사용자 인증 시스템의 보안성 향상을 위한 생체인식 데이터의 암호화

Encryption of Biometrics data for Security Improvement in the User Authentication System

朴祐根*
Woo Geun Park*

요 약

본 논문에서는 생체인식 데이터의 보안성을 향상시키기 위하여 MD5(Message Digest5)와RSA(Ron Rivest, Adi Shamir, Len Adleman) 알고리즘 등을 이용한 새로운 생체인식 데이터 전송 모델을 제시함으로써 보다 안전하게 사용자 인증을 수행할 수 있도록 하였다. 즉, 클라이언트를 통해 생체인식 종류 가운데 지문을 입력 하도록 하고, 처리된 지문을 서버로 전송한다. 지문 정보가 전송 될 때, 외부로부터의 불법적인 생체 정보를 가로채는 등의 문제를 해결하기 위해 MD5 알고리즘을 이용하여 정보를 Digest화하고, 이것을 RSA 방식으로 다시 전송하는 과정을 거치도록 하는 것을 보여주었으며, 암호화 되지 않은 일반 텍스트 데이터와 생체 데이터, 암호화 하여 전송하는 생체 데이터의 전송 속도 및 보안성을 각각 비교 실험 하였다. 이러한 개선된 방법을 통하여 사용자 인증을 수행함으로써 인증 절차를 간소화하고 좀 더 정확하고 안정된 방법으로 여러 분야에 적용될 수 있을 것으로 예상된다.

Abstract

This paper presented new biometrics data transfer model, and use MD5 (Message Digest5) and RSA (Ron Rivest, Adi Shamir, Len Adleman) algorithm to improve biometrics data's security. So, did so that can run user authentication more safely. That is, do so that may input fingerprint among biometrics through client, and transmit processed fingerprint to server. When fingerprint information is transmitted, it uses MD5 algorithm to solve problem that get seized unlawful living body information from outside and information does Digest. And did to pass through process that transmit again this by RSA method. Also, experimented general text data and living body data that is not encoded, transmission speed and security of living body data that encoding and transmit each comparison. By running user authentication through such improved method, is expected to be applied in several fields by method to simplify certification procedure and is little more correct and stable.

Keywords : Biometrics, Fingerprint, MD5, RSA, User Authentication System, Encryption

I. 서론

최근 정보통신 기술의 발전과 인터넷 이용의 확산으로 인하여 정보의 수집 및 분석 등이 편리하게 되었으

* 광주대학교 컴퓨터학과
(Department of Computer Science & Engineering, Gwangju University)

接受日:2005年 5月 12日, 修正完了日:2005年 7月 15日

나, 한편으로 개개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 보안상의 심각한 문제가 제기 되고 있다. 또한 기업의 중요한 정보 또는 전자상거래 등의 경제 활동에 필요한 여러 가지 정보의 손상과 파괴의 사례도 점차 증가되고 있는 것이 현실이다. 따라서 타인에게 노출되거나 망각해 버리는 등의 문제점이 있는 패스워드 또는 PIN(Personal Identification Number)을 대체하거나 보완하기 위하여 개인의 신체 정보를 활용한 생체인식 사용자 인증 방법에 관한 연구가 진행되고 있다. 그러나 네트워크로 전송되어지는 생체 정보는 스푸핑(Spoofing)과 같은 외부의 침입에 의하여 전송 도중 정보가 누출 되는 문제가 발생할 수 있으며, 누출 된 정보는 어렵지 않게 복호화 작업을 통해 원본 이미지 데이터의 형태로 전환 될 수 있다. 이와 같이 생체인식 기술의 활용에서 발생할 수 있는 여러 가지 문제점은 IST(Information Society Technologies)의 BIOVISION 프로젝트에서도 제기 된 적이 있으며, 많은 연구기관에서 문제 해결 및 보완을 위한 연구가 진행 중에 있다.

본 논문에서는 이와 같은 문제점을 해결하고, 생체인식 데이터의 보안성을 향상시키기 위하여 MD5(Message Digest5)와RSA(Ron Rivest, Adi Shamir, Len Adleman) 알고리즘 등을 이용한 새로운 생체인식 데이터 전송 모델을 제시함으로써 보다 안전한 사용자 인증 시스템을 구현할 수 있도록 하였다. 본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 위해 생체인식의 정의와 암호화 알고리즘에 대하여 기술하고, 3장에서는 사용자 인증 시스템의 구현을 설명하였다. 4장에서는 생체인식 데이터의 전송 방법에 따른 전송 속도 및 효율성을 실험을 통하여 측정 비교. 분석하였고, 마지막으로 5장에서 결론 및 향후 연구 방향을 기술하였다.

