(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년07월22일
(11) 등록번호 10-2424619
(24) 등록일자 2022년07월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06N 3/08* (2006.01)
G06V 10/40 (2022.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06N 3/08 (2013.01)
(21) 출원번호 10-2021-0169635
(22) 출원일자 2021년12월01일
심사청구일자 2021년12월01일
(56) 선행기술조사문헌
KR1020210030791 A*
KR1020210114169 A*
US20190197238 A1*
Mordechai Guri et al., "BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness"(2020.02.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
송재승
경기도 성남시 분당구 수내로 206, 310동 1001호 (수내동, 푸른마을)
이지호
서울특별시 중랑구 동일로92길 40, 108동 1203호 (면목동, 사가정 센트럴 아이파크)
이영준
서울특별시 종로구 낙산길 198, 206동 1004호(창신동, 창신쌍용아파트 2지구)
(74) 대리인
민영준

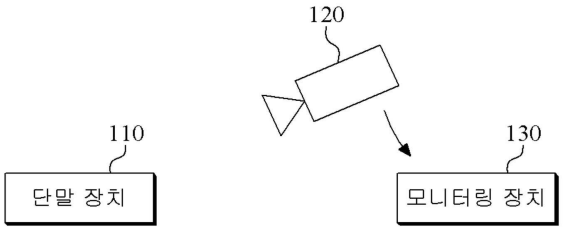
전체 청구항 수 : 총 7 항 심사관 : 정성훈

(54) 발명의 명칭 **에어갭 환경에서의 공격 감지 방법 및 공격 감지를 위한 학습 방법**

(57) 요 약

에어갭 환경에서 광학 신호를 이용하여 공격을 감지하는 방법 및 공격 감지를 위한 학습 방법이 개시된다. 개시된 에어갭 환경에서의 공격 감지 방법은 단말 장치의 광학 신호로부터, 상기 광학 신호의 특징값을 추출하는 단계; 및 상기 특징값을 이용하여, 상기 단말 장치에 대한 공격을 감지하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06V 10/40 (2022.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711139205
과제번호	2021-0-01816-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성(R&D)
연구과제명	메타버스 자율트윈 핵심기술 연구
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2021.07.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

컴퓨팅 장치에서 수행되는, 에어갭 환경에서의 공격 감지 방법에 있어서,

단말 장치의 광학 신호로부터, 상기 광학 신호의 특징값을 추출하는 단계; 및

상기 특징값을 이용하여, 상기 단말 장치에 대한 공격을 감지하는 단계를 포함하며,

상기 광학 신호의 특징값을 추출하는 단계는

사람이 상기 단말 장치에 근접한 상태에서, 상기 광학 신호의 특징값을 추출하며, 상기 특징값의 추출이 시작된 이후 미리 설정된 시간 내에 공격이 감지되지 않은 경우, 상기 특징값의 추출을 중단하는

에어갭 환경에서의 공격 감지 방법.

청구항 2

제 1항에 있어서,

상기 광학 신호의 특징값을 추출하는 단계는

상기 단말 장치를 포함하는 비디오에서, 상기 광학 신호의 발생 영역에 대한 이미지 패치를 추출하는 단계; 및

상기 이미지 패치에서, 상기 특징값을 추출하는 단계

를 포함하는 에어갭 환경에서의 공격 감지 방법.

청구항 3

제 2항에 있어서,

상기 광학 신호의 발생 영역은

상기 단말 장치의 모니터, 저장 장치, 키보드 또는 마우스를 포함하는 영역인

에어갭 환경에서의 공격 감지 방법.

청구항 4

제 2항에 있어서,

상기 특징값은

상기 광학 신호의 점멸 패턴, 주파수 또는 밝기값에 대한 시계열 데이터인

에어갭 환경에서의 공격 감지 방법.

청구항 5

제 3항에 있어서,

상기 광학 신호의 특징값을 추출하는 단계는

상기 이미지 패치를 상기 비디오의 프레임별로 분석하여, 상기 특징값을 추출하는

에어갭 환경에서의 공격 감지 방법.

청구항 6

제 1항에 있어서,

상기 단말 장치에 대한 공격을 감지하는 단계는

훈련 데이터를 통해 학습된 인공 신경망을 이용하여, 상기 단말 장치에 대한 공격을 감지하며,

상기 훈련 데이터는

상기 단말 장치의 정상 동작 상태 또는 상기 단말 장치에 대한 공격 상태로부터 획득된 훈련용 광학 신호의 특징값을 포함하는

에어갭 환경에서의 공격 감지 방법.

