韓國컴퓨터情報學會 論文誌
第14卷 第7號, 2009. 7.

2009-14-7-3-5

신뢰기관 비참여의 핑거프린팅 기법에 관한 연구

용 승 림*

A Study on the Fingerprinting scheme without Trusted Third Party

Seunglim Yong*

요 약

핑거프린팅 기법은 디지털 데이터의 저작권을 보호하기 위하여 암호학적인 기법들을 이용한 방법이다. 디지털 데이터에 구매자 각각의 유일한 핑거프린트를 삽입하고 이를 이용하여 디지털 데이터를 불법적으로 재배포한 구매자를 찾아내게 된다. 핑거프린팅 기법은 구매자의 프라이버시 보호를 위하여 비대칭성이 보장되어야 한다.

본 논문에서는 대칭키 암호를 기반으로 하지만 비대칭성 만족을 위하여 신뢰기관의 참여가 필요하지 않은 핑거프린팅 기법에 대하여 제안한다. 제안한 프로토콜은 대칭키 암호를 기반으로 하지만 신뢰기관이 구매자의 핑거프린트 생성에 참여하지 않으면서도 비대칭성을 만족한다. 신뢰기관의 비 참여로 인하여 제안한 프로토콜에서는 신뢰기관의 관리가 필요 없으며 구매자는 공모 공격으로부터 안전할 수 있다.

Abstract

Fingerprinting scheme is a technique which supports the copyright protection to track redistributors of digital content using cryptographic techniques. These schemes enable the original merchant to identify the original buyer of the digital data by embedding fingerprints into digital contents. Asymmetric property of fingerprinting schemes is important to keep the buyer's privacy.

In this paper, we propose a symmetric encryption based fingerprinting protocol without trusted third party. Our scheme enables the reduction of computational costs for the encryption using symmetric key encryption scheme. Since a trusted third party doesn't take part in making the fingerprint of each buyer, the protocol doesn't need to control the trusted third party and it is more secure against collusion attack.

▸ Keyword : 콘텐츠 보호(content protection), 핑거프린팅 기법(fingerprinting scheme), 신뢰기관(Trusted Third Party), 대칭 암호(symmetric encryption)

• 제1저자 : 용승림
• 투고일 : 2009. 05. 12, 심사일 : 2009. 05. 18, 게재확정일 : 2009. 07. 24.
* 인하공업전문대학 컴퓨터시스템과 교수
※ 이 논문은 2008학년도 인하공업전문대학 교내연구비지원에 의하여 연구되었음.

Ⅰ. 서 론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 전자상거래가 활발해지고 디지털 데이터의 확산 및 보급이 일반화되고 있다. 디지털 데이터는 디지털의 속성으로 인하여 누구나 쉽게 복사, 배포를 할 수 있기 때문에 이로 인한 저작권 문제가 야기되어왔다. 따라서 정보 기반의 전자 상거래에서 디지털 데이터의 저작권 보호는 아주 중요한 문제이다. 이에 저작권 보호를 위하여 디지털 데이터의 불법 복제를 방지하는 방법이나 재배포자를 추적하는 기술 등 저작권 보호에 관한 다양한 연구가 진행되고 있다.

핑거프린팅 기법은 저작권 보호를 위하여 데이터의 복사 자체를 막는 것이 아니라 디지털 데이터를 불법적으로 재배포한 사람을 찾아내는 방법을 제공한다[1]. 핑거프린트라는 구매자마다의 유일한 식별정보를 디지털 데이터에 삽입하고, 이를 불법적인 복제물이 발견되었을 때 구매자를 식별하는 정보로 이용한다. 핑거프린팅 기법은 크게 대칭적 핑거프린팅 기법과 비대칭적 핑거프린팅 기법으로 분류된다. 대칭적 핑거프린팅 기법은 판매자가 핑거프린트를 생성하고 콘텐츠에 삽입도 하기 때문에 판매자에 의하여 합법적인 구매자도 재배포자로 오인될 수 있는 약점이 있다[2]-[3]. 반면 비대칭적 핑거프린팅 기법은 핑거프린트를 삽입하는 주체는 판매자이지만 핑거프린팅된 콘텐츠를 판매자는 볼 수 없고 구매자만이 볼 수 있는 방법이다[4]-[5]. 따라서 정당한 구매자는 판매자에 의하여 재배포자로 오인되지 않는다.

