IC 카드를 이용한 생체인식 기술 개발 동향

한국전자통신연구원 반성범* · 정용화* · 김호원 · 박영수

1. 서 론

21세기 정보의 시대는 인터넷 보급 등으로 인하여 원하는 정보를 수집, 분석, 가공 등이 편리하게 되었다. 그러나 인터넷을 이용하여 글로벌 네트워크가 형성되어 편리하게 수집, 분석 및 가공한 개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 심각한 문제가 제기되고 있으며 개인의 정보만이 손실되는 것이 아니라 국가의 중요 정보와 전자상거래 등의 경제 활동에 필요한 정보도 손실되는 현상이 발생되고 있는 현실이다. 그러므로 현재까지 사용되고 있는 사용자 패스워드 또는 PIN (Personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인, 산업, 국가의 중요 정보를 안전하게 보관할 수 없는 실정이다. 이러한 문제를 해결하기위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 형태학적 특징에 따라 사람들의 신원을 확인하는 바이오메트릭 즉, 생체인식 기술이 대두되고 있다[1~5].

미국 Washington DC에 있는 Biometric Consortium에서는 바이오메트릭을 "자동화된 특정 개인의 소추된 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 학문"으로 정의하고 있다. 이러한 생체정보를 이용한 생체인식의 예로는 지문, 음성, 얼굴 모양, 홍채 패턴, 손의 형태, 손등의 정맥 분포 등 아주 다양하며, 이들은 신체의 일부분이거나 개개인의 행동 특성을 반영하므로 잊어버리거나 타인에게 대여 혹은 도난 복사가 되지 않는다. 그러므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다.

서명이나, 손의 모양 등에 의한 생체인식을 살펴보더라도 모든 사람의 서명은 서명하는 매 시간마다 약간씩 변화되고 그들의 손가락도 매 시간마다 놓이는 위치가 조금씩 달라지기 때문에, 사용자 인증을 위해 저장된 생체정보와 인증을 위해 입력된 정보가 매번 100% 정확하게 일치할 수는 없지만 100%에 매우 가깝게 일치할 수는 있다. 또한 패스워드 또는 PIN 입력 방식에 의한 사용자 인증 방법에 비해 생체정보를 이용한 기술의 주요 장점은 생체정보는 개인별로 고유한 것으로 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 집에 두고 올 수도 없다는 것에 있다. 생체인식 기술이 앞에서 말한 것과 같은 장점이 있지만 사용자 인증을 위해 저장된 생체정보가 타인에게 도용된다면 패스워드나 PIN과 같이 변경이 불가능하므로 심각한 문제를 발생할 수도 있다.

현재 생체인식 기술에 관한 연구는 생체정보를 획득하고 가공하여 인식하는 방법에 관한 연구가 주로 진행되고 있지만, 사용자 인증을 위한 생체정보가 중앙 DB 컴퓨터 등에 저장되면 타인에 의해 도난 위험 등이 있으므로 생체정보 등록 데이터가 중앙 DB 컴퓨터등에 저장하지 않고 보안 토큰 또는 IC 카드 등에 저장되어 이러한 문제도 막을 수 있는 연구가 활발히 진행되고 있다[6,7].

본 고에서는 앞으로 개인 및 국가 등의 주요 정보를 타인으로부터 지킬 수 있는 기술인 IC 카드를 이용한 생체인식 기술에 관하여 설명한다. 본 고의 2장에서는 최근 급속한 발전을 하고 있는 IC 카드에 관하여 알아보고 3장에서는 IC 카드를 이용한 생체인식 기술 방법에 관하여 설명한다. 그리고 4

* 정회원

장에서는 기술 개발 현황을 살펴보고 5장에서 결론을 맺는다.

2. IC 카드

전자 상거래와 인터넷 사용이 급증하면서 개인의 신분 확인과 보안의 중요성이 매우 커진 현재 사용자 인증 수단으로 각광을 받으면서 세계 IC 카드 시장은 2004년까지 연평균 24% 정도의 고성장이 예측되고 있다. IC 카드는 전자상거래, 교통 및 운수, 방송 및 통신분야 등 다양한 정보 통신 서비스에 사용될 수 있으며, POS(Point Of Sale) 터미널, ATM(Automated Teller Machine), 전화, 컴퓨터, 자동판매기, 통행 제어기 등에 사용될 수 있다. 이러한 분야에서, IC 카드는 개인 정보를 생성 및 저장, 복구하거나 정보 시스템에 대한 사용자 인증 및 정보 자원에 대한 접근 통제 수단으로 사용될 수 있다.

