(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0152679
(43) 공개일자 2021년12월16일

(51) 국제특허분류(Int. Cl.)
G06K 9/32 (2006.01) *G06N 3/08* (2006.01)
(52) CPC특허분류
G06K 9/3258 (2013.01)
G06N 3/08 (2013.01)
(21) 출원번호 10-2020-0069459
(22) 출원일자 2020년06월09일
심사청구일자 2020년06월09일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
이우기
경기도 군포시 산본로432번길 25, 1222동 1302호 (산본동, 한양목련아파트)
이효준
인천광역시 미추홀구 소성로 16, 629호(용현동, 인하아리스타오피스텔)
(뒷면에 계속)
(74) 대리인
양성보

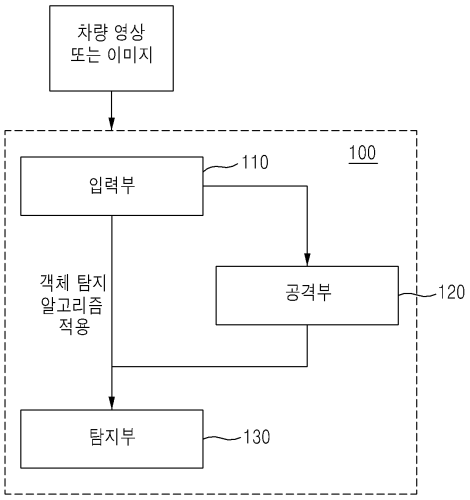
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **강화된 차량 번호판 자동탐지 시스템**

(57) 요 약

강화된 차량 번호판 자동탐지 시스템이 개시된다. 일 실시예에 따른 탐지 시스템에 의해 수행되는 강화된 차량 번호판 자동탐지 방법은, 영상 정보가 입력됨을 수신하는 단계; 상기 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성하는 단계; 및 상기 수신된 영상 정보와 관련된 정상 데이터 및 상기 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지하는 단계를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06K 2209/15 (2013.01)
(72) 발명자
이철기
서울특별시 영등포구 당산로 1(문래동3가)

강명철
경기도 성남시 분당구 판교역로 49, 907동 702호(백현동, 백현마을 아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 1345304925
과제번호 2019S1A5C2A03081234
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 대학중점연구소지원사업
연구과제명 플랫폼 기반 공공서비스 체제와 스마트시티 사회보안 거버넌스 연구 (1차년도)
기 여 율 1/2
과제수행기관명 인하대학교
연구기간 2019.09.01 ~ 2020.08.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711103369
과제번호 2019-0-00136-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 방송통신산업기술개발사업
연구과제명 [Ezbaro] 스마트시티 산업 생산성 혁신을 위한 AI융합 기술 개발(2차년도)
기 여 율 1/2
과제수행기관명 세종대학교 산학협력단
연구기간 2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

탐지 시스템에 의해 수행되는 강화된 차량 번호판 자동탐지 방법에 있어서,

영상 정보가 입력됨을 수신하는 단계;

상기 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성하는 단계; 및

상기 수신된 영상 정보와 관련된 정상 데이터 및 상기 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지하는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 2

제1항에 있어서,

상기 공격 데이터를 생성하는 단계는,

상기 수신된 영상 정보를 이용하여 탐지 혹은 오탐지를 유발하는 임의의 노이즈(noise), 섭동(perturbation) 또는 변형(transformation)시켜 공격 데이터를 생성하는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 3

제1항에 있어서,

상기 입력하는 단계는,

상기 수신된 영상 정보를 통해 번호판을 탐지하기 위한 객체 탐지 모델을 구성하고, 상기 수신된 영상 정보를 의미하는 정상 데이터 및 상기 수신된 영상 정보에 대한 공격 데이터를 훈련 데이터로 사용하여 상기 구성된 객체 탐지 모델을 학습시키는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 4

제1항에 있어서,

상기 구성된 객체 탐지 모델은, 딥러닝 기술 분야 중 객체 탐지(Object Detection) 알고리즘이 적용된 것으로, 상기 수신된 영상 정보의 차량 영역으로부터 번호판으로 보이는 객체 영역을 탐지하기 위한 것인, 강화된 차량 번호판 자동탐지 방법.

