(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0086844
(43) 공개일자 2022년06월24일

(51) 국제특허분류(Int. Cl.)
G06T 7/187 (2017.01) *G06F 21/62* (2013.01)
G06N 3/08 (2006.01) *G06T 11/60* (2006.01)
H04L 9/08 (2006.01) *H04N 21/2743* (2011.01)
(52) CPC특허분류
G06T 7/187 (2017.01)
G06F 21/6245 (2013.01)
(21) 출원번호 10-2020-0177003
(22) 출원일자 2020년12월17일
심사청구일자 2020년12월17일

(71) 출원인
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
김성륜
서울특별시 용산구 이촌로 303, 32동 1304호 (이촌동, 현대아파트)
오승은
서울특별시 서대문구 성산로22길 24-18, 405호 (창천동)
(74) 대리인
특허법인(유한)아이시스

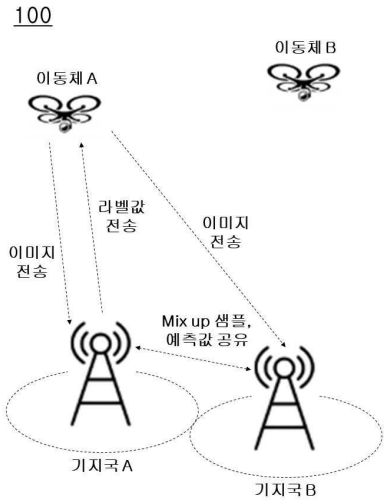
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **개인정보를 보장하는 실시간 라벨링 방법 및 장치**

(57) 요 약

개시된 기술은 개인정보를 보장하는 실시간 라벨링 방법 및 장치에 관한 것으로, 복수의 이동체가 카메라를 이용하여 지상에 대한 복수의 이미지를 각각 촬영하고 복수의 디바이스들에게 각각 전송하는 단계; 상기 복수의 디바이스가 딥러닝 모델에 상기 복수의 이미지를 입력하여 믹스업(Mix up) 된 샘플 데이터를 출력하고 각자 출력한 샘플 데이터에서 개인정보(Privacy)를 제외한 나머지인 샘플 이미지를 서로 공유하는 단계; 상기 복수의 디바이스가 상기 공유된 샘플 이미지에 대한 예측값을 각자 측정하고 상기 예측값을 서로 공유하는 단계; 상기 복수의 디바이스가 상기 공유된 예측값을 상기 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력하는 단계; 및 상기 복수의 디바이스가 상기 역 믹스업된 예측값을 상기 복수의 이미지에 대한 라벨값으로 입력하는 단계;를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06N 3/08 (2013.01)
G06T 11/60 (2013.01)
H04L 9/0816 (2013.01)
H04N 21/2743 (2013.01)
G06T 2207/20081 (2013.01)
G06T 2207/20084 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711103168
과제번호 2016-0-00208-005
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원(한국연구재단부설)
연구사업명 정보통신방송연구개발사업
연구과제명 (창조씨앗-2단계) 차세대 5G V2X 서비스 실현을 위한 정밀 측위탐색 연계 고효율 다중안테나 정보전송 및 네트워크 기술 연구
기 여 율 1/1
과제수행기관명 연세대학교 산학협력단
연구기간 2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

복수의 이동체가 카메라를 이용하여 지상에 대한 복수의 이미지를 각각 촬영하고 복수의 디바이스들에게 각각 전송하는 단계;

상기 복수의 디바이스가 딥러닝 모델에 상기 복수의 이미지를 입력하여 믹스업(Mix up) 된 샘플 데이터를 출력하고 각자 출력한 샘플 데이터에서 개인정보(Privacy)를 제외한 나머지인 샘플 이미지를 서로 공유하는 단계;

상기 복수의 디바이스가 상기 공유된 샘플 이미지에 대한 예측값을 각자 측정하고 상기 예측값을 서로 공유하는 단계;

상기 복수의 디바이스가 상기 공유된 예측값을 상기 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력하는 단계; 및

상기 복수의 디바이스가 상기 역 믹스업된 예측값을 상기 복수의 이미지에 대한 라벨값으로 입력하는 단계;를 포함하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 2

제 1 항에 있어서,

상기 복수의 이동체가 촬영한 이미지는 라벨값이 입력되지 않은 로데이터(Raw data)이고, 상기 이미지는 상기 복수의 이동체가 지나는 경로를 포함하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 3

제 1 항에 있어서,

상기 복수의 디바이스는 상기 딥러닝 모델 각각의 믹스비율(Mixing ratio)에 따라 상기 복수의 이미지를 각각 믹스업하고,

상기 믹스비율은 상기 복수의 디바이스 간에 공유되지 않는 개인키(Private Key)인 것을 특징으로 하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 4

제 1 항에 있어서,

상기 복수의 이동체 및 상기 복수의 디바이스는 분산 네트워크를 형성하는 복수개의 노드이고,

상기 복수의 이동체는 공중을 비행하는 드론이고, 상기 복수의 디바이스는 지상의 기지국 내 탑재되는 것을 특징으로 하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 5

제 1 항에 있어서, 상기 역 믹스업 된 예측값을 출력하는 단계는,

상기 복수의 디바이스가 상기 공유된 예측값의 평균을 계산하고 자신의 믹스비율을 이용하여 상기 예측값을 역 믹스업하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 6

제 1 항에 있어서, 상기 라벨값으로 입력하는 단계는,

상기 복수의 디바이스가 상기 라벨값을 이용하여 상기 딥러닝 모델을 트레이닝하는 단계를 더 포함하는 개인정보를 보장하는 실시간 라벨링 방법.