IC 카드의 주요 장점은 IC 카드 내의 데이터에 대한 보안성이 뛰어나다는 것과 위조를 막을 수 있으며, 다양한 응용에 사용될 수 있고, 사용자 키 확인 등과 같은 보안과 관련된 인증 작업을 IC 카드 내에서 오프라인(off-line) 처리가 가능하다는 것이다. 키 확인 작업을 IC 카드 내에서 독자적으로 수행함으로써, 키 값을 외부로 유출함으로써 발생할 지도 모르는 보안 위험성을 사전에 차단시켜 준다. 앞으로는 PIN이나 패스워드를 이용한 사용자 키 확인방식과 더불어 사용자 고유의 생체정보를 이용한 생체인식을 이용한 사용자 인증 방식도 사용될 것으로 예상된다.

그리고 IC 카드는 일반적으로 암호화 및 복호화 키를 외부로 유출시키지 않으면서, 물리적으로 안전한 회로내부에 키 값이 저장되고 처리된다는 측면에서 기존의 MS(Magnetic Stripe) 카드보다 보안성이 우수하다. IC 카드는 기존의 MS 카드에 비해서 다음과 같은 장점이 있다. IC 카드는 MS 카드보다 더 많은 정보를 저장할 수 있으며, 저장된 정보에 대한 보안성이 뛰어나다. 기존의 MS 카드는 간단한 장비를 사용하여 쉽게 자성체에 기록된 정보를 읽을 수 있고 위조할 수 있다. 반면에 IC 카드는 내부에 메모리를 가지고 있기 때문에 많은 정보를 저장할 수 있으며, 불법적인 방법을 사용한 접근을 허용하지 않는다.

IC 카드는 IC 카드 칩을 내장한 카드로써, 메모리와 프로세서를 내장하고 있으므로, 저장 능력과 연산 능력을 가진다. 최근까지 수십에서 수백 바이트 크기의 메모리를 가졌으나, 최근에는 IC 카드에 내장되는 메모리 용량이 급속히 늘어나고 있다. 또한, 플래시메모리와 강유전체 메모리(FeRAM)와 같은 최신 메모리 기술을 사용하여, IC 카드에 내장할 수 있는 메모리의 용량과 사용 수명을 크게 개선시키고 있다.

IC 카드 내에 사용되는 프로세서는 특정 암호 연산을 실행하여 암호화 및 복호화를 수행하고, 인증, 서명, 프로토콜 처리, 트랜잭션 처리 등의 작업을 수행한다. 기존의 IC 카드에는 8비트 프로세서(8051 계열 및 6805 계열 프로세서)를 사용하는 경우가 많았지만, 최근에는 다양한 응용 서비스를 수행하기 위해서 16비트 혹은 32비트 프로세서를 사용하기도 한다.

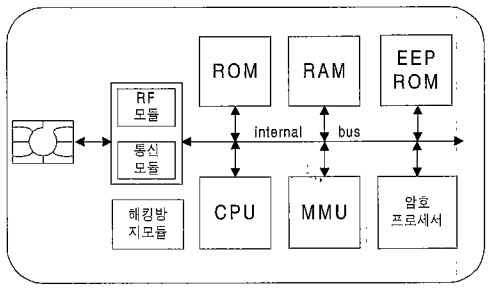


그림 1 차세대 IC 카드의 구조

그림 1은 현재 한국전자통신연구원에서 연구 개발중인 차세대 IC 카드로서, 32비트 프로세서를 채택하고 있고 암호처리 전용 코프로세서는 비대칭키 암호 알고리즘을 고속으로 처리하며, 개방형 특성을 가지기 때문에 다양한 IC 카드 응용 서비스를 수용할 수 있다. 또한 차세대 IC 카드는 접촉식과 비접촉식을 모두 지원하는 통신 모듈을 가지며, 적정 전압과 주파수 범위를 벗어난 신호를 필터링하는 해킹 방지 모듈을 가지고 있다[8].

