



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0090733
(43) 공개일자 2018년08월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) G06F 21/45 (2013.01)
G06F 21/62 (2013.01) G06K 9/00 (2006.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2018-0011778
(22) 출원일자 2018년01월31일
심사청구일자 2018년01월31일
(30) 우선권주장
1020170014761 2017년02월02일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울특별시 광진구 아차산로 503-23, 103동 1701호 (광장동, 청구아파트)
정재열
서울특별시 성북구 안암로9가길 55 304호 (안암동5가)
(뒷면에 계속)
(74) 대리인
김홍석

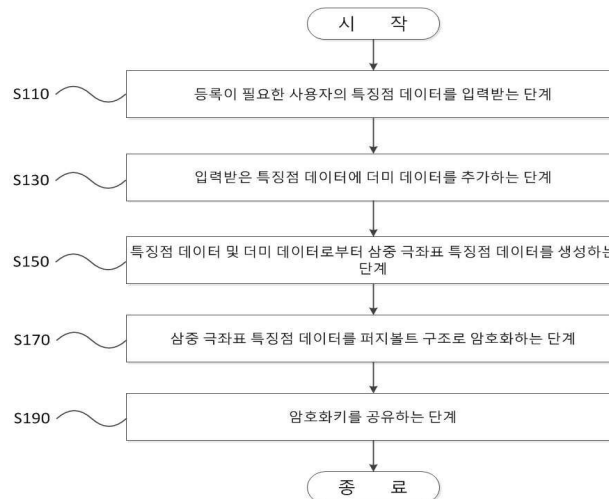
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 삼중 극좌표 특징점 구조를 이용한 지문 등록 및 인증 방법

(57) 요약

지문 등록 방법이 개시된다. 상기 지문 등록 방법은 (a) 지문 등록이 필요한 사용자 지문의 특징점(minutiae)들에 대한 데이터인 특징점 데이터를 입력받는 단계, (b) 상기 특징점 데이터에 랜덤하게 생성된 더미 데이터를 추가하는 단계, 및 (c) 상기 특징점 데이터 중에서 임의로 선택된 제1 특징점 데이터(M_i) 및 상기 더미 데이터가 추가된 특징점 데이터 중에서 상기 선택된 어느 하나의 특징점 데이터를 제외하고 임의로 선택된 제2 특징점 데이터(M_j, M_k)를 이용하여 삼중 극좌표(triple-polar) 특징점 데이터를 생성하는 단계를 포함하고, 상기 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함한다.

대표도 - 도4



(52) CPC특허분류

G06F 21/6245 (2013.01)

G06K 9/0004 (2013.01)

(72) 발명자

권태연

경기도 남양주시 별내4로 8, 4607동 1201호(별내동, 한화꿈에그린아파트)

안정호

서울특별시 영등포구 도신로 68, 106동 202호(신길동, 신길우성아파트)

안정연

경기도 고양시 일산서구 경의로 605, 1204동 1102호

박민서

서울특별시 영등포구 선유동2로 56 204동 301호 (당산동5가, 유원2차아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 R71151610080001002

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 SW중심대학지원사업

연구과제명 [SW중심대학-세부]SW중심대학

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2016.03.01 ~ 2017.02.28

명세서

청구범위

청구항 1

(a) 지문 등록이 필요한 사용자 지문의 특징점(minutiae)들에 대한 데이터인 특징점 데이터를 입력받는 단계;
 (b) 상기 특징점 데이터에 랜덤하게 생성된 더미 데이터를 추가하는 단계; 및
 (c) 상기 특징점 데이터 중에서 임의로 선택된 제1 특징점 데이터(M_i) 및 상기 더미 데이터가 추가된 특징점 데이터 중에서 상기 선택된 어느 하나의 특징점 데이터를 제외하고 임의로 선택된 제2 특징점 데이터(M_j, M_k)를 이용하여 삼중 극좌표(triple-polar) 특징점 데이터를 생성하는 단계를 포함하고,
 상기 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함하는 지문 등록 방법.

청구항 2

제1항에 있어서,

상기 넓이 정보는 상기 제1 특징점 데이터(M_i) 및 상기 제2 특징점 데이터(M_j, M_k)의 각 특징점이 형성하는 삼각형의 넓이 정보이며,

상기 거리 정보는 상기 제1 특징점 데이터(M_i)의 특징점과 상기 제2 특징점 데이터(M_j, M_k)의 특징점 간에 거리 정보이며,

상기 제1 각도 정보는 상기 제1 특징점 데이터(M_i)의 방향성(orientation)과 $\overline{M_i, M_j}$ 또는 $\overline{M_i, M_k}$ 가 이루는 각도 정보이며,

상기 제2 각도 정보는 상기 제1 특징점 데이터(M_i)의 방향성과 상기 제2 특징점 데이터(M_j, M_k)의 방향성이 이루는 각도 정보인 지문 등록 방법.

청구항 3

제1항에 있어서,

상기 (a) 단계는

(a-1) 상기 특징점들에서 임의로 선택된 세 개의 특징점들이 이루는 삼각형의 넓이가 기 설정된 임계값 이하일 때의 특징점들을 추출하는 단계; 및

(a-2) 상기 추출된 특징점들에 대한 특징점 데이터만을 입력받는 단계를 포함하는 지문 등록 방법.

청구항 4

제1항에 있어서,

(d) 상기 삼중 극좌표 특징점 데이터를 퍼지볼트(fuzzy vault) 구조로 암호화하는 단계를 더 포함하는 지문 등록 방법.

