情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

스마트카드와 바이오메트릭스

반 성 범*, 안 도 성**, 정 윤 수***

요 약

다양한 온라인 서비스의 보급으로 인해 안정적인 보안수준을 제공하면서 사용이 편리한 사용자 인증 시스템의 필요성이 대두되었다. 사용자 인증 수단으로 많이 사용되던 개인장치나 비밀번호 등은 분실 가능성 및 도용의 위험이 있어 보안이 중요한 환경에서는 사용상의 제약이 따른다. 그러므로 바이오메트릭 정보를 이용한 사용자 인증에 대한 관심이 꾸준히 증가하고 이에 따라 바이오메트릭스 기술의 발전으로 적용이 되고 있으나, 바이오메트릭 정보는 비밀번호와 같이 사용자가 임의로 변경할 수 없으므로 외부로 유출된다면 심각한 문제가 발생할 수 있다는 문제가 있다. 그러므로 본 고에서는 이러한 문제를 해결할 수 있는 바이오메트릭 정보의 취득, 저장 및 인증을 스마트카드에서 처리하는 기술에 대하여 설명하고 이의 활용 현황에 대하여 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. 그러나 사이버 활동의 비대면 특성을 이용하여 신원을 위장, 도용함으로써 온라인 활동의 안전성을 위협하는 상황이 빈번히 발생하고 있다. 이에 기존의 신원 확인 방법보다 더 안전하고 신뢰할 수 있는 사용자 인증 방법으로 신체의 고유 특성을 이용한 바이오메트릭스 기술이 활용되기 시작하였다.

패스워드 또는 PIN 입력 방식에 의한 사용자 인증 방법에 비해 바이오메트릭 정보를 이용한 기술의 주요 장점은 바이오메트릭 정보는 개인별로 고유한 것으로 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 분실할 수 없다는 것에 있다. 그러나 사용자 인증을 위해 저장된 바이오메트릭 정보가 타인에게 도용된다면 패스워드나 PIN과 같이 변경이 불가능하므로 심각한 문제를 발생할 수 있다. 그러므로 바이오메트릭 정보를 획득하고 가공하여 인식하는 방법에 관한 연구뿐만 아니라 최근에는 바이오메트릭 정보를 중앙 데이터베이스에 저장하지 않고 스마트카드 등에 저장하고 인식 관련 연산을 수행하여 이러한 문제를 해결할 수 있는 연구도 활발히 진행되고 있다.

또한, 2001년 미국 테러사건이후 기존의 개인 신원 확인 수단보다 강력한 바이오메트릭스 기술과 스마트카드를 이용한 신원확인 시스템에 대한 개발과 활용이 진행되고 있다. 즉, 기존의 신분증이 스마트카드로 발전하면서 얼굴, 지문, 홍채 등의 바이오메트릭 정보가 스마트카드에 저장되고 이를 통한 신원확인 시스템 도입이 진행되고 있다.

본 고에서는 스마트카드와 바이오메트릭스 기술의 융합에 대하여 설명하고 이의 활용 예에 대하여 설명한다. II장에서는 스마트카드에 바이오메트릭 정보를 저장하는 경우, 저장/인증을 수행하는 경우 및 취득/저장/인증을 수행하는 경우에 대하여 설명한다. III장에서는 이의 활용 현황에 대하여 살펴본 후 IV장에서 결론을 맺는다.

Ⅱ. 스마트카드 기반 바이오메트릭스 기술

스마트카드에 바이오메트릭 정보를 저장하는 경우,

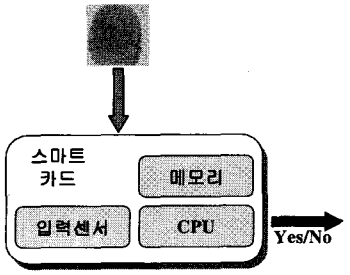
* 조선대학교 정보제어계측공학과(sbpan@chosun.ac.kr)
** 한국전자통신연구원 정보보호기반그룹 생체인식기술연구팀(dosung@etri.re.kr)
*** 한국전자통신연구원 정보보호기반그룹 생체인식칩셋연구팀(yoonsu@etri.re.kr)

저장/인증을 수행하는 경우 및 취득/저장/인증을 수행하는 경우에 따라 Store-on-Card, Match-on-Card 및 Sensor-on-Card로 나눌 수 있다.

