신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법
(An Anonymous Asymmetric Fingerprinting Scheme with Trusted Third Party)

용 승 림 † 이 상 호 ††
(Seung-Lim Yong) (Sang-Ho Lee)

요 약 디지털 형식으로 저장되어 있는 데이타의 불법적인 복사와 재분배는 전자상거래 상에서 디지털 콘텐츠를 판매하는 판매자에게 매우 큰 문제가 된다. 핑거프린팅 기법은 암호학적인 기법들을 이용하여 디지털 콘텐츠를 불법적으로 재배포한 구매자를 찾아냄으로써 저작자의 저작권을 보호한다. 익명적 비대칭적 핑거프린팅 기법은 대칭적인 기법과 달리 구매자만이 핑거프린트가 삽입된 콘텐츠를 알 수 있어 구매자가 콘텐츠를 재배포했을 경우만 구매자가 고발되며, 데이타가 재배포되기 전에는 구매자의 익명성이 보장되는 기법이다.

본 논문에서는 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법을 제안한다. 이 기법에서는 구매자의 핑거프린트는 신뢰기관인 핑거프린트 인증센터에서 생성한다. 또한, 판매자가 핑거프린트를 삽입할 때, 준동형의 암호를 이용하여 콘텐츠에 삽입함으로써 판매자는 구매자의 핑거프린트를 알 수 없으며 익명 공개키를 이용함으로써 구매자의 익명성을 보장하였다.

키워드 : 익명적 비대칭 핑거프린팅 기법, 신뢰기관, 저작권 보호

Abstract The illegal copying and redistribution of digitally-stored information is a crucial problem to distributors who electronically sell digital data. Fingerprinting scheme is a technique which supports copyright protection to track redistributors of electronic information using cryptographic techniques. Anonymous asymmetric fingerprinting scheme prevents the merchant from framing a buyer by making the fingerprinted version known to the buyer only. And this scheme allows the buyer to purchase goods without revealing her identity to the seller.

In this paper, a new anonymous asymmetric fingerprinting scheme with TTP is introduced. The buyer's fingerprint is generated by the Fingerprint Certificate Authority which is a TTP. When the seller embeds the fingerprint in the digital data, the protocol uses the homomorphic encryption scheme. Thus the seller cannot know the buyer's fingerprint and the buyer's anonymity is guaranteed by using anonymous key pair.

Key words : Anonymous asymmetric fingerprinting, Trusted third party, Copyright protection

1. 서 론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 전자상거래가 활발해지고 디지털 데이타의 확산 및 보급이 일반화되고 있다. 그러나 이러한 데이타들은 디지털이라는 속성으로 인하여 누구나 손쉽게 불법적인 복제를 통해서 이들을 획득할 수 있게 되고, 이 때문에 저작권 문제가 야기되고 있다. 따라서 정보기반 전자 상거래에서 디지털 데이타의 저작권 보호는 아주 중요한 문제가 되었다. 이에, 몇몇의 하드웨어를 이용한 복사방지 기법이나 암호를 이용한 불법적 행위 등이 일어나지 못하도록 막는 방법이 많이 이용되었다, 그러나 이러한 방법들은 복호화된 콘텐츠의 불법 복제를 막을 수 없거나 해커들에 의하여 안전성이 상실되었다.

후에 디지털 데이타의 저작권을 보호할 수 있는 방법으로 복사본을 찾아내는 방법이 많이 제안되었다. 즉 디지털 데이타의 저작권을 보호하기 위해 데이타의 복사 자체를 막는 것이 아니라 디지털 데이타를 불법적으로 재분배한 사람을 찾아내도록 하는 기법이다.

핑거프린팅 기법[1]은 데이타가 불법적으로 재배포 되었을 때 판매자가 그 데이타를 구매한 재배포자를 식별

† 정 회 원 : 이화여자대학교 컴퓨터학과
dragon@ewhain.net
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2005년 10월 26일
심사완료 : 2007년 4월 26일

할 수 있게끔 구매자마다 서로 다른 마크를 삽입하게 함으로써 디지털 저작권을 보호한다. 워터마킹 기법과의 차이점은 워터마킹 기법[2]은 모든 콘텐츠에 판매자의 같은 마크가 삽입되지만 핑거프린팅 기법에는 구매자마다 다른 마크가 삽입된다는 점이다. 하지만 핑거프린팅 기법에서 구매자의 마크를 삽입할 때는 워터마킹 시스템을 이용한다.

