한국산학기술학회논문지
Vol. 8, No. 3, pp. 549-555, 2007

생체정보 기반의 부인봉쇄 디지털 다중서명 기법

윤성현[1*]

The Undeniable Digital Multi-Signature Scheme based on Biometric Information

Sung-Hyun Yun[1*]

요 약 디지털 서명 기법은 디지털 문서에 대한 무결성, 서명자 인증 및 부인봉쇄 기능을 제공한다. 디지털 서명에 필요한 서명키는 일반적으로 하드디스크 또는 이동식 저장 매체에 보관한다. 이 경우의 문제점은 서명자가 대리인에게 키 정보를 알려주어 대리로 서명을 할 수 있다는 것이다. 전자 선거와 같은 응용에 악용될 수 있다. 본 논문에서는 대리 서명이 허용되어서는 안 되는 응용에 적합한 생체정보 기반의 부인봉쇄 디지털 다중 서명 기법을 제안한다. 부인봉쇄 다중 서명 기법은 여러 서명자를 필요로 하며 지정된 사용자에게만 다중 서명을 검증할 수 있도록 한다. 제안한 다중서명 기법은 부인봉쇄 성질을 만족하며 서명자에 의한 다중서명 부정 및 변조 공격에 대해서 안전하다. 또한 지문정보에 기반을 두어 키를 생성함으로써 대리 서명과 같은 위협에 대해서 안전하다.

Abstract A digital signature scheme provides integrity of the document, authentication and non-repudiation of a signer. Usually the key for digital signature is stored in hard disk or removal disk storage. The drawback of this approach is that the signer can let the agent to sign instead of the signer by providing the key information. It can be abused in applications such as electronic election. In this paper, we propose the undeniable biometric digital multi-signature scheme suitable for applications where the signer should not make an agent sign instead of himself/herself. The undeniable multi-signature scheme requires many signers and only the designated user can confirm the authenticity of multi-signature. The proposed scheme satisfies undeniable property and it is secure against active attacks such as modification and denial of the multi-signature by signers. As the key is generated through the signer's fingerprint image, it's also secure against signing by an agent.

Key Words : 지문 인증, 부인봉쇄 다중서명, 부인봉쇄 서명, Biometrics, Biometric Security

1. 서론

디지털 서명 기법은 메시지 무결성과 사용자 인증 기능을 함께 제공하며 서명자에 대한 부인봉쇄 기능을 제공하는 매우 강력한 수단의 정보보호 기법이다[7,8]. 이메일, 전자 결재, 인터넷 뱅킹, 저작권 보호, 전자선거 등의 많은 응용 분야에 필수적으로 사용된다. 디지털 서명에 사용되는 키는 일반적으로 하드디스크 또는 USB 디스크와 같은 이동식 저장 매체에 저장된다. 이 경우의 문제점은 저장된 키 정보는 키를 사용하는 서명자와 독립적이기 때문에 서명자가 대리인에게 키를 넘겨주어 대리로 서명하는 것이 가능하다는 것이다. 본 논문에서는 전자선거와 같이 대리 서명이 허용되어서는 안 되는 응용 분야에 적합한 생체정보 기반의 부인봉쇄 디지털 다중 서명 기법을 제안한다.

디지털 서명을 생성하는 과정에 서명자의 생체정보를 이용해야만 서명키를 추출할 수 있도록 함으로써 서명자 본인이 직접 개입하지 않고서는 서명을 수행할 수 없도록 해야 한다. 전자선거 및 공항에서의 출입국 사용자 식별 등의 응용 분야에 적용될 수 있다. 또한 부인봉쇄 다중서명 기법을 적용함으로써 공동 저작권 보호 등과 같은 콘텐츠 유통 및 지적 재산권 보호 분야에 적용이 가능하다.