청구항 7

제 1항에 있어서,

상기 광학 신호의 특징값을 추출하는 단계는

상기 광학 신호를 감지하는 광센서의 출력값으로부터 상기 광학 신호의 특징값을 추출하는

에어갭 환경에서의 공격 감지 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 공격 감지 방법 및 공격 감지를 위한 학습 방법에 관한 발명으로서, 더욱 상세하게는 에어갭 환경에서의 공격 감지 방법 및 공격 감지를 위한 학습 방법에 관한 것이다.

배 경 기 술

[0003] 외부 공격으로부터 시스템을 보호하기 위해, 시스템을 네트워크로부터 분리하는 에어갭(air-gapped) 환경이 구축되고 있다. 에어갭 환경에서는 공격자가 네트워크를 통해 시스템에 접근할 수 없으므로, 네트워크를 통해 시스템의 정보를 탈취하는 것은 불가능하다.

[0004] 하지만 최근에는 네트워크를 이용하지 않고, 에어갭 환경의 시스템을 공격하는 시도가 발견되고 있다. 에어갭

환경에서도 시스템은 USB 등을 통해 악성 코드에 감염될 수 있으며, 단말 장치의 광학 신호를 이용하여, 시스템의 정보를 탈취하는 공격 방법이 보고되고 있다. 예컨대, 공격자는, 악성 코드를 이용하여, 사용자가 인지할 수 없을 정도로 모니터의 주사율을 변경하거나 단말 장치의 LED를 점멸시키고, 단말 장치에 대한 영상으로부터 정보를 탈취할 수 있다. 따라서 에어갭 환경에서 공격을 탐지하는 방법에 대한 니즈가 대두되고 있다.

[0005] 관련 선행문헌으로 특허 문헌인 대한민국 공개특허 제2021-0125234호, 비특허 문헌인, "에어 갭 네트워크 정보 유출기법 분석과 대응개념에 관한 연구, 김기현, 김용철, 한국통신학회, 2019"가 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 에어갭 환경에서 광학 신호를 이용한 공격을 감지할 수 있는 방법을 제공하기 위한 것이다.

[0008] 또한 본 발명은 본 발명은 에어갭 환경에서 광학 신호를 이용한 공격의 감지를 위한 학습 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0010] 상기한 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 단말 장치의 광학 신호로부터, 상기 광학 신호의 특징값을 추출하는 단계; 및 상기 특징값을 이용하여, 상기 단말 장치에 대한 공격을 감지하는 단계를 포함하는 에어갭 환경에서의 공격 감지 방법이 제공된다.

[0011] 또한 상기한 목적을 달성하기 위한 본 발명의 다른 실시예에 따르면, 상기 단말 장치의 정상 동작 상태 또는 상기 단말 장치에 대한 공격 상태에서 획득된 훈련용 광학 신호로부터 특징값을 추출하는 단계; 및 인공 신경망을 이용하여, 상기 특징값에 대한 공격 여부를 학습하는 단계를 포함하는 에어갭 환경에서의 공격 감지를 위한 학습 방법이 제공된다.

발명의 효과

[0013] 본 발명의 일실시예에 따르면, 에어갭 환경에서도 효과적으로 광학 신호를 이용하는 공격을 감지할 수 있다.

[0014] 또한 본 발명의 일실시예에 따르면, 사람이 단말 장치에 접근하는 상황과 같이 공격자에 의해 단말 장치가 감염될 수 있는 상황에서 특징값을 추출하고, 공격이 감지되지 않은 경우 특징값 추출을 중단함으로써, 공격 감지에 소요되는 비용과 시간을 줄일 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일실시예에 따른 에어갭 환경에서 공격을 탐지하는 시스템을 설명하기 위한 도면이다.

도 2는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 감지 방법을 설명하기 위한 도면이다.

도 3은 본 발명의 일실시예에 따른 특징값 추출 방법을 설명하기 위한 도면이다.

도 4는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 감지를 위한 학습 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0018] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 도 1은 본 발명의 일실시예에 따른 에어갭 환경에서 공격을 탐지하는 시스템을 설명하기 위한 도면이다.

