



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년10월24일
(11) 등록번호 10-1668958
(24) 등록일자 2016년10월18일

(51) 국제특허분류(Int. Cl.)
G07C 9/00 (2006.01)
(52) CPC특허분류
G07C 9/00071 (2013.01)
G06K 9/00221 (2013.01)
(21) 출원번호 10-2015-0105874
(22) 출원일자 2015년07월27일
심사청구일자 2015년07월27일
(56) 선행기술조사문헌
JP2003286779 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)
(72) 발명자
김웅식
서울특별시 종로구 종로 347, 롯데캐슬 인동 603호 (송인동)
고해선
충청남도 천안시 서북구 입장면 연곡길 421
(74) 대리인
김대영

전체 청구항 수 : 총 3 항

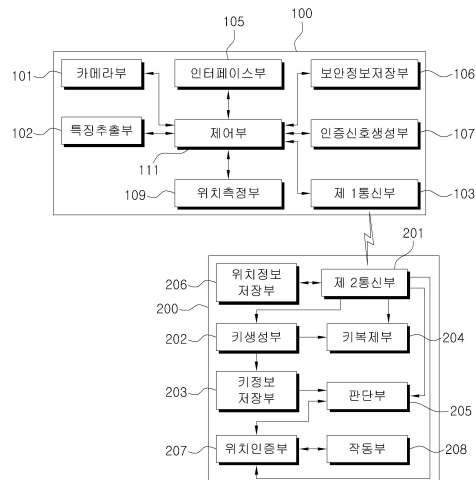
심사관 : 김동성

(54) 발명의 명칭 **휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템**

(57) 요약

본 발명은 사용자의 얼굴인식을 통해 해당 단말기에 전자 키를 생성하여 보안성을 강화함으로써 인증되지 않는 사용자의 접근을 차단하여 스마트 단말기의 도난, 아이디 및 비밀번호의 노출 등에 따른 범죄행위를 예방할 수 있는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템에 관한 것이다.

대표도 - 도2



(52) CPC특허분류

G06K 9/00268 (2013.01)

G07C 9/00134 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 C0192078

부처명 중소기업청

연구관리전문기관 (사)한국산학연합회

연구사업명 산학협력기술개발사업

연구과제명 핸드폰을 이용한 차량 도난방지 시스템 개발

기 여 율 1/1

주관기관 건양대학교산학협력단

연구기간 2014.06.01 ~ 2015.05.31

명세서

청구범위

청구항 1

안면인식을 이용한 보안시스템에 있어서,

사용자의 얼굴을 촬영하여 이미지화하는 카메라부(101)와, 상기 카메라부(101)를 통해 획득된 이미지의 특징점을 추출하되 설정된 보안 레벨에 따라 무표정일 때 추출되는 일반 얼굴 화상 특징점과 사용자가 웃거나 눈을 깜빡일 때 추출되는 특수 얼굴 화상 특징점을 구분하여 추출하는 특징추출부(102)와, 식별코드를 갖는 무선통신모듈로 이루어지는 제1통신부(103)와, 원격의 지정된 서버와 데이터 송수신을 위한 웹통신부(104)와, 사용자로부터 제어명령 및 핀 번호를 포함하는 보안정보를 입력받고 그래픽 처리신호를 출력하는 인터페이스부(105)와, 사용자가 초기단계에서 등록한 사용자 본인의 등록 안면정보 및 특징점과 보안정보와 상기 제1통신부로 수신된 키정보가 저장되는 보안정보저장부(106)와, 상기 제1통신부(103)를 통해 웹 인증정보를 수신시 상기 특징추출부(102)를 통해 추출된 특징점 및 상기 인터페이스부(105)를 통해 입력되는 보안정보를 상기 보안정보저장부(106)에 저장된 정보와 비교하여 일치시 암호화된 인증신호를 생성하는 인증신호생성부(107)와, 상기 특징추출부(102)를 통해 추출된 특징점 및 상기 인터페이스부(105)를 통해 입력된 보안정보에 대한 웹 인증을 상기 웹통신부(104)를 통해 요청하는 인증요청부(108)와, 상기 인증신호 및 식별코드 또는 키정보를 상기 제1통신부(103)를 통해 송신하고 상기 보안정보저장부(106)의 등록 안면정보 및 특징점과 핀 번호를 상기 웹통신부(104)를 통해 송신하는 제어부(111)를 구비하는 단말기(100);

상기 제1통신부(103)와 데이터 송수신이 가능한 제2통신부(201)와, 상기 제2통신부(201)에서 수신된 암호화된 인증신호를 복호화하고 수신된 식별코드를 반영하여 키정보를 생성하는 키생성부(202)와, 상기 키정보를 저장하는 키정보저장부(203)와, 상기 키정보를 상기 단말기(100)로 전송하는 키복제부(204)와, 상기 제2통신부(201)를 통해 키정보가 수신됨에 상기 키정보저장부(203)의 키정보와 일치 여부를 판단하는 판단부(205)와, 상기 판단부(205)의 일치판단에 따라 설정된 동작을 수행하는 작동부(208)와, 상기 작동부(208)에 외력이 가해지는 것을 감지하는 비인가감지부(209)와, 상기 비인가감지부(209)의 감지 이력이 누적됨에 따라 상기 키정보저장부(203)의 키정보를 삭제하고 재인증요청신호를 생성하여 상기 단말기(100)로 전송하는 재인증요청부(210)를 구비하는 보안모듈(200);

상기 웹통신부(104)와 데이터 송수신이 가능한 제3통신부(301)와, 상기 제3통신부(301)를 통해 수신된 등록 안면정보 및 특징점과 핀 번호를 저장하는 데이터베이스(302)와, 이후 동일한 식별코드를 갖는 단말기로부터 웹 인증 요청시 상기 데이터베이스(302)에 저장된 정보와 일치 여부를 비교하여 웹 인증정보를 생성하고 해당 단말기로 송신하는 웹인증부(303)를 구비하는 인증서버(300); 로 이루어지며,

상기 제어부(111)는 상기 보안모듈(200)로부터 재인증요청신호를 수신함에 따라 이를 상기 인터페이스부(105)로 출력하고 상기 보안정보저장부(106)의 키정보를 삭제하도록 구성되는 것을 특징으로 하는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 단말기(100)는 GPS신호를 통해 현재 위치정보를 생성하는 위치측정부(109)를 더 포함하고,

상기 제어부(111)는 상기 인터페이스부(105)를 통해 입력되는 위치저장명령에 의해 생성되는 최종위치정보 또는 상기 현재 위치정보를 상기 보안모듈(200)로 전송하도록 구성되며,

상기 보안모듈(200)은 상기 단말기(100)로부터 송신된 최종위치정보를 저장하는 위치정보저장부(206)와, 상기

판단부(205)의 일치결과에 따라 상기 단말기(100)로부터 현재 위치신호를 전송받아 상기 위치정보저장부(206)의 최종위치정보와 비교하여 일치시 상기 작동부(208)를 동작시키는 위치인증부(207)를 더 포함하는 특징으로 하는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 단말기(100)는 시간정보를 생성하되 암호화된 인증신호에 현재 시간정보를 포함시켜 상기 제1통신부(103)를 통해 송신하는 제1타이머부(110)를 더 포함하고,

상기 보안모듈(200)은 시간정보를 생성하되 상기 제2통신부(201)를 통해 암호화된 인증신호가 수신됨에 따라 상기 제2통신부(201)를 통해 수신되는 시간정보와 동기화하는 제2타이머부(211)를 더 포함하고,

상기 키생성부(202)는 키정보 생성시 상기 제2타이머부(211)를 통해 생성되는 시간정보를 반영하도록 구성되는 것을 특징으로 하는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템.

