The Journal of Digital Policy & Management 2013 Sep; 11(9): 173-179

서버 기반 실시간 바이오메트릭 서명 기법

윤성현*
백석대학교 정보통신학부*

The Server based Realtime Biometric Signature Scheme

Sunghyun Yun*
Div. of Information & Communication Engineering, Baekseok University*

요 약 바이오메트릭 인증은 사용자 고유의 신체 정보인 바이오메트릭 데이터를 이용하여 제 3자에게 본인임을 입증하는 것이다. 사용자는 매 인증 세션 마다 직접 참여해야 하기 때문에 제 3자에 의한 대리 인증이 불가능하다. 바이오메트릭 서명은 인증과 달리 서명한 메시지 내용이 틀림이 없다는 것을 제 3자에게 입증하는 것이다. 서명에 사용된 개인키는 바이오메트릭 데이터를 이용하여 생성된다. 하지만 일단 생성된 서명키는 서명자가 접근할 수 있어서 제 3자에게 서명키를 임대할 수 있다. 본 연구에서는 서명자가 직접 서명에 참여해야 하는 서버 기반의 실시간 바이오메트릭 서명 기법을 제안한다. 제안한 기법은 대리서명이 허용되지 않는 전자 선거에서의 투표권 인증, DRM이 적용된 모바일 상거래에서의 저작권자 인증에 적용될 수 있다.

주제어 : 바이오메트릭 인증, 바이오메트릭 서명, 실시간 사용자 인증, 서버 기반 서명, 전자투표

Abstract In a biometric authentication scheme, a user's biometric data that is unique to the user is used to prove the user's identity to the third party. Since the user should have to participate in every authentication sessions, it's not possible to delegate other users to authenticate instead of himself/herself. In a biometric signature scheme, contrary to authentication scheme, a user's biometric data is used to prove that "this message is signed by the signer who claims to be" to the third party. However, once the biometric key is created, it can be accessed by the signer. Thus, it's possible to lend the biometric key to other users. In this study, the server based biometric realtime signature scheme is proposed. The proposed scheme can be applied to sign the vote in electronic voting or to authenticate the copyright owner in DRM enabled mobile commerce where the proxy signatures are not allowed.

Key Words : Biometric Recognition, Biometric Signature, Realtime User Authentication, Proxy Signature Scheme, Electronic Voting

1. 서론

사용자 인증은 제 3자에게 본인의 신분을 입증하는 것으로 사용자의 기억에 기반을 두는 패스워드 방식, 사용자가 가지고 있는 것에 기반을 두는 카드 방식 그리고 사용자 고유의 바이오메트릭 정보를 이용하는 방식으로 구

* 본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(지역대학우수과학자사업, No. 2012-0004515)
Received 21 July 2013, Revised 25 August 2013
Accepted 20 September 2013
Corresponding Author: Sunghyun Yun(Baekseok University)
Email: shcrpt@gmail.com

ISSN: 1738-1916

분된다.

패스워드 방식은 비용이 적게 들고 사용이 편리한 장점이 있지만 다른 사용자에게 아이디와 패스워드를 임대하여 본인 대리로 인증하는 것이 가능하다.

카드 방식은 주민등록증, 여권, 스마트카드 등과 같이 본인임을 증명하는 카드를 가지고 제 3자에게 본인임을 입증하는 것이다. 주로 오프라인 인증에 많이 사용되고 온라인 인증을 위해서는 카드 리더기가 있어야 한다. 사용자가 항상 가지고 다녀야 하는 불편함이 있고 카드 위조가 가능하여 제 3자에 의한 가장 공격에 취약하다.

바이오메트릭 인증은 사용자의 바이오메트릭 데이터를 이용하여 본인임을 입증하는 것이다. 지문, 홍채 등과 같은 바이오메트릭 데이터는 신체의 일부분이기 때문에 도난 및 위조의 위험이 카드 방식과 비교하여 상대적으로 적다 [1, 10].