비대칭적 핑거프린팅 기법은 공개키 암호 알고리즘에 기반을 둔 방법과 대칭키 암호 알고리즘에 기반을 둔 방법이 있다. 공개키 암호 알고리즘에 기반을 둔 방법들은 대부분 대용량의 콘텐츠가 공개키 암호 알고리즘으로 암·복호화되기 때문에 효율성 측면에서 단점이 있다. 반면 대칭키 암호 알고리즘을 기반으로 한 기법들은 콘텐츠 암호화를 대칭키 암호 알고리즘을 기반으로 하기 때문에 효율성은 향상시킬 수 있다. Balleste 등과 Kurobayashi등이 제안한 논문에서는 대칭 암호 시스템을 이용하여 공개키 암호 기반보다는 효율성을 향상시켰다[6]-[7]. 그러나 핑거프린팅 기법에서 프로토콜 상의 중요한 많은 부분을 신뢰기관(TTP:Trusted Third Party)에 의존하고 있으며, 신뢰기관의 의존도가 줄어든 Kurobayashi의 논문에서도 구매자의 식별정보를 신뢰기관이 생성하기 때문에 판매자와의 공모를 통하여 정직한 구매자를 고발할 수 있어 구매자의 안전성에 문제가 발생될 수 있다.

본 논문에서는 신뢰기관을 이용하지 않는 대칭키 암호 기반의 핑거프린팅 기법을 제안한다. 제안된 시스템은 디지털 데이터를 대칭 암호 시스템을 이용하여 암호화하기 때문에 공개키 암호 기반의 핑거프린팅 기법에서의 암호화에 대한 효율성 문제를 개선할 수 있다. 또한 일반적인 대칭형 암호 기반의 시스템에서 비대칭성을 만족시키기 위한 신뢰기관을 두지 않고 프로토콜이 설계되기 때문에 판매자와 신뢰기관 사이의 공모 공격으로부터 구매자를 보호하여 구매자의 안전성을 강화할 수 있다.

Ⅱ. 기존 연구

1. 관련연구

1.1 핑거프린팅 기법

핑거프린팅은 디지털 콘텐츠의 저작권 보호를 위한 암호학적인 기법으로 디지털 데이터를 불법적으로 재분배한 사람을 찾아내어 불법적 재배포 행위를 막을 수 있다. 핑거프린팅 기법은 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[8]. 따라서 모든 판매된 콘텐츠들은 모두 동일한 워터마크가 삽입되어 있다. 반면, 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 상호 교환 프로토콜에 의하여 핑거프린트를 삽입하게 된다. 따라서 비대칭 기법들은 프로토콜이 수행되는 동안에 구매자가 자신의 비밀 정보를 삽입할 수 있으며 프로토콜이 끝나면 단지 사용자만이 데이터에 삽입된 핑거프린트를 알 수 있다. 익명성 보장 비대칭적 기법은 사용자의 프라이버시를 위하여 삽입된 핑거프린트를 모를 뿐 아니라 사용자가 데이터를 재배포하지 않는 한 사용자의 익명성도 철저히 보장되는 기법이다[9].

1.2 대칭 암호 기반 핑거프린팅 기법

핑거프린팅 기법은 구매자의 프라이버시를 위하여 구매자가 자신의 비밀 정보를 삽입하고 구매자만이 삽입된 핑거프린트를 알 수 있도록 비대칭성이 만족되어야 한다. 비대칭성 만

족을 위한 기법들에는 준동형 암호라는 공개키 암호를 기반으로 하는 기법들이 있다. 이러한 기법들은 공개키 암호 기반으로 프로토콜이 구성되어 있기 때문에 비대칭성은 만족할 수 있다. 그러나 콘텐츠가 공개키 암호를 기반으로 암호화되기 때문에 암·복호화하는 데에 많은 시간이 걸리는 단점이 있다. 이러한 단점을 해결하기 위하여 콘텐츠를 암호화하고 복호화할 때 대칭 암호를 기반으로 하는 핑거프린팅 기법들이 제안되었다.