발명의 설명

기술 분야

[0001] 본 발명은 보안시스템에 관한 것으로, 자세하게는 사용자의 얼굴인식을 통해 보안성을 강화하여 등록된 사용자 이외의 비인가자의 접근을 제한하도록 하는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템에 관한 것이다.

배경 기술

[0002] 최근 비인가자의 시스템 접근을 방지하는 방안으로 허가된 사용자의 신체적 특징을 이용하는 방법들이 사용되고 있다. 이러한 보안체계 구축에 사용되는 신체의 특성은 다음의 조건을 만족하여야 한다.

[0003] 첫째로 개인마다 분명하게 구별되는 특징이어야 하고, 둘째로 쉽게 변하지 않는 영구불변의 특징이어야 하며, 셋째로 명백히 정의되는 특징이어야 하고, 넷째로 사용의 편리성이 있어야 한다는 것으로 여러가지 방식들이 제시되어 왔다.

[0004] 이러한 신체특징을 활용한 보안체계 중 잘 알려진 음성 인증은 신체의 접촉이 필요 없다는 편리성에서는 장점이 본인거부율이 5~10%, 타인수락율이 0.2~0.4%로 높은 편으로 고급통제를 요하는 시스템에서는 사용되지 못하고 있다.

[0005] 또한, 망막인증 방식의 경우 본인거부율 및 타인수락율이 매우 낮아 최고의 보안성을 자랑하지만 망막의 특징 추출을 위한 장치의 부피가 크고 고가이며 사용시 눈을 근접시키는 행동에 대한 심리적 거부감이 있다는 점이 단점으로 지적되고 있다.

[0006] 이에 반해 얼굴의 특징을 추출하여 본인 여부를 판별하는 방식의 경우, 본인 거부율이 0.05%, 타인수락율이 0.0002% 수준의 양호한 보안성과 사용상의 편리 및 경제성도 매우 좋아 고급 통제시스템으로부터 일반 상용 시스템에까지 그 응용 분야가 매우 넓으 것으로 알려져 있다.

[0007] 더불어, 최근 스마트폰 및 패드 타입의 스마트 단말기의 보급이 폭발적으로 증가함에 따라 하면서 이를 활용한 다양한 보안인증방식도 제안되고 있다. 하지만, 휴대용이라는 특성상 스마트 단말기의 도난 및 분실에 따른 불법적 정보누출 및 사용위험성이 도사리고 있으며, 인터넷의 발전과 함께 복합적인 보안체계의 필요성이 대두되고 있으나 아이디나 비밀번호(암호)를 이용한 종래의 인증체계에서는 해킹 등에 의해 비 인가자의 인증위험성이 높은 현실이다.

[0008] 따라서, 무선통신기술의 발전과 함께 스마트 단말기를 이용하여 일정 거리에서도 각종 보안 인증이 처리될 수 있는 상황에서, 안면인식을 조합을 비롯하여 다차원의 복합적인 방식에 따른 스마트 단말기의 강화된 인증기능

의 필요성이 증가하고 있다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국등록특허 제10-1448592호(1034.10.14. 공고)

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기와 같은 문제점을 해결하기 위하여 창출된 것으로, 본 발명의 목적은 사용자의 얼굴인식을 통해 해당 단말기에 전자 키를 생성하여 보안성을 강화함으로써 인증되지 않는 사용자의 접근을 차단하여 스마트 단말기의 도난, 아이디 및 비밀번호의 노출 등에 따른 범죄행위를 예방할 수 있는 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템을 제공하는 것이다.

과제의 해결 수단

[0011] 상기와 같은 목적을 위해 본 발명은 사용자의 얼굴을 촬영하여 이미지화하는 카메라부와, 상기 카메라부를 통해 획득된 이미지의 특징점을 추출하는 특징추출부와, 식별코드를 갖는 무선통신모듈로 이루어지는 제1통신부와, 사용자로부터 제어명령 및 핀 번호를 포함하는 보안정보를 입력받고 그래픽 처리신호를 출력하는 인터페이스부와, 등록 안면정보 및 특징점과 보안정보와 상기 제1통신부로 수신된 키정보가 저장되는 보안정보저장부와, 상기 특징추출부를 통해 추출된 특징점 및 상기 인터페이스부를 통해 입력되는 보안정보를 상기 보안정보저장부에 저장된 정보와 비교하여 일치시 암호화된 인증신호를 생성하는 인증신호생성부와, 상기 인증신호 및 식별코드 또는 키정보를 상기 제1통신부를 통해 송신하는 제어부를 구비하는 단말기; 상기 제1통신부와 데이터 송수신이 가능한 제2통신부와, 상기 제2통신부에서 수신된 암호화된 인증신호를 복호화하고 수신된 식별코드를 반영하여 키정보를 생성하는 키생성부와, 상기 키정보를 저장하는 키정보저장부와, 상기 키정보를 상기 단말기로 전송하는 키복제부와, 상기 제2통신부를 통해 키정보가 수신됨에 상기 키정보저장부의 키정보와 일치 여부를 판단하는 판단부와, 상기 판단부의 일치판단에 따라 설정된 동작을 수행하는 작동부를 구비하는 보안모듈; 로 이루어지는 것을 특징으로 한다.

[0012] 이때 상기 단말기는 원격의 지정된 서버와 데이터 송수신을 위한 웹통신부와, 상기 특징추출부를 통해 추출된 특징점 및 상기 인터페이스부를 통해 입력된 보안정보에 대한 웹 인증을 상기 웹통신부를 통해 요청하는 인증요청부를 더 포함하고, 상기 제어부는 상기 보안정보저장부의 등록 안면정보 및 특징점과 핀 번호를 상기 웹통신부를 통해 송신하도록 구성되며, 상기 인증신호생성부는 상기 제1통신부를 통해 웹 인증정보를 수신시 암호화된 인증신호를 생성하도록 구성되고, 상기 웹통신부와 데이터 송수신이 가능한 제3통신부와, 상기 제3통신부를 통해 수신된 등록 안면정보 및 특징점과 핀 번호를 저장하는 데이터베이스와, 이후 동일한 식별코드를 갖는 단말기로부터 웹 인증 요청시 상기 데이터베이스에 저장된 정보와 일치 여부를 비교하여 웹 인증정보를 생성하고 해당 단말기로 송신하는 웹인증부를 구비하는 인증서버; 를 더 포함할 수 있다.