일반적으로 IC 카드는 IC 카드와 단말기 사이의 인터페이스 방식에 따라 접촉형과 비접촉형으로 분류되며, 비접촉형 카드를 RF 카드라고도 한다. 비접촉식 카드는 RF 신호에 의해서 전원을 공급받고 통신을 수행한다. 현재 IC 카드와 관련된 국제 표준에서는 IC 카드의 물리적인 특성, 전기적인 특성, 단말기간의 통신방식·운영 방식 등에 관하여 다루

고 있으며, 이를 접촉형 IC 카드와 비접촉형 IC 카드로 나눠서 보면 다음과 같다.

접촉형 IC 카드의 국제 표준과 관련된 모든 제반사항은 ISO/IEC JTC1/SC17 Working Group 4에서 관리하고 있으며, 이곳에서 접촉형 IC 카드의 각 부분에 대한 표준을 제정하고 있다. 이곳에서는 접촉형 IC 카드의 물리적 특성, 접점의 크기 및 위치, 전송 프로토콜, 카드와 단말기 사이에서 교환되는 정보 구조, 기본적인 산업간 명령어 형식, 응용 서비스 제공자와 카드 발행자 등록 절차, 산업간 명령어의 보안 절차 및 방식 등에 대한 표준제정을 담당하고 있다.

비접촉형 IC 카드의 국제 표준과 관련된 모든 제반사항은 ISO/IEC JTC1/SC17 Working Group 8에서 관리하고 있으며, 이곳에서 비접촉형 IC 카드의 각 부분에 대한 표준을 제정하고 있다. 비접촉형 IC 카드는 카드와 단말기 사이의 커플링(coupling) 거리에 따라 세 가지 종류로 구분된다. 밀착형(Close Coupling) IC 카드, 근접형(Proximity Coupling) IC 카드, 그리고 근방형(Vicinity Coupling) IC 카드가 여기에 해당된다. Working Group 8에서는 세 가지 종류의 IC 카드 각각에 대한 물리적 특성, 커플링 영역의 크기 및 위치 그리고 카드와 단말기간의 전송 프로토콜 및 인터페이스 방식, 테스트 방법 등에 대한 표준 제정을 담당하고 있다.

IC 카드는 교통 및 통신, 신분 카드에서 앞으로는 전자상거래 및 다양한 정보통신 분야에서 사용자 인증 및 정보보호 수단으로 각광을 받을 것으로 예상되고 있다. 또한 반도체 기술의 발달로 인하여 IC 카드의 계산 능력과 사용 가능한 하드웨어 자원이 향상됨으로써 PIN이나 패스워드 방식을 이용한 방식에서 발전하여 개인의 생체정보를 이용한 사용자 인증도 IC 카드에서 수행이 가능할 것이다.

3. IC 카드를 이용한 생체인식 기술

IC 카드를 이용하여 보안에 응용하는 경우에는 현재까지 보통 4자리수 또는 6자리수의 PIN 또는 패스워드를 이용하였는데, 이는 PIN 또는 패스워드를 잊어버리거나 타인에 의해 도용되는 등의 이유로 고도의 보안을 요구하는 응용에 적합하지 않다. 그러므로 앞으로는 PIN 또는 패스워드를 대체하거나 보완하기위해 생체정보를 이용한 사용자 인증 기술이 IC 카드와 결합하는 방향으로 논의가 활발히 이루어지고 있다.

생체정보를 이용한 사용자 인증 기술은 지문과 같은 생체정보가 개인별로 고유한 특징임이 증명된 이후부터 계속적으로 사용자 인증에 사용할려는 연구가 진행되어왔다. 그리고 이러한 연구가 실생활에 적용되기 시작한 것은 지문의 경우 광학식 또는 반도체식 지문 획득기가 개발되고 지문인식에 필요한 많은 계산을 실시간으로 처리할 수 있는 고성능 컴퓨터가 일반 사용자에게 보급된 90년대 이후부터이다. 그리고 앞으로의 사용자 인증은 본장의 제목에서 알 수 있듯이 IC 카드만을 가지고서도 생체정보를 이용한 사용자 인증이 가능하게 될 것으로 예상된다. 그것은 2장에서 설명하였듯이 IC 카드가 계속적인 성능향상으로 인하여 32비트 RISC 프로세서를 내장하게 되고 또한 주변장치로 생체정보를 저장할 수 있는 메모리를 갖추기 시작하면서 부터이다.

