(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0053438
(43) 공개일자 2025년04월22일

(51) 국제특허분류(Int. Cl.)
G07C 9/00 (2020.01) *E05B 9/00* (2014.01)
G01S 17/06 (2006.01) *G06F 21/31* (2013.01)
G07C 9/30 (2020.01)
(52) CPC특허분류
G07C 9/00944 (2013.01)
E05B 9/002 (2013.01)
(21) 출원번호 10-2023-0136692
(22) 출원일자 2023년10월13일
심사청구일자 2023년10월13일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
박기웅
서울특별시 광진구 능동로17길 21, 304호(화양동)
이세한
서울특별시 광진구 광나루로13길 4, 404호(군자동)
(74) 대리인
양성보

전체 청구항 수 : 총 10 항

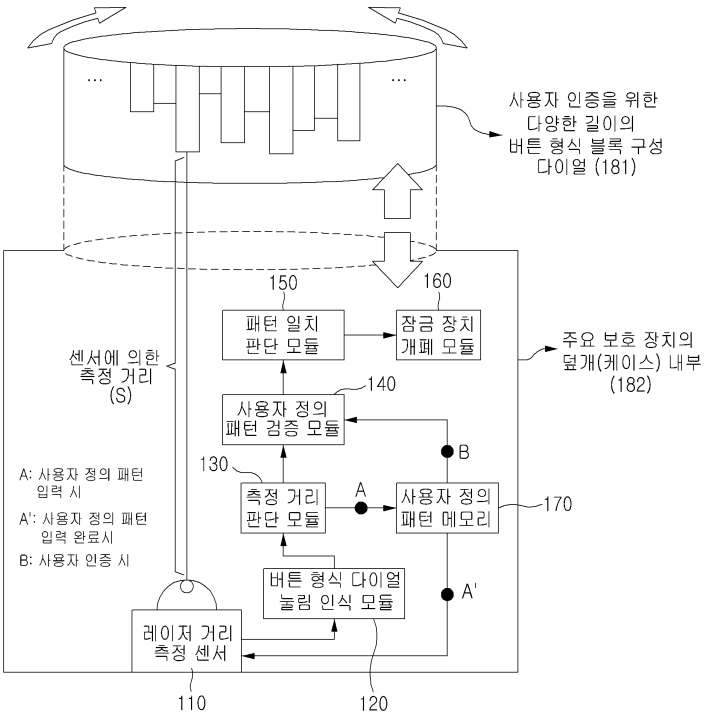
(54) 발명의 명칭 **버튼 형식의 블록 구성 다이얼 및 거리 측정 센서를 활용한 다회성 사용자 인증 기반의 주요 보호 장치 안티 탬퍼링 메커니즘 및 그 사용자 인증 방법 및 시스템**

(57) 요 약

주요 보호 장치 안티 탬퍼링 사용자 인증 방법 및 시스템이 제시된다. 본 발명에서 제안하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템은 다양한 길이를 갖는 버튼 형식의 블록 구성 다이얼, 주요 보호 장치의 덮개를 분해 및 조립하는 디지털 잠금 장치, 상기 주요 보호 장치의 덮개를 분해 및 조립할 수 있도록 개폐 여부를 판단

(뒷면에 계속)

대 표 도 - 도1



및 제어하는 잠금 장치 개폐 모듈, 버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단하는 버튼 형식 다이얼 눌림 인식 모듈, 사용자 정의 인증 패턴을 저장하는 사용자 정의 패턴 메모리, 레이저 거리 측정 센서에 의해 측정되는 블록 구성 다이얼에 구성되어 있는 상이한 길이의 블록들과 레이저 거리 측정 센서 사이의 블록-센서 간 거리 값을 측정 및 판단하는 측정 거리 판단 모듈, 측정된 블록-센서 간 거리 값과 사용자 정의 인증 패턴을 비교 및 분석하여 검증하는 사용자 정의 패턴 검증 모듈 및 사용자가 정의한 모든 패턴이 일치하였는지를 판단하는 패턴 일치 판단 모듈을 포함한다.

(52) CPC특허분류
G01S 17/06 (2013.01)
G06F 21/31 (2013.01)
G07C 9/30 (2020.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711193909
과제번호 2021-0-01816-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성
연구과제명 메타버스 자율트윈 핵심기술 연구
기 여 율 10/100
과제수행기관명 세종대학교 산학협력단
연구기간 2023.01.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711195724
과제번호 00228996
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 실감콘텐츠핵심기술개발
연구과제명 우주상황인식을 위한 실-가상 연동형 국방 메타버스 기반기술 개발
기 여 율 70/100
과제수행기관명 한국전자통신연구원
연구기간 2023.04.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711193732
과제번호 2022-0-00701-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 국방ICT융합(정보화)
연구과제명 국방정보통신망-상용망(5G) 연동을 위한 보안 기술개발
기 여 율 20/100
과제수행기관명 세종대학교 산학협력단
연구기간 2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

다양한 길이를 갖는 버튼 형식의 블록 구성 다이얼;

주요 보호 장치의 덮개를 분해 및 조립하는 디지털 잠금 장치;

상기 주요 보호 장치의 덮개를 분해 및 조립할 수 있도록 개폐 여부를 판단 및 제어하는 잠금 장치 개폐 모듈;

버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단하는 버튼 형식 다이얼 눌림 인식 모듈;

사용자 정의 인증 패턴을 저장하는 사용자 정의 패턴 메모리;

레이저 거리 측정 센서에 의해 측정되는 블록 구성 다이얼에 구성되어 있는 상이한 길이의 블록들과 레이저 거리 측정 센서 사이의 블록-센서 간 거리 값을 측정 및 판단하는 측정 거리 판단 모듈;

측정된 블록-센서 간 거리 값과 사용자 정의 인증 패턴을 비교 및 분석하여 검증하는 사용자 정의 패턴 검증 모듈; 및

사용자가 정의한 모든 패턴이 일치하였는지를 판단하는 패턴 일치 판단 모듈

을 포함하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 2

제1항에 있어서,

상기 버튼 형식 다이얼 눌림 인식 모듈은,

사용자가 버튼 형식의 블록 구성 다이얼을 두 번 누르는 행동을 인식하는 경우, 사용자 정의 인증 패턴 입력 프로세스가 동작하도록 하는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 3

제2항에 있어서,

상기 측정 거리 판단 모듈은,

사용자 정의 인증 패턴 입력 프로세스에 있어서,

원하는 블록을 사용자 정의 인증 패턴으로 등록하기 위해 다이얼이 눌려진 상태에서 원하는 블록을 레이저 거리 측정 센서 상에 위치시킨 후 누르고 있는 다이얼을 떼면, 해당 위치에서의 블록-센서 간 거리를 측정하여 해당 블록-센서 간 거리 값을 사용자 정의 인증 패턴으로 등록하는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 4

제1항에 있어서,

상기 버튼 형식 다이얼 눌림 인식 모듈은,

사용자가 버튼 형식의 블록 구성 다이얼을 한 번 누르는 행동을 인식하는 경우, 해당 위치에 존재하는 블록과 레이저 거리 측정 센서 사이의 거리 값을 기반으로 사용자 인증 프로세스가 동작하도록 하는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 5

제4항에 있어서,

상기 패턴 일치 판단 모듈은,

사용자 인증 프로세스에 있어서,

미리 입력된 사용자 정의 인증 패턴과 블록 구성 다이얼을 좌 또는 우로 돌려서 인증하기 위한 블록을 위치시키고, 블록 구성 다이얼을 한 번 누르고 뗀 상태에서의 블록-센서 간 거리 값을 비교하여 사용자 정의 인증 패턴의 일치 여부를 판단하고, 상기 미리 입력된 사용자 정의 인증 패턴은 입력된 각각의 블록-센서 간 거리 값으로 이루어진 복수의 길이의 숫자 배열 형태를 의미하는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 6

제5항에 있어서,

상기 잠금 장치 개폐 모듈은,

상기 사용자 정의 인증 패턴이 일치하는 경우, 상기 디지털 잠금 장치와 통신하여 덮개를 분해하도록 하고,

상기 사용자 정의 인증 패턴이 일치하지 않는 경우, 덮개를 분해하지 않는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템.