생체정보를 이용한 사용자 인식은 개개인 고유의 생체

이 논문은 2006년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2006-521-D00464)
[1]백석대학교 정보통신학부
*교신저자: 윤성현(shyoon@bu.ac.kr)

정보를 인식하기 위한 방법을 의미하며, 기술적으로 지문, 정맥, 홍채, 망막, 얼굴 및 음성 등 다양한 개인 고유의 정보를 추출하여 미리 등록되어있는 데이터와 비교하여 사용자를 식별하는 기술이다. 개인의 식별 혹은 인증을 위한 목적으로 주로 사용되고 있으며, 더 나아가서 접근제어를 위한 기술로 활용되고 있다. 최근에는 공개키 기반의 전자서명 기술의 응용이 다양화되면서, 지문인식과 전자서명의 연계성에 대한 연구가 활발히 진행되고 있다. 지문정보를 이용하여 전자서명에 필요한 키를 생성하고 이를 통해 사용자에 대한 인증 및 안전하게 메시지를 전송하는 방법에 대한 연구가 필요하다. 본 논문에서는 사용자의 여러 가지 생체 정보 중 지문정보로 서명키를 생성하고 이를 이용하여 부인봉쇄 다중서명을 생성 및 검증하는 방법을 제안한다.

지문정보만을 이용하여 키를 생성할 경우에 동일한 사용자는 매 번 같은 키를 생성하게 된다. 지문정보는 개인마다 유일한 특성을 갖기 때문에 한 번 도용되면 다시 사용할 수 없는 치명적인 단점을 갖는다. 따라서 키 생성 시 동일한 지문정보에 대해서 서로 다른 여러 개의 키를 만들 수 있도록 하는 방법이 필요하다. IBM에서 제안한 취소 가능한 생체정보 모델(Cancelable Biometrics Model)[1]에서는 키 생성시에 지문정보 외에 난수 값을 추가로 적용함으로써 사용자 키가 도용되더라도 다른 키를 재생성하여 등록할 수 있다.

전자서명에 사용되는 개인키는 그 특성상 키 소유자만이 알고 있어야 하며, 도용되거나 노출될 경우에 해당 전자서명의 안전성은 보장될 수 없다. 일반적으로 개인키 보호를 위해서 키를 암호화하여 하드디스크 또는 이동식 저장 매체에 보관한다. 이러한 방법이 갖는 공통적인 특징은 개인키 값이 변형된 형태로 보관되며 이 값이 제 3자에게 노출될 수 있는 위험성을 수반한다는 것이다. 따라서 서명에 사용될 키 추출시에 개인키 소유자가 제 3자에게 위탁할 수 있는 위험요소가 존재한다. 사용자의 지문정보를 활용해야만 개인키를 추출할 수 있도록 하는 키 보관 기법의 적용이 필수적이다. 본 연구에서는 퍼지 볼트 모델(fuzzy vault model)[4]을 적용하여 사용자의 개인키를 지문정보에 은닉하고 추출할 수 있도록 한다.

기존의 생체정보 기반의 키 생성 및 전자서명 기법은 단일 사용자에 대한 신분 및 문서 인증을 대상으로 한다. 멀티미디어 콘텐츠와 같이 여러 저작자들의 권리 표현이 필요한 응용을 위해서는 부인봉쇄 다중서명 기법의 적용이 필수적이다. 부인봉쇄 다중 서명 기법은 여러 서명자를 필요로 하며 지정된 사용자에게만 다중 서명을 검증할 수 있도록 한다. 제안한 지문정보 기반의 부인봉쇄 다중서명 기법은 부인봉쇄 성질을 만족하며 서명자에 의한 다중서명 부정 및 변조 공격에 대해서 안전하다. 또한 지문정보에 기반을 두어 서명키를 생성함으로써 대리 서명 등의 부정행위에 대해서 안전하다.

2 장에서는 생체정보 기반의 키 생성 및 은닉 기법에 대해서 살펴보고 3 장에서는 이를 접목한 부인봉쇄 다중서명 기법에 대해서 알아본다. 4 장에서는 제안한 기법의 응용에 대해서 설명하고 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 관련연구

생체정보는 개인마다 고유한 정보이기 때문에 한 번 도용되면 재사용할 수 없는 단점이 있다. 따라서 키 생성 과정에 생체정보와 더불어 난수 정보를 이용함으로써 키가 도용되더라도 키를 재등록할 수 있어야 한다. 또한 키 추출 과정에 생체정보를 이용함으로써 대리 서명의 위험을 최소화할 수 있다. 생체정보는 그 특성 상 스캔할 때마다 입력 값이 조금씩 차이가 나게 된다. 퍼지볼트 기법은 확률적으로 데이터를 은닉 및 추출할 수 있는 방법이므로 생체정보에 키 값을 은닉하고 추출하는 기법으로 적합하다.