3장에서는 현재 활발하게 연구가 진행되고 일부에서 상용화가 이루어지기 시작한 IC 카드를 이용한 생체인증 기술에 관한 것을 설명한다. 생체정보를 이용한 IC 카드는 현재 그림 2에 나타낸 것과 같은 IC 카드에서 IC 카드 내에 메모리만 있는 경우, 연산 프로세서도 있는 경우, 센서까지 있는 경우에 따라 Store-on-Card, Match-on-Card 및 Sensor-on-Card로 나눌 수 있다.

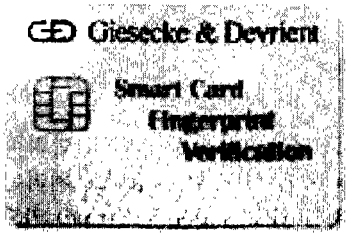


그림 2 생체인증을 위한 IC 카드

Store-on-Card 방식은 지문과 같은 생체정보를 중앙 집중식 DB에 저장하지 않고 IC 카드 내의 메모리에 저장한 후 인증을 요청할 시에 저장된 생체정보를 단말에 보내어 단말기에서 인증을 하는 시스템이고, Match-on-Card는 저장된 생체정보와 인증을 요청할 시에 취득한 생체정보를 IC 카드에서 인증 알고리즘을 계산하여 IC 카드에서 인증

결과만을 단말쪽으로 보내는 것이다. 그리고 위의 두 종류의 카드에서 생체정보 획득은 단말기에서 이루어지는 반면, Sensor-on-Card는 생체정보 획득이 IC 카드에서 이루어진다는 것이다. 예로 지문 획득 반도체 센서가 단말기에 있지않고 IC 카드에 있다는 것이다.

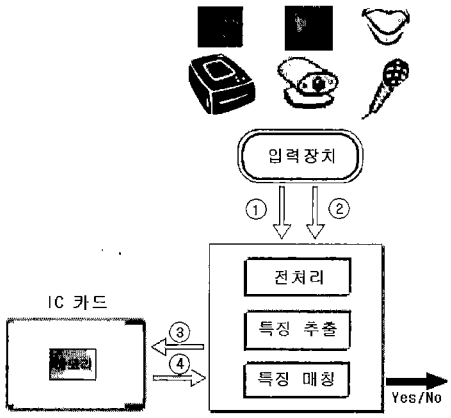


그림 3 Store-on-Card

그림 3은 Store-on-Card를 나타낸 것으로 IC 카드에 연산 능력을 갖는 프로세서 등은 내장하지 않고 단순히 생체정보를 저장하는 메모리만을 가지고 있다. 사용자 생체정보를 중앙 집중식 DB에 저장하는 방식을 택할 경우, 중앙 DB를 유지하고 관리하는데 어려움이 있고 해킹의 위험, 프라이버시의 침해 등의 문제가 발생할 수 있다. 그러므로 개인의 생체정보를 IC 카드에 저장하여 각 개인이 보유하게 함으로써 앞에서 언급한 문제 등을 해결할 수 있고, 인증 절차가 보안 토큰내의 생체정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다.

Store-on-Card를 이용한 사용자 등록 과정과 사용자 인증 과정을 살펴보면 그림 3에서 ①과 ③의 사용자 등록 과정으로 단말기에 부착된 생체정보 입력 장치를 통하여 지문, 얼굴, 음성 등의 정보를 입력받아 전처리와 인증 과정에서 사용되는 각각의 생체정보의 특징을 추출하여 Store-on-Card의 메모리에 저장하여 사용자를 등록한다. 그림 3의 ②와 ④는 사용자 인증 과정으로 인증을 요구한 사용자의 생체정보를 등록 과정과 마찬가지로 입력기로부터 입력받아 특징 추출 단계까지 거친 생체특징 정보와 Store-on-Card에 등록된 생체 특징 정보를 단말기로 보내서 단말기에서 특징 매칭을 수행하여 인증 결과를 단말기에서 출력하는 것이다.