핑거프린팅 기법에서 정직한 구매자는 불법적인 행위를 하기 전까지는 그의 신원이 알려져서는 안된다[3-6]. 즉, 특정한 구매자의 익명성은 불법적인 행위를 수행하기 전까지는 보장되어야 한다. 그러나 대칭적인 기법에서는 판매자가 서로 다른 콘텐츠의 복사본들을 각 구매자에게 나누어주기 때문에 악의적인 판매자가 복사본을 재배포하고 정직한 구매자를 재배포자로 고발할 수 있다[7]. 이러한 경우 구매자는 자신이 콘텐츠를 재배포하지 않았음을 증명할 수 있는 방법이 전혀 없다. 이러한 문제점을 해결한 것이 비대칭적인 핑거프린팅 기법이다[8]. 익명적 비대칭 기법은 구매자와 판매자가 마크를 삽입하는 과정을 프로토콜로 수행함으로써 핑거프린트가 삽입된 데이타를 구매자만이 알 수 있고 판매자는 핑거프린팅된 데이타를 알 수 없도록 한다.

본 논문에서는 준동형의 암호와 신뢰기관을 이용하여 좀 더 효율적인 익명적 비대칭적 핑거프린팅 기법을 제안한다. 또한 구매자가 익명 공개키 쌍을 이용함으로써 구매자의 익명성을 보장해 준다.

2. 관련 연구

2.1 핑거프린팅

2.1.1 핑거프린팅이란

핑거프린팅(fingerprinting) 기술은 콘텐츠의 상거래시 구매자의 정보도 포함하는 핑거프린팅 정보를 콘텐츠에 삽입하여 후에 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 저작권 보호 기술이다. 콘텐츠에 저작권 정보를 삽입할 때 워터마킹 기법을 이용한다. 워터마킹 기술은 디지털 콘텐츠에 원래의 소유주를 표시하는 저작권 정보, 즉 워터마크를 넣어 배포하고 불법복제 후의 콘텐츠에 대해 워터마크를 다시 추출함으로써 원소유주를 증명한다. 따라서 모든 판매된 콘텐츠들은 모두 동일한 워터마크가 삽입되어 있다. 이와는 달리, 핑거프린팅 기법은 판매되는 콘텐츠마다 서로 다른 구매자 정보를 삽입하기 때문에 핑거프린팅된 콘텐츠는 서로 조금씩 다르게 된다. 일반적으로 핑거프린팅 기법은 대칭 기법, 비대칭 기법 그리고 익명성 보장 비대칭 기법으로 나뉜다. 대칭 기법은 판매자가 핑거프린트를 삽입하는 반면, 비대칭 기법과 익명성 보장 비대칭 기법은 판매자와 구매자 사이에서의 상호교환 프로토콜에 의하여 핑거프린트를 삽입하게 된다. 따라서 익명성 보장 비대칭적 기법은 사용자의 프라이버시를 위하여 삽입된 핑거프린트를 모를 뿐 아니라 구매자가 데이타를 재배포하지 않는 한 구매자의 익명성도 철저히 보장된다.

기존의 익명성을 보장하는 기법들은 Ju의 기법에서와 같이 검증 가능한 암호 알고리즘을 이용하여 익명성을 보장하거나 Choi의 핑거프린트 생성센터에서 서로 다른 n개의 핑거프린트를 생성하고 이들 중 하나를 구매자가 선택하게 하는 방법으로 익명성을 보장하도록 하였다[9,10]. 그러나 Ju의 기법은 재판관이 프로토콜의 처음 단계부터 프로토콜에 참여해야 하는 단점이 있으며, Choi의 기법은 구매자마다 서로 다른 핑거프린트를 생성하고 저장해야 하는 오버헤드가 발생하는 단점이 있다.

2.1.2 요구사항

핑거프린팅 기법에서 판매자의 저작권을 보호하기 위하여 만족해야 할 요구사항은 다음과 같다.

□ 추적성

콘텐츠를 불법으로 재분배한 구매자는 어떠한 경우라도 판매자나 다른 기관에 의하여 추적되어야 한다.

□ 견고성

콘텐츠를 불법으로 재분배하려고 하는 공격자는 삽입된 핑거프린팅 정보에 손상을 가하기 위하여 여러 가지 조작을 하게 된다. 견고성(robustness)은 이러한 조작에 대해 삽입된 핑거프린팅 정보가 얼마나 잘 견디어 내는지를 평가하는 척도이다.

□ 비대칭성

콘텐츠를 구매할 시점에서 핑거프린팅된 콘텐츠를 구매자만이 알고 판매자는 알지 못하도록 하는 조건을 비대칭성(asymmetry)이라고 한다. 핑거프린팅된 콘텐츠를 판매자도 접근할 수 있다면 불법 재분배자 식별에 있어서 모호함이 발생할 수 있다. 단지 구매자만이 핑거프린팅된 콘텐츠를 소유할 수 있어야만 재분배했을 경우에 확실한 불법의 증거가 된다.

