



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0127437
(43) 공개일자 2020년11월11일

(51) 국제특허분류(Int. Cl.)

G06F 21/32 (2013.01) G06F 1/16 (2006.01)
G06F 21/31 (2013.01) G06F 21/45 (2013.01)
G06F 21/60 (2013.01) G06F 3/01 (2006.01)

(52) CPC특허분류

G06F 21/32 (2013.01)
G06F 1/163 (2013.01)

(21) 출원번호 10-2019-0051527

(22) 출원일자 2019년05월02일
심사청구일자 2019년05월02일

(71) 출원인

연세대학교 산학협력단

서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)

(72) 발명자

권태경

서울특별시 강남구 선릉로 221, 410동 1602호(도곡동, 도곡렉슬아파트)

구예은

서울특별시 서대문구 연희로8길 28-47, 205호(연희동)

박래현

서울특별시 도봉구 도당로31길 20, 302호 (방학동, 세광빌라)

(74) 대리인

특허법인우인

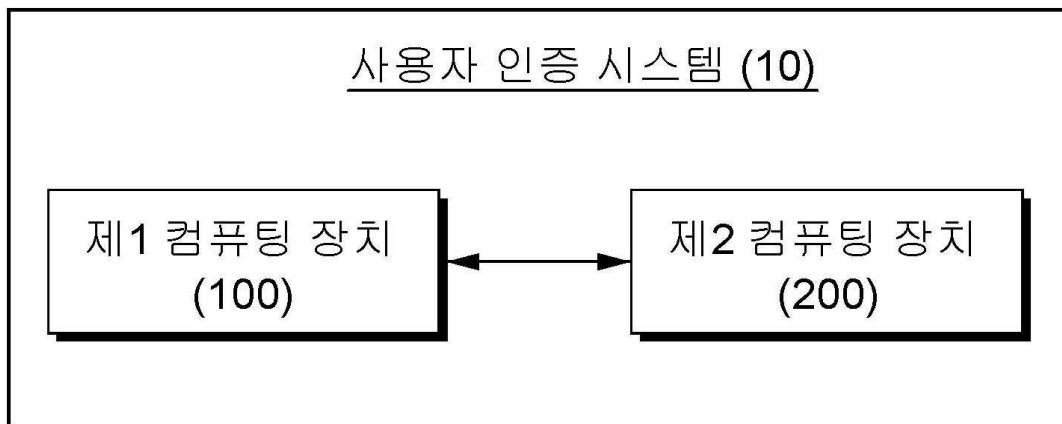
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 복수의 컴퓨팅 장치에 내장된 센서를 활용한 사용자 인증 시스템

(57) 요약

본 실시예들은 연동된 제1 컴퓨팅 장치와 제2 컴퓨팅 장치에 내장되어 있는 센서들에서 추출된 센서 데이터의 유사성 분석을 통해 인증 시도자와 등록 사용자 간의 동일인 일치 여부를 확인하고, 센서 데이터에서 추출한 행위 특징을 통해 기계학습 기반의 사용자 행위 기반 인증을 제공하는 사용자 인증 시스템을 제공한다.

대표도 - 도1



(52) CPC특허분류

G06F 21/316 (2013.01)

G06F 21/45 (2013.01)

G06F 21/602 (2013.01)

G06F 3/017 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711082833
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원(한국연구재단부설)
연구사업명	정보통신방송연구개발사업
연구과제명	[이지바로] 차세대 인증 기술 개발 (3/3)
기 여 율	1/1
과제수행기관명	연세대학교 산학협력단
연구기간	2019.01.01 ~ 2019.12.31

명세서

청구범위

청구항 1

제1 프로세서, 상기 제1 프로세서에 의해 실행되는 프로그램을 저장하는 제1 메모리, 하나 이상의 제1 센서, 및 제2 컴퓨팅 장치와 통신하는 제1 통신 인터페이스를 포함하는 제1 컴퓨팅 장치에 있어서,

상기 제1 통신 인터페이스는 상기 제2 컴퓨팅 장치에 내장된 하나 이상의 제2 센서를 통해 수집한 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수신하고,

상기 하나 이상의 제1 센서는 제1 생체 데이터 및 제1 모션 데이터를 포함하는 제1 센서 데이터를 수집하고,

상기 제1 프로세서는,

상기 제1 생체 데이터와 상기 제2 생체 데이터 간의 유사도를 산출하고, 상기 유사도에 따라 상기 제1 컴퓨팅 장치의 사용자 및 상기 제2 컴퓨팅 장치의 사용자 간의 동일인 여부를 판단하고,

상기 제1 센서 데이터 및 상기 제2 센서 데이터를 통한 사용자의 행위 분석을 기반으로 상기 제2 컴퓨팅 장치의 사용자 인증 결과를 생성하는 과정을 수행하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 2

제1항에 있어서,

상기 제1 프로세서는,

상기 제1 생체 데이터, 상기 제2 생체 데이터, 상기 제1 모션 데이터, 및 상기 제2 모션 데이터의 노이즈를 제거하는 전처리 과정을 더 수행하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 3

제1항에 있어서,

상기 제1 프로세서가 상기 동일인 여부를 판단하는 과정은 측정 시간에 따라 상이한 파형을 갖는 상기 제1 생체 데이터와 상기 제2 생체 데이터의 측정 구간을 동기화하고 상기 제1 생체 데이터의 파형과 상기 제2 생체 데이터의 파형을 비교하여 상기 유사도를 산출하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 4

제1항에 있어서,

상기 제1 프로세서는,

상기 유사도가 임계값을 넘을 경우, 상기 제1 컴퓨팅 장치의 사용자 및 상기 제2 컴퓨팅 장치의 사용자를 동일인으로 판단하며,

상기 유사도가 임계값을 넘지 못할 경우, 상기 제2 컴퓨팅 장치로 인증 실패 신호를 전송하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 5

제1항에 있어서,

상기 제1 프로세서가 상기 사용자의 행위 분석을 기반으로 상기 제2 컴퓨팅 장치의 사용자 인증 결과를 생성하는 과정은,

상기 제1 센서 데이터 및 상기 제2 센서 데이터를 기반으로 행위의 특징을 추출하고,

상기 제2 컴퓨팅 장치의 등록 사용자의 원본 센서 데이터를 등록하여 인증 모델을 학습하고,

상기 학습된 인증 모델을 기반으로 상기 제2 컴퓨팅 장치의 사용자가 상기 제2 컴퓨팅 장치의 상기 등록 사용자인지 확인하는 과정을 포함하는 제1 컴퓨팅 장치.

청구항 6

제5항에 있어서,

상기 제1 프로세서가 상기 행위의 특징을 추출하는 과정은 상기 제1 센서 데이터 및 상기 제2 센서 데이터에 대해서 시간 영역과 주파수 영역을 고려하며 특징 데이터를 추출하고,

상기 특징 데이터는 3개의 축에 대응하는 데이터 및 3개의 축에 따른 데이터의 크기를 포함하며,

상기 주파수 영역의 센서 데이터는 상기 시간 영역의 센서 데이터를 푸리에 변환하여 획득하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 7

제5항에 있어서,

상기 제1 프로세서가 상기 인증 모델을 학습하는 과정은,

복수의 인증 모델을 병렬로 연결하여, 상기 제2 컴퓨팅 장치의 등록 사용자의 행위에 대한 원본 센서 데이터로부터 랜덤하게 추출한 서브 특징 데이터의 조합에 대한 학습 데이터의 집합을 생성하고, 상기 학습 데이터를 단일 클래스 학습 알고리즘에 적용하여 상기 복수의 인증 모델을 학습하고,

상기 복수의 인증 모델을 학습하는데 사용된 상기 학습 데이터를 상기 제1 컴퓨팅 장치에서 삭제하고,

상기 추출한 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘을 암호화하는 과정을 포함하는 제1 컴퓨팅 장치.

청구항 8

제7항에 있어서,

상기 메모리는 (i) 상기 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘과 (ii) 상기 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘을 복호화하는 코드를 저장하고,

상기 제1 프로세서는 상기 제2 컴퓨팅 장치의 사용자가 인증을 시도할 때 복호화 과정을 수행하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 9

제7항에 있어서,

상기 제1 프로세서가 상기 제2 컴퓨팅 장치의 사용자가 상기 제2 컴퓨팅 장치의 상기 등록 사용자인지 확인하는 과정은,

상기 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘을 복호화시키고,

상기 추출한 특징 데이터로부터 랜덤하게 추출한 서브 특징 데이터의 조합에 대한 테스트 데이터의 집합을 생성하고,

상기 복수의 인증 모델에 상기 테스트 데이터의 집합을 적용하여 상기 복수의 인증 모델의 분류 결과에 따라 상기 제2 컴퓨팅 장치의 인증 여부를 결정하는 과정을 포함하는 제1 컴퓨팅 장치.