[0013] 또한, 상기 단말기는 GPS신호를 통해 현재 위치정보를 생성하는 위치측정부를 더 포함하고, 상기 제어부는 상기 인터페이스부를 통해 입력되는 위치저장명령에 의해 생성되는 최종위치정보 또는 상기 현재 위치정보를 상기 보안모듈로 전송하도록 구성되며, 상기 보안모듈은 상기 단말기로부터 송신된 최종위치정보를 저장하는 위치정보저장부와, 상기 판단부의 일치결과에 따라 상기 단말기로부터 현재 위치신호를 전송받아 상기 위치정보저장부의 최종위치정보와 비교하여 일치시 상기 작동부를 동작시키는 위치인증부를 더 포함할 수 있다.

[0014] 또한, 상기 보안모듈은 상기 작동부에 외력이 가해지는 것을 감지하는 비인가감지부와, 상기 비인가감지부의 감지 이력이 누적됨에 따라 상기 키정보저장부의 키정보를 삭제하고 재인증요청신호를 생성하여 상기 단말기로 전송하는 재인증요청부를 더 포함하고, 상기 제어부는 상기 보안모듈로부터 재인증요청신호를 수신함에 따라 이를 상기 인터페이스부로 출력하고 상기 보안정보저장부의 키정보를 삭제하도록 구성될 수 있다.

[0015] 또한, 상기 단말기는 시간정보를 생성하되 암호화된 인증신호에 현재 시간정보를 포함시켜 상기 제1통신부를 통해 송신하는 제1타이머부를 더 포함하고, 상기 보안모듈은 시간정보를 생성하되 상기 제2통신부를 통해 암호화된 인증신호가 수신됨에 따라 상기 제2통신부를 통해 수신되는 시간정보와 동기화하는 제2타이머부를 더 포함하

고, 상기 키생성부는 키정보 생성시 상기 제2타이머부를 통해 생성되는 시간정보를 반영하도록 구성될 수 있다.

발명의 효과

[0016] 본 발명을 통해 기본적으로 사용자의 안면인식결과와 보안정보 및 사용자 단말기의 식별코드를 암호화하여 전자적인 키를 생성하여 비인가자에 의한 시스템 접근을 원천적으로 봉쇄할 수 있다. 이때 1회의 인증 이후에는 생성된 키정보를 통해 복잡한 인증과정을 생략하여 편의성을 제공하게 되며, 원격의 인증서버, 위치변동, 시간 동기화 등을 조합하여 보안성을 대폭적으로 향상시킬 수 있다.

[0017] 또한, 외력에 의한 접근을 감지하여 키정보를 삭제시키고 이후 재인증을 요청함에 따라 해킹 등의 시도를 효과적으로 무력화할 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 개요도,
 도 2는 본 발명의 제1실시예에 따른 구성 및 연결관계를 나타낸 블록도,
 도 3은 본 발명의 제2실시예에 따른 구성 및 연결관계를 나타낸 블록도,
 도 4는 본 발명의 제3실시예에 따른 구성 및 연결관계를 나타낸 블록도,
 도 5는 본 발명의 제4실시예에 따른 구성 및 연결관계를 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 첨부된 도면을 참조하여 본 발명 휴대용 스마트 단말기 및 안면인식을 이용한 보안시스템의 구성을 구체적으로 설명한다.

[0020] 도 1은 본 발명의 개요도로서, 본 발명은 기본적으로 개인이 휴대하는 스마트폰이나 패드 방식의 스마트 단말기(100, 이하 '단말기'라 칭함)를 통해 구현되어 사용자의 얼굴을 인식하여 각종 보안모듈(200)에 대한 보안인증이 이루어지며 부가적으로 위성신호, 원격의 인증서버(300)를 통한 웹 인증 등 다중화된 보안이 이루어질 수 있도록 한다.

[0021] 즉 사용자의 안면인식을 통한 보안인증을 거쳐 지정된 보안대상에 설치되는 보안모듈(200)을 통해 잠금을 해제할 수 있는 전자적인 키(Key)를 생성하여 상기 단말기(100)로 복사가 이루어지게 되며, 상기 단말기(100)에 키의 복사 이후로는 인증이 없이도 생성된 키를 통해 간편하게 상기 보안모듈(200)에 접속하여 보안대상의 잠금을 해제할 수 있게 된다. 상기 보안대상은 첨부된 도 1에서는 보안대상의 예로써 차량이나 도어록을 도시하고 있으나 금고와 같은 보안이 요구되는 캐비닛을 비롯하여 특정구역의 출입을 위한 출입문 등이 될 수 있으며, 필요에 따라 신용조회단말기, ATM, POS 등과 같은 금융기기 등에 적용될 수 있는 전자적인 보안수단이 될 수도 있다.

[0022] 도 2는 본 발명의 제1실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 본 발명이 단말기(100)와, 보안모듈(200)의 구성으로 이루어지는 예를 나타내고 있다.

[0023] 먼저, 상기 단말기(100)는 카메라부(101)와 특징추출부(102)와 제1통신부(103)와 인터페이스부(105)와 보안정보저장부(106)와 인증신호생성부(107)와 제어부(111)의 세부구성을 구비한다.

[0024] 상기 카메라부(101)는 통상의 카메라 기능을 갖는 것으로 본 발명에서는 특별히 사용자의 얼굴을 촬영하여 이미지화한다.

[0025] 이때 상기 카메라부(101)와 함께 반도체 기술을 이용한 촉지방식의 지문인식센서를 부가함 추가적인 불법 인증등을 방지할 수 있다.

[0026] 상기 특징추출부(102)는 상기 카메라부(101)를 통해 안면 이미지의 특징점을 추출하는 구성이다. 기본적으로 사용자의 안면형상을 비롯하여 눈, 코, 입 등으로 이루어진 다수의 특징점이 존재하며 각 특징점들 간의 거리도 추출하게 되며, 사용자가 표정을 지을 때 사용하는 근육의 위치를 분석한 데이터 즉, 상기 인증 대상자를 식별할 수 있도록 하는 얼굴의 특징을 포함하게 된다.

[0027] 이와 더불어 사용자가 무표정일 때 추출되는 일반 얼굴 화상 특징점과 사용자가 웃거나 눈을 깜빡일 때 추출되는 특수 얼굴 화상 특징점을 구분할 수 있으며 이때, 상기 일반 얼굴 화상 특징점과 상기 특수 얼굴 화상 특징점은 미리 설정된 보안 레벨에 따라 다르게 추출될 수 있다. 상기 보안 레벨이 낮은 경우에 상기 일반 얼굴 화

상 특징점을, 상기 보안 레벨이 높은 경우에 상기 특수 얼굴 화상 특징점을 추출할 수 있다.

