{w}_p^t\boldsymbol{x}+\alpha\rho-\alpha/\rho+\lambda b \\ &\approx \alpha\rho-\alpha/\rho+\lambda\boldsymbol{w}_s^t I \end{aligned} \quad (11)$$

이 때 $|C_{wu}^p| < T$을 만족하는 λ를 찾으면 공개 검출을 불가능 하게 할 수 있다. 다음으로, Wu의 공격 후 개인키를 이용한 검출은 다음과 같다.

$$|C_{wu}^{s}| = \boldsymbol{w}_s^t \bar{\boldsymbol{y}} \approx \lambda \boldsymbol{w}_s^t I \qquad (12)$$

식 (10)으로부터, $\boldsymbol{w}_s^t I$는 무작위로 선택된 $\boldsymbol{w}_s$의 성분들의 합으로 생각할 수 있으므로 $\lambda \boldsymbol{w}_s^t I \approx 0$ 이다. 따라서 Wu의 공격은 기존의 개인키를 이용한 검출을 불가능하게 한다.

4.2 검출 성능의 비교

표 1은 변환키 비대칭 워터마킹 시스템 하에서 기존의 검출 방식과 제안하는 새로운 검출 방식과의 성능 비교를 보여주고 있다. 실험에서 사용된 워터마크 셋 $\{w_i, i = 1,..,10\}$은 가우시안 분포를 갖는 길이가 1024인 10개의 난수 시퀀스를 직교화 및 정규화 과정을 통하여 획득하였다. 개인키 및 공개키를 위한 선형 변환 행렬 $\boldsymbol{A}$는 [7]의 방식을 이용하여 설계하였으며 개인키와 공개키가 원본신호 $\boldsymbol{x}$와 직교임을 만족시키기 위해 우리는 원본신호 $\boldsymbol{x}$로 길이가 1024인 가우시안 분포를 갖은 난수 시퀀스를 사용하였다. 워터마크의 삽입 세기는 약 10dB로 조정하였으며 이는 다음과 같이 계산된다.

$$10\log_{10}\frac{P_x}{P_w} \qquad (13)$$

여기서 P_x는 원본신호의 파워를, P_w는 워터마크 신호의 파워를 나타낸다. 개인키 및 공개키로 얻은 검출 값은 삽입된 워터마크 파워로 정규화 됐으며 따라서 검출 값은 온전히 ρ에 의해서 결정되고 0과 1사이의 값을 갖는다. 마지막으로 표는 본 실험을 3000번 반복해서 얻은 결과의 평균 값을 보여주고 있음을 밝힌다.

표 1에서 [7]은 기존의 변환키 시스템 방식에 $\rho = 0.5$를 적용했을 때의 결과이며 '제안1'은 변환키 방식에 3.2절에서 제안 하는 최적 상관도 계수 $\rho_{opt} \approx 0.62$를 적용했을 때의 결과이다. '제안2'는 3.3절의 새로운 비공개 검출키를 적용했을 때의 결과 이다. 먼저 표의 검출 성능 지표 부분을 살펴보면 '제안2' 방식이 가장 성능이 우수함을 볼 수 있다. 또한 '제안1'의 경우도 '변환키' 보다 더 나은 성능을 보임을 알 수 있다. 다음으로 빼기공격의 경우 세 방식 모두 공개 검출은 불가능 하나 비공개 검출은 가능함을 보여준다. 하지만 Wu의 공격 하에서 [7]과 '제안1'의 경우 공개 검출과 비공개 검출이 모두 실패하였으나 '제안2'의 경우 비공개 검출이 가능하였다. 따라서 제안하는 새로운 개인키는 기존의 변환키 비대칭 워터마킹 시스템의 강인성을 한 단계 더 높임을 알 수 있다.

