

# IC 카드를 이용한 생체인식 기술 개발 동향

## Technology Trends of the Biometrics Authentication Using IC Cards

반성범(S.B. Pan)

생체인식기술연구팀 선임연구원

정용화(Y.W. Chung)

생체인식기술연구팀 책임연구원, 팀장

조현숙(H.S. Cho)

차세대보안응용연구부 책임연구원

정보통신 기술의 발전과 인터넷 이용 확산 등으로 사용자 인증이 중요한 문제로 대두되면서 타인에게 노출되거나 잊어버리는 등의 문제점이 있는 패스워드 또는 PIN을 이용한 사용자 인증 방법을 대체하거나 보완하기 위한 방법으로 개인의 고유한 생체정보를 이용한 사용자 인증 방법에 관한 연구가 진행되고 있다. 또한 컴퓨터 관련 기술의 발달로 32비트 CPU와 메모리 등을 내장한 IC 카드가 개발되면서 최근에는 생체정보를 이용한 사용자 인증 기술과 IC 카드와의 접목이 시도되고 있다. 즉, IC 카드를 이용한 생체인식 기술은 각 개인의 중요한 정보인 생체정보가 중앙컴퓨터에 저장되지 않고 개인이 소지하고 있는 IC 카드에 저장되고 사용자 인증도 IC 카드에서 수행하는 것이다. 본 고에서는 생체인증과 IC 카드에 관하여 알아보고 IC 카드를 이용한 생체인증 기술과 개발 현황에 대하여 설명한다.

## I. 서론

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 있다. 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 해결하기 위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 형태학적 특징에 따라 사람들의 신원을 확인하는 바이오메트릭 즉, 생체인식 기술에 관한 연구가 진행되고 있다[1]-[5].

IC 카드는 IC 칩을 내장한 카드로써 현재 사용되고 있는 크레디트 카드와 크기와 모양이 유사한 것

으로, 프로세서와 메모리를 내장하고 있어 연산 능력과 저장 능력을 가진다. 기존의 IC 카드는 8비트 또는 16비트 프로세서를 사용하는 경우가 많았지만, 최근에는 32비트를 사용하여 다양한 응용 서비스 수행이 가능하게 되었다. 또한 컴퓨터 관련 기술의 발달로 내장되는 메모리 용량이 증가하고 있다.

현재 생체인식 기술에 관한 연구는 생체정보를 획득하고 가공하여 인식하는 방법에 관한 연구가 주로 진행되고 있지만, 사용자 인증을 위한 생체정보가 중앙컴퓨터 등에 저장되면 타인에 의해 도난 위험 등이 있으므로 생체정보 등록 데이터가 중앙컴퓨터 등에 저장하지 않고 보안 토큰 또는 IC 카드 등에 저장되고 사용자 인증도 보안토큰 또는 IC 카드에서 수행하도록 하는 연구가 활발히 진행되고 있다.

본 고에서는 앞으로 개인 및 국가 등의 주요 정보를 타인으로부터 지킬 수 있는 기술인 IC 카드를 이용한 생체인식 기술에 관하여 설명한다. II장에서는 생체인식 기술에 관하여 설명하고 III장에서는 최근

급속한 발전을 하고 있는 IC 카드에 관하여 알아본다. IV장에서는 IC 카드를 이용한 생체인식 기술 방법에 관하여 설명하고 V장에서 기술개발 현황을 살펴본 후 VI장에서 결론을 맺는다.

## II. 생체인식

바이오메트릭 컨소시엄(biometric consortium)에서는 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. 즉, 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 집에 두고 올 수도 없다는 것이다. 그러므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다. 생체인식 기술이 이러한 장점이 있지만 사용자 인증을 위해 저장된 생체정보가 타인에게 도용된다면 패스워드나 PIN과 같이 변경이 불가능하므로 심각한 문제를 발생시킬 수도 있다.