청구항 7

복수의 이동체로부터 전송되는 복수의 이미지를 수신하는 안테나;

상기 복수의 이미지에 믹스업(Mix up)하는 딥러닝 모델을 저장하는 저장장치; 및

상기 딥러닝 모델에 상기 복수의 이미지를 입력하여 믹스업 된 샘플 데이터를 출력하고 상기 샘플 데이터에서 개인정보를 제외한 샘플 이미지를 타 디바이스에 전송하여 획득한 예측값을 상기 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력하고 상기 역 믹스업된 예측값을 상기 복수의 이미지에 대한 라벨값으로 입력하는 연산장치;를 포함하는 개인정보를 보장하는 실시간 라벨링 장치.

청구항 8

제 7 항에 있어서,

상기 복수의 이동체가 촬영한 이미지는 라벨값이 입력되지 않은 로데이터(Raw data)이고, 상기 이미지는 상기 복수의 이동체가 지나는 경로를 포함하는 개인정보를 보장하는 실시간 라벨링 장치.

청구항 9

제 7 항에 있어서,

상기 연산장치는 상기 딥러닝 모델의 믹스비율(Mixing ratio)에 따라 상기 복수의 이미지를 믹스업하고,

상기 믹스비율은 상기 타 디바이스와 공유하지 않는 개인키(Private Key)인 것을 특징으로 하는 개인정보를 보장하는 실시간 라벨링 장치.

청구항 10

제 7 항에 있어서,

상기 연산장치는 상기 타 디바이스에서 전송된 상기 예측값의 평균을 계산하고 상기 딥러닝 모델의 믹스비율을 이용하여 상기 예측값의 평균을 역 믹스업하는 개인정보를 보장하는 실시간 라벨링 장치.

청구항 11

제 7 항에 있어서,

상기 연산장치는 상기 라벨값을 이용하여 상기 딥러닝 모델을 트레이닝하는 개인정보를 보장하는 실시간 라벨링 장치.

발명의 설명

기 술 분 야

[0001] 개시된 기술은 이동체에서 획득한 영상을 개인정보 노출 없이 실시간으로 라벨링하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 이동체들로 이루어진 네트워크 상에서 실시간으로 얻은 데이터 셈플을 강화학습에 활용하기 위해서는 빠른 속도로 라벨링을 입력하는 기술이 요구된다. 라벨링을 입력을 위해 단말과 단말 또는 단말과 서버 간에 데이터를 교환할 수 있다. 이때, 데이터 교환 과정에서 각 이동체가 얻은 샘플에 대하여 개인정보(Privacy)를 보장하는 것이 중요한 이슈이다. 일반적인 데이터 교환 방식으로는 단말기 갖는 샘플을 직접 교환하는 방식, 단말이 트레이닝하는 모델을 교환하는 방식, 단말이 트레이닝하는 모델의 결과값을 교환하는 방식 등이 존재한다.

[0003] 한편, 개인정보 유출을 방지하기 위해서 이용되는 방법 또한 다양하게 존재한다. 예컨대, 샘플에 랜덤하게 생성한 노이즈를 섞어서 전송하거나 양자화 레벨(Quantization Level)을 제어하는 방식, 그리고 믹스업(Mix up)을 이용하는 방식이 존재한다. 이 중 믹스업은 레이블이 다른 임의의 두 샘플을 섞는 방식으로 데이터 증강(Data Augmentation)에 주로 이용되는 것으로 샘플에 포함된 개인정보를 방지하는 데에도 효과적이다.

[0004] 한편, 상술한 바와 같이 단말이 직접 샘플을 교환하는 방식의 경우에는 테스트 정확도를 충분히 향상시킬 수 있지만 개인정보의 유출이 발생하는 문제가 있었다. 그리고 트레이닝된 모델을 교환하는 방식은 샘플을 직접 교환하는 대신 모델을 이용하여 간접적인 교환을 함으로써 개인정보의 유출은 피할 수 있으나 모델 자체의 정보량이 커서 통신 환경이 양호하지 않은 경우에는 테스트가 실패할 확률이 높아지는 문제가 있었다. 그리고 모델에서 출력된 결과값을 이용하는 방식은 개인정보가 유출되지 않고 교환되는 정보량 또한 적은 편이라는 장점이 있으나 테스트 정확도가 충분하지 못하다는 문제가 있었다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국 등록특허 제10-1843066호

발명의 내용

해결하려는 과제

[0006] 개시된 기술은 이동체에서 획득한 영상을 개인정보 노출 없이 실시간으로 라벨링하는 방법 및 장치를 제공하는데 있다.

