바이오정보 기반 전자서명 및 디지털 키생성 기법

이형우(한신대학교), 윤성현(백석대학교)
문기영(한국전자통신연구원), 정윤수(한국전자통신연구원)

차 례

1. 서 론

급속도로 발전하는 사이버 공간에서 인터넷 사용자의 증가는 실생활과 마찬가지로 개개인의 영역을 형성하였으며, 중요정보를 포함하고 있는 문서 및 전자상거래 등의 응용서비스가 증가되면서 사이버 공간 내의 보안이 강조되고 있다. 기존의 ID/PW 기반의 보안 시스템이 복제 및 분실 위험에 노출되기 시작하면서 사용자들은 좀 더 안전한 보안을 원하게 되었고, 신체의 일부분 및 행동 특성을 적용하는 바이오 인식도 이 점에서 관심을 끌게 되었다.

바이오인식(Biometrics)은 개개인 고유의 바이오정보를 인식하기 위한 방법을 의미하며, 기술적으로 지문, 정맥, 홍채, 망막, 얼굴, 정적·동적 서명 및 음성 등 다양한 개인 고유의 정보를 추출하여 미리 등록되어있는 데이터와 비교하기 위한 기술을 의미한다. 따라서 개인의 식별 혹은 인증을 위한 목적으로 주로 사용되고 있으며, 더 나아가서 접근제어를 위한 기술로 활용되고 있다[1,2].

특히 바이오인식 산업은, PC와 네트워크 접속, 범죄자 식별, 전화통신, 물리적 접근, 전자상거래를 포함하는 응용적인 요구가 점점 커지면서, 개인을 식별하고 검증하기 위한 바이오인증 기술을 바탕으로 성장하고 있지만, 프라이버시와 관련되어 해결되어할 부분도 많다.

이를 통해 기존의 바이오 인식 기반 제품 등에 정보보호 기술을 접목할 수 있으며 기존의 PKI 구조와 연계된 새로운 인증 체계도 개발할 수 있을 것으로 전망된다[3]. 최근에는 공개키 기반의 전자서명 기술이 크게 발전하면서, 바이오 인식과 전자서명의 연계성에 대한 연구가 활발히 진행되고 있다. 바이오 정보를 이용하여 전자서명에 필요한 키를 생성하고 이를 통해 사용자에 대한 인증 및 안전한 메시지 전송 기법에 대한 연구가 필요하다. 이와 관련하여 바이오인식 과정에서 입력된 정보를 이용하여 기존의 정보보호 기술과 접목하고자 하는 연구가 시도되고 있다[4,5,6,7,8]. 예를 들어 바이오인식 과정에서 입력 및 변환된 정보를 이용하여 안전한 사용자 인증 구조에 적용할 수 있으며, 기존의 전자서명 알고리즘[9,10] 등과 연계하여 바이오 정보 기반 인증 시스템 및 바이오 정보 기반 디지털 키생성 기술에도 적용 가능하다.

기존의 바이오 인증 관련 기술은 바이오인식 장비를 통한 사용자 인증 기술에 국한되었기 때문에 앞으로 급속히 확대될 것으로 예상되는 바이오 기반 정보보호 기술 등에 활용하기 위해서는 결국 바이오 정보에 기반한 키생성 및 전자서명 알고리즘 기술에 대한 연구 및 개발이 필수적이다.

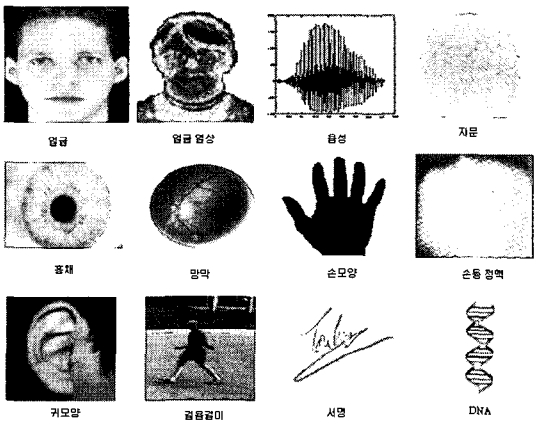
이에 본 연구에서는 먼저 2장에서 기존의 바이오 인식 기술에 관해 검토하고 인식 기술을 기반으로한 국내외 표준화 현황을 조사하였다. 표준화 관련해서는 ITU-T SG 17 기반 텔리바이오메트릭스(Telebiometrics) 분야 및 정보보호 관련 분야에 대한 현황을 중심으로 분석하였다. 3장에서는 바이오 정보를 이용한 기존의 전자서명 기술에 대해 분석하였다. 4장에서는 전자서명을 위한 바이오정보 기반 디지털 키생성 기법에 대해 고찰하였으며 5장에서 응용가능한 분야를 제시하였다.

2. 바이오인식 기술 표준화 동향

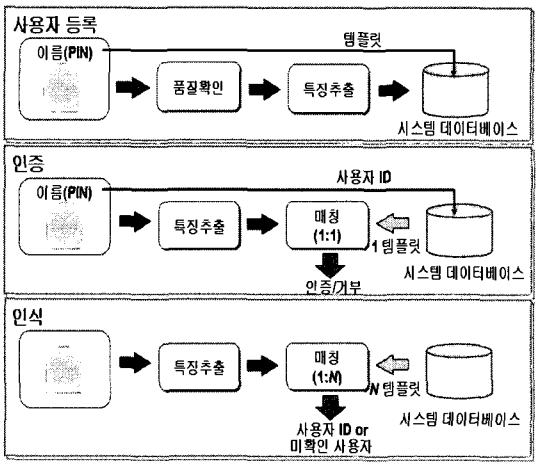
2.1 바이오 인식 기술

현재까지 연구된 바이오인식 방법으로는 (그림 1)과 같은 것들이 있으며, 이러한 바이오특징은 얼굴모양, 홍채, 망막, 정맥, 지문, DNA 등의 신체적 특성을 이용한 방법과 서명, 음성, 걸음걸이 등의 행동학적 특성을 이용하는 방법으로 분류할 수 있다.

바이오인식 시스템은 많은 응용 분야에 다양하게 사용되고 있지만, 기본적으로는 (그림 2)와 같이 사용자를 등록하는 과정과 사용자 자신이 자신임을 확인받는 인증(verification, 1:1), 데이터베이스에서 사용자를 찾아내는 인식(identification, 1:N)으로 나누어진다[2].



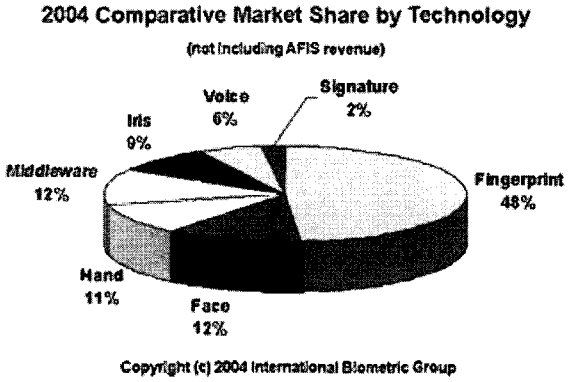
▶▶그림 1. 여러 가지 바이오인식 방법



▶▶그림 2. 사용자 등록 및 인증, 인식 과정

[표 1]에서 보는 바와 같이 전세계 바이오인식 시장에서 지문인식이 48% 시장점유율로 개발비용이 저렴하고 보안성이 우수하여 단일 바이오인식기술 중에서 각광을 받고 있다. 하지만 최근에는 바이오여권 도입에 따라 얼굴인식 및 홍채인식기술의 보급이 확대되고 있는 추세이며, 향후에는 열상정보·DNA·다중바이오인식 등과 같은 첨단 신기술로 발전할 것으로 예상된다. 특히 해외에서는 지문센서, 카메라 등 바이오정보 입력장비 및 칫셉 등 HW 제조기술과 실시간 다중검색을 위한 서버기술 등이 상용화단계에 이르고 있다. 특히, 일본에서는 한국이 기술특허를 갖고 있는 정맥인식기술을 활용한 손가락 정맥 또는 손등정맥기술을 특화하여 금융권에 급속히 확산되고 있는 추세이다.

