(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0050423
(43) 공개일자 2021년05월07일

(51) 국제특허분류(Int. Cl.)
*B60R 25/24* (2013.01) *B60R 25/102* (2013.01)
(52) CPC특허분류
*B60R 25/245* (2013.01)
*B60R 25/102* (2013.01)
(21) 출원번호 10-2020-0052699
(22) 출원일자 2020년04월29일
심사청구일자 2020년04월29일
(30) 우선권주장
1020190134340 2019년10월28일 대한민국(KR)

(71) 출원인
**고려대학교 산학협력단**
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
**이동훈**
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
**주경호**
서울특별시 성북구 지봉로 24길 52-8
**최원석**
서울특별시 강북구 삼양로 256, 105동 501호
(74) 대리인
**김홍석**

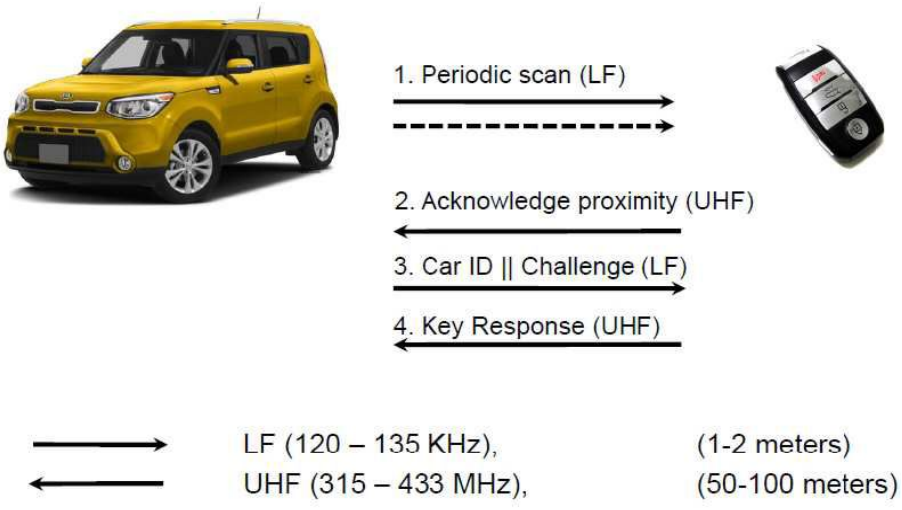
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **LF 핑거프린트 기법을 활용한 공격 탐지 장치 및 방법**

## (57) 요 약

LF 핑거프린트 기법을 이용한 공격 탐지 장치 및 방법이 개시된다. 상기 공격 탐지 장치인 스마트키(smart key)는 차량으로부터 수신된 신호의 캐리어 주파수(carrier frequency)를 제거하여 제1 신호를 생성하고, 상기 제1 신호를 복조(demodulation)하여 블프리앰 영역(preamble region)의 제2 신호와 아이들 영역(idle region)의 제3 신호 중 적어도 하나를 추출하는 전처리부, 상기 제1 신호, 상기 제2 신호, 및 상기 제3 신호 중 적어도 하나의 신호의 피처(feature)를 추출하는 피처 추출부, 및 추출된 피처에 대한 분류기의 출력값을 이용하여 공격 여부를 탐지하는 탐지부를 포함한다.

*대 표 도* - 도1



(52) CPC특허분류
*B60R 2025/1013* (2013.01)
*B60Y 2400/90* (2013.01)

# *명 세 서*

## *청구범위*

### 청구항 1

차량으로부터 수신된 신호의 캐리어 주파수(carrier frequency)를 제거하여 제1 신호를 생성하고, 상기 제1 신호를 복조(demodulation)하여 블프리앰 영역(preamble region)의 제2 신호와 아이들 영역(idle region)의 제3 신호 중 적어도 하나를 추출하는 전처리부;

상기 제1 신호, 상기 제2 신호, 및 상기 제3 신호 중 적어도 하나의 신호의 피처(feature)를 추출하는 피처 추출부; 및

추출된 피처에 대한 분류기의 출력값을 이용하여 공격 여부를 탐지하는 탐지부를 포함하는 스마트키(smart key).

### 청구항 2

제1항에 있어서,

상기 피처 추출부는 상기 제1 신호를 퓨리에 변환(fourier transformation)하여 비트 1을 표현하는 주파수를 상기 피처로 추출하는,

스마트키.

### 청구항 3

제1항에 있어서,

상기 피처 추출부는 상기 제2 신호의 비트 타이밍 오프셋(bit timing offset)을 상기 피처로 추출하는,

스마트키.

### 청구항 4

제1항에 있어서,

상기 피처 추출부는 상기 제3 신호의 지속 시간을 상기 피처로 추출하는,

스마트키.

### 청구항 5

제1항에 있어서,

상기 피처는 평균(Mean), 표준편차(Standard Deviation), 평균편차(Average Deviation), 왜도(Skewness), 첨도(Kurtosis), RMS(Root Mean Square), 최저값(Lowest Value), 최고값(Highest Value), ZCR(Zero-Crossing Rate), 또는 비음성 카운트(Non-negative Count)인,

스마트키.

