(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0046635
(43) 공개일자 2009년05월11일

(51) Int. Cl.
G06T 1/00 (2006.01) *G06K 9/00* (2006.01)
G06T 7/00 (2006.01) *A61B 5/117* (2006.01)
(21) 출원번호 10-2007-0112889
(22) 출원일자 2007년11월06일
심사청구일자 2007년11월06일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
정용화
대전 유성구 지족동 877 열매마을아파트 505동 402호
이성주
서울 마포구 성산2동 한맥아이홈 47-14 302호
김학재
경기 화성시 향남면 도이리 328-1
(74) 대리인
현종철

전체 청구항 수 : 총 12 항

(54) 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬방법, 부분 기하학적 해싱을 이용한 지문 데이터 인증방법, 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의정렬 장치 및 부분 기하학적 해싱을 이용한 지문 데이터인증 시스템

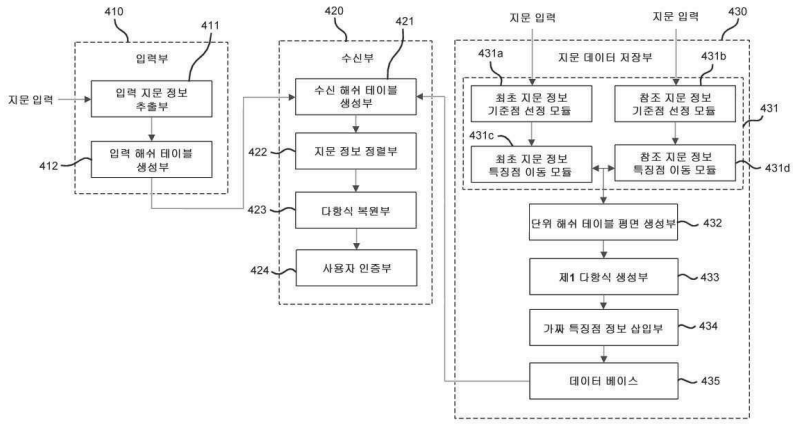
(57) 요 약

부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법, 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법, 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치 및 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템이 개시된다.

본 발명에 따른 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법은 센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하고, 상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 단계; 상기 센싱 장치를 이용하여 수신된 인증 사용자의 참조 지문 정보를 추출하고, 상기 참조 지문 정보의 특징점을 이용하여 참조 등록 해쉬 테이블을 생성하는 단계; 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단계; 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 단계; 및 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장하는 단계를 포함한다.

본 발명에 의하면, 생체 정보를 안전하게 보호하기 위하여 일반적으로 사용되는 퍼지 볼트 이론을 이용하고, 인증 사용자의 최초 지문 정보 및 참조 지문 정보를 이용하여 단위 등록 해쉬 테이블 평면 하나 만을 저장함으로써 서버에 저장되는 생체 정보의 데이터 저장량 및 메모리 사용을 효율적으로 수행할 수 있고, 유비쿼터스 임베디드 환경에서 스마트카드에 지문 정보를 저장하는 정책으로 활용될 수 있을 뿐만 아니라 기존의 지문 데이터 서버 등에 사용되는 메모리나 데이터의 가용성을 극대화할 수 있는 효과가 있다.

대 표 도



특허청구의 범위

청구항 1

센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하고, 상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 단계;

상기 센싱 장치를 이용하여 수신된 인증 사용자의 참조 지문 정보를 추출하고, 상기 참조 지문 정보의 특징점을 이용하여 참조 등록 해쉬 테이블을 생성하는 단계;

상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단계;

상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 단계; 및

상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장하는 단계를 포함하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법.

청구항 2

제 1 항에 있어서,

상기 최초 등록 해쉬 테이블을 생성하는 단계는

상기 최초 지문 정보의 특징점 중 기준점을 선정하는 단계; 및

상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점들을 기하학적으로 이동시키는 단계를 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법.

청구항 3

제 1 항에 있어서,

상기 참조 등록 해쉬 테이블을 생성하는 단계는

상기 참조 지문 정보의 특징점 중 기준점을 선정하는 단계; 및

상기 선정된 기준점을 기반으로 나머지 참조 지문 정보의 특징점들을 기하학적으로 이동시키는 단계를 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법.

청구항 4

센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상 및 참조 지문 영상으로부터 특징점들로 구성되는 최초 지문 정보 및 참조 지문 정보를 추출하고, 상기 추출된 최초 지문 정보 및 참조 지문 정보 각각의 특징점을 이용하여 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 생성하는 단계;

상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하고, 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 단계;

상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장하는 단계;

사용자의 지문 영상에서 입력 센싱 장치를 이용하여 특징점들로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적으로 변환하여 입력 해쉬 테이블을 생성하는 단계;

상기 단위 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 가짜 특징점을 제거하는 단계;

상기 정합된 지문 정보를 계수로 하는 제 2 다항식을 생성하고, 상기 제 1 다항식 및 제 2 다항식을 비교하여

사용자 인증의 결과를 검증하는 단계를 포함하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법.

청구항 5

센싱 장치를 이용하여 인증 사용자의 최초 지문 영상을 수신하고, 상기 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하는 최초 지문 정보 추출부;

상기 센싱 장치를 이용하여 인증 사용자의 참조 지문 영상을 수신하고, 상기 참조 지문 영상에서 특징점으로 구성되는 참조 지문 정보를 추출하는 참조 지문 정보 추출부;

상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 최초 등록 해쉬 테이블 생성부;

상기 참조 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 참조 등록 해쉬 테이블 생성부;

상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단위 해쉬 테이블 평면 생성부;

상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 제 1 다항식 생성부;

상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하는 가짜 특징점 정보 삽입부; 및

상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 저장하는 데이터베이스를 포함하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치.

청구항 6

제 5 항에 있어서,

상기 최초 등록 해쉬 테이블 생성부는

상기 최초 지문 정보의 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점들을 기하학적으로 이동시킴으로써 생성된 것을 특징으로 하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치.

청구항 7

제 5 항에 있어서,

상기 참조 등록 해쉬 테이블 생성부는

상기 참조 지문 정보의 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점들을 기하학적으로 이동시킴으로써 생성된 것을 특징으로 하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치.

청구항 8

인증을 수행하고자 하는 사용자의 지문 정보를 추출하는 입력부, 인증 사용자의 지문 정보를 저장하는 지문 데이터 저장부 및 사용자의 인증을 수행하는 수신부를 포함하는 지문 데이터 인증 시스템에 있어서,

상기 입력부는

사용자의 지문 영상에서 입력 지문 정보를 추출하는 입력 지문 정보 추출부; 및

상기 추출된 지문 정보를 기하학적으로 변형하여 입력 해쉬 테이블을 생성하는 입력 해쉬 테이블 생성부를 포함하며,

상기 지문 데이터 저장부는

인증 사용자의 최초 지문 정보를 이용하여 최초 등록 해쉬 테이블을 생성하고, 상기 인증 사용자의 참조 지문 정보를 이용하여 참조 등록 해쉬 테이블을 생성하는 등록 해쉬 테이블 생성부;

상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단위 해쉬 테이블 평면 생성부;

상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 다항식 생성부; 및

상기 단위 등록 해쉬 테이블 평면에 가짜 특징점을 삽입하여 상기 제 1 다항식 및 상기 가짜 특징점이 삽입된 단위 등록 해쉬 테이블을 저장하는 데이터베이스를 포함하며,

상기 수신부는

상기 입력 해쉬 테이블 및 상기 데이터 베이스에 저장된 단위 등록 해쉬 테이블을 이용하여 수신 해쉬 테이블을 생성하는 수신 해쉬 테이블 생성부;

상기 수신 해쉬 테이블에 저장된 지문 정보를 계수로 하는 제 2 다항식을 생성하는 다항식 복원부; 및

상기 제 1 다항식과 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하는 사용자 인증부를 포함하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템.

청구항 9

제 8 항에 있어서,

상기 수신 해쉬 테이블 생성부는

상기 입력 해쉬 테이블 생성부에서 전송된 입력 해쉬 테이블 및 상기 데이터베이스에서 전송된 단위 등록 해쉬 테이블을 이용하여 기준점을 추출하는 기준점 후보 추출부를 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템.

청구항 10

제 8 항에 있어서,

상기 수신부는

상기 수신 해쉬 테이블 생성부에서 생성된 수신 해쉬 데이블과 상기 입력 해쉬 테이블을 정렬하는 지문 정보 정렬부를 더 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템.

청구항 11

제 10 항에 있어서,

상기 수신부는

에러 정정 코드를 이용하여 상기 정렬된 지문 정보부터 가짜 특징점을 삭제하는 에러 정정부를 더 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템.

청구항 12

제 8 항에 있어서,

상기 등록 해쉬 테이블 생성부는

최초 지문 정보의 특징점 중 기준점을 선정하는 최초 지문 정보 기준점 선정부;

참조 지문 정보의 특징점 중 기준점을 선정하는 참조 지문 정보 기준점 선정부;

상기 최초 지문 정보의 기준점을 기준으로 나머지 최초 지문 정보의 특징점을 기하학적으로 이동시키는 최초 지문 정보 특징점 이동부; 및

상기 참조 지문 정보의 기준점을 기준으로 나머지 참조 지문 정보의 특징점을 기하학적으로 이동시키는 참조 지문 정보 특징점 이동부를 포함하는 것을 특징으로 하는 부분 기하학적 해싱을 이용항 지문 데이터 인증 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 바이오 인식 정보 보안에 관한 것으로서, 퍼지 볼트 이론을 이용하여 안전하게 보호된 지문을 등록할 경우, 인증 시스템에서 필요한 정렬 방법으로 사용되는 기하학적 해싱 기법을 수정함으로써 등록되는 지문의 데이터량을 감소시킬 수 있는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법, 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법, 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치 및 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템에 관한 것이다.

배 경 기 술

<2> 최근 급속한 정보화 및 인터넷의 발달로 인하여 네트워크를 통한 정보의 교류가 활발해지고, 온라인 자금거래 등 전자상거래와 관련된 산업의 규모가 커지면서 정확한 개인의 인증에 대한 요구가 증대되고 있다.

