(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0012115
(43) 공개일자 2022년02월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) *G06F 21/45* (2013.01)
G06F 21/55 (2013.01) *H04B 13/00* (2006.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2020-0091245
(22) 출원일자 2020년07월22일
심사청구일자 2020년07월22일

(71) 출원인
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
이경한
울산광역시 울주군 언양읍 유니스트길 50 울산과학기술원
이성용
울산광역시 울주군 언양읍 유니스트길 50 울산과학기술원
(74) 대리인
제일특허법인(유)

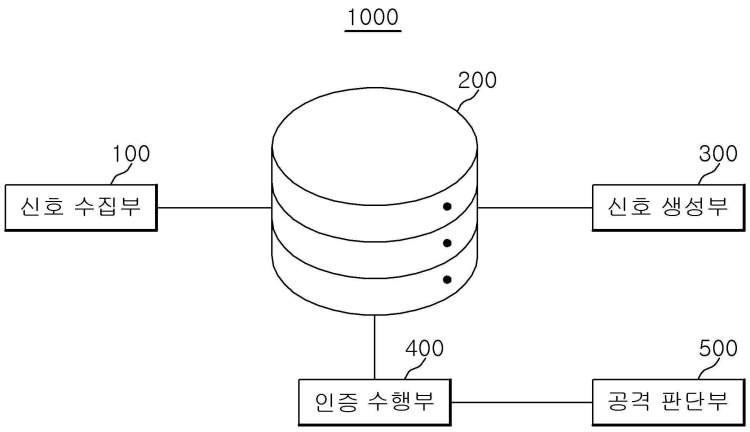
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **인체 통신을 이용한 인증 장치 및 인증 방법**

(57) 요 약

실시예의 인체 통신을 이용한 인증 장치는 사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 복수개 수집하는 신호 수집부와, 상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 신호 저장부와, 상기 저장부에 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 신호 생성부와, 상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하여 인증을 수행하는 인증 수행부와, 상기 인체로부터 출력되는 반응 신호의 측정 시간을 이용하여 외부의 공격 여부를 판단하는 공격 판단부를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/55 (2013.01)
H04B 13/005 (2013.01)

명 세 서

청구범위

청구항 1

사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 복수개 수집하는 신호 수집부;

상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 신호 저장부;

상기 저장부에 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 신호 생성부; 및

상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하여 인증을 수행하는 인증 수행부

를 포함하는 인체 통신을 이용한 인증 장치.

청구항 2

제1항에 있어서,

상기 인체로부터 출력되는 반응 신호의 측정 시간을 이용하여 외부의 공격 여부를 판단하는 공격 판단부를 더 포함하는 인체 통신을 이용한 인증 장치.

청구항 3

제2항에 있어서,

상기 공격 판단부는

상기 인체로부터 출력되는 반응 신호가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 있다고 판단하는 인체 통신을 이용한 인증 장치.

청구항 4

제1항에 있어서,

상기 신호 저장부는

사용자 별로 상기 제1 인증신호 및 상기 제1 반응신호를 저장하고,

상기 제1 반응신호를 미리 저장된 사용자의 제1 반응신호와 유사도를 비교하여 상기 사용자 별로 구분하여 저장하는 인체 통신을 이용한 인증 장치.

청구항 5

제4항에 있어서,

상기 신호 저장부는

상기 미리 저장된 상기 제1 인증신호 및 상기 제2 반응신호 중 일정 시간이 지난 상기 제1 인증신호 및 상기 제2 반응신호를 폐기하는 인체 통신을 이용한 인증 장치.

청구항 6

인체 통신을 이용한 인증 장치에서 수행되는 인증 방법에 있어서,

서로 다른 조건에서 사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 수집하는 단계;

상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계;

상기 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 단계; 및

상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하는 단계

를 포함하는 인체 통신을 이용한 인증 방법.

청구항 7

제6항에 있어서,

상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하는 단계 이후,

상기 인체로부터 출력되는 반응 신호가 측정되는 시간을 이용하여 외부의 공격 여부를 판단하는 단계를 더 포함하는 인체 통신을 이용한 인증 방법.

청구항 8

제7항에 있어서,

상기 외부의 공격 여부를 판단하는 단계에서,

상기 인체로부터 출력되는 반응 신호가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 있다고 판단하는 인체 통신을 이용한 인증 방법.