### 청구항 6

제1항에 있어서,

상기 탐지부는 미리 정해진 평균과 미리 정해진 표준편차를 이용하여 상기 출력값을 정규화하고, 정규화된 출력값을 미리 정해진 임계값과 비교하여 릴레이 공격(Relay attack) 여부를 탐지하는,

스마트키.

**청구항 7**

제1항에 있어서,

상기 차량과 통신하는 송수신부를 더 포함하고,

탐지부가 공격을 탐지한 경우, 상기 송수신부는 상기 차량으로부터 수신된 질의 메시지(challenge message)에 대한 응답 메시지(response message)의 송신을 수행하지 않는,

스마트키.

**청구항 8**

제1항에 있어서,

상기 분류기는 SVM(Support Vector Machine)인,

상기 차량과 상기 스마트키는 PKES(Passive Keyless Entry and Start) 시스템에 포함되는,

스마트키.

**청구항 9**

차량으로부터 송신된 복수의 신호들 각각에 대하여, 캐리어 주파수(carrier frequency)를 제거하여 제1 신호를 생성하고, 상기 제1 신호를 복조(demodulation)하여 블프리앰 영역(preamble region)의 제2 신호와 아이들 영역(idle region)의 제3 신호 중 적어도 하나를 추출하는 전처리부;

상기 제1 신호, 상기 제2 신호, 및 상기 제3 신호 중 적어도 하나의 신호의 피처(feature)를 추출하는 피처 추출부;

상기 복수의 신호들 각각에 대한 상기 피처를 이용하여 분류기를 학습하는 학습부를 포함하고,

상기 학습부는 학습된 분류기의 출력값의 평균과 표준편차를 포함하는 정규화 파라미터를 계산하는,

탐지 모델 생성 장치.

**청구항 10**

제9항에 있어서,

상기 피처 추출부는 상기 제1 신호를 퓨리에 변환하여 비트 1을 표현하는 주파수를 상기 피처로 추출하거나, 상기 제2 신호의 비트 타이밍 오프셋(bit timing offset)을 상기 피처로 추출하거나, 또는 상기 제3 신호의 지속시간을 상기 피처로 추출하는,

탐지 모델 생성 장치.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 차량이나 스마트키를 대상으로 하는 공격 탐지 방법에 관한 것으로, 특히 차량으로부터 수신되는 신

호의 피처(feature)를 추출하여 분류기를 학습함으로써 공격을 탐지할 수 있는 장치 및 방법에 관한 것이다.

## 배 경 기 술

[0002] 차량의 KES(Keyless Entry System)는 운전자가 스마트키(smart key)를 직접 동작시키지 않더라도 차량과 스마트키 간의 RF 통신을 통해 운전자의 개입 없이 차량의 문(door)을 개폐하고 시동을 킬 수 있도록 하는 편의 기능이다. 이러한 편의성에도 불구하고 KES에 대한 취약점이 발견되었고, 이를 이용한 다양한 사이버 공격이 가능함이 입증되었다. 하지만, 차량 제조사들은 여전히 추가적인 보안대책 없이 차량을 생산하고 있다.

[0003] 본 명세서에서는 위와 같은 보안 문제점을 해결하기 위해 Device Fingerprinting 기법을 이용하여 정당한 스마트키를 사전에 등록시켜 놓음으로써 릴레이 공격을 방지하는 기술을 제안하고자 한다.

## 선행기술문헌

### 특허문헌

[0004] (특허문헌 0001) 대한민국 공개특허 제10-2016-0149500호

(특허문헌 0002) 대한민국 등록특허 제10-1562124호

## 발명의 내용

### 해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적인 과제는 차량으로부터 송신되는 신호의 특징을 이용하여 분류기를 학습하고, 이를 통해 공격을 탐지할 수 있는 장치 및 방법을 제공하는 것이다.

### 과제의 해결 수단

[0006] 본 발명의 실시예에 따른 스마트키는 차량으로부터 수신된 신호의 캐리어 주파수(carrier frequency)를 제거하여 제1 신호를 생성하고, 상기 제1 신호를 복조(demodulation)하여 블프리앰 영역(preamble region)의 제2 신호와 아이들 영역(idle region)의 제3 신호 중 적어도 하나를 추출하는 전처리부, 상기 제1 신호, 상기 제2 신호, 및 상기 제3 신호 중 적어도 하나의 신호의 피처(feature)를 추출하는 피처 추출부, 및 추출된 피처에 대한 분류기의 출력값을 이용하여 공격 여부를 탐지하는 탐지부를 포함한다.

[0007] 또한, 본 발명의 실시예에 따른 탐지 모델 생성 장치는 차량으로부터 송신된 복수의 신호들 각각에 대하여, 캐리어 주파수(carrier frequency)를 제거하여 제1 신호를 생성하고, 상기 제1 신호를 복조(demodulation)하여 블프리앰 영역(preamble region)의 제2 신호와 아이들 영역(idle region)의 제3 신호 중 적어도 하나를 추출하는 전처리부, 상기 제1 신호, 상기 제2 신호, 및 상기 제3 신호 중 적어도 하나의 신호의 피처(feature)를 추출하는 피처 추출부, 상기 복수의 신호들 각각에 대한 상기 피처를 이용하여 분류기를 학습하는 학습부를 포함하고, 상기 학습부는 학습된 분류기의 출력값의 평균과 표준편차를 포함하는 정규화 파라미터를 계산한다.

