(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년01월16일
(11) 등록번호 10-1938856
(24) 등록일자 2019년01월09일

(51) 국제특허분류(Int. Cl.)
B60R 25/24 (2013.01) *B60R 25/30* (2013.01)
H01Q 1/32 (2015.01)
(52) CPC특허분류
B60R 25/245 (2013.01)
B60R 25/30 (2013.01)
(21) 출원번호 10-2017-0098873
(22) 출원일자 2017년08월04일
심사청구일자 2017년08월04일
(56) 선행기술조사문헌
JP09144404 A*
KR1020100101849 A*
JP2007224663 A
JP11503388 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
주경호
서울특별시 성북구 개운사2길 34, 302호 (안암동5가)
최원석
서울특별시 강북구 삼양로 256 105동 501호 (미아동,삼성래미안미아1차아파트)
(74) 대리인
김등용, 김홍석

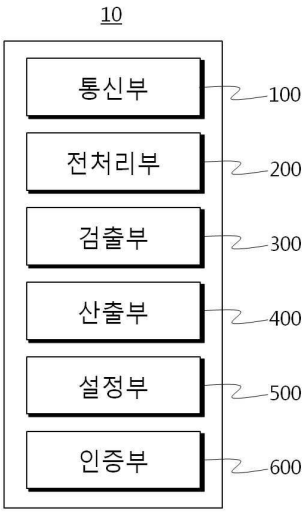
전체 청구항 수 : 총 5 항 심사관 : 이대길

(54) 발명의 명칭 **차량용 KES에서 사용되는 정당한 스마트키 인증 장치 및 그 방법**

(57) 요 약

정당한 스마트키 인증 장치가 개시된다. 상기 정당한 스마트키 인증장치는 차량용 KES(Keyless Entry System)에서 사용되는 정당한 스마트키 인증 장치로서, 상기 정당한 스마트키 또는 인증이 필요한 스마트키와 신호를 주고받는 통신부, 상기 정당한 스마트키 또는 상기 인증이 필요한 스마트키로부터 수신한 RF(Radio Frequency)신호를 전처리하는 전처리부, 전처리된 RF신호로부터 특징(feature)을 검출하는 검출부, 상기 검출부에서 검출된 특징을 SVM(Support Vector Machine)을 이용하여 단일 클래스(one-class)로 학습시키고, 학습을 통해 생성된 분류기(classifier)를 이용하여 수신한 RF신호의 스코어(score)를 산출하는 산출부, 및 상기 산출부를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 설정부를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H01Q 1/3241 (2013.01)

명 세 서

청구범위

청구항 1

차량용 KES(Keyless Entry System)에서 사용되는 정당한 스마트키 인증 장치로서,

상기 정당한 스마트키 또는 인증이 필요한 스마트키와 RF(Radio Frequency)신호를 주고 받는 통신부;

상기 정당한 스마트키 또는 상기 인증이 필요한 스마트키로부터 수신한 RF신호를 전처리하는 전처리부;

전처리된 RF신호로부터 특징(feature)을 검출하는 검출부;

상기 검출부에서 검출된 특징을 SVM(Support Vector Machine)을 이용하여 단일 클래스(one-class)로 학습시키고, 학습을 통해 생성된 분류기(classifier)를 이용하여 수신한 RF신호의 스코어(score)를 산출하는 산출부; 및

상기 산출부를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 설정부를 포함하고,

상기 전처리부는 상기 정당한 스마트키 또는 상기 인증이 필요한 스마트키로부터 수신한 RF신호의 노이즈를 제거하고, 노이즈가 제거된 RF신호에서 반송파 주파수를 제거하여 제1 신호를 추출하고, 상기 제1 신호를 디지털 신호로 변환하여 변환된 제1 신호의 프리앰블 신호인 제2 신호를 추출하는,

정당한 스마트키 인증 장치.