□ 공모허용

핑거프린팅된 콘텐츠는 워터마킹된 콘텐츠와는 달리 서로 다른 구매자 정보를 삽입하기 때문에 구매자에 따라 조금씩 다르다. 다수의 구매자들이 서로 공모하여 콘텐츠 내에서 핑거프린팅된 위치를 파악할 수 있고 또한 콘텐츠끼리의 상대적인 차이를 이용하여 핑거프린팅 정보를 지우거나 새로운 핑거프린팅 정보를 삽입하여 재분배함으로써 공모자의 신분을 숨길 수 있다. 공모허용(collusion tolerance) 조건은 이런 공모에 대비하여 많은 핑거프린팅된 콘텐츠가 공격자에게 제공되어 공모공격이 가해지더라도 최소 1명 이상의 공모자의 정보도 추출 가능해야 한다.

□ 익명성

콘텐츠를 구매한 구매자는 그 콘텐츠를 재배포하기 전까지는 구매자의 익명성이 보장되어야 한다.

2.2 그 외의 개념들

2.2.1 준동형의 암호

암호시스템 E가 준동형의 성질을 가질 때 암호시스템은 준동형적이라고 정의한다. 즉, 어떤 정의된 연산 $\oplus$에 대하여, 알려지지 않은 평문 x와 y에 대한 암호문 $E(x)$와 $E(y)$가 주어졌을 때, 누구든지 개인키 없이도 $E(x \oplus y)$를 계산할 수 있는 암호시스템이다. 본 논문에서는 [9]와 같이, 공개키 암호시스템이 핑거프린트를 삽입하는 연산에 대해서 프라이버시 준동형의 성질을 만족한다고 가정한다.

2.2.2 워터마킹 기법

워터마킹 기법은 디지털 콘텐츠에 핑거프린트를 삽입하기 위하여 신호처리 기법을 이용한다. 일반적으로 워터마킹 기법은 워터마크 삽입과 워터마크 추출의 두 단계로 구성되어 있다. 디지털 콘텐츠 $X=\{x_1, x_2, \cdots, x_n\}$와 핑거프린트 $W=\{w_1, w_2, \cdots, w_m\}$가 있다고 하자. 워터마크가 삽입된 콘텐츠 X'은 식 $X'=I(X, W)$에 의하여 생성될 수 있다. 워터마크를 삽입하는 삽입함수 I는 다음과 같다.

$$X \otimes W = \{x_1 \otimes w_1, x_2 \otimes w_2, \cdots, x_m \otimes w_m, x_{m+1}, \cdots, x_n\} \quad (1)$$

해당하는 삽입함수 I에 대하여 워터마크를 추출하는 추출함수 D가 있다. 이 함수는 콘텐츠 X'에 해당하는 워터마크가 삽입되어 있는지의 여부를 알려준다. 본 논문에서는 핑거프린트를 삽입하기 위하여 워터마킹 기법을 적용한다. 따라서 핑거프린트가 삽입된 컨텐츠의 품질과 핑거프린트의 왜곡 여부는 워터마킹 기법의 안전성에 근거한다.

3. 익명성 보장 비대칭 핑거프린팅 기법

본 장에서는 안전한 비대칭적 핑거프린팅 기법에 대하여 설명한다. 본 논문에서 제안하는 핑거프린팅 기법은 등록, 핑거프린팅 및 신원확인 프로토콜로 구성되어 있다. 먼저 각각의 프로토콜에 참여하는 참여자와 사용기호를 정의한 후 각각의 프로토콜을 자세히 설명한다.

3.1 용어정의

제안한 핑거프린팅 기법에 참여하는 참여자와 사용기호는 다음과 같으며 전체적인 구성도는 그림 1과 같다.

□ 참여자

각각의 프로토콜에 참여하는 참여자는 다음과 같다.

- 핑거프린트 인증센터(FCA) : 핑거프린트를 생성, 관리하는 제3의 신뢰기관이다.
- 등록센터(RC) : 구매자의 키를 등록하고 그에 대한 인증서를 생성하는 제3의 신뢰기관이다.
- 판매자(S) : 디지털 콘텐츠를 판매하는 개체이다.
- 구매자(B) : 디지털 콘텐츠를 구매하는 개체로서 구매한 콘텐츠를 불법적으로 재배포할 수 있는 절대적으로 신뢰할 수 없는 개체이다.
- 재판관 : 신원확인 프로토콜에서 불법 배포자의 신원을 제공된 자료들을 기반으로 확인해주는 개체이다.

