

명세서

발명의 명칭: 보안 카드를 이용한 사용자 인증 장치 및 사용자 인증 방법

기술분야

- [1] 아래 설명은 보안 카드를 이용한 사용자 인증 장치 및 사용자 인증 방법에 관한 것이다.

배경기술

- [2] 중요 시설을 포함하는 보안이 필요한 시설의 출입구에는 일반적으로 출입자의 신분을 확인하고 출입 권한에 따라 사용자의 출입을 통제하는 사용자 인증 시스템이 설치되고 있다. 이러한 사용자 인증 시스템에서는 사용자의 출입 권한을 확인하기 위한 수단으로서 출입 카드가 널리 사용되고 있으며, 보안성을 높이기 위해 생체 인증을 사용하는 출입 통제 시스템도 개발되었다.
- [3] 출입 카드를 이용하는 방식의 경우, 출입 카드의 분실, 미반납, 권한이 없는 제3자가 출입 카드를 습득하거나 편취하여 시설에 출입하는 문제가 발생할 우려가 있다. 또한, 얼굴, 지문, 홍채 등의 생체 정보를 이용하는 출입 통제 시스템은 위 설명된 출입 카드를 이용하는 방식의 문제점을 극복할 수는 있으나, 오거부율이 존재하고, 사용자가 많아 질수록 오인식율이 높아지며 출입 통제 시스템의 구현을 위한 비용이 커진다는 한계가 존재한다. 또한, 사용자의 고유한 생체 정보의 저장 및 관리에 많은 비용이 지출되며, 생체 정보의 해킹에 대한 우려도 존재한다.
- [4] 위와 같은 문제점들을 효과적으로 해소할 수 있는 사용자 인증 기술에 대한 연구와 개발이 요구된다.

발명의 상세한 설명

과제 해결 수단

- [5] 일 실시예에 따른 사용자 인증 장치는, 카드가 인식되는 경우, 상기 카드에 저장된 얼굴 이미지를 획득하는 카드 리더기; 사용자를 향해 적외선을 방사하는 적외선 광원; 상기 사용자의 얼굴 영역을 포함하는 적외선 이미지를 획득하는 적외선 카메라; 상기 사용자의 얼굴 영역을 포함하는 컬러 이미지를 획득하는 컬러 카메라; 및 상기 적외선 이미지, 상기 컬러 이미지 및 상기 얼굴 이미지 중 적어도 하나에 기초하여 사용자 인증 결과를 결정하고, 상기 사용자 인증 결과에 따른 제어 신호를 생성하는 제어부를 포함하고, 상기 제어부는, 상기 적외선 이미지를 기초로 라이브니스 검사를 수행하여 상기 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에 나타난 얼굴 영역의 정보와 상기 카드로부터 획득한 얼굴 이미지에 기초하여 얼굴 인증 결과를 결정할 수 있다.
- [6] 상기 제어부는, 상기 적외선 이미지를 기초로 라이브니스 검사를 수행하여

상기 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에 나타난 얼굴 영역의 정보와 상기 카드로부터 획득한 얼굴 이미지에 기초하여 얼굴 인증 결과를 결정할 수 있다.

- [7] 상기 제어부는, 상기 사용자 인증 결과가 결정된 경우, 상기 획득한 적외선 이미지, 상기 획득한 컬러 이미지 및 상기 획득한 얼굴 이미지를 저장부에서 삭제하도록 제어할 수 있다.
- [8] 상기 제어부는, 상기 적외선 이미지에서 상기 적외선이 사용자의 동공에 반사되어 나타난 반사점의 존재 여부를 검사하고, 상기 적외선 이미지에 상기 반사점이 존재하지 않는 것으로 결정된 경우, 상기 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [9] 상기 제어부는, 상기 적외선 이미지에 동공의 반사점이 존재하는 것으로 결정된 경우, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나와 상기 카드에 저장된 얼굴 이미지에 기초하여 얼굴 인증을 수행할 수 있다.
- [10] 상기 제어부는, 상기 적외선 이미지에서 상기 사용자의 얼굴 영역의 존재 여부를 검사하고, 상기 적외선 이미지에서 상기 얼굴 영역의 검출이 실패한 경우, 상기 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [11] 상기 제어부는, 상기 적외선 이미지에서 적외선의 투과 현상 및 포화 현상 중 적어도 하나가 발생하였는지 여부를 검사하고, 상기 투과 현상 및 상기 포화 현상 중 적어도 하나가 발생한 경우 상기 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [12] 상기 카드는, 암호화된 얼굴 이미지를 포함하는 보안 카드이고, 상기 제어부는, 상기 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 상기 카드 리더기를 통해 획득한 암호화된 얼굴 이미지에서 제1 얼굴 특징을 추출하고, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에서 제2 얼굴 특징을 추출하고, 상기 제1 얼굴 특징과 상기 제2 얼굴 특징 간의 비교 결과에 기초하여 얼굴 인증 결과를 결정할 수 있다.
- [13] 일 실시예에 따른 사용자 인증 방법은, 카드 리더기를 통해 카드에 저장된 얼굴 이미지를 획득하는 단계; 사용자를 향해 적외선을 방사하는 단계; 사용자의 얼굴 영역을 포함하는 적외선 이미지와 상기 사용자의 얼굴 영역을 포함하는 컬러 이미지를 획득하는 단계; 및 상기 적외선 이미지, 상기 컬러 이미지 및 상기 얼굴 이미지 중 적어도 하나에 기초하여 사용자 인증 결과를 결정하는 단계를 포함하고, 상기 사용자 인증 결과를 결정하는 단계는, 상기 적외선 이미지를 기초로 라이브니스 검사를 수행하여 상기 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에 나타난 얼굴 영역의 정보와 상기 카드로부터 획득한 얼굴 이미지에 기초하여 얼굴 인증 결과를 결정하는 단계를 포함할 수 있다.
- [14] 일 실시예에 따른 사용자 인증 방법은, 상기 사용자 인증 결과가 결정된 경우, 상기 획득한 적외선 이미지, 상기 획득한 컬러 이미지 및 상기 획득한 얼굴

이미지를 저장부에서 삭제하는 단계를 더 포함할 수 있다.