청구항 7

주요 보호 장치의 덮개를 개폐하기 위한 사용자 인증 과정에 필요한 사용자 정의 인증 패턴을 입력하기 위해 버튼 형식 다이얼 눌림 인식 모듈을 통해 버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단하는 단계 -상기 버튼 형식의 블록 구성 다이얼이 두 번 눌리는 것을 인식하는 경우, 사용자 정의 인증 패턴 입력 프로세스를 시작함-;

등록하고자 하는 블록이 누린 상태로 해당 블록 구성 다이얼을 좌 또는 우 방향으로 돌려 상기 등록하고자 하는 블록이 레이저 거리 측정 센서 상에 위치하도록 한 후 블록 구성 다이얼을 떼는 단계;

레이저 거리 측정 센서를 통해 블록-센서 간 거리를 측정하고, 측정 거리 판단 모듈을 통해 블록-센서 간 거리 값을 판단하는 단계; 및

상기 블록-센서 간 거리 값을 사용자 정의 패턴 메모리에 사용자 정의 인증 패턴으로 등록하는 단계

를 포함하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 정의 인증 패턴 입력 방법.

청구항 8

제7항에 있어서,

사용자 정의 인증 패턴 등록을 완료하기 위해서는 등록하고자 하는 블록을 사용자 정의 인증 패턴으로 등록 후, 해당 블록 구성 다이얼을 마지막 위치에서 더 이상 돌리지 않고 두 번 누르고 떼는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 정의 인증 패턴 입력 방법.

청구항 9

사용자 인증을 위해 인증하기를 원하는 블록 구성 다이얼을 누르지 않고 좌 또는 우 방향으로 돌려서 센서 상에 위치시키는 단계;

센서 상에 위치 한 해당 블록을 인증을 하기 위해 다이얼을 한 번 누르고 떼는 단계;

레이저 거리 측정 센서를 통해 해당 블록-센서 간 거리를 측정하고, 측정 거리 판단 모듈을 통해 블록-센서 간 거리 값을 판단하는 단계;

상기 블록-센서 간 거리 값을 사용자 인증을 위한 해당 블록으로 인식하고, 미리 등록된 사용자 정의 인증 패턴과 비교 분석하는 단계 -상기 미리 입력된 사용자 정의 인증 패턴은 입력된 각각의 블록-센서 간 거리 값으로 이루어진 복수의 길이의 숫자 배열 형태를 의미함-; 및

미리 등록된 사용자 정의 인증 패턴과 상기 블록-센서 간 거리 값이 모두 일치하는 경우, 사용자 인증이 완료된 것으로 판단하여 잠금 장치 개폐 모듈을 통해 주요 보호 장치 덮개의 디지털 잠금 장치와 통신하여 잠금을 해제하고 덮개를 분해하는 단계

를 포함하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 인증 방법.

청구항 10

제9항에 있어서,

상기 미리 등록된 사용자 정의 인증 패턴과 상기 블록-센서 간 거리 값이 일치하지 않는 경우, 사용자 인증 프로세스를 종료하는

주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 버튼 형식의 블록 구성 다이얼과 거리 측정 센서를 활용하여 기존의 주요한 보호 대상 장치의 덮개(다시 말해, 케이스)에 대한 탬퍼링 공격으로부터 반영구적으로 사용이 가능한 다회성 사용자 인증 메커니즘을 활용하여 주요 장치를 보호하고 탬퍼링 공격에 의한 역 분석, 물리적인 회로기판 손상 등의 방지를 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 오늘날 정보화 시대에는 스마트 헬스 케어, 스마트 센서 네트워크 시스템 등 다양한 산업 분야에 있어 사물인터넷 기술이 활용되고 있다. 특히 사용자의 편리성을 위해 사물인터넷 관련 장치들이 점점 소형화되어 제품이 출시되고 있으며 그 형태는 다양하게 나타나고 있다. 이러한 상황에서 사물인터넷 기술의 발전과 더불어 사물인터넷에 대한 보안 위협도 많이 증가하고 있는 상황이다. 그러나 시중에 출시된 제품을 인위적으로 분해하여 역분석을 시도하고 시스템의 구성을 그대로 따라 하는 범죄 행위가 일어나고 있으며, 이러한 행위를 통해 유사 제품을 만드는 산업 범죄와 시스템을 분석하여 악의적인 목적으로 취약점을 찾고 사이버 공격을 시도하는 경우가 발생하고 있는 상황이다. 현재 이러한 상황을 해결하기 위해 IoT 관련 제품을 출시할 때 장치 내부를 확인하기 어렵게 만들기 위해 다양한 씰링 기법 또는 안티 탬퍼링 기법(예를 들어, 특수 나사를 이용한 덮개 조립, 특수 접착제 또는 스티커를 이용한 덮개 조립 등)을 사용하고 있다. 하지만 특수 나사를 이용한 덮개 조립의 경우 나사모가 다른 경우가 많으며 해당 나사모와 맞는 특수 공구를 잃어버리거나 하게 되면 제품을 열 수 없는 경우가 발생하며, 특수 접착제 또는 스티커를 이용한 덮개 조립을 하게 되면 제품을 분해하고 다시 조립을 할 때 특수 접착제 또는 스티커를 새롭게 붙여야 하는 등 일회성 사용이라는 특성으로 인해 비용적 효과 측면에 있어 매우 불리하다는 단점이 존재한다.

[0003] 다이얼을 활용한 잠금 장치와 관련하여, 한국등록특허 제10-2495927호(2023.01.31)(이하, 특허문헌 1), 한국등록특허 제10-1245184호(2013.03.13)(이하, 특허문헌 2)와 같이 존재하지만, 특허문헌 1과 특허문헌 2를 실제 구현하기 위해서는 내부에 암호 입력을 위한 특수장치(예를 들어, 레버 및 기어 등)를 따로 제작하여 조립해야 하는 단점이 존재한다.

[0004] 따라서, 오늘날 정보화 시대에 발생할 수 있는 사물인터넷 환경 내 장치들에 대한 물리적인 위협 중 역분석 위협, 물리적 장치 내부 회로 기판 손상 위협, 산업 스파이에 의한 제품 복제 위협 등 주요 보호 장치 대상의 탬퍼링 공격을 막을 수 있는 방안이 필요하다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국등록특허 제10-2495927호(2023.01.31)

(특허문헌 0002) 한국등록특허 제10-1245184호(2013.03.13)

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적 과제는 탬퍼링 공격을 막기 위해 물리적인 장치를 이용하여 일회성 또는 희소성으로 구현을 하는 것보다 쉽게 구할 수 있는 버튼 형식의 블록 구성 다이얼 및 거리 측정 센서를 활용한 다회성 사용자 인증 기반의 주요 보호 장치 안티 탬퍼링 메커니즘 및 그 사용자 인증 방법 및 시스템을 제공하는데 있다. 버튼 형식의 블록 구성 다이얼과 거리 측정 센서를 활용하여 주요 보호 장치를 분해하기 위한 사용자 정의 패턴을 자유롭게 구현하고, 사용자가 원할 때 자유롭게 인증 패턴 변경이 가능하며, 주요 보호 장치를 최초 생산할 때 사용자 인증 장치를 함께 구현함으로써 반영구적으로 사용 가능하다.

과제의 해결 수단

[0007] 일 측면에 있어서, 본 발명에서 제안하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템은 다양한 길이를 갖는 버튼 형식의 블록 구성 다이얼, 주요 보호 장치의 덮개를 분해 및 조립하는 디지털 잠금 장치, 상기 주요 보호 장치의 덮개를 분해 및 조립할 수 있도록 개폐 여부를 판단 및 제어하는 잠금 장치 개폐 모듈, 버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단하는 버튼 형식 다이얼 눌림 인식 모듈, 사용자 정의 인증 패턴을 저장하는 사용자 정의 패턴 메모리, 레이저 거리 측정 센서에 의해 측정되는 블록 구성 다이얼에 구성되어 있는 상이한 길이의 블록들과 레이저 거리 측정 센서 사이의 블록-센서 간 거리 값을 측정 및 판단하는 측정 거리 판단 모듈, 측정된 블록-센서 간 거리 값과 사용자 정의 인증 패턴을 비교 및 분석하여 검증하는 사용자 정의 패턴 검증 모듈 및 사용자가 정의한 모든 패턴이 일치하였는지를 판단하는 패턴 일치 판단 모듈을 포함한다.