### 발명의 효과

[0008] 본 발명의 실시예에 따른 스마트키와 탐지 모델 생성 장치에 의할 경우, KES(Keyless Entry System)을 보호하여 안전한 사용자 인증 시스템을 구축함으로써 차량 도난 사고를 예방하고 운전자에게 편의를 제공할 수 있는 효과가 있다.

### 도면의 간단한 설명

[0009] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 PKES 시스템을 도시한다.

도 2는 본 발명의 일 실시예에 따른 탐지 모델 생성 장치의 기능 블럭도이다.

도 3은 도 1에 도시된 스마트키의 기능 블럭도이다.

도 4는 도 1에 도시된 스마트키의 다른 실시예에 따른 기능 블럭도이다.

도 5는 도 3 또는 도 4에 도시된 스마트키가 수신한 신호를 도시한다.

도 6은 도 2에 도시된 피쳐 추출부에 의해 추출되는 피쳐들을 도시한다.

## *발명을 실시하기 위한 구체적인 내용*

[0010] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0011] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0012] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0013] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0014] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0015] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0016] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0018] 도 1은 본 발명의 일 실시예에 따른 PKES 시스템을 도시한다. 이하에서는, 도 1은 참조하여 PKES(Passive Keyless Entry and Start) 시스템 또는 KES(Keyless Entry System)의 동작을 설명한다.

[0019] PKES 시스템에 포함된 차량과 스마트키는 PKES 시스템에서 차량과 스마트키는 서로 통신하기 위해 두 가지 주파수 채널 신호를 사용한다. 차량은 도달 거리가 1 내지 2 미터로 짧은 LF(Low Frequency, 120 ~ 135 KHz) 신호를 사용하며 스마트키는 먼 거리에서 차량을 제어하기 위해 도달 거리가 50 내지 100 미터인 UHF(Ultra High Frequency, 315 ~ 433 MHz) 신호를 사용한다.

[0020] 우선, 차량은 주기적으로 LF 신호(스마트키의 존재 확인 및/또는 웨이크업(Wake up) 신호를 차량 주위로 송신하며, 이를 수신한 스마트키는 웨이크업되면서 수신된 LF 신호에 대한 응답 신호로 UHF 신호(존재 확인 신호)를

차량으로 송신한다. 스마트키의 존재가 확인된 경우, 차량은 질의(Challenge) 정보 및/또는 차량의 식별 정보(예컨대, 차량의 ID)가 포함된 LF 신호를 다시 스마트키로 송신한다. 스마트키는 질의에 대응하는 응답(Response) 정보가 포함된 UHF 신호를 차량으로 송신한다. 수신한 응답 정보가 정상적으로 확인된 경우, 차량은 차량 제어(문의 개폐, 시동 등)를 수행한다.

[0021] 이러한 PKES 시스템에서 공격자는 릴레이 공격을 수행할 수 있다. 릴레이 공격은 차량과 운전자의 스마트키 사이에서 두 개의 신호 중계기를 이용하여 차량과 스마트키가 서로 근접되어 있다고 판단하게 하여 정상 과정과 동일하게 차량 제어를 수행하는 공격을 의미한다. 차량은 스마트키에서 송신한 질의에 대응하는 응답 신호가 실제 정당한 스마트키가 전송한 신호인지 파악할 수 없기 때문에 이러한 공격이 가능하다.

[0022] 본 발명에서는 차량에서 송신하는 신호(또는 스마트키가 차량으로부터 수신하는 신호), 즉 웨이크업 신호(또는 웨이크업 메시지) 및/또는 질의 신호(또는 질의 메시지)의 피쳐(Feature, 특징)를 추출하여 릴레이 공격 여부를 탐지하고자 한다. 이러한 의미에서 본 발명은 LF 핑거프리트(Fingerprint) 기법을 이용한 릴레이 공격 방지 기법이라 명명될 수 있다.

[0023] 도 2는 본 발명의 일 실시예에 따른 탐지 모델 생성 장치의 기능 블럭도이다.

[0024] 도 2를 참조하면, 탐지 모델 생성 장치(100)는 적어도 프로세서(또는 (마이크로) 컨트롤러) 및/또는 메모리를 포함하는 컴퓨팅 장치를 의미할 수 있다. 실시예에 따라, 탐지 모델 생성 장치(100)는 도 1에 도시된 스마트키를 의미할 수도 있으나, 본 발명이 이에 제한되는 것은 아니다. 즉, 경우에 따라 탐지 모델 생성 장치(100)는 도 1의 스마트키와는 구별되는 컴퓨팅 장치를 의미할 수도 있다.

[0025] 탐지 모델 생성 장치(100)는 송수신부(110), 전처리부(120), 피쳐 추출부(130), 학습부(140) 및 저장부(150) 중 적어도 하나를 포함할 수 있다.

[0026] 송수신부(110)는 차량으로부터 송신되는 신호들을 수신할 수 있다. 수신된 신호는 저장부(150)에 저장될 수 있다. 실시예에 따라, 탐지 모델 생성 장치(100)는 송수신부(110)를 포함하지 않을 수도 있다. 이 경우, 차량으로부터 송신되는 신호들은 별도의 수신 장치를 통하여 수신된 후 저장부(150)에 미리 저장되어 있을 수도 있다.