청구항 5

제4항에 있어서,

상기 (d) 단계는

(d-1) 암호화키를 계수로 하는 퍼지볼트 다항식에 상기 삼중 극좌표 특징점 데이터를 변수로 입력하여, 상기 제2 특징점 데이터(M_j, M_k)가 상기 더미 데이터에 해당될 때의 연산되는 값인 제1 집합 데이터를 생성하고, 상기 제2 특징점 데이터(M_j, M_k)가 상기 더미 데이터에 해당되지 않을 때의 값인 제2 집합 데이터를 생성하는 단계; 및

(d-2) 상기 제1 집합 데이터 및 제2 집합 데이터를 합성하여 볼트 데이터를 생성하는 단계를 더 포함하는 지문 등록 방법.

청구항 6

(a) 인증이 필요한 사용자 지문의 특징점(minutiae)들에 대한 데이터인 특징점 데이터를 입력받는 단계;

(b) 상기 특징점 데이터 중에서 임의로 선택된 특징점 데이터(M_i, M_m, M_n)를 이용하여 삼중 극좌표(triple-polar) 특징점 데이터를 생성하는 단계; 및

(c) 상기 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 상기 인증이 필요한 사용자에게 대한 인증을 수행하는 단계를 포함하고,

상기 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함하는 지문 인증 방법.

청구항 7

제6항에 있어서,

상기 넓이 정보는 상기 선택된 세 개의 특징점 데이터(M_i, M_m, M_n)의 특징점들이 형성하는 삼각형의 넓이 정보이며,

상기 거리 정보는 상기 선택된 세 개의 특징점 데이터(M_i, M_m, M_n) 중 M_i 의 특징점과 M_m, M_n 의 특징점 간에 거리 정보이며,

상기 제1 각도 정보는 상기 선택된 세 개의 특징점 데이터(M_i, M_m, M_n) 중 M_i 의 방향성(orientation)과 M_m 또는 M_n 이 이루는 각도 정보이며,

상기 제2 각도 정보는 상기 선택된 세 개의 특징점 데이터(M_i, M_m, M_n) 중 M_i 의 방향성과 M_m 의 방향성 또는 M_n 의 방향성이 이루는 각도 정보인 지문 인증 방법.

청구항 8

제7항에 있어서,

상기 (c) 단계는 상기 삼중 극좌표 특징점 데이터에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보와 상기 기 등록된 볼트 데이터에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 이용하

여 인증을 수행하는 지문 인증 방법.

발명의 설명

기술 분야

- [0001] 본 발명은 지문 등록 및 인증 방법에 대한 것으로서, 보다 구체적으로 triple-polar 구조를 기반으로 하는 특징점 데이터를 이용하여 지문을 등록 및 인증하는 방법에 대한 것이다.

배경 기술

- [0002] 퍼지볼트(fuzzy vault) 이론은 생체정보를 안전하게 보호하기 위해 암호학적인 방법으로 연구되고 있는 이론이다. 생체정보를 통한 사용자 인증을 수행하는 경우에 개개인이 소유한 생체특성의 최소성과 제한성 때문에, 생체인식 템플릿은 패스워드나 핀, 토큰카드와 같은 다른 인증기법과는 달리 대체되기 어려운 특징을 보인다. 따라서, 데이터베이스에 저장된 중요한 생체정보들이 타인에게 유출되어 도용된다면 심각한 문제를 야기할 수 있다.
- [0003] 이에 따라 저장되는 데이터의 안전성을 높이기 위해 퍼지볼트 이론을 지문인식 시스템에 적용한다면, 사용자의 지문 이미지 자체를 저장하여 사용하지 않는다. 등록과정에서 다항식을 생성하고 지문 이미지로부터 추출된 사용자의 지문 특징정보를 다항식에 사영한 뒤, 여기에 타인으로부터 진짜 특징정보를 은닉하기 위해, 생성된 다항식 위에 놓이지 않는 거짓 특징정보를 추가하여 볼트라는 형태로 함께 저장하여 사용한다.
- [0004] 사용자의 지문등록이 완료되면 이후에 인증과정에서는 입력된 지문 이미지로부터 추출된 특징정보와 미리 저장된 특징정보 사이에 정합을 수행함으로써 입력된 지문이 저장된 지문과 동일한 지문인지를 판단한다. 보다 상세하게는 등록과정과 동일하게 전처리 단계를 거친 후에 거짓 특징정보까지 모두 포함하고 있는 볼트에서 진짜 특징정보만을 추출하고, 그로부터 생성되는 다항식이 등록과정에서 사용되었던 것과 동일한 것인지를 비교한다. 즉 퍼지볼트 이론을 기반으로 하는 지문 퍼지볼트 시스템의 보안성은, 볼트로부터 사용자의 진짜 지문특징정보와 거짓 지문특징정보를 구분하는 어려움의 정도에 의존한다.
- [0005] 한편, pair-polar는 사용자의 지문이미지에서 추출되어 저장되는 특징정보의 형태이다. 각 지문에서의 특징점들을 개별로 사용한다면, 지문등록 혹은 인증 당시에 가해지는 압력이나, 피부의 수분, 전류, 회전 등의 가변적인 요소들에 의해 인증의 정확성 차원에서 큰 손실을 유발할 수 있다. 한 지문 내에서의 개별 특징점이 아니라 그들의 상대적인 위치나 방향성 등의 관계정보를 사용한다면, 상황별 가변 요소로부터의 영향을 최소화하여 지문 자체의 특성을 유지(transformation-invariant)하고 특징정보의 신뢰성을 한 단계 높일 수 있다. 보다 상세하게는, 사용자의 지문 안에서 각 특징점을 극좌표로 매칭시켜 세 점으로 이루어지는 삼각형을 구성하고 인증과정에서 면적, 각에 대한 한계점(threshold)를 정해 등록된 지문정보와의 유사한 정도를 판별한다.
- [0006] 아래의 비특허문헌 1에서는 pair-polar 구조를 기반으로 한 퍼지볼트 지문 인증 기술을 제안하였으며, 비특허문헌 2에서는 Multiple 퍼지볼트를 기반으로 한 지문 암호화 시스템을 제안하였다. 하지만, 전자의 경우 1차원 선과 각을 인증 정보로 이용하므로 인증과정에서의 정확도가 떨어지며, 후자의 경우 퍼지볼트만을 이용하는 경우 거짓 특징정보를 제외하는 과정에서 오차가 생길 수 있는 문제점이 있다.

