한국산학기술학회논문지
Vol. 11, No. 5, pp. 1670-1676, 2010

바이오정보 기반 전환 부인봉쇄 다중서명 기법

윤성현[1*]
[1]백석대학교 정보통신학부

The Biometric based Convertible Undeniable Multi-Signature Scheme

SungHyun Yun[1*]
[1]**Div. of Information & Communication Engineering, Baekseok University**

요 약 디지털 콘텐츠는 쉽게 조작 및 복사가 가능하며 원본과 복사본의 구분이 어렵다. 콘텐츠 저작자의 권리보호 및 안전한 콘텐츠 분배를 위해서 디지털 서명 기법이 사용된다. 일반적으로 애니메이션, 동영상, 게임 등의 디지털 콘텐츠는 여러 사람의 노력으로 완성된다. 공동 저작자들의 권리 및 권익을 보호할 수 있는 정보보호 기법의 적용이 필수적이다. 본 논문에서는 바이오정보에 기반을 둔 전환 부인봉쇄 다중서명 기법을 제안한다. 제안한 방법은 바이오정보 기반의 키를 생성하기 때문에 키 위탁이 불가능하며 서명자가 직접 서명 생성 및 검증에 참여해야 한다. 또한 필요에 따라서 부인봉쇄 서명을 일반 서명으로 전환하여 검증자에 의한 자체 서명검증이 가능하다. 제안한 방법의 응용으로 공동으로 저작된 디지털 콘텐츠에 대한 저작권 보호 및 분배 방안을 제시한다.

Abstract It is easy to reproduce and manipulate the digital contents. It's difficult to distinguish the original contents with a pirate one. A digital signature scheme is used to protect the contents author's ownership and to provide secure contents distribution. Generally, the digital contents is completed with many authors' help. It's necessary to apply a cryptographic method for protecting co-authors' rights and interests. In this paper, the biometric based convertible undeniable multi-signature scheme is proposed. In the proposed scheme, keys are generated by using a signer's biometric data. Consigning the private key to another signer is infeasible. Signers must participate in signature generation and verification stages. Our scheme also provides signature conversion protocol in which the undeniable signature is converted to the ordinary one. For applications, we show how the proposed scheme is used to protect co-authors' rights and to distribute the contents securely.

Key Words : Biometric Authentication, Biometric Based Digital Signature Scheme, Undeniable Property, Multi-Signature Scheme, Contents Business

1. 서론

사진이나 그림은 각각 필름 또는 낙관으로 원본과 저작권 소유에 대한 구분이 가능하지만 디지털화 된 이미지, 동영상 등의 콘텐츠는 원본과 복사본의 내용이 동일하기 때문에 조작 및 복제 시 이를 구분하기 어렵다. 디지털 서명 기법은 법적 구속력이 있는 서명 파일을 생성하여 서명자 인증과 메시지 인증을 가능하게 한다. 디지털 콘텐츠 소유권 증명 및 콘텐츠 분배 기법에 적용될 수 있다. 특히 디지털 콘텐츠 비즈니스를 활성화하기 위해서 저작권자(개발자), 판매자(콘텐츠 분배자), 사용자(고객) 모두가 만족할 수 있는 콘텐츠 분배 기법에 대한 연구가 필요하다.

기존의 연구[9,10]는 대부분 워터마킹, 핑거프린팅 등 저작권 보호를 위한 기법에 초점을 맞추고 있다. 콘텐츠 판매와 관련하여 저작권자의 권익을 보장하는 연구는 미

이 논문은 2006년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임.
(KRF-2006-521-D00464)
*교신저자 : 윤성현(shyoon@bu.ac.kr)
접수일 10년 04월 23일 수정일 10년 05월 11일 게재확정일 10년 05월 13일

흡한 실정이다. 저작권자는 자신이 만든 콘텐츠로 비즈니스를 할 때 정당한 수익을 기대할 수 있어야 한다. 저작권자의 권익을 보장하고 콘텐츠 비즈니스를 활성화시키기 위해서 다음과 같은 항목들을 고려해야 한다.