표 1. 세계 바이오인식 시장규모 전망



(단위 : 억 달러)

연도	2004	2005	2006	2007	2008	성장률
시장규모	12.01	18.47	26.84	36.82	46.39	31%

※ 바이오인식 시장 보고서(International Biometric Group, 2004)

우리나라 기술수준은 '04년말 현재, 미국에 등록된 한국의 기술특허는 미국, 일본, 캐나다, 영국, 대만에 이어 세계 6위 수준이며, 최근 3년간(2002~4) 해외에서 발표된 논문은 미국, 중국, 영국, 일본에 이어 세계 5위 수준으로 일부 기술우위를 점하고 있기도 하다. 다만 Match on Card와 같은 칩셋 등 HW 설계기술, 열상정보/DNA 등과 같은 첨단 바이오인식 알고리즘에 대한 원천기술에서는 다소 미흡한 실정이다.

특히, 국내 바이오인식업체는 대부분이 벤처기업 형태로 영세하여 대부분 내수 30%, 동남아지역에 편중된 수출 70%(일본 32.1%, 미국 16%, 중국 14.2%, 유럽 10%) 등의 매출구조를 갖고 있다. 국내 시장규모는 [표 2]에서 보는 바와 같이, '04년 630억원에서 '08년에는 3,000억원으로 연평균 47%의 높은 성장률을 기록할 전망이다.

표 2. 국내 바이오인식 시장규모 전망 (단위 : 억원)

연도	2004	2005	2006	2007	2008	성장률
시장규모	630	950	1,310	1,970	3,000	47 %

※ 국내 바이오인식 산업현황 조사보고서(KBA, 2005)

국내 바이오 인식 및 보안 분야 가운데 가장 활발한 활동을 보이고 있는 부분은 지문인식 분야로서 국내 바이오 인식 시장의 50% 정도를 차지하는데, 이는 세계 시장의 전반적 추세와도 일치한다. 그 이유는 지문 인식 기술이 가장 경제적인 개인 인증 수단으로서 상용화가 비교적 수월하며 일정한 수요도 발생하고 있기 때문이다.

2.2 기타 바이오 인식 기술

가. 홍채 인식 기술

홍채인식 기술은 사람마다 고유한 눈동자의 망막혈관과 홍채 패턴을 구별해 본인 여부를 판정하는 기술로, 바이오인식 분야에서도 특히 정확도 면에서는 가장 뛰어난 것으로 평가되어지고 있고, 이 기술이 본격적으로 가시화 된 것은 1980년대에 들어서였다.

홍채인식은 망막과 달리 눈의 동공 주변에 위치한 홍채의 무늬 패턴을 이용한 것이기 때문에 안구 내 질병 또는 눈의 충혈과도 상관이 없고, 자연스러운 상태에서 획득된 영상을 이용하게 되므로 망막인식에서와 같은 단점도 없다. 특히 개인 식별을 할 수 있는 특징점이 지문의 경우 40여 가지에 불과한데 비해 그 여섯 배를 넘는 무려 250여 가지의 패턴을 가지고 있어, 그 정확도에 있어서 바이오인식 부문 중 타의 추종을 불허하고 있는 부문이기도 하다.

향후 홍채를 개인 식별의 수단으로 널리 적용할 수 있도록 보다 다양한 홍채 특징 추출방법과 이를 효과적으로 저장할 수 있는 부호화기법에 대한 연구, 대용량 데이터베이스에서 효과적인 비교를 위하여 지문과 같은 홍채를 유형별로 분류하는 방법에 관한 연구가 필요하다. 여기서 가장 중요한 사항은 사용자의 편리성을 최대한으로 보장하는 것이다. 이를 위해 active vision과 같은 기술을 바탕으로 한 입력장치의 완전 자동화를 위한 연구는 홍채인식 시장의 확대를 위해서 시급히 해결해야 할 과제이다.

나. 얼굴 인식 기술

얼굴 인식 기술이란 정지영상이나 동영상에 존재하는 한 사람 이상의 얼굴에 대하여 주어진 얼굴 데이터베이스를 이용하여 그 신원을 확인하는 기술을 일컫는다. 얼굴인식기술은 다른 바이오인식기술인 지문인식등과 다르게 자신의 신체 일부를 인식장치에 직접 접촉시키지 않아도 되고 바이오정보의 획득방법에서 강제성이 적어 다른 바이오인식기술이 사용자에게 줄 수 있는 거부감과 불편함이 존재하지 않는 특징을 갖는다. 한마디로 이야기 하자면 가장 인간 친화적인 기술이라는 것이다. 우리가 누군가를 알아볼 때 그들의 지문이나 홍채를 들여다보지 않는 것과 같은 이치이다. 얼굴인식기술이 다른 바이오인식기술에 비해 가지는 이러한 비접촉성, 비강제성, 편리성의 특징으로 인해 얼굴인식기술은 신원 확인 분야 외에도 신분확인 대상자가 모르는 사이에 자연스럽게 정보를 획득해야 하는 지능형 무인감시등의 분야를 중요 응용분야로 가진다.

다. 음성 인식 기술

사람의 억양과 음의 높낮이가 서로 다르다는 특성에 기인한 방식으로 마이크 등을 통해 전달된 음성의 특징을 분석한 후 가장 근접한 것을 찾아내는 방식으로 다른 바이오인식과 달리 멀리 떨어진 곳에서도 전화를 이용하여 신분을 확인할 수 있고, 사용하기 위한 별도의 교육이 필요하지 않으며 시스템 가격이 저렴하다는 장점이 있다. 하지만 감기나 기타 요인에 의해 목이 쉬었을 때나, 의도적으로 타인의 목소리를 흉내내거나 주변환경에 큰 소음이 있을 경우에는 오인식을 할 수 있다는 단점이 있다.

라. 바이오정보별 장단점

밑의 표는 앞에서 설명한 바이오인식시스템별 장단점을 [표 3]에 제시하였고 성능에 대해 [표 4]에 제시하였다.

표 3. 바이오정보별 장단점

구 분	장 점	단 점
지문인식	보안성이 뛰어나며 시스템 구축가격이 저렴	접촉필요, 손상되거나 건조한 지문은 인증이 어려움
얼굴인식	인증이 빠르고 쉬우며 시스템 구축가격이 저렴	주위 조명에 민감하고 표정, 수염에 의한 변장 약함
홍채인식	최고의 식별성과 복제 불가능	비교적 비싸며, 거부감이 생기고 사용이 불편
음성인식	원격지에서 사용 가능하고 저렴한 가격	신체적(감기), 감정적 특성에 따른 변화에 다르게 반응
서명인식	사용이 편하고 가격이 저렴	정확도가 떨어지며 타인의 도용 가능

표 4. 각 시스템별 성능

구 분	지 문	홍 채	얼 굴
본인거부율(%)	1 미만	0~12	0.1 미만
타인승낙률(%)	0.001	0	0.1 미만
EER(1:n) *	1:500	1:131,000	자료 없음
거래소요시간(초)	9~19	12	10
템플릿크기(Byte)	250~1,000	512	84~1,300
장비가격 수준	낮음	높음	중간
성능에 영향을 미치는 요소	먼지,습도, 마모	시력,섬광, 반사광	빛,선글라스, 방향

* n명중에서 잘못 인식(거부)될 인원이 1명이라는 의미로 n이 커질수록 정확도는 증가
* 자료 : Card Technology(2003년), Biometric Technolgy사(2002년) 및 uggles report(1998년)에서 재구성

2.3 바이오 인식 관련 표준화 동향

현재 ISO 및 ITU-T를 중심으로 바이오 정보에 대한 정보보호 기술 표준화를 진행하고 있다.