청구항 5

제3항에 있어서,

상기 입력하는 단계는,

상기 학습된 객체 탐지 모델에 차량 번호판을 탐지하기 위한 차량 영상 정보를 입력하는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 6

제1항에 있어서,

상기 입력하는 단계는,

상기 탐지된 차량 번호판을 출력하는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 7

제1항에 있어서,

상기 수신하는 단계는,

서로 다른 각도에서 촬상된 또는 입력된 번호판 영역을 포함하는 영상 정보 또는 이미지 데이터를 수신하는 단계

를 포함하는 강화된 차량 번호판 자동탐지 방법.

청구항 8

강화된 차량 번호판 자동탐지하기 위한 탐지 시스템에 있어서,

영상 정보가 입력됨을 수신하는 입력부;

상기 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성하는 공격부; 및

상기 수신된 영상 정보와 관련된 정상 데이터 및 상기 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지하는 탐지부

를 포함하는 탐지 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 강화된 차량 번호판 자동탐지 시스템 또는 그 방법에 관한 것으로서, 더욱 상세하게는 번호판을 자동으로 탐지할 때 이를 무력하기 위한 공격을 방어 및 최소화할 수 있는 차량 번호판 자동탐지 시스템 또는 그 방법에 관한 것이다.

배 경 기 술

[0003] 최근 인공지능 기술의 발전과 더불어 차량 번호판 인식 시스템에 다양한 방식을 통해 단속 카메라와 톨게이트 카메라 시스템, 무인 주차 시스템 등에 사용되는 차량 번호판 인식의 경우 영상 또는 이미지를 통해 처리하여 이루어진다.

[0004] 영상에서 차량 번호판을 인식하는 것은 크게 두 단계로 나누어서 진행된다. 차량을 인식하여 차량 내의 번호판을 인식하는 단계가 있고, 다음으로 인식한 차량 번호판의 글자 및 숫자를 인식하는 단계이다. 이 두 단계를 거쳐서 차량 번호판을 인식하는 것은 경제적, 사회적, 기술적으로 중요한 문제이다. 또한, 인식 정확도가 100%에 이르도록 결과가 도출되는 것을 목표로 한다.

[0005] 하지만, 정확도가 우수한 인공지능을 활용한 차량 번호판 인식 시스템이라 하더라도, 악의적 의도를 갖고 번호판 인식을 어렵게 하려고 물리적인 공격을 통해 변형하거나, 기타 광원을 송출하여 카메라를 교란하는 형태 등의 방법을 통해 인식을 방해하는 사례가 존재한다. 만일, 육안으로는 이러한 악의적인 방법을 구별할 수 없으면서 인공지능이 인식하지 못하는 공격을 할 때 이를 방어하기란 매우 어렵다. 하지만, 이러한 인공지능의 약점을 이용한 공격을 방어할 수 있는 차량 번호판을 개발한다면, 악의적인 공격에 대한 피해를 상당히 줄일 수 있다.

[0006] 따라서 차량 번호판 탐지를 방해하는 공격에 대응하기 위해 새로운 차량 번호판 탐지 시스템 혹은 방법을 제공하는 데 있어, 실제 인식률을 떨어뜨리는 공격을 방어하여 탐지율을 최대화하는 기법이 요구된다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 향후 딥러닝을 활용한 차량 번호판 탐지 시스템에 가해질 악의적인 목적의 공격을 사전에 차단하거나, 최소화하기 위함에 있다. 상세하게는, 차량 번호 탐지에 대한 공격이 있을 때, 차량 번호판을 탐지함에 있어, 차량 번호판을 탐지하지 못하거나 다른 물체 혹은 객체로 탐지할 가능성을 최소화하는 강화된 차량 번호판 탐지 시스템 또는 그 방법을 제공하는 데 목적이 있다.

과제의 해결 수단

[0010] 탐지 시스템에 의해 수행되는 강화된 차량 번호판 자동탐지 방법은, 영상 정보가 입력됨을 수신하는 단계; 상기 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성하는 단계; 및 상기 수신된 영상 정보와 관련된 정상 데이터 및 상기 수신된 영상 정보와 관련하여 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지하는 단계를 포함할 수 있다.