대칭 암호 기반의 핑거프린팅 기법은 대칭 암호 시스템을 이용하는 두 통신 개체가 키를 나누어 가져야 하는 특성이 있다. 이러한 특성은 구매자만이 핑거프린트가 삽입된 콘텐츠를 알도록 하는 비대칭성을 제공하기 어렵다. 따라서 Balleste, Kurobayashi의 논문들은 신뢰기관을 기반으로 하여 콘텐츠에 삽입되는 핑거프린트 정보를 신뢰기관이 삽입하도록 프로토콜을 설계하여 비대칭성을 만족시켰다[6]-[7]. 그러나 신뢰기관 기반의 핑거프린팅 기법에서는 구매자의 중요 정보를 신뢰기관이 생성하기 때문에 구매자의 안전성이 신뢰기관의 신뢰성에 크게 의존하게 된다. 따라서 안전한 프로토콜이 되기 위해서는 신뢰기관을 엄격하게 운영해야 할 필요가 있으며 그렇지 않을 경우에 구매자는 판매자와 신뢰기관 사이의 공모 공격으로 인하여 정직한 구매자가 재배포자로 오인될 수 있는 단점이 있다.

III. 본 론

1. 프로토콜

본 절에서 신뢰기관을 이용하지 않는 대칭 암호 기반의 핑거프린팅 기법의 상세 프로토콜에 대하여 기술한다. 구매자는 프로토콜 상에서 이용할 익명 공개키를 등록한 후 콘텐츠를 복호화할 키를 분배받고 판매자와 구매 프로토콜을 진행하게 된다. 각각의 자세한 프로토콜과 프로토콜에 참여하는 참여자, 그리고 참여자의 역할은 다음과 같다.

□ 참여자의 역할

프로토콜의 참여자는 등록 센터, 키 관리 센터, 구매자, 판매자, 그리고 재판관이다. 각 참여자의 역할은 다음과 같다.

- 등록 센터(RC): 등록 센터는 구매자와 등록 프로토콜을 수행하여 구매자의 익명 공개키 쌍을 등록받고 익명 공개키 쌍에 대한 인증서를 발급한다. 등록센터는 다른 참여자와 공모를 수행하지 않는 기관으로 가정한다.
- 키 관리 센터(KMC): 키 관리 센터는 콘텐츠 암호화에 필요한 키를 생성하고 이를 프로토콜을 통하여 판매자와 구매자에게 제공하는 역할을 수행한다.
- 구매자(B): 구매자는 익명 공개키 쌍을 등록 센터에 등록하고 구매 행위를 할 때 등록한 익명 공개키 쌍을 이용한다. 구매자는 일반 CA(Certificate Authority)로부터 인증 받은 공개키 쌍 (x_B, y_B)을 가지고 있다.
- 판매자(C): 판매자는 구매자와 핑거프린트 프로토콜을 수행하며, 구매자의 핑거프린트를 임의로 생성하고 이를 콘텐츠에 삽입한다.
- 재판관(J): 재배포가 발생되었을 때 판매자의 요청에 의하여 재배포자를 판단하는 기관이다.

제안한 핑거프린팅 프로토콜은 그림 1과 같이 익명 공개키 등록, 암호화 키 분배, 구매, 그리고 신원 확인의 네 가지 단계로 구성된다.

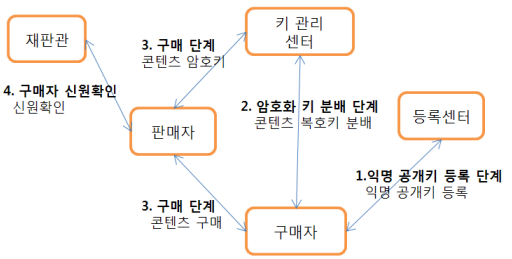

그림 1 핑거프린팅 참여자와 프로토콜 단계

자세한 단계별 프로토콜은 다음과 같다.

1.1 익명 공개키 등록 단계

구매자와 등록 센터는 일반 CA(Certificate Authority)로부터 인증 받은 공개키 쌍을 가지고 있다고 가정한다. 구매자의 비밀키는 x_B이고 공개키는 $y_B = g^{x_B}$이다. 등록 센터는 자신의 비밀키 x_R를 인증서를 생성하는데 이용한다. 등록 센터의 공개키는 모든 구매자에게 알려져 있으며 인증되어 있다고 가정한다.

1) 등록 센터는 임의의 값 $x_R \in_R Z_p$을 선택하여 $y_R = g^{x_R}$을 계산하여 y_R을 구매자에게 보낸다.