○ 공동 저작물에 대한 저작권 보호

일반적으로 디지털 콘텐츠는 여러 사람의 공동 작업으로 완성된다. 콘텐츠에 대한 공동 인증을 위해서 다중서명 기법의 적용이 필요하다. 단일 서명을 여러 개 생성하여 공동 인증을 하는 것보다 하나의 서명으로 표현하는 것이 서명 크기 및 관리 측면에서 효율적이다.

○ 서명키 도용 및 대리서명 방지

서명에 사용되는 키는 일반적으로 하드디스크나 이동식 저장 매체에 저장된다. 이 경우 서명키는 서명자와 독립적이기 때문에 키 도용의 위험이 있다. 서명자가 지정한 제 3 자에 의한 대리 서명이 가능하여 전자선거에서의 매표 또는 다중 서명 생성 시에 서명자에 의한 부정이 가능하다. 이를 방지하기 위해서 바이오정보의 접목은 필수적이다.

○ 저작자의 권익을 보장하는 콘텐츠 분배

디지털 콘텐츠는 저작권, 제어 정보, 서명 등을 포함한 패키지 형태로 유통된다. 저작자의 위임을 받은 판매자와 구매자 간에 콘텐츠 거래가 이루어지며 거래 후에 콘텐츠를 활성화하기 위하여 라이센스 및 서명 검증을 한다. 패키지에 서명된 저작자의 일반 서명은 자체 검증 기능을 갖기 때문에 저작자가 직접 콘텐츠 검증에 참여할 수 없다. 이 경우 저작자는 거래를 위임한 판매자의 신뢰성에 전적으로 의존할 수밖에 없다.

판매 및 콘텐츠 인증 과정을 분리하여 패키지 인증 시 저작자가 직접 개입하도록 하면 콘텐츠 유통이 투명해지고 권익을 보장받을 수 있다. 부인봉쇄 서명 기법에서 서명자는 서명 검증을 요구하는 사용자를 직접 지정할 수 있다. 더불어 저작자에 의해 검증된 콘텐츠는 구매자 편의를 위해서 자체검증 기능을 갖는 일반서명으로 전환해 줄 수 있어야 한다.

본 논문에서는 상기한 조건에 적용될 수 있는 바이오정보 기반 전환 부인봉쇄 다중서명 기법을 제안한다. 2 장에서는 기존의 바이오정보 기반 전자서명 기법에 대해서 살펴보고 3 장에서는 제안한 기법에 대해서 알아본다. 4 장에서는 서명자 부정 및 서명 전환 방법의 안전성에 대해서 분석한다. 5 장에서 기존 서명 기법과의 비교 분석 및 응용에 대해서 기술한다.

2. 관련연구

바이오정보 기반의 Janbandhu-Siyal 서명 기법과 Nagpal-Nagpal 서명 기법은 RSA 공개키 서명 방식에 기반하고 있으며 서명키 생성에 바이오정보를 이용한다.

2.1. Janbandhu-Siyal 서명 기법[1]

Janbandhu와 Siyal이 제안한 기법은 바이오정보를 접목한 공개키 기반의 디지털서명 방법이다.

- 키 생성을 위해서 각각 256 바이트 크기의 매우 큰 소수 p와 q를 구하고 법 $n=p\times q$과 오일러 함수 $\phi(n)=(p-1)(q-1)$ 을 구한다.
- 홍채 템플릿으로부터 512 바이트 크기의 수를 추출하여 1씩 증가시켜 $\phi(n)$ 과 서로소가 되는 값을 찾아 개인키 d를 구한다.
- 공개키 $e=d^{-1}\bmod\phi(n)$ 를 계산한다.
- 메시지를 해쉬하고 이 값을 개인키로 RSA 암호화하여 디지털 서명을 만든다.
- 서명자는 검증자와 공유하는 비밀키로 디지털 서명을 암호화하고 이를 검증자에게 전송한다.
- 검증자는 공유 비밀키로 암호문을 복호한다. 추출된 해쉬값을 이용하여 디지털 서명을 검증한다.

