Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.665

한국형 금융 바이오 인식 기술 도입을 위한 분석 및 방안연구*

신 용 녀,[1†] 전 명 근[2‡]
[1]금융보안원, [2]충북대학교

Analysis on international financial biometric adoption cases and propose a scheme for korean financial telebiometrics*

Yong-Nyuo Shin,[1†] Myung Geun Chun[2‡]
[1]Financial Security Institute, [2]Chungbuk National University

요 약

본 논문에서는 스마트폰 및 ATM 등의 전자금융 환경에서 바이오인식 도입 해외사례를 분석하였다. 국가별 프라이버시 이슈, 금융서비스 여건, 정부의 정책방향 등의 차이에 따라 바이오인식 도입 양상이 다르게 나타나고 있었다. 국내에서도 핀테크 활성화 및 편의성이 뛰어난 모바일 중심의 금융서비스로의 규제환경의 변화로 인해 바이오인식기술 도입이 적극적으로 논의되고 있는 시점이다. 본 논문에서는 각국의 금융 분야 도입 사례 분석을 통해 한국형 금융 바이오인식 기술 도입을 위한 방안을 제시한다. 그리하여 금융 분야 바이오인식 도입을 위한 정책 수립 시 정확한 의사결정 방향에 도움이 되고자 한다.

ABSTRACT

In this paper, we analyze the international financial biometric adoption cases in smart phones and ATMs and propose a scheme for Korean financial telebiometrics. Regional privacy issues, financial services environment, according to the differences in the direction of government policy introducing biometric aspects were appearing differently. In Korea, due to changes in fin-tech vitalization and outstanding convenience mobile oriented service to the regulatory environment, the introduction of biometric technology is the point that is being actively discussed. In this paper, we propose a scheme for the Korean banking financial sector through the introduction of biometric technology adoption case analysis of each country. Thus, this paper is intended to help that the financial sector makes a precise decision when it is establishes a policy of biometric technology application for electronic financial services.

Keywords: Financial Security, Policy, Banking Services, Biometrics, ATM, SmartPhone, Mobile Device, Privacy

I. 서 론

세계 바이오인식 기술 금융 분야의 사용은 2012년에 9억 달러에서 2015년에는 18억 달러에 이를것으로 전망되고 있다. 이것은 금융 시장 70억 달러 12%에 해당하는 수치로 지속적으로 증가될 것으로 예상되고 있다[1].

스마트폰에서의 바이오인식기술 도입이 수요증가의

접수일(2015년 3월 9일), 수정일(2015년 4월 3일), 게재확정일(2015년 4월 22일)
* 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2013R1A1A2011593)
† 주저자, ynshin@fsec.or.kr
‡ 교신저자,mgchun@chungbuk.ac.kr (Corresponding author)

한 원인이기도 하지만, 아시아등을 포함한 개발도상국에서 금융시장 바이오인식 도입이 지속적일 것으로 예상되고 있다.

바이오 정보의 네트워크 전송에 있어서 북미 등의 지역은 매우 신중한 모습을 띄는 반면에 아시아 지역에서 적극적이다. 특히, 인도 등 정부주도로 바이오인식 인식 프로그램을 뱅킹 및 바이오 지급 결제 프로세스까지 확장한 국가들의 성장세가 두드러진다. 법률적 한계나 프라이버시 우려가 상대적으로 큰 미국 등에서는 모바일 결제 플랫폼인 애플페이(Apple Pay)[2]나 FIDO(Fast IDentity Online)[3] 등 바이오인식 인증 결과 값으로 지급결제를 수행하는 방향으로 금융시장에 도입이 이루어지고 있다. 애플페이의 주요 협력업체인 BOA(Bank of America)는 자사의 고객 가운데 80만명이 애플 페이를 사용하기 시작했다고 밝혔다[4]. 금융위원회는 "IT 금융융합 지원방안[5]" 하나로 오프라인 위주의 금융제도를 개편함에 따라 한국형 인터넷 전문은행 모델이 수립되고 있고, 비대면 실명확인 허용 등 엄격한 대면확인 원칙에 대한 합리적인 완화방안 강구되고 있다. 또한, 금융당국은 공인인증서 등의 특정 기술 사용을 강제하는 금융업법상 의무규정을 일괄 폐지·개선하였다. 공인인증서에 의한 전자서명의 한계를 극복하며 절도나 누출에 의하여 도용 되거나 분실할 위험성이 상대적으로 적은 새로운 형태의 전자인증 방법에 대한 요구가 지속적으로 제기되고 있다. 이에, 국내 전자지급결제에 보안성이 강화된 바이오인증기술을 활용하기 위해서 해외 금융권 바이오인식 도입사례를 조사·분석함으로써 한국형 금융바이오 인식 기술 도입을 위한 방안을 도출하고자 한다.