(1) 취소 가능한 생체정보 모델[1]

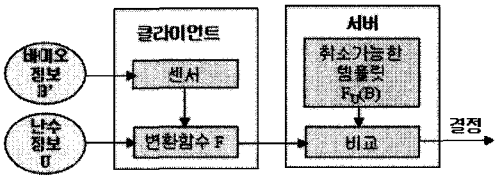

그림 1. 취소 가능한 생체 정보 모델

그림 1은 IBM에서 처음으로 제안한 취소 가능한 템플릿(template)과 이를 이용한 사용자 인증 모델을 보여준다. 생체정보는 고유한 특성을 가지며 도용되었을 경우에 취소할 수 없는 특성이 있다. 이러한 생체정보의 특성을 없애기 위하여 생체정보 외에 비밀값 U(Secret Parameter U)를 이용하여 취소 가능한 템플릿을 생성한다. 그림 1에서 F 함수는 생체정보와 비밀값 U를 입력으로 받고 이 값들을 이용하여 템플릿 $F_U(B')$를 만들어낸다. 사용자는 비밀값 U를 달리하여 서로 다른 템플릿들을 여러 개 생성할 수 있다. 따라서 저장된 템플릿이 노출되거나 도용되었을 경우에 템플릿 재등록이 가능하다.

(2) 퍼지볼트 모델을 이용한 키 은닉 및 추출[4]

퍼지볼트 모델(fuzzy vault)은 데이터를 은닉하기 위한 용도로 사용된다. 원래 볼트(금고)는 정확한 자물쇠 번호들을 알고 있어야만 열 수 있는데, 퍼지 볼트 기법은 임계치(threshold) 이상의 번호들만 알고 있으면 전체 번호를 모르더라도 해당 볼트를 열 수 있도록 하는 기법이다. 생체정보는 매 번 입력할 때 마다 조금씩 틀린 값을 갖게 된다. 보정을 하게 되면 정확하게 모두 일치하지는 않지만 같은 특징점을 갖는 데이터들을 추출해 낼 수 있다. 생체정보의 이러한 특성은 퍼지볼트 모델을 이용하여 생체정보에 키 값을 은닉하기에 매우 적합하다.

3. 생체정보에 기반한 부인봉쇄 다중서명 기법

생체정보를 이용한 기존의 전자서명 기법의 특징은 단일 사용자에 대한 인증 및 메시지의 무결성을 대상으로 한다[2,3]. 본 논문에서는 여러 서명자들의 생체정보를 이용하여 다중서명을 생성하고 검증하는 방법에 대해서 제안한다. 제안한 기법은 키 생성, 다중서명 생성 및 검증 단계로 구성된다.

3.1 절에서 생체정보 기반의 키 생성 및 은닉 기법을 3.2 절에서 생체정보 기반의 부인봉쇄 다중서명 기법에 대해서 제안한다.

3.1 키 생성 및 은닉

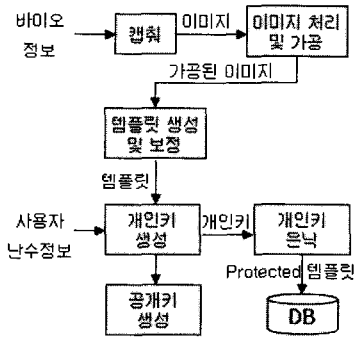

그림 2. 생체정보 기반 전자서명 키 생성 모델

그림 2는 지문정보 기반의 키 생성 단계를 보여준다. 지문정보(fingerprint)와 사용자 입력 난수 정보를 가지고 디지털 서명에 사용될 개인키와 공개키를 생성하며 퍼지볼트 기법을 이용하여 개인키를 지문정보에 은닉하는 절차로 구성된다. 각 단계별로 살펴보면 다음과 같다.

단계 1: 지문정보에 대한 템플릿 생성

사용자는 지문인식 센서를 이용하여 지문을 캡춰하고 이를 디지털 데이터로 변환한다. 단계 1은 이미지 처리 및 특징점 추출 절차로 구성된다. 이미지 처리에서는 지문인식 장치로부터 입력받은 원시 이미지에 대한 노이즈 제거, 지문 융선 복원, 세선화 등의 작업을 수행한다. 지문의 특징점은 지문 융선이 끝나는 단점(end point)과 갈라지는 분기점(bifurcation point)으로 구성된다. 특징점의 (x, y) 좌표와 각도 정보를 포함하는 템플릿을 생성한다.