청구항 2

제1항에 있어서,

상기 인증이 필요한 스마트키의 스코어가 기 설정된 임계값 이상이면 정당한 스마트 키로 판단하는 인증부를 포함하는 정당한 스마트키 인증 장치.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 정당한 스마트키 또는 상기 인증이 필요한 스마트키로부터 수신한 RF신호는 FSK(Frequency Shift Keying) 변조된 신호이고,

상기 특징은 상기 제1 신호를 푸리에 변환한 신호에서 비트 1과 비트 0을 표현하는 각각의 주파수 및 상기 제2 신호를 푸리에 변환한 신호에서 첫 번째 피크 주파수인 것을 특징으로 하는 정당한 스마트키 인증 장치.

청구항 5

차량용 KES(Keyless Entry System)에서 사용되고, 통신부, 전처리부, 검출부, 산출부, 설정부 및 인증부를 포함하는 정당한 스마트키 장치에 의해 수행되는 정당한 스마트키 인증 방법으로서,

상기 통신부가 상기 정당한 스마트키로부터 RF(Radio Frequency)신호를 수신하는 단계;

상기 전처리부에 의해 상기 정당한 스마트키로부터 수신한 RF신호를 전처리하는 제1 전처리 단계;

상기 검출부가 전처리된 RF신호로부터 특징(feature)을 검출하는 단계;

상기 산출부가 상기 검출부에서 검출된 특징을 SVM(Support Vector Machine)을 이용하여 단일 클래스(one-class)로 학습시키고, 학습을 통해 생성된 분류기(classifier)를 이용하여 수신한 RF신호의 스코어(score)를 산출하는 단계; 및

상기 정당한 스마트키 인증 장치의 설정부가 상기 산출부를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 단계를 포함하고,

상기 제1 전처리 단계는 상기 정당한 스마트키로부터 수신한 RF신호의 노이즈를 제거하고, 노이즈가 제거된 RF신호에서 반송파 주파수를 제거하여 제1 신호를 추출하고, 상기 제1 신호를 디지털 신호로 변환하여 변환된 제1 신호의 프리앰블 신호인 제2 신호를 추출하고,

상기 정당한 스마트키로부터 수신한 RF신호는 FSK(Frequency Shift Keying) 변조된 신호이고,

상기 특징은 상기 제1 신호를 푸리에 변환한 신호에서 비트 1과 비트 0을 표현하는 각각의 주파수 및 상기 제2 신호를 푸리에 변환한 신호에서 첫 번째 피크 주파수인,

정당한 스마트키 인증 방법.

청구항 6

제5항에 있어서,

상기 통신부가 인증이 필요한 스마트키로부터 RF신호를 수신하는 단계;

상기 전처리부에 의해 상기 인증이 필요한 스마트키로부터 수신한 RF신호를 전처리하는 제2 전처리 단계;

상기 검출부가 전처리된 RF신호로부터 특징을 검출하는 단계;

상기 산출부가 상기 검출부에서 검출된 특징을 분류기를 이용하여 분류하고, 상기 분류기를 이용하여 수신한 RF신호의 스코어를 산출하는 단계; 및

상기 인증부에 의하여 상기 인증이 필요한 스마트키의 스코어가 기 설정된 임계값 이상이면 정당한 스마트 키로 판단하는 단계를 더 포함하는 정당한 스마트키 인증 방법.

청구항 7

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 차량용 KES(Keyless Entry System)에서 사용되는 스마트키의 인증 장치 및 방법에 관한 것으로, 보다 구체적으로 사전에 등록된 정당한 스마트키인지 여부를 인증하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] KES는 운전자의 편의증대를 위해 차량에 탑재되는 사용자 인증시스템이다. KES는 RKES(Remote Keyless Entry System)와 PKES(Passive Keyless Entry System)으로 분류된다. RKES는 실제 열쇠를 열쇠 구멍에 넣지 않고 스마트키의 버튼을 누르기만 하면 자동차의 잠금을 해제할 수 있으며, PKES는 스마트키를 소지한 운전자가 차량에 접근하기만 하면 자동차의 잠금을 해제할 수 있다.

[0003] 이러한 편의성에도 불구하고 KES에 대한 취약점이 발견되었고, 이를 이용한 다양한 사이버 공격이 가능함이 입증되었다. 그럼에도 여전히 차량 제조사들은 추가적인 보안대책 없이 차량을 생산하고 있다.