II. 관련 연구

2.1 생체인식의 정의

생체인식은 사람의 고유한 신체적(Physiological), 행동적(Behavioral)인 특징을 이용하여 개인을 인식 또는 측정하는 것을 의미하며, 이것을 통해 접근 권한 등을 확인하여 인증하는 것을 생체 인증이라 한다. 신체적 특징을 이용한 대표적인 생체인식 기술로는 홍채, 얼굴, 지문인식 등이 있으며, 행동적인 특징을 이용한 기술로는 음성, 서명 인식 등이 대표적인 것들이다.

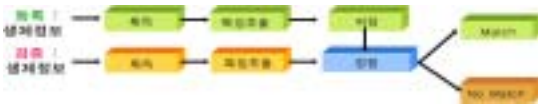

그림 2.1 생체인식에서의 등록과 검증

기존의 개인인증방법과 차별화 된 특징을 가지고 있는 이러한 생체인식 인증 메커니즘은 그림 2.1과 같이 전형적으로 등록과 검증이라는 두 가지 모드를 가지고 있다. 일반적으로 생체인식을 처음 사용할 때 각 개인은 허가된 이용자임을 검증해 주는 시스템 관리자에 의해 등록되어야 한다. 일단 이용자가 등록된 다음 이용자를 인증할 필요가 있을 때, 센서에 의해 이용자의 생물학적 특성이 획득되게 된다. 센서로 획득한 아날로그 정보는 디지털 형태로 변환되며, 이 디지털 형태의 정보는 등록 시 저장된 생체인식 형판(Template)과 비교된다. 비교 알고리즘은 디지털 형태의 정보가 저장된 형판과 얼마나 유사한지에 대한 결과를 산출한다. 만일 결과가 수용범위에 든다면 확증 반응이 주어지고 수용할 수 없는 범위에 든다면 부적 반응이 주어지는데, 수용범위는 각 생체인식 방법에 따라 다르다. 이러한 생체인식 기술이 가져야 할 조건 및 평가항목은 다음과 같이 7가지로 구분된다.

① 보편성(University) : 모든 대상자들이 보편적으로 지니고 있는 생체 특징이어야 한다.
② 유일성(Uniqueness) : 개개인별로 특징이 확연히 구별되어야 한다.
③ 지속성(Permanence) : 대상으로 하는 생체 특징점은 사람이 살아가는 동안 그 특성을 변함없이 지니고 있어야 한다.
④ 수집성(Collectability) : 특징점의 취득이 용이하여야 한다.
⑤ 성능(Performance) : 개인 확인 및 인식의 우수성이 높아야 한다.
⑥ 수용성(Acceptance) : 생체인식 대상자의 거부감이 없어야 한다.
⑦ 위/변조가능성(Circumvention) : 위조 또는 변조가 불가능해야 한다.

이상적인 생체인식 특성은 보편성, 유일성, 지속성, 수집성과 같은 요구사항을 만족시켜야 할 것이지만, 실제로 이러한 요구사항 모두를 만족하는 생체인식 특

성을 찾기는 매우 어려운 일이다.

2.2 생체인식의 종류 및 특징

1) 홍채인식(Iris Recognition)

홍채인식(Iris Recognition)이란 특정인의 눈 영상을 카메라로부터 취득하여 홍채 영역내의 특징을 추출하고 신원을 확인하는 것으로 정의될 수 있으며, 홍채인식 시스템은 이러한 작업을 수행하는 시스템을 말한다. 홍채인식을 위한 일반적인 처리 과정은 등록 절차와 검증 절차로 나누어진다. 등록 절차는 등록자의 ID와 함께 눈 영상을 입력 받아 전처리 과정과 특징 추출 과정을 거쳐 데이터베이스에 저장하는 단계이고, 검증 절차는 입력 홍채 영상에 대해 전처리 과정과 특징 추출 과정을 거쳐 이미 데이터베이스에 저장된 참조 홍채 특징과 비교하여 최종 인식 결과를 내는 단계이다. 두 단계에서 필요로 하는 세부 과정은 영상 획득 과정, 홍채 영역 분리 과정, 특징 추출 과정, 비교 과정 등이 있다.