2.2. Nagpal-Nagpal 디지털 서명 기법[2]

R. Nagpal과 S. Nagpal에 의해 제안된 서명 기법은 RSA 방식에 기반하고 있으며 사용자로부터 망막, 홍채, 지문 정보를 스캔하고, 이 값으로부터 p, q, e를 각각 구한 후, $\phi(n)$ 과 개인키 d를 구한다.

- 키 생성은 512 바이트 크기의 망막 템플릿으로부터 64 바이트 크기의 p를 구하는데 1씩 증가하여 소수가 되는 값을 찾는다.
- 512 바이트 크기의 홍채 템플릿으로부터 64 바이트 크기의 q를 구하는데 1씩 증가하여 소수가 되는 값을 찾는다.
- 법 $n=p\times q$과 오일러 함수 $\phi(n)=(p-1)(q-1)$ 을 구한다.
- 512 바이트 크기의 지문 템플릿으로부터 공개키 e를 구하는데 1씩 증가하여 $\phi(n)$ 과 서로소가 되는 값을 찾는다.
- 개인키 $d=e^{-1}\bmod\phi(n)$ 를 구한다.
- RSA 알고리즘을 이용하여 개인키로 메시지 해쉬 값을 암호화하여 검증자에게 전달한다.
- 검증자는 서명자의 공개키를 서버에게 요청하여 획득하고 수신한 메시지의 해쉬값을 구한 후에 RSA 서명 검증을 한다.

3. 바이오기반 다중서명 생성 및 검증

제안한 기법은 서명자들의 동의에 의해서만 서명 검증이 가능한 부인봉쇄 성질을 가지며 개인의 바이오정보에 기반 함으로써 서명 위탁이 불가능하다. 또한 필요에 따라서 부인봉쇄 성질을 제거하여 자체검증 기능을 갖는 일반 다중서명으로의 전환이 가능하다.

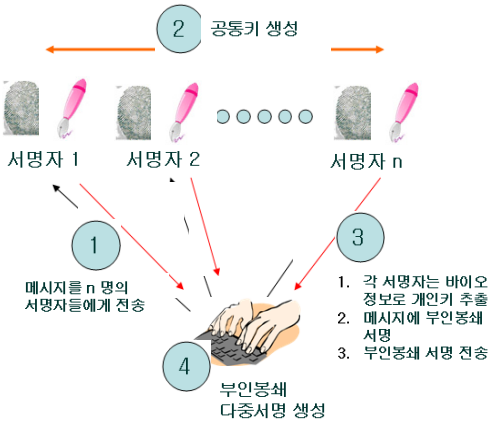
3.1. 바이오 기반 키 생성 및 은닉

다중서명 생성 및 검증에 참여하는 서명자들은 각각 자신의 바이오정보를 이용하여 개인키와 공개키를 생성한다. n 명의 서명자들이 참여한다고 가정할 때 각 서명자의 개인키 sk_i 및 공개키 pk_i 는 다음과 같다.

서명자 S_i의 개인키	$sk_i = H(BT_i,\ RN_i) \in Z_{p-1},\ i=[1..n]$
서명자 S_i의 공개키	$pk_i \equiv g^{sk_i} (\mathrm{mod}\, p)\ ,\ i=[1..n]$
· p 는 큰 소수로 p 를 법으로 하는 유한체 $GF(p)$ 를 가정한다. g 는 법 p 에 대한 위수 $p-1$ 을 갖는 생성자이다. · BT_i : 서명자 S_i의 바이오 템플릿 · RN_i : 서명자 S_i의 난수 · H : 해쉬 함수	

개인키는 퍼지볼트 기법을 적용하여 서명자 바이오 템플릿에 은닉한다[3, 11]. 서명 생성 및 검증 시 개인키 추출을 위해서 반드시 바이오정보를 입력해야 한다.

