



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년05월23일
(11) 등록번호 10-1036367
(24) 등록일자 2011년05월16일

(51) Int. Cl.

G06K 9/00 (2006.01)

(21) 출원번호 10-2009-0123899

(22) 출원일자 2009년12월14일

심사청구일자 2009년12월14일

(56) 선행기술조사문헌

KR1020080070363 A

KR1020090110026 A

(73) 특허권자

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

정용화

대전광역시 유성구 지족동 877 열매마을아파트
505-402

이성주

서울특별시 마포구 성산동 47-14

(뒷면에 계속)

(74) 대리인

나승택, 조영현

전체 청구항 수 : 총 9 항

심사관 : 변종길

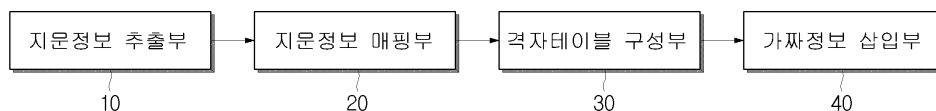
(54) 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치 및 방법

(57) 요약

본 발명은 상관공격에 강인한 퍼지볼트를 이용하여 지문 템플릿을 형성하는 장치 및 방법에 관한 것으로, 특히 퍼지볼트를 이용하여 특징점의 위치(평면 좌표) 및 각도 정보로 구성되는 3차원 격자 구조 공간의 빈 격자 공간에 거짓 특징점을 비임의적(규칙적)으로 삽입하여 지문 템플릿을 형성함으로써, 동일한 지문 정보로부터 생성된 두 개의 지문 템플릿을 획득하더라도 진짜와 거짓 특징점을 구별하기 어렵게 하여 상관 공격으로부터 강인하게 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치 및 방법에 관한 것이다.

본 발명인 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치를 이루는 구성수단은, 지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출하는 지문정보 추출부, 상기 지문 정보를 이용하여 상기 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시키는 지문정보 매핑부, 상기 지문 특징점이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형하는 격자 테이블 구성부, 상기 격자 테이블의 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점을 삽입하는 가짜 정보 삽입부를 포함하여 이루어진 것을 특징으로 한다.

대표도 - 도2



(72) 발명자

홍승우

서울특별시 강남구 삼성동 상아아파트 2차 3동
1012호

최한나

서울특별시 강서구 화곡8동 394-18 해풍맨션 203호

이은지

경상북도 경산시 정평동 130 현대타운 106-602

특허청구의 범위

청구항 1

지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출하는 지문정보 추출부;

상기 지문 정보를 이용하여 상기 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시키는 지문 정보 매핑부;

상기 지문 특징점이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형하는 격자 테이블 구성부;

상기 격자 테이블의 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입하는 가짜 정보 삽입부를 포함하여 이루어진 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치.

청구항 2

청구항 1에 있어서,

상기 가짜 정보 삽입부는 상기 거짓 특징점들을 상기 지문 특징점들이 위치하지 않는 모든 격자 공간 하나씩 삽입하는 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 지문정보 매핑부는 상기 지문 정보의 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑하는 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치.

청구항 4

청구항 1 또는 청구항 2에 있어서,

상기 격자 테이블 구성부는 각 격자에 하나의 지문 특징점만 위치될 수 있도록 상기 격자 테이블을 구성하는 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치.

청구항 5

지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출하는 단계;

상기 지문 정보를 이용하여 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시키는 단계;

상기 지문 특징점이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형하는 단계;

상기 격자 테이블의 격자들 중, 상기 지문 특징점이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입하는 단계를 포함하여 이루어진 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법.

청구항 6

청구항 5에 있어서,

상기 거짓 특징점들을 삽입하는 단계는, 상기 거짓 특징점들을 상기 지문 특징점이 위치하지 않는 모든 격자 공간에 하나씩 삽입하는 단계인 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성

방법.

청구항 7

청구항 5 또는 청구항 6에 있어서,

상기 지문 특징점들을 상기 3차원 테이블에 매핑시키는 단계는, 상기 지문 정보의 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑하는 단계인 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법.

청구항 8

청구항 7에 있어서,

$$Z_i = \frac{\theta_i}{360} \times M_z$$

상기 Z축 좌표값(Z_i)은 을 통해 계산되는 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법.

여기서, θ_i 는 i번째 지문 특징점의 각도이고, Z_i 는 i번째 지문 특징점의 각도가 변환된 i번째 지문 정보에 대한 Z축 좌표 값이며, M_z 는 설정된 최대 Z축 좌표값임.

청구항 9

청구항 5 또는 청구항 6에 있어서,

상기 격자 테이블 구조로 변형하는 단계는 각 격자에 하나의 지문 특징점만 위치될 수 있도록 상기 2차원 또는 3차원 테이블을 격자 테이블로 변형하는 단계인 것을 특징으로 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법.

명세서

발명의 상세한 설명

기술분야

[0001] 본 발명은 퍼지볼트를 이용하여 지문 템플릿을 형성하는 장치 및 방법에 관한 것으로, 특히 퍼지볼트를 이용하여 특징점의 위치(평면 좌표) 및 각도 정보로 구성되는 3차원 격자 구조 공간의 빈 격자 공간에 거짓 특징점을 비임의적(규칙적)으로 삽입하여 지문 템플릿을 형성함으로써, 동일한 지문 정보로부터 생성된 두 개의 지문 템플릿을 획득하더라도 진짜와 거짓 특징점을 구별하기 어렵게 하여 상관 공격으로부터 강인하게 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치 및 방법에 관한 것이다.