- ISO SC17 : 카드 및 개인 식별 정보 중심 바이오 정보 보호
- ISO SC27 : IT 보호 기술 관련된 내용
- ISO SC37 : Biometrics 관련 표준화 내용
- ITU-T SG17 Q.8 : Telebiometrics 관련 기술 표준화 연구

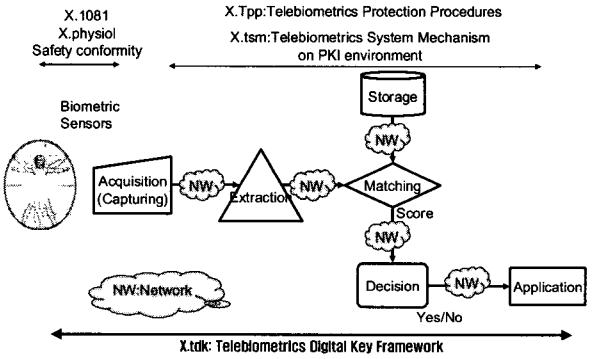
ISO/IEC JTC1에 스마트카드 기술규격을 다루는 SC17(Cards and Personal Identification), 바이오정보 보안기술을 다루는 SC27(IT Security Techniques), 바이오인식 핵심기술을 다루는 SC37(Biometrics), 바이오정보를 활용한 금융분야의 보안기술을 다루는 ISO TC68(Banking Securities and other Financial Services) 그리고 정보통신망에서의 바이오정보의 보안기술을 다루는 ITU-T SG17/Q.8 (Telebiometrics) 등이 대표적인 바이오인식기술과 관련되는 국제 표준화기구라 할 수 있다.

ITU-T SG17(보안, 프로그래밍 언어, 정보통신 소프트웨어) 표준화그룹에서는 2004년 3월에 관련분과(Working Party, WP) 조직을 재구성함에 따라 정보통신 보안기술분과인 WP2내에 작업반인 Q8. 텔레바이오메트릭스분과에서 통신 네트워크에서의 사용자 신원을 확인하기 위해 한·중·일 전문가를 중심으로 바이오정보 통신보안에 대한 표준화가 추진중이다. 현재 아래 [표 5]와 같이 Telebiometrics 환경에서의 표준화 활동이 진행중이다.

표 5. ITU-T SG17/Q8 Telebiometrics 표준화 활동 현황

Title	Summary
X.tmmf	Telebiometrics의 물리적 운영 환경 내에서 시스템과 인간 사이의 다양한 인터랙션을 정의
X.physiol	X.tmmf에 정의된 인터랙션들의 물리량, 단위, 안전 수치 등을 예시와 함께 정의
X.tsm-1 X.tsm-2	PKI 기반의 telebiometric 시스템의 구성요소의 사양, 다양한 모델, 메커니즘 등을 정의
X.tpp-1 X.tpp-2	X.tpp-1과 X.tpp-2는 일반적인 telebiometrics 환경 내에서 모든 가능한 위협으로부터 생체 자료와 정보를 보호하기 위한 가이드라인 및 프로토콜을 제시
X.bip	ISO SC37 국제표준인 BioAPI에 기반한 Telebiometrics 환경에서의 바이오정보 통신 메커니즘 정의
X.tdk	바이오정보기반 암호학적 보안기법을 이용하여 전자서명 키생성방법 및 인증기술 제시
X.tai	X.tsm의 특별한 경우로서 PKI와 동시에 PMI 환경에서 생체인증을 이용한 신원 및 권한 확인 시에 생체정보 인증 모델 및 프로토콜을 정의

최근까지 개최된 ITU-T SG17/Q8 회의에서는 아래 (그림 3)과 같이 바이오 정보를 이용하여 개방형 네트워크 환경을 이용하여 인증, 정보보호 및 프라이버시 보호 등을 수행할 수 있는 기술 표준에 대해 연구하고 있다.



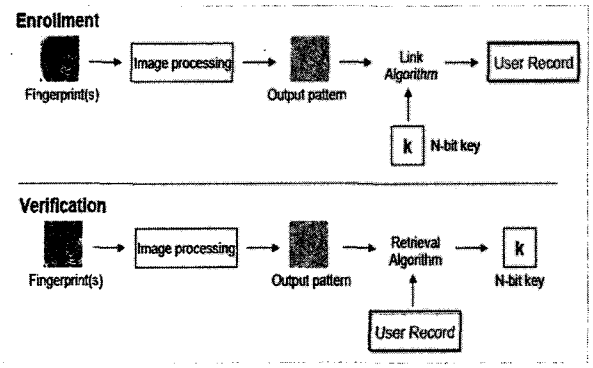
▶▶그림 3. Telebiometrics 기반 ITU-T SG17/Q8 표준

3. 바이오정보 기반 전자서명 기술 분석

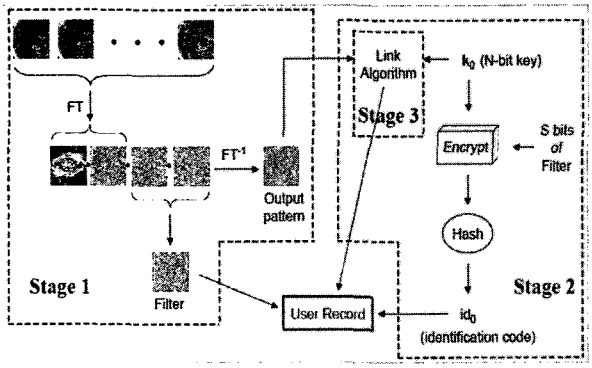
3.1 바이오정보를 이용한 전자서명 기술

가. Bioscrypt 기술

Mytec Technology에서 개발한 Bioscrypt는 기존의 특징점 중심의 지문 인식 알고리즘에 비해 푸리에 변환과 Biometric encryption, 해쉬 과정을 추가한 독창적인 알고리즘을 개발, 다양한 응용 분야를 제공하고 있다. 특히 이 알고리즘을 본 연구에서 중점적으로 살펴보는 이유는, 바이오 정보를 바탕으로 하여, 일종의 키 정보를 유도할 수 있기 때문이다. Bioscrypt 기술인 경우 지문정보에 대한 입력 후 키를 생성한다. 즉 이 기술은 지문정보를 기반으로 템플릿을 생성하는 기법을 제공한다.



▶▶그림 4. Bioscrypt 등록 및 검증 과정 개요



▶▶그림 5. Bioscrypt 키생성 과정

하지만 Bioscrypt 기술은 사용자 인증 및 메시지 인증 부분이 취약하기 때문에 이를 개선한 새로운 전자서명 키 생성 기법이 필요하다.

나. FingerCode 기술

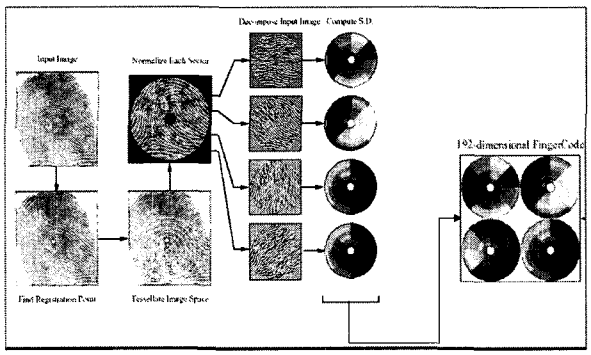
AK Jain, S. Prabhakar, L. Hong, and S. Pankanti 에 의해 개발된 Fingercode는 J. Daugman 박사의 Iriscode를 모티브로 하여 생성된 것으로 지문의 융선 방향을 각도에 따른 마스크를 이용하여 정보를 추출해 내는 방법이다. 이에 추가적으로 Peter Orvos가 제안한 바이오 인식 기술과 전자서명의 연계 방법[4]이 연구되고 있다. 이것은 공개키 기반 구조를 바탕으로 스마트카드에 저장된 FingerCode를 이용하여, 숨겨진 개인키 정보를 복구하도록 하는 방법이다.

