지문 데이터베이스의 보안관리 연구

현영숙, 김창수
부경대학교 전산교육전공

A Study on the Security Management for Fingerprint Database

Young-sook Hyun Chang-soo Kim
Dept. of Computer Science Education, PuKyong National University
E-mail : youngsuki@mail1.pknu.ac.kr, cskim@pknu.ac.kr

요 약

최근 개인 신분확인 기술로 개인의 신체적 특징을 이용한 생체인식시스템이 주목을 받고 있다. 그러나 생체인식시스템에 저장된 생체 정보가 개인의 고유한 신체정보라는 점에서 정보가 유출되거나 의도적인 데이터의 변경으로 침해 발생 시 막대한 피해가 우려된다. 이러한 문제들을 기본적으로 해결하기 위해서는 생체인식 정보가 저장된 데이터베이스를 보호해야 한다. 본 논문에서는 생체인식시스템 중 지문인식 시스템을 사용하여 지문 데이터베이스내의 데이터에 대한 위조 및 변조를 체크하여 신뢰성 있는 데이터를 관리할 수 있는 지문데이터베이스 보안관리에 관한 내용을 설계하고자 한다.

1. 서론

생체인식 기술은 개인의 독특한 특성을 측정해 그 결과를 사전에 측정한 특징과 비교함으로써 개인의 신원을 인증 하는 방법이다. 오늘날 네트워크의 발달과 더불어 보안 및 개인 사생활 보호에 대한 관심이 높아지면서 이들의 연구가 활발히 진행되고 있다. 하지만 이들 생체 인식시스템내의 생체 정보가 개인의 고유한 신체정보라는 점에서 정보가 유출되거나 의도적인 데이터의 변경으로 침해 발생 시 막대한 피해 및 경제적인 손실이 발생 할 수 있다. 그러므로 데이터의 일관성을 저해하는 우발적인 사고 등으로부터 데이터 혹은 데이터베이스를 보호해야 할 필요성이 있다.

본 논문에서는 생체인식 시스템 중에서도 정확도 및 처리 속도 등의 성능, 이용의 편리성과 친밀성, 경제성 등이 높이 평가되어 최근 많은 연구와 활용이 구체화되고 있는 지문인식시스템을 사용하여 데이터가 수정 및 변조되었는지 확인하는 무결성 검증 시스템을 설계하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 지문인식 시스템을 소개하고 데이터의 무결성 검증의 필요성과 방법을 소개한다. 3장은 2장에서 제시한 방법을 활용한 무결성 보안에 관한 설계를 하고 끝으로 4장에서는 결론 및 향후과제를 제시한다.

2.관련연구

2.1 지문인식 시스템

사람의 지문은 평생불변, 만인부동의 특징을 가지고 있어서 사람 식별의 가장 확실한 수단으로 생각되어져 왔다. 범죄 현장에서의 용의자의 지문은 매우 중요한 단서로 활용되어지며 주민등록상에서도 우리의 지문은 중요한 개인의 식별을 위해 사용되어져 왔다. 이에 따른 자동화 연구가 활발히 진행되어 왔으며 지문을 이용한 개인인증에 관한 연구는 많은 성과를 보이고 있고 현재에도 다양한 분야에 적용되고 있다[1].

2.1.1 지문의 형태적인 특성

지문 형상은 복합적인 곡선들의 모음이며 다른 손가락에 의한 두 지문은 같은 융선(Ridge)을 가지고 있지 않으며 그 형태는 평생동안 변하지 않는다.

지문의 각 특성들은 그림 1에 나타나 있다.

