(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년08월28일
(11) 등록번호 10-1973589
(24) 등록일자 2019년04월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06K 19/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
G06K 19/06037 (2013.01)
(21) 출원번호 10-2017-0120472
(22) 출원일자 2017년09월19일
심사청구일자 2017년09월19일
(65) 공개번호 10-2019-0032035
(43) 공개일자 2019년03월27일
(56) 선행기술조사문헌
KR101348430 B1*
KR1020120037330 A*
KR1020120093596 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 베스티언
서울특별시 강남구 논현로 166 ,401호(도곡동,풍양빌딩)
(72) 발명자
김영석
경기도 성남시 분당구 정자로 144, 403동 1902호 (정자동, 정든마을우성4단지아파트)
(74) 대리인
특허법인세원

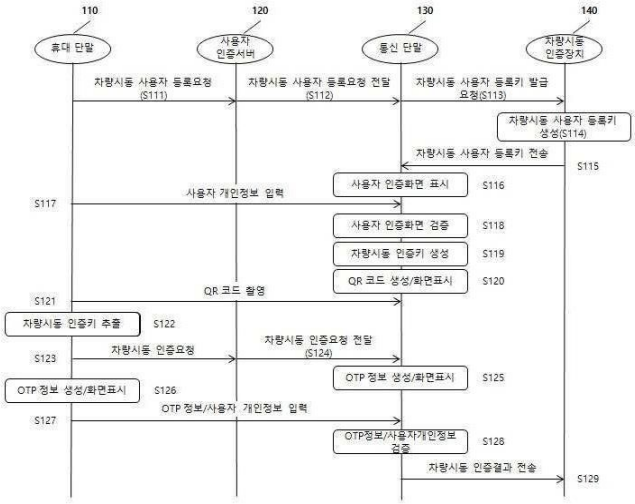
전체 청구항 수 : 총 12 항 심사관 : 양종필

(54) 발명의 명칭 **QR 코드와 OTP 정보를 이용한 차량 시동 인증 시스템 및 그 방법**

(57) 요 약

본 발명에 의한 QR 코드와 OTP 정보를 이용한 차량 시동 인증 시스템 및 그 방법이 개시된다. 본 발명의 일 실시예에 따른 차량 시동 인증 방법은 차량시동 인증장치에서 차량 시동할 사용자의 차량시동 사용자 등록 요청에 따라 차량시동 사용자 등록키를 생성하는 단계; 통신 단말에서 상기 생성된 차량시동 사용자 등록키를 기반으로 차량시동 인증키를 생성하고, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는 단계; 휴대 단말에서 상기 화면에 표시된 QR 코드를 촬영하여 차량시동 인증키를 추출하고, 상기 추출된 차량시동 인증키를 이용하여 제1 OTP 정보를 생성하는 단계; 및 상기 통신 단말에서 상기 생성된 차량시동 인증키를 이용하여 제2 OTP 정보를 생성하고, 상기 제1 OTP 정보와 상기 제2 OTP 정보를 비교하여 차량 시동 인증 결과를 판단하며 상기 판단한 결과를 상기 차량시동 인증 장치에 제공하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 9/0816 (2013.01)
H04L 9/0869 (2013.01)
H04L 2209/84 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 10060105
부처명 산업통상자원부
연구관리전문기관 한국산업기술평가관리원
연구사업명 2015년도 제6차 산업핵심기술개발사업
연구과제명 OTP기반의 HSM을 활용한 차량용 인증 · 보안 · 예지보전 플랫폼 기술 개발
기 여 율 1/1
주관기관 (주)미래테크놀로지
연구기간 2015.12.01 ~ 2018.11.30

명 세 서

청구범위

청구항 1

차량시동 인증장치에서 차량 시동할 사용자의 차량시동 사용자 등록 요청에 따라 차량시동 사용자 등록키를 생성하는 단계;

통신 단말에서 상기 생성된 차량시동 사용자 등록키를 기반으로 차량시동 인증키를 생성하고, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는 단계;

휴대 단말에서 상기 화면에 표시된 QR 코드를 촬영하여 차량시동 인증키를 추출하고, 상기 추출된 차량시동 인증키를 이용하여 제1 OTP 정보를 생성하는 단계; 및

상기 통신 단말에서 상기 생성된 차량시동 인증키를 이용하여 제2 OTP 정보를 생성하고, 상기 제1 OTP 정보와 상기 제2 OTP 정보를 비교하여 차량 시동 인증 결과를 판단하며 상기 판단한 결과를 상기 차량시동 인증 장치에 제공하는 단계;를 포함하며,

상기 차량시동 사용자 등록키를 생성하는 단계는,

상기 차량 시동할 사용자가 휴대 단말에서 사용자 개인정보의 입력과 함께 차량시동 사용자 등록요청을 사용자 인증 서버에 하고,

상기 사용자 인증 서버에서 상기 입력된 사용자 개인 정보와 미리 등록된 사용자 개인정보로 사용자 인증을 한 후 상기 미리 등록된 사용자 개인정보와 상기 차량시동 사용자 등록요청을 상기 통신 단말에 전달하며,

상기 통신 단말에서 상기 차량시동 사용자 등록키 발급을 상기 차량시동 인증장치에 요청하며,

상기 차량시동 인증장치에서, 상기 차량시동 사용자 등록키를 생성하고 상기 생성된 차량시동 사용자 등록키를 상기 통신 단말에 전송하는, 차량 시동 인증 방법.

청구항 2

삭제

청구항 3

제1 항에 있어서,

상기 차량시동 사용자 등록키를 생성하는 단계는,

임의의 시각을 사용하여 랜덤값을 생성하고, 상기 생성된 랜덤값과 사용자 개인정보 및 차대번호를 조합하여 해당 사용자의 차량사용 등록정보를 생성하며, 상기 생성된 차량사용등록정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 상기 차량시동 사용자 등록키를 생성하는, 차량 시동 인증 방법.

청구항 4

제1 항에 있어서,

상기 QR 코드를 화면에 표시하는 단계는,

사용자 인증화면을 표시하여 사용자로부터 사용자 개인 정보를 입력 받으면, 상기 입력 받은 사용자 개인 정보를 검증하고,

상기 사용자 개인 정보의 검증이 완료되면, 상기 차량시동 인증키를 생성하며,

상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는, 차량 시동 인증 방법.

청구항 5

제1 항에 있어서,

상기 QR 코드를 화면에 표시하는 단계는,

소정의 시각을 사용하여 랜덤값를 생성하고, 상기 생성된 랜덤값과 사용자 개인정보 및 차량시동 사용자 등록키를 조합하여 해당 사용자의 차량시동 인증정보를 생성하며, 상기 생성된 차량시동 인증정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 차량시동 인증키를 생성하는, 차량 시동 인증 방법.

청구항 6

제1 항에 있어서,

상기 제1 OTP 정보를 생성하는 단계는,

현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키를 조합하여 그 조합한 결과로 해당 사용자의 상기 제1 OTP 정보를 생성하는, 차량 시동 인증 방법.

청구항 7

제1 항에 있어서,

상기 제2 OTP 정보를 생성하는 단계는,

현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키를 조합하여 그 조합한 결과로 해당 사용자의 상기 제2 OTP 정보를 생성하는, 차량 시동 인증 방법.

