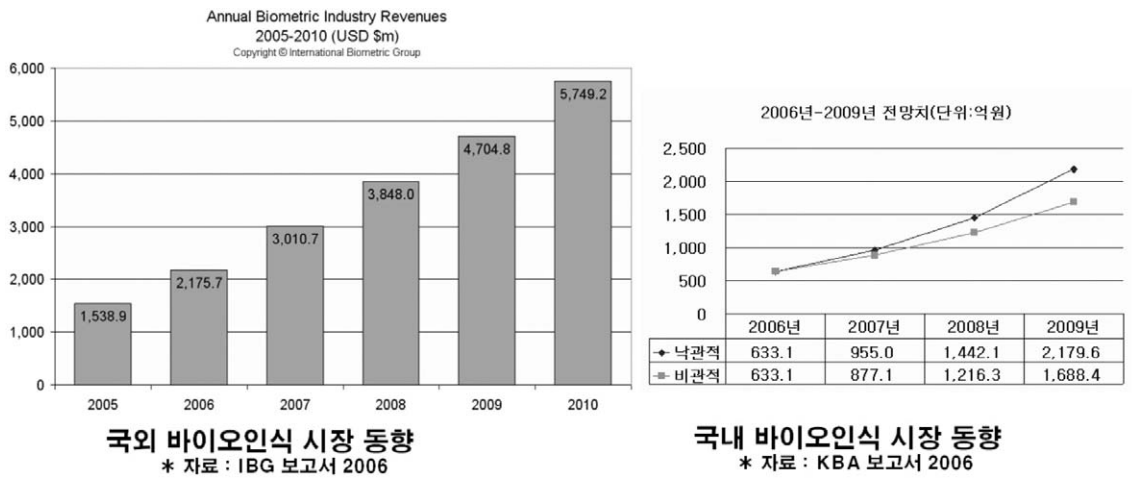
Telebiometrics 융합 기술 및 국제 표준화 동향

정 윤 수 | 한국전자통신연구원 바이오인식기술연구팀
길 연 희 | 한국전자통신연구원 바이오인식기술연구팀
배 영 래 | 충북과학대학 전자상거래과
문 기 영 | 한국전자통신연구원 바이오인식기술연구팀

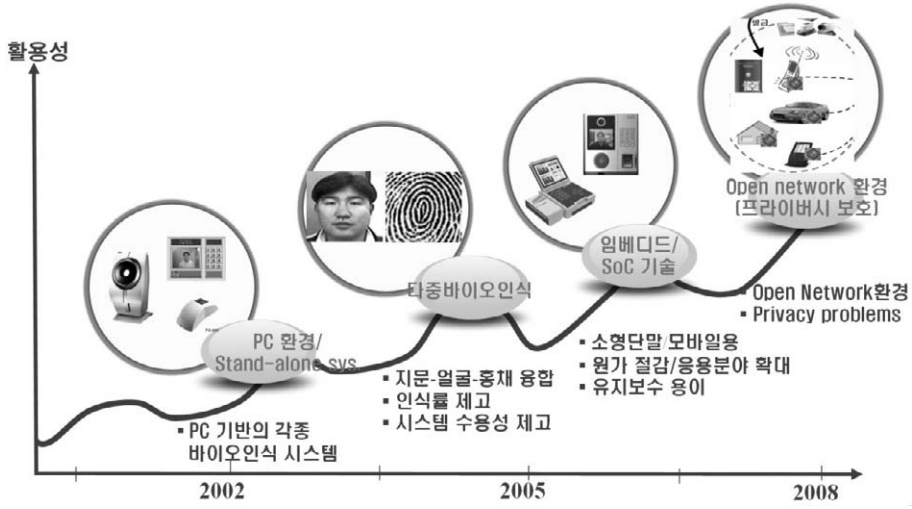
1. 서론

바이오 인식이란 개인의 신체적(physiological) 또는 행동적(behavioral) 특징을 기반으로 개인의 신원을 자동 인식하는 것으로 ATM(Automated Teller Machines), 휴대폰, 스마트카드, 데스크톱 PC, 워크스테이션 및 컴퓨터 망의 불법 사용이나 불법 접속을 방지할 수 있어 잊어버리기 쉬운 기존의 PIN(Personal Identification Number)이나 패스워드 등에 대안으로서 커다란 관심을 받아왔다[1].

