情 報 保 護 學 會 誌
第 12 券 第 2 號, 2002. 4

IC 카드 사용자 인증을 위한 Match-on-Card 기술 동향

반 성 범*, 정 용 화*, 정 교 일**, 손 승 원***

요 약

인터넷의 급속한 성장으로 인하여 안정적인 보안수준을 제공하면서 사용이 편리한 사용자 인증 시스템의 필요성이 대두되었다. 90년대까지 사용자 인증 수단으로 많이 사용되던 개인장치나 비밀번호 등은 분실 가능성 및 도용의 위험이 있어 보안이 중요한 환경에서는 사용상의 제약이 따른다. 그러므로 이러한 제약을 보완할 수 있는 생체정보를 이용한 사용자 인증에 대한 관심이 꾸준히 증가하고 있으나, 생체정보는 비밀번호와 같이 사용자가 임의로 변경할 수 없으므로 외부로 유출된다면 심각한 문제가 발생할 수 있다. 본 고에서는 생체정보를 중앙 데이터베이스에 저장하지 않고 사용자가 휴대할 수 있는 IC 카드에 저장하고, 생체정보를 이용한 사용자 인증 과정도 IC 카드 내부의 프로세서를 이용하여 수행하는 Match-on-Card 기술 개발에 관하여 설명한다.

Ⅰ. 서 론

인터넷을 이용한 글로벌 네트워크가 형성되어 정보의 수집, 분석, 가공 등이 편리하게 되었으나 개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 문제가 제기되고 있다. 또한 개인의 정보만이 손실되는 것이 아니라 국가 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 해결하기위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 형태학적 특징에 따라 사람들의 신원을 확인하는 생체인식 기술이 활발하게 연구되고 있다[1-5].

생체인식 기술의 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 않으므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다. 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. 그러므로 현재 생체인식 기술에 관한 연구는 생체정보를 획득하고 가공하여 인식하는 방법에 관한 연구가 주로 진행되고 있지만, 생체정보 등록 데이터를 중앙 DB 컴퓨터 등에 저장하지 않고 IC 카드 등에 저장하고 인식 관련 연산을 수행하여 이러한 문제를 해결할 수 있는 연구도 활발히 진행되고 있다.

본 고에서는 생체 정보를 중앙 데이터베이스에 저장하거나, 사용자 인증 연산을 수행하지 않고 개인이 소유하고 있는 IC 카드에서 개인 생체정보를 저장하고 인증 연산을 처리하여 개인 및 국가 등의 주

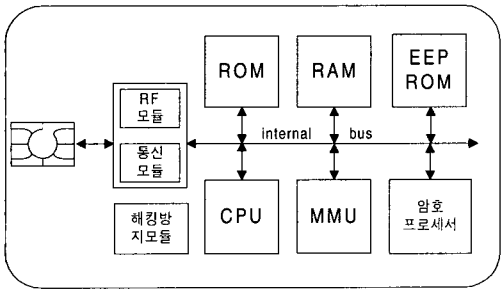
* 한국전자통신연구원 정보보호기반연구부 생체인식기술연구팀(sbpan,ywchung@etri.re.kr)
** 한국전자통신연구원 정보보호기반연구부(kyoil@etri.re.kr)
*** 한국전자통신연구원 네트워크보안연구부(swsohn@etri.re.kr)

요 정보를 타인으로부터 지킬 수 있는 기술인 IC 카드 사용자 인증을 위한 Match-on-Card 시스템에 관하여 설명한다. 본 고의 II장에서는 생체인식을 이용한 IC 카드 기반 사용자 인증 기술에 대하여 소개하고 III장에서는 지문을 이용한 Match-on-Card 시스템 구현 방법에 대하여 설명한다. IV장에서는 기술 개발 현황을 살펴본 후 V장에서 결론을 맺는다.