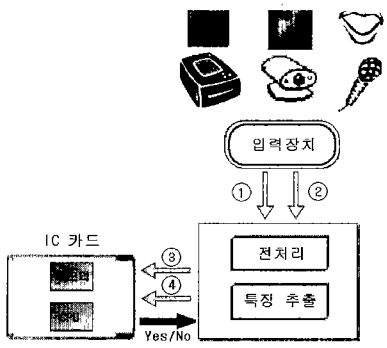


그림 4 Match-on-Card

그러나 이 경우 IC 카드는 생체 특징 정보를 저장한 단순한 메모리 기능만 제공할 뿐 사용자 인증 기능을 수행하지 않아 보안성에 문제가 있다. 즉, 입력된 생체정보에 대한 인식 처리가 단말기내의 프로세서에서 수행되기 위하여 그 생체정보가 단말기로 전송될 때, 정보 누출의 위험성이 있다. 따라서 개인 정보 누출의 위험을 최소화하여 고도 보안 응용에 적용하기 위해서는 그림 4의 Match-on-card와 같이 개인의 생체정보를 IC 카드 내에 저장할 뿐만 아니라 IC 카드 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 토큰 외부로 유출되지 않도록 하여야 한다.

Match-on-Card를 이용한 사용자 등록 과정과 사용자 인증 과정을 살펴보면 다음과 같다. 그림 4에서 ①과 ③은 사용자 등록 과정으로 Sensor-on-Card와 같은 반면에 사용자 인증 과정은 차이가 있다. 그림 4의 ②와 ④는 사용자 인증 과정으로 인증을 요구한 사용자의 생체정보를 등록 과정과 마찬가지로 입력기로부터 입력받아 특징 추출 단계까지 거친 후 Match-on-Card에 전달한다. IC 카드는 저장되어 있던 생체 특징 정보를 이용하여 IC 카드에 내장된 프로세서에서 특징 매칭을 수행하여 인증 결과를 출력함으로써 IC 카드내에 저장된 특징정보가 외부로 유출되지 않는 특징을 갖는다.

Store-on-Card와 Match-on-Card는 생체정보를 생체정보 입력기로부터 전달받아 IC 카드에 저장하여 처리하지만, Sensor-on-Card는 생체정

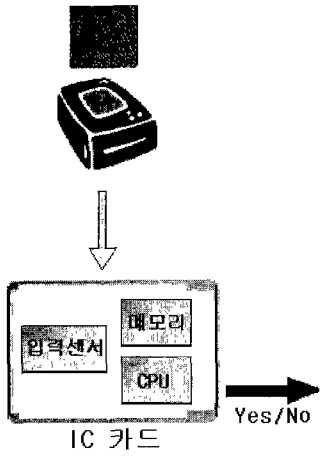


그림 5 Sensor-on-Card

보를 입력받는 장치도 IC 카드에 내장되어 있는 것을 의미한다. 예로 그림 5와 같이 지문 인증 시스템인 경우에 Match-on-Card에 반도체식 지문 입력 센서를 장착하여 등록과 인증 과정 모두를 IC 카드에서 수행하는 것이다. Sensor-on-Card는 Store-on-Card나 Match-on-Card에 비하여 생체정보가 타인에 의해 훼손 되거나 도용되는 문제가 전혀 없고 IC 카드 생체인증 시스템 중 가장 높은 보안성을 제공하지만, 입력기와 프로세서 및 메모리를 모두 내장한 상용 시스템은 아직 발표되지 않고 있다. 다만 지문 인증 시스템의 경우에는 Sensor-on-Card에 관한 연구가 일부에서 진행되고 있다.

표 1 범용 생체인식 알고리즘의 계산량 및 메모리 요구량

	총 명령어 수	8051 예상시간	ARM7 예상시간	메모리 요구량
지문	471,864,396	202.8 sec	7.8 sec	2.9 MB
얼굴	89,845,129	58.5 sec	1.5 sec	1.5 MB

* 표 1은 현재 PC에서 수행되는 범용의 생체인식 알고리즘을 8-bit 8051 프로세서와 32-bit ARM7 프로세서가 장착된 보안토큰에서 수행할 경우의 성능을 나타낸 것임