현재 이러한 바이오인식 기술은 그 시장 규모가 나날이 성장하고 있으며(그림 1), 접근 제어 등 Stand-alone형 시스템에서 금융, 여권 등의 개방형 네트워크 기반 시스템으로 그 응용 분야가 발전하고 있다[2-3]. 이와 함께, 바이오 인식 기술의 발전 방향도 PC기반기술, 다중 바이오 인식 및 SoC(System on Chip)기술에서 Open network 환경을 고려하여 암호화 기술과 워



[그림 1] 국내/외 바이오인식 시장 동향



[그림 2] 바이오인식기술의 진화 방향

터마킹/DRM(Digital Rights Management) 기술 등과의 융합 기술로 기술적인 진화를 계속하고 있다(그림 2). 본 고에서는 이러한 개방형 네트워크 환경에서의 바이오 인식기술의 응용인, 종전 기술들과의 융합을 통해서 어떻게 진화하고 있는지 그 발전 방향과 관련 국제 표준화 동향을 소개하고자 한다.

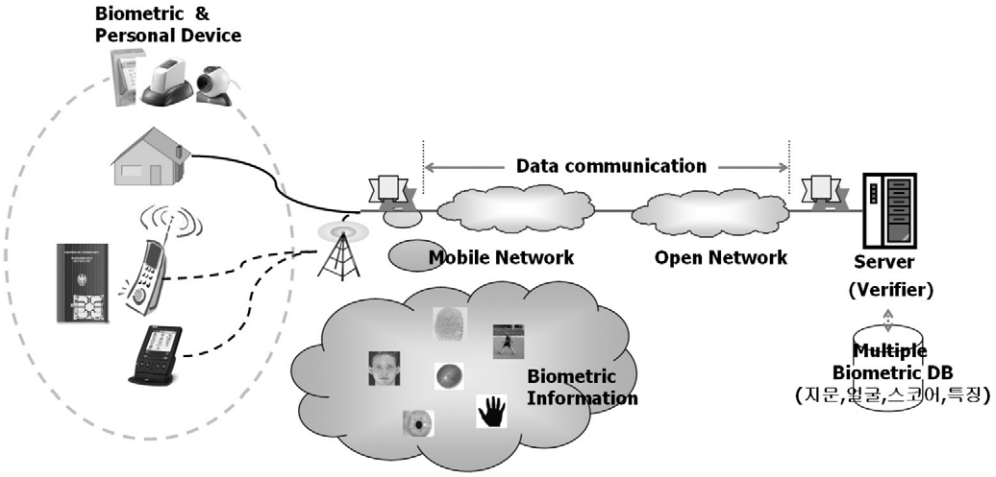
2. 텔레바이오인식 융합 기술

가. 텔레바이오인식의 정의 및 구성 환경

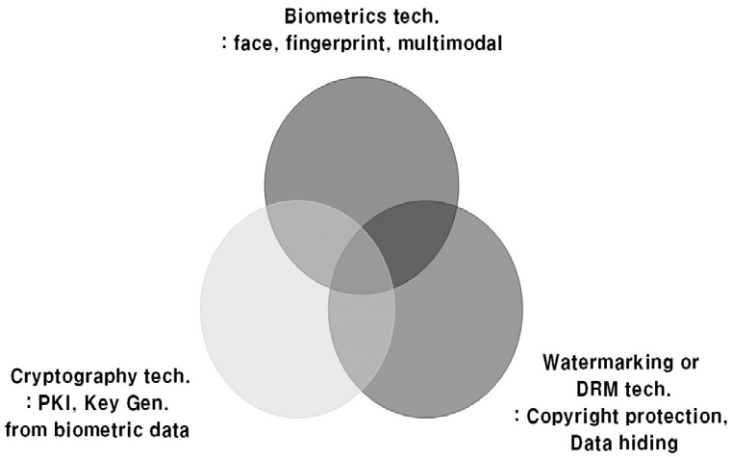
텔레바이오인식은 Tele(원거리 통신의)와 Biometrics(바이오인식)의 합성어로서 원거리 통신에 의한 또는 통신을 통한 바이오인식 기술로 정의할 수 있다. 일반적으로, 텔레바이오인식시스템은 지문, 얼굴, 홍채와 같은 바이오 정보를 획득하는 획득 단말, 바이오 정보의 전송을 위한 유/무선 네트워크, 기 저장된 바이오 템플릿과의 바이오 정보 획득 단말을 통하여 획득된 바이오 정보와의 인증을 수행하는 인증서버 및 바이오 정보 등 관련 정보를 저장하는 데이터베이스 등으로 구성된다(그림 3).

