신뢰기관을 이용한 비대칭적 핑거프린팅 기법

용승림° 이상호
이화여자대학교
dragon°@ewhain.net shlee@ewha.ac.kr

Asymmetric Fingerprinting Scheme with TTP

Seunglim Yong° Sang-Ho Lee
Ewha Womans University

요 약

디지털 형식으로 저장되어 있는 데이터의 불법적인 복사와 재분배는 전자상거래 상에서 디지털 컨텐츠를 판매하는 상점에게 매우 큰 문제가 된다. 핑거프린팅 기법은 암호학적인 기법들을 이용하여 디지털 컨텐츠를 불법적으로 재배포한 사용자를 찾아냄으로써 저작자의 저작권을 보호한다. 비대칭적 핑거프린팅 기법은 대칭적인 기법과 달리 사용자만이 핑거프린트가 삽입된 컨텐츠를 알 수 있어 사용자가 컨텐츠를 재배포했을 경우만 사용자가 고발되는 기법이다.

본 논문에서는 신뢰기관을 이용한 비대칭적 핑거프린팅 기법을 제안한다. 사용자의 핑거프린트는 신뢰기관이 생성하고 사용자의 익명공개키 쌍과 준동형의 암호를 이용하여 컨텐츠에 핑거프린트를 삽입함으로써 상점은 사용자의 핑거프린트를 알 수 없도록 하여 비대칭성을 만족하며 컨텐츠가 재배포되었을 경우 상점은 신뢰기관으로부터 정보를 받아 재배포자를 추적할 수 있다.

1. 서 론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 전자상거래가 활발해지고 디지털 데이터의 확산 및 보급이 일반화되고 있다. 그러나 이러한 데이터들은 디지털이라는 속성으로 인하여 누구나 손쉽게 불법적인 복제를 통해서 이들을 획득할 수 있게 되고, 이 때문에 저작권 문제가 야기되고 있다. 따라서 정보기반 전자 상거래에서 디지털 데이터의 저작권 보호는 아주 중요한 문제가 되었다.

핑거프린팅 기법은 디지털 데이터의 저작권을 보호하기 위해 데이터의 복사 자체를 막는 암호학적인 기법이 아니라 암호학적인 기법들을 이용하여 디지털 데이터를 불법적으로 재분배한 사람을 찾아내는 기법이다[1,2]. 저작권 보호에 관한 규칙을 어기고 데이터를 불법적으로 분배하는 사람을 재배포자(traitor)라 한다. 핑거프린팅 기법은 데이터가 불법적으로 재배포 되었을 때 상점이 그 데이터를 구매한 재배포자를 식별할 수 있게끔 함으로써 디지털 저작권을 보호한다. 핑거프린팅 기법에서 정직한 사용자는 불법적인 행위를 하기 전까지는 그의 신원이 알려져서는 안된다[3,4,5,6]. 즉, 특정한 사용자의 익명성은 불법적인 행위를 수행하기 전까지는 보장되어야 한다.

대칭적인 기법은 상점이 서로 다른 컨텐츠의 복사본들을 각 사용자에게 나누어주고 데이터가 재배포 되었을 경우 그 복사본을 어떤 사람에게 나누어준 것인지를 찾아내어 재배포자를 찾아내는 방법이다[1,2,7]. 따라서 상점과 사용자가 모두 복사본을 알고 있게 된다. 이 기법의 문제점은 악의적인 상점이 복사본을 재배포하고 정직한 사용자를 재배포자로 고발할 수 있다는 것이다. 이러한 경우 사용자는 자신이 컨텐츠를 재배포하지 않았음을 증명할 수 있는 방법이 전혀 없다.

이러한 문제점을 해결한 것이 비대칭적인 핑거프린팅 기법이다[8]. 비대칭적인 기법은 사용자와 상점이 마크를 삽입하는 과정을 프로토콜로 수행함으로써 핑거프린트가 삽입된 데이터를 사용자만이 알 수 있고 상점은 핑거프린트된 데이터를 알 수 없도록 한다.

본 논문에서는 준동형의 암호를 이용하여 좀 더 효율적인 비대칭적 핑거프린팅 기법을 제안한다.

2. 관련연구 및 용어정리

2.1 준동형의 암호

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

2.2 용어정리

본 논문에 참여하는 참여자와 사용되는 기호는 다음과 같다.

