스마트카드 인증 시스템

손인구, 민경진, 조영우, 유기영
경북대학교 컴퓨터공학과
e-mail:sig3@infosec.knu.ac.kr

Smartcard Authentication System

In-Gu Son, Kyung-Jin Min, Young-Woo Cho, Ki-Young Yoo
Dept of Computer Engineering, Kyungpook National University

요 약

본 논문에서는 다양한 응용 분야에 이용되는 스마트 카드의 효율성과 보안성을 높이기 위하여 스마트 카드와 단말기간의 인증을 설계하였다. 기존의 스마트 카드와 단말기의 PIN 인증을 이용하지 않고, 스마트 카드가 단말기간에는 지문 인증을 수행하도록 하여 보안성을 높였고, 스마트 카드내에 저장된 지문의 정보를 효율적으로 최소화하여 저장함으로서 스마트 카드의 저장공간을 최소화시키는 동시에 단말기 상에서 입력된 지문과 스마트 카드 내에 지문이 매칭될 때 발생하는 계산 부하도 줄일 수 있다. 제안된 인증시스템은 무선 단말기와 같은 장비를 인증하기에 적당하다.

1. 서론

차세대 디지털 기술을 대표하는 무선 인터넷과 M-commerce 가 점차 활성화되고 있는 추세에 있고, 이에 따라 무선 단말기에 대한 보안의 필요성이 증대되고 있다. 기존의 단말기 인증 방법은 개인이 배타적으로 알고 있는 지식, 예를 들면 패스워드나 PIN(Personal Identification Number)을 사용하는 방법과 ID 카드나 열쇠 같은 개인이 소지할 수 있는 물건을 통해 이루어 졌으나, 이러한 방법은 타인에 의한 도용이나 분실, 망각의 위험이 있어 높은 수준의 보안을 보장할 수 없으므로 높은 수준의 보안을 요하는 인증 시스템에 적용하는데 문제점이 있다.

이러한 문제점을 해결하기 위해 생체 인식과 스마트 카드를 이용한 보안 기술이 적용될 수 있다. 생체 인식(biometrics)은 각 개인마다 다른 신체적 특징을 다른 사람과 구별해 개인을 인증하는 기술이다. 생체 인식의 예로는 홍채 인식, 정맥 인식, 지문 인식, 음성 인식 등 아주 다양하며, 이들은 신체의 일부분이므로 패스워드처럼 잊어버리거나 도난, 복사 혹은 공유가 되지 않는다. 그러므로 사용자 인증에 있어 신뢰성 있는 보안을 제공한다. 그 중에서 지문 인식은 정확도가 높고, 편의성이 뛰어나며 여러 측면에서 가격 대 성능비가 탁월하기 때문에 사용 범위가 아주 넓다. 하지만 이러한 장점을 지닌 생체 인식 정보가 데이터 서버에 저장되어 이용되면 해킹이나 분실의 위험이 있으므로 생체정보는 서버에 저장되지 않고 스마트 카드나 USB 토큰 등에 저장되어 이용될 수 있다[1][2].

스마트 카드는 1974년 프랑스에서 최초로 개발된 이후, 1986년 스마트 카드 표준안인 ISO-7816이 등장하기까지 은행카드로 사용되기 시작하였다. 90년대에 들어서는 전 세계적으로 스마트 카드의 시장이 빠르게 확장되어 가고 있는 추세이다. 이러한 스마트 카드는 허락되지 않은 사용자에게 도움이 될 수 없도록 하는 보안성을 가지는 것이 매우 중요하며, 생체 인식과 연계하여 정보의 보안성을 더욱 높일 수 있는 매개체이다.[3]

본 논문에서는 스마트 카드 내에 저장되는 지문 정보와 단말기 상에서 입력되는 지문들간의 매칭을

통한 인증을 수행하는 스마트 카드 인증시스템을 설계하고 구현하였다. 이를 위하여 스마트 카드 내에 지문의 특징점들을 저장하는 방법과 지문 인식 시스템에서 지문 매칭 방법을 제안하였다. 제안된 시스템은 스마트 카드에 저장될 지문의 정보를 최소화 시켜서 스마트 카드의 적은 메모리에 이용하기에 용이하며, 지문 인식 시스템에서 입력된 지문과 스마트 카드 내의 지문 정보가 매칭될 때 보다 빠르고 효율적인 매칭작업이 수행된다.

