



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0116695
(43) 공개일자 2023년08월04일

(51) 국제특허분류(Int. Cl.)
G06V 40/18 (2022.01) G06V 40/50 (2022.01)
(52) CPC특허분류
G06K 19/06 (2013.01)
(21) 출원번호 10-2023-0007413
(22) 출원일자 2023년01월18일
심사청구일자 2023년01월18일
(30) 우선권주장
1020220012178 2022년01월27일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
정익래
서울특별시 광진구 아차산로 69길 19, 904동 220
5호
이연주
충청남도 천안시 서북구 백석로 136, 113동 1102
호 (백석동, 백석현대아파트)
(뒷면에 계속)
(74) 대리인
김등용

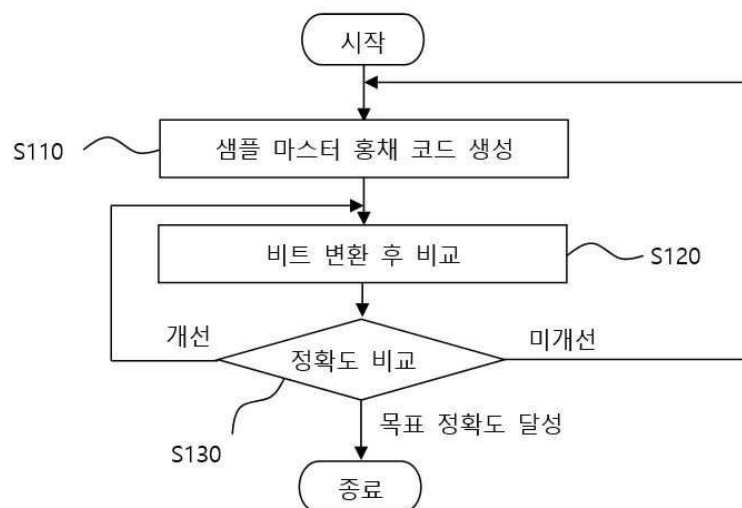
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 취소 가능한 홍채 템플릿을 이용한 마스터 홍채 코드 생성 장치 및 방법

(57) 요약

취소 가능한 홍채 템플릿을 이용한 마스터 홍채 코드 생성 장치 및 방법이 개시된다. 상기 마스터 홍채 코드 생성 방법은 적어도 프로세서(processor)를 포함하는 컴퓨팅 장치에 의해 수행되고, 샘플 마스터 홍채 코드를 생성하는 단계, 상기 샘플 마스터 홍채 코드의 적어도 하나의 비트의 값을 변환하여 변환된 샘플 마스터 홍채 코드들을 생성하는 단계, 상기 변환된 샘플 마스터 홍채 코드들 각각의 정확도를 산출하는 단계, 및 산출된 정확도 중 가장 높은 정확도가 목표 정확도 보다 크거나 같은 경우, 가장 높은 정확도를 갖는 변환된 샘플 마스터 홍채 코드를 마스터 홍채 코드로 결정하는 단계를 포함한다.

대표도 - 도3



(72) 발명자

정재열

서울특별시 성북구 안암로9가길 55, 304호

최재현

서울특별시 성북구 안암로9가길 55, 305호

이 발명을 지원한 국가연구개발사업

과제고유번호 1711104076

과제번호 2019R1F1A1060637

부처명 과학기술정보통신부

과제관리(전문)기관명 한국연구재단

연구사업명 개인기초연구(과기정통부)(R&D)

연구과제명 생체 정보에 대한 프라이버시 보장 연산 연구

기 여 율 1/1

과제수행기관명 고려대학교 산학협력단

연구기간 2020.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

적어도 프로세서(processor)를 포함하는 컴퓨팅 장치에 의해 수행되는 마스터 홍채 코드 생성 방법에 있어서,
샘플 마스터 홍채 코드를 생성하는 단계;

상기 샘플 마스터 홍채 코드의 적어도 하나의 비트의 값을 변환하여 변환된 샘플 마스터 홍채 코드들을 생성하는 단계;

상기 변환된 샘플 마스터 홍채 코드들 각각의 정확도를 산출하는 단계; 및

산출된 정확도 중 가장 높은 정확도가 목표 정확도 보다 크거나 같은 경우, 가장 높은 정확도를 갖는 변환된 샘플 마스터 홍채 코드를 마스터 홍채 코드로 결정하는 단계를 포함하는 마스터 홍채 코드 생성 방법.