2) 구매자는 $x_1 + x_2 = x_B$를 만족하는 임의의 두 비밀값 $x_1, x_2 \in_R Z_p$를 선택한다. 구매자는 생성한 비밀값 x_1을 이

용하여 $y_1 = g^{x_1}$을 계산하고, 등록 센터로부터 받은 값과 자신의 비밀값 x_2를 이용하여 $Y = y_R^{x_2}$를 계산한다. 구매자는 등록 센터에게 위에서 계산한 값을 보낸다.

3) 등록 센터는 구매자에게 받은 y_1에 x_R값을 이용하여 $y_1^{x_R}$을 계산한다. 그리고 식 (1)과 같은 계산을 통하여 구매자의 익명 공개키의 유효성 여부를 확인한다.

$$\begin{aligned} Y \bullet y_1^{x_R} &= y_R^{x_2} \bullet y_1^{x_R} = g^{x_R x_2} \bullet g^{x_1 x_R} \\ &= g^{x_R(x_1+x_2)} \\ &= y_B^{x_R} \end{aligned} \quad (1)$$

4) 식 (1)이 참으로 확인되면 등록 센터는 구매자에게 인증서 $Cert(y_1)$을 보내준다. 인증서는 구매자의 공개키 y_1이 올바르게 생성되었고, 구매자의 익명 공개키가 등록되었음을 나타낸다.

1.2 암호화 키 분배 단계

암호화 키 분배 단계에서는 구매자가 콘텐츠 복호화를 수행할 때 필요한 t개의 키를 받는 프로토콜을 수행한다. 키 관리 센터는 구매자와 판매자에게 키를 분배하는 역할을 하는 참여자이지만 기존의 논문들과 다르게 키분배를 위하여 신뢰기관으로 관리해야 할 필요가 없다. 구매자는 콘텐츠 구매에 앞서 키 관리 센터와 키 분배 프로토콜을 진행하게 된다. 프로토콜을 통하여 구매자는 최종적으로 콘텐츠 복호화에 필요한 t개의 키로 구성된 키벡터 K_B를 얻어낸다.

1) 구매자는 콘텐츠 복호화에 사용될 키를 받기 위하여 먼저 익명 공개키 y_1과 $Cert(y_1)$을 키 관리 센터에게 보낸다.

2) 키 관리 센터는 t개의 서로 다른 키로 구성된 키 벡터 K_0, K_1을 수식 (2)의 과정을 통하여 생성한다.

$$\begin{aligned} K_0 &= \{k_{0,j} \mid 0 \le j \le t-1\} \\ K_1 &= \{k_{1,j} \mid 0 \le j \le t-1\} \end{aligned} \quad \cdots\cdots (2)$$

3) 키 관리 센터는 교환 암호 알고리즘에 사용할 키 S를 생성한다. 그리고 교환 암호 알고리즘 CE를 이용하여 (2)을 통하여 생성된 키벡터 K_i를 암호화한다. 암호화된 두 개의 키 벡터 C_0, C_1은 (3)과 같이 생성한다.

$$\begin{aligned} C_0 &= \{c_{0,j} \mid c_{0,j} = CE(S, k_{0,j}),\ 0 \le j \le t-1\} \\ C_1 &= \{c_{1,j} \mid c_{1,j} = CE(S, k_{1,j}),\ 0 \le j \le t-1\} \end{aligned} \quad (3)$$

4) 구매자는 익명 공개키를 생성할 때의 비밀값 x_1을 2진 수열로 바꾸어 t비트열 $L = \{l_0, ..., l_{t-1}\}$를 생성한다. 구매자는 비트열 L을 기반으로 C_i로부터 t개의 암호화된 키를 선택하여 벡터 $C' = (c'_0, c'_1, ..., c'_{t-1})$를 구성한다.

$$c'_j = \begin{cases} c_{0,j} & (l_j = 0) \\ c_{1,j} & (l_j = 1) \end{cases}, 0 \le j \le t-1 \quad \cdots (4)$$

5) C'을 생성한 후 구매자는 교환 암호에 사용될 비밀키 R을 생성한 후 교환 암호 알고리즘 CE를 이용하여 C'을 암호화한 $D = \{d_0, d_1, ..., d_{t-1}\}$를 생성한다.

$$d_j = CE(R, c'_j),\ 0 \le j \le t-1 \quad \cdots\cdots (5)$$

구매자는 생성된 D의 값에 익명 공개키 쌍을 이용하여 서명을 생성한 후 D와 서명을 키 관리 센터에게 보낸다.