청구항 9

제6항에 있어서,

상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계에서,

사용자 별로 상기 제1 인증신호 및 상기 제1 반응신호를 저장하고,

상기 제1 반응신호를 미리 저장된 사용자의 제1 반응신호와 유사도를 비교하여 상기 사용자 별로 구분하여 저장하는 인체 통신을 이용한 인증 방법.

청구항 10

제9항에 있어서,

상기 미리 저장된 상기 제1 인증신호 및 상기 제2 반응신호 중 일정 시간이 지난 상기 제1 인증신호 및 상기 제2 반응신호를 폐기하는 인체 통신을 이용한 인증 방법.

발명의 설명

기 술 분 야

[0001] 실시예는 인체 통신을 이용한 인증 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 지문인식, 홍채인식 등으로 대표되는 생체인증 기술은 다른 인증 기술들에 비해 별도의 보관 및 암기가 불필요하며 분실우려가 없고 도용 및 양도가 불가능하다는 편리성이 있어 개발 속도가 빠르게 진행되고 있다.

[0003] 하지만, 생체인증 기술은 해킹의 가능성이 있기 때문에 영구적인 보안문제가 발생하는 등의 심각한 취약성을 가지고 있다. 즉, 지문, 홍채와 같이 외형적으로 드러나 있는 생체인증 도구의 경우, 물리적인 복제 가능성이 크다. 또한, 서버를 해킹하거나 서버로 전송되는 메시지를 탈취하여 인증에 필요한 생체 정보를 복원하는 방식으로 복제를 하는 것도 가능하다.

[0004] 이러한 보안 문제가 타 인증기술에도 동일하게 존재하지만 유독 생체인증 시스템에서 문제가 되는 이유는 생체정보의 불변성과 유일성 때문이다. 일례로, 일반 보안 시스템은 보안키를 탈취당했을 경우, 보안키를 변경하는 것으로 탈취당한 보안키의 유효성을 제거할 수 있으나, 지문이나 홍채와 같은 생체정보를 탈취당한 경우, 이에 대한 유효성 제거가 불가능하여 해당 생체 정보에 의한 인증이 근본적으로 불가능하다.

발명의 내용

해결하려는 과제

[0005] 상술한 문제점을 해결하기 위해, 실시예는 외형적으로 복제가 불가능하고, 데이터 복원을 통해 복제를 성공했다고 하더라도, 유효성 제거 및 리프로그래밍이 가능한 인증 장치 및 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0006] 실시예의 인체 통신을 이용한 인증 장치는 사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 복수개 수집하는 신호 수집부와, 상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 신호 저장부와, 상기 저장부에 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 신호 생성부와, 상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하여 인증을 수행하는 인증 수행부를 포함할 수 있다.

[0007] 상기 인체로부터 출력되는 반응 신호의 측정 시간을 이용하여 외부의 공격 여부를 판단하는 공격 판단부를 더 포함할 수 있다.

[0008] 상기 공격 판단부는 상기 인체로부터 출력되는 반응 신호가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 있다고 판단할 수 있다.

[0009] 상기 신호 저장부는 사용자 별로 상기 제1 인증신호 및 상기 제1 반응신호를 저장하고, 상기 제1 반응신호를 미리 저장된 사용자의 제1 반응신호와 유사도를 비교하여 상기 사용자 별로 구분하여 저장할 수 있다.

[0010] 상기 신호 저장부는 상기 미리 저장된 상기 제1 인증신호 및 상기 제2 반응 신호 중 일정 시간이 지난 상기 제1 인증신호 및 상기 제2 반응신호는 폐기할 수 있다.

[0011] 실시예에 따른 인체 통신을 이용한 인증 장치에서 수행되는 인증 방법은 서로 다른 조건에서 사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 수집하는 단계와, 상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계와, 상기 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 단계와, 상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하는 단계를 포함할 수 있다.

[0012] 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하는 단계 이후, 상기 인체로부터 출력되는 반응 신호가 측정되는 시간을 이용하여 외부의 공격 여부를 판단하는 단계를 더 포함할 수 있다.

[0013] 상기 외부의 공격 여부를 판단하는 단계에서, 상기 인체로부터 출력되는 반응 신호가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 있다고 판단할 수 있다.

[0014] 상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계에서, 사용자 별로 상기 제1 인증신호 및 상기 제1 반응신호를 저장하고, 상기 제1 반응신호를 미리 저장된 사용자의 제1 반응신호와 유사도를 비교하여 상기 사용자 별로 구분하여 저장할 수 있다.