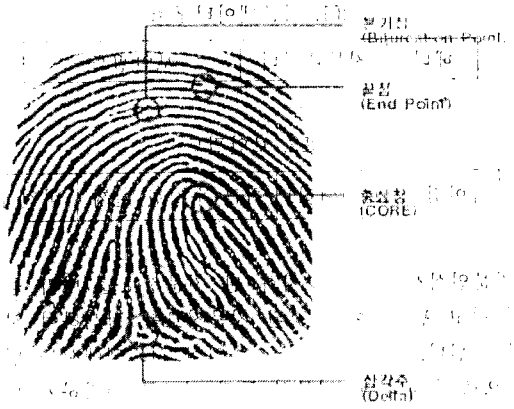

그림 1. 지문의 형태

지문의 여러 가지 형태의 선의 흐름을 융선(Ridge)이라고 하며 지문의 어두운 부분을 말한다. 융선과 융선 사이 즉, 밝은 부분을 골(valley)이라고 한다. Galton은 지문 융선의 일정한 흐름을 깨는 비연속점(local discontinuities)들이 지문 형상에 많이 존재한다고 밝혔으며 이를 특징점(minutiae)이라고 부른다. Glaton feature란 지문의 융선 위에 나타난 특징점을 뜻하는데 8가지를 분류했으나 현재 지문인식 시스템에서는 모든 Glaton feature들이 대부분 사용되지 않고 대표적인 2가지 특징점인 끝점(ending point)과 분기점(bifurcation) 만으로 나머지 Galton Feature를 표현할 수 있다[2]. 끝점(Ending point)은 융선이 부드럽게 흐르다가 끊어지는 점이며 분기점(Bifurcation point)은 융선이 부드럽게 흐르다가 두 갈래로 갈라지는 점을 말한다.

지문에는 특징점 외에 특이점을 보유하고 있을 수 있는데 중심점(core)과 삼각주(delta)를 들 수 있다. 중심점은 지문의 융선 중 방향이 가장 급격하게 변하는 곳이며, 삼각주는 융선의 흐름이 세 방향으로 나누어지는 곳을 말한다. 이 특이점을 지문의 기준점을 잡거나 분류할 때 사용되는 요소들이다. 이에 반해 Henry는 지문의 전체적인 구조에 대해 연구했으며 기본적인 5가지 지문을 분류하였으며 그 분류는 arch, tented arch, left loop, right loop, whorl이다.

현재 지문인식 시스템은 지문의 데이터베이스 양이 많을 때 검색시간과 계산의 복잡성을 줄여 효율적으로 하기 위해 Henry system을 통해 지문을 분류하며 Glaton Features들을 사용해 matching을 수행할 수 있다.

2.1.2 지문인식방법

지문을 인식하는 방법은 크게 Galton Features를 이용한 특징점 기반인식 시스템과 Galton features를 이용하지 않고 지문의 다른 특징들을 이용하는 시스템으로 나눌 수 있다[2]. 특징점 기반인식 시스템은 지문의 특징점과 주변의 특징점 분포를 이용한 비교 방법을 사용하여 이루어지는데 먼저 특징점을 찾은 후 특징점의 속성과 상대적 위치, 각도의 계산으로 개인 식별을 할 수 있게 된다. 특징점 기반인식 시스템은 융선의 전체적인 형태를 고려하지 않고 또 지문의 상태가 양호하지 않은 경우 특징점을 정확하게 추출하기 어려운 단점이 있다. 지문 융선의 특징점을 이용하는 방식이 아닌 다른 특징을 이용하는 시스템은 지문 상에 존재하는 땀샘의 분포를 이용하는 지문인식 방법이 있기는 하지만 널리 사용되는 방식은 아니다.

2.2 지문 데이터베이스 무결성 검증 요구사항

2.2.1 무결성 검증의 필요성

데이터베이스 무결성은 정보의 내용이 허가된 사람에 의해서만 생성, 삭제, 변경을 가능하게 하는 것으로 허가되지 않은 비인가자가 함부로 변조나 위조를 못하게 하는 것이다. 지문데이터는 개인의 고유한 신체정보라는 점에서 정보가 유출되거나 의도적인 데이터의 변경으로 침해 발생 시 막대한 피해가 우려된다.

만일 A라는 사람이 의도적으로 B라는 지문데이터에 자신의 지문데이터를 복사하였고 B는 데이터가 변경되었는지 모른다고 가정하자. A는 B의 정보를 남용할 것이며 B는 자신의 정보가 유출되고 있는 지도 모르는 현상이 일어난다. 이로 인해 프라이버시 침해는 물론 컴퓨터 범죄 등 많은 문제를 발생시킬 수 있다.

2.2.2 해쉬 함수

무결성을 검증하기 위한 방법으로는 해쉬 함수가 널리 사용된다. 해쉬함수는 다양한 길이의 입력을 고정된 짧은 길이의 출력으로 변환하는 함수로써 (식 1)과 같이 표현되어 질 수 있다.

$$y=h(x) \quad \text{(식 1)}$$

여기서 x는 가변길이 데이터이고, y는 해쉬 함수 h를 통하여 생성되어지는 고정길이의 해쉬값(hash code)이다. 해쉬 함수의 대표적인 응용분야로는 디지털 서명(digital signature)의 효율성 증대와 중요 정보의

무결성 확인을 들 수 있다.

