(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
*G06K 19/07* (2006.01)
*G06K 19/00* (2006.01)

(45) 공고일자 2007년08월31일
(11) 등록번호 10-0753908
(24) 등록일자 2007년08월24일

(21) 출원번호 10-2006-0046099
(22) 출원일자 2006년05월23일
심사청구일자 2006년05월23일

(65) 공개번호
(43) 공개일자

(73) 특허권자 한국과학기술원
대전 유성구 구성동 373-1

(72) 발명자 박기웅
서울 노원구 월계4동 500-11번지

임상석
광주 광산구 월곡2동 일신아파트 104동 1403호

박규호
충남 공주시 장기면 금암리 314-98번지

(74) 대리인 이원희

(56) 선행기술조사문헌
JP2006011892 A
KR1020060030456 A
KR1020060024199 A
KR1020060035148 A

심사관 : 이승주

전체 청구항 수 : 총 10 항

# (54) 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템 및방법

(57) 요약

본 발명은 보안 단말기에 사용자의 의사를 인식하기 위한 2축 가속도 센서를 구비하여 인증 연산 수행시 사용자의 의사를 반영함으로써 불필요한 인증연산 및 인증연산의 자동화로 인한 오류를 줄일 수 있도록 한 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템 및 방법을 제공한다.

본 발명은, 보안 단말기; 상기 보안 단말기에서 인증요청을 위해 송신되는 신호를 인증 서버로 전달하는 지그비 송수신기; 및 상기 보안 단말기의 인증을 위한 인증 서버를 포함하는 인증 시스템에서, 상기 보안 단말기는 사용자 얼굴의 움직임을 감지하는 2축 가속도 센서; 상기 지그비 송수신기와 무선 통신하기 위한 지그비 통신모듈; 상기 2축 가속도 센서의 센싱값을 바탕으로 사용자 얼굴의 움직임을 판단하여 얼굴 움직임 판단에 따른 기 정해진 인증 프로토콜을 수행하는 중앙처리장치; 보안 단말기의 전원 차단 또는 전원 공급을 제어하는 전원관리모듈; 상기 전원관리모듈의 전원 공급시 상기 중앙처리장치의 제어에 따라 RSA 암호화를 행하는 암호 프로세서; 및 스피커를 포함하는 것을 특징으로 한다.

대표도

도 4

## 특허청구의 범위

### 청구항 1.

보안 단말기; 상기 보안 단말기에서 인증요청을 위해 송신되는 신호를 인증 서버로 전달하는 지그비 송수신기; 및 상기 보안 단말기의 인증을 위한 인증 서버를 포함하는 인증 시스템에 있어서,

상기 보안 단말기는

사용자 얼굴의 움직임을 감지하는 2축 가속도 센서;

상기 지그비 송수신기와 무선 통신하기 위한 지그비 통신모듈; 및

상기 2축 가속도 센서의 센싱값을 바탕으로 사용자 얼굴의 움직임을 판단하여 얼굴 움직임 판단에 따른 기 정해진 인증 프로토콜을 수행하는 중앙처리장치;

를 포함하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템.

### 청구항 2.

제 1 항에 있어서, 상기 보안 단말기는

보안 단말기의 전원 차단 또는 전원 공급을 제어하는 전원관리모듈을 더 포함하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템.

### 청구항 3.

제 2 항에 있어서, 상기 보안 단말기는

상기 전원관리모듈의 전원 공급시 상기 중앙처리장치의 제어에 따라 RSA(Rivest Shamir Adleman) 암호화를 행하는 암호 프로세서를 더 포함하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템.

### 청구항 4.

제 1 항 내지 제 3 항 중 어느 한항에 있어서, 상기 보안 단말기는 스피커를 더 포함하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템.

### 청구항 5.

2축 가속도 센서 및 중앙처리장치를 구비하여 사용자의 의사를 반영한 인증수행을 가능케 하는 보안 단말기; 상기 보안 단말기의 인증을 위한 지그비 송수신기 및 인증 서버를 포함하는 인증 시스템에서의 인증 방법에 있어서,

상기 중앙처리장치에서 상기 2축 가속도 센서의 센싱값을 바탕으로 사용자 얼굴 움직임을 감지하기 위한 제1과정;

상기 2축 가속도 센서에 의한 사용자의 얼굴 움직임 감지값을 바탕으로 사용자의 의사를 인식하기 위한 연산을 수행하는 제2과정; 및

상기 제2과정에서 인식한 정보를 바탕으로 기 정해진 인증 프로토콜을 수행하는 제3과정;

을 수행함을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

## 청구항 6.

제 5 항에 있어서, 상기 제 1 과정에서 중앙처리장치는

상기 2축 가속도 센서의 센싱값 획득이전에 상기 보안 단말기의 스피커를 통해 사용에게 의사를 묻기 위한 소리를 출력하고, 일정 시간동안 사용자의 얼굴 움직임을 감지하기 위해 타이머를 가동하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

## 청구항 7.

제 6 항에 있어서, 상기 제1과정에서

상기 2축 가속도 센서로부터의 사용자의 얼굴 좌우 움직임 감지를 위한 X축 값이 상기 중앙처리장치에 기 설정되어 있는 사용자 얼굴 좌우 움직임 판단을 위한 기준값(-A)보다 작을 경우 얼굴의 좌측으로의 움직임 판단을 위한 제1 카운터 값을 증가시키고, 상기 X축의 값이 상기 얼굴의 좌우 움직임 판단을 위한 기준값(+A)보다 클 경우 얼굴의 우측으로의 움직임 판단을 위한 제2 카운터를 증가시키는 단계; 및

