소 특 집

# 생체인식 기술동향

반 성 범*, 정 용 화*, 정 교 일*, 김 재 희**

*한국전자통신연구원 정보보호기반연구부, **연세대학교 기계전자공학부

## I. 서 론

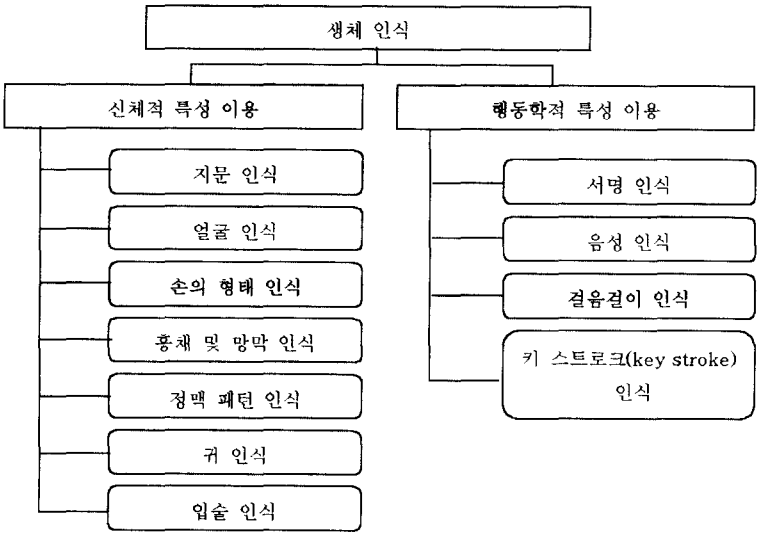
최근 인터넷에 의한 전자상거래, 전자 정부 등의 영향으로 사용자 인증이 중요한 문제로 대두되었다. 과거에는 모든 사회 생활이 오프라인에서 이루어져 개인이 직접 활동하면서 모든 일을 처리하였지만, 현재는 온라인 활동이 많아지면서 비대면 온라인 상에서 올바른 사용자가 사용하고 있는지의 여부가 중요한 문제로 대두되기 시작하였다. 사용자 인증 방법은 패스워드 또는 PIN 등 사용자가 알고 있는 정보, 열쇠 또는 스마트 카드 등 사용자가 소지하고 있는 장치, 지문 또는 음성 등 사용자의 고유 정보를 이용한 방법으로 나눌 수 있다. 현재까지 일상생활에서 널리 사용되고 있는 사용자가 알고 있는 정보 또는 소지하고 있는 장치를 이용한 사용자 인증 방법은 망각, 분실 또는 도난 등의 이유로 높은 보안 성능을 제공하지 못하게 되었다. 반면에 생체인식은 개인별로 차이가 있는 사용자의 고유한 생체정보 또는 독특한 행동을 이용하는 것으로 분실 및 도난 등의 문제가 없어 기존의 방법에 비해 높은 보안 성능을 제공할 수 있다.

생체인식은 지문, 손 모양, 홍채, 얼굴 모양 등의 신체적(physical) 특징을 이용한 방법과 서명, 음성, 걸음걸이 등의 행동학적(behavioral) 특징을 이용하는 방법으로 나누어진다[1-5]. 또한 생체인식 시스템은 많은 응용 분야에 다양하게 사용되고 있지만, 기본적으로는 사용자 자신이 자신임을 확인 받는 인증 (verification, 1 : 1)과 데이터베이스에서 사용자를 찾아내는 인식 (identification, 1 : $N$)으로 나누어진다. 그리고 생체인식 시스템은 생체정보를 획득한 후 올바른 사용자 여부를 판단하는 것이므로, 기본적으로 카메라 또는 마이크 등의 생체정보를 획득하는 센서와 범용 CPU, DSP 또는 생체인식 전용 하드웨어를 이용한 분석 등의 생체 인증/인식 연산을 수행하는 프로세서로 구성된다. 또한 생체정보를 저장하기 위한 장치가 추가적으로 필요하다. 특히 인증인 경우는 중앙 데이터베이스에 자신의 생체정보를 저장하는 방법 외에 최근에는 스마트 카드 또는 PDA 등 개인기기에 생체정보를 저장하는 연구가 진행되고 있다.