배경기술

[0002] 바이오 인식 기술은 패스워드 또는 PIN 방식에 비해서 타인에 의해 도용될 우려가 적고 사용자가 암기하지 않아도 되는 장점이 있다. 그러나 사용자 인증을 위해 저장된 바이오 정보가 타인에게 도용된다면 패스워드나 PIN과 달리 변경이 불가능하거나 제한적이기 때문에 심각한 문제를 일으킬 수 있다. 따라서 바이오 정보를 안전하게 전송/저장하는 방법이 필요하다[U. Uludag, *et al.*, "Biometric Cryptosystems: Issues and Challenges," *Proc. of IEEE*, 2004].

[0003] 2002년 Juels이 퍼지볼트 이론을 제안하면서부터 퍼지볼트를 지문에 적용하는 연구가 활발히 진행되고 있다.

[0004] 지문 퍼지볼트([T. Clancy, *et al.*, "Secure Smartcard-based Fingerprint Authentication," 2003.], [U.

Uludag, *et al.*, "Fuzzy Vault for Fingerprints," *LNCS 3546*, 2005.] 방법은 다수의 거짓 특징점(chaff minutiae)을 '임의'로 생성하여 진짜 특징점(real minutiae)과 함께 데이터베이스에 지문 템플릿으로 등록함으로써 지문 정보를 보호한다. 그러나 초기의 지문 퍼지볼트 방법은 퍼지볼트 이론을 지문에 적용하였을 때 발생하는 지문정렬 문제(Fingerprint Alignment Problem)를 가정하거나 수동으로 정렬하였다.

- [0005] 지문 퍼지볼트의 자동 정렬을 위해서 여러 가지 연구가 진행되었다. 그러나 대부분의 방법은 신뢰할 수 있는 지문 특징점이 있다고 가정하기 때문에 실제 응용에 적용하기에는 한계가 있다.
- [0006] 또한, 추가 정보를 이용해서 자동 정렬을 해결하는 방법이 보고되었지만([U. Uludag and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data," *Proc. of PRIV*, 2006.], [K. Nandakumar, *et al.*, "Fingerprint-based Fuzzy Vault: Implementation and Performance," *IEEE Tr. IFS*, 2007.], [A. Nagar, *et al.*, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors," *Proc. of ICPR*, 2008.]), 이러한 방법은 지문 퍼지볼트의 안전도가 저하 될 수 있다.
- [0007] 따라서 추가 정보 없이 자동 정렬을 해결해야 하며, Kholmatov[A. Kholmatov, *et al.*, "Secret Sharing using Biometric Traits," *Proc. of SPIE*, 2006.]는 전수조사(brute-force)를 통하여 퍼지볼트와 입력 지문을 정렬하였는데, 삽입되는 거짓 특징점의 수가 증가하게 되면 수행시간이 증가하게 된다는 문제가 있다.
- [0008] 전수조사 방법 외에 Chung은 기하학적 해싱(Geometric Hashing)[H. Wolfson and I. Rigoutsos, "Geometric Hashing: an Overview," *IEEE CSE*, 1997.]을 이용하여 지문 퍼지볼트에 추가 정보 없이 자동 정렬을 수행하였다. 또한, 수행시간을 감소시키기 위하여 빠른 다항식 복원 방법도 보고되었다[최우용, *et al.*, "지문 퍼지 볼트의 빠른 다항식 복원 방법," *정보보호학회 논문지*, 2008.].
- [0009] 그러나 최근, 이러한 지문 퍼지볼트를 효과적으로 크래킹할 수 있는 상관공격(Correlation Attack)에 관한 연구가 발표되었다([W. Scheirer and T. Boulton, "Cracking Fuzzy Vaults and Biometric Encryption," 2007.], [A. Kholmatov and B. Yanikoglu, "Realization of Correlation Attack against the Fuzzy Vault Scheme," *Proc. of SPIE*, 2008.]).
- [0010] 이것은 동일한 지문으로부터 생성되는 두 개 이상의 지문 템플릿을 획득하여 진짜 특징점과 거짓 특징점을 쉽게 구별하는 방법이다. 상관공격은 지문 퍼지볼트에만 국한되는 것이 아니라, 기밀성을 제공하기 위해 거짓 특징점을 "임의"로 삽입하는 방식에 기본적으로 적용 가능한 방법이다.
- [0011] 즉, 실제 지문 퍼지볼트에 적용 가능한 공격이기 때문에 이를 보호하는 방법이 반드시 필요하지만, 아직까지 이에 대한 연구결과가 발표되지 않고 있다.
- [0012] 지문 퍼지볼트의 상관공격은 동일한 지문으로부터 생성되는 두 개의 지문 템플릿을 취득함으로써 진짜 특징점과 거짓 특징점을 쉽게 구별하는 방법이다. 즉, 동일한 지문으로부터 생성된 지문 템플릿에서, 진짜 특징점은 유사한 위치와 각도를 유지하면서 생성되고, 거짓 특징점은 랜덤함수에 의해 위치와 각도가 "임의"로 결정된 후 삽입되게 된다.
- [0013] 따라서 두 지문 템플릿을 정렬하여 가장 많이 매칭되는 특징점을 획득하면, 매칭되는 특징점들 중에는 진짜 특징점 다수와 거짓 특징점 소수가 추출된다.
- [0014] 도 1은 상관공격에 의한 지문 퍼지볼트의 크래킹 과정의 예를 보여준다. 도 1의 (a)와 도 1의 (b)는 동일한 지문으로부터 생성된 각각의 지문 템플릿이다. 그러나 두 지문 템플릿이 매칭된다면 도 1의 (c)와 같이 진짜 특징점을 쉽게 추출할 수 있다.
- [0015] 더 구체적으로 설명하면, 특정 지문으로부터 진짜 특징점(흰 점)을 추출하고, 가짜 특징점(검은 점)을 "임의"로 생성하여 도 1의 (a)와 같은 지문 템플릿을 형성했다고 가정하자. 이 때, 상기 가짜 특징점은 랜덤하게 생성하여 상기 진짜 특징점들과 함께 지문 템플릿을 구성한다.
- [0016] 그런 다음, 상기 특정 지문과 동일한 지문으로부터 진짜 특징점(흰 점)을 추출하고, 가짜 특징점(검은 점)을 "임의"로 생성하여 도 1의 (b)와 같은 지문 템플릿을 형성했다고 하자. 이 때, 진짜 특징점은 도 1의 (a)에서의 진짜 특징점과 유사한 위치와 각도를 유지할 것이다. 그러나, 가짜 특징점은 랜덤하게 생성하기 때문에, 도 1의 (a)의 거짓 특징점과 상이한 위치 및 각도를 가진 거짓 특징점들이 지문 템플릿을 구성할 것이다.
- [0017] 이 상태에서, 도 1의 (c)와 같이, 도 1의 (a) 및 도 1의 (b)의 지문 템플릿을 정렬하여, 가장 많이 매칭되는 특징점(녹색 원의 특징점)들을 획득하면, 도 1의 (a) 및 도 1의 (b)의 진짜 특징점들은 서로 유사한 위치 및 각도

