



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0070363
(43) 공개일자 2008년07월30일

(51) Int. Cl.

G06K 9/00 (2006.01) G06T 1/00 (2006.01)
G06K 9/52 (2006.01)

(21) 출원번호 10-2007-0008359

(22) 출원일자 2007년01월26일

심사청구일자 2007년01월26일

(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

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 7 항

(54) 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉방법, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치 및 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템

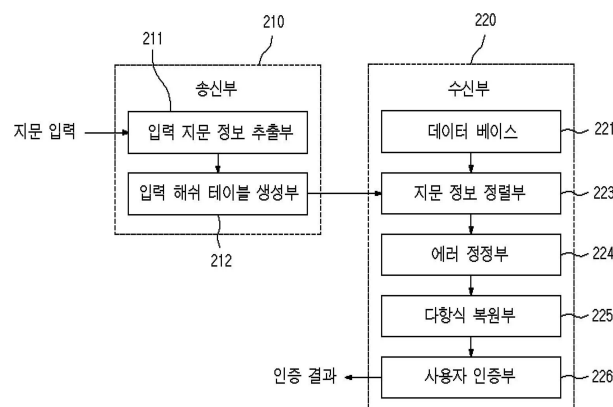
(57) 요약

퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치 및 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템이 개시된다.

본 발명은 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하는 단계, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하는 단계, 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 단계, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 복수의 그룹으로 분류하고, 상기 그룹마다 임의의 특징점을 기준점으로 선택하는 단계, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며, 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계 및 상기 제1다항식 및 상기 메모리 효율적인 등록 해쉬 테이블을 데이터 베이스에 저장하는 단계를 포함한다.

본 발명에 의하면, 생체정보를 안전하게 보호하기 위하여 퍼지 볼트 이론을 적용하고 메모리 효율적인 기하학적 해싱 기법을 적용함으로써, 인식률과 보안성을 저하시키지 않으면서 효과적으로 해쉬 테이블의 크기를 줄여 임베디드 시스템에서 시스템의 부하를 줄일 수 있고, 인증 과정에서도 다항식의 복원 과정을 이용하여 은닉된 지문 정보를 본래의 지문 정보로 복원하지 않고도 인증을 완료할 수 있어 지문 정보 해킹에 대한 안전성을 향상시킬 수 있다.

대표도 - 도2



(72) 발명자

문대성

대전 유성구 관평동 대덕테크노밸리 1단지 102동
2502호

조충호

충남 천안시 신부동 대림한들아파트 205동 1005호

신봉수

경기 수원시 영통구 영통동 988-2 살구골 서광아파
트 706동 603호

특허청구의 범위

청구항 1

센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하는 단계;

상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하는 단계;

가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 단계;

상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 복수의 그룹으로 분류하고, 상기 그룹마다 임의의 특징점을 기준점으로 선택하는 단계;

상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며, 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계; 및

상기 제1다항식 및 상기 메모리 효율적인 등록 해쉬 테이블을 데이터 베이스에 저장하는 단계를 포함하는 퍼지 볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법.

청구항 2

제 1 항에 있어서,

상기 기하학적으로 이동시키는 과정을 그룹마다 반복하는 단계는

상기 선택된 특징점과의 거리가 미리 설정된 해쉬 테이블 크기 이상인 특징점이 존재하면, 나머지 지문정보의 위치를 축소 변환하는 단계를 포함하는 것을 특징으로 하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법.

청구항 3

센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하며, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하고, 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 단계;

상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 복수의 그룹으로 분류하고, 상기 그룹마다 임의의 특징점을 기준점으로 선택하는 단계;

상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계;

사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점으로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성하는 단계;

상기 메모리 효율적인 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하는 단계;

상기 메모리 효율적인 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 상기 정합된 지문 정보로부터 가짜 특징점을 삭제하는 단계;

상기 정합된 지문 정보를 계수로 하는 제2다항식을 생성하는 단계; 및

상기 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증하는 단계를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법.

청구항 4

제 3 항에 있어서,

상기 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계는

상기 선택된 특징점과의 거리가 미리 설정된 해쉬 테이블 크기 이상인 특징점이 존재하면, 나머지 지문정보의 위치를 축소 변환하는 단계를 포함하는 것을 특징으로 하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법.

청구항 5

센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하는 지문정보 추출부;

상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하는 다항식 생성부;

가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 가짜 정보 삽입부;

상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택하며, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 메모리 효율적인 등록 해쉬 테이블 생성부; 및

상기 제1다항식 및 상기 메모리 효율적인 등록 해쉬 테이블을 저장하는 데이터 베이스를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치.

청구항 6

제 5 항에 있어서,

상기 메모리 효율적인 등록 해쉬 테이블 생성부는

상기 선택된 특징점과의 거리가 미리 설정된 해쉬 테이블 크기 이상인 특징점이 존재하면, 나머지 지문정보의 위치를 축소 변환하는 것을 특징으로 하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법.

청구항 7

사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점의 위치, 각도 및 형으로 구성되는 입력 지문 정보를 추출하는 입력 지문정보 추출부;

상기 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성하는 입력 해쉬 테이블 생성부;

센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하며, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하고, 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하고, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택하며, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 생성된 메모리 효율적인 등록 해쉬 테이블을 저장하는 데이터베이스;

상기 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하는 지문정보 정렬부;

상기 정렬된 등록 해쉬 테이블 및 입력 해쉬 테이블을 이용하여 상기 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 상기 정합된 지문 정보로부터 가짜 특징점을 삭제하는 에러 정정부;