[0011] 상기 공격 데이터를 생성하는 단계는, 상기 수신된 영상 정보를 이용하여 탐지 혹은 오탐지를 유발하는 임의의 노이즈(noise), 섭동(perturbation) 또는 변형(transformation)시켜 공격 데이터를 생성하는 단계를 포함할 수 있다.

[0012] 상기 입력하는 단계는, 상기 수신된 영상 정보를 통해 번호판을 탐지하기 위한 객체 탐지 모델을 구성하고, 상기 수신된 영상 정보를 의미하는 정상 데이터 및 상기 수신된 영상 정보에 대한 공격 데이터를 훈련 데이터로 사용하여 상기 구성된 객체 탐지 모델을 학습시키는 단계를 포함할 수 있다.

[0013] 상기 구성된 객체 탐지 모델은, 딥러닝 기술 분야 중 객체 탐지(Object Detection) 알고리즘이 적용된 것으로, 상기 수신된 영상 정보의 차량 영역으로부터 번호판으로 보이는 객체 영역을 탐지하기 위한 것일 수 있다.

[0014] 상기 입력하는 단계는, 상기 학습된 객체 탐지 모델에 차량 번호판을 탐지하기 위한 차량 영상 정보를 입력하는 단계를 포함할 수 있다.

[0015] 상기 입력하는 단계는, 상기 탐지된 차량 번호판을 출력하는 단계를 포함할 수 있다.

[0016] 상기 수신하는 단계는, 서로 다른 각도에서 촬상된 또는 입력된 번호판 영역을 포함하는 영상 정보 또는 이미지 데이터를 수신하는 단계를 포함할 수 있다.

[0017] 강화된 차량 번호판 자동탐지하기 위한 탐지 시스템은, 영상 정보가 입력됨을 수신하는 입력부; 상기 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성하는 공격부; 및 상기 수신된 영상 정보와 관련된 정상 데이터 및 상기 수신된 영상 정보와 관련하여 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지하는 탐지부를 포함할 수 있다.

발명의 효과

[0019] 본 발명은 강화된 차량 번호판 탐지 시스템 또는 그 방법을 활용하는 데 있어 적대적 공격 방어 딥러닝 기법을 활용하여 번호판 미탐지 및 오탐지에 대응하여 올바른 결과를 제공함으로써 공격자의 악의적인 공격을 무력화할 수 있는 이점이 있다.

[0020] 본 발명은 강화된 차량 번호판 탐지 시스템 또는 그 방법을 활용하는 데 있어 오탐지율을 현저히 줄이고, 적대적 공격으로 인한 오탐지가 확인되었을 때 발생되는 추가적인 비용을 감소시킬 수 있다.

도면의 간단한 설명

[0022] 도 1은 일 실시예에 따른 탐지 시스템의 구성을 설명하기 위한 블록도이다.

도 2는 일 실시예에 따른 탐지 시스템에서 강화된 차량 번호판 자동탐지 방법을 설명하기 위한 흐름도이다.

도 3은 일 실시예에 따른 탐지 시스템에서 적대적 공격을 가한 데이터의 예이다.

도 4는 일 실시예에 따른 탐지 시스템에서 영상 정보로부터 공격 데이터를 생성하는 것을 설명하기 위한 도면이다.

도 5는 일 실시예에 따른 탐지 시스템에서 객체 탐지 모델을 생성하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0025] 도 1은 일 실시예에 따른 탐지 시스템의 구성을 설명하기 위한 블록도이고, 도 2는 일 실시예에 따른 탐지 시스템에서 강화된 차량 번호판 자동탐지 방법을 설명하기 위한 흐름도이다.