[0008] 상기 버튼 형식 다이얼 눌림 인식 모듈은 사용자가 버튼 형식의 블록 구성 다이얼을 두 번 누르는 행동을 인식하는 경우, 사용자 정의 인증 패턴 입력 프로세스가 동작하도록 한다.

[0009] 상기 측정 거리 판단 모듈은 사용자 정의 인증 패턴 입력 프로세스에 있어서 원하는 블록을 사용자 정의 인증 패턴으로 등록하기 위해 다이얼이 눌려진 상태에서 원하는 블록을 레이저 거리 측정 센서 상에 위치시킨 후 누르고 있는 다이얼을 떼면, 해당 위치에서의 블록-센서 간 거리를 측정하여 해당 블록-센서 간 거리 값을 사용자 정의 인증 패턴으로 등록한다.

[0010] 상기 버튼 형식 다이얼 눌림 인식 모듈은 사용자가 버튼 형식의 블록 구성 다이얼을 한 번 누르는 행동을 인식하는 경우, 해당 위치에 존재하는 블록과 레이저 거리 측정 센서 사이의 거리 값을 기반으로 사용자 인증 프로세스가 동작하도록 한다.

[0011] 상기 패턴 일치 판단 모듈은 사용자 인증 프로세스에 있어서 미리 입력된 사용자 정의 인증 패턴과 블록 구성 다이얼을 좌 또는 우로 돌려서 인증하기 위한 블록을 위치시키고, 블록 구성 다이얼을 한 번 누르고 뗀 상태에서의 블록-센서 간 거리 값을 비교하여 사용자 정의 인증 패턴의 일치 여부를 판단하고, 상기 미리 입력된 사용자 정의 인증 패턴은 입력된 각각의 블록-센서 간 거리 값으로 이루어진 복수의 길이의 숫자 배열 형태를 의미한다.

[0012] 상기 잠금 장치 개폐 모듈은 상기 사용자 정의 인증 패턴이 일치하는 경우, 상기 디지털 잠금 장치와 통신하여 덮개를 분해하도록 하고, 상기 사용자 정의 인증 패턴이 일치하지 않는 경우, 덮개를 분해하지 않는다.

[0013] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 정의 인증 패턴 입력 방법은 주요 보호 장치의 덮개를 개폐하기 위한 사용자 인증 과정에 필요한 사용자 정의 인증 패턴을 입력하기 위해 버튼 형식 다이얼 눌림 인식 모듈을 통해 버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단하는 단계 -상기 버튼 형식의 블록 구성 다이얼이 두 번 눌리는 것을 인식하는 경우, 사용자 정의 인증 패턴 입력 프로세스를 시작함-, 등록하고자 하는 블록이 누린 상태로 해당 블록 구성 다이얼을 좌 또는 우 방향으로 돌려 상기 등록하고자 하는 블록이 레이저 거리 측정 센서 상에 위치하도록 한 후 블록 구성 다이얼을 떼는 단계, 레이저 거리 측정 센서를 통해 블록-센서 간 거리를 측정하고, 측정 거리 판단 모듈을 통해 블록-센서 간 거리 값을 판단하는 단계 및 상기 블록-센서 간 거리 값을 사용자 정의 패턴 메모리에 사용자 정의 인증 패턴으로 등록하는 단계를 포함한다.

[0014] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 주요 보호 장치 안티 탬퍼링 사용자 인증 시스템의 사용자 인증 방법은 사용자 인증을 위해 인증하기를 원하는 블록 구성 다이얼을 누르지 않고 좌 또는 우 방향으로 돌려서 센서 상에 위치시키는 단계, 센서 상에 위치 한 해당 블록을 인증을 하기 위해 다이얼을 한 번 누르고 떼는 단

계, 레이저 거리 측정 센서를 통해 해당 블록-센서 간 거리를 측정하고, 측정 거리 판단 모듈을 통해 블록-센서 간 거리 값을 판단하는 단계, 상기 블록-센서 간 거리 값을 사용자 인증을 위한 해당 블록으로 인식하고, 미리 등록된 사용자 정의 인증 패턴과 비교 분석하는 단계 -상기 미리 입력된 사용자 정의 인증 패턴은 입력된 각각의 블록-센서 간 거리 값으로 이루어진 복수의 길이의 숫자 배열 형태를 의미함-, 미리 등록된 사용자 정의 인증 패턴과 상기 블록-센서 간 거리 값이 모두 일치하는 경우, 사용자 인증이 완료된 것으로 판단하여 잠금 장치 개폐 모듈을 통해 주요 보호 장치 덮개의 디지털 잠금 장치와 통신하여 잠금을 해제하고 덮개를 분해하는 단계를 포함한다.

발명의 효과

[0015] 본 발명의 실시예들에 따르면 버튼 형식의 블록 구성 다이얼과 레이저 거리 측정 센서를 활용하여 안티 탬퍼링 메커니즘을 구현하고 사용자 인증을 기반으로 주요 보호 장치 덮개(다시 말해, 케이스)의 비 인가된 해체를 막을 수 있으며, 사용자 인증에 있어 사용자 정의 인증 패턴을 자유롭게 입력하여 다양한 패턴으로 사용자 인증 방안을 구현할 수 있다. 이에 따라, 주요 보호 장치 관리자 및 사후 관리 서비스 담당자의 경우 내부 규정 등을 활용한 특별한 패턴 구현이 가능하다. 또한, 우연 또는 악의적인 방법으로 인증 패턴을 파악한 제3자가 존재하더라도 또 다른 인증 패턴으로 쉽고 간편하게 변경이 가능하여 안전하게 주요 보호 장치를 운용할 수 있다.

[0016] 본 발명의 실시예들에 따르면 기존의 다양한 안티 탬퍼링 방식보다 비용 효과적인 측면에 있어 매우 유리하다. 예를 들어, 특수 모양의 나사모를 사용하게 되면 일반적으로 판매되고 있는 공구는 사용할 수 없고 특수 모양 나사모에 맞는 특수목적의 공구를 새롭게 만들어야 하며 이는 비용적 측면에서 매우 불리하고 볼 수 있다. 또한, 특수 접착제 또는 일회성 스티커를 부착하게 되면 주요 보호 장치의 내부 모듈 업그레이드 또는 고장에 대한 대처 등을 위해 제품을 분해하고 재조립을 하는 과정에서 덮개(케이스)에 새로운 접착제를 바르거나 스티커를 부착해야 하는 등 비용이 계속 발생하게 된다는 단점이 존재한다. 본 발명의 실시예들에 따르면 안티 탬퍼링 메커니즘은 한 번 구현하여 장치가 인위적으로 파괴되거나 고장이 발생하여 사용하지 못하게 되는 경우 외에는 반영구적으로 사용이 가능하게 된다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 버튼 형식의 블록 구성 다이얼 및 거리 측정 센서를 활용한 다회성 사용자 인증 기반의 주요 보호 장치 안티 탬퍼링 메커니즘 및 사용자 인증 시스템의 구성을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘에서 사용자 정의 인증 패턴을 입력하는 방안에 대한 예시를 보여주는 그래프이다.

도 3은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘에서 사용자 인증을 하는 방법에 대한 예시를 보여주는 그래프이다.

도 4는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘을 활용할 수 있는 하나의 예시를 나타내는 도면이다.

도 5는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증을 위한 사용자 정의 인증 패턴 입력 방법을 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증 방법을 설명하기 위한 흐름도이다.