청구항 8

차량 시동할 사용자의 차량시동 사용자 등록 요청에 따라 차량시동 사용자 등록키를 생성하는 차량시동 인증장치;

상기 생성된 차량시동 사용자 등록키를 기반으로 차량시동 인증키를 생성하고, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는 통신 단말; 및

상기 화면에 표시된 QR 코드를 촬영하여 차량시동 인증키를 추출하고, 상기 추출된 차량시동 인증키를 이용하여 제1 OTP 정보를 생성하는 휴대 단말;을 포함하고,

상기 통신 단말은 상기 생성된 차량시동 인증키를 이용하여 제2 OTP 정보를 생성하고, 상기 제1 OTP 정보와 상기 제2 OTP 정보를 비교하여 차량 시동 인증 결과를 판단하며 상기 판단한 결과를 상기 차량시동인증 장치에 제공하며,

상기 차량 시동할 사용자가 휴대 단말에서 사용자 개인정보의 입력과 함께 차량시동 사용자 등록요청을 받으면, 상기 입력된 사용자 개인 정보와 미리 등록된 사용자 개인정보로 사용자 인증을 한 후 상기 미리 등록된 사용자 개인정보와 상기 차량시동 사용자 등록요청을 상기 통신 단말에 전달하는 사용자 인증 서버;를 더 포함하고,

상기 차량시동 인증장치는, 상기 통신 단말에서 상기 사용자 인증 서버로부터 전달받은 차량시동 사용자 등록키 발급을 요청 받으면, 상기 차량시동 사용자 등록키를 생성하고 상기 생성된 차량시동 사용자 등록키를 상기 통신 단말에 전송하는, 차량 시동 인증 시스템.

청구항 9

삭제

청구항 10

제8 항에 있어서,

상기 차량시동 인증장치는,

임의의 시각을 사용하여 랜덤값을 생성하고, 상기 생성된 랜덤값과 사용자 개인정보 및 차대번호를 조합하여 해당 사용자의 차량사용 등록정보를 생성하며, 상기 생성된 차량사용등록정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 상기 차량시동 사용자 등록키를 생성하는, 차량 시동 인증 시스템.

청구항 11

제8 항에 있어서,

상기 통신 단말은,

사용자 인증화면을 표시하여 사용자로부터 사용자 개인 정보를 입력 받으면, 상기 입력 받은 사용자 개인 정보를 검증하고,

상기 사용자 개인 정보의 검증이 완료되면, 상기 차량시동 인증키를 생성하며,

상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는, 차량 시동 인증 시스템.

청구항 12

제8 항에 있어서,

상기 통신 단말은,

소정의 시각을 사용하여 랜덤값를 생성하고, 상기 생성된 랜덤값과 사용자 개인정보 및 차량시동 사용자 등록키를 조합하여 해당 사용자의 차량시동 인증정보를 생성하며, 상기 생성된 차량시동 인증정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 차량시동 인증키를 생성하는, 차량 시동 인증 시스템.

청구항 13

제8 항에 있어서,

상기 휴대 단말은,

현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키를 조합하여 그 조합한 결과로 해당 사용자의 상기 제1 OTP 정보를 생성하는, 차량 시동 인증 시스템.

청구항 14

제8 항에 있어서,

상기 통신 단말은,

현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키를 조합하여 그 조합한 결과로 해당 사용자의 상기 제2 OTP 정보를 생성하는, 차량 시동 인증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 시동 인증 기술에 관한 것으로서, 특히, QR(Quick Response Code) 코드와 OTP(One Time Password) 정보를 이용한 차량 시동 인증 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0003] 현재 차량을 시동하는 장치는 자동차 키 등과 같은 인가된 장치나 차량 내 이모빌라이저(Immobilizer) 등을 통해 엔진제어전자장치에 시동명령 보내고 이 제어전자장치를 통해 크랭크 샤프트(Crank shaft)를 구동하여 정지된 엔진을 구동하는 장치로, 시동장치는 키 스위치 조작방식, 스마트키 조작방식가 있으며 또한 최근에는 차량 내의 텔레매틱스(Telmatics)서비스 제공용이나 차량공유(Car Sharing)용 통신단말을 통해서 하는 방식도 있다.

[0004] 키 스위치 조작방식은 고전적인 방식으로 자동차의 키를 키 스위치에 삽입하고 스위치의 시동위치까지 키를 회전하여 차량을 구동한다. 이 방식은 인가되지 않는 사람의 키복사를 통해 차량 도난에 취약하다.

[0005] 스마트키 조작방식은 스마트 키를 보유한 채 키 버튼을 짧은 시간 동안 누르면 차량을 구동할 수 있다. 이 방식에서 사용하는 스마트키 시스템의 구성은 근거리 무선신호(LF, RF)로 차량의 문 열기(Unlock)/닫기(Lock) 및 시동 온(On) 등의 동작을 하는 PKE 시스템이 있다. 특히, 이 시스템은 무선신호의 송수신시 롤링 키를 사용하여

보안을 강화하였다. 롤링 키는 제한된 키 목록중 한 개의 키를 서비스 처리시 사용하고 다음 서비스 처리시 키 목록에서 사용된 키를 제외한 다른 키를 사용하는 방식이다. 이 경우는 키 스위치 조작방식보다는 보안이 강화되었으나 리버스 엔지니어링을 통해 키 목록이나 롤링 키 처리 알고리즘 노출 우려가 있다.

[0006] 키 스위치와 스마트키 조작방식은 보안을 강화하기 위해 이모빌라이저를 부가한 차량도 있다. 이모빌라이저는 키 실린더의 안테나 코일로부터 유도된 전자기력에 의해 작동되는 키의 트랜스폰더(Transponder)에 저장된 비밀코드가 키 실린더의 안테나를 통해 이모빌라이저 유니트로 전달되고, 상기 안테나를 통해 전달된 키의 정보가 차량에 입력되어 있는 비밀코드와 동일한지를 이모빌라이저 유니트가 판단한다. 그리고 키의 트랜스폰더로부터 전달받는 신호와 차량에 입력되어 있는 신호가 동일한 경우에만 상기 이모빌라이저의 유니트로부터 전달받은 신호에 의해 엔진제어전자장치는 시동을 온(On)한다. 이를 통해 기존의 키 스위치나 스마트키 조작방식보다 보안성은 강화되었으나 트랜스폰더의 리버스 엔지니어링후 키 복사 시 여전히 보안취약성을 가지고 있다.

[0007] 상기 기술들은 공통적으로 자동차 키의 보유하고 시동을 온(On)해야 한다는 사용상의 불편이 있다.

[0008] 텔레매틱스는 LTE, CDMA, GSM 등과 같은 무선통신과 GPS(Global Positioning system) 기술이 결합되어 자동차에서 위치 정보, 안전 운전, 오락, 금융 서비스, 예약 및 상품 구매 등의 다양한 이동통신 서비스 제공하는 서비스나 시스템을 말한다.

[0009] 텔레매틱스를 이용한 차량시동 방식의 예로서, 스마트폰을 통해서 원격으로 차량 시동을 텔레매틱스 서비스를 제공하는 시스템(이하, 센터 시스템)에 요청하면 센터 시스템은 무선통신 또는 이동통신망을 통해 차량내의 통신단말에 그 요청정보를 보내고 통신단말을 수신된 요청정보를 검증하고 차량내 엔진제어전자장치에 그 명령을 전달하여 차량엔진을 구동한다.

[0010] 텔레매틱스 시스템이 차량소유자(자동차 구매를 통해 자동차 키 소유자) 대상의 시스템인 것과 달리 차량공유는 차량을 보유하지 않은 차량공유 서비스를 제공받는 고객이 차량공유 서비스 제공자로부터 인증받고 차내에서 비치되어 있는 자동차 키를 이용하여 차량시동을 한다.

[0011] 최근의 자동차 보안사례와 같이, 스마트폰과 센터 시스템의 해킹시 대량의 정보유출에 취약하다.