[0004] 본 발명은 이와 같은 문제점을 해결하기 위해 Device Fingerprinting 기법을 이용하여 정당한 스마트키를 사전에 등록시켜 놓음으로써 릴레이 공격(Relay Attack), 부채널 공격(Side Channel Attack) 및 재밍 공격(Jamming Attack) 등의 공격으로 인한 보안상의 문제점을 해결하고자 한다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 공개특허 제10-2016-0149500호

(특허문헌 0002) 대한민국 등록특허 제10-1562124호

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 릴레이 공격, 부채널 공격 및 재밍 공격 등의 공격으로부터 차량용 KES를 보호함으로써 차량 도난사고를 예방하고 운전자에게 편의를 제공할 뿐만 아니라, 무선통신환경에도 뛰어난 정당한 스마트키 인증 장치 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명에 따른 차량용 KES에서 사용되는 정당한 스마트키 인증 장치는 상기 정당한 스마트키 또는 인증이 필요한 스마트키와 신호를 주고 받는 통신부, 상기 정당한 스마트키 또는 상기 인증이 필요한 스마트키로부터 수신한 RF(Radio Frequency)신호를 전처리하는 전처리부, 전처리된 RF신호로부터 특징(feature)을 검출하는 검출부, 상기 검출부에서 검출된 특징을 SVM(Support Vector Machine)을 이용하여 단일 클래스(one-class)로 학습시키고, 학습을 통해 생성된 분류기(classifier)를 이용하여 수신한 RF신호의 스코어(score)를 산출하는 산출부, 및 상기 산출부를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 설정부를 포함할 수 있다.

[0008] 본 발명에 따른 차량용 KES에서 사용되는 정당한 스마트키 인증 방법은 정당한 스마트키 인증 장치의 통신부가 상기 정당한 스마트키로부터 RF신호를 수신하는 단계, 정당한 스마트키 인증 장치의 전처리부가 상기 정당한 스마트키로부터 수신한 RF신호를 전처리하는 단계, 정당한 스마트키 인증 장치의 검출부가 전처리된 RF신호로부터 특징을 검출하는 단계, 정당한 스마트키 인증 장치의 산출부가 상기 검출부에서 검출된 특징을 SVM을 이용하여 단일 클래스로 학습시키고, 학습을 통해 생성된 분류기를 이용하여 수신한 RF신호의 스코어를 산출하는 단계, 및 정당한 스마트키 인증 장치의 설정부가 상기 산출부를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 단계를 포함할 수 있다.

발명의 효과

[0009] 본 발명의 일 실시 예에 따르면, 릴레이 공격, 부채널 공격 및 재밍 공격 등의 공격으로부터 차량용 KES를 효과적으로 보호할 수 있다.

[0010] 또한, 무선통신 환경에도 뛰어난 정당한 스마트키 인증 장치 및 방법을 제공할 수 있다.

도면의 간단한 설명

[0011] 도 1은 정당한 스마트키 인증 장치의 예시적인 기능 블록도이다.

도 2a는 도 1에 도시된 검출부에 의해 추출된 제1 신호의 특징을 도시한 것이다.

도 2b는 도 1에 도시된 검출부에 의해 추출된 제2 신호의 특징을 도시한 것이다.

도 3은 본 발명의 일 실시 예에 따른 정당한 스마트키 학습 방법의 순서도를 나타낸 것이다.

도 4는 본 발명의 일 실시 예에 따른 정당한 스마트키 인증 방법의 순서도를 나타낸 것이다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0013] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실

시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시 예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.

[0014] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시 예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0015] 우선, 본 발명에 대한 설명에 앞서, 본 발명의 배경이 되는 기술에 대해 설명하면 다음과 같다.

[0016] 본 발명은 차량용 KES에 대하여 RF 핑거프린팅(Fingerprinting) 기법을 적용한다. 핑거프린팅 기법은 특정 무선 디바이스로부터 수신된 정보(예를 들면, 무선모뎀 등 물리적 하드웨어 계층 정보, 비콘 헤더 등 MAC 소프트웨어 계층 정보 등)의 분석을 통하여 특정 디바이스를 고유하게 식별하고 유일하게 분류할 수 있는 특징적 지분, 즉 핑거프린트를 추출하는 것으로서 이러한 특징을 추출하는 방식에 따라 다양한 기법들이 존재한다.

