# 부정자 추적 후의 재분배를 고려한 익명 핑거프린팅

최재귀 박지환

부경대학교 대학원 정보보호학과

# An Anonymous Fingerprinting Scheme with Redistribution after Tracing a Traitor

Jae-Gwi Choi, Ji-Hwan Park
Dept. of Information Security, PuKyong Nat'l University

**요 약**

디지털 핑거프린팅(digital fingerprinting)은 멀티미디어 컨텐츠에 구매자의 정보를 삽입하여 불법적으로 컨텐츠를 재분배한 부정자(traitor)를 추적하는 기법이다. 기존에 제안된 대부분의 핑거프린팅 기법은 부정자를 식별하는 단계(identification protocol) 또는 그 증거를 제 3자에게 제출하여 확신받는 단계(trial protocol)까지만 고려했다. 대개의 경우 판매자는 해당 컨텐츠에서 부정자의 정보를 추출하여 그 신원을 확인하므로 재분배자 식별 단계를 거친 판매자는 해당 구매자의 정보를 알 수 있게 된다. 따라서 판매자는 이를 이용하여 원 컨텐츠에 해당 구매자의 정보를 삽입할 수 있으며, 이로 인해 또 다른 문제가 발생할 수 있다. 본 논문에서는 재분배자 식별 단계 이후, 판매자가 불법적으로 구매자의 정보를 컨텐츠에 삽입할 가능성을 제기하고, 이 문제를 해결하기 위해 2단계 핑거프린팅 기법을 이용한 익명 핑거프린팅 방식을 제안한다.

## 1. 서론

멀티미디어 관련 기술이 발전함에 따라 음성, 영상, 문서, 동영상 등 디지털화된 데이터의 수요가 급격하게 증가하고 있다. 또한 인터넷 등 네트워크의 빠른 보급과 디지털 데이터 제작 도구의 급속한 발달로 인해 이러한 데이터를 개인의 컴퓨터에 누구나 쉽게 전송할 수 있고, 이와 더불어 편집, 저장 및 원본 데이터와 거의 차이없는 복사도 가능해졌다. 따라서 이로 인해 지적 소유권 침해의 문제가 발생되고 있다.

일반적으로 디지털 데이터를 보호하기 위한 방법으로 암호화가 사용되어왔다. 암호화는 인가된 사용자만이 알고 있는 키를 이용하여 주어진 디지털 데이터를 암호화하여 전송함으로 디지털 데이터를 보호한다. 그러나 이 방식은 디지털 데이터에 적법한 허가를 얻은 후에는 불법 복제/배포가 가능하므로 원천적으로 데이터를 보호하기에는 미흡하다.

현재까지 이에 대한 해결책으로 디지털 워터마킹(digital watermarking)이 연구되어져 왔다. 디지털 워터마킹 기법은 인간의 지각 체계 또는 감지 능력으로는 검출할 수 없게 저작권자 또는 판매자의 정보를 멀티미디어 컨텐츠 내에 삽입해 둠으로써 이후에 발생하게 될 지적 재산권 분쟁에서 정당함을 증명하는 데 사용되고 있다. 그러나 만약 인터넷상에서 불법적으로 배포되고 있는 디지털 컨텐츠를 발견하였을 때, 디지털 워터마킹 기법을 사용한 컨텐츠는 저작권자나 판매자는 누구인 지 알 수 있지만, 누가 불법적으로 배포하였는지는 알 수가 없다. 그래서 새롭게 연구된 분야가 디지털 핑거프린팅(digital finger printing)이다[1]. 디지털 핑거프린팅은 기밀 정보를 디지털 컨텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하나, 삽입 정보의 내용에 있어서는 다르다. 디지털 워터마킹이 저작권자나 판매권자의 정보가 삽입되는 반면, 핑거프린팅은 디지털 컨텐츠를 구매한 사용자의 정보가 삽입되는 것이다. 따라서 만약 컨텐츠가 불법적으로 재배포 된다면, 해당 컨텐츠 내에서 핑거프린트된 정보를 추출하여 어떤 구매자에게

본 연구는 KOSEF 특정기초연구지원(R01-2002-000-00589-0)에 의해 수행되었음.

판매된 컨텐츠임을 식별할 수 있게 되어 법적인 조치를 가할 수 있게 된다.