를 가지기 때문에, 상기 매칭되는 특징점들의 다수를 차지할 것이고, 도 1의 (a) 및 도 1의 (b)의 가짜 특징점들은 서로 상이한 위치 및 각도를 가지기 때문에(랜덤하게 형성하기 때문에), 상기 매칭되는 특징점들의 극소수를 차지할 것이다.

[0018] 결국, 진짜 특징점들을 용이하게 추출할 수 있기 때문에, 이와 같은 종래의 일반적인 지문 템플릿은 상관공격으로부터 용이하게 공격당하는 문제점을 안고 있다.

발명의 내용

해결 하고자하는 과제

[0019] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하기 위하여 창안된 것으로, 퍼지볼트를 이용하여 특징점의 위치(평면 좌표) 및 각도 정보로 구성되는 3차원 격자 구조 공간의 빈 격자 공간에 거짓 특징점을 비임의적(규칙적)으로 삽입하여 지문 템플릿을 형성함으로써, 동일한 지문 정보로부터 생성된 두 개의 지문 템플릿을 획득하더라도 진짜와 거짓 특징점을 구별하기 어렵게 하여 상관 공격으로부터 강인하게 하는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치 및 방법을 제공하는 것을 그 목적으로 한다.

과제 해결수단

[0020] 상기와 같은 과제를 해결하기 위하여 제안된 본 발명인 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치를 이루는 구성수단은, 지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출하는 지문정보 추출부, 상기 지문 정보를 이용하여 상기 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시키는 지문정보 매핑부, 상기 지문 특징점들이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형하는 격자 테이블 구성부, 상기 격자 테이블의 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입하는 가짜 정보 삽입부를 포함하여 이루어진 것을 특징으로 한다.

[0021] 또한, 상기 가짜 정보 삽입부는 상기 거짓 특징점들을 상기 지문 특징점들이 위치하지 않는 모든 격자 공간에 하나씩 삽입하는 것을 특징으로 한다.

[0022] 여기서, 상기 지문정보 매핑부는 상기 지문 정보의 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑하는 것을 특징으로 한다.

[0023] 여기서, 상기 격자 테이블 구성부는 각 격자에 하나의 지문정보만 위치될 수 있도록 상기 격자 테이블을 구성하는 것을 특징으로 한다.

[0024] 또 다른 본 발명인 퍼지볼트를 이용한 지문 템플릿 형성 방법을 이루는 구성수단은, 지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출하는 단계, 상기 지문 정보를 이용하여 상기 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시키는 단계, 상기 지문 특징점들이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형하는 단계, 상기 격자 테이블의 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입하는 단계를 포함하여 이루어진 것을 특징으로 한다.

[0025] 또한, 상기 거짓 특징점들을 삽입하는 단계는, 상기 거짓 특징점들을 상기 지문 특징점들이 위치하지 않는 모든 격자 공간에 하나씩 삽입하는 단계인 것을 특징으로 한다.

