지문인식을 이용한 기본형 보안 시스템에 관한 연구

구하성*, 김진태*, 박길철**

*한서대학교 컴퓨터과학과, **한남대학교 멀티미디어대학

A Study on the Prototype Secure System using Fingerprint Recognition

Hasung Koo, Jintae Kim, Gilcheol Park

Hanseo Univ. Department of Computer Science,

Hannam Univ. College of multimedia

요약

최근들어 컴퓨터와 네트워크의 발전으로 일상업무의 대부분을 컴퓨터를 이용하여 할 수 있으므로 신원 확인은 중요한 분야로 부상되었으며, 지문은 편리한 입력과 종생불변하고 만인부동한 특성으로 생체 측정 분야 중 가장 각광받고 있는 분야가 되었으다. 근래에 반도체 지문 입력장치의 개발로 인하여 크기와 속도 문제를 해결하므로써, 키보드, 마우스 등에 부착하여 네트워크의 신원확인과 인증에 많은 수요가 예상된다. 본 논문에서는 반도체 입력 장치를 이용한 지문 인식기술과 암호학을 접목하여 지문을 이용한 신원확인과 인증하여 기본형 보안 시스템 적용에 관해 연구하였다.

I. 서 론

컴퓨터 네트워크가 점점 발전함에 따라 일상업무 뿐만 아니라 보안을 유지하여야 하는 정보들도 네트워킹 환경에서 주고 받을 필요성이 증가하고 있다. 이의 해결 방법으로 많은 정보 보호 기술이 개발되고 있으며, 그 중 하나의 방법으로 신체의 특성을 이용하는 생체측정학 역시 매우 중요한 기술 분야로 발전되고 있다. 인간의 신체에는 여러 개의 특징이 있으나 그 중 얼굴, 음문, 홍채, 망막, 족문, 손금, 지문, 서명, 족문 등이 쓰이고 있다. 아래의 표1은 최근들어 개발되고 있는 신체측정의 방법에 대한 도표이다. 지문은 도표에서 설명한 바와 같이 입력의 편리성과 데이터의 불변성 그리고 도용의 힘들기 때문에 신체측정의 여러 분야 중 가장 활발하게 발전되고 있으며 가장 많이 상용화되고 있다.

지문은 만인 부동하고 종생불변한 특성을 가지고 있으므로 아주 오래전부터 연구되고 사용되었으나 지문 관련 최초의 학계 발표는 1684년 N. Grew가 영국에 제출한 것으로 알려져 있다. 그후 1900년대에 Galton이 형태학상 3가지 분류를 하였으며, Henry가 지문 분류법을 지문 융선의 전체적인 흐름과 중심점(core)와 델타(delta)를 이용하여 체계적으로 분류하였다.

지문의 이용 방법으로는 크게 지문키와 같이 본인만을 확인하는 1: 1 매칭 방법과 신분이 밝혀지지 않은 유류 지문을 대상으로 후보자군에서 유류지문의 신원을 밝혀주는 1: 多 매칭 방법으로 나뉘어 진다. 1: 1 매칭의 경우 주로 지문을 이용한 금고키나 전자상거래시 본인 확인 등의 응용분야가 나뉘고 전자 주민증에 지문 데이터가 들어갈 경우 그 응용 범위가 매우 넓어 질 것으로 예상된다. 1: 多의 경우 범인이 현장에 남기고간 유류 지문을 이미 구축되어 있는 데이터베이스(Database)에서 범인 후보를 색출해주는 시스템으로 이용되고 있으다. 이러한 AFIS 기술의 발전으로 지문 인식 기술은 많은 발전이 있었으나, 사람의 지문을 직접 입력받는 지문 입력 획득기가 프리즘을 이용하는 방식으로 지문을 입력받기 위해 손가락을 프리즘에 접촉을 하면, 그 흔적이 남아 특수한 액체를 뿌리고 고무 성분으로 흔적