□ 사용되는 기호

- F : 구매자의 고유 인식정보인 핑거프린트
- M : 핑거프린트가 삽입될 원본 콘텐츠, 구매자가 구매하고자 하는 콘텐츠
- $\overline{M}$: 구매자의 핑거프린트가 삽입된 콘텐츠
- H : 충돌 회피성 해쉬함수
- AE/AD : 공개키 암호시스템, 암호화/복호화 알고리즘
- SE/SD : 대칭키 암호시스템, 암호화/복호화 알고리즘
- HE/HD : 준동형의 성질을 만족하는 암호시스템

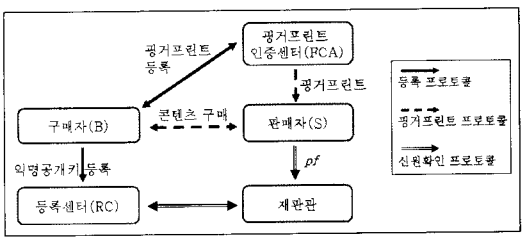

그림 1 시스템 구성도

3.2 구매자 등록하기

구매자와 핑거프린트 인증센터는 모두 공개키와 개인키 쌍을 가지고 있다고 가정한다. 구매자의 개인키는 x_B이고 공개키는 $y_B = g^{x_B}$이다. 핑거프린트 인증센터의 개인키는 핑거프린트 인증센터의 공개키를 이용하여 인증서를 검증할 수 있는 인증서를 생성하는데 이용된다. 또한 두 개체의 공개키는 인증되어 있다고 가정한다. 등록에 대한 상세 프로토콜은 다음과 같다.

프로토콜 1 (등록 프로토콜)

모든 구매자는 등록 센터에 자신의 익명 공개키와 자신의 아이디를 등록하고, 익명 공개키에 대한 등록 센터의 인증서를 전송받는다.

- 익명 공개키 등록

1) 구매자는 자신의 익명 공개키 쌍을 생성하기 위하여 $x_1 + x_2 = x_B$인 임의의 두 수 x_1, x_2를 선택한다. 먼저 구매자는 익명 공개키 $y_1 = g^{x_1}$를 생성하고 공개키, 개인키 쌍 (x_1, y_1)을 익명 공개키 쌍으로

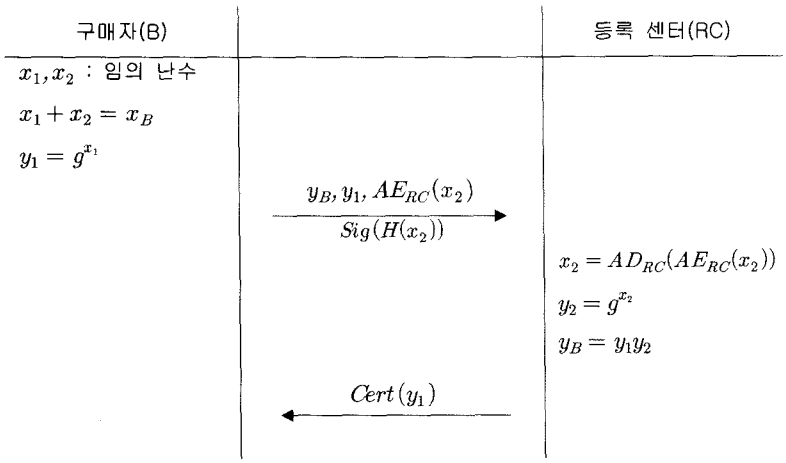

그림 2 등록 프로토콜 - 익명 공개키 등록

이용한다. 그리고 x_2를 등록센터의 공개키로 암호화한 $AE_{sRC}(x_2)$를 계산하고 $H(x_2)$에 익명 개인키 x_1을 이용하여 서명한 서명값 $Sig(H(x_2))$을 생성한다. 구매자는 자신의 공개키와 익명 공개키 $y_B, y_1, AE_{sRC}(x_2)$ 그리고 $Sig(H(x_2))$를 등록 센터에 보낸다. 서명값을 보냄으로써 구매자가 생성한 익명 공개키에 대한 개인키를 알고 있음을 증명할 수 있다.

2) 등록 센터는 자신의 개인키를 이용하여 $AD_{RC}(AE_{RC}(x_2))$를 계산하고 $y_2 = g^{x_2}$를 계산한 후 $y_1 y_2 = y_B$인지 확인한다.

3) 값이 맞을 경우 등록 센터는 구매자의 익명 공개키에 서명을 수행하여 인증서 $Cert(y_1)$을 구매자에게 전송한다.

• 핑거프린트 등록

1) 구매자는 핑거프린트 인증센터에게 익명 공개키 y_1과 인증서 $Cert(y_1)$을 전송한다. 핑거프린트 인증센터는 인증서를 검증한 후 공모 공격으로부터 안전한 구매자의 핑거프린트 F를 생성한 후 이를 구매자의 익명 공개키 y_1을 이용하여 암호화한 $HE_{y_1}(F)$을 생성한다. 공모 공격에 안전한 핑거프린트 F는 적절한 파라메터[9]를 이용하여 한 번도 이용되지 않은 코드워드로 생성한다.

