



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0045501
(43) 공개일자 2019년05월03일

(51) 국제특허분류(Int. Cl.)
G07C 9/00 (2006.01) G07C 9/02 (2006.01)
(52) CPC특허분류
G07C 9/00031 (2013.01)
G07C 9/00103 (2013.01)
(21) 출원번호 10-2017-0138173
(22) 출원일자 2017년10월24일
심사청구일자 2017년10월24일

(71) 출원인
한밭대학교 산학협력단
대전광역시 유성구 동서대로 125 (덕명동)
(주)덕분이앤씨
대전광역시 서구 유등로 641 ,타이어뱅크3층(용문동)
(72) 발명자
이현빈
대전광역시 서구 둔산로 155, 109동 703호(둔산동, 크로바아파트)
김대호
대전광역시 유성구 대정로28번안길 80, 202동 701호(대정동, 대전드리움아파트2단지)
(뒷면에 계속)
(74) 대리인
특허법인 플러스

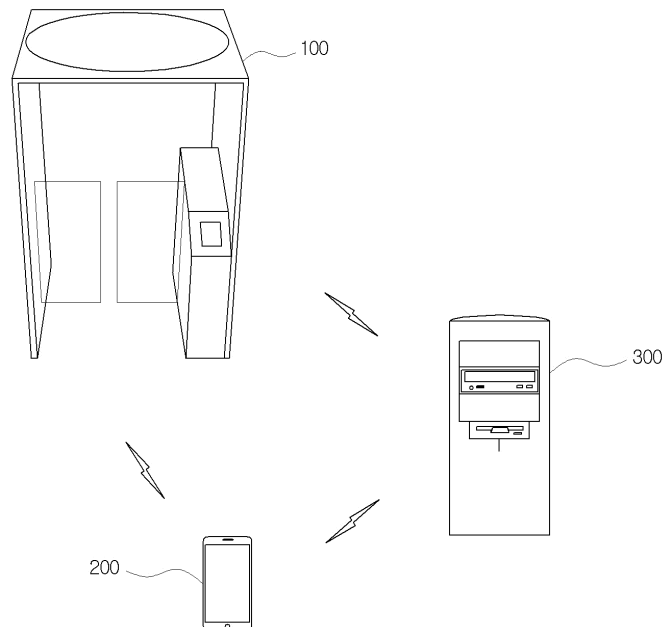
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 스마트기기 무선 통신과 파라볼라 안테나를 이용한 게이트 자동인증 시스템

(57) 요약

스마트기기 무선 통신과 파라볼라 안테나를 이용한 게이트 자동인증 시스템 및 그 방법이 개시된다. 본 게이트 자동인증 시스템은 사용자가 인식되면 접근 신호가 출력되도록 마련되는 게이트; 상기 접근 신호가 인식되면 전용 애플리케이션이 구동되도록 마련되는 스마트기기; 및 상기 스마트기기로부터 중요청신호가 전송되면 상기 게 (뒷면에 계속)

대표도 - 도1



이트가 개폐되도록 제어하는 서버;를 포함하고, 상기 게이트는, 상기 사용자가 기설정된 영역 내에 진입하면 상기 사용자를 인식하여 전기적 신호를 발생시키는 근접 센서; 및 상기 전기적 신호가 발생하면 상기 게이트의 아 이디 정보를 포함하는 상기 접근 신호를 출력시키는 게이트 무선통신 모듈;을 포함한다. 이에 의해, 출입 인증 과정에서 스마트기기의 대기모드를 해제시키거나 애플리케이션을 백그라운드에 상시 로딩시키지 않고도 인증이 수행되도록 하여, 사용자의 편의성을 증대시키고 스마트기기의 과도한 배터리 소모의 문제점을 해결하는 게이트 자동인증 시스템 및 그 방법을 제공할 수 있게 된다.

(52) CPC특허분류

G07C 9/00571 (2013.01)

G07C 9/02 (2013.01)

고병진

대전광역시 유성구 대정로28번안길 80, 210-404 (대정동, 대전드리움아파트2단지)

(72) 발명자

김유섭

경기도 수원시 권선구 동수원로145번길 24, 206-901(권선동, 수원아이파크시티2단지)

이 발명을 지원한 국가연구개발사업

과제고유번호 1425106629

부처명 중소기업청

연구관리전문기관 중소기업기술정보진흥원

연구사업명 첫걸음기술개발사업

연구과제명 스마트 폰을 이용한 보안게이트 자동인증 시스템 개발

기 여 율 1/1

주관기관 (주)덕분이앤씨

연구기간 2016.11.01 ~ 2017.10.31

명세서

청구범위

청구항 1

사용자가 인식되면 접근 신호가 출력되도록 마련되는 게이트;

상기 접근 신호가 인식되면 전용 애플리케이션이 구동되도록 마련되는 스마트기기; 및

상기 스마트기기로부터 인증요청신호가 전송되면 상기 게이트가 개폐되도록 제어하는 서버;를 포함하고,

상기 게이트는,

상기 사용자가 기설정된 영역 내에 진입하면 상기 사용자를 인식하여 전기적 신호를 발생시키는 근접 센서; 및

상기 전기적 신호가 발생하면 상기 게이트의 아이디 정보를 포함하는 상기 접근 신호를 출력시키는 게이트 무선 통신 모듈;을 포함하는 것을 특징으로 하는 게이트 자동인증 시스템.

청구항 2

제1항에 있어서,

상기 스마트기기는,

상기 사용자로부터 신원정보가 입력되고, 상기 접근 신호를 스캔하여 RSSI(Received signal strength indication) 데이터가 생성되면, 상기 아이디 정보, 상기 RSSI 데이터, 상기 신원정보 및 고유번호 정보를 포함하는 상기 인증요청신호를 상기 서버에 전송하도록 마련되고,

상기 서버는,

상기 스마트기기로부터 수신되는 상기 신원정보와 기저장된 신원정보를 비교하여 동일한 신원정보가 존재하는 경우, 상기 사용자의 출입이 허용되는 것으로 판단하고, 상기 사용자가 위치하는 게이트에 동작 제어 신호를 전송하는 것을 특징으로 하는 게이트 자동인증 시스템.

청구항 3

제2항에 있어서,

상기 서버는,

출입이 허용되는 사용자의 상기 신원정보와 출입 일시 정보를 저장하여 관리자에 의해 출입인원내역이 관리되도록 마련되는 것을 특징으로 하는 게이트 자동인증 시스템.

청구항 4

제1항에 있어서,

상기 스마트기기는,

상기 인식되는 접근 신호의 세기가 기설정된 세기 이상인 경우, 상기 서버에 상기 인증요청신호를 전송하는 것을 특징으로 하는 게이트 자동인증 시스템.

청구항 5

제1항에 있어서,

상기 게이트는,

상단에 파라볼라 안테나가 마련되어, 상기 접근 신호의 세기를 증폭시키는 것을 특징으로 하는 게이트 자동인증 시스템.

청구항 6

게이트가 사용자를 인식하여 접근 신호를 출력시키는 단계;

스마트기기가 상기 접근 신호를 인식하고 전용 애플리케이션을 구동시키는 단계;

상기 스마트기기가 서버에 인증요청신호를 전송하는 단계; 및

상기 인증요청신호가 수신되면 상기 서버가 상기 게이트가 개폐되도록 제어하는 단계;를 포함하고,

상기 접근 신호를 출력시키는 단계는,

상기 사용자가 기설정된 영역 내에 진입하면 근접 센서가 사용자를 인식하여 전기적 신호를 발생시키는 단계; 및

상기 전기적 신호가 발생하면 게이트 무선통신 모듈이 상기 게이트의 아이디 정보를 포함하는 상기 접근 신호를 출력하여 상기 스마트기기와 무선 통신하는 단계;를 포함하는 것을 특징으로 하는 게이트 자동인증 방법.