[0017] 핑거프린팅 기법은 크게 핑거프린트 생성과 분류단계로 나누어지는데, 생성 단계는 디바이스가 송신하는 무선신호를 수집하고 신호 처리하여 디바이스를 유일하게 구별할 수 있는 특징들을 추출하는 단계이고, 분류단계는 생성단계에서 추출한 특징값들을 통계적 방식으로 분류하고, 추출하여 보관하고 있는 디바이스의 핑거프린트와 매치하는지를 판단함으로써 클론 디바이스인지 여부를 판단하게 된다.

[0018] FSK(Frequency Shift Keying) 변조는 일정 진폭의 정현파의 주파수를 두 가지로 정하여 데이터가 1 혹은 0으로 변함에 따라 두 개의 주파수 중 할당된 주파수를 상대측에 보내는 변조 방식이다. ASK(Amplitude Shift Keying) 변조방식 보다 에러에 강하고, 회로도 비교적 간단하기 때문에 데이터 전송에서 많이 사용된다. 또한, FSK 변조는 비교적 저속(비동기식으로 200[BPS]이하)의 데이터 전송에 많이 이용된다.

[0019] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0020] 도 1은 정당한 스마트키 인증 장치의 예시적인 기능 블록도이다.

[0021] 정당한 스마트키 인증 장치(10)는 통신부(100), 전처리부(200), 검출부(300), 산출부(400), 설정부(500) 및 인증부(600)를 포함한다.

[0022] 통신부(100)는 정당한 스마트키 또는 인증이 필요한 스마트키와 무선 RF신호를 주고받을 수 있다. 이를 위해 통신부(100)는 소정 위치에 장착된 RF안테나를 포함할 수 있다. 이 때, 정당한 스마트키 또는 인증이 필요한 스마트키로부터 수신한 RF신호는 ASK 변조되거나 FSK 변조된 신호일 수 있다.

[0023] 전처리부(200)는 정당한 스마트키 또는 인증이 필요한 스마트키로부터 수신한 RF신호를 전처리할 수 있다. 우선, 전처리부(200)는 수신한 RF신호를 필터링하여 노이즈를 제거할 수 있다. 다음으로 노이즈가 제거된 RF신호에서 제1 신호 및 제2 신호를 추출할 수 있다.

[0024] 제1 신호는 노이즈가 제거된 RF신호에서 반송파 주파수를 제거하여 추출한 기저대역(baseband)의 신호일 수 있다. 제2 신호는 제1 신호를 디지털 신호로 변환하여 변환된 제1 신호에서 추출된 프리앰블 영역의 신호일 수 있다. 프리앰블 신호는 무선 통신에서 패킷 또는 비트의 동기화를 위해 사용되는 신호이다.

[0025] 검출부(300)는 수신한 RF신호의 특징을 검출할 수 있다. 보다 구체적으로, KES를 위해 생산되는 스마트키는 표준화된 공정에도 불구하고 스마트키마다 기기의 하드웨어적인 특성이 다르며, 이러한 하드웨어적인 특성은 복제가 불가능하다. 따라서, 이러한 하드웨어적인 특성에 기반하여 스마트키의 특징을 검출한다.

[0026] 검출부(300)는 전처리부(200)에서 추출된 제1 신호 및 제2 신호로부터 각각의 특징을 검출할 수 있다. 검출부(300)에서 검출된 특징은 곧 차량용 스마트키의 핑거프린트를 의미하는데 이를 통하여 정당한 스마트키를 식별할 수 있다.

[0027] FSK 변조는 변조하고자 하는 신호를 중심 주파수로부터 특정 주파수만큼 이동시킴으로써 디지털 신호의 각 비트를 나타내는데, 제1 신호로부터 검출되는 특징은 제1 신호를 푸리에변환(Fourier Transformation)한 주파수 영역의 신호에서 비트 1과 비트 0을 표현하는 주파수일 수 있다.

