情 報 保 護 學 會 誌
第 17 券 第 5 號, 2007. 10

개방형 네트워크 환경에서의 바이오 인식 융합 기술

정윤수*, 정성욱**, 문기영***

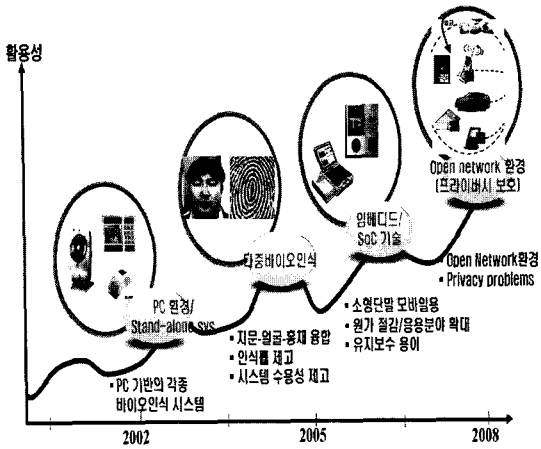
요 약

최근 인터넷에 의한 전자 상거래, 전자 정부 등 정보통신 인프라가 널리 보급되고, 이를 통한 서비스가 보편화됨에 따라 패스워드나 PIN을 대신할 수 있는 바이오인식 기술에 대한 관심이 증대되고 있다. 하지만, 개방형 네트워크 환경에서 바이오 인식 기술은 바이오 정보의 유출/오용등 기존 시스템에서와 다른 문제들을 내포하고 있다. 특히, 비밀 번호나 PIN과 같이 사용자가 임의로 변경할 수 없으므로 외부로 유출된다면 심각한 문제가 발생할 수 있다. 본 고에서는 개방형 네트워크 환경에서 바이오 인식 기술이 어떠한 종래 기술들과의 융합을 통해 발전해 가는지 살펴본다. 이를 위해, 스마트카드, 암호화 기술 및 DRM 기술 등 관련 기술과의 융합 예를 참조하여 발전 모델을 소개한다.

Ⅰ. 서 론

최근 인터넷에 의한 전자 상거래, 전자 정부 등 정보통신 인프라가 널리 보급되고 이를 통한 서비스가 보편화됨에 따라 정치, 경제, 문화 등 사회 전반의 활동이 사이버 공간으로 전환되어 가고 있다. 하지만, 사이버 활동의 비대면 특성을 이용하여 신원을 위장, 도용함으로써 온라인 활동의 안전성을 위협하는 상황이 빈번히 발생하고 있어, 이에 기존의 신원 확인 방법보다 더 안전하고 신뢰할 수 있는 사용자 인증 방법으로 개인의 신체적(physiological) 또는 행동적(behavioral) 특징을 이용하는 바이오 인식 기술이 폭 넓게 활용되기 시작하였다.

현재, 이러한 바이오인식 기술은 그 시장 규모가 나날이 성장하고 있으며, 접근 제어 등 Stand-lone형 시스템에서 금융, 여권 등의 개방형 네트워크 환경으로 그 응용 분야가 발전하고 있다[그림 1]. 하지만, 이러한 개방형 네트워크 환경에서는 기존의 Stand-alone형 시스템에서와 달리 바이오 정보의 유출 및 침해 등 다양한 문제들에 대한 근본적인 대책이 함께 요구되는 약점이 있다. 본고에서는 개방형 네트워크 환경에서 안전하고 신뢰성 있는 바이오인식 시스템의 구축을 위해 바이오 인식 기술이 어떤 기술들과의 융합을 통하여 자기 발전을



〔그림 1〕 바이오인식 기술의 진화 방향

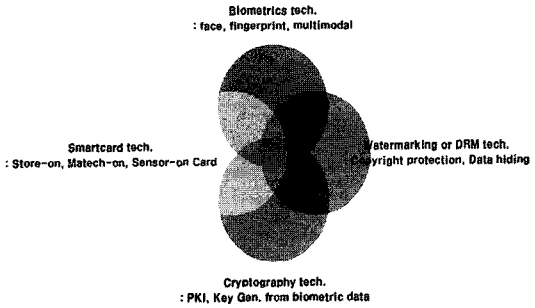
* 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀(yoonsu@etri.re.kr)
** 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀(brcastle@etri.re.kr)
*** 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀(kymoon@etri.re.kr)

가속화하고 있는지 살펴보고자 한다.