발명의 설명

기술 분야

[0001] 본 발명은 스마트기기 무선 통신과 파라볼라 안테나를 이용한 게이트 자동인증 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 스마트기기를 소지하는 것만으로 사용자의 출입인증이 가능하도록 마련되는 게이트 자동인증 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 출입보안 게이트는 공공기관이나 대기업에서 주로 사용되었으나, 최근에는 출입보안의 필요성이 강화되어 학교, 방송국, 연구소 등 다양한 장소에 설치되고 있다.

[0003] 출입보안 게이트는 비밀번호 입력, 열쇠 등 물리적인 방법과, RFID, 지문인식, 바코드 인식 등 근거리통신 및 생체인식 기술을 이용한 방식들이 주를 이루고 있다.

[0004] 그러나 이러한 근거리통신 및 생체인식 방식의 경우 출입자가 카드를 준비하여 접촉시키거나 지문을 인식시키는 동작을 취해야 하므로, 과거의 물리적인 방법에 비해 속도가 빨라졌을 뿐 출입자의 불편함은 해소하지 못하였다.

[0005] 대한민국 공개특허공보 제2016-0062369호(2016.6.2. 공개)에는 블루투스 및 스마트기기를 이용한 출입인증 시스템 및 인증방법이 개시되어 있다.

[0006] 이러한 무선통신방식은 사용자가 스마트기기를 소지하는 것만으로 보안인증이 수행되어 출입자의 불편함을 어느 정도 해결하였다는 데 의의가 있다.

[0007] 그러나, 상기 선행기술을 비롯한 다수의 특허문헌들은 다음의 몇 가지 과제들에 대한 해결책을 제시하지 못하고 있다.

[0008] 첫째, 사용자가 소지한 스마트기기는 평소에 대기모드 상태에 있다. 대기모드 상태에서는 무선통신 모듈로부터 송출되는 신호를 스캔하지 않기 때문에 사용자가 게이트를 통과할 때 스마트기기의 대기모드를 해제시켜야 하거나, 해당 애플리케이션을 백그라운드로 계속해서 로딩시켜 놓아야 한다. 사용자가 직접 대기모드를 해제하는 것은 출입자의 불편함을 해결하고자 하는 취지를 역행하는 것이고, 애플리케이션을 상시 로딩시키는 것은 배터리 소모의 문제와 메모리 점유의 문제가 있다.

[0009] 둘째, 스마트기기가 게이트의 Mac Address를 탐색하면 서버로 인증요청을 하게 되는데, 초당 수회씩의 인증요청에 의해 서버에 인증 데이터가 지나치게 많이 쌓여서 유효한 데이터를 골라내기 힘든 문제점이 있다.

[0010] 셋째, 스마트기기에서 무선 송출신호의 수신강도를 감지할 때 스마트기기와 무선통신 모듈 간의 거리에 따라 값의 차이가 명확하게 구별되지 않고 불규칙적으로 값이 튀는 현상이 발생하는 문제점이 있다.

[0011] 넷째, 사용자가 스마트기기를 소지한 상태로 게이트를 통과할 때 스마트기기의 인증요청과 서버의 인증과정에 소요되는 시간 때문에 실시간으로 게이트가 열리지 않아 사용자가 게이트에 부딪히거나 게이트 앞에서 대기해야

하는 문제점이 있다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 대한민국공개특허 제10-2016-0062369호 (발명의 명칭 : 출입 인증 시스템 및 그 인증 방법)

발명의 내용

해결하려는 과제

[0013] 본 발명은 상기와 같은 문제를 해결하기 위하여 안출된 것으로, 본 발명의 목적은 출입 인증 과정에서 스마트기기의 대기모드를 해제시키거나 애플리케이션을 백그라운드에 상시 로딩시키지 않고도 인증이 수행되도록 하여, 사용자의 편의성을 증대시키고 스마트기기의 과도한 배터리 소모의 문제점을 해결하는 게이트 자동인증 시스템 및 그 방법을 제공함에 있다.

과제의 해결 수단

[0014] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 게이트 자동인증 시스템은 사용자가 인식되면 접근 신호가 출력되도록 마련되는 게이트; 상기 접근 신호가 인식되면 전용 애플리케이션이 구동되도록 마련되는 스마트기기; 및 상기 스마트기기로부터 인증요청신호가 전송되면 상기 게이트가 개폐되도록 제어하는 서버;를 포함하고, 상기 게이트는, 상기 사용자가 기설정된 영역 내에 진입하면 상기 사용자를 인식하여 전기적 신호를 발생시키는 근접 센서; 및 상기 전기적 신호가 발생하면 상기 게이트의 아이디 정보를 포함하는 상기 접근 신호를 출력시키는 게이트 무선통신 모듈;을 포함한다.

[0015] 여기서 상기 스마트기기는, 상기 사용자로부터 신원정보가 입력되고, 상기 접근 신호를 스캔하여 RSSI(Received signal strength indication) 데이터가 생성되면, 상기 아이디 정보, 상기 RSSI 데이터, 상기 신원정보 및 고유번호 정보를 포함하는 상기 인증요청신호를 상기 서버에 전송하도록 마련되고, 상기 서버는, 상기 스마트기기로부터 수신되는 상기 신원정보와 기저장된 신원정보를 비교하여 동일한 신원정보가 존재하는 경우, 상기 사용자의 출입이 허용되는 것으로 판단하고, 상기 사용자가 위치하는 게이트에 동작 제어 신호를 전송할 수 있다.

[0016] 그리고 상기 서버는, 상기 확인 모듈에 의해 출입이 허용되는 사용자의 신원정보와 출입 일시 정보를 저장하여 관리자에 의해 출입인원내역이 관리되도록 마련될 수 있다.

[0017] 또한, 상기 스마트기기는, 상기 인식되는 접근 신호의 세기가 기설정된 세기 이상인 경우, 상기 서버에 상기 인증요청신호를 전송할 수 있다.

[0018] 그리고 상기 게이트는, 상단에 파라볼라 안테나가 마련되어, 상기 접근 신호의 세기를 증폭시킬 수 있다.

[0019] 또한, 본 발명의 일 실시예에 따른 게이트 자동인증 방법은 게이트가 사용자를 인식하여 접근 신호를 출력시키는 단계; 스마트기기가 상기 접근 신호를 인식하고 전용 애플리케이션을 구동시키는 단계; 상기 스마트기기가 서버에 인증요청신호를 전송하는 단계; 및 상기 인증요청신호가 수신되면 상기 서버가 상기 게이트가 개폐되도록 제어하는 단계;를 포함하고, 상기 접근 신호를 출력시키는 단계는, 상기 사용자가 기설정된 영역 내에 진입하면 근접 센서가 사용자를 인식하여 전기적 신호를 발생시키는 단계; 및 상기 전기적 신호가 발생하면 게이트 무선통신 모듈이 상기 게이트의 아이디 정보를 포함하는 상기 접근 신호를 출력하여 상기 스마트기기와 무선 통신하는 단계;를 포함할 수 있다.