[0028] 도 2a를 참조하면 중심 주파수(f_c)보다 특정 주파수(f_d)만큼 높은 주파수는 비트 1(또는 비트 0)을 나타내는 주

파수이며, 중심 주파수(f_c)보다 특정 주파수(f_d)만큼 낮은 주파수는 비트 0(또는 비트1)을 나타내는 주파수이다.

스마트키로부터 생성된 신호에서 비트 1과 비트 0을 나타내는 주파수는 스마트키별로 다른데, 이러한 차이점은 정당한 스마트키를 식별할 수 있는 특징으로 사용될 수 있다.

[0029] 제2 신호로부터 검출되는 특징은 제2 신호를 푸리에 변환한 주파수 영역의 신호에서 첫 번째 피크(peak) 주파수일 수 있다. 주파수 영역으로 표현된 프리앰블 신호는 몇 개의 지배적인 피크로 구성되는데, 스마트키별로 각각 다른 주파수에서 지배적인 피크를 나타내므로 첫 번째 피크의 주파수는 정당한 스마트키를 식별할 수 있는 특징으로 사용될 수 있다.

[0030] 도 2b를 참조하면 본 발명의 일 실시 예에 따라 푸리에 변환된 제2 신호는 각각 0 내지 50[Hz], 50 내지 100[Hz] 및 100 내지 150[Hz] 주파수 대역에서 지배적인 피크를 나타내는데, 이 중 0 내지 50[Hz]에 있는 첫 번째 피크 주파수를 특징으로 할 수 있다.

[0031] 산출부(400)는 검출부(300)에서 검출된 특징을 SVM을 이용하여 분류하고 그로부터 RF신호의 스코어를 산출한다. SVM이란 분류기 학습 알고리즘의 하나로서 주어진 데이터를 분류기를 이용하여 이진 클래스로 분류하는 알고리즘이다. SVM의 목적은 분류 오차를 줄이면서 동시에 두 클래스 간의 여백(margin)을 최대로 하는 초평면(hyperplane)을 학습하는 것이다. 만일 주어진 데이터를 단일 클래스로 분류하고자 하는 경우 단일 클래스에 속하는 모든 데이터를 둘러싸는 초구체(hyper-sphere)를 학습하거나, 원점으로부터 단일 클래스 간의 여백을 최대로 하는 초평면을 학습할 수 있다.

[0032] 검출부(300)에서 검출된 특징은 SVM을 이용하여 단일 클래스로 학습시킬 수 있다. 다음으로, 학습을 토대로 생성된 분류기를 이용하여 수신한 RF신호의 스코어를 산출한다. 산출된 스코어를 통해 SVM의 입력벡터가 분류된 단일 클래스에 속하는지 여부를 판단할 수 있다.

[0033] 설정부(500)는 산출부(400)를 통하여 산출된 정당한 스마트키의 스코어를 임계값으로 설정할 수 있다. 따라서, 추후에 인증부(600)를 통하여 기 설정된 임계값과 인증이 필요한 스마트키의 스코어를 비교하여 인증을 수행하도록 할 수 있다.

[0034] 인증부(600)는 인증이 필요한 스마트키의 스코어와 설정부(500)에서 설정된 임계값을 비교하여 인증이 필요한 스마트키의 스코어가 설정부(500)에서 설정된 임계값 이상이면 정당한 스마트키로 판단하여 인증을 수행할 수 있다. 인증이 필요한 스마트키의 인증이 완료된 경우 차량 제어부(미도시)를 통하여 차량의 시동을 걸거나 도어나 트렁크의 폐쇄 또는 개방 등을 제어할 수 있다.

[0035] 이하에서는 정당한 스마트키 인증 장치(10)가 정당한 스마트키를 학습하는 방법과 인증이 필요한 스마트키를 인증하는 방법에 대하여 설명한다. 상기 정당한 스마트키를 학습하는 방법과 인증이 필요한 스마트키를 인증하는 방법을 설명함에 있어서 앞서 기재된 내용과 중복되는 기재는 생략한다.

[0037] 도 3은 본 발명의 일 실시 예에 따른 정당한 스마트키 학습 방법의 순서도를 나타낸 것이다.