상기 2축 가속도 센서로부터의 사용자 얼굴의 상하 움직임 판단을 위한 Y축의 값이 상기 중앙처리장치에 기 설정되어 있는 사용자 얼굴의 상하 움직임 판단을 위한 기준값(-A)보다 작을 경우 사용자 얼굴의 하측으로의 움직임 판단을 위한 제3 카운터 값을 증가시키고, 상기 Y축의 값이 상기 상하 움직임 판단을 위한 기준값(+A)보다 클 경우 사용자 얼굴의 상측으로의 움직임 판단을 위한 제4 카운터를 증가시키는 단계;

를 수행하여 사용자 얼굴 움직임을 인식하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

## 청구항 8.

제 7 항에 있어서, 상기 제2과정에서

상기 사용자의 얼굴 움직임을 판단하기 위해 상기 타이머 값이 0이 될 경우, 상기 제1 내지 제4 카운터의 값을 이용하여 사용자의 의사를 인식하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

## 청구항 9.

제 8 항에 있어서, 상기 사용자의 의사 인식은

상기 제1 및 제2 카운터의 비율이 50:50에 근사하고, (제1 카운터 + 제2 카운터)/(제3 카운터 + 제4 카운터)값이 상기 중앙처리장치 내에 기 설정되어 있는 사용자 의사의 Yes와 No를 판단하기 위한 기준값(B) 이상이면 사용자의 얼굴이 위아래로 끄덕이는 행동인 Yes 의사표시로 인식하는 단계; 및

상기 제3 및 제4 카운터 비율이 50:50에 근사하고, (제3 카운터 + 제4 카운터) / (제1 카운터 + 제2 카운터) 값이 상기 사용자 의사의 Yes와 No를 판단하기 위한 기준값(B) 이상이면 사용자의 얼굴을 좌우로 내젓는 행동인 No 의사표시로 인식하는 단계;

를 수행하여 행하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

## 청구항 10.

제 9 항에 있어서, 상기 제1 내지 제4 카운터 값에 따른 사용자의 의사 인식 결과 Yes 또는 No가 아니면 don't know 결과값을 출력하는 것을 특징으로 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 방법.

명세서

# 발명의 상세한 설명

## 발명의 목적

### 발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 2축 가속도 센서를 이용하여 사용자의 의사를 전달하여 인증 연산의 오류를 막을 수 있도록 하는 인증 시스템에 관한 것으로서, 특히 2축 가속도 센서의 감지에 따른 사용자의 확실한 의사 표현이 있을 경우에 보안 프로토콜 연산이 수행되도록 함으로써 보안 연산의 오류나 불필요한 인증 연산을 줄일 수 있도록 하는 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템 및 방법에 관한 것이다.

일반적으로 보안이 중요시 되는 환경에서 허가를 요청하는 사용자가 등록되어 있거나 정당하게 허가받은 사용자인지를 확인하고 전자 상거래시 신용 시스템을 기반으로 거래를 하는 인증 시스템 및 신용 거래 시스템이 널리 사용되고 있다.

특히, RFID와 스마트카드와 같은 소형 보안 카드가 개발됨에 따라 인증 시스템을 구축하는데 있어서 RFID와 스마트카드가 널리 사용되고 있다.

도 1은 일반적인 보안 인증 시스템의 기본적인 구성을 나타낸 도로, 일반적인 보안 인증 시스템은 사용자의 정보가 저장되어 있는 보안카드(110), 보안카드 리더기(120), 인증 서버(130), 디렉토리 서버(140)로 구성된다.

상기 보안 카드(110)는 RFID 또는 스마트카드가 될 수 있으며, RFID의 경우에는 안테나와 IC칩으로 이루어지고, IC칩에는 고주파 신호를 처리하기 위한 RF회로, 제어로직 및 메모리 등이 내장되어 있다. 스마트카드의 경우에는 내부에 중앙처리장치, 메모리를 내장하여 카드 내부에서 특정 암호화 알고리즘의 수행이 가능하다.

한편, 보안카드 리더기(120)는 인증 서버(130)와 연결될 수 있으며, 상기 인증 서버(130)는 소정의 미들웨어 또는 응용 프로그램을 사용하여 보안카드 리더기(120)에 의해 독출된 정보를 분석.저장하고 디렉토리 서버(140)에 저장되어 있는 인증서를 이용하여 인증 프로토콜을 수행하게 된다.

RFID는 무선 주파수 인식기술로, 무선 주파수를 사용하여 고유한 식별정보를 가지고 있는 태그로부터 비접촉식으로 정보를 독출하거나 기록함으로써 태그가 부착된 물건이나 동물, 사람 등을 인식.추적.관리할 수 있는 기술이다.

RFID시스템은 고유한 식별정보를 지니고 물건이나 동물 등에 부착되는 다수의 RF 태그(Tag 또는 Transponder)와, 상기 RF 태그를 가지고 있는 정보를 읽거나 쓰기 위한 RF 리더로 구성된다.

RF 리더는 컴퓨터 등 정보처리장치와 연결될 수 있으며, 상기 정보처리장치는 소정의 미들웨어 또는 응용프로그램을 사용하여 RF 리더에 의해 독출된 정보를 분석하고 저장한다.

이러한 RFID를 인증 시스템에 이용할 경우, 자신이 가지고 있는 RFID 정보를 RFID 리더에 자신의 의사와 관계없이 송신함으로서 보안을 유지하는데 있어 많은 문제점을 노출한다.

또한, 특정 RFID 카드에 대한 복제가 가능하여 보안성이 낮아지는 단점이 있다. 이러한 문제점을 보완하기 위해 전자기장을 통해 유도되는 전력량을 고려하여 40비트 정도의 대칭키를 사용하여 송신시 데이터의 암호화를 시도하나 짧은 키의 길이에 의해 여전히 키의 해킹에 취약하다.