최근의 스마트폰은 음성, 지문, 얼굴모양 등을 캡춰할 수 있는 다양한 센서가 내장되어 있고 이를 활용할 수 있는 SDK도 함께 배포되어 바이오메트릭 인증 기술을 응용한 앱 개발이 가능하다. 더불어 매우 높은 시장 점유율을 갖는 스마트폰의 보급은 바이오메트릭 인증을 대중화하는 최적의 플랫폼이 되고 있다 [1, 2].

바이오메트릭 인증은 전자 투표, DRM이 적용된 상거래와 같이 대리 인증이 허용되지 않는 곳에 가장 적합한 인증 방법이다. 온라인에서는 그 특성상 로그인한 사용자들을 볼 수 없기 때문에 다른 사용자에 의한 대리 인증이 가능하다. 따라서 로그인한 사용자가 정말 사용자 본인인지 확인하기 위해서는 바이오메트릭 인증이 적용되어야 한다.

바이오메트릭 서명은 서명한 메시지에 대한 내용이 틀림이 없다는 것과 본인이 서명했다는 것을 제 3자에게 입증하는 것이다. 바이오메트릭 데이터가 접목된 서명키를 이용하여 메시지를 서명하고 검증한다. 서명자는 서명키에 접근할 수 있음으로 제 3자에게 서명키를 위임하여 대리로 서명하게 할 수 있다.

바이오메트릭 인증이 필요한 이유는 인터넷과 같이 상대방을 볼 수 없는 환경에서 상대방이 정말 그 사용자가 맞는지 확인하기 위해서이다. 마찬가지로 바이오메트릭 서명도 서명자 본인이 직접 서명했다는 것과 직접 검증했다는 것을 입증할 수 있어야 한다. 기존의 연구는 바이오메트릭 데이터를 이용한 서명키 생성에 관한 것이 대부분이고 서명자가 직접 참여하는 실시간 서명에 대한 연구는 미흡한 실정이다 [4, 5].

본 연구에서는 서명자가 직접 서명에 참여하는 서버 기반의 실시간 바이오메트릭 서명 기법을 제안한다. 제안한 방법은 바이오메트릭 데이터 기반의 키 생성 및 등록, 서명 생성 및 검증 프로토콜로 구성된다. 서명자에 의한 실시간 서명 인증과 검증이 가능하기 때문에 전자 선거에서의 투표권 서명, DRM이 적용된 모바일 상거래에서의 저작권자 인증과 같이 대리 인증이 허용되지 않는 응용에 적용될 수 있다.

2 장에서는 바이오메트릭 인증과 서명 기법에 대한 기존의 연구를 살펴보고 3 장에서는 서버 기반의 실시간 바이오메트릭 서명 기법을 제안한다. 4 장에서는 제안한 기법과 기존의 바이오메트릭 서명 기법과의 차이점을 분석하고 5 장에서는 결론 및 향후 연구 과제를 제시한다.

2. 연구 배경

바이오메트릭 인증과 관련된 주요 이슈를 살펴보고 바이오메트릭 서명 기법과의 차이점을 분석한다.

2.1 바이오메트릭 인증

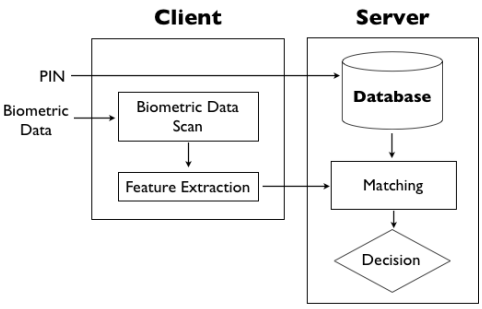
바이오메트릭 인증은 사용자의 바이오메트릭 데이터를 이용하여 해당 사용자의 신분을 확인하는 것이다. 사용자가 입력한 바이오메트릭 데이터와 이전에 등록한 바이오메트릭 데이터를 비교하여 얼마나 유사한 지에 따른 확률로 사용자를 인증한다. 본인이 직접 인증 세션에 참여해야 하기 때문에 제 3자가 사용자를 대신하여 인증할 수 없다.