[0021] 도 1을 참조하면, 본 발명의 일실시예에 따른 공격 탐지 시스템은, 단말 장치(110), 카메라(120) 및 모니터링 장치(130)를 포함한다.

[0022] 단말 장치(110)는 모니터, 저장 장치, 키보드 및 마우스 등을 포함한다. 모니터로부터 빛이라는 광학 신호가 생

성되며, HDD와 같은 저장 장치에서도 동작 상태를 나타내는 램프를 통해 빛, 즉 광학 신호가 생성된다. 마찬가지로 키보드 및 마우스 역시 광학 신호를 생성하는 램프가 탑재될 수 있다.

[0023] 카메라(120)는 단말 장치(110)를 촬영하며, 단말 장치(110)를 포함하는 비디오를 생성한다. 비디오에는 단말 장치(110)에서 생성되는 광학 신호가 포함된다. 카메라(120)는 고정된 상태로 단말 장치에 대한 비디오를 생성한다.

[0024] 모니터링 장치(130)는 단말 장치(110)의 광학 신호로부터 광학 신호의 특징값을 추출하며, 특징값을 이용하여 단말 장치(110)에 대한 공격을 감지한다. 모니터링 장치(130)는 카메라(120)에서 생성된 비디오에서 광학 신호의 특징값을 추출할 수 있다. 또는 실시예에 따라서 카메라(120) 대신, 단말 장치(110)의 광학 신호를 감지하는 광센서가 이용될 수 있으며, 이 경우 모니터링 장치(120)는 광센서의 출력값으로부터, 광학 신호의 특징값을 추출할 수 있다.

[0025] 특징값은 일실시예로서, 광학 신호의 점멸 패턴, 주파수 또는 밝기값일 수 있다. 단말 장치(110)가 정상적으로 동작하는 상태에서의 저장 장치의 램프의 점멸 패턴, 주파수 또는 밝기값은, 공격 상태에서의 저장 장치의 램프의 점멸 패턴, 주파수 또는 밝기값과 다를 수 있다. 예컨대 정상적으로 동작하는 상태에서의 저장 장치의 램프의 점멸 패턴은 불규칙하지만, 공격 상태에서 저장 장치의 램프는 규칙적이며 일예로 모스 부호나 이진 코드에 대응되도록 점멸될 수 있다. 또는 공격 상태에서 저장 장치의 램프의 밝기가 이진 코드에 대응되도록 변화할 수 있다. 따라서, 모니터링 장치(130)는 광학 신호의 특징값으로부터 단말 장치(110)에 대한 공격 여부를 감지할 수 있다.

[0026] 일실시예로서, 모니터링 장치(130)는 특징값을 미리 학습된 인공 신경망에 입력하여, 공격 여부를 감지할 수 있다.

[0027] 이와 같이, 본 발명의 일실시예는, 에어갭 환경에서 단말 장치의 광학 신호를 이용하여 정보를 탈취하는 공격 방식에 대응하여, 광학 신호의 특징값을 이용하여 공격을 감지하는 방법을 제안한다. 본 발명의 일실시예에 따르면, 에어갭 환경에서도 효과적으로 광학 신호를 이용하는 공격을 감지할 수 있다.

[0029] 도 2는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 감지 방법을 설명하기 위한 도면이다.

[0030] 본 발명의 일실시예에 따른 공격 감지 방법은 프로세서 및 메모리를 포함하는 컴퓨팅 장치에서 수행될 수 있으며, 전술된 모니터링 장치는 컴퓨팅 장치의 일예일 수 있다.

[0031] 도 2를 참조하면 본 발명의 일실시예에 따른 컴퓨팅 장치는 단말 장치의 광학 신호로부터, 광학 신호의 특징값을 추출(S210)하고, 추출된 특징값을 이용하여, 단말 장치에 대한 공격을 감지(S220)한다.

[0032] 단계 S210에서 컴퓨팅 장치는 일실시예로서, 단말 장치를 포함하는 비디오나 단말 장치의 광학 신호를 감지하는 광센서의 출력값으로부터 특징값을 추출할 수 있다.