[0026] 탐지 시스템(100)은 입력부(110), 공격부(220) 및 탐지부(230)를 포함할 수 있다. 이러한 탐지 시스템(100)의 구성요소들은 탐지 시스템(100)에 저장된 프로그램 코드가 제공하는 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 탐지 시스템(100) 및 탐지 시스템(100)의 구성요소들은 도 2의 강화된 차량 번호판 자동탐지 방법이 포함하는 단계들(210 내지 230)을 수행하도록 탐지 시스템을 제어할 수 있다. 이때, 탐지 시스템(100) 및 탐지 시스템(100)의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0027] 프로세서는 강화된 차량 번호판 자동탐지 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로딩할 수 있다. 예를 들면, 탐지 시스템에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로딩하도록 탐지 시스템을 제어할 수 있다. 이때, 탐지 시스템(100) 및 탐지 시스템(100)이 포함하는 입력부(210), 공격부(220) 및 탐지부(230) 각각은 메모리에 로딩된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(210 내지 230)을 실행하기 위한 탐지 시스템(100)의 서로 다른 기능적 표현들일 수 있다.

[0028] 단계(210)에서 입력부(110)는 영상 정보가 입력됨을 수신할 수 있다. 입력부(110)는 다른 각도에서 촬상된 또는 입력된 번호판 영역을 포함하는 영상 정보 또는 이미지 데이터를 수신할 수 있다. 예를 들면, 영상 정보 또는 이미지 데이터를 저장(장치)소 혹은 데이터베이스에 입력되어 저장될 수 있다.

[0029] 단계(220)에서 공격부(120)는 수신된 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성할 수 있다. 공격부(120)는 수신된 영상 정보를 이용하여 탐지 혹은 오탐지를 유발하는 임의의 노이즈(noise), 섭동(perturbation) 또는 변형(transformation)시켜 공격 데이터를 생성할 수 있다.

[0030] 단계(230)에서 탐지부(230)는 수신된 영상 정보와 관련된 정상 데이터 및 생성된 공격 데이터를 이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상 정보로부터 차량 번호판을 탐지할 수 있다. 탐지부(230)는 수신된 영상 정보를 통해 번호판을 탐지하기 위한 객체 탐지 모델을 구성하고, 수신된 영상 정보를 의미하는 정상 데이터 및 수신된 영상 정보에 대한 공격 데이터를 훈련 데이터로 사용하여 구성된 객체 탐지 모델을 학습시킬 수 있다. 이때, 구성된 객체 탐지 모델은, 딥러닝 기술 분야 중 객체 탐지(Object Detection) 알고리즘이 적용된 것으로, 수신된 영상 정보의 차량 영역으로부터 번호판으로 보이는 객체 영역을 탐지하기 위한 것일 수 있다. 탐지부(230)는 학습된 객체 탐지 모델에 차량 번호판을 탐지하기 위한 차량 영상 정보를 입력할 수 있다. 탐지부(230)는 탐지된 차량 번호판을 출력할 수 있다.

[0031] 도 3은 일 실시예에 따른 탐지 시스템에서 적대적 공격을 가한 데이터의 예이다.

[0032] 탐지 시스템은 영상 정보에 적대적 공격 방식을 적용하여 공격 데이터를 생성할 수 있다. 탐지 시스템은 영상 정보를 이용하여 탐지 혹은 오탐지를 유발하는 임의의 노이즈(noise), 섭동(perturbation) 또는 변형(transformation)시켜 공격 데이터를 생성할 수 있다.

[0033] 구체적으로, 적대적 공격(Adversarial attack)이란, 어떤 특정 노이즈 혹은 섭동(perturbation)을 분류 모델에 적용하여 모델의 정확도를 감소시키는 방법을 의미한다. 실시예에서는 다양한 방법론 중 FGSM, C&W, 그리고 PGD이 사용될 수 있으며, 특정 공격 방법에 제한되지 않는다. 적대적 공격의 지표(Baseline)가 되는 FGSM은 Ian Goodfellow에 의해 2014년 처음 소개된 바 있다. FGSM은 기존 신경망의 학습 방법인 경사 하강법(GradientDescent) 방식을 역으로 진행하는 방식이라 할 수 있으며, 비용함수(CostGradient)의 부호(Sign)방향

으로 손실함수(loss function)을 증가하도록 학습을 진행한다.

[0034] 수학식 1:

[0035] $$x = x + \epsilon \cdot sign(\nabla_x J(\theta, x, y))$$

[0036] 수학식 1에서 ϵ 가 커지면, 사람이 인지할 만큼의 노이즈가 추가된다고 해석될 수 있는데, 최적의 섭동을 찾아 학습을 진행하는 것이 분류기(Classifier)를 효과적으로 방해하는 공격이라고 할 수 있다.