Fingercode는 부분 영역별 정보를 이용하여 추출된 영역별 방향정보와 전체적인 융선 방향 정보를 가지는 융선 방향 모델을 이용하여 융선 방향 추출 및 코아와 델타의 위치를 추출하는 방법이다.

Fingercode는 참조점(Reference Point)을 중심으로 일정 크기의 관심지역(area of interest)을 추출하여 filter의 형식에 따라 적당한 크기의 sector로 나누어 정보를 처리한다. 아래의 식을 이용하여 Feature value를 계산한 후, 계산된 값을 이용하여 grayscale image를 형성한다.

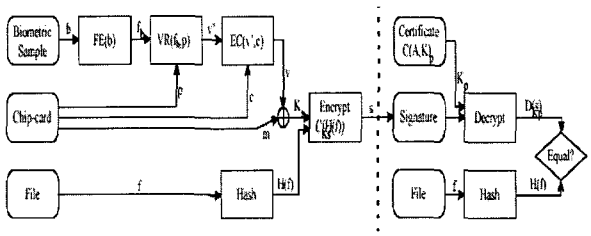
$$V_{i\theta} = \frac{1}{n_i}\left(\sum_{n_i} |F_{i\theta}(x, y) - P_{i\theta}|\right)$$

이렇게 형성된 grayscale image는 유효 영역(interesting area)의 융선 방향에 따라 아래 (그림 6)에서 보는 바와 같이 필터의 종류에 따라 일정 크기의 Fingercode로 변환되게 된다.



▶▶그림 6. FingerCode의 생성 과정

위의 (그림 6)에서 보는 바와 같이 입력 장치를 통해 얻게 된 지문 image는 core나 delta 등의 참조점을 중심으로 일정 부분을 구획하게 되며, 구획된 영역을 섹터별로 정규화시켜 일정 각도에 따라 나누게 된다. 위의 (그림 6)에서는 0°, 45°, 90°, 135°의 4개 각도로 fingercode를 생성한다.



▶▶그림 7. 바이오정보와 칩 카드를 이용한 전자서명 알고리즘
(출처 : Peter Orvos's Homepage)

위의 (그림 7)은 바이오정보와 칩 카드의 Fixed value를 이용한 전자서명 알고리즘의 한 예를 도식화 한 것이다. 입력 장치로부터 얻게 된 바이오정보 샘플(b)을 Feature Extraction(FE)하여, 생성된 바이오 특성 정보를 Vector generate function(VR)과 칩 카드에서 추출

한 fixed value(p)를 이용하여 사용자 벡터를 생성한다. 이 때, 벡터 생성에 생길 수 있는 에러를 최소화하기 위하여 Error Correction(EC)과정을 또 다른 fixed value(c)와 같이 적용하여 유일한 벡터를 생성한다. 여기에 master secret value(m)을 XOR 연산하여 secret key를 생성하고, 데이터를 해쉬 함수를 통해 $H(f)$를 생성하여 서명을 생성한다. 이렇게 생성된 서명과 해쉬값은 CA에서 주어지는 공개키(K_p)를 이용하여 복호화되고, 데이터를 해쉬한 값과 비교하여 전자서명의 유효성을 판별한다.

바이오 정보 샘플을 fingercode로 변환하여, 칩 카드 내에 있는 특정 정보를 이용하여 지문 입력과정에서 생길 수 있는 에러를 수정된 벡터로 변환하고, 수정된 사용자 벡터에 master secret value를 추가하여 사용자 고유의 비밀 키를 생성할 수 있다.

3.2 바이오정보 기반 전자서명 기술

가. Janbandhu-Siyal 바이오 인증 전자서명

2001년 Janbandhu와 Siyal이 제안한 바이오인증 전자서명 방식[7]은 RSA[9]와 DSA 공개키 기반 전자서명 알고리즘을 사용하는 기법에 해당한다. 특히 John Daugman의 IrisCode에 근간하여, 512바이트의 바이오 인식 데이터를 가정한다. 하지만 바이오 인식 샘플에서 비롯되는 정보가 결정적이거나 혹은 충분한 오류정정을 통하여 결정적인 값으로 항상 복원될 수 있도록 가정하고 있다. 따라서 현실적으로 구현하는 데는 많은 어려움이 있는 기법이라고 할 수 있다.

(1) RSA 기반 알고리즘

(그림 8)에 도시된 Janbandhu-Siyal 바이오인증 전자서명의 RSA 알고리즘을 요약하면 다음과 같다. 이 기법에서 눈여겨 볼 부분은 법의 크기와 서명을 암호화하여 전달한다는 사실이다. 또한 $\Phi(n)$을 안전하게 소지해야하는 부담이 있다.

가) 키 생성

○ 각각 256 바이트 크기의 매우 큰 소수 p와 q 생성

○ 법 $n = p \times q$와 오일러 함수 $\phi(n) = (p-1)(q-1)$을 계산

○ 512바이트 크기의 홍채 템플릿으로부터 개인 지수 d를 구하는데, 특별히 1씩 증가하여 $\phi(n)$과 서로소가 되는 값을 찾는다.

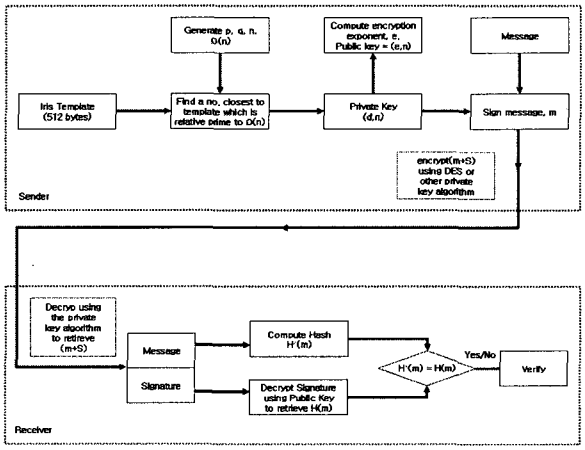
○ 공개 지수 $e = d^{-1} \bmod \phi(n)$를 구한다.

나) 서명생성

○ 메시지의 해쉬값을 구하여 RSA 서명한 후, 검증자와 공유하는 비밀키로 암호화하여 전달한다.

다) 서명검증

○ 전달된 서명 메시지를 서명자와 공유하는 비밀키로 복호화하여, 메시지의 해쉬값을 구한 후 RSA 서명 검증을 한다.



▶▶그림 8. 바이오 인식 전자서명 RSA 알고리즘

(2) DSA 기반 알고리즘

(그림 9)에 도시된 Janbandhu-Siyal 바이오인증 전자서명의 DSA 알고리즘을 요약하면 다음과 같다.

가) 키 생성

○ 64~128바이트 크기의 큰 소수 p를 구한다.

○ 20바이트 크기를 갖는 $p-1$의 소인수 q를 구한다.

○ 서브그룹의 생성자 $g = h^{(p-1)/q} \bmod p$를 구한다. 이때 $h < (p-1)$이며 $h^{(p-1)/q} \bmod p > 1$이다.

○ 512바이트 크기의 홍채 템플릿에 일방향 해쉬함수를 적용하여 20바이트 크기의 해쉬값을 구한다. 그리고 이 값을 개인키 x로 정의한다.