발명의 효과

[0020] 이에 의해, 출입 인증 과정에서 스마트기기의 대기모드를 해제시키거나 애플리케이션을 백그라운드에 상시 로딩시키지 않고도 인증이 수행되도록 하여, 사용자의 편의성을 증대시키고 스마트기기의 과도한 배터리 소모의 문제점을 해결하는 게이트 자동인증 시스템 및 그 방법을 제공할 수 있게 된다.

도면의 간단한 설명

- [0021] 도 1은 본 발명의 일 실시예에 따른 게이트 자동인증 시스템을 설명하기 위해 제공되는 도면,
 도 2는 본 발명의 일 실시예에 따른 게이트 자동인증 시스템의 구성을 설명하기 위해 제공되는 블록도,
 도 3은 본 발명의 일 실시예에 따른 게이트의 구성을 설명하기 위해 제공되는 도면,
 도 4는 본 발명의 일 실시예에 따른 신원 정보 등록 과정을 설명하기 위해 제공되는 도면,
 도 5는 본 발명의 일 실시예에 따른 서버의 신원 확인 과정을 설명하기 위해 제공되는 도면,
 도 6은 본 발명의 일 실시예에 따른 칼만 필터를 적용한 신호의 노이즈 제거를 설명하기 위해 제공되는 도면,
 도 7은 본 발명의 일 실시예에 따른 파라볼라 안테나의 중심의 전파원을 설명하기 위해 제공되는 도면,
 도 8은 본 발명의 일 실시예에 따른 게이트 자동인증 방법을 설명하기 위해 제공되는 흐름도, 그리고,
 도 9는 본 발명의 일 실시예에 따른 출입 인증 과정을 설명하기 위해 제공되는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 이하에서는 도면을 참조하여 본 발명에 대해 보다 상세히 설명하기로 한다. 이하에 소개되는 실시예들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위한 예로서 제공되는 것이다. 본 발명의 이하 설명되는 실시예들에 한정되지 않고 다른 형태로 구체화될 수도 있다.
- [0023] 도 1은 본 발명의 일 실시예에 따른 게이트 자동인증 시스템을 설명하기 위해 제공되는 도면, 도 2는 본 발명의 일 실시예에 따른 게이트 자동인증 시스템의 구성을 설명하기 위해 제공되는 블록도, 도 3은 본 발명의 일 실시예에 따른 게이트의 구성을 설명하기 위해 제공되는 도면, 도 4는 본 발명의 일 실시예에 따른 신원 정보 등록 과정을 설명하기 위해 제공되는 도면, 도 5는 본 발명의 일 실시예에 따른 서버(300)의 신원 확인 과정을 설명하기 위해 제공되는 도면, 도 6은 본 발명의 일 실시예에 따른 칼만 필터를 적용한 신호의 노이즈 제거를 설명하기 위해 제공되는 도면, 그리고 도 7은 본 발명의 일 실시예에 따른 파라볼라 안테나(150)의 중심의 전파원을 설명하기 위해 제공되는 도면이다.
- [0024] 본 실시예에 따른 게이트 자동인증 시스템은 인증된 사용자가 스마트폰을 소지하는 것 만으로 게이트를 통과할 수 있도록 하기 위해 마련된다.
- [0025] 이를 위해, 본 게이트 자동인증 시스템은 게이트(100), 스마트기기(200) 및 서버(300)를 포함하도록 구성된다.
- [0026] 게이트(100)는 출입 통제를 담당하며, 인증되지 않은 신원불명의 사용자는 통제하고 인증된 사용자만 통과할 수 있도록 하기 위해 마련된다. 이를 위해 게이트(100)는 근접 센서(110), 게이트 무선통신 모듈(120), 제어부(130), 출입부(140) 및 파라볼라 안테나(150)를 포함하도록 구성된다.
- [0027] 근접 센서(110)는 사용자가 게이트 내의 기설정된 영역 내로 진입하는 경우 사용자를 인식하기 위해 마련된다. 사용자를 인식하기 위해 근접 센서(110)는 적외선 센서로 마련될 수 있다
- [0028] 근접 센서(110)가 사용자를 감지하여 전기적 신호를 발생시키면, 게이트 무선통신 모듈(120)에 전원이 인가되고, 게이트 무선 통신 모듈(130)이 동작하게 된다.
- [0029] 물론 근접 센서(110)는 초음파 센서로 마련될 수도 있다. 초음파 센서는 대상의 색상과 온도 등 외부요인에 의해 인식에 영향을 받지 않는다는 장점이 있지만, 초음파 센서는 음파인 관계로 상대적으로 속도가 느려 신호인식 속도가 저하되는 문제점이 있을 수 있다. 사용자를 감지할 수 있다면, 적외선 센서, 초음파 센서 이외의 감지 장치가 마련될 수 있다.
- [0030] 게이트 무선통신 모듈(120)은 스마트기기(200)에 접근 신호를 출력시키기 위해 마련된다. 접근 신호는 해당 게이트의 아이디 정보를 포함할 수 있다.
- [0031] 예를 들면, 인증된 사용자가 통과하도록 다수의 게이트가 마련될 수 있고, 각각의 게이트는 서로 다른 아이디 정보를 가지게 된다. 이 경우, 사용자가 통과하게 되는 게이트(100)만이 개방되도록, 접근 신호에 게이트(100)의 아이디 정보가 포함될 수 있다.
- [0032] 첨언하면, 아이디 정보는 게이트의 Mac Address 등 게이트를 식별할 수 있는 고유의 정보를 말한다.
- [0033] 결과적으로, 아이디 정보를 포함하는 인증요청신호를 수신하는 서버(300)는 사용자가 접근하는 게이트(100)에

동작 제어 신호를 전송하여, 사용자가 접근하는 게이트(100)만이 개방되도록 할 수 있다. 서버(300)에 관하여서는 보다 구체적으로 후술하기로 한다.