나. 텔레바이오인식의 주요 이슈 및 기술적 융합 방향

오픈 네트워크 환경에서 이러한 텔레바이오인식 시스템의 구축 시 고려해야 할 주요 이슈 사항들을 살펴보면 다음과 같다. 먼저, 온라인 인증을 위한 바이오 정보의 획득과정에서 위조 지문이나 위조 얼굴에 의한 인증 시도가 있을 수 있으며, 바이오 정보 획득 단말에서 주로 발생한다. 다음으로 인증 서버/DB등의 해킹을 통한 바이오 정보의 유출 및 유출된 바이오 정보의 재사용 시도가 가능하다. 마지막으로 바이오 정보의 유일성(불변성)으로부터 비롯된 사항으로서, 바이오 정보는 한번 유출되면 재생성이 용이치 않으며, 유출된 정보(얼굴)로부터 신원 추측이 용이한 단점이 있다. 이러한 텔레바이오인식기술의 취약점을 해결하기 위하여 기존의 암호화 기술에서부터, 바이오 정보의 위/변조 검출기술, 폐기형 바이오인식 기술 및 워터마킹 기술 등을 활용한 다양한 솔루션들이 제시되고 있으며, 얼굴인식, 지문인식, 다중바이오인식과 같은 기존의 바이오인식기술, PKI(Public Key Infrastructure) 및 디지털 키 생성 기법과 같은 암호 기술 및 저작권 보호 및 데이터 은닉 등을 위한 워터마킹이나 DRM(Digital Rights Management) 기술들과의 융합을 통해 앞서 언급된 기술적 취약점들을 해결해 나가고 있다[4].