도 7은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 시스템 동작에서 전체 프로세스에 대한 상태 변화를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 버튼 형식의 블록 구성 다이얼 및 거리 측정 센서를 활용한 다회성 사용자 인증 기반의 주요 보호 장치 안티 탬퍼링 메커니즘 및 사용자 인증 시스템의 구성을 나타내는 도면이다.

[0021] 본 발명의 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘 및 사용자 인증 시스템 내의 구성 요소로는 크

게 H/W 모듈과 S/W 모듈로 나뉘어져 있다.

[0022] 본 발명의 실시예에 따른 H/W 모듈은 레이저 거리 측정 센서(110), 디지털 잠금 장치(또는 시건 장치)(도 4 참조), 잠금 장치 개폐 모듈(160)을 포함한다.

[0023] 본 발명의 실시예에 따른 레이저 거리 측정 센서(110)는 다양한 길이와 버튼 형식의 블록 구성 다이얼(181)과 해당 블록과 센서 간의 거리를 측정한다.

[0024] 본 발명의 실시예에 따른 디지털 잠금 장치(또는 시건 장치)(도 4 참조)는 주요 보호 장치의 덮개(다시 말해, 케이스)(182)를 분해 및 조립한다.

[0025] 본 발명의 실시예에 따른 잠금 장치 개폐 모듈(160)은 덮개(케이스)를 분해 및 조립할 수 있도록 개폐 여부를 판단 및 제어한다.

[0026] 본 발명의 실시예에 따른 S/W 모듈은 버튼 형식 다이얼 눌림 인식 모듈(120), 사용자 정의 패턴 메모리(170), 측정 거리 판단 모듈(130), 사용자 정의 패턴 검증 모듈(140), 패턴 일치 판단 모듈(150)을 포함한다.

[0027] 본 발명의 실시예에 따른 버튼 형식 다이얼 눌림 인식 모듈(120)은 버튼 형식의 블록 구성 다이얼이 눌렸는지 여부를 판단한다.

[0028] 본 발명의 실시예에 따른 사용자 정의 패턴 메모리(170)는 사용자 정의 인증 패턴이 저장된다.

[0029] 본 발명의 실시예에 따른 측정 거리 판단 모듈(130)은 레이저 거리 측정 센서(110)에 의해 블록 구성 다이얼에 구성되어 있는 여러 길이의 블록과 레이저 거리 측정 센서(110) 사이의 거리 값을 측정 및 판단한다.

[0030] 본 발명의 실시예에 따른 사용자 정의 패턴 검증 모듈(140)은 측정된 블록-센서 간 거리 값과 사용자 정의 인증 패턴을 비교 및 분석하여 검증한다.

[0031] 본 발명의 실시예에 따른 패턴 일치 판단 모듈(150)은 사용자가 정의한 모든 패턴이 일치하였는지를 판단한다.

[0032] 사용자 인증을 위한 다양한 길이와 버튼 형식의 블록 구성 다이얼(181)과 레이저 거리 측정 센서(110)가 본 발명의 실시예에 따른 큰 구성 요소이며, 사용자 인증 기반으로 주요 장치 보호를 위한 안티 탬퍼링 메커니즘의 동작 설명은 다음과 같다.

[0033] 본 발명의 실시예에 따르면, 사용자가 버튼 형식의 블록 구성 다이얼(181)을 누르는 행동을 인식하는 것으로 시작을 하게 되며, 사용자가 버튼 형식의 블록 구성 다이얼(181)을 한 번 누르게 되면 해당 위치에 존재하는 블록과 레이저 거리 측정 센서(110) 사이의 거리 값을 기반으로 사용자 인증 프로세스가 동작하고, 사용자가 버튼 형식의 블록 구성 다이얼(181)을 두 번 누르게 되면 사용자 정의 인증 패턴 입력 프로세스가 동작하게 된다.

[0034] 다음으로, 사전에 입력된 사용자 정의 인증 패턴(입력된 각각의 블록 - 레이저 거리 측정 센서 간 거리 값으로 이루어진 다양한 길이의 숫자 배열 형태)과 다이얼을 좌(반시계 방향) 또는 우(시계 방향)로 돌려서 인증하기 위한 블록을 위치시키고, 다이얼을 한 번 누르고 땐 상태에서의 블록-센서 간 거리 값을 비교하여 사용자 정의 인증 패턴의 일치 여부를 판단한다.

[0035] 패턴이 일치하면 주요 보호 장치에 부착되어 있는 디지털 잠금 장치(또는 시건 장치)와 통신하여 덮개(케이스)를 분해할 수 있도록 하며, 패턴이 일치하지 않으면 덮개(케이스)를 분해할 수 없도록 한다.

[0037] 도 2는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘에서 사용자 정의 인증 패턴을 입력하는 방안에 대한 예시를 보여주는 그래프이다.

[0038] 본 발명의 실시예에 따르면, 사용자 정의 인증 패턴을 입력하기 위해 사용자는 다이얼을 돌리지 않고 두 번 누르고 떼는 행동을 함으로써 사용자 정의 인증 패턴 입력 프로세스로 진입하게 된다.

[0039] 진입 후, 원하는 블록을 인증 패턴으로 등록하기 위해 다이얼을 누르고 있는 상태에서 원하는 블록을 레이저 거리 측정 센서 상에 위치시키고 누르고 있는 다이얼을 떼게 되면 블록-센서 간 거리를 측정하여 해당 거리 값을 사용자 정의 인증 패턴으로 등록하게 된다. 패턴을 더 등록하기 위해서는 이 과정을 반복하면 가능하다.

[0040] 도 2의 그래프는 사용자 정의 인증 패턴을 등록하는 과정의 버튼 형식의 블록 구성 다이얼 눌림 상태 변화(210)와 거리 측정 센서를 통한 거리 측정값(220)에 기반하여 어느 구간에서 등록이 이루어지는지를 나타낸 것이다.

[0041] 버튼 형식의 블록 구성 다이얼 눌림 상태 변화(210)에 따라, 원하는 블록이 위치할 수 있도록 다이얼을 누르고 있는 상태로 좌 또는 우로 다이얼을 돌리는 구간(211)과 원하는 블록에 위치시키고 누르고 있던 다이얼을 떼는 구간(212)을 나타내었다.

[0042] 거리 측정 센서를 통한 측정 거리(220)에 따라, 원하는 블록에 위치시키고 누르고 있던 다이얼을 떼는 순간(212) 해당 위치에서 측정된 블록-센서 간 거리값을 사용자 정의 인증 패턴으로 등록(221)한다.

[0044] 도 3은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘에서 사용자 인증을 하는 방법에 대한 예시를 보여주는 그래프이다.

[0045] 본 발명의 실시예에 따르면, 사용자 정의 인증 패턴 등록을 마치고, 사용자 인증을 위해 다이얼을 누르지 않고 인증하기를 원하는 블록이 센서 상에 위치할 수 있도록 좌(반시계 방향) 또는 우(시계 방향) 방향으로 돌리고 다이얼을 한 번 누르고 떼는 행동을 함으로써 사용자 인증 프로세스로 진입하게 된다.

[0046] 진입 후, 센서는 다이얼이 떼지는 구간에서 블록-센서 간 거리를 측정하여 측정된 거리 값과 사용자 정의 인증 패턴을 비교 분석하게 되고 검증을 하여 인증된 사용자가 맞는지 여부를 판단하게 된다. 복수의 블록을 사용자 정의 인증 패턴으로 등록한 경우 위 과정을 반복하여 수행하면 되고, 모든 패턴을 통과하게 되면 주요 보호 장치의 덮개(케이스)를 분해할 수 있게 된다.

[0047] 도 3의 그래프는 사용자 정의 인증 패턴이 등록되고 사용자 인증을 하는 과정의 버튼 형식의 블록 구성 다이얼 눌림 상태 변화(310)와 거리 측정 센서를 통한 거리 측정값(320)에 기반하여 어느 구간에서 사용자 인증이 이루어지는지를 나타낸 것이다.

[0048] 버튼 형식의 블록 구성 다이얼 눌림 상태 변화(310)에 따라, 사용자 인증을 위해 다이얼을 누르지 않고 원하는 블록이 위치할 수 있도록 다이얼을 좌 또는 우로 돌린 후, 다이얼을 한 번 누르고 떼는 구간(311)을 나타내었다.