접촉형 스마트카드를 인증 시스템에 이용할 경우, 카드 내부에 중앙처리장치, 메모리를 내장하여 카드 내부에서 특정 암호화 알고리즘의 수행이 가능하므로 RFID 카드에 비해 높은 보안성을 유지시킬 수 있지만 사용시 매번 리더에 삽입해야하는 번거로움 때문에 사용성이 매우 저하되고 비접촉형 스마트카드는 RFID의 키 해킹 취약성 문제점들을 갖고 있다.

이러한 문제를 해결하고자 다음과 같은 방안들이 모색되어지고 있다.

첫 번째로, 보안 단말기에 독립적인 전원 공급 장치를 부착하고 암호 프로세서를 장착하여 보다 높은 보안성을 제공하는 것이 가능하게 하는 방법이 있다.

이 방법은 전원이 독립적으로 공급되어 RFID기반의 카드시스템과 같이 카드를 직접 꺼내어 인증을 할 필요가 없고, 스마트카드와 같이 카드 리더기에 카드를 직접 삽입해야 할 필요성이 없어지며 독립적인 연산 장치가 있어 보다 강력한 보안성을 제공한다.

하지만 이 방법의 단점은 비접촉성과 자동화로 인해 사용자의 의사에 관계없이 인증 연산이 수행될 수 있고, 인증 시스템의 리더부분에 많은 사람들이 이동할 경우 불필요한 인증 연산이 수행되어 시스템에 과부하가 걸리기 쉽다.

두 번째 방법으로는 사용자의 행동을 영상정보를 이용하여 인식하여 사용자의 의사를 인식하여 사용자가 인증에 대한 의사를 표현할 경우에 인증 연산을 수행하는 방법이 있다. 이 방법의 단점은 각 인증 장치마다 영상 인식 장치와 이를 처리할 수 있는 프로세서가 있어야 하므로 구축하는데 비용이 많이 들고, 인식률이 떨어지는 단점이 있다.

세 번째 방법으로는 사용자의 단말기에 입력장치를 부착시켜 사용자의 입력에 따라 인증연산을 수행하게 하도록 하는 방법이 있다. 이 방법의 단점은 사용자가 인증을 필요로 할 시마다 보안 단말기를 꺼내어 버튼을 눌러야 하는 불편함이 존재한다.

종래 영상 정보를 이용하여 사용자의 의사를 인식하는 기술의 일예로, 대한민국 특허공개번호 제2004-53997호에 따른 "얼굴 움직임을 이용한 이동 통신 단말기의 제어 방법"을 들 수 있다. 이는 카메라의 영상처리를 이용하여 사용자의 의사를 판단하는 기술로서, 이를 실현하기 위해서는 카메라와 영상처리를 할 수 있는 프로세서가 필요함에 따라 시스템 구축 비용 및 보안 단말기의 제작비용이 높아지는 단점이 있다.

### 발명이 이루고자 하는 기술적 과제

본 발명은 이러한 점을 감안한 것으로, 본 발명의 목적은 보안 단말기에 사용자의 의사를 인식하기 위한 2축 가속도 센서를 구비하여 인증 연산을 수행하는데 있어서 사용자의 의사를 반영하여 수행하도록 함으로써 불필요한 인증연산 및 인증 연산의 자동화로 인한 오류를 줄일 수 있도록 하여 보안성과 안정성을 증대시킬 수 있도록 한 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템 및 방법을 제공함에 있다.

## 발명의 구성

상기 목적을 달성하기 본 발명에 따른 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템은, 보안 단말기; 상기 보안 단말기에서 인증요청을 위해 송신되는 신호를 인증 서버로 전달하는 지그비 송수신기; 및 상기 보안 단말기의 인증을 위한 인증 서버를 포함하는 인증 시스템에 있어서, 상기 보안 단말기는 사용자 얼굴의 움직임을 감지하는 2축 가속도 센서; 상기 지그비 송수신기와 무선 통신하기 위한 지그비 통신모듈; 및 상기 2축 가속도 센서의 센싱값을 바탕으로 사용자 얼굴의 움직임을 판단하여 얼굴 움직임 판단에 따른 기 정해진 인증 프로토콜을 수행하는 중앙처리장치;를 포함하는 것을 특징으로 한다.

상기 보안 단말기는 보안 단말기의 전원 차단 또는 전원 공급을 제어하는 전원관리모듈; 상기 전원관리모듈의 전원 공급시 상기 중앙처리장치의 제어에 따라 RSA(Rivest Shamir Adleman) 암호화를 행하는 암호 프로세서; 스피커를 더 포함한다.

상기 목적을 달성하기 위한 본 발명에 따른 가속도 센서를 이용한 얼굴 행동 인식 인증 방법은, 2축 가속도 센서 및 중앙처리장치를 구비하여 사용자의 의사를 반영한 인증수행을 가능케 하는 보안 단말기; 상기 보안 단말기의 인증을 위한 지그비 송수신기 및 인증 서버를 포함하는 인증 시스템에서의 인증 방법에 있어서, 상기 중앙처리장치에서 상기 2축 가속도 센서의 센싱값을 바탕으로 사용자 얼굴 움직임을 감지하기 위한 제1과정; 상기 2축 가속도 센서에 의한 사용자의 얼굴 움직임 감지값을 바탕으로 사용자의 의사를 인식하기 위한 연산을 수행하는 제2과정; 및 상기 제2과정에서 인식한 정보를 바탕으로 기 정해진 인증 프로토콜을 수행하는 제3과정;을 수행함을 특징으로 한다.