[0026] 여기서, 상기 지문 특징점들을 상기 3차원 테이블에 매핑시키는 단계는, 상기 지문 정보의 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑하는 단계인 것을 특징으로 한다.

$$Z_i = \frac{\theta_i}{360} \times M_z$$

[0027] 여기서, 상기 Z축 좌표값(Z_i)은 θ_i 을 통해 계산되는 것을 특징으로 하되, 여기서, θ_i 는 i번째 지문 특징점의 각도이고, Z_i 는 i번째 지문 특징점의 각도가 변환된 i번째 지문 특징점에 대한 Z축 좌표 값이며, M_z 는 설정된 최대 Z축 좌표값이다.

[0028] 또한, 상기 격자 테이블 구조로 변형하는 단계는 각 격자에 하나의 지문 특징점만 위치될 수 있도록 상기 2차원

또는 3차원 테이블을 격자 테이블로 변형하는 단계인 것을 특징으로 한다.

효 과

- [0029] 상기와 같은 과제 및 해결 수단을 가지는 본 발명인 상관공격에 강인한 퍼지볼트를 이용하여 지문 템플릿을 형성하는 장치 및 방법에 의하면, 퍼지볼트를 이용하여 특징점의 위치(평면 좌표) 및 각도 정보로 구성되는 3차원 격자 구조 공간의 빈 격자 공간에 거짓 특징점을 비임의적(규칙적)으로 삽입하여 지문 템플릿을 형성하기 때문에, 동일한 지문 정보로부터 생성된 두 개의 지문 템플릿을 획득하더라도 진짜와 거짓 특징점을 구별하기 어렵게 하고, 결국 상관 공격으로부터 강인하게 하는 장점이 있다.

발명의 실시를 위한 구체적인 내용

- [0030] 이하, 첨부된 도면을 참조하여 상기와 같은 과제, 해결수단 및 효과를 가지는 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치 및 그 방법에 관한 바람직한 실시예를 상세하게 설명한다.
- [0031] 도 2는 본 발명의 실시예에 따른 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치의 구성도이다.
- [0032] 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치는 지문정보 추출부(10), 지문정보 매핑부(20), 격자테이블 구성부(30) 및 가짜정보 삽입부(40)를 포함하여 구성된다.
- [0033] 상기 지문정보 추출부(10)는 지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들(진짜 특징점들)의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출한다. 즉, 상기 지문정보 추출부(10)는 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 지문 영상에서 지문 특징점들의 좌표에 해당하는 위치 및 각도를 포함하여 구성되는 지문 정보를 추출한다.
- [0034] 본 발명은 퍼지볼트를 이용하여 지문 템플릿을 형성하기 때문에, 상기 지문 특징점들의 지문 정보는 상기 위치 및 각도 정보뿐 아니라, 다항식 값으로 나타나며, $m_i = (x_i, y_i, \theta_i, f(x_i | y_i))$ 로 표현된다. 여기서, m_i 는 i 번째 지문 특징점을 의미하고, x_i 및 y_i 는 i 번째 지문 특징점의 평면상의 위치 좌표를 의미하고, θ_i 는 i 번째 지문 특징점의 각도를 의미하며, $f(x_i | y_i)$ 는 i 번째 지문 특징점에 대한 다항식 값을 의미한다.
- [0035] 상기 지문정보 추출부(10)에 의하여 지문의 특징점들에 대한 지문 정보가 추출되면, 상기 지문정보 매핑부(20)는 상기 지문 정보를 이용하여 상기 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시킨다.
- [0036] 상기 지문정보 매핑부(20)가 상기 지문 특징점들을 2차원 테이블에 매핑시킬 것인지 또는 3차원 테이블에 매핑시킬 것인지는 사전 설정에 의하여 결정될 수 있다. 즉, 사전 설정에 의하여, 상기 지문정보 매핑부(20)가 지문 특징점들을 2차원 테이블에 매핑시키도록 설정하거나, 3차원 테이블에 매핑시키도록 설정할 수 있다.
- [0037] 상기와 같이, 2차원 테이블에 지문 특징점들을 매핑시킬 수 있다. 그런데, 2차원 테이블에 지문 특징점들을 매핑시키는 경우에는, 지문 센서 크기의 제약으로 인하여 후술하는 거짓 특징점들의 삽입 개수가 제한적이다. 즉, 인증 정확도를 위해서 특징점들 사이에 임계적 거리를 유지해야할 필요가 있기 때문에, 정해진 지문 센서 크기의 이미지 평면에 삽입할 거짓 특징점의 개수는 제한적이다.
- [0038] 반면, 상관공격에 강인하고, 보안성을 향상시키기 위해서는 거짓 특징점들을 많이 삽입해야 한다. 따라서, 상기 지문 특징점들을 3차원 테이블 상에 매핑시킬 필요가 있다.
- [0039] 상기 지문정보 매핑부(20)에 의하여 지문정보를 이용하여 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시킨 후에는 격자 테이블 구성부(30)가 상기 지문 정보를 가지는 지문 특징점들이 매핑된 상기 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형한다.
- [0040] 즉, 2차원 테이블을 격자 테이블 구조로 변형하는 경우에는 평면 상의 가로 및 세로를 일정한 간격으로 나누어 격자 테이블을 구성한다. 후술하겠지만, 이 때, 격자 테이블 구조로 변형하는 방법은 상기 2차원 테이블에 매핑된 지문 특징점들이 각 격자에 하나씩 위치할 수 있도록 2차원 테이블을 격자 테이블로 구성한다.
- [0041] 만약, 3차원 테이블을 격자 테이블 구조로 변형하는 경우에는 평면 상의 가로 및 세로를 일정한 간격으로 나누

과 동시에, 높이(Z축) 방향으로도 일정한 간격으로 나누어 3차원 격자 테이블 구조로 변형한다. 후술하겠지만, 이 때, 3차원 격자 테이블 구조로 변형하는 방법은 상기 3차원 테이블에 매핑된 지문 특징점들이 각 격자에 하나씩 위치할 수 있도록 3차원 테이블을 격자 테이블로 구성한다.