선행기술문헌

특허문헌

[0013] (특허문헌 0001) 등록특허공보 제10-1348249호

발명의 내용

해결하려는 과제

[0014] 따라서 이러한 종래 기술의 문제점을 해결하기 위한 것으로, 본 발명의 목적은 통신 단말에서 사용자에 의해 입력된 사용자 개인 정보를 검증하여 차량 시동 인증키를 생성하고 그 생성된 차량 시동 인증키를 QR 코드로 변환하여 변환된 QR 코드로 차량 시동 인증키를 휴대 단말과 공유하며, 통신 단말과 휴대 단말에서 공유한 차량 시동 인증키를 이용하여 OTP 정보를 생성하면 통신 단말에서 생성된 OTP 정보와 사용자 개인 정보를 검증하여 그 검증한 결과에 따라 차량 시동할 사용자를 인증하도록 한, QR 코드와 OTP 정보를 이용한 차량 시동 인증 시스템 및 그 방법을 제공하는데 있다.

[0015] 그러나 본 발명의 목적은 상기에 언급된 사항으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0017] 상기 목적들을 달성하기 위하여, 본 발명의 한 관점에 따른 차량 시동 인증 방법은 차량시동 인증장치에서 차량시동할 사용자의 차량시동 사용자 등록 요청에 따라 차량시동 사용자 등록키를 생성하는 단계; 통신 단말에서 상기 생성된 차량시동 사용자 등록키를 기반으로 차량시동 인증키를 생성하고, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는 단계; 휴대 단말에서 상기 화면에 표시된 QR 코드를 촬영하여 차량시동 인증키를 추출하고, 상기 추출된 차량시동 인증키를 이용하여 제1 OTP 정보를 생성하는

단계; 및 상기 통신 단말에서 상기 생성된 차량시동 인증키를 이용하여 제2 OTP 정보를 생성하고, 상기 제1 OTP 정보와 상기 제2 OTP 정보를 비교하여 차량 시동 인증 결과를 판단하며 상기 판단한 결과를 상기 차량시동 인증 장치에 제공하는 단계를 포함할 수 있다.

[0018] 바람직하게, 상기 차량시동 사용자 등록키를 생성하는 단계는 상기 차량 시동할 사용자가 휴대 단말에서 사용자 개인정보의 입력과 함께 차량시동 사용자 등록요청을 사용자 인증 서버에 하고, 상기 사용자 인증 서버에서 상기 입력된 사용자 개인 정보와 미리 등록된 사용자 개인정보로 사용자 인증을 한 후 상기 미리 등록된 사용자 개인정보와 상기 차량시동 사용자 등록요청을 상기 통신 단말에 전달하며, 상기 통신 단말에서 상기 차량시동 사용자 등록키 발급을 상기 차량시동 인증장치에 요청하며, 상기 차량시동 인증장치에서, 상기 차량시동 사용자 등록키를 생성하고 상기 생성된 차량시동 사용자 등록키를 상기 통신 단말에 전송할 수 있다.

[0019] 바람직하게, 상기 차량시동 사용자 등록키를 생성하는 단계는 임의의 시각을 사용하여 랜덤값을 생성하고, 상기 생성된 랜덤값과 사용자 개인정보, 차대번호, 및 기타 정보를 조합하여 해당 사용자의 차량사용 등록정보를 생성하며, 상기 생성된 차량사용등록정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 상기 차량시동 사용자 등록키를 생성할 수 있다.

[0020] 바람직하게, 상기 QR 코드를 화면에 표시하는 단계는 사용자 인증화면을 표시하여 사용자로부터 사용자 개인 정보를 입력 받으면, 상기 입력 받은 사용자 개인 정보를 검증하고, 상기 사용자 개인 정보의 검증이 완료되면, 상기 차량시동 인증키를 생성하며, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시할 수 있다.

[0021] 바람직하게, 상기 QR 코드를 화면에 표시하는 단계는 소정의 시각을 사용하여 랜덤값를 생성하고, 상기 생성된 랜덤값과 사용자 개인정보, 차량시동 사용자 등록키, 및 기타 정보를 조합하여 해당 사용자의 차량시동 인증정보를 생성하며, 상기 생성된 차량시동 인증정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 차량시동 인증키를 생성할 수 있다.

[0022] 바람직하게, 상기 제1 OTP 정보를 생성하는 단계는 현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키, 및 기타 정보를 조합하여 그 조합한 결과로 해당 사용자의 상기 제1 OTP 정보를 생성할 수 있다.

[0023] 바람직하게, 상기 제2 OTP 정보를 생성하는 단계는 현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키, 및 기타 정보를 조합하여 그 조합한 결과로 해당 사용자의 상기 제1 OTP 정보를 생성할 수 있다.

[0024] 본 발명의 다른 한 관점에 따른 차량 시동 인증 시스템은 차량 시동할 사용자의 차량시동 사용자 등록 요청에 따라 차량시동 사용자 등록키를 생성하는 차량시동 인증장치; 상기 생성된 차량시동 사용자 등록키를 기반으로 차량시동 인증키를 생성하고, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시하는 통신 단말; 및 상기 화면에 표시된 QR 코드를 촬영하여 차량시동 인증키를 추출하고, 상기 추출된 차량시동 인증키를 이용하여 제1 OTP 정보를 생성하는 휴대 단말을 포함하고, 상기 통신 단말은 상기 생성된 차량시동 인증키를 이용하여 제2 OTP 정보를 생성하고, 상기 제1 OTP 정보와 상기 제2 OTP 정보를 비교하여 차량시동 인증 결과를 판단하며 상기 판단한 결과를 상기 차량시동 인증 장치에 제공할 수 있다.

[0025] 바람직하게, 상기 차량 시동할 사용자가 휴대 단말에서 사용자 개인정보의 입력과 함께 차량시동 사용자 등록요청을 받으면, 상기 입력된 사용자 개인 정보와 미리 등록된 사용자 개인정보로 사용자 인증을 한 후 상기 미리 등록된 사용자 개인정보와 상기 차량시동 사용자 등록요청을 상기 통신 단말에 전달하는 사용자 인증 서버를 더 포함하고, 상기 차량시동 인증장치는 상기 통신 단말에서 상기 사용자 인증 서버로부터 전달받은 차량시동 사용자 등록키 발급을 요청 받으면, 상기 차량시동 사용자 등록키를 생성하고 상기 생성된 차량시동 사용자 등록키를 상기 통신 단말에 전송할 수 있다.

[0026] 바람직하게, 상기 차량시동 인증장치는 임의의 시각을 사용하여 랜덤값을 생성하고, 상기 생성된 랜덤값과 사용자 개인정보, 차대번호, 및 기타 정보를 조합하여 해당 사용자의 차량사용 등록정보를 생성하며, 상기 생성된 차량사용등록정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 상기 차량시동 사용자 등록키를 생성할 수 있다.

[0027] 바람직하게, 상기 통신 단말은 사용자 인증화면을 표시하여 사용자로부터 사용자 개인 정보를 입력 받으면, 상기 입력 받은 사용자 개인 정보를 검증하고, 상기 사용자 개인 정보의 검증이 완료되면, 상기 차량시동 인증키를 생성하며, 상기 생성된 차량시동 인증키를 QR 코드로 변환하여 상기 변환된 QR 코드를 화면에 표시할 수 있

다.

