



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0154169
(43) 공개일자 2024년10월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) G06F 18/21 (2023.01)
G06F 21/71 (2013.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 18/21 (2023.01)
(21) 출원번호 10-2023-0050406
(22) 출원일자 2023년04월18일
심사청구일자 2023년04월18일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
송재승
경기도 성남시
유재훈
경기도 안양시 동안구 관평로212번길 21, 305동 308호(관양동, 공작부영아파트)
(74) 대리인
수안특허법인, 민영준

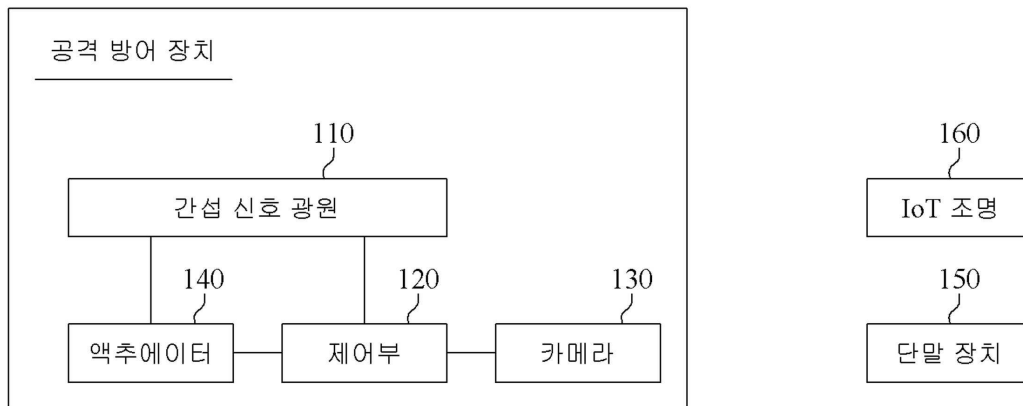
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 에어갭 환경에서의 공격을 방어하는 방법 및 장치

(57) 요약

에어갭 환경에서의 광학 신호를 이용하는 공격을 방어하는 방법 및 장치가 개시된다. 개시된 에어갭 환경에서의 공격을 방어하는 방법은 미리 학습된 공격 감지 모델을 이용하여, 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하는 단계; 및 상기 광학 신호를 이용하는 공격이 감지된 경우, 적어도 하나의 간섭 신호 광원을 이용하여 상기 타겟 장소에 간섭 신호를 출력하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

G06F 21/71 (2013.01)

(72) 발명자

박장용

서울특별시 강동구 상암로 251, 904동 1002호(명일동, 고덕주공아파트)

이지호

서울특별시 중랑구 동일로92길 40, 108동 1203호(면목동, 사가정 센트럴 아이파크)

최유라

경기도 광명시 하안로 284, 1207동 1403호 (하안동, 하안12단지고층주공아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호

1711193096

과제번호

2021-0-00188-003

부처명

과학기술정보통신부

과제관리(전문)기관명

정보통신기획평가원

연구사업명

정보통신방송표준개발지원(R&D, 정보화)

연구과제명

AI 기능 지원 프레임워크 기반의 이기종 IoT 플랫폼 연동 오픈소스 및 국제 표준 개

발

기 여 율

1/1

과제수행기관명

세종대학교 산학협력단

연구기간

2023.01.01 ~ 2023.12.31

명세서

청구범위

청구항 1

미리 학습된 공격 감지 모델을 이용하여, 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하는 단계; 및
상기 광학 신호를 이용하는 공격이 감지된 경우, 적어도 하나의 간접 신호 광원을 이용하여 상기 타겟 장소에
간접 신호를 출력하는 단계
를 포함하는 에어갭 환경에서의 공격을 방어하는 방법.

청구항 2

제 1항에 있어서,

상기 광학 신호의 광원은

상기 타겟 장소에 위치하는 단말 장치의 모니터, 저장 장치 램프, 키보드 램프, 마우스 램프, 상기 타겟 장소의
IoT 조명 또는 인터넷 전화 램프

를 포함하는 에어갭 환경에서의 공격을 방어하는 방법.