[0033] 광학 신호는 비디오의 전체 영역 중 모니터, 저장 장치, 키보드 또는 마우스가 존재하는 위치에서 발생하므로, 광학 신호에 대한 정확한 특징값을 추출하기 위해, 컴퓨팅 장치는 비디오에서, 광학 신호의 발생 영역에 대한 이미지 패치를 추출하고, 추출된 이미지 패치에서, 특징값을 추출할 수 있다. 광학 신호의 발생 영역은 비디오에서 전술된 모니터, 저장 장치, 키보드 또는 마우스를 포함하는 영역일 수 있다. 단말 장치에 대한 비디오를 생성하는 카메라는 고정된 상태에서 단말 장치를 촬영하므로, 비디오의 전체 프레임에서 광학 신호의 발생 영역은 일정하며, 따라서 비디오로부터 용이하게 이미지 패치가 추출될 수 있다. 이미지 패치는 비디오의 프레임 별로 추출될 수 있다.

[0034] 전술된 바와 같이, 특징값은 광학 신호의 점멸 패턴, 주파수 또는 밝기값에 대한 시계열 데이터이며, 컴퓨팅 장치는 이미지 패치를 비디오의 프레임별로 분석하여, 특징값을 추출할 수 있다.

[0035] 예컨대 컴퓨팅 장치는 프레임별 이미지 패치에서 광학 신호가 점등되었는지 꺼져있는지를 분석하여 시계열 데이터 형태의 점멸 패턴을 생성할 수 있다. 제1프레임에 광학 신호가 점등되어 있고, 제2프레임에 광학 신호가 꺼져있고, 다시 제2프레임에 광학 신호가 점등되어 있다면, 101과 같은 시계열 데이터가 생성될 수 있다.

[0036] 또는 컴퓨팅 장치는 프레임별 이미지 패치에서의 화소값에 대한 평균값을 계산하고, 프레임별로 계산된 시계열 형태의 평균값을 밝기값으로 이용할 수 있다. 또는 이미지 패치에 대한 주파수 분석을 통해 주파수 특징값을 추출할 수 있다.

[0037] 단계 S220에서 컴퓨팅 장치는 일실시예로서, 훈련 데이터를 통해 학습된 인공 신경망을 이용하여, 단말 장치에

대한 공격을 감지할 수 있다. 훈련 데이터는 단말 장치의 정상 동작 상태 또는 단말 장치에 대한 공격 상태로부터 획득된 훈련용 광학 신호의 특징값을 포함한다. 이러한 특징값은 전술된 바와 같이 시계열 형태이기 때문에, LSTM 기반의 인공 신경망이 공격 감지에 이용될 수 있다.

[0039] 도 3은 본 발명의 일실시예에 따른 특징값 추출 방법을 설명하기 위한 도면이다.

[0040] 카메라가 단말 장치를 연속적으로 촬영하고 있는 상태에서 생성되는 비디오의 용량은 매우 크며, 따라서 비디오로부터 생성되는 특징값 역시 촬영 시간에 비례하여 증가한다. 이러한 특징값을 이용하여 공격을 감지하는 것은 매우 많은 시간과 비용이 소모되며, 본 발명의 일실시예는 공격 감지에 소요되는 비용과 시간을 줄일 수 있는 특징값 추출 방법을 제안한다.

[0041] 일반적으로 에어갭 환경에서의 공격은, 공격자가 USB 등을 통해 악성 코드를 단말 장치에 감염시키는 행동으로부터 시작되는 점에 착안하여, 본 발명의 일실시예에 따른 컴퓨팅 장치는 사람이 단말 장치에 접근하였는지 여부를 판단(S310)하고, 사람이 단말 장치에 근접한 상태에서, 광학 신호의 특징값을 추출(S320)한다.

[0042] 단계 S310에서 컴퓨팅 장치는 일실시예로서, 비디오에서 사람이 단말 장치를 미리 설정 시간 동안 가리는 경우, 즉 사람이 미리 설정 시간 동안 단말 장치 상에 오버랩된 경우에, 사람이 단말 장치에 접근한 것으로 판단할 수 있다. 또는 컴퓨팅 장치는 사람이 단말 장치로부터 미리 설정된 거리 내에, 미리 설정된 시간 동안 위치한 경우, 사람이 단말 장치에 접근한 것으로 판단할 수 있다.