[0028] 바람직하게, 상기 통신 단말은 소정의 시각을 사용하여 랜덤값를 생성하고, 상기 생성된 랜덤값과 사용자 개인 정보, 차량시동 사용자 등록키, 및 기타 정보를 조합하여 해당 사용자의 차량시동 인증정보를 생성하며, 상기 생성된 차량시동 인증정보를 소정의 해쉬 알고리즘을 이용하여 해쉬 처리하여 차량시동 인증키를 생성할 수 있다.

[0029] 바람직하게, 상기 휴대 단말은 현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키, 및 기타 정보를 조합하여 그 조합한 결과로 해당 사용자의 상기 제1 OTP 정보를 생성할 수 있다.

[0030] 바람직하게, 상기 통신 단말은 현재 시각을 미리 정해진 유효시간 범위 내로 축약하여 유효시각을 구하고, 상기 구한 유효시각과 상기 차량시동 인증키, 및 기타 정보를 조합하여 그 조합한 결과로 해당 사용자의 상기 제2 OTP 정보를 생성할 수 있다.

발명의 효과

[0032] 이처럼, 본 발명은 통신 단말에서 사용자에 의해 입력된 사용자 개인 정보를 검증하여 차량 시동 인증키를 생성하고 그 생성된 차량 시동 인증키를 QR 코드로 변환하여 변환된 QR 코드로 차량 시동 인증키를 휴대 단말과 공유하며, 통신 단말과 휴대 단말에서 공유한 차량 시동 인증키를 이용하여 OTP 정보를 생성하면 통신 단말에서 생성된 OTP 정보와 사용자 개인 정보를 검증하여 그 검증한 결과에 따라 차량 시동할 사용자를 인증하도록 함으로써, 차량 시동을 위한 보안 인증을 강화할 수 있다.

[0033] 또한, 본 발명은 차량시동 사용자 등록키, 차량시동 인증키, OTP 정보를 사용자와 차량에서 유일하게 매칭되기 때문에, 대용량 보안 피해를 방지할 수 있다.

[0034] 또한, 본 발명은 차량 시동 인증 과정에서 사용자 개인 정보와 OTP 정보를 사용자가 수동으로 차량 내 통신 단말에 직접 입력하여 검증해야 하기 때문에, 통신 채널에 대한 중간자 공격(Man In The Middle Attack; MITM)을 원천적으로 봉쇄할 수 있다.

도면의 간단한 설명

[0036] 도 1은 본 발명의 일 실시예에 따른 차량 시동 인증 시스템을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 차량 시동 인증 방법을 나타내는 도면이다.

도 3은 도 1에 도시된 통신 단말의 상세한 구성을 나타내는 도면이다.

도 4는 도 1에 도시된 차량시동 인증장치의 상세한 구성을 나타내는 도면이다.

도 5는 본 발명의 일 실시예에 따른 차량시동 사용자 등록키 생성 과정을 나타내는 도면이다.

도 6은 본 발명의 일 실시예에 따른 차량 시동 인증키 생성 과정을 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 OTP 정보 생성 과정을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0037] 이하에서는, 본 발명의 실시예에 따른 QR 코드와 OTP 정보를 이용한 차량 시동 인증 시스템 및 그 방법을 첨부한 도면을 참조하여 설명한다. 본 발명에 따른 동작 및 작용을 이해하는 데 필요한 부분을 중심으로 상세히 설명한다.

[0038] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 동일한 명칭의 구성 요소에 대하여 도면에 따라 다른 참조부호를 부여할 수도 있으며, 서로 다른 도면임에도 불구하고 동일한 참조부호를 부여할 수도 있다. 그러나, 이와 같은 경우라 하더라도 해당 구성 요소가 실시예에 따라 서로 다른 기능을 갖는다는 것을 의미하거나, 서로 다른 실시예에서 동일한 기능을 갖는다는 것을 의미하는 것은 아니며, 각각의 구성 요소의 기능은 해당 실시예에서의 각각의 구성 요소에 대한 설명에 기초하여 판단하여야 할 것이다.

[0039] 특히, 본 발명에서는 통신 단말에서 사용자에 의해 입력된 사용자 개인 정보를 검증하여 차량 시동 인증키를 생성하고 그 생성된 차량 시동 인증키를 QR 코드로 변환하여 변환된 QR 코드로 차량 시동 인증키를 휴대 단말과 공유하며, 통신 단말과 휴대 단말에서 공유한 차량 시동 인증키를 이용하여 OTP 정보를 생성하면 통신 단말에서

생성된 OTP 정보와 사용자 개인 정보를 검증하여 그 검증한 결과에 따라 차량 시동할 사용자를 인증하도록 한, 새로운 차량 시동 인증 방안을 제안한다.

[0040] **도 1은 본 발명의 일 실시예에 따른 차량 시동 인증 시스템을 나타내는 도면이다.**

[0041] 도 1을 참조하면, 본 발명의 일 실시예에 따른 차량 시동 인증 시스템은 휴대 단말(110), 사용자 인증서버(120), 통신 단말(130), 차량시동 인증장치(140)를 포함할 수 있다. 이때, 각 장치들은 시스템 개발시 기능 등을 분리하여 구성할 수도 있다. 일 예로서, 사용자 인증서버(120)은 서비스 처리하는 웹 시스템과 인증정보를 저장하는 데이터베이스 시스템으로 분리할 수 있다. 또한 차량 내 통신단말도 화면 표시하는 디스플레이 장치와 이동통신모뎀을 분리하여 구성할 수도 있다.

[0042] 휴대 단말(110)은 사용자가 사용하는 장치로서, LTE, WCDMA, GSM, CDMA 등의 이동통신망에 연결되어 사용자 인증서버와 통신하여 차량 내 통신단말에 차량시동 사용자 등록 요청 및 차량시동 인증 요청을 수행할 수 있다. 이러한 휴대 단말(110)은 스마트폰이 예가 될 수 있다.

[0043] 사용자 인증서버(120)는 LTE, WCDMA, GSM, CDMA 등의 이동통신망에 연결되어 휴대단말을 통해 사용자 인증을 하고 휴대단말의 요청정보를 통신단말에 전달할 수 있다. 이러한 사용자 인증 서버(120)는 텔레매틱스나 차량공유 서비스 제공사의 서버시스템이 예가 될 수 있다.

[0044] 통신 단말(130)은 차량 내에 설치되고 사용자인증서버와 LTE, WCDMA, GSM, CDMA 등의 이동통신망에 연결되고 차량 내부의 차량시동인증장치와 CAN, MOST, FlexRay 및 Ethernet 등의 차량네트워크에 연결되어 사용자개인정보 확인, 차량시동 인증키 생성, OTP 생성 및 차량시동 인증을 수행할 수 있다. 이러한 통신 단말(130)은 차량 내에서는 이동통신용 모뎀이 내장되거나 연결된 네비게이션(Navigation)이나 오디오(Audio) 시스템이 그 예가 될 수 있다.

[0045] 차량시동 인증장치(140)는 차량 내에 설치되고 통신단말이나 차량엔진제어전자장치등과 CAN, MOST, FlexRay 및 Ethernet 등의 차량네트워크에 연결되어 차량시동사용자를 위한 차량시동 등록키를 생성하고 통신단말의 차량시동인증결과를 받아서 차량을 시동하도록 차량엔진제어장치에 명령을 전달할 수 있다. 이러한 차량시동 인증장치(140)는 이모빌라이저나 스마트키 시스템이 예가 될 수 있다.