단계 2: 템플릿 정보를 이용한 보정값 계산

지문 정보는 매 번 센서로 입력받을 때 마다 차이가 나기 때문에 이를 보정할 수 있는 함수와 보정값이 필요하다. 단계 1에서 생성된 템플릿의 특징점들의 위치 정보와 각도 정보를 이용하여 향후 입력될 지문정보의 특징점들을 보정할 수 있는 보정값을 계산한다.

단계 3: 디지털 서명 키 생성

개인키는 사용자 입력 난수 값과 단계 1에서 생성된 템플릿을 해쉬하여 만든다. 공개키 기반 디지털 서명 알고리즘에서 키 생성 방법 및 조건은 알고리즘마다 서로 상이하기 때문에 조건에 맞는 키 값을 구하기 위하여 사용자 난수 값을 조정하여 해쉬한다. 지문정보는 고유하기 때문에 개인키 생성을 위하여 템플릿 정보만을 이용할 경우에 항상 똑 같은 키 만을 생성하게 된다. 이 경우 키가 노출 및 도용되면 키를 다시 재생성할 수 없다.

단계 4: 개인키 은닉

개인키 보호를 위하여 퍼지볼트 기법을 적용하여 키를 은닉한다. 은닉된 키를 추출하기 위해서 사용자는 직접 지문정보를 입력해야 한다. 개인키를 이용한 대리서명의 위험을 최소화할 수 있다. 단계 1에서 생성된 템플릿에 가짜 특징점 정보들을 추가한다. 퍼지볼트 기법을 이용하여 개인키를 은닉하기 위해서 템플릿의 실제 특징점에 적용할 함수와 가짜 특징점에 적용할 함수를 따로 준비한다. 개인키 값을 각각의 함수에 적용하여 결과 값을 구한다. 템플릿 정보에 이 결과 값을 추가하여 protected 템플릿을 생성한다. Protected 템플릿은 특징점의 (x, y) 위치 정보, 각도 정보 그리고 함수값을 포함한다.

3.2 생체정보 기반 부인봉쇄 다중서명 기법

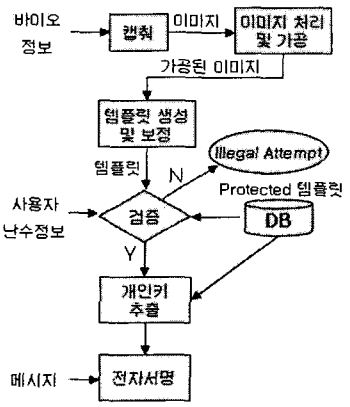

그림 3. 생체정보 기반 전자서명 모델

그림 3은 생체정보 기반의 전자서명 모델을 보여준다. 서명자는 서명에 사용될 개인키를 추출하기 위하여 센서를 이용하여 지문을 입력하고 protected 템플릿에 등록된 기존의 템플릿과 비교하여 식별과정을 거치게 된다. 서명 생성에 반드시 서명자가 참여해야만 하기 때문에 대리 서명의 위험성을 최소화할 수 있다.

제안한 기법에서 서명자들은 그림 3과 같은 서명자 식별 과정을 통해서 신분 인증을 수행한 후에 다중서명 프로토콜에 참여할 수 있다. 부인봉쇄 다중서명 기법은 여러 서명자의 서명이 필요한 다중서명 기법에서 서명자들의 동의 없이는 서명을 검증할 수 없는 특성을 갖는다. 공동 저작된 저작물에 대한 저작권 생성에 응용될 수 있으며, 저작물의 유통 과정에서 모든 저작자들의 동의하에서만 라이센스를 발급할 수 있도록 함으로써 저작권자들의 권리를 보장받을 수 있게 한다. 하지만 서명에 사용될 개인키가 노출되어 도용될 경우에 저작권자의 권리를 보장받을 수 없다. 또한 개인키를 다른 사람에게 맡겨서 대리로 서명하게 할 경우에 대리 서명자에 의한 부정이 발생할 수 있는 위험요소가 존재한다. 따라서 저작권자 본인이 반드시 서명할 수 있도록 하는 기법 및 절차가 필수적이며 고유 정보인 생체 정보를 이용한 키 생성 기법의 적용이 필수적이다.