- [15] 상기 사용자 인증 결과를 결정하는 단계는, 상기 적외선 이미지에서 상기 적외선이 사용자의 동공에 반사되어 나타난 반사점의 존재 여부를 검사하는 단계; 및 상기 적외선 이미지에 상기 반사점이 존재하지 않는 것으로 결정된 경우, 상기 사용자 인증 결과를 인증 실패로 결정하는 단계를 포함할 수 있다.
- [16] 상기 사용자 인증 결과를 결정하는 단계는, 상기 적외선 이미지에 동공의 반사점이 존재하는 것으로 결정된 경우, 상기 카드에 저장된 얼굴 이미지와, 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에 기초하여 얼굴 인증을 수행하는 단계를 포함할 수 있다.
- [17] 상기 사용자 인증 결과를 결정하는 단계는, 상기 적외선 이미지에서 상기 사용자의 얼굴 영역의 존재 여부를 검사하는 단계; 및 상기 적외선 이미지에서 상기 얼굴 영역의 검출이 실패한 경우, 상기 사용자 인증 결과를 인증 실패로 결정하는 단계를 포함할 수 있다.
- [18] 상기 사용자 인증 결과를 결정하는 단계는, 상기 적외선 이미지에서 적외선의 투과 현상 및 포화 현상 중 적어도 하나가 발생하였는지 여부를 검사하는 단계; 및 상기 투과 현상 및 상기 포화 현상 중 적어도 하나가 발생한 경우 상기 사용자 인증 결과를 인증 실패로 결정하는 단계를 포함할 수 있다.
- [19] 상기 사용자 인증 결과를 결정하는 단계는, 상기 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 상기 카드 리더기를 통해 획득한 암호화된 얼굴 이미지에서 제1 얼굴 특징을 추출하는 단계; 상기 컬러 이미지 및 상기 적외선 이미지 중 적어도 하나에서 제2 얼굴 특징을 추출하는 단계; 및 상기 제1 얼굴 특징과 상기 제2 얼굴 특징 간의 비교 결과에 기초하여 얼굴 인증 결과를 결정하는 단계를 포함할 수 있다.

도면의 간단한 설명

- [20] 도 1은 일 실시예에 따른 보안 카드를 활용한 사용자 인증 시스템의 개요를 설명하기 위한 도면이다.
- [21] 도 2는 일 실시예에 따른 보안 카드와 사용자 인증 장치를 포함하는 사용자 인증 시스템의 구성을 도시하는 도면이다.
- [22] 도 3은 일 실시예에 따른 사용자 인증 장치의 동작을 설명하기 위한 도면이다.
- [23] 도 4는 일 실시예에 따른 사용자 인증 방법의 동작을 설명하기 위한 흐름도이다.

발명의 실시를 위한 최선의 형태

- [24] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 그러나, 실시예들에는 다양한 변경이 가해질 수 있어서 특허출원의 권리 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 실시예들에 대한 모든 변경, 균등물 내지 대체물이 권리 범위에 포함되는 것으로 이해되어야 한다.
- [25] 실시예에서 사용한 용어는 단지 설명을 목적으로 사용된 것으로, 한정하려는

의도로 해석되어서는 안된다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

- [26] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [27] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.
- [28] 도 1은 일 실시예에 따른 보안 카드를 활용한 사용자 인증 시스템의 개요를 설명하기 위한 도면이다.
- [29] 도 1을 참조하면, 사용자(110)는 사용자 인증 장치(130)를 통해 사용자 인증을 시도할 수 있다. 본 명세서에서, 사용자(110)는 사용자 인증 장치(130)에 사용자 인증을 시도하고자 하는 사람을 가리킬 수 있으며, 인증 대상자로도 지칭될 수 있다. 사용자(110)는 사용자 인증을 위해 사용자 인증 장치(130)에 카드를 인식시킬 수 있고, 사용자 인증 장치(130)는 카드가 인식되면 사용자 인증 절차를 수행할 수 있다. 사용자 인증 절차는 검사 대상자가 살아있는 진짜 객체(genuine object)인지, 아니면 종이, 사진, 디지털 기기, 모형 등의 가짜 객체(fake object)인지 여부를 구별하는 라이브니스 검사 과정과 얼굴 이미지에 기초하여 인증 결과를 결정하는 얼굴 인증 과정을 포함할 수 있다.
- [30] 일 실시예에서, 사용자 인증 절차는 카드의 유효성 여부를 판단하는 과정을 포함할 수 있다. 사용자 인증 장치(130)는 카드가 인식되면 카드로부터 카드 정보를 수신하고, 수신한 카드 정보(예, 카드 식별 정보 등)를 기초로 해당 카드가 유효한 카드인지 여부를 결정할 수 있다. 사용자 인증 장치(130)는 해당 카드가 유효한 카드인 것으로 결정되면 라이브니스 검사 과정과 얼굴 인증 과정의 사용자 인증 절차를 계속 수행하고, 해당 카드가 유효한 카드가 아닌 것으로 결정되면 사용자 인증 절차를 중단하고 사용자(110)의 접근을 차단할 수 있다.
- [31] 본 명세서에서, 카드는 얼굴 이미지를 포함하는 보안 카드(120)일 수 있다. 보안 카드(120)는 예를 들어 얼굴 이미지가 압축 또는 암호화되어 저장되어 있는 생체 ID 카드일 수 있다. 보안 카드(120)가 얼굴 이미지를 저장함으로써, 다른

시스템에서 얼굴 인증 알고리즘이 변경되더라도 기존에 발급된 보안 카드가 호환되어 사용될 수 있다는 장점을 제공한다.