상기 제 1 과정에서 중앙처리장치는 상기 2축 가속도 센서의 센싱값 획득이전에 상기 보안 단말기의 스피커를 통해 사용에게 의사를 묻기 위한 소리를 출력하고, 일정 시간동안 사용자의 얼굴 움직임을 감지하기 위해 타이머를 가동한다.

또한, 상기 제1과정에서, 상기 2축 가속도 센서로부터의 사용자의 얼굴 좌우 움직임 감지를 위한 X축 값이 상기 중앙처리장치에 기 설정되어 있는 사용자 얼굴 좌우 움직임 판단을 위한 기준값(-A)보다 작을 경우 얼굴의 좌측으로의 움직임 판단을 위한 제1 카운터 값을 증가시키고, 상기 X축의 값이 상기 얼굴의 좌우 움직임 판단을 위한 기준값(+ A)보다 클 경우 얼굴의 우측으로의 움직임 판단을 위한 제2 카운터를 증가시키는 단계; 및 상기 2축 가속도 센서로부터의 사용자 얼굴의 상하 움직임 판단을 위한 Y축의 값이 상기 중앙처리장치에 기 설정되어 있는 사용자 얼굴의 상하 움직임 판단을 위한 기준값(-A)보다 작을 경우 사용자 얼굴의 하측으로의 움직임 판단을 위한 제3 카운터 값을 증가시키고, 상기 Y축의 값이 상기 상하 움직임 판단을 위한 기준값(+ A)보다 클 경우 사용자 얼굴의 상측으로의 움직임 판단을 위한 제4 카운터를 증가시키는 단계;를 수행하여 사용자 얼굴 움직임을 인식한다.

상기 제2과정에서, 상기 사용자의 얼굴 움직임을 판단하기 위해 상기 타이머 값이 0이 될 경우, 상기 제1 내지 제4 카운터의 값을 이용하여 사용자의 의사를 인식하며, 사용자의 의사 인식은 상기 제1 및 제2 카운터의 비율이 50:50에 근사하고, (제1 카운터 + 제2 카운터)/(제3 카운터 + 제4 카운터)값이 상기 중앙처리장치 내에 기 설정되어 있는 사용자 의사의 Yes와 No를 판단하기 위한 기준값(B) 이상이면 사용자의 얼굴이 위아래로 끄덕이는 행동인 Yes 의사표시로 인식하는 단계; 및 상기 제3 및 제4 카운터 비율이 50:50에 근사하고, (제3 카운터 + 제4 카운터) / (제1 카운터 + 제2 카운터) 값이 상기 사용자 의사의 Yes와 No를 판단하기 위한 기준값(B) 이상이면 사용자의 얼굴을 좌우로 내젓는 행동인 No 의사표시로 인식하는 단계;를 수행하여 행한다.

그리고 상기 제1 내지 제4 카운터 값에 따른 사용자의 의사 인식 결과 Yes 또는 No가 아니면 don't know 결과값을 출력한다.

이하, 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 보다 상세하게 설명한다. 단, 하기 실시 예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시 예에 한정되는 것은 아니다.

도 2는 본 발명에 따른 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템의 개략적인 구성도를 도시한 것으로, 보안 단말기(210), 지그비 송수신기(220), 인증 서버(230), 인증서 데이터베이스(240)로 구성된다.

상기 보안 단말기(210)는 도 3에 도시한 바와 같이, 사용자의 얼굴 움직임을 감지하기 위한 2축 가속도 센서(211), 사용자의 의사를 묻기 위한 소리가 출력되는 스피커(212), 상기 2축 가속도 센서(211)로부터 얻은 값을 이용하여 사용자 얼굴의 움직임을 연산하여 정해진 인증 프로토콜을 수행하는 중앙처리장치(213), 지그비 통신모듈(214), 상기 중앙처리장치(213)의 제어에 따라 RSA(Rivest Shamir Adleman) 암호화를 행하는 암호 프로세서(215) 및 전원관리모듈(216)로 구성된다.

이와 같은 인증 시스템에서 사용자는 보안 단말기(210)를 이용하여 인증을 받게 된다.

사용자가 소지하고 있는 보안 단말기(210)와 지그비 송수신기(220) 사이의 거리가 가까워 지게 되면, 지그비 송수신기(220)는 보안 단말기(210)에 인증에 필요한 요청(이하, challenge라 칭함) 메시지를 보낸다.

Challenge 메시지를 수신한 보안 단말기(210)는 내부에 있는 스피커(212)를 이용하여 보안 단말기(210)를 소지한 사용자의 의사를 판단하기 위해 의문형을 표시하는 벨을 울리게 된다. 또한, 보안 단말기(210) 내부에 있는 2축 가속도 센서(211)가 초기화 되며, 사용자의 얼굴 움직임을 감지할 준비를 하게 된다.

이후, 2축 가속도 센서(211)는 일정 시간동안 사용자의 얼굴 움직임에 대한 정보를 보안 단말기(210) 내부의 중앙처리장치(213)로 내보내게 되고, 중앙처리장치(213)는 일정 시간 후 센싱된 값을 이용하여 얼굴 움직임을 판단하게 된다.

만약, 이때 사용자가 얼굴을 끄덕이는 행동을 취하였음을 인식하면 보안 단말기(210) 내부의 중앙처리장치(213)는 기 정해진 인증 연산을 수행하게 되고, 아무 행동을 취하지 않거나 좌우로 내젓는 행동을 취하였을 경우에는 인증 연산을 수행하지 않고 지그비 송수신기(220)에 인증을 하지 않겠다는 메시지를 송신하게 된다.

