(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년03월23일
(11) 등록번호 10-2377147
(24) 등록일자 2022년03월17일

(51) 국제특허분류(Int. Cl.)
G06K 19/07 (2006.01)
(52) CPC특허분류
G06K 19/0718 (2013.01)
G06K 19/0719 (2013.01)
(21) 출원번호 10-2018-7026708
(22) 출원일자(국제) 2017년03월01일
심사청구일자 2020년02월25일
(85) 번역문제출일자 2018년09월14일
(65) 공개번호 10-2018-0118152
(43) 공개일자 2018년10월30일
(86) 국제출원번호 PCT/EP2017/054778
(87) 국제공개번호 WO 2017/149015
국제공개일자 2017년09월08일
(30) 우선권주장
1603602.2 2016년03월02일 영국(GB)
(56) 선행기술조사문헌
US20130129162 A1*
US20140101737 A1*
WO2015034552 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
즈와이프 에이에스
노르웨이 0151 오슬로 레이드허스가타 24
(72) 발명자
홈보르스타드, 킴 크리스티안
노르웨이 0194 오슬로 소렝카이아 115
(74) 대리인
특허법인 무한

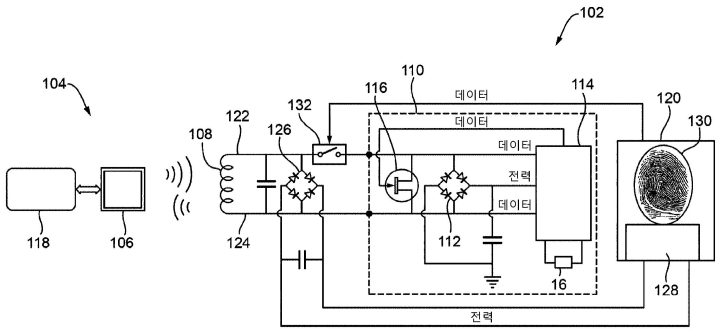
전체 청구항 수 : 총 18 항 심사관 : 하은주

(54) 발명의 명칭 **지문 인증 가능 장치**

(57) 요 약

지문 인증 가능 장치(102)는 사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서(130), 및 상기 장치(102)를 제어하기 위한 제어 시스템(114, 128)을 포함한다. 상기 제어 시스템(114, 128)은 인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하도록 구성되고, 상기 제어 시스템(114, 128)은 지문 실패 피쳐를 더 포함하고, 상기 지문 실패 피쳐에서, 적어도 부분적으로 상기 지문 인증을 대체하기 위해 비-지문 인증이 동작할 수 있어서, 사용자가 상기 비-지문 인증을 통해 식별될 때, 상기 제어 시스템(114, 128)이 상기 장치(102)의 하나 이상의 기능 중 적어도 일부에 대한 액세스를 제공하도록 구성된다. 상기 비-지문 인증은 상기 사용자에 의한 상기 지문 인증 가능 장치(102)와의 인터랙션을 요구하고, 상기 인터랙션은 상기 지문 센서(130)를 통해 검출된 하나 이상의 동작을 포함한다.

대 표 도



명 세 서

청구범위

청구항 1

지문 인증 가능 장치에 있어서,

사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서, 및

상기 장치를 제어하기 위한 제어 시스템

을 포함하고,

상기 제어 시스템은,

인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하도록 구성되고,

상기 제어 시스템은,

사용자가 비-지문 인증을 통해 식별되는 경우, 상기 비-지문 인증이 상기 지문 인증을 대체하도록 동작하여, 상기 제어 시스템이 상기 장치의 상기 하나 이상의 기능에 대한 액세스를 제공하도록 구성되는 지문 실패 피쳐를 포함하고,

상기 비-지문 인증은,

상기 사용자에 의한 상기 지문 인증 가능 장치와의 인터랙션을 요구하고,

상기 인터랙션은,

상기 지문 센서를 통해 검출된 하나 이상의 동작을 포함하고,

상기 지문 인증 가능 장치는 스마트카드인,

지문 인증 가능 장치.

청구항 2

제1항에 있어서,

상기 지문 센서를 통해 검출된 상기 동작은,

상기 센서와의 정적인 접촉,

상기 센서와의 동적인 접촉,

상기 센서와의 접촉의 시간 기간,

상기 센서와의 접촉의 이동의 방향,

상기 센서와의 접촉의 수, 또는

상기 센서와의 접촉이 없는 시간 기간

중 하나 이상을 포함하는지문 인증 가능 장치.

청구항 3

제1항에 있어서,

상기 비-지문 인증은,

서로 다른 동작의 조합을 요구하는

지문 인증 가능 장치.

청구항 4

제1항에 있어서,

상기 동작은,

회전 접촉 또는 원형 이동과 같은 상기 사용자에 의해 정의된 더 복합적인 이동 또는 평행 및/또는 수직 이동을 갖는 시퀀스를 포함하는

지문 인증 가능 장치.

청구항 5

제1항에 있어서,

상기 지문 센서에 의해 검출된 상기 동작은,

하나 이상의 접촉의 시간 기간, 접촉의 수 및/또는 접촉 사이의 간격을 포함하는

지문 인증 가능 장치.

청구항 6

제1항에 있어서,

상기 제어 시스템은,

상기 지문 센서를 통해 지문 데이터를 획득함으로써 인증된 사용자를 등록하도록 구성되는

지문 인증 가능 장치.

청구항 7

제1항에 있어서,

상기 제어 시스템은,

사용자가 상기 지문 센서를 통해 상기 사용자의 지문을 등록할 수 있는 등록 모드를 가지며, 등록 중에 생성된 상기 지문 데이터는 메모리에 저장되고,

상기 제어 시스템은,

지문 등록에 추가로 및/또는 상기 사용자 등록에 실패한 경우에, 비-지문 인증 코드의 등록을 위해 상기 사용자를 프롬프트하도록 구성되는

지문 인증 가능 장치.

청구항 8

제1항에 있어서,

상기 장치는,

지문 인증 가능한 RFID 카드인 지문 인증 가능 장치.

청구항 9

제1항에 있어서,

상기 장치는,

단일-목적 장치인 지문 인증 가능 장치.

청구항 10

제1항에 있어서,

상기 비-지문 인증은,

상기 지문 센서와의 인터랙션, 및

하나 이상의 버튼, 정전식 감응 센서 또는 가속도계와 같은 하나 이상의 추가 센서와의 인터랙션

을 포함하는 지문 인증 가능 장치.

청구항 11

제1항에 있어서,

상기 장치는,

상기 장치의 이동을 감지하기 위한 가속도계

를 포함하며,

상기 제어 시스템은,

상기 가속도계의 출력에 기초하여 상기 장치의 이동을 식별하도록 구성되고,

상기 비-지문 인증은,

상기 가속도계에 의해 감지된 이동과 함께 상기 지문 센서를 통해 검출된 하나 이상의 동작의 조합을 포함하는

지문 인증 가능 장치.

청구항 12

제1항에 있어서,

상기 지문 센서를 통해 검출된 동작은,

상기 장치의 다수의 작동 모드 중 서로 다른 모드 사이를 전환하도록 상기 제어 시스템을 프롬프트 할 수 있는

지문 인증 가능 장치.

청구항 13

지문 인증 가능 장치를 제어하기 위한 방법에 있어서,

상기 지문 인증 가능 장치는,

사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서, 및

상기 장치를 제어하기 위한 제어 시스템

을 포함하고,

상기 지문 인증 가능 장치는 스마트카드이고,

상기 방법은,

인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하는 단계; 및

비-지문 인증이 상기 지문 인증을 대체하도록 동작하는 상기 제어 시스템의 지문 실패 피처의 일부로서, 사용자가 상기 비-지문 인증을 통해 식별되는 경우, 상기 장치의 상기 하나 이상의 기능에 대한 액세스를 대안적으로 또는 추가적으로 제공하는 단계

를 포함하고,

상기 비-지문 인증은 상기 사용자에 의한 상기 지문 인증 가능 장치와의 인터랙션을 요구하고, 상기 인터랙션은 상기 지문 센서를 통해 검출된 하나 이상의 동작을 포함하는

방법.

청구항 14

제13항에 있어서,

제1항 내지 제12항 중 어느 한 항의 상기 장치를 사용하는 단계

를 포함하는 방법.

청구항 15

제13항에 있어서,

지문 인증에 사용하기 위한 지문 데이터를 사용자가 제공하지 않거나 제공할 수 없는 경우, 상기 지문 실패 피처가 이용되는

방법.

청구항 16

제13항에 있어서,

등록된 사용자의 지문 인증이 성공하지 않는 경우, 상기 지문 실패 피처가 이용되는

방법.

청구항 17

컴퓨터 판독가능 매체에 저장된 컴퓨터 프로그램에 있어서,

제1항 내지 제12항 중 어느 한 항에 따른 지문 인증 가능 장치의 제어 시스템에서 실행될 때, 상기 제어 시스템이,

인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하고; 및

비-지문 인증이 상기 지문 인증을 대체하도록 동작하는 상기 제어 시스템의 지문 실패 피처의 일부로서, 사용자가 상기 비-지문 인증을 통해 식별되는 경우, 상기 장치의 상기 하나 이상의 기능에 대한 액세스를 대안적으로 또는 추가적으로 제공하도록 하는

명령어를 포함하고,

상기 비-지문 인증은 상기 사용자에 의한 지문 인증 가능 장치와의 인터랙션을 요구하고, 상기 인터랙션은 상기 지문 센서를 통해 검출된 하나 이상의 동작을 포함하는

컴퓨터 판독가능 매체에 저장된 컴퓨터 프로그램.

청구항 18

지문 실패 피처를 제공하기 위하여 지문 인증 가능 장치를 구성하는 방법에 있어서,

상기 지문 인증 가능 장치는,

사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서, 및

상기 장치를 제어하기 위한 제어 시스템

을 포함하고,

상기 지문 인증 가능 장치는 스마트카드이고,

상기 방법은,

상기 지문 인증 가능 장치에 제17항에 따른 컴퓨터 프로그램 제품을 설치하는 단계

를 포함하는 방법.