청구항 3

제 2항에 있어서,

상기 타겟 장소에 간접 신호를 출력하는 단계는

상기 광학 신호의 광원의 크기에 따라서, 상기 간접 신호 광원을 선택하여 간접 신호를 출력하는

에어갭 환경에서의 공격을 방어하는 방법.

청구항 4

제 3항에 있어서,

상기 타겟 장소에 간접 신호를 출력하는 단계는

상기 광학 신호의 광원이 상기 저장 장치 램프, 키보드 램프, 마우스 램프, 인터넷 전화 램프 또는 상기 타겟
장소의 IoT 조명인 경우, 상기 광학 신호의 광원으로 레이저빔을 조사하는

에어갭 환경에서의 공격을 방어하는 방법.

청구항 5

제 3항에 있어서,

상기 타겟 장소에 간접 신호를 출력하는 단계는

상기 광학 신호의 광원이 상기 단말 장치의 모니터인 경우, 상기 IoT 조명 또는 상기 모니터보다 광량이 많은
간접 신호 광원의 빛을 출력하는

에어갭 환경에서의 공격을 방어하는 방법.

청구항 6

제 5항에 있어서,
상기 간섭 신호 광원은
플래시 라이트 또는 서치 라이트인
에어갭 환경에서의 공격을 방어하는 방법.

청구항 7

제 1항에 있어서,
상기 광학 신호를 이용하는 공격을 감지하는 단계는
상기 광학 신호를 통해 전송되는 데이터의 전송 주기를 추정하며,
상기 타겟 장소에 간섭 신호를 출력하는 단계는
상기 전송 주기에 따라서, 상기 간섭 신호를 출력하는
에어갭 환경에서의 공격을 방어하는 방법.

청구항 8

제 7항에 있어서,
상기 타겟 장소에 간섭 신호를 출력하는 단계는
상기 전송 주기의 정수배 주기로, 상기 간섭 신호를 출력하는
에어갭 환경에서의 공격을 방어하는 방법.

청구항 9

제 1항에 있어서,
상기 광학 신호를 이용하는 공격을 감지하는 단계는
상기 타겟 장소에 대한 영상으로부터 상기 광학 신호에 대한 특징값을 추출하는 단계; 및
상기 특징값으로부터 상기 광학 신호를 이용하는 공격을 감지하는 단계
를 포함하는 에어갭 환경에서의 공격을 방어하는 방법.

청구항 10

적어도 하나의 간섭 신호 광원; 및
타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하고, 공격 감지 결과에 따라서, 상기 간섭 신호 광원의 출력을 제어하는 제어부
를 포함하는 에어갭 환경에서의 공격을 방어하는 장치.

청구항 11

제 10항에 있어서,
상기 간섭 신호 광원은
상기 광학 신호의 광원보다 광량이 많은 광원 또는 레이저 광원
을 포함하는 에어갭 환경에서의 공격을 방어하는 장치.

청구항 12

제 11항에 있어서,
상기 레이저 광원은
상기 광학 신호의 광원을 향해 레이저빔이 출력되도록, 배치되는
에어갭 환경에서의 공격을 방어하는 장치.

청구항 13

제 11항에 있어서,
상기 광학 신호의 광원 위치에 따라서, 상기 레이저 광원의 레이저빔 출력 방향을 조절하는 액츄에이터
를 더 포함하는 에어갭 환경에서의 공격을 방어하는 장치.

청구항 14

제 11항에 있어서,
상기 제어부는
상기 광학 신호의 광원의 크기에 따라서, 상기 간섭 신호를 출력하는 간섭 신호 광원을 선택하는
에어갭 환경에서의 공격을 방어하는 장치.

청구항 15

제 11항에 있어서,
상기 제어부는
상기 광학 신호를 통해 전송되는 데이터의 전송 주기에 따라서, 상기 간섭 신호 광원의 출력 주기를 제어하는
에어갭 환경에서의 공격을 방어하는 장치.

발명의 설명

기술 분야

본 발명은 에어갭 환경에서의 공격을 방어하는 방법 및 장치에 관한 것으로서, 더욱 상세하게는 광학 신호를 이용하는 공격을 방어하는 방법 및 장치에 관한 것이다.