초기의 핑거프린팅 방식은 분배자/판매자가 각 구매자의 정보를 원본 데이터에 삽입하는 대칭형 방식(symmetric fingerprinting)이었다[1]. 대칭형 방식의 문제점은 불법 사용된 데이터를 판매자가 발견했을 때 제3자에게 구매자의 잘못을 증명할 수 없다는 것이다. 판매자와 구매자 모두 핑거프린트된 데이터를 알고 있으므로 판배자가 불법 배포했는지 구매자가 불법 배포했는지 구별이 불가능하기 때문이다. 이런 문제점 때문에 암호학적 방식을 적용한 비대칭형 핑거프린팅(asymmetric fingerprinting)이 제안되었다[2]. 이 방식은 판매자와 구매자가 2-party protocol에 참여함으로써 구매자만이 핑거프린팅된 데이터를 알 수 있는 방법으로, 판매자는 불법 복사된 데이터를 찾은 후에도 부정자의 잘못을 제3자에게 증명할 수 있는 기법이다. 그 후 구매자의 익명성을 보장하는 익명 핑거프린팅 기법(anonymous fingerprinting)이 제시되었다[3]. 익명 핑거프린팅 기법은 비대칭형 핑거프린팅 개념을 포함한 방식으로 판매자는 구매자에게 컨텐츠를 판매하지만, 프로토콜 진행과정에서 구매자의 신원은 알지 못하는 방식이다.

본 논문에서는 비대칭형 핑거프린팅이 제기된 배경에 관심을 두고자 한다. 본 논문에서는 다음의 일련의 상황: 1) 먼저 구매자가 자신의 컨텐츠를 불법 배포하였고, 2) 이를 발견한 판매자가 불법 배포된 컨텐츠에서 구매자의 정보를 추출하여 해당 구매자의 신원을 밝힐 것이다. 3) 이 후, 또 다시 동일한 컨텐츠가 불법 배포되고 있다는 가정을 한다. 이후의 기술에서는 이를 '2차 불법 배포'라 명시하고자 한다.

대개의 익명 핑거프린팅의 경우, 불법 복제물이 발견되면 판매자는 해당 컨텐츠에서 부정자의 정보(fingerprints)를 추출하여 그 신원을 확인한다. 따라서 재분배자 식별 단계를 거친 판매자는 비록 그가 불법 배포자라 할지라도 해당 구매자의 정보를 알 수 있게 된다. 따라서 판매자는 상업적인 이득을 위해 불법적으로 이를(구매자의 정보) 해당 컨텐츠에 삽입할 수 있게 된다. 또한 부정자로 추적된 구매자 역시도 또 다시 해당 컨텐츠를 불법 배포할 수도 있다. 따라서 후에 이에 대한 불법 배포가 문제된다면 해당 부정자가 누구인지, 규명이 어렵게 된다. 즉 초기의 대칭형 핑거프린팅과 같은 문제에 직면하게 되는 것이다. 결론적으로 대부분의 익명 핑거프린팅은 2차 불법 배포에서는 대칭형이 되는 것이다. 따라서 디지털 컨텐츠에 대한 핑거프린트 정보의 일부만이 검증자에게 제공되어야 하며, 핑거프린트의 완전한 정보는 해당 구매자만이 알 수 있는 구조가 제공되어야 한다. 본 논문에서는 이의 해결을 위해 2단계 다중 핑거프린팅기법을 이용하여 제2, 제3의 불법 배포에 대해서도 안전하게 재분배자를 식별할 수 있는 익명 핑거프린팅을 제안한다.

## 2. 제안 방식의 개요

### 2.1 제안 방식의 사용 기법

본 논문에서는 2단계 핑거프린팅 기법을 사용하여 부정자 추적시 이전의 부정자로 식별된 구매자가 재식별된다고 하더라도 재분배의 책임을 명확히 할 수 있는 기법을 제안한다. 여기서 '재분배의 책임을 명확히 한다'는 것은 판매자가 임의의 제3자에게 해당 구매자가 부정 배포했음을 증명할 수 있는 확실한 증거를 제시할 수 있다는 것을 의미한다. 제안 방식에서 사용하는 방법은 하나의 컨텐츠에 2개 이상의 서로 다른 정보(핑거프린트)를 삽입하는 것이다[1]. 제안 방식에서는 삽입정보를 2개로 만들어 원 컨텐츠에 삽입한다. 하나는 판매자가 부정 배포에 대한 신원을 확인할 때 사용하는 정보이고, 다른 하나는 부정 배포자에 대한 확실한 증거 제시를 위해 사용하는 정보이다. 이는 판매자와 구매자 양측이 서로의 부정행위로부터 자신을 보호하기 위한 단계로 판매자나 구매자 모두 서로의 도움 없이는 절대로 추출될 수 없는 정보이다. 본 절에서는 직교화를 이용한 2단계 핑거프린팅에 대해 그림1,2로 간략히 설명한다.