선행기술문헌

비특허문헌

- [0007] (비특허문헌 0001) Cai Li and Jiankun Hu, "A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.11, NO.3, MARCH 2016.
- (비특허문헌 0002) Ali Akbar Nasiri and Mahmood Fathy, "Alignment-Free Fingerprint Cryptosystem Based On Multiple Fuzzy Vaults", ARTIFICIAL INTELLIGENCE AND SIGNAL PROCESSING (AISP), 2015 INTERNATIONAL SYMPOSIUM ON.

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 기존의 지문 인증 모델보다 더 높은 분별력을 가지는 triple-polar 구조를 기반으로 하는 지문 등록 및 인증 방법을 제공하는데 있다.

과제의 해결 수단

[0009] 본 발명의 일 실시 예에 따른 지문 등록 방법은 (a) 지문 등록이 필요한 사용자 지문의 특징점(minutiae)들에 대한 데이터인 특징점 데이터를 입력받는 단계, (b) 상기 특징점 데이터에 랜덤하게 생성된 더미 데이터를 추가하는 단계, 및 (c) 상기 특징점 데이터 중에서 임의로 선택된 제1 특징점 데이터(M_i) 및 상기 더미 데이터가 추가된 특징점 데이터 중에서 상기 선택된 어느 하나의 특징점 데이터를 제외하고 임의로 선택된 제2 특징점 데이터(M_j, M_k)를 이용하여 삼중 극좌표(triple-polar) 특징점 데이터를 생성하는 단계를 포함하고, 상기 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함할 수 있다.

[0010] 본 발명의 일 실시 예에 따른 지문 인증 방법은 (a) 인증이 필요한 사용자 지문의 특징점(minutiae)들에 대한 데이터인 특징점 데이터를 입력받는 단계, (b) 상기 특징점 데이터 중에서 임의로 선택된 특징점 데이터(M_i, M_m, M_n)를 이용하여 삼중 극좌표(triple-polar) 특징점 데이터를 생성하는 단계, 및 (c) 상기 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 상기 인증이 필요한 사용자에게 대한 인증을 수행하는 단계를 포함하고, 상기 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함할 수 있다.

발명의 효과

[0011] 본 발명의 일 실시 예에 따르면 기존의 pair-polar 기법보다 더 정확하게 특징점들을 비교하여 높은 분별력을 제공할 수 있다.

[0012] 또한, 템플릿 보호에 유용한 솔루션을 제공함과 동시에 작은 오버헤드를 가지는 지문 암호 시스템을 제공할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시 예에 따른 지문 등록 장치의 블록도이다.

도 2는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 설명하기 위한 좌표계를 도시한 것이다.

도 3은 본 발명의 일 실시 예에 따른 지문 인증 장치의 블록도이다.

도 4는 본 발명의 일 실시 예에 따른 지문 등록 방법의 순서도이다.

도 5는 본 발명의 일 실시 예에 따른 지문 인증 방법의 순서도이다.

도 6은 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 인증을 수행하는 단계의 구체적인 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0015] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에 상세하게 설명하고자 한다. 그러나 이는 본 발명의 개념에 따른 실시예들을 특정한 개시형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0016] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들

에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만, 예를 들어 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0017] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 표현들, 예를 들어 "~사이에"와 "바로~사이에" 또는 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0018] 본 명세서에서 사용한 용어는 단지 특정한 실시예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다. 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0021] 도 1은 본 발명의 일 실시 예에 따른 지문 등록 장치의 블록도이다.

[0022] 도 1을 참조하면, 본 발명의 일 실시 예에 따른 지문 등록 장치(10)는 입력부(110), 터미 데이터 추가부(130), 삼중 극좌표 변환부(150) 및 볼트 데이터 생성부(170)를 포함한다.

[0023] 입력부(110)는 인증이 필요한 사용자로부터 지문의 정보에 대한 데이터인 특징점(minutiae) 데이터를 입력받는다. 지문 등록 및 인증에 필요한 지문의 정보는 지문 센서를 통하여 획득된 사용자의 지문에 대한 이미지로부터 추출되는 지문의 특징점에 대한 정보를 의미하는데, 이때 추출되는 특징점은 획득된 지문에 대한 이미지에 나타나는 용선이 끝나는 끝점(ending point)와 하나의 용선이 둘로 나뉘어지는 분기점(bifurcation point)를 포함한다.