<표 1>은 주요 생체 인식 기술을 비교한 것으로 생체 인식에 이용되는 신체적 특징은 가장 활발히 상용화가 되고 있는 지문을 비롯해 얼굴, 손모양, 홍채와 망막, DNA 등이고 행동학적 특징은 음성, 서

명, 걸음걸이 등이 있다. <표 1>에 설명한 것과 같이 각각의 생체 인식 기술은 특성에 따라 기술 발전 정도와 적용에 차이를 보이고 있다. 음성과 서명은 편리성이 뛰어나지만 보안성이 취약하고, 홍채는 보안성은 뛰어나지만 가격이 높다는 문제점을 갖고 있다. 그러나 지문은 가장 오래된 연구를 통해 신뢰성이 입증되었고 가격이 저렴하여 적용 분야가 광범위하다. 지문의 이용 방법으로는 인증(verification, 1:1)과 인식(identification, 1:many)이 있다. 인증의 경우는 주로 지문을 이용한 출입 통제, 금고, 정보 보안, 전자 상거래 시의 본인 확인 분야에 사용된다. 인식의 경우는 지문을 등록된 지문 데이터베이스에서 검색을 하여 찾아주는 기술로 AFIS(Automated Fingerprint Identification System)가 있다. 또한, 지문 인식 기술은 마우스, 키보드, ATM 단말기 등에 사용되고 있으며 휴대폰 PDA 등에 적용된 지문 인식 제품도 선보일 예정이다. 홍채 인식 시스템은 다른 생체 인식 시스템에 비해 정확성이 뛰어나고 위, 변조가 불가능해 보안성이 우수하나 가격이 다소 비싸다는 단점을 갖고 있는데, 앞으로 고도의 보안을 요구하는 핵시설, 의료 분야 등을 중심으로 수요가 점진적으로 늘어날 것으로 예상되고 있다.

앞으로는 하나의 생체 정보만을 활용한 시스템의 한계를 극복하기 위하여 여러 개의 생체 정보를 이용한 다중 생체인식 기술, 생체정보 데이터베이스 유지와 보완의 어려움을 해결할 수 있는 IC 카드와의 통합 기술 등에 연구가 진행되고 있다.

<표 1> 생체인식 기술 비교

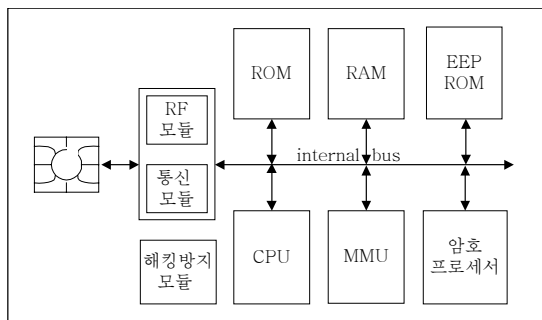
기술 분류	장 점	단 점	비 고
지문	• 안전성 우수 • 비용 저렴	• 훼손된 지문 인식 곤란	범죄수사 및 산업분야에 이용
얼굴	• 인식 용이 • 비용 저렴	• 주위 조명에 민감 • 표정 변화에 약점	출입통제
손모양	• 처리정보량이 적음 • 작동이 용이	• 상대적으로 처리속도 낮음 • 정확성 낮음	제조업분야
홍채/망막	• 타인에 의한 복제 불가능	• 사용 불편 • 이용에 따른 거부감	핵시설, 의료분야, 교도소
음성	• 원격지 사용 가능 • 비용 저렴	• 정확도 낮음 • 타인에 의한 도용 가능	원격 은행업무, 증권 ARS

### III. IC 카드

전자상거래와 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 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.

(그림 1)은 현재 한국전자통신연구원에서 연구 개발중인 차세대 IC 카드로서, 32비트 프로세서를 채택하고 있고 암호처리 전용 코프로세서는 비대칭 키 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[6].



(그림 1) 차세대 IC 카드의 구조

IC 카드는 교통 및 통신, 신분 카드에서 앞으로는 전자상거래 및 다양한 정보통신 분야에서 사용자 인증 및 정보보호 수단으로 각광을 받을 것으로 예상

되고 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.