[0015] 상기 미리 저장된 상기 제1 인증신호 및 상기 제2 반응신호 중 일정 시간이 지난 상기 제1 인증신호 및 상기 제2 반응신호는 폐기할 수 있다.

발명의 효과

[0016] 실시예는 복수의 인증 신호를 조합하여 새로운 인증 신호를 생성함으로써, 사용자 인증을 위한 보안 수준을 높일 수 있는 효과가 있다.

[0017] 또한, 실시예는 인증 신호를 복잡한 구조로 재생성함으로써, 외부 공격을 보다 효과적으로 탐지할 수 있는 효과

가 있다.

도면의 간단한 설명

[0018] 도 1은 실시예에 따른 인체 통신을 이용한 인증 장치를 나타낸 블록도이다.

도 2는 인체 통신의 예를 나타낸 도면이다.

도 3은 신호 송수신기가 다양한 공간에 설치되는 모습을 나타낸 도면이다.

도 4는 실시예에 따른 인증 장치의 신호 저장부를 나타낸 도면이다.

도 5는 신호 생성부의 동작을 나타낸 도면이다.

도 6 및 도 7은 인증 수행부의 동작을 나타낸 도면이다.

도 8은 공격 판단부의 동작을 나타낸 도면이다.

도 9는 실시예에 따른 인체 통신을 이용한 인증 장치를 이용하여 인증을 수행하는 방법을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 도면을 참조하여 실시예를 상세히 설명하기로 한다.

[0021] 도 1은 실시예에 따른 인체 통신을 이용한 인증 장치를 나타낸 블록도이고, 도 2는 인체 통신의 예를 나타낸 도면이고, 도 3은 신호 송수신기가 다양한 공간에 설치되는 모습을 나타낸 도면이고, 도 4는 실시예에 따른 인증 장치의 신호 저장부를 나타낸 도면이고, 도 5는 신호 생성부의 동작을 나타낸 도면이고, 도 6 및 도 7은 인증 수행부의 동작을 나타낸 도면이고, 도 8은 공격 판단부의 동작을 나타낸 도면이다.

[0022] 도 1 내지 도 3을 참조하면, 실시예에 따른 인체 통신을 이용한 인증 장치(1000)는 신호 수집부(100)를 포함할 수 있다.

[0023] 신호 수집부(100)는 인체 통신을 통해 신호를 수집할 수 있다. 도 2에 도시된 바와 같이, 인체 통신은 인체(10)로 입력된 전기 신호 예컨대, 제1 인증신호(AS1)와 상기 제1 인증신호(AS1)가 인체(10)를 거쳐 되돌아 출력되는 전기 신호 예컨대, 제1 반응신호(RS1) 간의 주파수 응답 특성을 표현하는 것을 의미할 수 있다. 제1 반응신호(RS1)는 인체의 크기, 근 밀도, 혈액량, 공격, 장기의 위치 등 개개인이 가지는 인체 내부의 복합적인 요인에 의해 결정되기 때문에 수학적 모델링이 어렵고 신체 변화에 따라 영속적이지 않다. 이에 인체 통신은 개개인을 효과적으로 구별할 수 있다.

[0024] 제1 반응신호(RS1)는 수학식 1에 의해 측정될 수 있다.

[0025] [수학식 1]

[0026] $y=Hx+n$ (여기서, y는 제2 반응신호 값이며, x는 제1 인증신호 값이며, H는 인체에 흐르는 전기 신호의 값이며, n은 임의의 상수를 의미함)

[0027] 신호 수집부(100)는 신호 송수신기(미도시)로부터 신호를 수집할 수 있다. 신호 송수신기는 사용자의 생활 공간에 다양하게 설치될 수 있다. 도 3에 도시된 바와 같이, 신호 송수신기는 각종 장치의 스위치 또는 차량의 운전대 등에 설치될 수 있으나, 이에 한정되지 않는다. 신호 송수신기는 사용자의 인체(10)에 제공하는 제1 인증신호(AS1) 및 제1 반응신호(RS1)를 수신하여 신호 수집부(100)로 전송할 수 있다. 여기서, 신호 송수신기에는 사용자의 인체(10)에 제1 인증신호(AS1)를 제공하기 위한 별도의 전기제공장치(미도시)를 포함할 수 있다.

[0028] 이로 인해 신호 수집부(100)는 서로 다른 조건에서의 사용자의 인체(10)에 제공하는 제1 인증신호(AS1) 및 인체(10)를 통해 출력된 제1 반응신호(RS1)를 복수개 수집할 수 있게 된다.