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

발명의 설명

기 술 분 야

본 발명은 지문 인증 가능 장치 및 지문 인증 가능 장치를 제어하기 위한 방법에 관한 것이다.

배 경 기 술

스마트카드(smartcards)와 같은 지문 인증 장치는 점차 널리 사용되고 있다. 생체 인식 인증(biometric authorisation)이 제안된 스마트카드에는 액세스 카드(access cards), 신용 카드, 직불 카드, 선불 카드, 로얄티 카드(loyalty cards), 신원 카드, 암호 카드 등을 포함한다. 스마트카드는 데이터를 저장하고 사용자 및/또는 외부 장치(예를 들어, RFID와 같은 비접촉 기술)를 통해 인터랙트(interact) 할 수 있는 전자 카드다. 이 카드는 센서와 인터랙트하여 액세스를 허용하고 거래를 승인하는 등등을 위해 정보를 교환할 수 있다. 지문 인증과 같은 생체 인식 인증을 사용하는 다른 장치도 공지되어 있으며, 컴퓨터 메모리 장치, 빌딩 액세스 제어 장치, 군사 기술, 차량 등을 포함한다.

몇몇 경우들에서, 지문 인증은 실패하거나 불가능할 수 있다. 예를 들어, 사용자의 지문이 부상에 의해 손상되거나, 커버될(covered) 수 있다. 또한, 센서는 손상되거나 작동하지 않을 수 있다. 지문 센서로 발생할 수 있는 또 다른 상황은 등록 실패이다. 이는 일부 또는 모든 센서를 사용하여 어떤 이유로든 지문을 등록할 수 없는 지문을 가진 소수의 인구가 가지고 있는 근본적인 문제이며, 손가락이 없거나 손상된 사람의 경우에도 발생한다. 또한, 일부 사용자는 지문 세부 정보를 기록하지 않으려 한다. 기존의 지문 인증 장치에서는 이것이 중대한 문제를 나타내며, 종종 일부 사용자를 위해 대안적인 장치가 제공되어야 한다는 것을 의미한다.

발명의 내용

해결하려는 과제

과제의 해결 수단

제1 측면으로 보면, 본 발명은 지문 인증 가능 장치(fingerprint authorizable device)를 제공하며, 사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서(fingerprint sensor), 및 상기 장치를 제어하기 위한 제어 시스템(control system)을 포함하고, 상기 제어 시스템은, 인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하도록 구성되고, 상기 제어 시스템은, 지문 실패 피쳐(finterprint failure feature)를 포함하고, 상기 지문 실패 피쳐에서, 적어도 부분적으로 상기 지문 인증을 대체하기 위해 비-지문 인증(non-fingerprint authorization)이 동작(act)할 수 있어서, 사용자가 상기 비-지문 인증을 통해 식별될 때, 상기 제어 시스템이 상기 장치의 하나 이상의 기능 중 적어도 일부에 대한 액세스를 제공하도록 구성되고, 상기 비-지문 인증은 상기 사용자에 의한 상기 지문 인증 가능 장치와의 인터랙션(interaction)을 요구하고, 상기 인터랙션은 상기 지문 센서를 통해 검출된 하나 이상의 동작(action)을 포함한다.

따라서, 이 측면의 지문 인증 가능 장치로 지문 인증에 등록할 수 없는 사용자는 비-지문 인증을 통해 장치의 일부 또는 모든 피쳐(features)를 여전히 사용할 수 있다. 또한, 비-지문 인증은, 예를 들어 등록된 지문에 대

한 손상 또는 액세스를 막는 부상으로 인해 등록된 사용자가 지문 인증을 제공할 수 없을 때 장치를 계속 사용할 수 있는 방법을 제공한다. 또한, 위에서 언급한 것처럼, 일부 사용자는 지문을 통해 등록하는 것을 원하지 않을 수 있으며, 이 피쳐는 해당 사용자가 순전히(purely) 비-지문 인증을 기반으로 장치를 사용할 수 있으며, 동시에 장치 및 인증 프로세스와의 인터랙션을 위한 입력으로서 지문 센서를 여전히 사용할 수 있다. 지문 센서는 비-지문 인증 프로세스(fingerprint authorisation process)의 일부 또는 전부에 사용되며, 이는 추가 센서를 장치에 추가할 필요 없이 제안된 비-지문 인증은 수행될 수 있음을 의미하지만, 다른 센서가 있는 경우, 아래에 설명된 바와 같이 활용될 수 있다. 등록 실패 피쳐를 허용하는 수정은 순전히 장치의 제어 시스템에 대한 조정에 기반하여 구현될 수 있으며, 이는 유리하게는 일부 경우에서는 순전히 소프트웨어 수정일 수 있다.

상기 지문 센서를 통해 검출된 상기 동작은 상기 센서와의 정적인 접촉(stationary contact), 상기 센서와의 동적인 접촉(moving contact), 상기 센서와의 접촉의 시간 기간(time period), 상기 센서와의 접촉의 이동의 방향(direction of movement), 상기 센서와의 접촉의 수(number of contacts), 또는 상기 센서와의 접촉이 없는 시간 기간(즉, 접촉 사이의 시간 기간) 중 하나 이상을 포함할 수 있다. 바람직하게는, 상기 비-지문 인증은 서로 다른 동작의 조합을 요구하며, 이는 다른 입력 또는 센서를 통해 적어도 하나의 동작과 조합하여 상기 지문 센서에서의 적어도 하나의 동작 및/또는 지문 센서에서의 동작의 시퀀스(sequence)를 포함할 수 있다.

상기 접촉은 상기 장치의 지문 센서를 통해 검출 가능한 임의의 접촉일 수 있다. 상기 지문 센서의 특성(nature)은 피부와의 접촉을 식별하도록 구성되어 있어 접촉이 피부의 접촉일 수 있음을 의미한다(예를 들어, 손가락 끝(fingertip) 또는 엄지 손가락 끝(thumbtip)과의 접촉). 사용자는 어떤 이유로 등록될 수 없는 지문 특성(fingerprint characteristics)을 가질 수 있거나, 지문을 등록하지 않기로 결정했을 수 있으므로, 지문 센서는 지문 인증을 가능하게 하기 위한 접촉에 대한 정보의 충분한 수준을 수집하는 데 사용되지 않는다는 사실에 의해, 비-지문 인증 동안 사용되는 지문 센서와의 인터랙션은 지문 인증 동안의 인터랙션과 구분될 수 있다.

지문 센서에 의해 검출된 정적인 접촉의 형태의 동작은 접촉의 부재와는 달리 접촉의 존재의 검출을 포함할 수 있다. 대안적으로, 지문 센서에 의해 검출된 동작은 2개의 서로 다른 접촉 사이의 구별을 가능하게 하는 접촉의 특성의 검출을 포함할 수 있지만(예를 들어, 한 사람의 엄지 손가락 접촉과 다른 사람의 엄지 손가락 접촉 사이의 차이), 전체 지문 등록을 위해서는 충분히 상세하거나 복잡하지 않다. 이러한 특성은 등록된 사용자의 지문 데이터와 동일한 방식으로 저장될 수 있다.

지문 센서에 의해 검출된 동적인 접촉의 형태의 동작은 이동의 방향 및/또는 이동의 속도의 검출을 포함할 수 있다. 방향은 장치의 하나 이상의 축에 관하여 식별될 수 있다. 예를 들어, 스마트 카드의 경우, 제어 시스템은 카드의 긴 변(long side)과 평행하게 이동하는 접촉과 카드의 짧은 변(short side)과 평행하게 이동하는 접촉을 구별하도록 구성될 수 있다. 동작은 회전 접촉(rotating contact) 또는 원형 이동(circular movement)과 같은, 상기 사용자에 의해 정의된 더 복합적인 이동(more complex movements) 또는 평행(parallel) 및/또는 수직(perpendicular) 이동을 갖는 시퀀스(sequence)를 포함할 수 있다.

상기 지문 센서가 단순히 접촉의 존재를 검출하는데 또는 더 복합적인 특성을 검출하는데 사용되는지에 대해, 상기 지문 센서에 의해 검출된 상기 동작은 하나 이상의 접촉의 시간 기간, 접촉의 수 및/또는 접촉 사이의 간격(spacing)을 포함할 수 있으며, 예를 들어 모스 부호(Morse code)와 같은 코드와 유사하다. 따라서, 비-지문 인증을 위해 요구되는 상기 장치와의 인터랙션은 상기 센서와의 정적인 또는 동적인 접촉의 시퀀스에 의해 입력된 코드를 포함하거나 구성할 수 있다.

상기 비-지문 인증이 상기 장치의 하나 이상의 기능에 액세스하는데 사용될 때, 사용자는 지문 인증을 통해 액세스 할 수 있는 모든 기능에 대한 액세스가 허용되거나, 사용자는 이 기능에 대한 제한된 액세스만 받을 수 있다. 하나의 가능한 구현예에서, 등록 실패의 경우, 즉 지문 인증을 위해 이용 가능한 지문 데이터가 없는 경우에서, 사용자는 비-지문 인증을 사용하여 상기 장치의 하나 이상의 기능에 대한 완전한 액세스가 허용될 수 있다. 그러면, 보안이 저하될 수는 있지만, 등록할 수 없거나 등록하지 않는(unwilling) 사람에 의해 장치가 완전히 사용될 수 있다. 지문 데이터가 있지만 어떤 이유로 사용자가 지문 인증 프로세스를 완료할 수 없는 경우, 예를 들어, 손가락 부상의 경우, 장치는 비-지문 인증에 응답하여 부분 액세스(partial access)만을 허용하도록 구성될 수 있다. 이는 일반적으로 지문 승인을 사용하는 사용자가 일시적으로 지문 인증을 제공할 수 없거나 비-지문 인증을 사용하기로 결정할 때, 장치의 제한된 사용을 허용할 수 있다. 예를 들어, 장치가 금융 거래를 위한 스마트카드 사용인 경우, 비-지문 인증은 지불의 크기의 한도로 지불을 허용할 수 있지만, 지문 인증은 한도 없이 또는 더 큰 한도로 지불을 허용할 수 있다.