본 논문의 구성은 다음과 같다. 2절에서는 지문인증 방법과 스마트 카드에 대해서 소개한다. 3절에서는 본 논문에서 제안하는 인증 시스템의 구조 및 인증과정을 설명하고, 4절은 구현 및 결과에 대해서 설명한다. 마지막으로 5절에서 결론으로 끝을 맺는다.

2. 관련연구

본 장에서는 스마트 카드 인증 시스템에서 필요한 지문 인식 시스템과 스마트 카드에 대하여 기술한다.

2.1 지문 인식 시스템

과거에는 손가락에 잉크를 바르고 종이에 찍어 지문 지문을 채취하고 지문 감식 전문가에 의해 지문 인증이 이루어졌다. 따라서 대규모의 자료에서 검색이 필요한 지문을 이용한 범인 조회와 같은 일대다 시스템에서 지문을 인증하는 것은 시간과 비용이 많이 소요되는 작업이었다. 그러나 지문을 입력받을 수 있는 live- scan 방식의 지문 입력기가 개발되고 전기 및 전자 기술이 발전됨에 따라 컴퓨터로 지문을 인식할 수 있는 AFIS가 개발되어 지문은 범죄 수사뿐만 아니라 개인을 인증하기 위한 수단으로 사용되기 시작했다.

자동 지문 인식 시스템은 아래 그림1 에서와 같이 크게 두 단계의 처리 과정을 거친다. 등록 모듈은 특징 추출기로 이루어지고 인증 모듈은 특징 추출기와 비교기로 구성된다. 사용자의 지문을 지문 입력기를 통해 입력받아 특징 추출기로 영상을 처리하여 특징점을 추출해 등록해 두고, 사용자의 인증이 필요한 시점에서 다시 지문을 입력받아 똑같은 처리 과정으로 특징점을 추출하여 비교기로 두 지문의 특징점을 비교하여 사용자의 신원을 인증하게 된다.

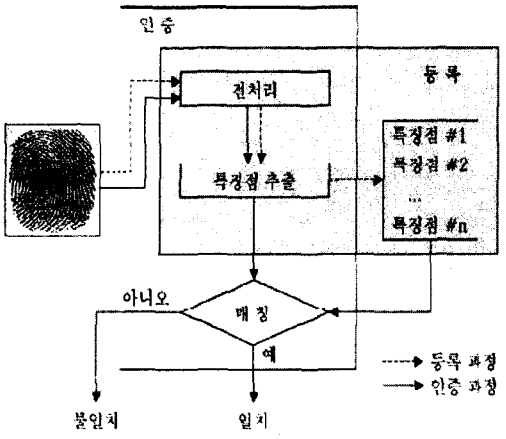

그림1. 자동 지문인식 시스템

특징점 추출 과정은 대체로 그림 2와 같이 4단계로 구성된다. 각 단계는 (1)원시 입력 지문 영상의 품질을 향상시키는 전처리 과정, (2)융선의 방향성분을 찾아내는 방향성 추출 과정, (3)융선과 골을 0과 1의 흑백 영상으로 이진화하여 융선을 굵기가 1인 선으로 세선화하는 과정 그리고 (4)세선화된 영상에서 특징점을 검출하는 과정이다[1].

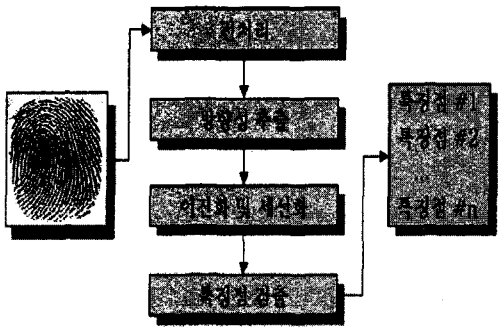

그림 2. 지문 특징 추출기

2.2 스마트카드

스마트 카드는 기존의 플라스틱 카드에 마이크로프로 세서와 메모리 등을 내장한 IC 칩과 8개의 접속단자를 통하여 외부의 카드 리더기로부터 전원 및 데이터 송수신을 하는 독립된 연산장치이다. 이는 각별한 보안을 필요로 하는 전자 상거래와 전자 지

갑 등의 응용 분야에서 사용된다. 그리고 스마트 카드 리더기간의 인증, 명령어 처리, 명령어 처리시의 보안 유지 등의 작업을 수행한다. 이러한 작업을 수행하기 위해서 스마트 카드 운영체제는 카드와 카드 리더기와의 통신, 비휘발성 메모리에 데이터 쓰기, 읽기, 지우기 등의 기본적인 기능과 보안 유지를 위한 암호화 기능을 수행하여야 한다[4][5].