본 절에서는 공동 저작권 보호에 적합한 생체정보 기반의 부인봉쇄 다중서명 프로토콜을 제안한다. 생체정보를 접목함으로써 대리 서명이 가능하지 않으며 상기한 바와 같이 경제적 가치를 지니는 디지털 콘텐츠 비즈니스에서의 저작권 보호 및 관리를 위한 용도로 활용될 수 있다. 저작권 정보 생성 및 검증에 모든 저작권자가 직접 개입하도록 하여 콘텐츠 유통 및 판매의 신뢰성을 높일 수 있으며 불법 복제 및 유통을 방지하기 위한 용도로 적용될 수 있다.

생체정보가 접목된 부인봉쇄 다중서명 생성 및 검증 프로토콜은 다음과 같다.

p는 큰 소수로 p를 법으로 하는 유한체 $GF(p)$ 상에서 g 는 법 p 에 대한 위수$p-1$ 을 갖는 생성자이다. n 명의 서명자들이 참여한다고 가정하고 각 서명자의 개인키 및 공개키는 다음과 같다.

* 서명자 i의 개인키
  $sk_i \in Z_{p-1},\ i=[1..n]$
* 서명자 i의 공개키
  $pk_i \equiv g^{sk_i} (\mathrm{mod} p),\ i=[1..n]$

3.2.1 부인봉쇄 다중서명 생성

서명자들은 3.1절의 키 생성 프로토콜을 이용하여 공개키/개인키 쌍을 만들고 메시지 기안자는 서명 대상 메시지 m 을 서명자들에게 전송한다. 서명자들은 부인봉쇄 다중서명에 필요한 공통키를 생성하고 메시지 m 에 대한 부인봉쇄 서명을 만들어 메시지 기안자에게 전송한다. 메시지 기안자는 각 서명자의 부인봉쇄 서명을 조합하여 부인봉쇄 다중서명을 생성한다.

먼저 메시지 기안자는 메시지 m에 대한 해쉬값 m_h 가 법 p에 대한 원시근(primitive root)이 되도록 hpr을 설정한다.

$$m_h = h(m, hpr)$$

메시지 m 과 해쉬 파라미터 hpr 을 서명자들에게 전송한다.

(1) 첫 번째 서명자의 공통키 생성

단계 1: Z_{p-1} 상에서 p-1과 서로소인 임의의 난수 k_1 을 선택하여 r_1 을 계산한다.

$$\gcd(k_1, p-1)=1,\ r_1 \equiv m_h^{k_1} (\mathrm{mod} p)$$

단계 2: 서명자들의 대표 공개키 PK 를 생성하기 위해서 PK_1 을 다음과 같이 설정한다.

$$PK_1 = pk_1$$

단계 3: 첫번째 서명자는 단계 1과 2에서 생성된 (r_1, PK_1)을 두번째 서명자에게 전송한다.

(2) 서명자 i의 공통키 생성($i=[2..n]$)

단계 1: 서명자 i는 바로 전 단계에서 서명한 서명자 i-1로부터 (r_{i-1}, PK_{i-1}) 을 수신한다.

$$r_{i-1} \equiv r_{i-2}^{k_{i-1}} \equiv m_h^{\prod_{j=1}^{i-1} k_j} (\mathrm{mod} p),$$

$$PK_{i-1} \equiv PK_{i-2}^{x_{i-1}} \equiv g^{\prod_{j=1}^{i-1} sk_j} (\mathrm{mod} p)$$

단계 2: 서명자 i는 다음과 같이 p-1과 서로소인 임의의 난수 k_i 를 선택하고 이를 이용하여 r_i 를 생성한다.

$$\gcd(k_i, p-1) = 1,\ k_i \in Z_{p-1},$$

$$r_i \equiv r_{i-1}^{k_i} \equiv m_h^{\prod_{j=1}^{i} k_j} (\mathrm{mod} p)$$

단계 3: 서명자 i는 지문정보를 입력하여 사용자 식별과정을 거친 후에 개인키 sk_i 을 추출하고 다음과 같이 PK_i 를 생성한다.

$$PK_i \equiv PK_{i-1}^{sk_i} \equiv g^{\prod_{j=1}^{i} sk_j} (\mathrm{mod} p)$$

단계 4: 서명자 i는 서명자 i+1에게 (r_i, PK_i) 를 전송한다.