[0029] 도 1로 돌아가서, 실시예에 따른 인체 통신을 이용한 인증 장치(1000)는 신호 저장부(200)를 포함할 수 있다.

[0030] 신호 저장부(200)는 신호 수집부(100)로부터 수집된 복수의 제1 인증신호(AS1) 및 복수의 제1 반응신호(RS1)를 저장할 수 있다. 여기서, 신호 저장부(200)는 일예로 서버 또는 메모리일 수 있으나, 이에 한정되지 않는다. 신호 저장부(200)는 사용자 별로 구분하여 신호를 저장할 수 있다.

[0031] 도 4에 도시된 바와 같이, 신호 저장부(200)는 복수의 저장부를 포함할 수 있다. 제1 저장부(210)에는 A 사용자에 대한 복수의 제1 인증신호 및 복수의 제1 반응신호가 저장될 수 있다. 제2 저장부(230)에는 B 사용자에 대한 복수의 제1 인증신호 및 복수의 제1 반응신호가 저장될 수 있다. 제3 저장부(250)에는 C 사용자에 대한 복수의 제1 인증신호 및 복수의 제1 반응신호가 저장될 수 있다. 여기서, 저장부(200)는 3개로 한정되지 않으며, 4개 이상으로 구비될 수도 있다.

[0032] 신호 저장부(200)는 제1 인증신호(AS1) 및 제1 반응신호(RS1)가 수신되면, 제1 반응신호(RS1)를 제1 저장부 내지 제3 저장부(210, 230, 250)에 미리 저장된 제1 반응신호(RS1)들과 유사도를 비교하고, 유사도가 임계값 이상인 제1 인증신호(AS1) 및 제1 반응신호(RS1)를 저장할 수 있다.

[0033] 신호 저장부(200)에 저장된 제1 인증신호(AS1) 및 제1 반응신호(RS1)는 일정 시간이 지나면 폐기될 수 있다. 즉, 인체(10)는 시간이 지남에 따라 천천히 변화하기 때문에 너무 오래된 신호는 현재의 신호와 다를 수 있기 때문에 일정 시간이 지난 신호는 폐기될 수 있다.

[0034] 도 1로 돌아가서, 실시예에 따른 인체 통신을 이용한 인증 장치(1000)는 신호 생성부(300)를 포함할 수 있다.

[0035] 신호 생성부(300)는 신호 저장부(200)에 저장된 복수의 제1 인증신호(AS1)를 이용하여 제2 인증신호를 생성할 수 있다. 예컨대, 복수의 제1 인증신호(AS1)들을 조합하여 제2 인증신호를 생성할 수 있다.

[0036] 도 5에 도시된 바와 같이, 신호 저장부(200) 예컨대, 제1 저장부(210)에는 동일한 사용자에 대한 서로 다른 조건에서의 복수의 제1 인증신호(AS1)와 복수의 제1 반응신호(RS1)들이 저장될 수 있다. 신호 생성부(300)는 복수의 제1 인증신호(AS1)를 이용하여 제2 인증신호(AS2)를 생성할 수 있다.

[0037] 예컨대, 신호 생성부(300)는 복수의 제1 인증신호(AS1) 중 A,B,C,D 신호를 이용하여 제2 인증신호(AS2)를 생성할 수 있다. 신호 생성부(300)는 제1 인증신호(AS1)에 대응하는 복수의 제1 반응신호(RS1) 중 A',B',C',D' 신호를 이용하여 제2 반응신호(RS2)를 생성할 수 있다.

[0038] 신호 생성부(300)는 복수의 제1 인증신호(AS1) 중 A,C 신호를 이용하여 제2 인증신호(AS2)를 생성할 수 있다. 신호 생성부(300)는 제1 인증신호(AS1)에 대응하는 복수의 제1 반응신호(RS1) 중 A',C' 신호를 이용하여 제2 반응신호(RS2)를 생성할 수 있다.

[0039] 신호 생성부(300)는 복수의 제1 인증신호(AS1) 중 A,C,A 신호를 이용하여 제2 인증신호(AS2)를 생성할 수 있다. 신호 생성부(300)는 제1 인증신호(AS1)에 대응하는 복수의 제1 반응신호(RS1) 중 A',C',A' 신호를 이용하여 제2 반응신호(RS2)를 생성할 수 있다.

[0040] 상기와 같이, 제2 인증신호(AS2)를 조합하는 방식은 이에 한정되지 않으며 다양한 조건을 이용하여 생성할 수 있다.