상기 정합된 지문 정보를 계수로 하는 제2다항식을 생성하는 다항식 복원부; 및

상기 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증하는 사용자 인증부를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <17> 본 발명은 사용자 인증에 관한 것으로, 특히, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법, 그 기록매체, 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치 및 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템에 관한 것이다.
- <18> 급속한 정보화 및 인터넷의 발달로 인해 네트워크를 통한 정보의 교류가 활발해지고 온라인 banking 등 전자상거래와 관련된 산업의 규모가 커지면서 정확한 개인의 인증에 대한 요구가 증대되었다. 이러한 환경에서 가장 일반적인 인증 수단으로 PIN(Personal Identification Number) 또는 패스워드 방식이 사용이 되지만 유출 및 망각의 위험이 상존하므로 이에 따른 보안상의 문제가 최근 들어 크게 부각되고 있다. 이러한 방식의 단점을 해결할 수 있는 개인 인증기술로서 생체인식의 도입이 확산되고 있다.
- <19> 사용자 인증을 위해 저장된 생체정보가 타인에게 도용된다면 패스워드나 PIN과 달리 변경이 불가능하거나 변경이 제한적이기 때문에 심각한 문제를 일으킨다. 따라서, 암호, 워터마킹, 스테가노그래피(Steganography) 등의 기술을 이용하여 사용자의 중요한 지문정보를 보호하기 위한 연구가 활발히 진행되고 있다.
- <20> 지문인식 시스템은 경제적인 설치 비용과 보안성에 대한 매우 높은 신뢰성을 가지고 있고, 수백년 이상의 전세계적인 적용사례를 바탕으로 유일무이한 사람의 고유 특성으로 검증된 지문의 인식 시스템이다. 특히, 소형화된 시스템 구성이 가능하므로 이동성과 공간 활용 능력이 매우 높다. 특히, 요즘 네트워크의 발달과 더불어 보안 및 개인 사생활 보호에 대한 관심이 높아지면서 개인 인증 방법으로서의 지문 인식 기술은 화상인식기술분야 중에서 가장 각광받는 기술분야로 발전하고 있다. 이와 같은 지문인식기술은 단순한 출입통제 시스템에서 인터넷 banking, 전자정부 등의 원격응용 시스템으로 발전하고 있다.
- <21> 기하학적 해싱 기법을 퍼지 볼트 이론을 적용한 지문정보를 보호하는데 사용할 경우, 지문정보의 양과 지문정보를 보호하는데 사용되는 가짜 지문정보의 양이 많아질수록 등록과정에서 메모리의 사용량이 많아진다. 왜냐하면 기하학적 해싱 기법은 전체의 진짜와 가짜의 정보를 기준점으로 하여 기하학적 해쉬 테이블을 생성하기 때문이다.
- <22> 따라서, 종래의 지문 정보 은닉 및 인증 방법은 유비쿼터스 환경의 임베디드 시스템 등에서 과다한 메모리 사용으로 시스템의 부하를 과중시키고, 단순히 해쉬 테이블의 크기를 줄이면 보안성과 인식률 등의 성능이 저하되는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <23> 따라서, 본 발명이 이루고자 하는 첫번째 기술적 과제는 생체정보를 안전하게 보호하기 위하여 퍼지 볼트 이론을 적용하고 메모리 효율적인 기하학적 해싱 기법을 적용함으로써, 인식률과 보안성을 저하시키지 않으면서 효과적으로 해쉬 테이블의 크기를 줄여 임베디드 시스템에서 시스템의 부하를 줄일 수 있는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법을 제공하는 데 있다.
- <24> 본 발명이 이루고자 하는 두번째 기술적 과제는 생체정보를 안전하게 보호하기 위하여 퍼지 볼트 이론을 적용하고 메모리 효율적인 기하학적 해싱 기법을 적용함으로써, 인식률과 보안성을 저하시키지 않으면서 효과적으로 해쉬 테이블의 크기를 줄여 임베디드 시스템에서 시스템의 부하를 줄일 수 있고, 인증 과정에서도 다항식의 복원 과정을 이용하여 은닉된 지문 정보를 본래의 지문 정보로 복원하지 않고도 인증을 완료할 수 있어 지문 정보 해킹에 대한 안전성을 향상시킬 수 있는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법을 제공하는 데 있다.
- <25> 본 발명이 이루고자 하는 세번째 기술적 과제는 상기의 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법이 적용된 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치를 제공하는 데 있다.
- <26> 본 발명이 이루고자 하는 네번째 기술적 과제는 상기의 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법이 적용된 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템을 제공하는 데 있다.

발명의 구성 및 작용

- <27> 상기의 첫번째 기술적 과제를 이루기 위하여, 본 발명은 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력

받고, 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하는 단계, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하는 단계, 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 단계, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 복수의 그룹으로 분류하고, 상기 그룹마다 임의의 특징점을 기준점으로 선택하는 단계, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며, 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계 및 상기 제1다항식 및 상기 메모리 효율적인 등록 해쉬 테이블을 데이터베이스에 저장하는 단계를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법을 제공한다.

<28> 상기의 두번째 기술적 과제를 이루기 위하여, 본 발명은 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력 받고 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하며, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하고, 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 단계, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 복수의 그룹으로 분류하고, 상기 그룹마다 임의의 특징점을 기준점으로 선택하는 단계, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 단계, 사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점으로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성하는 단계, 상기 메모리 효율적인 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하는 단계, 상기 메모리 효율적인 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 상기 정합된 지문 정보로부터 가짜 특징점을 삭제하는 단계, 상기 정합된 지문 정보를 계수로 하는 제2다항식을 생성하는 단계 및 상기 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증하는 단계를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법을 제공한다.

<29> 상기의 세번째 기술적 과제를 이루기 위하여, 본 발명은 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력 받고, 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하는 지문정보 추출부, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하는 다항식 생성부, 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하는 가짜 정보 삽입부, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택하며, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문 정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 메모리 효율적인 등록 해쉬 테이블을 생성하는 메모리 효율적인 등록 해쉬 테이블 생성부 및 상기 제1다항식 및 상기 메모리 효율적인 등록 해쉬 테이블을 저장하는 데이터 베이스를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치를 제공한다.

<30> 상기의 네번째 기술적 과제를 이루기 위하여, 본 발명은 사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점의 위치, 각도 및 형으로 구성되는 입력 지문 정보를 추출하는 입력 지문정보 추출부, 상기 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성하는 입력 해쉬 테이블 생성부, 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하며, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하고, 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성하고, 상기 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택하며, 상기 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 상기 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복하여 생성된 메모리 효율적인 등록 해쉬 테이블을 저장하는 데이터베이스, 상기 등록 해쉬 테이블 및 상기 입력 해쉬 테이블을 정렬하는 지문정보 정렬부, 상기 정렬된 등록 해쉬 테이블 및 입력 해쉬 테이블을 이용하여 상기 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 상기 정합된 지문 정보로부터 가짜 특징점을 삭제하는 에러 정정부, 상기 정합된 지문 정보를 계수로 하는 제2다항식을 생성하는 다항식 복원부 및 상기 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증하는 사용자 인증부를 포함하는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템을 제공한다.

<31> 생체인증 시스템 및 지문 인증 시스템은 사용자의 생체정보를 데이터베이스등에 등록시키는 등록과정과 사용자의 인증을 위한 검증과정으로 나누어진다.

<32> 본 발명에서는 퍼지 볼트 이론을 이용하여 안전하게 보호된 지문을 등록할 때, 인증시스템에서 필요한 중간과정인 정렬(alignment) 방법으로 사용되는 기하학적 해싱(Geometric Hashing) 기법을 수정하여 메모리 효율적으로

등록과정을 수행한다. 즉, 등록과정에서 가짜 특징점과 관계없이 진짜 특징점을 기준점으로 사용하는 메모리 효율적인 방법을 적용함으로써 인식률과 보안성의 성능을 저하하지 않고 수행성능을 높일 수 있다.