[0043] 그리고 본 발명의 일실시예에 따른 컴퓨팅 장치는 단말 장치에 대한 공격이 감지되었는지 여부(S330)에 따라, 계속 특징값을 추출하거나, 특징값 추출을 중단할 수 있다. 컴퓨팅 장치는 특징값의 추출이 시작된 이후 미리 설정된 시간 내에 공격이 감지되지 않은 경우, 비디오에서 검출된 사람이 공격자가 아니라고 판단하여 특징값 추출을 중단할 수 있다. 다시 말해, 특징값의 추출이 시작된 이후 미리 설정된 시간 내에 공격이 감지되지 않은 경우에, 컴퓨팅 장치는, 비디오에서 검출된 사람이 공격을 위한 악성 코드를 단말 장치에 감염시키지 않은 것으로 판단하여, 특징값 추출을 중단할 수 있다.

[0044] 공격이 감지된 경우에는, 단말 장치가 악성 코드에 감염된 경우이므로, 컴퓨팅 장치는 지속적으로 특징값을 추출하여 공격을 감지한다.

[0045] 본 발명의 일실시예에 따르면, 사람이 단말 장치에 접근하는 상황과 같이 공격자에 의해 단말 장치가 감염될 수 있는 상황에서 특징값을 추출하고, 공격이 감지되지 않은 경우 특징값 추출을 중단함으로써, 공격 감지에 소요되는 비용과 시간을 줄일 수 있다.

[0047] 도 4는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 감지를 위한 학습 방법을 설명하기 위한 도면이다.

[0048] 본 발명의 일실시예에 따른 학습 방법은 프로세서 및 메모리를 포함하는 컴퓨팅 장치에서 수행될 수 있으며, 전술된 모니터링 장치는 컴퓨팅 장치의 일예일 수 있다.

[0049] 도 4를 참조하면, 본 발명의 일실시예에 따른 컴퓨팅 장치는 훈련용 데이터로부터 특징값을 추출(S410)하고, 인공 신경망을 이용하여, 특징값에 대한 공격 여부를 학습(S420)한다. 여기서, 훈련용 데이터는 단말 장치의 정상 동작 상태 또는 단말 장치에 대한 공격 상태에서 획득된 훈련용 광학 신호를 포함한다.

[0050] 단말 장치의 정상 동작 상태에서 획득된 훈련용 광학 신호로부터 추출된 특징값에는 정상 동작 상태가 레이블링되고, 단말 장치에 대한 공격 상태에서 획득된 훈련용 광학 신호로부터 획득된 특징값에는 공격 상태가 레이블링되어, 인공 신경망에 대한 학습이 이루어질 수 있다. 실시예에 따라서, 단말 장치의 정상 동작 상태 및 단말 장치에 대한 공격 상태에 대한 특징값이 모두 이용되거나 선택적으로 이용되어 학습이 이루어질 수 있다.

[0051] 광학 신호는 단말 장치의 모니터, 저장 장치, 키보드 또는 마우스로부터 생성된 신호이며, 특징값은 광학 신호의 점멸 패턴, 주파수 또는 밝기값에 대한 시계열 데이터일 수 있다.

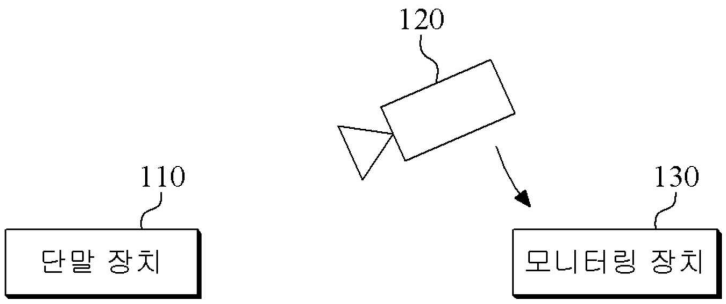
[0053] 앞서 설명한 기술적 내용들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예들을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행

하도록 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. 하드웨어 장치는 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

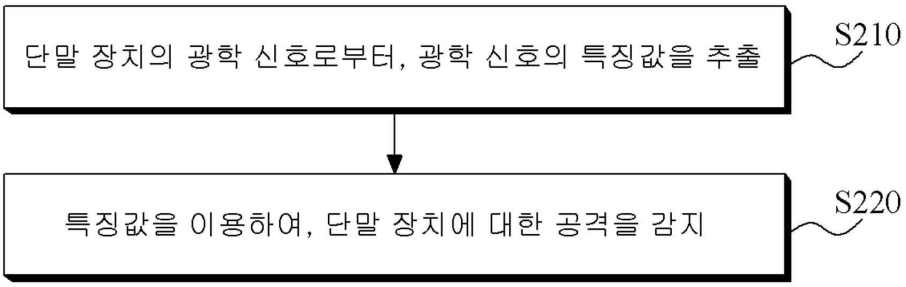
[0055] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