- [32] 실시예에 따라, 보안 카드(120)에는 이름, 이메일 주소, 고유 식별 부호, 개인 키, 공개 키, 인증서, 개인 데이터 등의 정보가 더 암호화되어 저장되어 있을 수 있다. 사용자(110)는 보안 카드(120)를 활용하여 사용자 인증 장치(130)에 사용자 인증을 시도할 수 있으며, 사용자 인증 장치(130)는 보안 카드(120)에서 획득한 암호화된 얼굴 이미지와 함께 사용자(110)의 얼굴을 촬영한 이미지를 이용하여 사용자 인증을 수행할 수 있다. 이 때, 사용자 인증 장치(130)는 이미지 획득부(140)를 통해 사용자(110) 얼굴에 대한 컬러 이미지와 적외선 이미지를 획득할 수 있다. 사용자 인증 장치(130)는 적외선 이미지 및/또는 컬러 이미지를 통해 사용자(110)에 대한 라이브니스 검사를 수행하며, 보안 카드(120)로부터 획득한 얼굴 이미지와 컬러 이미지 및/또는 적외선 이미지에 기초하여 얼굴 인증을 수행할 수 있다.
- [33] 사용자(110)가 사용자 인증 장치(130)의 카드 리더기(150)에 보안 카드(120)를 태그하는 경우, 보안 카드(120)에 저장된 생체 정보(예, 얼굴 이미지)가 카드 리더기(150)를 통해 사용자 인증 장치(130)에 전송될 수 있다. 카드 리더기(150)는 근거리 무선 통신 기능을 수행할 수 있는 통신부(미도시)를 포함할 수 있다. 사용자 인증 장치(130)는 이미지 획득부(140)를 통해 사용자(110)의 얼굴(160)에 관한 얼굴 이미지를 획득하고, 실시간으로 이미지 분석을 수행하는 것에 의해 보안 카드(120)로부터 획득한 얼굴 이미지와, 얼굴 이미지(컬러 이미지 및/또는 적외선 이미지)에 나타난 얼굴 이미지를 비교하여 얼굴 인증을 수행할 수 있다.
- [34] 보안 카드(120)의 경우, 보안 카드(120)를 소유한 사용자(110)가 실제로 정당한 권한이 있는지 여부를 판단하기 어려운 측면이 있는데, 사용자 인증 장치(130)는 카메라를 통해 사용자(110)의 얼굴(160)을 촬영하여 얼굴 이미지를 획득하고, 획득한 얼굴 이미지와 보안 카드(120)로부터 획득한 얼굴 이미지에 기초하여 얼굴 인증을 수행함으로써 보안 카드(120)의 단점을 보완하여 사용자 인증의 정확도와 보안성을 개선할 수 있다. 또한, 사용자 인증 장치(130)는 사용자 인증 결과가 도출되면, 사용자 인증 과정에서 이용된 데이터(예, 보안 카드(120)로부터 획득한 얼굴 이미지, 이미지 획득부(140)를 통해 획득한 컬러 이미지 및 적외선 이미지 등)를 삭제함으로써, 생체 정보의 유출로 인해 발생할 수 있는 문제점들을 미연에 방지할 수 있다. 또한, 사용자 인증 장치(130)는 단순히 얼굴 인증을 수행하는 것 뿐만 아니라 라이브니스 검사를 수행함으로써, 모형이나 사진, 디스플레이 장치에 의한 스푸핑 공격을 효과적으로 걸러 내어 사용자 인증의 정확도를 개선시킬 수 있다.
- [35] 따라서, 본 명세서에서 제안하는 사용자 인증 장치(130)와 사용자 인증 방법에 의하면, 기존의 보안 카드(120)만을 이용하는 방식이 가지는 단점들과 생체 인식만을 이용한 방식이 가지는 단점들을 동시에 효과적으로 극복하여

정확도가 높은 사용자 인증 기술의 구현이 가능해 진다.