[0027] 전처리부(120)는 송수신부(110)에 의해 수신된 신호들 각각에 대한 전처리 동작을 수행할 수 있다. 전처리 동작은 제1 전처리 동작 및/또는 제2 전처리 동작을 포함할 수 있다.

[0028] 제1 전처리 동작은 노이즈 제거 및/또는 캐리어 주파수 제거를 포함할 수 있다. 구체적으로, 전처리부(120)는 소정의 필터(예컨대, LPF(Low Pass Filter))를 이용하여 신호에 포함된 노이즈를 제거할 수 있다. 또한, 전처리부(120)는 캐리어(Carrier) 주파수를 제거하여 베이스밴드(baseband)의 신호를 추출할 수 있다. 제1 전처리 동작의 결과로 생성된 신호를 제1 신호(Signal 1)라 명명할 수 있다.

[0029] 제2 전처리 동작은 복조(Demodulation)를 포함할 수 있다. 구체적으로, 전처리부(120)는 제1 신호를 복조하여 프리앰블(Preamble) 영역과 아이들(Idle) 영역을 추출할 수 있다. PKES 시스템은 ASK(Amplitude Shift Keying) 변조(Modulation) 기법을 사용하기 때문에, 전처리부(120)는 ASK의 복조 기법을 사용하여 제1 신호를 복조할 수 있다. ASK는 중심 주파수($f_c$)를 기준으로 일정한 크기($A_0$)만큼 신호의 진폭을 변화시켜 비트를 나타낸다. 진폭이 $A_0$인 신호는 비트 1을 표현하며, 진폭이 0인 신호는 비트 0을 나타낸다. 프리앰블 영역은 무선 통신에서 패킷 혹은 비트(bit)의 동기화(synchronization)를 위해 사용되는 영역이며, 아이들 영역은 두 개의 LF 대역 신호의 간격에 위치한 신호를 의미한다. 여기서, 프리앰블 영역의 신호를 제2 신호(Signal 2)라 하고, 아이들 영역의 신호를 제3 신호(Signal 3)라 명명할 수 있다. 제1 신호, 제2 신호, 및 제3 신호는 저장부(150)에 저장될 수 있다.

[0030] 피쳐 추출부(130)는 제1 신호, 제2 신호, 및 제3 신호 중 적어도 하나의 특징(feature)을 추출할 수 있다.

[0031] 구체적으로, 피쳐 추출부(130)는 제1 신호를 퓨리에 변환(Fourier Transformation)하여 비트 1을 표현하는 주파수($f_c^{offset}$)를 산출한다. 또한, 피쳐 추출부(130)는 제2 신호에 포함되는 펄스들 사이의 간격을 측정할 수 있다. 펄스들 사이의 간격(개별 펄스의 지속 시간을 의미할 수 있음)은 비트 타이밍 오프셋(bit timing offset, $T_b^{offset}$)으로 표현될 수 있다. 또한, 피쳐 추출부(130)는 제2 신호의 다양한 통계적 특성을 나타내는 적어도 하나의 피쳐를 추출할 수 있다. 추출되는 통계적 특성들은 도 6에 도시되어 있다. 또한, 피쳐 추출부(130)는 제3 신호를 대상으로 적어도 하나의 통계적 특성을 추출할 수 있다. 추가적으로 제3 신호, 즉 아이들 영역의 길이

(또는 지속 시간) 또한 추출되는 피처가 될 수 있다. 추출된 피처들은 저장부(150)에 저장될 수 있다.

[0032] 추출되는 피처(Feature)는 평균(Mean), 표준편차(Standard Deviation), 평균편차(Average Deviation), 왜도(Skewness), 첨도(Kurtosis), RMS(Root Mean Square), 최저값(Lowest Value), 최고값(Highest Value), ZCR(Zero-Crossing Rate), 비음성 카운트(Non-negative Count), 도심(Spec. Centroid), 엔트로피(Spec. Entropy), 스프레드(Spec. Spread), 왜도(Spec. Skewness), 첨도(Spec. Kurtosis), 편평도(Spec. Flatness), 휘도(Spec. Brightness), 롤 오프(Spec. Roll off), 비정규성(Spec. Irregularity), 플럭스(Spec. flux) 중 적어도 하나일 수 있다.

[0033] 학습부(140)는 추출된 피처를 이용하여 분류기를 생성하고 정규화 파라미터를 생성할 수 있다. 구체적으로, 학습부(140)는 추출된 피처를 분류기 모델(예컨대, SVM(Support Vector Machine), k-NN 알고리즘, 또는 결정 트리(decision tree) 알고리즘을 이용하여 원-클래스 러닝(One-Class learning)을 수행할 수 있다. 그러나, 본 발명의 권리범위가 사용되는 알고리즘의 종류에 제한되는 것은 아니며, 원-클래스 러닝이 가능한 알고리즘이라면 알고리즘의 종류에 무관하게 적용가능하다. 학습 과정에서는 정상 신호에서 추출된 피처만을 사용하며, 전체 학습 데이터 중 랜덤하게 선택된 X%의 데이터를 사용하여 분류기를 생성하며, 나머지 (100-X)%의 학습 데이터를 사용하여 생성된 분류기에 대한 테스트를 수행할 수 있다. 해당 과정은 Y번 반복 수행되어 정상 학습 데이터에 대한 분류기의 출력값을 누적하여 평균($\mu_0$)과 표준 편차($\sigma_0$)를 산출하고, 이를 정규화 파라미터로 사용할 수 있다.