[0038] S100 단계에서는 정당한 스마트키 인증 장치(10)의 통신부(100)가 상기 정당한 스마트키로부터 RF신호를 수신한다. S200 단계에서는 정당한 스마트키 인증 장치(10)의 전처리부(200)가 상기 정당한 스마트키로부터 수신한 RF신호를 전처리한다. S300 단계에서는 정당한 스마트키 인증 장치(10)의 검출부(300)가 전처리된 RF신호로부터 특징을 검출한다. S400 단계에서는 정당한 스마트키 인증 장치(10)의 산출부(400)가 검출부(300)에서 검출된 특징을 SVM을 이용하여 단일 클래스로 학습시키고, 학습을 통해 생성된 분류기를 이용하여 수신한 RF신호의 스코어를 산출한다. S500 단계에서는 정당한 스마트키 인증 장치(10)의 설정부(500)가 상기 산출부(400)를 통하여 산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정한다.

[0039] 정당한 스마트키 인증 장치(10)는 위와 같은 학습 방법을 통하여 정당한 스마트키를 사전에 학습할 수 있다.

[0041] 도 4는 본 발명의 일 실시 예에 따른 정당한 스마트키 인증 방법의 순서도를 나타낸 것이다.

[0042] S110 단계에서는 정당한 스마트키 인증 장치(10)의 통신부(100)가 인증이 필요한 스마트키로부터 RF신호를 수신한다. S210 단계에서는 정당한 스마트키 인증 장치(10)의 전처리부(200)가 상기 인증이 필요한 스마트키로부터 수신한 RF신호를 전처리한다. S310 단계에서는 정당한 스마트키 인증 장치(10)의 검출부(300)가 전처리된 RF신호로부터 특징을 검출한다. S410 단계에서는 정당한 스마트키 인증 장치(10)의 산출부(400)가 검출부(300)에서 검출된 특징을 상기 분류기를 이용하여 분류하고, 상기 분류기를 이용하여 수신한 RF신호의 스코어를 산출한다. S510 단계에서는 정당한 스마트키 인증 장치(10)의 인증부(600)에 의하여 상기 인증이 필요한 스마트키의 스코

어가 기 설정된 임계값 이상이면 정당한 스마트 키로 판단하여 인증을 완료한다.

[0044] 본 발명의 일 실시 예에 따른 스마트키 인증 장치 및 그 방법은 RKES 뿐만 아니라 PKES 환경에서도 적용될 수 있다. PKES에 적용되는 경우 스마트키가 일반적으로 인식될 수 있는 세 가지 환경(손, 주머니, 가방)을 고려할 수 있다. 본 발명의 일 실시 예에 따른 스마트키 인증 장치 및 그 방법의 성능은 FAR(False Acceptance Rate) 및 FRR(False Rejection Ratio)를 통해 평가할 수 있다.

[0045] 아래의 표 1은 본 발명의 일 실시 예에 따른 스마트키 인증 장치 및 방법을 통하여 각각 RKES 및 PKES 환경에서 정당한 스마트키를 식별할 수 있는지에 대하여 실험한 결과를 나타낸 것이다.

표 1

[0047]

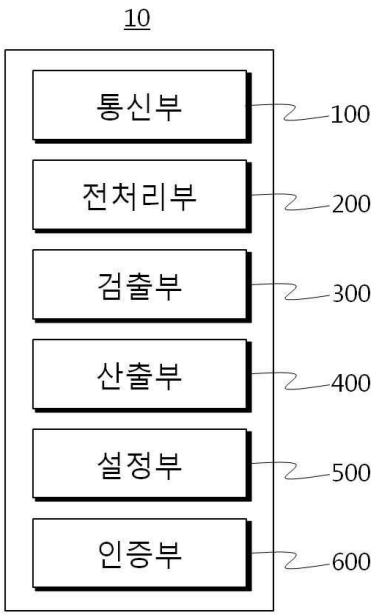
RKES 실험			PKES 실험			
Key Type	FAR	FRR	Key Type	통신환경	FAR	FRR
#1	-	2.2	#1	손	-	0
#2	0	-		주머니	-	2.6
#3	0	-		가방	-	1.1
#4	0	-	#2	손	0	-
#5	0	-		주머니	0	-
#6	0	-		가방	0	-
#7	0	-	#3	손	0	-
#8	0	-		주머니	3.6	-
#9	0	-		가방	3.1	-