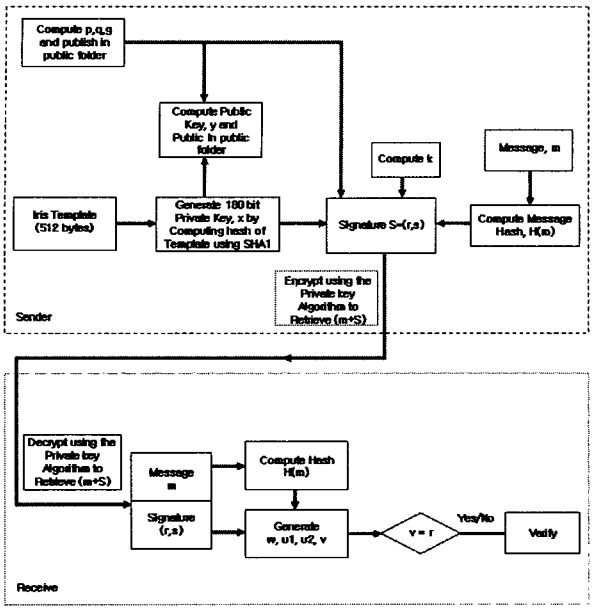
○ 공개키 $y = g^x \bmod p$를 구한다.

나) 서명생성

○ 메시지의 해쉬값을 구하여 DSA 서명한 후, 검증자와 공유하는 비밀키로 암호화하여 전달한다.

다) 서명검증

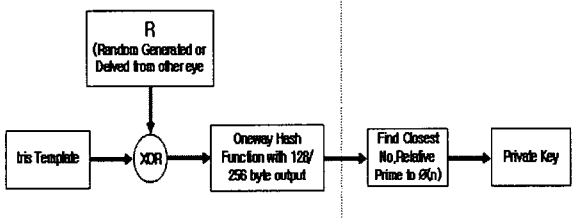
○ 전달된 서명 메시지를 서명자와 공유하는 비밀키로 복호화하여, 메시지의 해쉬값을 구한 후 DSA 서명 검증을 한다.



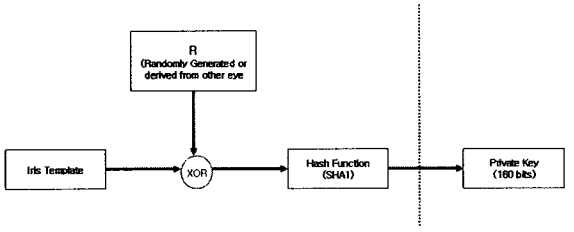
▶▶그림 9. 바이오 인식 전자서명 DSA 알고리즘

(3) 키의 랜덤성 개선

(그림 10)과 (그림 11)에서는 개인키를 구할 때 홍채 템플릿에 다른 눈으로부터 획득된 값을 난수로 첨가하여 동일한 홍채 템플릿으로부터 동일한 키가 나오지 않는 방법에 대해서 제안하고 있다.



▶▶그림 10. 바이오 인식 전자서명 RSA 수정된 키 생성 알고리즘



▶▶그림 11. 바이오 인식 전자서명 DSA 수정된 키 생성 알고리즘

(4) 기존 기법의 안전성 평가

본 안전성 평가 기준에 따라서, 키 크기와 바이오 인식 샘플 혹은 템플릿의 크기는 최소한 다음의 식을 만족하여야 한다.

$$BiometricDataSize = KeySize \times 3 + Redundancy$$

Janbandhu-Siyal의 바이오 인식 전자서명 시스템의 RSA 알고리즘은 오히려 바이오 인식 데이터의 크기와 같은 512바이트의 키를 요구하고 있다. 하지만 John Daugman의 이론과 잉여의 필요성에 따라서 그와 같은 키를 결정적으로 구할 수 없다. 따라서 일정한 크기로 추출되거나 변환될 수 있는 기법이 적용되어야 Janbandhu-Siyal의 바이오 인식 전자서명 시스템에서 RSA 알고리즘을 안전하게 적용 가능하다.

Janbandhu-Siyal의 바이오 인식 전자서명 시스템의 DSA 알고리즘은 기준식에 따라서 512바이트 크기의 바이오 인식 데이터에 대해서 20바이트의 키 크기와 452바이트 크기의 잉여를 갖게 된다. 이것은 이론적으로 유도 가능한 키 크기이며, 따라서 바이오 인식 샘플이 안정적으로 획득될 경우 Janbandhu-Siyal의 바이오 인식 전자서명 시스템의 DSA 알고리즘을 안전하게 구현할 수 있다. 하지만 키의 랜덤성을 위하여 난수를 추가해야 하며 20바이트의 키가 충분한 엔트로피를 가진다는 보장이 없다.

2. Nagpal-Nagpal 바이오인증 전자서명

2002년 R. Nagpal과 S. Nagpal에 의해 제안된 바이오 인식 기반 전자서명[8]은 RSA 알고리즘에 기초하고 있다. 특히 이 기법은 사용자의 망막, 홍채, 그리고 지문 등 세 가지 바이오정보를 이용하는 다중 바이오 인식 방식이다. 따라서 다양한 입력장치를 요구하게 된다.

(1) 알고리즘 개요

가) 키 생성

○ 512바이트 크기의 망막 템플릿으로부터 64바이트 크기의 큰 수 p를 구하는데, (비록 망막 스캐닝의 결과로 항상 고정된 정수를 만들어 내는 알고리즘은 여전히 개발이 진행 중인 상태이더라도) 특별히 1씩 증가하여 소수가 되는 값을 찾도록 한다.

○ 512바이트 크기의 홍채 템플릿으로부터 64바이트

크기의 큰 수 q를 구하는데, (비록 홍채 스캐닝의 결과로 항상 고정된 정수를 만들어 내는 알고리즘은 여전히 개발이 진행 중인 상태이더라도) 특별히 1씩 증가하여 소수가 되는 값을 찾도록 한다.

○ 법 $n = p \times q$와 오일러 함수 $\phi(n) = (p-1)(q-1)$을 구한다.

○ 512바이트 크기의 지문 템플릿으로부터 공개 지수 e를 구하는데, (비록 지문 스캐닝의 결과로 항상 고정된 정수를 만들어 내는 알고리즘은 여전히 개발이 진행 중인 상태이더라도) 특별히 1씩 증가하여 $\phi(n)$과 서로소가 되는 값을 찾도록 한다.

○ 개인 비밀키 $d = e^{-1} \bmod \phi(n)$를 구한다.

나) 서명생성

○ 키 생성 단계를 반복한다. 즉, 사용자는 망막, 홍채, 그리고 지문 인식을 받고, 이 값으로부터 p, q, e를 각각 구한 후, $\phi(n)$과 d를 구한다.

○ 메시지의 해쉬값을 구하여 RSA 서명한 후, 검증자에게 전달한다.

다) 서명검증

○ 전달된 서명 메시지의 서명자의 공개키를 서버에게 요청하여 획득한다.

○ 메시지의 해쉬값을 구한 후 RSA 서명 검증을 한다.

(2) 안전성 평가

Nagpal-Nagpal의 바이오 인식 전자서명 시스템은 우리의 직접 서명 모델의 방법 2에 해당한다. 따라서 그에 해당하는 평가를 수행해볼 수 있다.

본 안전성 평가 기준에 따라서, 키 크기와 바이오 인식 샘플 혹은 템플릿의 크기는 다음의 식을 만족하여야 한다.

$$BiometricDataSize = KeySize \times 3 + Redundancy$$

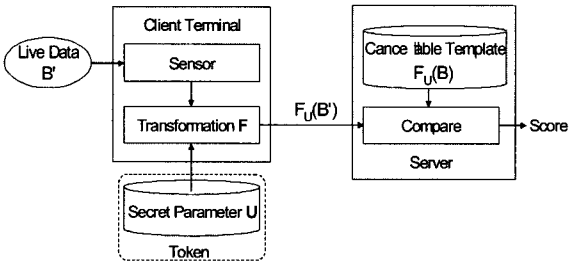
Nagpal-Nagpal의 바이오 인식 전자서명 알고리즘은 기준식에 따라서 p, q, e 모두를 고려할 때 512바이트 크기의 바이오 인식 데이터에 대해서 128바이트의 키 크기와 128바이트 크기의 잉여를 갖게 된다. 이것은 본 평가 기준에는 못 미치지만 이론적으로 유도 가능한 키 크기이며, 따라서 바이오 인식 샘플이 안정적으로 획득될 경우 Nagpal-Nagpal의 바이오 인식 전자서명 알고리즘을 안전하게 구현할 수 있다. 하지만 바이오 인식 과정으로부터 생성된 키가 충분한 엔트로피를 갖을 수 있도록 새로운 접근방향에 대한 연구가 필요하여 또한 키의 랜덤성을 위하여 난수를 추가해야 하는 등의 연구가 수행되어야 한다.