II. 금융 산업의 바이오인식 도입 현황

2.1 애플페이

애플(Apple)은 2014년 9월 모바일 결제서비스인 애플 페이(Apple Pay)를 출시하였다. NFC 기반 오프라인 결제, 원터치의 편이성 제공하며, 등록된 아이튠즈 결제정보를 이용하거나 사진을 찍어서 신용카드를 추가하는 기능 제공한다. 애플페이는 아이폰6와 아이폰6플러스, 애플워치에 탑재된 근거리 무선통신(NFC) 기술을 이용해 신용카드 없이 결제가 가능하다. 작동방식에 있어서 아이폰 홈버튼에 본인 손가락을 올리고 매장에 위치한 기기에 가까이 댄 후 지문인식을 수행한다. 지문센서에 있어 에어리어(Area) 방식의 반도체식 센서에 내구성 강화를 위해 사파이어글라스를 사용함으로써 고난도 기술 적용하였다. 보안적 특징을 살펴보면, 지문인식, 보안영역 활용, 토큰화로 보안성을 강화하였다. 지문인식에 있어서도 반도체식 센서로 홈버튼에 장착되어 터치 ID로 추출된 특징점은 보안칩(Secure Enclave)에 저장한다. 템플릿은 보안 영역(Secure Data Repository)에 저장되며, 비교(Matching)를 위해 보안 프로세서(Secure Enclave Processor)와 별도 채널을 사용한다. 특히, 결제정보는 토큰화 기술을 이용해 암호화되기 때문에 결제단말기는 암호화된 결제정보만 전달하고, 결제 시스템을 제공하는 신용카드 회사만이 암호 해독 가능하다. 일회성 동적 보안코드(Transaction-Specific Dynamic Security Code)와 단말기 계정정보(Device Account Number)만을 애플페이가 전달한다.

2.2 FIDO

FIDO(Fast IDentity Online) 얼라이언스는 온라인 환경에서 바이오인식기술을 활용한 인증방식에 대한 기술표준(De Facto)을 정하기 위해 2012년에 설립되었다. 이용자 단말에서의 사용자 로컬 인증과 서비스 제공 기관의 서버에서 수행하는 원격 인증을 분리하는 것으로, 사용자는 지문, PIN, H/W등 다양한 인증방식을 사용하더라도, 서버 측에서는 하나의 FIDO 모듈만 설치하면 모든 인증수단을 수용할 수 있는 구조이다. FIDO(Fast IDentity Online) 인증 기법은 크게 범용 인증 프레임워크(Universal Authentication Framework) 프로토콜과 범용 투팩터(Universal 2nd Factor) 프로토콜로 나뉜다. UAF는 사용자 디바이스에서 제공하는 인증방법을 온라인 서비스와 연동하여 사용자를 인증하는 기술로 Fig.1.과 같다.