- <33> 본 발명에서는 지문정보를 보호하는 방법으로 퍼지 볼트 이론을 사용한다. 또, 은닉된 지문정보와 사용자가 인증을 위해 요청한 지문정보를 비교하는 지문정보 정렬단계에서는, 기준점 부재 및 시스템 부하 문제를 해결하기 위해 메모리 효율적인 기하학적 해싱 기법을 사용할 수 있다. 그리고, 정렬된 두 지문정보의 결과로 추출된 결과에서 에러를 정정하기 위해 에러정정코드(Error Correction Code)를 사용한다.
- <34> 본 발명에 이용되는 메모리 효율적인 등록 해쉬 테이블은 은닉되어있는 지문정보가 정렬을 위해 새로운 좌표를 갖는 테이블을 의미한다. 본 발명에 이용되는 입력 해쉬 테이블은 사용자가 인증을 위해 입력한 지문정보가 정렬을 위해 새로운 좌표를 갖는 테이블을 의미한다.
- <35> 도 1은 지문인식 시스템의 블록도이다.
- <36> 지문인식 시스템은 지문영상에서 지문정보를 추출하는 송신부와 지문영상에서 추출된 지문정보를 이용하여 인증과정을 수행하는 수신부로 나누어질 수 있다.
- <37> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시예를 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다.
- <38> 도 2는 본 발명의 일 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템의 블록도이다.
- <39> 송신부(210)는 입력 지문정보 추출부(211) 및 입력 해쉬 테이블 생성부(212)를 포함한다.
- <40> 입력 지문정보 추출부(211)는 사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점의 위치, 각도 및 형으로 구성되는 입력 지문 정보를 추출한다. 바람직하게는, 입력센싱장치는 지문 스캐너를 포함할 수 있다. 이하에서는 특징점의 형이란, 지문 영상에서 지문 선이 분기되는 특징점, 지문 선이 끊어지는 특징점 등 특징점의 타입을 의미한다.
- <41> 입력 해쉬 테이블 생성부(212)는 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성한다.
- <42> 수신부(220)는 데이터베이스(221), 지문정보 정렬부(223), 에러 정정부(224), 다항식 복원부(225) 및 사용자 인증부(226)를 포함한다.
- <43> 데이터베이스(221)는 메모리 효율적인 등록 해쉬 테이블을 저장한다.
- <44> 메모리 효율적인 등록 해쉬 테이블은 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택하며, 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하며 선택된 특징점에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 그룹마다 반복하여 생성된다. 이때, 은닉 지문 정보는 미리 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고 상기 지문 영상에서 특징점으로 구성되는 지문 정보를 추출하며, 상기 추출된 지문 정보를 계수로 하는 제1다항식을 생성하고, 랜덤하게 생성된 가짜 특징점으로 구성되는 복수의 가짜 지문 정보를 상기 추출된 지문 정보에 삽입하여 생성된다.
- <45> 이하에서는 제1다항식의 차수는 보안 시스템의 설계자가 고려하는 보안성 정도에 따라 임의로 정할 수 있는 차수로 정의한다.
- <46> 이때, 인증 사용자란 본 발명이 이용되는 출입통제 시스템, 인터넷 뱅킹, 전자정부의 원격응용 시스템 등에서 미리 사용을 허가받은 사용자를 의미한다. 이때, 제1다항식은 지문 데이터 인증의 기준이 되는 다항식을 의미한다.
- <47> 지문정보 정렬부(223)는 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 정렬한다. 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 정렬하는 이유는 사용자로부터 지문 정보를 추출할 때마다 얼라이먼트가 조금씩 어긋날 수 있는데, 이러한 얼라이먼트를 조정하지 않으면, 입력받은 지문 정보와 미리 저장된 지문 정보의 특징점을 서로 비교할 수 없기 때문이다.
- <48> 에러 정정부(224)는 정렬된 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 이용하여 지문 정보를 정합한 후, 에러 정정 코드(Error Correction Code, ECC)를 이용하여 정합된 지문 정보로부터 가짜 특징점을 삭제한다. 이때, 정합이란, 비교 대상인 두 지문 정보 즉, 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블

에서 일정한 바운더리(boundary)의 쓰레쉬홀드(threshold) 이내에, 매칭되는 특징점들이 존재하도록 하는 것이다.

<49> 다항식 복원부(225)는 정합된 지문 정보를 계수로 하는 제2다항식을 생성한다. 이때, 제2다항식은 인증의 대상이 되는 지문 정보에 대한 다항식을 의미한다.

<50> 제1다항식 및 제2다항식은 다음의 수학식 1과 같이 생성될 수 있다.

수학식 1

$$p = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0$$

<51> a_i : 하나의 지문정보

<52> 사용자 인증부(226)는 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증한다. 이때, 제2다항식의 차수가 제1다항식의 차수보다 작으면, 입력 지문 정보로부터 추출된 특징점의 개수가 인증 사용자의 지문 정보로부터 추출된 특징점의 개수보다 작은 것이므로, 제1다항식과 제2다항식이 일치하지 않는 것으로 판단할 수 있다. 사용자 인증부(226)는 제1다항식과 제2다항식이 일치하면, 다항식의 복원이 성공한 것으로 판단할 수 있다. 필요에 따라, 사용자 인증부(226)는 다항식의 복원이 성공한 경우, 사용자의 인증이 성공하였다는 인증 결과를 출력할 수 있다.

<53> 도 3은 도 2에 적용되는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치(300)의 블록도이다.

<54> 지문정보 추출부(320)는 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 지문 영상에서 특징점의 위치, 각도 및 형으로 구성되는 지문 정보를 추출한다.

<55> 다항식 생성부(330)는 추출된 지문 정보를 계수로 하는 제1다항식을 생성한다.

<56> 가짜정보 삽입부(340)는 특징점의 위치, 각도 및 형으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 추출된 지문 정보에 삽입한다. 이때, 특징점의 위치, 각도, 형으로 구성된 가짜 지문 정보를 랜덤하게 다수 생성하여 사용자의 지문정보와 구별할 수 없게 한다. 가짜 지문 정보를 삽입 할 때는 지문정보의 위치와 각도 그리고 이전에 삽입된 지문정보의 위치와 각도를 고려하여 삽입하여 은닉 지문 정보를 생성한다.

<57> 메모리 효율적인 등록 해쉬 테이블 생성부(350)는 은닉 지문 정보에서 가짜 특징점을 제외한 특징점들을 기준점으로 선택한다. 메모리 효율적인 등록 해쉬 테이블 생성부(350)는 선택된 특징점의 위치를 원점으로 이동시키고 각도를 기준 각도로 변경하고, 선택된 특징점의 변환 정도에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복한다.

<58> 데이터 베이스(360)는 제1다항식 및 은닉 지문 정보를 저장한다. 데이터 베이스(360)는 비휘발성 메모리 소자, 휘발성 메모리 소자 또는 하드 디스크 드라이브, 광학 기록매체 등을 포함할 수 있다.

<59> 도 4는 본 발명의 다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템의 블록도이다.

<60> 송신부(410)는 입력 지문정보 추출부(411) 및 입력 해쉬 테이블 생성부(412)를 포함한다.

<61> 입력 지문정보 추출부(411)는 사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점의 위치, 각도 및 형으로 구성되는 입력 지문 정보를 추출한다.

<62> 입력 해쉬 테이블 생성부(412)는 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성한다.

<63> 수신부(420)는 지문정보 정렬부(423), 예러 정정부(424), 다항식 복원부(425) 및 사용자 인증부(426)를 포함한다.

<64> 지문정보 정렬부(423)는 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 정렬한다.

<65> 예러 정정부(424)는 정렬된 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 이용하여 지문 정보를 정합한 후, 예러 정정 코드를 이용하여 정합된 지문 정보로부터 가짜 특징점을 삭제한다.

<66> 다항식 복원부(425)는 정합된 지문 정보를 계수로 하는 제2다항식을 생성한다. 이때, 제2다항식은 인증의 대상

이 되는 지문 정보에 대한 다항식을 의미한다.