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

Store-on-Card는 스마트카드에 연산 능력을 갖는 프로세서 등은 내장하지 않고 단순히 바이오메트릭 정보를 저장하는 메모리만을 가지고 있다. 사용자 바이오메트릭 정보를 중앙 집중식 DB에 저장하는 방식을 택할 경우, 중앙 DB를 유지하고 관리하는데 어려움이 있고 해킹의 위험, 프라이버시의 침해 등의 문제가 발생할 수 있다. 그러므로 개인의 바이오메트릭 정보를 스마트카드에 저장하여 각 개인이 보유하게 함으로써 앞에서 언급한 문제 등을 해결할 수 있고, 인증 절차가 스마트카드내의 바이오메트릭 정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다. 최근 스마트카드 기반 바이오메트릭스 시스템은 Store-on-Card 방식이다.

그러나 이 경우 스마트카드는 바이오메트릭 정보를 저장한 단순 메모리 기능만 제공할 뿐 사용자 인증 기능을 수행하지 않아 보안성에 문제가 있다. 즉, 입력



〔그림 1〕 Sensor-on-Card

된 바이오메트릭 정보에 대한 인식 처리가 단말기내의 프로세서에서 수행되기 위하여 그 바이오메트릭 정보가 단말기로 전송될 때, 정보 누출의 위험성이 있다. 따라서 개인 정보 누출의 위험을 최소화하여 고도 보안 응용에 적용하기 위해서는 개인의 바이오메트릭 정보를 스마트카드 내에 저장할 뿐만 아니라 스마트카드 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 초기 발급 시 저장된 개인의 정보가 사용단계에서 스마트카드 외부로 유출되지 않도록 하여야 한다.

Store-on-Card와 Match-on-Card는 바이오메트릭 정보를 바이오메트릭 정보 입력기로부터 전달받아 스마트카드에 저장하여 처리하지만, Sensor-on-Card는 바이오메트릭 정보를 입력받는 장치도 스마트카드에 내장되어 있는 것을 의미한다. 예로 그림 1과 같이 지문 인증 시스템인 경우에Match-on-Card에 지문 입력 센서를 장착하여 등록과 인증 과정 모두를 스마트카드에서 수행하는 것이다. Sensor-on-Card는 Store-on-Card나 Match-on-Card에 비하여 바이오메트릭 정보가 타인에 의해 훼손 되거나 도용되는 문제가 전혀 없고 표 1과 같이 스마트카드기반 바이오메트릭스 시스템 중 가장 높은 보안성을 제공한다.

〔표 1〕 보안 취약성 비교

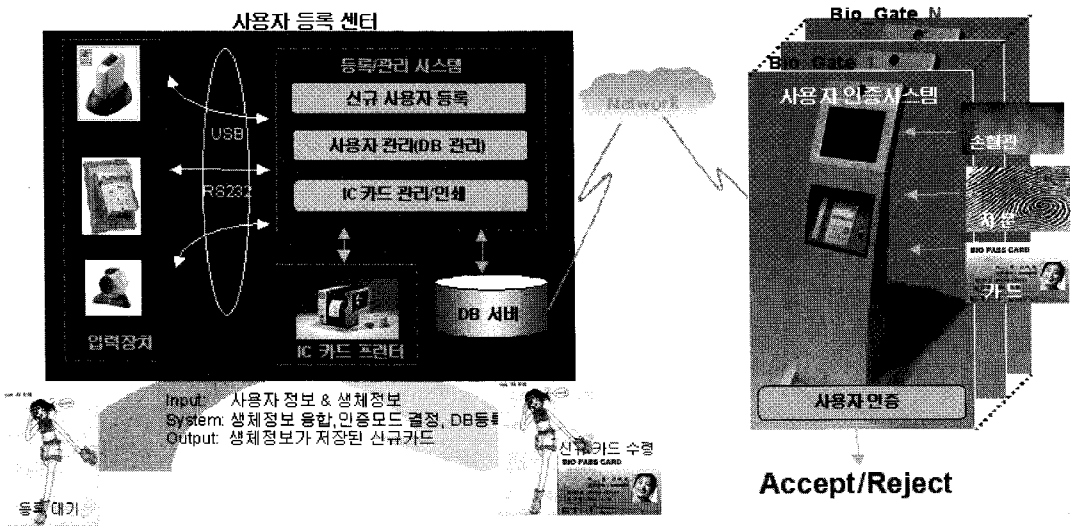
	보안 위협	영향	등급
Store-on-Card	- 카드 → 카드단말기: 저장템플릿 . 가로채기 . 조작/대체	도난/분실 카드 사용 (높음)	C
	- 카드단말기 → 카드: 인증결과 . 수정	도난/분실 카드 사용 (매우 높음)	
Match-on-Card	- 카드 -〉 카드단말기: 없음	없음	A-
	- 카드단말기 -〉 카드: 입력지문특징 . 가로채기 . 조작/대체	도난/분실 카드 사용 (중간)	
Sensor-on-Card	- 없음	없음	A+