3.2 부인봉쇄 다중서명 생성



[그림 1] 부인봉쇄 다중서명 생성

그림 1은 서명 제작자와 n 명의 서명자가 부인봉쇄 다중서명을 생성하는 단계를 보여준다. 서명 제작자는 서명자들 모두가 신뢰하는 제 3 자라고 가정한다.

서명 제작자는 메시지 msg 에 대한 해쉬 값 msg_H가 법 p 에 대한 원시근이 되도록 임의의 난수 k_0 를 선택하여 1씩 증가시키면서 메시지 msg 와 함께 해쉬한다.

$msg_H = H(msg,\ k_0)$

서명 제작자는 (msg, k_0, msg_H) 를 n 명의 서명자들에게 전송한다.

○ 첫 번째 서명자의 공통키 생성

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

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

단계 2 : 공통 공개키 PK 를 생성하기 위해서 첫 번째 서명자의 공개키를 다음과 같이 설정한다.

$PK_1 = pk_1$

단계 3 : 첫 번째 서명자는 단계 1과 단계 2에서 생성된 $(r_1,\ PK_1)$ 을 두 번째 서명자에게 전송한다.

○ 중간 서명자의 공통키 생성($i=[2..n]$)

단계 1 : 서명자 S_i는 이전 서명자 S_{i-1}로부터 $(r_{i-1},\ PK_{i-1})$ 을 수신한다.

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

$$r_i \equiv r_{i-1}^{k_i} (\mathrm{mod} p),\ \gcd(k_i,\ p-1)=1$$

단계 3 : 서명자 S_i는 자신의 개인키 sk_i 를 이용하여 다음과 같이 PK_i 를 생성한다.

$$PK_i \equiv PK_{i-1}^{sk_i} (\mathrm{mod} p)$$

단계 4 : 서명자 S_i는 서명자 S_{i+1}에게 $(r_i,\ PK_i)$ 를 전송한다.

단계 5 : 마지막 서명자까지 단계 1부터 단계 4를 반복한다. 마지막 서명자 S_n은 $(R,\ PK)$ 를 서명 제작자와 모든 서명자들에게 전송한다.

$$R \equiv r_{n-1}^{k_n} (\mathrm{mod} p),\ PK \equiv PK_{n-1}^{sk_n} (\mathrm{mod} p)$$

○ 다중서명 생성

서명자들은 각자의 바이오정보로 개인키를 추출하여 메시지에 대한 부인봉쇄 서명을 생성한다.

단계 1 : 서명자 S_i는 R 을 이용하여 다음 식을 만족하는 s_i 를 구한다. k_i 와 $p-1$ 은 서로소이므

로 s_i 에 대한 유일한 해가 존재한다.

$$k_i \cdot s_i \equiv sk_i \cdot R - k_i \cdot msg_h \pmod{p-1}$$

단계 2 : 서명자 S_i는 부인봉쇄 서명 s_i 를 서명 제작자에게 전송한다.

단계 3 : 서명 제작자는 다음과 같이 다중서명 S를 생성한다.

$$S \equiv \prod_{j=1}^{n}(msg_h + s_j) \pmod{p-1}$$

3.3 부인봉쇄 다중서명 검증

검증자는 $(R,\ S)$가 메시지 msg에 대한 올바른 다중서명인지 확인하기 위해서 순차적으로 다중서명을 검증한다. 검증자는 ch를 생성하여 첫 번째 서명자에게 전송한다. $(a,\ b)$는 검증자가 선택한 임의의 두 난수이다.

$$ch \equiv R^{S \cdot a} \cdot PK^{R^n \cdot b} \pmod{p}$$

○ 첫 번째 서명자의 응답 생성

단계 1 : 첫 번째 서명자는 자신의 바이오정보로 개인키 sk_1을 추출한다.

단계 2 : ch에 대한 응답 rsp_1을 생성하여 두 번째 서명자에게 전송한다.

$$rsp_1 \equiv ch^{sk_1^{-1}} \pmod{p}$$

$$sk_1 \cdot sk_1^{-1} \equiv 1 \pmod{p-1}$$

○ 서명자 S_i의 응답 생성$(i = [2..n])$

단계 1 : 서명자 S_i는 자신의 바이오정보로 개인키 sk_i를 추출한다.