- [0028] 상기 제1통신부(103)는 고유의 ID 즉 식별코드를 갖는 근거리 무선통신모듈로서, 통상의 단말기에 기본적으로 구비되는 블루투스(Bluetooth)나 와이파이(Wi-Fi) 통신모듈로 이루어질 수 있다.
- [0029] 상기 인터페이스부(105)는 사용자로부터 제어명령 및 핀 번호를 포함하는 보안정보를 입력받고 그래픽 처리신호를 출력하는 입출력수단으로서, 통상의 단말기에 구비되는 터치스크린을 통해 구현된다. 이때 상기 제어명령은 단말기(100)를 통해 구현되는 여러 가지 기능을 위한 제어동작을 위한 명령이고, 상기 보안정보는 핀(PIN) 번호를 포함하여 보안을 위해 사용자로부터 설정받는 정보를 의미한다.
- [0030] 상기 보안정보저장부(106)는 상기 단말기(100)에 구비되는 메모리로서, 등록 안면정보 및 특징점과 핀 번호를 포함하는 보안정보와, 상기 보안모듈(200)로부터 생성되어 상기 제1통신부(103)로 수신된 키정보가 저장된다. 상기 등록 안면정보는 사용자가 초기단계에서 등록한 사용자 본인의 안면정보로서, 상기 카메라부(101)를 통해 촬영되고 상기 특징추출부(102)를 통해 추출된 특징점을 저장하여 등록이 이루어지게 되며, 상기 보안정보저장부(106)에 저장된 등록 안면정보 및 특징점은 이후 인증을 위해 입력되는 얼굴 이미지와의 비교를 위한 기준정보로 활용된다. 또한, 상기 보안정보저장부(106)에 저장되는 핀 번호 또한 사용자가 초기단계에서 설정한 핀 번호로써, 이후 인증을 위해 입력되는 핀 번호의 식별을 위한 기준정보가 된다.
- [0031] 상기 인증신호생성부(107)는 초기에 등록된 안면정보 및 특징점과 핀 번호가 상기 보안정보저장부(106)에 저장된 이후 인증을 위해 상기 특징추출부(102)를 통해 추출된 특징점 및 상기 인터페이스부(105)를 통해 입력되는 보안정보를 상기 보안정보저장부(106)에 저장된 정보와 비교하여 일치시 인증에 성공한 것으로 판단하여 암호화 알고리즘을 통해 암호화된 인증신호를 생성하게 된다. 이때 생성되는 인증신호는 상기 제1통신부(103)의 식별코드 및 상기 보안정보저장부(106)에 저장된 핀 번호를 기본적으로 포함하되 필요에 따라 상기 보안정보저장부(106)에 저장된 특징점을 포함할 수도 있다.
- [0032] 상기 제어부(111)는 단말기(100)의 MCU에 해당하는 구성으로 기본적으로 상기 제1통신부(103)와 인터페이스부(105)와 보안정보저장부(106)와 인증신호생성부(107)를 제어하되, 특별히 상기 인증신호 및 식별코드 또는 키정보를 상기 제1통신부(103)를 통해 송신하게 된다. 즉 먼저 상기 인증신호와 식별코드를 상기 제1통신부(103)를 통해 상기 보안모듈(200)로 전송하게 되며, 이를 토대로 상기 보안모듈(200)로부터 생성된 키정보를 전송받아 상기 보안정보저장부(106)에 저장이 이루어진다. 상기 키정보가 생성되어 상기 보안정보저장부(106)에 저장된 이후에는 별도의 인증절차 없이 상기 제어부(111)는 상기 키정보를 상기 보안모듈(200)에 전송함으로써 보안모듈에 대한 접속이 이루어져 후술되는 작동부(208)를 통해 보안대상의 잠금 해제를 비롯하여 설정된 동작이 수행되도록 한다.
- [0033] 다음으로, 상기 보안모듈(200)은 보안대상에 설치되어 잠금 해제를 비롯한 보안을 위해 설정된 동작을 수행하는 구성으로, 제2통신부(201)와, 키생성부(202)와, 키정보저장부(203)와, 키복제부(204)와, 판단부(205)와, 작동부(208)를 구비한다.
- [0034] 상기 제2통신부(201)는 상기 제1통신부(103)와 동일한 근거리 무선통신모듈로 이루어져 상호 간에 데이터 송수신을 수행하게 된다.
- [0035] 상기 키생성부(202)는 상기 제2통신부(201)에서 수신된 암호화된 인증신호를 복호화하고 상기 제1통신부(103)의 식별코드 및 핀 번호를 반영하여 키정보를 생성하게 된다. 즉 보안모듈(200)을 통해 각종 잠금 상태를 해제함에 있어 차량이나 도어록과 같이 사용빈도가 높은 보안대상의 경우 문을 열기 위해 매번 안면인식 및 핀 번호를 위한 인증이 이루어진다면 매우 번거로운 일이 될 것이다. 이에 따라 본 발명에서는 1회의 인증을 통해 전자적인 열쇠역할을 하는 키정보를 생성하고 이를 통해 이후 별도의 인증절차 없이도 생성된 키정보를 통해 잠금 해제가 이루어질 수 있도록 한다. 이때 해킹이나 여타의 불법적인 방법으로 키정보가 생성되는 것을 방지하기 위해 상기 인증신호생성부(107)의 암호화 알고리즘을 통해 인증정보가 암호화됨에 더불어 상기 키생성부(202)에 상기 암호화 알고리즘에 대응되는 복호화 알고리즘을 구비하여 인증정보를 복호화하며, 인증정보에 포함된 식별코드 및 핀 번호 등을 키정보에 반영하게 된다.
- [0036] 상기 키정보저장부(203)는 상기 보안모듈(200)에 구비되는 메모리로서, 상기 키생성부(202)에서 생성된 키정보를 저장하여, 추후 상기 단말기(100)로부터 전송되는 키정보의 식별을 위한 기준정보로 활용하도록 한다.
- [0037] 상기 키복제부(204)는 상기 키생성부(202)를 통해 생성된 키정보를 복사하여 상기 제2통신부(201)를 통해 상기 단말기(100)로 전송하는 구성으로, 상기 단말기(100)에서 수신한 키정보는 앞서 언급한 바와 같이 상기 보안정

보저장부(106)에 저장된다.