[0049] 거리 측정 센서를 통한 측정 거리(320)에 따라, 원하는 블록으로 위치시키기 위해 다이얼을 누르지 않고 돌리는 구간(321)과 다이얼을 한 번 누르고 떼는 구간에 위치한 블록에서 블록-센서 간 거리값을 인증 블록으로 인식하고 인증을 진행(322)한다.

[0051] 도 4는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘을 활용할 수 있는 하나의 예시를 나타내는 도면이다.

[0052] 본 발명의 실시예에 따른 메커니즘을 활용하면 다양한 사물인터넷 장치를 생산할 때 버튼 형식의 블록 구성 다이얼 및 레이저 거리 측정 센서를 부착하여 인가되지 않은 주요 보호 장치 분해로부터 장치를 안전하게 보호할 수 있게 된다.

[0053] 도 4를 참조하면, 사용자 인증을 위한 버튼 형식의 블록 구성 다이얼(460) 및 회로 기판(440)에 추가된 레이저 거리 측정 센서(410)가 부착된 사물인터넷 장치의 예시를 나타내는 도면이다. 본 발명의 실시예에 따르면, 회로 기판(440)에는 잠금 장치 개폐 모듈(420)을 포함할 수 있다.

[0054] 본 발명의 실시예에 따르면, 사용자 인증 프로세스에서, 센서는 다이얼이 떼지는 구간에서 블록-센서 간 거리를 측정하여 측정된 거리 값과 사용자 정의 인증 패턴을 비교 분석하게 되고 검증을 하여 인증된 사용자가 맞는지 여부를 판단하게 된다.

[0055] 패턴이 일치하면 주요 보호 장치에 부착되어 있는 디지털 잠금 장치(또는 시건 장치)(430)와 통신하여 덮개(케이스)(450)를 분해할 수 있도록 하며, 패턴이 일치하지 않으면 덮개(케이스)(450)를 분해할 수 없도록 한다.

[0057] 도 5는 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증을 위한 사용자 정의 인증 패턴 입력 방법을 설명하기 위한 흐름도이다.

[0058] 본 발명의 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증을 위한 사용자 정의 인증 패턴 입력 방법은 다음과 같다:

[0059] 단계(510)에서, 주요 보호 장치의 덮개(케이스)를 개폐하기 위한 사용자 인증 과정에 필요한 사용자 정의 인증 패턴을 입력하기 위해 사용자(또는 제품 제작자, 사후 관리 서비스 담당자)가 다이얼을 돌리지 않고 두 번 누르고 떼는 행동을 하게 되면 자동으로 사용자 정의 인증 패턴 프로세스로 진입하게 된다. 이때, 이전에 등록된 사용자 정의 인증 패턴이 메모리에 존재한다면 해당 메모리에 등록된 패턴은 삭제되고 새로운 패턴이 등록될 준비를 하게 된다.

[0060] 단계(520)에서, 다이얼을 누른 상태로 사용자 정의 인증 패턴으로 등록하고자 하는 블록이 센서에 위치할 수 있도록 좌 또는 우 방향으로 돌리고 누르고 있는 다이얼을 땐다.

[0061] 단계(530)에서, 레이저 거리 측정 센서는 블록-센서 간 거리를 측정하여 측정 거리 판단 모듈을 통해 거리 값을 판단한다.

[0062] 단계(540)에서, 해당 거리 값을 사용자 정의 인증 패턴으로 등록한다.

[0063] 단계(550)에서, 인증 패턴을 더 등록하기 위해서는 단계(520)부터 반복한다.

[0064] 사용자 정의 인증 패턴 등록을 완료하기 위해서는 단계(560)에서, 마지막 다이얼 위치에서 더 이상 돌리지 않고 두 번 누르고 떼게 되면 사용자 정의 인증 패턴 등록 프로세스가 종료된다.

[0066] 도 6은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증 방법을 설명하기 위한 흐름도이다.

[0067] 본 발명의 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 사용자 인증 방법은 다음과 같다:

[0068] 사용자 정의 인증 패턴 등록 후, 단계(610)에서 사용자 인증을 위해 인증하기를 원하는 블록을 다이얼을 누르지 않고 좌 또는 우 방향으로 돌려서 센서 상에 위치시킨다.

[0069] 단계(620)에서, 해당 블록으로 인증을 하기 위해 다이얼을 그대로 한 번 누르고 뗀다.

[0070] 단계(630)에서, 거리 측정 센서는 블록-센서 간 거리를 측정하여 거리 값을 판단한다.

[0071] 단계(640)에서, 해당 거리 값을 사용자 인증을 위한 블록으로 인식하며 미리 등록되어 있는 사용자 정의 인증 패턴과 비교 분석을 실시한다.

[0072] 등록된 패턴 중 n번째 거리 값과 미리 등록되어 있는 사용자 정의 인증 패턴과 비교하여 일치하는 경우, 단계(650)에서 n개의 패턴을 모두 인증했는지를 검증하기 위해 모든 패턴에 대하여 단계(610)부터 반복한다.

[0073] 등록된 패턴 중 n번째 거리 값과 미리 등록되어 있는 사용자 정의 인증 패턴과 비교하여 불일치 하는 경우, 인증 프로세스를 종료한다.

[0074] 단계(660)에서, 등록된 n개의 패턴을 모두 통과하였다면 인증이 완료된 것으로 판단하고, 잠금 장치 개폐 모듈에 의해 주요 보호 장치 덮개(케이스)의 디지털 잠금 장치(또는 시건 장치)와 통신하여 잠금을 해제하여 덮개(케이스)를 분해할 수 있도록 한다.

[0076] 도 7은 본 발명의 일 실시예에 따른 주요 보호 장치 안티 탬퍼링 메커니즘의 시스템 동작에서 전체 프로세스에 대한 상태 변화를 나타내는 도면이다.

[0077] 본 발명에서 제안하는 메커니즘이 시스템으로 구성되어 동작을 하게 되었을 때, 시스템 내 프로세스 상태 변화에 대하여 설명하고 있으며, Idle 상태에서 버튼을 누르는 행동을 통해 변화되는 상태에 따라 사용자 정의 인증 패턴 등록 프로세스인지, 사용자 인증 프로세스인지를 구분하도록 되어 있는 것을 확인할 수 있다.

[0079] 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.

[0080] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

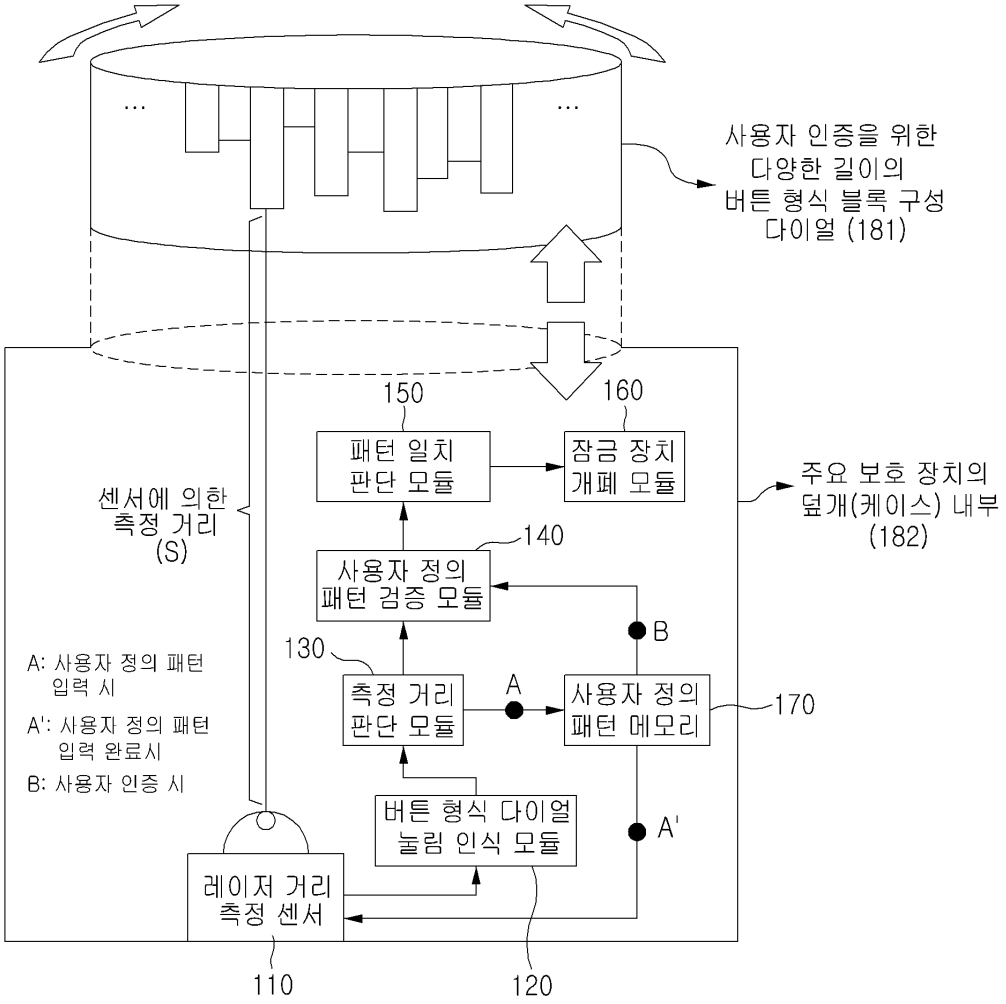
[0081] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0082] 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.