<3> 이러한 환경에서 가장 일반적인 인증 수단으로 개인 식별 넘버(Personal Identification Number:PIN) 또는 패스워드 방식이 사용되고 있지만, 이는 정보의 유출 및 망각의 위험이 상존하므로 이에 따른 보안상의 문제가 최근 들어 크게 부각되고 있다.

<4> 따라서, 이와 같은 인증 수단의 단점을 해결할 수 있는 개인 인증 기술로 생체 인식의 도입이 확산 되고 있다.

<5> 사용자 인증을 위하여 저장된 생체 정보가 타인에게 도용된다면, 패스워드나 개인 식별 넘버와 달리 상기 생체 정보를 변경할 수 없거나, 변경이 제한적이기 때문에 심각한 문제를 일으키게 된다.

<6> 따라서, 암호, 워터마킹(Watermarking), 스테가노그래피(Steganography) 등의 기술을 이용하여 사용자의 중요한 지문 정보를 보호하기 위한 연구가 활발하게 진행되고 있다.

<7> 지문 인식 시스템은 경제적인 설치 비용과 보안성에 대한 매우 높은 신뢰성을 가지고 있고, 수백 년 이상의 전 세계적인 적용 사례를 바탕으로 유일무이한 사람의 고유 특성으로 검증된 지문의 인식 시스템이다.

<8> 특히, 소형화된 시스템의 구성이 가능하므로 이동성과 공간 활용 능력이 매우 높다.

<9> 그리고, 최근 네트워크의 발달과 더불어 보안 및 개인 사생활 보호에 대한 관심이 높아지면서 개인 인증 방법으로서의 지문 인식 기술은 화상인식기술분야 중에서 가장 각광받는 기술분야로 발전하고 있다.

<10> 이와 같은 지문인식 기술은 단순한 출입통제 시스템에서 인터넷 뱅킹, 전자 정부 등의 원격응용 시스템으로 발전하고 있다.

<11> 아울러, 최근 바이오 및 지문데이터를 보호하기 위한 방법 중 퍼지볼트 이론을 적용한 연구가 활성화되고 있다. 퍼지볼트 이론은 암호학적인 방법으로써, 일반적으로 사용되고 있는 암호학적인 방법들과는 다르게 인증값과 등록값의 완전한 일치여부가 아닌 상기 인증값과 등록값의 유사도에 따라서 사용자의 인증 여부를 결정한다.

<12> 기하학적 해싱 기법을 퍼지 볼트 이론을 적용한 지문정보를 보호하는데 사용할 경우, 지문정보의 양과 지문정보를 보호하는데 사용되는 가짜 지문 정보의 양이 많아질수록 등록과정에서 메모리의 사용량이 많아진다.

<13> 왜냐하면, 기하학적 해싱 기법은 전체의 진짜와 가짜의 지문 정보를 기준점으로 하여 기하학적 해쉬 테이블을 생성하기 때문이다.

<14> 퍼지볼트를 적용한 지문 인증 시스템에서 등록 지문 특징점에는 복수 개의 가짜 특징점이 섞임으로써, 지문 정보를 보호하게 되며, 이러한 보호된 등록 지문과 입력 지문의 검증 과정을 위해서는 정렬(alignment) 과정과 정합(matching) 과정이 필요하다.

<15> 종래의 지문 정보 은닉 및 인증에 있어서, 정렬 과정을 해결하기 위한 종래의 방법으로는 세 가지가 있다.

<16> 첫 번째는, 지문을 등록시킬 때, 복수 회에 걸쳐서 사용자의 지문을 등록함으로써, 신뢰성 높은 지문 특징점 및 좌표를 선정하는 방법이고,

<17> 두 번째는, 지문 특징점의 위치를 노출하지 않고 정렬 과정을 위한 새로운 특징점을 추출하는 방법이다.

<18> 세 번째는, 기하학적 해싱을 이용하여 해쉬 테이블을 생성하고, 이를 이용하여 지문 데이터를 정렬하고, 정합하는 방법이다.

<19> 그러나, 종래의 지문 정보 은닉 및 인증에 있어서, 복수 회에 걸쳐 사용자의 지문을 등록하는 방법 및 지문 특

징점의 위치를 노출하지 않고 정렬 과정을 위한 새로운 특징점을 추출하는 방법은 지문의 인식률이 낮으며, 기하학적 해싱을 이용하여 해쉬 테이블을 생성하고, 이를 이용하여 지문 데이터를 정렬하고 정합하는 방법은 저장해야 하는 보호된 지문데이터의 크기가 너무 크고, 정렬 과정의 수행시 메모리 효율성이 낮아 서버에 과중한 부담을 줄 수 있고, 단순히 해쉬 테이블의 크기를 줄이면 보안성과 인식률의 성능이 저하되는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<20> 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는,

<21> 생체정보를 안전하게 보호하기 위하여 퍼지 볼트 이론을 적용하고, 보안성과 인식률의 성능을 향상시키면서도 인증시스템에서 필요한 중간 과정인 정렬 방법으로 사용되는 기하학적 해싱을 수정함으로써, 등록되는 지문 데이터의 양을 획기적으로 줄이면서도 신뢰된 인증 사용자의 지문을 등록할 수 있는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법을 제공하는 것이다.

<22> 그리고, 본 발명이 해결하고자 하는 두 번째 과제는,

<23> 상기 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법에 따른 지문 데이터로부터 인증 사용자의 지문과 인증을 수행하고자 하는 사용자의 지문을 비교하여 인증을 수행할 수 있는 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법을 제공하는 것이다.

<24> 또한, 본 발명이 해결하고자 하는 세 번째 과제는,

<25> 상기 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법을 이용한 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치를 제공하는 것이다.

<26> 아울러, 본 발명이 해결하고자 하는 네 번째 과제는,

<27> 상기 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법을 이용한 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템을 제공하는 것이다.

과제 해결수단

<28> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<29> 센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하고, 상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 단계; 상기 센싱 장치를 이용하여 수신된 인증 사용자의 참조 지문 정보를 추출하고, 상기 참조 지문 정보의 특징점을 이용하여 참조 등록 해쉬 테이블을 생성하는 단계; 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단계; 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 단계; 및 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장하는 단계를 포함하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법을 제공한다.

<30> 그리고, 상기 최초 등록 해쉬 테이블을 생성하는 단계는 상기 최초 지문 정보의 특징점 중 기준점을 선정하는 단계; 및 상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점들을 기하학적으로 이동시키는 단계를 포함하는 것을 특징으로 한다.

<31> 아울러, 상기 참조 등록 해쉬 테이블을 생성하는 단계는 상기 참조 지문 정보의 특징점 중 기준점을 선정하는 단계; 및 상기 선정된 기준점을 기반으로 나머지 참조 지문 정보의 특징점들을 기하학적으로 이동시키는 단계를 포함하는 것을 특징으로 한다.

<32> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<33> 센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상 및 참조 지문 영상으로부터 특징점들로 구성되는 최초 지문 정보 및 참조 지문 정보를 추출하고, 상기 추출된 최초 지문 정보 및 참조 지문 정보 각각의 특징점을 이용하여 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 생성하는 단계; 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하고, 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 단계; 상기 단위 등록 해쉬 테이블

평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장하는 단계; 사용자의 지문 영상에서 입력 센싱 장치를 이용하여 특징점들로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적으로 변환하여 입력 해쉬 테이블을 생성하는 단계; 상기 단위 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 가짜 특징점을 제거하는 단계; 상기 정합된 지문 정보를 계수로 하는 제 2 다항식을 생성하고, 상기 제 1 다항식 및 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하는 단계를 포함하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법을 제공한다.

<34> 상기 세 번째 과제를 해결하기 위하여 본 발명은,

<35> 센싱 장치를 이용하여 인증 사용자의 최초 지문 영상을 수신하고, 상기 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하는 최초 지문 정보 추출부; 상기 센싱 장치를 이용하여 인증 사용자의 참조 지문 영상을 수신하고, 상기 참조 지문 영상에서 특징점으로 구성되는 참조 지문 정보를 추출하는 참조 지문 정보 추출부; 상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 최초 등록 해쉬 테이블 생성부; 상기 참조 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성하는 참조 등록 해쉬 테이블 생성부; 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단위 해쉬 테이블 평면 생성부; 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 제 1 다항식 생성부; 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하는 가짜 특징점 정보 삽입부; 및 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 저장하는 데이터베이스를 포함하는 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치를 제공한다.

<36> 상기 네 번째 과제를 해결하기 위하여 본 발명은,

<37> 인증을 수행하고자 하는 사용자의 지문 정보를 추출하는 입력부, 인증 사용자의 지문 정보를 저장하는 지문 데이터 저장부 및 사용자의 인증을 수행하는 수신부를 포함하는 지문 데이터 인증 시스템에 있어서, 상기 입력부는 사용자의 지문 영상에서 입력 지문 정보를 추출하는 입력 지문 정보 추출부; 및 상기 추출된 지문 정보를 기하학적으로 변형하여 입력 해쉬 테이블을 생성하는 입력 해쉬 테이블 생성부를 포함하며, 상기 지문 데이터 저장부는 인증 사용자의 최초 지문 정보를 이용하여 최초 등록 해쉬 테이블을 생성하고, 상기 인증 사용자의 참조 지문 정보를 이용하여 참조 등록 해쉬 테이블을 생성하는 등록 해쉬 테이블 생성부; 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하는 단위 해쉬 테이블 평면 생성부; 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성하는 다항식 생성부; 및 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점을 삽입하여 상기 제 1 다항식 및 상기 가짜 특징점이 삽입된 단위 등록 해쉬 테이블을 저장하는 데이터베이스를 포함하며, 상기 수신부는 상기 입력 해쉬 테이블 및 상기 데이터 베이스에 저장된 단위 등록 해쉬 테이블을 이용하여 수신 해쉬 테이블을 생성하는 수신 해쉬 테이블 생성부; 상기 수신 해쉬 테이블에 저장된 지문 정보를 계수로 하는 제 2 다항식을 생성하는 다항식 복원부; 및 상기 제 1 다항식과 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하는 사용자 인증부를 포함하는 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템을 제공한다.