2) 얼굴인식(Face Recognition)

얼굴은 인식 정보를 담고 있고 전달해 주는 가장 자연스러운 도구로 이미지 해석과 이해의 가장 성공적인 응용 중 하나이다. 얼굴인식 기술은 정지 영상이나 동영상에 존재하는 한 사람 이상의 얼굴로부터 특징 데이터를 추출하여 얼굴 데이터베이스에 저장되어 있는 특징 데이터와의 유사도 비교를 통하여 신원을 확인하는 것으로 값비싼 입력 장치를 필요로 하지 않는 특징을 가지고 있으나, 복제가 쉽고, 조명에 영향을 많이 받으며, 시간에 따른 변화, 변장 등에 취약하기 때문에 인식률이 낮다는 단점이 있다.

일반적으로 많이 사용되고 있는 얼굴인식 방법은 특징점 기반 방식으로 눈, 코, 입 등 얼굴의 특징을 나타낼 수 있는 곳에 점을 찍고 이 점들 사이의 관계를 이용해 얼굴을 구분하는 방법이다. 일반적으로 많이 사용하는 것이 눈 사이의 거리, 눈썹의 꺾어진 각도, 코의 길이, 입의 크기 등이다. 특징점의 개수나 위치는 정해진 것이 없고 주어진 얼굴 데이터베이스를 잘 구분해 내는 정도에서 최소한으로 잡아야 한다.

3) 지문인식(Fingerprint Recognition)

지문을 이용한 사용자 인증 방법은 생체 정보를 이용한 개인 인증 방식 가운데 가장 오래된 것일 뿐만 아니라 현재 가장 널리 사용되고 있는 방식이다. 이처럼 개개인마다 고유한 사용자의 지문을 전자적으로 읽어서 미리 입력된 데이터와 비교하여 본인 여부를 판별하여 신분을 확인하는 것을 지문인식이라고 한다.

그림 2.2 특징점 추출 과정

지문인식은 입력 장치를 통하여 그림 2.2와 같이 사용자의 지문 영상을 획득하고, 획득된 지문 영상으로부터 지문의 특징을 추출하여, 미리 입력.저장된 지문 데이터베이스와 비교해 본인 여부를 판별하게 된다. 또한 지문에서 추출할 수 있는 30가지의 판단근거를 기준으로 수행되며, 동작 방식에 따라 다음과 같이 두 가지 방식으로 분류할 수 있다.

▶ 1대 N 시스템(Identification mode) : 특정 사용자의 정보가 입력되었을 때 데이터베이스에 저장된 모든 정보와 비교하는 방식으로 수사기관의 지문대조시스템과 같은 범죄수사용으로 사용하고 사용자의 수가 적을 때 사용하는 AFIS(Automated Fingerprint Identification System)을 사용한다. 특히 AFIS는 지문인식시장의 90%를 차지하는 방식이다.

▶ 1대 1 시스템(Verification mode) : 사용자가 신체정보와 함께 사용자번호를 입력함으로써 두 데이터의 비교만으로 사용자를 인증하는 방식으로 다수의 사용자가 이용할 때 주로 사용된다. 이 시스템의 응용분야는 출입통제, 금고, 정보보안, 전자상거래의 본인확인에 응용된다.

지문인식 기술에서 가장 중요한 것으로 특징점(Minutiae) 추출이 있는데 다음과 같은 과정을 거치게 된다. 먼저 융선(Ridge)의 끝점(Ending point)과 분기점(Bifurcation point)의 위치, 방향 등의 특성을 추출하고 입력장치로부터 입력받은 지문 영상의 방향 성분을 추출하고, 융선과 골(Valley)을 1과 0으로 이진화(Binarization)한다. 그리고 각 융선의 굵기를 판단하여 1 pixel의 선으로 세선화(Thinning)하고, 세선화 된 영

상은 잡음 제거 과정을 거치며 이후 지문에서의 방향과 좌표 등으로 그 특징점들이 추출된다. 추출된 특징점들은 차후의 인증을 위하여 데이터베이스 등으로 저장된다. 이렇게 추출된 특징점들로 구성된 특징 데이터들을 데이터베이스에 미리 등록 저장되어 있는 사용자의 표준 템플릿과 비교함으로써 본인 여부를 판단한다. 이때 두 지문 사이의 차이를 비교하여 점수로 산출하고, 미리 설정된 임계값을 기준으로 인증을 수행하게 된다.