본 고에서는 현대 생활에서 보안의 필요성이 증대되고 생체정보를 획득하는 장비인 카메라, 마이크 등의 장비가격의 하락 및 컴퓨터 하드웨어의 급속한 발전으로 인하여 생체인식의 실시간 처리가 가능해지면서 활발하게 실생활에 적용되고 있는 생체인식 기술에 대하여 살펴본다. 2장에서는 지문, 얼굴 모양, 홍채 등 대표적인 생체인식 기술의 특징 및 장단점에 관하여 간단히 설명한다. 3장에서는 생체인식 기술을 이용한 최근의 연구 분야 및 응용분야에 대하여 설명하고, 4장에서 결론을 맺는다.

## II. 생체인식 기술

생체인식은 <그림 1>과 같이 얼굴 모양, 홍채, 망막, 손등의 정맥, 지문 등 신체적 특성을 이용한 방법과 서명, 키보드 타이핑 습관, 걸음걸이




〈그림 1〉 생체인식의 종류

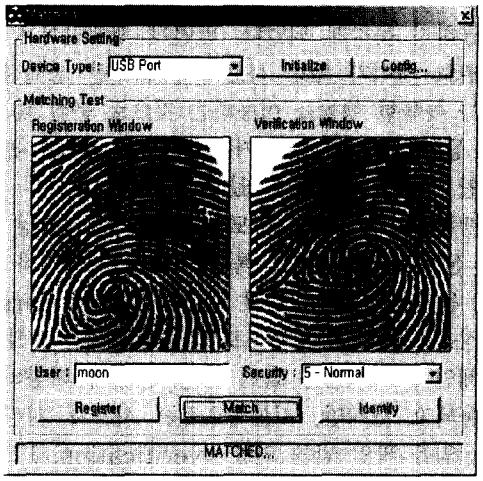
습관 등 행동학적 특성을 이용한 방법으로 나눌 수 있다. 대표적인 생체인식 기술에 관하여 소개하면 다음과 같다[1][3].

## 1. 지문

현대 지문 비교 기술은 1684년 영국 황실 사회의 네에미아 크류가 처음으로 사람들의 지문들이 서로 다르다는 것을 알게 되면서부터 시작되었고, 또 그것들이 루프와 소용돌이 그리고 궁상문들을 포함하는 많은 수의 키 패턴에 의해 분류될 수 있음을 알았다. 현재에는, 주 특징에 의해 분류되어질 수 있을 뿐만 아니라, 지문들이 지문상의 융선의 종점이나 가지들에서 발생하는 특징점(minutiae)으로 알려진 더 작은 특징들에 의해서도 분류될 수 있다.

지문 인식 장치를 사용하기 위해서는 하나의 손가락을 영상 획득 장치에 있는 평면 위에 놓는데, 대부분의 지문 인식 장치들은 원본 데이터로 원래의 지문의 영상을 그대로 저장하는 대신에 특징점들의 위치와 관련된 정보를 저장한다. 이러한 시스템들은 원본 데이터로부터 지문 영상을 재생할 수 없기 때문에, 등록자들의 지문들은 법 시행 기관들에 의한 증명 방법으로 사용될 수는 없다. 또한, 최근 출시되는 지문 인식 장치들은 손가락을 스캔하면서 손가락이 살아있는 사람의 것인지도 검사하는 데, 이것은 불법 사용자가 절단된 손가락을 이용하여 정당한 사용자를 가장하는 것을 막기 위한 것이다.

〈그림 2〉와 같은 지문 인식 시스템은 현재 생체인식 시스템 가운데 가장 광범위하게 응용되고 있는 분야이다. 체이스맨해튼, 시티뱅크 등 대규모 금융 기관에서 현금자동지급기 (ATM)의 고객 인증을 위해 지문인식 시스템을 활용하고 있




〈그림 2〉 지문 인증 시스템

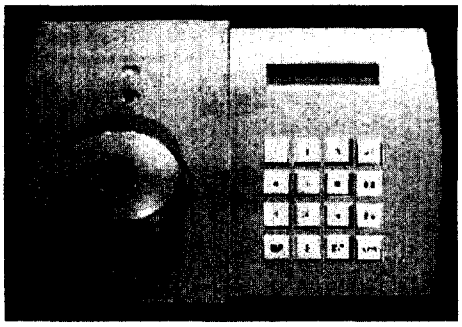
으며, 뉴욕과 캘리포니아의 복지담당관청에서는 복지 수당의 이중 인출을 방지하기 위해 지문 인식시스템을 사용하고 있다.