청구항 2

제1항에 있어서,

상기 샘플 마스터 홍채 코드를 생성하는 단계는,

복수의 홍채 이미지들 각각에 대응하는 홍채 코드를 생성하는 단계;

홍채 코드들 각각에 대응하는 취소 가능한 홍채 템플릿을 생성하는 단계; 및

가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응하는 홍채 코드를 상기 샘플 마스터 홍채 코드로 선택하는 단계를 포함하는,

마스터 홍채 코드 생성 방법.

청구항 3

제1항에 있어서,

상기 샘플 마스터 홍채 코드를 생성하는 단계는,

임의의 값들을 갖는 홍채 코드들을 생성하는 단계;

상기 홍채 코드들 각각에 대응하는 취소 가능한 홍채 템플릿을 생성하는 단계; 및

가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응하는 홍채 코드를 상기 샘플 마스터 홍채 코드로 선택하는 단계를 포함하는,

마스터 홍채 코드 생성 방법.

청구항 4

제1항에 있어서,

산출된 정확도 중 가장 높은 정확도가 목표 정확도 보다 작지만 상기 샘플 마스터 홍채 코드의 정확도 보다 큰 경우, 상기 변환된 샘플 마스터 홍채 코드들을 생성하는 단계가 재차 수행되는,

마스터 홍채 코드 생성 방법.

청구항 5

제1항에 있어서,

산출된 정확도 중 가장 높은 정확도가 상기 샘플 마스터 홍채 코드의 정확도 보다 크지 않는 경우, 상기 샘플 마스터 홍채 코드를 생성하는 단계가 재차 수행되는,

마스터 홍채 코드 생성 방법.

발명의 설명

기술 분야

- [0001] 본 발명은 홍채인식 환경에서 마스터 홍채 코드 생성 방법에 관한 것으로, 특히 취소 가능한 홍채 템플릿을 이용하여 홍채 코드의 일정 수준의 정확도를 가지는 마스터 홍채 코드를 생성할 수 있는 장치 및 방법에 관한 것이다.