2.3 암호화 알고리즘

1) RSA 알고리즘

1978년 R.Rivest, A. Shamir, L. Adleman이 제안한 RSA는 소인수 분해(Prime Factorization)의 어려움에 그 기반을 두고 있는 블록 암호로써 Diffie와 Hellman이 제안한 공개키 암호시스템에 대한 개념을 가장 효율적으로 반영한 암호 알고리즘으로 알려져 있다. RSA는 DES(Data Encryption Standard)나 IDEA(International Data Encryption Algorithm) 등의 대칭형 암호와는 달리 RSA 공개키 암호에 사용되는 키의 길이는 가변적이다. 가장 일반적으로 사용되고 있는 키의 길이는 512Byte, 768Byte, 1024Byte이다. 또한 암호화의 기본 단위가 되는 평문의 길이 역시 가변적이다. 단지, 평문의 길이는 키의 길이 보다 작기만 하면 된다. RSA 공개키 암호에 사용될 공개키 Ke = {n,e}와 개인키 Kd={d}를 생성하기 위해서는 다음과 같은 절차를 거쳐야 한다.

① 두 개의 소수 p와 q를 선정한 다음, 법n = p.q 과 ϕ(n)를 계산한다.
② 공개키 e는 ϕ(n) = (p-1).(q-1)과 서로 소(素)의 관계가 되게 임의로 선정한다.
③ e.d mod ϕ(n) = 1 의 관계에 있는 개인키 d를 유클리드 알고리즘을 통해 구한다.
④ {e,n}을 공개키로 공개하고, {d}는 개인키로 자신이 안전하게 보관한다.

2) MD5 알고리즘

MD5는 길이에 상관없는 임의의 입력 데이터로부터 128bit 메시지 축약을 만듦으로써 데이터 무결성을 검증하는데 사용되는 해쉬 알고리즘 중 하나이다. MD5는 그림 2.3과 같이 임의의 길이의 메시지를 입력으로 취하고, 128bit 메시지 다이제스트를 출력으로 제시한다. 또한 입력은 512bit 블록으로 처리한다.

MD5 알고리즘에서 다이제스트를 만들기 위한 메시지 처리과정은 크게 4단계로 구분된다.

① 패딩 비트의 부가

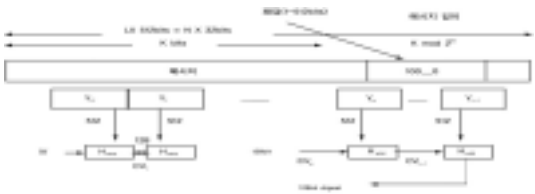

그림 2.3 MD5를 이용한 메시지 다이제스트 생성

메시지는 비트의 길이가 512를 법으로 하여 448과 합동이 되도록 패딩 된다. 즉, 패딩 된

메시지의 길이는 512비트의 정수배보다 64bit 적다. 메시지가 원하는 길이일지라도 패딩은

항상 부가된다.

② 메시지 길이의 부가

본래 메시지의 길이를 64bit로 표현하여 단계 1(LSB: Least Significant Byte)의 결과에 붙인다. 만일 길이가 264보다 크면 길이의 하위 64bit만이 사용된다. 그러므로 필드는 법 264로서 원래의 메시지 길이를 포함한다. 처음 두 단계의 결과로 길이가 512bit의 정수배가 되는 메시지를 얻는다.

③ MD5 버퍼의 초기화

128bit 버퍼는 해쉬 함수의 중간과 최종 결과를 보관하기 위하여 사용된다. 버퍼는 4개의 32bit 레지스터(A,B,C,D)로 표현할 수 있다.

④ 512Bit 블록의 메시지 처리

이 알고리즘의 핵심은 4개의 라운드 처리로 구성된 압축함수 모듈이다. 이 모듈은 (그림 2.3)에서 HMD5로 표시되어 있다. 4개의 라운드는 비슷한 구조를 가지나, 각각은 F,G,H,I로 표현되는 다른 기약 논리 함수를 사용한다.

각 라운드는 처리된 현재의 512bit 블록(Yq)과 128bit 버퍼 값 ABCD와 버퍼의 내용을 입력으로 취하고, 버퍼의 내용을 갱신한다. 또한, 각 라운드는 사인 함수로 구성되는 64요소의 T[1 ... 64]의 1/4를 사용한다. T[i]로 표시하는 T의 i번째 요소는 232 x abc(sin(i))의 정수 부분과 일치하는 값을 갖는다. 여기에서 i는 라디안이다. abs(sin(i))가 0과 1사이의 수이

므로 T의 각 요소는 32bit로 표시되는 정수이다.

네 번째 라운드의 출력은 그림 2.4와 같이 첫 번째 라운드의 입력이었던 CVq에 더해져서 CVq+1을 생성한다. 덧셈은 법 232의 덧셈을 사용하여 버퍼에서의4 단어의 각각에 대하여 CVq에서 대응하는 단어와 독립적으로 수행된다.