청구항 10

제9항에 있어서,

상기 제1 프로세서가 상기 제2 컴퓨팅 장치의 인증 여부를 결정하는 과정은, 상기 복수의 인증 모델의 분류 결과를 투표 알고리즘을 통해 과반수 이상이 상기 제2 컴퓨팅 장치의 등록 사용자로 판단하는 경우, 상기 제2 컴퓨팅 장치로 인증 성공 신호를 전송하며,

상기 복수의 인증 모델의 분류 결과를 투표 알고리즘을 통해 과반수 이상이 상기 제2 컴퓨팅 장치의 등록 사용

자가 아닌 것으로 판단하는 경우, 상기 제2 컴퓨팅 장치로 인증 실패 신호를 전송하는 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 11

제1항에 있어서,

상기 제1 컴퓨팅 장치는 웨어러블 장치인 것을 특징으로 하는 제1 컴퓨팅 장치.

청구항 12

제2 프로세서, 상기 제2 프로세서에 의해 실행되는 프로그램을 저장하는 제2 메모리, 하나 이상의 제2 센서, 및 제1 컴퓨팅 장치와 통신하는 제2 통신 인터페이스를 포함하는 제2 컴퓨팅 장치에 있어서,

상기 하나 이상의 제2 센서는 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수집하고,

상기 제2 통신 인터페이스는 상기 제2 생체 데이터 및 상기 제2 모션 데이터를 포함하는 상기 제2 센서 데이터를 전송하고,

상기 제2 통신 인터페이스는 상기 제1 컴퓨팅 장치로부터 상기 제2 컴퓨팅 장치의 사용자 인증 결과를 수신하는 과정을 수행하는 것을 특징으로 하는 제2 컴퓨팅 장치.

청구항 13

제12항에 있어서,

상기 제2 통신 인터페이스가 상기 사용자 인증 결과를 수신하는 과정은,

상기 제1 컴퓨팅 장치가 획득한 제1 생체 데이터와 상기 제2 생체 데이터 간의 유사도를 상기 제1 컴퓨팅 장치가 판단한 후 상기 유사도가 임계값을 넘지 못할 경우에 전송하는 인증 실패 신호를 수신하는 것을 특징으로 하는 제2 컴퓨팅 장치.

청구항 14

제12항에 있어서,

상기 제2 통신 인터페이스가 상기 사용자 인증 결과를 수신하는 과정은,

상기 제1 컴퓨팅 장치가 복수의 인증 모델의 분류 결과를 투표 알고리즘을 통해 과반수 이상이 상기 제2 컴퓨팅 장치의 등록 사용자로 판단하는 경우에 상기 제2 컴퓨팅 장치로 전송하는 인증 성공 신호를 수신하는 것을 특징으로 하는 제2 컴퓨팅 장치.

발명의 설명

기술 분야

[0001] 본 발명은 사용자 인증 방법 및 장치에 관한 것으로, 특히 복수의 컴퓨팅 장치에 내장된 센서를 활용한 사용자 인증 시스템에 관한 것이다.

배경 기술

[0002] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 모바일 기기가 보급화되고 많은 기능들을 제공하면서 사용자의 중요 정보가 기기에 다량으로 저장되어 모바일 기기에 대한 사용자 인증 문제가 중요하게 대두되고 있다. 이에 따라, 기존 PC에서 사용하던 패스워드 방식부터 터치스크린을 이용한 그래픽 인증 방식, 사용자의 생체 정보를 활용하는 생체 인식까지 다양한 방식으로의 인증 기술들이 제안되어 왔다.

[0004] 기존 모바일 기기에 대한 사용자 인증 기술은 인증 시도자의 신원 확인을 위해 기기에 저장되어 있는 PIN, 암호, 지문 등의 정보(template)와 인증 시도자의 입력 정보를 대조하는 템플릿 매칭 방식을 사용한다. 이러한 방식은 인증 시도자와 기기 소유자의 동일여부를 확인하지 않으며 악의적인 사용자가 내부에 민감한 정보를 저장한 기기를 훔친 경우 인증 시스템 우회가 가능하다는 문제점이 있다. 나아가, 생체 인증을 비롯한 기존 인증

방식에 대한 각종 공격 방법이 존재하며 기기가 탈취되었을 경우 충분히 공격이 가능한 문제가 있다.

- [0005] 모바일 기기 대상의 기존 사용자 인증 기술은 지식 기반 인증 뿐만 아니라 생체 인증이라 할지라도 인조지문, 사진 또는 녹음 등 다양한 방법으로 인증 시스템을 속일 수 있다. 따라서, 모바일 기기의 연산 능력과 기계 학습 기술의 발전 속에서 사용자가 정보를 입력할 필요 없이 기기에 내장된 센서를 활용한 행위 기반 인증을 통해 사용자를 인증할 필요가 있다.

발명의 내용

해결하려는 과제

- [0006] 본 발명의 실시예들은 사용자의 스마트워치를 기반으로 연동된 기기 (예: 스마트폰)의 인증을 해제하는 기술을 제안한다. 본 발명은 연동된 두 기기에 동일하게 내장되어 있는 센서들 (HR Sensor, Accelerometer, and Gyroscope)에서 추출된 데이터의 유사성 파악을 통해 인증 시도자와 스마트워치 착용자의 동일인 일치 여부를 확인하고, 센서 데이터에서 추출한 행위 특징을 통해 기계학습 기반의 사용자 행위 기반 인증을 제공하는 것이다. 이는 스마트워치 착용자는 기기 소유자일 가능성이 높다는 것을 의미한다.
- [0007] 본 발명은 기존 인증 방식이 지니고 있는 인증 시도자와 기기 소유자의 일치 문제, 인증 시스템 우회 문제를 해결할 수 있는 스마트워치 기반의 인증 방식을 제공해 정확하고 안전한 사용자 인증에 기여하는데 발명의 주된 목적이 있다.
- [0008] 본 발명의 명시되지 않은 또 다른 목적들은 하기의 상세한 설명 및 그 효과로부터 용이하게 추론할 수 있는 범위 내에서 추가적으로 고려될 수 있다.

과제의 해결 수단

- [0009] 본 실시예의 일 측면에 의하면, 제1 프로세서, 상기 제1 프로세서에 의해 실행되는 프로그램을 저장하는 제1 메모리, 하나 이상의 제1 센서, 및 제2 컴퓨팅 장치와 통신하는 제1 통신 인터페이스를 포함하는 제1 컴퓨팅 장치에 있어서, 상기 제1 통신 인터페이스는 상기 제2 컴퓨팅 장치에 내장된 하나 이상의 제2 센서를 통해 수집한 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수신하고, 상기 하나 이상의 제1 센서는 제1 생체 데이터 및 제1 모션 데이터를 포함하는 제1 센서 데이터를 수집하고, 상기 제1 프로세서는, 상기 제1 생체 데이터와 상기 제2 생체 데이터 간의 유사도를 산출하고, 상기 유사도에 따라 제1 컴퓨팅 장치의 착용자 및 제2 컴퓨팅 장치의 인증 시도자 간의 동일인 여부를 판단하고, 상기 제1 센서 데이터 및 상기 제2 센서 데이터를 통한 사용자의 행위 분석을 기반으로 제2 컴퓨팅 장치에서의 인증 시도에 대한 결과를 결정 및 전송하는 과정을 수행하는 것을 특징으로 하는 제1 컴퓨팅 장치를 제공한다.
- [0010] 본 실시예의 다른 측면에 의하면, 제2 프로세서, 상기 제2 프로세서에 의해 실행되는 프로그램을 저장하는 제2 메모리, 하나 이상의 제2 센서, 및 제1 컴퓨팅 장치와 통신하는 제2 통신 인터페이스를 포함하는 제2 컴퓨팅 장치에 있어서, 상기 하나 이상의 제2 센서는 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수집하고, 상기 제2 통신 인터페이스는 상기 제2 생체 데이터 및 상기 제2 모션 데이터를 포함하는 상기 제2 센서 데이터를 전송하고, 상기 제2 통신 인터페이스는 상기 제1 컴퓨팅 장치로부터 상기 제2 컴퓨팅 장치의 사용자 인증 결과를 수신하는 과정을 수행하는 것을 특징으로 하는 제2 컴퓨팅 장치를 제공한다.