Fig. 1. UAF User Authentication

UAF 모듈이 설치된 사용자가 온라인 결제를 위해 인증 시도 후 사용자는 모바일 디바이스에서 바이오 인식을 수행한다. 즉, 지문과 PIN등의 멀티 팩터 인증 메커니즘이 가능하다. U2F는 기존 패스워드를 사용하는 온라인 서비스에서 두번째 인증요소로 강한 인증을 사용자 로그인 시에 추가할 수 있는 Fig. 2. 와 같은 프로토콜이다. U2F 사용자 인증에서는 UAF 모듈이 패스워스를 사용해 1차 인증을 수행하고, 보안키를 저장한 동글(Dongle)을 USB 포트에 꽂아 2차 인증을 수행한다. 즉, FIDO 모듈이 설치된 웹 서버에서 사용 가능한 인증 리스트를 클라이언트에 제시된다.

Fig. 2. U2F User Authentication

2.3 해외은행 바이오인식 도입현황

각 국가별 프라이버시 이슈, 금융서비스 여건, 정부의 정책방향 등의 차이에 따라 바이오인식 도입 양상이 다르게 나타났다. 프라이버시나 법률적인 이슈로 인해 인도, 터키 등 개발도상국과 아시아권 위주의 금융권 바이오인식 도입사례가 대다수였다. 미국의 경우, 프라이버시나 법률적 이슈로 인해 ATM 바이오인식 도입 사례는 전무하나, 모바일 뱅킹서비스에서 개인정보 입력 없이 목소리로만 본인 확인 및 이체 가능하였다. 또한, 애플의 터치ID(지문인식) 센서를 활용하여 뱅킹 서비스 로그인 시 패스워드 대체 수단으로 사용되고 있다. US Bank, USAA 등 음성인식기반 모바일 뱅킹 서비스 위주로 사용자 인증 및 계좌 조회, 이체 등 명령실행 가능하다. PIN, 얼굴인식, 음성인식 등의 인증옵션들을 제공하고, 앱에서 생성되는 보안코드와 함께 결합하는 형태의 멀티팩터(Multi Factor) 인증방식을 채택하는 경향을 보였다.

프랑스에서는 은행 간 카드협회(Groupement d'Interet Economique des Cartes Bancaires; CB그룹)가 ATM이나 소매결제에 지문인식 적용하고 있다. 바이오인증을 이용하는 고객이 바이오정보를 저장한 매체를 소지하는 형태로 은행은 바이오정보를 소유하지 않는다. 일본의 경우, 대지진 등의 자연재해로 통장이나 은행카드의 분실 소지가 많아 대부분의 ATM 내 정맥인식기가 탑재되면서 위조가 상대적으로 어려운 정맥인식이 활성화된 측면이 있었다. Japan Post Bank, Mega Bank 등 약 80,000 대의 ATM 내 정맥인식 탑재되어 있다. 은행 서버에 바이오정보 등록 및 생년월일을 입력해 데이터베이스에서 검색 대상 정보를 한정하고 있다. 인도등의 개발도상국에서는 국가 ID 사업과 연계된 ATM 바이오인식 적용 사례가 다수이며, 바이오인식만으로 신원을 인식하고 해당 은행 계좌로 연결하여 결제 진행하고 있다. 홍채, 지문, 얼굴인식 등 다양한 모달리티(Modality)를 사용하며 국가, 은행이 바이오정보를 소유한다. 인도는 국민 전체에 바이오정보가 포함된 신분증을 제공하는 Aadhaar 프로젝트의 일환으로 ICICI Bank, State Bank of India 등의 ATM에서 이용 가능하다. 2014년 2월 기준 인도인구 중 약 7억 5천만 명 이상이 등록을 완료하였다. 브라질 CAIXA Bank에서는 모바일 뱅킹 앱에서 지문인식을 이용한 계정 로그인 기능 제공 및 ATM 내 탑재된 지문인식을 통해 현금 인출이 가능하다. 터키 Deniz Bank의 81개 지역 ATM 기기에서 모바일 앱 음성인식 아이콘을 누르고 모바일 기기에 음성인식 후 인출이 가능하다. 르완다에서는 상점 결제 등 모든 금융거래가 신용카드나 ID카드 없이 계좌 소유자의 등록된 지문만으로 가능하다. 선진국에서는 프라이버시 이슈로 인해 중앙 집중적 바이오인식 데이터베이스 구축에 소극적인 반면, 개발도상국에서는 국가 ID 사업과 연계된 바이오인식 도입사례가 다수이며 은행이 바이오정보를 소유하는 특징을 가진다. 선진국에서도 편이성 측면에서 음성, 지문 등 금융권 바이오인식 도입사례 증가와 더불어 바이오 저장 매체 기반 인증 및 보안성 강화 추세가 두드러진다.