3. 지문DB의 무결성 보안 설계

3.1 지문DB의 무결성 보안 구성도

지문 데이터 베이스의 무결성을 보안하기 위한 전체적인 구성도는 그림 2와 같다.

첫째, 지문데이터베이스내의 무결성 검사를 위해 특정 정보에 대한 무결성 항목을 설정한다. 둘째 설정된 무결성 항목으로 정보가 변경되었는지 검사를 한다. 마지막으로 무결성 검사 결과 데이터가 변경되었으면 경고 정보를 로그에 남기고 침입상황을 파악할 수 있도록 관리자에게 알려준다.

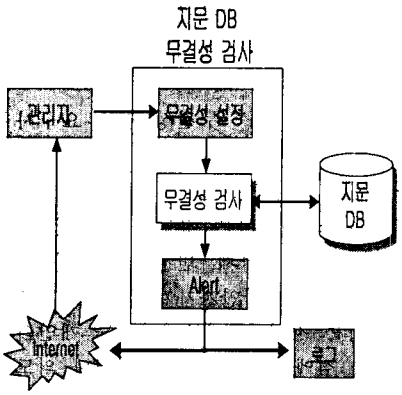

그림2. 무결성 검사를 위한 시스템 구성도

3.2 무결성 설정

지문 데이타베이스내의 데이타의 변경 여부를 판단하기 위해서 관리자는 지문데이터베이스의 중요 데이터들에 대한 무결성 항목을 설정 한다.

3.3 무결성 검사

무결성 검사를 통하여 특정 데이터의 정보변경 유무를 판단하는데 검사되는 정보로는 지문DB의 중요데이터들, 가장 최근에 수정된 날짜등이 있다.

무결성 검사를 하기 위해서 지문 데이터베이스의 구조에 보안을 위한 항목이 필요하다. 본 논문에서는 BioAPI Specification Version 1.00에서 제안한 BIR구조[7] 기반에 무결성 보안을 위한 필드를 추가한다. 지문데이터구조는 <표1>과 같으며 무결성 검사 필드는 <표2>와 같다.

표1. 지문데이터구조

헤더	지문데이터	보안필드

표2. 보안필드

특이점 정보(해쉬값)	최근 수정한 날짜	버전

지문인식시스템은 수치화 된 지문정보를 미리 등록해 두고 필요시에 저장된 지문정보를 검색하여 사용하게 된다. 특징점 기반 지문인식 시스템에서는 일반적으로 수치화 된 지문의 특징 정보를 저장하게 된다[3]. 그리고 특징점 matching은 서로 다른 지문 이미지에서 추출된 특징점 고유의 속성과 특이점과 특징점 사이의 상대적 속성이 허용 오차 범위 내에서 서로 일치 할 때 서로 같은 특징점이라 한다. 이렇게 볼 때 특징점과 특이점은 지문인식시스템에서 개인을 인식할 수 있는 중요한 정보가 되며 이 데이터의 무결성 검증은 필수적이라 할 수 있다.

특징점 기반 지문인식 시스템에서 사용하는 일반적인 특징점의 속성정보들은 다음과 같이 주어진다.

특징점의 종류: ridge ending 또는 Bifurcation
기준점의 종류: core 또는 delta point
특징점의 위치: 이미지 상의 절대적인 위치 또는 특이점(core, delta point)으로 부터의 상대적인 위치
특징점이 이루는 각: ridge ending 과 bifurcation이 이루는 각

이들 속성에 의해 하나의 특징점 정보를 저장하기 위한 구조는 <표3>과 같으며 [3]에서도 이와 비슷한 방법으로 설계되어 있다.

표3. 특징점 정보

x 좌표	y 좌표	특징점, 특이점 구분	기준점 구분	융선의 각도	상대적 위치 (x좌표)	상대적 위치 (y좌표)

무결성 보안필드의 특징점 값은 해쉬 함수를 이용하여 얻어낸 해쉬 값을 저장하며 그 값을 이용하여 무결성을 검사하는 방법은 그림3에 나타난다.