단계 2 : 서명자 S_i는 ch에 대한 응답 rsp_i를 생성하여 서명자 S_{i+1}에게 전송한다.

$$rsp_i \equiv rsp_{i-1}^{sk_i^{-1}} \pmod{p}$$

단계 3 : 마지막 서명자까지 단계 1과 단계 2를 반복한다. 마지막 서명자 S_n은 ch에 대한 응답 rsp_n을 검증자에게 전송한다.

○ 검증자의 다중서명 검증

검증자는 rsp_n이 $msg_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p}$와 일치하는지 확인한다.

4. 안전성 분석

서명자에 의한 부정과 일반 다중서명으로 전환할 경우의 안전성에 대해서 분석한다.

4.1 서명자 부정

$$rsp_n \neq msg_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p} \quad (4.1)$$

검증자가 식 4.1과 같이 다중서명 검증에 실패하면 서명자에 의한 부정인지를 식별해야 한다.

검증자는 임의의 난수 (c,d)를 선택하여 ch'을 생성하고 3.3 절의 검증 프로토콜을 수행하여 서명자들의 응답 $rsp_n{}'$을 구한다.

$$ch' \equiv R^{S \cdot c} \cdot PK^{R^n \cdot d} \pmod{p}$$

$$a \cdot d \neq b \cdot c \pmod{p-1}$$

$$rsp_n{}' \equiv ch'^{\prod_{j=1}^{n} sk_j^{-1}} \pmod{p}$$

다음 판별식 R_1과 R_2가 같지 않으면 서명자가 올바른 다중 서명에 대해서 부인하는 경우이다.

$$R_1 \equiv (rsp_n \cdot g^{-R^n \cdot b})^c \pmod{p}$$

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

[정리 4.1] 올바른 다중서명에 대해서 서명자들은 부인할 수 없다. 한 서명자 이상이 부인하는 경우에 서명자의 부정을 입증할 수 있다.

(증명)

msg_h에 대한 올바른 서명 (R,S)는 다음과 같다.

·올바른 다중서명 (R,S)

$$R \equiv msg_h^{\prod_{j=1}^{n} k_j} \pmod{p}$$

$$S \equiv \prod_{j=1}^{n}(msg_h + s_j) \pmod{p-1}$$

$$X \equiv \prod_{j=1}^{n} sk_j \pmod{p-1}$$

$$\prod_{j=1}^{n} k_j (msg_h + s_j) \equiv R^n \cdot X \pmod{p-1}$$

서명자들 중 누군가가 서명에 대해서 부정할 경우 응답 과정에서 ch에 대한 모듈라 곱셈의 역이 변하게 된다. 올바른 모듈라 곱셈의 역은 X^{-1}이고 잘못된 역은 X'^{-1}라 가정한다.

$$X^{-1} \equiv \prod_{j=1}^{n} sk_j^{-1} \pmod{p-1}$$

$$X'^{-1} \equiv \prod_{j=1}^{n} sk_j'^{-1} \pmod{p-1} \quad ,\ sk_j \neq sk_j'$$

검증자는 다중서명 (R,S)의 검증을 위해서 다음과

같이 ch 를 생성한다.

$$ch \equiv R^{S \cdot a} \cdot PK^{R^n \cdot b} (\mathrm{mod} p)$$
$$\equiv msg_h^{a \cdot R^n \cdot X} \cdot g^{b \cdot R^n \cdot X} (\mathrm{mod} p)$$

ch 에 대한 서명자들의 응답 rsp_n 은 다음과 같다.

$$rsp_n \equiv ch^{X^{-1}} (\mathrm{mod} p)$$
$$\equiv msg_h^{a \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{b \cdot R^n \cdot X \cdot X^{-1}} (\mathrm{mod} p)$$

$$rsp_n \not\equiv msg_h^{a \cdot R^n} \cdot g^{b \cdot R^n} (\mathrm{mod} p) \quad (4.2)$$