Store-on-Card는 2장에서 설명한 것과 같은 IC 카드 내에 프로세서를 내장하지는 않고 있고 다만 메모리만을 가지고 있으면서 생체정보만을 저장하기 위한 메모리만이 있는 것으로, 현재 여러 업체에서 상품이 출시되고 있는 상황이다. 반면에 Match-on-Card는 IC 카드내에 연산 프로세서를 내장하여 인증도 IC 카드에서 수행하는 것으로, 표 1에서 나타낸 것과 같이 아직까지 고성능 컴퓨터에서 수행이 가능한 생체인증 알고리즘을 IC 카드에서 수행하기는 힘든 상황이다[6]. 그러므로 세계적인 몇몇 연구업체에서 IC 카드에서 수행이 가능한 사용자 인증 알고리즘에 관한 연구를 진행하고 있다.

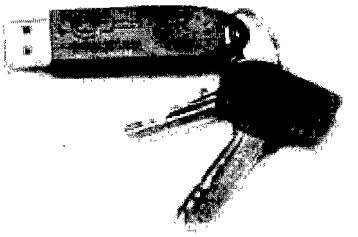


그림 6 USB 토큰 방식의 생체인증 시스템

또한 아직까지 IC 카드의 연산 능력과 하드웨어 자원이 생체인증 알고리즘을 완벽하게 수행하기에는 문제점이 있는 반면, 현재 사용되는 거의 모든 컴퓨터들이 USB 인터페이스를 지원한다는 것에 착안하여 그림 6과 같은 USB 토큰 방식의 생체인증 시스템에 관한 연구도 활발히 진행되고 있다. USB 토큰 방식의 생체인증 시스템도 IC 카드를 이용한 생체인증 시스템과 같이 USB 토큰에 생체정보만을 저장하고 인증은 단말기에서 이루어지는 것과 생체인증도 USB 토큰에서 이루어지는 것이 있다.

4. 기술 개발 현황

1990년대 후반부터 생체정보를 이용한 생체인식 기술과 IC 카드 기술이 접목되기 시작하여, 현재는 전자상거래, 인트라넷, 물리적 접근 등의 시장에서 급격하게 시장이 형성되고 있다. 앞으로는 성장속도도 급격하게 증가하고 응용분야도 다양해질 것으로 예상되므로, 국가적으로 생체인식과 IC 카드를 결합한 프로젝트를 수행하는 경우가 많고 산업계에서도 현재 활발한 연구와 연구 결과물을 발표하고 있다.

생체인식과 IC 카드를 결합하는 프로젝트로는, 스페인에서 IC 카드에 지문 정보를 저장하여 주민증과 의료 서비스에 활용하는 TASS 프로젝트를

범국가적으로 수행 중에 있다. 미 정부에서도 U.S. Smart Access Common ID 프로젝트를 통해 IC 카드와 생체인식의 접목을 시도하고 있고 미 해군에서는 시범적으로 지문정보를 저장한 IC 카드를 발급하여 네트워크 접근제어 등의 용도로 활용할 예정이다. 또한 멕시코 등 남미 여러 국가에서도 공장 노동자에게 임금을 현금으로 지급할 때 본인 여부를 확인하기 위해 지문이나 홍채 정보를 저장한 IC 카드를 이용하고 있으며, 인도에서는 지문정보를 저장한 IC 카드를 이용하여 운전면허증 발급을 추진중이다.

남아프리카공화국은 IC 카드와 생체인식 사용에 있어서 가장 앞서가는 나라 중의 하나로, 남아프리카의 스탠다드 은행의 E 은행부는 ATM기계에 접근하는 고객을 증명하기 위하여 2가지의 생체인식 기술을 사용하고 있으며, 수천만명의 연금 수령자가 연금을 수령하기 전에 생체인식에 의해 신원확인을 하는 프로젝트가 추진되고 있다.

생체인증을 위한 IC 카드 시스템과 관련한 산업계 연구는 주로 Store-on-Card 방식으로 연구가 진행되어 왔고 최근에 와서 Match-on-Card 방식에 관한 연구가 진행되고 있다.