발명의 효과

- [0011] 이상에서 설명한 바와 같이 본 발명의 실시예들에 의하면, 본 발명은 인증 정보가 노출되는 것을 사전에 차단하여 사용자의 인증이 요구되는 개인정보 및 금융 서비스로의 접근을 보호하는데 활용할 수 있다. 또한, 스마트폰이 도난 되더라도 인증 템플릿의 노출이 전혀 없으며, 인증 시도자와 기기 소유자의 동일인 여부를 사전에 확인하므로 강화된 인증 성능을 제공할 수 있다.
- [0012] 기업적인 측면에서는 해당 서비스 제공을 위한 추가적인 기기가 필요하지 않아 해당 기술을 경제적인 개발 및 제공이 가능하며, 사용자의 측면에서는 기존 텍스트 인증 방식에 비해 심박 센서에 신체를 접촉하는 것 외의 다른 입력이 필요 없어 사용자의 거부감이 적고 더 편의적인 인증 서비스를 제공받을 수 있다.
- [0013] 여기에서 명시적으로 언급되지 않은 효과라 하더라도, 본 발명의 기술적 특징에 의해 기대되는 이하의 명세서에서 기재된 효과 및 그 잠정적인 효과는 본 발명의 명세서에 기재된 것과 같이 취급된다.

도면의 간단한 설명

- [0014] 도 1은 본 발명의 일 실시예에 따른 사용자 인증 시스템을 예시한 블록도이다.
- 도 2는 본 발명의 일 실시예에 따른 사용자 인증 시스템의 인증 절차의 흐름을 나타내는 도면이다.
- 도 3은 본 발명의 일 실시예에 따른 제2 컴퓨팅 장치 및 제1 컴퓨팅 장치 내부에서의 사용자 인증 과정을 자세히 도시한 도면이다.
- 도 4는 본 발명의 일 실시예에 따른 사용자 인증 시스템의 동작 방법을 나타내는 흐름도이다.
- 도 5는 본 발명의 일 실시예에 따른 제1 컴퓨팅 장치의 동작을 예시한 흐름도이다.
- 도 6은 본 발명의 일 실시예에 따른 제2 컴퓨팅 장치의 동작을 예시한 흐름도이다.
- 도 7은 실시예들에서 사용되기에 적합한 컴퓨팅 기기를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 이하, 본 발명을 설명함에 있어서 관련된 공지기능에 대하여 이 분야의 기술자에게 자명한 사항으로서 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하고, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다.
- [0016] 도 1은 사용자 인증 시스템을 예시한 블록도이다. 도 1에 도시한 바와 같이, 사용자 인증 시스템(10)은 제1 컴퓨팅 장치(100) 및 제2 컴퓨팅 장치(200)를 포함한다. 사용자 인증 시스템(10)은 도 1에서 예시적으로 도시한 다양한 구성요소들 중에서 일부 구성요소를 생략하거나 다른 구성요소를 추가로 포함할 수 있다.
- [0017] 사용자 인증 시스템(10)은 두 기기의 심박수 데이터의 유사도를 측정하여 기기의 사용자와 또 다른 기기의 착용자가 동일한지를 확인한다. 두 기기는 스마트폰 및 스마트워치를 사용할 수 있으며 반드시 이에 한정되는 것은 아니며, 사용자의 인증을 통해 사용할 수 있는 기기 또는 사용자의 신체에 착용되어 운용 가능한 기기일 수 있다.
- [0018] 사용자 인증 시스템(10)은 연동된 두 기기에 동일하게 내장되어 있는 센서에서 추출된 심박수를 나타내는 데이터의 유사성을 파악하여 인증 시도자와 스마트워치 착용자가 동일인인지 여부를 확인하고, 센서 데이터에서 추출한 행위 특징 데이터를 통해 기계학습 기반의 사용자 행위 기반 인증을 제공한다. 스마트워치는 기기 소유자 또는 등록 사용자가 일상 생활을 하는 중에 몸에 지니고 있는 기기로 분실우려가 낮으며, 이는 스마트워치 착용자가 기기 소유자 또는 등록 사용자일 가능성이 높다는 것을 의미한다.
- [0019] 사용자 인증 시스템(10)은 기존 인증 방식이 지니고 있는 스마트폰의 인증 시도자와 스마트폰의 실제 소유자의 일치 문제, 인증 시스템 우회 문제를 해결할 수 있는 스마트워치 기반의 인증 방식을 통해 정확하고 안전한 사용자 인증을 한다.
- [0020] 사용자 인증 시스템(10)은 인증 대상 기기와 연동된 타 기기를 포함하는 두 기기의 심박수 데이터의 유사성을 파악하여 동일인 여부를 결정하며, 이를 통해 오인식률(False Acceptance Rate : FAR)을 낮출 수 있으며, 인증 여부 결정 과정이 인증 대상 기기가 아닌 연동된 타 기기에서 진행되므로 인증 대상 기기가 탈취되었을 경우, 인증 시스템 우회가 불가능하게 된다.
- [0021] 사용자 인증 시스템(10)은 다른 사용자의 데이터를 얻어서 학습시키기에는 현실적으로 불가능하므로 One-class classification 알고리즘의 실제적인 적용이 가능하다. 또한, 시간 및 주파수 영역에서의 데이터를 모두 고려하여 각 영역에서 고유하게 획득 가능한 분별력 있는 사용자의 행위 특징을 추출할 수 있다.
- [0022] 사용자 인증 시스템(10)은 기기의 잠금 해제나 금융 서비스를 위해 사용자 인증이 필요한 기기에 사용되며, 스마트폰의 심박 센서에 사용자의 신체가 접촉되면 스마트폰이 스마트워치에 인증 시도를 요청하고 다음의 과정으로 시스템이 동작한다.
- [0023] 제1 컴퓨팅 장치(100)는 제2 컴퓨팅 장치(200)와 통신이 가능하며, 제2 컴퓨팅 장치(200)에서 전송된 제2 생체 데이터를 수신한다. 제1 컴퓨팅 장치(100)는 내장된 제1 센서를 통해 제1 센서 데이터를 수집한다. 제1 센서 데이터는 제1 생체 데이터 및 제1 모션 데이터를 포함한다.