Table 1. International Financial Biometric Cases('12~'14)

Country	Bank	Modality	Methods
U.S	US-Bank	Voice	- Enable customers to view and account information in
	JPMorgan Chase		

			the mobile app - Identify authenticity for comparison with the audio information stored in
	Wells Frago		
UK	Barclays	Finger Vein	Approach that combines electronic signatures through the finger vein authentication technology(PKI)
Turkey	Biyokimlik	Finger Vein	3,400 branch ATM Sensor
Australia	National Australia Bank	Voice	Voice recognition system can be selected in phone banking system
Spain	BBVA	Voice	Voice recognition support in banking apps
Poland	BPH S.A	Finger Vein	- Customers finger vein authentication at the ATM, No need to enter PIN
Russia	Sberbank	Voice	- system for all credit transactions, including credit card issuers to make available from ATM
	Leto-Bank	Finger	- Fingerprint branch ATM Sensor
Palestine Jordan	Cairo Amman Bank	Iris	- Store 100,000 biometric data - More than 500 cameras for iris used in Customer
			service desk, Teller Secrion and ATM
Brazil	CAIXA	Finger	- Fingerprint branch ATM Sensor
	Itautec	Finger	- 12,000 branch ATM Sensor
Japan	Japan Post Bank	Finger Vein	- 20,239 branch ATM Sensor(100%)
	Mega Bank	Finger, Palm Vein	- 2,408 branch ATM Sensor
	Trust Bank	Finger Vein	- 295 branch ATM Sensor (63%)
	Regional Bank	Finger, Palm Vein	- 7,487 branch ATM Sensor
	Local Bank	Finger, Palm Vein	- 3,283 branch ATM Sensor

III. 한국형 금융 바이오 인식 기술 도입을 위한 방안

아직까지도 선진국에서는 바이오정보의 보안적 이슈로 인해 바이오 정보의 네트워크 전송에 있어서 매우 신중한 모습이며, 바이오 저장 매체기반 인증 및 보안성 강화 추세에 있다. 국내에서는 금융환경에 바이오인식 도입을 위한 시도는 지속적으로 있어왔으나, 유출 시 바이오 정보의 특성상 영구적으로 악용될 수 있는 우려로 인해 금융 산업 전반에 바이오인식 기술의 적극적 도입이 어려웠다. 핀테크 산업의 안전장치로써 바이오인식 기술이 온라인상에서 안전하고 편리한 본인확인 수단으로 활용되기 위해서, 기술적·관리적으로 도입되어야하는 방안들을 3장에서 기술하고자 한다.

3.1 바이오인식 원본영상 보호를 위한 기술적 방안

템플릿으로부터 원본 이미지 복원이 가능하기 때문에 이를 어렵게 만드는 기술적 방안 도입 필요하다. [6]에서는 NIST-4f 데이터베이스에 저장된 템플릿에 대하여 상용 알고리즘을 사용하여 원본 이미