식 4.2와 같이 검증에 실패한 경우 검증자는 ch' 을 생성하고 이에 대한 응답 rsp_n' 을 구한다.

$$ch' \equiv R^{S \cdot c} \cdot PK^{R^n \cdot d} (\mathrm{mod} p)$$
$$\equiv msg_h^{a \cdot R^n \cdot X} \cdot g^{b \cdot R^n \cdot X} (\mathrm{mod} p)$$
$$rsp_n' \equiv ch'^{X^{-1}} (\mathrm{mod} p)$$
$$\equiv msg_h^{c \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{d \cdot R^n \cdot X \cdot X^{-1}} (\mathrm{mod} p)$$

$$rsp_n' \not\equiv msg_h^{c \cdot R^n} \cdot g^{d \cdot R^n} (\mathrm{mod} p) \quad (4.3)$$

식 4.2와 4.3에서 서명자들의 응답은 검증자가 생성한 검증 값과 다르다. 검증자는 rsp_n, rsp_n' 을 이용해서 다음 식을 계산한다.

$$R_1 \equiv (rsp_n \cdot g^{-R^n \cdot b})^c$$
$$\equiv msg_h^{a \cdot c \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{c \cdot (b \cdot R^n \cdot X \cdot X^{-1} - b \cdot R^n)}$$
$$R_2 \equiv (rsp_n' \cdot g^{-R^n \cdot d})^a$$
$$\equiv msg_h^{c \cdot a \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{a \cdot (d \cdot R^n \cdot X \cdot X^{-1} - d \cdot R^n)}$$

제안한 부인 프로토콜에서 서명자들이 부정을 하는 경우에 다음 식과 같이 R_1 과 R_2 는 다른 값을 갖게 된다.

$$msg_h^{a \cdot c \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{c \cdot b \cdot R^n \cdot (X \cdot X^{-1} - 1)}$$
$$\not\equiv msg_h^{c \cdot a \cdot R^n \cdot X \cdot X^{-1}} \cdot g^{a \cdot d \cdot R^n (X \cdot X^{-1} - 1)}$$
$$(\because\ b \cdot c \not\equiv d \cdot a (\mathrm{mod} p-1)\ \ )$$

Z_{p-1} 상에서 선택된 a, b, c, d 는 검증자가 생성한 것으로 서명자들은 이 값을 모르기 때문에 R_1 과 R_2 를 같게 할 수 없다. Q.E.D.

4.2 다중서명 전환

부인봉쇄 다중서명을 일반 다중서명으로 전환하는 방법은 다음과 같다.

- 첫 번째 서명자는 $g^{k_1} (\mathrm{mod} p)$ 를 생성하여 두 번째 서명자에게 전송한다.
- 서명자 $S_i (i = [2..n])$는 $g^{K_{i-1}} (\mathrm{mod} p)$ 를 수신한다.
  $K_{i-1} = \prod_{j=1}^{i-1} k_j$.
- k_i 를 이용하여 $g^{K_i} \equiv (g^{K_{i-1}})^{k_i} (\mathrm{mod} p)$ 를 계산한다.
- 마지막 서명자는 $g^{K_n} (\mathrm{mod} p)$ 를 서명 제작자에게 전송한다.
- 서명 제작자는 $g^{K_n} (\mathrm{mod} p)$ 를 공개함으로써 부인봉쇄 다중서명을 일반 다중서명으로 전환한다.

다음 식은 전환된 다중서명이 서명자들의 도움 없이 자체적으로 검증될 수 있음을 보여준다.

$$sk_i \cdot R \equiv k_i (s_i + msg_h)\ \ (\mathrm{mod} p-1), [i = 1..n]$$
$$PK \equiv g^{\prod_{j=1}^{n} sk_j} (\mathrm{mod} p)$$
$$S \equiv \prod_{j=1}^{n} (msg_h + s_j) (\mathrm{mod} p-1)$$
$$(g^{K_n})^S \equiv PK^{R^n} (\mathrm{mod} p)$$

5. 비교 분석 및 응용

기존의 전자서명 기법과 제안한 서명기법을 기능적인 측면에서 비교 분석하고 응용 방안에 대해서 기술한다.