- [0024] 제2 컴퓨팅 장치(200)는 인증 시도가 감지되면 하나 이상의 제2 센서를 통해 제2 센서 데이터를 수집하며, 제2 센서 데이터를 제1 컴퓨팅 장치(100)로 전송한다. 제2 센서 데이터는 제2 생체 데이터 및 제2 모션 데이터를 포함한다.
- [0025] 제1 컴퓨팅 장치(100)에 내장된 제1 센서 및 제2 컴퓨팅 장치(200)에 내장된 제2 센서는 서로 같은 종류의 센서를 포함한다. 본 발명의 일 실시예에 따르면, 제1 센서 및 제2 센서는 심박 센서(HR Sensor), 가속도 센서(accelerometer Sensor) 및 자이로 센서(Gyroscope Sensor)로 이루어져 있으나 반드시 이에 한정되는 것은 아니다.
- [0026] 본 발명의 일 실시예에 따르면, 제1 생체 데이터 및 제2 생체 데이터는 심박 센서를 이용하여 수집한 심박 데이터이고, 제1 모션 데이터 및 제2 모션 데이터는 가속도 센서를 이용하여 수집한 가속도 데이터 및 자이로 센서를 이용하여 수집한 자이로 데이터일 수 있다.
- [0027] 제1 컴퓨팅 장치(100)는 제1 생체 데이터와 제2 생체 데이터 간의 유사도를 산출하고, 유사도에 따라 제1 컴퓨팅 장치(100)의 사용자 및 제2 컴퓨팅 장치(200)의 사용자 간의 동일인 여부를 판단하고, 제1 센서 데이터 및 제2 센서 데이터를 통한 사용자 행위 분석을 기반으로 제2 컴퓨팅 장치(200)의 사용자 인증 결과를 생성하는 과정을 수행한다.
- [0028] 제1 컴퓨팅 장치(100)는 제1 생체 데이터, 제2 생체 데이터, 제1 모션 데이터, 및 제2 모션 데이터의 노이즈를 제거하는 전처리 과정을 더 수행한다.
- [0029] 제2 컴퓨팅 장치(200)는 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 전송하고, 제1 컴퓨팅 장치(100)로부터 상기 제2 컴퓨팅 장치(200)의 사용자 인증 결과를 수신하는 과정을 수행한다.
- [0030] 이하에서는 컴퓨팅 장치가 형성하는 절차의 흐름에 대해 설명하기로 한다. 도 2는 사용자 인증 시스템의 인증 절차 흐름을 나타내는 도면이다.
- [0031] 도 2를 참조하면, 본 발명에서 제1 컴퓨팅 장치(100)는 스마트워치이며, 제2 컴퓨팅 장치(200)는 스마트폰이다. 본 발명에서 스마트폰은 인증을 시도하는 기기이고, 스마트워치는 사용자의 몸에 부착된 기기를 나타낸다.
- [0032] 사용자 인증 시스템(10)은 스마트워치와 연동된 스마트폰과 같이 연동된 두 기기에 내장되어 있는 센서를 이용하여 사용자 인증 여부를 결정한다. 결과적으로 인증 과정이 인증을 시도하는 기기가 아닌 인증을 시도하는 기기와 연동된 사용자의 신체에 부착된 기기에서 진행되기 때문에 인증 시스템 우회 가능성을 해결할 수 있다.
- [0033] 도 2를 참조하면, 스마트폰은 인증 시도를 감지하면 인증 시도 요청 신호를 스마트워치에 전송하며, 스마트폰에 내장된 제2 센서를 통해 측정된 제2 센서 데이터를 스마트워치에 전송한다.
- [0034] 스마트워치는 인증을 시도하는 기기가 아닌 인증을 시도하는 기기와 연동되어 사용자의 몸에 부착된 기기로서, 스마트폰에서 전송한 제2 센서 데이터를 수신한다. 스마트워치는 내장된 제1 센서를 통해 제1 생체 데이터를 측정한다.
- [0035] 스마트워치는 제1 센서 데이터 및 제2 센서 데이터를 기반으로 사용자 인증 여부를 결정하고, 생성된 사용자 인증 결과를 스마트폰에 전송한다.
- [0036] 스마트폰은 수신한 사용자 인증 결과를 기반으로 인증 시도자가 기기 소유자인 것으로 판명될 경우, 스마트폰의 사용자의 접근을 허용한다.
- [0037] 이하에서는 제1 컴퓨팅 장치 및 제2 컴퓨팅 장치를 통한 사용자 인증 과정에 대해 흐름을 따라 설명한다. 도 3은 제2 컴퓨팅 장치 및 제1 컴퓨팅 장치 내부에서의 사용자 인증 과정을 자세히 도시한 도면이고, 도 4는 본 발명의 일 실시예에 따른 사용자 인증 시스템의 동작 방법을 나타내는 흐름도이다.
- [0038] 사용자 인증 시스템(10)은 스마트폰에서 사용자가 인증 시도를 요청하면 일정 시간 동안 스마트폰 및 스마트워치에서 심박 센서, 가속도 센서, 자이로 센서로부터 데이터를 수집한다(S410, S412). 이 때, 스마트폰에서 수집된 데이터는 스마트워치로 전송되며(S310), 전송된 스마트폰에서 측정된 제1 생체 데이터와 스마트워치에서 수집된 제2 생체 데이터의 노이즈를 제거한다(S320, S420).
- [0039] 사용자 인증 시스템(10)은 스마트폰 및 스마트워치에서 측정된 심박수 데이터를 통해 두 데이터의 유사도를 측정하고, 사전에 설정된 임계값을 기준으로 두 기기의 현재 사용자가 동일한지의 여부를 결정한다(S330, S430).
- [0040] 측정된 유사도가 임계값을 넘지 못한 경우, 제1 컴퓨팅 장치(100)는 인증 과정을 중단하고 인증 실패 신호를 제

2 컴퓨팅 장치(200)로 전송한다(S460).

- [0041] 측정된 유사도가 임계값을 넘은 경우, 제1 컴퓨팅 장치(100)는 두 기기의 현재 사용자가 동일인이라고 판단하고, 스마트폰 기기 소유자일 가능성이 높으므로 다음 단계를 진행한다.
- [0042] 동일인이라고 판단된 경우 다음 단계는 심박 센서, 가속도 센서, 자이로 센서에서 측정된 데이터에 대한 푸리에 변환과 함께 사용자 인증을 위한 행위 특징을 추출하고(S340, S440), 행위 특징을 사용자 인증 모델에 입력하여 사용자의 인증여부를 결정한다(S350, S450).
- [0043] 사용자 인증 시스템(10)은 단계 S350에서의 결과에 따라 스마트폰의 인증 시도를 승인 또는 거부 한다.
- [0044] 이하에서는 사용자 인증 과정에 대해 자세하게 설명한다.
- [0045] 사용자 인증 시스템(10)은 스마트폰과 스마트워치를 기반으로 동작된다. 스마트폰에서 인증 시도가 감지되면, 스마트폰 및 스마트워치는 데이터를 수집한다.
- [0046] 데이터 수집(Data Collection)은 스마트폰 및 스마트워치에 내장된 센서로부터 데이터를 획득하는 과정으로, 본 발명에서는 세가지 센서가 사용된다. 세가지 센서는 심박 센서, 가속도 센서 및 자이로 센서이다.
- [0047] 심박 센서(HR Sensor)는 분당 비트 수 단위의 심장 박동수를 측정하는 센서이다. 심장박동은 지문처럼 개개인이 모두 독특한 리듬과 특징을 가지고 있기 때문에 사용자 개개인을 판단하기 위한 인증에 활용된다. 심박수를 측정하는 센서는 예를 들어, 심전도 센서(electrocardiogram, ECG) 또는 광혈류측정(photoplethysmography, PPG) 센서가 있다.
- [0048] 가속도 센서(accelerometer Sensor)는 물체의 가속도나 충격의 세기를 측정하는 센서이다. 가속도 센서는 x, y, z축 정보를 처리하여 물체의 가속도, 진동, 충격 등의 동적 힘을 측정하며, 주로 사용자의 팔을 움직이거나 걷는 것과 같은 사용자의 더 큰 동작 패턴을 기록한다.
- [0049] 자이로 센서(Gyroscope Sensor)는 x, y, z축 정보를 처리하여 물체의 회전 속도인 각속도를 측정하는 센서이다. 자이로 센서는 물체를 잡는 방법 등 사용자의 세밀한 동작을 기록한다.
- [0050] 데이터 수집(Data Collection) 과정은 스마트폰의 인증 시도가 감지될 때 활성화된다. 인증 시도는 심박 센서에 신체 접지가 감지되었을 때를 의미한다. 데이터 수집이 끝나면, 데이터 전처리 과정을 수행한다.
- [0051] 전처리(Preprocessing) 과정은 수집한 센서 데이터를 전처리하는 과정으로 데이터가 가지는 노이즈를 제거(Noise Removal)하여 인증 정확도를 높이기 위해 동작한다. 전처리 과정은 센서 데이터의 특징에 따라 각기 알맞은 필터가 적용되며, 불필요한 잡음과 오차 보정 등을 위해 Low-pass Filter(LPF), High-pass Filter(HPF), Band-pass Filter(BPF), Moving Average Filter(MAF) 등이 적용 가능하다.
- [0052] 전처리 과정에서, 필터링을 통해 노이즈가 제거된 데이터들은 스마트워치 사용자와 스마트폰 인증 대상자가 동일한지와 스마트폰의 사용자가 스마트폰의 등록 사용자인지를 확인하는데 활용한다.
- [0053] Low-pass Filter(LPF)는 저역 통과 필터로 입력 신호의 주파수 성분 중에서 차단 주파수보다 낮은 주파수 성분인 저역 주파수 성분만을 통과시킨다. High-pass Filter(HPF)는 고역 통과 필터로 입력 신호의 주파수 성분 중에서 차단 주파수보다 높은 주파수 성분인 고역 주파수 성분만을 통과시킨다.
- [0054] Band-pass Filter(BPF)는 통과대역 필터로 원하는 특정 주파수 대역내의 세력만 감쇠없이 통과시키고, 나머지 주파수 세력은 감쇠한다. Moving Average Filter(MAF)는 연속적으로 입력되는 값들을 평균하여 가며 출력을 내며, 값의 변화 추이를 반영한다.
- [0055] 사용자 인증을 위한 첫 번째 단계(1st Phase)는 동일 판단(Identical Decision) 과정이며, 스마트폰과 스마트워치에서 획득한 심박수 데이터를 통해 스마트워치 사용자와 스마트폰의 사용자가 동일인인지 판단 여부를 결정한다.
- [0056] 본 발명의 일 실시 예에 따르면, 동일인 판단 과정은 동적 시간 워핑(Dynamic Time Warping, DTW) 알고리즘을 활용하여 두 심박수 데이터의 유사도를 평가한다. 두 데이터의 유사도가 설정해둔 임계값(Threshold)을 넘을 경우 두 기기의 사용자가 동일인일 확률이 높으므로 인증 과정(2nd Phase)을 수행하며, 만약 두 데이터의 유사도가 임계값을 넘지 못할 경우, 인증 시도를 종료하고 인증 실패 신호를 스마트폰에 전송한다.
- [0057] 동적 시간 워핑(Dynamic Time Warping, DTW)은 속도가 다를 수 있는 비슷한 두 개의 데이터를 비교하여 두 시간

순서간의 유사성을 측정하는 알고리즘으로, 심박수의 유사성을 평가하기 위해 사용한다.