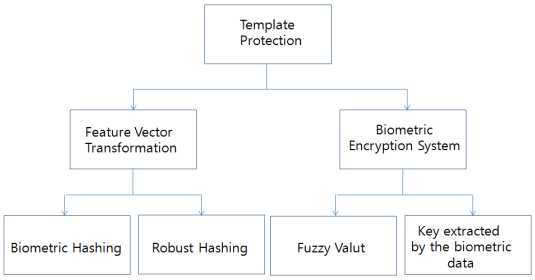


Fig. 3.Template Protection Scheme

지 복원 증명하였다. 일부 바이오인식 벤더들은 템플릿 포맷이 각 사의 고유의 포맷이며, 템플릿이 유출되더라도 제 3자의 도용이 불가능하다고 주장하고 있다. 그러나, 상호호환성 및 표준적합성 시험을 위해 국제 표준 ISO SC37 19794-2[7] 템플릿포맷 준용이 국제적 추세이며, 원본 이미지 일부 복원도 프라이버시 침해로 이어질 개연성 존재한다. 따라서, 특징벡터 변환이나 바이오 암호시스템을 통한 바이오인식 템플릿 보호를 위한 기법 도입 방안 마련이 필요하다. Fig. 3.은 템플릿 보호기법을 보여주고 있다.

특징벡터 변환 방법은 사용자가 지정한 킷값이나 패스워드로부터 정의되는 함수에 기초한 방법으로 역변환이 가능한 경우나 가능하지 않은 경우로 나뉜다. 바이오암호시스템의 대표적 방법으로 비밀키와 특징점 정보를 통합하여 정당한 사용자만이 비밀키를 획득할 수 있는 퍼지볼트(Fuzzy Valut)가 있다[8]. 퍼지볼트(Fuzzy Valut)는 사용자의 비밀키를 이용하여 다항식을 생성하고, 거짓 특징점(chaff minutiae)을 랜덤으로 생성한 후 특징점과 함께 지문 템플릿을 구성한다.

3.2 분할 템플릿에 기반한 분산 관리 방안

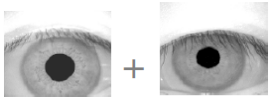
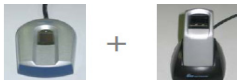
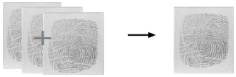
바이오정보 유출 방지를 위한 분할 템플릿으로 복수 개의 데이터베이스에 분산 관리 방안 관련 특허는 국내외적으로 꾸준히 출원되고 있다. 국내 특허로는 분산형 생체 인식 서비스 제공 방법(출원번호:10-2013-0045825, 슈프리마), 생체인증 시스템과 그 생체 인증방법(10-2010-0137482, 유니온커뮤니티)이 대표적이다. 바이오 인증 정보는 변경할 수 있는 것이 아니므로 인증수단 측의 서버에 저장해 둔 바이오 정보가 유출될 경우에는 그 피해는 다른 인증수단보다 더 심각하다. 금융권에서는 바이오정보 관리센터의 카드승인 과정의 사인, 인터넷뱅킹 공인인증서 절차에 바이오인증을 도입하기 위해 금융결제원에서 테스트베드를 구축·운영 중에 있다. 보안적 관점에서 보면 특징점 정보가 네트워크상에 전송되지 않고, 별도의 채널로 분리된 하드웨어 상에 저장되어 인증 결과만으로 금융서비스를 제공하는 것이 바람직하나, 네트워크로 전송이 불가피 할 경우, 바이오정보를 분할하여 분산 관리함으로써, 해킹 등에 의해 사용자의 바이오정보가 유출될 위험을 낮출 수 있는 방안 마련이 필요하다.