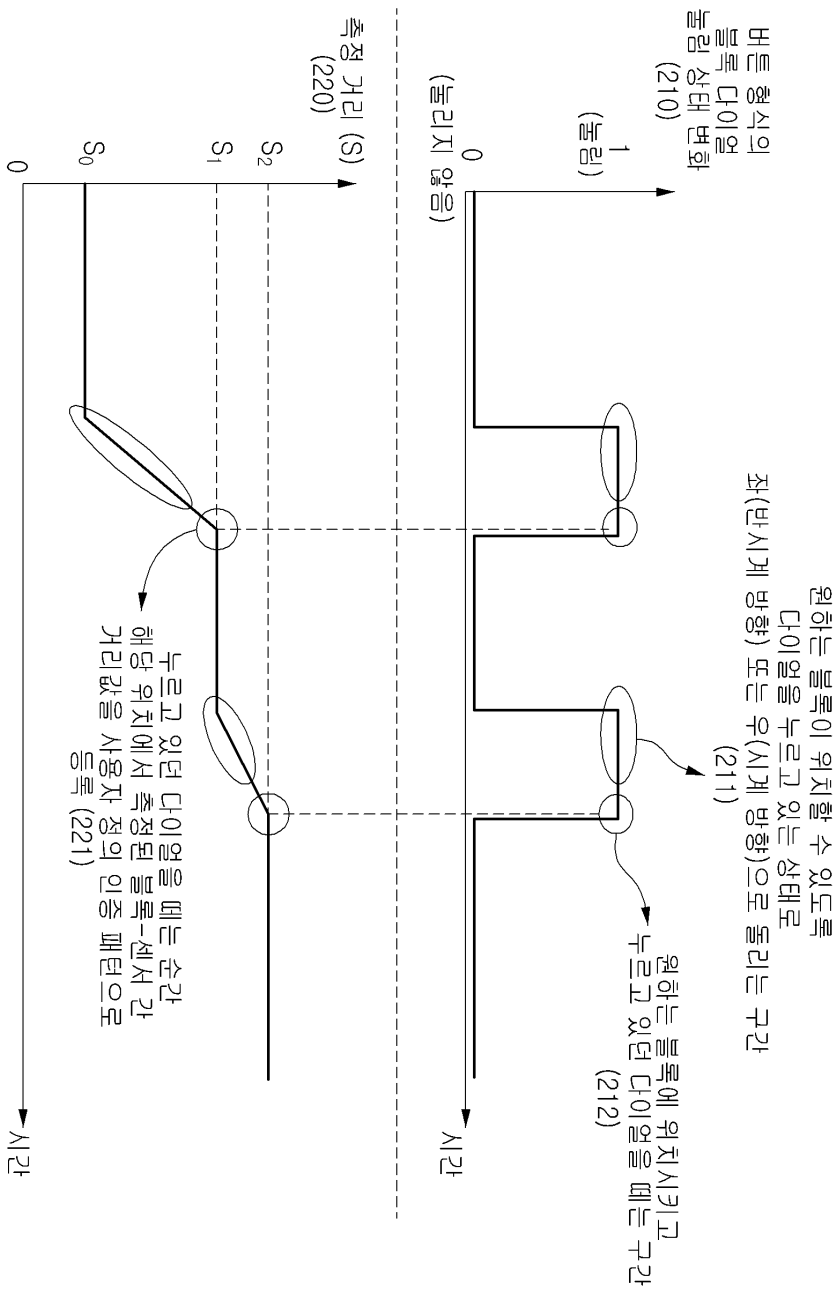
[0083] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

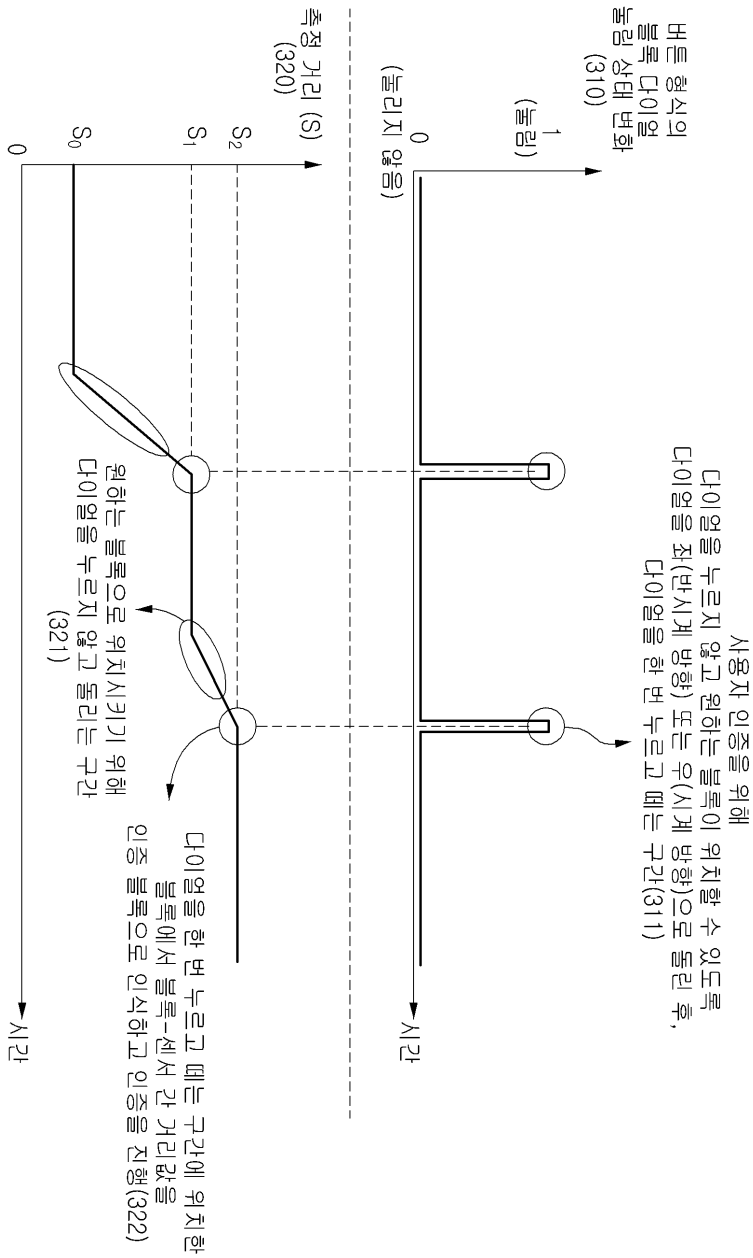
도면1


사용자 인증을 위한
다양한 길이의
버튼 형식 블록 구성
다이얼 (181)
150
160
패턴 일치
판단 모듈
잠금 장치
개폐 모듈
주요 보호 장치의
덮개(케이스) 내부
(182)
센서에 의한
측정 거리
(S)
140
사용자 정의
패턴 검증 모듈
B
130
측정 거리
판단 모듈
A
사용자 정의
패턴 메모리
170
A: 사용자 정의 패턴
입력 시
A': 사용자 정의 패턴
입력 완료시
B: 사용자 인증 시
버튼 형식 다이얼
눌림 인식 모듈
A'
레이저 거리
측정 센서
110
120