을 채취하는 물리적 방법이 매우 용이했으므로 보안상의 문제를 완전히 해결하지 못하였다. 그러나, 최근들어 반도체를 이용한 지문 인식 방법이 개발되어 이 입력 방식을 이용하면 지문을 반도체에 접촉한 다음에도 지문이거의 남지 않아 물리적인 도용이 거의 불가능하므로 보안의 어려움을 해결하였으며, 입력 장치의 크기 역시 매우 소형화되어 지문 인식 연구에 매우 획기적인 전환을 가져왔다. 지문의 인식과정은 지문에서 추출된 특징 데이터를 200byte로 패킹(packing)하고, 이 패킹된 데이터들이 server의 데이터베이스에 저장되었다가 단말에서 지문 비교 요구가 요청되면 매칭(matching)과정을 통해 신원확인과 인증을 하게된다. 이 과정에서 주전산기의 지문 데이터베이스가 해킹될 위험 소지를 안고 있으므로 지문의 추출 데이터의 암호화가 필요하게 되나, 지문 인식 연구는 화상처리 및 인식 분야이고, 암호화 역시 암호학이라는 서로 다른 분야에서 연구 되어 왔기 때문에 지문의 암호화와 관련된 연구는 전무한 실정이다. 본 논문에서는 반도체를 이용한 지문 인식 방법과 추출된 지문의 특징 데이터를 server에 암호와 하여 저장하는 방법에 대하여 제안하였다. 본 논문은 II장에서 반도체를 이용한 지문의 특징점 추출과 매칭에 관해서 설명하였으며, III장은 지문을 통한 신원확인,인증 그리고 win95/98에 쓰이는 기본형 secure 시스템에 관한 설계를 IV장은 결론으로 구성된다.

II. 특징점 추출과 매칭

1:1 이나 1: few 매칭시스템에서는 지문 감식 시스템에서 쓰이는 분류기법은 쓰이지 않는다. 그러므로 이장에서는 지문의 특징점 추출과 매칭에 관하여 기술한다.

2.1. 특징점 추출

다양한 조건 및 잡음이 석인 지문 화상으로부터 그 지문의 특성을 규정 지울 수 있는 융선의 특이점이 있으며, 추출과정의 전체 블록도는 그림 1에서 나타 내었다.

위의 그림에서 단점은 융선이 시작되거나 끝나는 점이며, 분기점은 융선이 갈라지는 곳이며, 중심점은 지문의 융선중 방향이 가장 급격하게 변하는 곳이며, 삼각주는 융선의 흐름이 세방향으로 나뉘어지는 곳을 말한다. 이러한 특징점의 추출은 다음과 같은 단계를 거친다.

1) 원화상 입력

2) 입력영상의 Noise 제거 및 Normalization

3) 전경과 배경의 분리 및 융선 방향 추출

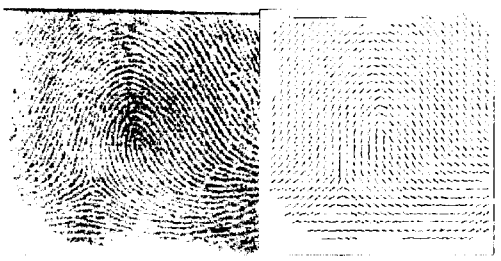
4) 여러 가지 필터에 의한 gray level 화상의 이진화

5) 이진 화상의 세선화 및 세선화 후 잡음 제거

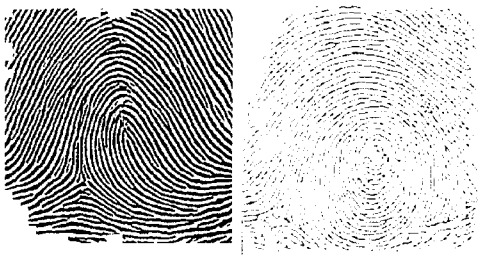
6) 방향성분을 이용한 중심점과 삼각주 검출

7) 특징점과 특징점의 방향 성분 추출 및 특징점 주위의 융선 밀도 검출

그림1에서는 위의 여러 단계중 중요한 단계를 나타내었으며, 특징점 추출에서의 가장 중요한 기술로는 사람에 따라서 나타날 수 있는 지문상의 잔주름과 잡음에 강한 추출 방법을 택하는 것이다.



a) 원영상 b) 방향추출 영상



c) 이진화 영상 d) 세선화 영상

그림 1. 특징점 추출 과정

2-2. 지문의 매칭기술

지문은 아래와 같은 변형을 가지게 된다.