[0001]

배경 기술

- [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 모니터나, LED 등 다양한 광원의 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 등록특허 제10-2509322호, 제10-2424619호, 비특허 문헌인, "에어 갭 네트워크 정보유출기법 분석과 대응개념에 관한 연구, 김기현, 김용철, 한국통신학회, 2019"가 있다.

발명의 내용

해결하려는 과제

- [0007] 본 발명은 에어갭 환경에서 광학 신호를 이용한 공격을 무력화시킬 수 있는 방어 방법 및 장치를 제공하기 위한 것이다.
- [0008] 또한 본 발명은 이동형으로 구현되어 다양한 장소에서 활용될 수 있는, 에어갭 환경에서의 공격을 방어하는 장치를 제공하기 위한 것이다.

과제의 해결 수단

- [0010] 상기한 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 미리 학습된 공격 감지 모델을 이용하여, 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하는 단계; 및 상기 광학 신호를 이용하는 공격이 감지된 경우, 적어도 하나의 간섭 신호 광원을 이용하여 상기 타겟 장소에 간섭 신호를 출력하는 단계를 포함하는 에어갭 환경에서의 공격을 방어하는 방법이 제공된다.
- [0011] 또한 상기한 목적을 달성하기 위한 본 발명의 다른 실시예에 따르면, 적어도 하나의 간섭 신호 광원; 및 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하고, 공격 감지 결과에 따라서, 상기 간섭 신호 광원의 출력을 제어하는 제어부를 포함하는 에어갭 환경에서의 공격을 방어하는 장치가 제공된다.

발명의 효과

- [0013] 본 발명의 일실시예에 따르면, 간섭 신호에 의해 타겟 장소에 대한 영상에서 광학 신호가 식별되기 어려우므로, 타겟 장소에 대한 영상의 촬영 장소와 무관하게, 광학 신호를 이용하는 공격이 효과적으로 차단될 수 있다.
- [0014] 또한 본 발명의 일실시예에 따르면, 사용자가 방어할 필요가 있는 타겟 장소로, 공격 방어 장치를 이동시킬 수 있으므로, 장소에 구애됨이 없이 광학 신호를 이용하는 공격이 효과적으로 차단될 수 있다.