또한, 보안 단말기(210)의 중앙처리장치(213)는 2축 가속도 센서(211)의 센싱값 판단에 따라 사용자가 인증을 필요로 한다는 의사가 인식되면 암호 프로세서(215)를 통해 수신된 Challenge 메시지를 개인키로 암호화하여 지그비 송수신기(220)로 응답한다.

이때, 지그비 송수신기(220)는 이전에 수신된 식별 아이디를 인증 서버(230)로 전송하게 되며, 인증 서버(230)는 수신된 식별 아이디에 해당하는 공개키를 얻기 위하여 쿼리를 인증서 데이터베이스(240)로 보낸다.

쿼리를 수신한 인증서 데이터베이스(240)는 보안 단말기(210)에 해당하는 인증서를 인증 서버(230)로 전송하게 된다. 인증 서버(230)는 수신된 인증서에서 공개키를 추출하고 그것의 폐지여부를 확인한다.

공개키가 유효할 경우 사용자 보안 단말기(210)가 암호화하여 전송하였던 응답 메시지를 해독하여 처음 송신하였던 challenge 메시지와의 동일여부를 검사하여 인증 여부를 결정한다.

이러한 연산에서 보안 단말기(210)와 지그비 송수신기(220) 사이의 메시지 전송은 무선통신 수단인 지그비가 될 수 있고, 블루투스(Bluetooth), WLAN 등의 다른 무선 신호일 수 있다.

한편, 상기 전원관리모듈(216)은 상기 지그비 송수신기(220)와 보안 단말기(210)가 가까워져 인증이 필요한 경우, 보안 단말기(210)의 2축 가속도 센서(211), 중앙처리장치(213), 암호 프로세서(215)에 전원을 인가하여 인증 연산이 수행될 수 있도록 한다.

도 4는 상기 보안 단말기(210)의 중앙처리장치(213)에서 사용자의 얼굴 움직임을 감지하는 알고리즘에 따른 흐름도를 나타낸 것이다.

사용자의 의사를 인식하기 위해 알고리즘을 수행하게 되면 사용자에게 의사를 묻기 위한 소리가 스피커(212)를 통해 출력되며, 일정 시간동안 얼굴 움직임을 감지하기 위해 보안 단말기(210) 내의 도시하지 않은 타이머가 정해진 시간만큼 가동이 된다(S110).

타이머가 가동되는 동안 중앙처리장치(213)에서는 2축 가속도 센서(211) 값을 읽어 이를 처리하게 된다. 이를 위해 상기 중앙처리장치(213)에는 사용자의 얼굴의 좌우(X축) 및 상하(Y축) 움직임을 판단하기 위한 기준값(A) 및 사용자 의사의 Yes와 No를 판단하기 위한 기준값(B)이 설정되어 있게 된다.

만약, 상기 2축 가속도 센서(211)로부터의 사용자 얼굴의 좌우 움직임 인식을 위한 X축의 값이 상기 기준값(-A)보다 작을 경우에는 얼굴의 좌측으로의 움직임 인식을 위한 카운터인 X_n 카운터 값을 증가시키게 되고, 상기 X축의 값이 상기 기준값(+A)보다 클 경우에는 얼굴의 우측으로의 움직임 인식을 위한 카운터인 X_p 카운터를 증가시키게 된다 (S120,S121,S122).

이와 마찬가지로, 상기 2축 가속도 센서(211)로부터의 사용자 얼굴의 상하 움직임 인식을 위한 Y축의 값이 상기 기준값(-A)보다 작을 경우에는 사용자 얼굴의 하측으로의 움직임 인식을 위한 카운터인 Y_n 카운터 값을 증가시키게 되고, Y축의 값이 상기 기준값(+A)보다 클 경우에는 사용자 얼굴의 상측으로의 움직임 인식을 위한 Y_p 카운터를 증가시키게 된다 (S130,S131,S132).

도 5는 상기 사용자의 얼굴의 상하 및 좌우 움직임 판단에 대한 이해를 돕기 위한 2축 가속도 센서(211)의 내부 구조를 도시한 것으로, 센서 모듈이 좌우로 움직이면 즉, 좌우로 얼굴을 움직이면 수직 스프링위에 위치한 공이 좌우로 움직일 것이며, 그러면 센서는 얼마만큼 공이 기울었는지를 반환할 것이다. 반대로 센서 모듈이 위아래로 움직이면 즉, 얼굴을 끄덕이면 수평 스프링에 위치한 공이 위아래로 움직일 것이며, 그러면 센서는 위아래로 얼마만큼 공이 기울었는지를 반환할 것이

다. 상기 기준값(-A, +A)이 주어진 것은 아주 미세한 움직임 까지 모두 카운터로 추가시킨 다면 연산량이 증가할뿐더러 사용자가 의도 하지 않은 인식을 할 수 있을 것임에 따라 -A보다 작거나 +A보다 큰 경우에만 카운트를 증가시킴으로서 필터링을 할 수 있도록 한 것이다.

그리고 상기 중앙처리장치(213)는 상기 타이머가 0이 될 경우, 상기 X_p, X_n, Y_p, Y_n 카운터 값을 이용하여 얼굴 행동을 인식하게 된다(S140,S150).

만약, 상기 X_p와 X_n의 비율이 50:50에 근사하고 (X_p + X_n) / (Y_p+ Y_n)이 상기 기준값(B) 이상이면 사용자의 얼굴이 위아래로 끄덕이는 행동 즉, 사용자가 Yes 의사표시를 취했다는 것을 인식하게 된다(S151).