아래의 그림 3은 스마트 카드와 리더기 간의 데이터 전송을 나타내고 있다.

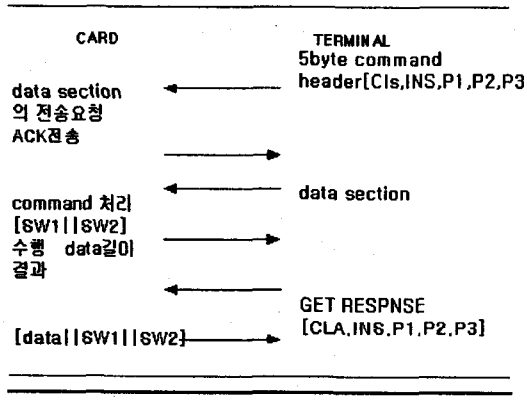

그림 3. 단말기와 카드간의 데이터 전송 과정

3. 인증 시스템 설계

본 장에서는 제안된 시스템의 전체적인 구조와 구체적인 인증의 과정들을 설명한다.

3.1 제안된 시스템의 구조

본 논문에서 제안하는 전체 시스템은 아래 그림 4와 같다. 사용자의 지문 정보인 특징점들이 입력된 스마트 카드와 지문센서가 갖추어진 단말기로 구성되어 있다.

현재 스마트카드의 안정성을 위해선 스마트 카드와 단말기간에 PIN매칭을 수행한다. 그러나 정당한 사용자가 아닐지라도 인증과정을 수행하는데 문제가 없을 수 있다. 이러한 문제는 지문 인증 기술로 어느 정도 해결이 가능하지만 스마트 카드에 저장할 수 있는 정보량의 한계와 매칭과정이 수행될 때 야기되는 계산 부하가 문제를 발생시킬 수 있다. 이러한 문제를 해결해 보고자 본 논문은 스마트 카드에 저장될 지문 정보와 단말기에서 지문 이미지를 처리하는 과정에서 평균 위치를 고려하여 문제를 해결해 보고자 하였다.

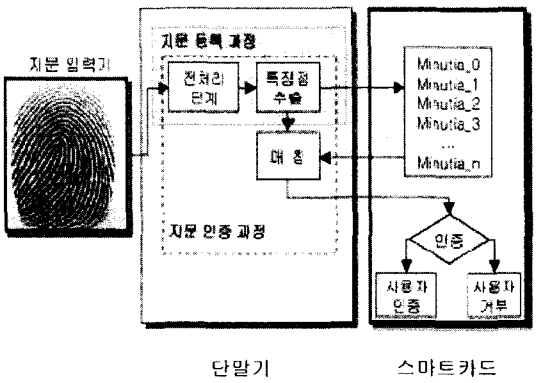

그림 3. 스마트카드 인증시스템

3. 2 제안된 방법

우선적으로 우리가 고려한 것은 스마트 카드 내에 최소한의 정보를 입력함으로서 스마트 카드 내에 최소한의 메모리를 사용하여 스마트 카드를 효율적으로 사용하도록 만들고자 하는 것이었다. 보통 선명한 지문에서는 특징점의 개수가 50 - 70개 정도 추출되어 진다. 본 논문은 추출된 특징점을 모두 스마트 카드에 저장하지 않도록 하였다. 대신 추출된 특징점에서 평균 위치를 찾아서 평균위치를 중심으로 모여 있는 특징점들을 30 - 35개 정도 추출하여 스마트 카드 내에 저장하였다.

평균위치(MP)는 2차원 좌표로서 (MP_X, MP_Y)로 구성되어 있고,

$$MP\_X = \sum Xi/N \qquad (1)$$
$$MP\_Y = \sum Yi/N$$

이때 X_i는 i번째 특징점들의 x축 좌표값이고, Y_i는 i번째 특징점들의 y축 좌표값이다. N은 스마트 카드에 등록될 특징점들의 전체 개수이다. 이러한 방법으로 추출된 특징점들은 단말기 상으로 전송이 되어진 후 단말기 상에서 입력받은 지문과 매칭이 이루어 진다.