[0024] 이러한 특징점에 대한 정보를 포함하는 특징점 데이터는 $M_i = (x_i, y_i, \theta_i)$ 와 같이 나타낼 수 있다. 여기서, x_i, y_i 는 직교좌표계에서 특징점의 좌표 정보이며, θ_i 는 특징점의 방향성(orientation)을 나타내는 각도이다. 여기에, 특징점이 지문의 용선의 끝점을 나타내는지 또는 용선의 분기점을 나타내는지를 알 수 있는 유형 정보(t_i)를 더 포함할 수 있다. 만일 사용자의 지문에 대하여 N개의 특징점 데이터를 입력받는 경우, 특징점 데이터는 $SM^T = \{M_i\}_{i=1}^{N^T}$ 와 같이 나타낼 수 있다.

[0025] 터미 데이터 추가부(130)는 입력부(110)를 통하여 입력된 특징점 데이터에 랜덤하게 생성된 터미 데이터를 추가한다. 터미 데이터는 사용자의 지문에 포함되는 특징점이 아니라 랜덤으로 생성되는 거짓 특징점(chaff minutiae)에 대한 데이터로서, 진짜 지문에 대한 정보를 보호하기 위해 추가된다. R개의 터미 데이터를 추가할 때, 터미 데이터는 $CM = \{M_c\}_{c=1}^R$ 와 같이 나타낼 수 있다.

[0026] 삼중 극좌표 변환부(150)는 입력부(110)를 통하여 입력된 특징점 데이터를 삼중 극좌표(triple-polar) 형태로 변환한다. 우선, 삼중 극좌표 변환부(150)는 입력된 특징점 데이터 중에서 제1 특징점 데이터(M_i)를 임의로 선택하고, 터미 데이터 추가부(130)를 통하여 터미 데이터가 추가된 특징점 데이터 중에서 상기 선택된 제1 특징점 데이터(M_i)를 제외하고 두 개의 제2 특징점 데이터(M_j, M_k)를 임의로 선택한다. 다음으로, 상기 임의로 선

택된 제1 특징점 데이터(M_i) 및 제2 특징점 데이터(M_j, M_k)를 결합하여 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함하는 삼중 극좌표 특징점 데이터를 생성한다. 생성되는 삼중 극좌표 특징점 데이터는 $v_{ijk}^T = \{B_{a_{ik}}, B_{r_{ij}}, B_{r_{ik}}, B_{\phi_{ij}}, B_{\phi_{ik}}, B_{\theta_{ij}}, B_{\theta_{ik}}\}$ 와 같이 나타낼 수 있으며, 이 값들을 결합시킨 값은 $CB_{ijk}^T = B_{a_{ik}} \| B_{r_{ij}} \| B_{r_{ik}} \| B_{\phi_{ij}} \| B_{\phi_{ik}} \| B_{\theta_{ij}} \| B_{\theta_{ik}}$ 으로 나타낼 수 있다. 이때, B값은 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보의 비트 문자열 데이터를 의미한다.

[0027] 삼중 극좌표 특징점 데이터가 포함하는 각각의 정보는 제1 특징점 데이터(M_i) 및 제2 특징점 데이터(M_j, M_k) 정보가 포함되는 세 개의 특징점에 대한 넓이 정보 및 극좌표 정보를 의미한다.

[0029] 도 2는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 설명하기 위한 좌표계를 도시한 것이다.

[0030] 도 2를 참조하면, 넓이 정보는 세 개의 특징점이 이루는 삼각형의 넓이 정보로서 $a_{ijk} = \frac{1}{2} |(x_i y_j + x_j y_k + x_k y_i) - (x_j y_i + x_k y_j + x_i y_k)|$ 으로 나타낼 수 있다. 즉, 각 특징점의 직교 좌표정보를 이용하여 넓이 정보를 연산할 수 있다. 거리 정보는 두 개의 특징점 간에 거리에 대한 정보로서, M_i 와 M_j 간에 거리 정보는 r_{ij} 로 나타낼 수 있다. 제1 각도 정보는 제1 특징점 데이터(M_i)의 방향성(orientation)과 $\overrightarrow{M_i, M_j}$ 또는 $\overrightarrow{M_i, M_k}$ 가 이루는 각도 정보이다. 제2 각도 정보는 제1 특징점 데이터(M_i)의 방향성과 제2 특징점 데이터(M_j, M_k)의 방향성이 이루는 각도 정보이다.

[0031] 이러한 정보를 포함하는 삼중 극좌표 특징점 데이터는 $V_i^T = \{CB_{ijk}^T\}_{j=1, k=2, j \neq k \neq i}^{N+R}$ 으로 나타낼 수 있다. 여기서, N+R은 더미 데이터가 추가된 특징점 데이터의 개수를 의미한다. 즉, 삼중 극좌표 특징점 데이터는 등록하려는 사용자의 지문의 특징점에 가짜 특징점이 추가된 특징점 집합에서 임의로 선택된 세 개의 특징점 데이터를 기존의 형태($M_i = (x_i, y_i, \theta_i)$)와 달리 넓이 정보 및 극좌표 정보를 포함하도록 변환시킨 데이터이다.

[0032] 볼트 데이터 생성부(170)는 변환된 삼중 극좌표 특징점 데이터를 퍼지볼트(fuzzy vault) 구조로 암호화한다. 암호화에 대한 설명에 앞서, 본 명세서에 있어서 모든 산술적 연산은 유한체(finite field) 내에서 수행될 수 있다. 유한체는 유한한 원소의 개수를 가진 체(field)이며, 갈루아체(Galois field)로도 불릴 수 있다. 즉, 후술하는 다항식 및 상기 다항식 및 상기 유한체 내에서 수행되는 모든 연산의 결과는 상기 유한체 내에서 정의될 수 있다.