### IV. IC 카드를 이용한 생체인식 기술

PIN 또는 패스워드를 대체하거나 보완하기 위해 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 사용하려는 연구가 진행되어 왔다. 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 이후부터 이다. 그리고 앞으로의 사용자 인증은 IC 카드만을 가지고서도 생체정보를 이용한 사용자 인증이 가능하게 될 것으로 예상된다. III장에서 설명하였듯이 IC 카드가 계속적인 성능향상으로 인하여 32비트 RISC 프로세서를 내장하게 되고 또한 주변장치로 생체정보를 저장할 수 있는 메모리를 갖추기 시작하면서부터 이다.

생체정보를 이용한 IC 카드는 (그림 2)에 나타난 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.

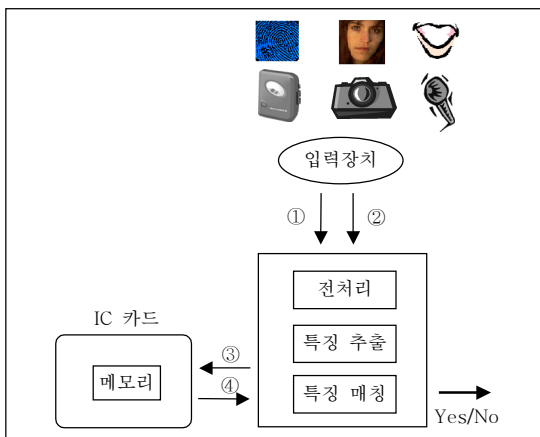


(그림 2) 생체인증을 위한 IC 카드

Store-on-Card 방식은 지문과 같은 생체정보를 중앙 집중식 DB에 저장하지 않고 IC 카드 내의 메모리에 저장한 후 인증을 요청할 시에 저장된 생체정보를 단말기에 보내어 단말기에서 인증을 하는 시스템이고, Match-on-Card는 저장된 생체정보와 인증을 요청할 시에 취득한 생체정보를 IC 카드에서 인증 알고리즘을 계산하여 IC 카드에서 인증 결과만을 단말기 쪽으로 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 있지 않고 IC 카드에 있다는 것이다.

(그림 3)은 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 관리하는 데 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 토큰 내의 생체정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다.

Store-on-Card를 이용한 사용자 등록 과정과

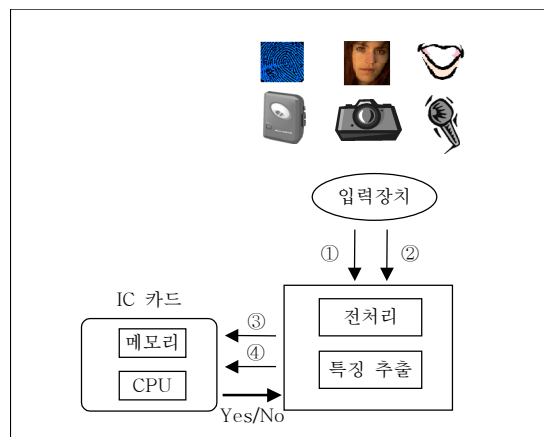


(그림 3) Store-on-Card 시스템

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

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 단말기 내의 프로세서에서 수행되기 위하여 그 생체정보가 단말기로 전송될 때, 정보 누출의 위험성이 있다. 따라서 개인정보 누출의 위험을 최소화하여 고도 보안 응용에 적용하기 위해서는 (그림 4)의 Match-on-Card와 같이 개인의 생체정보를 IC 카드 내에 저장할 뿐만 아니라 IC 카드 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 IC 카드 외부로 유출되지 않도록 하여야 한다.

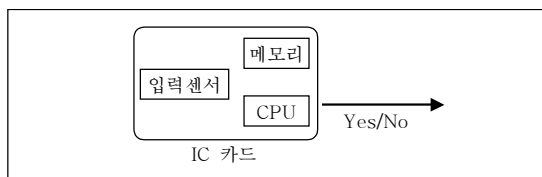
Match-on-Card를 이용한 사용자 등록 과정과



(그림 4) Match-on-Card 시스템

사용자 인증 과정을 살펴보면 다음과 같다. (그림 4)에서 ①과 ③은 사용자 등록 과정으로 Sensor-on-Card와 같은 반면에 사용자 인증 과정은 차이가 있다. (그림 4)의 ②와 ④는 사용자 인증 과정으로 인증을 요구한 사용자의 생체정보를 등록 과정과 마찬가지로 입력기로부터 입력 받아 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 카드 내에 저장된 특징정보가 외부로 유출되지 않는 특징을 갖는다.