지문 매칭이 수행될 단말기에서는 지문이 입력될 때 전처리 작업을 거친 후 지문의 특징점을 추출하게 된다. 이때 추출한 특징점은 스마트 카드에서 전송된 특징점과 elastic 매칭 알고리즘을 통해서 처리된다[6]. 이 때 단말기에서도 식(1)과 같이 평균 위치를 중심으로 한 200*200 픽셀의 지문 영상만

추출해서 처리하게 된다. 보통 지문은 400*400 픽셀의 지문 영상을 처리하지만 본 논문에서는 평균 위치를 중심으로 매칭에 충분한 특징점을 얻을 수 있을 것이라는 가정 아래 이와 같은 방법으로 구현해서 실험해 보았다.

4. 실험 및 결과

실험을 위해서 COS(Card Operating System)를 우선적으로 개발하였다. ISO/IEC 7816-1,2,3,4 에 기반한 T=0 프로토콜로 데이터를 전송하도록 구현하였으며, 개발한 COS모듈을 8051보드에 탑재하였다. 그리고 단말기에 이용될 지문 프로그램을 개발하였으며, elastic 매칭을 통한 실험을 수행하였다. 입력된 지문은 서로 다른 지문 100쌍을 입력받아 실험을 진행시켰으며, 이 때 실험은 제안한 방법을 통해서 매칭한 결과와 스마트 카드내에 추출한 모든 특징점을 삽입해서 400*400 픽셀의 지문 이미지를 elastic 매칭한 결과를 비교 분석하였다. 실험결과, 제안한 방법에서 매칭의 정확도는 elastic 매칭만 사용한 모듈에 약 95%정도의 성공률을 보였고, 지문 매칭의 처리속도는 감소하는 것을 확인 할 수 있었다.

5. 결론

본 논문에서는 보안성과 효율성을 높이는 스마트 카드 인증 시스템을 구축하였다. 보안성을 높이기 위해서 기존의 PIN 매칭을 이용하지 않고, 지문 인식을 적용하였으며, 효율성을 높이기 위해서는 스마트 카드 내에 개인에게서 획득할 수 있는 모든 지문의 특징점들을 입력하지 않고, 평균 위치를 구하여 그 위치를 중심으로 어느 정도의 특징점만을 구하여 입력하도록 하였다. 또 지문 매칭이 수행될 단말기 상에서는 스캔하여 지문의 특징점들을 구할 이미지의 크기를 줄여서 단말기의 계산량을 줄이는 동시에 매칭시에 처리속도의 개선도 이루어졌다. 이러한 시스템이 주는 장점은 단말기를 인증하는데 있어서 스마트 카드를 이용하여 보다 안전하고, 응용되는 분야가 많을 것이라고 기대된다. 특히, 효율적인 인증을 수행해야 하는 뱅킹, 전자 지불, 증권 거래 등 다양한 금융 거래와 효율적인 단말기 상에서의 처리가 요구되는 분야에서 이용하기에 적합하다.

향후 연구과제로 우리가 제안한 시스템에서 원거리 응용 서버에 대한 인증 수행의 프로토콜을 추가하여 보다 발전된 시스템이 필요하다.

참고문헌

[1] 류시룡, "지문의 특징점과 방향성 정보를 이용한 매칭 방법", 경북대학교 석사 학위 논문, 2002

[2] 최정호, "데이터보안을 위한 생체측정 보안시스템", 경영과 컴퓨터,1992

[3] 배재형, "자동지문인식(AFI)을 이용한 자바카드 인증 시스템", 경북대학교 석사 학위 논문, 2001

[4] 김증섭, 조병호, 김효철, 이종국, 유기영, "다양한 응용을 위한 스마트카드 운영체제", 정보과학회논문지, 2002

[5] W. Rankl, W. Effing, "Smart Card Handbook", WILEY-VCH, 2000

[6] Kalle Karu, Shaoyun Chen, Anil K. Jain, "A Real-Time Matching System for Large Fingerprint Databases", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 1996