4. 바이오정보 기반 디지털 키생성 기술

4.1 바이오정보 기반 키생성 관련 모델 검토

가. 취소 가능한 바이오 정보 모델(Cancellable Biometrics Model)

(그림 12)는 IBM에서 처음으로 제안한 취소 가능한 템플릿(template)과 이를 이용한 사용자 인증 모델을 보여준다. 기존의 바이오정보 데이터는 고유한 특성을 가지며 도용되었을 경우에 취소할 수 없다는 문제점이 있다. 이러한 바이오정보의 특성을 없애기 위하여 바이오정보 외에 비밀값 U(Secret Parameter U)를 이용하여 취소 가능한 템플릿을 생성한다. (그림 12)에서 F 함수는 바이오정보와 비밀값 U를 입력으로 받고 이 값들을 이용하여 템플릿 FU(B)를 만들어낸다. 사용자는 비밀값 U를 달리하여 서로 다른 템플릿들을 여러 개 생성할 수 있다. 따라서 저장된 템플릿이 노출되거나 도용되었을 경우에 템플릿에 대한 재등록이 가능하며 이를 통해 바이오 정보에 대한 보안성 향상 및 프라이버시 보호 기능을 제공할 수 있다. 따라서 이와 같은 메커니즘을 바이오정보 기반 디지털 키생성 구조에 적용 가능하다.

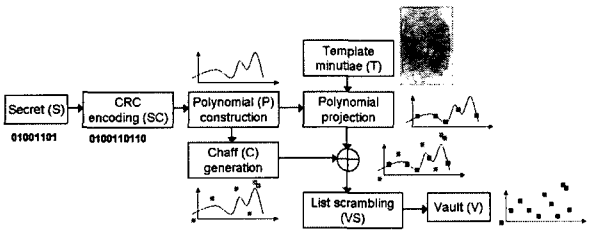


▶▶그림 12. 취소 가능한 바이오 정보 모델

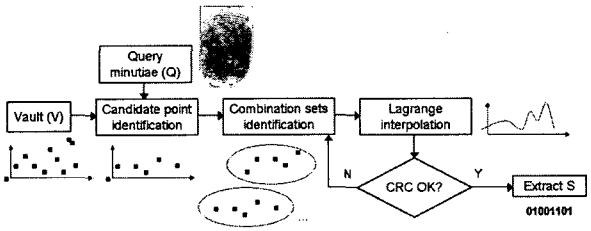
나. 퍼지볼트 모델(fuzzy vault model)을 이용한 키 은닉 및 추출

퍼지볼트 모델(fuzzy vault)[11]은 데이터를 은닉하기 위한 용도로 사용된다. 원래 볼트(금고)는 정확한 자물쇠 번호 들을 알고 있어야 만 열 수 있는데, 퍼지 볼트는 임

계치(threshold) 이상의 번호 들만 알고 있으면 전체 번호들을 모르더라도 해당 볼트를 열 수 있다는 개념이다. 바이오정보는 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. 바이오정보의 이러한 특성은 퍼지볼트 모델을 이용하여 바이오정보에 키 값을 은닉하기에 매우 적합하다. (그림 13)은 퍼지 볼트 모델을 이용하여 키를 은닉하는 방법을 보여주며, (그림 14)는 퍼지 볼트로부터 키를 추출하는 방법을 보여준다.



▶▶그림 13. 퍼지 볼트 모델을 이용한 키 은닉 방법



▶▶그림 14. 퍼지 볼트 모델을 이용한 키 추출 방법

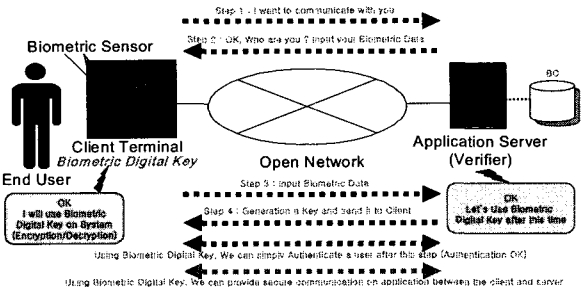
다. 새로운 모델에 대한 고찰

바이오 정보는 개인마다 유일한 특성을 갖기 때문에 한 번 도용되면 다시 사용할 수 없는 치명적인 단점을 갖는다. 따라서 바이오 정보만을 이용하여 전자서명 키를 생성할 경우에는 동일한 사용자는 매 번 같은 키를 생성할 수밖에 없다. 바이오정보를 이용하여 만들어진 전자서명 키의 안전성 및 관리를 위해서 동일한 사용자가 여러 개의 키를 만들 수 있는 방법이 필수적이다. 본 연구에서는 취소 가능한 바이오 정보 모델을 적용하여 사용자 키가 도용될 경우에 또 다른 키를 등록할 수 있도록 한다.

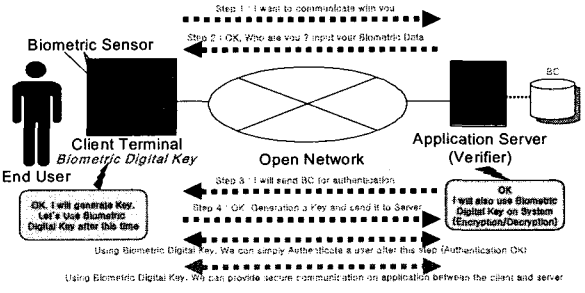
전자서명에 사용되는 개인키는 그 특성 상 키 소유자만이 알고 있어야 하며, 도용되거나 노출될 경우에 해당 전자서명의 안전성은 보장할 수 없다. 개인키 보호를 위한 방법으로 개인키를 암호화하여 하드디스크에 저장하거나 또는 스마트카드 등과 같은 이동식 저장 장치에 보관한다. 이러한 방법이 갖는 공통적인 특징은 개인키 값이 변형된 형태로 보관되며 이 값이 제 3자에게 노출될 수 있는 위험성을 수반한다. 또한, 개인키 소유자가 직접 서명하지 않고 제 3자에게 대리 서명을 위탁할 수 있는 위험요소가 존재한다. 따라서 사용자의 바이오정보를 활용해야만 개인키를 사용할 수 있도록 하는 방법이 필요하다. 결국 퍼지 볼트 모델을 적용하여 사용자의 개인키 값을 바이오정보에 은닉할 수 있다.

바이오 정보를 이용하여 개방형 네트워크 환경에서 사용 가능하며 동시에 바이오 정보를 접목한 응용 소프트웨어 개발이 가능하다. 만일 바이오 정보 등을 통해 인증을 수행하였다면, 사용자는 바이오 정보의 특성을 활용하여 좀 더 안전한 통신 구조를 제공할 수 있을 것이다. 특히 바이오 정보에 정보보호 기술 등을 접목한다면 기존의 시스템 보다 더욱 안전한 시스템을 구축할 수 있을 것이다.