- <67> 사용자 인증부(426)는 제1다항식과 제2다항식을 비교하여 사용자 인증의 결과를 검증한다. 필요에 따라, 사용자 인증부(426)는 다항식의 복원이 성공한 경우, 사용자의 인증이 성공하였다는 인증 결과를 출력할 수 있다.
- <68> 메모리 효율적인 기하학 해싱 기법을 이용한 메모리 효율적인 지문 데이터 은닉 장치(430)는 지문정보 추출부(432), 다항식 생성부(433), 가짜정보 삽입부(434), 메모리 효율적인 등록 해쉬 테이블 생성부(435) 및 데이터 베이스(436)를 포함한다.
- <69> 지문정보 추출부(432)는 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 지문 영상에서 특징점의 위치, 각도 및 형으로 구성되는 지문 정보를 추출한다.
- <70> 다항식 생성부(433)는 추출된 지문 정보를 계수로 하는 제1다항식을 생성한다.
- <71> 가짜정보 삽입부(434)는 특징점의 위치, 각도 및 형으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 추출된 지문 정보에 삽입하여 은닉 지문 정보를 생성한다.
- <72> 메모리 효율적인 등록 해쉬 테이블 생성부(435)는 은닉 지문 정보에서 가짜 특징점을 제외한 진짜 특징점들을 기준으로 선택한다. 메모리 효율적인 등록 해쉬 테이블 생성부(435)는 선택된 특징점의 위치를 원점으로 이동시키고 선택된 특징점의 각도를 기준 각도로 변경한다. 메모리 효율적인 등록 해쉬 테이블 생성부(435)는 선택된 특징점의 변환 정도에 대응하여 나머지 지문정보를 기하학적으로 이동시키는 과정을 상기 그룹마다 반복한다.
- <73> 데이터 베이스(436)는 제1다항식 및 메모리 효율적인 등록 해쉬 테이블을 저장한다. 데이터 베이스(436)는 비휘발성 메모리 소자, 휘발성 메모리 소자 또는 하드 디스크 드라이브, 광학 기록매체 등을 포함할 수 있다.
- <74> 도 5a는 본 발명의 또다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법의 흐름도이다.
- <75> 먼저, 지문 스캐너 등의 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 지문 영상에서 특징점의 위치, 각도 및 형으로 구성되는 지문 정보를 추출한다(510 과정).
- <76> 지문 정보가 추출되면, 추출된 지문 정보를 계수로 하는 제1다항식을 생성한다(520 과정).
- <77> 다음, 특징점의 위치, 각도 및 형으로 구성되는 복수의 가짜 지문 정보를 랜덤하게 생성하고, 생성된 가짜 지문 정보를 위 과정(510 과정)에서 추출된 지문 정보에 삽입한다(530 과정). 바람직하게는, 이 과정(530 과정)은 이전에 삽입된 가짜 지문 정보의 위치 및 각도의 차가 임계값 이상이 되는 가짜 지문 정보를 생성하여 추출된 지문 정보에 삽입하는 과정일 수 있다. 이때, 임계값은 본 발명이 속하는 기술 분야의 통상의 지식을 가진 자가 지문 인식률이나 보안성 등을 고려하여 정할 수 있는 범위의 값이다.
- <78> 다음, 진짜 특징점들을 몇개의 그룹으로 분류하고, 각 그룹마다 진짜 특징점만을 기준으로 하는 기하학적 해싱 기법을 적용하는 메모리 효율적인 등록 해쉬 테이블 생성 과정(540 과정)을 수행한다.
- <79> 마지막으로, 제1다항식 및 메모리 효율적인 등록 해쉬 테이블을 데이터 베이스에 저장한다(550 과정).
- <80> 도 5b는 도 5a의 메모리 효율적인 등록 해쉬 테이블 생성 과정(540 과정)의 상세 흐름도이다.
- <81> 기준점의 선택은 다음의 수학적 2를 이용할 수 있다.

수학적 2

- <82>
$$\text{New_basis} = \text{basis} \% \text{delta}, \text{ where } 0 < \text{delta} < \text{Max_basis}$$
- <83> 이때, New_basis는 선택된 기준점들의 집합이고, basis는 현재 선택된 기준점 번호, delta는 $0 < \text{delta} < \text{Max_basis}$ 를 만족하는 임의의 수이다. Max_basis는 진짜 특징점의 총 갯수이다.
- <84> 입력 해쉬 테이블 및 메모리 효율적인 등록 해쉬 테이블은 다음의 수학적 3에 의한 이동 및 회전 변환, 수학적 4에 의한 축소 변환을 이용하여 생성될 수 있다.

수학적 3

$${}_{TR}m_j(I) = \begin{pmatrix} {}_{TR}x_j(I) \\ {}_{TR}y_j(I) \\ {}_{TR}z_j(I) \\ {}_{TR}t_j(I) \end{pmatrix} = \begin{pmatrix} \cos(\theta_1) & \sin(\theta_1) & 0 & 0 \\ -\sin(\theta_1) & \cos(\theta_1) & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_j - x_1 \\ y_j - y_1 \\ \theta_j \\ t_j \end{pmatrix}$$

<85>

, where $1 < j \leq r$

<86>

수학식 4

$$m_j(I) = \begin{pmatrix} x_j(I) \\ y_j(I) \\ \theta_j(I) \\ t_j(I) \end{pmatrix} = \begin{pmatrix} \lfloor {}_{TR}x_j(I)/\alpha + 0.5 \rfloor \\ \lfloor {}_{TR}y_j(I)/\alpha + 0.5 \rfloor \\ \lfloor {}_{TR}\theta_j(I)/\beta \rfloor \\ {}_{TR}t_j(I) \end{pmatrix}$$

<87>

이때, m_j 는 기준점을 의미한다. 특징점 정보 획득 단계는 사용자의 지문 영상으로부터 특징점들을 획득하는 단계이다. 특징점은 위치, 각도, 및 형(또는 종류)로 나타내지며 $m_i = (x_i, y_i, \theta_i, t_i)$ 로 표현된다.

<88>

사용자의 지문 정보는 특징점들의 집합으로 표현된다. 가짜 특징점과 사용자의 특징점이 포함된 라깅셋을 $L = \{m_i | 1 \leq i \leq n\}$ 으로 표현할 수 있다. L에서 사용자의 특징점과 가짜 특징점들의 집합은 각각 $G = \{m_i | 1 \leq i \leq n\}$, $C = \{m_i | n+1 \leq i \leq r\}$ 으로 표현한다. 등록 특징점은 L에서 만들어지며, 메모리 효율적인 등록 테이블 생성 단계의 각 과정은 다음과 같다.

<89>

먼저, 기준점 선택 단계이다. 단순히 진짜 특징점만을 기준점으로 사용할 경우 기하학적 변환(이동, 회전, 축소)등이 역추적당할 수 있다. 인증 사용자의 진짜 특징점들의 집합을 몇개의 그룹으로 나누고(541 과정), 각 그룹마다 특징점을 선택한다(542 과정). 이때, 선택된 특징점을 m_1 이라고 가정한다.

<90>

다음, 기준점 보정 단계(543 과정)이다. 기준점을 좌표 평면의 원점으로 이동시키고, 각도를 기준 각도로 변경시킨다. 이때, 기준 각도는 0로 정의할 수 있다.

<91>

다음, 지문 정보 보정 단계(544 과정)이다. 지문 정보 보정 단계는 선택된 특징점을 제외한 다른 특징점 $m_2, m_3, \dots, m_n$ 에 대하여 변환 특징점을 구하는 과정이다. T_1 은 m_1 을 기준으로 변환된 특징점인 $m_{j(1)}$ 의 집합이며, $m_{j(1)}$ 는 m_1 을 기준으로 변환된 j번째 특징점을 나타낸다.