인증된 사용자는 임의로 다른 장치를 통해 선택적으로 간접적으로, 그러나 바람직하게는 지문 센서를 통해 장치

상에 직접적으로 지문을 초기에 장치에 등록할 수 있으며, 일반적으로 장치의 일부 또는 모든 사용을 인증하기 위하여 지문 센서에 손가락 또는 엄지 손가락을 위치시키도록 요구될 수 있다. 제어 시스템에서의 지문 매칭 알고리즘(fingerprint matching algorithm)은 등록된 사용자와 지문 센서에 의해 감지된 지문 사이의 지문 매칭을 식별하는데 사용될 수 있다. 지문을 매칭하는데 실패한 경우, 제어 시스템은 비-지문 인증을 위한 프롬프트(prompt)를 발행(issue)할 수 있다.

예를 들어 지문 템플릿(fingerprint template) 등등에 의한, 비-지문 인증 및/또는 지문을 통해 사용자를 식별하기 위해 사용된 데이터를 추출하는 것이 불가능하게 장치를 구성하는 것이 바람직하다. 장치의 외부에서 데이터의 이러한 유형의 전송은 장치의 보안에 대한 가장 큰 위험 중 하나로 간주된다.

장치의 외부에서 지문 데이터의 통신할 필요가 없도록 하기 위해, 상기 장치는 자체-등록(self-enrol)할 수 있으며, 즉, 제어 시스템은 지문 센서를 통해 지문 데이터를 획득함으로써 인증된 사용자를 등록하도록 구성될 수 있다. 또한, 동일한 기하학(geometry)을 구비한 동일한 센서가 지문 인증과 같이 등록을 위해 사용된다는 사실로부터 이점이 있다. 서로 다른 장치의 서로 다른 센서가 등록에 사용되는 경우와 비교하여, 지문 데이터는 이 방식으로 더 일관되게 획득될 수 있다. 지문 생체 인식(fingerprint biometrics)을 사용하면, 전용 등록 단말기(dedicated enrolment terminal)와 같은 한 곳에서 초기 등록이 이루어지고, 매칭을 위한 후속의 등록이 매칭이 요구되는 단말기와 같은 다른 곳에서 이루어질 때, 하나의 문제점은 반복 가능한 결과를 획득하는 것이 어렵다는 것이다. 각 지문 센서 주변의 하우징(housing)의 기계적 피쳐(mechanical features)는 다수의 센서(multiple sensors) 중 임의의 하나에 의해 판독될 때마다 손가락을 일관된 방식으로 가이드(guide)하도록 신중하게 설계되어야 한다. 지문이 여러 다른 단말기로 스캔되는 경우, 각 단말기는 약간씩 다르므로, 지문을 판독 중 오류가 발생할 수 있다. 반대로, 동일한 지문 센서가 매회 사용될 경우, 이러한 오류가 발생할 가능성이 감소된다.

제안된 장치에 따라, 매칭 및 등록 스캔은 모두 동일한 지문 센서를 사용하여 수행될 수 있다. 결과적으로, 스캔 오류는 균형을 이루는데, 예를 들어 사용자가 등록하는 동안 사용자의 손가락을 옆쪽 편향(lateral bias)으로 제시하는 경향이 있는 경우, 매칭하는 동안에도 사용자는 그렇게 할 가능성이 있기 때문이다.

상기 제어 시스템은 사용자가 상기 지문 센서를 통해 상기 사용자의 지문을 등록할 수 있는 등록 모드(enrolment mode)를 가지며, 등록 중에 생성된 상기 지문 데이터는 메모리에 저장될 수 있다. 상기 제어 시스템은 지문 등록에 추가로(즉, 지문 인증에 실패 후 허용할) 및/또는 상기 사용자 등록에 실패한 경우에, 비-지문 인증 코드(non-fingerprint authorization code)의 등록(enrolment)을 위해 상기 사용자를 프롬프트(prompt)하도록 구성될 수 있다.

상기 제어 시스템은 상기 장치가 사용자에게 처음 제공될 때 등록 모드에 있을 수 있어서, 사용자가 지문 데이터를 즉시 등록할 수 있다. 제1 등록 사용자는, 예를 들어 식별이 확인된 후에 장치의 입력 장치에서의 입력을 통해, 추가될 추후 사용자를 위해 등록 모드를 나중에 프롬프트할 수 있는 어빌리티(ability)를 제공받을 수 있다. 대안적으로(alternatively) 또는 추가적으로(additionally), 장치와 보안 시스템 사이의 인터랙션을 통해서와 같이, 외부 수단을 통해 제어 시스템의 등록 모드를 프롬프트하는 것이 가능할 수 있으며, 이는 제조자 또는 다른 인증된 기관에 의해 제어되는 보안 시스템일 수 있다.

상기 제어 시스템은 지문 매칭 알고리즘을 실행하기 위한 지문 프로세서(fingerprint processor) 및 등록된 지문에 대한 지문 데이터를 저장하기 위한 메모리를 포함할 수 있다. 상기 장치의 제어 시스템은 다수의 프로세서를 포함할 수 있으며, 지문 프로세서는 지문 센서와 관련된 별도의 프로세서(separate processor)일 수 있다. 다른 프로세서는 다른 장치와의 통신(예를 들어, 비접촉 기술), 수신기/송신기의 활성화 및 제어, 금융 거래와 같은 보안 요소의 활성화 및 제어 등과 같이, 장치의 기본 기능을 제어하기 위한 제어 프로세서를 포함할 수 있다. 다양한 프로세서는 개별적인 하드웨어 요소로 구현될 수 있거나, 아마도 개별적인 소프트웨어 모듈을 구비하여, 단일 하드웨어 요소로 결합될 수 있다.

상기 장치는 휴대용 장치일 수 있는데, 이는 사람에 의해 운반되도록 설계된 장치, 바람직하게는 작고 가볍게 편리하게 운반될 수 있는 장치를 의미한다. 이 장치는 예를 들어 주머니, 핸드백 또는 지갑 내에 운반되도록 구성될 수 있다. 상기 장치는 지문 인증 가능한 RFID 카드(fingerprint authorisable RFID card)와 같은 스마트카드일 수 있다. 상기 장치는 컴퓨터 시스템에 대한 액세스를 위한 일회용 패스워드 장치(one-time-password device) 또는 차량 키리스 엔트리 시스템(vehicle keyless entry system)을 위한 포브(fob)와 같이 제어 토큰(control token) 외부의 시스템에 대한 액세스를 제어하기 위한 제어 토큰일 수 있다. 상기 장치는 바람직하게는 유선 전원에 의존하지 않는다는 점에서 휴대 가능하다. 상기 장치는 내부 배터리 및/또는 RFID 판독기(RFID

reader)와 같은 판독기 등으로부터 비접촉으로 수집된 전력에 의해 전력이 공급될(powered) 수 있다.

상기 장치는 단일-목적 장치(single-purpose device), 즉, 단일 외부 시스템 또는 네트워크와 인터랙트하거나 외부 시스템 또는 네트워크의 단일 유형과 인터랙트하기 위한 장치일 수 있으며, 상기 장치는 임의의 다른 목적을 가질 수 없다. 따라서, 상기 장치는 스마트폰 등과 같은 복합 및 다중-기능 장치(complex and multi-function devices)와 구별되는 것이다.

상기 장치가 스마트카드인 경우, 상기 스마트카드는 액세스 카드, 신용 카드, 직불 카드, 선불 카드, 로얄티 카드, 신원 카드, 등등 중 어느 하나일 수 있다. 스마트카드는 바람직하게는 85.47㎜와 85.72㎜ 사이의 폭, 및 53.92㎜와 54.03㎜ 사이의 높이를 갖는다. 스마트카드는 0.84㎜ 보다 작은, 바람직하게는 약 0.76㎜(예를 들어, ± 0.08㎜)의 두께를 가질 수 있다. 더 일반적으로, 스마트카드는 스마트카드의 사양인, ISO 7816을 준수할 수 있다.

상기 장치가 제어 토큰인 경우, 예를 들어 차량을 위한 키리스 엔트리 키(keyless entry key)일 수 있으며, 이 경우 외부 시스템은 차량의 잠금/액세스 시스템 및/또는 점화 시스템일 수 있다. 외부 시스템은 더 광범위하게는 차량의 제어 시스템일 수 있다. 제어 토큰은 마스터 키 또는 스마트 키로서 동작할 수 있으며, 무선 주파수 신호는 인증된 사용자의 지문 식별에 응답하여 전송되는 차량 피쳐(vehicle features)에 대한 액세스를 제공한다. 대안적으로, 제어 토큰은 원격 잠금형 키(remote locking type key)로서 동작할 수 있으며, 차량을 잠금 해제하기 위한 신호는 지문 인증 모듈이 인증된 사용자를 식별하는 경우에만 송신될 수 있다. 이 경우, 인증된 사용자의 식별은 종래 기술의 키리스 엔트리형 장치(keyless entry type devices)의 잠금 해제 버튼(unlock button)을 누르는 것과 동일한 효과를 가질 수 있고, 차량을 잠금 해제하기 위한 신호는 인증된 사용자의 지문 또는 비-지문 식별시 자동으로 송신될 수 있으며, 또는 인증된 사용자의 인증에 의해 제어 토큰이 활성화될 때 버튼 누름에 응답하여 송신될 수 있다.

비-지문 인증은 지문 센서와의 선택적으로 하나 이상의 센서와의 인터랙션을 포함할 수 있다. 일부 구현예에서는, 비-지문 인증 없는 '표준' 장치에 비해 센서가 추가되지 않지만, 추가 센서가 이미 존재하는 경우 비-지문 인증은 해당 장치와의 인터랙션과 함께 지문 센서와의 인터랙션을 포함할 수 있다. 지문 인증 가능 장치에서의 추가 센서는, 예를 들어, 하나 이상의 버튼(button), 정전식 감응 센서(capacitive sensor) 또는 가속도계(accelerometer)를 포함할 수 있다.