[0042] 상기와 같이, 격자테이블 구성부(30)에 의하여 2차원 또는 3차원 격자 테이블이 구성되면, 상기 지문 특징점들 하나의 격자에 하나씩 위치할 것이고, 상기 지문 특징점들이 위치하지 않는 격자 공간들이 존재할 것이다.

[0043] 상기 격자테이블이 완성된 후, 가짜 정보 삽입부(40)는 상기 격자 테이블을 구성하는 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입한다. 이 때, 상기 비어있는 격자 공간에 삽입되는 거짓 특징점들은 랜덤하게(임의적으로) 생성하는 것이 아니라, 비임의적으로(규칙적으로) 생성되어 상기 빈 격자 공간에 삽입된다. 여기서 "규칙적"(비임의적)이란 종래 기술과 같이 거짓 특징점들을 임의적으로 생성하는 것이 아니라, 빈 격자 공간의 위치에 맞추어 비임의적으로 생성하여 상기 빈 격자 공간에 삽입한다는 의미이다.

[0044] 여기서, 상기 가짜 정보 삽입부(40)는 상기 거짓 특징점들을 상기 지문 특징점(진짜 특징점)이 위치하지 않는 빈 격자 공간들 중 일부의 격자 공간에 삽입할 수도 있고, 비어있는 모든 격자 공간에 상기 거짓 특징점들을 삽입할 수도 있다. 다만, 상관공격에 가장 강인하기 위하여, 거짓 특징점들을 상기 지문 특징점들(진짜 특징점들)이 위치하지 않는 모든 격자 공간에 하나씩 삽입하는 것이 바람직하다.

[0045] 이와 같이, 상기 가짜 정보 삽입부(40)에 의하여 거짓 특징점들을 빈 격자 공간에 규칙적으로 삽입되면, 상관공격에 강인한 지문 템플릿이 형성된다. 이와 같이 형성된 지문 템플릿을 등록시켜 인증 절차에 활용할 수 있다.

[0046] 한편, 상기 지문 특징점(진짜 특징점)들을 2차원 또는 3차원 테이블에 매핑시키는 지문정보 매핑부(20)가 상기 지문 특징점들을 3차원 테이블에 매핑시키기 위해서는 Z축 좌표가 존재해야 한다.

[0047] 따라서, 상기 지문정보 매핑부(20)는 상기 지문 특징점에 대한 지문 정보 중, 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑한다. 결국, 3차원 테이블에 상기 지문 특징점들을 매핑하게 되면, 상기 지문 특징점들의 지문 정보는 Z축 성분이 더 추가된다.

[0048] 즉, 앞서 설명한, 추출된 지문 정보는 $m_i = (x_i, y_i, \theta_i, f(x_i | y_i))$ 로 표현되지만, 3차원 테이블로 확장된 후의 지문 정보는 $m_i = (x_i, y_i, z_i, \theta_i, f(x_i | y_i))$ 가 된다.

[0049] 또한, 상기 격자 테이블 구성부(30)는 상기 지문 특징점들이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 구성하는 과정에서, 각 격자에 하나의 지문 특징점만 위치될 수 있도록 상기 2차원 또는 3차원 테이블을 격자 테이블로 구성한다.

[0050] 이상에서 설명한 구성요소들에 의하여 형성된 지문 템플릿은 거짓 특징점들이 "임의적"으로 삽입되는 것이 아니라, 해당 위치 즉, 빈 격자 공간에 "규칙적"으로 삽입되기 때문에, 동일한 지문에 의하여 형성된 두 개의 지문 템플릿을 매칭하더라도, 진짜 특징점들을 쉽게 분리할 수 없어 상관공격에 강인하게 된다. 즉, 진짜 특징점뿐만 아니라, "규칙적" 삽입에 의하여 거짓 특징점들도 다수 일치하게 되기 때문에, 진짜 특징점들을 구별하는 것은 매우 어렵다.

[0051] 다음은, 이상에서 설명한 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치를 이용하여 지문 템플릿을 형성하는 방법에 대하여 구체적으로 설명한다.

[0052] 도 3은 본 발명의 실시예에 따른 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법에 관한 절차도이다.

[0053] 도 3에 도시된 바와 같이, 먼저, 지문 영상을 입력받아 상기 지문 영상에서 지문 특징점들(진짜 특징점들)의 위치 및 각도를 포함하여 구성되는 지문 정보를 추출한다(s10). 즉, 센싱장치를 이용하여 인증 사용자의 지문 영상을 입력받고, 지문 영상에서 지문 특징점들의 좌표에 해당하는 위치 및 각도를 포함하여 구성되는 지문 정보를 추출한다.