1) 밀리는 효과에 의해서 좌표 변환이 일어나는 경우로서 같은 지문을 여러번 취득하더라도 피부의 유연성에 기인하여 특징점의 좌표값이 틀려지게 된다.

2) 지문이 회전된 경우로서 이는 전체적인 회전과 부분적인 회전이 일어나게 된다.

3) 부분적인 밀림 또는 왜곡에 의해서 1)번과 2)번 현상이 국부적으로 다르게 발생하는 경우가 많다.

4) 지문 입력시 받아들이지 못한 부분에 의하여 특징점이 소멸되거나 잡음에 의하여 없는 특징점이 추가되는 경우가 발생한다.

위의 현상이 복합적으로 일어나는 것이 지문 영상이므로 이상적인 매칭 알고리듬을 구현하기 위해서는 다음과 같은 조건을 가져야 한다.

1) 빠진점이 있거나 잡음에 의해 추가된 특징점이 있더라도 이의 영향을 최소화하여야 한다.

2) 지문 입력시 흔히 일어나는 밀림 현상에 유연한 알고리듬이 되어야 한다.

3) 지문의 회전에 관한 영향을 최소화한다.

4) 상대적인 특징점의 개수 차이에 따른 영향을 최소화한다.

5) 단순히 특징점의 수적 우세가 매칭시 유리한 요소로 작용하지 않도록 한다.

지문 매칭 알고리듬은 특징점이 추출되고 난 뒤 이루어지는 단계로서 지문에 가장 특화된 알고리듬이다. 일반적인 경우 1:1 매칭시에는 타인을 본인으로 판단하는 TYPE I ERROR가 0%에 가까운 성능을 가져야 하며, 1:many인 경우 타인을 본인으로 판단하는 경우에는 관대하나 본인을 본인으로 판단하지 못하는 TYPE II ERROR에는 매우 엄격한 오류 허용률을 가져야 한다. 또한, 1:1인 경우 본인 비교만 이루어지는 형식으로서 특징점의 모든 분포를 고려해 단계별로 비교하지만 1:many 인 경우 100만 이상의 지문을 매칭하기 위해서는 가능한한 매칭의 전처리 단계에서 단순 비교하여 후보군을 줄여야 한다. 이런 견지에서 분류를 이용하며, 매칭의 전처리 단계에서 특정 후보군을 제외시키는 알고리듬의 설계가 요구된다. 일반적으로 매칭 알고리듬은 특징점간의 기하적으로 구성된 그래프 패턴의 비교 산정과 특징점의 x축과 y축의 위치와 특징점과 융선과의 비교를 통해 특징점의 방향 성분을 추출하여 이용한다.

III. 지문을 이용한 신원확인과 인증

3.1 지문 인식 장치

기존의 프리즘을 이용한 지문 입력 장치는 사람이 지문을 인식하기 위해 손가락을 프리즘에 접촉을 하면, 그 흔적이 남아 특수한 액체를 뿌리고 고무 성분으로 흔적을 채취하는 물리적 방법이 매우 용이했다. 그러나, 그림 2에 나타난 반도체 입력 방식을 이용하면 지문을 반도체에 접촉한 다음에도 지문이 거의 남지 않아 물리적인 도용이 거의 불가능하다. 또한, 프리즘을 이용한 방식은 camera와 프레임 그래버를 이용하여야 하기 때문에 크기가 마우스 키보드에 삽입하기에 매우 불편하나, 반도체 입력 방식은 그림 2에 나타난 것과 같이 두께가 매우 가늘며, 전체적인 크기가 세로X가로X높이가 39mmX69mmX2mm로 매우 적어 그림 3와 같이 마우스와 키보드에 삽입이 가능하다.