[0037] C&W는 Carlini와 Wagner가 제안한 공격 방법으로 FGSM만큼이나 자주 사용되는 공격방식이다. 크게 세 가지의 공격 방법으로 $L0$, $L2$ 그리고 $L\infty$ 공격을 제안함으로써 섭동의 크기를 더 작게 만들어 공격을 가하는 방법이다. 이전 공격 방법들보다 섭동의 크기는 작지만, 높은 성능을 보여주는 C&W는 적대적 공격의 방어 방법으로 제시되었던 Defensive Distillation의 한계를 지적하며, 공격을 성공적으로 진행한 강력한 방법이다.

[0038] Madry에 의하여 MinMax 함수를 적용하여 적대적 공격을 가하고 해당 공격을 적대적 훈련(Adversarial Training)을 통해 강인한 모델을 생성할 수 있는 방법으로 PGD이 제안되었다.

[0039] 수학식 2:

[0040] $$x^{t+1} = \pi_{x+S}\left(x^t + \mathrm{a} \cdot sign(\nabla_x L(\theta, x, y))\right)$$

[0041] PGD는 제약 조건이 존재 한다고 할 때, 범위 안쪽으로 a 만큼 다시 정사영(projection)시키는 multi-step 방법의 FGSM이라 생각할 수 있다. 공격에 대응방법으로 PGD 학습은 가장 강력한 공격을 최대화하여(Max) 생성된 공격을 바탕으로 손실 함수를 최소화(Min)하는 방법이다.

[0042] 이와 같이, 탐지 시스템은 적대적 샘플을 생성하기 위하여 InceptionV3모델을 활용하여 FGSM, C&W, PGD 공격을 가한 샘플 데이터들을 추출할 수 있다. 객체 탐지 모델에 적대적 샘플 데이터를 투과하여 객체 탐지가 진행될 수 있다. 도 3에 도시된 바와 같이, 정상 샘플(Benign)은 두 개의 차량을 포함하는 이미지로 검출된 바와 같이 두 개의 차량 번호판을 탐지한 것이다. 하지만, FGSM, C&W, PGD공격을 통해 생성된 적대적 예제들은 한 개의 객체만을 탐지하였고, 임계치(Threshold)값을 기 설정된 기준(예를 들면, 50% 이하)까지 조절하여 객체 탐지 가능성을 대폭 증진시켰음에도 적대적 공격에 대응하지 못함을 확인할 수 있다. 오히려 기존 정상 샘플이 번호판과 유사한 다른 객체를 탐지하는 역효과를 가져왔다. 특히, C&W공격은 다른 공격 기법들에 비해 객체를 탐지하는데 더욱 오랜 시간이 걸리는 것을 확인할 수 있다. 이는 실시간 영상을 탐지하는 모델에 이러한 공격이 적용될 경우 탐지 시간을 늘려 모델에 해를 가할 수 있는 잠재적 위험을 가진다고 해석할 수 있다.

[0043] 도 4는 일 실시예에 따른 탐지 시스템에서 영상 정보로부터 공격 데이터를 생성하는 것을 설명하기 위한 도면이다.

[0044] 탐지 시스템은 영상 정보가 입력됨을 수신할 수 있다. 이때, 영상 정보는 다양한 각도(예를 들면, 180도 각도, 90도 각도 등)에서 촬상된 또는 입력된 번호판 영역을 포함하는 차량 영상 또는 번호판 영역을 포함하는 이미지 데이터를 포함할 수 있다. 예를 들면, 카메라, CCTV 등을 이용하여 번호판 영역 또는 다량의 차량을 포함하는 영상 정보가 촬영될 수 있고, 촬영된 영상 정보가 입력될 수 있으며, 이미 다양한 각도로 촬영되어 있는 영상 정보가 입력될 수 있다. 이러한 영상 정보를 입력 데이터로 인식될 수 있다. 또한, 차량을 포함하는 영상 또는 이미지 데이터에는 입력된 데이터 자체에 위/변조가 진행된 경우도 포함될 수 있다.