[0054] 본 발명은 퍼지볼트를 이용하여 지문 템플릿을 형성하기 때문에, 상기 지문 특징점들의 지문 정보는 상기 위치 및 각도 정보뿐 아니라, 다항식 값으로 나타나며, $m_i = (x_i, y_i, \theta_i, f(x_i | y_i))$ 로 표현된다. 여기서, m_i 는 i 번째 지문 특징점을 의미하고, x_i 및 y_i 는 i 번째 지문 특징점의 평면상의 위치 좌표를 의미하고, θ_i 는 i 번째 지문 특징점의 각도를 의미하며, $f(x_i | y_i)$ 는 i 번째 지문 특징점에 대한 다항식 값을 의미한다.

[0055] 상기 단계(s10)에 의하여 지문의 특징점들에 대한 지문 정보가 추출되면, 상기 지문 정보를 이용하여 상기 지문

특징점들을 2차원 또는 3차원 테이블에 매핑시킨다(s20).

- [0056] 상기 지문 특징점들을 2차원 테이블에 매핑시킬 것인지 또는 3차원 테이블에 매핑시킬 것인지는 사전 설정에 의하여 결정될 수 있다. 즉, 사전 설정에 의하여, 지문 특징점들을 2차원 테이블에 매핑시키도록 설정하거나, 3차원 테이블에 매핑시키도록 설정할 수 있다.
- [0057] 상기와 같이, 2차원 테이블에 지문 특징점들을 매핑시킬 수 있다. 그런데, 2차원 테이블에 지문 특징점들을 매핑시키는 경우에는, 지문 센서 크기의 제약으로 인하여 후술하는 거짓 특징점들의 삽입 개수가 제한적이다. 즉, 인증 정확도를 위해서 특징점들 사이에 임계적 거리를 유지해야할 필요가 있기 때문에, 정해진 지문 센서 크기의 이미지 평면에 삽입할 거짓 특징점의 개수는 제한적이다.
- [0058] 반면, 상관공격에 강인하고, 보안성을 향상시키기 위해서는 거짓 특징점들을 많이 삽입해야 한다. 따라서, 상기 지문 특징점들을 3차원 테이블 상에 매핑시킬 필요가 있다.
- [0059] 상기 단계(s20)에 의하여 지문정보를 이용하여 지문 특징점들을 2차원 또는 3차원 테이블에 매핑시킨 후에는, 상기 지문 정보를 가지는 지문 특징점들이 매핑된 상기 2차원 또는 3차원 테이블을 격자 테이블 구조로 변형한다.
- [0060] 즉, 2차원 테이블을 격자 테이블 구조로 변형하는 경우에는 평면 상의 가로 및 세로를 일정한 간격으로 나누어 격자 테이블을 구성한다. 후술하겠지만, 이 때, 격자 테이블 구조로 변형하는 방법은 상기 2차원 테이블에 매핑된 지문 특징점들이 각 격자에 하나씩 위치할 수 있도록 2차원 테이블을 격자 테이블로 구성한다.
- [0061] 만약, 3차원 테이블을 격자 테이블 구조로 변형하는 경우에는 평면 상의 가로 및 세로를 일정한 간격으로 나눔과 동시에, 높이(Z축) 방향으로도 일정한 간격으로 나누어 3차원 격자 테이블 구조로 변형한다. 후술하겠지만, 이 때, 3차원 격자 테이블 구조로 변형하는 방법은 상기 3차원 테이블에 매핑된 지문 특징점들이 각 격자에 하나씩 위치할 수 있도록 3차원 테이블을 격자 테이블로 구성한다.
- [0062] 상기와 같이, 단계 s30 의하여, 2차원 또는 3차원 격자 테이블이 구성되면, 상기 지문 특징점들 하나의 격자에 하나씩 위치할 것이고, 상기 지문 특징점들이 위치하지 않는 격자 공간들이 존재할 것이다.
- [0063] 상기 격자테이블이 완성된 후, 상기 격자 테이블을 구성하는 격자들 중, 상기 지문 특징점들이 위치하지 않는 격자 공간에 거짓 특징점들을 삽입한다(s40). 이 때, 상기 비어있는 격자 공간에 삽입되는 거짓 특징점들은 랜덤하게(임의적으로) 생성하는 것이 아니라, 비임의적으로(규칙적으로) 생성되어 상기 빈 격자 공간에 삽입된다.
- [0064] 여기서 "규칙적"(비임의적)이란 종래 기술과 같이 거짓 특징점들을 임의적으로 생성하는 것이 아니라, 빈 격자 공간의 위치에 맞추어 비임의적으로 생성하여 상기 빈 격자 공간에 삽입한다는 의미이다.
- [0065] 여기서, 상기 거짓 특징점들을 상기 지문 특징점(진짜 특징점)이 위치하지 않는 빈 격자 공간들 중 일부의 격자 공간에 삽입할 수도 있고, 비어있는 모든 격자 공간에 상기 거짓 특징점들을 삽입할 수도 있다. 다만, 상관공격에 가장 강인하기 위하여, 거짓 특징점들을 상기 지문 특징점들(진짜 특징점들)이 위치하지 않는 모든 격자 공간에 하나씩 삽입하는 것이 바람직하다.
- [0066] 이와 같이, 거짓 특징점들을 빈 격자 공간에 규칙적으로 삽입되면, 상관공격에 강인한 지문 템플릿이 형성된다. 이와 같이 형성된 지문 템플릿을 등록시켜 인증 절차에 활용할 수 있다.
- [0067] 한편, 상기 지문 특징점(진짜 특징점)들을 2차원 또는 3차원 테이블에 매핑시키는 단계(s20)에서, 상기 지문 특징점들을 상기 3차원 테이블에 매핑시키기 위해서는 Z축 좌표가 존재해야 한다.
- [0068] 따라서, 상기 지문 특징점들을 상기 3차원 테이블에 매핑시키는 단계(s20)에서, 상기 지문 특징점에 대한 지문 정보 중, 각도를 Z축 좌표로 변환하여, 상기 지문 특징점들을 3차원 테이블에 매핑한다. 결국, 3차원 테이블에 상기 지문 특징점들을 매핑하게 되면, 상기 지문 특징점들의 지문 정보는 Z축 성분이 더 추가된다.
- [0069] 즉, 앞서 설명한, 추출된 지문 정보는 $m_i = (x_i, y_i, \theta_i, f(x_i | y_i))$ 로 표현되지만, 3차원 테이블로 확장된 후의 지문 정보는 $m_i = (x_i, y_i, z_i, \theta_i, f(x_i | y_i))$ 가 된다.
- [0070] 상기와 같이 지문 정보의 각도를 이용하여 Z축 좌표 값으로 변환하기 위한 수식 1은 아래와 같다.