[0034] 저장부(150)에는 송수신부(110)에 의해 수신된 신호, 전처리부(120)의 전처리 결과, 즉 제1 신호, 제2 신호, 및 제3 신호, 피처 추출부(130)에 의한 피처 추출의 결과, 즉 각 신호의 피처들, 학습부(140)에 의해 학습된 분류기, 정규화 파라미터 등이 저장될 수 있다.

[0035] 도 3은 도 1에 도시된 스마트키의 기능 블럭도이다.

[0036] 도 3을 참조하면, 스마트키(200)는 송수신부(210), 전처리부(220), 피처 추출부(230), 탐지부(240), 알람부(250), 및 저장부(260) 중 적어도 하나를 포함할 수 있다. 또한, 스마트키(200)에는 도 2의 탐지 모델 생성 장치에 의해 생성된 탐지 모델(분류기), 평균($\mu_0$), 표준 편차($\sigma_0$) 등이 미리 저장되어 있을 수 있다. 스마트키(200)의 구성과 동작을 설명함에 있어 앞선 기재와 중복되는 내용에 관하여는 그 기재를 생략하기로 한다.

[0037] 송수신부(210)는 신호 또는 메시지를 송수신함으로써 차량과 통신할 수 있다. 구체적으로, 송수신부(210)는 차량으로부터 송신되는 웨이크업 신호(웨이크업 메시지)를 수신하고, 웨이크업 신호에 응답하여 생존 확인 신호(생존 확인 메시지)를 송신할 수 있다. 또한, 송수신부(210)는 차량으로부터 질의 신호(질의 메시지)를 수신하고, 질의 신호에 응답하여 응답 신호(응답 메시지)를 송신할 수 있다. 다만, 탐지부(240)가 릴레이 공격을 탐지한 경우에 송수신부(210)는 응답 신호를 송신하지 않을 수 있다. 이를 통해, 정당하지 않은 사용자가 차량을 제어하는 것을 예방할 수 있다.

[0038] 송수신부(210)에 의해 송수신되는 신호는 저장부(260)에 저장될 수 있다.

[0039] 전처리부(220)는 송수신부(210)에 의해 수신된 신호들 각각에 대한 전처리 동작을 수행할 수 있다. 전처리 동작은 제1 전처리 동작 및/또는 제2 전처리 동작을 포함할 수 있다.

[0040] 제1 전처리 동작은 노이즈 제거 및/또는 캐리어 주파수 제거를 포함할 수 있다. 구체적으로, 전처리부(220)는 소정의 필터(예컨대, LPF(Low Pass Filter))를 이용하여 신호에 포함된 노이즈를 제거할 수 있다. 또한, 전처리부(120)는 캐리어(Carrier) 주파수를 제거하여 베이스밴드(baseband)의 신호를 추출할 수 있다. 제1 전처리 동작의 결과로 생성된 신호를 제1 신호(Signal 1)라 명명할 수 있다.

[0041] 제2 전처리 동작은 복조(Demodulation)를 포함할 수 있다. 구체적으로, 전처리부(120)는 제1 신호를 복조하여 프리앰블(Preamble) 영역과 아이들(Idle) 영역을 추출할 수 있다. PKES 시스템은 ASK(Amplitude Shift Keying) 변조(Modulation) 기법을 사용하기 때문에, 전처리부(120)는 ASK의 복조 기법을 사용하여 제1 신호를 복조할 수 있다. 여기서, 프리앰블 영역의 신호를 제2 신호(Signal 2)라 하고, 아이들 영역의 신호를 제3 신호(Signal 3)라 명명할 수 있다. 제1 신호, 제2 신호, 및 제3 신호는 저장부(150)에 저장될 수 있다.

[0042] 피처 추출부(230)는 제1 신호, 제2 신호, 및 제3 신호 중 적어도 하나의 특징(feature)을 추출할 수 있다.

[0043] 구체적으로, 피처 추출부(230)는 제1 신호를 퓨리에 변환(Fourier Transformation)하여 비트 1을 표현하는 주파수($f_c^{offset}$)를 산출한다. 또한, 피처 추출부(230)는 제2 신호에 포함되는 펄스들 사이의 간격을 측정할 수 있다.

펄스들 사이의 간격(개별 펄스의 지속 시간을 의미할 수 있음)은 비트 타이밍 오프셋(bit timing offset, $T_b^{offset}$)으로 표현될 수 있다. 또한, 피쳐 추출부(130)는 제2 신호의 다양한 통계적 특성을 나타내는 적어도 하나의 피쳐를 추출할 수 있다. 추출되는 통계적 특성들은 도 6에 도시되어 있다. 또한, 피쳐 추출부(130)는 제3 신호를 대상으로 적어도 하나의 통계적 특성을 추출할 수 있다. 추가적으로 제3 신호, 즉 아이들 영역의 길이(또는 지속 시간) 또한 추출되는 피쳐가 될 수 있다. 추출된 피쳐들은 저장부(150)에 저장될 수 있다.