- [0058] 특징 추출(Feature Extraction) 단계는 사용자 인증(2nd Phase)을 위해 데이터에서 행위의 특징을 추출하는 단계이다. 높은 인증 정확도를 위해 사용자마다 고유하여 분별력 있는 행위의 특징을 추출한다.
- [0059] 특징 추출을 위해 고려되는 특징 데이터는 가속도 데이터, 자이로 데이터, 심박수 데이터에서 산출한다. 가속도 센서 및 자이로 센서는 x, y, z축의 출력 값을 하나의 대푯값으로 처리하는 데이터 크기를 연산하여 특징 추출을 위한 특징 데이터로 고려한다. 나아가, 데이터의 시간 영역(Time domain)과 주파수 영역(Frequency domain)을 모두 고려한다.
- [0060] 주파수 영역의 센서 데이터는 시간 영역의 센서 데이터에 푸리에 변환을 수행함으로써 얻을 수 있으며, 신속한 인증을 위해 고속 푸리에 변환(fast fourier transform, FFT)을 사용한다. 가속도 데이터(x, y, z, magnitude)를 시간 영역(time domain)과 주파수 영역(frequency domain)에서, 자이로 데이터(x, y, z, magnitude)를 시간 영역(time domain)과 주파수 영역(frequency domain)에서, 심박수 데이터를 시간 영역(time domain)과 주파수 영역(frequency domain)에서 푸리에 변환을 수행하며, $4 \times 2 + 4 \times 2 + 2 = 18$ 으로, 총 18개 데이터 스트림에서 특징 추출이 이뤄진다.
- [0061] 사용자 인증을 위한 두 번째 단계(2nd Phase)는 사용자 인증(User Authentication) 과정이며, 스마트폰과 스마트워치의 심박수 데이터, 가속도 데이터 및 자이로 데이터에서 추출된 행위의 특징들을 활용하여 스마트폰의 사용자가 스마트폰의 등록 사용자인지를 결정한다.
- [0062] 사용자 인증은 기계학습 알고리즘과 비사용자의 학습 데이터를 요구하지 않는 단일 클래스 학습(One-class classification, OCC) 알고리즘으로 사용자 인증 여부를 결정한다. OCC 알고리즘은 비사용자의 데이터를 학습하지 않기 때문에 실제적인 적용이 가능한 알고리즘으로, One-Class Support Vector Machine, One-Class K-Means 등이 활용될 수 있다.
- [0063] 사용자 인증은 사용자의 행위의 특징들로 학습된 기계학습 모델에 사용자의 행위 특징을 입력(input)으로 하여 인증 여부를 결정한다. 사용자 인증은 인증 모델 학습 단계와 인증 여부 결정 단계로 나뉜다. 스마트워치는 스마트폰의 등록 사용자의 인증 템플릿 탈취 가능성이 존재하므로 각 단계에 인증 템플릿을 보호하기 위한 방법이 적용된다.
- [0064] 인증 모델 학습은 사용자 인증을 위한 인증 여부 결정을 위해서 스마트폰의 등록 사용자를 확인하기 위해 사전에 스마트폰의 등록 사용자의 데이터를 등록하는 과정이다. 인증 모델 학습 단계는 스마트폰의 등록 사용자가 본 인증 방식을 선택했을 때 실행되며, 공격자에게 인증 모델과 특징 데이터가 탈취되는 것을 예방하기 위해 3단계에 걸쳐 인증 모델을 학습한다.
- [0065] 인증 모델 학습의 1단계는 동일한 기계학습 알고리즘 기반의 인증 모델을 2개 이상 배치하고 배깅(bagging, bootstrap aggregating)을 적용해 다수의 인증 모델을 학습한다. 배깅(bagging)은 기계학습에서 사용되는 앙상블 기법 중 하나로, 모델의 안정성과 정확성을 높여주며, 모델이 과적합되는 것 또한 예방해준다.
- [0066] 인증 모델 학습 과정은 길이 M의 원본 특징으로부터 M' (단, $M' < M$)개의 특징을 랜덤으로 추출한 서브 특징 데이터의 조합에 대한 학습 데이터 t_i 를 생성하고, 이를 반복하여 학습 데이터의 집합 $T = \{t_1, t_2, \dots, t_N \mid N = n(f)\}$ 를 생성하고, 생성된 학습 데이터의 집합에 OCC 알고리즘 L에 t_i 를 적용해 모델 f_i 를 학습시킨다. 즉, $F = \{f_i = L(t_i) \mid i \in \{1, 2, \dots, N\}\}$ 이다.
- [0067] 따라서, 배깅을 통해 학습한 인증 모델은 $F = \{f_1, f_2, \dots, f_N\}$ 이며, f_i 는 OCC 알고리즘 L 기반 인증 모델이다.
- [0068] 인증 모델 학습의 2단계는 학습 데이터를 제거하는 단계이며, 배깅을 통한 인증 모델의 학습이 완료되면 학습에 사용된 데이터를 스마트워치에서 전부 삭제한다. 이를 통해 학습 데이터의 탈취 가능성이 제거되며, 학습 데이터의 재사용 공격에 대한 예방이 가능하다.
- [0069] 인증 모델 학습의 3단계는 서브 특징 데이터의 조합 추출 및 인증 과정을 패킹(packing)을 통해 난독화시키는 단계로, 패킹의 대표적인 방식인 암호화를 적용한다.
- [0070] 패킹은 프로그램 내에 2개의 섹션을 생성하고 하나의 섹션에서는 서브 특징 데이터의 조합 추출을 포함한 인증 프로그램을 공개키를 활용하여 암호화한 코드를 저장하고, 다른 섹션에서는 암호화된 섹션을 복호화하는 코드를 저장한다.