2) 핑거프린트 인증센터는 임의의 키 k를 생성한 후, 생성된 키와 대칭키 암호시스템을 이용하여 $C = SE_k(HE_{y_1}(F))$를 생성한다. 그리고 C의 해쉬함수에 대한 서명값 $Sig(H(C))$를 생성하여 구매자에게 보내준다.

3) 핑거프린트 인증센터는 익명 공개키 y_1, 핑거프린트 F, 서명값 $Sig(H(C))$ 그리고 대칭키 k를 핑거프린트 인증센터의 데이타베이스에 저장한다.

3.3 상품 구매하기

구매자가 판매자로부터 콘텐츠를 구매하고자 할 때 다음의 프로토콜이 수행된다. 구매자는 판매자에게 자신의 익명 공개키와 그의 인증서, 핑거프린트 인증센터로부터 받은 암호화된 핑거프린트를 판매자에게 주고 판

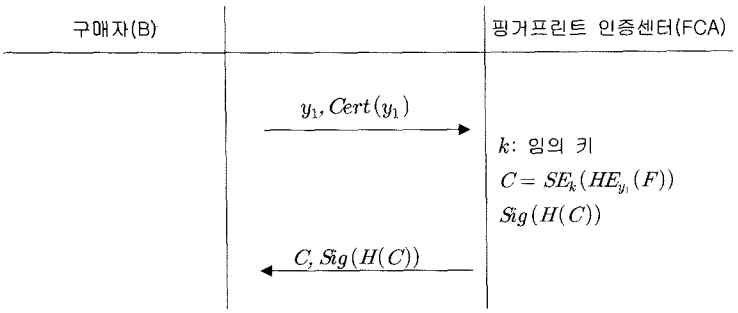

그림 3 등록 프로토콜 - 핑거프린트 생성

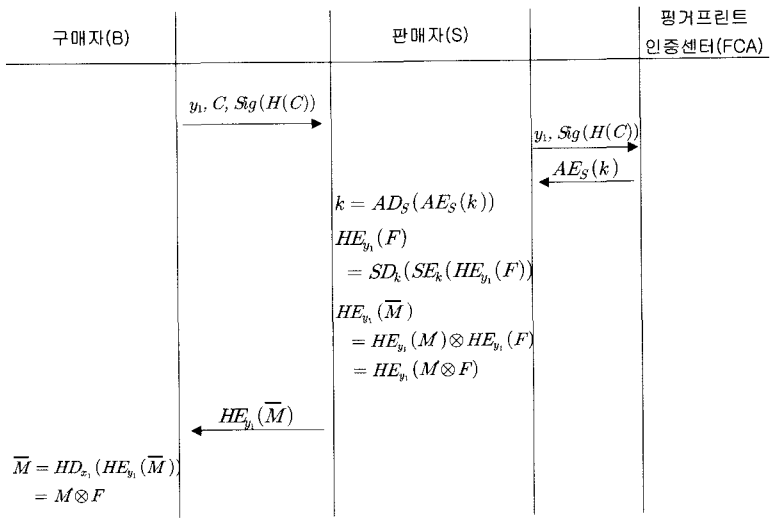

그림 4 핑거프린팅 프로토콜

매자는 핑거프린트 인증센터로부터 암호화된 핑거프린트를 복호화할 수 있는 키를 받아온다. 상세한 핑거프린팅 프로토콜은 그림 4와 같다.

프로토콜 2 (핑거프린팅 프로토콜)

1) 구매자는 판매자에게 $y_1, C, Sig(H(C))$를 보낸다.
2) 판매자는 핑거프린트 인증센터의 공개키를 이용하여 C값에 해쉬함수를 적용하여 $Sig(H(C))$가 맞는지 확인한다. 정당한 서명으로 검증이 되면 판매자는 $y_1, Sig(H(C))$를 핑거프린트 인증센터에게 보낸다.
3) 핑거프린트 인증센터는 판매자로부터 받은 y_1에 대한 복호화 키 k를 판매자의 공개키를 이용하여 암호화한 $AE_S(k)$와 서명값 $Sig(H(C))$를 판매자에게 보낸다.
4) 판매자는 자신의 개인키를 이용하여 키 k를 복호화한 후 암호문 C를 복호화하여 다음을 얻는다.

$$HE_{y_1}(F) = SD_k(C)$$
$$= SD_k(SE_k(HE_{y_1}(F)))$$

5) 판매자는 유일한 핑거프린트 V를 생성하고 콘텐츠 M에 이를 삽입하여 핑거프린트가 삽입된 콘텐츠 M'을 생성한다. 핑거프린트 V는 콘텐츠가 재배포되었을 경우 특정한 구매자를 찾을 수 있는 도구로 이용된다.
6) 판매자는 구매자의 익명 공개키 y_1을 이용하여 M'을 암호화한 $HE_{y_1}(M')$에 핑거프린트 인증센터로부터 받은 암호화된 핑거프린트 $HE_{y_1}(F)$를 임베드한다. 준동형의 암호화 성질에 의해서 암호화된 핑거프린트는 콘텐츠에 삽입될 수 있다[12].