- [0038] 이와 같이 키정보가 생성되어 상기 단말기(100)에 저장된 이후에는 상기 단말기(100)를 통해 보안모듈에 접속이 이루어짐에 있어 키정보의 일치확인 절차가 이루어지게 된다. 이를 위해 상기 판단부(205)는 상기 제2통신부(201)를 통해 상기 단말기(100)로부터 키정보가 수신됨에 상기 키정보저장부(203)의 키정보와 일치 여부를 판단하여, 일치할 경우 정상적인 인가자의 접속을 판단하게 된다.
- [0039] 상기 작동부(208)는 상기 판단부(205)의 일치판단에 따라 설정된 동작을 수행하는 구성으로, 본 발명에서는 전동모터 내지는 액추에이터를 구비하여 출입문이나 금고를 비롯하여 각종 금융기기 등에서의 잠금장치를 해제하는 구성이 되거나, 특별히 차량 등에 본 발명을 적용함에 있어 차량의 시동모터와 연동하여 시동을 걸 수 있도록 구성할 수도 있다.
- [0040] 도 3은 본 발명의 제2실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 앞서 설명한 제1실시예에 원격의 인증서버(300)를 통한 웹 인증을 부가함으로써 보안성을 더욱 강화할 수 있는 구성을 나타내고 있다. 이하의 설명에서는 상술한 제1실시예에서와 동일한 구성 및 동작에 대한 구체적인 설명은 생략하기로 하며, 부가되는 구성을 중심으로 설명한다.
- [0041] 먼저, 본 발명의 제2실시예에서 상기 단말기(100)는 웹통신부(104)와 인증요청부(108)의 구성을 추가적으로 구비한다.
- [0042] 상기 웹통신부(104)는 원격의 지정된 서버와 데이터 송수신을 위한 구성으로, 통상의 단말기에 구비되는 3G/4G, LTE 등을 통해 인터넷과 같은 상용 통신망을 사용할 수 있는 통신모듈로 이루어진다. 본 발명을 실내에서 구현하는 등 경우에 따라서는 상기 제1통신부(103)와 함께 Wi-Fi 통신모듈로 구비할 수 있으나, 차량 등의 도난방지 목적을 위해 실외나 기타 Wi-Fi의 사용이 원활치 못한 장소에서 사용할 경우 상용 휴대전화 통신망을 사용하는 것이 바람직하다.
- [0043] 본 발명의 제2실시예에서 사용자는 미리 얼굴 이미지 및 핀 번호를 인증서버(300)에 등록해야만 하며, 상기 카메라부(101)를 통해 인식된 사용자의 얼굴 및 특징점과 상기 인터페이스부(105)를 통해 입력된 핀 번호가 상기 웹통신부(104)를 통해 인증서버(300)로 전송되도록 구성된다.
- [0044] 상기 인증요청부(108)는 인증서버(300)에 사용자의 얼굴 이미지 및 특징점과 핀 번호가 등록된 이후에, 상기 특징추출부(102)를 통해 추출된 특징점 및 상기 인터페이스부를 통해 입력된 보안정보에 대한 웹 인증을 상기 웹통신부(104)를 통해 상기 인증서버(300)로 요청하게 된다.
- [0045] 이와 같은 웹통신부(104) 및 인증요청부(108)의 구성이 부가됨에 따라, 상기 제어부(111)는 상기 보안정보저장부(106)의 등록 안면정보 및 특징점과 핀 번호를 상기 웹통신부를 통해 송신하도록 구성되며, 상기 인증번호생성부(107)는 상기 인증서버(300)를 통해 생성된 웹 인증정보를 상기 제1통신부(103)를 통해 수신할 경우에만 암호화된 인증번호를 생성하도록 구성된다.
- [0046] 다음으로, 상기 인증서버(300)의 경우 원격의 장소에 위치하여 상기 단말기(100)와 통신을 하며 인증작업을 수행하는 구성으로 제3통신부(301)와 데이터베이스(302)와 웹인증부(303)의 세부구성을 구비하게 된다.
- [0047] 상기 제3통신부(301)는 상기 웹통신부(104)와 데이터 송수신을 하기 위한 구성으로 기본적으로 상기 웹통신부(104)와 동일한 통신모듈로 이루어질 수 있다.
- [0048] 상기 데이터베이스(302)는 상기 제3통신부(301)를 통해 수신된 등록 안면정보 및 특징점과 핀 번호를 저장하는 구성으로, 앞서 언급한 바와 같이 사용자는 웹 인증을 위해 초기에 미리 상기 인증서버(300) 측에 본인의 얼굴 이미지와 본인이 설정한 핀 번호를 저장하여 기준자료로 활용하여 추후 이를 근거로 인증이 이루어지도록 한다. 이때 수신된 등록 안면정보 및 특징점과 핀 번호를 단말기의 식별코드와 함께 저장함으로써 다수의 단말기에 대한 웹 인증을 동시에 수행할 수 있도록 한다.
- [0049] 상기 웹인증부(303)는 이후 동일한 식별코드를 갖는 단말기로부터 웹 인증 요청시 요청에 따라 전송된 얼굴 이미지와 핀 번호를 상기 데이터베이스(302)에 저장된 정보와 일치 여부를 비교하여 일치할 경우 웹 인증정보를 생성하여 이를 상기 제3통신부(301)를 통해 웹 인증을 요청한 단말기로 회신하게 된다.
- [0050] 이와 같은 웹 인증 방식을 부가함으로써 인증절차가 한층 복잡해짐에 따라 보안성을 강화할 수 있을 뿐만 아니라 상기 인증서버(300)의 경우 원격지에서 보안관리가 이루어지게 되므로 단말기의 분실과 단말기 해킹에 따른 불법적인 인증을 효과적으로 방지할 수 있게 된다.