이와 마찬가지로, Y_P와 Y_N의 비율이 50:50에 근사하고 (Y_p + Y_n) / (X_p+ X_n)이 상기 기준값(B) 이상이면 사용자의 얼굴을 좌우로 내젓는 행동 즉, No의 의사표시를 취했다는 것을 인식하게 된다(S152). 상기 두 조건에 만족하지 않았을 경우에는 don't know 결과값을 출력하게 된다(S153).

도 6은 상기 보안 단말기(210)를 이용하여 인증을 하는데 있어 필요한 인증 프로토콜 상세 설명을 위한 도이다.

상기 보안 단말기(210)와 지그비 송수신기(220)의 거리가 가까워 짐에 따라 보안 단말기(210)는 도시하지 않은 메모리에 기록되어 있는 사용자 식별 아이디(500)를 지그비 통신모듈(214)을 통해 송신하게 된다.

이때, 사용자 식별 아이디(500)의 전송 실패에 대비하기 위하여 사용자 식별 아이디 전송(500) 후, 도시하지 않은 타이머를 가동하여 일정 시간 초과시까지 challenge 메시지(501) 수신이 없으면 재전송(502)을 수행한다. 그리고 보안 단말기(210)에서는 사용자의 의사를 판단하기 위하여 일정시간 동안 2축 가속도 센서(211)를 이용하여 사용자의 의사를 인식하게 된다.

사용자 식별 아이디(500)을 수신한 인증 서버(230)는 무작위 생성된 데이터(challenge) 메시지(501)를 보안 단말기(210)로 전송한다.

인증 서버(230)에서는 challenge 메시지(501)의 소실을 대비하여 타이머를 사용하여 일정 시간 초과시 재전송(503)을 수행한다.

지그비 통신모듈(211)을 통해 challenge 메시지(501)를 수신한 보안 단말기(210)는 중앙처리장치(213)의 제어에 따라 개인키를 이용하여 암호 프로세서(214)에서 RSA(Rivest Shamir Adleman)암호화(504)를 한 후, 응답(respnse) 메시지(505)를 인증 서버(230)로 전송한다.

응답 메세지(505)를 수신한 인증 서버(230)는 이전에 수신한 사용자 식별 아이디(500)를 인증서 데이터 베이스(240)로 전송하여 해당하는 공개키를 검색하고, 보안 단말기(210)의 개인키로 암호화(504)된 응답 메시지(505) 데이터를 공개 키로 해독(506)하여 처음에 송신한 challenge(501)와 데이터가 일치하는지 비교한다.

일치할시 억셉트(Accept) 메시지(507)를 보안 단말기(210)로 전송하여 인증여부를 알려준다.

상술한 바와 같이, 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 또는 변형하여 실시할 수 있다.

## 발명의 효과

이상에서 살펴본 바와 같이, 본 발명은 종래의 인증 방식에서 수반되는 단점들, 즉 RFID에서는 사용자의 의사와 관계없이 ID정보가 유출이 되어 복제의 위험성과 스마트 카드 형태의 인증 시스템에서 발생되는 보안의 취약성을 해결할 수 있으며, 독립적인 중앙처리장치와 암호 프로세서, 지그비 통신모듈, 얼굴 행동 인식을 위한 2축 가속도 센서를 통해 불필요한 인증 연산의 횟수와 오류를 줄일 수 있게 된다.

또한, 본 발명은 전원관리모듈에 의해 보안 단말기의 전원을 관리하여 저전력 인증을 가능케 한다.

## 도면의 간단한 설명

도 1은 일반적인 보안카드를 이용한 인증 시스템의 기본적인 구성을 나타낸 도.

도 2는 본 발명에 따른 가속도 센서를 이용한 얼굴 행동 인식 인증 시스템의 개략 구성도.

도 3은 도 2의 보안 단말기의 얼굴 행동 인식을 위한 상세 구성도.

도 4는 본 발명에 따른 얼굴 행동 인식을 위한 알고리즘에 대한 흐름도.

도 5는 본 발명의 이해를 돕기 위한 2축 가속도 센서의 구조도.

도 6은 본 발명에 따른 보안 단말기를 이용한 인증시의 인증 프로토콜 다이어그램.