[0046] **도 2는 본 발명의 일 실시예에 따른 차량 시동 인증 방법을 나타내는 도면이다.**

[0047] 도 2를 참조하면, 먼저 차량 시동할 사용자를 차량시동장치에 등록하는 과정으로, 사용자가 사전에 별도로 사용자인증서버에 등록된 사용자의 정보 중 아이디와 비밀번호를 차량시동사용자등록 요청정보를 함께 암호화하여 사용자인증서버에 전송하면(S111), 사용자 인증서버는 수신된 데이터를 복호화하고 사전에 등록되어 저장된 아이디와 비밀번호와 비교하여 동일한지 확인하여 사용자인증을 완료하고, 이후 사전에 등록되어 저장된 사용자의 사용자개인정보를 차량시동사용자등록요청정보와 함께 암호화 하여 차량내 통신단말에 전송할 수 있다(S112).

[0048] 다음으로, 통신단말은 수신된 데이터를 복호화하고 사용자개인정보를 차량시동 사용자 등록키 발급요청정보와 함께 암호화하여 차량시동인증장치에 전송할 수 있다(S113).

[0049] 다음으로, 차량시동인증장치는 수신된 데이터를 복호화하고 차량시동 사용자 등록키 생성 알고리즘을 이용하여 차량시동 사용자 등록키를 생성할 수 있다(S114).

[0050] 다음으로, 차량시동인증장치는 통신단말로 차량시동 사용자 등록키를 암호화하여 전송하고 이때 통신단말은 수신데이터를 복호화하고 차량시동 사용자 등록키를 보안저장소(Secure Storage)에 저장할 수 있다(S115).

[0051] 차량 시동할 사용자를 차량시동장치에 등록 후 차량 내 통신단말에서 차량시동 인증키를 생성하고 배포하는 과정으로, 먼저 통신단말은 사용자인증서버로부터 수신한 사용자개인정보(PI)확인을 위한 화면을 표시하고(S116), 사용자는 수동으로 사용자 개인정보를 화면에 수동 입력할 수 있다(S117).

[0052] 통신단말은 사용자가 수동 입력한 사용자개인정보와 사용인증서버에서 수신한 사용자개인정보를 비교하여 동일한지 검증할 수 있다(S118). 검증되면 통신단말은 차량시동 인증키 생성알고리즘을 사용하여 차량시동 인증키를 생성하고(S119), 생성된 차량시동 인증키를 휴대단말에 통신채널을 통하지 않고 배포하기 위해서 QR(Quick Response Code) 코드로 변환하여 화면에 출력할 수 있다(S120).

[0053] 다음으로, 사용자는 휴대단말로 통신단말화면의 QR코드를 촬영하고(S121), 휴대단말에 내장된 QR코드 인식기를 통해서 차량시동 인증키를 추출하고 휴대단말에 저장하여(S122) 차량시동 인증키를 생성하고 배포할 수 있다. 여기서 QR 코드는 2차원 매트릭스형태의 패턴으로 정보를 저장하고 있는 이차원 바코드로 자동차 부품생산관리

등 상품관리에서부터 제품의 광고에 이르기 까지 다양하게 사용하는 기술이다. QR코드 생성기를 통해 정보를 이미지로 변환하고 스마트폰 카메라로 이미지를 활용하여 획득한 이미지를 QR코드인식기를 사용하여 변환전 정보를 추출할 수 있다.

[0054] 사용자의 휴대단말과 차량의 통신단말이 배포과정에서 공유하게 된 차량시동 인증키를 이용하여 OTP 정보를 생성하는 과정으로, 먼저 휴대단말은 차량시동요청정보를 암호화하여 사용자인증서버에 전송하고(S123), 사용자인증서버는 등록된 사용자의 사용자개인정보와 차량시동인증요청정보를 함께 암호화하여 차량내 통신단말에 전송할 수 있다(S124).

[0055] 다음으로, 통신단말은 OTP 생성알고리즘을 이용하여 OTP정보를 생성하고 OTP정보와 사용자개인정보 입력 화면을 표시할 수 있다(S125).

[0056] 다음으로, 사용자는 OTP 입력화면이 표시되면 휴대단말에서 OTP 생성 알고리즘을 이용하여 OTP 정보를 생성하고 OTP 정보를 휴대단말 화면에 표시하여(S126) 휴대단말과 통신단말은 OTP 정보를 생성하게 된다.

[0057] 차량시동 인증 요청을 처리하는 과정으로, 먼저 사용자는 휴대단말에서 생성한 OTP 정보와 사용자개인정보를 통신단말화면에 수동으로 입력하고(S127) 통신단말은 사용자가 입력된 정보들과 통신단말에서 생성한 OTP정보와 사용자인증서버로부터 수신한 사용자개인정보를 비교하여 일치하면 차량시동인증요청을 성공으로 판단할 수 있다(S128).

[0058] 다음으로, 통신단말은 성공한 차량시동 인증결과를 암호화하여 전송하여(S129) 차량시동 인증요청을 처리할 수 있다. 이후 차량시동 인증장치는 엔진제어 전장장치에 엔진구동을 명령하는 메시지를 보내고 엔진제어 장치는 크랭크샤프를 회전시켜 엔진을 구동할 수 있다.

[0059] **도 3은 도 1에 도시된 통신 단말의 상세한 구성을 나타내는 도면이다.**

[0060] 도 3을 참조하면, 본 발명의 일 실시예에 따른 통신 단말(130)은 프로세서(131), 로직 제어기(132), 메모리(133), 인터페이스(134)를 포함할 수 있다.

[0061] 프로세서(131)는 통신 단말 내 각종 장치와 연동하여 각 기능을 제어할 수 있다.

[0062] 로직 제어기(132)는 로직 처리부(132a), QR 코드 생성기(132b), OTP 생성기(132c), 암호 처리부(132d)로 이루어질 수 있다. 로직 처리부(142a)는 차량 내부와 외부와 통신을 위한 통신 단말 본연의 기능을 처리할 수 있다. 여기서 말하는 본연의 기능의 예로서, 차량 내 통신단말의 제조나 업그레이드시 암/복호화시 사용되는 비밀키(Private Key)를 삽입/삭제/변경처리기능, 차량시동인증장치의 차량시동 사용자 등록키 수신하고 저장하는 기능, 사용자인증서버로부터 사용자 개인정보를 수신하고 저장하는 기능을 최소화된 본연의 기능이라 할 수 있다. QR 코드 생성기(132b)는 차량시동 인증키 정보를 QR코드 이미지로 변환할 수 있다. OTP 생성기(132c)는 OTP 생성 알고리즘을 통해 OTP 정보를 생성할 수 있다. 암호 처리부(132d)는 블록 대칭키 방식의 암호화 알고리즘인 DES, 3DES, AES, ARIA, LEA, 스트림 대칭키 방식의 MASK, 비대칭키 방식의 암호화 알고리즘인 RSA, DSA, DSS, ECC 등의 암호화 알고리즘으로 암호화 및 복호화를 처리할 수 있다.

[0063] 메모리(133)는 사용자 인증서버로부터 제공한 사용자 개인정보(PI), 차량시동 인증키 생성 알고리즘으로 생성한 차량시동 인증키(Auth Key), 차량시동 인증장치로부터 수신한 차량시동 사용자 등록키(Enroll Key) 및 암/복호화 처리시 사용할 비밀키(Private Key)를 저장할 수 있다.

[0064] 인터페이스(134)는 차량내부 통신으로 한 개 이상의 다양한 차량 네트워크를 통해 차량 내 차량시동 인증장치와 연동하고 차량외부 통신으로 LTE, WCDMA, CDMA 등과 같은 이동통신망과 연동할 수 있다. 여기서 한 개 이상의 다양한 차량 네트워크의 범위는 LIN, CAN, MOsT, FlexRay, 이더넷, 모뎀뿐만 아니라 향후 적용될 통신(네트워크) 기술을 포함할 수 있다.