$$Z_i = \frac{\theta_i}{360} \times M_z$$

[0071] (수식 1)

$$Z_i = \frac{\theta_i}{360} \times M_z$$

[0072] 즉, 상기 Z축 좌표값(Z_i)은 을 통해 계산되는데, 여기서, θ_i 는 i 번째 지문 특징점의 각도이고, Z_i 는 i 번째 지문 특징점의 각도가 변환된 i 번째 지문 정보에 대한 Z축 좌표 값이며, M_z 는 설정된 최대 Z축 좌표값이다.

[0073] 예를 들어, 특정 지문 특징점의 각도가 60° 라 하고, 사전에 설정된 최대 Z축 좌표값이 360이라 하면, 상기 수식 1에 의하여, 상기 특정 지문 특징점이 3차원 테이블에 매핑되는 Z축 좌표값은 60이 된다.

[0074] 한편, 상기 격자 테이블 구조로 변형하는 단계(s30)에 해당하는 상기 지문 특징점들이 매핑된 2차원 또는 3차원 테이블을 격자 테이블 구조로 구성하는 과정에서, 각 격자에 하나의 지문 특징점만 위치될 수 있도록 상기 2차원 또는 3차원 테이블을 격자 테이블로 구성한다.

[0075] 이상에서 설명한 구성요소들에 의하여 형성된 지문 템플릿은 거짓 특징점들이 "임의적"으로 삽입되는 것이 아니라, 해당 위치 즉, 빈 격자 공간에 "규칙적"으로 삽입되기 때문에, 동일한 지문에 의하여 형성된 두 개의 지문 템플릿을 매칭하더라도, 진짜 특징점들을 쉽게 분리할 수 없어 상관공격에 강인하게 된다. 즉, 진짜 특징점뿐만 아니라, "규칙적" 삽입에 의하여 거짓 특징점들도 다수 일치하게 되기 때문에, 진짜 특징점들을 구별하는 것은 매우 어렵다.

[0076] 도 4는 본 발명에서 제안하는 3차원 격자 테이블을 이용하여 거짓 특징점이 삽입된 지문 템플릿의 예를 보여준다. 도 4의 (a)와 도 4의 (b)는 동일한 지문에서 생성된 두개의 지문 템플릿이며, 도 4의 (c)는 두 지문 템플릿을 매칭한 결과를 보여준다. 결과적으로, 도 4의 (c)에서 보여준 바와 같이, 두 개의 지문 템플릿은 매칭을 하여도 다량의 특징점이 추출되기 때문에 진짜와 거짓 특징점을 구별하기 어려워 상관공격을 피할 수 있다.

[0077] 이와 같은 결과는, 종래와 달리, 거짓 특징점들을 임의적으로(랜덤하게) 생성하여 삽입하는 것이 아니라, 빈 격자 공간에 규칙적(비임의적)으로 삽입하기 때문에, 발생되는 결과이다.

[0078] 본 발명의 성능을 실험하기 위해 FVC2002(<http://bias.csr.unibo.it/fvc2002/databases.asp>.)의 DB1 Set A를 사용하였다. 지문 이미지의 크기는 388 x 374이다. 또한, 진짜와 거짓 특징점은 3차원 좌표를 이용하여 총 4,000개를 생성하였고, 지문 정렬을 위하여 3차원 기하학적 해싱 기법[이성주, *et al.*, "3차원 기하학적 해싱을 이용한 퍼지블릿에서의 지문 정합," 정보보호학회 논문지, 2008.]과, 수행시간과 메모리사용량을 줄이기 위하여 부분 기하학적 해싱 기법[S. Lee, *et al.*, "Memory-Efficient Fuzzy Fingerprint Vault based on the Geometric Hashing", *IEEE ISA*, 2008.]을 수정 적용하였다. 모든 실험은 2.66GHz CPU에 2GB RAM이 탑재된 PC에서 수행하였다.