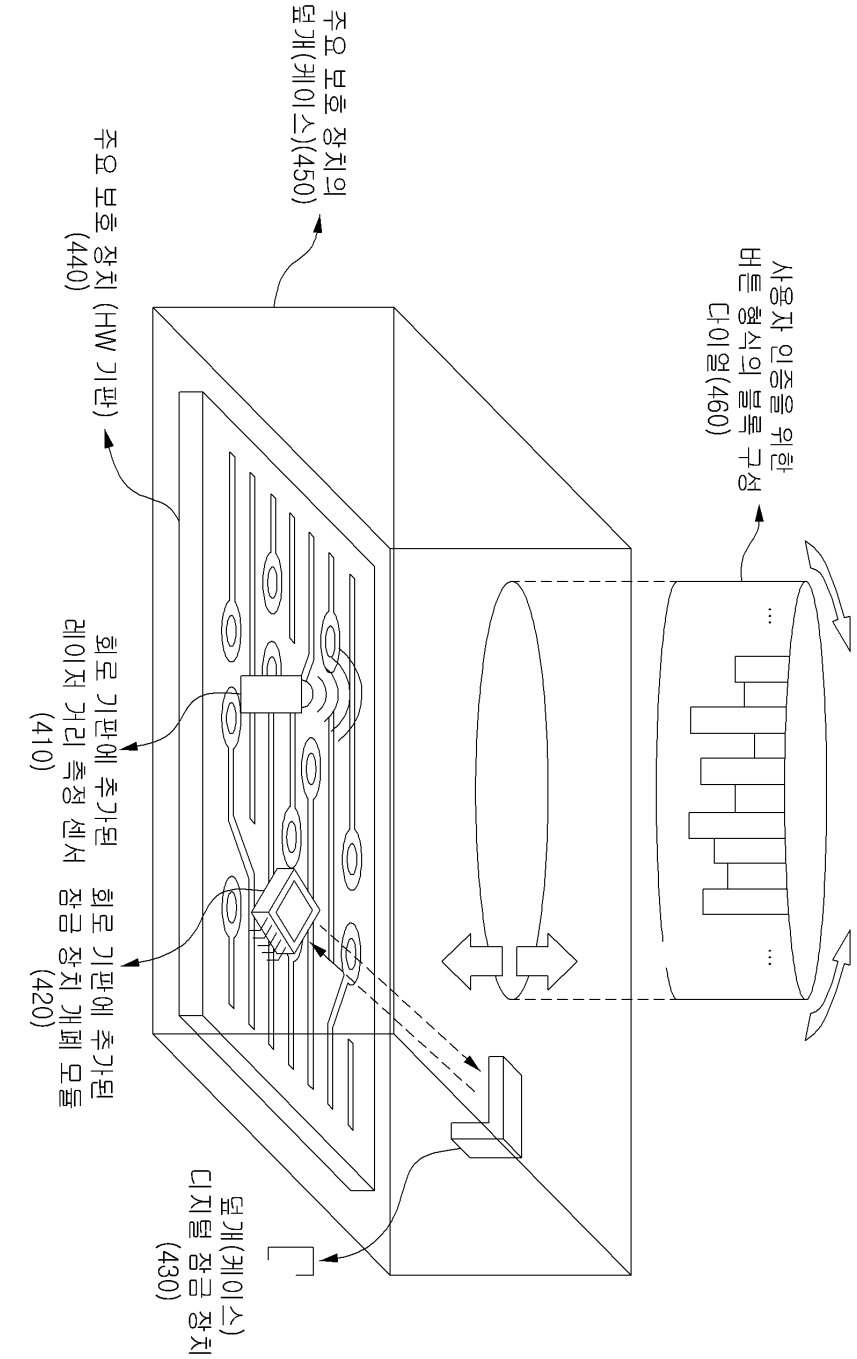
도면2


버튼 형식의
블록 다이얼
눌림 상태 변화
(210)
1
(눌림)
0
(눌리지 않음)
시간
원하는 블록이 위치할 수 있도록
다이얼을 누르고 있는 상태로
좌(반시계 방향) 또는 우(시계 방향)으로 돌리는 구간
(211)
원하는 블록에 위치시키고
누르고 있던 다이얼을 때는 구간
(212)
측정 거리 (S)
(220)
S0
S1
S2
0
시간
누르고 있던 다이얼을 때는 순간
해당 위치에서 측정된 블록-센서 간
거리값을 사용자 정의 인증 패턴으로
등록 (221)

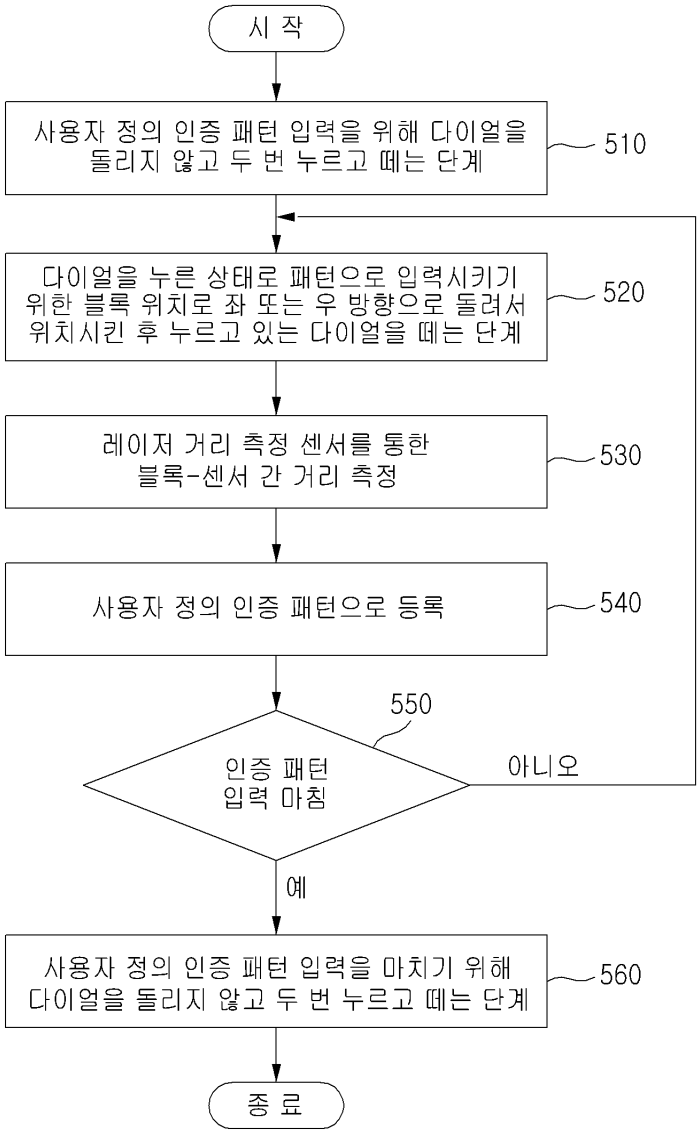
도면3


버튼 형식의
블록 다이얼
눌림 상태 변화
(310)
1
(눌림)
0
(눌리지 않음)
시간
사용자 인증을 위해
다이얼을 누르지 않고 원하는 블록이 위치할 수 있도록
다이얼을 좌(반시계 방향) 또는 우(시계 방향)으로 돌린 후,
다이얼을 한 번 누르고 때는 구간(311)
측정 거리 (S)
(320)
S_2
S_1
S_0
0
시간
원하는 블록으로 위치시키기 위해
다이얼을 누르지 않고 돌리는 구간
(321)
다이얼을 한 번 누르고 때는 구간에 위치한
블록에서 블록-센서 간 거리값을
인증 블록으로 인식하고 인증을 진행(322)