그러나 지문 인식 시스템이 완벽한 개인 식별 수단이 될 수는 없다. 지문인식 시스템은 일반적으로 지문 융기의 분기점, 끝점 등으로 구성되는 특징점의 위치와 속성을 추출, 저장, 비교하는 알고리즘을 채용하고 있는데, 불과 4-5개의 특징점만으로 개인을 식별하는 시스템들도 산재하기 때문이다. 또한 땀이나 물기가 스캐너에 배어있는 경우 에러 발생률이 크게 높아진다는 점, 여러 사람이 연속적으로 접촉한 곳에 자신의 손가락을 댄다는 불쾌감, 지문이 닳아 없어진 사람도 간혹 있다는 점 등이 지문 인식 시스템의 한계로 인식되고 있다.

## 2. 홍채/망막

사람의 눈을 이용한 생체 인증에서 눈은 홍채와 망막의 혈관이 인증을 목적으로 사용되고 있다. 망막 인식은 사용자의 안구 배면에 위치한 모세 혈관의 구성이 인간의 지문과 같이 종생불변의 특성을 가지고 있다는 점을 이용하는 것으로, 이러한 망막 패턴을 읽기 위해서는 미약한 강도의 연필 지름 만한 적색 광선이 안구를 투시하여 망막에 있는 모세혈관에 반사된 역광을 측정해야 한다. 따라서 성공적인 망막 패턴 검색을 위해서는 사용자가 안경을 낀 경우 안경을 벗고 검색기에 접안해야 하며, 접안기의 내부 원통 내 어두운 부분 중 적색광선이 반사되는 접에 눈의 초점을 맞춰야 한다. 이러한 망막 패턴 검색 기술은 고도의 보안성을 만족시킬 수 있지만, 사용자의 불편과 레이저 빛에 대한 두려움을 유발하는 등 일반인을 대상으로 하여 사용하기에는 비효율적인 면이 있다.

이에 반해 〈그림 3〉과 같은 홍채 인식 시스템은 자연스러운 상태에서 획득된 영상을 이용하므로 망막 인식에서와 같은 단점이 없어 많은 분야로의 적용이 기대되는 분야이다. 특히 사람의 홍채는 신체적으로 상당한 특징이 있는 유기체 조직으로, 쌍둥이들도 다른 홍채 패턴들을 가지고



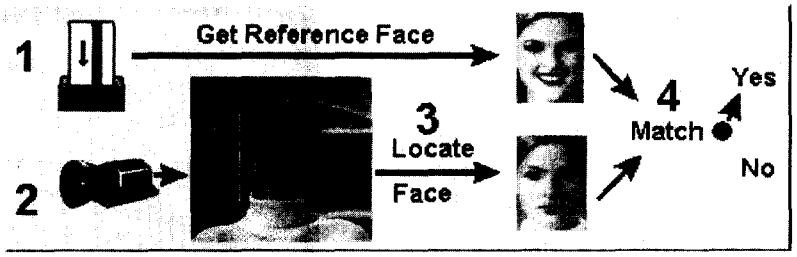
〈그림 3〉 홍채 인식 시스템

있고 통계학적으로도 DNA 분석보다 정확하다고 알려져 있다. 그리고 외상 또는 아주 드문 병을 제외하고는 홍채는 사람의 일생 동안 변화되지 않으며, 콘택트렌즈나 안경을 착용해도 인식이 가능하므로 활용 범위가 넓다.

홍채 인식을 인터넷에서 활용하는 예로서, 인터넷 상에서 컴퓨터 모니터, 핸드 헬드 컴퓨터, 탁상용 컴퓨터 안에 내장된 카메라가 사용자의 홍채를 인식하여 사이트로 전송하면, 이전에 사용자가 암호화하여 등록한 패턴과 비교하여 일치하면 신분이 확인되는 여러 가지 응용에 사용될 수 있다. 그러나 만약 안경에 타인의 홍채 사진을 붙여 접근을 시도할 경우에 대한 대책은 망막이나 홍채 모두 신체위해 가능성을 염두에 두어야 한다는 점이다. 이 같은 문제점을 해결하기 위해 시스템 개발자들은 망막이나 홍채의 색, 패턴, 무늬 등을 인식하는 동시에 눈에서 발생하는 파장을 감지, 진위를 구별할 수 있도록 하는 연구도 병행하고 있다.