- [0034] 제어부(130)는 게이트(100)의 전반을 제어하기 위해 마련된다. 예를 들어, 근접 센서(110)가 사용자를 감지하여 전기적 신호를 발생시키면, 게이트 무선통신 모듈(120)에 전원이 인가되도록 하고, 게이트 무선 통신 모듈(130)이 접근 신호를 출력시키도록 한다.
- [0035] 여기서, 접근 신호는 스마트기기(200)의 전용 애플리케이션을 구동하는 이벤트 신호 역할을 하게 된다. 이를 통해, 전용 애플리케이션이 백그라운드에 상시 로딩되지 않더라도 인증이 수행될 수 있다.
- [0036] 또한, 제어부(130)는 서버(300)로부터 동작 제어 신호가 수신되는 경우, 출입부(140)를 개방하여 사용자가 통과할 수 있도록 할 수 있다.
- [0037] 이러한 출입부(140)는 사용자의 출입을 제한하도록 게이트를 개폐하기 위해 마련된다. 예를 들면, 출입막을 설치하여 사용자의 출입을 제한할 수 있다. 서버(300)로부터 동작 제어 신호가 수신되면, 출입막과 함께 설치된 모터를 동작시켜 출입막이 개방되도록 할 수 있다.
- [0038] 한편, 파라볼라 안테나(150)는 인식범위 내의 접근 신호와 인식범위 외의 접근 신호가 명확히 구분되도록 하기 위해 마련된다.
- [0039] 예를 들어, 스마트 무선통신 모듈(220)의 인식범위 내의 접근 신호를 클래스 A, 인식범위 외의 신호를 클래스 B라고 하면 클래스 A와 클래스 B의 경계가 되는 신호 세기가 임계값이 된다.
- [0040] 위치와 환경별로 신호의 세기가 다르기 때문에 임계값은 하나로 특정될 수 없고 따라서 임계값 설정을 자동화하는 것은 불가능하다. 그럼에도 불구하고 위치와 환경에 따라 해당 상황에서의 임계값이 명확히 정해져야 동일 주파수 대역을 사용하는 다른 프로토콜과 주변 사물이나 벽에 의해 수신되는 장애전파(멀티패스)로 인한 전파 방해에 의해 발생하는 게이트(100)의 작동오류를 방지할 수 있다.
- [0041] 구체적으로, 임계값을 주어 클래스 A와 클래스 B로 분류하는 방법으로는 소프트웨어적 방법과 하드웨어적 방법이 있다.
- [0042] 첫째, 소프트웨어적 방법으로는 칼만 필터와 같은 보정 알고리즘을 적용하여 신호의 노이즈를 제거하는 것이다. 칼만 필터를 적용한 장치를 구성하여 인식범위 내외의 위치에서 직접 신호를 측정하여 인식범위의 신호세기를 임계값으로 설정한다. 도 6를 참조하면, 칼만 필터를 적용하여 신호의 노이즈를 제거한 예시가 도시되어 있다. α 는 필터 적용 전의 신호를 나타내고, β 는 필터 적용 후의 신호를 나타낸다.
- [0043] 둘째, 하드웨어적 방법으로 파라볼라 안테나(150)를 이용하여 인식범위 내의 신호세기를 증폭시키고, 인식범위 외의 신호세기를 감쇄시켜 임계값 도출이 보다 용이하도록 할 수 있다.
- [0044] 발명의 배경이 되는 기술에서 언급한 바와 같이, 게이트 무선통신 모듈(120)의 접근 신호의 수신강도를 감지할 때 값의 차이가 명확하게 구별되지 않고 불규칙적으로 값이 튀는 문제점이 있다. 이를 위해 본 발명은 파라볼라 안테나(150)를 이용하여 신호를 집중시켜 인식의 정확성을 향상시킬 수 있다.
- [0045] 도 7을 참조하면, 파라볼라 안테나(150)의 중심에 전파원이 위치하여 신호가 반사되도록 한다. 게이트 무선통신 모듈(120)이 전파원에 해당하므로 파라볼라 안테나(150)의 중심에 장착될 수 있다. 파라볼라 안테나(150)의 오목한 면이 사용자가 지나가는 방향을 향하도록 배치하고, 오목한 면의 초점에 해당되는 위치에 게이트 무선통신 모듈(120)이 배치될 수 있다. 이를 통해, 스마트 무선통신 모듈(220)은 파라볼라 안테나(150)의 오목면에 반사된 신호를 수신하게 된다.
- [0046] 전술한 바와 같이, 스마트기기(200)에서 접근 신호의 수신강도를 감지할 때 스마트기기(200)와 게이트 무선통신 모듈(120) 간의 거리에 따라 값의 차이가 명확하게 구별되지 않고 불규칙적으로 값이 튀는 현상이 발생하는 문제점이 있다. 본 발명의 파라볼라 안테나(150)는 인식범위 내외의 신호가 서로 명확히 구분되도록 한다.
- [0047] 한편, 스마트기기(200)는 게이트(100)로부터 접근 신호를 수신하고, 서버(300)에 인증을 요청하여 스마트기기(200)를 소지하는 사용자의 출입을 인증하기 위해 마련된다.
- [0048] 이를 위해, 스마트기기(200)는 스마트 무선통신 모듈(210), 제어부(220), 인증요청 제한 모듈(230), 디스플레이부(240)를 포함하도록 구성된다.
- [0049] 스마트 무선통신 모듈(210)은 RSSI(Received signal strength indication) 데이터를 생성하고, 게이트(100)의

아이디 정보, RSSI 데이터, 스마트기기(200)의 고유번호 정보 및 신원정보를 포함하는 인증요청신호를 서버(300)에 전송하기 위해 마련된다.

- [0050] RSSI 데이터는 수신된 신호강도의 지표로써 이를 이용하면 통신하고 있는 모듈과의 상대적인 거리를 구할 수 있다. (RSSI = $-10n \log d + \text{Tx Power}$ (n은 손실))
- [0051] 따라서, 게이트 무선통신 모듈(120)의 Tx Power(송출신호세기)는 스마트기기(200)와 게이트 무선통신 모듈(120) 간의 거리와 함께, 스마트기기(200)의 스마트 무선통신 모듈(210)의 RSSI 데이터에 영향을 미치게 된다.
- [0052] 스마트 무선통신 모듈(210)은 접근 신호를 스캔하면, RSSI 데이터를 생성하고, 스마트기기(200)에 전용 애플리케이션이 실행되도록 할 수 있다. 전용 애플리케이션이 실행되면, 인증요청신호를 서버(300)에 전송하여 사용자의 인증이 수행되도록 할 수 있다.
- [0053] RSSI 데이터는 출입 인증을 하고자 하는 위치의 게이트(100)를 파악하는데 이용될 수 있다. 예를 들어, 다수의 게이트(100)로부터 스마트기기(200)에 수신되는 접근 신호 중 RSSI 데이터 값의 세기가 가장 큰 게이트(100)를 사용자가 출입 인증 하고자 하는 게이트(100)로 판단할 수 있다. 즉, RSSI 데이터 값이 가장 큰 Mac Address를 선택하여 접근 신호를 수신할 수 있다.
- [0054] 한편, 종래와 같이, 인증요청을 위해 사용자가 직접 애플리케이션을 구동시키게 되는 경우, 출입자의 불편함을 해결하고자 하는 취지를 역행하는 것이고, 전용 애플리케이션을 백그라운드에 상시 로딩시키는 것은 배터리 소모의 문제와 메모리 점유의 문제를 발생시키게 된다.
- [0055] 스마트 무선통신 모듈(210)을 통해 접근 신호가 전용 애플리케이션을 구동시키는 이벤트 신호 역할을 하게 됨으로써, 사용자가 스마트기기(200)를 소지하여 게이트에 접근하는 것만으로 출입인증이 수행될 수 있다.
- [0056] 제어부(220)는 스마트기기(200)의 전반을 제어하기 위해 마련된다. 예를 들어, 디스플레이부(240)에 신원정보가 입력되면 사용자의 신원정보를 서버(300)에 전송할 수 있다.
- [0057] 또한, 제어부(220)는 스마트 무선통신 모듈(210)에 의해 접근 신호가 스캔되면 전용 애플리케이션이 구동되도록 하고, 사용자의 신원정보를 포함하는 인증요청신호를 서버(300)에 전송할 수 있다.
- [0058] 인증요청 제한 모듈(230)은 스마트 무선통신 모듈(210)이 스캔하는 접근 신호의 RSSI 데이터 값이 일정값 이상일 경우에만 서버(300)에 인증 요청하도록 하기 위해 마련된다.
- [0059] 스마트기기(200)가 게이트(100)의 아이디 정보를 포함하는 접근 신호를 스캔하면 서버(300)로 인증요청을 하게 되는데, 초당 수회씩의 인증요청에 의해 서버(300)에 인증 데이터가 지나치게 많이 쌓여서 유효한 데이터를 골라내기 힘든 문제점이 있다. 이를 위해, 본 발명의 인증요청 제한 모듈(230)은 RSSI 데이터 값이 일정값 이상인 경우에만 서버(300)로 인증을 요청하도록 함으로써 서버 과부하 문제를 해결할 수 있게 된다. 즉, 스마트기기(200)에서 인식되는 접근 신호의 세기가 기설정된 세기 이상인 경우에만 서버(300)에 인증요청신호를 전송하도록 마련될 수 있다.
- [0060] 디스플레이부(240)는 사용자의 신원을 증명할 수 있는 정보와 사용자가 사용할 아이디 및 패스워드를 입력 받기 위해 마련된다. 이를 위해, 디스플레이부는 신원등록 영역(241)을 포함할 수 있다. 도 4(a)에 도시된 바와 같이, 사용자가 신원등록 영역(241)을 클릭하거나 터치하면, 도 4(b)에 도시된 바와 같이 디스플레이부(240)는 성명, 주민등록번호, 아이디 또는 패스워드를 입력하도록 디스플레이 될 수 있다.
- [0061] 이러한 과정을 통해 입력된 신원 정보는 출입 인증 수행을 위해 서버(300)에 전송될 수 있다.
- [0062] 한편, 서버(300)는 인증요청신호를 수신하고, 출입이 허용되는 사용자가 게이트(100)를 통과하도록 게이트(100)를 제어하기 위해 마련된다.
- [0063] 이를 위해, 서버(300)는 통신 모듈(310), 신원정보 등록 모듈(320), 제어부(330), 출입 일시 기록 모듈(340) 및 출력부(350)를 포함하도록 구성된다.
- [0064] 통신 모듈(310)은 게이트 무선통신 모듈(120) 또는 스마트 무선통신 모듈(210)과 무선통신하기 위해 마련된다.
- [0065] 예를 들면, 통신 모듈(310)은 스마트 무선통신 모듈(210)로부터 인증요청신호를 수신할 수 있고, 사용자의 인증이 완료되면, 게이트 무선통신 모듈(120)에 동작 제어 신호를 전송할 수 있다.
- [0066] 신원정보 등록 모듈(320)은 사용자의 신원을 증명할 수 있는 정보와 사용자가 사용하는 고유 아이디와 패스워드