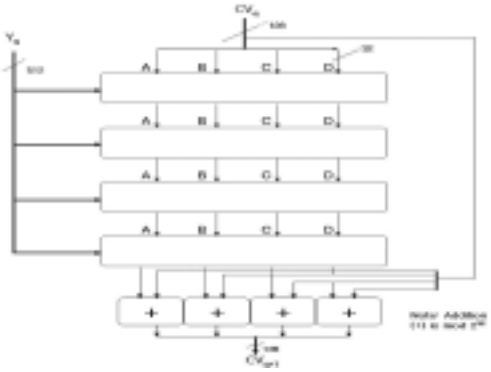

그림 4. 단일 512bit 블록의 MD5 처리

III. 사용자 인증 시스템의 구현

3.1 클라이언트 시스템의 설계 및 구현

시스템은 크게 클라이언트와 서버 시스템 부분으로 나눌 수 있다. 그 중 클라이언트 시스템은 지문 입력 및 등록 프로세스, 지문 추출 프로세스, 데이터 암호화 프로세스를 통하여 지문 입력 단말기로부터 사용자의 지문을 입력 받는 작업을 수행하게 된다.

1) 지문 입력 및 등록 프로세스

본 논문에서는 지문 입력 프로세스를 수행하기 위해 지문 입력 단말기로 Magic Secure3500 을 이용하였으며, FRR은 0.01% 이내이며, FAR은 0.001% 이내로 측정 되었다. 지문 입력 및 등록을 위해 제공되는 API는 다음과 같다.

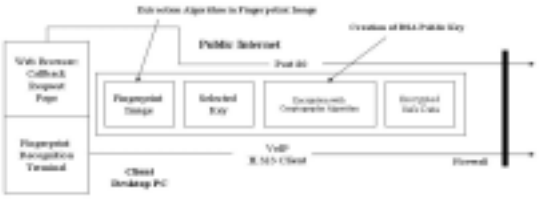

그림 3.2 클라이언트 시스템의 구조

① JFPInitDevice : 장치를 열고 초기화한다.

② JFPCloseDevice : JFPInitDevice 함수로 장치를 열고 사용 후 더 이상 장치를 사용하지 않을 경우에 이 함수를 이용하여 장치를 닫는다.

③ JFPGetFinger : 입력되는 지문 영상과 지문 영상을 처리하여 얻어지는 특징점 자료들을 장치로부터 얻어온다.

④ JFPDrawRawImage : JFPGetFinger 함수로 얻어오는 지문 영상을 화면에 그려준다. 윈도우즈에서는 비트맵(Bitmap) 이미지를 사용하는 반면, JFPGetFinger 함수에서 얻어진 지문 영상이 열 영상 형태로 되어 있기 때문에 화면에 직접 그릴 수 없다. 이 함수를 이용하면 열 형태의 지문 영상을 화면에 그릴 수 있다.

⑤ JFPMatchFinger : 저장된 지문 자료와 현재 입력한 지문 자료를 비교한다. 두 개의 특징점을 비교하여 지문이 일치하는지에 대한 결과를 리턴 하고 보안 등급(Security Level)을 준다.

지문 입력 및 등록 순서도는 그림 3.2와 같다.

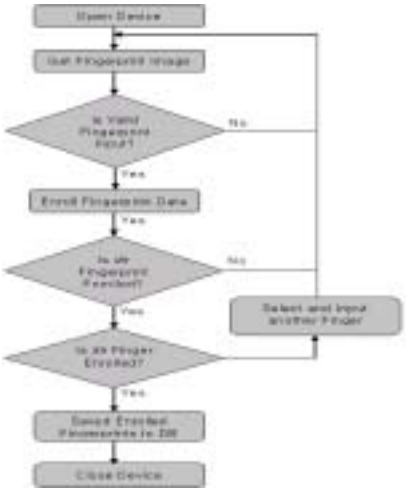

그림 3.2 사용자 지문 입력 및 등록 순서도

2) 지문 추출 프로세스

입력 된 지문 영상으로부터 이진화 된 데이터를 추출하기 위해 크게 다음과 같은 과정을 거치게 된다. 먼저 원시 입력 지문 화상의 감도를 높이기 위해 전처리 과정을 수행하고, 각 융선의 방향성분 및 융선과 골을 구분하여 이를 이진화하는 단계 및 각 융선의 굵