- [0071] 패킹을 통해 변형된 프로그램은 역공학(reverse-engineering) 등의 바이너리 분석으로부터 강인하며, 결과적으로 인증 과정에 대한 정보를 탈취 위협으로부터 보호할 수 있다.
- [0072] 인증 여부 결정은 학습된 인증 모델을 기반으로 입력된 데이터가 스마트폰의 등록 사용자의 것인지를 확인하는 단계이다. 인증 시 첫 번째 단계(1st Phase)의 동일 판단(Identical Decision) 과정이 통과된 다음 실행되며 총 3 단계에 걸쳐 진행된다.
- [0073] 인증 여부 결정의 1단계는 인증 모델 학습 단계에서 패킹 과정을 통해 암호화된 인증 프로그램을 복호화시키는 언패킹(unpacking) 단계이다. 언패킹 이후에는 메모리상에 학습 당시 구현된 서브 특징 데이터의 조합 추출 및 인증 과정의 알고리즘이 복구된다.
- [0074] 인증 여부 결정의 2단계는 입력된 데이터의 행위 데이터에서 추출된 특징 데이터로부터 서브 특징 데이터의 조합에 대한 테스트 데이터의 집합 $D = \{d_1, d_2, \dots, d_N \mid N = n(f)\}$ 를 생성한다. 이 때 d_i 는 인증 모델 학습의 1단계에서 수행하는 과정을 통해 t_i 와 동일한 서브 특징 데이터의 조합을 추출한다.
- [0075] 인증 여부 결정의 3단계는 f_i 에 d_i 를 적용해 각 모델의 분류 결과에 대한 집합 $R = \{r_1, r_2, \dots, r_N\}$ 을 생성하며, $i \in \{1, 2, \dots, N\}$ 일 때 $r_i = f_i(d_i)$ 이다. 인증 여부 결정은 각 모델의 결과를 취합하고, 과반수이상이 결정한 분류 결과를 최종결과로 도출한다. 예를 들어, 과반수이상이 입력된 데이터를 스마트폰의 등록 사용자의 것으로 결정하면, 스마트워치는 사용자의 스마트폰의 접근을 허용한다.
- [0076] 도 5는 본 발명의 다른 실시예에 따른 제1 컴퓨팅 장치의 동작을 예시한 흐름도이다. 사용자 인증 방법은 컴퓨팅 기기에 의하여 수행될 수 있으며, 컴퓨팅 장치가 수행하는 동작에 관한 상세한 설명과 중복되는 설명은 생략하기로 한다.
- [0077] 단계 S510에서, 제1 컴퓨팅 장치(100)는 제2 컴퓨팅 장치(200)에 내장된 하나 이상의 제2 센서를 통해 수집한 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수신한다.
- [0078] 단계 S520에서, 제1 컴퓨팅 장치(100)와 하나 이상의 제1 센서를 통해 제1 생체 데이터 및 제1 모션 데이터를 포함하는 제1 센서 데이터를 수집한다.
- [0079] 제1 컴퓨팅 장치(100)는 제1 생체 데이터, 제2 생체 데이터, 제1 모션 데이터, 및 제2 모션 데이터의 노이즈를 제거하는 전처리 과정을 더 수행한다.
- [0080] 단계 S530에서, 제1 컴퓨팅 장치(100)는 제1 생체 데이터와 상기 제2 생체 데이터 간의 유사도를 산출하고, 유사도에 따라 제1 컴퓨팅 장치의 사용자 및 제2 컴퓨팅 장치의 사용자 간의 동일인 여부를 판단한다.
- [0081] 동일인 여부를 판단하는 과정은 측정 시간에 따라 상이한 파형을 갖는 제1 생체 데이터와 제2 생체 데이터의 측정 구간을 동기화하고, 제1 생체 데이터의 파형과 제2 생체 데이터의 파형을 비교하여 상기 유사도를 산출한다.
- [0082] 제1 컴퓨팅 장치(100)는 유사도가 임계값을 넘을 경우, 제1 컴퓨팅 장치(100)의 사용자 및 제2 컴퓨팅 장치(200)의 사용자를 동일인으로 판단하며, 상기 유사도가 임계값을 넘지 못할 경우, 상기 제2 컴퓨팅 장치(200)로 인증 실패 신호를 전송한다.
- [0083] 단계 S540에서, 제1 컴퓨팅 장치(100)는 제1 센서 데이터 및 제2 센서 데이터를 통한 사용자의 행위 분석을 기반으로 제2 컴퓨팅 장치(200)의 사용자 인증 결과를 생성하는 과정을 수행한다.
- [0084] 상기 사용자의 행위 분석을 기반으로 사용자 인증 결과를 생성하는 과정은 제1 센서 데이터 및 제2 센서 데이터를 기반으로 행위의 특징을 추출하고, 제2 컴퓨팅 장치(200)의 등록 사용자의 원본 센서 데이터를 등록하여 인증 모델을 학습하고, 학습된 인증 모델을 기반으로 제2 컴퓨팅 장치(200)의 사용자가 제2 컴퓨팅 장치(200)의 등록 사용자인지 확인하는 과정을 포함한다.
- [0085] 행위의 특징을 추출하는 과정은 제1 센서 데이터 및 제2 센서 데이터에 대해서 시간 영역과 주파수 영역을 고려하며 특징 데이터를 추출하고, 특징 데이터는 3개의 축에 대응하는 데이터 및 3개의 축에 따른 데이터의 크기를 포함하며, 주파수 영역의 센서 데이터는 시간 영역의 센서 데이터를 푸리에 변환하여 획득한다.
- [0086] 인증 모델을 학습하는 과정은 복수의 인증 모델을 병렬로 연결하여, 제2 컴퓨팅 장치(200)의 등록 사용자의 행위에 대한 원본 센서 데이터로부터 랜덤하게 추출한 서브 특징 데이터의 조합에 대한 학습 데이터의 집합을 생성하고, 학습 데이터를 단일 클래스 학습 알고리즘에 적용하여 복수의 인증 모델을 학습하고, 복수의 인증 모델을 학습하는데 사용된 학습 데이터를 제1 컴퓨팅 장치(100)에서 삭제하고, 추출한 서브 특징 데이터의 조합을

포함하는 사용자 인증 알고리즘을 암호화하는 과정을 포함한다.

- [0087] 제1 컴퓨팅 장치(100)는 (i) 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘과 (ii) 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘을 복호화하는 코드를 저장하고, 제2 컴퓨팅 장치(200)의 사용자가 인증을 시도할 때 복호화 과정을 수행한다.
- [0088] 제2 컴퓨팅 장치(200)의 사용자가 상기 제2 컴퓨팅 장치(200)의 상기 등록 사용자인지 확인하는 과정은 암호화된 서브 특징 데이터의 조합을 포함하는 사용자 인증 알고리즘을 복호화시키고, 추출한 특징 데이터로부터 랜덤하게 추출한 서브 특징 데이터의 조합에 대한 테스트 데이터의 집합을 생성하고, 복수의 인증 모델에 테스트 데이터의 집합을 적용하여 복수의 인증 모델의 분류 결과에 따라 제2 컴퓨팅 장치(200)의 인증 여부를 결정한다.
- [0089] 제2 컴퓨팅 장치(200)의 인증 여부를 결정하는 과정은 복수의 인증 모델의 분류 결과를 투표 알고리즘을 통해 과반수 이상이 제2 컴퓨팅 장치(200)의 등록 사용자로 판단하는 경우, 제2 컴퓨팅 장치(200)로 인증 성공 신호를 전송한다. 과반수 이상이 제2 컴퓨팅 장치(200)의 등록 사용자가 아닌 것으로 판단하는 경우, 제2 컴퓨팅 장치(200)로 인증 실패 신호를 전송한다.
- [0090] 도 5에서는 각각의 과정을 순차적으로 실행하는 것으로 개제하고 있으나 이는 예시적으로 설명한 것에 불과하고, 이 분야의 기술자라면 본 발명의 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 도 5에 기재된 순서를 변경하여 실행하거나 또는 하나 이상의 과정을 병렬적으로 실행하거나 다른 과정을 추가하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이다.
- [0091] 도 6는 본 발명의 다른 실시예에 따른 제2 컴퓨팅 장치의 동작을 예시한 흐름도이다. 제2 컴퓨팅 장치를 이용한 사용자 인증은 컴퓨팅 장치에 의하여 수행될 수 있으며, 컴퓨팅 장치가 수행하는 동작에 관한 상세한 설명과 중복되는 설명은 생략하기로 한다.
- [0092] 단계 S610에서, 제2 컴퓨팅 장치(200)는 하나 이상의 제2 센서는 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 수집한다.
- [0093] 단계 S620에서, 제2 컴퓨팅 장치(200)는 제2 생체 데이터 및 제2 모션 데이터를 포함하는 제2 센서 데이터를 전송한다.
- [0094] 단계 S630에서, 제2 컴퓨팅 장치(200)는 제1 컴퓨팅 장치(100)로부터 상기 제2 컴퓨팅 장치(200)의 사용자 인증 결과를 수신하는 과정을 수행한다.
- [0095] 상기 사용자 인증 결과를 수신하는 과정은 제1 컴퓨팅 장치(100)가 획득한 제1 생체 데이터와 상기 제2 생체 데이터 간의 유사도를 상기 제1 컴퓨팅 장치(100)가 판단한 후 상기 유사도가 임계값을 넘지 못할 경우에 전송하는 인증 실패 신호를 수신한다.
- [0096] 상기 사용자 인증 결과를 수신하는 과정은 제1 컴퓨팅 장치(100)가 복수의 인증 모델의 분류 결과를 투표 알고리즘을 통해 과반수 이상이 상기 제2 컴퓨팅 장치(200)의 등록 사용자로 판단하는 경우에 제2 컴퓨팅 장치(200)로 전송하는 인증 성공 신호를 수신한다.
- [0097] 도 6에서는 각각의 과정을 순차적으로 실행하는 것으로 개제하고 있으나 이는 예시적으로 설명한 것에 불과하고, 이 분야의 기술자라면 본 발명의 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 도 6에 기재된 순서를 변경하여 실행하거나 또는 하나 이상의 과정을 병렬적으로 실행하거나 다른 과정을 추가하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이다.
- [0098] 도 7은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 기기를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.
- [0099] 도시된 컴퓨팅 환경은 사용자 인증 시스템(10)을 포함한다. 일 실시예에서, 사용자 인증 시스템(10)은 타 단말기와 신호를 송수신하는 모든 형태의 컴퓨팅 기기일 수 있다.
- [0100] 사용자 인증 시스템(10)은 적어도 하나의 프로세서(710), 컴퓨터 판독 가능한 저장매체(720) 및 통신 버스(760)를 포함한다. 프로세서(710)는 사용자 인증 시스템(10)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(710)는 컴퓨터 판독 가능한 저장 매체(720)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(710)에 의해 실행되는 경우 사용자 인증 시스템(10)으로 하여금