[0041] 도 1로 돌아가서, 실시예에 따른 인체 통신을 이용한 인증 장치(1000)는 인증 수행부(400)를 포함할 수 있다. 여기서, 인증 수행부(400)는 휴대용 단말, 차량 및 출입문과 같은 인증 단말에 설치될 수 있으며, 이와 다르게, 인증 단말과는 별도로 구비되어 인증 단말에 제2 인증신호(RS2)만을 제공해 줄 수 있다.

[0042] 도 6에 도시된 바와 같이, 인증 수행부(400)는 사용자가 인증 요청을 할 경우, 사용자의 인체(10)에 제2 인증신호(AS2)를 제공할 수 있다. 도 7에 도시된 바와 같이, 인증 수행부(400)는 사용자의 인체(10)를 통해 출력되는 반응 신호(S)를 제2 인증신호(AS2)에 대응하는 제2 반응신호(RS2)와 비교하여 인증을 수행할 수 있다. 여기서, 반응 신호(S)와 제2 반응신호(RS2)의 유사도가 미리 정해진 임계값 보다 크면 인증을 수행할 수 있다.

[0043] 도 1로 돌아가서, 실시예에 따른 인체 통신을 이용한 인증 장치(1000)는 공격 판단부(500)를 포함할 수 있다.

[0044] 공격 판단부(500)는 인체(10)로부터 출력되는 반응 신호(S)의 측정 시간을 이용하여 외부의 공격 여부를 판단할 수 있다.

[0045] 도 8에 도시된 바와 같이, 외부 공격이 발생된 경우, 인체(10)에 제공되는 제2 인증신호(AS2) 또는 제2 반응신호(RS2)의 패턴을 파악하기 위해 상당한 연산 시간이 필요하게 된다. 통상 외부 공격이 없을 경우, 제2 인증신호(AS2)는 빛의 속도로 전파되기 때문에 짧은 시간 안에 인증 과정이 완료된다. 반면, 외부 공격이 발생될 경우, 제2 인증신호(AS2) 또는 제2 반응신호(RS2) 패턴을 파악하기 위한 연산을 위한 시간이 소요된다.

[0046] 따라서, 공격 판단부(500)는 인체(10)로부터 출력되는 반응 신호(S)가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 발생된 것으로 판단할 수 있다. 이로 인해 공격 판단부(500)는 외부 공격이 발생되었다고 판단하여

인증을 중단할 수 있다.

[0047] 실시예는 복수의 인증 신호를 조합하여 새로운 인증 신호를 생성함으로써, 사용자 인증을 위한 보안 수준을 높일 수 있는 효과가 있다.

[0048] 또한, 실시예는 인증 신호를 복잡한 구조로 재생성함으로써, 외부 공격을 보다 효과적으로 탐지할 수 있는 효과가 있다.

[0049] 이하에서는 실시예에 따른 인증 장치를 이용한 인증 방법에 대해 살펴본다. 도 9는 실시예에 따른 인체 통신을 이용한 인증 장치를 이용하여 인증을 수행하는 방법을 나타낸 순서도이다.

[0050] 실시예에 따른 인증 방법은 서로 다른 조건에서 사용자의 인체에 제공하는 제1 인증신호 및 상기 인체를 통해 출력된 제1 반응신호를 수집하는 단계(S100)와, 상기 수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계(S200)와, 상기 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고, 상기 제2 인증신호에 대응하는 제2 반응신호를 생성하는 단계(S300)와, 상기 사용자가 인증 요청을 할 경우, 상기 사용자의 인체에 상기 제2 인증신호를 제공하고, 상기 사용자의 인체로부터 출력되는 반응 신호를 상기 제2 반응신호와 비교하여 인증을 수행하는 단계(S400)와, 상기 인체로부터 출력되는 반응 신호가 측정되는 시간을 이용하여 외부의 공격 여부를 판단하는 단계(S500)를 포함할 수 있다.

[0051] 제1 인증신호 및 제1 반응신호를 수집하는 단계(S100)는 신호 수집부에서 수행될 수 있다.

[0052] 제1 인증신호 및 제1 반응신호를 수집하는 단계(S100)는 인체 통신을 통한 신호를 수집할 수 있다. 제1 인증신호 및 제1 반응신호를 수집하는 단계(S100)는 서로 다른 조건에서의 사용자의 인체에 제공하는 제1 인증신호 및 인체를 통해 출력된 제1 반응신호를 수집할 수 있다.