[0045] 탐지 시스템은 수신된 영상 정보를 통해 번호판을 탐지하기 위한 객체 탐지 모델을 구성할 수 있다. 예를 들면, 객체 탐지 모델은 CNN, RNN 등 다양한 형태로 구성될 수 있다. 일례로, 탐지 시스템은 차량 영역이 포함된 영상 정보와 검출하고자 하는 영상의 어노테이션(Annotation) 파일을 활용하여 YOLOv3를 활용한 객체 탐지 모델(License Plate Detection, LPD)을 구성할 수 있다.

[0046] 탐지 시스템은 입력 데이터에 공격을 가하여 객체 탐지 모델의 정확도가 감소됨을 판단하기 위하여 구성된 객체 탐지 모델에 공격에 공격 데이터를 입력할 수 있다. 탐지 시스템은 정상 데이터를(400) 이용하여 공격 데이터(401)를 생성할 수 있다. 다시 말해서, 영상 정보와 관련된 데이터를 정상 데이터, 영상 정보와 관련하여 가공된 데이터를 공격 데이터(비정상 데이터)라고 정의할 수 있다. 이때, 탐지 시스템은 적대적 공격의 전이성(Transferability)을 감안하여 적대적 샘플을 생성할 수 있다. 탐지 시스템은 영상 정보를 이용하여 탐지 혹은 오탐지를 유발하는 임의의 노이즈(noise), 섭동(perturbation) 또는 변형(transformation)시켜 공격 데이터를

생성할 수 있다. 예를 들면, 탐지 시스템은 구성된 객체 탐지 모델에 직접적인 공격을 가하지 않고, 영상 정보(입력 데이터)에 공격을 가하고자ImageNet으로 학습된 InceptionV3모델에 강제로 특정 레이블(예를 들면, 'Giant-Panda')을 가진 차량(Benign) 샘플을 삽입하여 FGSM, C&W그리고PGD 공격 방법을 해당 샘플에 섭동(Perturbed)된 적대적 샘플을 생성할 수 있다.

[0047] 도 5는 일 실시예에 따른 탐지 시스템에서 객체 탐지 모델을 생성하는 방법을 설명하기 위한 흐름도이다.

[0048] 도 5에서는 탐지 시스템은 객체 탐지 모델을 생성함에 있어, 서로 다른 종류의 데이터를 훈련 데이터로 사용하여 객체 탐지 모델을 강화시키는 방법을 설명하기로 한다.

[0049] 단계(510)에서 탐지 시스템은 정상 데이터(400) 및 비정상 데이터(공격 데이터)(401)를 객체 탐지 모델에 입력할 수 있다. 이때, 정상 데이터 및 비정상 데이터로 영상 정보로 입력된 입력 데이터를 의미한다. 예를 들면, 입력 데이터로 국내 차량 번호판 데이터(KarPlate Dataset)를 사용할 수 있다. 해당 데이터 셋은 번호판 탐지를 위한 데이터 셋, 번호판 인식을 위한 데이터 셋, 엔드 투 엔드 인식을 위한 데이터 셋을 포함하고 있는데, 실시예에서는 번호판 탐지를 위한 이미지와 어노테이션 데이터를 사용하여 수정한 YOLOv3를 생성할 수 있다.

[0050] 단계(520)에서 탐지 시스템은 객체 탐지 알고리즘을 통한 객체 탐지 모델을 훈련시킬 수 있다. 탐지 시스템은 수신된 영상 정보를 통해 번호판을 탐지하기 위한 객체 탐지 모델을 구성하고, 수신된 영상 정보를 의미하는 정상 데이터 및 수신된 영상 정보에 대한 공격 데이터를 훈련 데이터로 사용하여 구성된 객체 탐지 모델을 학습시킬 수 있다. 예를 들면, 탐지 시스템은 기 설정된 기준의 성능을 가지는 객체 탐지 모델을 구성할 수 있다.