## 3. 얼굴

얼굴을 이용한 인식 방법은 생체인식 방법 중 가장 자연스러운 방법으로, 지문과 같이 지문 입력 장치에 손가락을 접촉하지 않고 비접촉으로 자연스럽게 인식할 수 있는 장점이 있다. 그러나 조명의 변화에 민감하고, 변장 및 세월이 흐르면서 생기는 얼굴 변화 등에 약점을 가지고 있어, 아직까지는 지문 및 홍채와 같은 높은 인식률을 나타내지는 못하고 있다. 얼굴인식에서 가장 중




〈그림 4〉 얼굴 인식 시스템의 얼굴 인식 순서

요하고 어려운 문제 가운데 하나는 입력된 영상으로부터 처리 대상인 얼굴 영역을 추출하는 방법으로, 얼굴의 열상을 이용하는 방식과 2차원/3차원 얼굴 영상을 이용하는 방식으로 크게 구분된다. 특히, 얼굴의 열 분포를 이용하는 방식은 얼굴 혈관에서 발생하는 열을 적외선 카메라로 촬영, 디지털 정보로 변환해 저장하는 것으로, 얼굴에 외과적인 손상이 발생하더라도 변하지 않는 장점이 있다.

미국 Technology Recognition Systems사는 안면 열상(Facial Thermogram) 방법을 이용하며, 영국 Neurodynamics Biometrics사의 "NVISAGE"는 적외선을 사용해 생성한 3차원 안면 영상을 사용한다. 미국 Miros도 안면 열 분포를 이용한 "TrueFace"를 PC, 출입 관리용 등으로 개발, 판매하고 있으며, 현금자동지급기 등에서도 활용되고 있다. 또한 미국 Visionics사의 "FaceIt"도 많이 알려진 얼굴 인식 시스템이다.

〈그림 4〉와 같이 작동하는 얼굴 인식 기법은 사용자의 기분과 상황에 따라 표정이 변하게 되는 특성을 고려해야 하며, 주위 조명에 많은 영향을 받게 되는 등의 단점이 있다. 또, 이들 안면 인식 시스템들의 한 가지 기본적인 문제점은 얼굴 인식을 위해 원본 데이터로 저장된 인상 사진들은 자연스러운 자세가 아닌 인공적인 자세에서 찍혀진다는 것이다. 따라서, 데이터베이스상의 사진과 다른 사진 영상을 비교하여 동일인인가를 판단하기는 여전히 어렵다. 현재 많은 회사들이 어떤 사람이 문을 향해서 걸어가거나 어떤 고정된 점을 지날 때 카메라에 찍힌 사진 영상과 데이터베이스에 저장된 사진을 비교하는 시스템을 개발하고 있다.

### 4. 화자

음성을 이용한 개인인식은 화자(speaker) 인증이라고도 하며, 다른 생체인식에 비해 에러율은 높지만 음성 인식과 관련하여 활발하게 연구되고 있는 분야이다. 특히, 다른 생체 획득 장치와는 달리 음성 취득 장치인 마이크는 저가이고 일반 PC 또는 PDA, 핸드폰 등에 기본적으로 탑재될 수 있으므로, 다른 생체인식에 비해 취득 장치에 드는 비용이 거의 없다는 장점이 있다. 또한, 전화나 인터넷을 이용하여 원격지에서도 사용이 가능하여, 텔레뱅킹 등 다른 생체인식방법을 적용할 수 없는 응용분야에서 사용될 수 있다.

### 5. 손 모양

생체인식 분야에서 가장 먼저 자동화된 기법으로, 스탠포드 대학의 한 연구팀이 개인마다 손가락의 길이가 다르다는 점에 착안, 약 4,000명의 손가락 형태를 분석하여 이를 데이터화하여 만든 시스템이다. 특히, 영상처리 분야의 발전으로 단순한 길이를 측정하는 것에서 벗어나, 다양한 특징점을 추출하여 사용하고 있다. 손 모양 인식기는 3-D 이미지 상태로 사람 손의 높이, 길이, 너비를 측정하며, 적외선 불빛과 디지털 카메라는 손 데이터를 인식하는데 사용된다.