$$HE_{y_1}(\overline{M}) = HE_{y_1}(M') \otimes HE_{y_1}(F)$$
$$= HE_{y_1}(M \otimes F)$$

7) 판매자는 핑거프린트가 삽입된 암호화된 콘텐츠 $HE_{y_1}(\overline{M})$을 구매자에게 보내고 데이타베이스에 $y_1, V, k, C, Sig(H(C))$를 저장해 놓는다.
8) 구매자는 익명 공개키 y_1에 대한 개인키 x_1을 이용하여 판매자로부터 받은 $HE_{y_1}(\overline{M})$을 복호화하여 핑거프린트가 삽입된 콘텐츠를 얻는다.

$$\overline{M} = HD_{x_1}(HE_{y_1}(\overline{M}))$$
$$= M' \otimes F$$
$$= M \otimes V \otimes F$$

3.4 재배포자의 신원확인

신원확인 프로토콜은 판매자가 불법적으로 재배포된 콘텐츠 $\overline{M}$을 발견하였을 경우에 수행된다. 예를 들어 불법적으로 배포된 콘텐츠 $\overline{M}$이 판매자에 의해서 Kazaa [13]나 eDonkey[14]와 같은 P2P 환경에서 발견될 수 있다. 이때 공모 공격에 의하여 변경된 $\overline{M}$ 또는 $\hat{M}$와 같은 복사본 역시 인터넷상에서 찾을 수 있다. 이러한 경우 신원확인 프로토콜에서 콘텐츠 $\overline{M}$의 원 소유주나 $\hat{M}$을 생성해 낸 공모자들을 찾아내어 신원을 확인한다.

프로토콜 3 (신원확인 프로토콜)

불법적으로 배포된 콘텐츠 $\overline{M}$ 또는 $\hat{M}$이 발견되었을 때, 판매자는 다음의 프로토콜을 수행한다.

1) 판매자는 재배포된 콘텐츠에서 핑거프린트 U를 추출해낸다.
2) 판매자는 추출된 핑거프린트 U와 자신의 데이타베이스에 저장되어 있는 핑거프린트들 중에 유사

도가 높은 핑거프린트를 찾아서 그 핑거프린트에 해당하는 정보들을 찾아낸다. 판매자는 불법복제의 증거 pf를 추출된 핑거프린트, 구매자의 익명 공개키와 개인키, 암호화된 핑거프린트로 구성하여 재판관에게 보낸다.

$$pf = < U, y_1, k, C, Sig(H(C)) >$$

3) 재판관은 pf값들과 핑거프린트 인증센터의 공개키를 이용하여 서명 $Sig(H(C))$이 올바른지를 확인한다. 서명이 확인되면 핑거프린트 인증센터에게 익명 공개키 y_1에 대한 인증서와 핑거프린트를 요청한다. 재판관은 익명 공개키의 인증서를 검증하고 나서 핑거프린트를 구매자의 익명 공개키로 암호화한 값과 C를 비밀키 k로 복호화한 값이 맞는지 확인한다. 값이 일치하면 재판관은 등록 센터에게 익명 공개키 y_1에 대한 구매자의 실제 아이디를 요청한다.

4. 결과 및 분석

본 논문에서 제안한 핑거프린팅 기법은 판매자가 핑거프린트가 삽입된 콘텐츠를 알 수 없으며 구매자가 재배포하기 전에는 구매자를 찾아낼 수 없기 때문에 비대칭성과 익명성을 만족한다. 본 논문에서는 삽입된 구매자의 핑거프린트가 공모공격에 안전하고 재배포된 데이타로부터 증거값을 찾을 수 있다는 안전성을 가정한다.

□ 추적성

핑거프린트를 삽입하는 삽입 기법의 특성에 근거하여, 최대 공모 공격의 크기를 넘지 않거나 공모하여 재배포된 디지털 데이타가 원래의 데이타와 충분히 비슷한 경우에, 판매자는 핑거프린트를 추출하는 알고리즘의 정의에 입각하여 구매자의 핑거프린트를 추출해낼 수 있다.