[0051] 단계(530)에서 탐지 시스템은 강화된 번호판 탐지를 진행할 수 있다. 탐지 시스템은 공격 데이터를 활용하여 객체 탐지 모델을 학습시킴에 따라 견고한 모델로 강화시킬 수 있다. 다시 말해서, 탐지 시스템은 정상 데이터와 공격 데이터를 이용하여 객체 탐지 모델을 재구성할 수 있다. 이에, 탐지 시스템은 번호판 영역을 미탐지 혹은 오탐지를 유발하는 공격을 방어할 수 있다. 구체적으로, 탐지 시스템은 공격 데이터의 특징을 추출하고, 추출된 특징들을 기반으로 객체 탐지 모델의 성능을 향상시켜 모델의 성능을 더욱 견고하게 만들 수 있다. 탐지 시스템은 학습된 객체 탐지 모델에 차량 번호판을 탐지하기 위한 차량 영상 정보를 입력할 수 있다. 탐지 시스템은 학습된 객체 탐지 모델을 이용하여 차량 영상 정보로부터 차량 번호판을 탐지할 수 있다. 탐지 시스템은 탐지된 차량 번호판을 출력할 수 있다. 또한, 탐지 시스템은 탐지된 차량 번호판에 존재하는 차량 번호판 식별 정보(예를 들면, 차량 번호)를 출력할 수 있다. 예를 들면, 탐지 시스템은 차량 번호판에 존재하는 문자, 숫자로 구성된 번호판 식별 정보를 출력할 수 있다.

[0052] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate 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(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 기술분야에서 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.

[0053] 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, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 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.

[0054] 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 등

을 단독으로 또는 조합하여 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), 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.

[0055] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0056] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0058] 100: 탐지 시스템