Ⅱ. 바이오인식 융합 기술의 발전 모델

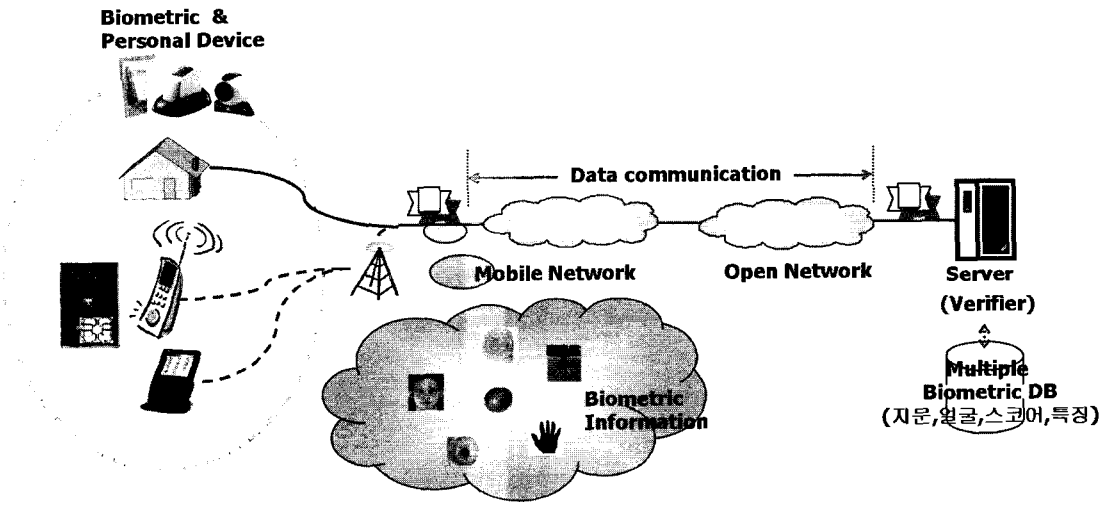
개방형 네트워크 환경에서 바이오인식 시스템 즉, 텔레바이오인식 시스템은 지문, 얼굴, 홍채와 같은 바이오 정보를 획득하는 획득 단말, 바이오 정보의 전송을 위한 유/무선 네트워크, 기 저장된 바이오 템플릿과의 바이오 정보 획득 단말을 통하여 획득된 바이오 정보와의 인증을 수행하는 인증 서버 및 바이오 정보 등 관련 정보를 저장하는 데이터베이스 등으로 구성된다[그림 2].

이러한 텔레바이오인식 시스템의 구축 시 고려



〔그림 3〕 바이오인식 기술과 타기술의 융합 관계

기술의 취약점을 해결하기 위하여 스마트카드 기술, 암호화 기술 및 워터마킹/DRM 기술 등을 활용한 다양한 솔루션들이 제시되고 있다[그림 3].



〔그림 2〕 텔레바이오인식의 구성 환경

해야 할 주요 이슈 사항들을 살펴보면 다음과 같다. 먼저, 온라인 인증을 위한 바이오 정보의 획득 과정에서 위조 지문이나 위조 얼굴에 의한 인증 시도가 있을 수 있으며, 바이오 정보 획득 단말에서 주로 발생한다. 다음으로, 인증 서버/DB 등의 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 텔레바이오인식

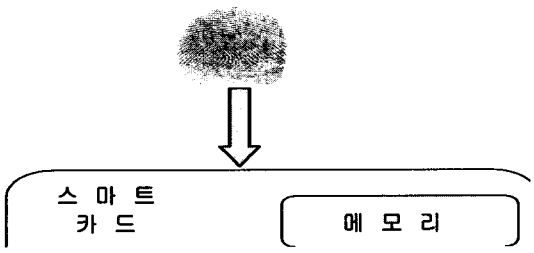
2.1. 바이오인식 기술 + 스마트카드

사용자 인증을 위해 저장된 바이오인식 정보가 타인에게 도용된다면 패스워드나 PIN과 같이 변경이 불가능하므로 심각한 문제를 발생할 수 있다. 이러한 문제에 대처하기 위한 한 방법으로, 바이오인식 정보를 중앙 데이터베이스에 저장하지 않고 스마트카드 등에 저장하고 인식하는 방법들이 활용 될 수 있다.