도면의 간단한 설명

- [0016] 도 1은 본 발명의 일실시예에 따른 에어갭 환경에서의 공격을 방어하는 장치를 설명하기 위한 도면이다.
- 도 2는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격을 방어하는 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.
- [0019] 연구실과 같은 특정 장소가 에어갭 환경인 경우, 전술된 바와 같이 공격자는 광학 신호를 이용하여 정보를 탈취할 수 있다. 공격자는 연구실과 같은, 공격을 위한 타겟 장소의 단말 장치를 악성 코드에 감염시키고, 타겟 장소에 위치하는 광원의 광학 신호로부터 정보를 탈취할 수 있다. 광학 신호의 광원은, 타겟 장소에 위치하는 단말 장치의 모니터, 저장 장치 램프, 키보드 램프, 마우스 램프, 타겟 장소의 IoT 조명, 인터넷 전화 램프 등일 수 있다.
- [0020] 악성 코드에 감염된 단말 장치는 모니터의 주사율을 조절하거나, 모니터에 특정 이미지나 QR 코드를 표시하여 공격자에게 데이터를 전송할 수 있다. 또는 악성 코드에 감염된 단말 장치는 저장 장치, 키보드 또는 마우스의 램프의 점등 패턴, 밝기 등을 조절하여 데이터를 전송하거나, IoT 조명의 점등 패턴, 밝기, 주파수 등을 조절하여 데이터를 전송할 수 있다. 그리고 공격자는 타겟 장소에 설치된 CCTV의 영상이나, 타겟 장소의 외부에서 타겟 장소를 촬영한 영상 등에 포함된 광학 신호를 디코딩함으로써 데이터를 탈취할 수 있다.
- [0021] 본 발명은 이러한 에어갭 환경에서 광학 신호를 이용하는 공격을 무력화시키기 위해, 간섭 신호를 이용한다. 광학 신호를 이용하는 공격을 무력화시키기 위해, CCTV를 비활성화시키거나 외부에서 타겟 장소를 촬영할 수 없도록 창문을 폐쇄하는 등의 방어 방법이 이용될 수 있다. 하지만, 이러한 방어 방법은 타겟 장소에 대한 영상의 촬영 장소에 따라서 선택적으로만 활용될 수 있다. 이에 본 발명은 타겟 장소에 대한 영상의 촬영 장소와 무관하게, 광학 신호를 이용하는 공격이 효과적으로 차단될 수 있도록 간섭 신호를 이용한다.
- [0022] 본 발명의 일실시예는 광학 신호를 이용하는 공격이 감지되는 경우 타겟 신호에 간섭 신호를 출력한다. 따라서 타겟 장소에 대한 영상에는 광학 신호 뿐만 아니라 간섭 신호도 포함되므로, 공격자는 타겟 장소에 대한 영상에 포함된 광학 신호를 디코딩하여 데이터를 탈취하기 어려우며, 광학 신호를 이용하는 공격이 무력화될 수 있다.
- [0023] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.
- [0025] 도 1은 본 발명의 일실시예에 따른 에어갭 환경에서의 공격을 방어하는 장치를 설명하기 위한 도면이다.
- [0026] 도 1을 참조하면, 본 발명의 일실시예에 따른 공격 방어 장치는 적어도 하나의 간섭 신호 광원(110) 및 제어부(120)를 포함하며, 실시예에 따라서 카메라(130)나 광센서, 액츄에이터(140) 등을 더 포함할 수 있다. 공격 방어 장치는, 공격 방어 장치의 전방이, 타겟 장소에 위치하는 광학 신호의 광원을 향하도록 설치될 수 있으며, 카메라(130)나 광센서, 간섭 신호 광원(110) 등은 공격 방어 장치의 전방 방향을 향하도록, 공격 방어 장치에 포함될 수 있다. 공격 방어 장치는 이동 가능한 박스 형태로 구현될 수 있으며, 사용자는 방어할 필요가 있는 타겟 장소로, 공격 방어 장치를 이동시킬 수 있다.
- [0027] 제어부(120)는 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지하고, 공격 감지 결과에 따라서, 간섭 신호 광원(110)의 출력을 제어한다. 타겟 장소는 에어갭 환경이며, 제어부(120)는 미리 학습된 공격 감지 모델을 이용해 광학 신호를 이용하는 공격을 감지할 수 있다.
- [0028] 공격 감지 모델은 타겟 장소에 대한 영상으로부터 광학 신호의 특징값을 추출하고, 특징값으로부터 광학 신호를 이용하는 공격을 감지할 수 있다. 공격 감지 모델의 학습에는 이러한 특징값이 이용될 수 있다. 타겟 장소에 대한 영상은 타겟 장소의 CCTV 영상이거나 또는 공격 방어 장치에 포함된 카메라(130)에서 촬영된 영상일 수 있다.
- [0029] 또는 공격 감지 모델은 광센서의 센싱값으로부터 광학 신호의 특징값을 추출하고, 특징값으로부터 광학 신호를 이용하는 공격을 감지할 수 있다.
- [0030] 광학 신호의 광원은, 타겟 장소에 위치하는 단말 장치(150)의 모니터, 저장 장치 램프, 키보드 램프, 마우스 램프, 타겟 장소의 IoT 조명(160), 인터넷 전화 램프 등을 포함할 수 있으며, 특징값은 일실시예로서, 광학 신호의 점멸 패턴, 주파수 또는 밝기값 등일 수 있다.
- [0031] 단말 장치(130)가 정상적으로 동작하는 상태에서의 광원의 점멸 패턴, 주파수 또는 밝기값은, 공격 상태에서의

광원의 점멸 패턴, 주파수 또는 밝기값과 다를 수 있다. 예컨대 정상적으로 동작하는 광원의 점멸 패턴은 불규칙하지만, 공격 상태에서 광원은 규칙적이며 일예로 모스 부호나 이진 코드에 대응되도록 점멸될 수 있다. 또는 공격 상태에서 광원의 밝기가 이진 코드에 대응되도록 변화할 수 있다. 따라서, 공격 감지 모델은 광학 신호의 특징값으로부터 광학 신호를 이용하는 공격을 감지할 수 있다.