6) 키 관리 센터는 서명을 확인하고, D를 비밀키 S를 이용하여 복호화하여 $U = \{u_0, u_1, ..., u_{t-1}\}$을 생성한다.

$$\begin{aligned} u_j &= CE^{-1}(S, d_j) \\ &= CE^{-1}(S, CE(R, c'_j)) \\ &= CE^{-1}(S, CE(R, CE(S, k_{l_j}))) \\ &= CE^{-1}(S, CE(S, CE(R, k_{l_j}))) \\ &= CE(R, k_{l_j}) \end{aligned} \quad \cdots\cdots (6)$$

키 관리 센터는 생성된 U에 서명을 작성하고 U와 서명을 구매자에게 보낸다.

7) 구매자는 키 관리 센터로부터 받은 U의 서명을 확인하

고 이를 비밀키 R을 이용하여 U를 복호화화여 t개의 키 key_j를 획득한다.

$$key_j = CE^{-1}(R,u_j) \quad \cdots\cdots (7)$$
$$= CE^{-1}(R,CE(R,k_{l_j})) \ , \ 0 \le j \le t-1$$

구매자는 복호화 결과로 t개의 키로 구성된 키벡터 K_B를 얻을 수 있다.

$$K_B = \{key_0, key_1, ..., key_{t-1}\} \quad \cdots\cdots (8)$$

1.3 구매 단계

구매 단계는 구매자의 구매 요청에 대하여 판매자가 콘텐츠에 핑거프린트를 삽입하고 콘텐츠를 암호화하여 구매자에게 제공하는 프로토콜로 구성되어 있다. 구매자는 판매자에게 디지털 콘텐츠의 구매를 요구한다. 구매자로부터 구매요구와 돈을 받으면, 판매자는 구매자의 두 개의 핑거프린트 F_0^B와 F_1^B를 생성한다. 생성된 핑거프린트와 Cox의 알고리즘의 W는 같은 특성을 가진다.

1) 구매자는 판매자에게 자신의 익명 공개키 y_1, $cert(y_1)$을 보내고 콘텐츠 구매 요청을 한다.

2) 판매자는 삽입할 두 개의 핑거프린트 F_0^B, F_1^B를 생성한 후 $f = h(F_0^B \| F_1^B)$를 계산한 후 이에 서명 $S_c(f)$을 생성하여 구매자에게 보낸다.

3) 구매자는 판매자한테 받은 f값에 익명 비밀키 x_1 값을 이용하여 서명 $S_B(S_C(f))$을 생성하고 이를 판매자에게 보낸다.

4) 판매자는 키 관리 센터로부터 구매자의 익명 공개키 값 y_1에 해당하는 식 (2)에서 생성된 구매자의 두 개의 키벡터 K_0, K_1를 받아온다.

5) 판매자는 콘텐츠 Z를 t개의 프레임으로 나누고, 나뉘어진 콘텐츠 조각(프레임)에 핑거프린트를 삽입하여 두 가지 형태의 콘텐츠를 식(9)와 같이 생성한다. Z_0^B은 콘텐츠 조각 각각에 핑거프린트 F_0^B을 삽입하여 생성하고, Z_1^B는 핑거프린트 F_1^B를 삽입하여 생성하게 된다.

$$Z_i^B = \{z_{i,0}^B, z_{i,1}^B, ..., z_{i,t-1}^B \mid i \in \{0,1\}\} \text{ where}$$
$$z_{0,j}^B = z_j \otimes F_0^B \ , \quad 0 \le j \le t-1$$
$$z_{1,j}^B = z_j \otimes F_1^B \ , \quad 0 \le j \le t-1 \quad \cdots\cdots (9)$$

6) 판매자는 생성된 Z_i^B의 t개의 콘텐츠 프레임을 4)번의 키벡터 K_0, K_1을 이용하여 암호화하여 $EX_i^B = \{ex_{i,0}^B, ex_{i,1}^B, ..., ex_{i,t-1}^B \mid i \in \{0,1\}\}$를 식(10)과 같이 생성한다.

$$ex_{0,j}^B = SE(k_{0,j}, z_{0,j}^B) = SE(k_{0,j}, z_j \otimes F_0^B)$$
$$ex_{1,j}^B = SE(k_{1,j}, z_{1,j}^B) = SE(k_{1,j}, z_j \otimes F_1^B) \cdots (10)$$

콘텐츠에 핑거프린트를 삽입하고 암호화하는 과정은 그림 2와 같다.