[0033] 퍼지볼트 구조로 암호화하기 위해, 볼트 데이터 생성부(170)는 암호화키($K_i = k_{i,n-1} \| k_{i,n-2} \| \dots \| k_{i,0}$)를 생성하고, 상기 암호화키를 계수로 하는 퍼지볼트 다항식을 생성한다. 퍼지볼트 다항식은 아래의 수학적 식 1과 같이 정의될 수 있다.

수학적 식 1

[0034]
$$p_i(x) = k_{i,n-1}x^{n-1} + k_{i,n-2}x^{n-2} + \dots + k_{i,0}$$

[0035] 여기서, n은 자연수로서 다항식의 차수를 의미하며, 다항식의 계수는 암호화키를 의미한다.

[0036] 다음으로, 생성된 퍼지볼트 다항식에 상기 삼중 극좌표 특징점 데이터를 변수로 입력 및 연산하여 제1 집합 데이터 및 제2 집합 데이터를 생성한다. 여기서, 제1 집합 데이터는 제2 특징점 데이터(M_j, M_k)가 더미 데이터에 해당되지 않을 때의 연산되는 값으로서 $GS_i = \{(CB_{ijk}^T, p_i(CB_{ijk}^T))\}_{M_j, M_k \in SM^T, j=1, k=2, j \neq k \neq i}$ 으로 나타내

며, 제2 집합 데이터는 제2 특징점 데이터(M_j, M_k)가 더미 데이터에 해당될 때의 연산되는 값으로서 $CS_i = \{(CB_{ijk}^T, u_{ijk})\}_{M_j, M_k \in CM, j=1, k=2, j \neq k \neq i}$ 으로 나타낼 수 있다. 여기서, $u_{ijk} \neq p_i(CB_{ijk}^T)$ 인 난수이다.

[0037] 마지막으로, 생성된 상기 제1 집합 데이터 및 제2 집합 데이터를 갈루아체에서 합성하여 볼트 데이터를 생성하고, 상기 암호화키에 대한 해쉬값($H(K_i)$)을 함께 저장한다.

[0038] 여기에, 지문 등록 장치(10)는 비밀키 공유부를 더 포함할 수 있다. 비밀키 공유부는 퍼지볼트 구조로 암호화하기 위해 사용된 암호화키를 안전하게 공유하기 위해 비밀키($K = k_m || k_{m-1} || \dots || k_0$)를 생성하고, 상기 비밀키를 계수로 갖는 다항식을 생성한다. 생성되는 다항식은 아래의 수학적 식 2와 같이 정의될 수 있다.

수학적 식 2

[0039]
$$p(x) = k_m x^m + k_{m-1} x^{m-1} + \dots + k_0$$

[0040] 여기서, m은 자연수로서 다항식의 차수를 의미하며, 다항식의 계수는 비밀키를 의미한다.

[0041] 다음으로, 생성된 다항식에 상기 암호화키를 변수로 입력 및 연산하여 $p(K_i)$ 를 생성하고, 상기 암호화키에 대한 해쉬값($H(K_i)$)을 함께 저장한다. 또한, 난수(K_0)를 생성하고 상기 난수를 이용하여 $(p(K_0), H(K_0))$ 을 생성하여 암호화키와 함께 공개할 수 있다.

[0043] 도 3은 본 발명의 일 실시 예에 따른 지문 인증 장치의 블록도이다.

[0044] 도 3을 참조하면, 본 발명의 일 실시 예에 따른 지문 인증 장치(20)는 입력부(210), 삼중 극좌표 변환부(230) 및 인증부(250)를 포함한다. 이하에서는 앞서 지문 등록 장치(10)에서 기재한 부분과 중복되는 구성에 대한 설명은 생략 또는 간략히 하기로 한다.

[0045] 입력부(210)는 인증이 필요한 사용자 지문의 특징점들에 대한 데이터인 특징점 데이터를 입력받는다. 인증이 필요한 사용자 지문의 N개의 특징점 데이터는 $SM^Q = \{M_i\}_{i=1}^{N^Q}$ 으로 나타낼 수 있다.

[0046] 삼중 극좌표 변환부(230)는 입력부(210)를 통하여 입력된 특징점 데이터 중에서 임의로 선택된 세 개의 특징점 데이터(M_i, M_m, M_n)를 삼중 극좌표 형태로 변환하여 삼중 극좌표 특징점 데이터를 생성한다. 이때, 생성된 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함하는 형태인 $V_i^Q = \{v_{lmn}^T = \{B_{\alpha_{lmn}}, B_{r_{lmn}}, B_{\theta_{1n}}, B_{\phi_{lmn}}, B_{\phi_{1n}}, B_{\theta_{lmn}}, B_{\theta_{1n}}\}\}_{m=1, n=2, j \neq m \neq n}^{S^Q}$ 로 나타낼 수 있다.

[0047] 인증부(250)는 인증이 필요한 사용자 지문에 대한 삼중 극좌표 특징점 데이터(V_i^Q)와 지문 등록 장치(10)를 통해 기 등록된 볼트 데이터를 비교하여 상기 인증이 필요한 사용자에 대한 인증을 수행한다. 기 등록된 볼트 데이터는 지문 등록 방법에서 생성된 볼트 데이터일 수 있다. 인증부(250)는 삼중 극좌표 특징점 데이터(V_i^Q)에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보와 상기 기 등록된 볼트 데이터에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 이용하여 인증을 수행한다. 인증부(250)가 지문 인증을 수행하는 방법에 대한 보다 구체적인 설명은 도 5를 통하여 후술하기로 한다.