를 포함하는 신원 정보 및 스마트기기(200)의 고유 번호 정보를 저장하기 위해 마련된다.

- [0067] 스마트기기(200)에 입력된 사용자의 신원정보와 스마트기기(200)의 고유 번호 정보는 서버(300)에 전송되어 신원정보 등록 모듈(230)에 저장될 수 있다.
- [0068] 제어부(330)은 인증을 요청하는 스마트기기(200)의 스마트 무선통신 모듈(210)로부터 수신한 신원정보와, 신원정보 등록 모듈에 의해 기 저장된 신원정보를 비교하여 사용자의 출입허용 여부를 판단하는 신원확인 절차를 수행하기 위해 마련된다.
- [0069] 스마트기기(200)로부터 수신되는 신원정보와 신원정보 등록 모듈(330)에 기저장된 신원정보를 비교하여 동일한 신원정보가 존재하는 경우, 사용자의 출입이 허용되는 것으로 판단하고, 사용자가 위치하는 게이트(100)에 동작 제어 신호를 전송할 수 있다.
- [0070] 다만, 사용자에게 의해 스마트기기(200) 분실 신고되는 경우, 제어부(330)는 신원정보 등록 모듈(320)에 저장된 고유 번호 정보에 해당하는 스마트기기(200)의 인증 수행을 제한할 수 있다.
- [0071] 제어부(330)를 통해, 신원확인 절차를 수행하여 사용자의 출입 인증을 수행할 수 있게 된다.
- [0072] 출입 일시 기록 모듈(340)은 출입이 허용되어 출입하는 사용자의 신원정보, 게이트(100)의 아이디 정보 및 출입 일시를 저장하여 관리하기 위해 마련된다. 출입 일시 기록 모듈(340)을 통해 관리자는 출입 인원 내역을 확인 및 관리할 수 있게 된다.
- [0073] 출력부(350)는 출입 일시 기록 모듈(340)에 저장된 출입 인원 내역을 출력하기 위해 마련된다. 예를 들어, 출력부(350)는, 도 5에 도시된 바와 같이, 신원 영역(351), 게이트 번호 영역(352) 및 시간 영역(353)을 포함할 수 있다.
- [0074] 신원 영역(351)은 사용자의 이름을 출력하도록 마련될 수 있으며, 게이트 번호 영역(352)는 게이트(100)를 구분하기 위해 아이디 정보를 출력할 수 있다.
- [0075] 또한, 시간 영역(353)에는 게이트의 개방 시간이 출력되도록 마련될 수 있다.
- [0076] 이를 통해, 관리자는 사용자의 출입 내역을 확인하고 관리할 수 있게 된다.
- [0077] 도 8은 본 발명의 일 실시예에 따른 게이트 자동인증 방법을 설명하기 위해 제공되는 흐름도이다.
- [0078] 전술한 바와 같이, 게이트(100)에 구비되는 근접 센서(110)가 동작할 수 있다(S810). 근접 센서(110)는 게이트(100)에 접근하는 사용자를 인식하도록 마련될 수 있다.
- [0079] 근접 센서(110)에 의해 사용자가 인식되면(S820-Yes), 게이트 무선통신 모듈(120)은 접근 신호를 출력할 수 있고(S830), 접근 신호를 수신하는 스마트기기(200)는 전용 애플리케이션이 구동되도록 할 수 있다. 반면에, 근접 센서(110)에 의해 사용자가 인식되지 않는 경우, 접근 신호는 출력되지 않는다(S820-No).
- [0080] 전용 애플리케이션이 구동되면, 스마트기기(200)는 서버(300)에 인증요청신호를 전송할 수 있다(S850). 서버(300)는 사용자의 신원정보를 포함하는 인증요청신호를 수신하면 사용자의 출입 허용여부를 판단할 수 있다.
- [0081] 그리고 서버(300)는 출입이 허용되는 사용자라고 판단되는 경우 게이트(100)를 개방하도록 제어할 수 있다(S860). 개방된 게이트는 기설정된 딜레이 시간 이후 폐쇄되도록 할 수 있다. 출입 허용여부 판단 과정에 관하여서는 도 9에서 보다 구체적으로 설명하기로 한다.
- [0082] 이를 통해, 사용자가 스마트기기(200)의 대기모드를 해제시키거나, 전용 애플리케이션을 백그라운드에 상시 구동시키지 않고도, 출입 인증을 수행할 수 있게 된다.
- [0083] 도 9는 본 발명의 일 실시예에 따른 출입 인증 과정을 설명하기 위해 제공되는 흐름도이다.
- [0084] 우선 전술한 바와 같이, 사용자를 인식하도록 근접 센서(110)가 동작할 수 있다(S905). 사용자가 게이트(100)에 진입하여 근접 센서(110)가 사용자를 인식하는 경우(S910-Yes), 근접 센서(110)는 전기적 신호를 발생시킬 수 있다(S915).
- [0085] 반면에, 사용자가 인식되지 않는 경우 전기적 신호는 발생하지 않는다(S910-No).
- [0086] 근접 센서(110)가 전기적 신호를 발생시키면 제어부(130)는 게이트 무선통신 모듈(120)에 전원이 인가되도록 할 수 있다(S920). 게이트 무선통신 모듈(120)에 전원이 인가되어 동작하면, 제어부(130)는 게이트 무선통신 모듈

(120)이 아이디 정보를 포함하는 접근 신호를 출력하도록 제어할 수 있다(S925).