[0053] 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계(S200)는 신호 저장부에서 수행될 수 있다. 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계(S200)는 사용자 별로 구분하여 제1 인증신호와 제1 반응신호를 저장할 수 있다.

[0054] 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계(S200)는 제1 인증신호 및 제1 반응신호가 수신되면, 제1 반응신호를 미리 저장된 제1 반응신호들과 유사도를 비교하고, 유사도가 임계값 이상인 제1 인증신호 및 제1 반응신호를 저장할 수 있다.

[0055] 제2 인증신호 및 제2 반응신호를 생성하는 단계(S300)는 신호 생성부에서 수행될 수 있다.

[0056] 제2 인증신호 및 제2 반응신호를 생성하는 단계(S300)는 복수의 제1 인증신호들을 조합하여 제2 인증신호를 생성할 수 있다. 또한, 복수의 제1 인증신호들에 대응되는 제1 반응신호들을 조합하여 제2 반응신호를 생성할 수 있다.

[0057] 인증을 수행하는 단계(S400)는 인증 수행부에서 수행될 수 있다.

[0058] 인증을 수행하는 단계(S400)는 사용자가 인증 요청을 할 경우, 사용자의 인체에 제2 인증신호를 제공할 수 있다. 인증을 수행하는 단계(S400)는 사용자의 인체를 통해 출력되는 반응 신호를 제2 인증신호에 대응하는 제2 반응신호와 비교하여 인증을 수행할 수 있다.

[0059] 외부의 공격 여부를 판단하는 단계(S500)는 공격 판단부에서 수행될 수 있다.

[0060] 외부의 공격 여부를 판단하는 단계(S500)는 인체로부터 출력되는 반응 신호의 측정 시간을 이용하여 외부의 공격 여부를 판단할 수 있다. 외부의 공격 여부를 판단하는 단계(S500)는 인체로부터 출력되는 반응신호가 측정되는 시간이 제1 기준값 보다 길면 외부 공격이 발생된 것으로 판단할 수 있다. 외부 공격이 발생되었다고 판단되면, 인증을 중단할 수 있다.

[0061] 상기에서는 도면 및 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 실시예의 기술적 사상으로부터 벗어나지 않는 범위 내에서 실시예는 다양하게 수정 및 변경시킬 수 있음은 이해할 수 있을 것이다.