[그림 3] 텔레바이오인식의 구성 환경



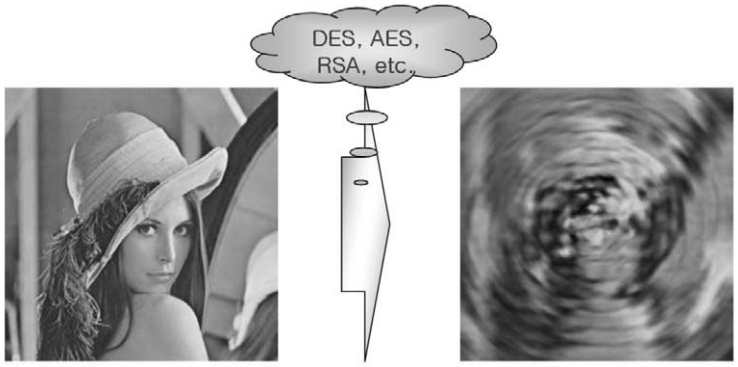
[그림 4] 텔레바이오인식의 기술적 융합 방향

다. 텔레바이오인식 융합 기술 및 활용 예

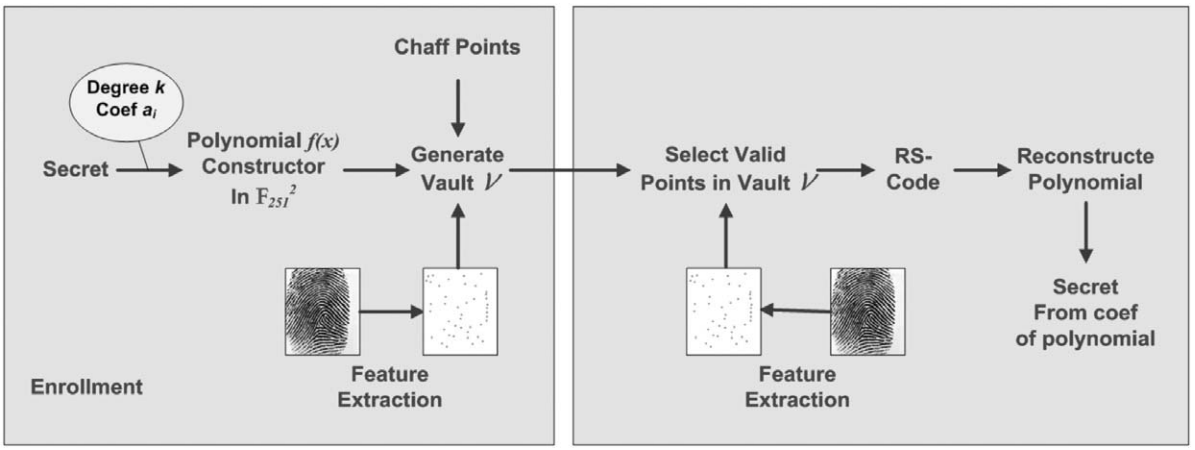
1) 바이오인식 + 암호 기술

바이오 인식 분야에 대한 암호 기술의 용이한 적용은 일반적인 데이터 보호 기법에서와 마찬가지로 DES (Data Encryption Standard), AES(Advanced Encryption Standard), RSA와 같은 기존 암호 방식[5]을 그대로 활용한 경우이다. [그림 5]에서 나타난 바와 같이, 이러한 방법의 주요한 목적은 얼굴 영상과 같은 바이오 정보를 제 3자가 쉽게 인지하지 못하게 하는 데 있으며, 일반적인 데이터 보호 방법을 바이오 영상 데이터에 단순히 적용한 것이라고 볼 수 있다.

[그림 6]은 바이오 인식 기술과 암호 기술이 좀 더 강하게 융합된 예를 나타낸다. 기존 암호 분야에서 많이 논의 되던 퍼지 볼트의 개념에 바이오 인식 개념이 접목된 일 예라고 볼 수 있다. 이러한 융합 기술은 개인의 비밀 정보를 가상의 금고인 볼트에 넣는 키로서 지문 템플릿을 이용하고, 또 한 볼트로부터 비밀정보를 꺼내기 위