바이오메트릭 데이터는 스캐너를 이용하여 캡춰되고 디지털 파일로 저장된다. 저장된 이미지를 가공하여 특징점을 추출하고 이 점들의 좌표 값으로 구성된 템플릿 파일을 생성한다. 매칭 단계에서는 스캔한 템플릿과 데이터베이스에 등록된 템플릿 간의 유사도를 비교한다. 동일한 사용자라도 항상 똑 같이 스캔할 수 없기 때문에 바이오메트릭 인증은 두 템플릿이 얼마나 일치하는지 확률로 인증해야 한다.

바이오메트릭 데이터로부터 생성된 템플릿은 사용자 고유 정보이기 때문에 제 3자에게 노출되면 재사용할 수

없다. 따라서 템플릿은 취소 및 재등록이 가능하도록 원본이 아닌 변형된 형태로 저장되어야 한다. 원본 변형을 위한 함수는 일방향성을 가져야 하고 원본의 성질을 그대로 유지할 수 있어야 한다 [3].

바이오메트릭 인증 모델은 스탠드얼론(stand-alone)과 네트워크 모델로 구분된다. 인터넷 기반 서비스에는 네트워크형 인증 모델이 적합하다. 그림 1은 클라이언트-서버 기반의 바이오메트릭 인증 모델을 보여준다. 클라이언트는 바이오메트릭 데이터를 스캔하여 템플릿을 만들고 이를 서버로 전송한다. 서버는 PIN 번호를 이용하여 데이터베이스에 등록된 클라이언트 템플릿과 수신한 템플릿을 비교하여 사용자를 인증한다. 인터넷은 공중망이기 때문에 템플릿이 전송 중에 노출될 위험이 있다. 따라서 안전한 템플릿 전송을 위하여 암호화 및 서명 등의 정보보호 기술을 템플릿 파일에 접목하는 것이 필수적이다.



PIN: Personal Identification Number

[Fig. 1] Network based Biometric Recognition Model

네트워크형 바이오메트릭 인증 모델에서 클라이언트와 서버간의 일대일 인증은 비대면으로 이루어지고 클라이언트의 바이오메트릭 템플릿은 서버의 데이터베이스에 보관되어 있어야 한다. 바이오메트릭 템플릿은 개개인의 고유한 신체 정보이어서 인증 과정에서 개인 프라이버시 침해 위험성이 높다. 따라서 인터넷에서 바이오메트릭 인증 모델을 활용하기 위해서는 바이오메트릭 템플릿을 체계적으로 인증 및 관리할 수 있는 PKI(Public Key Infrastructure)와 같은 정부 주도의 바이오메트릭 템플릿 신뢰 기반 구조가 만들어져야 한다.

2.2 바이오메트릭 서명

일반적으로 공개키 암호를 이용한 디지털 서명 기법에서 개인키는 서명을 생성하고 공개키는 서명을 검증하는 용도로 사용된다. 바이오메트릭 서명 기법에서 개인키와 공개키는 사용자의 바이오메트릭 템플릿을 이용하여 생성된다 [4, 5]. 사용자는 키 생성 과정에 직접 참여하여 바이오메트릭 데이터를 입력해야 한다. 하지만 키가 생성 된 이후에는 일반 서명 기법에서와 똑 같이 서명 생성 및 검증이 이루어지기 때문에 서명자는 개인키를 제3자에게 임대하여 본인을 대신하여 서명하게 할 수 있다.

대리 서명은 서명자가 서명키에 접근할 수 있기 때문에 발생하는 문제이다. 이를 해결하려면 바이오메트릭 인증을 통해서 서명자 인증이 된 후에만 서명자가 본인의 개인키에 접근할 수 있어야 한다. 퍼지볼트 기법으로 개인키를 사용자 템플릿에 은닉하고 추출하는 방법이 대표적인 사례이다 [6]. 서명자는 템플릿에 은닉된 개인키를 추출하기 위하여 매 세션마다 본인의 바이오메트릭 데이터를 제출해야 한다.