<92>

이를 “ m_1 -변환 특징점 집합”이라고 하며, $T_1 = \{m_{j(1)} = (x_{j(1)}, y_{j(1)}, \theta_{j(1)}, t_{j(1)}) | 1 < j \leq r\}$ 으로 표현된다. 수학식 3은 기준점 m_1 의 값이 원점으로 변환되고, 각도가 기준 각도가 되도록 나머지 특징점들에 대하여 이동 및 회전 변환을 수행한 결과를 나타낸다. 여기서 ${}_{TR}m_{j(1)}$ 은 m_1 과 관련된 j번째 특징점을 나타낸다. 이때, 기준점으로 선택된 특징점과의 거리가 미리 설정된 해쉬 테이블 크기 이상인 특징점이 존재하면, 나머지 지문정보의 위치를 축소 변환하는 과정을 수행할 수 있다. 이때의 축소 변환은 수학식 4를 이용할 수 있다. 미리 설정된 해쉬 테이블 크기는 유비쿼터스 환경의 임베디드 시스템의 메모리를 고려한 크기로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 임베디드 시스템의 상황에 적절하도록 설정하는 해쉬 테이블 크기이다.

<93>

다음은 반복 단계(545 과정)이다. 위의 기준점 선택 단계, 기준점 보정 단계 및 지문 정보 보정 단계는 기준점 선택 단계에서 나누어진 그룹들 중 어느 하나의 그룹에 포함된 진짜 특징점인 m_1 에 대하여 수행한 것이다. 동일한 과정을 다른 그룹에 대해서도 반복 수행(543-544 과정)하여 메모리 효율적인 등록 해쉬 테이블을 생성한다. 이때, 모든 그룹의 기준점에 대한 평면이 생성되면, 메모리 효율적인 등록 해쉬 테이블 생성 과정

<94>

(540 과정)을 종료한다.

- <95> 도 6은 본 발명의 또다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법의 흐름도이다.
- <96> 먼저, 은닉 지문 정보를 기하학적 변환하여 메모리 효율적인 등록 해쉬 테이블을 생성한다(620 과정). 이때, 기하학적 변환은 가짜 특징점을 제외한 진짜 특징점들을 복수의 그룹으로 분류하는 과정, 각 그룹마다 기준점을 선택하는 과정, 기준점을 보정하고, 기준점 보정에 대응하여 나머지 지문 정보를 보정하는 과정을 포함한다. 이때, 가짜 특징점을 제외한 진짜 특징점들을 복수의 그룹으로 분류하는 과정 및 각 그룹마다 기준점을 선택하는 과정에 수학적 2와 같이 모듈라 연산이 이용될 수 있다.
- <97> 다음, 사용자의 지문 영상에서 입력센싱장치를 이용하여 특징점의 위치, 각도 및 형으로 구성되는 입력 지문 정보를 추출하고, 추출된 지문 정보를 기하학적 변환하여 입력 해쉬 테이블을 생성한다(610 과정).
- <98> 입력 해쉬 테이블이 생성되면, 메모리 효율적인 등록 해쉬 테이블 및 입력 해쉬 테이블을 정렬하여 지문 정보를 정합한 후, 에러 정정 코드를 이용하여 정합된 지문 정보로부터 가짜 특징점을 삭제한다(630 과정).
- <99> 다음, 정합된 지문 정보를 계수로 하는 제2다항식을 생성한다(640 과정).
- <100> 제2다항식이 생성되면, 제1다항식과 제2다항식을 비교하여 다항식이 복원되었는지 판단한다(650 과정). 이때, 제1다항식과 제2다항식이 일치하면, 다항식의 복원이 성공한 것으로 판단할 수 있다.
- <101> 다음, 다항식의 복원이 성공하면, 인증 성공으로 판단하고(651 과정), 다항식의 복원이 실패하면, 인증 실패로 판단한다(652 과정). 필요에 따라, 다항식의 복원이 성공한 경우, 사용자의 인증이 성공하였다는 인증 결과를 출력하는 과정을 더 포함할 수 있다.
- <102> 이때, 사용자 인증을 위해 은닉된 지문정보를 본래의 지문정보로 복원하는 과정이 필요없게 된다.
- <103> 도 7은 지문 영상에서 추출된 지문 정보 및 2차원에서 은닉된 지문 정보를 도시한 것이다.
- <104> 도 8은 도 7의 지문 정보를 이용하여 생성된 종래의 등록 해쉬 테이블을 도시한 것이다.
- <105> 도 9는 종래의 하나의 기준점을 이용하여 생성된 등록 해쉬 테이블과 입력 해쉬 테이블의 정합 과정을 도시한 것이다.
- <106> 도 10a은 종래의 하나의 기준점을 이용하여 생성된 등록 해쉬 테이블의 진짜 특징점과 가짜 특징점의 상태를 도시한 것이다. 도 10b는 본 발명에 따라 복수의 기준점을 이용하여 생성된 메모리 효율적인 등록 해쉬 테이블의 진짜 특징점과 가짜 특징점의 상태를 도시한 것이다.
- <107> 도 11a는 종래의 진짜 특징점과 가짜 특징점을 모두 기준점으로 이용하여 생성된 등록 해쉬 테이블의 크기를 도시한 것이다. 도 11b는 본 발명에 따라 진짜 특징점만을 기준점으로 이용하여 생성된 메모리 효율적인 등록 해쉬 테이블의 크기를 도시한 것이다. 도 11a와 도 11b를 비교하면, 본 발명에 따라 생성된 메모리 효율적인 등록 해쉬 테이블은 종래 등록 해쉬 테이블의 1/6 이하의 크기를 갖는다는 것을 알 수 있다.
- <108> 도 12는 종래의 지문 데이터 은닉 방법 및 인증 방법과 본 발명에 따른 인식률을 비교한 그래프이다.
- <109> 도 12에서와 같이, 본 발명에 의하면 크기가 작은 등록 해쉬 테이블을 이용하여도 인식률의 저하가 미비한 수준임을 알 수 있다. 이는 등록 해쉬 테이블 생성시에 복수의 그룹으로 나누어진 진짜 특징점들을 기준점으로 이용하여 지문 정보를 보정하기 때문이다.
- <110> 도 13은 종래의 지문 데이터 은닉 방법 및 인증 방법과 본 발명에 따른 해쉬 테이블의 크기를 비교한 그래프이다.
- <111> 본 발명에 따른 메모리 효율적인 등록 해쉬 테이블은 크기가 상당히 감소하였음을 알 수 있다.
- <112> 바람직하게는, 본 발명의 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.
- <113> 바람직하게는, 본 발명의 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.
- <114> 본 발명은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업

을 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.

<115> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 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.