3.3 다중 바이오정보 혹은 멀티팩터 인증 방안

단일 바이오인식에 의존할 경우 저가형 센서의 보급으로 인식성능 저하 사례가 발생할 수 있다. 또한, 개인의 신체적 특징에 의해 단일 바이오인식 제공이 힘든 사례 존재할 수 있다[9]. 국내 금융 서비스의 안전성과 범용성을 획득하기 위해서는 Table 2와 같은 다중 바이오정보 및 다중 개체 등의 도입이 필수적이다. 또한, 국내 ATM에 바이오인식 도입 고려에 있어서 아프리카 등에서 에볼라 바이러스로 인해 비접촉식에 대한 요구가 있다는 점에 주목해야 한다. 애플페이 등의 개인사용에 한정된 모바일 디바이스의 경우 지문 인식 등 접촉식이 적합할 수 있으나, ATM등 공공적으로 사용되는 서비스에 있어서는 홍채 등 비접촉식에 대한 요구가 현대화 사회에서 증대될 수 있다. 일본 ATM의 경우 지문과 PIN의 멀티팩터(Multi Factor) 인증 메커니즘으로 보안 등급을 강화한 모델을 도입하고 있다. ATM을 통해 본인의 생년월일을 입력하여 검색 대상을 한정하고, 센서에 손바닥정맥을 인식하여 정보 일치여부 확인 후 비밀번호를 입력하여 거래에 이용하고 있다.

Table 2. Multiple Recognition Model Features

Classification	Feature	Note
Multi-modal	Recognize at least two different modality data (ex. face + fingerprint) 	

Multi-instance	Acquire a number of instances from same modality (ex. right iris + left iris, right thumb fingerprint + left thumb fingerprint) 	
Multi-algorithms	Applying a different recognition algorithm for a single instance 	Based on S/W
Multi-sensor	Using multiple sensors on a single instance 	Based on H/W
Multi-sample	Information extracted with several representations with respect to the biometric data of a single instance 	Based on User Input

모바일 디바이스 사실표준(De-facto)인 FIDO의 멀티팩터 인증이 국제적 추세이다. 기존 패스워드를 사용하는 온라인 서비스에서 두 번째 인증요소로 바이오인식을 사용하고 있다. NIST[10]의 보안 등급별 적용 인증 수단에서도 높은 등급의 레벨(Level) 3 이상의 인증을 위해서는 싱글 팩터(Single Factor) 사용 보다는 멀티 팩터 소프트웨어 암호 토큰, 멀티 팩터 OTP 장치, 멀티 팩터 암호장치를 권장하고 있다.

3.4 위조 판별 성능평가 방안 도입

국제 범죄자나 테러리스트의 입국을 막기 위해 2007년 11월부터 외국인의 지문 등록 및 얼굴 사진 촬영을 의무화한 일본은 공항과 항만에 600여개의 지문 인식 기계를 설치해 효과를 보고 있다. 하지만 위조지문을 이용하여 일본 공항의 지문감식시스템을 통과하는 사고가 빈번하게 발생 되었다. 지문을 떠낼 때 사용하는 본드는 문구점에서 판매하는 평범한 제품이었지만, 위조를 위해 지문의 융선(隆線)까지 가장 잘 재현 하는 본드를 찾기 위해 여러 차례 실험을 거쳤다고 한다[11]. 안정성을 보장하는 전자금융 환경에 바이오인식 기술 도입 시 위조에 강인 할 수 있도록 위조 판별 성능평가 방안 도입은 매우 중요하다. 비밀번호는 유출시 변경 가능하지만 바이오 정보는 유출 시 바이오 정보의 특성상 영구적으로 악용될 수 있으며, 애플페이등에 적용된 아이폰의 지문 인식 기능은 보안 위협이 존재한다. 독일의 해커단체 Chaos Computer Club(CCC)은 독일 국방부 장관의 사진에서 엄지손가락 부분을 이용해서 아이폰6의 지문 복제를 시연한 바 있다[12]. 기존 국가기반시설 바이오인식 도입에 대한 위조지문 비공개 BMT의 경우도 피시험자의 개수가 적어 신뢰성에 의문이 제기된바 있다. 피시험자(지문제공자, 연령 20~40대 남녀 총 12명)에 대하여 종이모조지문(A社 스캔오류), OHP 필름(4개社탐지), 실리콘(4개社탐지), 젤라틴(3개社실패)등으로 한정되어 있었다. 금융권 위조 판별 성능평가를 체계적으로 수행하기 위해서는 위조지문 데이터베이스 구축 활용이 불가피하다. 위조지문판별 기법은 크게 하드웨어 방식과 소프트웨어 방식을 나뉜다[13]. 하드웨어 방식은 추가적인 하드웨어를 사용하여 맥박이나 온도와 같은 바이오인식 고유의 신호를 측정한다. 관련특허는 광 투과도 검출을 이용한 위조지문 검출(니트젠), 정전용량 변화 방식의 위조지문 검출(유니온커뮤니티)등이 있다. 소프트웨어 방식은 지문 인식 센서로부터 얻은 영상에서 바이오 지문과 위조 지문 영상의 차이를 분별한다. 즉, 발한작용기반, 피부왜곡기반, 영상품질 기반으로 구분한다[14]. 위조지문을 위한 검증시나리오는 Table 3.과 같다.