바이오메트릭 서명은 서명에 사용된 키가 서명자의 바이오메트릭 데이터로부터 만들어진다는 점을 제외하면 일반 서명 기법에서 제공하는 서명 생성 및 검증 프로토콜과 차이점이 없다. 일반적으로 서명 검증에 서명자의 공개키가 이용되며 공개키는 제 3자가 접근할 수 있고 서명자의 도움 없이 서명 검증이 가능하다. 따라서 검증자는 바이오메트릭 서명을 검증하는 과정에서 서명자 본인이 직접 서명한 것인지 아니면 대리로 서명한 것인지 구분할 수 없다.

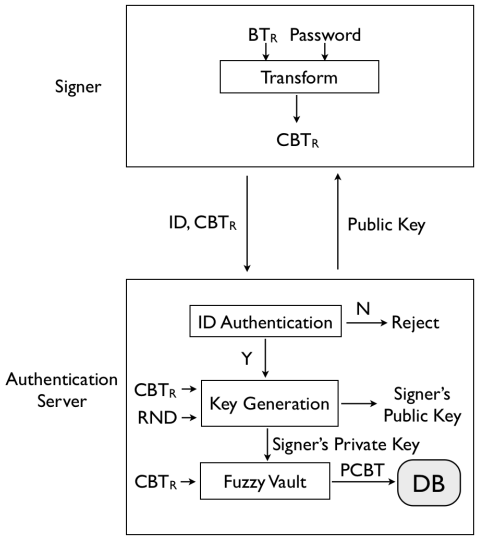
3. 서버 기반 바이오메트릭 서명 기법

본 논문에서는 서명 생성 및 검증 단계에 서명자가 직접 참여하는 바이오메트릭 서명 기법을 제안한다. 제안한 서명 기법은 키 생성, 서명 생성 그리고 서명 검증 프로토콜로 구성된다.

서명자가 개인키에 접근할 수 있으면 서명 임대가 가능하기 때문에 바이오메트릭 서명은 다음과 같은 요구사항을 만족해야 한다.

구분	요구사항
서명 생성	- 서명자 본인이 직접 서명해야 함 - 제 3자에 의한 대리 서명이 불가해야 함
서명 검증	- 일반적인 서명 검증 기법으로는 해당 서명이 임대된 것인지, 아니면 서명자가 직접 서명한 것인지 확인할 수 없음 - 서명자는 제 3자에게 바이오메트릭 서명이 본인에 의해서 직접 생성된 것임을 증명할 수 있어야 함

3.1 서명키 생성 및 등록



BT: Biometric Template, CBT:Cancelable Biometric Template

RND: RaNDom number, PCBT:Protected CBT

[Fig. 2] Registration of the Biometric Template and the Private Key

그림 2는 바이오메트릭 템플릿을 이용한 공개키 및 개인키 생성 방법을 보여준다. 인증 서버(Authentication Server)는 PKI에서의 CA(Certificate Authority)와 같이 모든 사용자들이 신뢰하는 기관이라고 가정한다.

단계 1: 서명자(Signer)는 자신의 바이오메트릭 데이터를 스캔하여 템플릿 BT_R을 만든다. BT_R과 서명자만 알고 있는 패스워드(Password)를 변형 함수(Transform)에 입력하여 취소 가능한 템플릿 CBT_R을 생성한다. 바이오메트릭 템플릿은 서명자 고유 정보이기 때문에 템플릿이 노출되거나 도용되면 재사용할 수 없게 된다. 따라서 템플릿 취소 및 재등록이 가능하도록 원본을 변형한 템플릿을 등록해야 한다.

단계 2: 서명자는 인증 서버로 자신의 ID와 템플릿 CBT_R을 전송한다.