구매자는 핑거프린팅 프로토콜 단계에서 핑거프린트 인증센터가 생성한 핑거프린트가 무엇인지 알 수 없다. 핑거프린트 인증센터는 구매자의 핑거프린트를 구매자의 익명 공개키를 이용하여 암호화하고, 이를 판매자만 복호화할 수 있도록 다시 암호화하기 때문에 구매자는 자신의 핑거프린트가 무엇인지 알 수 없다. 따라서 핑거프린트가 삽입된 컨텐츠 $item'$에서 자신의 핑거프린트 F를 제거할 수 없다. 또한 구매자는 판매자로부터 디지털 데이타를 구매하기 전에 등록 센터에 자신의 아이디를 등록하고 이에 대한 정당한 인증서를 받아야 핑거프린트 인증센터로부터 핑거프린트를 받을 수 있다. 판매자가 재배포된 데이타를 발견하면 판매자는 재배포된 컨텐츠로부터 핑거프린트를 추출해 내고, 핑거프린트를 이용하여 구매자의 익명 공개키 쌍과 구매자의 신원을 확인하여 재배포자를 추적할 수 있다. 따라서 판매자는 구매자로부터 구매자의 정당한 정보를 획득하지 못한 경우 디지털 데이타를 구매자에게 주지 않을 수 있으며, 재배포된 데이타에 대해서는 재배포자를 언제든지 추적할 수 있다. 또한

□ 견고성

핑거프린팅 프로토콜에서 판매자가 핑거프린트를 콘텐츠에 삽입할 때 Cox의 알고리즘[15]과 같이 공격에 안전한 알고리즘을 이용한다. 공격자가 삽입된 핑거프린팅 정보에 손상을 가하기 위하여 행하는 모든 조작에 대하여 본 논문에서 제안한 핑거프린팅 기법이 잘 견디어 내는지에 대한 견고성은 알려진 알고리즘의 견고성에 기인한다.

□ 비대칭성

핑거프린트 인증센터는 판매자에게 보낼 핑거프린트를 구매자의 익명 공개키를 이용하여 암호화한 $HE_{y_1}(F)$를 보내기 때문에 판매자는 컨텐츠에 삽입하는 구매자의 핑거프린트가 무엇인지 알 수 없다. 여기서의 핑거프린트 인증센터와 같은 신뢰기관은 일반적으로 인증기관에 의해서 요구되는 일반적인 동의나 일치가 전제되어 있어야 한다. 핑거프린트 인증센터는 제 3의 신뢰기관으로 정직한 구매자에 대해서는 그의 신원과 구매자의 핑거프린트가 무엇인지 밝히지 않는다고 가정한다. 비정직한 판매자는 핑거프린트 인증센터에게 구매자의 핑거프린트가 어떤 것인지를 요구할 수 없다.

□ 공모허용

구매자의 핑거프린트는 공모공격에 안전하다고 알려진 기법[9,10]들을 이용하여 구성함으로써 다수의 구매자들이 서로 공모하여 콘텐츠 내에 핑거프린트를 지우거나 새로운 정보를 삽입하여 재분배하는 경우에도 공모자나 구매자의 신원을 확인할 수 있다.

□ 익명성

구매자는 먼저 등록 센터에 자신의 아이디에 대한 익명 공개키를 등록하고 익명 공개키만을 이용하여 핑거프린트 인증센터로부터 핑거프린트를 제공받는다. 따라서 핑거프린트 인증센터는 구매자의 실제 아이디는 알지 못한다. 또한 구매자는 등록된 익명 공개키를 이용하여 구매활동을 하기 때문에 판매자는 구매자의 신원은 알지 못한 채 거래를 수행하게 된다. 핑거프린팅 프로토콜 단계에서 판매자는 구매자의 익명 공개키를 받는다. 판매자가 구매자의 공개키 y_B를 찾기 위해서는 x_2를 알아야 한다. 그러나 암호 알고리즘이 안전하다면 x_2를 알아내기 위해서는 $\log_g y_B$를 계산해야만 한다. 그러나 이산대수문제를 해결하는 선형시간 알고리즘이 존재하지 않기 때문에 공격자는 x_2를 계산해낼 수 없다. 따라서 구매자는 불법적인 행위를 하지 않는 한 자신의 신원을

표 1 효율성 분석

		Ju의 기법	Choi의 기법	Goi의 기법	제안한 기법
등록	누승연산	9	8	0	2
	통신횟수	5	5	5	4
핑거프린팅	통신횟수	2	2	2	2
신원확인	구매자 참여	O	O	O	X

알리지 않고 익명 공개키를 이용하여 익명적으로 컨텐츠를 구매할 수 있다.