- [36] 이하, 사용자 인증 장치(130)와 사용자 인증 장치(130)에 의해 수행되는 사용자 인증 방법을 보다 자세히 설명한다.
- [37] 도 2는 일 실시예에 따른 보안 카드와 사용자 인증 장치를 포함하는 사용자 인증 시스템의 구성을 도시하는 도면이다.
- [38] 도 2를 참조하면, 사용자 인증 시스템은 보안 카드(120)와 사용자 인증 장치(130)를 포함한다. 보안 카드(120)는 보안 카드(120)에 대응하는 사용자의 얼굴 이미지를 포함할 수 있다. 실시예에 따라, 보안 카드(120)는 해당 사용자와 관련된 개인 정보나 고유 식별 부호에 대한 정보를 더 포함할 수도 있다.
- [39] 일 실시예에서, 보안 카드(120)는 13.56MHz의 주파수를 사용하는 근거리 통신이 가능한 스마트 카드 계열의 카드일 수 있다. 보안 카드(120)는 사용자 인증 이벤트의 발생 시 암호화되어 저장된 정보를 사용자 인증 장치(130)로 전송하는 사용자 인증용 도구로 이용될 수 있다. 보안 카드(120)는 마이크로칩(220), 마이크로칩(220)과 연결된 안테나(210), 얼굴 이미지와 그 밖에 관련 정보를 저장하는 저장부(미도시)를 포함할 수 있다. 안테나(210)는 통신부(미도시)에 포함될 수도 있으며, 통신부는 근거리 무선 통신 기능을 가지는 외부 기기와 통신을 수행할 수 있다. 보안 카드(120)에 저장된 데이터는 암호화된 형태로 저장될 수 있다. 보안 카드(120)의 저장부에 저장된 데이터는 안테나(210)를 통해 보안 카드(120)의 외부로 전송될 수 있다.
- [40] 본 명세서에서 보안 카드(120)의 형태는 도면이나 실시예에 기술된 내용에 의해 한정되지 않으며, 다양한 형태로 구현될 수 있다. 예를 들어, 근접 통신을 수행할 수 있는 안테나와 특정 데이터를 저장하는 칩(chip)을 포함하는 것이면 형태에 상관없이 이용될 수 있다.
- [41] 일 실시예에 따른 사용자 인증 장치(130)는 광원(230), 적외선 카메라(250), 컬러 카메라(240), 카드 리더기(150), 제어부(260) 및 저장부(270)를 포함할 수 있다.
- [42] 사용자 인증 장치(130)에 의한 사용자 인증 이벤트의 발생은, 예를 들어 보안 카드(120)가 카드 리더기(150)에 태깅(tagging)되거나, 적외선 카메라(250)나 컬러 카메라(240)가 얼굴 영역을 검출하거나 또는 근접 센서를 통해 객체가 사용자 인증 장치(130)로 접근했음이 감지된 경우에 이루어질 수 있다. 사용자 인증 이벤트가 발생하는 경우, 라이브니스 검사 과정 및/또는 얼굴 인증 과정을 포함하는 일련의 사용자 인증 과정이 수행된다.
- [43] 일 실시예에서, 광원(230)은 사용자를 향해 적외선을 방사하는 적외선 광원을 포함할 수 있다. 적외선 카메라(250)는 사용자의 얼굴 영역을 포함하는 적외선 이미지를 획득할 수 있다. 컬러 카메라(240)는 사용자의 얼굴 영역을 포함하는 컬러 이미지를 획득할 수 있다. 카드 리더기(150)는 보안 카드(120)와 같은 카드가 인식되는 경우, 보안 카드(120)에 저장된 얼굴 이미지를 획득할 수 있다. 획득한 얼굴 이미지, 적외선 이미지 및/또는 컬러 이미지는 저장부(270)에 임시적으로 저장될 수 있다.

- [44] 제어부(260)는 사용자 인증 장치(130)의 전체적인 동작을 제어한다.
제어부(260)는 사용자 인증 장치(130)의 각 컴포넌트들의 제어 및 처리 데이터를 송수신하고, 사용자의 출입 권한에 따라 사용자 인증 성공 또는 사용자 인증 실패에 따른 동작을 실행시킬 수 있다.
- [45] 예를 들어, 제어부(260)는 보안 카드(120)로부터 획득한 얼굴 이미지, 적외선 이미지 및 컬러 이미지 중 적어도 하나에 기초하여 사용자 인증 결과를 결정하고, 사용자 인증 결과에 따른 제어 신호를 생성할 수 있다. 제어부(260)는 획득한 적외선 이미지를 기초로 사용자에게 대한 라이브니스 검사를 수행할 수 있다. 제어부(260)는 라이브니스 검사 결과, 사용자가 진짜 객체인 것으로 결정되는 경우 라이브니스 검사 결과가 성공인 것으로 결정할 수 있다. 이 경우, 제어부(260)는 얼굴 인증을 수행하여 얼굴 인증 결과를 결정할 수 있다. 제어부(260)는 라이브니스 검사 결과, 사용자가 가짜 객체인 것으로 결정되는 경우 라이브니스 검사 결과가 실패인 것으로 결정하고, 사용자 인증의 최종 결과가 실패한 것으로 결정하고 사용자의 접근을 차단하거나 출입을 제한하도록 제어할 수 있다.
- [46] 제어부(260)는 예를 들어 라이브니스 검사 과정에서 적외선 이미지의 포화 및 투과 여부를 검사하는 과정 및/또는 적외선 이미지에서 적외선이 사용자의 동공에 반사되어 나타난 반사점의 존재 여부를 검사하는 과정을 수행할 수 있다. 제어부(260)는 적외선 이미지에서 적외선의 투과 현상 및 포화 현상 중 적어도 하나가 발생하였는지 여부를 검사하고, 해당 투과 현상 및 포화 현상 중 적어도 하나가 발생한 경우 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [47] 다른 예로, 제어부(260)는 라이브니스 검사 과정에서 적외선 이미지 및/또는 컬러 이미지에서 전자 장치의 디스플레이나 사진, 종이 등에 대응하는 박스 영역의 검출 여부, 손가락 등의 검출 여부를 검사하는 과정을 수행할 수 있다. 제어부(260)는 해당 박스 영역이 검출되거나 또는 손가락 등의 신체 부위가 검출된 경우, 얼굴 인증을 수행하는 것 없이 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [48] 또한, 적외선 이미지에 적외선이 사용자의 동공에 반사되어 나타난 반사점이 존재하는 것으로 결정된 경우, 제어부(260)는 카드에 저장된 얼굴 이미지와, 컬러 이미지 및 적외선 이미지 중 적어도 하나에 기초하여 얼굴 인증을 수행할 수 있다. 이와 다르게, 적외선 이미지에 해당 반사점이 존재하지 않는 것으로 결정된 경우, 제어부(260)는 사용자 인증 결과를 인증 실패로 결정할 수 있다. 또한, 제어부(260)는 적외선 이미지 및/또는 컬러 이미지에서 사용자의 얼굴 영역의 존재 여부를 검사하여, 얼굴 영역의 검출이 실패한 경우, 사용자 인증 결과를 인증 실패로 결정할 수 있다.
- [49] 일 실시예에서, 제어부(260)는 적외선 이미지를 기초로 라이브니스 검사를 수행하여 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 컬러 이미지 및/또는 적외선 이미지에 나타난 얼굴 영역의 정보와 카드로부터 획득한 얼굴