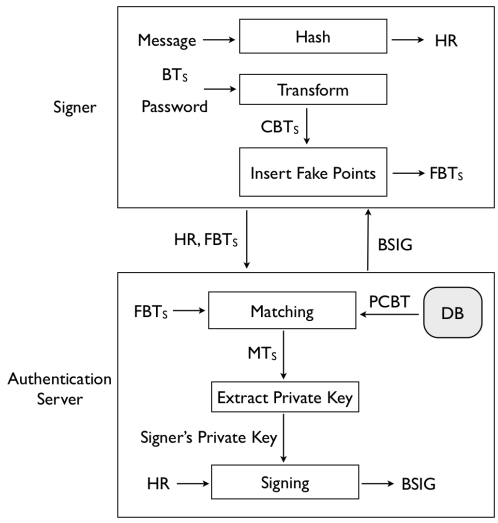
단계 3: 인증 서버는 먼저 PKI 인증서를 이용하여 서명자 ID를 인증한다. ID 인증에 실패하면 템플릿 및 키 등록을 취소한다.

단계 4: 인증 서버는 템플릿 CBT_R과 임의로 생성한 난수 RND를 키 생성 모듈(Key Generation)에 입력하여 서명자의 개인키와 공개키를 생성한다.

단계 5: 인증 서버는 서명자의 개인키를 퍼지볼트 기법을 이용하여 템플릿 CBT_R에 은닉한다 [6]. 개인키가 은닉되어 있는 템플릿 PCBT를 서명자 ID와 함께 데이터베이스에 저장하고 공개키는 서명자에게 전송한다.

3.2 바이오메트릭 서명 생성

그림 3은 바이오메트릭 서명 생성 단계를 보여준다.



HR: Hash Result, FBT: Faked Biometric Template

MT: Matched Template, BSIG: Biometric SIGnature

[Fig. 3] Biometric Signature Generation

단계 1: 서명자는 메시지를 해쉬하여 HR을 만든다. 서명자의 바이오메트릭 템플릿(BT_S)과 패스워드

(Password)를 입력하여 BT_S를 취소 가능한 템플릿(CBT_S)으로 변환한다. CBT_S에 가짜 특징점들을 섞은 템플릿(FBT_S)을 만든다 [7].

단계 2: 서명자는 HR과 FBT_S를 인증 서버로 전송한다.

단계 3: 인증 서버는 서명자가 전송한 FBT_S와 데이터베이스에 등록된 PCBT를 비교하여 좌표 값이 일치하거나 유사한 특징점들로 구성된 템플릿(MT_S)을 생성한다. MT_S에 퍼지볼트 기법을 적용하여 PCBT에 은닉된 개인키를 추출한다 [6, 7].

단계 4: 인증 서버는 서명자의 개인키로 HR을 서명하여 바이오메트릭 서명(BSIG)을 생성하고 BSIG를 서명자에게 전송한다. 제안한 서명 기법은 서명자 본인이 직접 서명 검증에 참여해야 하는 부인봉쇄 성질(Undeniability)을 갖는다 [8].

3.3 바이오메트릭 서명 검증

그림 4는 바이오메트릭 서명 검증 단계를 보여준다. 검증자는 서명 검증을 위한 도전 값(Challenge)을 생성하고 이에 대한 인증 서버의 응답(Response)을 검증한다. 도전 값은 검증자가 생성한 임의의 난수와 서명자의 공개키로 생성된다. 응답은 서명자의 개인키를 이용하여 인증 서버가 생성한다. 서명자는 응답을 만들기 위해서 자신의 바이오메트릭 템플릿을 인증 서버로 직접 전송해야 한다.