<38> 한편, 상기 수신 해쉬 테이블 생성부는 상기 입력 해쉬 테이블 생성부에서 전송된 입력 해쉬 테이블 및 상기 데이터베이스에서 전송된 단위 등록 해쉬 테이블을 이용하여 기준점을 추출하는 기준점 후보 추출부를 포함하는 것을 특징으로 한다.

<39> 그리고, 상기 수신부는 상기 수신 해쉬 테이블 생성부에서 생성된 수신 해쉬 데이블과 상기 입력 해쉬 테이블을 정렬하는 지문 정보 정렬부를 더 포함하는 것을 특징으로 한다.

<40> 아울러, 상기 수신부는 에러 정정 코드를 이용하여 상기 정렬된 지문 정보부터 가짜 특징점을 삭제하는 에러 정정부를 더 포함하는 것을 특징으로 한다.

<41> 또한, 상기 등록 해쉬 테이블 생성부는 최초 지문 정보의 특징점 중 기준점을 선정하는 최초 지문 정보 기준점 선정부; 참조 지문 정보의 특징점 중 기준점을 선정하는 참조 지문 정보 기준점 선정부; 상기 최초 지문 정보의 기준점을 기준으로 나머지 최초 지문 정보의 특징점을 기하학적으로 이동시키는 최초 지문 정보 특징점 이동부; 및 상기 참조 지문 정보의 기준점을 기준으로 나머지 참조 지문 정보의 특징점을 기하학적으로 이동시키는 참조 지문 정보 특징점 이동부를 포함하는 것을 특징으로 한다.

효 과

<42> 본 발명에 의하면, 생체 정보를 안전하게 보호하기 위하여 일반적으로 사용되는 퍼지 볼트 이론을 이용하고, 인증 사용자의 최초 지문 정보 및 참조 지문 정보를 이용하여 단위 등록 해쉬 테이블 평면 하나 만을 저장함으로써 서버에 저장되는 생체 정보의 데이터 저장량 및 메모리 사용을 효율적으로 수행할 수 있고, 유비쿼터스 임베디드 환경에서 스마트카드에 지문 정보를 저장하는 정책으로 활용될 수 있을 뿐만 아니라 기존의 지문 데이터 서버 등에 사용되는 메모리나 데이터의 가용성을 극대화할 수 있다.

발명의 실시를 위한 구체적인 내용

<43> 생체 인증에 따른 지문 인증 시스템은 사용자의 생체 정보를 데이터베이스에 등록시키는 등록과정과 사용자의 인증을 위한 검증 과정으로 나누어진다.

<44> 본 발명에서는 퍼지 볼트(Fuzzy vault) 이론을 이용하여 안전하게 보호된 지문을 등록할 때, 인증 시스템에서 필요한 중간 과정인 정렬(alignment) 방법으로 사용되는 기하학적 해싱(Geometric Hashing) 기법을 수정함으로써 등록되는 지문 데이터량을 줄임으로써, 인식률과 보안성의 성능을 저하하지 않고 메모리 효율적으로 인증과정을 수행할 수 있다.

<45> 즉, 등록 과정에서 입력되는 지문에 따라 입력 해쉬 테이블 평면 하나만을 생성하여 정렬 및 정합 과정을 거친 후 에러를 정정하여 진짜 특징점을 추출함으로써 메모리의 효율적으로 사용할 수 있고, 이와 동시에 인식률과 보안성의 성능을 저하하지 않고, 지문 인증의 수행 성능을 높일 수 있다.

<46> 그리고, 본 발명에서는 지문 정보를 보호하는 방법으로 퍼지 볼트 이론을 적용한다.

<47> 또한, 은닉된 지문 정보와 사용자가 인증을 위하여 요청한 지문 정보를 비교하는 지문 정보 정렬 단계에서는 기준점 부재 및 시스템의 부하 문제를 해결하기 위하여 부분 기하학적 해싱 방법을 적용할 수 있다.

<48> 본 발명에 적용되는 등록 해쉬 테이블은 은닉되어 있는 지문 정보가 정렬을 위하여 새로운 좌표를 가지는 테이블을 의미한다.

<49> 또한, 본 발명에 이용되는 입력 해쉬 테이블은 사용자가 인증을 위하여 입력한 지문 정보가 정렬을 위하여 새로운 좌표를 가지는 테이블을 의미한다.

<50> 도 1은 지문 인식 시스템의 블럭도를 도시한 것이다.

<51> 지문 인식 시스템은 인증을 수행하고자 하는 사용자의 지문 영상에서 지문 정보를 추출하는 송신부(110)와 사용자의 인증을 위하여 미리 저장된 지문 정보를 이용하여 인증 과정을 수행하는 수신부(120)로 이루어질 수 있다.

<52> 그리고, 인증 과정을 수행하는 수신부(120)는 인증을 위하여 지문 정보를 저장하기 위하여 지문 정보를 추출하는 인증 지문정보를 추출하고, 추출한 인증 지문 정보를 데이터 베이스에 저장하여, 데이터 베이스에 저장된 인증 지문 정보와 송신부(110)에서 추출한 지문 정보를 특정 다항식에 의하여 상호 비교하고, 특정 다항식에 의해 연산된 두 지문 정보가 유사할 경우 사용자의 인증을 수행하고, 유사하지 않을 경우 사용자의 인증에 실패하게 된다.

<53> 도 2는 본 발명과 대비되는 지문 데이터의 등록 과정을 도시한 것이다.

<54> 도 2를 참조하면, 사용자의 인증을 위하여 미리 지문 정보를 등록하기 위하여 사용자의 지문 영상(210)을 특정 센서를 이용하여 캡쳐한다.

<55> 그러면, 캡쳐한 사용자의 지문 영상으로부터 복수 개의 지문 특징점을 추출(220)하고, 추출된 지문 정보를 퍼지 볼트 이론을 적용하여 다항식을 생성한다.

<56> 그런 후, 복수 개의 지문 특징점에 가짜 특징점 정보를 삽입하여 등록 해쉬 테이블(230)을 생성하고, 이를 기반으로 사용자의 인증을 수행할 수 있는 기반을 마련한다.

<57> 이와 같이 본 발명과 대비되는 지문 데이터를 등록하는 방법은 사용자의 지문 영상으로부터 추출된 복수 개의 지문 특징점과 가짜 특징점 모두를 이용하여 기준점을 생성하고, 이에 따라 생성되는 모든 평면을 등록하게 된다.

<58> 이는 산술적으로, 생성되는 평면의 갯수를 N 이라고 할 때, x와 y의 좌표를 저장하여야 하므로 사용되는 데이터 저장량은 N^2 이며, 이에 따른 메모리의 사용량도 N^2 이 된다.

<59> 여기서, 지문 데이터는 사용자의 지문 정보에 따른 특징점과 가짜 특징점을 포함한다.

<60> 지문 데이터는 x와 y의 위치 좌표와 각도가 각각 1 바이트(byte)씩 사용되고, 지문 정보를 이용하여 퍼지 볼트 이론에 따라 생성된 다항식의 값으로 1 바이트가 추가적으로 사용되게 된다.

<61> 예를 들어, 사용자의 지문 정보에 따른 특징점을 30개, 가짜 특징점을 200개 사용할 경우, 데이터 사용량은 4×230×230 바이트인 211600바이트가 된다.

<62> 또한, 런 타임 시에는 해쉬 테이블의 자료 구조를 고려하여 포인터가 사용되므로 특징점 하나당 추가적으로 4바이트가 소요되어 전체 메모리 사용량은 8×230×230 바이트인 423200바이트가 된다.

<63> 이와 같이, 전체 메모리 사용량이 과다하여 시스템에 부하가 생기게 되고, 처리 속도 또한 저하되며, 지문 데이터의 보안에 가용되는 비용의 부담이 증가하게 된다.

<64> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세히 설명하기로 한다.

<65> 한편, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.

<66> 도 3은 본 발명에 따른 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치의 블록도(300)를 도시한 것이다.

<67> 도 3을 참조하면, 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 은닉 장치(300)는 안전하면서도 데이터 저장 공간을 최소화하는 구성을 가지고 있다.

<68> 여기서, 본 발명에 따른 인증 사용자는 본 발명이 이용되는 출입통제 시스템, 인터넷 뱅킹, 전자 정부의 원격응용 시스템에서 미리 사용을 허가받은 사용자를 의미한다. 그리고, 하기에 상술되는 제 1 다항식은 지문 데이터의 인증이 되는 다항식을 의미한다.

<69> 인증 사용자는 자신의 지문 정보를 등록할 경우, 두 번 이상의 지문을 입력하여 등록하고, 상기 두 번 이상 입력된 지문 정보를 기반으로 하나의 단위 해쉬 테이블 평면만을 생성하고, 이를 기반으로 가짜 특징점이 삽입된 가장 신뢰성 있는 단위 등록 해쉬 테이블만을 데이터 베이스에 저장함으로써 안전하면서도 저장 공간을 최소화할 수 있는 지문 데이터 은닉 장치를 구성할 수 있다.

<70> 우선, 최초 지문 정보 추출부(311)는 인증 사용자의 최초 지문 정보를 추출한다.

<71> 이는 특정의 센싱 장치를 이용하여 인증 사용자의 지문 영상을 최초로 입력받고, 지문 영상에서 특징점의 위치 좌표 및 각도를 포함하는 지문 정보를 추출한다.

<72> 상기 최초 지문 정보는 인증 사용자의 조작에 따라서 초기화된 다음, 다시 인증 사용자에 의해 최초 지문 영상이 입력될 수 있다.

<73> 참조 지문 정보 추출부(312)는 인증 사용자의 참조 지문 정보를 추출한다.

<74> 이 역시 마찬가지로 상기 특정의 센싱 장치를 이용하여 인증 사용자의 참조 지문 영상을 입력받고, 지문 영상에서 특징점의 위치 좌표 및 각도를 포함하는 참조 지문 정보를 추출한다.