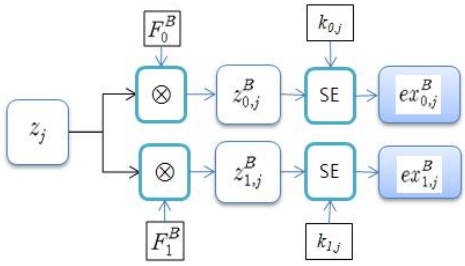

그림 2 핑거프린트 삽입과 암호화

콘텐츠를 암호화할 때 이용하는 암호 알고리즘 $SE(\ )$는 콘텐츠를 고려한 대칭 암호 시스템을 이용한다. 판매자는 두 개의 암호화된 콘텐츠 벡터를 구매자에게 보낸다.

6) 구매자는 판매자로부터 암호화된 콘텐츠를 받고, 키 관리 센터에게서 받은 식 (8)의 K_B를 이용하여 암호화된 콘텐츠를 식 (11)의 과정으로 복호화한다.

$$z_{l_j,j}^B = SE^{-1}(key_j, ex_{l_i,j}^B)$$
$$= SE^{-1}(key_j, SE(key_j, z_{l_j,j}^B)) \quad \cdots\cdots (11)$$

구매자는 자신이 가지고 있는 키로 암호화된 콘텐츠 프레임만 복호화할 수 있으며 다른 키로 암호화된 콘텐츠 프레임은 복호화할 수 없다. 구매자는 각각의 프레임들을 순서대로 정리하여 완전한 핑거프린트가 삽입된 콘텐츠 $Z^B = \{z^B_{l_j,j} | 0 \le j \le t-1\}$를 구할 수 있다.

1.4 구매자 신원확인 단계

불법적으로 재배포된 콘텐츠가 발견되면 판매자는 그 콘텐츠로부터 핑거프린트를 추출하여 구매자가 누구인지 추적하게 된다. 판매자는 구매자를 추적하기 위하여 다음과 같은 프로토콜을 진행한다.

1) 불법 재배포된 콘텐츠를 Z'라 하자. 판매자는 재배포된 콘텐츠를 발견하게 되면 콘텐츠로부터 핑거프린트 F_0^B, F_1^B를 추출한다.

2) 판매자는 추출된 핑거프린트 F_0^B, F_1^B에 해당하는 익명 공개키와 구매자의 정보를 데이터베이스로부터 검색한다.

3) 판매자는 검색된 익명 공개키 y_1와 인증서 $cert(y_1)$, 추출된 핑거프린트 F_0^B, F_1^B와 핑거프린트 비트 패턴 L, 재배포된 콘텐츠, 구매자의 서명 $S_B(S_C(f))$를 재판관에게 증거자료로 보낸다.

4) 재판관은 t비트 패턴 L을 이용하여 y_1을 검증하고 Z'에 해당 핑거프린트가 삽입되어 있는지 확인한다.

4) 검증이 완료되면 y_1을 등록 센터에 보내서 구매자의 원래의 아이디를 요청하여 재배포자가 누구인지 알아낸다.

2. 안전성 분석

2.1 판매자에 대한 안전성

□ 추적성

구매자는 두 개 또는 그 이상의 정당한 Z^B을 얻어서 인가되지 않은 Z'^B을 재배포하고도 고발되지 않도록 할 수 있다. 이를 위해서 구매자는 키 관리 센터와 공모를 하여 t개 이상의 키를 받아내어 자신의 키에 해당하지 않는 다른 비트열의 콘텐츠를 배포하면 된다. 그러나 구매자가 키 관리 센터와 공모를 하여 t개 이상의 프레임을 얻었다 하더라도 콘텐츠가 재배포되면 판매자는 재배포된 콘텐츠에서 삽입된 핑거프린트 F_0^B와 F_1^B를 추출할 수 있으며 핑거프린트 F_0^B와 F_1^B은 구매자마다 다르기 때문에 판매자는 재배포자를 찾아낼 수 있다. 따라서 구매자가 키 관리 센터와 공모하여 t개 이상의 키를 이용하여 콘텐츠를 복호화하고 재배포 한다 해도 판매자는 불법 재배포자 추적이 가능하게 된다.