[0032] 제어부(120)는 광학 신호를 이용하는 공격이 감지된 경우, 간섭 신호 광원(110)의 간섭 신호의 출력을 제어한다. 간섭 신호 역시 광학 신호와 같은 광 신호로서, 간섭 신호 광원(110)은 일실시예로서, 플래시 라이트나 서치 라이트와 같이, 광학 신호의 광원보다 광량이 많은 광원이거나 또는 레이저 광원일 수 있다. 레이저 광원은 광학 신호의 광원을 향해 레이저빔이 출력되도록, 배치될 수 있다.

[0033] 또한 제어부(120)는 광학 신호의 광원의 크기에 따라서, 간섭 신호를 출력하는 간섭 신호 광원을 선택할 수 있으며, 또는 광학 신호를 통해 전송되는 데이터의 전송 주기에 따라서, 간섭 신호 광원의 출력 주기를 제어할 수 있다.

[0034] 한편, 상황에 따라서 광학 신호의 광원의 위치는 달라질 수 있기 때문에, 본 발명의 일실시예는 액츄에이터(140)를 이용하여, 간섭 신호 광원의 출력 방향을 제어할 수 있다. 액츄에이터(140)는 광학 신호의 광원 위치에 따라서, 레이저 광원의 레이저빔 출력 방향을 조절할 수 있다.

[0035] 제어부(120)는 타겟 장소에 대한 영상이나 광센서의 센싱값으로부터, 광학 신호의 광원의 위치를 추정할 수 있으며, 액츄에이터(140)는 추정된 위치에 따라서 간섭 신호 광원의 출력 방향을 조절할 수 있다.

[0036] 제어부(120)는 광학 신호를 이용하는 공격이 감지된 경우, 전송된 바와 같이 간섭 신호를 출력할 뿐만 아니라, 미리 지정된 관리자나 제어 센터로 공격 사실을 통지할 수 있다. 관리자는 단말 장치의 악성 코드를 제거한 후, 간섭 신호의 출력을 리셋시킬 수 있다.

[0037] 본 발명의 일실시예에 따르면, 간섭 신호에 의해 타겟 장소에 대한 영상에서 광학 신호가 식별되기 어려우므로, 타겟 장소에 대한 영상의 촬영 장소와 무관하게, 광학 신호를 이용하는 공격이 효과적으로 차단될 수 있다.

[0039] 도 2는 본 발명의 일실시예에 따른 에어갭 환경에서의 공격을 방어하는 방법을 설명하기 위한 도면으로서, 공격 방어 방법은 프로세서 및 메모리를 포함하는 컴퓨팅 장치에서 수행될 수 있으며, 전송된 공격 방어 장치는 이러한 컴퓨팅 장치의 일예이다. 도 2에서는 전송된 공격 방어 장치의 공격 방어 방법이 일실시예로서 설명된다.

[0040] 도 2를 참조하면, 본 발명의 일실시예에 따른 공격 방어 장치는 미리 학습된 공격 감지 모델을 이용하여, 타겟 장소에 대한 광학 신호를 이용하는 공격을 감지(S210)한다. 공격 방어 장치는 타겟 장소에 대한 영상으로부터 광학 신호에 대한 특징값을 추출하고, 추출된 특징값으로부터 광학 신호를 이용하는 공격을 감지할 수 있다.

[0041] 또한 공격 방어 장치는 단계 S210에서 광학 신호를 통해 전송되는 데이터의 전송 주기를 추정할 수 있다. 예컨대 광학 신호의 광원이 50ms 주기로 점등되는 경우, 공격 방어 장치는 전송 주기를 50ms로 추정할 수 있다. 이를 위해 공격 감지 모델은 광학 신호를 이용하는 공격뿐만 아니라, 전송 주기를 추정할 수 있도록 학습될 수 있다. 공격 감지 모델은 미리 설정된 전송 주기에 따라 점등 되는 광학 신호를 통해, 전송 주기를 추정할 수 있도록, 학습될 수 있다.

[0042] 본 발명의 일실시예에 따른 공격 방어 장치는 단계 S210에서 광학 신호를 이용하는 공격이 감지된 경우, 적어도 하나의 간섭 신호 광원을 이용하여 타겟 장소에 간섭 신호를 출력(S220)한다.