본 연구에서 고찰한 내용은 (그림 14)와 같이 바이오 정보를 이용하여 전자서명 또는 암복호화 과정에 사용가능한 키를 생성하고자 하는 것이다. 이를 통해 좀 더 안전하고 효율적인 개방형 네트워크 환경을 구축할 수 있다. 사용자는 서버를 기반으로 인증 과정도 수행하면서 동시에 안전한 네트워크 환경을 구축할 수 있다. (그림 15)는 서버 중심의 키생성 방식을 보이며, (그림 16)은 클라이언트 중심의 키생성 과정을 보여준다.

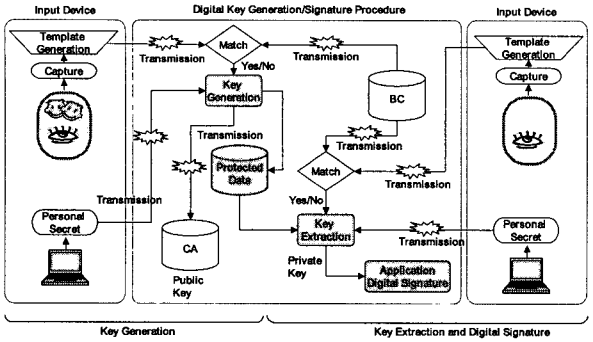


▶▶그림 15. 서버 중심 바이오 디지털 키 기반 응용 구조



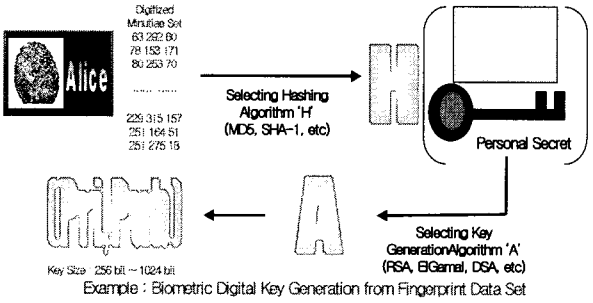
▶▶그림 16. 클라이언트 중심 바이오 디지털 키 기반 응용 구조

새로운 접근방식은 (그림 17)과 같이 일반화할 수 있다.



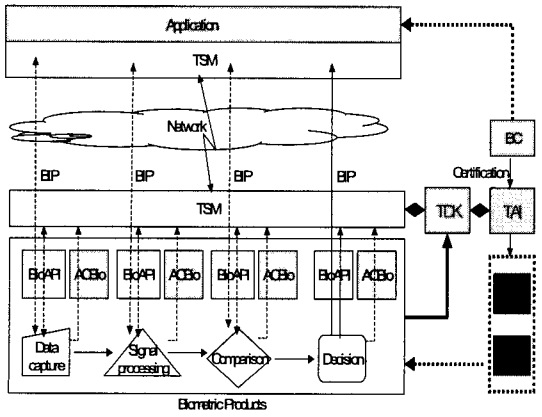
▶▶그림 17. 바이오 정보 기반 키생성 및 전자서명 구조

제안한 기법은 (그림 18)와 같이 지문과 같은 바이오 정보에서 특징점에 해당하는 바이오 템플릿 정보를 추출하고 이를 이용하여 개인키와 비밀키 쌍을 생성할 수 있다.



▶▶그림 18. 바이오 정보 기반 디지털 키 생성 단계

본 연구에서 개발한 바이오 정보 기반 키생성 및 전자서명 알고리즘 등은 (그림 19)와 같이 현재 ITU-T SG17에서 진행중인 기존의 연구과제와 연관성 및 차별성을 갖는다.



▶▶그림 19. 기존 ITU-T SG17 Q.8 기술과의 연계성

4.2 바이오정보 기반 키생성 모델

가. 제안한 모델에서의 주요 모듈 구성

(1). 사용자 바이오정보

사용자 바이오정보는 고유하기 때문에 각 사용자의 신분 정보를 대신할 수 있는 특성을 갖으며 전자서명 키를 생성하기 위해서 사용자가 임의로 선택하는 비밀 값과 함께 사용된다. 바이오정보와 사용자 비밀 값을 같이 사용함으로써 전자서명 키를 취소하고 재등록할 수 있는 특성을 갖게 된다.

(2) 사용자 비밀 값

사용자 비밀 값은 전자서명 키 생성 단계에서 사용자에 의해서 직접 입력된다. 키 생성 시에 사용자 비밀 값을 달리하여 여러 개의 서로 다른 전자서명 키 값을 생성할 수 있다. 이렇게 함으로써 전자서명 키의 취소 및 재등록을 가능하게 한다.

(3) 해쉬 함수

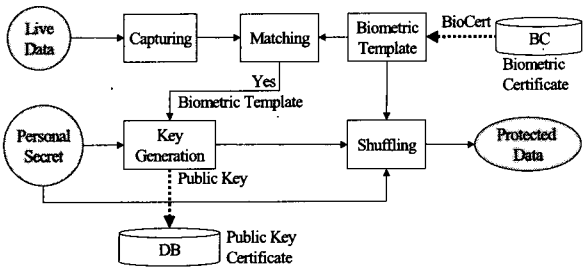
전자서명 개인 키 생성을 위해서 해쉬 함수를 사용한다. 사용자 비밀 값과 바이오정보를 해쉬 함수의 입력으로 받는다. 사용자 비밀 값을 조정하여 전자서명 개인키로 사용할 수 있는(적용되는 디지털 서명 알고리즘에 따라서 공개키 및 개인키 생성 조건이 서로 상이함) 해쉬 결과 값을 찾아낸다.

(4) 키 은닉 함수

전자서명 개인키 보호를 위해서 퍼지볼트 기법과 같은 키 은닉 함수가 필요하다. 바이오정보를 이용하여 키를 은닉함으로써 개인키를 이용한 대리 서명 등의 위험요소를 배제할 수 있다.

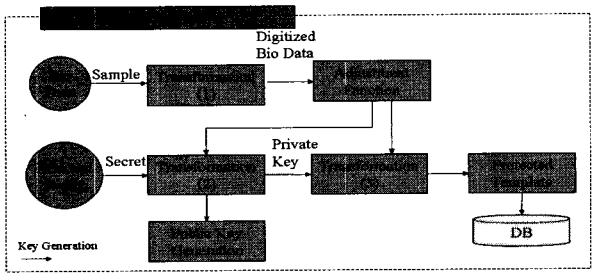
나. 제안한 바이오 정보 기반 키 생성 방법

(그림 20)과 같이 바이오 정보로부터 디지털 키를 생성하고 이를 안전하게 저장하는 구조를 형성할 수 있다. 개인에 대한 바이오 정보를 입력받아 기존에 저장되어 있는 정보와 비교하고 인증이 성공한다면 바이오 정보로부터 공개키/개인키 쌍을 생성하는 과정을 수행한다. 생성된 개인키에 대해서는 안전한 형태로 보호/저장하고 공개키 정보는 기존의 PKI 방식과 유사하게 공개한다.



▶▶그림 20. 바이오 기반 전자서명 키생성 단계

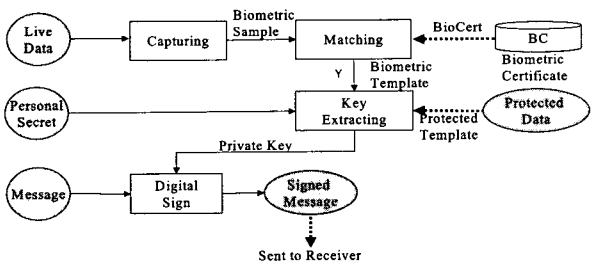
좀 더 구체적으로 살펴보면 다음과 같다. (그림 21)은 제안한 키 생성 모델을 보여준다. 사용자는 바이오정보를 캡춰하고 이를 디지털 데이터로 변환할 수 있는 지문 인식 장치를 이용하여 자신의 바이오정보를 입력한다. Transformation 1 함수는 입력된 사용자 바이오 이미지로부터 특징점을 추출한다. Transformation 2 함수는 특징점 데이터와 사용자 비밀 값을 함께 해쉬하여 취소 및 재등록할 수 있는 특성을 갖는 전자서명 개인키를 생성한다. Transformation 3 함수는 개인키를 바이오정보에 은닉한 protected 템플릿을 만들어 낸다.