예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

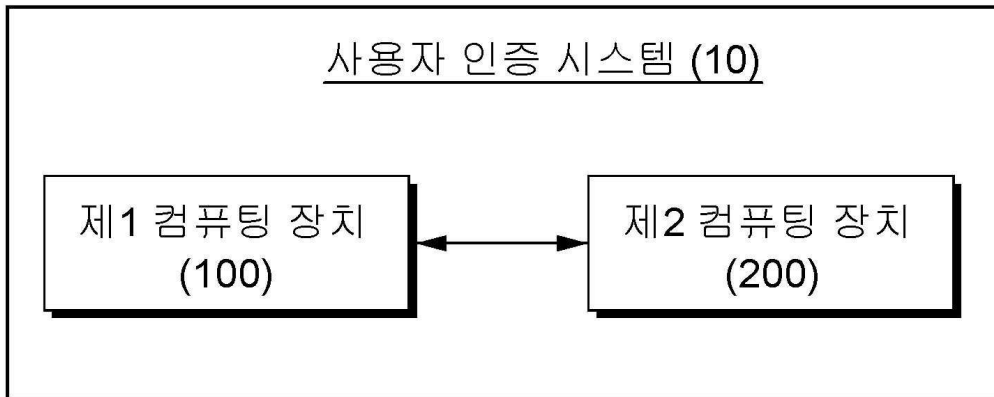
- [0101] 컴퓨터 판독 가능한 저장 매체(720)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능한 저장 매체(720)에 저장된 프로그램(730)은 프로세서(710)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능한 저장 매체(720)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 기기들, 광학 디스크 저장 기기들, 플래시 메모리 기기들, 그 밖에 사용자 인증 시스템(10)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.
- [0102] 통신 버스(760)는 프로세서(710), 컴퓨터 판독 가능한 저장 매체(720)를 포함하여 사용자 인증 시스템(10)의 다른 다양한 컴포넌트들을 상호 연결한다.
- [0103] 사용자 인증 시스템(10)은 또한 하나 이상의 입출력 장치(미도시)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(740) 및 하나 이상의 통신 인터페이스(750)를 포함할 수 있다. 입출력 인터페이스(740) 및 통신 인터페이스(750)는 통신 버스(760)에 연결된다. 입출력 장치(미도시)는 입출력 인터페이스(740)를 통해 사용자 인증 시스템(10)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(미도시)는 사용자 인증 시스템(10)을 구성하는 일 컴포넌트로서 사용자 인증 시스템(10)의 내부에 포함될 수도 있고, 사용자 인증 시스템(10)와는 구별되는 별개의 장치로 컴퓨팅 기기와 연결될 수도 있다.
- [0104] 본 실시예들에 따른 동작은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능한 매체에 기록될 수 있다. 컴퓨터 판독 가능한 매체는 실행을 위해 프로세서에 명령어를 제공하는 데 참여한 임의의 매체를 나타낸다. 컴퓨터 판독 가능한 매체는 프로그램 명령, 데이터 파일, 데이터 구조 또는 이들의 조합을 포함할 수 있다. 예를 들면, 자기 매체, 광기록 매체, 메모리 등이 있을 수 있다. 컴퓨터 프로그램은 네트워크로 연결된 컴퓨터 시스템 상에 분산되어 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수도 있다. 본 실시예를 구현하기 위한 기능적인(Functional) 프로그램, 코드, 및 코드 세그먼트들은 본 실시예가 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있을 것이다.
- [0105] 본 실시예들은 본 실시예의 기술 사상을 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

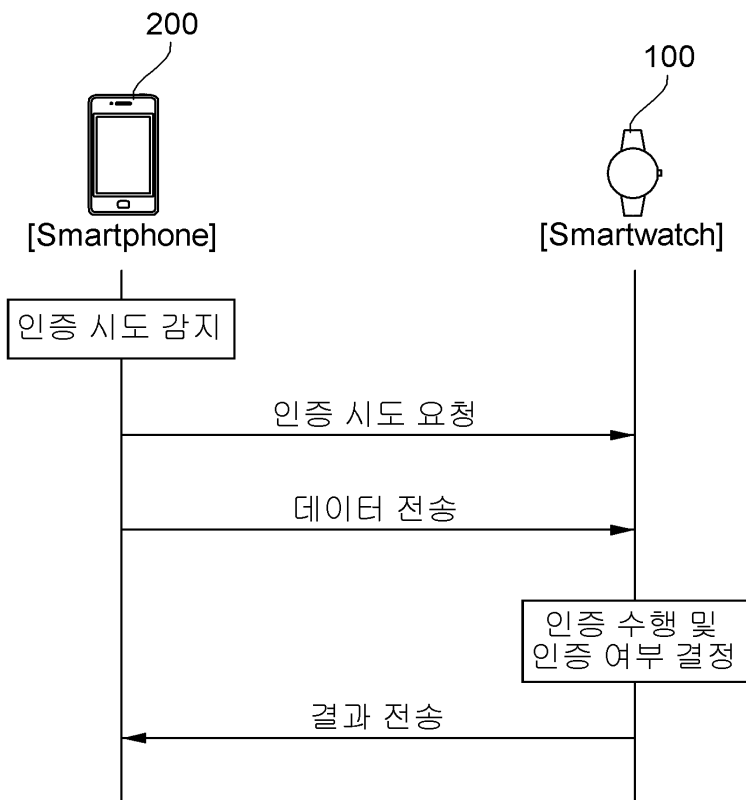
- [0106] 10: 사용자 인증 시스템
- 100: 제1 컴퓨팅 장치
- 200: 제2 컴퓨팅 장치