<75> 상기 참조 지문 영상은 최초 지문 정보 추출부에 의해 인증 사용자의 최초 지문 정보을 추출한 다음, 인증 사용자에 의해 입력된 지문 영상으로서, 인증 사용자에 의해 복수 회에 걸쳐 입력될 수 있다.

<76> 그리고, 참조 지문 정보 역시 인증 사용자의 조작에 따라 참조 지문 정보를 초기화 한 다음, 다시 복수 회에 걸쳐 인증 사용자에 의해 참조 지문 영상이 입력될 수 있다.

<77> 최초 등록 해쉬 테이블 생성부(321)는 상기 최초 지문 정보 추출부(311)에서 추출된 인증 사용자의 최초 지문 정보에 포함된 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점

들을 기하학적으로 이동시켜서 최초 등록 해쉬 테이블을 생성한다.

<78> 예를 들어, m_1, m_2, m_3 $\cdots$, m_n으로 이루어진 n개의 진짜와 거짓 특징점을 가지고 있는 지문 정보로부터 상기 m_1을 기준점으로 선정하고, 나머지 모든 점 m_2, m_3 $\cdots$, m_n을 상기 기준점 m_1을 기준으로 회전 및 이동한 만큼 변환시킨다.

<79> 이 때, m_1을 기준점으로 선정하는 과정은 상기 m_1의 m_x, m_y, m_θ의 좌표를 원점 좌표 및 기준 각도인 (O, O, O)으로 이동 및 회전 변환하는 것이다. 이렇게 m_1에 의하여 이동 및 회전 변환된 것이 m_1의 해쉬 테이블 평면이며, m_1, m_2, m_3 $\cdots$, m_n까지 모든 특징점을 선정하고, 이동 및 회전 변환을 수행하여 등록 해쉬 테이블을 생성하게 된다.

<80> 더욱 상세하게는, 선정된 기준점을 원점으로 이동시키고, 선정된 기준점의 각도를 미리 설정된 기준 각도로 변경한다. 이에 따라서 상대적으로 나머지 최초 지문 정보의 특징점들을 상기 선정된 기준점에 대응되는 위치로 기하학적으로 이동시켜 최초 등록 해쉬 테이블을 생성한다.

<81> 참조 등록 해쉬 테이블 생성부(322)는 상기 참조 지문 정보 추출부(312)에서 추출된 인증 사용자의 참조 지문 정보에 포함된 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 참조 지문 정보의 특징점들을 기하학적으로 이동시켜서 참조 등록 해쉬 테이블을 생성한다.

<82> 여기서, 참조 지문 정보 추출부(312)에서 복수 회에 걸쳐서 인증 사용자의 참조 지문 정보를 추출한 경우, 참조 지문 정보에 포함된 특징점 중 기준점은 상기 복수 회의 참조 지문 정보의 특징점 중 사용자에 의해 정해진 특정 특징점에 해당되는 점을 취할 수 있다.

<83> 단위 해쉬 테이블 평면 생성부(330)는 상기 최초 등록 해쉬 테이블 및 상기 참조 등록 해쉬 테이블을 이용하여 단위 해쉬 테이블 평면을 생성한다.

<84> 상기 참조 등록 해쉬 테이블은 진짜 특징점으로만 이루어진 지문 정보로부터 해쉬 테이블을 생성하므로, 상기 참조 등록 해쉬 테이블은 진짜 특징점으로만 이루어져 있다. 따라서, 참조 등록 해쉬 테이블과 거짓 특징점을 포함하는 최초 등록 해쉬 테이블을 비교 후, 가장 유사도가 높은 하나의 단위 해쉬 테이블 평면을 생성하게 된다.

<85> 예를 들어, m_1, m_2, m_3 $\cdots$, m_n으로 진짜와 거짓 특징점으로 이루어져 있는 지문 정보와 m_1', m_2', m_3' $\cdots$, m_n'로 이루어진 진짜만으로 이루어져 있는 지문 정보에서 각각 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 생성할 수 있다. 최초 등록 해쉬 테이블과 참조 등록 해쉬 테이블을 비교하여 하나의 해쉬 테이블 평면을 추출할 수 있는데 m_1과 m_1', m_2', m_3' $\cdots$, m_n'을 비교하고, m_2와 m_1', m_2', m_3' $\cdots$, m_n'을 비교하고, 이와 동일한 과정으로 m_n과 m_1', m_2', m_3' $\cdots$, m_n'을 비교하여 m_1, m_2, m_3 $\cdots$, m_n에서 가장 유사도가 높았던 해쉬 테이블 평면을 선택하여 상기 단위 해쉬 테이블 평면을 생성한다.

<86> 이는 두 개 이상의 지문이 기하학적 해싱 기법을 이용하여 생성된 인증 사용자의 지문 정보와 가장 유사도가 높은 평면을 생성하는 것으로, 단위 해쉬 테이블 평면 생성부는 최초 등록 해쉬 테이블과 참조 등록 해쉬 테이블을 이용하여 사용자의 지문 정보와 가장 유사한 지문 정보를 등록할 수 있는 단위 해쉬 테이블 평면을 생성한다.

<87> 종래의 인증 사용자의 지문 정보는 인증 사용자의 하나의 지문 정보를 기반으로 특징점들을 복수 군으로 분류하여, 이를 기반으로 해쉬 테이블 평면을 복수 개 생성하게 되는데, 이는 인증 사용자의 지문 등록에 있어서 대량

의 지문 데이터 저장 공간을 필요로 하며, 복수 명의 인증 사용자의 지문 정보를 저장해야 할 경우, 지문 정보의 저장 공간이 방대해 지게 되고, 하나의 지문 정보를 기반으로 인증 사용자를 인식하여야 하므로, 인식률이 저하되게 된다.

<88> 따라서, 본 발명은 최초 지문 정보와 참조 지문 정보를 기반으로 생성된 해쉬 테이블을 기반으로 하여 인증 사용자의 정확한 단위 해쉬 테이블 평면 하나만을 기반으로 인증 사용자의 지문 정보를 등록하게 되므로, 인증 사용자의 지문 정보의 저장 공간을 최소화할 수 있고, 정확한 인식률에 따른 인증 사용자의 인증을 수행할 수 있게 된다.

<89> 제 1 다항식 생성부(340)는 상기 단위 해쉬 테이블 생성부(330)에서 생성된 단위 해쉬 테이블 평면에 존재하는 인증 사용자의 지문 정보를 계수로 하는 제 1 다항식을 생성한다. 여기서 상기 제 1 다항식의 차수는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라 임의로 정할 수 있는 차수로 정의한다.

<90> 이와 같이, 제 1 다항식은 하기의 수학식 1과 같이 생성할 수도 있으며, 실시 형태 및 사용 태양에 따라 본 발명의 구성을 해하지 않은 범위 내에서 다양하게 구성할 수 있다.

수학식 1

<91>
$$p(x) = a_{n-1}x^{0} + a_{n-2}x^{1} \cdots a_{0}x^{n-1}$$

<92> 여기서, $a_{n-1}, a_{n-2}, \cdots, a_0$ 는 n 개의 지문 정보 중의 각각의 지문 정보를 의미하며, 상기 각각의 지문 정보에 따른 계수를 기반으로 제 1 다항식 $p(x)$ 가 생성된다.

<93> 사용자 지문 정보는 x, y 좌표, 각도, 및 융선의 단점 또는 분기점으로 이루어진 지문 타입으로 이루어지는데, 이는 $n-1$ 차 다항식을 설계할 경우, n 개의 계수가 필요하다.

<94> 즉, n 개의 계수를 $a_{n-1}, a_{n-2}, \cdots, a_0$ 로 설정하여 $p(x)$ 의 $n-1$ 차 다항식을 설계할 수 있다.

<95> 이와 같은 과정으로 상기 다항식의 계수를 연결하여 k 비트의 데이터인 $a_{n-1} \mid a_{n-2} \mid \cdots \mid a_0$ 를 생성하여 저장하게 된다.

<96> 가짜 특징점 정보 삽입부(350)는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라서 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 특징점 정보를 상기 단위 해쉬 테이블 평면에 삽입한다.

<97> 상세하게는, 가짜 특징점 정보 삽입부(350)는 인증 사용자의 지문 정보에 포함된 특징점의 위치 좌표 및 각도로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 추출된 지문 정보에 삽입하게 된다. 이때, 특징점의 위치 좌표 및 각도로 구성된 가짜 지문 정보를 랜덤하게 복수 개 생성하여 사용자의 지문 정보와 구별할 수 없게 하는 것이다.

<98> 가짜 지문 정보를 삽입할 경우에, 특징점의 위치 좌표 및 각도를 고려하여 삽입하여 인증 사용자의 은닉 지문 정보를 생성하게 된다.

<99> 데이터 베이스(360)는 상기 생성된 제 1 다항식 및 가짜 특징점이 삽입된 단위 등록 해쉬 테이블을 저장한다.

<100> 상기 데이터 베이스는 비휘발성 메모리 소자, 메모리 소자 또는 하드 디스크 드라이브, 광학 기록매체 등을 포함할 수 있다.

<101> 도 4는 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템의 블록도를 도시한 것이다.

<102> 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템은 인증을 수행하고자 하는 사용자의 지문 정보를 추출하는 입력부(410), 인증 사용자의 지문 정보를 저장하는 지문 데이터 저장부(420) 및 사용자의 인증을 수행하는 수신부(420)를 포함할 수 있다.

<103> 그리고, 상기 입력부(410)는 입력 지문 정보 추출부(411) 및 입력 해쉬 테이블 생성부(412)를 포함한다.

<104> 입력 지문 정보 추출부(411)는 사용자의 지문 영상에서 입력 지문 정보를 추출한다.

<105> 이는 상술한 바와 같이, 인증을 수행하고자 하는 사용자의 지문 영상에서 입력 센싱 장치를 이용하여 특징점의 위치 좌표 및 각도로 구성되는 입력 지문 정보를 추출한다.

<106> 입력 해쉬 테이블 생성부(412)는 상기 사용자의 지문 영상으로부터 추출된 지문 정보를 기하학적으로 변환하여 입력 해쉬 테이블을 생성한다.