배경 기술

- [0002] 전자 기기와 인터넷의 발전으로 다양한 분야에서 사용자 인증을 통한 거래 및 출입인증 시스템이 증가함에 따라 인증에 대한 많은 관심이 증가하고 있다. 그러나 기존에 많이 사용되고 있는 패스워드, PIN 등의 지식기반 인증은 비밀키를 유추할 수 있다는 취약점이 존재한다.
- [0003] 이러한 문제를 개선한 생체기반 인증은 보편적인 이용자가 모두 가지고 있으며 그 특징이 타인과 사용자를 구별할 만큼 독자적이고 영구적으로 보존되어 기계적 인식 및 수집을 할 수 있어 다양한 응용 프로그램에서 이를 활용한 인증 시스템을 사용하고 있다
- [0004] 생체 정보는 개인의 신체 특징을 활용한다는 점에서 강력한 보안성을 지녔지만, 지문, 홍채 등과 같이 인간의 부분적 특징은 한정되어 있어 생체 정보를 저장한 서버의 해킹 및 유출시 이를 대체할 인증수단이 존재하지 않는다. 이러한 생체 정보의 불변성은 다양한 응용 프로그램에서 치명적인 위협으로 작용할 수 있다.
- [0005] 생체 정보의 보호 방법으로는 암호화와 특징 변환 방법이 존재한다. 이 중 특징 변환 방법은 대표적으로 Rathgeb 기타 등의 연구에서 제안한 비가역 변환을 활용한 취소 가능한 템플릿(cancelable template) 생성 방법이 존재한다. 취소 가능한 템플릿의 사용은 서버에 저장된 템플릿이 유출되더라도 유출된 정보를 통해서 원본 템플릿을 알 수 없다. 또한, 서버에서 새롭게 생성한 취소 가능 템플릿 사용 시 인증을 정상적으로 진행할 수 있다는 장점이 존재한다.
- [0006] 또한, 지문, 얼굴, 홍채 등을 이용한 생체인증은 현재 모바일 기기 인증, 금융거래, 출입관리, 출입국 심사 등 다양한 응용 프로그램에서 사용되고 있다. 다양한 환경에서 사용되는 응용 프로그램에 따라서 렌즈의 크기가 다양화되어 있고, 특히 지문인증에서는 지문의 전체 정보를 이용하는 것이 아닌 부분 정보만을 이용하여 인증하는 부분 지문인증이 연구되고 있다. 부분 지문인증을 사용하면 센서의 크기가 작아도 인증이 잘 된다는 장점이 있지만 오인식율인 FAR(False Accept Rate)이 증가한다는 단점이 존재한다.
- [0007] 2017년, Aditi Roy 기타 등의 연구에서는 부분 지문을 사용하는 환경에서의 공격 방법인 ‘마스터 지문’ 개념과 이를 생성하는 방법을 제안하였다. 마스터 지문은 모든 인증 자물쇠를 열 수 있는 마스터키와 유사한 개념으로 서버에 저장된 템플릿과 인증을 시도했을 때 일정 확률 이상으로 성공하는 지문 템플릿이다. 마스터 지문은 다양한 사용자의 손가락 지문 및 저장된 템플릿의 부분 지문과 일치할 확률이 상당히 높다. 이는 합성과 실제 부분 지문 중 하나로 전수조사를 통한 지문 공격으로 만약 성공 확률이 20%라면 하나의 지문 템플릿으로 전체 데이터베이스에서 저장된 템플릿 중 20% 템플릿에서 인증에 성공할 수 있다.
- [0008] 본 발명에서는 취소 가능한 홍채 템플릿을 사용하는 프로그램에서의 마스터 홍채 코드 생성 기법을 제안한다.

선행기술문헌

비특허문헌

- [0009] (비특허문헌 0001) Roy, A., Memon, N., & Ross, A. (2017). Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Transactions on Information Forensics and Security, 12(9), 2013-2025.

발명의 내용

해결하려는 과제

- [0010] 현재까지 마스터 생체인증에 관한 연구는 활발히 진행되었으나, 홍채 인증에서의 마스터 홍채 템플릿 생성 기법은 제안되지 않았다. 지문, 얼굴, 홍채 등을 이용한 생체인증은 현재 모바일 기기 인증, 금융거래, 출입관리, 출입국 심사 등 다양한 응용 프로그램에서 사용되고 있다. 이러한 점을 고려하여 홍채 인증에서 마스터 홍채 템플릿에 대한 공격 대비가 필요하다.

과제의 해결 수단

- [0011] 본 발명의 일 실시예에 따른 마스터 홍채 코드 생성 방법은 적어도 프로세서(processor)를 포함하는 컴퓨팅 장치에 의해 수행되고, 샘플 마스터 홍채 코드를 생성하는 단계, 상기 샘플 마스터 홍채 코드의 적어도 하나의 비트의 값을 변환하여 변환된 샘플 마스터 홍채 코드들을 생성하는 단계, 상기 변환된 샘플 마스터 홍채 코드들 각각의 정확도를 산출하는 단계, 및 산출된 정확도 중 가장 높은 정확도가 목표 정확도 보다 크거나 같은 경우, 가장 높은 정확도를 갖는 변환된 샘플 마스터 홍채 코드를 마스터 홍채 코드로 결정하는 단계를 포함한다.