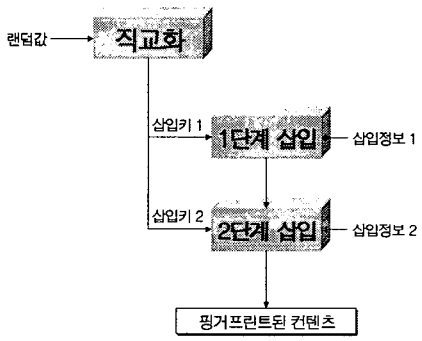


그림1. 삽입과정

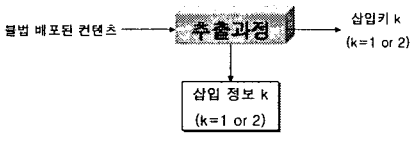


그림2. 식별 과정

### 2.2 제안 방식의 구성

제안 방식은 크게 다음 4개 부분으로 이루어진다.

① 시스템 설정: 등록 센터는 자신의 비밀키와 공개키를 설정한다. 등록 센터는 자신의 비밀키를 이용하여 인증서를 발급하고, 인증서는 등록 센터의 공개키를 가지고 검증된다. 모든 구매자들의 공개키는 알려지고 인증되었다고 가정한다.

② 등록 프로토콜: 구매자와 등록 센터 사이의 프로토콜로, 실행 결과 구매자는 익명의 키를 얻게 되고, 등록 센터는 해당 구매자의 등록 레코드를 가지게 된다.

③ 핑거프린팅 프로토콜: 구매자와 판매자간의 프로토콜로, 본 논문에서는 Secure Multi-Party Computation 프로토콜[5]과 2.1절에서 기술한 2단계 핑거프린팅 기법을 사용한다. 실행 결과 구매자는 핑거프린트된 컨텐츠를 얻게 된다.

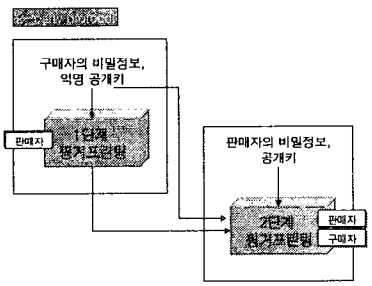


그림3. 2단계 핑거프린팅

④ 식별 프로토콜: 재 배포된 컨텐츠를 발견했을 때, 판매자는 재분배자의 신원을 밝히기 위해 식별 프로토콜을 수행한다. 해당 프로토콜은 2단계 식별 프로토콜로, 먼저 판매자가 부정자를 추적하기 위해 첫 번째 식별 알고리즘을 수행하고, 추적된(고소된) 구매자가 식별에 의의가 있을 때, 판매자와 구매자가 함께 두 번째 식별 프로토콜을 수행한다.

## 3. 재분배 추적 가능한 익명 핑거프린팅

기존의 대부분의 익명 핑거프린팅 방식[3,5,6]은 본 제안 방식에 적용 가능하다. 본 제안 방식의 핵심은 판매자가 식별 프로토콜을 수행할 때에 삽입된 모든 정보를 추출할 수 없도록 하는 것이다. 본 장에서는 Domingo 기법[5]에 본 제안 방식을 적용함으로 일예를 보인다.

### 3.1 시스템 설정

- $p$ : 소수 $q=(p-1)/2$ 를 만족하는 큰 소수
- $G$ : $(p-1)$ 위수를 갖는 그룹
- $g$ : 그룹 $G$의 원시원소
- $x_B, y_B=g^{x_B} \bmod p$ : 구매자의 비밀키, 공개키
- $x_M$ : 판매자의 비밀키
- $y_{BM}=g^{x_B x_M} \bmod p$:구매자·판매자의 공통 공개키

### 3.2 등록 프로토콜

구매자는 다음과 같은 순서로 등록 센터에 자신의 신원을 등록하고, 익명의 공개키를 얻는다.