[0044] 탐지부(240)는 차량 및/또는 스마트키를 대상으로 하는 공격(예컨대, 릴레이 공격)의 유무를 탐지할 수 있다. 구체적으로, 탐지부(240)는 추출된 피쳐를 분류기에 입력하고 분류기의 출력값(x)를 획득할 수 있다. 이후, 탐지부(240)는 정규화 파라미터(평균($\mu_0$), 표준 편차($\sigma_0$))를 이용하여 출력값(x)를 정규화한다($\frac{|x-\mu|}{\sigma}$). 마지막으로, 탐지부(240)는 정규화된 출력값($\frac{|x-\mu|}{\sigma}$)과 미리 정의된 임계값($\Gamma$)을 비교하여 릴레이 공격을 탐지할 수 있다. 일 예로, 정규화된 출력값이 임계값 보다 큰 경우($\frac{|x-\mu|}{\sigma} > \Gamma$)를 릴레이 공격이 수행된 경우로 판단할 수 있다. 임계값은 관리자에 의해 미리 정해질 수 있으며, 예시적인 값은 4 내지 5 범위의 값일 수 있다.

[0045] 알람부(250)는 탐지부(240)의 탐지 결과를 운전자(또는 스마트키(200)의 소지자)에게 알릴 수 있다. 일 예로, 알람부(250)는 발광 장치(예컨대, LED), 디스플레이 장치, 음성 출력 장치 등을 포함하도록 구성될 수 있고, 릴레이 공격이 탐지된 경우, 발광 장치, 디스플레이 장치, 또는 음성 출력 장치를 구동함으로써 운전자에게 릴레이 공격을 알릴 수 있다.

[0046] 저장부(260)에는 송수신부(210)에 의해 송수신되는 신호, 전처리부(220)의 전처리 결과, 즉 제1 신호, 제2 신호, 및 제3 신호, 피쳐 추출부(230)에 의해 추출된 피쳐들, 탐지부(240)에 의한 탐지 결과, 탐지 모델(분류기), 평균($\mu_0$), 표준 편차($\sigma_0$) 등이 저장될 수 있다.

[0047] 도 4는 도 1에 도시된 스마트키의 다른 실시예에 따른 기능 블럭도이다.

[0048] 도 4를 참조하면, 스마트키(300)는 모델 생성부(310)과 공격 탐지부(330)를 포함한다. 모델 생성부(310)는 도 2에 도시된 탐지 모델 생성 장치(100)와 동일한 구성 및 기능을 갖고, 공격 탐지부(330)는 도 3에 도시된 스마트키(200)와 동일한 구성 및 기능을 갖도록 구현될 수 있으므로, 이에 대한 상세한 설명은 생략하기로 한다.

[0049] 도 2 내지 도 4에 도시된 탐지 모델 생성 장치(100), 스마트키(200), 및 스마트키(300)의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0050] 또한, 본 명세서에서 '~부'라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0051] 도 5는 도 3 또는 도 4에 도시된 스마트키가 수신한 신호를 도시한다.

[0052] 스마트키는 ASK 변조된 신호를 수신할 수 있다. 스마트키가 수신한 ASK 변조된 신호는 도 5의 상부에 도시되어 있다. 실시예에 따라, 도 5의 상부에 도시된 신호는 전처리된 신호(제1 신호), 즉 노이즈와 캐리어 주파수가 제거된 신호일 수 있다.

[0053] ASK 변조된 신호는 ASK 복조 과정을 거치는 데, 복조된 신호는 도 5의 하부에 도시되어 있다. 복조된 신호는 순차적으로, 웨이크업 신호, 아이들 영역(제3 신호), 블프리앰 영역(제2 신호), 및 페이로드(payload)를 포함한다. 본 발명에서는 블프리앰 영역 및/또는 아이들 영역의 신호로부터 피쳐(특징)를 추출하고, 추출된 피쳐를 이용하여 분류기를 학습하고, 학습된 분류기를 이용하여 릴레이 공격을 탐지한다.

[0055] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크

로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0056] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0057] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조ㅂ하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0058] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