따라서, 상기 장치는 상기 장치의 이동(movements)을 감지하기 위한 가속도계를 포함할 수 있고, 상기 제어 시스템은 상기 가속도계의 출력에 기초하여 상기 장치의 이동을 식별하도록 구성되며, 상기 비-지문 인증은 상기 가속도계에 의해 감지된 이동과 함께 상기 지문 센서를 통해 검출된 하나 이상의 동작의 조합을 포함한다.

상기 지문 센서를 통해 검출된 동작, 가속도계에 의해 검출된 이동 및/또는 버튼 또는 다른 센서를 통한 입력을 포함하여, 사용자가 상기 장치와 인터랙트 할 수 있는 다양한 가능한 방식은 상기 장치의 다수의 작동 모드(operation modes) 중 서로 다른 모드 사이를 전환(switch)하도록 상기 제어 시스템을 위한 명령어(instructions)로서 사용될 수 있다.

가속도계에 의해 감지된 이동은 하나 이상의 방향(시계 방향/반 시계 방향) 및/또는 하나 이상의 회전의 축에서의 장치의 회전, 하나 이상의 방향(전방/후방)에서의 및 하나 이상의 축을 따른 장치의 병진 이동(translation), 및/또는 하나 이상의 방향(전방/후방)에서의 및 하나 이상의 축을 따른 가속도 뿐만 아니라 하나 이상의 방향(전방/후방)에서의 및 하나 이상의 축을 따른 저크(jerk) 또는 임펄스(impulses)를 포함할 수 있다. 이러한 이동의 조합은, 예를 들어 가속도계에 의해 검출된 이동을 특성화하기 위한 병진 이동 및 가속/감속의 조합을 포함하는 "플릭(flick)" 모션이 또한 검출될 수 있다. 상기 장치가 스마트카드일 때, 위에서 언급된 축은, 예를 들어 카드의 긴 변, 카드의 짧은 변, 및 카드의 법선으로 정렬된 x, y, z 축일 수 있다. 또한, 가속도계는, 예를 들어 장치가 떨어졌을 때 자유 낙하 이동(free fall movement)을 검출하도록 구성될 수 있다. 자유 낙하를 검출하기 위한 가속도계의 사용은 잘 정립되어 있으며, 예를 들어 하드 디스크 드라이브의 안전 피쳐(safety features)를 활성화하여 떨어졌을 때의 손상을 방지하는 데 사용된다.

가속도계에 의해 감지된 장치의 회전은, 예를 들어 스마트카드를 세로 방향으로부터 가로 방향으로 전환하거나 카드를 뒤집는 것과 같이, 장치의 방향 변경을 포함할 수 있다. 회전은 임의의 방향으로 90도 회전, 180도 회전, 270도 회전 또는 360도 회전 또는 중간 값을 포함할 수 있다.

병진 이동적 이동(Translational movements)은 물결 모션(waving motions)을 포함할 수 있고, 선택적으로 플릭킹 유형 모션(flicking type motion) 또는 탭핑 모션(tapping motion)과 같은 가속/감속과 조합될 수 있다.

제어 시스템은 가속도계의 출력에 기초하여 장치의 이동을 식별하고, 비-지문 인증에서 이것을 사용하고 및/또는 사전-설정된 이동에 응답하여 장치의 작동 모드를 변경하도록 구성될 수 있다. 사전-설정된 이동은 위에서 언급한 일부 또는 모든 이동을 포함할 수 있다. 또한, 제어 시스템은 모션이 없는 시간 기간의 길이, 즉 장치의 활성화된 사용을 나타내지 않는 시간 기간을 결정할 수 있으며, 이는 또한 장치의 작동 모드를 변경하는 데 사용될 수 있다. 또한, 제어 시스템은 이중 탭(double tap) 또는 슬라이딩 및 비틀림 모션(sliding and twisting motion)과 같은 회전에 뒤따르는 병진 이동과 같은 반복된 이동 또는 이동의 시퀀스를 식별하도록 구성될 수 있다. 바람직하게는, 상기 장치는 사용자가 이동 및/또는 이동의 조합을 설정할 수 있도록 구성될 수 있다. 예를 들어, 제어 시스템은 학습 모드를 가질 수 있으며, 사용자에 의한 이동의 조합이 제어 시스템에 가르쳐 질 수 있고 그 다음에 장치의 작동 모드의 특정 변경에 할당될 수 있다. 이는 각 개인에게 고유할 수 있는 이동의 사용에 의해 증가된 보안을 제공할 수 있다.

사용자와 장치의 인터랙션에 의해 제어되는 장치의 작동 모드는, 예를 들어 장치 켜기 또는 끄기, 비접촉식 지불과 같은 장치의 보안 측면 활성화하기, 또는 예를 들어 액세스 카드, 지불 카드 또는 교통 스마트카드로 작동하는 사이에서 스마트카드를 전환하여 장치의 기본 기능을 변경하거나, 동일한 유형의 다른 계정(예를 들어, 2개의 은행 계좌) 사이를 전환하기 등의 높은 수준 기능(high level function)과 관련될 수 있다.

대안으로 또는 추가적으로, 사용자와 장치의 인터랙션에 의해 제어되는 장치의 작동 모드는, 예를 들어 통신 프로토콜(예를 들어, 블루투스, 와이파이, NFC) 사이에서 전환하기 및/또는 통신 프로토콜을 활성화하기, LCD 또는 LED 디스플레이와 같은 디스플레이를 활성화하기, 일회용 패스워드 등과 같은 장치로부터의 출력 획득하기 등의 장치의 많은 특정 기능에 영향을 미칠 수 있다.

대안으로 또는 추가적으로, 사용자와 장치의 인터랙션에 의해 제어되는 장치의 작동 모드는 장치의 표준 작동을 자동으로 수행하도록 장치에 프롬프트하는 것을 포함할 수 있다. 이러한 표준 작동의 예시로는 ATM과 통신하는 동안 또는 통신하기 전에 특정 이동에 응답하여 사전-설정된 현금 인출, 학습 또는 설정 모드 진입하기, 스마트카드의 PIN 활성화(예를 들어, 외부 카드 판독기의 키패드를 통한 PIN 엔트리의 대신에 사용된 이동(movements)), 비접촉식 판독기 또는 스마트폰(예를 들어, NFC를 통한)으로 메시지 송신하기 등을 포함할 수 있다.

제어 시스템은 사용자가 어떤 인터랙션(서로 다른 인터랙션 또는 이동의 조합을 포함하여)이 특정 작동 모드를 활성화해야 하는지를 지정하고 및/또는 비-지문 인증의 일부로서 사용될 이동을 지정할 수 있도록 구성될 수 있다. 제어 시스템은 일련의 작동 모드의 각각에 대해 서로 다른 이동을 사용할 수 있거나, 또는 반복적인 이동에 응답하여 일련의 작동 모드의 작동 모드를 통해 순환할 수 있다.

상기 장치의 작동 모드의 이동 및 변경의 조합의 예시로는, 예를 들어 액세스 카드, 지불 카드, 전송 시스템 카드 사이에서 카드 애플리케이션(card application)을 전환하기 위해 스마트카드를 플리킹하기(flicking), 사전-설정된(바람직하게는, 사용자 지정된) 활성화 제스처를 통해 장치를 켜기, 장치를 180도 회전시켜 블루투스와 NFC 사이를 전환하기, 표면(surface)을 더블 탭(double tap)하여 디스플레이를 활성화하기 등을 포함한다.

일 예시는 자유 낙하가 검출될 때 장치를 떨어진 장치 모드로 두기(placing the device into a dropped device)를 포함한다. 이 모드는 장치를 집어 올린 후에 추후 장치의 사용이 허용되기 전이나 장치의 전체 사용이 허용되기 전에 보안 기능을 통한 재인증을 요구할 수 있다. 이렇게 하면, 권한이 없는 사용자에 의해 발견된 경우 떨어진 장치를 부정하게(fraudulently) 사용할 수 없다. 보안 기능은 지문 인증, 비-지문 인증 및/또는 스마트카드를 위한 카드 판독기에서의 PIN의 사용일 수 있다. 지불 카드에 대한 일 예시로, 카드가 떨어진 후 후속 인증이 제공될 때까지 비접촉식 지불을 통한 자동 거래에 대한 인증이 없을 수 있다.

장치는 휴면/오프 모드(dormant/off mode)로 들어갈 수 있으며, 예를 들어 애플리케이션에 따라 며칠 또는 수주일 동안 시간의 기간 동안 사용하지 않은 상태로 둔 후에, 재-활성화 또는 재인증을 요구할 수 있다. 재-활성화는 이동의 특정 시퀀스가 검출되거나, 센서와의 인터랙션을 통한 활성화를 요구할 수 있다. 재 인증은 떨어진 장치 모드와 관련하여 위에서 설명된 바와 같을 수 있다.

단일 감지 축(single sensing axis)이 있는 가속도계에 의해 이동은 검출될 수 있지만, 모든 방향의 가속도를 검출할 수 있는 것이 바람직하다. 이것은 다수의 가속도계를 통해 수행될 수 있지만, 바람직하게는 3-축 가속도계(tri-axis accelerometer)와 같은 모든 방향에서 가속도를 검출할 수 있는 단일 가속도계가 사용된다.