[0049] 도 4는 본 발명의 일 실시 예에 따른 지문 등록 방법의 순서도이다.

[0050] 도 4를 참조하면, S110 단계는 지문 등록이 필요한 사용자 지문의 N개의 특징점들에 대한 데이터인 특징점 데이

터($SM^T = \{M_i\}_{i=1}^{N^T}$)를 입력받는다.

- [0051] 특징점 데이터를 입력받는 S110 단계에 앞서, 지문 센서를 통하여 획득된 사용자의 지문에 대한 이미지로부터 신뢰도 높은 특징점이 추출될 수 있도록 전처리(pre-processing) 단계를 더 포함할 수 있다. 이때, 전처리 단계는 지문 이미지에 포함된 이미지 왜곡에 대한 영상 개선 처리를 포함할 수 있다. 전처리 단계를 더 포함하는 경우 S110 단계는 전처리된 이미지로부터 추출되는 지문 특징점에 대한 특징점 데이터를 입력받을 수 있다.
- [0052] 한편, S110 단계는 미리 입력받은 특징점 데이터의 개수를 조절하는 단계를 더 포함할 수 있다. 보다 구체적으로, 지문 이미지로부터 추출된 특징점들에서 임의로 선택된 세 개의 특징점들이 이루는 삼각형의 넓이를 연산하고, 연산된 넓이가 기 설정된 임계값 이하일 때의 특징점들을 추출할 수 있다. 다음으로, 상기 추출된 특징점들에 대한 특징점 데이터만을 입력받음으로써 지문 등록 및 인증에 필요한 연산의 정확도 및 속도를 높일 수 있다.
- [0053] S130 단계는 S110 단계에서 입력된 특징점 데이터에 랜덤하게 생성된 더미 데이터를 추가한다. 더미 데이터는 랜덤하게 생성되는 데이터로서, R개의 더미 데이터는 $CM = \{M_c\}_{c=1}^R$ 로 나타낼 수 있다.
- [0054] S150 단계는 입력된 특징점 데이터 중에서 임의로 선택된 제1 특징점 데이터(M_i) 및 더미 데이터가 추가된 특징점 데이터 중에서 상기 선택된 어느 하나의 특징점 데이터를 제외하고 임의로 선택된 제2 특징점 데이터(M_j, M_k)를 이용하여 삼중 극좌표 특징점 데이터를 생성한다. 생성되는 삼중 극좌표 특징점 데이터는 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 포함한다.
- [0055] S170 단계는 S150 단계에서 생성된 삼중 극좌표 특징점 데이터를 퍼지볼트 구조로 암호화한다. S170 단계에 포함되는 S171 단계는 암호화키를 계수로 하는 퍼지볼트 다항식에 상기 삼중 극좌표 특징점 데이터를 변수로 입력하여, 상기 제2 특징점 데이터(M_j, M_k)가 상기 더미 데이터에 해당될 때의 연산되는 값인 제1 집합 데이터($GS_i = \{(CB_{ijk}^T, p_i(CB_{ijk}^T))\}_{M_j, M_k \in SM^T, j=1, k=2, j \neq k \neq i}$)를 생성하고, 상기 제2 특징점 데이터(M_j, M_k)가 상기 더미 데이터에 해당되지 않을 때의 값인 제2 집합 데이터($CS_i = \{(CB_{ijk}^T, u_{ijk})\}_{M_j, M_k \in CM}$)를 생성한다.
- [0056] 다음으로, S170 단계에 포함되는 S173 단계는 상기 제1 집합 데이터 및 제2 집합 데이터를 합성하여 볼트 데이터를 생성한다.
- [0057] 여기에, 암호화키를 공유하는 S190 단계를 더 포함할 수 있다. S190 단계는 퍼지볼트 구조로 암호화하기 위해 사용된 암호화키를 안전하게 공유하기 위해 비밀키($K = k_m || k_{m-1} || \dots || k_0$)를 생성하고, 상기 비밀키를 계수로 갖는 다항식을 생성하여 생성된 다항식에 상기 암호화키를 변수로 입력 및 연산하여 $p(K_i)$ 를 생성하고, 상기 암호화키에 대한 해쉬값($H(K_i)$)을 함께 저장한다. 마지막으로, 난수(K_0)를 생성하고 상기 난수를 이용하여 $(p(K_0), H(K_0))$ 을 생성하여 암호화키와 함께 공개한다.
- [0059] 도 5는 본 발명의 일 실시 예에 따른 지문 인증 방법의 순서도이다. 이하에서는 앞서 지문 등록 방법에서 기재한 부분과 중복되는 구성에 대한 설명은 생략 또는 간략히 하기로 한다.
- [0060] 도 5를 참조하면, S210 단계는 인증이 필요한 사용자 지문의 특징점들에 대한 데이터인 특징점 데이터를 입력받는다. 한편, S210 단계는 미리 입력받은 특징점 데이터의 개수를 조절하는 단계를 더 포함할 수 있다.
- [0061] S230 단계는 S210 단계에서 입력된 특징점 데이터 중에서 임의로 선택된 특징점 데이터(M_i, M_m, M_r)를 이용하여 삼중 극좌표 특징점 데이터를 생성한다.
- [0062] S250 단계는 생성된 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 상기 인증이 필요한 사용자에게 대한 인증을 수행한다. 기 등록된 볼트 데이터는 지문 등록 방법에서 생성된 볼트 데이터일 수 있다. S250 단계는 상기 삼중 극좌표 특징점 데이터에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보와 상

기 기 등록된 볼트 데이터에 포함된 넓이 정보, 거리 정보, 제1 각도 정보 및 제2 각도 정보를 이용하여 인증을 수행한다.