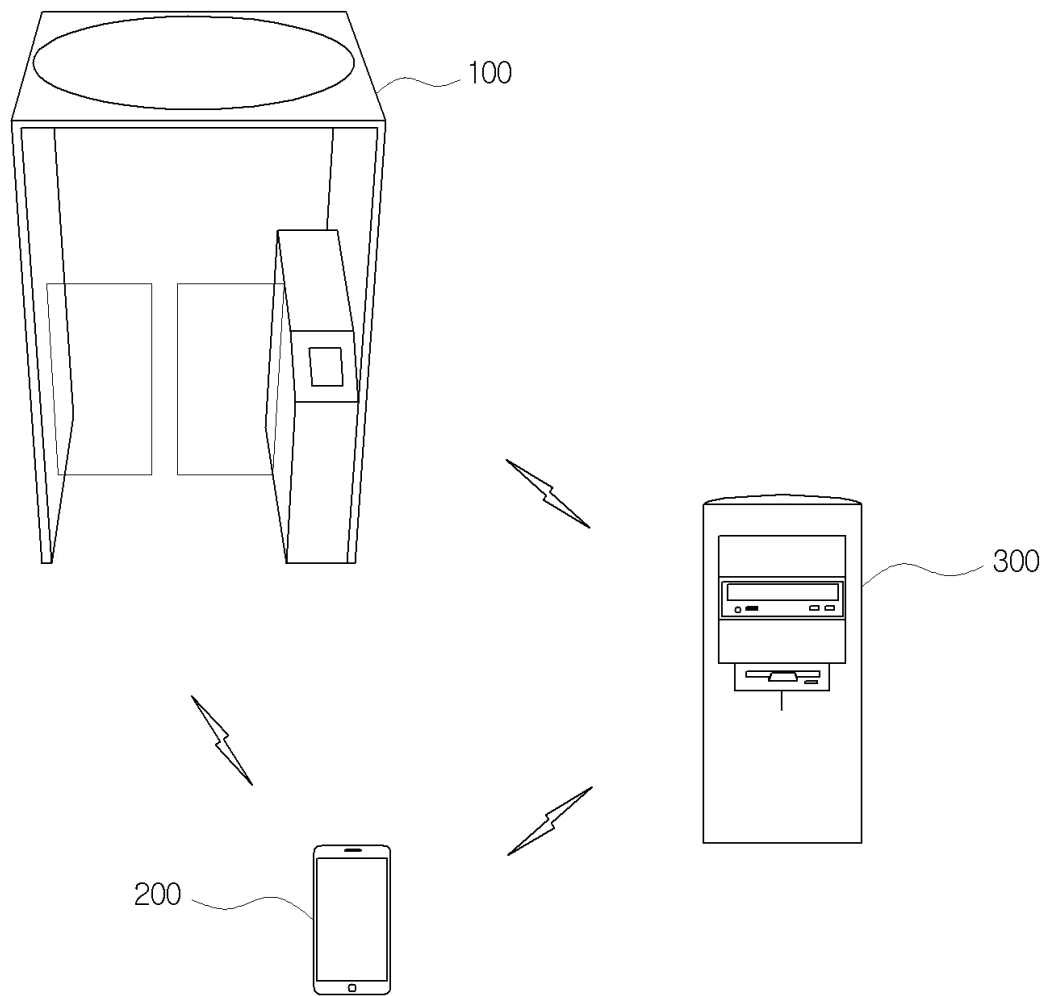
- [0087] 게이트 무선통신 모듈(120)이 접근 신호를 출력하면, 사용자가 소지하는 스마트기기(200)의 스마트 무선통신 모듈(210)은 접근 신호를 스캔할 수 있고, 신호의 세기에 따라 RSSI 데이터를 생성할 수 있다.
- [0088] 이 경우, 서로 다른 게이트(100)에서 접근 신호가 출력되는 경우, 스마트 무선통신 모듈(210)은 RSSI 데이터 값이 가장 큰 접근 신호를 스캔함으로써(S930), 사용자가 출입하고자 하는 게이트(100)를 판단할 수 있다.
- [0089] 접근 신호가 스캔되는 경우, 스마트기기(200)는 전용 애플리케이션이 구동될 수 있다(S935). 전용 애플리케이션이 구동되면, 사용자의 신원정보, 스마트기기(200)의 고유번호 정보 및 게이트(100)의 아이디 정보를 포함하는 인증요청신호를 서버(300)에 전송할 수 있다(S940).
- [0090] 서버(300)는 인증요청신호를 수신하면, 수신되는 사용자의 신원정보와 기저장된 신원정보를 비교하여, 동일한 신원정보가 존재하는 경우(S945-Yes), 게이트(100)가 개방되도록 게이트(100)에 동작 제어 신호를 전송할 수 있다(S950).
- [0091] 반면에, 동일한 신원정보가 존재하지 않는 경우(S945-No), 출입이 허용되지 않는 사용자로 판단하여, 게이트(100)에 동작 제어 신호를 전송하지 않게 된다. 첨언하면, 게이트(100)에 경고음을 발생시키도록 마련될 수도 있을 것이다.
- [0092] 게이트(100)는 동작 제어 신호를 수신하면, 사용자가 통과할 수 있도록 게이트(100)를 개방할 수 있다(S955).
- [0093] 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특징의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

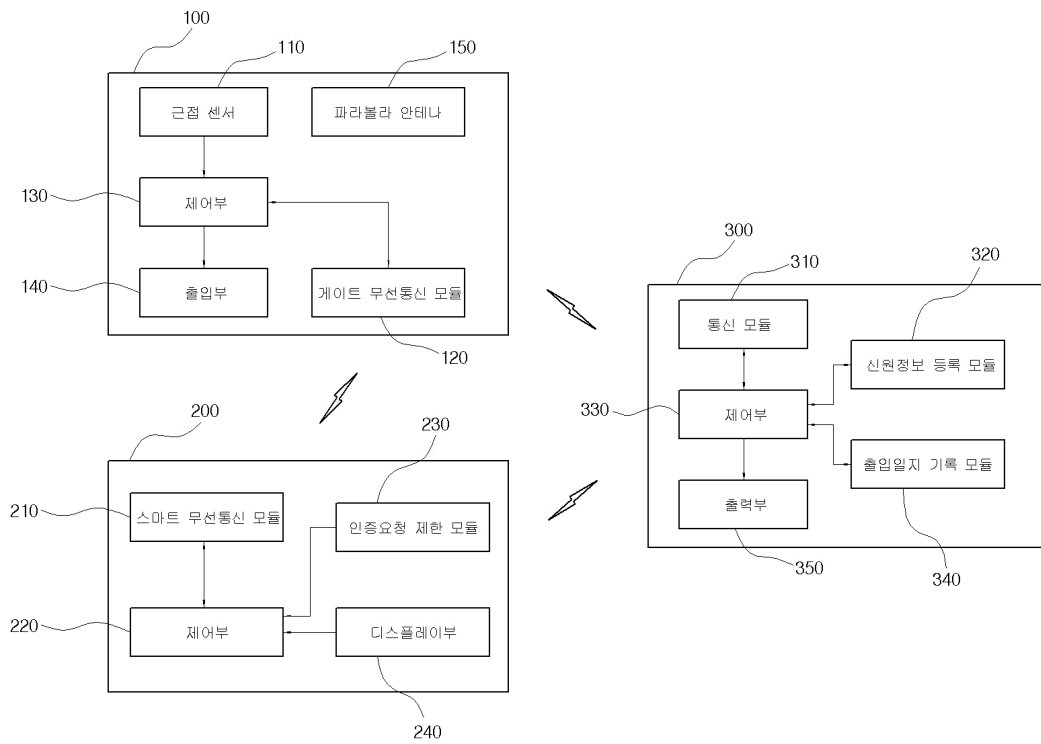
- [0094]
- | | |
|------------------|------------------|
| 100: 게이트 | 110: 근접 센서 |
| 120: 게이트 무선통신 모듈 | 130: 제어부 |
| 140: 출입부 | 150: 파라볼라 안테나 |
| 200: 스마트기기 | 210: 스마트 무선통신 모듈 |
| 220: 제어부 | 230: 인증요청 제한 모듈 |
| 240: 디스플레이부 | 300: 서버 |
| 310: 통신 모듈 | 320: 신원정보 등록 모듈 |
| 330: 제어부 | 340: 출입일지 기록 모듈 |
| 350: 출력부 | |