II. Match-on-Card 시스템

생체정보를 이용한 사용자 인증 기술은 지문과 같은 생체정보가 개인별로 고유한 특징임이 증명된 이후부터 계속적으로 사용자 인증에 이용하려는 연구가 진행되어왔다. 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. IC 카드를 이용하여 보안에 응용하는 경우 현재까지 보통 4자리 또는 6자리의 PIN 또는 패스워드를 이용하였으나 IC 카드의 계속적인 성능향상으로 인하여 앞으로는 PIN 또는 패스워드를 보완하거나 대체하기위해 생체정보를 이용한 사용자 인증 기술이 IC 카드와 결합하는 방향으로 논의가 활발히 이루어지고 있다.

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.

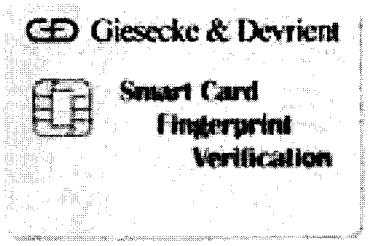


〔그림 1〕 차세대 IC 카드의 구조

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 프로세서를 사용하는 경우가 많았지만, 최근에는 다양한 응용 서비스를 수행하기 위해서 16비트 혹은 32비트 프로세서를 사용하기도 한다.

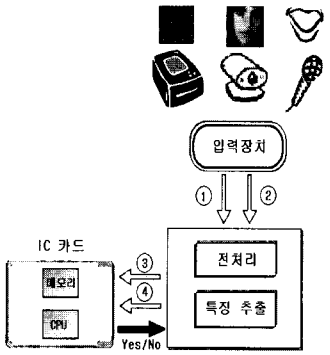
그림 1은 현재 한국전자통신연구원에서 연구 개발중인 차세대 IC 카드로서, 32비트 프로세서를 채택하고 있고 암호처리 전용 코프로세서는 비대칭키 암호 알고리즘을 고속으로 처리하며, 개방형 특성을 가지기 때문에 다양한 IC 카드 응용 서비스를 수용할 수 있다. 또한 차세대 IC 카드는 접촉식과 비접촉식을 모두 지원하는 통신 모듈을 가지며, 적정 전압과 주파수 범위를 벗어난 신호를 필터링하는 해킹 방지 모듈을 가지고 있다.

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 각각 Store-on-Card, Match-on-Card 및 Sensor-on-Card로 나눌 수 있다.



〔그림 2〕 생체인증을 위한 IC카드

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 있지 않고 IC 카드에 있다는 것이다.



〔그림 3〕 Match-on-Card 시스템

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 Store-on-Card에 저장하여 각 개인이 보유하게 함으로써 앞에서 언급한 문제 등을 해결할 수 있고, 인증 절차가 IC 카드 내의 생체정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다.

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 3의 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 사용자 인증 과정을 살펴보면 다음과 같다. 그림 3에서 ①과 ③은 사용자 등록 과정으로 입력장치로부터 생체정보를 획득한 후 전처리와 특징 추출 과정을 거친 후 IC 카드내부의 메모리에 저장된다. 그림 3의 ②와 ④는 사용자 인증 과정으로 인증을 요구한 사용자의 생체정보를 등록 과정과 마찬가지로 입력기로부터 입력 받아 특징 추출 단계 까지 거친 후 Match-on-Card에 전달한다. IC 카드는 저장되어 있던 생체 특징 정보를 이용하여 IC 카드에 내장된 프로세서에서 특징 정합을 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. 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.

Ⅲ. 지문을 이용한 Match-on-Card 시스템

생체정보를 이용한 사용자 인증 알고리즘은 기본적으로 많은 계산량과 메모리 등의 하드웨어 자원을 필요로 하지만 하드웨어 기술의 급속한 발전으로 PC 기반 생체인증 시스템은 실시간으로 동작이 가능하게 되었다. 반면에 현재 IC 카드의 하드웨어 자원은 CPU, ROM, RAM이 각각 33MHz, 64KB, 4KB으로 일반 PC의 하드웨어 자원과 큰 차이를 나타내고 있으므로 PC 기반 생체 인증 시스템을 이용하여 IC 카드 기반 생체 인증 시스템 즉, Match-on-Card 시스템을 구성하기 위해서는 필요 계산량과 메모리량에 대한 고려가 필요하다. 그러므로 본 장에서는 지문을 이용한 Match-on-Card 시스템 구현 예에 대하여 간단하게 설명한다[6].