5.1 비교분석

[표 1] 기능 및 효율성 비교

기능 및 효율성 비교	서명생성 단계	서명검증 단계	다중서명크기
	서명위탁	자체검증	서명자 수에 비례
일반 서명 기법[1]	O	O	비례함
바이오 기반 서명 기법[2]	X	O	비례함
부인봉쇄 서명 기법[3]	O	X	비례함
일반 다중서명 기법[4]	O	O	비례하지 않음
제안한 기법	X	△	비례하지 않음

O : 가능함, X : 불가능함, △ : 가능함 또는 불가능함
1) 일반 서명 기법 : RSA[4], DSA[5], Elgamal[6]
2) 바이오 기반 서명 기법 : Janbandun[1], Nagpal[2]
3) 부인봉쇄 서명 기법 : Chaum[8]
4) 일반 다중서명 기법 : Harn[7]

RSA, DSA, Elgamal 기반의 일반 서명 기법, 바이오 기반의 일반 서명 기법, 부인봉쇄 서명 기법, 일반 다중서명 기법, 제안한 기법을 기능적인 측면에서 비교 분석한다.

일반 서명 기법[4,5,6], 다중서명 기법[7], 부인봉쇄 서명 기법[8]은 서명 생성 시 서명자에 의한 서명 위탁의 위험이 있다. 서명자가 서명 생성에 사용되는 개인키를 제 3 자에게 위탁함으로써 대리 서명이 가능하다. 전자선거 등의 응용에서 매표 행위로 악용될 수 있다. 바이오정보를 이용하여 서명키를 생성하고 추출할 수 있어야만 서명 위탁을 방지할 수 있다. 제안한 기법, Janbandu-Siyal 기법[1], Nagpal-Nagpal 기법[2]은 바이오 기반 서명 방식으로 서명 위탁으로부터 안전하다.

부인봉쇄 성질이 없는 일반 서명 기법[1,2,4,5,6,7]은 자체 검증 기능을 갖는다. 검증자는 서명자의 도움 없이 디지털 서명을 검증할 수 있다. Chaum의 서명 기법[8]과 제안한 기법은 부인봉쇄 성질을 갖기 때문에 서명자가 검증자를 선택할 수 있고 서명자의 개입 없이는 검증이 이루어질 수 없다. 콘텐츠 구매 후의 활성화를 위한 라이센스 및 서명 검증 과정에 서명자(판매자 또는 저작권자)가 직접 참여함으로써 콘텐츠 분배에 대한 신뢰를 확보할 수 있다. 또한 제안한 기법은 구매자가 자체적으로 서명을 검증할 수 있도록 부인봉쇄 서명을 일반 서명으로 전환할 수 있다. 활성화된 콘텐츠의 부인봉쇄 서명을 일반 서명으로 전환함으로써 콘텐츠 사용의 편의성을 도모한다.

단일 서명 기법[1,2,4,5,6,8]을 이용하여 공동 서명을 표현하려면 서명자 수 만큼의 서명이 필요하다. 제안한 기법과 Harn의 다중서명 기법[7]을 이용하면 하나의 서명으로 여러 서명자들의 서명을 표현할 수 있다.

5.2 응용

일반적으로 디지털 콘텐츠는 저작자의 권리 보호를 위해서 저작권 정보를 콘텐츠에 워터마킹하고 제어, 권한 정보 등과 같은 메타 데이터를 함께 패키징하여 배포한다. 패키징 된 콘테이너 파일은 사용자가 올바른 콘텐츠와 라이센스를 구매 했는지 인증할 수 있도록 디지털 서명을 한다. 사용자는 서명을 검증함으로써 구매한 콘텐츠의 내용과 서명자(판매자 또는 저작자)에 대해서 인증한다.