- [0051] 도 4는 본 발명의 제3실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 상술한 제1실시예에 대하여 차량을 비롯하여 도난과 함께 위치이동이 발생하는 대상의 최종위치검증에 따라 재인증을 요구하기 위한 구성이 부가되고 있다.
- [0052] 본 발명의 제3실시예에서 먼저 상기 단말기(100)는 GPS신호를 통해 현재 위치정보를 생성하는 위치측정부(109)를 더 포함하게 된다. 이는 통상적인 단말기에 구비되는 GPS 통신모듈로서 사용자가 동작명령을 입력함에 따라 실시간으로 현재 위치를 측정하여 지도상에 표시할 수 있다.
- [0053] 상기 제어부(111)는 상기 인터페이스부(105)를 통해 입력되는 위치저장명령에 의해 생성되는 최종위치정보 또는 상기 현재 위치정보를 상기 보안모듈(200)로 전송하도록 구성된다. 즉 실시간으로 상기 위치측정부(109)를 통해 생성되는 위치정보를 보안모듈(200)로 전송하고 상기 단말기(100)가 보안모듈(200)과 통신이 끊어짐에 의한 최종 위치를 보안모듈(200)에 저장하는 방법도 사용할 수 있으나 이는 불필요한 전력의 소모와 시스템 부하의 증가로 이어지므로 사용자가 상기 보안모듈(200)에 대한 접속을 끊기 전 상기 인터페이스부(105)를 통해 위치저장명령을 입력함으로 상기 위치측정부(109)에서 생성된 현재 위치를 최종위치정보로 지정하여 상기 제1통신부(103)를 통해 상기 보안모듈(200)로 전송하는 것이 바람직하다.
- [0054] 이에 대응하여 상기 보안모듈(200)에는 위치정보저장부(206)와 위치인증부(207)의 구성이 부가된다.
- [0055] 상기 위치정보저장부(206)는 상기 단말기(100)로부터 송신된 최종위치정보를 저장하는 메모리의 구성으로, 저장된 최종위치정보는 시간이 지난 후 생성되었던 키정보를 통해 사용자의 접속이 이루어졌을 때 위치변동 유무를 판단하기 위한 기준데이터로 사용된다.
- [0056] 상기 위치인증부(207)는 상기 단말기(100)의 키정보와 상기 보안모듈(200)의 키정보가 일치한다는 상기 판단부(205)의 판단에 따라 상기 단말기(100)로부터 상기 위치측정부(109)를 통해 생성된 현재 위치정보를 전송받고 이를 상기 최종위치정보와 비교하여 일치시에만 상기 작동부(208)를 동작시키도록 구성된다.
- [0057] 이때 상기 단말기(100)로부터 전송된 현재위치정보와 상기 위치정보저장부(206)에 저장된 최종위치정보가 일치하지 않을 경우 상기 작동부(208)가 동작하지 않을 뿐만 아니라 재인증요청신호를 생성하여 상기 단말기(100)로 전송함으로 사용자는 기존 저장된 키정보를 삭제하고 본인의 지문과 핀 번호 입력을 통한 재인증으로 새로운 키정보를 생성하여 상기 작동부를 작동시키도록 하게 된다.
- [0058] 이와 같은 구성은 특별히 차량과 같이 도난에 의해 위치이동이 발생하는 보안대상에 적용하여 위치 이동이 감지되었을 경우 재인증을 통한 키정보를 다시 생성하지 않는 한 상기 작동부(208)가 동작하지 않도록 하기 위한 것으로, 도난에 의한 위치이동이 발생하더라도 실질적으로 비인가자는 대상의 잠금 상태를 쉽게 해제할 수 없게 된다.
- [0059] 도 5는 본 발명의 제4실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 외력에 의한 보안모듈(200)의 파손 등의 물리적 접근에 따른 대응구성과, 상기 키정보의 보안성을 더욱 높일 수 있는 구성이 부가되고 있다.
- [0060] 먼저, 보안모듈(200)에 대한 비인가자의 접근에 대응하기 위해 상기 보안모듈(200)에는 비인가감지부(209)와, 재인증요청부(210)의 구성이 부가된다.
- [0061] 상기 비인가감지부(209)는 상기 작동부(208)에 물리적인 외력이 가해지는 것을 감지하는 센서로서, 충격이나 분해 등을 감지할 수 있는 센서를 사용할 수도 있으나 바람직하게는 상기 작동부(208)가 비정상적으로 동작하는 것을 감지할 수 있는 센서를 사용한다. 예를 들어 상기 작동부(208)가 전동모터이고 차량 출입문의 잠금장치를 개폐할 수 있도록 구성된 경우 정상적인 상태에서는 상기 작동부(208)에 전원이 공급됨으로 출입문의 개폐 동작이 이루어지게 된다. 하지만, 비인가자가 비정상적인 방법 이를테면 특정도구를 사용하여 출입문의 개방을 시도함으로 상기 작동부(208)에 전원이 공급되지 않는 상태에서 역으로 전동모터의 축이 돌아가는 현상이 발생하므로 이를 비인가자의 물리적 접근으로 인지하여 감지하는 것이다.
- [0062] 상기 재인증요청부(210)는 상기 비인가감지부(209)의 감지 이력이 누적됨에 따라 상기 키정보저장부(203)의 키정보를 삭제하고 재인증요청신호를 생성하여 상기 단말기(100)로 전송하는 구성이다. 이는 상기 비인가감지부(209)가 비인가자의 불법적인 접근 외에 통상의 충격 등에 의해 오동작하는 것을 방지하기 위한 것으로, 상기 비인가감지부(209)의 감지결과가 설정된 횟수나 설정된 패턴의 양상과 일치할 경우 이전에 생성된 키정보를 삭제하여 사용할 수 없도록 하고, 재인증요청신호를 상기 단말기(100)로 전송하고 상기 인터페이스부(105)를 통해 사용자에게 출력함으로 새로운 키정보를 생성하는 절차가 이루어지도록 한다.
- [0063] 또한, 이에 대응하여 상기 단말기(100)의 제어부(111)는 상기 보안모듈(200)로부터 재인증요청신호를 수신함에

따라 이를 상기 인터페이스부(105)로 출력하고 상기 보안정보저장부(106)의 키정보를 삭제하게 된다.