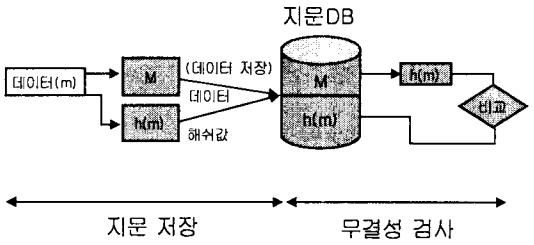

그림 3. 해쉬 함수를 이용한
지문데이터저장 및 무결성 검사

무결성 검사 방법은 저장된 데이터를 동일한 해쉬 함수를 사용하여 해쉬 값을 생성한 후 저장된 해쉬 값과 비교한다. 만약 비교한 값이 같다면 그 데이터는 변조되지 않은 원래의 데이터이고 비교한 값이 다르면 데이터 무결성에 위배된다. 지문데이터의 무결성을 위한 해쉬 함수 적용시 특징점 전체에 해쉬 함수를 적용하여 해쉬 값을 추가할 수도 있고 각 속성 정보의 무결성 검증을 위해서는 각 필드마다 해쉬 값을 저장하는 필드를 추가 할 수도 있다.

3.4 경고(Alert)

무결성 검사를 하여 데이터가 변조되거나 수정되었을 때 무결성 검사에 관련된 정보를 로그파일에 저장하고 관리자에게 알려준다.

지문데이터의 중요정보가 수정되거나 변조되었을 때 변경된 정보를 관리자에게 알려줌으로써 문제의 시간대에 어떠한 사용자가 접속하였고 어떤 데이터가 변조 되었는지 상황을 보고 받을 수 있다. 관리자에게 정보를 제공하는 방법으로 메일을 보내는 방법이나 무선단말기에 메시지를 보내는 방법 등이 있을 수 있다.

로그(audit trails 또는 log)는 시스템에서 일어나는 여러 상태에 대한 기록을 나타내는 것으로 데이터베이스의 무결성을 유지하는데 필요하며, 데이터베이스 접근에 대한 후속 적인 분석을 가능하게 한다. 무결성 검사와 관련된 정보를 로그 정보로 남겨 문제의 원인을 확인하고 파악할 수 있다.

무결성 검사와 관련된 로그 정보는 <표4>에 나타나 있다.

표4. 로그자료 구조

사용자 ID	사용자가 수행한 명령어	변경된 정보	변경된 날짜	접속 시간	사용 기간

4.결론 및 향후 과제

기존의 지문인식 시스템들은 지문데이터에 대한 매칭방법들에 대해서는 활발히 연구가 진행되고 있다. 하지만 지문데이터베이스의 공격으로 인한 지문데이터의 보안에 관한 연구는 전무한 실정이다. 따라서 본 논문은 지문데이터의 저장구조나 무결성 정보에 있어서 부족한 점이 있지만 보안이 강화되어야 하는 지문데이터베이스에 무결성이 유지되는지 판단할 수 있는 지문DB 무결성 검증을 위한 초기의 프로토타입 역할을 하였다. 지문데이터의 무결성을 유지하기 위하여 보안필드를 추가하고 데이터의 변조나 수정이 발생하면 관련 정보를 로그로 남기고 관리자에게 경고메시지를 보내도록 하는 무결성 검사 시스템의 모델을 제시하였다. 향후 연구로 본 논문에서 제시한 모델을 구현하고 지문DB의 보안을 위한 데이터베이스 설계에 관한 연구가 계속 진행되어야 할 것이다.

[참고문헌]

[1] 장동혁, 이동선, 이상범 "상관성이 적은 동일인 지문영상에서의 지문인식 알고리즘에 관한 연구" 한국정보처리학회 추계 학술발표논문집 제6권 제2호 '99.

[2] 황준호, "생체측정을 이용한 안전한 인증 프로토콜 설계 및 효율적 지문인식 알고리즘의 구현" 포항공과대학교 석사학위논문, 2001.

[3] 김현철, "특징점의 융선 연결정보를 이용한 지문인식" 안동대학교 석사학위논문 2000.

[4] "암호학의 이해와 응용" 정보보호21C 99.09.

[5] 김정덕 "데이타베이스 보안을 위한 통제기술" 데이터베이스 연구회지 2000.8.

[6] 심갑식 편저 "데이터베이스 보안" 다성 출판사 2001.

[7] "생체특정시스템 기술/시장 보고서" 한국전자통신연구원

[8] 이만영,김지홍,류재철,송유진,염홍열,이임영 공저 "전자상거래 보안기술", 생능 출판사 1999.