[0064] 도 6은 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 인증을 수행하는 단계의 구체적인 순서도이다.

[0065] 도 6을 참조하면, S250 단계는 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하는 S251 단계, 볼트 데이터를 제1 열린 집합에 포함시키는 S253 단계, 해쉬값을 비교하는 S255 단계 및 $(A_i, p(K_i))$ 을 제2 열린 집합에 포함시키는 S257 단계를 포함할 수 있다.

[0066] 보다 구체적으로, S251 단계는 S230 단계에서 생성된 삼중 극좌표 특징점 데이터와 기 등록된 볼트 데이터를 비교하여 아래의 유사 조건을 만족하는 볼트 데이터가 있는지를 판단한다.

[0067] 유사 조건이란 두 개의 삼중 극좌표 형태의 특징점 데이터가 일치하기 위한 조건으로서, 세 가지 조건을 모두 만족할 때 삼중 극좌표 특징점 데이터가 서로 일치한다고 볼 수 있다.

[0068] 1. $|dec(B_{a_{ijk}}^T) - dec(B_{a_{ijn}}^Q)| \leq a_{threshold}$

[0069] 2. $\min(m_1, m_2) \leq d_{threshold}$

[0070] 3. $\min(m_3, m_4) \leq \theta_{threshold}$

[0071] 여기서, $a_{threshold}$, $d_{threshold}$, $\theta_{threshold}$ 는 각 유사 조건에 대하여 사용자가 미리 설정해놓은 임계값이다. 또한, m_1, m_2, m_3, m_4 는 아래와 같다.

[0072]
$$m_1 = \sqrt{(dec(B_{r_{ij}}^T)^2 + dec(B_{r_{jn}}^Q)^2 - 2dec(B_{r_{ij}}^T)dec(B_{r_{jn}}^Q)\cos(dec(B_{\phi_{ij}}^T) - dec(B_{\phi_{jn}}^Q)))}$$

[0073]
$$m_2 = \sqrt{(dec(B_{r_{ij}}^T)^2 + dec(B_{r_{jn}}^Q)^2 - 2dec(B_{r_{ij}}^T)dec(B_{r_{jn}}^Q)\cos(dec(B_{\phi_{ij}}^T) - dec(B_{\phi_{jn}}^Q)))}$$

[0074]
$$m_3 = |dec(B_{\theta_{ijk}}^T) - dec(B_{\theta_{ijn}}^Q)|, \quad m_4 = |dec(B_{\theta_{ijk}}^T) - dec(B_{\theta_{ijn}}^Q)|$$

[0075] 여기서, $dec(x)$ 는 x를 10진수로 변환한 것을 의미한다.

[0076] S253 단계는 S251 단계에서 유사 조건을 모두 만족하는 것으로 판단된 볼트 데이터에 속한 (CB_{ijk}^T, y) 를 제1 열린 집합(unlocking set) UL_i 에 포함시킨다. 여기서, y는 제1 집합 데이터의 $p_i(CB_{ijk}^T)$ 또는 제2 집합 데이터의 y_{ijk} 를 의미한다. 만약 상기 유사 조건 중 어느 하나라도 만족하지 못한다면, S251 단계로 돌아가서 다른 볼트 데이터와의 비교를 수행한다. 한편, S251 단계 내지 S253 단계는 $|UL_i| \geq n_0$ 를 만족할 때까지 반복 수행되며, $|UL_i| \geq n$ 을 만족하는 경우 S255 단계가 수행된다.

[0077] S255 단계는 해쉬값을 비교하는 단계로서, $|UL_i| \geq n$ 을 만족할 때의 UL_i 로 퍼지볼트 다항식을 재구성해서 상기 재구성된 다항식의 계수 값인 $A_i = a_{i,n-1}a_{i,n-2} \dots a_{i,0}$ 을 생성하여 해쉬값 $H(A_i)$ 을 계산하고, $H(A_i)$ 와 $H(K_i)$ 의 비교를 수행한다. 다항식을 재구성하는 것은 라그랑주 보간법(Lagrange interpolation)을 이용할 수 있다.

[0078] S257 단계는 S255 단계에서 해쉬값을 비교한 결과 같다고 판단되면 $(A_i, p(K_i))$ 를 제2 열린 집합 UL 에 포함시킨다. 만약 해쉬값이 다르다고 판단되면 S251 단계부터 다시 수행한다.

[0079] 상기 S251 내지 S257 단계는 모든 삼중 극좌표 특징점 데이터에 대하여 반복 수행하여 생성되며, 최종적으로 생

성된 제2 열린집합이 $|UL| \geq m$ 을 만족하면 사용자에게 대한 인증이 성공한 것이며, 만족하지 못하면 인증이 실패한 것으로 볼 수 있다.