3.2 사용자 ID를 이용한 일반적 식별 인증

서버 또는 호스트 컴퓨터에 대한 사용자의 신원확인 및 인증 방법은 일반적으로 다음과 같은 방법으로 이루어진다. 그림 4는 사용자가 ID와 Password를 입력하고 server를 통하여 신원 확인과 인증을 하는 일반적인 log on 과정을 나타내고 있다. 이 방법은 사용자 ID와 패스워드를 이용하는 것으로, 서버에서 유일하게 부여된 ID는 사용자의 식별 정보가 되며, 로그 온 될 때 입력되는 패스워드는 이미 서버에 저장되어 있는 패스워드와의 매칭을 통하여 그 사용자의 신원을 인증하는 방법으로써, 기존 많은 시스템에서 일반적으로 사용되는 방법이다. 대표적인 예로서 UNIX 시스템의 경우에는 서버에서 사용자의 패스워드를 보호하기 위해서 DES 암호 알고리즘을 이용하여 처음에 입력하는 패스워드를 암호화한 후 Salt(실시간과 프로세스 ID로부터 생성된 12비

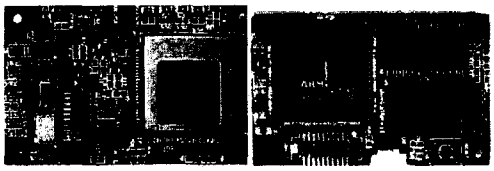


그림 2. 지문 입력용 반도체

그림 3. 지문 입력용 마우스와 키보드

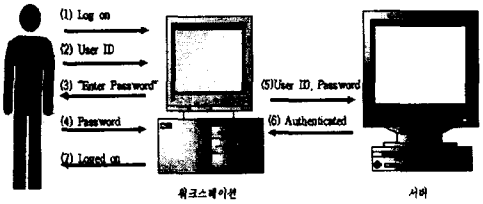


그림 4. ID와 패스워드를 이용한 로그온 절차

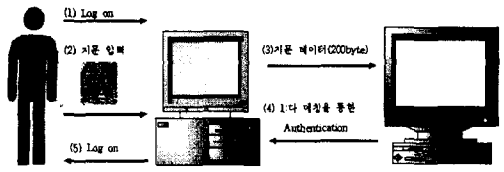


그림 5. 지문만을 이용한 로그 온 절차

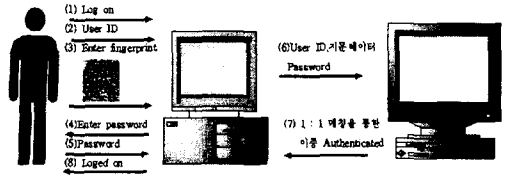


그림 6. 사용자 ID, 지문과 패스워드를 모두 이용한 로그 온 절차

트)와 같이 Shadow 파일에 저장한다. 이 Salt를 사용하는 이유는 동일한 패스워드가 존재할 때 암호화된 패스워드 들이 동일하게 나타남을 방지하기 위해서이다. 다음 로그 온 시에 입력되는 사용자의 패스워드를 같은 암호 알고리즘으로 암호화한 후 이미 Shadow 파일에 저장되어 있는 암호화된 패스워드와 일치하는 경우 사용자를 정상적으로 인증하게 된다.

3.3 지문을 이용한 식별 및 인증 방법

지문을 이용하는 경우에는 클라이언트에서 추출된 지문 자체가 다른 사용자와 다르다는 특징으로 서버 내에서 다른 사용자에 대해 유일하므로, 그 지문 자체만으로 사용자 ID가 될 수 있다. 또한 일반적인 패스워드 같이 문자 · 숫자 · 특수문자 등으로 구성된 것이 아니므로 해커나 공격자에게 누출될 가능성이 적어 패스워드와 같은 역할도 할 수 있다. 따라서 지문을 서버의 사용자 식별 인증에 이용하는 경우, 다음과 같이 여러 가지 방법으로 여러 응용 분야의 환경에 따라서 사용자 식별 및 인증이 가능 할 것이다.

3.3.1 사용자의 ID와 지문을 이용한 사용자 식별 인증

지문을 입력할 때의 log on 과정을 나타낸 것으로 클라이언트로부터 ID와 지문을 동시에 입력을 받아 신원 확인과 인증을 행하는 것으로 ID를 통하여 server 상에 등록된 본인의 지문 추출 데이터만을 택하여 매칭 과정을 행하는 것으로 server 상에서는 단순히 1: 1 매칭만을 행하는 것으로 인증 속도가 매우 빠르다.