스마트카드에 바이오인식 정보를 저장하는 경우, 저장/인증을 수행하는 경우 및 취득/저장/인증

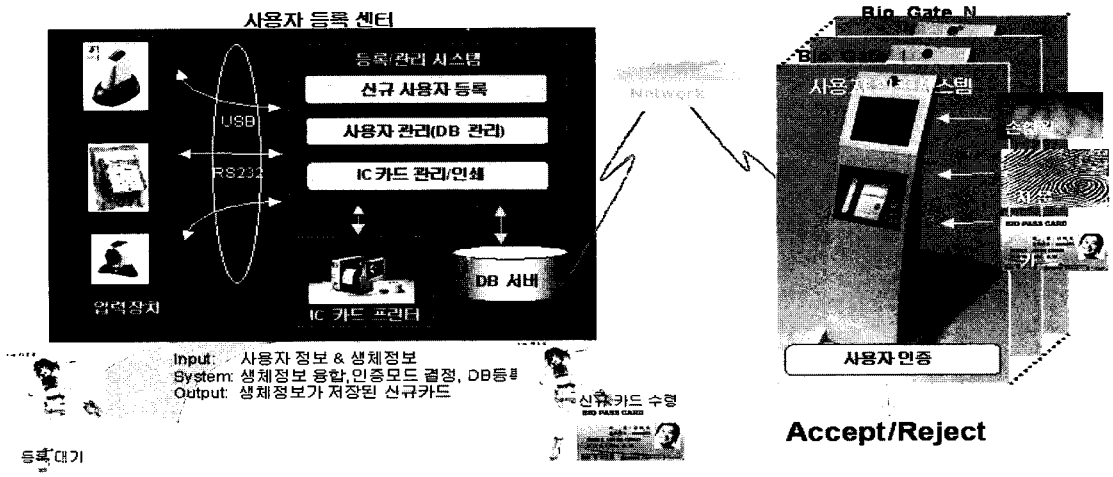
을 수행하는 경우에 따라 Store-on-Card, Match-on-Card 및 Sensor-on-Card로 나눌 수 있다. Store-on-Card 방식은 지문과 같은 바이오인식 정보를 중앙 집중식 DB에 저장하지 않고 스마트카드 내의 메모리에 저장한 후 인증을 요청할 시에 저장된 바이오인식 정보를 단말에 보내어 단말기에서 인증을 하는 시스템이고, Match- on-Card는 저장된 바이오인식 정보와 인증을 요청할 시에 취득한 바이오인식 정보를 스마트카드에서 인증 알고리즘을 계산하여 스마트카드에서 인증 결과만을 단말기로 보내는 것이다. 그리고 위의 두 종류의 카드에서 바이오인식 정보 획득은 단말기에서 이루어지는 반면, Sensor-on-Card는 바이오인식 정보 획득이 스마트카드에서 이루어진다는 것이다. 예로 지문 획득 반도체 센서가 단말기에 있지 않고 스마트카드에 있다는 것이다.

[그림 4]는 Match-on-Card에 지문 입력 센서를 장착하여 등록과 인증 과정 모두를 스마트카드에서 수행하는 것이다. 이러한 Sensor-on-Card는 Store- on-Card나 Match-on-Card에 비하여 바이오인식 정보가 타인에 의해 훼손 되거나 도용되는 문제가 전혀 없고, 스마트카드기반 바이오인식 시스템 중 가장 높은 보안성을 제공한다.



〔그림 4〕 Sensor-On-Card

[그림 5]는 지문과 손 혈관을 이용한 Store-on-Card 시스템의 예를 나타낸다. [그림 5]와 같이 사용자 등록 센터가 인증 시스템과 독립적으로 운영되며, 신규 사용자 등록, 사용자 데이터베이스 관리 및 스마트카드 관리 기능을 담당한다. 데이터베이스 서버에는 등록된 사용자의 개인정보가 저장되는 것으로 동일인의 중복 등록을 방지하고 인증 시 인가된 사용자의 정보 요구에 대응하기 위한 것이다. 유출 시 심각한 문제가 야기될 수 있는 개인의 바이오인식 정보는 중앙 DB에서 관리하지 않고 개인에게 지급되는 스마트카드에 저장된다. 본 시스템은 지문과 손 혈관 인증을 사용하되 사용자에 적응적으로 두 단일 인증 모드를 동시에 사용하거나 하나만 사용할 수 있는 기능을 갖는다. 즉, 지문을 사용할 수 없는 사용자의 경우에는 손 혈관만으로도 인증을 수행하도록 하여 지문인증이 불가능한 사용자라 하더라도 시스템을 활용할 수 있도록 하였다. 그리고 바이오인식 정보를 중