도면

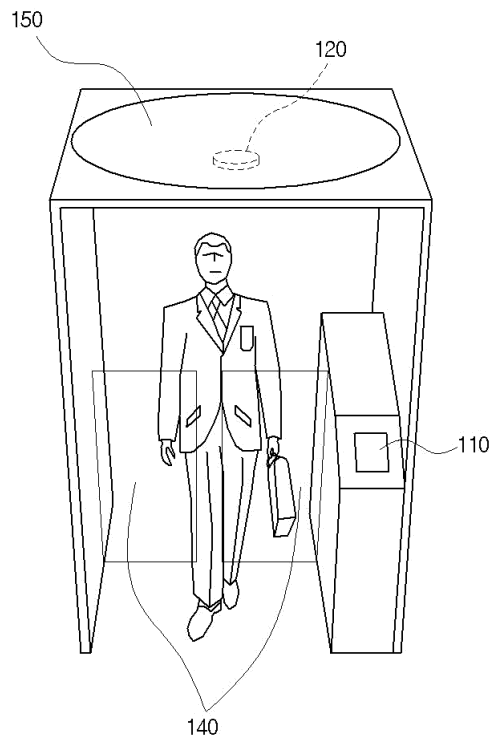
도면1



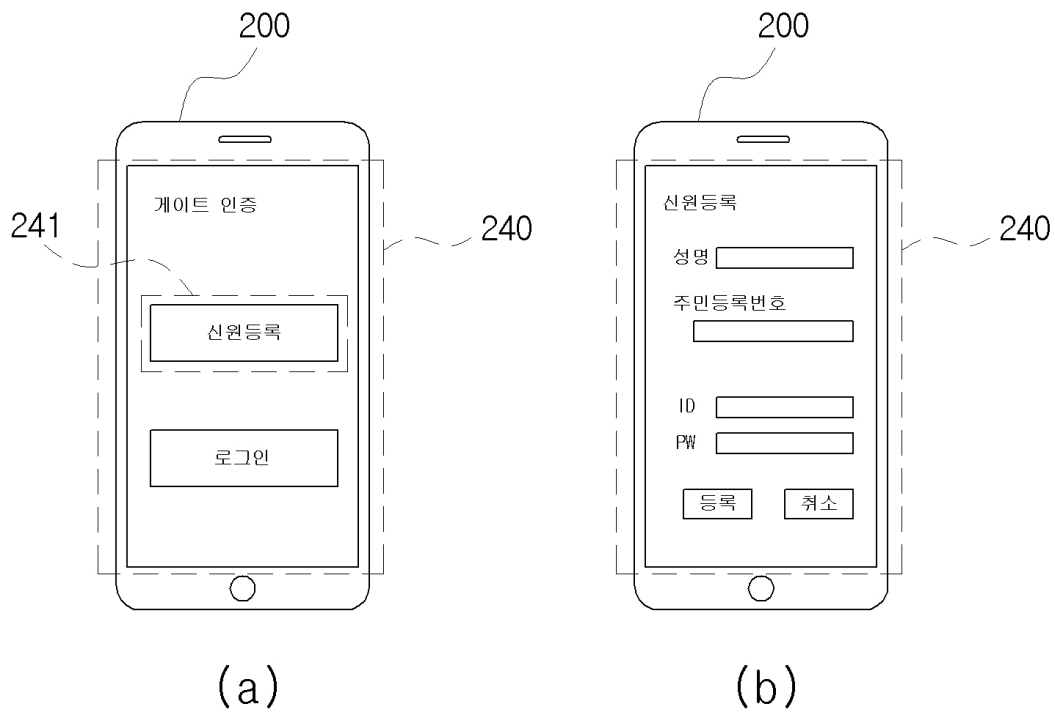
도면2



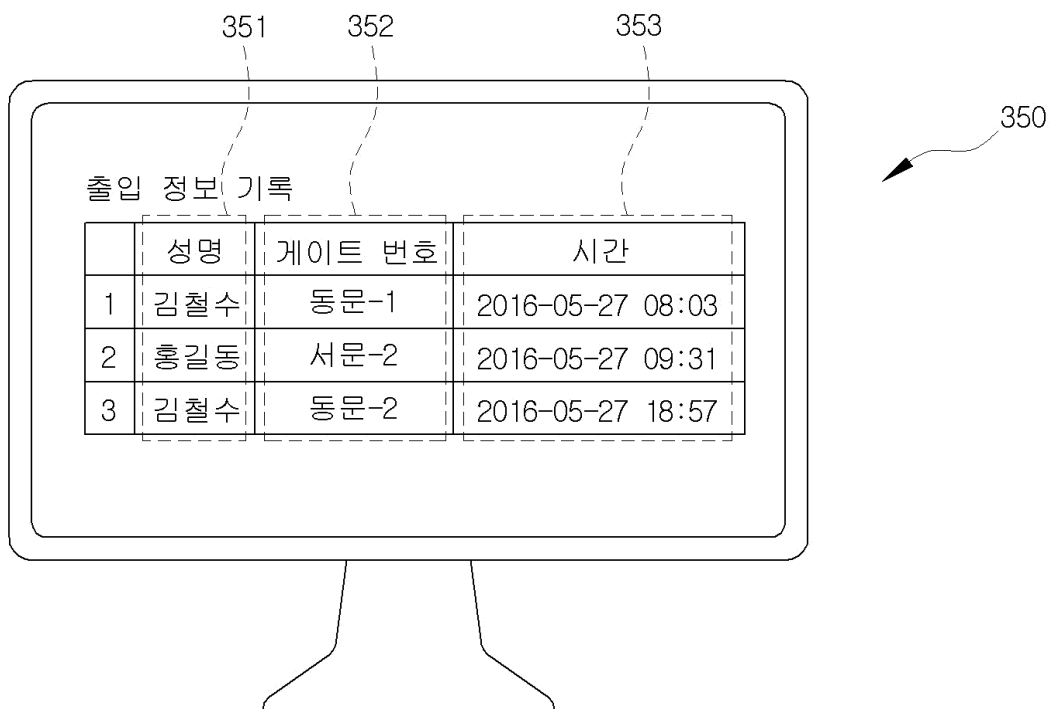
도면3