이미지에 나타난 얼굴 영역의 정보에 기초하여 얼굴 인증 결과를 결정할 수 있다. 카드에 저장된 얼굴 이미지는 암호화된 얼굴 이미지일 수 있다.

- [50] 제어부(260)는 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 카드 리더기(150)를 통해 획득한 암호화된 얼굴 이미지에서 제1 얼굴 특징을 추출하고, 컬러 카메라(240)를 통해 획득한 컬러 이미지 및 적외선 카메라(250)를 통해 획득한 적외선 이미지 중 적어도 하나에서 제2 얼굴 특징을 추출할 수 있다. 일 실시예에서, 제어부(260)는 카드로부터 획득한 얼굴 이미지에서 얼굴의 특징점들을 추출 및 분석하여 제1 얼굴 특징을 결정하고, 컬러 이미지 및/또는 적외선 이미지에서 얼굴의 특징점들을 추출 및 분석하여 제2 얼굴 특징을 결정할 수 있다.
- [51] 제어부(260)는 제1 얼굴 특징과 제2 얼굴 특징을 비교하고, 제1 얼굴 특징과 제2 얼굴 특징 간의 비교 결과에 기초하여 얼굴 인증 결과를 결정할 수 있다. 예를 들어, 제어부(260)는 제1 얼굴 특징과 제2 얼굴 특징 간의 유사도를 계산하고, 계산된 유사도가 임계 값 이상인 경우에는 얼굴 인증 결과가 성공한 것으로 결정할 수 있다. 만약, 해당 유사도가 임계 값 미만인 경우에는 얼굴 인증 결과가 실패한 것으로 결정될 수 있다.
- [52] 사용자 인증 결과가 결정된 후, 제어부(260)는 사용자 인증 과정에서 획득한 적외선 이미지, 컬러 이미지 및 카드의 얼굴 이미지를 저장부(270)에서 삭제하도록 제어할 수 있다.
- [53] 사용자 인증 장치(130)는 기본적으로 사용자의 얼굴 인증에 의한 사용자 인증을 수행하나, 다른 인증 장치들과는 다르게 카드에 저장된 얼굴 이미지와 카메라를 통해 획득한 얼굴 이미지를 이용하여 오인식율과 오거부율을 현저히 낮추어 보안성과 사용 편리성을 높일 수 있다. 또한, 사용자 인증 장치(130)는 카드의 발급 과정에서 사용자 등록 과정이 수행되어, 사용자와 관리자에게 편의성을 제공하고, 플러그앤플레이 방식으로 손쉬운 설치 운용을 가능하게 하는 이점을 제공한다.
- [54] 그리고, 사용자 인증 시스템은 얼굴 인증을 위한 생체 정보가 사용자 인증 장치(130)나 다른 외부의 서버에 저장하는 방식이 아니라, 사용자가 소유한 보안 카드(120)에 저장되어 있는 얼굴 이미지 등과 같은 생체 정보를 사용자 인증 장치(130)에서 일회성으로 사용하는 방식으로 동작하므로 생체 정보에 대한 해킹으로부터 자유롭고 개인 정보의 관리 비용 및 인증 시스템의 구축 비용을 낮추는 효과를 제공한다.
- [55] 또한, 사용자 인증 시스템에서, 보안 카드(120)에 저장된 생체 정보는 사용자 인증 장치(130) 앞에서 사용자 인증을 시도하는 실제 사람으로부터 획득한 정보와 비교되므로, 보안 카드(120)가 분실되더라도 제3자의 보안 카드(120)의 편취 사용이 불가능하게 되어 사용자 인증 시스템은 우수한 보안성을 제공한다.
- [56] 도 3은 일 실시예에 따른 사용자 인증 장치의 동작을 설명하기 위한 도면이다.
- [57] 도 3을 참조하면, 사용자 인증 장치는 카드 리더기(150)에 보안 카드(120)의

접근이 인식되어 사용자 인증 이벤트가 발생하는지 여부를 모니터링할 수 있다. 카드 리더기(150)를 통해서 보안 카드(120)의 접근이 인식되면, 사용자 인증 장치는 카드 리더기(150)를 통해 보안 카드(120)로부터 전달된 카드 정보에 기초하여 해당 보안 카드(120)가 인가된 보안 카드(120)인지 여부를 검사할 수 있다. 해당 보안 카드(120)가 인가된 보안 카드(120)인 경우, 사용자 인증 이벤트가 발생하고, 근거리 무선 통신을 통해 보안 카드(120)에 저장된 얼굴 이미지가 사용자 인증 장치에 전달될 수 있다. 해당 얼굴 이미지는 제어부(260)에 의해 복호화되고, 저장부(270)에 저장될 수 있다.