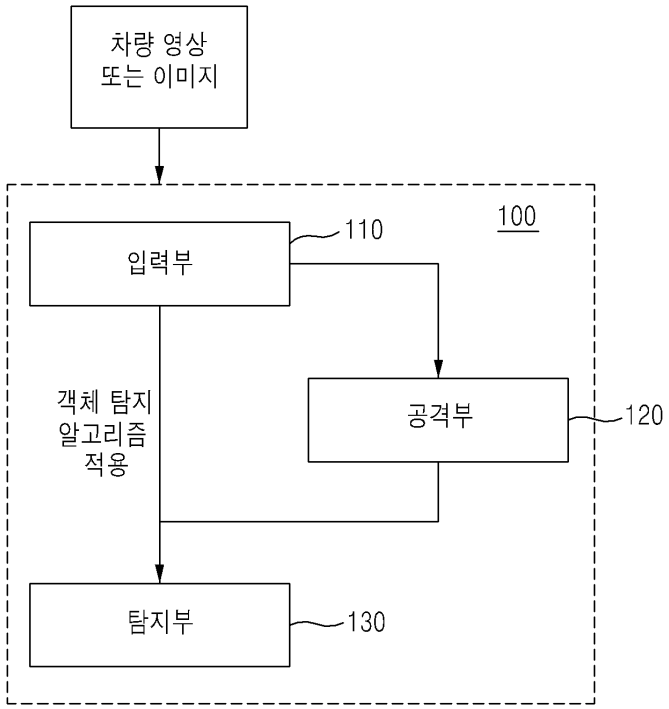
110: 입력부

120: 공격부

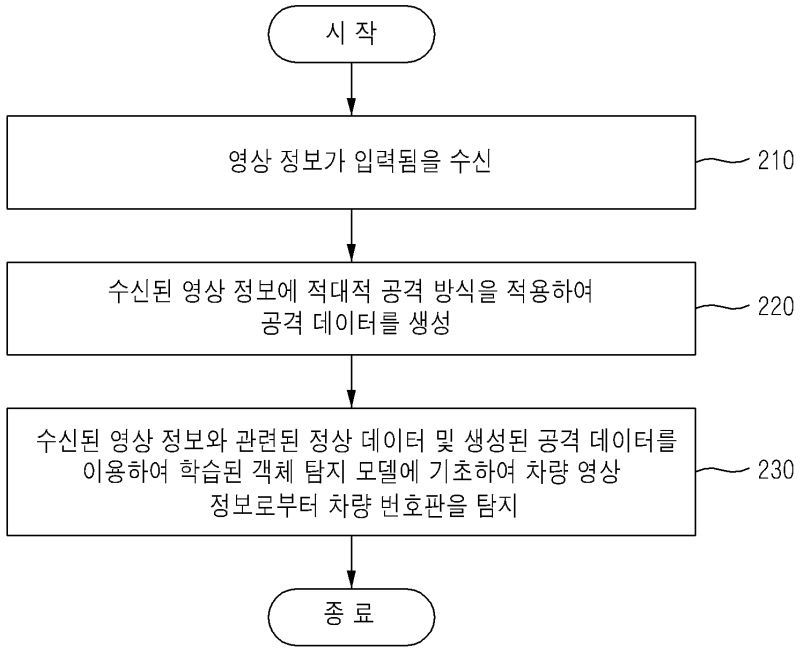
130: 탐지부

도면

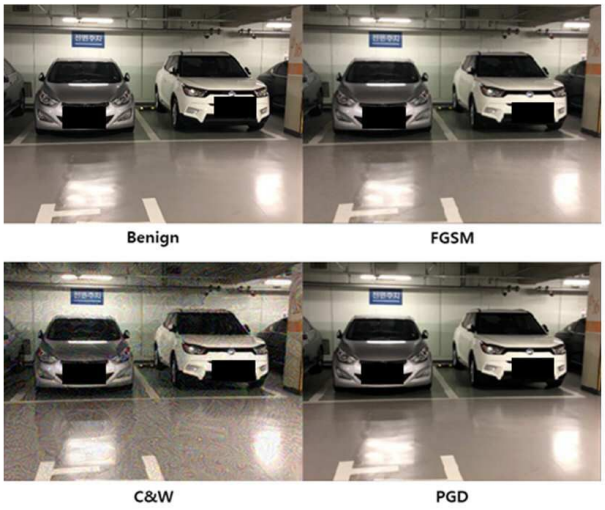
도면1



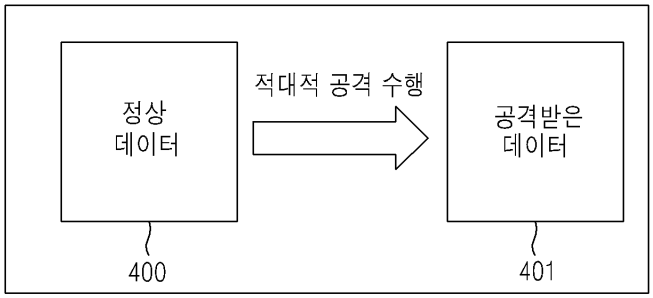
도면2


시 작
영상 정보가 입력됨을 수신
210
수신된 영상 정보에 적대적 공격 방식을 적용하여
공격 데이터를 생성
220
수신된 영상 정보와 관련된 정상 데이터 및 생성된 공격 데이터를
이용하여 학습된 객체 탐지 모델에 기초하여 차량 영상
정보로부터 차량 번호판을 탐지
230
종 료

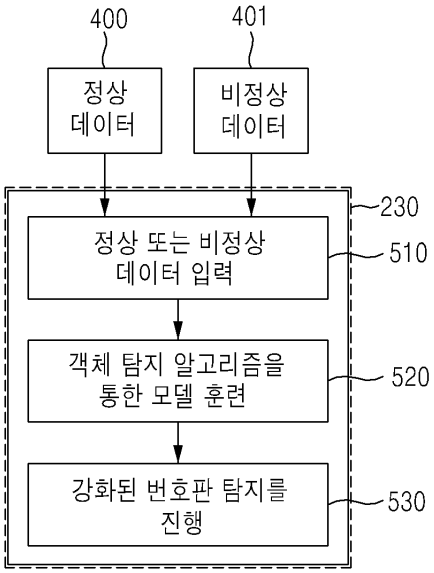
도면3


Benign
FGSM
C&W
PGD

도면4


정상
데이터
적대적 공격 수행
공격받은
데이터
400
401

도면5


400
401
정상
데이터
비정상
데이터
230
정상 또는 비정상
데이터 입력
510
객체 탐지 알고리즘을
통한 모델 훈련
520
강화된 번호판 탐지를
진행
530