□ 부인 봉쇄

핑거프린팅 프로토콜에서 구매자는 구매자마다의 서로 다른 핑거프린트가 삽입되게 되어 있다. 핑거프린팅 프로토콜에서 구매자는 판매자에게 받은 $f = h(F_0^B \| F_1^B)$값에 자신의 익명 비밀키 값 x_1을 이용하여 서명을 생성해 보내게 되고 이를 프로토콜 상에서 판매자가 확인한다. 판매자는 재배포된 콘텐츠가 발견되었을 때 구매자로부터 받은 서명값 $S_B(S_C(f))$ 을 이용하여 구매자가 콘텐츠를 구매하였음을 증명할 수 있기 때문에 구매자는 재배포된 콘텐츠가 구매자의 것임을 부인할 수 없다.

□ 견고성

핑거프린팅 프로토콜에서 판매자가 핑거프린트를 콘텐츠에 삽입할 때 Cox의 알고리즘[10]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.

□ 공모 공격으로부터의 안전성

핑거프린팅 기법은 구매자마다의 삽입 정보가 다르기 때문에 구매자끼리의 공모를 통하여 삽입 정보를 추출 제거할 수 있는 위험이 존재한다. 그러나 이러한 위험은 삽입 알고리즘의 특성에 따라, 최대 공모 공격의 한계를 넘지 않을 경우, 그리고 삽입된 데이터가 원래의 데이터와 유사할 경우, 구매자는 공모를 통하여 삽입된 핑거프린트와 그에 관련된 값들을 찾을 수 없다.

2.2 구매자에 대한 안전성

등록 센터는 공모를 통하여 정직한 구매자의 신원을 노출시키지 않는 기관이라고 가정한다. 정직한 구매자는 판매자가 재판관을 확신시킬 증거자료를 정확히 제출하지 못한다면 불법 재배포자로 오인되지 않고 안전할 수 있다.

□ 비대칭성

판매자는 프로토콜을 올바르게 수행하지 않았다 하더라도 구매자가 어떤 정보를 선택하였는지 전혀 알 수 없다. 핑거프린팅 프로토콜에서 구매자로부터 판매자가 알 수 있는 정보는 구매자의 익명 공개키 y_1와 인증서 $cert(y_1)$, 그리고 핑거프린트에 대한 서명값 밖에 없다. 판매자가 정직한 구매자를 고발하기 위해서는 구매자의 핑거프린트 비트 패턴을 알아내야 한다. 이를 위해서 판매자는 키 관리 센터와 공모하여 구매자의 x_1값을 알아내거나 구매자가 가지고 있는 익명 비밀키를 알지 못한 채로 d_i로부터 c'_i가 어떤 값인지를 계산해내야 한다. 그러나 이 계산은 교환 암호 알고리즘 CE를 공격하는 방법과 같기 때문에 안전하다고 증명된 알고리즘을 이용하면 불가능하다고 할 수 있다. 또한 모든 t개의 프레임에 대하여, 구매자가 선택한 c'_i가 c_0인지 c_1인지를 알아낼 수 있는 확률은 $1/2^t$와 같다. 따라서 판매자는 구매자가 선택한 정보를 비밀키 R을 알지 않고서 비트패턴을 찾아내기는 계산상 불가능하다.

□ 비연결성

구매자가 콘텐츠를 구매하고자 할 때마다 구매자는 등록센터에 일회 사용하는 익명 공개키 쌍을 등록해 놓고 이를 이용하여 구매행위를 수행한다. 따라서 구매자가 서로 다른 판매자에게서 콘텐츠를 구입할 경우라도 그때 마다 사용되는 익명 공개키가 다르기 때문에 구매자의 서로 다른 구매 행위는 연결되지 않는다.

□ 공모 공격으로부터의 안전성

판매자는 키 분배 센터와 공모하여 정직한 구매자 B에 해당하는 핑거프린트 F_0^B, F_1^B를 삽입한 후 이를 배포하고 구매자 B를 재배포자로 고발할 수 있다. 판매자가 구매자를 고발할 때에는 재판관을 확신시키기 위하여 추출된 핑거프린트의 비트 패턴 L과 비트 패턴을 키로 생성하여 서명을 확인하였을 때 구매자의 서명이 일치함을 증명해야 한다. 그러나 판매자는 키 분배 센터와 공모를 하였다 하더라도 구매자의 익명 비밀키 x_1값을 알아낼 수 없기 때문에 재판관을 증거 자료로 확신시킬 수 없게 된다. 따라서 구매자는 판매자와 키 관리 센터의 공모 공격으로부터도 안전할 수 있다.