<116> 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 보호범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

발명의 효과

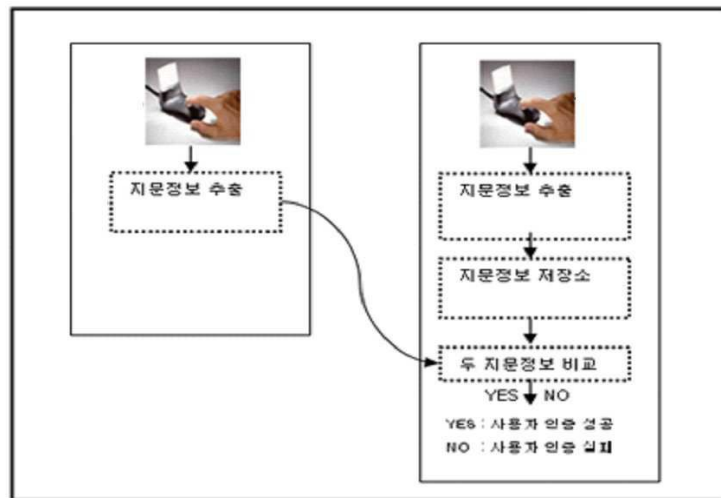
<117> 상술한 바와 같이, 본 발명에 의하면, 생체정보를 안전하게 보호하기 위하여 퍼지 볼트 이론을 적용하고 메모리 효율적인 기하학적 해싱 기법을 적용함으로써, 인식률과 보안성을 저하시키지 않으면서 효과적으로 해쉬 테이블의 크기를 줄여 임베디드 시스템에서 시스템의 부하를 줄일 수 있고, 인증 과정에서 다항식의 복원 과정을 이용하여 은닉된 지문 정보를 본래의 지문 정보로 복원하지 않고도 인증을 완료할 수 있어 지문 정보 해킹에 대한 안전성을 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

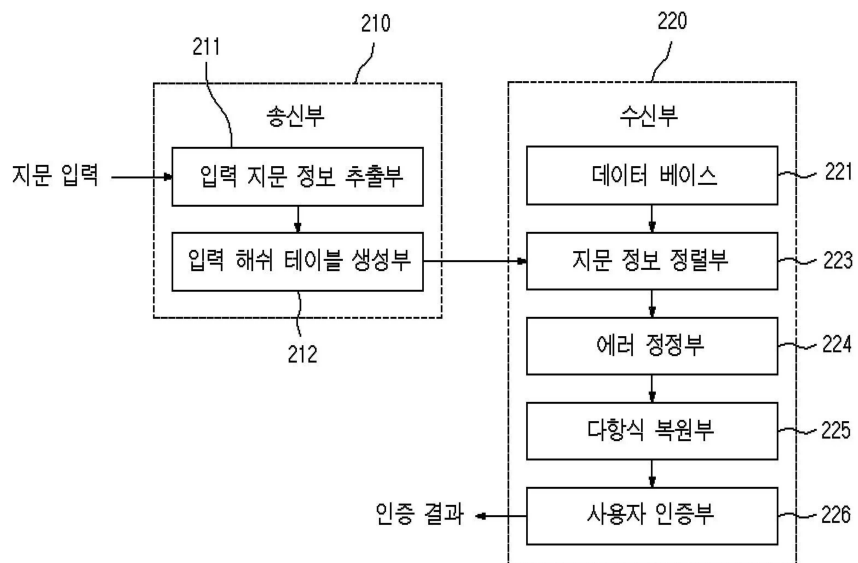
- <1> 도 1은 지문인식 시스템의 블록도이다.
- <2> 도 2는 본 발명의 일 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템의 블록도이다.
- <3> 도 3은 도 2에 적용되는 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 장치의 블록도이다.
- <4> 도 4는 본 발명의 다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 시스템의 블록도이다.
- <5> 도 5a는 본 발명의 또다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 은닉 방법의 흐름도이다.
- <6> 도 5b는 도 5a의 메모리 효율적인 등록 해쉬 테이블 생성 과정(540 과정)의 상세 흐름도이다.
- <7> 도 6은 본 발명의 또다른 실시 예에 따른 퍼지볼트를 이용한 메모리 효율적인 지문 데이터 인증 방법의 흐름도이다.
- <8> 도 7은 지문 영상에서 추출된 지문 정보 및 2차원에서 은닉된 지문 정보를 도시한 것이다.
- <9> 도 8은 도 7의 지문 정보를 이용하여 생성된 종래의 등록 해쉬 테이블을 도시한 것이다.
- <10> 도 9는 종래의 등록 해쉬 테이블과 입력 해쉬 테이블의 정합 과정을 도시한 것이다.
- <11> 도 10a은 종래의 등록 해쉬 테이블의 진짜 특징점과 가짜 특징점의 상태를 도시한 것이다.
- <12> 도 10b는 본 발명에 따라 생성된 메모리 효율적인 등록 해쉬 테이블의 진짜 특징점과 가짜 특징점의 상태를 도시한 것이다.
- <13> 도 11a는 종래의 등록 해쉬 테이블의 크기를 도시한 것이다.
- <14> 도 11b는 본 발명에 따라 생성된 메모리 효율적인 등록 해쉬 테이블의 크기를 도시한 것이다.
- <15> 도 12는 종래의 지문 데이터 은닉 방법 및 인증 방법과 본 발명에 따른 인식률을 비교한 그래프이다.
- <16> 도 13은 종래의 지문 데이터 은닉 방법 및 인증 방법과 본 발명에 따른 해쉬 테이블의 크기를 비교한 그래프이다.