가속도계는 MEMS 가속도계와 같은 마이크로-가공된 가속도계(micro-machined accelerometer)일 수 있다. 대안적으로, 가속도를 감지할 수 있는 전용 압전 가속도계(dedicated piezoelectric accelerometer) 또는 다른 압

전 센서(예를 들어, 압전 음향기(piezoelectric sounder) 또는 마이크로폰(microphone))와 같은 압전 센서(piezoelectric sensor)가 사용될 수 있다. 가속도계의 이러한 유형의 사용은 장치의 크기를 늘릴 필요없이 휴대용 장치에 설치할 수 있다. 또한, 전력 소비도 적으며, 이는 스마트카드와 같은 휴대용 장치의 또 다른 설계 제한이 될 수 있다. 압전 센서는 입력이 압전 센서에 의해 검출될 때까지 전력 소비가 제로가 되는 방식으로 장치에 유리하게 통합될 수 있다. 가속도계는 마이크로-가공된 캔틸레버(micro-machined cantilever) 또는 사이즈믹 매스(seismic mass)와 같은 감지 요소를 사용할 수 있다. 일 예시적인 구현에서, 가속도 감지는 감지 요소의 가속-유도 모션(acceleration-induced motion)으로부터 발생하는 차동 커패시턴스(differential capacitance)의 원리에 기초한다. 사용될 수 있는 가능한 가속도계는 미국 뉴욕 이타카(Ithaca)의 키오닉스 사(Kionix, Inc.)에 의해 제공되는 3-축 디지털 가속도계(Tri-axis Digital Accelerometer)이다. 일 예시적인 실시예는 Kionix KXCJB-1041 가속도계를 사용한다.

상기 장치는 RFID 또는 NFC 통신을 사용하는 것과 같이 무선 통신을 할 수 있다. 대안적으로 또는 추가적으로, 상기 장치는, 예를 들어 "칩 및 핀" 지불 카드를 위해 사용되는 것과 같이 또는 접촉 패드를 통한 접촉 연결(contact connection)을 포함할 수 있다. 다양한 실시예에서, 상기 장치는 무선 통신 및 접촉 통신 모두를 허용할 수 있다.

제2 측면으로 보면, 본 발명은 사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서, 및 상기 장치를 제어하기 위한 제어 시스템을 갖는 지문 인증 가능 장치를 제어하기 위한 방법을 제공하고, 상기 방법은, 인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하는 단계; 및 적어도 부분적으로 상기 지문 인증을 대체하기 위해 비-지문 인증이 동작할 수 있는 상기 제어 시스템의 지문 실패 피처의 일부로서 비-지문 인증을 통해 사용자가 식별될 때, 상기 장치의 하나 이상의 기능 중 적어도 일부에 대한 액세스를 대안적으로 또는 추가적으로 제공하는 단계를 포함하고, 상기 비-지문 인증은 상기 사용자에 의한 상기 지문 인증 가능 장치와의 인터랙션을 요구하고, 상기 인터랙션은 상기 지문 센서를 통해 검출된 하나 이상의 동작을 포함한다.

상기 방법은 지문 인증 가능 장치와 관련하여 위에서 설명된 바와 같은 피처(features)를 포함할 수 있다. 따라서, 지문 센서를 통해 검출된 동작은 위에서 설명된 바와 같은 하나 이상의 동작을 포함할 수 있다. 상기 장치는 위에서 설명된 일부 또는 모든 기능을 포함할 수 있다. 예를 들어, 상기 방법은 가속도계를 포함하는 장치의 사용을 포함할 수 있으며, 따라서 상기 장치의 이동을 검출하는 단계 및 비-지문 인증 및/또는 작동 모드의 변경을 프롬프트 하는 것과 관련하여 이동을 사용하는 단계를 포함할 수 있다. 상기 방법은 제어 시스템에서 지문 매칭 알고리즘을 사용하여 등록된 사용자와 지문 센서에 의해 감지된 지문 사이의 지문 매칭을 식별하는 단계를 포함할 수 있다. 상기 방법은 상기 지문 센서를 통해 지문 데이터를 획득함으로써 인증된 사용자를 등록하기 위해 상기 제어 시스템의 등록 모드를 사용하는 단계를 포함할 수 있다. 상기 제어 시스템은 사용자가 지문 센서를 통해 사용자의 지문을 등록할 수 있는 등록 모드를 가질 수 있으며, 사용자는 지문 등록에 추가로(즉, 추후 지문 인증 실패를 위해 허용하는) 및/또는 사용자의 등록에 실패한 경우에, 비-지문 인증 코드의 등록을 위해 프롬프트 받는다.

비-지문 인증은 위에서 설명된 바와 같이, 지문 센서 및 선택적으로 하나 이상의 센서와의 인터랙션을 포함할 수 있다.

제3 측면에서, 본 발명은 위에서 설명된 바와 같이, 지문 인증 가능 장치의 제어 시스템에서 실행될 때, 상기 제어 시스템이, 인증된 지문의 식별에 응답하여 상기 장치의 하나 이상의 기능에 대한 액세스를 제공하고; 및 적어도 부분적으로 상기 지문 인증을 대체하기 위해 비-지문 인증이 동작할 수 있는 상기 제어 시스템의 지문 실패 피처의 일부로서 비-지문 인증을 통해 사용자가 식별될 때, 상기 장치의 하나 이상의 기능 중 적어도 일부에 대한 액세스를 대안적으로 또는 추가적으로 제공하도록 하는 명령어를 포함하는 컴퓨터 프로그램 제품을 제공하며, 상기 비-지문 인증은 상기 사용자에 의한 지문 인증 가능 장치와의 인터랙션을 요구하고, 상기 인터랙션은 상기 지문 센서를 통해 검출된 하나 이상의 동작을 포함한다. 상기 명령어는 상기 제어 시스템이 위에서 설명된 선택적 및 바람직한 피처 중 일부 또는 전부에 따라 작동하도록 구성될 수 있다.

위의 설명으로부터, 지문 인증을 위한 지문 센서를 구비한 기존의 지문 인증 가능 장치 및 상기 장치를 제어하기 위한 제어 시스템은 본 명세서에 설명된 유익한 지문 실패 피처를 구현하도록 수정될 수 있음을 알 수 있을 것이다. 이는 위에서 설명된 바와 같이 컴퓨터 프로그램 제품을 설치함으로써 수행될 수 있다. 따라서, 본 발명의 다른 측면은 지문 실패 피처를 제공하기 위하여 지문 인증 가능 장치를 구성하는 방법을 제공하며, 상기 지문 인증 가능 장치는 사용자의 손가락 또는 엄지 손가락으로부터 지문 데이터를 획득하기 위한 지문 센서, 및

상기 장치를 제어하기 위한 제어 시스템을 포함하고; 상기 방법은 상기 지문 인증 가능 장치에 위에서 설명된 바와 같은 컴퓨터 프로그램 제품을 설치하는 단계를 포함한다.

현재 청구되지 않은 제4 측면에서, 본 발명은 다수의 작동 모드를 갖는 스마트카드를 제공하며, 상기 스마트카드는 상기 스마트카드의 작동을 제어하기 위한 프로세서 및 상기 스마트카드의 이동을 감지하는 가속도계를 포함하며, 상기 프로세서는 상기 가속도계에 의해 감지된 상기 이동에 응답하여 상기 다수의 작동 모드 중 서로 다른 모드 사이를 전환하도록 구성된다.

이 스마트카드는 사용자가 카드를 잡고 있거나 만져서 이동 또는 제스처(gestures)를 사용하여 사용자와 스마트카드 사이의 인터랙션을 허용함으로써 추가 기능을 제공한다. 이는 직접 물리적 접촉을 필요로 하는 버튼 또는 다른 센서와 같은 카드의 입력 장치를 조작할 필요없이 대안적인 카드 피처를 활성화할 수 있다. 유리하게는, 스마트카드는 비접촉식 카드이며, 따라서 사용자는 사용자에 의해 카드를 잡는(holding) 접촉만으로 카드 판독기를 통해 카드를 사용하는 것뿐만 아니라 서로 다른 모드 사이를 전환할 수 있다. 이는 카드의 작동의 용이함(ease)에 해를 끼치지 않으면서, 스마트카드 사용 방식에서의 복합성(complexity)이 증가되고 피처가 증가될 수 있다.

가속도계에 의해 감지된 이동은 예를 들어 위에서 설명된 바와 같을 수 있다. 이 측면의 스마트카드는 제1 측면의 장치를 위해 위에서 설명된 일부 또는 모든 피처를 포함할 수 있다.

가속도계는 사용자에 의해 선택된 시퀀스로 특정한 진동/이동 패턴을 측정한다. 프로세서는 스마트카드에 등록될 이동 패턴을 수신하고 기록하도록 구성될 수 있다. 대안적으로 또는 추가적으로 이동 패턴에 의해 생성된 가속도계 출력 데이터는 등록 동안 카드로부터 전송되고 외부 데이터베이스에 기록될 수 있다. 프로세서는, 생체 센서를 통해 사용자의 신원의 인증이 있고 가속도계에 의해 감지된 이동 모두가 등록된 이동 패턴과 매칭되는 것으로 결정될 때, 하나 이상의 보안 피처에 대한 액세스를 허용하도록 구성될 수 있다.

가속도계의 출력은 사용자에 의해 만들어진 이동의 시퀀스에 고유하며, 또한 스마트카드에 고유하다. 각 스마트카드는 자체 고유 진동수를 가지며 사용자와 카드의 인터랙션을 다른 카드와 다른 방식으로 동적으로 반응할 것이다. 예를 들어, 더 뻣뻣한 카드(stiffer card)는 사용자가 더 유연한 카드보다 카드를 흔들거나 탭한 후에 다르게 이동(move)할 것이다. 따라서, 가속도계에 의해 검출되는 카드의 이동에는 스마트카드의 동적 반응의 영향이 포함된다는 것을 이해하는 것이 중요하다. 가속도계에 의해 검출된 이동에 대한 설명은 그 맥락에서 이해되어야 한다. 가속도계로부터의 출력 신호(즉, 가속도계 출력 데이터)는 만들어진 이동뿐만 아니라 스마트카드의 동적 반응의 표현이다.

가속도계 출력 데이터는 사용자와 카드 모두에 특정하므로 데이터를 복제할 수 없다. "가짜" 카드가 생성되고, 탭 시퀀스 데이터(the tap sequence data)가 마이크로 프로세서에 "주입(injected)"되면, 새 카드의 동적 반응이 원래 카드와 다를 수 있으므로 이동 패턴을 모방하여 해킹 당할 수 없다. 대량 생산된 스마트카드의 경우, 스마트카드의 구성에 있어서 허용 오차와 불가피한 작은 변화가 스마트카드의 이동의 특성의 차이로 이어질 가능성이 있다.