[0080] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0081] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

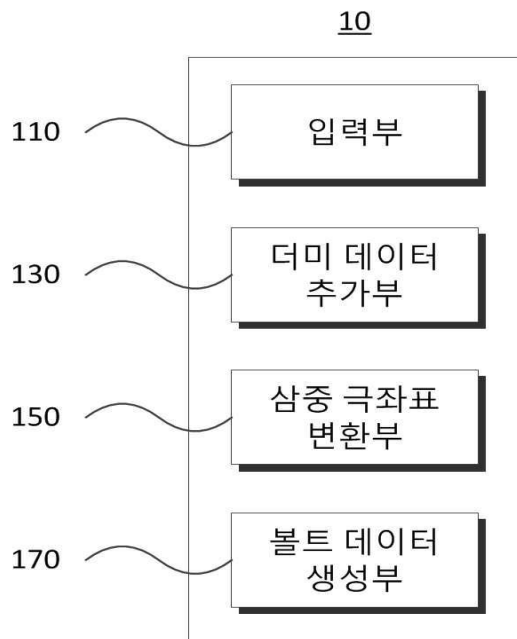
[0082] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0083] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

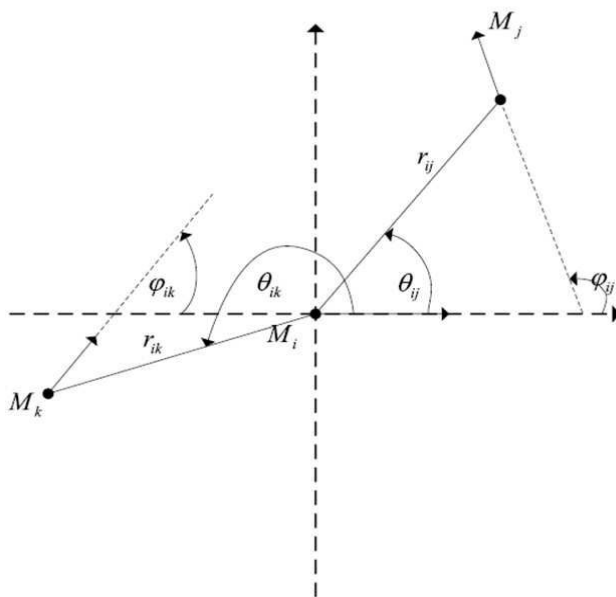
[0084] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

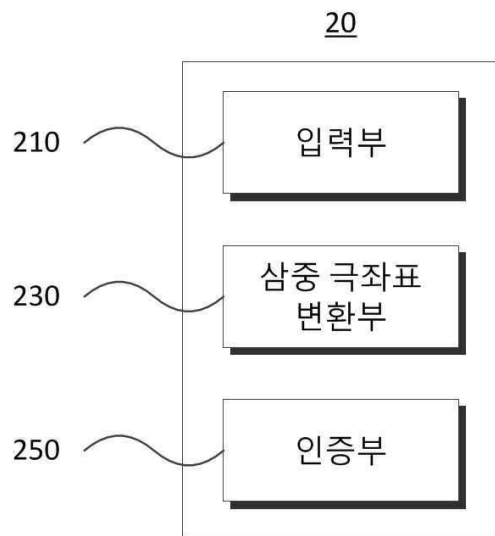
도면1



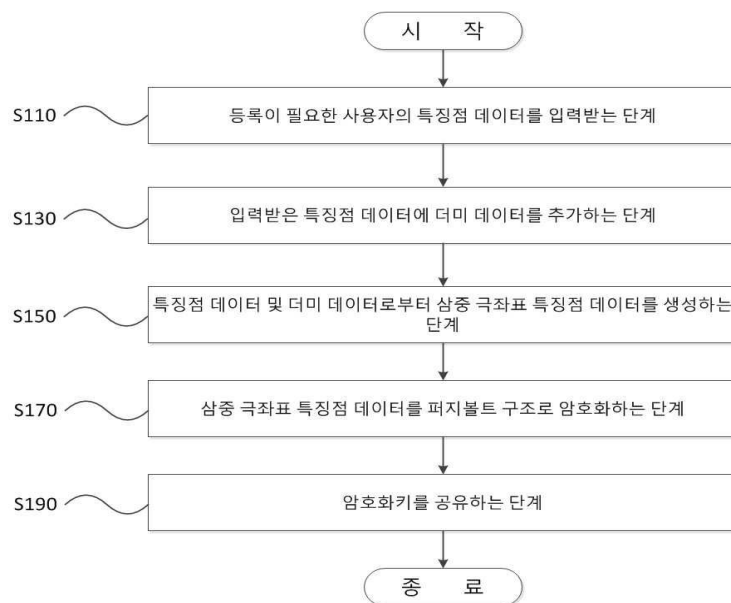
도면2



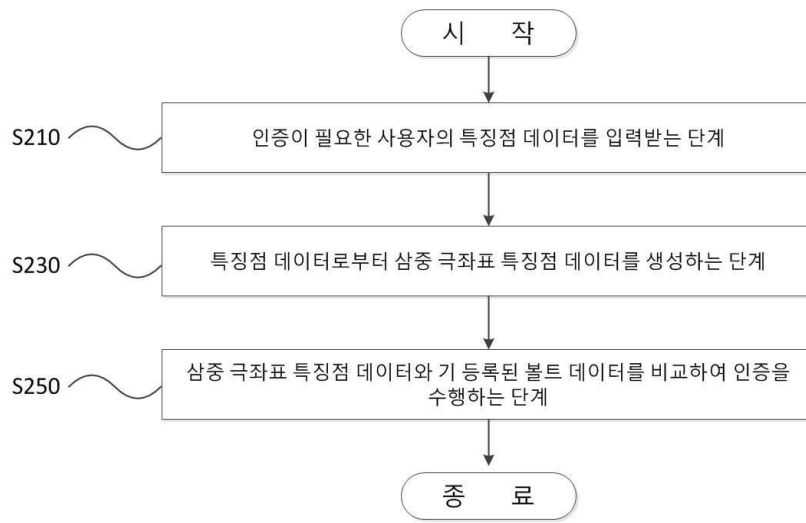
도면3



도면4



도면5



도면6