[0079] 먼저 본 발명에서 제안한 방법이 상관공격에 강인한지를 확인하기 위해 4,000개의 진짜와 거짓 특징점으로 구성된 두 개의 지문 템플릿을 매칭하여 상관공격을 수행하였다. 수행 결과, 본 발명에서 제안한 방법 하에서 상관공격으로 획득된 특징점에는 진짜가 평균 5개, 거짓이 평균 300개 정도로, 상관공격에 강인함을 확인하였다. 상관공격에 취약한 기존 방법과 상관공격에 강인한 본 발명에서 제안한 방법을 비교하면 다음 표 1과 같다.

	상관 공격
기존 방법(2D with 200 chaffs)	50초 ~ 8분내 성공
제안 방법(3D with 4,000 chaffs)	없음

[0081] - 표 1 -

[0082] 또한, 하나의 지문 템플릿으로 수행하는 전수조사 공격[K. Nandakumar, *et al.*, "Fingerprint-based Fuzzy Vault: Implementation and Performance," *IEEE Tr. IFS*, 2007.]에 따른 안전성을 측정하였다. 아래 표 2에서와 같이, 특징점이 4,000개인 경우 전수조사를 이용하여 다항식을 푸는데 1.06×10^{15} 초가 소요되어, 일반적으로 수백개의 거짓 특징점을 삽입하는 기존 방법에 비하여 매우 높은 보안성을 제공할 수 있다. 마지막으로, 본 발명에서 제안한 방법의 수행시간을 측정한 결과, 4,000개의 특징점으로 구성된 지문 템플릿을 이용하여 본인 정

합을 수행하는데 2.64초가 소요되어 실시간 처리가 가능함을 확인하였다.

[0083]

진짜와 거짓 특징점 개수	전수조사 공격
250(기존 방법)	1.35×10^4 초
4,000(제안 방법)	1.06×10^{15} 초

[0084]

- 표 2 -

도면의 간단한 설명

[0085]

도 1은 종래의 지문 퍼지볼트에 대한 상관공격의 예를 설명하기 위한 지문 템플릿이다.

[0086]

도 2는 본 발명의 실시예에 따른 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 장치의 구성도이다.

[0087]

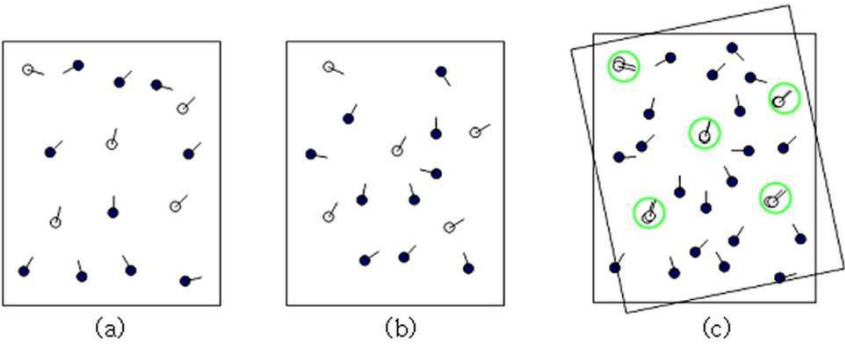
도 3은 본 발명의 실시예에 따른 상관공격에 강인한 퍼지볼트를 이용한 지문 템플릿 형성 방법의 절차도이다.

[0088]

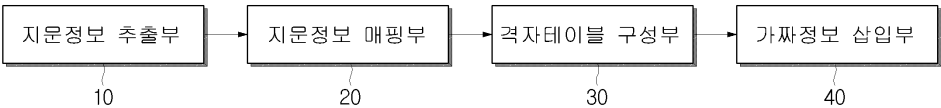
도 4는 본 발명에 따라 형성되는 3차원 격자 테이블을 이용한 지문 템플릿이다.

도면

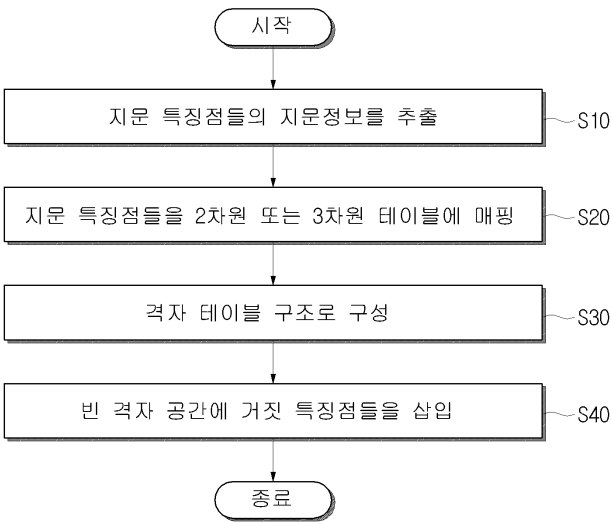
도면1



도면2



도면3



도면4