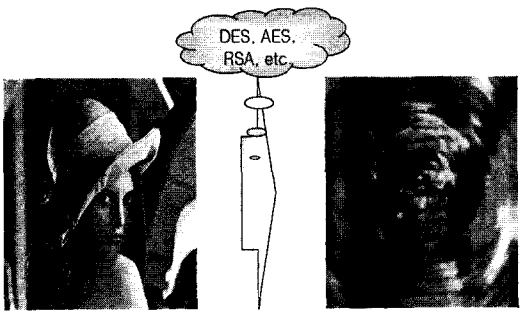


〔그림 5〕 스마트카드 사용 예

앙 데이터베이스가 아닌 스마트카드에 저장하여 바이오인식 정보가 타인에 의해 오용될 소지를 줄였다. [그림 5]에 나타난 바와 같이 사용자 등록 센터는 제어 시스템에 지문과 손 혈관을 입력하기 위한 화상 카메라 및 카드 발급을 위한 카드 프린터, 데이터베이스 서버가 연결되어 구성되고, 인증 시스템은 키오스크 타입으로 지문 및 손 혈관 입력장치와 카드 리더기로 구성된다.

2.2. 바이오인식 기술 + 암호 기술

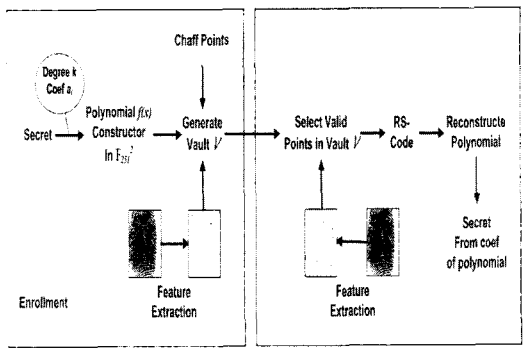
바이오 인식 분야에 대한 암호 기술의 적용은 일반적인 데이터 보호 기법에서와 마찬가지로 DES(Data Encryption Standard), AES(Advanced Encryption Standard), RSA와 같은 기존 암호 방식[5]을 그대로 활용한 경우이다.



〔그림 6〕 DES등 적용 예

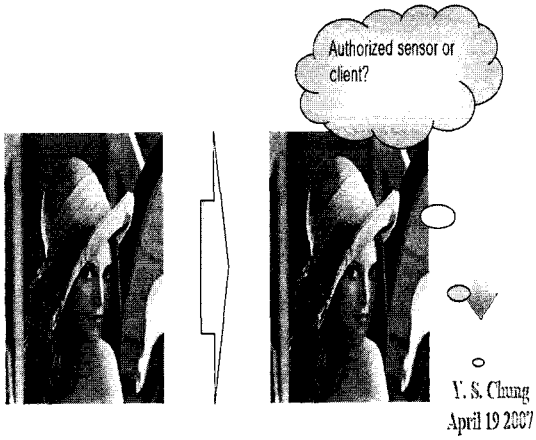
[그림 6]에서 나타난 바와 같이, 이러한 방법의 주요한 목적은 얼굴 영상과 같은 바이오 정보를 제 3자가 쉽게 인지하지 못하게 하는데 있으며, 일반적인 데이터 보호 방법을 바이오 영상 데이터에 단순히 적용한 것이라고 볼 수 있다.

[그림 7]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 일예라고 볼 수 있다. 이러한 융합 기술은 개인의 비밀 정보를 가상의 금고인 볼트에 넣는 키로서 지문 템플릿을 이용하고, 또한 볼트로부터 비밀정보를 꺼내기 위해서 지문 템플릿을 이용하는 것이 주요한 특징이라고 할 수 있다[6].



〔그림 7〕 퍼지볼트에 지문 템플릿을 활용한 예

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 노력들



〔그림 8〕 Copyright protection의 예

도 많이 진행되고 있으며, '바이오 해쉬' 기술이나 폐기형 바이오인식(Cancelable Biometrics) 기술의 형태로 관련 연구가 확산되고 있다.

2.3. 바이오인식 기술 + 워터마킹/DRM

바이오인식과 워터마킹기술의 융합 예는 크게 2가지로 요약될 수 있다.