콘텐츠는 저작자가 직접 판매하는 경우보다 위임을 받은 전문 판매자를 통해서 거래되는 경우가 보다 일반적이다. 일반 서명은 자체 검증 기능을 갖기 때문에 저작자는 자신이 만든 콘텐츠에 대한 구매 여부를 직접 확인할 수 없다. 판매자에 의한 부정이 가능하며 이를 방지하기 위해서는 저작자가 직접 콘텐츠 구매 여부를 확인할 수 있어야 한다.

부인봉쇄 서명은 서명자의 동의 없이는 서명 검증이 불가능하다. 저작자는 콘텐츠 패키지에 부인봉쇄 서명하고 구매된 콘텐츠에 대한 사용자의 서명 검증을 직접 도와준다. 서명 검증 후에는 부인봉쇄 서명을 일반 서명으로 전환하여 사용자가 매 번 서명 검증을 위하여 저작자의 도움을 요청하지 않도록 한다.

제안한 서명 기법을 이용하여 서명된 콘텐츠 패키지를 온라인으로 판매할 경우에, 구매자는 다중서명 검증 프로토콜을 진행하여 구매한 콘텐츠에 대한 인증을 시도한다. 부인봉쇄 다중서명의 특성상 모든 저작자의 동의 없이는 해당 패키지의 서명을 확인할 수 없고, 인증이 안 된 콘텐츠는 사용할 수 없도록 제어함으로써 저작자들의 권익을 보장할 수 있다. 또한, 저작자들은 바이오정보를 이용하여 다중서명 생성 및 검증을 하기 때문에 키 도용 및 위탁에 따른 공모 위험을 최소화할 수 있다. 공동 저작권과 관련된 분쟁이 발생하였을 경우에, 서명자의 부정 여부를 식별할 수 있으며 저작자들은 콘텐츠 패키지에 서명한 다중서명에 대해서 부인할 수 없다.

6. 결론

본 논문에서는 바이오정보 기반의 전환 부인봉쇄 다중서명 기법을 제안하였다. 제안한 기법은 부인봉쇄 성질을 만족하며 필요에 따라 일반 다중서명으로 전환할 수 있다. 바이오정보를 이용하여 서명키를 생성 및 검출하기 때문에 서명 생성 및 검증 과정에 반드시 서명자 본인이 참여해야 한다. 서명 위탁을 통한 서명자들 간의 공모, 전자 선거에서의 매표 위험 등을 최소화 할 수 있다.

다중서명 검증에 실패했을 경우에 서명자 부인 여부를 식별할 수 있으며 서명 전환 시의 안전성에 대해서 분석하였다. 제안한 기법과 기존 기법과의 차이를 기능적인 측면에서 분석하였으며 공동 저작된 콘텐츠 분배 시 저작권자의 권익을 보장할 수 있는 방법에 대해서 논의하였다.

참고문헌

[1] 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.

[2] R. Nagpal and S. Nagpal, "Biometric based Digital Signature Schemes," Internet Draft, http://tools.ietf.

org/id/draft-nagpal-biometric-digital-signature-00.txt, May 2002.
[3] A. Juels and M. Sudan. A Fuzzy Vault Scheme. International Symposium on Information Theory, 2002.
[4] R.L.Rivest, A.Shamir, L.Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, ACM, Vol. 21, No. 2, 1978.
[5] FIPS PUB 186-3, Digital Signature Standard(DSS), NIST, 2009.
[6] 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.
[7] L. Harn, "Group-Oriented (t, n) threshold digital signature scheme and digital multisignature," IEE Proc-Comput. Digit. Tech., vol. 141, No. 5, Sep. 1994, pp. 307-313.
[8] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216, 1990.
[9] 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.
[10] 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.
[11] ITU-T X.1088, A Framework for biometric digital key generation, 2008.

윤 성 현(SungHyun Yun) **[정회원]**

- 1992년 2월 : 고려대학교 컴퓨터학과 (이학사)
- 1994년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학박사)
- 1994년 3월 ~ 1998년 2월 : 고려대학교 기초과학연구소 연구원
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야>
콘텐츠 보호, 모바일 OS, 모바일 보안, 전자상거래