도면

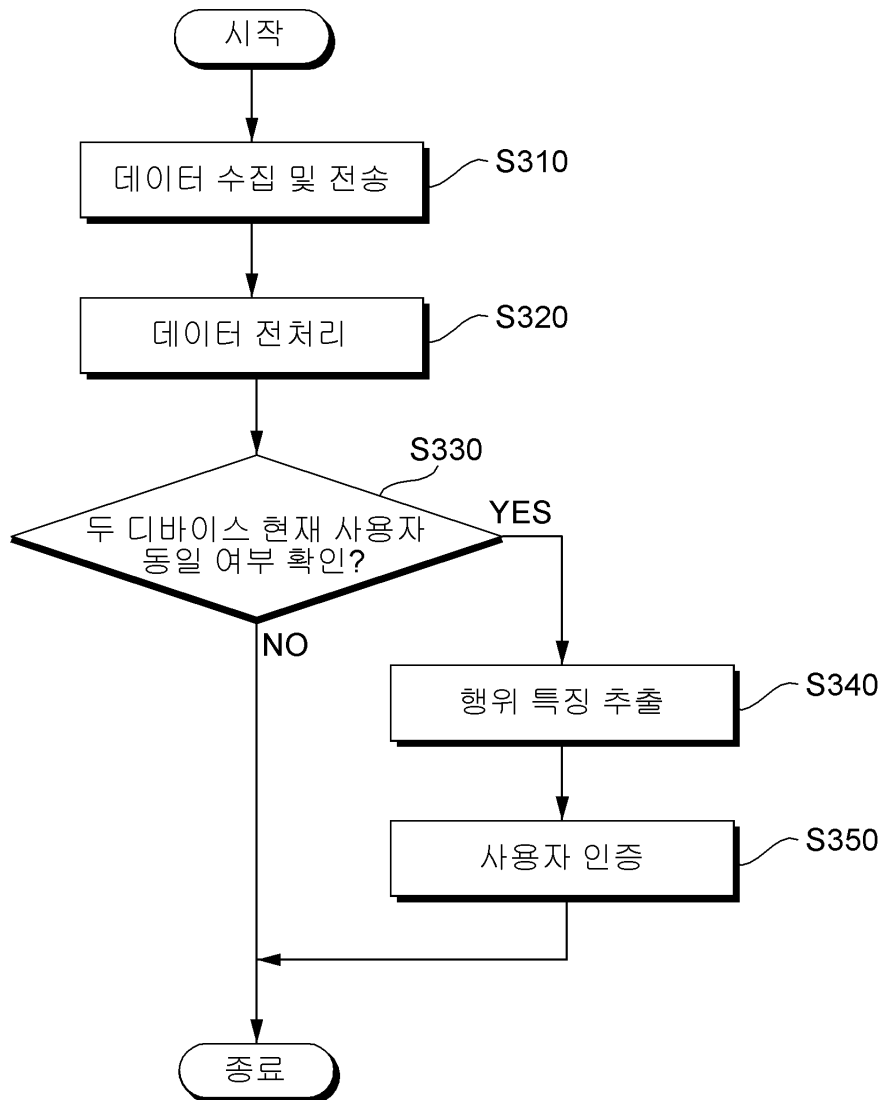
도면1



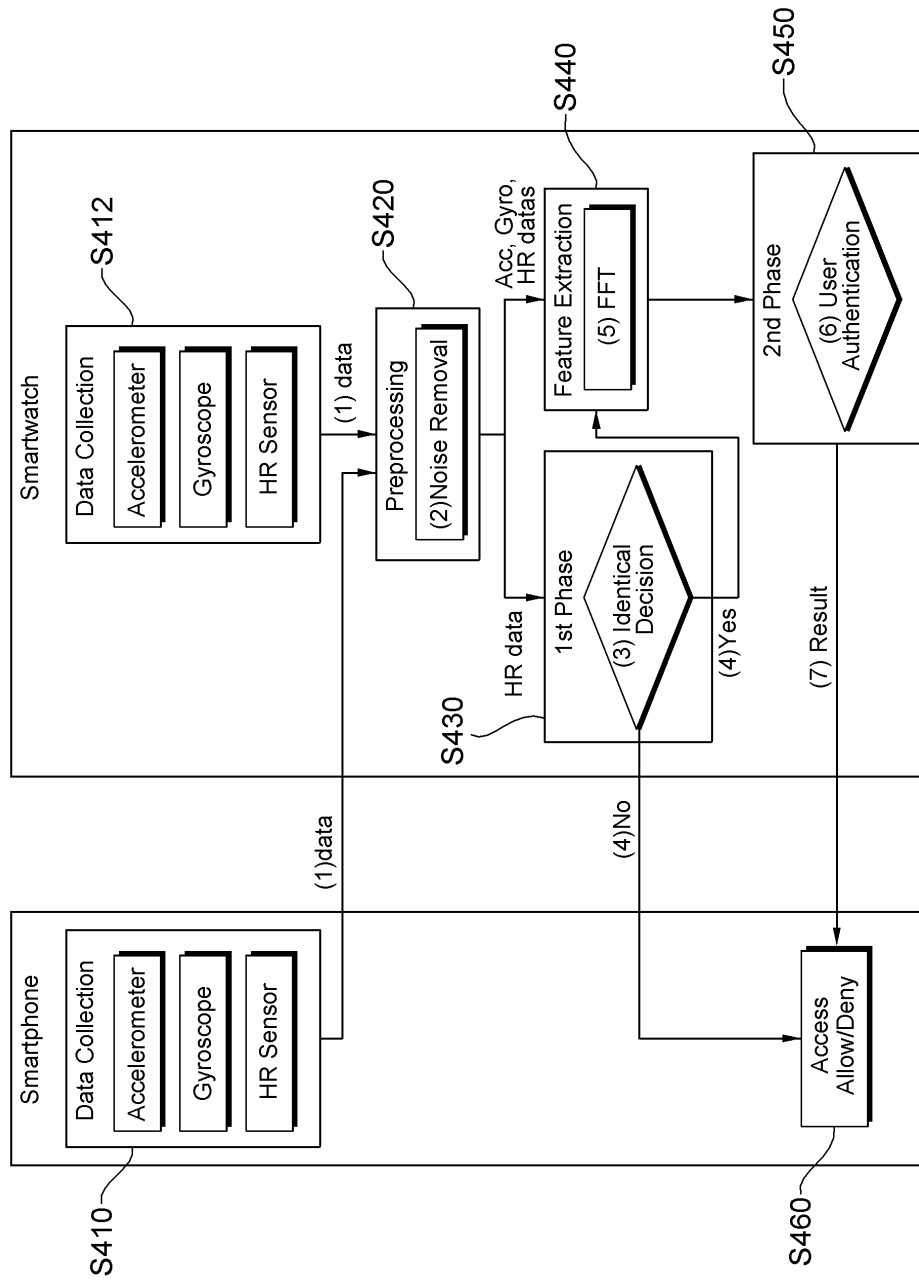
도면2



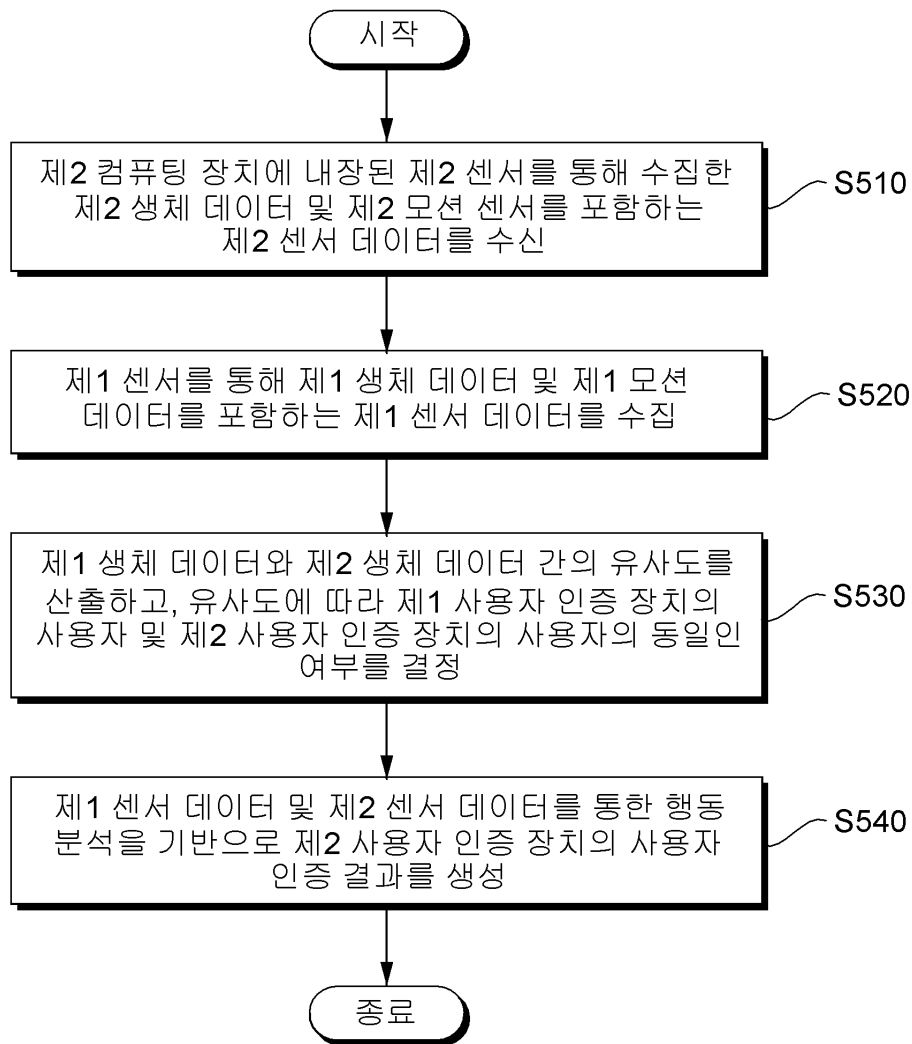
도면3



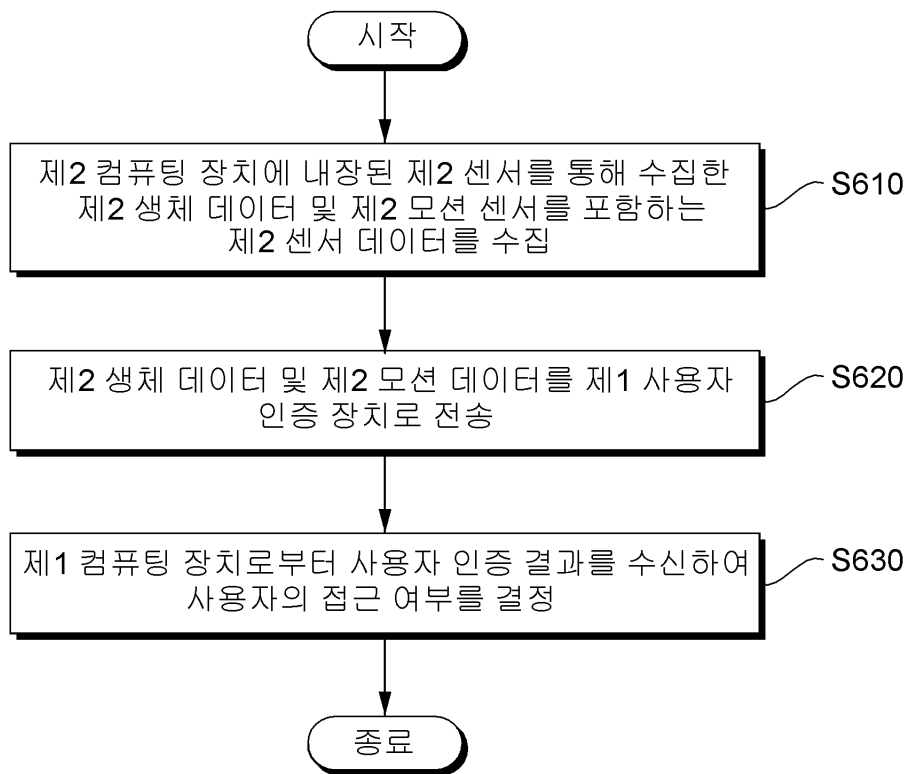
도면4



도면5



도면6



도면7