특징점 기반 지문 인증 시스템은 지문 영상에서 특징점 정보를 추출하는 과정, 등록 및 인증 과정의 두 지문을 정렬하는 과정, 정렬된 특징점 정보를 이용하여 정합하는 과정으로 Match-on-Card에서 수행되는 정렬 및 정합과정만을 설명하면 다음과 같다.

정렬 과정에서 위치 등의 변화량을 계산해 내는 과정은 기준점의 부재로 인해 복잡하고 메모리 요구량도 클 뿐 아니라, 정렬의 정확성 여부에 따라 지문 인증 전체 시스템의 정확도가 좌우되기 때문에 중요한 부분을 차지한다. 본 예에서 사용할 정렬 방법은 등록 지문과 인증 지문 사이의 위치 차이를 테이블에 누적한 후 테이블에 누적된 가장 큰 값으로 정렬하는 방법이다. 정렬 과정에서 필요 메모리량이 가장 큰 부분은 테이블을 구성하는 것인데, 위치만을 고려한 테이블을 구성한다면 허용 위치 변화량 크기의 테이블이 필요하게 된다. 즉, 허용 위치 변

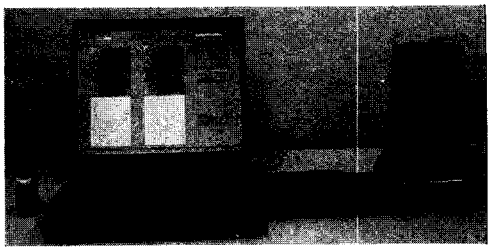
화량이 -63/+64이고 최대 누적값이 255라고 가정한다면 16,384Byte(=128×128×8)가 필요하게 된다. 그러므로 테이블 구성시 위치만을 이용하더라도 필요 메모리량이 16KB이 필요하게 되어 Match-on-Card 시스템 구현이 불가능하게 된다. 반면에 테이블 구성 시 아래와 같은 피라미드 기법을 이용하면 필요 메모리량은 4KB가 된다.

단계 1. 등록 및 인증 지문의 특징점 쌍 설정
단계 2. 두 특징점의 위치 차를 측정하여 일정 범위 내인 경우, 테이블 내 해당 빈(bin)에 누적
단계 3. 등록 및 인증 지문의 특징점 쌍을 모두 고려한 후, 가장 레벨이 큰 빈을 찾음
단계 4. 찾은 큰 빈을 중심으로 테이블 간격을 1/2로 조정 후, 단계 1~단계 3을 1회 반복함

〔표 1〕 지문 정합 알고리즘 성능 분석

	명령어수	계산시간 (ARM7)	필요 메모리량
기존 알고리즘 (Jain[7])	8M	0.13 초	400 KB
제안 알고리즘 (피라미드)	18M	0.29 초	10 KB

표 1은 피라미드 기반 빈 테이블을 이용한 지문 정렬 방법을 포함하여 개발한 지문 정합 알고리즘의 성능을 나타낸 것으로 명령어 수와 필요 메모리량은 (주)다이나릿 사에서 제공한 시뮬레이터를 사용하였다. 기존 알고리즘은 대표적인 지문인식 알고리즘인 Jain[7]의 연구를 본 논문에서 제안한 알고리즘과 같은 조건으로 구현한 것이다. 표 1에서와 같이 두 가지 알고리즘 모두 ARM7TDMI CPU에서 실시간으로 동작 가능한 명령어 수를 가진다. 제안된 피라미드 기법을 이용한 지문 인증 알고리즘은 10 KB의 메모리를 필요로 하여 기존 알고리즘에 비해 현격한 차이를 보였다. 기존 알고리즘은 많은 메모리량을 필요로 하여 IC 카드에 비해 다소 풍부한 자원을 가진 USB용 보안토큰에서 조차 동작을 할 수가 없으나, 피라미드 기법을 이용한 지문 인증 알고리즘은 USB용 보안토큰 상에서 충분히 동작 가능하다는 것을 알 수 있다. 또한 IC 카드에서도 최적화 과정을 거치면 동작이 가능할 것으로 예상한다.