### 6. 정맥

손등의 정맥 인식시스템은 지문이나 손 모양을 이용하는 방법에 비해 사용자의 거부감을 줄일

수 있다. 지문 또는 손가락이 없는 사람도 이용할 수 있다는 장점을 갖고 있으며, 손등의 정맥패턴이 쌍둥이조차도 그 모양이 다르다고 알려져 있다. 손등의 피부로부터 정맥 패턴을 추출하는 방법은 적외선 조명과 필터를 사용해 피부에 대한 혈관의 밝기 대비를 최대화한 다음, 입력된 디지털 영상으로부터 정맥 분포 정보를 추출한다. 지문인식과 같이 특징점을 좌표로 인식할 뿐 아니라 전체적인 혈관 모양도 비교한다. 정맥패턴을 추출한 후는 지문 등의 기법과 같이 인증을 수행하는 것으로, 사용이 편리하면서 사용자의 거부감이 적고, 일반적으로 지문보다 많은 정보를 보유하고 있어 인식률이 높아 응용분야가 많다. 특히 적외선을 사용, 혈관을 투시한 후 잔영을 이용해 신분을 확인하는 방식으로, 복제가 거의 불가능하여 매우 높은 보안성을 지니고 있다.

### 7. 기타

유일하고도 측정 가능한 신체적 또는 행동적인 특징은 한 사람의 신원을 확인하는 데 사용될 수 있다. 물론 이런 특징 들 중 어떤 것이 사용하기 쉽고 어려운 가에는 차이가 있다. 앞서 언급한 특징 이외에 현재 개발되고 있는 다른 시스템은 귀 인식, 근전도 신호(손/팔의 동작), 걸음걸이 인식, 타이핑 리듬 인식, 입술 인식 등이 있다.

타이핑 리듬에 의한 인식은 사람이 타이핑을 함에 있어 숙련자이든 한 손가락만을 사용하는 사람이든 그들 자신의 타이핑 리듬을 가지고 있다는 사실에 기초하고 있다. 개발의 목표는 특별한 컴퓨터의 사용자를 계속하여 모니터할 수 있고 로그온 한 사용자를 대신하여 다른 누군가가 컴퓨터를 사용하는 것을 탐지하는 시스템을 개발하는 것이다. 그러나 계속적인 모니터링은 타이핑 리듬이 사용자가 피곤하고, 스트레스를 받고 혹은 술을 먹었는가에 따라서 변화하기 때문에 어려움이 있다.

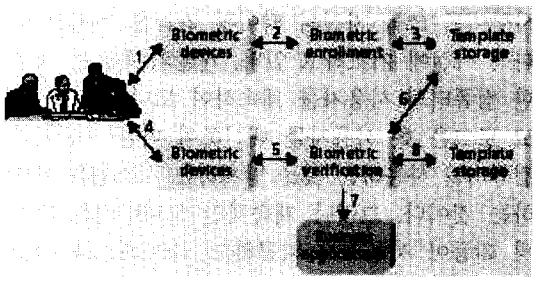
귀의 모양에 의하여 개인들을 증명하는 시스템은 프랑스와 네덜란드에서 개발하고 있는데, 한 예는 전화 핸드셋이 귀에 닿을 때 귀의 영상을 획득할 수 있는 작은 카메라가 달린 전화형 핸드셋을 사용한 시스템이다.

## III. 생체인식 시스템 응용 예

대표적인 생체인식 기술의 특징을 사용 편리성, 에러 원인, 인식률 등의 측면에서 비교한 것을 〈표 1〉에 나타내었는데, 각각의 응용 분야에 따라 적합한 생체 정보를 선택하여야 함을 나타내고 있다. 또한 하나의 생체인식만이 사용되는 것이 아니라 얼굴, 음성, 입술 모양 등의 여러 개의 생체인식 기술이 동시에 사용되는 다중 생체인식 방법을 이용하여 좀 더 높은 인식률을 제공

〈표 1〉 생체인식 기술 비교

| 특징 | 지문 | 손모양 | 망막 | 홍채 | 얼굴 | 서명 | 화자 |
|---|---|---|---|---|---|---|---|
| 사용 편리성 | high | high | low | medium | medium | high | high |
| 에러원인 | dryness, dirt, age | hand injury, age | glasses | poor lightning | lighting, age, glasses, hair | changing signature | noise, colds, weather |
| 인식률 | high | high | very high | very high | high | high | high |
| 거부감 | medium | medium | medium | medium | medium | very high | high |
| 보안성 | high | medium | high | very high | medium | medium | medium |
| 영구성 | high | medium | high | high | medium | medium | medium |




〈그림 5〉 생체인증 및 인식 과정

하는 연구도 필요함을 알 수 있다.