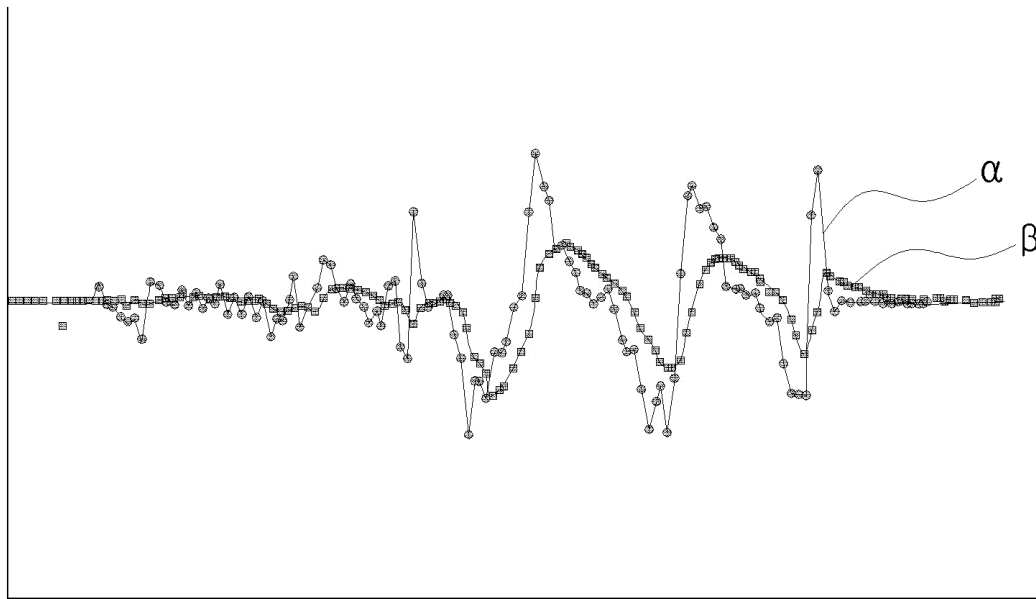
도면4



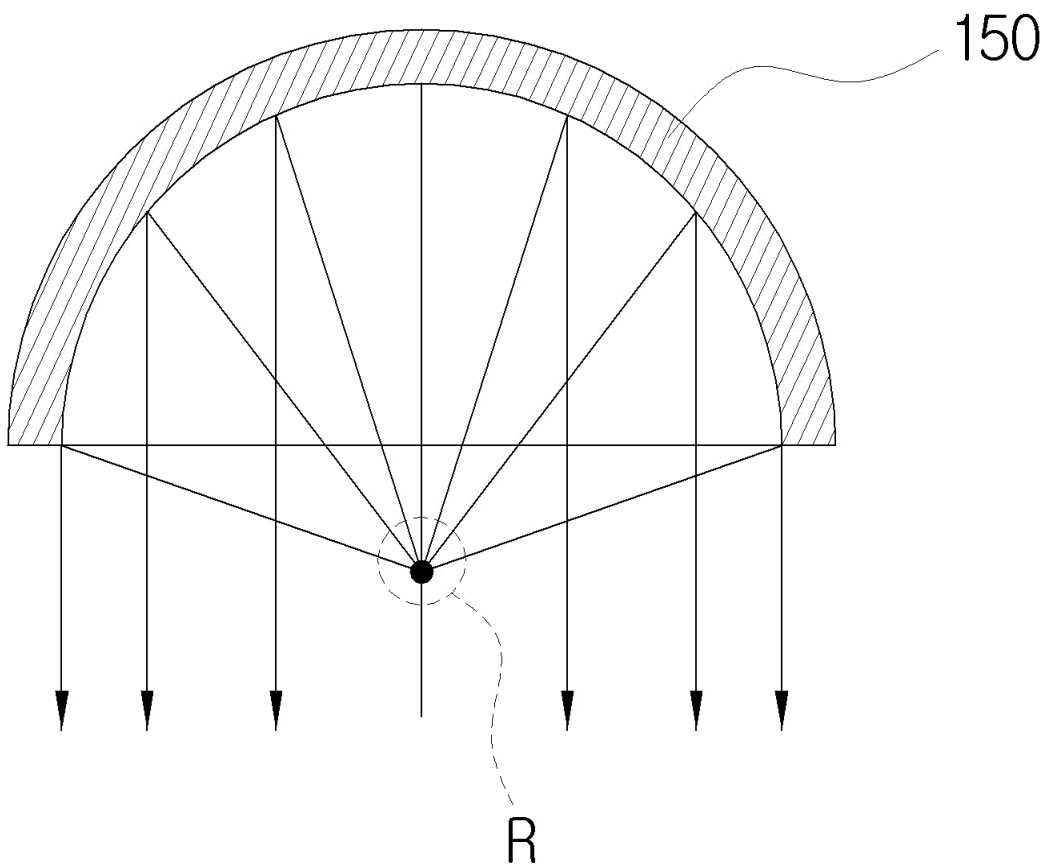
도면5



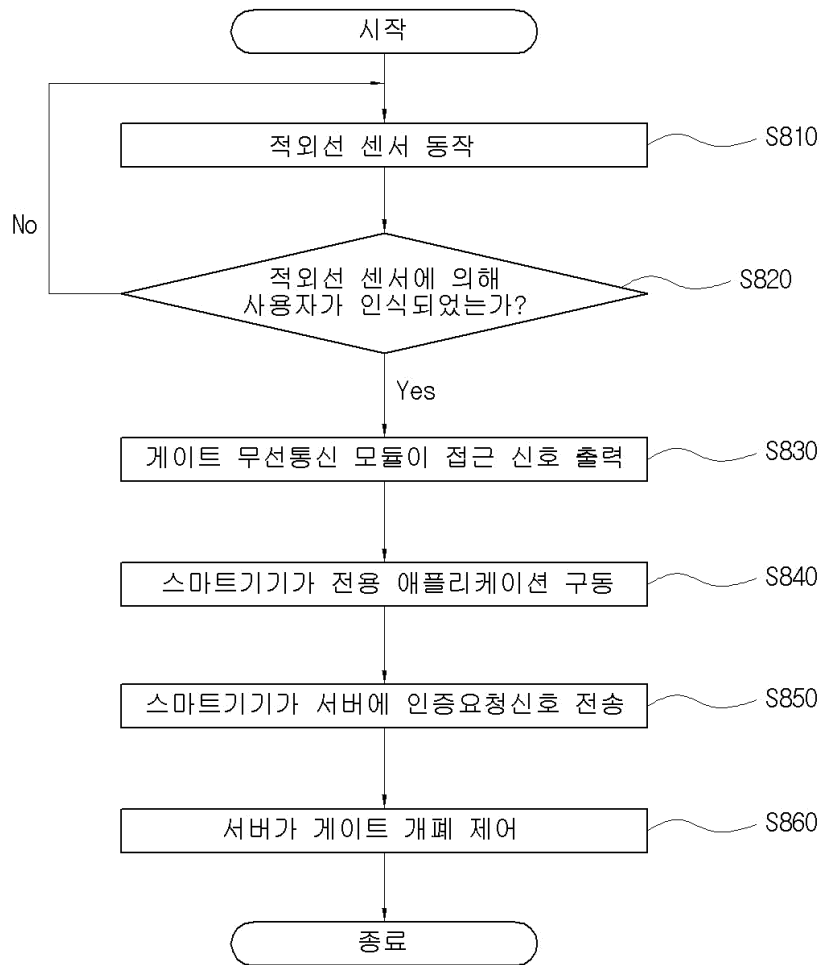
도면6



도면7



도면8



도면9