□ 조작 봉쇄

정직한 구매자는 악의적인 판매자나 다른 제3자에 의해서 재배포하였다고 누명을 쓸 수 없다. 비록 판매자가 구매자의 핑거프린트를 알고 있다 하더라도, 핑거프린트가 삽입된 콘텐츠는 t개의 프레임으로 나뉘어 있기 때문에 모든 가능한 조합의 수는 2^t가지가 되므로 판매자는 구매자가 어떤 프레임을 선택했는지 알 수 없다. 따라서 판매자는 구매자의 익명 비밀키에 해당하는 비트 패턴 L을 만들어 내어 정직한 구매자를 고소할 수 없으며 구매자의 익명 비밀키 x_1를 모르기 때문에 정당한 서명을 생성해 낼 수 없으므로 신원확인 프로토콜에서 재판관을 확신시킬 수 없다.

IV. 결 론

본 논문에서는 대칭키 암호를 기반으로 하지만 핑거프린트를 생성할 때 신뢰기관의 도움을 받지 않는 핑거프린팅 프로토콜에 대하여 제안하였다. 제안한 기법에서는 재배포된 콘텐츠가 발견되었을 때에는 언제든지 판매자가 구매자를 찾아내어 고발 할 수 있기 때문에 판매자가 안전하게 프로토콜을 이용할 수 있다. 기존의 대칭키 암호 기반의 기법들은 비대칭성 만족을 위하여 구매자 각각의 핑거프린트를 신뢰기관이 생성함으로써 공모 공격으로부터 취약하게 된다. 그러나 제안한 기법에서는 대칭키 암호를 기반으로 하지만 비대칭성 만족을 위하여 신뢰기관에 의존을 하지 않고 프로토콜을 통하여 비대칭성을 만족시켰기 때문에 신뢰기관의 관리가 필요 없으며 공모 공격으로부터 안전하게 설계함으로써 구매자의 안전성을 향상시켰다.

참고문헌

〔1〕 B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," EYROCRYPT'96, LNCS 1070, pp. 84 -95, 1996.

〔2〕 D. Boneh and J. Shaw, "Collision-secure fingerprinting for digital data," IEEE Trans. Inf. Theory, vol.44, no.5, pp. 1897-1905, 1998.

〔3〕 W. Trappe, M. Wu, Z.J. Wong, and KJ.R. Liu, "Anti-collusion fingerprinting for multimedia," IEEE Trans. Signal Process., vol.51, no.4, pp. 804-821, 2003.

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

〔5〕 N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Transactions on Image Processing, 10(4), pp. 643-649, 2001.
〔6〕 A.M. Balleste, F. Sebe, J.D. Ferrer, andM. Soriano, ""Practical asymmetric fingerprinting with a TTP,"" Proc. DEXA''03, pp.352 - -356, 2003.
〔7〕 M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting scheme with high enciphering rate," INDOCRYPT'01, LNCS 22247, pp. 30-39, 2001.
〔8〕 F. Bao, R. H. Deng and P. Feng, "An effcient and practical scheme for privacy protection in the E-commerce of digital goods," ICICS'00, LNCS2836, pp. 162-170, 2000,
〔9〕 B. Pfitzmann and A. R. Sadeghi, "Coin-based anonymous fingerprinting," Advances in Cryptology - EUROCRYPT'99, LNCS 1592, pp. 150-164, 1999.
〔10〕 I. J. Cox, J. Kilian, T. Leighton, and T. Shamnon, "Secure spread spectrum watermarking for image, audio and video", IEEE Transactions on Image Processing,6(12), pp. 1673-1678, 1997.

저 자 소 개

용승림

2006: 이화여자대학교 공학박사
2006-2007: 이화여자대학교 컴퓨터 정보공학부 전임강사
2008 - 현재: 인하공업전문대학 컴퓨터시스템과 전임강사
관심분야: 정보보호, 암호프로토콜, 디지털 저작권 보호