<도면의 주요 부분에 대한 부호의 설명>

210 : 보안 단말기 211 : 2축 가속도 센서

212 : 스피커 213 : 중앙처리장치

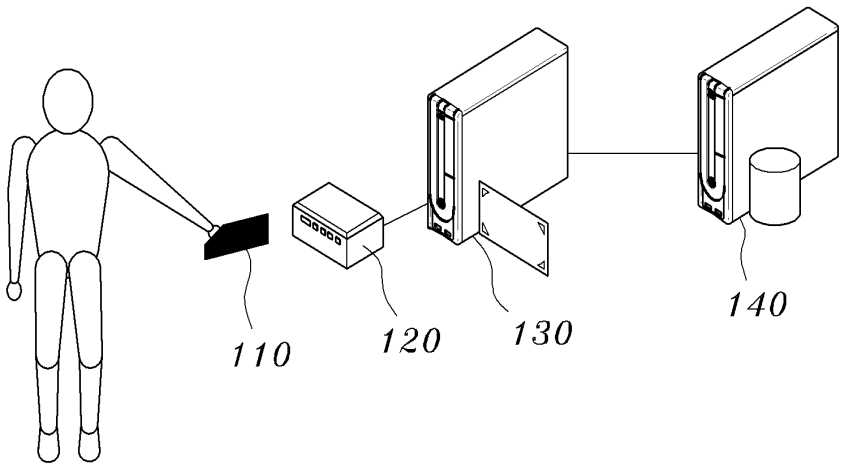
214 : 지그비 통신모듈 215 : 암호 프로세서

216 : 전원관리모듈 220 : 지그비 송수신기

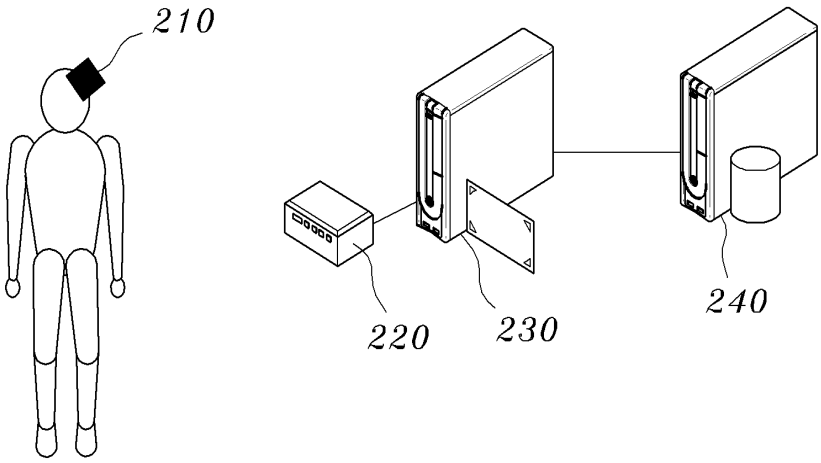
230 : 인증 서버 240 : 인증서 데이터베이스

도면

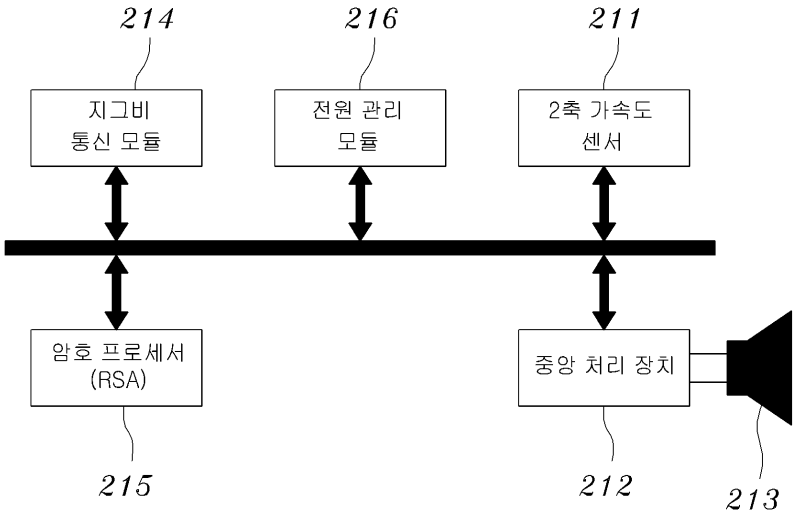
도면1



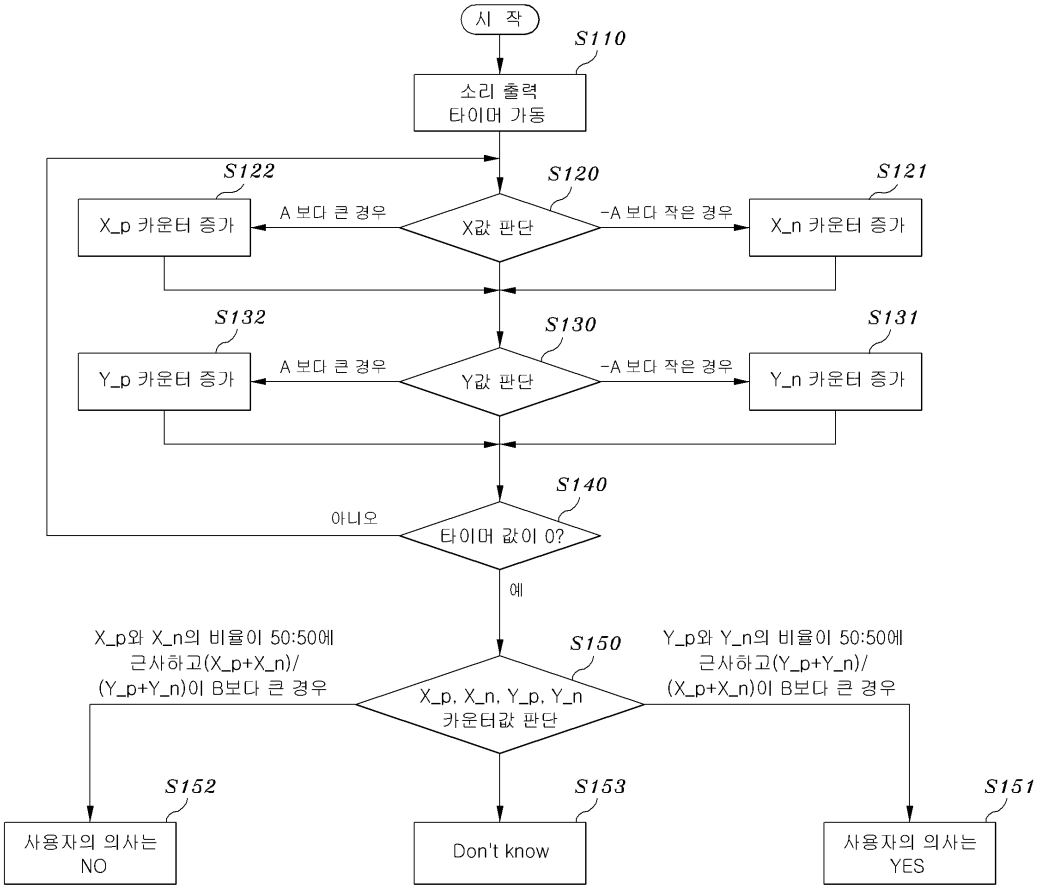
도면2


210
220
230
240

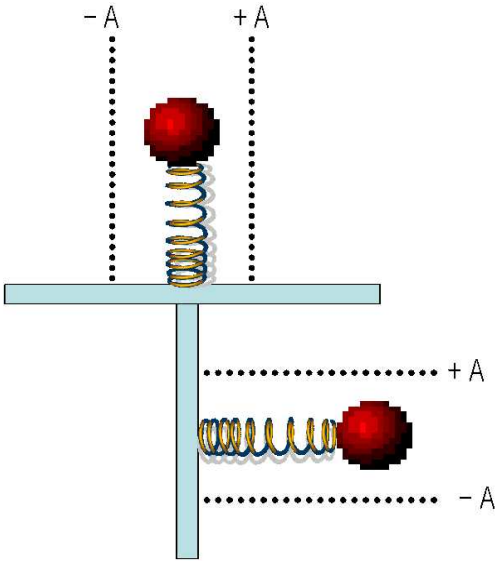
도면3


214
216
211
지그비
통신 모듈
전원 관리
모듈
2축 가속도
센서
암호 프로세서
(RSA)
중앙 처리 장치
215
212
213

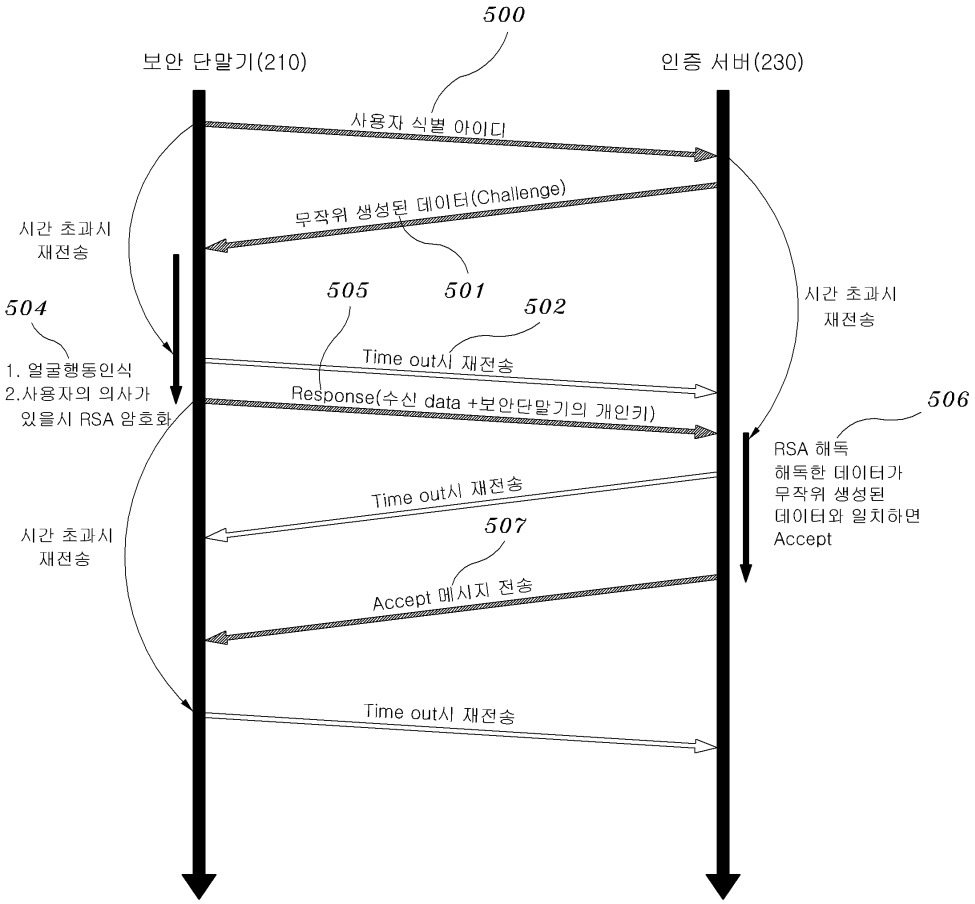
도면4


시 작
S110
소리 출력
타이머 가동
S122
S120
S121
X_p 카운터 증가
A 보다 큰 경우