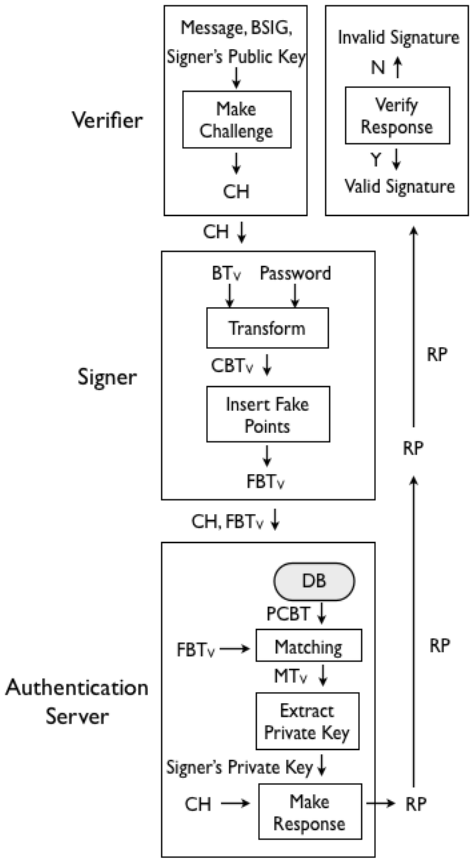
단계 1: 검증자는 임의로 생성한 난수와 서명자의 공개키를 이용하여 BSIG에 대한 도전 값(CH)을 생성하고, CH를 서명자에게 전송한다.

단계 2: 서명자는 CH에 대한 응답(RP)을 생성하기 위하여 서명자의 템플릿 FBT_V와 CH를 인증 서버로 전송한다.

단계 3: 인증 서버는 서명자 템플릿을 확인하고 PCBT에 은닉되어 있는 서명자의 개인키를 추출한다. 서명자의 개인키를 이용하여 도전 값 CH에 대한 응답 RP를 생성하고 이를 서명자에게 전송한다.

단계 4: 서명자는 RP를 검증자에게 전송한다.

단계 5: 검증자는 도전 값 CH에 대한 응답 RP를 검증함으로써 바이오메트릭 서명 BSIG를 인증한다.



CH: CHallenge, RP: ResPonse

[Fig. 4] Biometric Signature Verification

4. 안전성 분석 및 비교

제안한 서버 기반의 바이오메트릭 서명 기법의 안전성을 분석하고 기존 서명 기법과의 차이점을 비교한다.

4.1 안전성 분석

가정 1. 사용자의 바이오메트릭 템플릿과 개인키를 저장 및 관리하는 신뢰할 수 있는 인증 서버가 존재한다.

정리 1. 서명자는 제 3자에게 서명을 위임할 수 없다.

(증명) 3.2절의 바이오메트릭 서명 생성 과정에서 서명자는 해쉬 값 HR과 템플릿 FBT_S를 인증 서버로 전송한다. 인증 서버는 FBT_S와 데이터베이스에 등록된

PCBT를 비교하여 좌표 값이 매칭되는 템플릿 MT_S를 생성한다. 서명자 본인의 템플릿이 맞으면 MT_S를 이용하여 PCBT에 은닉된 개인키를 추출할 수 있다. 그 이외의 경우는 FBT_S의 가짜 특징점이 포함되어 PCBT로부터 개인키를 추출할 수 없다. 가정 1에서 인증 서버는 전적으로 신뢰할 수 있고, 서명자는 자신의 바이오메트릭 템플릿을 인증 서버로 전송해야만 개인키에 접근할 수 있다. 따라서 서명자는 제 3자에게 서명을 위임할 수 없다. Q.E.D.

정리 2. 검증자는 서명 검증 단계에서 서명자가 직접 검증에 참여 했다는 사실을 확인할 수 있다.

(증명) 3.3절의 바이오메트릭 서명 검증 과정에서 검증자와 서명자는 도전-응답 방식의 대화형 프로토콜을 사용하여 서명을 검증한다. 검증자는 서명 확인을 위하여 서명자에게 도전 값을 전송한다. 서명자는 응답을 만들기 위해서 인증 서버에 템플릿과 도전 값을 전송한다. 인증 서버는 PCBT로부터 추출된 개인키로 도전 값 CH에 대한 응답 RP를 생성하여 전송한다. 올바른 서명자의 요청으로 올바른 개인키가 추출되어야만 올바른 응답이 생성된다. 검증자는 CH에 대한 응답 RP를 검증함으로써 서명자가 직접 검증에 참여했다는 것을 확인할 수 있다. Q.E.D.