위조지문 판별기술은 다양한 방식으로 많이

Table 3. Fake Fingerprint Verification Scenarios

Scenario	Enrollment	Authentication
Real - gummy	Real Fingerprint	gummy Fingerprint
gummy - Real	gummy Fingerprint	Real Fingerprint
gummy - gummy	gummy Fingerprint	gummy Fingerprint

제안되어 있지만 실제 환경에서 잘 응용되는 사례는 적다. 가장 큰 문제의 하나가 위조지문 판별기술의 안정성이다. 이를 위해서는, 위조지문을 만드는 재료에서부터 만드는 과정을 모두 규격화해야 한다. 위조지문을 만드는 재료는 가능한 모든 재료를 포함시켜주어야 하고 만드는 과정도 다양하게 하되 품질이 상, 중, 하로 모두 제작되어야 한다.

표준화 샘플 세트가 제작 되면 하드웨어적 또는 소프트웨어적 방식의 위조지문 판별 기술에 대해 모두 평가 할 수 있다. 하드웨어적 방식을 평가하는 경우, 위조지문으로 직접 하여 판별 여부를 체크하면 된다. 소프트웨어적 방식을 평가하는 경우 지문영상 데이터베이스를 먼저 구축해야 하는데 광학식, 반도체방식, 열방식 등 다양한 센서를 사용하여 지문영상을 수집하여야 한다.

IV. 결 론

국내에서는 천송이 코드 사건이후로 금융분야 있어서 핀테크 활성화 및 편의성이 뛰어난 모바일 중심의 금융서비스로의 규제환경의 변화로 금융당국의 정책이 변화하였다. 공인인증서 등의 특정기술 사용을 강제하는 금융업법상 의무규정을 일괄 폐지되었고, 새로운 형태의 전자인증 방법에 대한 요구 및 금융회사 자율에 따라 안전한 인증방법 선정 필요하게 되었다. 특히, 한국형 인터넷 전문은행 도입을 위한 비대면 방식의 실명확인 허용 등 금융거래 시 엄격한 대면확인 원칙이 완화될 예정이다. 온라인상의 안전하고 편리한 본인확인 수단은 핀테크 산업의 안전장치로써 반드시 해결해야 하는 사항이다. 이에, 본 논문에서는 국내 전자금융 환경에 보안성이 강화된 바이오인증기술을 활용하기 위해 해외 금융권 바이오인식 도입사례를 조사·분석함으로써 기술적·관리적 이슈를 도출하였다. 국내 금융시장에서 바이오인식기술 도입 시 고려해야할 사항에 대하여 도출함으로써, 바이오인식 산업 활성화에 기여할 수 있을 것으로 판단된다.

References

〔1〕 Biometrics Research Group, http://biometrics.cse.msu.edu/, 2014년.