먼저, 저작권 보호를 위해 생성자나 생성일자 등의 관련 정보를 바이오 정보에 삽입하여 저작권을 보호하는 경우이다. [그림 8]은 바이오 영상에 소유자 정보 및 생성 날짜를 삽입하여 바이오 영상

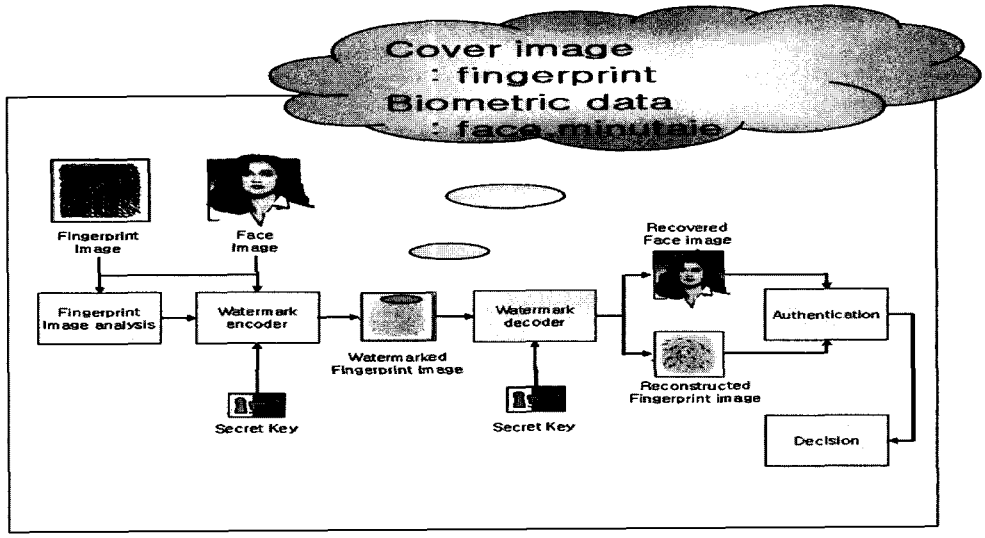
처리부나 특징 추출 단에서 인증된 영상인지를 판단할 수 있게 하는 한 예를 나타낸다.

다음으로, [그림 9]는 사용자가 의도한 정보가 어떤 것인지 확인할 수 없도록 커버 영상에 바이오 정보를 삽입하는 스테거나그러피 기술을 적용한 경우이다[7].

[그림 9]에서는 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 있는 바이오인식/워터마킹 기술의 융합 방법에 대해 많은 연구가 필요한 부분이라고 할 수 있다.

Ⅲ. 결 론

본고에서는 개방형 네트워크 환경에서 바이오인식기술이 어떤 종래 기술들과의 기술적 융합을 통해서 발전해가고 있는지에 대하여 살펴보았다. 특히, 바이오인식기술 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, 스마트카드, 암호화 기술 및 DRM 기술 등과의 융합이 점차 가속화 될 것으로 예상된다.



[그림 9] Steganography 개념의 적용 예

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

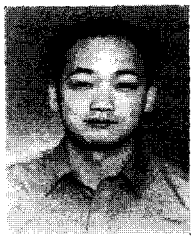
[7] Ingemar J.Cox, Matthew L.Miller and Jeffrey A. Bloom, "Digital Watermar-king," Morgan Kaufmann

[8] "The Biometric Consortium," http:// www.biometrics.org/.

[9] J. Adams, "Survey: Biometrics and smart cards," BTT, pp.8-11, Aug. 2000.

[10] 길연희, 정윤수, 안도성, 이경희, 반성범, "다중 생체인식 기술 동향," 전자통신동향분석, 2005.

〈著者紹介〉



정 윤 수 (Yun Su Chung)
정회원
1993년 2월 : 경북대학교 전자공학과 졸업
1995년 2월 : 경북대학교 전자공학과 석사
1998년 8월 : 경북대학교 전자공학과 박사
1999년 ~ 현재 : 한국전자통신연구원 바이오인식기술연구팀, 선임연구원
관심분야 : 바이오인식, 정보보호, 영상처리

정 성 욱 (Sung Uk Jung)
비회원
2003년 2월 : 고려대학교 전기전자전파공학부 졸업
2005년 2월 : 한국과학기술원 전기및 전자공학 석사
2005년 ~ 현재 : 한국전자통신연구원 바이오인식기술연구팀, 연구원
관심분야 : 바이오인식, 정보보호, 영상처리

문 기 영 (Ki Young Moon)
종신회원
1986년 2월 : 경북대학교 전자공학과 학사
1989년 2월 : 경북대학교 전산학 석사
2006년 2월 : 충남대학교 전산학 박사
1994년 ~ 현재 : 한국전자통신연구원 바이오인식기술연구팀, 팀장
관심분야 : 바이오인식, 정보보호, 웹서비스보안