▶▶그림 21. 바이오 기반 전자서명 키 생성 모델

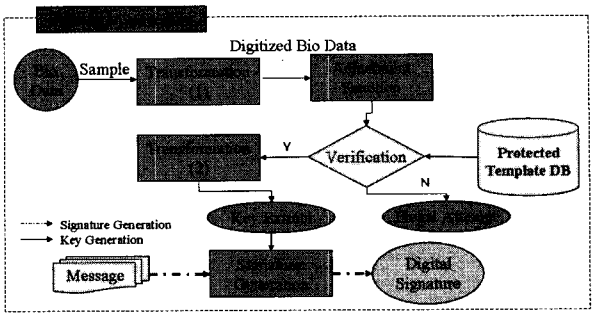
다. 바이오 정보 기반 전자서명 생성 모델

아래 그림과 같이 개인에 대한 인증 과정을 수행하고 만일 정당한 사용자라고 한다면, 기존에 안전하게 저장된 키 값을 추출하고 이를 사용하여 메시지에 대한 전자서명 또는 암복호화 과정을 수행할 수 있다.



▶▶그림 22. 바이오 기반 전자서명 키 추출 및 전자서명 단계

바이오 정보로부터 생성된 키를 사용하기 위해서는 우선 안전한 추출 과정이 선행되어야 한다. 구체적으로 아래 (그림 23)과 같은 과정을 수행한다.

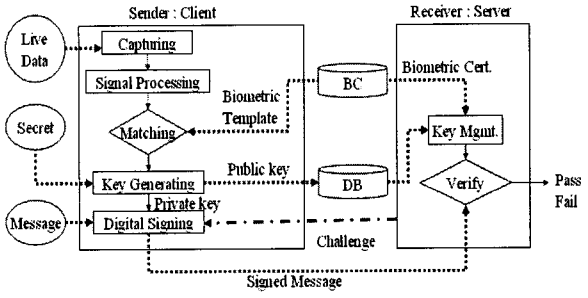


▶▶그림 23. 바이오 정보 기반 전자서명 모델

정보보호 기법에 바이오 인증 기법을 접목하기 위하여 제안한 모델에서는 보정 함수를 사용한다. 보정 함수는 동일한 사용자의 서로 다른 바이오 이미지로부터 고유한 특징점을 추출할 수 있도록 도와준다. 키 생성 모델에서 개인키 보호를 위하여 퍼지 볼트 등의 기법을 적용하여 protected 템플릿에 개인키 정보를 은닉한다.

5. 응용분야

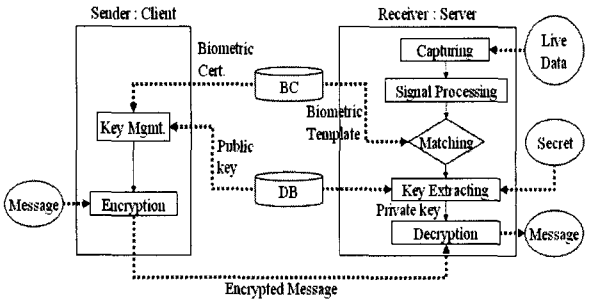
메시지에 대한 디지털 서명은 원격 통신 시스템에서 메시지에 대한 인증, 무결성 및 부인봉쇄 기능을 제공한다. 따라서 아래 그림과 같이 적용 가능하다.



▶▶그림 24. 바이오 정보 기반 디지털 서명 구조

또한 바이오 정보를 기반으로 디지털 키를 사용하여 메시지에 대한 암복호화 기능을 제공할 수 있다. 바이오 기반 암복호화 방식에서 수신자의 공개키를 CA 인증서로부터 받은 후에 안전한 통신을 위해 보내고자 하는 메시지에 대한 암호화 과정을 수행한다. 복호화 과정에서

는 바이오 기반 인증 과정을 수행한 후에 개인키를 추출하고 수신된 메시지에 대해 적용하는 과정은 아래 그림과 같다.



▶▶그림 25. 바이오 정보 기반 메시지 암복호화 구조

6. 결 론

본 연구에서는 바이오인식 기술 표준화 동향 분석을 토대로 바이오정보를 이용한 기존의 전자서명 기법을 고찰하였고, ITU-T SG17/Q8을 통해 추진중에 있는 바이오정보 기반 디지털 키생성 프레임워크에 대해 제시하였다. 바이오 정보를 기반으로 한 키 생성 및 전자서명 기술은 다양한 응용 분야를 갖게 될 것으로 예상된다. 따라서 안전하고 체계적인 전자서명 키 생성 기술의 개발 및 연구를 통해 국내 바이오 정보보호 기술의 발전과 바이오 인식 기반 정보보호 시장의 활성화를 선도할 수 있을 것으로 예상된다.

아직 바이오정보를 이용한 전자서명 키 생성 기술은 초기 연구 단계로서, 기술적인 측면에서의 안정적인 구현 가능성 및 안전성 평가 방안이 개발되어야 한다. 이를 통해 앞으로 바이오 인증 기술과 전자서명 기술을 연계한 시제품이 개발될 것으로 예상되며 해당 기술에 대한 국제 표준화 과정도 시급할 것으로 판단된다.

참고문헌

[1] A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," to appear in the International Conference on Image Processing(ICIP), Greece, October 7-10, 2001

[2] Digital Persona, Inc. Fingerprint-based Biometric Authentication. http://www.digitalpersona.com

[3] RealID Technology, "Biometrics PKI Note," http://www.realid.co.kr

[4] Peter Orvos, "Biometric generation of digital keys," Mini Symposium, DMIS-BUTE, 2001

[5] FindBiometrics, "The distinction between biometric and digital signatures," http://www.findbiometrics.com

[6] CyberSign, "Biometric electronic signature authenti cation system," http://www.cybersign.com

[7] 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

[8] 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

[9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key crypto systems," Communications of the ACM, vol.21, pp.120-126, 1978.

[10] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-30, No. 4, pp.469-472, 1985.

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

[12] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," Proceedings of BioAW 2004, Lecture Notes in Com puter Science 3087, Springer-Verlag, pp.158-170, 2004.

[13] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometrics," Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science 3494, Springer-Verlag, pp.147-163, 2005.

저자소개

◉ 이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1996년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1999년 3월~ 2003년 2월 : 천안대학교 정보통신학부 조교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 부교수

<관심분야> : 바이오 정보보호, 네트워크 보안 등

● 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

● 문 기 영(Ki-Young Moon) 정회원

- 1986년 : 경북대학교 전자공학과 학사(공학사)
- 1989년 : 경북대학교 전자공학과 석사(공학석사)
- 2006년 : 충남대학교 전산학 박사(이학박사)
- 1992년 ~ 1994년 : (주)대우정보시스템 기술연구소 전임연구원
- 1994년 3월~현재 : 한국전자통신연구원 정보보호연구단 바이오인식기술연구팀 팀장

<관심분야> : 바이오인식, 웹서비스 보안, 분산시스템 등

● 정 윤 수(Yun-Su Chung) 정회원

- 1993년 : 경북대학교 전자공학과 학사(공학사)
- 1995년 : 경북대학교 전자공학과 석사(공학석사)
- 1998년 : 경북대학교 전자공학과 박사(공학박사)
- 1999년 ~ 현재 : 한국전자통신연구원
- 2005년 ~ 현재 : SC37 Korea 생체인식전문위 전문위원, TTA PG103 바이오인식 프로젝트그룹 부의장, 바이오인식포럼 운영위원

<관심분야> : 바이오인식, 컴퓨터비젼, HCI, HRI