① 등록 센터는 랜덤 비밀값를 $x_r \in Z_p$선택하고 $y_r=g^{x_r} \bmod p$를 계산한 후 구매자에게 $y_r$를 전송한다.

② 구매자는 $x_1+x_2=x_B$를 만족하는 랜덤한 비밀값 $x_1, x_2$를 선택하고 $S_1=y_r^{x_1}$와 $S_2=y_r^{x_2}$를 계산하여 등록 센터에 $S_1$과 $S_2$를 전송한다. 그러한 후에, 구매자는 자신이 $x_1, x_2$를 알고 있다는 사실을 영지식 증명 방식을 이용하여 등록 센터에 증명한다. 구매자는 핑거프린팅에서 공개키로 사용할 $y_2=g^{x_2} \bmod p$ 를 계산하여, 등록 센터에게 전송한다. 핑거프린팅 프로토콜에서 $S_1$은 익명성을 제공하기 위한 인증정보로 사용된다.

③ 등록 센터는 구매자로부터 받은 $S_1, S_2$이 $S_1S_2=y_B^{x_r}$를 만족하고, 익명성을 제공하는 공개키 $y_2$가 $y_2^{x_r}=S_2$를 만족하는지 검증한다. 두 개의 검증이 성공한다면 등록 센터는 인증서 $Cert(S_1 \| y_r)$와 $Cert(S_2 \| y_r)$를 생성하고 처음에 선택한 랜덤한 비밀값 $x_r$과 함께 이를 구매자에게 전송한다.

### 3.3 핑거프린팅 프로토콜

구매자는 디지털 컨텐츠를 구매하기 위하여 판매자와 핑거프린팅 프로토콜을 수행한다.

#### 3.3.1 인증 프로토콜

① 구매자는 $y_r, y_2, [S_1, Cert(S_1 \| y_r)]$ 그리고 구매하고자 하는 디지털 컨텐츠를 나타내는 문자열 *text*를 판매자에게 전송하고, *text*를 자신의 비밀키

$x_2$를 사용하여 서명을 생성한다. 이 때 서명 $sig_1$는 판매자에게 전송되지 않는다.

$$sig_1 = (text, r_1, s_1)$$
$$r_1 = text - g^{-k_{B1}}, s_1 = k_{B1} - x_2 \cdot r_1 \quad (1)$$

② 판매자는 구매자로부터 전송 받은 인증서 $Cert(S_1||y_r)$를 검증한다.

#### 3.3.2 1단계 핑거프린팅 프로토콜

검증이 성공할 경우에, 구매자와 판매자는 안전한 양자간 계산(secure two-party computation)[7]를 수행한다. 판매자의 입력은 $y_r, y_2, text, x_M, k_{M1}$와 구매자가 구매하고자 하는 디지털 컨텐츠 $item$이고, 구매자의 입력은 $x_r, sig_1, S_2, k_{B2}, x_2$와 인증서 $Cert(S_2||y_r)$이다. 안전한 양자간 계산은 다음과 같다.

① $view_1 = verify(text, sig_1, y_2)$를 검증한다. $text$에 관한 서명 $sig_1$는 공개키 $y_2$를 사용하여 검증된다. 출력 $view_1$는 서명 검증이 성공한 경우에, 판매자에게만 보여 지는 불리언 변수이다.

$$text = y_2^{r_1} \cdot g^{s_1} \cdot r_1 \quad (2)$$

② $view_2 = verify(S_2, Cert(S_2||y_r), x_r, y_r, y_2)$를 검증한다. 먼저 $S_2$에 관한 인증서를 검증하고, $g^{x_r} = y_r$ 그리고 나서 $y_r^{x_2} = S_2$인지 검증하고 마지막으로 판매자에 의하여 이전에 검증된 $S_1$에 관한 인증서에서 $y_r$을 검증한다. 출력 $view_2$는 이전의 3가지 검증이 성공하는 경우에 판매자에게만 보여 지는 불리언 변수이다.

③ 위의 ①,②과정이 성공하면 핑거프린팅 알고리즘을 이용하여 원본 컨텐츠 $item$에 다음의 $emb_1$을 삽입한다.

$$emb_1 = text||sig_1||y_2||x_r||y_r||S_2||Cert(S_2||y_r)$$

#### 3.3.3 2단계 핑거프린팅 프로토콜

1단계 핑거프린팅 프로토콜이 성공하면 2단계 핑거프린팅 프로토콜을 다음과 같이 수행한다.