X값 판단
-A 보다 작은 경우
X_n 카운터 증가
S132
S130
S131
Y_p 카운터 증가
A 보다 큰 경우
Y값 판단
-A 보다 작은 경우
Y_n 카운터 증가
S140
아니오
타이머 값이 0?
예
X_p와 X_n의 비율이 50:50에
근사하고(X_p+X_n)/
(Y_p+Y_n)이 B보다 큰 경우
S150
X_p, X_n, Y_p, Y_n
카운터값 판단
Y_p와 Y_n의 비율이 50:50에
근사하고(Y_p+Y_n)/
(X_p+X_n)이 B보다 큰 경우
S152
S153
S151
사용자의 의사는
NO
Don't know
사용자의 의사는
YES

도면5


-A
+A
+A
-A

도면6


500
보안 단말기(210)
인증 서버(230)
사용자 식별 아이디
무작위 생성된 데이터(Challenge)
501
시간 초과시
재전송
505
502
504
1. 얼굴행동인식
2.사용자의 의사가
있을시 RSA 암호화
Time out시 재전송
Response(수신 data +보안단말기의 개인키)
506
RSA 해독
해독한 데이터가
무작위 생성된
데이터와 일치하면
Accept
Time out시 재전송
507
Accept 메시지 전송
Time out시 재전송