기를 판단하여 이를 1 포인트의 선으로 세션화 하는 과정이다. 전처리 과정에서는 명암의 구분을 높임으로써 보다 정확한 지문 추출을 가능하게 한다. 이렇게 전처리 과정을 거친 영상은 다시 방향성분을 추출하는 단계를 거치게 되고, 원래의 화상을 융선과 배경으로 구분하게 된다. 이렇게 융선과 골이 구분된 영상은 그 굵기를 판단하여, 이를 1 포인트의 선으로 세션화하게 되며 이후 지문에서의 방향과 좌표 등으로 그 특이점들이 추출된다. 본 논문에서는 원래의 화상을 융선과 배경으로 구분하기 위하여 8*8 pixel로 구분하고 각 블록의 대표 방향을 구하기 위해 Sobel 알고리즘을 이용하였다. 또한 정확한 특징점을 추출하기 위해 배경 영역을 분리하여야 하는데, 이 과정은 방향성 추출 과정에서 얻은 정보를 함께 사용함으로써 처리 시간을 단축할 수 있다. 블록 내의 밝기의 변화량 M값을 계산하고, 만약 M 값이 미리 설정된 값보다 크면 지문이 찍힌 전경 영역으로 표기하고, 작으면 배경 영역으로 분리해 낸다.

3) 데이터 암호화 프로세스

입력 된 지문 영상으로부터 이진화 된 데이터를 추출하기 위해 다음과 같은 과정을 거치게 된다. 먼저 지문 입력으로부터 추출된 1024bit의 입력정보는 상위 512bit A와 하위 512bit B, 두 부분으로 나눈다. 그리고 나누어진 A, B는 안전성과 실용성이 뛰어난 MD5를 이용한 해시함수를 통해 128bit의 Digest DA, DB를 얻게 된다. 128bit 버퍼는 해쉬 함수의 중간 값과 최종 결과 값을 저장하기 위해 사용되며 32bit 레지스터 ABCD로 표시된다.

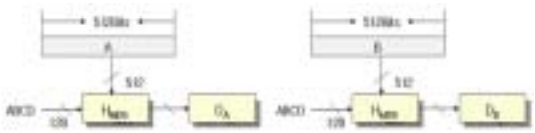

그림 3.3 MD5 해쉬 프로세스

MD5를 통해서 얻어진 두개의 Digest A, B는 RSA 공개키 암호 알고리즘의 두 소수로 사용된다. DA, DB로부터 가장 근접해 있는 소수를 각각 p, q로 정의한다. 소수의 판정은 Euler의 함수 $\phi(n) = n-1$에서 임의의 수 n이 소수일 때 $\phi(n)$가 n-1인 특성을 이용하였다. 또한 DA와 p의 차를 δ_A, DB와 q의 차를 δ_B로 정의한다. δ_A와 δ_B는 저장해 두었다가 소수 생성시에 소수를 찾아내는 중간 과정 없이 DA, DB로부터 바로 소수 p,q를 찾아 실시간으로 키 생성을 가능하도록 하였다. 마지막으로 두개의 소수 p,q를 이용하여 RSA 알고리즘을 적용한 공개키를 생성하였다. 또한 개인키 생성을 위해 앞에서 정의한 MD5 해시 함수를 통해 다이제스트 DA, DB를 얻는다. 먼저 Fingerprint Matching 과정을 거치고, 확인이 되면 DA, DB와 가지고 있던 δ_A와 δ_B을 이용하여 p,q를 계산해낸다. n과 공개키 Kp는 알려져 있으므로 $\phi(n) = (p-1)(q-1)$와 Kp를 이용하여 개인키를 생성한다.

3.2 인증 서버 시스템의 설계 및 구현

인증 서버 시스템은 사용자 인증 프로세스를 통하여 클라이언트로부터 전송 된 암호화 된 지문 데이터를 복호화 모듈을 거쳐 본래의 이진데이터로 변환되고, 저장되어 있는 원래의 지문 데이터와 비교 검사하여 본인임을 확인하게 된다.

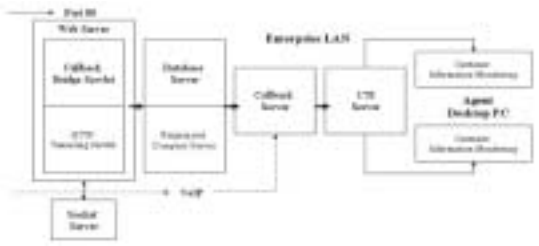

그림 3.4 서버 시스템의 구조

인증 서버 시스템에서 구현해야 될 사용자 인증 프로세스의 순서도는 그림 3.5와 같다. 사용자 인증 클라이언트 시스템으로부터 전송 된 사용자의 지문과 데이터베이스내의 지문 데이터를 비교하여 본인임을 인증하는 과정이다.