〔그림 4〕 지문을 이용한 Match-on-Card 시스템

그림 4는 지문 정합 알고리즘의 하드웨어 칩 개발을 위한 지문 인증 시스템으로 여기서 ㈜다이나릿 사에서 제공한 iSAVE(in-System Algorithm Verification Engine)[8]는 본 연구에서 구현하려고 하는 IC카드를 에뮬레이션 하는 장비로서 추후 iSAVE가 추후 IC 카드로 대체되는 것이다.

Ⅳ. 기술 개발 현황

1990년대 후반부터 생체정보를 이용한 생체인식 기술과 IC 카드 기술이 접목되기 시작하여, 국가적으로 생체인식과 IC 카드를 결합한 프로젝트를 수행하는 경우가 많아지고 있고 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 있다. 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.

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 제어용

으로 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. Match-on-Card 방식의 기술 개발 사례는 Gemplus사에서 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 개발 중이다. 또한 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.

특히 2001년 미국 테러이후 생체 인식 기술을 사용자 인증 등에 사용하기 시작한 예는 다음과 같다. 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, 비자면제국들은 여권에 생체정보 저장을 의무화하는 비자면제프로그램 수정안을 법제화 중이다. 영국에서는 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 스마트 카드를 이용한 자동출입국관리 (Automated Border Crossing) 시스템"을 본격 도입하기 위하여, 2002년 1월부터 법무부 주관으로 시범 운용 중이다.

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 개발 진행되고 있다.

V. 결 론

사용자 인증의 중요정보로 사용되는 개별 인간의 생체정보가 중앙 DB에서 관리된다면 'big brother' 문제가 발생할 수 있고 생체정보 등록 단말기와 중앙 DB 사이에서의 생체정보 도난 등의 문제가 발생할 수 있으므로, IC 카드에서 개인 생체정보를 저장하고 인증 연산을 처리하여 개인 및 국가 등의 주요 정보를 타인으로부터 지킬 수 있는 기술인 IC 카드 사용자 인증을 위한 Match-on-Card 시스템에 관한 연구가 활발하게 진행되고 있다. 그러므로 본 고에서는 생체인식을 이용한 IC 카드 기반 사용자 인증 기술을 소개하고 지문을 이용한 Match-on-Card 시스템 구현 방법에 대하여 설명하였다. 또한 현재 기술 개발 현황을 간단히 소개하여 앞으로의 생체인식 기술과 IC 카드 기술의 연구방향을 제시하는데 도움이 되도록 하였다.

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 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] 반성범, 길연희, 문대성, 정용화, "사용자 인증을 위한 Match-on-Card 시스템에 관한 연구," 제2회 생체인식기술 워크샵, pp.16-20,

2002년 1월.
[7] N. Ratha, A. Jain, "A Real-Time Matching System for Large Fingerprint Database," *IEEE Trans on PAMI*, pp.799-813, 1996.
[8] iSAVE, http://www.dynalith.com.

〈著 者 紹 介〉

반 성 범 (Sung Bum Pan)
정회원

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

정 용 화 (Yongwha Chung)
정회원

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

정 교 일 (Kyo-Il Chung)
정회원

1981년 : 한양대학교 전자공학과 졸업
1983년 : 한양대학교 산업대학원 전자계산학과 석사
1997년 : 한양대학교 전자공학과 박사
1981년~현재 : 한국전자통신연구원 정보보호연구본부 정보보호기반연구부 부장
관심분야 : IC카드, 정보보호, 생체인식, 신호처리

손 승 원 (Sung-Won Sohn)
정회원

1984년 : 경북대학교 전자공학과 졸업
1994년 : 연세대학교 전자공학과 석사
1999년 : 충북대학교 컴퓨터공학과 박사
1991년~현재 : 한국전자통신연구원 네트워크보안연구부 부장
관심분야 : 네트워크 보안, 라우팅 알고리즘, 생체인식