① 판매자와 구매자의 비밀키를 사용하여 $sig_2 = (text, r_2, s_2)$를 계산한다.

$$r_2 = text \cdot g^{-k_{B_2}k_{M_1}}$$
$$s_2 = k_{B_2} \cdot k_{M_1} - r_2 x_2 x_M \quad (3)$$

② 2단계 다중 핑거프린팅 알고리즘을 이용하여 $emb_1$이 삽입된 컨텐츠에 다음의 $emb_2$을 삽입한다.

$$emb_2 = text||sig_2||y_M||y_2||y_{BM}$$

위의 안전한 양자간 계산에서 $view_1$과 $view_2$ 둘 다 참일 때, 구매자는 출력을 얻고, 둘 중에 하나라도 거짓이면 구매자는 출력을 얻을 수 없다. 이 때 출력은 구매자에게만 보여 지는 핑거프린트된 정보 $item^* = (item, emb_1, emb_2)$이다. 위의 2단계 핑거프린팅 단계의 삽입키로는 각각 $key_1, key_2$을 이용한다.

$key_1$: 구매자의 비밀키

$key_2$: 구매자와 판매자의 비밀키

### 3.4 재분배자 식별 프로토콜

#### 3.4.1 판매자의 식별 프로토콜

판매자는 재분배된 복사본이 발견되면, 복사본으로부터 $emb_1$추출한다. 그리고 추출된 $emb_1$안에 $y_r$값과 같은 인증서를 판매기록으로부터 찾아 식별 프로토콜에 들어간다. 식별 프로토콜은 다음과 같이 진행된다.

① 익명성을 제공하는 공개키 $y_2$를 사용하여 $text$에 관한 서명 $sig_1$을 검증한다. $y_r$값은 인증서 $S_1$과 $S_2$에 관련된 값이다. 즉 인증서의 일부분이기 때문에 변경될 수 없다. $x_r$값은 익명성 공개키 $y_2$의 소유자와 $S_2$의 소유자가 같다는 것을 증명한다. 이는 등록 프로토콜에서 구매자가 $y_2^{x_r} = S_2$를 만족하는 $y_2$를 제공한 후에, 등록센터가 $x_r$를 구매자에게 제공했기 때문이다.

② 판매자는 재분배한 구매자를 식별하기 위하여, $S_1 S_2 = y_B^{x_r}$를 만족하는 공개키 $y_B$가 발견될 때까지 공개키 디렉토리의 공개키에 $x_r$지수 연산을 수행한다.

#### 3.4.2 구매자의 식별 프로토콜

재분배자로 식별된 구매자가 식별에 의의가 있을 때는 판매자와 함께 컨텐츠에서 $emb_2$을 추출하여 다음의 식을 검증한다. 여기에서 $y_{BM}$은 앞의 판매자의 식별 프로토콜에서 검증된 $y_2$값과 판매자와 구매자가 동시 동의로 검증되어진다.

$$text = r_2 \cdot g^{s_2} \cdot y_{BM}^{r_2} \quad (4)$$

식(4)에서 유도된 $text$값이 이전에 판매자가 추출한 $emb_1$에서 검증한 $text$값과 같으면 해당 구매자는 불법 배포자이다. 만약 판매자나 다른 사람이 해당 컨텐츠를 불법 배포하였다면 그 컨텐츠에서는 올바른 $emb_2$를 추출할 수 없을 것이다. 왜냐하면 구매자의 비밀키를 사용하지 않고서는 $emb_2$를 추출하거나 삽입

할 수가 없기 때문이다. 반대로 재분배된 컨텐츠에서 $emb_2$를 추출하여, *text* 값이 정확하게 나온다면 이는 구매자가 부정 배포자임을 재확인시켜 주는 것이다. 역으로 구매자가 $emb_2$를 추출한 후 컨텐츠를 재분배하여 판매자에게 부정배포에 대한 책임을 전가할 수도 없다. 왜냐하면 $emb_2$의 추출과 삽입에는 판매자와 구매자의 비밀키가 동시에 필요하기 때문이다.

## 4. 안전성 분석 및 기존 연구와 비교

제안방식은 다음과 같이 판매자와 구매자의 안전성을 제공한다.