그림 3.5 사용자 인증 순서도

Ⅳ. 실험 결과 및 분석

본 논문에서 제안하고 구현한 시스템의 보안성과 효율성을 확인하기 위하여 다음의 3가지 시스템 모델을 이용하여 클라이언트에서 서버까지의 데이터 전송속도를 비교 측정하였다.

① 8Byte의 ID와 16Byte의 Password를 그대로 전송	- Case1
② 256 X 256 pixel을 512bit 단위로 전송	- Case2
③ 256 X 256 pixel을 MD5, RSA로 암호화하여 전송	- Case3

먼저 8Byte의 ID와 16Byte의 Password를 표본으로 삼은 목적은 일반적인 웹사이트에서 사용되고 있는 ID가 영숫자를 포함한 8Byte, Password 역시 영숫자를 포함한 16Byte로 되어 있기 때문이며, 두 번째 표본은 지금까지 생체인식 정보로만 사용자 인증을 하던 방식과 암호화 전송 방식을 혼용한 기법과의 전송 및 인증 속도 차이를 측정하기 위해서이다. 전송 속도를 측정하는 데는 다음의 알고리즘을 사용하였으며, C언어를 통해 측정 프로그램을 구현하였다.

```
#include <time.h>
time_t start, end;
double duration;
start = clock(); // transmit start
.....
end = clock();transmit end
duration = double(end-start) / CLOCKS_PER_SEC;
```

또한 각각의 표본을 통해 데이터 전송 시간을 측정한 결과는 그림 4.1과 같으며, 표본 ?,?의 경우에는 사용자 지문 정보를 스캔하는 시간을 제외하였다.

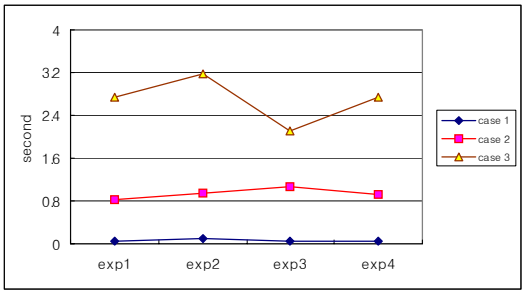

그림 4.1 데이터 전송 처리 속도 비교 그래프

표 4.1 데이터 전송 처리 속도 비교표

	exp1	exp2	exp3	exp4
Case1	0.1	0.14	0.08	0.11
Case2	0.82	0.91	1.2	0.89
Case3	2.71	3.16	2.13	2.57

첫 번째의 경우는 일반적으로 웹 브라우저에서 사용하는 8Byte의 ID와 16Byte Password를 전송하였을 때의 속도를 나타내며, 두 번째의 경우는 지문 픽셀을 나눈 512bit 데이터를 전송할 때의 속도이며, 마지막 세 번째의 경우는 512bit를 암호화하여 전송할 때 걸리는 속도를 나타낸다.

실험결과를 통해 얻을 수 있는 결과는 일반적인 사용자가 자신의 정보를 입력하고 인증을 받기까지 걸리는 지연 시간은 3가지의 경우 모두 큰 차이를 나타내지 않는 것을 알 수 있다. 따라서 데이터 자체의 무결성과 기밀성의 비중에 따른 효율성이 더 높게 된다. 결국 이용자가 크게 불편을 느낄 만큼의 본인 인증 처리의 시간이 소요되지 않는다면, 네트워크상의 보안을 우선시 하는 것이 바람직하다고 할 수 있을 것이며, 과거 생체인증만으로 완벽하지 못했던 데이터 전송상의 정보 유출 등의 문제를 근본적으로 해결할 수 있을 것으로 예상된다.

V. 결론

생체인식 사용자 인증 방법만으로는 완벽한 데이터의 보안을 유지하기 어려운 문제점이 있다. 만약 입력된 생체 정보가 이진 데이터로 변조 되어 전송 될 때, 외부로부터의 침입이 발생하게 된다면, 원래의 생체 정보가 그대로 복호화 될 수 있는 보안상의 한계가 있게 되는 것이다. 물론 웹브라우저를 이용하여 사용자의 아이디와 패스워드를 텍스트로 입력하여 전송하는 과거의 방법보다는 비교적 안정성이 높아지긴 하였으나, 위와 같은 문제를 방지 하는 데에는 여러 가지 보완해야 할 문제점이 들이 있다. 이러한 문제점을 해결하기 위하여 생체 인증을 2가지 이상 수행하는 멀티 인증 방법이 연구되기도 하였으나, 데이터 전송상의 문제는 해결하지 못하였었다. 따라서 본 논문에서는 이진화 된 생체 정보를 서버에 전송하고자 할 때, MD5 및 RSA 알고리즘을 적용한 보안 전송을 수행함으로써 보다 안전하게 사용자의 정보를 전송할 수 있도록 하였다.