3.3.2 지문과 패스워드를 이용한 사용자 식별 인증

다단계 인증을 요구하는 경우 사용될 수 있는 방법으로 지문을 통한 유일한 사용자 식별과 1단계 인증 및 패스워드를 통한 2단계 인증을 실행할 수 있다. 이 경우 사용자가 패스워드를 암기함으로써 신변의 안전을 도모할 수 있다는 장점이 있는 반면, 인증 절차의 복잡성과 식별 인증에 소요되는 시간이 비교적 느리다는 단점이 존재한다. 그러나 고도의 철저한 인증이 요구되는 시스템에서 활용될 수 있을 것이다. 이러한 방법은 컴퓨터 시스템의 경우, 인증 후에 사용자 프로세스의 관리 측면에서 구현이 어렵게 된다.

3.3.3 지문만을 이용한 사용자 식별 인증

그림 5은 ID와 Password 모두를 지문 입력으로 대치하는 경우로 network의 보안 측면에서 볼 때에는 매우 안전도가 높은 방법이나 server 측면에서는 ID를 받지 않았기 때문에 등록된 모든 지문과 매칭을 행하여 인증을 하여야 한다. 이 경우 인증에서 소요되는 시간은 pentium 166MHz 상에서 지문의 상태에 따라 약간의 오차는 가지나 한 지문 비교당 0.1초내의 시간이 소요되므로 등록된 인원에 비례하여 시간이 많이 소용되는 단점을 가지게 된다.

3.3.4 사용자 ID, 패스워드, 지문을 이용한 식별 인증

사용자의 Id, 패스워드, 지문을 모두 이용하는 방법으로, 지문과 패스워드를 이용하는 고도의 보안을 요구하는 시스템의 다단계 인증 방법의 매칭 절차에 있어 소요되는 시간을 줄일 수 있는 장점과 사용자의 신변을 보호할 수 있다는 장점을 가질 수 있다. 즉, 사용자의 ID를 가지고 사용자를 식별한 후, 지문으로 1차의 인증을 실시하고 패스워드를 이용하여 2단계의 인증을 비교적 빨리 수행할 수 있다. 빠른 속도가 요구되는 고도의 인증을 필요로 하는 응용 환경에서 이용될 수 있을 것이다. 그림 6은 이 과정을 보여 주고 있다.

3.4 안전성 고찰

log on 과정에서 클라이언트로부터 ID와 지문을 동시에 입력을 받아 서버와 데이터 전송을 하면서 신원 확인과 인증을 행하는 경우, ID를 통하여 server 상에 등록된 본인의 지문 추출 데이터만을 택하여 지문 매칭 알고리즘을 통해서 매칭을 행하는 것으로 server 상에서는 단순히 1: 1 매칭만을 행하게 된다. 이 경우에 인증 속도가 매우 빠르기는 하나, 클라이언트와 서버와의 인증 과정에서 ID와 해당 사용자의 지문 데이터를 해커가 가로챌 경우, 다음 로그 온 시 가로챈 사용

자의 ID와 지문 데이터의 재 입력을 통하여 불법 침투가 가능해질 수 있는 재생 공격(Replay Attack) 위험이 존재할 수 있다. 또 다른 위험으로서는, 서버 내부에서 사용자의 지문 데이터가 암호화 절차 없이 그대로 저장될 경우에는 해당 사용자의 지문 데이터의 변조 및 노출이 용이해질 수 있다. 따라서 지문 데이터를 서버에 저장 관리하는 경우, 암호화를 통하여 이를 저장한 후, 사용자의 다음 로그 인 시에 매칭을 위해서 암호화된 지문 데이터를 복호화한 후 지문 매칭 알고리즘에 의해서 매칭이 실행될 수 있다. 매번 로그 온 할 때마다 암호화된 사용자의 지문 데이터를 복호화를 해야되는 이유는, 매번 사용자로부터 추출되어 입력되는 지문 입력 데이터의 비트 스트림이 저장된 지문 데이터와 똑 같지 않을 수 있기 때문이다. 따라서 복호화되는 지문 데이터는 매칭이 실행된 후 파기 과정이 실행되도록 설계되어야 한다. 한편, 서버 내에서 패스워드의 저장과 인증 방법은 Unix 시스템에서와 같이 최초 패스워드 등록 시 이를 단방향 암호화 방식(One-way encryption)으로 암호화하여 파일로 저장한 후, 다음의 로그 온 시마다 암호화한 데이터를 가지고 이미 저장된 암호화된 패스워드와 일치여부를 판단하여 인증이 실행될 수 있다. 따라서 이때는 복호화가 불필요하다는 장점이 있다.