[그림 5] DES등 적용 예



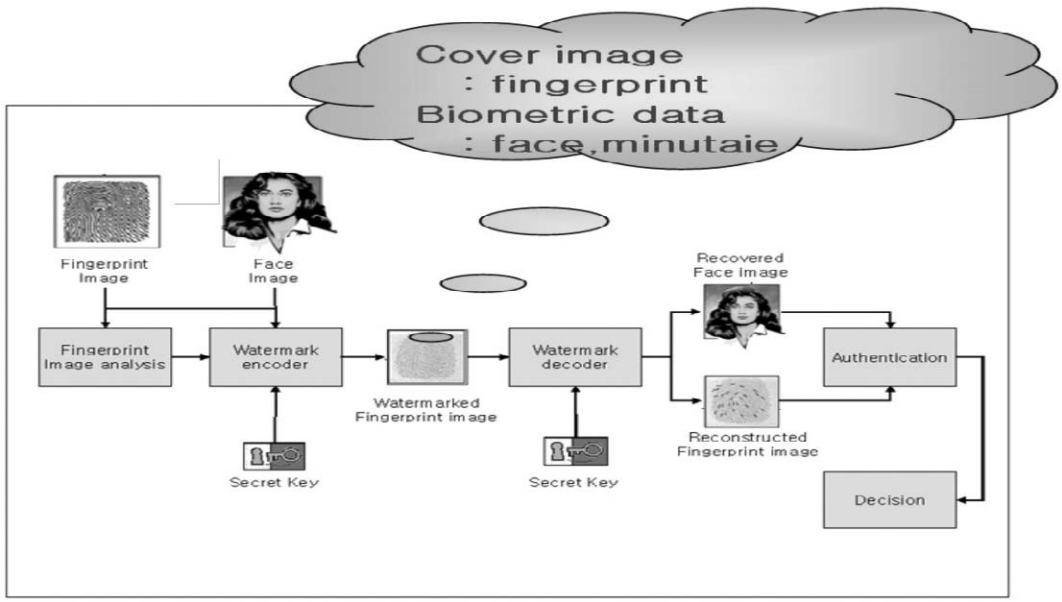
[그림 6] 퍼지볼트에 지문 템플릿을 활용한 예

해서 지문 템플릿을 이용하는 것이 주요한 특징이라고 할 수 있다[6]. 이와 함께, 얼굴, 홍채 등의 바이오 정보에 대해서도 관련 연구가 폭 넓게 진행되고 있다. 한편으로, 암호기술에서 많이 사용되는 해쉬 함수 또는 해쉬 개념을 바이오 인식 분야에 접목하는 노력들도 많이 진행되고 있으며, '바이오 해쉬' 기술이나 폐기형 바이오 인식(Cancelable Biometrics) 기술의 형태로 관련 연구가 확산되고 있다.

2) 바이오인식 + 워터마킹/DRM

바이오인식과 워커마킹기술의 융합 예는 크게 2가지로 요약될 수 있다. 먼저, 저작권 보호를 위해 생성자나 생성일자 등의 관련 정보를 바이오 정보에 삽입하는 경우(그림 7)와 [그림 8]과 같이 사용자가 의도한 정보가 어떤 것인지 확인할 수 없도록 커버 이미지에 바이오 정보를 삽입하는 스케거나그러피 기술을 적용한 경우이다[7]. [그림 8]은 커버영상으로 지문 영상을 그리고 은닉대상인 데이터로 얼굴 영상과 지문 특징을 은닉하는 예를 나타낸다. 하지만, 커버 영상에 바이오 정보를 은닉하는 것은 디코딩 과정에서 정보의 손실을 피할 수 없는 문제가 발행하며, 디코딩된 바이오 정보에 의한 인식과정에서 인식률의 저하가 발생한다. 따라서, 인식률의 저하를 최소화할 수 있는 바이오인식/워터마킹 기술의 융합 방법에 대해 많은 연구가 필요한 부분이라고 할 수 있다.

[그림 7] Copyright protection의 예



[그림 8] Steganography 개념의 적용 예

3. 텔레바이오인식 국제 표준화 동향

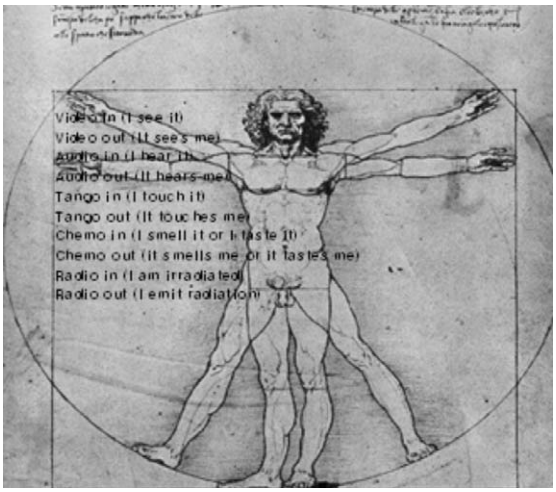
현재, 텔레바이오인식 국제 표준화는 ITU-T SG17/Q. 8에서 추진하고 있으며, 관련 표준화 추진 현황은 〈표 1〉과 같다. 〈표 1〉에 나타난 바와 같이 관련 표준화 추진을 위해 한국, 일본, 중국 등 아시아권의 나라들이 주도적인 역할을 하고 있음을 알 수 있다.