5. 결론

본 논문에서는 변환키 비대칭 워터마킹 시스템의 강인성을 분석하고 개선 방향을 제안하였다. 먼저 공개 검출과 비공개 검출이 모두 가능한 변환키 비대칭 워터마킹 방식을 고려하여 워터마크 제거 공격에 대한 워터마킹 시스템의 강인성 척도를 새롭게 제안하였다. 또한 제안하는 척도를 바탕으로 변환키 시스템이 워터마크 제거공격에 강인해지기 위한 최적의 조건을 분석하였으며 그에 더해 워터마킹 시스템의 강인성을 더욱 높이기 위하여 새로운 개인키도 제시하였다. 워터마크 제거 공격인 빼기공격(subtraction attack)과 Wu의 공격에 대한 분석은 제안하는 새로운 개인키가 기존의 변환키 시스템의 강인성을 개선시킴을 보였다.

참 고 문 헌

[1] I. Cox, M. L. Miller and A. L. Mckellips, "Watermarking as communication with side information", *Proceedings of IEEE*, Vol. 87, No. 7, pp. 1127-1141, 1999.

[2] T. Kalker, J. -P. Linnartz and M. van Dijk, "Watermark estimation through detector analysis", *Proceeding of IEEE*

international conference on Image Processing, Vol. 1, pp. 425-429, 1998.

[3] J. -P. Linnartz, and M. van Dijk, "Analysis of the sensitivity attack against electronic watermarks in image", *Information Hiding 1998, LNCS,* pp. 258-272, 1998.

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

[5] T. Furon and P. Duhamel, "An asymmetric watermarking method", *IEEE Trans. on Signal Processing,* Vol. 51, No. 4, pp. 981-995, April 2003.

[6] J. Tzeng, W. Hwang and I. Chern, "An asymmetric subspace watermarking method for copyright protection", *IEEE Trans. on Signal Processing,* Vol. 53, No. 2, pp. 784-792, February 2005.

[7] H. Choi, K. Lee and T. Kim, "Transformed-key asymmetric watermarking system", *IEEE Signal Processing Letters,* Vol. 11, No. 2, pp. 251-254, February 2004.

[8] Y. Wu, F. Bao and C. Xu, "On the security of two public key watermarking schemes", *Info. Comm. and Signal Processing 2003,* Vol. 2, pp. 975-979, December 2003.

◐ 저 자 소 개 ◑

김 남 진

2004년 서울대학교 공과대학 전기공학부 졸업(학사)
2006년 서울대학교 공과대학원 전기컴퓨터공학부 졸업(석사)
2006 ~ 현재 KT 중앙연구소 연구원
관심분야 : 이동통신, 정보보호.
E-mail : nkim@kt.com

송 원 석

2006년 서울대학교 전기공학부 졸업(학사)
2008년 서울대학교 대학원 전기컴퓨터공학부 졸업(석사)
2008년 ~ 현재 서울대학교 대학원 전기컴퓨터공학부 박사과정 재학중
관심분야 : 신호 처리, 패턴 인식, 생체 인식 등
E-mail : metro@infolab.snu.ac.kr

최 두 섭
2006년 고려대학교 전자공학과 졸업(학사)
2008년 서울대학교 대학원 전기컴퓨터공학부 졸업(석사)
2008년 ~ 현재 서울대학교 대학원 전기컴퓨터공학부 박사과정 재학중
관심분야 : 디지털 워터마킹, 멀티미디어 신호 처리, 패턴 인식 등
E-mail : dschoi@infolab.snu.ac.kr

최 혁
1996년 서울대학교 전자공학과 졸업(학사)
1998년 서울대학교 대학원 전자공학과 졸업(석사)
2002년 서울대학교 대학원 전자공학과 졸업(박사)
2003년 ~ 현재 서울시립대학교 컴퓨터과학부 교수
관심분야 : 디지털 워터마킹, 정보 보호, 신호 처리 등
E-mail : chyuk@venus.uos.ac.kr

김 태 정
1976년 서울대학교 전자공학과 졸업(학사)
1978년 KAIST 전자공학과 졸업(석사)
1986년 University of Michigan 전자공학과 졸업(박사)
1978년 ~ 1981년 ETRI 재직
1986년 ~ 1988년 AT&T Bell Lab. 재직
1988년 ~ 현재 서울대학교 전기컴퓨터공학부 교수
관심분야 : 신호 처리, 신호원 부호화 등
E-mail : tjkim@infolab.snu.ac.kr