- [58] 제어부(260)는 보안 카드(120)로부터 획득한 얼굴 이미지를 분석하여 제1 생체 정보에 해당하는 제1 얼굴 특징을 추출할 수 있다. 예를 들어, 제1 얼굴 특징은 얼굴의 특징점 정보를 포함할 수 있다. 제어부(260)는 추출한 제1 얼굴 특징에 대한 정보를 저장부(270)에 임시적으로 저장할 수 있다.
- [59] 제어부(260)는 보안 카드(120)를 소지한 사용자의 얼굴을 촬영하도록 광원(230), 컬러 카메라(240) 및 적외선 카메라(240)를 활성화시킬 수 있다. 광원(230)은 사용자의 얼굴(160)을 향해 적외선을 방사할 수 있고, 적외선 카메라(250)는 광원(230)에서 방사된 적외선이 사용자의 얼굴(160)에 반사되어 되돌아온 반사광을 수광하여 사용자의 얼굴 영역이 나타난 적외선 이미지를 획득할 수 있다. 컬러 카메라(240)는 사용자의 얼굴(160)을 촬영하여 얼굴 영역이 나타난 컬러 이미지를 획득할 수 있다.
- [60] 제어부(260)는 획득한 적외선 이미지 및/또는 컬러 이미지에 기초하여 라이브니스 검사를 수행할 수 있다. 라이브니스 검사는 실제 사람의 얼굴과 사진, 모형, 영상 등을 통해 재현된 가짜 얼굴을 구분하기 위한 검사로서, 실제 사람의 얼굴이 아니라고 판단된 경우에는 라이브니스 검사 결과가 실패인 것으로 결정되고, 실제 사람의 얼굴인 것으로 판단된 경우에는 라이브니스 검사 결과가 성공인 것으로 결정될 수 있다.
- [61] 일 실시예에서, 라이브니스 검사는 광원(230)이 무작위 패턴의 적외선을 발광하고, 적외선 이미지에 투과 현상 및/또는 포화 현상이 나타나는지 여부를 확인하는 과정, 적외선 이미지에서 사용자의 얼굴 영역의 존재 여부나 적외선이 사용자의 동공에 반사되어 나타난 반사점의 존재 여부를 확인하는 과정을 포함할 수 있다. 이러한 과정은 적외선 이미지에서 사용자의 동공 영역을 검출하고, 검출된 동공 영역에서 반사점의 존재 여부를 검사하는 과정을 포함할 수 있다. 투과 현상이나 포화 현상이 발생한 것으로 확인된 경우나 해당 반사점이 검출되지 않은 경우, 라이브니스 검사 결과가 실패인 것으로 결정될 수 있다. 또한, 라이브니스 검사는 적외선 이미지 및/또는 컬러 이미지에서 전자 장치의 디스플레이나 사진, 종이 등에 대응하는 박스 영역의 검출 여부, 손가락 등의 검출 여부를 검사하는 과정을 수행할 수 있다. 적외선 이미지 및/또는 컬러 이미지에서 해당 박스 영역이 검출되거나 또는 손가락 등의 신체 부위가 검출된 경우, 라이브니스 검사 결과가 실패인 것으로 결정될 수 있다.

- [62] 라이브니스 검사 결과가 실패로 결정된 경우에는, 다음 단계로 진행되지 않고 사용자 인증 결과가 최종적으로 실패한 것으로 결정될 수 있다. 이와 반대로, 라이브니스 검사 결과가 성공으로 결정된 경우에는 얼굴 인증 절차를 동작시킬 수 있다.
- [63] 얼굴 인증 절차가 동작하는 경우, 제어부(260)는 컬러 이미지 및/또는 적외선 이미지를 분석하여 컬러 이미지로부터 제2 생체 정보에 해당하는 제2 얼굴 특징을 추출할 수 있다. 제2 얼굴 특징은 컬러 이미지 및/또는 적외선 이미지에서 추출한 얼굴의 특징점 정보를 포함할 수 있다. 제어부(260)는 컬러 이미지 및/또는 적외선 이미지에서 사용자의 얼굴 영역을 검출하고, 검출된 얼굴 영역에서 얼굴의 특징점들(예, 눈, 코, 입 꼬리, 눈썹 등의 영역에 위치하는 특징점들)을 제2 얼굴 특징으로서 추출할 수 있다. 제어부(260)는 추출한 제2 얼굴 특징에 대한 정보를 저장부(270)에 임시적으로 저장할 수 있다.
- [64] 제어부(260)는 제1 얼굴 특징과 제2 얼굴 특징을 비교하여 두 얼굴 특징 간의 유사도를 계산할 수 있다. 제어부(260)는 계산된 유사도가 특정한 조건을 만족(예, 임계 값 이상인 경우)시키면 얼굴 인증이 성공한 것으로 결정하고, 해당 조건을 만족시키지 않은 경우에는 얼굴 인증이 실패한 것으로 결정할 수 있다.
- [65] 제어부(260)는 사용자 인증 결과에 따라 사용자 인증 결과 정보를 전송하거나 사용자 인증 성공에 따른 대응 동작을 수행할 수 있다. 예를 들어, 라이브니스 검사 결과가 실패로 결정된 경우나 얼굴 인증 결과가 실패한 것으로 결정된 경우, 사용자 인증은 실패한 것으로 최종 결정되며, 제어부(260)는 게이트(310)로의 출입을 차단하는 제어 동작을 수행할 수 있다. 라이브니스 검사 결과와 얼굴 인증 결과가 모두 성공한 것으로 결정된 경우, 사용자 인증은 성공한 것으로 최종 결정되며, 제어부(260)는 게이트(310)로의 출입을 허용하여 게이트를 오픈(open)시키는 등의 제어 동작을 수행할 수 있다.
- [66] 라이브니스 검사 및/또는 얼굴 인증 과정을 포함하는 사용자 인증 과정이 모두 종료되면, 제어부(260)는 저장부(270)에서 사용자 인증에 사용된 데이터들(예, 보안 카드(120)로부터 획득된 정보, 적외선 이미지, 컬러 이미지, 사용자 인증 결과 정보 등)을 삭제하도록 제어할 수 있다. 따라서, 사용자 인증 장치는 등록된 사용자의 생체 정보를 저장하는 별도의 데이터베이스를 구비할 필요가 없으며, 이에 따라 생체 정보의 해킹 위험을 근본적으로 제거할 수 있다.
- [67] 도 4는 일 실시예에 따른 사용자 인증 방법의 동작을 설명하기 위한 흐름도이다. 사용자 인증 방법은 본 명세서에서 설명되는 사용자 인증 장치에 의해 수행될 수 있다.
- [68] 도 4를 참조하면, 단계(410)에서 사용자 인증 장치는 보안 카드와 같은 카드가 카드 리더기에 접근하는 것을 대기할 수 있다. 사용자 인증 장치의 카드 리더기는 보안 카드의 정보를 획득하기 위한 요청 신호를 방송하며 대기하고 있을 수 있다.
- [69] 단계(415)에서, 사용자 인증 장치는 카드가 인식되었는지 여부를