도면

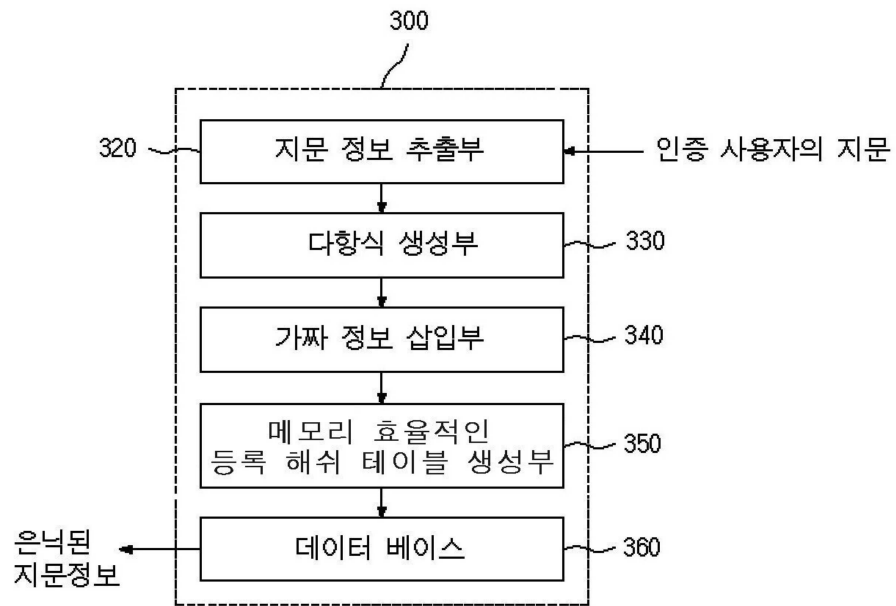
도면1



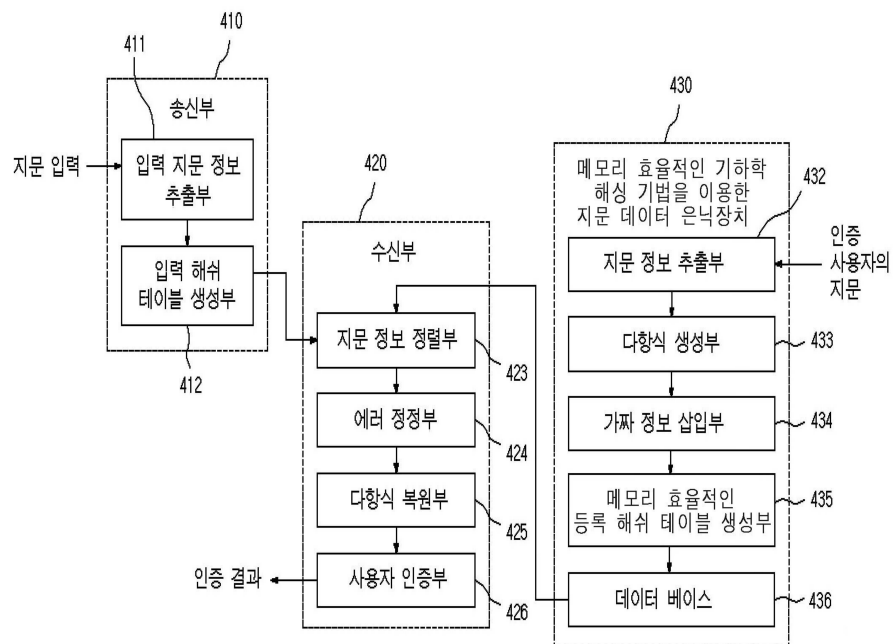
도면2



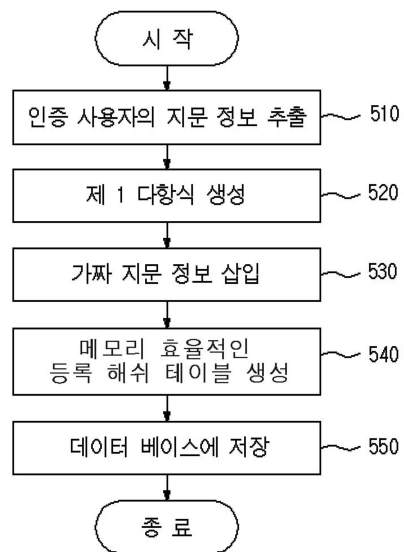
도면3



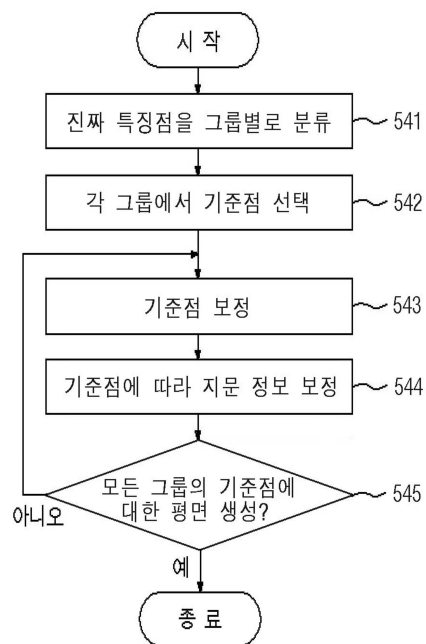
도면4



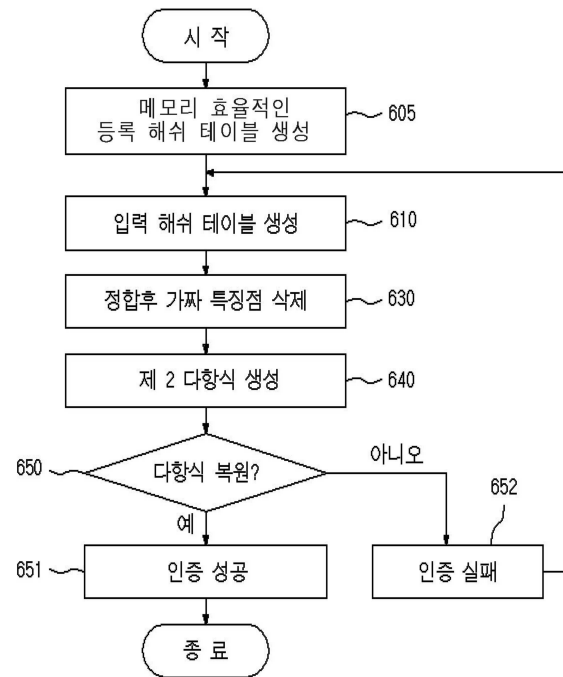
도면5a



도면5b

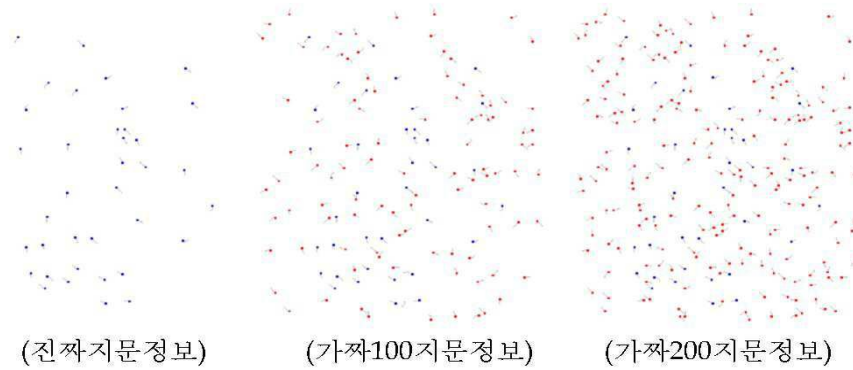


도면6



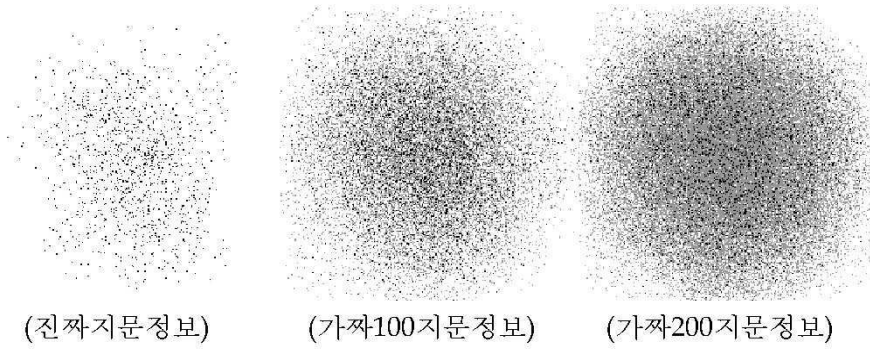
도면7

fingerprint image table(248×292)



도면8

Geometric hash table(256×256)

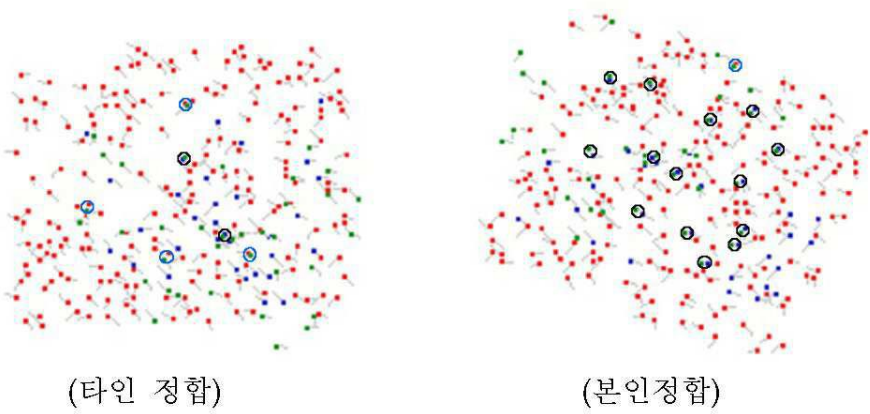


(진짜지문 정보)