부호의 설명

[0062] 100: 신호 수집부

200: 신호 저장부

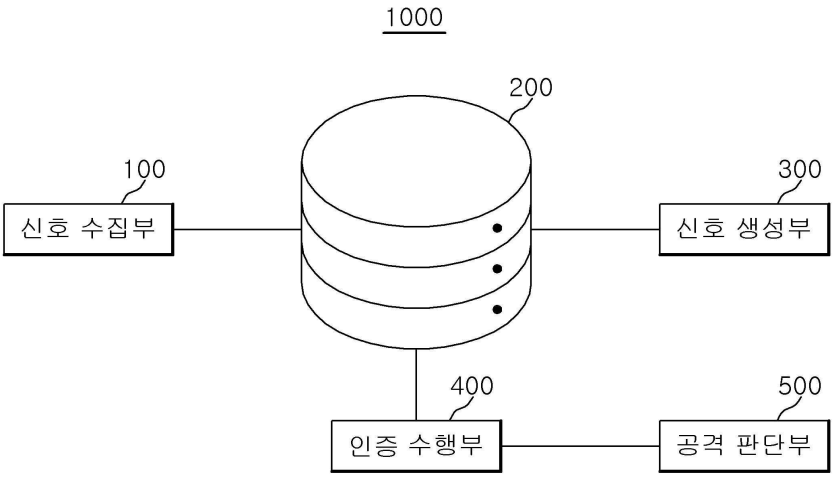
300: 신호 생성부

400: 인증 수행부

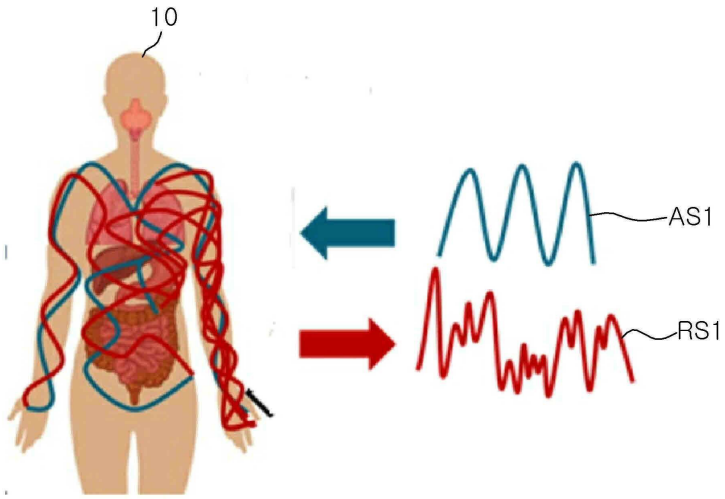
500: 공격 판단부

도면

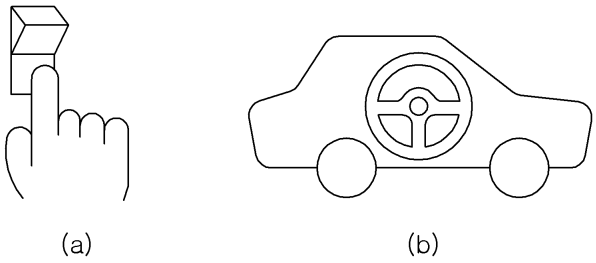
도면1



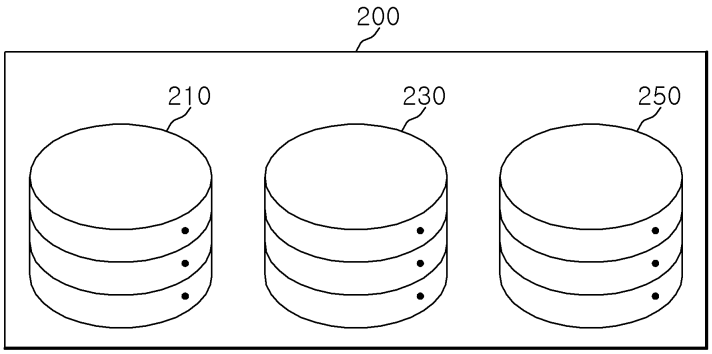
도면2



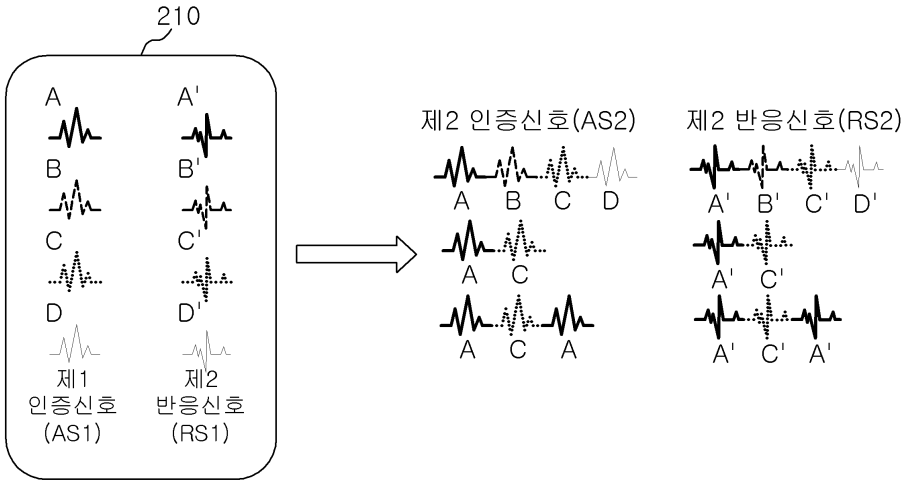
도면3


(a)
(b)

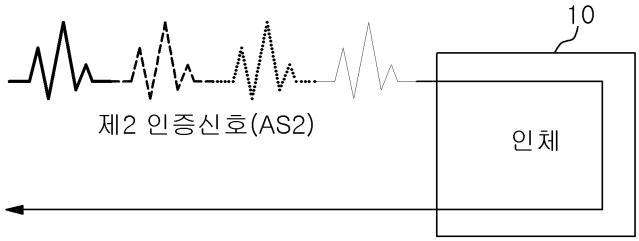
도면4


200
210
230
250

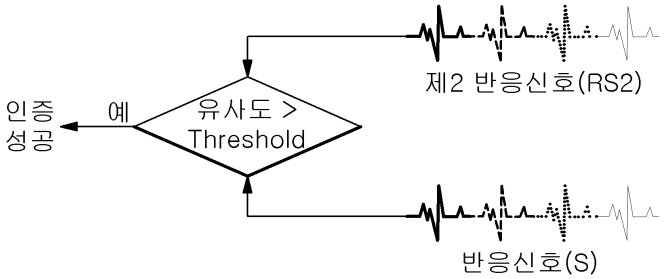
도면5


210
A
A'
B
B'
C
C'
D
D'
제1
인증신호
(AS1)
제2
반응신호
(RS1)
제2 인증신호(AS2)
A B C D
A C
A C A
제2 반응신호(RS2)
A' B' C' D'
A' C'
A' C' A'