〈표 1〉을 참조하여 주요 표준화 내용을 살펴보면 다음과 같다. 먼저, TMMF(Telebiometrics Multimodal Model Framework)는 텔레바이오인식 멀티모달 모델을 정의하고, 안전한 인간과 시스템간의 상호작용을 다루며, X.physiol에서는 바이오인식 모달에 따른 상호작용들의 분류를 다룬다. TMMF에서는 [그림 9]와 같이 한사람 주위의 반경 1m인 구의 영역인 Biosphere 개념을 활용하여 Personal Privacy Sphere 개념을 소개하였다. 이때 Personal Privacy Sphere는 인간이

〈표 1〉 텔레바이오인식 국제 표준화 추진 현황

Recommendation	Title	Editor	Submission by
X.bip	BioAPI Interworking Protocol	프랑스	2Q. 2007
X.tmmf/X.physiol	Telebiometrics Multimodal Framework/Physiological quantitles and units in telebiometrics	스위스	3Q. 2007
X.tsm-1	General biometric authentication protocol and profile on telecommunication system	일본/한국	3Q. 2007
X.tsm-2	Profile of client verification model on Telebiometrics System Mechanism	일본/한국	2Q. 2008
X.tpp-1	A guideline of technical and managerial counte measures for biometric data security	한국	3Q. 2007
X.tpp-2	Protection procedures of multibiometric data	한국	2Q. 2008
X.tal	Telebiometrcis authentication infrastructure	중국	2Q. 2008
X.tdk	Telebiometrics digital key framework	한국	2Q. 2008

신체의 안전을 보장받고 사생활을 보호 받고자 하는 Bioshpere의 보안과 안전을 위한 방법을 나타낸다.



[그림 9] Bioshpere

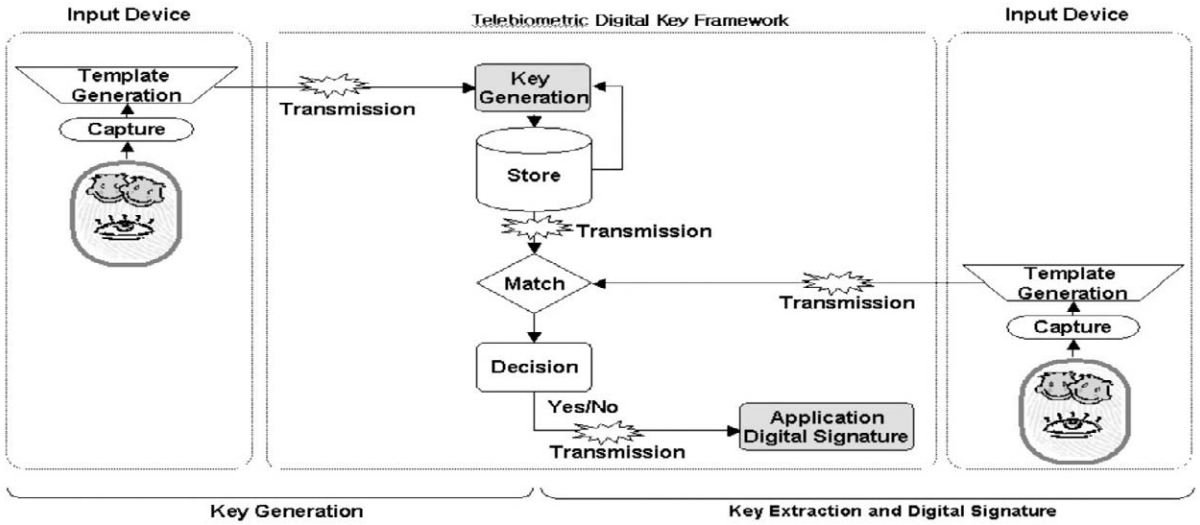
다 음 으 로 TSM(Telebiometrics System Mechanism)은 개방형 네트워크에서의 클라이언트와 응용 서버간에 사용자 인증을 위해 바이오 정보를 이용하는 시스템 메커니즘에 대한 정의를 목적으로 한다. 주요하게는 X.509(공개키 기반구조)환경에서 인증서버, 클라이언트 및 TTP(Trusted Third Party)간의 9개의 바이오 정보 인증 모델을 정의하고, PKI(Public Key Infrastructure)기반의 보안 메커니즘을 나타낸다.