<107> 한편, 지문 데이터 저장부(430)에 포함된 등록 해쉬 테이블 생성부(431)는 인증 사용자의 최초 지문 정보를 이용하여 최초 등록 해쉬 테이블을 생성하고, 상기 인증 사용자의 참조 지문 정보를 이용하여 참조 등록 해쉬 테이블을 생성한다.

<108> 상세하게는, 상기 등록 해쉬 테이블 생성부(431)는 최초 지문 정보 기준점 선정 모듈(431a), 참조 지문 정보 기준점 선정 모듈(431b), 최초 지문 정보 특징점 이동모듈(431c) 및 참조 지문 정보 특징점 이동 모듈(431d)을 포함할 수 있다.

<109> 최초 지문 정보 기준점 선정 모듈(431a)은 인증 사용자의 최초 지문 정보의 특징점 중 기준점을 선정하고, 참조 지문 정보 기준점 선정 모듈(431b)은 인증 사용자의 참조 지문 정보의 특징점 중 기준점을 선정한다.

<110> 그러면, 최초 지문 정보 특징점 이동모듈(431c)은 상기 최초 지문 정보의 기준점을 기준으로 나머지 최초 지문 정보의 특징점을 기하학적으로 이동시켜서 최초 등록 해쉬 테이블을 생성한다.

<111> 참조 지문 정보 특징점 이동 모듈(431d)은 상기 참조 지문 정보의 기준점을 기준으로 나머지 참조 지문 정보의 특징점을 기하학적으로 이동시켜서 참조 등록 해쉬 테이블을 생성한다.

<112> 그 다음, 단위 해쉬 테이블 평면 생성부(432)는 상기 최초 등록 해쉬 테이블 및 상기 참조 등록 해쉬 테이블을 이용하여 단위 해쉬 테이블 평면을 생성한다.

<113> 이는 두 개 이상의 지문이 기하학적 해싱 기법을 이용하여 생성된 인증 사용자의 지문 정보와 가장 유사도가 높은 평면을 생성하는 것으로, 단위 해쉬 테이블 평면 생성부는 최초 등록 해쉬 테이블과 참조 등록 해쉬 테이블을 이용하여 사용자의 지문 정보와 가장 유사한 지문 정보를 등록할 수 있는 단위 해쉬 테이블 평면을 생성한다.

<114> 종래의 인증 사용자의 지문 정보는 인증 사용자의 하나의 지문 정보를 기반으로 특징점들을 복수군으로 분류하여, 이를 기반으로 해쉬 테이블 평면을 복수개 생성하게 되는데, 이는 인증 사용자의 지문 등록에 있어서 대량의 지문 데이터 저장 공간을 필요로 한다.

<115> 그리고, 복수 명의 인증 사용자의 지문 정보를 저장해야 할 경우, 지문 정보의 저장 공간이 방대해 지게 되고, 하나의 지문 정보를 기반으로 인증 사용자를 인식하여야 하므로, 인식률이 저하되게 된다.

<116> 따라서, 본 발명은 최초 지문 정보와 참조 지문 정보를 기반으로 생성된 해쉬 테이블을 기반으로 하여 인증 사용자의 정확한 단위 해쉬 테이블 평면 하나만을 기반으로 인증 사용자의 지문 정보를 등록하게 되므로, 인증 사용자의 지문 정보의 저장 공간을 최소화 할 수 있고, 정확한 인식률에 따른 인증 사용자의 인증을 수행할 수 있게 된다.

<117> 다항식 생성부(433)는 상기 단위 해쉬 테이블 평면 생성부(432)에서 생성된 단위 해쉬 테이블 평면에 존재하는 인증 사용자의 지문 정보를 계수로 하는 제 1 다항식을 생성한다. 여기서 상기 제 1 다항식의 차수는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라 임의로 정할 수 있는 차수로 정의한다.

<118> 이와 같이, 제 1 다항식은 상기의 수학식 1과 같이 생성할 수 있다.

<119> 가짜 특징점 정보 삽입부(434)는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라서 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 특징점 정보를 상기 단위 해쉬 테이블 평면에 삽입한다.

<120> 상세하게는, 가짜 특징점 정보 삽입부(434)는 인증 사용자의 지문 정보에 포함된 특징점의 위치 좌표 및 각도로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 추출된 지문 정보에 삽입하게 된다. 이때, 특징점의 위치 좌표 및 각도로 구성된 가짜 지문 정보를 랜덤하게 복수 개 생성하여 사용자의 지문 정보와 구별할 수 없게 하는 것이다.

<121> 가짜 지문 정보를 삽입할 경우에, 특징점의 위치 좌표 및 각도를 고려하여 삽입하여 인증 사용자의 은닉 지문

정보를 생성하게 된다.

<122> 데이터 베이스(435)는 상기 생성된 제 1 다항식 및 가짜 특징점이 삽입된 단위 등록 해쉬 테이블 평면을 저장한다.

<123> 한편, 수신 해쉬 테이블 생성부(421)는 상기 입력 해쉬 테이블 및 상기 단위 등록 해쉬 테이블을 이용하여 수신 해쉬 테이블을 생성한다.

<124> 이는, 상기 입력 해쉬 테이블 생성부(412)에서 전송된 입력 해쉬 테이블 및 상기 데이터베이스(435)에서 전송된 단위 등록 해쉬 테이블을 이용하여 기준점을 추출하는 기준점 후보 추출부(미도시)를 포함할 수 있다.

<125> 수신 해쉬 테이블 생성부(421)는 상기 입력 해쉬 테이블 및 상기 데이터 베이스(435)에 저장된 단위 등록 해쉬 테이블을 이용하여 수신 해쉬 테이블을 생성한다.

<126> 이는 데이터 베이스(435)에 저장된 지문 정보와 입력 해쉬 테이블 생성부(412)에서 생성된 입력 해쉬 테이블을 상호 비교하여 기준점 후보를 추출하고, 상기 추출된 기준점을 이용하여 수신 해쉬 테이블을 생성한다.

<127> 상세하게는, 상기 수신 해쉬 테이블 생성부(421)는 상기 입력 해쉬 테이블 생성부(412)에서 전송된 입력 해쉬 테이블 및 상기 데이터베이스(435)에서 전송된 단위 등록 해쉬 테이블을 이용하여 기준점을 추출하는 기준점 후보 추출부(미도시)를 포함할 수 있다.

<128> 이와 더불어, 지문 정보 정렬부(422)는 상기 추출된 기준점에 의해 생성된 수신 해쉬 테이블 및 상기 입력 해쉬 테이블을 정합하여 정렬한다.

<129> 그리고, 상기 수신 해쉬 테이블 및 입력 해쉬 테이블에 저장된 지문 정보를 기반으로 데이터 정합 및 정렬된 지문 정보에 에러 정보가 포함될 가능성이 있으므로 에러 정정부(미도시)를 거쳐서 진짜 특징점을 추출하게 된다.

<130> 그러면, 다항식 복원부(423)에서 상기 추출된 특징점을 기반으로 제 2 다항식을 생성하게 된다.

<131> 이는, 상기 추출된 특징점($x1, x2, \cdots, x_n$)을 하기 수학식 2에 대입하여 $a_{n-1}, a_{n-2}, \cdots, a_0$의 값을 연산하여, 상기 연산된 계수 값과 상기 수학식 1의 계수 값을 비교하게 된다.

수학식 2

<132> $$p(x1) = a_{n-1}x1^{0} + a_{n-2}x1^{1} \cdots a_0 x1^{n-1}$$

<133> $$p(x2) = a_{n-1}x2^{0} + a_{n-2}x2^{1} \cdots a_0 x2^{n-1}$$

<134> $\cdots$

<135> $$p(x_n) = a_{n-1}x_n^{0} + a_{n-2}x_n^{1} \cdots a_0 x_n^{n-1}$$

<136> 이는, 상기 수학식 1에서 $p(x)$의 $n-1$ 차 다항식을 설계할 경우, 상기 수학식 2와 같이 n개의 방정식을 획득한다면, 연립방정식에 의하여 $a_{n-1}, a_{n-2}, \cdots, a_0$의 계수를 복원하여 제 2 다항식을 생성할 수 있게 된다.

<137> 마지막으로, 사용자 인증부(424)에서 상기 제 1 다항식과 제 2 다항식을 비교하여 사용자 인증의 결과를 검증한다.

<138> 즉, 전술한 바와 같이 상기 수학식 1에 따른 상기 제 1 다항식과 상기 수학식 2에 따라 복원된 제 2 다항식을 비교하여, 두 다항식의 일치 여부에 따라 사용자 인증을 수행하게 되는 것이다.

<139> 도 5는 본 발명에 따른 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법의 흐름도이다.

<140> 도 5를 참조하면, 우선, 센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상에서 특징점으로 구성되는 최초 지문 정보를 추출하고, 상기 최초 지문 정보의 특징점을 이용하여 최초 등록 해쉬 테이블을 생성한다(510 과정).

<141> 이는 특정의 센싱 장치를 이용하여 인증 사용자의 지문 영상을 최초로 입력받고, 지문 영상에서 특징점의 위치 좌표 및 각도를 포함하는 지문 정보를 추출한다.

<142> 상기 최초 지문 정보는 인증 사용자의 조작에 따라서 초기화된 다음, 다시 인증 사용자에 의해 최초 지문 영상이 입력될 수 있다.

<143> 그러면, 상기 추출된 인증 사용자의 최초 지문 정보에 포함된 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 최초 지문 정보의 특징점들을 기하학적으로 이동시켜서 최초 등록 해쉬 테이블을 생성한다.

<144> 더욱 상세하게는, 선정된 기준점을 원점으로 이동시키고, 선정된 기준점의 각도를 미리 설정된 기준 각도로 변경한다. 이에 따라서 상대적으로 나머지 최초 지문 정보의 특징점들을 상기 선정된 기준점에 대응되는 위치로 기하학적으로 이동시켜 최초 등록 해쉬 테이블을 생성한다.