- 등록센터(RA) : 사용자가 구매를 하기 전에 자신의 정보를 등록해 놓는 제3의 신뢰기관이다.
- 핑거프린트 생성센터(FA) : 핑거프린트를 생성하는 제3의 신뢰기관이다.
- 상점(M) : 멀티미디어를 판매하는 개체이다.
- 사용자(C) : 멀티미디어 컨텐츠를 구매하는 개체로서 구매한 컨텐츠를 불법적으로 재배포할 수 있는 절대적으로 신뢰할 수 없는 개체이다.
- W : 핑거프린트

· M : 핑거프린트가 삽입될 원본 컨텐츠
· M' : 핑거프린트가 삽입된 컨텐츠
· E_* /D_*: 공개키 암호시스템 암호화/복호화 알고리즘
· HE/DE : 준동형의 성질을 만족하는 공개키 암호시스템

3. 핑거프린팅 기법

본 장에서는 안전한 비대칭적 핑거프린팅 기법에 대하여 설명한다. 본 논문에서 제안하는 핑거프린팅 기법은 등록, 핑거프린팅 및 신원확인 프로토콜로 구성되어 있다.

3.1 사용자 등록 프로토콜

사용자와 등록센터는 모두 공개키와 비밀키 쌍을 가지고 있다고 가정한다. 사용자의 비밀키는 x_B이고 공개키는 $y_B = g^{x_B}$이다. 등록센터의 비밀키는 등록센터의 공개키를 이용하여 인증서를 검증할 수 있는 인증서를 생성하는데 이용된다. 또한 두 개체의 공개키는 인증되어 있다고 가정한다.

1) 사용자는 자신의 익명 공개키 쌍을 생성하기 위하여 $x_1 + x_2 = x_B$인 임의의 두 수 x_1, x_2 를 선택한다. 사용자는 y_B, $y_1 (y_1 = g^{x_1})$와 $E_{RC}(x_2)$를 계산하여 등록센터에게 보낸다. 사용자는 영지식증명을 이용하여 자신이 x_1을 가지고 있음을 등록센터에게 증명한다 [10]. 위에서 생성된 공개키, 비밀키 쌍 (x_1, y_1)이 익명공개키 쌍으로 이용된다.
2) 등록센터는 자신의 비밀키를 이용하여 $E_{RC}(x_2)$를 복호화하고 $y_2 = g^{x_2}$를 계산한 후 $y_1 y_2 = y_B$인지 확인한다. 값이 맞을 경우 등록센터는 사용자에게 y_1에 대한 인증서 $Cert(y_1)$를 보내준다.

3.2 핑거프린팅 프로토콜

사용자는 상점에게 자신의 익명공개키 쌍과 그의 인증서를 상점에게 주고 상점은 이를 이용하여 사용자의 핑거프린트를 핑거프린트 생성센터로부터 받아온다.

1) 사용자는 상점에게 $y_1, Cert(y_1)$을 보낸다.
2) 상점은 등록센터의 공개키를 이용하여 $Cert(y_1)$이 맞는지 확인한다. 정당한 서명으로 검증이 되면 상점은 이를 핑거프린트 생성센터에게 보낸다.
3) 핑거프린트 생성센터는 상점으로부터 받은 키와 인증서를 저장해 두고 공모공격으로부터 안전한 핑거프린트 W를 생성한다. 핑거프린트 생성센터는 공개키 y_1을 이용하여 $HE_{y_1}(W)$을 상점에게 보낸다.
4) 상점은 사용자의 익명공개키 y_1을 이용하여 M을 암호화한 $HE_{y_1}(M)$에 핑거프린트 생성센터로부터 받은 암호화된 핑거프린트 $HE_{y_1}(W)$를 임베드한다. 준동형의 암호화 성질에 의해서 암호화된 핑거프린트는 컨텐츠에 삽입될 수 있다.

$$HE_{y_1}(M') = HE_{y_1}(M) \otimes HE_{y_1}(W) = HE_{y_1}(M \otimes X)$$

5) 사용자는 자신의 익명비밀키 x_1을 이용하여 상점으로부터 받은 $HE_{y_1}(M')$을 복호화하여 핑거프린트가 삽입된 컨텐츠를 얻는다.

$$HD_{x_1}(HE_{y_1}(M')) = M' = M \otimes X$$

3.3 신원확인 프로토콜

상점이 불법적으로 재배포된 컨텐츠 M'을 발견하였을 경우 상점은 컨텐츠로부터 핑거프린트를 추출하고 이를 핑거프린트 생성센터에 보낸다. 핑거프린트 생성센터는 자신이 데이터베이스에서 핑거프린트와 해당하는 공개키를 찾아 이를 등록센터에 보내어 사용자의 신원을 확인한다.

1) 만약 M'이 재배포된 것이 발견되면 상점은 핑거프린트를 추출해 내는 알고리즘을 이용하여 핑거프린트 W를 추출해 낸다.
2) 상점은 추출해낸 핑거프린트 W를 핑거프린트 생성센터에 보낸다.
3) 핑거프린트 생성센터는 자신의 데이터베이스에서 상점으로부터 받은 핑거프린트 W와 그에 해당하는 공개키 y_1, 인증서 $Cert(y_1)$를 추출해내고 이를 등록센터에 보낸다.
4) 등록센터는 등록 데이터베이스로부터 공개키 y_1에 해당하는 사용자가 누구인지를 확인한다.