(가짜100지문 정보)

(가짜200지문 정보)

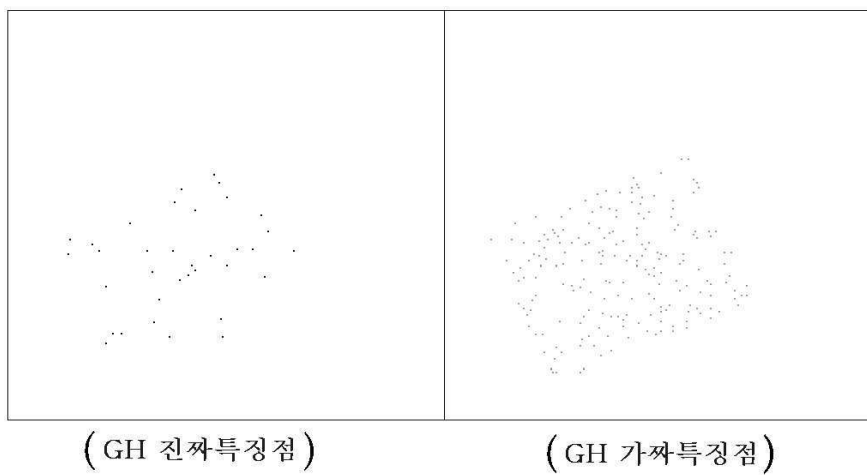
도면9



(타인 정합)

(본인정합)

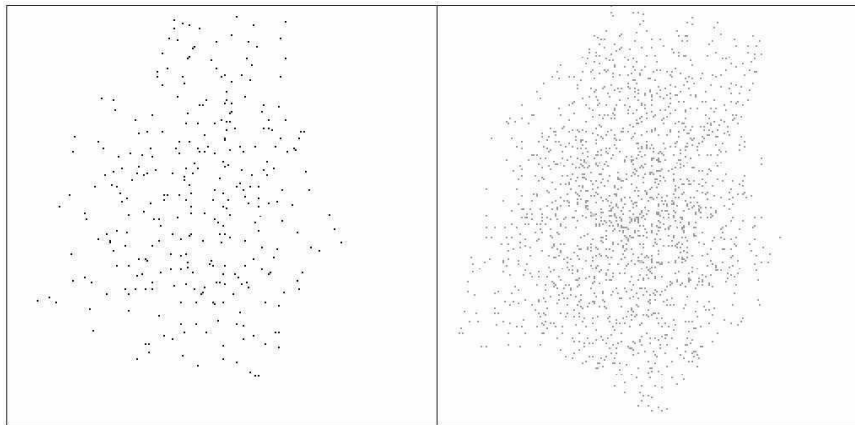
도면10a



(GH 진짜특징점)

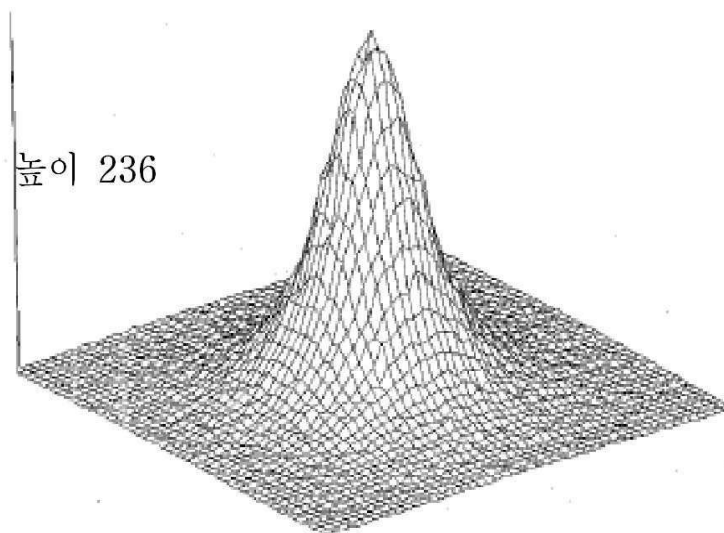
(GH 가짜특징점)

도면10b

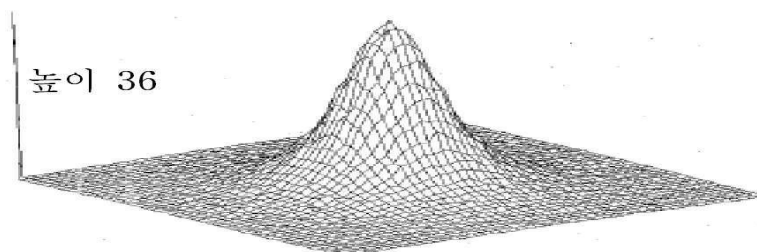


(본발명에 따른 GH 진짜특징점) (본발명에 따른 GH 가짜특징점)

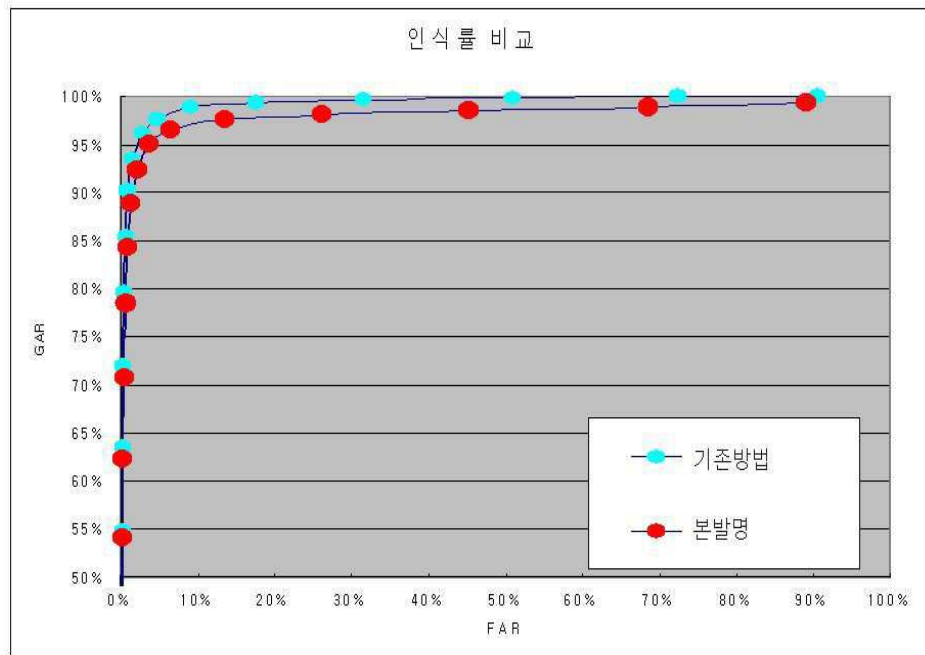
도면11a



도면11b



도면12



도면13