[0065] **도 4는 도 1에 도시된 차량시동 인증장치의 상세한 구성을 나타내는 도면이다.**

[0066] 도 4를 참조하면, 본 발명의 일 실시예에 따른 차량시동 인증장치(140)는 프로세서(141), 로직 제어기(142), 메모리(143), 인터페이스(144)를 포함할 수 있다.

[0067] 프로세서(141)는 차량시동 인증장치 내 각종 장치와 연동하여 각 기능을 제어할 수 있다.

[0068] 로직 제어기(142)는 로직 처리부(142a)와 암호 처리부(142b)로 이루어질 수 있다. 로직 처리부(142a)는 차량 내 통신을 위한 차량시동인증장치 본연의 기능을 처리할 수 있다. 여기서 말하는 본연의 기능의 예로서, 차량시동

인증장치의 제조나 업그레이드시 차대번호(VIN)과 암/복호화시 사용되는 비밀키(Private Key)를 삽입/삭제/변경 처리기능, 통신단말의 차량시동 사용자 등록키 생성 기능, 사용자 개인정보의 저장 기능을 최소화된 본연의 기능이라 할 수 있다. 암호 처리부(142b)는 블록 대칭키 방식의 암호화 알고리즘인 DES, 3DES, AES, ARIA, LEA, 스트림 대칭키 방식의 MASK, 비대칭키 방식의 암호화 알고리즘인 RSA, DSA, DSS, ECC 등의 암호화 알고리즘으로 암호화 및 복호화를 처리할 수 있다.

[0069] 메모리(143)는 차량고유번호인 차대번호(VIN), 사용자 인증서버로부터 제공한 사용자 개인정보(PI), 차량시동 사용자 등록키 생성 알고리즘으로 생성된 등록키(Enroll Key) 및 암/복호화 처리시 사용할 비밀키(Private Key)를 저장할 수 있다.

[0070] 인터페이스(144)는 한 개 이상의 다양한 차량 네트워크을 통해 차량 내 통신 단말이나 엔진 구동하는 엔진제어 전장장치 등과 연동할 수 있다. 여기서 한 개 이상의 다양한 차량 네트워크의 범위는 LIN, CAN, MOsT, FlexRay, 이더넷 뿐만 아니라 향후 적용될 통신(네트워크) 기술을 포함할 수 있다.

[0071] **도 5는 본 발명의 일 실시예에 따른 차량시동 사용자 등록키 생성 과정을 나타내는 도면이다.**

[0072] 도 5를 참조하면, 먼저 임의의 시각을 사용하여 랜덤값(RE)을 생성할 수 있다(S410). 여기서 임의의 시각은 랜덤값을 생성하기 시작한 현재시각(Tc)과 차대번호(VIN)를 입력한 입력시각(Tv)의 XOR 연산한 값을 말하고, 랜덤값은 임의의 시각을 일반적인 난수 발생기로 얻은 난수값을 의미할 수 있는데, 다음의 [수학식 1]과 같다.

[0073] [수학식 1]

[0074] $RE = F(Random(Tv \oplus Tc))$

[0075] 여기서, 차대번호(VIN)는 차량의 외관에 부착하거나 차량등록증에 명기되어 악의 의도자가 쉽게 얻을 수 있다. 차량제조사에서 차대번호를 만든 시각은 차량제조사만이 알 수 있기 때문에 보안이 강화된다.

[0076] 다음으로, 사용자 개인정보(PI), 차대번호(VIN), 랜덤값(RE) 및 기타 정보를 조합하여 해당 사용자의 차량사용등록정보(VUI)를 생성하는데(S420), 다음의 [수학식 2]와 같다.

[0077] [수학식 2]

[0078] $VUI = F(Append(PI, VIN, RE))$

[0079] 이때, 조합의 순서는 순차적 또는 램덤 방식 등으로 제조사의 설계정책에 따라 다양하게 고려될 수 있다. 기타 정보는 통신단말이나 자동차 제조사에서 부가적으로 추가될 수 있다.

[0080] 다음으로, 차량사용등록정보(VUI)를 소정의 해쉬(Hash) 알고리즘을 이용하여 해쉬 처리하여 차량시동 사용자 등록키(VEK)를 생성할 수 있다(S430). 여기서 해쉬는 임의의 길이의 데이터를 고정된 길이의 데이터로 매핑 또는 변환시키는 것을 말한다. 해쉬의 목적은 입력 메시지에 대한 변경할 수 없는 증거값을 뽑아냄으로서 메시지의 오류나 변조를 탐지할 수 있는 무결성을 제공하는 것이다. 특히 해쉬 함수는 전자 서명과 함께 사용되어 효율적인 서명 생성을 가능하게 하고 긴 메시지에 대해 서명을 하는 경우, 전체 메시지에 대해 직접 서명하는 것이 아니고 짧은 해쉬값을 계산해 이것에 대해 서명을 하게 된다. 따라서 해쉬를 통해 축약된 메시지는 축약으로 단방향성을 가지기 때문에 입력값을 유추하기가 어렵다.

[0081] 해쉬 알고리즘으로는 MD5, SHA-1, SHA-256, SHA-512 등 다양하게 사용될 수 있지만, 본 발명에서는 해쉬 알고리즘의 선정에 제한을 두지 않고 있으며 본 발명을 가지고 양산하는 제조사나 이용자의 정책이나 여건 등에 따라 선정할 수 있다.

[0082] **도 6은 본 발명의 일 실시예에 따른 차량 시동 인증키 생성 과정을 나타내는 도면이다.**

[0083] 도 6을 참조하면, 먼저 소정의 시각을 사용하여 랜덤값(RA)를 생성할 수 있다(S610). 여기서 임의의 시각은 랜덤값을 생성시작한 현재시각(Tc)과 차량 내 통신단말에 비밀키(Private Key)를 입력한 입력시각(Tp)의 XOR한 값을 말하고, 랜덤값은 임의의 시각값을 일반적인 난수 발생기로 얻은 난수값을 의미하는데, 다음의 [수학식 3]과 같다.

[0084] [수학식 3]

[0085] $RE = F(Random(Tp \oplus Tc))$

[0086] 여기서, 차량내 통신단말에 비밀키(Private Key)는 차량제조사만이 알 수 있기에 보안이 강화된다.

[0087] 다음으로, 사용자 개인정보(PI), 차량시동 사용자 등록키(VEK), 랜덤값(RA) 및 기타 정보를 조합하여 해당 사용자의 차량시동인증정보(VAI)를 생성하는데(S620), 다음의 [수학식 4]와 같다.

[0088] [수학식 4]

[0089] VAI = F(Append(PI, VEK, RA))

[0090] 이때, 조합의 순서는 순차적 또는 램덤 방식 등으로 제조사의 설계정책에 따라 다양하게 고려될 수 있다. 기타 정보는 통신단말이나 자동차 제조사에서 부가적으로 추가될 수 있다.

[0091] 다음으로, 생성된 차량시동인증정보(VAI)를 소정의 해쉬(Hash) 알고리즘을 이용하여 해쉬 처리하여 그 해쉬 처리한 결과로 차량시동 인증키(VAK)를 생성할 수 있다(S630).

[0092] **도 7은 본 발명의 일 실시예에 따른 OTP 정보 생성 과정을 나타내는 도면이다.**

[0093] 도 7을 참조하면, 먼저 현재 시각을 유효시간 범위 내 예컨대, 1분으로 축약하여 유효시각(Te, Effective Time)을 구할 수 있다(S710). 여기서 유효 시간 범위라는 것은 휴대단말과 차량 내 통신단말 간 OTP 생성 시각이 상이함을 보상하기 위한 시간이다. 즉 이 유효시간 범위 내에서는 동일한 OTP정보가 생성되어야 한다.