## *부호의 설명*

[0059] 100 : 탐지 모델 생성 장치 110 : 송수신부

120 : 전처리부 130 : 피쳐 추출부

140 : 학습부 150 : 저장부

200 : 스마트키 210 : 송수신부

220 : 전처리부 230 : 피쳐 추출부

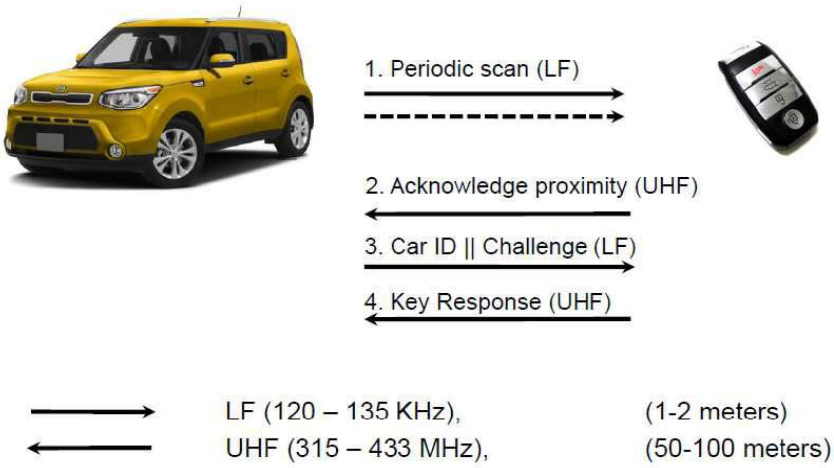
240 : 탐지부 250 : 알람부

260 : 저장부 300 : 스마트키

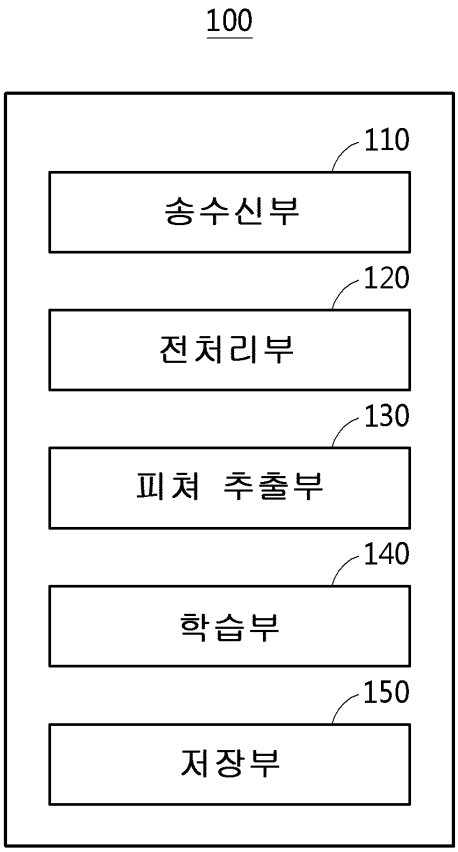
310 : 모델 생성부 330 : 공격 탐지부

도면

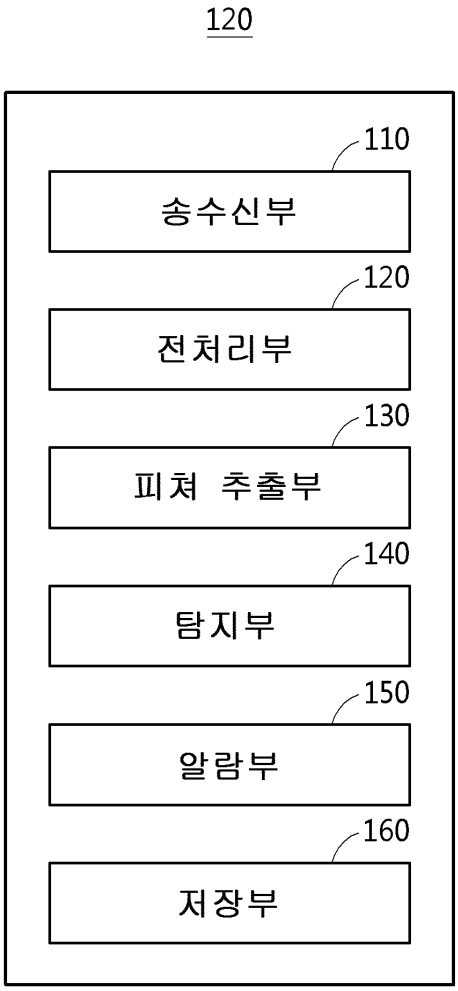
도면1


1. Periodic scan (LF)
2. Acknowledge proximity (UHF)
3. Car ID || Challenge (LF)
4. Key Response (UHF)
LF (120 – 135 KHz), (1-2 meters)
UHF (315 – 433 MHz), (50-100 meters)