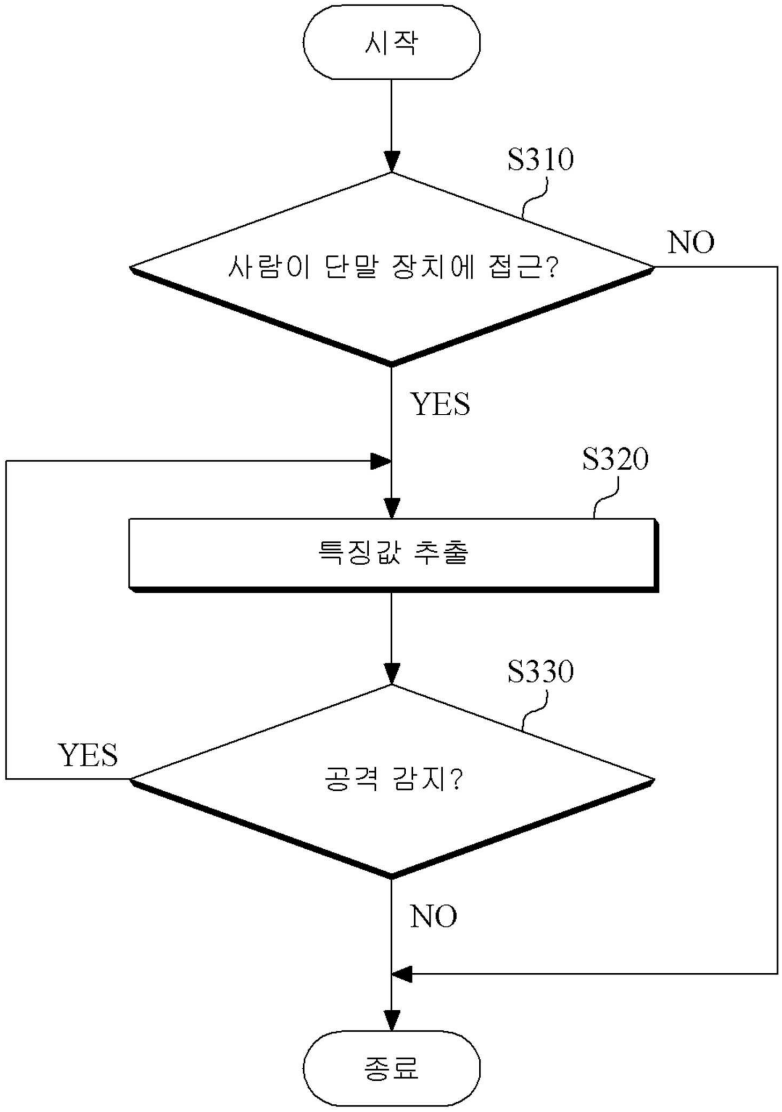
도면1



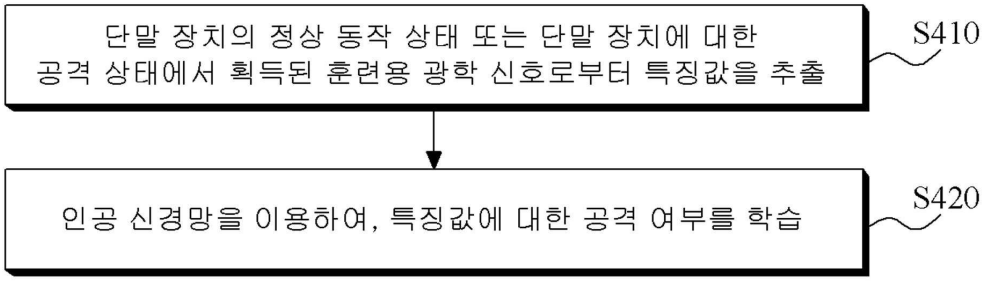
도면2



도면3


시작
S310
사람이 단말 장치에 접근?
NO
YES
S320
특징값 추출
S330
YES
공격 감지?
NO
종료

도면4


단말 장치의 정상 동작 상태 또는 단말 장치에 대한
공격 상태에서 획득된 훈련용 광학 신호로부터 특징값을 추출
S410
인공 신경망을 이용하여, 특징값에 대한 공격 여부를 학습
S420