<145> 그 다음, 상기 센싱 장치를 이용하여 수신된 인증 사용자의 참조 지문 정보를 추출하고, 상기 참조 지문 정보의 특징점을 이용하여 참조 등록 해쉬 테이블을 생성한다(520 과정).

<146> 이 역시 마찬가지로 상기 특정의 센싱 장치를 이용하여 인증 사용자의 참조 지문 영상을 입력받고, 지문 영상에서 특징점의 위치 좌표 및 각도를 포함하는 참조 지문 정보를 추출한다.

<147> 상기 참조 지문 영상은 최초 지문 정보 추출부에 의해 인증 사용자의 최초 지문 정보을 추출한 다음, 인증 사용자에 의해 입력된 지문 영상으로서, 인증 사용자에 의해 복수 회에 걸쳐 입력될 수 있다.

<148> 그리고, 참조 지문 정보 역시 인증 사용자의 조작에 따라 참조 지문 정보를 초기화 한 다음, 다시 복수 회에 걸쳐 인증 사용자에 의해 참조 지문 영상이 입력될 수 있다.

<149> 그러면, 추출된 인증 사용자의 참조 지문 정보에 포함된 특징점 중 기준점을 선정하고, 상기 선정된 기준점을 기반으로 나머지 참조 지문 정보의 특징점들을 기하학적으로 이동시켜서 참조 등록 해쉬 테이블을 생성한다.

<150> 여기서, 복수 회에 걸쳐서 인증 사용자의 참조 지문 정보를 추출한 경우, 참조 지문 정보에 포함된 특징점 중 기준점은 상기 복수 회의 참조 지문 정보의 특징점 중 사용자에 의해 정해진 특정 특징점에 해당되는 점을 취할 수 있다.

<151> 그 다음, 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성한다(530 과정).

<152> 이는 두 개 이상의 지문이 기하학적 해싱 기법을 이용하여 생성된 인증 사용자의 지문 정보와 가장 유사도가 높은 평면을 생성하는 것으로, 단위 해쉬 테이블 평면 생성부는 최초 등록 해쉬 테이블과 참조 등록 해쉬 테이블을 이용하여 사용자의 지문 정보와 가장 유사한 지문 정보를 등록할 수 있는 단위 해쉬 테이블 평면을 생성한다.

<153> 종래의 인증 사용자의 지문 정보는 인증 사용자의 하나의 지문 정보를 기반으로 특징점들을 복수 군으로 분류하여, 이를 기반으로 해쉬 테이블 평면을 복수개 생성하게 되는데, 이는 인증 사용자의 지문 등록에 있어서 대량의 지문 데이터 저장 공간을 필요로 한다.

<154> 그리고, 복수 명의 인증 사용자의 지문 정보를 저장해야 할 경우, 지문 정보의 저장 공간이 방대해 지게 되고, 하나의 지문 정보를 기반으로 인증 사용자를 인식하여야 하므로, 인식률이 저하되게 된다.

<155> 따라서, 본 발명은 최초 지문 정보와 참조 지문 정보를 기반으로 생성된 해쉬 테이블을 기반으로 하여 인증 사용자의 정확한 단위 해쉬 테이블 평면 하나만을 기반으로 인증 사용자의 지문 정보를 등록하게 되므로, 인증 사용자의 지문 정보의 저장 공간을 최소화 할 수 있고, 정확한 인식률에 따른 인증 사용자의 인증을 수행할 수 있게 된다.

<156> 그 다음, 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성한다(540 과정)

<157> 이는, 상기 생성된 단위 해쉬 테이블 평면에 존재하는 인증 사용자의 지문 정보를 계수로 하는 제 1 다항식을 생성하는 것이다.. 여기서 상기 제 1 다항식의 차수는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라 임의로 정할 수 있는 차수로 정의한다.

<158> 이와 같이, 제 1 다항식은 상기의 수학식 1과 같이 생성할 수 있다.

<159> 마지막으로, 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장한다(550 과정).

<160> 가짜 특징점 정보는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라서 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 특징점 정보를 상기 단위 해쉬 테이블 평면에 삽입한다.

<161> 상세하게는, 가짜 정보는 인증 사용자의 지문 정보에 포함된 특징점의 위치 좌표 및 각도로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 추출된 지문 정보에 삽입하게 된다. 이때, 특징점의 위치 좌표 및 각도로 구성된 가짜 지문 정보를 랜덤하게 복수 개 생성하여 사용자의 지문 정보와 구별할 수 없게 하는 것이다.

<162> 가짜 지문 정보를 삽입할 경우에, 특징점의 위치 좌표 및 각도를 고려하여 삽입하여 인증 사용자의 은닉 지문 정보를 생성하게 된다.

<163> 그런 후, 상기 생성된 제 1 다항식 및 가짜 특징점이 삽입된 단위 등록 해쉬을 데이터 베이스에 저장한다.

<164> 상기 데이터 베이스는 비휘발성 메모리 소자, 메모리 소자 또는 하드 디스크 드라이브, 광학 기록매체 등을 포함할 수 있다.

<165> 도 6은 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법의 흐름도를 도시한 것이다.

<166> 도 6을 참조하면 우선, 센싱 장치를 이용하여 수신된 인증 사용자의 최초 지문 영상 및 참조 지문 영상으로부터 특징점들로 구성되는 최초 지문 정보 및 참조 지문 정보를 추출하고, 상기 추출된 최초 지문 정보 및 참조 지문 정보 각각의 특징점을 이용하여 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 생성한다(610 과정).

<167> 이는, 특정 센싱 장치를 이용하여 인증 사용자의 최초 지문 정보 및 참조 지문 정보를 수신하여 인증 사용자의 최초 지문 정보의 특징점 중 기준점을 선정하고, 인증 사용자의 참조 지문 정보의 특징점 중 기준점을 선정한다.

<168> 그러면, 최초 지문 정보 특징점 중 기준점을 선정하여 상기 최초 지문 정보의 기준점을 기준으로 나머지 최초 지문 정보의 특징점을 기하학적으로 이동시켜서 최초 등록 해쉬 테이블을 생성한다.

<169> 마찬가지로, 참조 지문 정보 특징점 중 기준점을 선정하여 상기 참조 지문 정보의 기준점을 기준으로 나머지 참조 지문 정보의 특징점을 기하학적으로 이동시켜서 참조 등록 해쉬 테이블을 생성하는 것이다.

<170> 그 다음, 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성하고, 상기 단위 등록 해쉬 테이블 평면을 이용하여 인증 사용자의 지문 정보가 포함된 제 1 다항식을 생성한다(620 과정).

<171> 즉, 최초 지문 정보와 참조 지문 정보를 기반으로 생성된 해쉬 테이블을 기반으로 하여 인증 사용자의 정확한 단위 해쉬 테이블 평면 하나만을 기반으로 인증 사용자의 지문 정보를 등록하게 되므로, 인증 사용자의 지문 정보의 저장 공간을 최소화 할 수 있고, 정확한 인식률에 따른 인증 사용자의 인증을 수행할 수 있도록, 상기 최초 등록 해쉬 테이블 및 참조 등록 해쉬 테이블을 이용하여 단위 등록 해쉬 테이블 평면을 생성한다.

<172> 그리고, 상기 생성된 단위 해쉬 테이블 평면에 존재하는 인증 사용자의 지문 정보를 계수로 하는 제 1 다항식을 생성한다. 여기서 상기 제 1 다항식의 차수는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라 임의로 정할 수 있는 차수로 정의한다.

<173> 이와 같이, 제 1 다항식은 상기의 수학식 1과 같이 생성할 수 있다.

<174> 그 다음, 상기 단위 등록 해쉬 테이블 평면에 가짜 특징점 정보를 삽입하고, 상기 제 1 다항식 및 상기 가짜 특징점 정보가 삽입된 단위 등록 해쉬 테이블을 데이터베이스에 저장한다(630 과정).

<175> 마찬가지로, 상기 데이터 베이스는 비휘발성 메모리 소자, 메모리 소자 또는 하드 디스크 드라이브, 광학 기록매체 등을 포함할 수 있다.

<176> 그 다음, 사용자의 지문 영상에서 입력 센싱 장치를 이용하여 특징점들로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적으로 변환하여 입력 해쉬 테이블을 생성한다(640 과정).

<177> 이는 데이터 베이스에 저장된 인증 사용자의 지문 정보와 인증을 수행하고자 하는 사용자의 지문 정보가 일치하

는지의 여부에 따라 인증을 수행하기 위하여 사용자가 지문 정보를 입력하는 과정이다.

<178> 그 다음, 상기 단위 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 가짜 특징점을 제거한다(650 과정).

<179> 즉, 상기 단위 등록 해쉬 테이블 및 입력 해쉬 테이블에 저장된 지문 정보를 기반으로 데이터 정합 및 정렬된 지문 정보에 에러 정보가 포함될 가능성이 있으므로 에러 정정을 통하여 진짜 특징점을 추출하게 되는 것이다.

<180> 마지막으로, 상기 정합된 지문 정보를 계수로 하는 제 2 다항식을 생성하고, 상기 제 1 다항식 및 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하는 단계를 포함하는 부분 기하학적 해싱을 이용한 지문 데이터 인증을 수행한다(660 과정).

<181> 이는, 상기 제 1 다항식과 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하는 것으로, 전술한 바와 같이 상기 수학식 1에 따른 상기 제 1 다항식과 상기 수학식 2에 따라 복원된 제 2 다항식을 비교하여, 두 다항식의 일치 여부에 따라 사용자 인증을 수행하게 되는 것이다.

<182> 필요에 따라, 사용자 인증과정에서 다항식의 복원이 성공한 경우, 사용자의 인증이 성공하였다는 인증 결과를 음성이나, 시각적 장치를 이용하여 사용자에게 알려줄 수 있다.

<183> 도 7은 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법의 전체적 흐름을 도시한 것이다.

<184> 도 7을 참조하면, 인증 사용자의 최초 지문(701)으로부터 최초 지문의 특징점(711)을 추출하고 상기 추출된 특징점으로부터 최초 등록 해쉬 테이블(721)을 생성하며, 인증 사용자의 참조 지문(702)으로부터 참조 지문의 특징점(712)을 추출하여 상기 추출된 특징점으로부터 참조 등록 해쉬 테이블(722)을 생성한다.