동일한 기본 프로세스를 사용하여 제조된 대량 생산된 스마트 카드 사이의 구분을 강화하기 위해, 제조 방법에 가속도계의 위치를 변경하거나 및/또는 다른 특성을 가진 질량/강성 요소(mass/stiffness elements)를 카드에 추가하는 것을 포함할 수 있어, 각 개별 카드가 완전히 고유한 이동 패턴을 가진다. 따라서, 일부 예시에서 스마트카드는 추가 질량 또는 강성 요소를 포함할 수 있다. 다른 사용자가 소유자의 탭 시퀀스에 따라 원래 카드를 사용하려고 시도하면, 사기를 치는 사용자(fraudulent user)가 카드를 잡는 방식(예를 들어, 허위 생체 인식을 성공적으로 생성한 후), 및 그/그녀의 탭핑 버릇(his/her tapping mannerisms)은 또한 다른 반향(different resonance)을 생성할 것이다.

스마트카드는 지문 센서와 같은 생체 인식 센서를 포함할 수 있으며, 이는 바람직하게는 카드에 내장된다. 이 피처를 사용하여 인증된 사용자는 처음에 실제 카드에 지문을 등록할 수 있으며, 카드의 일부 또는 모든 사용을 인증하기 위하여 지문 센서에 손가락이나 엄지 손가락을 두도록 요구될 수 있다. 프로세서의 지문 매칭 알고리즘은 등록된 사용자와 지문 센서에 의해 감지된 지문 사이의 지문 매칭을 식별하는데 사용될 수 있다.

생체 인식 센서는 이동에 의해 카드의 후속 제어를 활성화하거나, 지불/은행 카드로 지불 또는 인출하거나, 스마트카드가 액세스 카드일 때는 더 안전한 영역으로 액세스하는 것과 같이, 더 높은 보안으로 표시된 피처를 활성화하는데 사용될 수 있다. 더 안전한 작동을 완료하기 위해서는 카드의 이동에 추가로 생체 인식 인증이 요구될 수 있다.

일부 경우에서, 생체 인식 인증이 실패하거나 불가능할 수 있다. 예를 들어, 지문 센서의 경우 사용자의 지문이 부상에 의해 손상되거나 커버될 수 있다. 센서가 손상되었거나 작동하지 않을 수도 있다. 이 경우, 스마트카드는 유리하게도 생체 인식 인증을 위한 백업(back-up)으로서 동작하는 사전-설정된, 바람직하게는 복합적인 이동을 허용할 수 있다. 복합적인 이동은 둘 이상의 이동, 예를 들어 회전, 병진 이동 등과 같은 3, 4 또는 5개의 이동을 포함하는 모션 시퀀스일 수 있다. 바람직하게는, 사전-설정된 이동은 사용자 정의되므로 사용자에게 고유할 수 있다.

특히 생체 인식 센서 및 지문 센서의 일부 형태로 발생할 수 있는 상황은 등록 실패이다. 이는 어떤 이유로든 공지된 생체 인식 센서를 사용하여 등록될 수 없는 지문 또는 생체 특성을 가진 소수의 인구가 가지고 있는 근본적인 문제이다. 지문에 대한 이러한 실패는 손가락이 없거나, 흐린 지문뿐만 아니라 손상된 손가락과 같은, 보통 없거나 약한 특성에 의해 발생한다. 생체 인식 등록에 대한 대안을 제공하는 시스템은 기록된 생체 인식 세부 정보를 갖지 않는 사용자가 생체 인식 카드를 사용할 수 있게 한다. 가속도계에 의해 감지된 이동은 생체 인식 시스템을 사용하지 않고 사람들이 여전히 시스템 또는 서비스에 액세스 할 수 있도록 생체 인식 카드에 대한 대안으로 비-생체 인식이 사용될 수 있다. 이 경우, 생체 인식 센서뿐만 아니라 가속도계를 포함하는 스마트카드는 생체 인식 데이터의 대안으로서 가속도계에 의해 감지된 이동을 통해 등록할 수 있는 어빌리티가 제공될 수 있다. 사용자는, 위에서 설명된 유형의 복합적인 이동과 같은, 카드의 사용의 인증을 위한 이동 또는 이동의 시퀀스를 설정할 수 있다. 이는 감지된 이동의 유일한 목적일 수 있고 및/또는 감지된 이동은 추가의 다른 작동 모드 사이에서 카드를 변경하는 데에도 사용될 수 있다.

현재 청구되지 않은 제5 측면에서 보면, 본 발명은 스마트카드를 제어하기 위한 방법을 제공하며, 상기 스마트카드는 상기 스마트카드의 작동을 제어하기 위한 프로세서 및 상기 스마트카드의 이동을 감지하기 위한 가속도계를 포함하며, 상기 방법은 상기 가속도계 및 상기 프로세서를 사용하는 상기 스마트카드의 이동을 검출하는 단계, 및 검출된 이동에 응답하여 스마트카드의 다수의 작동 모드 중 서로 다른 모드 사이에서 전환하는 단계를 포함한다.

상기 방법은 제1 측면 또는 제4 측면과 관련하여 위에서 설명된 바와 같은 피처를 갖는 스마트카드의 사용을 포함할 수 있다. 검출된 이동은 위에서 설명된 바와 같을 수 있고 및/또는 작동 모드는 위에서 설명된 바와 같을 수 있다.

상기 방법은 사용자가 어떤 이동(이동의 조합 포함)이 특정 작동 모드를 활성화시켜야 하는지를 지정할 수 있게 하는 단계를 포함할 수 있다.

스마트카드는 지문 센서와 같은 생체 인식 센서를 포함할 수 있으며, 바람직하게는 카드에 내장된다. 상기 방법은 생체 인식 센서를 사용하여 이동에 의한 카드의 후속 제어를 활성화하거나, 지불/은행 카드로 지불 또는 인출하거나 스마트카드가 액세스 카드일 때 더 안전한 장소로 액세스하는 것과 같은, 더 높은 보안으로 표시된 피처를 활성화하는데 사용될 수 있다.

상기 방법은 스마트카드 내에 내장된 생체 인식 센서를 사용하여 스마트카드의 소지자의 신원을 인증하는 단계, 및 신원이 인증된 후에만 사용자와 카드의 이동 활성화된 인터랙션을 가능하게 하는 단계를 포함할 수 있다. 카드와의 이동 활성화된 인터랙션은 생체 인식 인증 후 설정된 기간, 예를 들어 수 시간 또는 며칠의 기간 동안일 수 있다. 이 방식으로 사용자는 계속 재인증하지 않아도 카드의 피처에 액세스 할 수 있지만, 생체 인식의 사용에 의해 향상된 보안이 제공된다.

상기 방법은, 예를 들어 생체 인식 인증이 실패할 때 카드의 일부 또는 모든 작동 모드의 사용을 허용하거나 생체 인식 센서를 사용하지 않고 등록을 허용하기 위해, 생체 인식 인증 대신에 이동의 시퀀스의 사용을 포함할 수 있다.

또한, 본 발명은 스마트카드를 제조하는 방법을 포함할 수 있다. 이는 제1 측면 또는 제4 측면에서와 같은 피처를 제공하는 단계로 구성될 수 있다. 또한, 상기 제조 방법은 위에서 설명된 바와 같이 일부 또는 모든 선택적인 피처를 제공하는 단계를 포함할 수 있다. 상기 방법은 위에서 설명된 바와 같이 기능하도록 프로세서를 프로그래밍하는 단계를 포함할 수 있다. 진동 패턴의 차이를 강화하고 동일한 이동에 노출된 동일한 프로세스를 사용하여 제조된 카드 사이에 가속도계 출력의 차이를 더 크게 하기 위해, 상기 제조 방법은 가속도계의 위치를 변경하는 단계 및/또는 카드에 상이한 위치 및/또는 상이한 특성을 갖는 질량/강성 요소를 추가하는 단계를 포함하여, 각각의 개별 카드가 고유한 진동 패턴을 갖도록 알 수 있다. 상기 방법은 선택적으로 질량 및/또는 강성 요소를 카드에, 예를 들어 카드의 회로 기판에 추가하는 단계를 포함할 수 있으며, 상기 질량 및/또는

강성 요소는 상이한 질량 및/또는 강성 특성을 구비한 요소의 세트로부터 선택된다. 이는 추가된 질량 및/또는 강성 요소가 동일한 위치에 배치되도록 허용하며, 이는 용이한 제조를 허용하면서, 추가된 요소의 질량 및/또는 강성이 변하기 때문에 카드의 이동에 대한 가변 효과를 보장한다. 대안적으로 또는 추가적으로 질량 및/또는 강성 요소는 각각의 카드에 대해 변하는 위치에서 카드에 추가될 수 있다. 이는 각각의 카드에 대해 동일한 질량 및/또는 강성 요소를 사용하거나 질량 및/또는 강성 요소가 상이한 질량 및/또는 강성 특성을 구비한 요소의 세트로부터 선택될 수 있다.

또 다른 측면에서, 본 발명은 위에서 설명된 바와 같이 스마트카드의 프로세서상에서 실행될 때, 프로세서로 하여금 가속도계로부터의 출력에 기초하여 스마트카드의 이동을 식별하게 하고, 및 검출된 이동에 응답하여 스마트카드의 다수의 작동 모드 중 서로 다른 모드 사이에서 전환하게 하는 명령어를 포함하는 컴퓨터 프로그램 제품을 제공할 수 있다. 상기 명령어는 프로세서가 위에서 설명된 선택적 및 바람직한 피쳐 중 일부 또는 전부에 따라 작동하게 하도록 구성될 수 있다.

도면의 간단한 설명

본 발명에 대한 특정 바람직한 실시예는 첨부된 도면을 참조하여 예시로서만 더 상세히 설명될 것이다.

도 1은 지문 센서를 갖는 스마트카드를 위한 회로를 도시한다.

도 2는 외부 하우징을 포함하는 스마트카드의 제1 실시예를 도시한다.