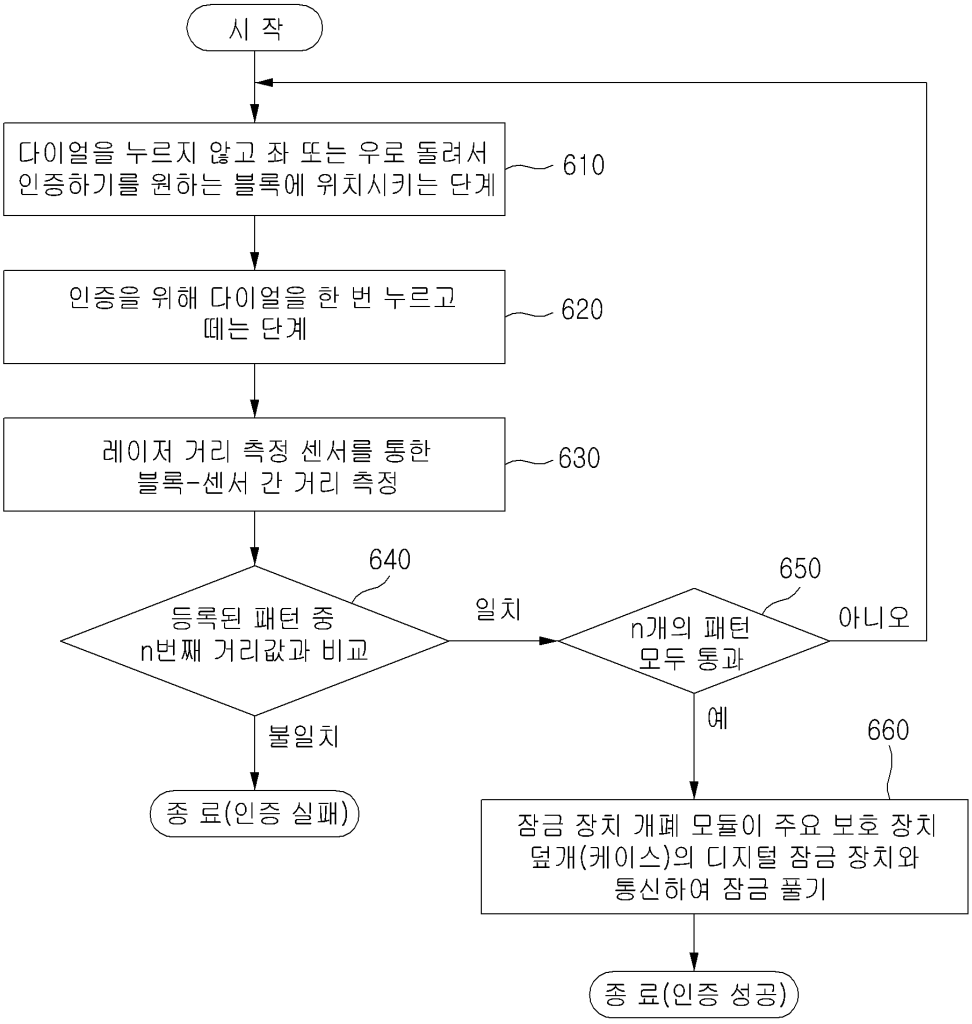
도면4


주요 보호 장치의 덮개(케이스)(450)
주요 보호 장치 (HW 기판) (440)
사용자 인증을 위한 버튼 형식의 블록 구성 다이얼(460)
회로 기판에 추가된 레이저 거리 측정 센서 (410)
회로 기판에 추가된 잠금 장치 개폐 모듈 (420)
덮개(케이스) 디지털 잠금 장치 (430)

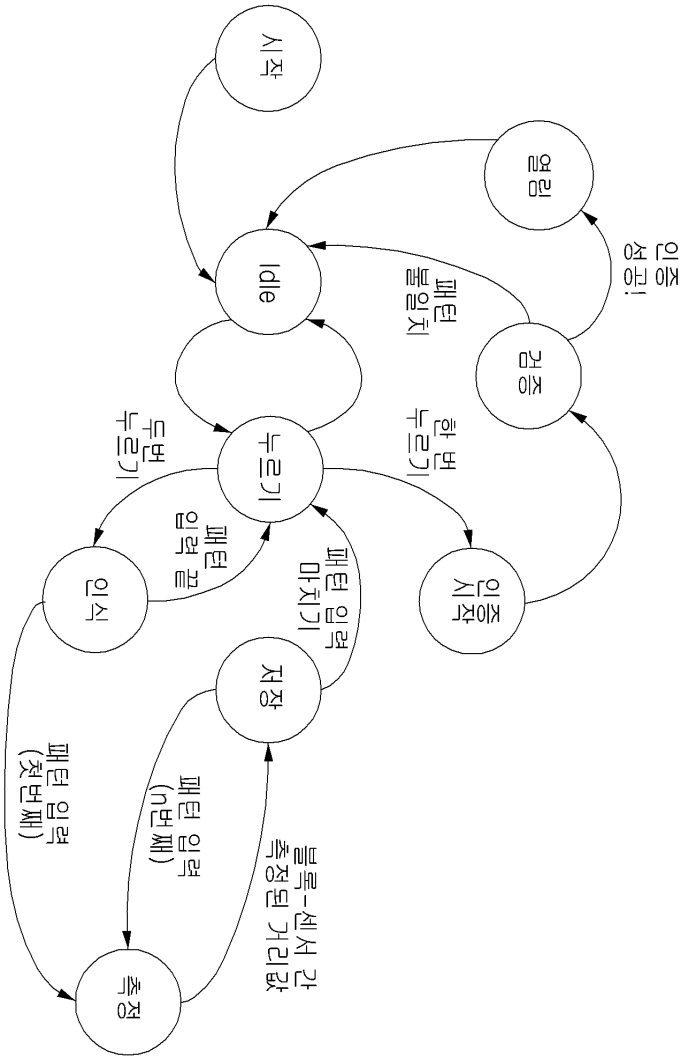
도면5


시 작
사용자 정의 인증 패턴 입력을 위해 다이얼을 돌리지 않고 두 번 누르고 떼는 단계
510
다이얼을 누른 상태로 패턴으로 입력시키기 위한 블록 위치로 좌 또는 우 방향으로 돌려서 위치시킨 후 누르고 있는 다이얼을 떼는 단계
520
레이저 거리 측정 센서를 통한 블록-센서 간 거리 측정
530
사용자 정의 인증 패턴으로 등록
540
550
인증 패턴 입력 마침
아니오
예
사용자 정의 인증 패턴 입력을 마치기 위해 다이얼을 돌리지 않고 두 번 누르고 떼는 단계
560
종 료

도면6


시 작
다이얼을 누르지 않고 좌 또는 우로 돌려서 인증하기를 원하는 블록에 위치시키는 단계
610
인증을 위해 다이얼을 한 번 누르고 떼는 단계
620
레이저 거리 측정 센서를 통한 블록-센서 간 거리 측정
630
640
등록된 패턴 중 n번째 거리값과 비교
일치
650
n개의 패턴 모두 통과
아니오
예
불일치
660
잠금 장치 개폐 모듈이 주요 보호 장치 덮개(케이스)의 디지털 잠금 장치와 통신하여 잠금 풀기
종 료(인증 실패)
종 료(인증 성공)

도면7


시작
idle
누르기
인식
저장
측정
입력
감응
인증 시작
인증 실패
패턴 불일치
5번 누르기
패턴 입력 마치기
패턴 입력 프로그램
5번 누르기
패턴 입력 (첫번째)
패턴 입력 (n번째)
블록-센서 간 측정된 거리값