〔2〕 Apple, "iOS Security Guide," https://www.apple.com/br/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

〔3〕 FIDO Alliance, "UAF Specifications," https://fidoalliance.org/specifications/download

〔4〕 Biometrics Research Group, "Banking and Biometrics White Paper," http://www.biometricupdate.com/201412/special-report-biometrics-and-banking

〔5〕 Financial Services Commission, Financial Services Commission 2015 work plan, http://www.fsc.go.kr/info/ntc_bref_view.jsp?menu=7210200&bbsid=BBS0029&no=30558

〔6〕 Arun Ross, "From Template to Image : Reconstructing Fingerprint from Minutiae Points, IEEE Transaction on pattern analysis and machine intelligence," pp.544-560, VOL. 29, No. 4, April 2007.

〔7〕 ISO/IEC JTC1 SC27 WG5 International Standard 24745, "Biometric Information protection," 2011.

〔8〕 Yong-Nuyo Shin, "Biometric and Identity Reference Protection," Journal of Korean Institute of Intelligent Systems, p.160-167, VOL. 19, No. 2, April 2009.

〔9〕 Yong Nyuo Shin and Woo Chang Shin, "A Security Reference Model for the Construction of Mobile Banking Services based on Smart Phones," INTERNATIONAL JOURNAL of FUZZY LOGIC and INTELLIGENT SYSTEMS Vol.11 No.4, pp 229-237, DEC 2011.

〔10〕 NIST Special Publication 800-63-2, "Electronic Authentication Guideline," 2013.

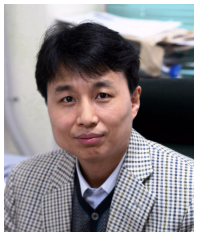
〔11〕 YTN, "Silicon fingerprint forgery Japan to help illegal entry," http://search.ytn.co.kr/ytn_2008/view.php?s_mcd=0103&key=201005061206516637&q=%B5%B7, May.2010.

〔12〕 Hacker News, "Hacker Clones German Defense Minister's Fingerprint Using Just her Photos," Dec.2014, http://thehackernews.com/2014/12/hacker-clone-fi

ngerprint-scanner.html
[13] TTA(TTAR-12.0006), Technical Report on Fake Fingerprints Detection, 2010.11.
[14] T. Shimamura, H. Morimura, N. Shimoyama, T. Sakata, S. Shigematsu, K. Machida, and M. Mamoru, "A Fingerprint Sensor with Impedance Sensing for Fraud Detection," presented at IEEE International Solid-State Circuits Conference (ISSCC), 2008.

〈저자소개〉

신 용 녀 (Yong-Nyuo Shin) 종신회원
1999년 2월: 숭실대학교 컴퓨터학과 졸업
2001년 ~ 2008년: 고려대학교 컴퓨터학과 (석사, 박사)
2002년 1월~2009년 6월: KISA(舊한국정보보호진흥원) 주임연구원
2009년 7월~2010년 7월: 한국은행 전자금융팀 과장
2010년 9월~2014년 7월: 한양사이버대학교 해킹보안학과 학과장
2014년 7월~현재: 금융보안원(舊금융보안연구원) 책임연구원
2012년~현재: 한국정보보호학회 이사
2008년~현재: TTA PG505 표준위원회 부의장
2008년~현재: ISO/IEC SC27 정보보호표준화전문위원
〈관심분야〉 바이오인식, 금융보안, 프라이버시



전 명 근 (Myung-Geun Chun) 종신회원
1987년 2월: 부산대학교 전자공학과 졸업
1989년 2월: KAIST 전기 및 전자공학과 석사
1993년 2월: KAIST 전기 및 전자공학과 박사
1993년~1996년: 삼성전자 자동화연구소 선임연구원
2000년~2001년: University of Alberta 방문교수
1996년~현재: 충북대학교 전자공학부 교수
2008년~현재: TTA PG505 표준위원회 의장
2007년~현재: ISO/IEC SC27 정보보호표준화전문위원
〈관심분야〉 바이오인식, 개인정보보호, 지능시스템