[0094] 다음으로, 차량시동 인증키(VAK), 유효시각 및 기타 정보를 조합하여 그 조합한 결과로 해당 사용자의 OTP 정보(OCI)를 생성할 수 있는데(S720), 다음의 [수학식 5]와 같다.

[0095] [수학식 5]

[0096] OCI = F(Append(VAK, Te))

[0097] 이때, 조합의 순서는 순차적 또는 램덤 방식 등으로 제조사의 설계정책에 따라 다양하게 고려될 수 있다. 기타 정보는 통신단말이나 자동차 제조사에서 부가적으로 추가될 수 있다.

[0098] 한편, 이상에서 설명한 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합하거나 결합하여 동작하는 것으로 기재되어 있다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성 요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 또한, 이와 같은 컴퓨터 프로그램은 USB 메모리, CD 디스크, 플래쉬 메모리 등과 같은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체, 캐리어 웨이브 매체 등이 포함될 수 있다.

[0099] 이상에서 설명한 실시예들은 그 일 예로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0101] 110: 휴대 단말

120: 사용자 인증서버

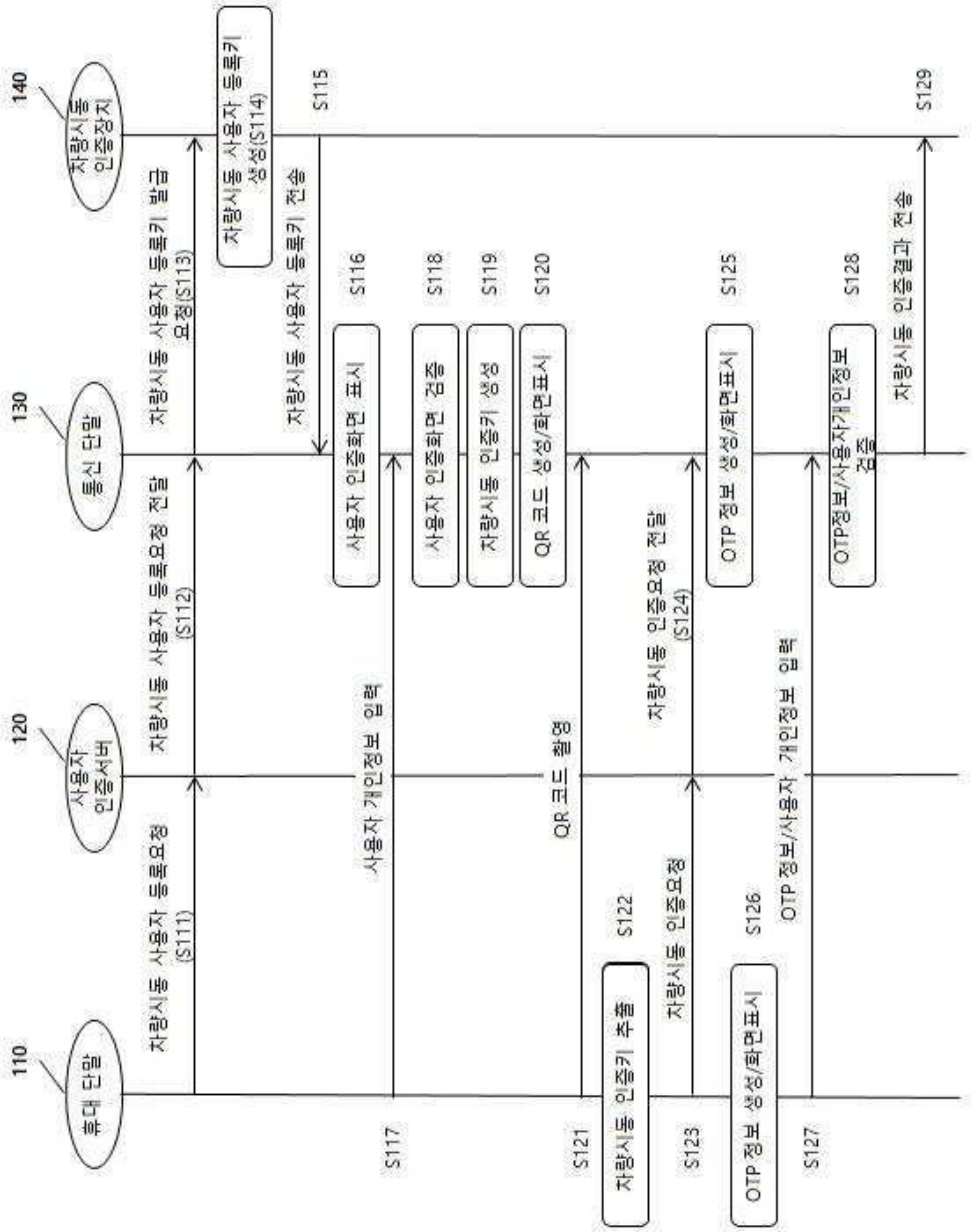
130: 통신 단말

140: 차량시동 인증 장치

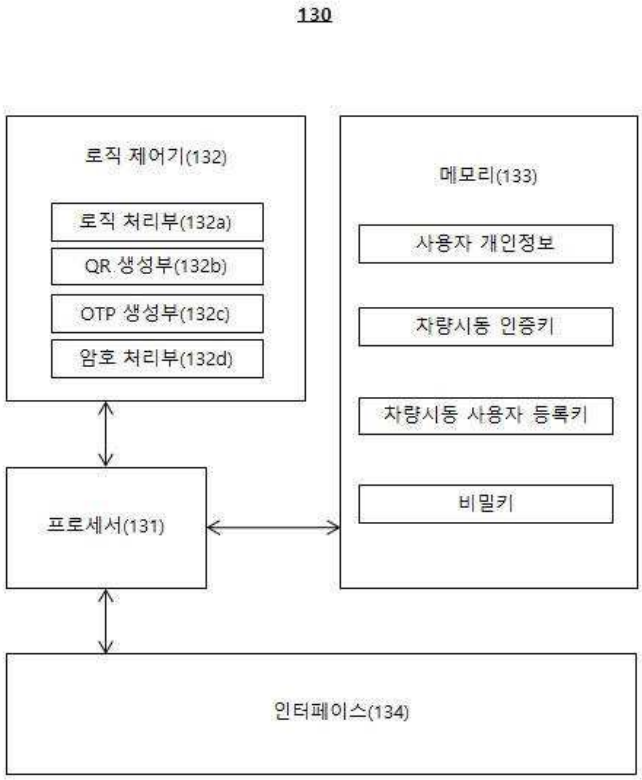
도면

도면1

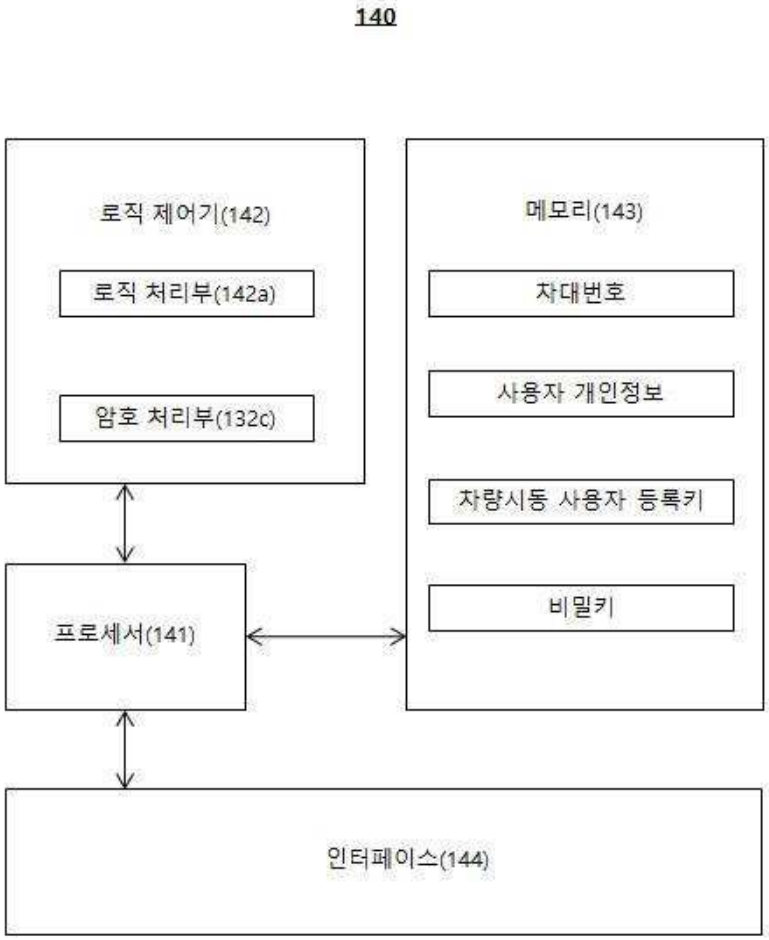
도면2


110
휴대 단말
120
사용자 인증서버
130
통신 단말
140
차량시동 인증장치
차량시동 사용자 등록요청 (S111)
차량시동 사용자 등록요청 전달 (S112)