단계 5: 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 4를 반복한다. 마지막 서명자는 다음과 같이 서명자들의 공통키 R 과 대표 공개키 PK 를 구해서 모든 서명자들과 메시지 기안자에게 (R, PK) 를 전송한다.

$$R \equiv r_{n-1}^{k_n} \equiv m_h^{\prod_{j=1}^{n} k_j} (\mathrm{mod} p),$$

$$PK \equiv PK_{n-1}^{sk_n} \equiv g^{\prod_{j=1}^{n} sk_j} (\mathrm{mod} p)$$

(3) 다중서명 생성

단계 1: 각 서명자는 지문정보를 이용하여 개인키를 추출하고 공통키 R 을 이용하여 다음 식을 만족하는 s_i 를 구한다. k_i 와 $p-1$은 서로소이므로 s_i 에 대한 유일한 해가 존재한다.

$$k_i \cdot s_i \equiv sk_i \cdot R - k_i \cdot m_h (\mathrm{mod} p-1)$$

단계 2: 각 서명자는 부인봉쇄 서명 s_i 를 메시지 기안자에게 전송한다.

단계 3: 메시지 기안자는 각 서명자로부터 전송받은 s_i 를 조합하여 부인봉쇄 다중서명 S 를 다음과 같이 생성한다.

$$S \equiv \prod_{j=1}^{n} (m_h + s_j) (\mathrm{mod} p)$$

3.2.2 다중서명 확인 프로토콜

메시지 기안자는 (R, S)가 메시지 m에 대한 올바른 다중서명인지 확인하기 위해서 순차적으로 다음과 같은 다중서명 확인 프로토콜을 수행한다.

먼저 메시지 기안자는 임의의 두 난수 (a, b) 를 선택하고 다음과 같이 도전 ch 를 생성하여 첫번째 서명자에게 ch 를 전송한다.

$$ch \equiv R^{S \cdot a} \cdot Y^{R^n \cdot b} (\mathrm{mod} p)$$

$$\equiv m_h^{a \cdot R^n \cdot \prod_{j=1}^{n} sk_j} \cdot g^{b \cdot R^n \cdot \prod_{j=1}^{n} sk_j} (\mathrm{mod} p)$$

(1) 첫 번째 서명자의 응답 생성

단계 1: 첫 번째 서명자는 지문정보를 입력하여 사용자 식별과정을 거친 후에 개인키 sk_1 을 추출한다.

단계 2: 첫 번째 서명자는 다음과 같이 응답 rsp_1 을 생성해서 두 번째 서명자에게 전송한다. sk_1^{-1} 는 법 $p-1$에 대한 sk_1 의 모듈라 곱셈의 역이다.

$$rsp_1 \equiv ch^{sk_1^{-1}} (\mathrm{mod} p)$$

(2) 서명자 i의 응답 생성

단계 1: 서명자 i는 지문정보를 입력하여 사용자 식별과정을 거친 후에 개인키 sk_i 를 추출한다.

단계 2: 서명자 i는 서명자 i-1로부터 응답 rsp_{i-1} 을 수신한다.

$$rsp_{i-1} \equiv rsp_{i-2}^{sk_{i-1}^{-1}} \equiv ch^{\prod_{j=1}^{i-1} sk_j^{-1}} (\mathrm{mod} p)$$

단계 3: 서명자 i는 sk_i^{-1} 를 이용하여 다음과 같이 응답 rsp_i 를 생성한다.

$$rsp_i \equiv rsp_{i-1}^{sk_i^{-1}} (\mathrm{mod} p)$$

단계 4: 서명자 i는 서명자 i+1에게 응답 rsp_i 를 전송한다.

단계 5: 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 3을 반복한다. 마지막 서명자는 도전 ch 에 대한 전체 서명자의 응답 rsp_n 을 메시지 기안자에게 전송한다.

(3) 메시지 기안자의 다중서명 검증

메시지 기안자는 다음과 같이 전체 서명자들의 응답을 검증한다.

$$rsp_n \equiv m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \quad (\mathrm{mod} p) \qquad (3.1)$$

$$rsp_n \neq m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \quad (\mathrm{mod} p) \qquad (3.2)$$

식 3.1이 성립하면 메시지 기안자는 (R, S)가 메시지 m 에 대한 올바른 다중서명임을 확인한다. 식 3.2는 다중서명이 잘못된 경우와 서명자들 중 적어도 한 서명자 이상이 부정을 하는 경우이다. 이 경우에는 다음과 같이 추가적인 부인 프로토콜을 통해서 서명자들이 부정하는 것인지 다중서명이 잘못된 것인지 확인한다. 부인 프로토콜은 상기한 다중서명 확인 프로토콜을 한 번 더 수행하여 그 결과값을 가지고 판별식을 만든다.