발명의 효과

- [0012] 본 발명은 홍채 인증에 대한 마스터 홍채 코드 생성 기법에 관하여 기술한다. 마스터 홍채 코드는 임의의 샘플 템플릿을 생성하는 SAMI(Sampled Master Iris), 비교, 저장, 반복의 총 4가지 단계를 통하여 사용자가 지정한 일정 수준의 정확도를 가지는 마스터 홍채 코드를 생성할 수 있다.
- [0013] 제안한 발명은 최초의 마스터 홍채 생성 기법으로 향후 개발이 완료되면 상당한 정확도를 가지는 마스터 홍채 코드를 생성할 수 있을 것으로 예상된다. 또한, 취소 가능한 홍채 템플릿은 홍채인식을 이용하는 시스템에서 공격자의 공격으로부터 대비할 수 있을 것으로 예상된다.

도면의 간단한 설명

- [0014] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 마스터 홍채 코드의 생성 원리를 설명하기 위한 도면이다.
- 도 2는 취소 가능한 홍채 템플릿 생성 방법을 설명하기 위한 도면이다.
- 도 3은 본 발명의 일 실시예에 따른 마스터 홍채 코드 생성 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 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 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.
- [0016] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0017] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0018] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등 도 마찬가지로 해석되어야 한다.

- [0019] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0020] 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.
- [0021] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0022] 우선, 마스터 지문 생성에 관하여 설명한다.
- [0023] 소형 센서를 활용하여 지문을 인식할 경우, 센서에 인식된 부분 지문만을 사용한 인증은 등록된 지문 템플릿과의 일치성 검증을 통해 이뤄진다. 지문 템플릿은 지문의 다양한 각도로 지문 패턴들을 저장한 부분 지문들로 공격자 등록된 지문과 일치한 지문을 제출할 경우 정당한 사용자로 오(誤)인증될 수 있다. 2017년 Aditi Roy는 이러한 지문 템플릿을 활용한 사용자 오인증 공격 생성 방법인 마스터 지문을 제안하였다.
- [0024] Aditi Roy 기타 등의 연구에서는 마스터 지문을 생성하는 두 가지 방안을 제안하였다. 기존의 데이터 세트에서 마스터 지문을 선택하는 방법인 SAMP(Sampled Master Prints)와 인위적으로 생성하는 SYMP로 지문의 다양한 패턴들을 저장하고 있다.
- [0025] Philip Bontrager 기타 등의 연구(P. Bontrager, A. Roy, J. Togelius, N. Memon, and A. Ross, "DeepMasterPrints: Generating masterprints for dictionary attacks via latent variable evolution," IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1-9, 2018.)에서는 특징 레벨(feature level)에서 생성한 것을 이미지 레벨(image level)에서 마스터 지문을 생성함으로써 기존의 단일 마스터 지문보다 일치 확률이 향상되었다.
- [0026] 취소 가능한 홍채 템플릿은, 비가역 변환은 역 변환할 수 없는 함수 또는 알고리즘을 이용해서 초기 생체 템플릿으로부터 템플릿을 변경하여 생체 정보를 보호하는 개념이다. 변경된 템플릿은 초기 홍채 템플릿으로 복원할 수 없으므로 안전하다.
- [0027] Dwivedi 기타 등의 연구(R. Dwivedi, S. Dey, R. Singh and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping," Computers & Security, vol. 65, pp. 373-386, 2017)에서는 룩업 테이블(look-up table)로부터 취소 가능한 홍채 템플릿 생성을 제안하였다. 취소 가능한 홍채 템플릿 생성 방법으로는 초기 홍채 이미지로부터 추출한 홍채 코드를 다음 행으로 나누어 하나의 벡터로 합친다. 이후 합친 코드를 원하는 크기로 나누어 그 값을 10진수로 변환하고 변환된 값은 룩업 테이블을 이용하여 최종 취소 가능한 홍채 템플릿으로 생성한다. 이러한 취소 가능한 홍채 템플릿은 홍채 이미지와 룩업 테이블에 따라 다른 이미지이지만 같은 취소 가능한 홍채 템플릿이 생성될 수 있다.
- [0028] 이하에서는, 부분 홍채를 사용하는 환경에서의 공격 방법인 마스터 홍채 코드를 생성하는 기법에 대해 상세히 설명한다.
- [0029] 기존의 홍채 인증은 다른 홍채 이미지에서 동일한 홍채 코드가 나오기 어려워 마스터 홍채 코드를 생성하기에 거의 불가능하였다. 하지만 취소 가능한 홍채 템플릿을 이용하는 응용 프로그램에서는, 마스터 홍채 코드의 생성 원리를 도식한 도 1과 같이, 다른 지문에서 같은 템플릿이 생성될 수 있다는 것과 유사하게 다른 홍채에서 같은 템플릿이 생성될 수 있으므로 마스터 홍채 코드 생성이 가능하다. 이에 마스터 홍채 코드를 추출하는 방법을 제안한다.
- [0030] 마스터 홍채 코드 생성 방법
- [0031] 취소 가능한 홍채 코드는 기존에 제안된 Dwivedi 기타 등의 연구에서 사용한 룩업 테이블(look-up table)을 사