본 논문에서는 일반 텍스트만으로 인증하는 방법과, 생체 정보만을 전송하여 인증하는 방법과의 비교 실험을 통해 암호화 알고리즘을 적용하여 생체 데이터를 적용하는 것이 보다 안전하고 신뢰성 있는 사용자 인증 방법이라는 것을 알 수 있게 되었다. 또한 실험에서와 같이 이러한 보안적 사용자 인증 시스템을 구축하게 되면, 신뢰성 있는 시스템을 구현할 수 있고, 반복적인 인증 절차를 간소화하여 빠르고 편리한 접근 방식도 제공할 수 있다는 장점을 얻을 수 있을 것이다. 본 논문에서 제안한 생체 데이터를 암호화 하여 사용자 인증을 수행하는 방법을 적용하게 되었을 경우 보안성 향상으로 인한 기업의 비용 절감 효과를 가져올 수 있으며, 전자상거래, 인터넷 뱅킹 등의 응용 분야에도 폭넓게 활용 될 수 있을 것으로 예상된다. 그러나 단말기를 통해 인식 된 생체 데이터를 암호 및 복호화 하는데 소요되는 시간을 최소화 시켜야 할 것이며, MD5 및 RSA 알고리즘 보다 더욱 효과적으로 적용될 수 있는 암호 알고리즘을 통한 지속적인 연구가 필요할 것이다. 향후 음성 인식 및 홍채인식 등과 같이 다양한 생체인식 기술을 복합적으로 적용하는 방법에 대해서도 검토할 예정이다.

참고 문헌

[1] A.K. Jain, R. Belle, and S. Pankanti, "Biometrics-Personal Identification Using Thermal Image Processing,"IEEE International Workshop on Robot and Human Communication, pp. 374-379, 1997.

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

[3] A. Farina, Z. M. Kovacs-Vajna, A. Leone, "Fingerprint minutiae extraction from skeletonized binary images," Pattern Recognition, Vol. 32 No. 5, pp. 877-889, 1999.

[4] Boneh, D., and J. Shaw, "Collusion-secure Fingerprinting for Digital Data," in Advances in Cryptology, Proceedings of CRYPTO '95, Lecture Notes in Computer Science, Springer-Verlag, Vol. 963, pp. 453-465, 1995.

[5] Joo-Young Kim, Sun-Young Lee, Sang-Rak Lee, Byoung-Soo Lee, "A Study on Design and Implementation of efficient ICC using Fingerprint Recognition," Conference of KIPS(Korea Information Processing Society), Vol. 9, No. 2, pp. 909-912, 2002.

[6] Lin Hong, Yifei Wan and A. K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," Department of Computer Science, Micigan State University.

[7] M.R. Verma, A.K. Majumdar, B. Chatterjee, "Edge detection in fingerprints," Pattern Recognition, Vol.20, No. 5, pp.513-523, 1987.

[8] NTL Group, "Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems," August 2000.

[9] Pfitamann, B., and M. Waidner, "Anonymous Fingerprinting," in Advances in Cryptology, Proceedings of EUROCRYPT '97, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1233, pp. 88-102, 1997.

[10] Rivest, R., "The MD4 Message Digest Algorithm," Proceedings, Crypto '90, August 1990; published by Springer-Verlag.

[11] R. L. Rivest, A. Shamir and Adleman, "A method of obtaining digital signature and public key

cryptosystem," ACM Communication 21 No. 2, pp. 120-126, 1978.
[12] Sharat Chikkerur, Sharath Pankanti, Nalini Ratha, Ruud Bolle, and Venu Govindaraju, "Minutiae Verification in Fingerprint Images Using Steerable Wedge Filters,"2004 IEEE Workshop on Applications of Computer Vision, WACV-04.

저 자 소 개

박 우 근

1983년 전남대학교 계산통계학과 (이학사)
1985년 전남대학교 전산통계학과 (이학석사)
2005년 인천대학교 컴퓨터공학과 (공학박사)
1986년 ~ 현재 : 광주대학교 컴퓨터학과 교수
1983년 ~ 현재 : 한국정보과학회 정회원
1993년 ~ 현재 : 한국정보처리학회 종신회원
1994년 ~ 현재 : 한국정보처리학회 학회지 편집위원
2005년 ~ 현재 : 한국정보처리학회 이사

<주관심분야> 데이터베이스 설계, 데이터마이닝, 생체인식, eCRM, BPR