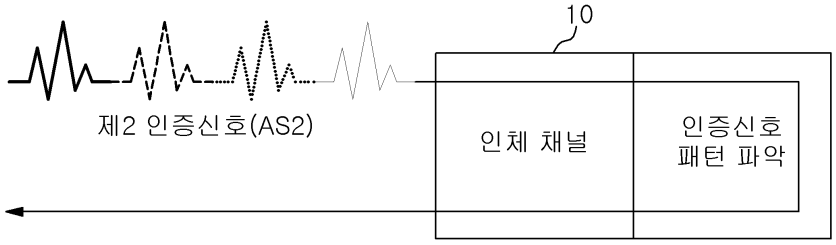
도면6


10
제2 인증신호(AS2)
인체

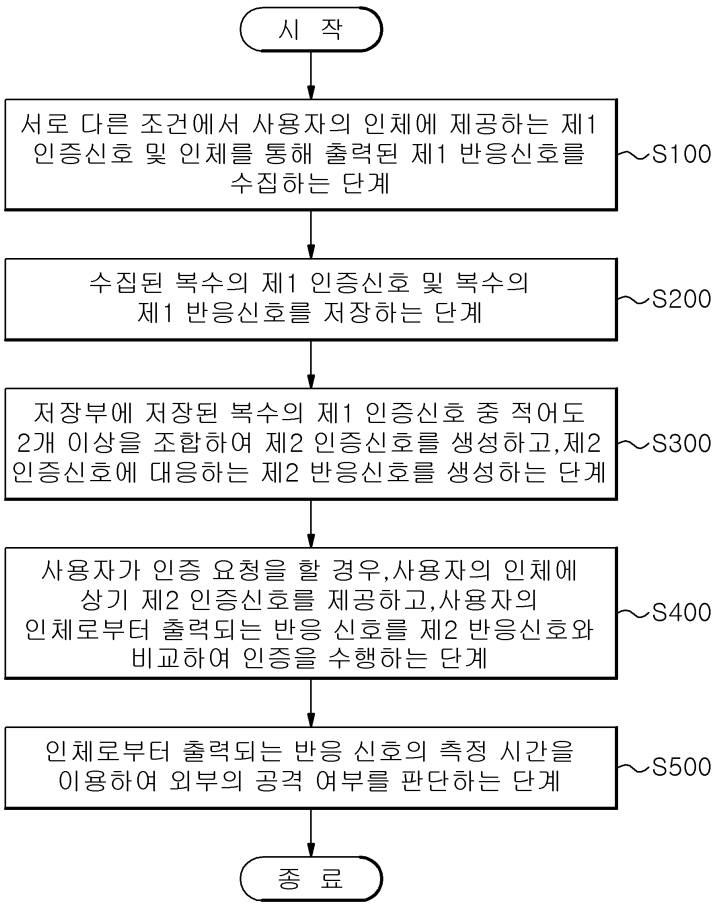
도면7


제2 반응신호(RS2)
인증
성공
예
유사도 >
Threshold
반응신호(S)

도면8


10
제2 인증신호(AS2)
인체 채널
인증신호
패턴 파악

도면9


시 작
서로 다른 조건에서 사용자의 인체에 제공하는 제1 인증신호 및 인체를 통해 출력된 제1 반응신호를 수집하는 단계
S100
수집된 복수의 제1 인증신호 및 복수의 제1 반응신호를 저장하는 단계
S200
저장부에 저장된 복수의 제1 인증신호 중 적어도 2개 이상을 조합하여 제2 인증신호를 생성하고,제2 인증신호에 대응하는 제2 반응신호를 생성하는 단계
S300
사용자가 인증 요청을 할 경우,사용자의 인체에 상기 제2 인증신호를 제공하고,사용자의 인체로부터 출력되는 반응 신호를 제2 반응신호와 비교하여 인증을 수행하는 단계
S400
인체로부터 출력되는 반응 신호의 측정 시간을 이용하여 외부의 공격 여부를 판단하는 단계
S500
종 료