Store-on-Card 방식의 기술 개발 사례는 세계적인 생체인식 업체인 Veridicom사에서 자사의 지문 인식 시스템을 이용한 Store-on-Card 방식의 IC 카드를 개발하여 PC 및 인터넷 액세스 제어용으로 판매하고 있으며, 세계적인 IC 카드 업체인 Bull사는 Keyware사의 화자 인증 시스템을 이용한 Store-on-Card 방식의 IC 카드 개발을 1997년에 시작하였고, Motorola사도 Identix사와 공동으로 Store-on-Card 방식의 지문 인식 시스템과 IC 카드와의 연계 기술을 개발하고 있다. 그 외에도 생체인식 기술을 보유 하고 있거나 IC 카드 기술을 보유하고 있는 거의 모든 업체에서 Store-on-Card 연구 개발을 하고 있다.

앞에서도 언급하였듯이 Store-on-Card 방식에서는 인식 처리가 단말기 내의 프로세서에서 수행되기 위하여 그 생체정보가 단말기로 전송될 때 정보 누출의 위험성이 있어, 개인의 생체정보를 IC 카드에 저장할 뿐만 아니라 IC 카드 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 보안 토큰 외부로 유출되지 않는 Match-on-Card 기술 개발이 현재 활발히 진행중이다. 예를 들어, Gemplus사는 Biometric Identification 사 및 Precise Biometric사와 공동으로 지문 인증 방식을 적용한 Store-on-Card 방식의 IC 카드 솔루션을 바탕으로 카드 내에서 인식 처리를 수행하는 Match-on-Card 기술을 현재 개발 중이다. 또한 그림 7과 같이 Obethur Card System사는 id3 semiconductors사와 공동으로 최근 스마트 카드와 카드 리더로 구성된 지문 인증 시제품을 발표하였다. 즉, 카드 리더에 있는 지문 입력 센서를 통하여 지문을 입력 받아 특징을 추출한 후 스마트 카드에 지문 특징 정보를 저장한다. 그리고 스마트 카드에서 매칭을 수행하여 인증 결과를 출력하도록 되어있다.

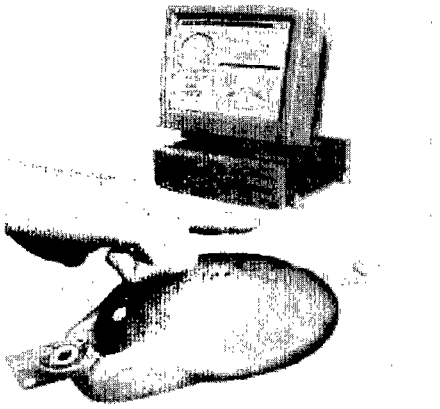


그림 7 Match-on-Card 시스템(Oberthur Card System사)

국내에서는 몇 개 회사에서 경찰청 지문 인식 시스템 구축 사업에 참여함으로써 지문인식 알고리즘 및 지문 획득 장치를 개발 생산하고 있으며, 최근 손 정맥 시스템의 상용화에 성공하였다. 또한, 홍채 획득 장치의 국산화에 성공하였으며, 음성 인식 기술을 이용한 화자 인식도 활발히 연구하고 있는 실정이다. 그러나 이러한 생체인증 기술을 IC 카드와 접목하는 연구 개발은 아직까지 활발히 이루어지고 있지 않다. 다만 일부 지문인식 회사에서 IC 카드에 지문정보를 저장하고 인식 처리는 PC에서 수행되는 Store-on-Card 방식의 지문 인식 기술을 작년에 개발하였으며, IC 카드와 같은 보안 토큰에서 생체인식을 처리하는 Match-on-Card와 Sensor-on-Card 방식의 기술을 정부출연연구소 주도로

개발에 착수하였다.

5. 맺음말

우리는 현재 정보의 홍수 시대에 살고 있다. 이에 개인의 중요 정보를 보호하기 위해, 1인당 평균 4~5개의 열쇠를 소유하거나 약 10개 정도의 비밀번호를 기억하는 등 많은 노력을 기울이고 있다. 또한 산업계, 국가적으로 중요 정보를 보호하기 위해 엄청난 자원과 시간을 투입하고 있지만 완전한 정보보호는 이루어 질 수 없다. 왜냐하면 '모든 암호 및 암호 장치는 해제 또는 도난 당할 수 있고 모든 잠금 장치는 해제될 수 있다'는 평범한 진리 때문이다. 즉, 열쇠나 비밀번호는 절대 유일의 보안 장치가 될 수 없기 때문에 컴퓨터가 사용되기 수백년 전부터 절대 유일의 보안 장치를 개발하려는 노력이 진행되어 왔고, 그 결과 살아있는 개별 인간의 신체 일부를 이용한 생체인식 기술이 발달하여 오늘에 이르게 되었다.