도 3은 적층된 스마트카드의 제2 실시예를 도시한다.

발명을 실시하기 위한 구체적인 내용

예시로서, 본 발명은 비접촉 기술을 포함하고 카드 판독기로부터 수집된(harvested) 전력을 사용하는 지문 인증 스마트카드의 맥락에서 설명된다. 이러한 특징은 제안된 지문 실패 피쳐의 하나의 응용의 유리한 특징이지만, 필수 특징으로 간주되지는 않는다. 따라서, 스마트카드는 대안적으로 물리적 접촉을 사용할 수 있고/있거나, 예를 들어 내부 전력을 제공하는 배터리를 포함할 수 있다. 또한, 지문 실패 피쳐는 지문 인증을 사용하는 임의의 다른 장치 또는 시스템에서 적절히 수정하여 구현될 수 있다.

도 1은 제안된 지문 실패 특징이 제공되는 스마트카드(102)의 아키텍처를 도시한다. 전원 카드 판독기(powered card reader)(104)는 안테나(106)를 통해 신호를 송신한다. 이 신호는 NXP 반도체에 의해 제조된 MIFARE® 및 DESFire® 시스템(MIFARE® and DESFire® systems)에 대해 전형적으로 13.56MHz이지만, HID 글로벌 코퍼레이션(HID Global Corp.)에 의해 제조된 저주파수 PROX® 제품에 대해서는 125kHz일 수 있다. 이 신호는 튜닝된 코일(tuned coil) 및 커패시터(capacitor)를 포함하는 스마트카드(102)의 안테나(108)에 의해 수신된 다음, 통신 칩(110)으로 전달된다. 수신된 신호는 브리지 정류기(bridge rectifier)(112)에 의해 정류되고, 정류기(112)의 DC 출력은 통신 칩(110)으로부터의 메시징(messaging)을 제어하는 프로세서(114)에 제공된다.

프로세서(114)로부터의 제어 신호 출력은 안테나(108)를 통해 연결된 전계 효과 트랜지스터(field effect transistor)(116)를 제어한다. 트랜지스터(116)를 켜고 끔으로써, 신호는 스마트카드(102)에 의해 송신될 수 있고, 센서(104)에서의 적절한 제어 회로(118)에 의해 디코딩된다(decoded). 이러한 유형의 시그널링(signalling)은 후방 산란 변조(backscatter modulation)로서 공지되어 있으며, 센서(104)가 자신에 대한 리턴 메시지(return message)에 전력을 공급하는데 사용된다는 사실을 특징으로 한다.

선택적인 특징인 가속도계(16)는 프로세서(114)에 적절한 방식으로 연결된다. 가속도계(16)는 미국 뉴욕 이타카(Ithaca)의 키오닉스 사(Kionix, Inc.)에 의해 제공되는 3-축 디지털 가속도계(Tri-axis Digital Accelerometer)일 수 있으며, 이 예시에서는 Kionix KXCJB-1041 가속도계이다. 가속도계는 카드의 이동을 감지하고, 프로세서(114)에 출력 신호를 제공하며, 이는 후술되는 바와 같이 카드에서 요구되는 작동 모드와 관련된 이동을 검출하고 식별하도록 구성된다. 가속도계(16)는 전원 카드 판독기(powered card reader)(104)로부터 수집될 때만 사용될 수 있거나, 대안적으로 스마트카드(102)는 가속도계(16)를 허용하는 배터리(도시되지 않음), 프로세서(114)의 관련된 기능들 및 임의의 시간에 사용될 장치의 다른 특징이 추가적으로 제공될 수 있다.

스마트카드는 지문 프로세서(128) 및 지문 센서(130)를 포함하는 지문 인증 엔진(fingerprint authentication engine)(120)을 더 포함한다. 이는 지문 식별을 통한 등록 및 허가를 허용한다. 통신 칩(110)을 제어하는 지문 프로세서(128) 및 프로세서(114)는 함께 장치의 제어 시스템을 형성한다. 실제로 두 개의 프로세서는 별도의 하드웨어를 사용될 수 있지만 동일한 하드웨어에 소프트웨어 모듈(software modules)로 구현될 수 있다. 가

속도계(16)(존재하는 경우)와 마찬가지로, 지문 센서(130)는 전력이 전원 카드 판독기(104)로부터 수집될 때만 사용될 수 있거나, 또는 대안적으로 스마트 카드(102)는 지문 센서(130) 및 지문 프로세서(128)뿐만 아니라 프로세서(114) 및 장치의 다른 특징을 위해 언제든지 제공될 전력을 허용하는 배터리(도시되지 않음)가 추가적으로 제공될 수 있다.

안테나(108)는 유도 코일(induction coil) 및 커패시터를 포함하는 동조 회로(tuned circuit)를 포함하고, 이는 카드 판독기(104)로부터 RF 신호를 수신하도록 튜닝된다. 센서(104)에 의해 생성된 여기 필드(excitation field)에 노출될 때, 전압은 안테나(108)를 통해 유도된다.

안테나(108)는 안테나(108)의 각 단부에 하나씩 제1 및 제2 단부 출력 라인(first and second end output lines)(122, 124)을 갖는다. 안테나(108)의 출력 라인은 지문 인증 엔진(120)에 전력을 제공하기 위해 지문 인증 엔진(120)에 연결된다. 이 구성에서, 정류기(rectifier)는 안테나(108)에 의해 수신된 AC 전압을 정류하기 위해 제공된다. 정류된 DC 전압은 스무딩 커패시터(smoothing capacitor)를 사용하여 스무딩된(smoothed) 다음, 지문 인증 엔진(120)에 공급된다.

영역 지문 센서(area fingerprint sensor)(130)일 수 있는, 지문 인증 엔진의 지문 센서(130)는 도 2에 도시된 바와 같이 카드 하우징(card housing)(134)에 장착되거나, 도 3에 도시된 바와 같이 적층된 카드 바디(laminated card body)(140)로부터 노출되도록 끼워질(fitted) 수 있다. 카드 하우징(134) 또는 적층 바디(140)는 도 1의 모든 구성 요소를 포함하고, 종래의 스마트카드와 유사하게 크기가 정해진다. 지문 인증 엔진(120)은 패시브(passive)이며, 따라서 안테나(108)로부터의 전압 출력에 의해서만 전력이 공급된다. 프로세서(128)는 적절한 시간에 지문 매칭(fingerprint matching)을 수행할 수 있도록, 매우 낮은 전력 및 매우 높은 속도로 선택되는 마이크로 프로세서(microprocessor)를 포함한다.

지문 인증 엔진(120)은 지문 센서(130)에 제시된 손가락 또는 엄지 손가락을 스캔하고 프로세서(128)를 사용하여 손가락 또는 엄지 손가락의 스캔된 지문을 미리 저장된 지문 데이터와 비교하도록 구성된다. 스캔된 지문이 미리 저장된 지문 데이터와 매칭하는지에 대한 결정이 이루어진다. 바람직한 실시예에서, 지문 이미지를 캡처하고 카드(102)의 소지자를 인증하는데 요구된 시간은 1 초 보다 작다.

지문 매칭가 결정되고 및/또는 가속도계(16)를 통해 적절한 이동이 검출되면, 프로세서는 프로그래밍에 따라 적절한 동작을 취한다. 이 예시에서, 지문 인증 프로세스는 비접촉식 카드 판독기(104)와 함께 스마트카드(104)의 사용을 인증하는데 사용된다. 따라서, 통신 칩(110)은 지문 매칭이 이루어질 때 신호를 카드 판독기(104)로 전송하도록 인증된다. 통신 칩(110)은 종래의 통신 칩(110)과 동일한 방식으로 후방 산란 변조에 의해 신호를 전송한다. 카드는 제1 LED(136)와 같은 적절한 표시기를 사용하여 성공적인 인증의 표시를 제공할 수 있다.

지문 프로세서(128) 및 프로세서(114)는 지문 센서(130)와의 비-지문 인터랙션의 지시(indication)를 수신할 수 있으며, 이는 위에서 설명된 바와 같은 지문 센서(130)를 통해 검출 가능한 임의의 동작을 포함할 수 있다. 지문 센서(130)를 통한 카드와 사용자의 인터랙션은 비-지문 인증의 일부로서 사용되고, 또한 스마트카드의 서로 다른 작동 모드들 사이를 전환함으로써 사용자가 스마트카드를 제어하도록 허용하는데 사용될 수 있다.

일부 상황들에서, 지문 스마트카드(102)의 소유자는 카드(102)에 등록된 손가락의 손상을 초래하는 부상을 입을 수 있다. 예를 들어, 이 손상은 평가되는 손가락의 일부에서의 흉터일 수 있다. 이러한 손상은 지문 매칭이 이루어지지 않아 소유자가 카드(102)에 의해 인증되지 않을 수 있음을 의미할 수 있다. 이 경우, 프로세서(114)는, 이 경우에서는, 지문 센서(130)를 통해 검출된 하나 이상의 동작 및 선택적으로 가속도계(16)와 같은 다른 센서를 통해 검출된 동작을 포함하는, 스마트 카드(102)와의 대안적인 인터랙션을 통해 백업 식별/인증 체크(back-up identification/authorisation check)를 위해 사용자를 프롬프트할 수 있다. 카드는 사용자에게 제2 LED(138)와 같은 적절한 표시기를 사용하여 백업 식별/인증을 사용하도록 프롬프트 할 수 있다. 비-지문 인증을 위해서 사용자에 의해 카드와의 인터랙션의 시퀀스를 요구하는 것이 바람직하며, 이 시퀀스는 사용자에 의해 사전-설정된다. 비-지문 인증을 위한 사전-설정된 시퀀스는 사용자가 카드(102)를 등록할 때 설정될 수 있다. 따라서, 사용자는 지문 인증을 실패할 경우에 사용되도록 카드와의 비-지문 인터랙션을 사용하여 입력된 "패스워드"의 형태로 비-지문 인증을 가질 수 있다. 동일한 유형의 비-지문 인증은 사용자가 지문 센서(130)를 통해 카드 (102)를 등록할 수 없거나 등록하지 않는 경우에 사용될 수 있다.