□ 효율성

구매자는 자신의 익명 공개키 쌍을 생성하기 위하여 임의의 두 수 x_1, x_2을 선택하고 이 값들의 정당성을 인정받는다. 기존 기법들처럼 영지식 증명을 이용하지 않기 때문에 등록 프로토콜에서 효율성을 향상시킬 수 있다. 기존 기법들과 제안한 기법의 효율성을 비교하기 위하여 구현시 계산에 많은 시간과 메모리가 소요되는 누승연산과 통신횟수를 비교할 수 있다. 제안한 기법을 Ju의 기법과 Choi의 기법과 비교하였을 때 등록 프로토콜에서 누승연산과 통신회수가 현저히 줄었으며 Goi의 기법보다 통신횟수가 향상되었다. 또한 제안한 기법은 신원확인 프로토콜이 수행될 때 구매자가 참여할 필요가 없는 장점이 있다. 각 프로토콜 단계에서 통신횟수나 누승연산의 횟수를 기존 기법과 비교하면 표 1과 같이 제안한 기법에서 효율성이 향상됨을 볼 수 있다.

그러나 제안한 기법은 구매자의 익명 공개키를 등록하는 등록기관과 핑거프린트를 생성하는 핑거프린트 인증센터를 분리하여 신뢰기관으로 유지해야 하는 단점이 있다.

5. 결 론

본 논문에서는 신뢰기관에서 구매자의 고유 핑거프린트를 생성해 내고 판매자는 핑거프린트의 내용은 알지 못한 채 콘텐츠에 삽입하여 콘텐츠를 판매하게 된다. 따라서 구매자는 핑거프린트가 삽입된 콘텐츠를 알 수 있으나 판매자는 이를 알 수 없도록 하기 위하여 준동형의 암호를 이용하여 설계하였다. 또한 구매자는 등록시 자신의 익명 공개키 쌍을 등록하고 이를 이용하기 때문에 판매자나 핑거프린트 인증센터는 구매자의 신원을 알 수 없어 재배포자로 고발되기 전까지는 구매자의 익명성이 보장된다.

제안한 기법은 기존에 제안된 기법보다 등록과 핑거프린팅 프로토콜에서 누승연산의 횟수나 통신 횟수에 효율성을 보였고, 신원확인 프로토콜을 수행할 경우 구매자가 참여하지 않아도 되는 장점이 있다. 그러나 등록센터와 핑거프린트 인증센터의 두개의 신뢰기관을 유지해야 한다.

참 고 문 헌

[1] R. Wagner, "Fingerprinting," IEEE Symposium on Security and Privacy, Oakland, pp. 18-22, 1983.

[2] S. Katzenveisser and F. Petitcolas, Information Hiding, "Techniques for steganography and digital watermarking," Artech House, 2000.

[3] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," In Advances in Cryptology - EUROCRYPT'97, LNCS 1233, pp. 88-102, 1997.

[4] J. Camenish, "Efficient anonymous fingerprinting with group signature," Asisacrypt 2000, LNCS 1976, pp. 415-428, 2000.

[5] J. Domingo-Ferrer, "Anonymous fingerprinting of electronic information with automatic identification redistributors," IEE Electronic Letters, Vol. 43, No. 13, 1998.

[6] M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting scheme with high enciphering rate," INDOCRYPT'01, LNCS 22247, pp. 30-39, 2001.

[7] G. Blakley, C. Meadow and G. B. Purdy, "Fingerprinting long forgiving messages," In Advances in Cryptology - CRYPTO'85, LNCS 218, pp. 180-189, 1986.

[8] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," In Advances in Cryptology - EUROCRYPT'96, LNCS 1070, pp. 84-95, 1996.

[9] H. Ju, H. Kim, D. LEE and J. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," International Conference on Information and Communication Security(ICICS'02), LNCS 2587, pp. 421-432, 2003.

[10] J. G. Choi, K. Sakurai and J. H. Park, "Does it need trusted third party? Design of buyer-seller watermarking in digital contents," Applied Cryptography and Network Security(ACNS'03), LNCS 2846, pp. 265-279, 2003.

[11] D. Chaum, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations," In Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 127-141, 1987.

[12] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Transactions on Image Processing, Vol. 10, No. 4, pp. 643-649, 2001.

[13] http://www.kazaa.com

[14] http://www.edonkey2000.com

[15] I. J. Cox, J. Kilian, T. Leighton and T. Shamnon,

"Secure spread spectrum watermarking for image, audio and video," IEEE Transactions on Image processing, vol.6, no 12, pp. 1673-1678, 1997.

용 승 림

1998년 2월 이화여자대학교 컴퓨터학과 학사. 2000년 2월 이화여자대학교 컴퓨터학과 석사. 2006년 이화여자대학교 과학기술대학원 박사, 현 이화여자대학교 컴퓨터정보통신공학부 전임강사. 관심분야 - 정보보호, 컨텐츠보호, 생체정보보호 등

이 상 호

1979년 서울대학교 계산통계학과 이학사 1981년 한국과학기술원 전산학과 이학석사. 1987년 한국과학기술원 전산학과 공학박사. 1990년 미국 일리노이대학교 전산학과 방문교수. 현 이화여자대학교 컴퓨터학과 교수