용한다. 다른 취소 가능한 홍채 템플릿 생성 방법도 제안한 방법과 유사하다. 본 발명에서는, 취소 가능한 홍채 템플릿을 생성하는 다양한 기법들 중 어느 하나를 이용할 수 있다.

- [0032] 공격자는 서버에 저장된 템플릿의 정보를 모르기 때문에 빈도 분석 공격을 수행할 수 없다. 따라서 인위적으로 생성하는 기법을 이용하여 마스터 홍채 코드를 생성할 수 있다.
- [0033] 마스터 홍채 코드를 생성하는 방법으로는 (1) 샘플 마스터 홍채 코드 생성, (2) 비교, (3) 저장, (4) 반복 과정이 존재한다. 다음은 마스터 홍채 코드를 생성하는 구체적인 방법이다.
- [0034] (1) 샘플 마스터 홍채 코드가 생성된다. 샘플 마스터 홍채 코드는 미리 저장되어 있는 홍채 이미지를 이용하여 생성되거나 임의로 생성될 수 있다. 미리 저장되어 있는 홍채 이미지를 이용하여 샘플 마스터 홍채 코드를 생성하는 경우, 복수의 홍채 이미지를 각각에 대한 홍채 코드가 생성되고, 각 홍채 코드는 취소 가능한 홍채 템플릿으로 변환된다. 이때, 미리 저장되어 있는 (취소 가능한 홍채) 템플릿들과의 비교를 통해서 가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응되는 홍채 코드가 샘플 마스터 홍채 코드로 선택될 수 있다. 여기서, 미리 저장되어 있는 템플릿들은 홍채의 적어도 일부분에 대응하는 홍채 코드의 취소 가능한 홍채 템플릿일 수 있다.
- [0035] 임의로 샘플 마스터 홍채 코드를 생성하는 경우, 임의의 값을 갖는 홍채 코드들이 생성되고, 각 홍채 코드는 취소 가능한 홍채 템플릿으로 변환된다. 이때, 미리 저장되어 있는 (취소 가능한 홍채) 템플릿들과의 비교를 통해서 가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응되는 홍채 코드가 샘플 마스터 홍채 코드로 선택될 수 있다. 마찬가지로, 미리 저장되어 있는 템플릿들은 홍채의 적어도 일부분에 대응하는 홍채 코드의 취소 가능한 홍채 템플릿일 수 있다.
- [0036] (2) 생성된 샘플 마스터 홍채 코드를 도 2의 취소 가능한 홍채 템플릿으로 변환하여 서버에 저장된 템플릿과 비교한다.
- [0037] (3) 생성한 샘플 마스터 홍채 코드에서 한 비트씩 변환 (0→1, 1→0) 하여 가장 좋은 결과((2) 과정을 통하여 획득한 결과)가 나오는 비트를 구하고 샘플 마스터 홍채 코드에서 그 비트만 변환하여 저장한다.
- [0038] (4) 원하는 정확도가 나올 때까지 a-c 단계를 반복 수행한다.
- [0039] 다음은 (4) 사용자가 원하는 정확도가 나올 때까지 반복 수행하는 과정이다.
- [0040] (4)-a. (3)에서 생성한 한 비트씩 변환하여 획득한 좋은 결과에 대한 변환된 샘플 마스터 홍채 코드를 기준으로 한 비트씩 다시 변환하여 가장 좋은 결과가 나오는 비트를 구한다.