<185> 그 다음, 상기 최초 등록 해쉬 테이블(721) 및 참조 등록 해쉬 테이블(722)을 이용하여 신뢰성 높은 단위 등록 해쉬 테이블 평면(730)을 생성하고, 이를 기반으로 제 1 다항식을 생성하고, 생성된 제 1 다항식 및 가짜 특징점을 삽입한 단위 등록 해쉬 테이블 평면을 데이터 베이스에 저장(740)한다.

<186> 그런 후, 사용자의 지문 영상(750)에서 입력 센싱 장치를 이용하여 특징점들로 구성되는 입력 지문 정보를 추출(760)하고, 추출된 지문 정보를 기하학적으로 변환하여 입력 해쉬 테이블을 생성한다(770).

<187> 상기 단위 등록 해쉬 테이블 및 상기 입력 해쉬 테이블로부터 기준점 후보를 추출(780)하고, 기준점 후보를 이용하여 수신 해쉬 테이블을 생성(790)하여, 상기 입력 지문 정보 및 수신 해쉬 테이블을 정렬 및 정합을 수행하여, 정렬 및 정합을 수행한 수신 해쉬 테이블(799)에 저장된 지문 정보를 계수로 하는 제 2 다항식을 생성하고, 상기 제 1 다항식과 제 2 다항식을 비교하여 사용자 인증의 결과를 검증하게 된다.

<188> 도 8a는 종래의 지문 데이터 은닉 방법에 따라 생성된 등록 해쉬 테이블의 크기를 도시한 것이다.

<189> 도 8b는 본 발명에 따라 생성된 단위 등록 해쉬 테이블의 크기를 도시한 것이다.

<190> 도 8a와 도 8b를 비교하면, 본 발명에 따라 생성된 단위 등록 해쉬 테이블은 단위 등록 해쉬 테이블의 평면 하나만을 사용하여 지문 데이터를 은닉하므로, 종래의 등록 해쉬 테이블의 평균 높이는 238이고, 본 발명에 따른 단위 등록 해쉬 테이블의 크기는 20으로 본 발명에 따른 단위 등록 해쉬 테이블의 크기가 종래에 비하여 1/12의 크기에 불과하다는 것을 알 수 있다.

<191> 본 발명은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<192> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 테이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<193> 본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다. 그러나, 이와 같은 변형은 본 발명의 기술적 보호범위내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

도면의 간단한 설명

<194> 도 1은 지문 인식 시스템의 블럭도를 도시한 것이다.

<195> 도 2는 본 발명과 대비되는 지문 데이터의 등록 과정을 도시한 것이다.

<196> 도 3은 본 발명에 따른 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 장치의 블록도(300)를 도시한 것이다.

<197> 도 4는 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 시스템의 블록도를 도시한 것이다.

<198> 도 5는 본 발명에 따른 부분 기하학적 해싱을 이용한 은닉된 지문 데이터의 정렬 방법의 흐름도이다.

<199> 도 6은 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법의 흐름도를 도시한 것이다.

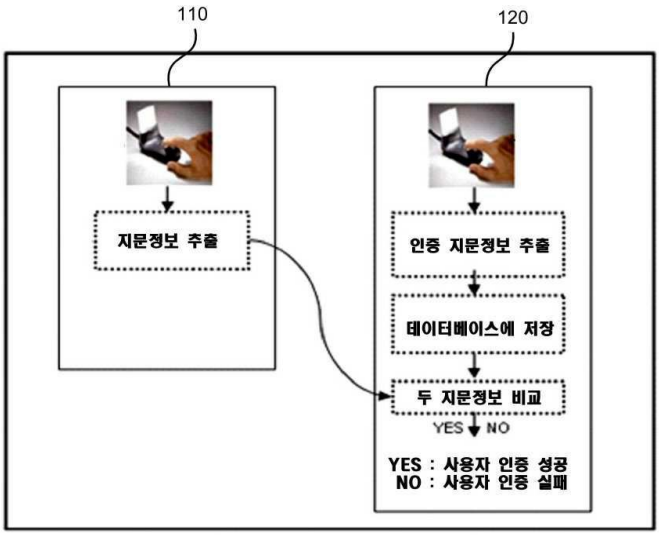
<200> 도 7은 본 발명에 따른 부분 기하학적 해싱을 이용한 지문 데이터 인증 방법의 전체적 흐름을 도시한 것이다.

<201> 도 8a는 종래의 지문 데이터 은닉 방법에 따라 생성된 등록 해쉬 테이블의 크기를 도시한 것이다.

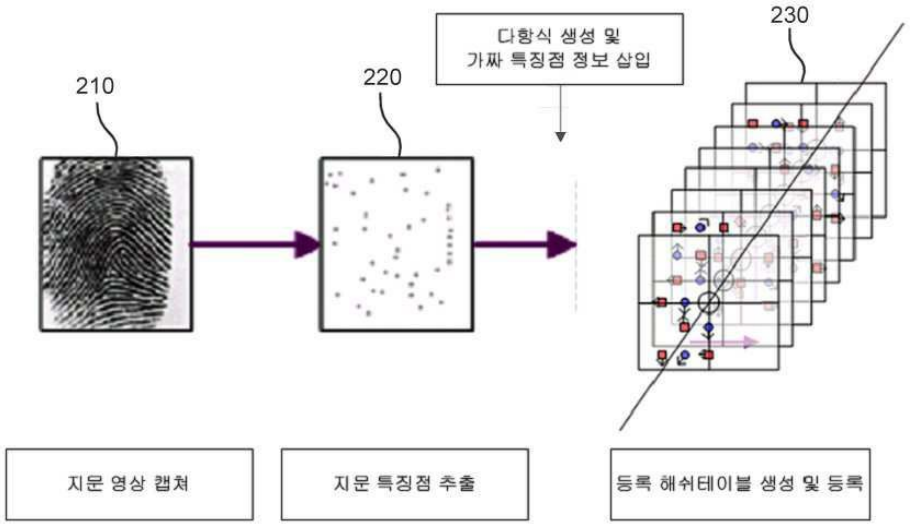
<202> 도 8b는 본 발명에 따라 생성된 단위 등록 해쉬 테이블의 크기를 도시한 것이다.