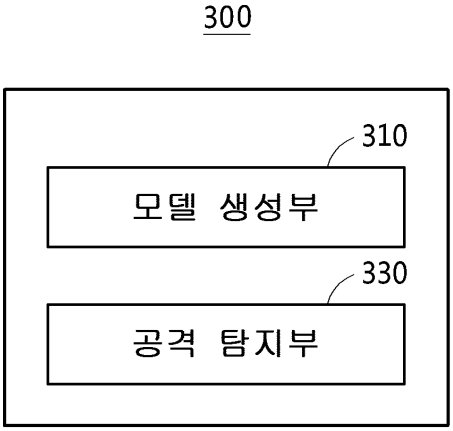
도면2


100
110
송수신부
120
전처리부
130
피쳐 추출부
140
학습부
150
저장부

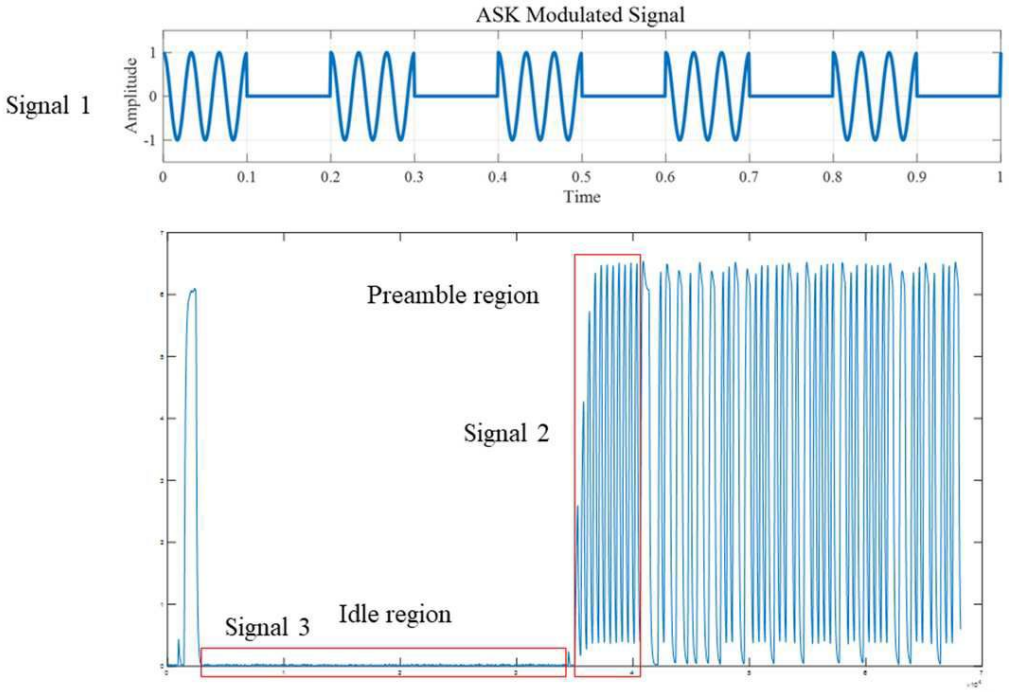
도면3


120
110
송수신부
120
전처리부
130
피쳐 추출부
140
탐지부
150
알람부
160
저장부

도면4


300
310
모델 생성부
330
공격 탐지부

도면5




도면6

| Feature | Description |
|---|---|
| Mean | $\mu = \frac{1}{N}\sum_{i=1}^{N} x(i)$ |
| Standard Deviation | $\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i)-\overline{x})}$ |
| Average Deviation | $D = \frac{1}{N}\sum_{i=1}^{N}\lvert x(i)-\mu\rvert$ |
| Skewness | $\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\overline{x}}{\sigma})^3$ |
| Kurtosis | $\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\overline{x}}{\sigma})^4$ |
| RMS | $RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i))^2}$ |
| Lowest Value | $L = Min\{x(i)\lvert_{i=1..N}\}$ |
| Highest Value | $H = Max\{x(i)\lvert_{i=1..N}\}$ |
| ZCR | $ZCR = \frac{1}{N}\sum_{i=1}^{N}\lvert s(i)-s(i-1)\rvert$ where $s(t) = 1$ if the signal has a positive amplitude at time $t$ and 0 otherwise. |
| Non-negative Count | $NC = \lvert S\rvert$, where $S = \{i\lvert x(i) \geq 0\}$ |

| Feature Name | Description |
|---|---|
| Spec. Centroid | $\mu = \frac{\sum_{i=1}^{N} y_f(i) y_m(i)}{\sum_{i=1}^{N} y_m(i)}$ |
| Spec. Entropy | $H = \sum_{i=1}^{N} w_i \cdot \log_2 w_i$, where $w_i = \frac{y_m(i)}{\sum_{i=1}^{N} y_m(i)}$ |
| Spec. Spread | $\sigma = \sqrt{\sum_{i=1}^{N}((f_i-\mu)^2 \cdot w_i)}$ |
| Spec. Skewness | $Skewness = \frac{\sqrt{\sum_{i=1}^{N}(f_i-\mu)^3 \cdot w_i}}{\sigma^3}$ |
| Spec. Kurtosis | $Kurtosis = \frac{\sqrt{\sum_{i=1}^{N}(f_i-\mu)^4 \cdot w_i}}{\sigma_s^4}$ |
| Spec. Flatness | $Flatness = \sum_{i=f_c}^{N}[y_m(i) \cdot \frac{\prod_{i=1}^{N} y_m(i))^{\frac{1}{N}}}{\frac{1}{N}\cdot\sum_{i=1}^{N} y_m(i)}]$ |
| Spec. Brightness | $Brightness = \sum_{i=f_c}^{N} y_m(i)$, where $f_c$ is the cut-off frequency |
| Spec. Roll off | $\underset{f\in 1,\ldots,N}{\operatorname{argmin}} \sum_{i=1}^{f} y_m(i) \geq 0.85 \cdot \sum_{i=1}^{N} y_m(i)$ |
| Spec. Irregularity | $Irregularity = \frac{\sum_{i=1}^{N-1}(y_m^2(i)-y_m^2(i+1))^2}{\sum_{i=1}^{N-1}(y_m^2(i))^2}$ |
| Spec. flux | $Flux = \sum_{i=1}^{N-1}(N(i)-N(i+1))^2$, where $N(i)$ is the normalized magnitude as $N(i) = \frac{y_m(i)}{\sum_{i=1}^{N} y_m(i)}$ |