4. 결과 및 분석

본 논문에서 제안한 핑거프린팅 기법은 상점이 핑거프린트가 삽입된 컨텐츠를 알 수 없기 때문에 비대칭성을 만족한다. 핑거프린트를 삽입하는 삽입 기법이 공모공격에 안전하고 재배포된 데이터로부터 증거값을 찾을 수 있다는 안전성을 가정한다.

4.1 상점에 대한 안전성

핑거프린트를 삽입하는 삽입기법의 특성에 근거하여, 최대 공모공격의 크기를 넘지 않거나 공모하여 재배포된 디지털 데이터가 원래의 데이터와 충분히 비슷한 경우에, 상점은 핑거프린트를 추출하는 알고리즘의 정의에 입각하여 사용자의 핑거프린트를 추출해낼 수 있다.

사용자는 핑거프린팅 프로토콜 단계에서 핑거프린트 생성센터가 생성한 핑거프린트가 무엇인지 알 수 없기 때문에 핑거프린트가 삽입된 컨텐츠에서 핑거프린트를 제거할 수 없다. 또한 사용자는 상점으로부터 디지털 데이터를 구매하기 전에 등록센터에 자신의 아이디를 등록하고 이에 대한 등록센터의 정당한 서명이 있어야 핑거프린팅 프로토콜을 수행할 수 있다. 상점이 재배포된 데이터를 발견하면 상점은 재배포된 컨텐츠로부터 핑거프린트를 추출해 내고, 핑거프린트를 이용하여 사용자의 익명 공개키 쌍과 사용자의 신원을 확인하여 재배포자를 추적할 수 있다. 따라서 상점은 사용자로부터 사용자의 정당한 정보를 획득하지 못한 경우 디지털 데이터를 사용자에게 주지 않을 수 있으며, 재배포된 데이터에 대해

서는 재배포자를 언제든지 추적할 수 있다 .만약 재배포자가 신원확인 프로토콜을 수행한 결과 핑거프린트 생성센터로부터 발각되면 그 사용자는 블랙리스트에 올리고 더 이상 그 사용자에게 컨텐츠를 판매하지 못하도록 조치할 수 있다.

4.2 사용자에 대한 안전성

핑거프린트 생성센터는 상점에게 핑거프린트를 사용자의 익명 공개키를 이용하여 암호화하여 보내기 때문에 상점은 컨텐츠에 삽입하는 사용자의 핑거프린트가 무엇인지 알 수 없다. 또한 사용자는 등록센터에 자신의 익명 공개키를 등록하고 이를 이용하여 구매활동을 하기 때문에 상점은 사용자의 신원은 알지 못한 채 거래를 수행하게 된다. 등록센터는 제 3의 신뢰기관으로 정직한 사용자에 대해서는 그의 신원을 밝히지 않는다고 가정한다.

핑거프린팅 프로토콜 단계에서 상점은 사용자의 익명 공개키와 그에 대한 인증서만을 받는다. 사용자의 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 상점은 사용자를 가장하여 컨텐츠를 재배포 할 수 없고 정직한 사용자는 재배포자로 고발될 수 없다.

여기서의 핑거프린트 생성센터와 같은 신뢰기관은 일반적으로 인증기관에 의해서 요구되는 일반적인 동의나 일치가 전제되어 있어야 한다. 인증기관이 서명을 부인하지 못하는 방식으로 인증기관의 정직성을 인정받듯이 핑거프린트 생성센터도 사용자의 핑거프린트를 이용하여 컨텐츠를 재배포하지 않는다는 정직성을 인정받아야 한다. 비정직한 상점은 핑거프린트 생성센터에게 사용자의 핑거프린트가 어떤 것인지를 요구할 수 없다.

5. 결론

본 논문에서는 신뢰기관에서 사용자의 고유 핑거프린트를 생성해 내고 상점은 핑거프린트의 내용은 알지 못한 채 컨텐츠에 삽입하여 컨텐츠를 판매하게 된다. 따라서 사용자는 핑거프린트가 삽입된 컨텐츠를 알 수 있으나 상점은 이를 알 수 없는 비대칭성을 만족하며 이는 준동형의 암호를 이용하여 구현될 수 있었다.

또한 사용자는 등록시 자신의 익명공개키 쌍을 등록하고 이를 이용하기 때문에 상점이나 핑거프린트 생성센터는 사용자의 신원을 알 수 없어 재배포자로 고발되기 전까지는 사용자의 익명성이 보장된다.

6. 참고문헌

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

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," In Advances in Cryptology - CRYPTO '95, LNCS 963, pp. 452-465, 1995.

[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] W. Trappe, M. Wu and K. Liu, "Collusion -resistant fingerprinting for multimedia," IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 4, pp. 3309-3312, 2002.

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

[9] N.Memon and P.W.Wong, "A buyer-seller watermarking protocol," IEEE Transactions on image processing, vol.10 no.4. pp. 643-649, 2001.

[10] 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.