TPP(Telebiometrics Protection Procedures)는 바이오 정보 관리 및 보호 절차에 목적을 두고, 바이오 정보의 생성, 전달, 관리, 폐기까지의 절차를 다룬다. TPP에서는 텔레바이오인식 시스템의 취약점 및 위협 요소를 정의하고 각 위협 요소별 대책에 대한 가이드라인을 제공한다. 본 표준 권고안에서는 앞서 언급한 융합 기술 중 암호화 기술 및 워터마킹 기술들을 활용한 다양한 보안 대책들을 제시하고 있는 점이 주요 특징이라고 할 수 있다.

〈표 2〉 텔레바이오인식 국제 표준화 추진

Store / Compare	Client	Server	TTP
Client	Local	Download	Reference Management on TTP for Client Comparison
Server	Attached	Center	Reference Management on TTP for Server Comparison
TTP	Comparison Outsourcing by Client	Comparison Outsourcing by Server	Strorage & Comparison Outsourcing

* TTP : Trusted Third Party, TLS : Transport Layer Security



[그림 10] Steganography 개념의 적용 예

마지막으로 TDK(Telebiometrics Digital Key)는 가장 늦게 시작한 과제로서, 텔레바이오인식 환경에서 바이오 정보로부터 디지털 키를 생성하는 기본 프레임워크를 정의하고 있으며, 암호화 기술의 한 분야인 퍼지 볼트 개념에 기반한 Key Binding 개념을 포함하고 있다.

4. 결론

본 고에서는 오픈 네트워크 환경에서 텔레바이오인식 기술이 어떤 종래 기술들과의 기술적 융합을 통해서 발전해가고 있는가와 그와 관련한 국제 표준화 동향에 대하여 살펴보았다. 텔레바이오인식기술 분야는 바이오 여권 등 공공분야의 바이오인식기반 신원인증 서비스 확대 및 금융거래/전자 상거래 분야에서의 안전한 서비스를 위해 필수적인 분야로서, 향후 바이오 인식 산업의 양적인 성장뿐만 아니라 관련 산업의 활성화에도 큰 기여를 할 수 있을 것으로 사료된다. 특히, 바이오 여권 등 공공 분야에서의 바이오 인식 기술 도입이 가시화되고 있는 시점임을 고려할 때 텔레바이오인식 분야에서의 다양한 기술뿐만 아니라 관련 국내 표준들에 대한 준비도 중요한 부분이라고 할 수 있다.

〈참고문헌〉

[1] 정윤수, “바이오인식기술의 현재”, IITA 주간기술동향, 2006. 09. 06

[2] 바이오 인식포럼, “바이오 인식포럼 2006년 보고서,” 2006. 12.

[3] 바이오 인식포럼, “국내 바이오 인식 산업현황 조사보고서,” 2006. 12.

[4] 정윤수, “텔레바이오인식 융합기술 및 국제 표준화 동향”, IT Forum 2007, TTA, 2007. 04. 19

[5] ETRI, “암호학의 기초”, 경문사

[6] 이형우, “X.tdk: Telebiometrics Digital Key Framework”, ITU-T SG17/Q. 8, 2007. 07

[7] Ingemar J.Cox, Matthew L.Miller and Jeffrey A. Bloom, “Digital Watermarking,” Morgan Kaufmann