- [0041] 만약 좋은 결과를 구하면 (4)-b 과정을 수행하고 그렇지 않으면 (4)-c 과정을 수행한다.
- [0042] (4)-b. (4)-a에서 도출한 결과값이 사용자가 원하는 정확도 이상일 경우 반복 수행 과정을 멈추고 결과값 비트를 수정한 변환된 샘플 마스터 홍채 코드를 최종 마스터 홍채로 선정한다.
- [0043] 만약 (4)-a에서 도출한 결과값이 원하는 정확도 보다 낮으면 변환된 샘플 마스터 홍채 코드에서 가장 좋은 결과를 나타내는 비트를 수정하고 그 값을 다시 (4)-a 과정으로 보낸다.
- [0044] (4)-c. 현재 기준인 SAMI로는 원하는 정확도를 만족하는 마스터 홍채를 생성할 수 없으므로 (1)과정으로 돌아가서 새로운 임의의 샘플 템플릿인 샘플 마스터 홍채 코드를 선택하여 과정을 다시 수행한다.
- [0045] 공격 시나리오
- [0046] 공격자는 본 발명에서 제안한 취소 가능한 홍채 템플릿을 이용한 마스터 홍채 코드 생성 방법을 사용하여 높은 인증률을 가지는 마스터 홍채 코드를 얻을 수 있다. 이는 임의의 샘플 마스터 홍채 코드로부터 생성되며, 생성된 코드는 악의적인 사용자로부터 홍채 인증 프로그램에 사용될 수 있다.
- [0047] 본 발명에서 제안한 공격 방법은 공격자가 설정한 정확도에 따라 수행시간이 결정된다. 이는 마스터 홍채 코드가 없거나 모든 가능한 홍채 코드로 인증을 요청한 것과 유사한 결과를 얻을 수 있다.
- [0048] 취소 가능한 템플릿의 룩업 테이블(look-up table)을 이용한 공격 이외에도 다양한 홍채 공격들이 존재한다. 그 중 마스터 홍채 코드는 현재까지 사용되고 있지 않다. 향후 마스터 홍채 코드 공격이 완성될 경우 이를 보호할 수단이 필요해 보인다.
- [0049] 이상에서 설명된 방법들과 이하에서 설명될 방법들은 적어도 프로세서(processor) 및/또는 메모리(memory)를 포

합하는 컴퓨팅 장치(computing device)에 의해 수행될 수 있다. 즉, 방법들 각각을 이루는 단계들 중 적어도 일부는 컴퓨팅 장치의 프로세서의 동작으로 이해될 수도 있다. 컴퓨팅 장치는 PC(Personal Computer), 서버(server), 랩탑 컴퓨터, 노트북 등을 포함할 수 있으며, 마스터 홍채 코드 생성 장치 등으로 명명될 수도 있다.

[0050] 도 3은 본 발명의 일 실시예에 따른 마스터 홍채 코드 생성 방법을 설명하기 위한 흐름도이다.

[0051] 도 1 내지 도 3을 참조하면, 샘플 마스터 홍채 코드가 생성된다(S110). 샘플 마스터 홍채 코드는 컴퓨팅 장치에 미리 저장되어 있는 홍채 이미지들을 이용하여 생성되거나, 임의의 비트 데이터를 생성하는 기법을 이용하여 생성될 수 있다.