Ⅲ. 스마트카드 기반 바이오메트릭스 기술 활용

그림 2는 멀티모달 바이오메트릭스 시스템의 예로 지문과 손 혈관을 이용한 Store-on-Card 시스템이다. 그림 2와 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 바이오메트릭 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 바이오메트릭 정보를 중앙 데이터베이스가 아닌 스마트카드에 저장하여 바이오메트릭 정보가 타인에 의해 오용될 소지를 줄였다. 그림 2에 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.

전 세계적으로 주민등록증과 같은 National Identification Document 사업의 전 단계로써 테러 위협 등의 안보 목적과 연계하여 여권, 비자 등이 우선적으로 검토되고 있으며 표 2와 같이 스마트카드 기반 바이오메트릭스 기술을 적용한 프로젝트가 진행 중에 있다. 특히, 미국은 테러사태 이후 출입국관리의 보안성을 향상시키기 위해 바이오메트릭스 기술 적용을 위한 법제화를 신속히 진행하였으며, 각 국의 참여를 위해 국제 표준을 제정하기 위해 노력중이다. 우리나라는 위 국제동향과 독립적으로, 현재 출입국관리 시스템이 텍스트 기반임에 따른 문제 해결을 위해 2007년부터 바이오메트릭 정보 기반으로 변경하기 위한 준비를 하고 있다.

미국은 2004년 10월 26일 이후 Enhanced Border Security and Visa Reform Act 제303조에 따라 27개 비자면제대상국 국민은 국제민간항공기구(ICAO)가 권고하는 바이오메트릭 정보를 포함한 여권을 소지하여야 하고, 비자 발급대상국가의 국민은 비자 신청 시 미국 대사관에 생체정보를 제공하여야 한다. Enhanced Border Security and Visa Reform Act의 경과조치로 US-VISIT 프로그램에 따라 2004년 1월 5일부터 공항입국 시 사증 발급대상 국가의 14세 이상 국민에 대하여 지문과 얼굴 영상을 채취 중이며, 브라질은 이에 대응하여 미국 국민에 대하여 지문을 채취하고 있으며 중국도 미국인의 입국과 비자 발급을 강



〔그림 2〕 스마트카드 기반 멀티모달 바이오메트릭스 시스템

〔표 2〕 국가별 스마트카드 기반 바이오메트릭스 기술 적용 프로젝트

국가	기관명	모드	사업목적
독일	연방범죄수사국 연방정보보호국	얼굴	- Travel documents의 사진과 얼굴 비교에 의한 신분확인 기술의 평가 - 2003.4-6 - 평가규모: 250여명
캐나다	여권국	얼굴	- 생체여권에 대비한 얼굴인식 기술 평가 - 평가규모: 5,764 Probes + 143.000 Gallery
	국경관리국 NIST	홍채	- 미국·캐나다 국경 빈번 출입자에 대한 신속한 서비스를 위해 홍채인식기술 적용(2003년 7월부터 설치 활용 중)
미국	기술표준국	지문	- US-VISIT으로 획득한 지문DB를 기반으로 지문인식 알고리즘의 비교 평가 - 알고리즘 테스트베드 구현
	교통안전관리국	다중	- TSA 지원으로 Knoxville에 비영리 컨소시엄을 설비하고, 생체인식 제품의 Operational 평가를 시행중
	국가안전부	지문/얼굴	- 육로로 출입하는 외국인들의 신분 확인을 위해 SENTRI 프로그램에 생체인식 적용
싱가포르	내무부	지문/얼굴	- 스마트카드와 지문인식을 결합한 IACS 시행중 - 얼굴인식도 결합하여 생체여권과의 연동 계획 중
호주	국방과학기술원	얼굴	- 여권의 사진과 어굴 비교에 의한 신분확인 기술 구현 및 시행 (Smartgate)
영국	경찰정보기술원	지문/얼굴/장문	- 범죄수사를 위한 다중생체 DB 구축 및 평가 시스템 계획중 - 2005년 6월 얼굴DB 구축 완료 - 기존 범죄수사용 시스템과의 연동 계획
남아프리카공화국	정부기관	지문	- 내무부의 AFIS 시스템(2002년 2월 완료) - 지문과 IC카드를 결합한 복지급여 지급 - 운전면허증에 2개의 지문 사용
말레이시아	여권관리국	지문/얼굴	- 지문과 얼굴을 저장한 chip을 내장한 여권 사용중(1998년) - 국제민간항공기구(International Civil Aviation Organization: ICAO) 표준에 따르는 e-Passport 구현 중

화하는 계획을 발표하였다.