두 번째 확인 프로토콜에서 메시지 기안자는 임의의 난수 (c,d) 를 선택하여 두번째 도전 ch' 을 생성하고 이에 대한 전체 서명자들의 두번째 응답 rsp_n'을 다음과 같이 생성한다.

$$a \cdot d \not\equiv b \cdot c (\mathrm{mod} p-1), \quad c, d \in Z_{p-1},$$

$$ch' \equiv R^{S \cdot c} \cdot Y^{R'' \cdot d} \pmod{p},$$

$$rsp_n' \equiv rsp_{n-1}'^{x_n^{-1}} \pmod{p}$$

판별식은 다음과 같다.

$$R_1 \equiv (rsp_n \cdot g^{-R'' \cdot b})^c (\mathrm{mod} p),$$

$$R_2 \equiv (rsp_n' \cdot g^{-R'' \cdot d})^a \pmod{p}$$

R_1 과 R_2 를 비교함으로써 서명자들의 부정인지 다중 서명이 잘못된 것인지 확인한다. $R_1 = R_2$인 경우는 다중서명이 잘못된 것이고, $R_1 \neq R_2$인 경우는 서명자들이 올바른 다중 서명에 대해서 부인하는 경우이다.

4. 부인봉쇄 다중서명 기법을 적용한 공동저작권 보호

본 절에서는 제안한 다중서명 기법의 응용에 대해서 기술한다. 디지털 콘텐츠는 많은 저작자들의 창의성과 노력으로 만들어진다. 하지만, 디지털 데이터는 그 특성 상 원본과 복사본의 구분이 불가능하기 때문에 디지털 콘텐츠 파일의 무단 복사 및 도용은 많은 저작자들의 저작 의욕을 저하시킬 뿐만 아니라 디지털 콘텐츠 사업에 심각한 위협을 초래하게 한다. 따라서 디지털 콘텐츠에 대한 불법 복제를 방지하기 위해서 저작권 정보를 생성하고 이를 디지털 콘텐츠 파일에 워터마킹하는 정보보호 기법의 적용이 필수적이다[10,11].

디지털 콘텐츠 저작은 개별적으로도 이루어질 수 있지만 대부분 여러 사람의 공동 노력으로 진행된다. 공동 저작물인 경우에 해당 디지털 콘텐츠에 대한 저작권을 저작자들이 함께 공유하여 권리를 똑같이 행사할 수 있도록 해 주는 공동 저작권 생성 및 보호 기법이 필요하다.

제안한 부인봉쇄 다중서명 기법을 적용하여 디지털 콘텐츠에 대한 공동 저작권을 생성하고 보호할 수 있는 방안에 대해서 살펴본다. 공동저작권은 3 장의 다중서명 생성 프로토콜을 이용하여 저작물에 모든 저작자들의 서명을 추가하여 생성한다. 서명 생성을 위한 개인키 추출 시에 각 저작권자의 지문 정보가 필요하기 때문에 저작권자 본인이 직접 서명 생성에 참여해야 한다. 저작권 정보는 라이센스 비용 등 경제적 가치를 지니는 민감한 데이터이기 때문에 저작권 도용 및 대리 서명 등의 부정에 안전해야 한다. 개인키 추출 후에 각 저작자는 디지털 콘텐츠에 대한 부인봉쇄 서명을 생성하고 저작권 제작자 (copyright maker)에게 이를 전송한다. 저작권 제작자는 각 저작자의 부인봉쇄 서명을 조합하여 부인봉쇄 다중서명을 생성하고 이를 디지털 콘텐츠 파일에 워터마킹한다.