생체 정보를 이용한 보안 시스템은 앞에서 언급한 것과 같이 사용자 인증과 인식으로 나누어진다. 일반적으로 인식이 데이터베이스를 검색하여야 하므로 인증에 비하여 시스템이 복잡하다. 〈그림 5〉는 생체정보를 이용한 인증과 인식을 수행하는 과정을 설명한 것으로, 응용 분야에 따라 각 과정이 수행하는 기기 또는 환경의 차이만 있을 뿐 전체 수행과정은 같다[4].

### 1. 물리적/가상적 사용자 인증

최근에 고도의 보안을 요구하는 환경에서 생체인식을 사용한 출입통제가 실용화되고 있다. 사무실 또는 빌딩 출입뿐만 아니라 병원, 카지노, 헬스클럽에서 사용되고 있으며 1996년 올림픽에서는 65,000명의 출입통제에 생체인식이 사용되었다.

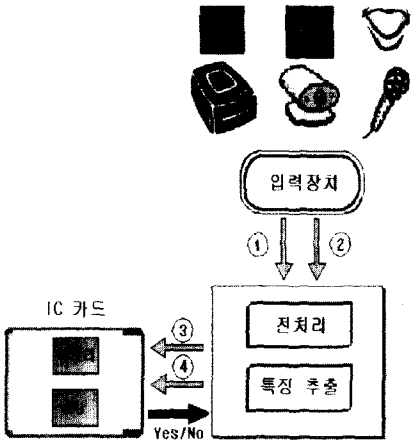
특히, 2001년 미국 테러이후 생체 인식 기술이 급속히 보급될 수 있을 것으로 예상되는데, 미국에서는 이민 및 비자발급에 생체 인식 기술 적용을 추진 중이며 국경 보호를 위하여 생체인식 기술의 활용을 의무화하는 법안 즉, 모든 외국인에 대하여 비자 신청 시 생체정보를 요구하고, 비자 면제국들은 여권에 생체정보 저장을 의무화하는 비자면제프로그램 수정안을 법제화 중이다. 영국에서도 자국민의 신원 확인을 위해, 향후 4년내에 지문 및 홍채 정보를 저장한 스마트 여권 도입을 검토 중이며, 네덜란드의 Schipol 공항(암스텔담)에서는 경찰청과 이민국 주관의 시험 기간을 거친 "홍채와 스마트카드를 이용한 자동출입국관리(Automated Border Crossing) 시스템"을 본격 도입하기 위하여, 2002년 1월부터 법무부 주관으로 시범 운용 중이다.

### 2. 보안연동 기술

단순히 생체인식이 비밀번호나 암호를 보완하거나 대체하는 것에 머물지 않고, 최근 급속한 발전을 하고 있는 스마트카드나 PKI(Public Key Infrastructure)와의 연동도 시도되고 있다. 생체인식을 적용하기 위하여 가장 큰 문제는 등록된 생체정보를 어떻게 안전하게 저장하느냐는 것인데, 그 해결책으로 개인이 소지하는 스마트카드에 암호화하여 저장하면 안전하게 저장할 수 있다. 여기에 보안성을 높이기 위하여, 단순히 저장만 하는 것이 아니라 스마트카드 내에서 사용자 인증까지 수행하는 연구도 진행되고 있다.

생체정보와 스마트카드를 연동시키는 방법으로는, 스마트카드 내에 메모리만 있는 경우, 연산 프로세서도 있는 경우, 센서까지 있는 경우에 따라 각각 Store-on-Card, Match-on-Card 및 Sensor-on-Card로 나눌 수 있다. Store-on-Card 방식은 지문과 같은 생체정보를 중앙 집중식 DB에 저장하지 않고 스마트카드 내의 메모리에 저장한 후, 인증을 요청할 시에 저장된 생체정보를 단말에 보내어 단말기에서 인증을 하는 시스템이다. 반면, Match-on-Card는 저장된 생체정보와 인증 요청용 생체정보 비교를 스마트카드내의 프로세서가 수행하는 것으로, 스마트카드에서는 인증 결과만을 단말 쪽으로 보내는 것이다. 마지막으로, 위 두가지 방식은 생체정보 획득이 단말기에서 이루어지는 반면, Sensor-on-Card는 생체정보 획득이 스마트카드 상에서 이루어진다는 차이가 있다.