일본은 2003년 7월, 외무성은 미국의 동향에 대응하기 위해, 2004년 정기국회에 여권법 개정안을 제출하였으며, 2005년도 도입을 목표로 하고 있다. 스마트카드에 기록될 데이터로는 얼굴윤곽과 미간 간격 등의 특징량 등이 검토되고 있으며, 여권법 개정안에서 구체적인 데이터 종류가 제시될 방침이다. EU는 미국 동향에 대한 대응책으로서, EU 가맹국이 발행하고 있는 여권에 비접촉 스마트카드 칩을 도입하기로 하였다. EU는 얼굴 정보뿐만 아니라, 지문과 홍채 정보를 스마트카드 칩에 내장시키는 것도 검토 중이다. 영국 정부는 영국 비자 신청자에게 바이오메트릭 정보의 제공을 의무화할 방침을 세우고 있다. 이 프로그램은 현재 스리랑카에서 시험 실시 중인 것을 다른 국가로 확대시킨 것이다. 이미 EU는 망명·난민 신청자 전원의 지문을 채취하여 데이터베이스와 대조하는 시스템을 가동 중에 있다. 또한 영국에서 발행되는 여권에도, 미국의 움직임과 발맞추어 바이오메트릭스 기술을 도입할 방침이다.

국내에서는 고급 두뇌 유입을 통하여 '사람이 모이는 동북아 관문'의 실현을 목표로 한 입국문호확대 및 선량한 외국인에 대한 최상의 행정 서비스를 제공하기 위해 바이오메트릭스 기술 도입을 추진하고 있는 법무부외에 많은 정부부처에서 스마트카드 기반 바이오메트릭스 기술 도입을 검토하고 있다.

Ⅳ. 결 론

사용자 인증의 중요정보로 사용되는 개별 인간의 바이오메트릭 정보가 중앙 데이터베이스에서 관리된다면 'big brother' 문제가 발생할 수 있으므로, 본 고에서는 이의 문제를 해결할 수 있는 스마트카드 기반 바이오메트릭스 기술 및 활용 예에 대하여 설명하였다. 향후 스마트카드 기반 바이오메트릭스 기술의 활용이 시작될 것이며, 최근 논의가 되고 있는 바이오메트릭 정보의 보호에 대한 연구가 성공적으로 진행되면 바이오메트릭스 산업이 활성화 될 것으로 예상한다.

참 고 문 헌

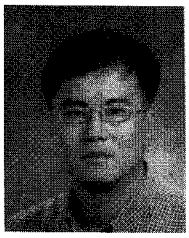
[1] A. Jain, R. Bolle, and S. Pankanti, *Biometrics-Personal Identification in Networked Society*, kluwer Academic Publishers, 1999.

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

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

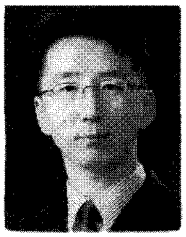
[4] 길연희, 정윤수, 안도성, 이경희, 반성범, "다중 생체인식 기술 동향," 전자통신동향분석, 2005.

〈著 者 紹 介〉



반 성 범 (Sung Bum Pan)
정회원

1991년 2월 : 서강대학교 전자공학과 졸업
1995년 2월 : 서강대학교 전자공학과 석사
1999년 2월 : 서강대학교 전자공학과 박사
1999년 2월~2005년 2월 : 한국전자통신연구원 생체인식기술연구팀 팀장
2005년 3월~현재 : 조선대학교 정보제어계측공학과 전임강사
〈관심분야〉 생체인식, 정보보호, 영상처리



안 도 성 (Dosung Ahn)
정회원

1992년 2월 : 인하대학교 자동화공학과 졸업
1994년 2월 : 인하대학교 기계공학과 석사
2001년 2월 : 인하대학교 자동화공학과 박사
2001년 11월~2005년 10월 : 한국전자통신연구원 생체인식기술연구팀, 선임연구원
〈관심분야〉 지문인식, 생체인식, 정보보호

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 생체인식칩셋연구팀, 선임연구원
〈관심분야〉 생체인식, 정보보호, 영상처리