[0052] 홍채 이미지들을 이용하여 샘플 마스터 홍채 코드가 생성되는 경우, 홍채 이미지들 각각에 대한 홍채 코드가 생성되고, 홍채 코드들 각각은 취소 가능한 홍채 템플릿으로 변환될 수 있다. 가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응하는 홍채 코드가 샘플 마스터 홍채 코드로 선택될 수 있다. 정확도는 컴퓨팅 장치에 미리 저장되어 있는 (취소 가능한 홍채) 템플릿들과의 비교를 통해 산출될 수 있다. 비교는 일치 여부(또는 포함 여부)를 판단하는 것을 의미할 수 있다. 예컨대, 정확도는 컴퓨팅 장치에 포함되어 있는 템플릿들 중 생성된 홍채 코드에 대응하는 취소 가능한 홍채 템플릿에 포함되는 비율을 의미할 수 있다.

[0053] 임의의 비트 데이터를 생성하는 기법을 이용하여 샘플 마스터 홍채 코드가 생성되는 경우, 임의의 비트값들을 갖는 복수의 홍채 코드들이 생성될 수 있다. 홍채 코드들 각각은 취소 가능한 홍채 템플릿으로 변환될 수 있다. 가장 높은 정확도를 보이는 취소 가능한 홍채 템플릿에 대응하는 홍채 코드가 샘플 마스터 홍채 코드로 선택될 수 있다.

[0054] 실시예에 따라, 임의의 홍채에 대한 홍채 코드를 생성하고, 생성된 홍채 코드를 샘플 마스터 홍채 코드로 선택할 수도 있다. 다른 예로, 임의로 생성한 홍채 코드를 샘플 마스터 홍채 코드로 선택할 수도 있다.

[0055] 샘플 마스터 홍채 코드에 대한 비트 변환 후 비교 동작이 수행될 수 있다(S120). 비트 변환은 샘플 마스터 홍채 코드에서 적어도 하나의 비트의 값을 변환하는 것을 의미한다. 일 예로, 하나의 비트의 값을 변환하거나 복수의 비트들의 값을 변환할 수 있다. 비트 변환을 통해, 비트값 0은 1로 변환되고, 비트값 1은 0으로 변환된다. 변환된 샘플 마스터 홍채 코드들 각각에 대한 취소 가능한 홍채 템플릿이 생성되고, 취소 가능한 홍채 템플릿들 각각에 대한 정확도가 산출될 수 있다.

[0056] S130 단계에서는, 산출된 정확도들 중 가장 높은 정확도가 비교된다. 가장 높은 정확도는 목표 정확도를 달성하거나(즉, 가장 높은 정확도가 목표 정확도 보다 크거나 같은 경우), 비트 변환 전 샘플 마스터 홍채 코드의 정확도 보다 크거나(목표 정확도 보다는 작은 경우를 의미할 수 있음), 비트 변환 전 샘플 마스터 홍채 코드의 정확도 보다 크지 않을 수 있다.

[0057] 가장 높은 정확도가 목표 정확도를 달성한 경우, 샘플 마스터 홍채 코드의 목표 정확도가 달성되었으므로, 샘플 마스터 홍채 코드를 최종 마스터 홍채 코드로 결정하고, 프로토콜의 진행이 중단될 수 있다.

[0058] 가장 높은 정확도가 비트 변환 전 샘플 마스터 홍채 코드의 정확도 보다 큰 경우, 아직 목표 정확도 보다는 작기 때문에, S120 단계가 다시 수행될 수 있다. 이를 통해, 정확도가 더욱 개선된 샘플 마스터 홍채 코드가 생성될 수 있다.

[0059] 가장 높은 정확도가 비트 변환 전 샘플 마스터 홍채 코드의 정확도 보다 크기 않은 경우(즉, 정확도의 개선이 없는 경우), S110 단계가 다시 수행된다. 기존에 생성된 샘플 마스터 홍채 코드로는 목표 정확도를 달성할 수 없기 때문에, S110 단계의 재 수행을 통해, 새로운 샘플 마스터 홍채 코드를 생성할 수 있다. 이때, 미리 저장되어 있는 홍채 이미지를 이용하는 경우에는, 두 번째로 높은 정확도를 갖는 홍채 이미지에 대응하는 홍채 코드가 샘플 마스터 홍채 코드로 선택될 수 있다. 가장 높은 정확도를 갖는 홍채 이미지에 대응하는 홍채 코드로는 목표 정확도를 달성할 수 없기 때문이다.