Store-on-Card와 Match-on-Card는 생체정보를 생체정보 입력기로부터 전달 받아 IC 카드에 저장하여 처리하지만, Sensor-on-Card는 생체정보를 입력 받는 장치도 IC 카드에 내장되어 있는 것을 의미한다. 예로 (그림 5)와 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 훼손되거나 도용되는 문제가 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.



(그림 5) Sensor-on-Card 시스템

## V. 기술개발 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 수행중에 있다. 미국 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 지문 정보를 저장한 IC 카드를 이용하여 운전면허증 발급을 추진중이다.

남아프리카공화국은 IC 카드와 생체인식 사용에 있어서 가장 앞서가는 나라 중의 하나로, 남아프리카의 스탠다드 은행은 ATM 기계에 접근하는 고객을 증명하기 위하여 2가지의 생체인식 기술을 사용하고 있으며, 수천만 명의 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 카

드와의 연계 기술을 개발하고 있다.

또한, 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, Gemplus 사는 Biometric Identification사 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 개발중이다. 또한 (그림 6)과 같이 Oberthur 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 되어 있다.

(그림 7)은 Sony사의 지문 인증 시스템으로 지문 정보 저장과 지문 인증 연산을 시스템 내에서 수행하는 것으로 USB 방식으로 호스트와 통신하도록 되어 있다. IC 카드 형식은 아니지만 일반 PC 등의 호스트가 일반적으로 USB를 지원하므로 추가비용 부담 없이 사용할 수 있는 장점이 있어 USB 보안 토큰 시스템 개발도 활발히 진행되고 있다.

국내에서는 몇 개 회사에서 경찰청 지문 인식 시스템 구축 사업에 참여함으로써 지문 인식 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 개발하였으며, IC 카드와 같은 보안 토큰에서 생체인식을 처리하는 Match-on-Card 방식의 기술을 정부출연연



(그림 6) Match-on-Card 시스템(Oberthur Card System사)



(그림 7) USB 토큰(Sony사)

구소 주도로 개발하고 있다.

## VI. 맺음말

우리는 현재 정보의 홍수 시대에 살고 있다. 이에 개인의 중요 정보를 보호하기 위해, 1인 당 여러 개의 열쇠를 소유하거나 비밀번호를 기억하는 등 많은 노력을 기울이고 있다. 또한 산업계, 국가적으로 중요 정보를 보호하기 위해 엄청난 자원과 시간을 투입하고 있다.

최근에 정보 보안 단계를 한 단계 높이기 위하여 32비트 CPU와 메모리가 내장된 IC 카드를 이용한 생체인증에 관한 연구가 세계적으로 유명한 칩 제조사와 생체인식 업체들을 시작으로 활발히 진행되고

있다. 우리도 생체인식 알고리즘의 원천 기술뿐만 아니라 개인이 소지할 것으로 예상되는 핸드폰, PDA, 입는 컴퓨터(wearable computer), 또는 IC 카드 등을 통한 생체인증이 가능하도록 기술 개발을 하여야 할 것이다. 또한 생체인식 기술에 관한 표준화가 진행되고 있으므로 국내에서도 활발하게 표준화에 참여하여야 할 것이다.

## 참 고 문 헌

- [1] A.K. 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*, Aug. 2000, pp. 8 - 11.
- [4] G. Lawton, "Biometrics: a New era in Security," *IEEE Computer*, Aug. 1998, pp. 16 - 18.
- [5] S. Liu and M. Silverman, "A Practical Guide to Biometric Security Technology," *IEEE IT Pro*, Jan./Feb. 2001, pp. 27 - 32.
- [6] 김호원, 정교일, 손승원, 조현숙, "차세대 IC 카드 기술," *한국통신학회지*, 제17권 3호, 2000, pp. 74 - 83.