[0049] RKES 및 PKES에서 #1의 스마트키를 정당한 스마트키로서 학습시켰다. 실험 결과, RKES 및 PKES 각각에서 정당한 스마트키에 대한 FRR 및 인증이 필요한 스마트키에 대한 FAR이 모두 매우 낮게 측정된 것을 확인할 수 있다. 따라서, 본 발명의 정당한 스마트키 인증 장치(10) 및 방법은 KES에서 정당한 스마트키인지 여부를 효과적으로 식별할 수 있을 뿐만 아니라, 무선통신 환경에도 뛰어남을 확인할 수 있다.

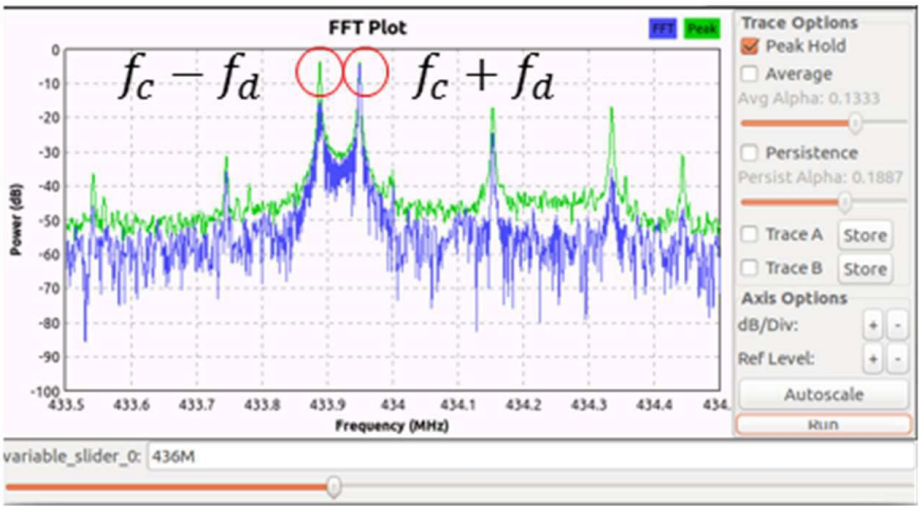
[0050] 본 발명의 기술적 사상 내에서 당해 분야의 통상의 지식을 가진 자에 의해 그 변형이나 개량이 가능함은 명백하다고 할 것이다. 본 발명의 단순한 변형 내지 변경은 모두 본 발명의 영역에 속하는 것으로 본 발명의 구체적인 보호범위는 첨부된 특허청구범위에 의하여 명확해질 것이다.