차량시동 사용자 등록키 발급 요청(S113)
차량시동 사용자 등록키 생성(S114)
S115
차량시동 사용자 등록키 전송
S116
사용자 인증화면 표시
사용자 개인정보 입력
S117
S118
사용자 인증화면 검증
S119
차량시동 인증키 생성
S120
QR 코드 생성/화면표시
QR 코드 촬영
S121
차량시동 인증키 추출
S122
차량시동 인증요청
S123
차량시동 인증요청 전달 (S124)
S125
OTP 정보 생성/화면표시
S126
OTP 정보/사용자 개인정보 입력
S127
S128
OTP정보/사용자개인정보 검증
차량시동 인증결과 전송
S129

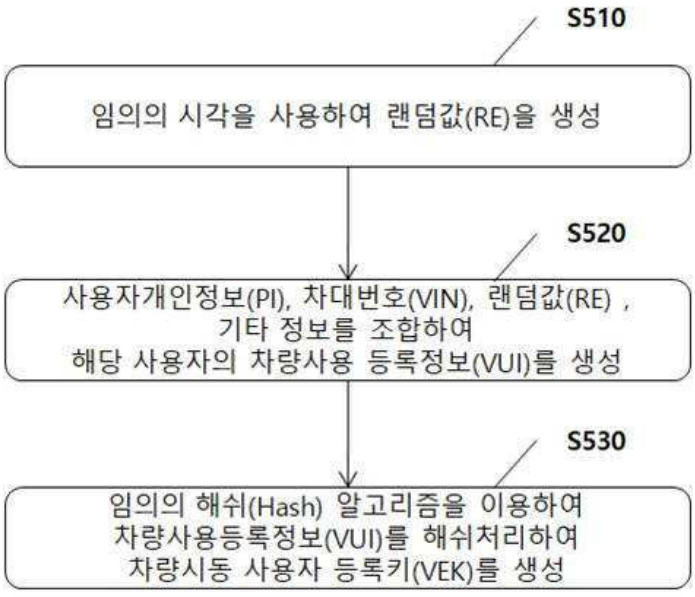
도면3


130
로직 제어기(132)
로직 처리부(132a)
QR 생성부(132b)
OTP 생성부(132c)
암호 처리부(132d)
메모리(133)
사용자 개인정보
차량시동 인증키
차량시동 사용자 등록키
비밀키
프로세서(131)
인터페이스(134)

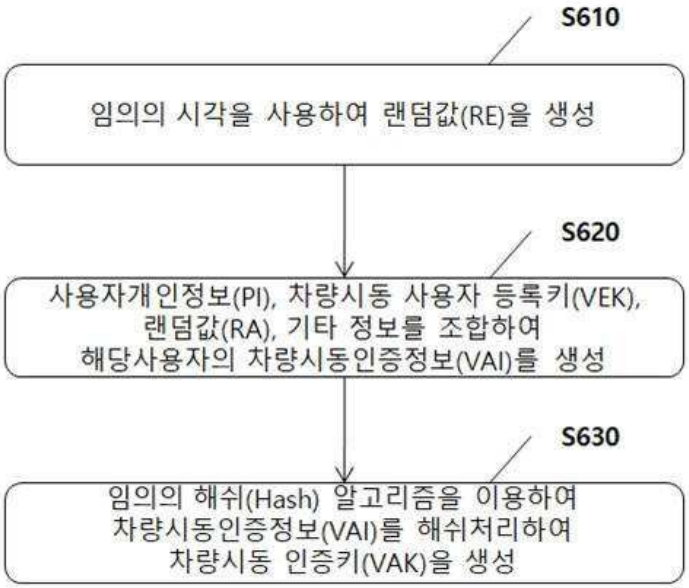
도면4


140
로직 제어기(142)
로직 처리부(142a)
암호 처리부(132c)
메모리(143)
차대번호
사용자 개인정보
차량시동 사용자 등록키
비밀키
프로세서(141)
인터페이스(144)

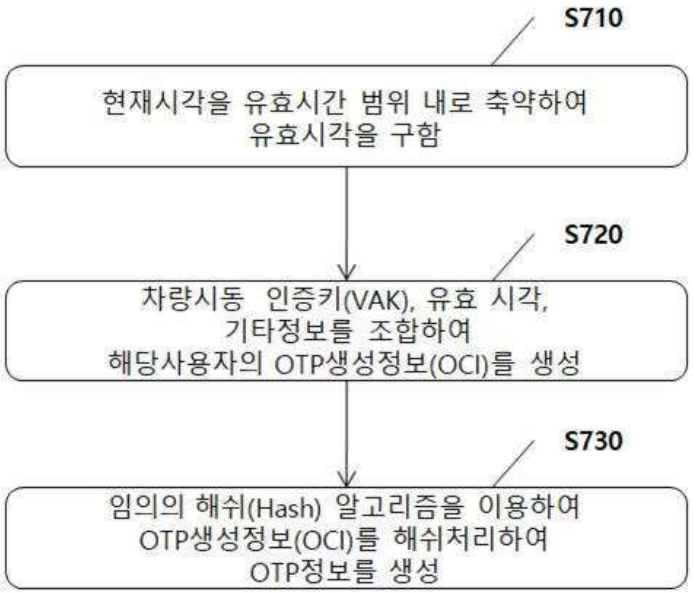
도면5


S510
임의의 시각을 사용하여 랜덤값(RE)을 생성
S520
사용자개인정보(PI), 차대번호(VIN), 랜덤값(RE) ,
기타 정보를 조합하여
해당 사용자의 차량사용 등록정보(VUI)를 생성
S530
임의의 해쉬(Hash) 알고리즘을 이용하여
차량사용등록정보(VUI)를 해쉬처리하여
차량시동 사용자 등록키(VEK)를 생성

도면6



도면7



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제7항

【변경전】

상기 제1 OTP 정보

【변경후】

상기 제2 OTP 정보