예를 들어, 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 스마트카드(Store-on-Card)에 저장하여 각 개인이 보유하게 함으로써 앞에서 언급한 문제 등을 해결할 수 있고,




〈그림 6〉 Match-on-Card 시스템

증 절차가 스마트카드 내의 생체정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다.

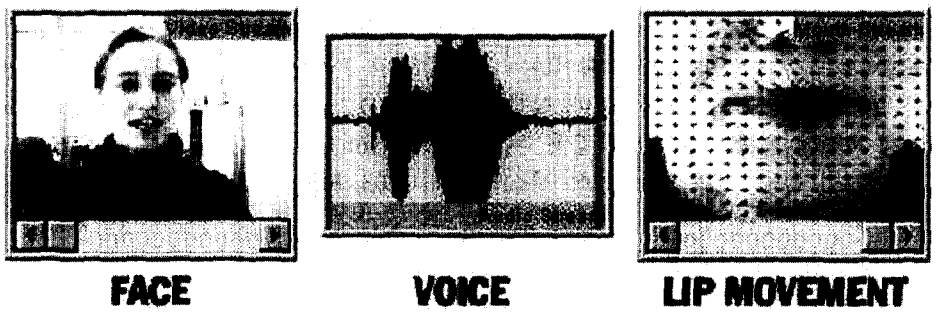
그러나 이 경우 스마트카드는 생체 특징 정보를 저장한 단순한 메모리 기능만 제공할 뿐 사용자 인증 기능을 수행하지 않아, 보안성에 문제가 있다. 즉, 입력된 생체정보에 대한 인식 처리가 단말기내의 프로세서에서 수행되기 위하여 그 생체정보가 단말기로 전송될 때, 정보 누출의 위험성이 있다. 따라서 개인 정보 누출의 위험을 최소화하여 고도 보안 응용에 적용하기 위해서는, 〈그림 6〉과 같이 개인의 생체정보를 스마트카드 내에 저장할 뿐만 아니라 스마트카드 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 스마트카드 외부로 유출되지 않도록 하여야 한다.

이상 언급한 Store-on-Card와 Match-on-Card는 생체정보를 별도의 생체정보 입력기로부터 전달받아 스마트카드에 저장하여 처리하지만, Sensor-on-Card는 생체정보를 입력받는 장치도 스마트카드에 내장되어 있는 것을 의미한다. 따라서, Sensor-on-Card는 Store-on-Card나 Match-on-Card에 비하여 생체정보가 타인에 의해 훼손되거나 도용되는 문제가 전혀 없고 스마트카드 생체인증 시스템 중 가장 높은 보안성을 제공하지만, 입력기와 프로세서 및 메모리를 모두 내장하기 때문에 가격이 높다는 문제가 있다.

## 3. 멀티모달 생체인식

정보보안, 금융서비스, 범인 색출, 정부의 대민 업무 등 유망한 생체인식의 실제 응용 분야들은 대부분 극히 낮은 에러율을 요구하기 때문에, 단일 생체특징에 의한 인증 기술로는 요구되는 성능을 만족시킬 수 없는 경우가 발생한다. 이에 따라 여러 가지의 생체인식 기술을 함께 사용하여 성능을 향상시키고 신뢰도를 높이는 멀티모달 생체인식 기술들에 관한 연구가 진행되고 있다[6].

멀티모달 생체인식 기술은 다중 센서(multiple sensors), 다중 생체특징(multiple biometrics), 동일 생체특징의 다중 유닛(multiple units of the same biometric), 동일 생체특징을 여러 번 획득(multiple instances/impressions of the same biometric), 및 동일 입력 생체특




〈그림 7〉 다중 생체 인식

징 신호에 대한 다중 표현과 매칭 알고리즘 (multiple representation and matching algorithms for the same input biometric signal)으로 나눌 수 있다. 또한, 멀티모달 생체인식 시스템을 구성하기 위해서는 다중 생체정보를 활용하는 시스템의 통합 수준, 상호 보완성이 좋은 생체정보들의 조합 선택, 응용분야에 따른 생체특징의 선택, 여러 인식 결과의 직렬/병렬 이용, 구성 시스템의 비용 대 효과 분석 등에 대한 고려가 있어야 한다.