도면

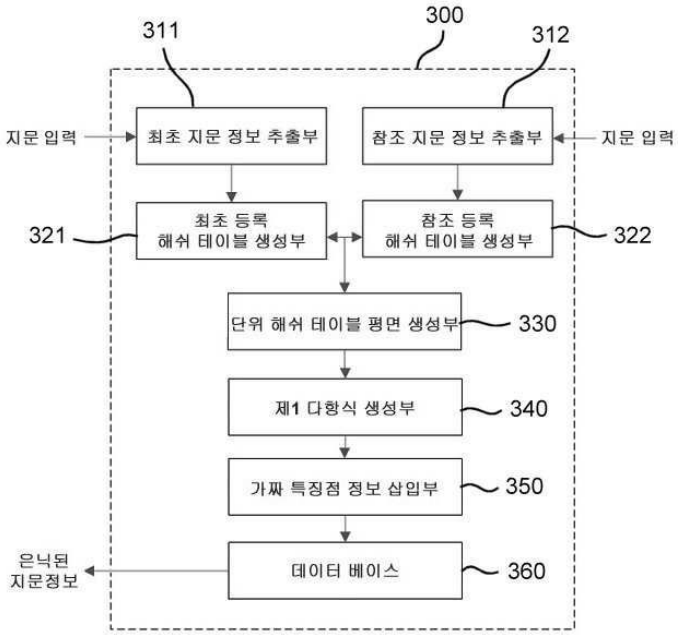
도면1



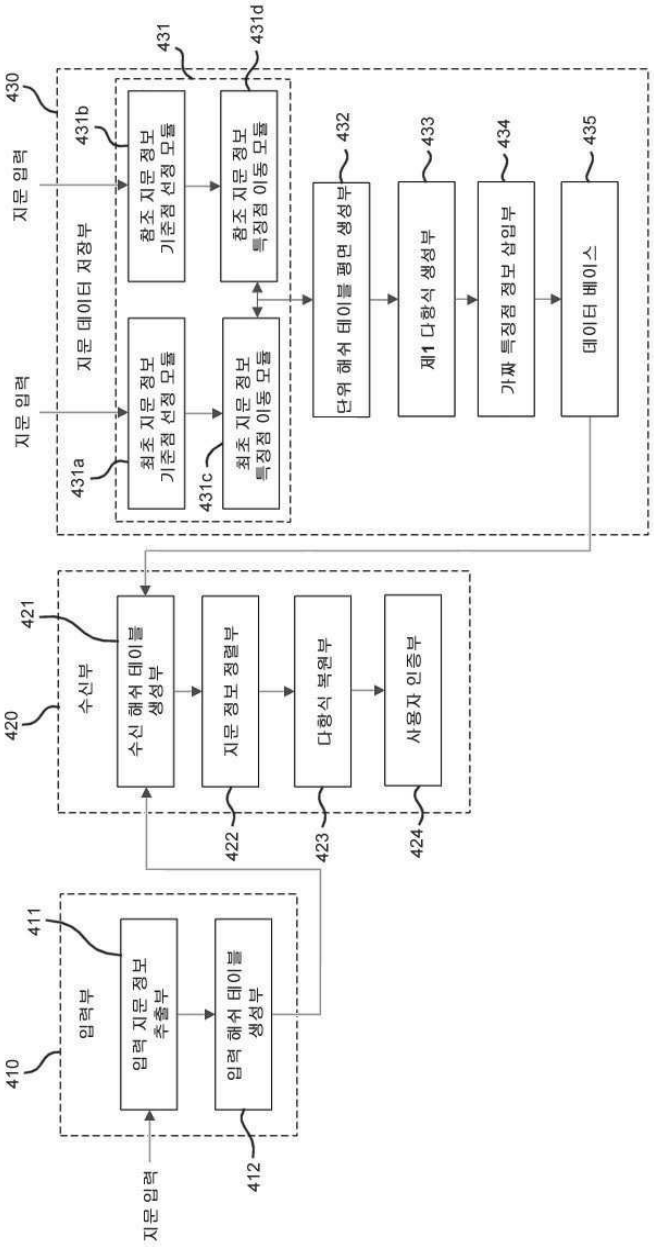
도면2


210
220
다항식 생성 및
가짜 특징점 정보 삽입
230
지문 영상 캡쳐
지문 특징점 추출
등록 해쉬테이블 생성 및 등록

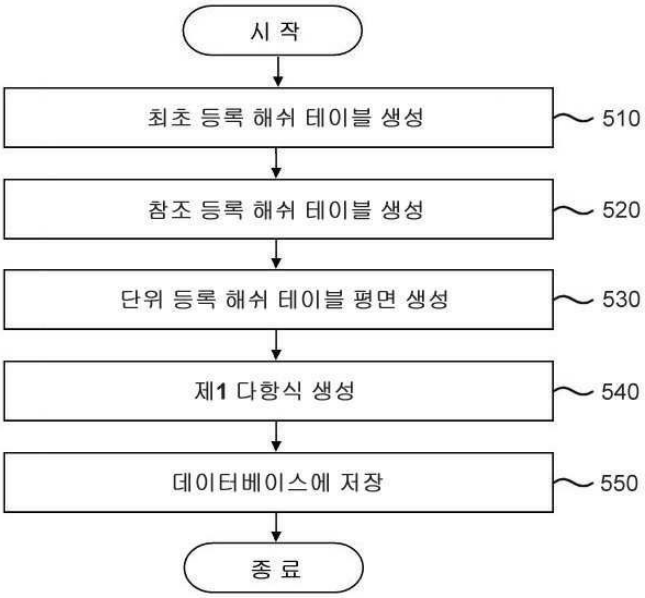
도면3


311
300
312
지문 입력
최초 지문 정보 추출부
참조 지문 정보 추출부
지문 입력
321
최초 등록
해쉬 테이블 생성부
참조 등록
해쉬 테이블 생성부
322
단위 해쉬 테이블 평면 생성부
330
제1 다항식 생성부
340
가짜 특징점 정보 삽입부
350
은닉된
지문정보
데이터 베이스
360

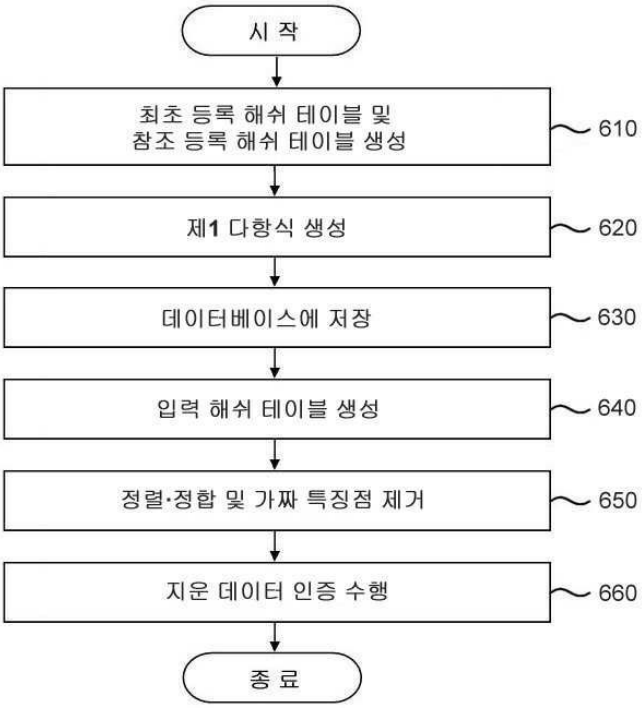
도면4


410
입력부
411
입력 지문 정보 추출부
입력 해쉬 테이블 생성부
412
지문 입력
420
수신부
421
수신 해쉬 테이블 생성부
422
지문 정보 정렬부
423
다항식 복원부
424
사용자 인증부
430
지문 데이터 저장부
지문 입력
431
431a
최초 지문 정보 기준점 선정 모듈
431b
참조 지문 정보 기준점 선정 모듈
431c
최초 지문 정보 특징점 이동 모듈
431d
참조 지문 정보 특징점 이동 모듈
432
단위 해쉬 테이블 평면 생성부
433
제1 다항식 생성부
434
가짜 특징점 정보 삽입부
435
데이터 베이스

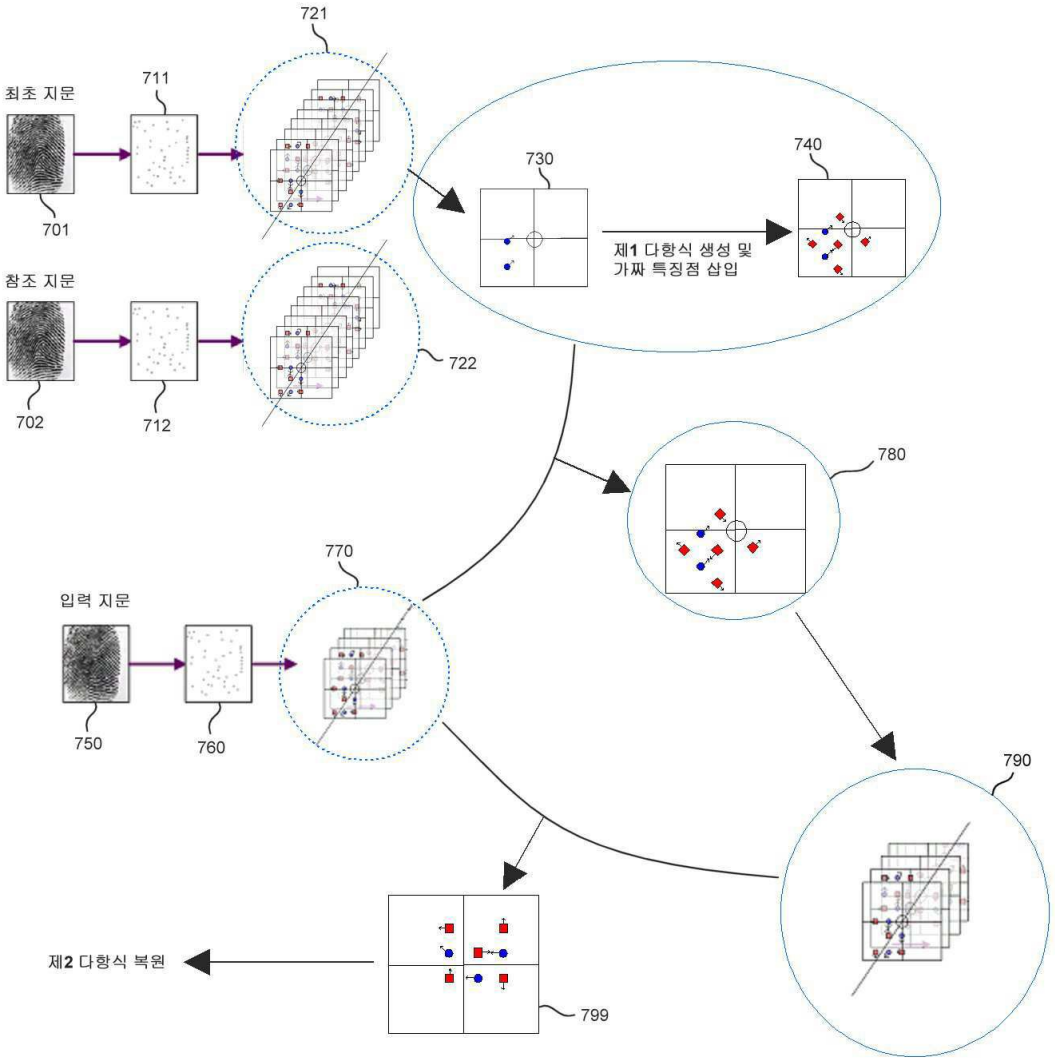
도면5


시 작
최초 등록 해쉬 테이블 생성
510
참조 등록 해쉬 테이블 생성
520
단위 등록 해쉬 테이블 평면 생성
530
제1 다항식 생성
540
데이터베이스에 저장
550
종 료

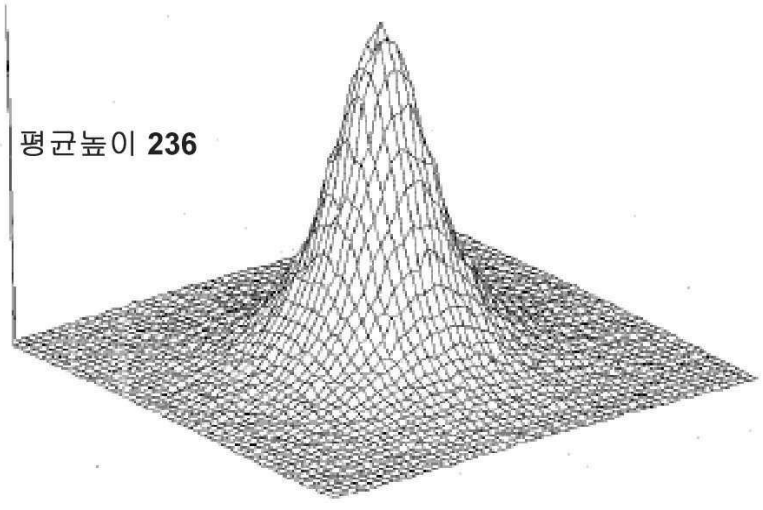
도면6


시 작
최초 등록 해쉬 테이블 및
참조 등록 해쉬 테이블 생성
610
제1 다항식 생성
620
데이터베이스에 저장
630
입력 해쉬 테이블 생성
640
정렬·정합 및 가짜 특징점 제거
650
지운 데이터 인증 수행
660
종 료

도면7


721
711
최초 지문
701
730
740
제1 다항식 생성 및
가짜 특징점 삽입
참조 지문
722
702
712
780
770
입력 지문
750
760
790
제2 다항식 복원
799

도면8a


평균높이 236

도면8b