모니터링한다. 모니터링 결과로서, 카드가 인식되지 않은 경우, 사용자 인증 장치는 단계(410)로 되돌아가 계속 대기한다. 일 실시예에서, 사용자가 보안 카드를 사용자 인증 장치의 카드 리더기에 근접시키면, 근거리 무선 통신을 수행할 수 있는 카드 리더기는 보안 카드의 인가 여부를 확인할 수 있다. 예를 들어, 사용자 인증 장치는 보안 카드에 저장된 발급 코드나 고유 식별 부호를 검증하여 보안 카드가 인가된 카드인지 여부를 확인할 수 있다. 비인가된 카드인 것으로 확인된 경우, 사용자 인증 장치는 단계(410)의 대기 상태로 회귀한다.

- [70] 카드가 인가된 카드인 것으로 인식되는 경우, 사용자 인증 이벤트가 발생되고, 사용자 인증 장치는 단계(420)에서 카드 리더기를 통해 카드에 저장된 정보를 획득한다. 사용자 인증 장치는 예를 들어 카드 리더기를 통해 카드에 저장된 얼굴 이미지나 고유 식별 부호에 대한 정보를 획득할 수 있다. 사용자 인증 장치는 획득한 얼굴 이미지나 고유 식별 부호에 대한 정보를 복호화하여 임시적으로 저장할 수 있다.
- [71] 카드가 인식되는 경우 이외에도, 예를 들어 적외선 카메라나 컬러 카메라가 얼굴 영역을 검출하거나 또는 근접 센서를 통해 객체가 사용자 인증 장치로 접근했음이 감지된 경우에 사용자 인증 이벤트가 발생될 수 있다.
- [72] 단계(425)에서, 사용자 인증 장치는 카드 리더기를 통해 획득한 정보에서 제1 얼굴 특징을 추출한다. 사용자 인증 장치는 카드 리더기를 통해 획득한 암호화된 얼굴 이미지를 복호화하고, 복호화된 얼굴 이미지에서 제1 얼굴 특징을 추출할 수 있다. 예를 들어, 사용자 인증 장치는 복호화된 얼굴 이미지를 분석하여 얼굴의 특징점 정보를 추출할 수 있다. 사용자 인증 장치는 추출된 제1 얼굴 특징에 대한 정보를 저장부에 임시적으로 저장시킬 수 있다.
- [73] 단계(430)에서, 사용자 인증 장치는 광원을 활성화시킨다. 광원이 활성화됨에 따라 사용자를 향해 적외선이 방사된다.
- [74] 단계(435)에서, 사용자 인증 장치는 컬러 카메라를 통해 사용자 인증의 대상자인 사용자의 얼굴 영역이 나타난 컬러 이미지를 획득하고, 적외선 카메라를 통해 사용자의 얼굴 영역이 나타난 적외선 이미지를 획득한다. 사용자 인증 장치는 실시간으로 사용자의 얼굴 영역이 나타난 컬러 이미지와 적외선 이미지를 획득하고, 적외선 이미지, 컬러 이미지 및 카드로부터 획득한 얼굴 이미지 중 적어도 하나에 기초하여 사용자 인증 결과를 결정할 수 있다. 사용자 인증 결과를 결정하기 위해, 사용자 인증 장치는 라이브니스 검사와 얼굴 인증 과정을 수행할 수 있다.
- [75] 사용자 인증 장치는 단계(440)에서 사용자가 진짜 객체인지 여부를 구별하기 위한 라이브니스 검사를 수행하고, 단계(445)에서 라이브니스 검사 결과가 미리 설정된 조건을 만족시키는지 여부를 판단할 수 있다.
- [76] 예를 들어, 사용자 인증 장치는 컬러 이미지 및/또는 적외선 이미지에서 사용자의 얼굴 영역의 존재 여부를 검사할 수 있다. 적외선 이미지 및/또는 컬러 이미지에서 얼굴 영역의 검출이 실패한 경우, 사용자 인증 장치는 사용자 인증

결과를 인증 실패로 결정할 수 있다. 사용자 인증 장치는 컬러 이미지 및/또는 적외선 이미지에서 사용자의 얼굴 영역을 실시간으로 검출하는 동작을 수행하고, 특정 시간을 지나도록 얼굴 영역이 검출되지 않는 경우에는 라이브니스 검사 결과가 조건을 만족시키지 않는 것으로 결정하고 최종적으로 사용자 인증이 실패한 것으로 결정할 수 있다.