따라서, 지문 센서(130) 및 지문 프로세서(128)를 통한 지문 인증에 응답하여 카드 판독기(104)와의 회로(110)를 통한 통신을 허용할 뿐만 아니라, 프로세서(114)는 비-지문 인증에 응답하여 이러한 통신을 가능하게 하도록 구성될 수 있다.

비-지문 인증이 사용될 때, 카드(102)는 정상적으로 사용되도록 구성될 수 있거나, 카드(102)의 더 적은 작동 모드 또는 더 적은 특징이 이용될 수 있는 저하된 모드(degraded mode)로 제공될 수 있다. 예를 들어, 스마트 카드(102)가 은행 카드로서 동작할 수 있다면, 비-지문 인증은 카드(102)에 대한 일반적인 최대 한도보다 더 낮은 최대 지출 한도를 갖는 거래를 허용할 수 있다.

프로세서(114)는 가속도계(16)로부터 출력을 수신하고, 이는 프로세서(114)가 스마트 카드(102)의 어떤 이동이 이루어졌는지를 결정하게 한다. 프로세서(114)는 스마트카드의 작동 모드에 대한 요구된 변경과 링크된 사용자의 사전 설정된 이동 및 다른 동작을 식별한다. 전술한 바와 같이, 이동은 회전, 병진 이동(translation), 가속, 임펄스(impulse) 및 가속도계(16)에 의해 검출 가능한 다른 이동의 임의의 유형을 포함할 수 있다. 사용자의 다른 동작은 탭(taps), 스와이프(swipes) 및 위에서 설명한 것과 같은, 지문 센서를 통해 검출된 동작을 포함할 수 있다.

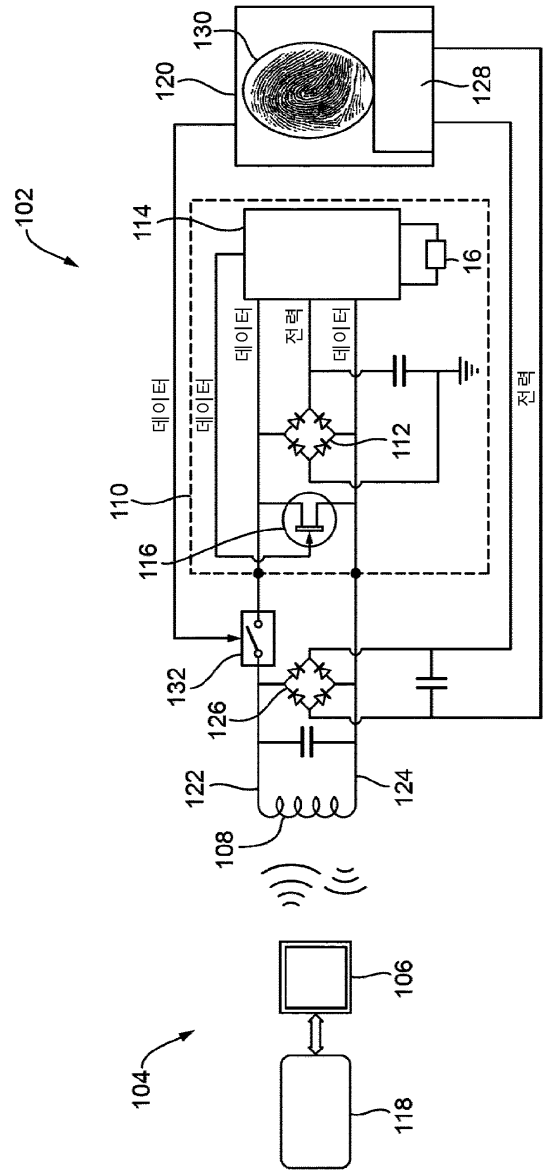
프로세서(114)가 작동 모드에서 요구된 변경과 관련된 식별된 이동에 응답하여 활성화 또는 전환하는 작동 모드는 상술한 바와 같은 작동의 임의의 모드를 포함할 수 있으며, 이는 카드 켜기 또는 끄기, 비접촉식 지불과 같은 카드(102)의 보안 측면을 활성화하기, 예를 들어, 액세스 카드, 지불 카드, 교통 스마트카드로서 작동하는 사이에서 전환하여 카드(102)의 기본 기능을 변경하기, 동일한 유형의 서로 다른 계좌(예를 들어, 2 개의 은행 계좌) 사이에서 전환하기, 통신 프로토콜(예를 들어, 블루투스, 와이파이, NFC) 사이에서 전환하기 및/또는 통신 프로토콜을 활성화하기, LCD 또는 LED 디스플레이와 같은 디스플레이를 활성화하기, 일회용 패스워드 등과 같은 스마트카드(102)로부터의 출력 획득하기, 또는 스마트카드(102)의 표준 작동을 자동적으로 수행하도록 카드(102)를 프롬프트하기를 포함한다.

프로세서(114)는 스마트카드(102)의 최초 사용시에 활성화될 수 있는, 등록 모드를 갖는다. 등록 모드에서, 사용자는 지문 센서(130)를 통해 자신의 지문 데이터를 등록하도록 프롬프트된다(prompted). 이는 지문 프로세서(128)가 지문 템플릿(fingerprint template)과 같은 적절한 지문 데이터를 구축할 수 있도록 지문 센서(130)를 통해 지문의 반복된 스캔을 요구한다. 지문 데이터가 성공적으로 또는 성공적이지 않게 등록된 후, 사용자는 비-지문 인증을 입력하도록 프롬프트된다. 이는 성공적인 지문 등록의 경우, 선택적일 수 있고, 지문 등록이 성공적이지 않은 경우 의무 사항일 수 있다. 비-지문 인증은 지문 센서(130)를 통해 검출된 사용자에 의한 적어도 하나의 동작을 포함하는 스마트카드(102)와의 인터랙션의 시퀀스를 포함한다. 프로세서 (114)는 메모리에 이러한 인터랙션들의 기록을 유지할 수 있고, 비-지문 인증이 사용자에 의해 제공되는 경우, 카드의 기능을 사용하기 위한 적어도 부분적인 인증을 제공한다.

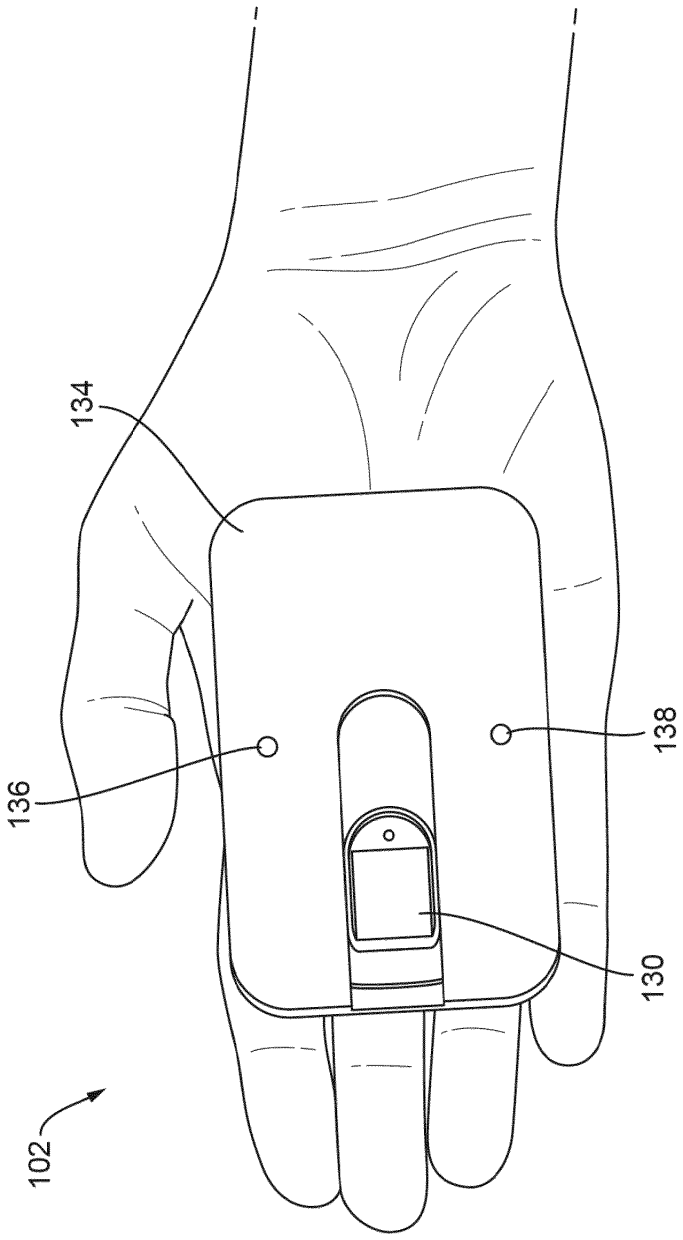
프로세서(114)는 사용자가 스마트카드(102)가 사용되는 동안 특정 작동 모드를 활성화해야 하는 동작들(동작들/인터랙션들의 조합을 포함하여)을 지정할 수 있게 하는 학습 모드를 가질 수 있다. 스마트카드(102)의 제어의 이러한 유형은 성공적인 지문 또는 비-지문 인증 후에만 가능해질 수 있다. 학습 모드에서, 프로세서(114)는 사용자로 하여금 원하는 동작의 시퀀스를 만들고, 미리 결정된 시간의 세트(predetermined set of times) 동안 움직임을 반복하도록 프롬프트한다. 이러한 움직임은 요구된 작동 모드 또는 비-지문 인증에 할당된다. 이 후자의 특징을 통해, 학습 모드는 종래의 PIN을 변경할 수 있는 것과 동일한 방식으로 사용자에 의해 변경될 비-지문 인증에 사용되는 움직임의 시퀀스를 허용할 수 있다.

도면

도면1


102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
16
데이터
데이터
데이터
전력
전력

도면2



도면3