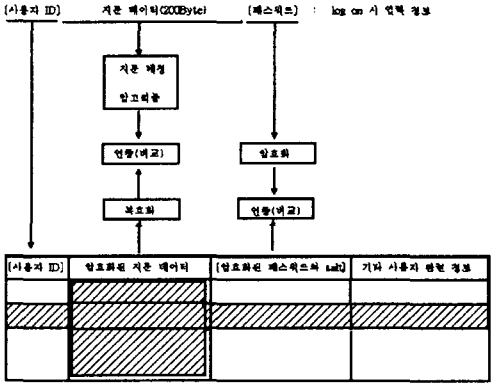


그림 7. 지문 및 패스워드 파일을 통한 인증

3.4 Win 95/98을 이용한 PC 기본형 보안시스템의 구현

*windows 95/98*에서 기본형 보안 시스템을 구현하기 위해서는 다음과 같은 점들이 고려되어야 한다.

1) log on시 패스워드 또는 지문데이타로 사용자를 확인하는 기능

2) administrator를 새로 수정하거나 새로 생성하는 기능

3) 디렉토리나 파일 자체를 암호화하거나 복호화하는 기능

4) 화면보호기를 지문을 통해 사용자를 확인하는 기능

5) 여러명의 사용자가 사용 가능하므로 각 사용자 권한을 주는 기능

6) 보호 모드를 위한 access control 기능

7) 도스 모드에서 dir로 보았을 때 파일의 고유 이름을 변경하여 정보를 숨기는 기능

windows 95/98은 windows NT와 틀리므로 사용자의 access control 기능이 매우 취약하므로 암호와 복호화 기능이 매우 중요하며, windows NT에서는 암호와 기능의 역할은 상대적으로 비중이 적으며 access control 기능에 더욱 더 비중을 두어 개발하여야 할 것이다.

VI. 결 론

지문은 사람의 신체의 특성을 이용하는 것으로 도용이 거의 불가능하다는 장점을 가지고 있으므로 최근들어 많이 연구되어 지는 정보 보호 학문의 한 분야로 충분한 가치가 있다고 생각된다. 지문을 이용함에 있어 지문키의 경우 보다 저렴한 가격에 빠른 알고리듬으로 발전 되어야 하며, 최근들어 지문 전용 입력 반도체의 개발로 발전 속도가 가속화 되고 있다. 본 논문에서는 지문과 암호를 이용하여 지문을 이용한 신원 확인과 인증을 행하고, 해캥의 위험에 대비하여 서버상의 자료를 단방향 암호화 방식으로 암호화하므로써 매우 높은 보안성을 가지는 시스템을 제안하였다. 차후의 연구과제로는 제안한 방식을 직접 구현하여 실제 상황에서 테스트하여야 하며, 전자상거래 등에 응용하여야 할 것이다.

참고 문헌

(1) A. K. Hrechak, "Automated Fingerprint Recognition Using Structural Matching," Pattern Recognition, 23, 1990.

(2) FBI's Manual, The Science of Fingerprints, U.S. Goverment Printting Office, Washington, D.C., 1963.

(3) B. M. Mettre, " Fingerprint Image Analysis for Automatic Identification," Machine Vision and Applications, 6, 1993.

(4) B. G. Sherlock, Fingerprint Enhancement by Directional Fourier Filtering," IEE., Proc.-Vis., Image Signal Processing, Vol 141, No.2, April, 1994.