[0060] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, 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(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응

답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 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 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

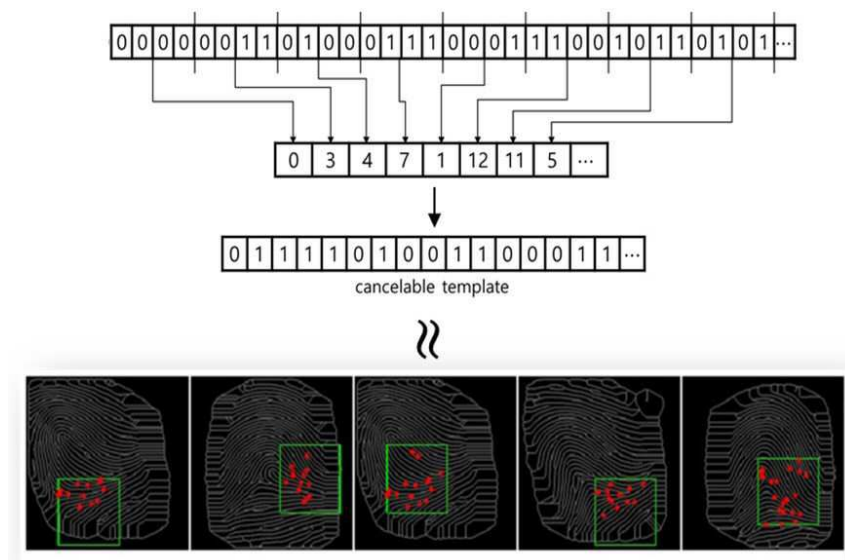
[0061] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 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.

[0062] 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), 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.

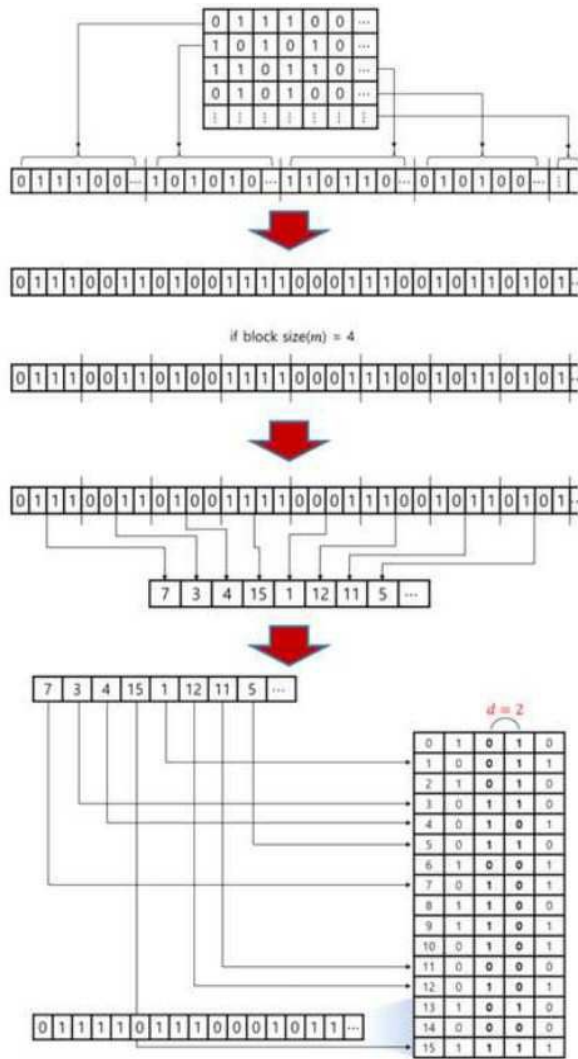
[0063] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

도면1



도면2



도면3