[0043] 공격 방어 장치는 광학 신호의 광원의 크기에 따라서, 간섭 신호를 출력하는 간섭 신호 광원을 선택하여 간섭 신호를 출력할 수 있다. 예컨대, 광학 신호의 광원이 단말 장치의 저장 장치 램프, 키보드 램프, 마우스 램프, 타겟 장소의 IoT 조명, 인터넷 전화 램프 등과 같이 소형인 경우, 공격 방어 장치는 레이저 광원을 간섭 신호 광원으로 선택하여, 광학 신호의 광원으로 레이저빔을 조사할 수 있다.

[0044] 반면, 광학 신호의 광원이 단말 장치의 모니터와 같이 대형인 경우, 공격 방어 장치는 타겟 장소의 IoT 조명 또는 모니터보다 광량이 많은 간섭 신호 광원을 선택하여, 선택된 간섭 신호 광원의 빛을 출력할 수 있다. 공격 방어 장치는 예컨대, 플래시 라이트나 서치 라이트와 같은 광원의 빛을 출력할 수 있다.

[0045] 레이저빔이 광학 신호의 광원으로 조사되는 경우, 타겟 장소에 대한 영상에서 광학 신호의 광원은 항상 점등된 형태로 표시될 것이므로, 공격자는 타겟 장소에 대한 영상에서 광학 신호를 디코딩하여 데이터를 탈취할 수 없다. 또한 플래시 라이트나 서치 라이트와 같은 광원의 밝은 빛이 출력되는 경우, 타겟 장소에 대한 영상에서 모

니터의 빛이 인식되기 어려우므로, 공격자는 타겟 장소에 대한 영상에서 광학 신호를 디코딩하여 데이터를 탈취할 수 없다.

[0046] 공격 방어 장치는 실시예에 따라서, 광학 신호를 통해 전송되는 데이터의 전송 주기를 이용하여 간섭 신호를 출력할 수 있다. 공격 방어 장치는 전송 주기의 정수배 주기로 간섭 신호를 출력할 수 있으며, 전송된 예시와 같이 광학 신호의 광원이 50ms 주기로 점등되는 경우, 공격 방어 장치는 전송 주기를 50ms의 두배인 100ms로 간섭 신호를 출력할 수 있다.

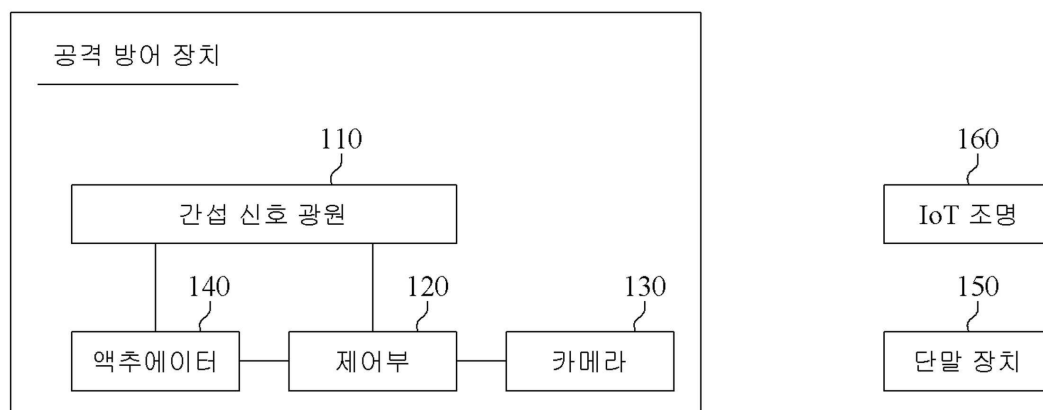
[0047] 따라서, 광학 신호의 광원을 통해 전송되는 데이터가 1010이라서, 광학 신호의 광원이 턴온, 턴오프, 턴온, 턴오프되는 경우, 간섭 신호에 의해 타겟 장소에 대한 영상에서의 광학 신호의 광원은 턴온, 턴온, 턴온, 턴온되는 것으로 인식되기 때문에, 공격자는 광학 신호를 디코딩하여 데이터를 탈취할 수 없다.

[0049] 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 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. 하드웨어 장치는 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0051] 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 특허청구범위뿐만 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

도면1



도면2