현재 살아있는 개인의 신체 만이 유일한 보안 도구라는 사실이 과학적으로도 입증되고 있으며 나아가 보안 도구를 결정하고 인증, 제어하는 통제 사령부 그 자체가 개별 인간이므로 생체인식 기술이 '유일성'을 보증하는 가장 훌륭한 보안 인증 수단이 되고 있다. 하지만 개별 인간의 생체정보가 중앙 DB에서 관리 된다면 'big brother' 문제가 발생할 수 있고 생체정보 등록 단말기와 중앙 DB 사이에서의 생체정보 도난 등의 문제가 발생할 수 있으므로, IC 카드에서 생체정보를 저장 및 처리하는 연구가 활발히 진행되고 있다. 또한 생체인증을 위한 IC 카드 연구가 주로 지문을 이용해서 이루어지고 있지만 말레이시아 공항의 예에서처럼 앞으로는 얼굴 또는 홍채 등 다양한 생체정보와 결합하게 될 것이고 응용분야도 다양화될 것으로 예상된다.

참고문헌

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

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

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

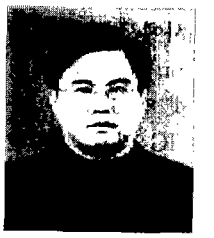
[4] G. Lawton, Biometrics: a new era in security, *IEEE Computer*, pp. 16-18, Aug. 1998.

[5] S. Liu and M. Silverman, A pratical guide to biometric security technology, *IEEE IT Pro*, pp. 27-32, Jan./Feb. 2001.

[6] Y.-H. Gil, *et al.*, A performance analysis for integrating fingerprints into smart cards for secure user authentication, *Proc. IFIP Conference E-commerce E-business E-government*, Zurich, Swiss, Oct. 2001, accepted.

[7] Y. S. Moon, *et al.*, Collaborative fingerprint authentication by smart card and a trusted host, *Proc. Canadian Conference Electrical Computer Engineering*, pp.108-112, 2000.

[8] 김호원, 정교일, 손승원, 조현숙, 차세대 IC 카드 기술, 한국통신학회지, 제17권 3호, pp. 74-83, 2000.



반 성 범

1991 서강대학교 전자공학과 졸업 (공학사)
1995 서강대학교 전자공학과 졸업 (공학석사)
1999 서강대학교 전자공학과 졸업 (공학박사)
1999~현재 한국전자통신연구원 정보보호기술연구본부 생체인식기술연구팀 선임연구원
관심분야:생체인식, 영상 처리, VLSI 신호처리 등
E-mail:sbpan@etri.re.kr

정 용 화

1984 한양대학교 전자통신공학과 졸업 (공학사)
1986 한양대학교 전자통신공학과 석사 (공학석사)
1997 미국 University of Southern California 컴퓨터공학과 졸업 (공학박사)
1986~현재 한국전자통신연구원 책임연구원 생체인식기술연구팀 팀장
관심분야:생체인식, 암호알고리즘, 병렬처리 등
E-mail:ywchung@etri.re.kr

김 호 원

1993 경북대학교 전자공학과(공학사)
1995 포항공과대학교 전자전기공학과 (공학석사)
1999 포항공과대학교 전자전기공학과 (공학박사)
1998~현재 한국전자통신연구원 정보보호기술연구본부 IC 카드구조연구팀 선임연구원
관심분야:IC 카드 설계, 정보보호, 타원곡선 암호모듈 설계, 암호 프로세서 설계 등
E-mail:khw@etri.re.kr

박 영 수

1985 중앙대학교 전자공학과(공학사)
1987 중앙대학교 전자공학과(공학석사)
1990~현재 한국전자통신연구원 선임연구원, IC 카드구조연구팀 팀장
관심분야:IC 카드 설계, CAD 및 VLSI 설계, 암호 프로세서 설계 등
E-mail:yspark@etri.re.kr