4.2 비교 분석

표 1은 일반 서명 기법, 바이오메트릭 서명 기법, 제안한 서명 기법의 기능상의 차이점을 보여준다. 부인봉쇄(Non-Repudiation) 기능은 서명자가 서명한 사실에 대해서 부인할 수 없는 것으로 일반 서명 기법, 바이오메트릭 서명 기법, 제안한 서명 기법 모두 이 요구사항을 만족한다.

대리 서명은 서명자가 자신의 개인키를 제 3자에게 빌려주어 서명을 대신하도록 하는 것이다. 일반적으로 서명에 사용되는 개인키는 하드디스크 또는 USB에 암호화되어 저장된다. 기존의 바이오메트릭 서명에서 개인키는 서명자의 바이오메트릭 데이터로부터 생성된다. 하지만 생성된 키 관리는 일반 서명 기법과 동일하기 때문에 서명자는 개인키에 접근할 수 있고 제 3자에게 서명을 위탁할 수 있다. 결국, 대리 서명을 못하게 하려면 서명자가 본인의 개인키를 알 수 없어야 한다는 명제가 성립한다. 제안한 기법은 대리 서명의 위험을 최소화하기 위해서 개인키 생성, 등록 및 관리를 인증 서버에서 수행하도록 한다.

〈Table 1〉 Comparison of Main Features of the Proposed Scheme with other Signature Schemes

	Ordinary Signature Scheme [9]	Biometric Signature Schemes [4, 5]	Proposed Scheme
Non-Repudiation	O	O	O
Proxy user can make the signature.	O	O	x
The private key can be made without help of the signer.	O	x	x
The signer should have to prove his/her identity in every signing sessions.	x	x	O
The signer should have to prove his/her identity in every signature verification sessions.	x	x	O

일반 서명 기법은 서명자의 도움 없이 키 생성이 가능하지만 제안한 기법과 바이오메트릭 서명 기법은 서명자가 직접 참여해야만 키 생성이 가능하다.

5. 결론

본 논문에서는 서버 기반의 실시간 바이오메트릭 서명 기법을 제안하였다. 서명자 본인이 직접 서명을 생성하고 검증에 참여해야 하는 바이오메트릭 서명 요구사항을 새로 정의하였고, 대리 서명의 위험을 최소화하기 위해서 서명자가 서명키에 접근할 수 없어야 한다는 정리를 증명하였다. 제안한 서명 기법에서 PKI의 인증기관과 같이 신뢰할 수 있는 인증 서버가 존재한다면 서명자는 제 3자에게 서명을 위임할 수 없다.

제안한 기법은 서명 생성 및 검증 단계에서 서명자에 대한 인증이 실시간으로 이루어지기 때문에 전자 선거에서 유권자들의 투표권 서명, 모바일 상거래에서 판매자

또는 저작권자의 구매 내역에 대한 공동 서명과 같이 대리 서명을 해서는 안 되는 응용에 적합하다.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2012-0004515)

REFERENCES

[1] C. Vivaracho-Pascual, J. Pascual-Gaspar, "On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, pp. 1-10, 2011.

[2] Want, "iPhone: Smarter Than the Average Phone," IEEE Pervasive Computing, Vol. 9, No. 3, pp. 6-9, 2010.

[3] N. Ratha, J. Connell, R. Bolle, "Enhancing security and privacy in biometric-based authentication systems," IBM Systems Journal, Vol. 40, No. 3, pp. 614 - 634, 2001.

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

[5] P. Orvos, "Towards biometric digital signatures," Networkshop, Eszterhazy College, Eger, pp. 26-38, 2002.

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

[7] T.Charles Clancy, "Secure Smartcard-Based Fingerprint Authentication," ACM Workshop on Biometrics, 2003.

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

[9] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, IT-31(4), pp. 469-472, 1985.

[10] Haizhou Li, Kar-Ann Toh, Liyuan Li, Advanced Topics in Biometrics, World Scientific, 2011.

윤 성 현(Yun, Sunghyun)

- 1992년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1994년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 모바일 보안, 바이오메트릭 인증, DRM, 전자투표
- E-Mail : shcrpt@gmail.com