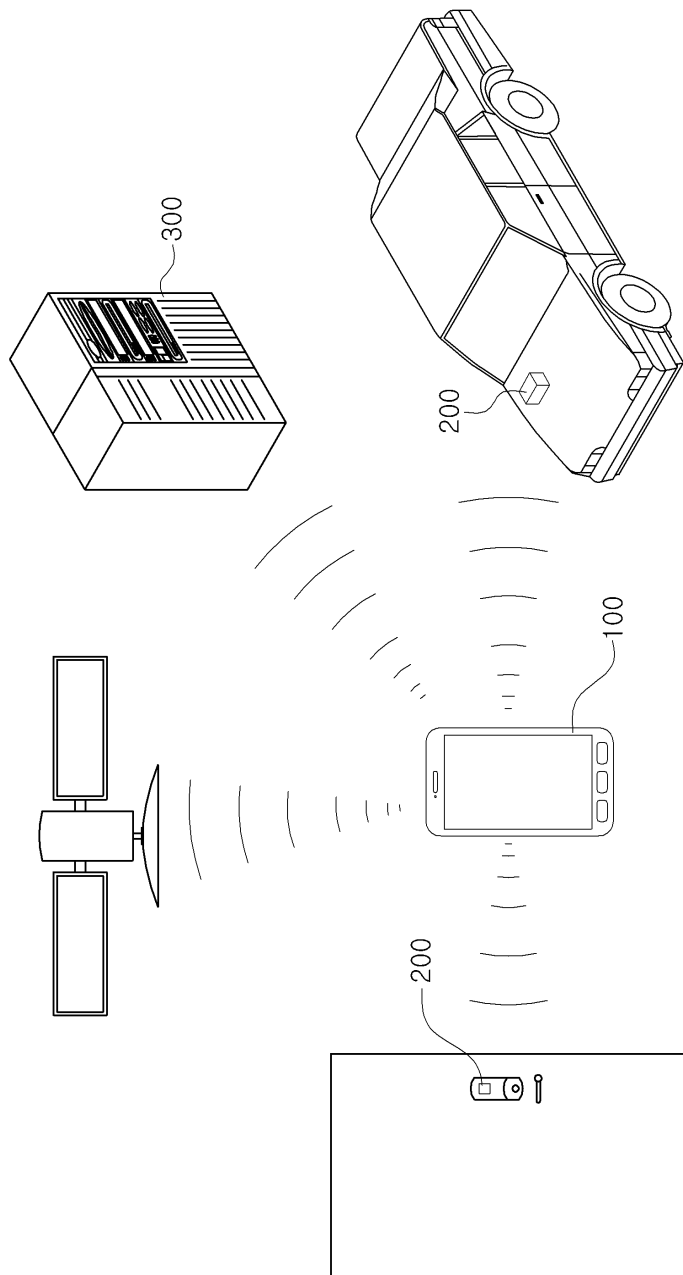
- [0064] 더불어 키정보의 보안성을 향상시키기 위해 상기 단말기(100)와 보안모듈(200) 모두 시간정보를 생성하되 이를 동기화시킴으로 해킹 또는 시간정보가 없거나 동기화되지 않는 경우 정상적인 키정보가 생성되지 않도록 구성할 수 있다.
- [0065] 이를 위해 상기 단말기(100)는 시간정보를 생성하되 암호화된 인증신호에 현재 시간정보를 포함시켜 상기 제1통신부(103)를 통해 송신하는 제1타이머부(110)를 더 포함하게 된다. 상기 제1타이머부(110)는 통상적인 단말기에 기본적으로 구비되는 시계 내지는 사용자에게 의해 설정되는 시간을 활용할 수 있으며, 필요에 따라 상기 위치측정부(109)에 구비되는 GPS 모듈을 통해 시간정보를 얻을 수 있다.
- [0066] 또한, 상기 보안모듈(200)도 마찬가지로 시계와 같은 구성을 통해 시간정보를 생성하되 상기 제2통신부(201)를 통해 암호화된 인증신호가 수신됨에 따라 상기 제2통신부(201)를 통해 수신되는 시간정보와 동기화하는 제2타이머부(211)를 더 포함하게 된다.
- [0067] 이후 상기 키생성부(202)는 키정보 생성시 상기 제2타이머부(211)를 통해 생성되는 시간정보를 반영하도록 구성되며, 상기 판단부(205)에서 키정보에 반영된 시간정보의 일치 여부까지 확인함에 따라 키정보의 보안성이 더욱 향상될 수 있다.
- [0068] 본 발명에서는 구체적인 구성을 편의에 의해 4가지의 실시예를 통해 설명이 이루어졌으나 상술한 4가지 실시예에서 설명한 구성의 일부를 조합하여 구현할 수 있음을 당연하다.
- [0069] 본 발명의 권리는 위에서 설명된 실시 예에 한정되지 않고 청구범위에 기재된 바에 의해 정의되며, 본 발명의 분야에서 통상의 지식을 가진 자가 청구범위에 기재된 권리범위 내에서 다양한 변형과 개작을 할 수 있다는 것은 자명하다.

부호의 설명

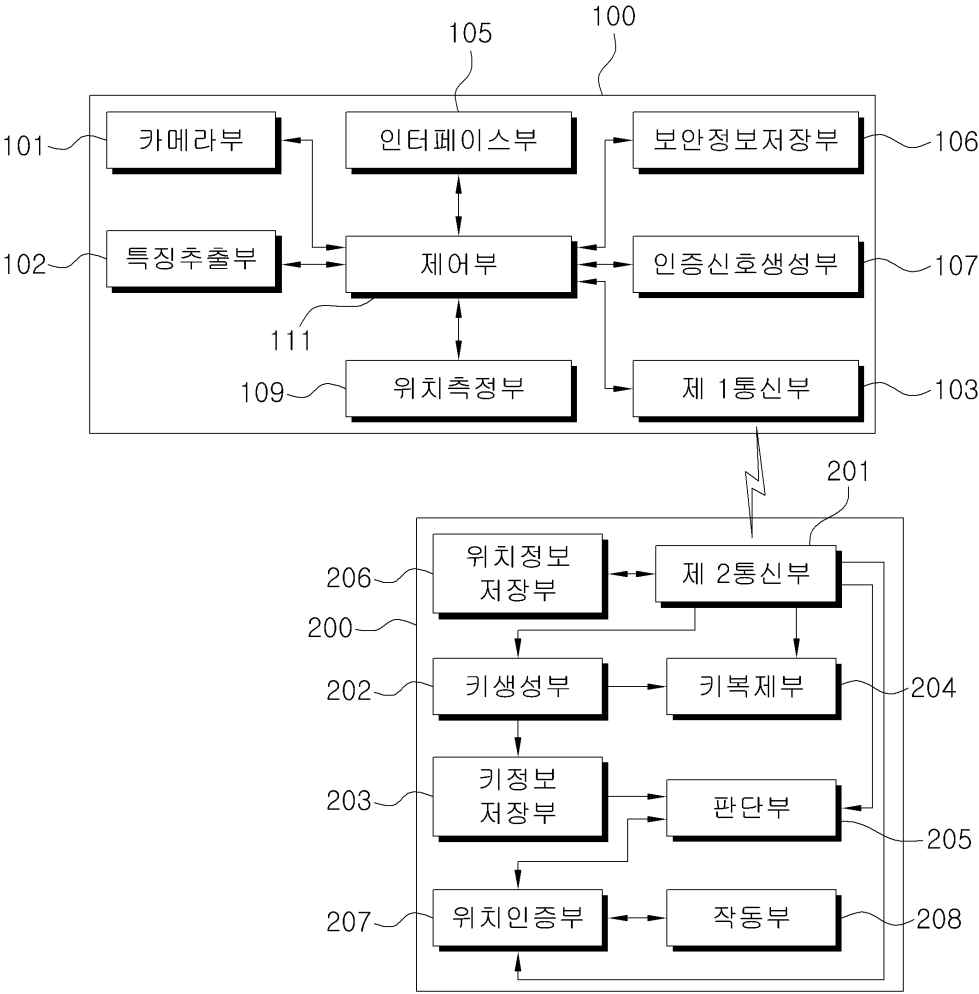
- [0070]
- | | |
|--------------|--------------|
| 100: 단말기 | 101: 카메라부 |
| 102: 특징추출부 | 103: 제1통신부 |
| 104: 웹통신부 | 105: 인터페이스부 |
| 106: 보안정보저장부 | 107: 인증신호생성부 |
| 108: 인증요청부 | 109: 위치측정부 |
| 110: 제1타이머부 | 111: 제어부 |
| 200: 보안모듈 | 201: 제2통신부 |
| 202: 키생성부 | 203: 키정보저장부 |
| 204: 키복제부 | 205: 판단부 |
| 206: 위치정보저장부 | 207: 위치인증부 |
| 208: 작동부 | 209: 비인가감지부 |
| 210: 재인증요청부 | 211: 제2타이머부 |
| 300: 인증서버 | 301: 제3통신부 |
| 302: 데이터베이스 | 303: 웹인증부 |