도면

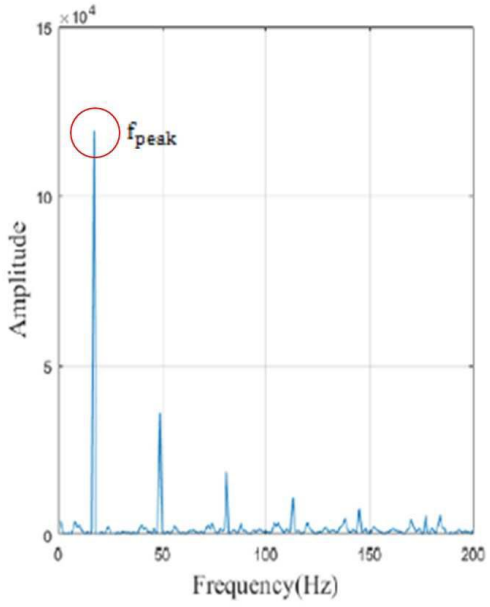
도면1



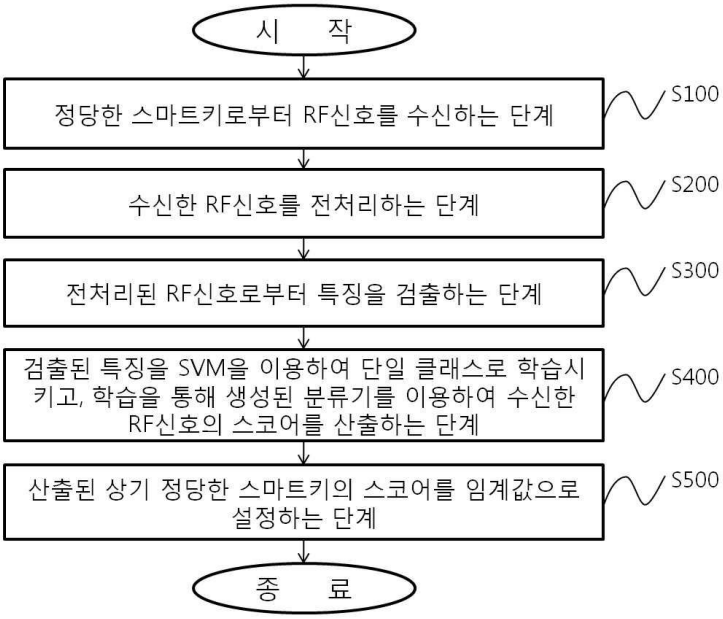
도면2a


FFT Plot
FFT
Peak
$f_c - f_d$
$f_c + f_d$
Power (dB)
Frequency (MHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.1333
Persistence
Persist Alpha: 0.1887
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Run
variable_slider_0:
436M

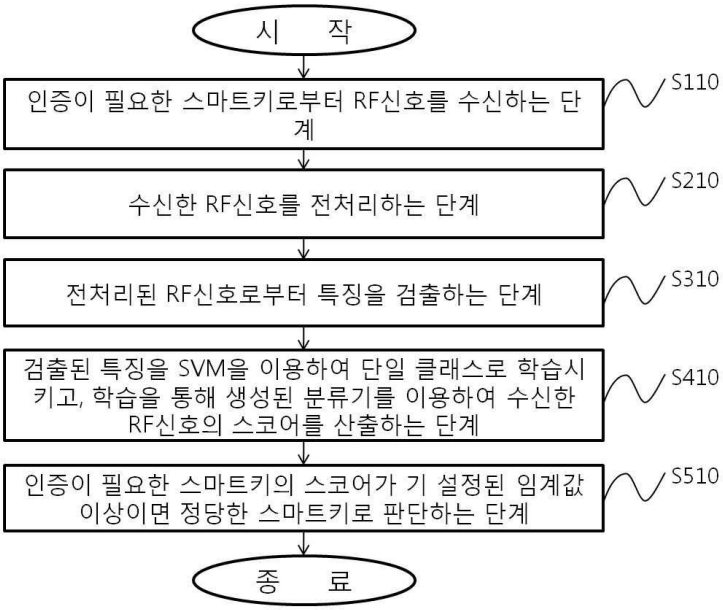
도면2b


$\times 10^4$
f_{peak}
Amplitude
Frequency(Hz)

도면3


시 작
정당한 스마트키로부터 RF신호를 수신하는 단계
S100
수신한 RF신호를 전처리하는 단계
S200
전처리된 RF신호로부터 특징을 검출하는 단계
S300
검출된 특징을 SVM을 이용하여 단일 클래스로 학습시키고, 학습을 통해 생성된 분류기를 이용하여 수신한 RF신호의 스코어를 산출하는 단계
S400
산출된 상기 정당한 스마트키의 스코어를 임계값으로 설정하는 단계
S500
종 료

도면4


시 작
인증이 필요한 스마트키로부터 RF신호를 수신하는 단계
S110
수신한 RF신호를 전처리하는 단계
S210
전처리된 RF신호로부터 특징을 검출하는 단계
S310
검출된 특징을 SVM을 이용하여 단일 클래스로 학습시키고, 학습을 통해 생성된 분류기를 이용하여 수신한 RF신호의 스코어를 산출하는 단계
S410
인증이 필요한 스마트키의 스코어가 기 설정된 임계값 이상이면 정당한 스마트키로 판단하는 단계
S510
종 료