부인봉쇄 다중서명이 삽입된 디지털 콘텐츠를 온라인 상에서 판매할 경우에, 구매자는 3 장의 다중서명 확인 프로토콜을 수행하여 디지털 콘텐츠 구매를 시도하게 된다. 부인봉쇄 다중서명의 특성상 모든 저작자의 동의 없이는 해당 디지털 콘텐츠의 저작권 정보를 확인할 수 없고, 저작권 정보가 확인되지 않은 디지털 콘텐츠는 판매할 수 없도록 함으로써, 저작자들의 공동의 권리를 보장한다. 또한, 저작자들은 다중서명 확인 과정에서 지문정보를 이용하여 개인키를 추출해야 하기 때문에 본인이 직접 참여해야 만 서명 확인을 할 수 있다. 저작권료 지불과 관련하여 발생할 수 있는 사기 등의 범죄 행위에 대해서 보다 안전하며 저작 권리를 안전하게 보장받을 수 있다. 공동 저작권과 관련된 분쟁이 발생하였을 경우에, 부인 프로토콜을 수행하여 삽입된 저작권 정보가 잘못된 것인지 아니면 저작자 중의 누군가가 올바른 저작권에 대해서 부인하는 것인지 밝혀낼 수 있다. 따라서 저작자들은 올바르게 삽입된 공동 저작권에 대해서 부인할 수 없다.

5. 결론

본 논문에서는 생체정보에 기반을 둔 부인봉쇄 디지털 다중서명 기법을 제안하였다. 제안한 기법은 키 생성 과정, 다중서명 생성 및 확인 과정으로 구성된다. 키 생성 과정에서 지문정보와 사용자 난수 정보를 이용하여 서명에 사용될 키를 생성하며 퍼지볼트 기법을 적용하여 지문 템플릿을 이용하여 개인키를 은닉한다. 제안한 키 생성 및 은닉 기법에서는 개인키 노출 및 도용시에 키를 재등록할 수 있으며 키 추출시에 지문정보를 입력하여 사

용자 식별 과정을 거친 후에 개인키를 추출할 수 있도록 함으로써 대리서명과 같은 위험요소를 최소화할 수 있다. 제안한 생체정보 기반의 다중서명 기법은 일반 다중서명 기법으로는 적용될 수 없는 많은 서명자와 지정된 수신자를 요구하는 응용에 적합하다. 여러 저작자의 공동 노력으로 생성된 디지털 콘텐츠에 대한 공동 저작권 생성 및 보호를 위한 용도로 활용될 수 있다.

참고문헌

[1] N. K. Ratha et al., "Enhancing security and privacy in biometric-based authentication systems", IBM System Journal, Vol.40, No.3, 2001.

[2] P. Janbandhu and M. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, Vol. 9, No. 5, 2001, pp, 205-212

[3] R. Nagpal and S. Nagpal, "Biometric based Digital Signature Schemes," Internet Draft, http://www.ietf.org/internet-drafts/draft-nagpal-biometric-digital-signature-00.txt, May 2002

[4] Ari Juels, Madhu Sudan, "A Fuzzy Vault Scheme," available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/fuzzy-vault/fuzzy-vault.pdf

[5] T.Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp.469-472, 1985.

[6] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216, 1990.

[7] F.Piper, "Digital Signatures," IFIP/SEC'91 Conference, Proceedings of the 7th International Conference and Exhibition on Information Security, pp.62-71, 1991.

[8] S.G.Akl, "Digital Signatures: A Tutorial Survey," IEEE Computer, pp.15-24, 1983.

[9] L.Harn, "(t,n) Threshold Signature and Digital Multisignature," Workshop on Cryptography & Data Security, pp.61-73, 1993.

[10] Andre Adelsbach, Birgit Pfitzmann, Ahmad-Reza Sadeghi, "Proving Ownership of Digital Content," 3rd International Information Hiding Workshop (IHW '99), LNCS 1768, Springer-Verlag, 117-133, 1999.

[11] Andre Adelsbach, Ahmad-Reza Sadeghi, "Zero-Knowledge Watermark Detection and Proof of Ownership," 4th International Information Hiding Workshop (IHW '01), LNCS 2137, Springer-Verlag, 273-288, 2001.

윤 성 현(Sung-Hyun Yun) **[정회원]**

- 1992년 2월: 고려대학교 컴퓨터학과(이학사)
- 1994년 2월: 고려대학교 컴퓨터학과 일반대학원(이학석사)
- 1997년 2월: 고려대학교 컴퓨터학과 일반대학원(이학박사)
- 1998년 3월~2002.2: LG 전자/정보통신 중앙 연구소 선임연구원
- 2002년 3월~현재: 백석대학교 정보통신학부 조교수

<관심분야>
콘텐츠 보호, 전자상거래, 정보보호