〈그림 7〉은 얼굴, 입술 움직임, 음성을 사용한 다중 생체인식의 예로, 사용자는 컴퓨터 앞에 앉아서 자신의 이름을 말하도록 되어 있다[7]. 이 시스템은 시스템 관리자가 개별 인식에 의한 결정 결과를 통합하는 방식을 선택할 수 있도록 하였다. 가능한 통합 방식은 합, 2 out of 3, 3 out of 3가 있고, 합의 경우 각 인식 모듈의 가중치와 합의 임계치를 설정할 수 있게 하였다.

## Ⅳ. 결 론

현대 정보화 사회에서 정보는 개인, 기업과 국가의 가장 중요한 자산으로 인식되고 있다. 이러한 정보는 네트워크의 발달로 인해 효과적이고 편리하게 사용이 가능하게 되었으나, 저장된 중요한 정보가 타인의 접근에 의해 파괴되거나 도용 당하는 등의 악영향을 피할 수 없는 실정이다. 본 고에서는 이러한 문제를 극복하기 위한 해결책으로 여겨지는 개개인의 고유한 신체적 또는 형태학적 특징에 따라 사람들의 신원을 확인하는 생체인식 기술에 대하여 알아보았다. 또한 실생활에 적용되기 시작한 생체인식 시스템 응용 예에 대하여 설명하였다. 앞으로는 생체인식 시스템의 성능 향상에 관한 연구뿐만 아니라 다양한 정보보호 연구 분야와의 공동 연구를 통하여 높은 보안 성능을 제공하기 위한 연구가 필요하다.

참고로 생체인식 관련 주요자료를 구할 수 있는 곳은 한국 생체인식협의회(www.biometrics.or.kr) 뿐만 아니라 The Biometric Consortium(www.biometrics.org), Association for Biometrics(www.afb.org.uk), Avanti(homepage.ntlworld.com/avanti/), International Biometric Industry Association(www.ibia.org) 등이 있다.

### 참 고 문 헌


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

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

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

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

[5] 생체측정시스템 기술/시장 보고서, 한국전자통신연구원, 2001년 12월.

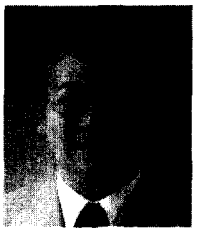
[6] 소정, 배영래, "멀티모달 생체인식 연구 현황," 한국전자통신연구원 주간기술동향, 2002년 3월.

[7] R. Frischholz and U. Dieckmann, "BioID : a multimodal biometric identification system," *IEEE Computer*, pp.64-68, Feb. 2000.

# 저 자 소 개

**潘 聲 範**

1991년 서강대학교 전자공학과 졸업, 1995년 서강대학교 전자공학과 석사, 1999년 서강대학교 전자공학과 박사, 1999년~현재 : 한국전자통신연구원 정보보호연구본부 생체인식기술연구팀 선임연구원, 〈주관심 분야 : 생체인식, 영상처리, VLSI 신호처리〉



**鄭 容 和**

1984년 한양대학교 전자통신공학과 졸업, 1986년 한양대학교 전자통신공학과 석사, 1997년 미국 Univ. of Southern California 컴퓨터공학과 박사, 1986년~현재 : 한국전자통신연구원 정보보호연구본부 생체인식기술연구팀장, 〈주관심 분야 : 생체인식, 암호알고리즘, 병렬처리 등〉

**鄭 敎 逸**

1981년 한양대학교 전자공학과 졸업, 1983년 한양대학교 산업대학원 전자계산학과 석사, 1997년 한양대학교 전자공학과 박사, 1981년~현재 : 한국전자통신연구원 정보보호연구본부 정보보호기반연구부 부장, 〈주관심 분야 : IC 카드, 정보보호, 생체인식, 신호처리〉

**金 在 熏**

1979년 연세대학교 전자공학과 졸업, 1982년 미국 Case Western Reserve Univ. 전기공학과 석사, 1984년 미국 Case Western Reserve Univ. 전기공학과 박사, 1984년~현재 : 연세대학교 기계전자공학부 교수, 〈주관심 분야 : 생체인식, 컴퓨터비전, 패턴인식, 인공지능〉