도면

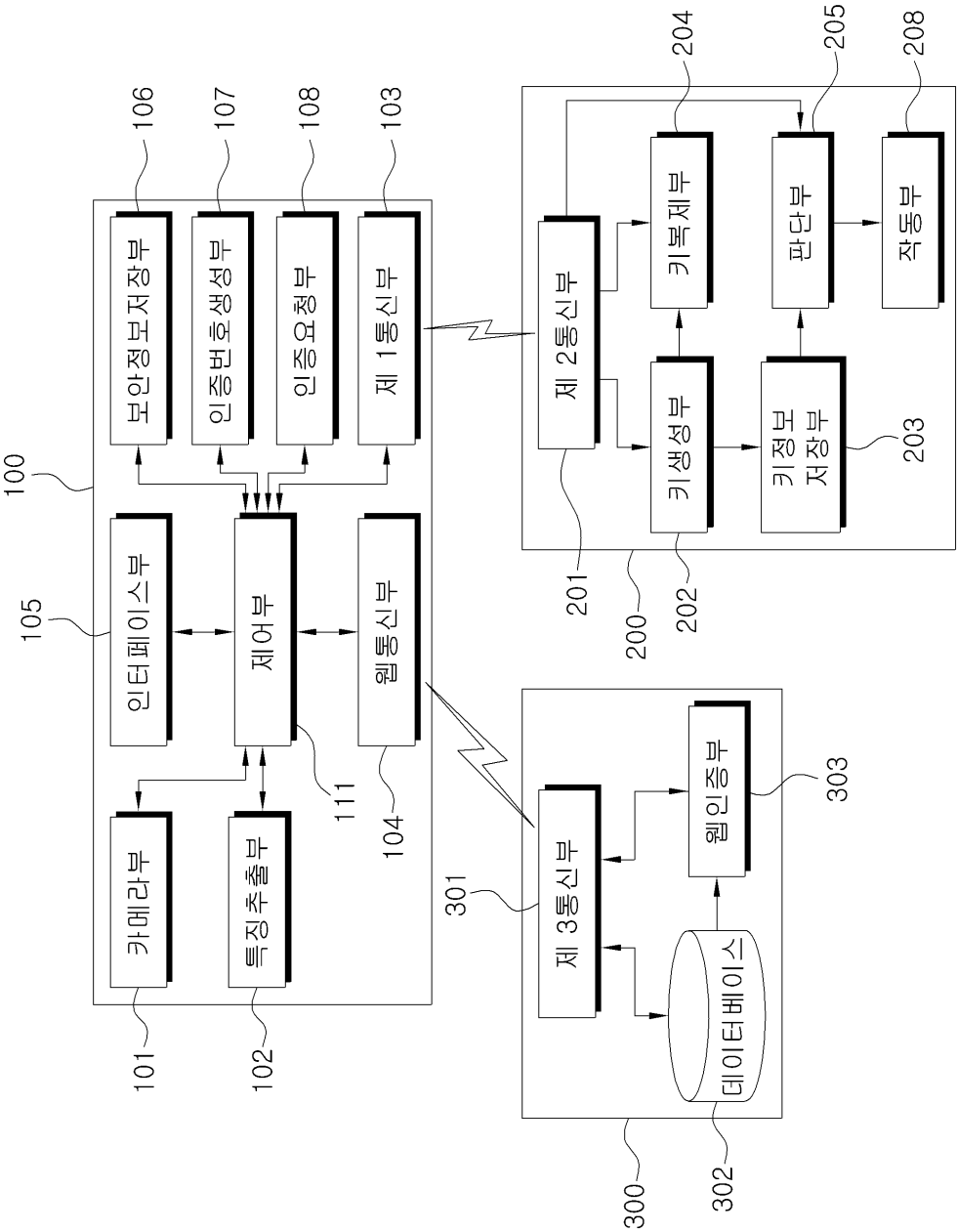
도면1



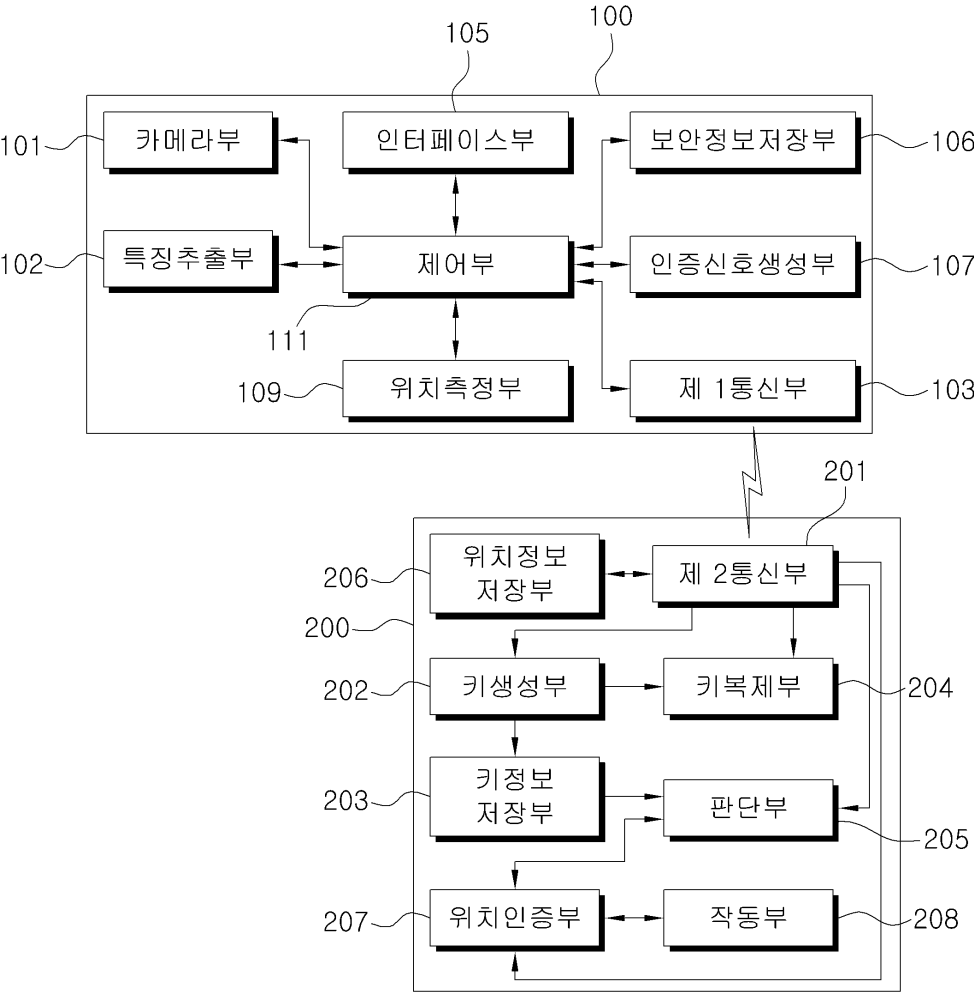
도면2



도면3



도면4



도면5