[77] 또한, 사용자 인증 장치는 적외선 이미지에서 적외선의 투과 현상 및 포화 현상 중 적어도 하나가 발생하였는지 여부를 검사하고, 해당 투과 현상 및 포화 현상 중 적어도 하나가 발생한 경우에는 라이브니스 검사 결과가 조건을 만족시키지 않는 것으로 결정하고 최종적으로 사용자 인증이 실패한 것으로 결정할 수 있다.

[78] 또한, 사용자 인증 장치는 적외선 이미지에서 적외선이 사용자의 동공에 반사되어 나타난 반사점의 존재 여부를 검사하고, 적외선 이미지에 해당 반사점이 존재하지 않는 것으로 결정된 경우에는 라이브니스 검사 결과가 조건을 만족시키지 않는 것으로 결정하고 최종적으로 사용자 인증이 실패한 것으로 결정할 수 있다.

[79] 또한, 사용자 인증 장치는 적외선 이미지 및/또는 컬러 이미지에서 전자 장치의 디스플레이나 사진, 종이 등에 대응하는 박스 영역의 검출 여부, 손가락 등의 검출 여부를 검사하는 과정을 수행하고, 해당 박스 영역이나 손가락 등의 신체 부위가 검출된 경우, 라이브니스 검사 결과가 조건을 만족시키지 않는 것으로 결정하고 최종적으로 사용자 인증이 실패한 것으로 결정할 수 있다.

[80] 라이브니스 검사 결과가 해당 조건을 만족시키지 않는 경우, 사용자 인증 장치는 사용자 인증 과정을 종료시키고, 단계(460)을 통해 저장부에서 관련 데이터를 삭제한다.

[81] 라이브니스 검사 결과가 조건을 만족시켜, 라이브니스 검사 결과가 성공인 것으로 결정된 경우, 사용자 인증 장치는 얼굴 인증 과정을 수행할 수 있다. 예를 들어, 적외선 이미지에 동공의 반사점이 존재하는 것으로 결정된 경우, 사용자 인증 장치는 라이브니스 검사 결과가 조건을 만족시키는 것으로 결정할 수 있다. 이 경우, 카드에 저장된 얼굴 이미지와 컬러 이미지 및/또는 적외선 이미지에 기초하여 얼굴 인증을 수행하는 단계가 수행되어, 얼굴 인증 결과가 결정될 수 있다.

[82] 라이브니스 검사 결과가 성공인 것으로 결정되어 얼굴 인증 과정이 수행되는 경우, 단계(450)에서 사용자 인증 장치는 컬러 이미지 및/또는 적외선 이미지에서 제2 얼굴 특징을 추출한다. 사용자 인증 장치는 컬러 이미지 및/또는 적외선 이미지를 분석하여 컬러 이미지 및/또는 적외선 이미지에 나타난 얼굴 이미지를 분석하여 얼굴의 특징점 정보를 추출할 수 있다. 사용자 인증 장치는 추출된 제2 얼굴 특징에 대한 정보를 저장부에 임시적으로 저장시킬 수 있다.

[83] 단계(455)에서, 사용자 인증 장치는 제1 얼굴 특징과 제2 얼굴 특징에 기초하여 얼굴 인증 결과를 결정한다. 사용자 인증 장치는 제1 얼굴 특징과 제2 얼굴 특징을 비교하여 유사도를 결정하고, 제1 얼굴 특징과 제2 얼굴 특징 간의 비교

결과에 기초하여 얼굴 인증 결과를 결정할 수 있다. 일 실시예에서, 사용자 인증 장치는 제1얼굴 특징과 제2 얼굴 특징이 각각 나타내는 특징점들을 비교하여 동일 사용자의 얼굴인지 여부를 판단하여 얼굴 인증을 수행할 수 있다.

- [84] 얼굴 인증 결과가 성공이면, 사용자 인증 장치는 사용자 인증 성공에 대응하는 처리 동작을 수행할 수 있다. 얼굴 인증 결과가 실패이면, 사용자 인증 장치는 사용자의 접근을 차단하거나 허용하지 않는 등의 사용자 인증 실패에 대응하는 처리 동작을 수행할 수 있다.
- [85] 사용자 인증 결과가 결정되는 경우, 사용자 인증 장치는 단계(460)에서 저장부에서 관련 데이터를 삭제한다. 예를 들어, 사용자 인증 결과가 결정된 경우, 사용자 인증 장치는 사용자 인증 과정에서 획득한 적외선 이미지, 컬러 이미지 및 카드로부터 획득한 얼굴 이미지를 저장부에서 삭제할 수 있다. 따라서, 사용자 인증 과정 이후에는 사용자 인증을 시도한 사용자에 대한 생체 정보가 사용자 인증 장치나 다른 장치에 잔존하지 않게 된다.
- [86] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate 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(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 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 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [87] 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), 및 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.

- [88] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [89] 그러므로, 다른 구현들, 다른 실시예들 및 청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.