◦ 구매자에 대한 안전성 제공

① 어떠한 개체도 혼자의 힘으로 $emb_i(i=1,2)$ 모두를 추출하거나 삽입할 수 없다. 다중 핑거프린팅 기법[4]에서는 삽입과 추출에 사용되는 *key*와 *key*간에는 상관성이 있으나, 하나의 *key*에서 다른 *key*를 유도하기는 힘들기 때문이다. 따라서 판매자는 정확히 $emb_1$만 추출할 수 있으므로 나머지 1개의 삽입정보는 식별 단계를 거쳤다고 해도 전혀 알 수 없다. 따라서 불법적인 컨텐츠를 발견한 후, 삽입 정보를 추출하여 다른 컨텐츠에 이를 삽입하여 재배포한다하여도 그 책임을 해당 구매자에게 전가할 수는 없다

② 이산 대수 문제가 안전한 한, 구매자의 등록 프로토콜의 안전성과 익명성은 제공된다. 왜냐하면 판매자는 구매자의 $x_r$값을 모르고는 $y_B$를 찾을 수 없으며, 등록 센터 역시 $x_1, x_2$값을 알지 못하고는 $x_B$값을 알 수 없기 때문이다.

◦ 판매자에 대한 안전성 제공

① 판매자와 구매자 모두 혼자의 힘으로 $emb_2$를 추출, 삽입할 수 없으므로, 후에 재분배된 컨텐츠에서 불법 배포자의 신원이 나오면 이는 정확히 해당 구매자가 배포한 것이 되므로, 임의의 제 3자에게 불법 배포자에 대한 증거를 정확히 확신시킬 수 있다. 판매자가 등록 센터와 공모한다하더라도 삽입 및 추출에는 구매자의 비밀키가 필요하므로 판매자는 불법 배포자를 정확히 규명할 수 있게 된다. (단 제한된 수 이상의 구매자가 공모한다면 불법 배포자에 대한 신원 확인이 실패할 수도 있다[8])

표1. 단계별 불법 배포에 대한 기능 비교

| 기능 | | 비대칭 핑거프린팅[2] | 익명 핑거프린팅[6] | 제안방식 |
|---|---|---|---|---|
| 1차불법배포 | 비대칭성 | 제공 | 제공 | 제공 |
| | 익명성 | 제공안함 | 제공 | 제공 |
| 2차불법배포 | 비대칭성 | 제공안함 | 제공안함 | 제공 |

## 5. 결론

본 논문에서는 재분배자 식별 단계 이후, 판매자가 불법적으로 구매자의 정보를 원 컨텐츠에 삽입할 가능성을 제기하고, 이의 해결을 위해 2단계 다중 핑거프린팅 기법을 이용한 익명 핑거프린팅 방식을 제안하였다. 제안한 방식을 적용한다면, 컨텐츠 제공자는 인터넷 등 개방된 컨텐츠 유통 채널에서 저작권을 보호하면서 컨텐츠를 배포할 수 있고, 컨텐츠 사용자는 안전하게 자신의 적법한 구매 소유권을 주장할 수 있다. 향후 제안 방식이 안전하게 사용되기 위해서는 다중 핑거프린팅 기법의 안전한 *key* 설정이 요구되어진다. 더불어 현재까지 제안된 핑거프린팅 방식은 디지털 컨텐츠 자체에 대한 공격으로 인한 핑거프린팅 정보의 손상에 대한 고려와 계산적 복잡도로 인한 효과적인 구현 문제가 남아있기 때문에 이에 대한 연구도 향후에 진행되어야 될 것이다.

## [참고문헌]


[1] N.R.Wagner, "Fingerprinting", *IEEE Symp. on Security and Privacy*. 1983

[2] B.Pfitzmann and M.Schunter, "Asymmetric Fingerprinting", Eurocrypt96, LNCS No.1070, Springer, 1996.

[3]B.Pfitzmann and W.Waidner, "Anonymous Fingerprinting", Eurocrypt97, LNCS No. 1233, Springer, 1997.

[4] 오윤희, 강현호, 박지환, "Gram-Schmidt 직교화를 이용한 다중 워터마킹", 정보처리학회 논문지 제8-C권, 6호.

[5] J.Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors", Electronics Letters 34/13. 1998.

[6] Jan.Camenisch, " Efficient Anonymous Fingerprinting with Group Signature", Asiacrypt 2000, Springer, LNCS 1976, 2000.

[7] D.Chaum et al., "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", Crypto'87, LNCS 293, Springer 1987.

[8] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", Crypto95, *LNCS No.963, Springer,* 1995.