과제의 해결 수단

[0007] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 1 측면은 복수의 이동체가 카메라를 이용하여 지상에 대한 복수의 이미지를 각각 촬영하고 복수의 디바이스들에게 각각 전송하는 단계, 상기 복수의 디바이스가 딥러닝 모델에 상기 복수의 이미지를 입력하여 믹스업(Mix up) 된 샘플 데이터를 출력하고 각자 출력한 샘플 데이터에서 개인정보(Privacy)를 제외한 나머지인 샘플 이미지를 서로 공유하는 단계, 상기 복수의 디바이스가 상기 공유된 샘플 이미지에 대한 예측값을 각자 측정하고 상기 예측값을 서로 공유하는 단계, 상기 복수의 디바이스가 상기 공유된 예측값을 상기 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력하는 단계 및 상기 복수의 디바이스가 상기 역 믹스업된 예측값을 상기 복수의 이미지에 대한 라벨값으로 입력하는 단계를 포함하는 개인정보를 보장하는 실시간 라벨링 방법을 제공하는데 있다.

[0008] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 2 측면은 복수의 이동체로부터 전송되는 복수의 이미지를 수신하는 안테나, 상기 복수의 이미지에 믹스업(Mix up)하는 딥러닝 모델을 저장하는 저장장치 및 상기 딥러닝 모델에 상기 복수의 이미지를 입력하여 믹스업 된 샘플 데이터를 출력하고 상기 샘플 데이터에서 개인정보를 제외한 샘플 이미지를 타 디바이스에 전송하여 획득한 예측값을 상기 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력하고 상기 역 믹스업된 예측값을 상기 복수의 이미지에 대한 라벨값으로 입력하는 연산장치를 포함하는 개인정보를 보장하는 실시간 라벨링 장치를 제공하는데 있다.

발명의 효과

[0009] 개시된 기술의 실시 예들은 다음의 장점들을 포함하는 효과를 가질 수 있다. 다만, 개시된 기술의 실시 예들이 이를 전부 포함하여야 한다는 의미는 아니므로, 개시된 기술의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0010] 개시된 기술의 일 실시예에 따르면 개인정보를 보장하는 실시간 라벨링 방법 및 장치는 라벨값을 입력할 때 개인정보를 이용하지 않아서 유출을 방지하는 효과가 있다.

[0011] 또한, 빠르게 입력된 라벨값을 이용하여 모델의 테스트 정확도를 높이는 효과가 있다.

[0012] 또한, 다른 모델의 예측값을 이용하여 공간 다이버시티를 획득하는 효과가 있다.

도면의 간단한 설명

[0013] 도 1은 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 시스템을 이용하는 과정을 나타낸 도면이다.

도 2는 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 방법에 대한 순서도이다.

도 3은 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 장치에 대한 블록도이다.

도 4는 믹스업 샘플을 생성하는 것을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 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.

[0015] 제 1 , 제 2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0016] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 한다. 그리고 "포함한다" 등의 용어는 설시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계 동작 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0017] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다.

[0018] 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다. 따라서, 본 명세서를 통해 설명되는 각 구성부들의 존재 여부는 기능적으로 해석되어야 할 것이다.

[0019] 도 1은 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 시스템을 이용하는 과정을 나타낸 도면이다. 도 1을 참조하면 시스템(100)은 복수의 이동체 및 복수의 디바이스를 포함한다. 복수의 이동체는 드론과 같이 이동 가능한 무인체일 수 있으며 복수의 디바이스는 지상의 기지국이나 인프라 등에 설치되어 복수의 이동체들과 통신하는 RSU일 수 있다. 복수의 이동체 및 복수의 디바이스는 분산 네트워크를 형성하는 복수개의 노드일 수 있다.

[0020] 복수의 이동체들은 지상에 대한 이미지를 각각 촬영한다. 이동체 A 및 이동체 B는 서로 다른 위치를 비행하는 중이므로 서로 다른 이미지가 촬영될 수 있다. 당연하게도 두 이미지 간에는 이동체 A와 이동체 B의 위치를 식별할 수 있는 정보들이 포함된다. 예컨대 지상의 도로나 교통표지판 내지는 구조물, 랜드마크 등과 같이 이동체의 경로를 나타낼 수 있는 정보를 포함할 수 있다.

[0021] 한편, 각 이동체들이 촬영한 복수의 이미지들은 라벨값이 입력되지 않은 데이터로 일종의 로데이터(Raw data)일 수 있다. 복수의 이동체들은 이러한 이미지를 촬영하고 실시간으로 네트워크를 통해 복수의 디바이스로 전송한다.

[0022] 복수의 디바이스들은 딥러닝 모델에 복수의 이미지를 입력하여 믹스업(Mix up) 된 샘플 데이터를 출력한다. 그리고 각자 출력한 샘플 데이터에서 개인정보(Privacy)를 제외한 나머지인 샘플 이미지를 서로 공유한다. 예컨대, 기지국 A의 디바이스와 기지국 B의 디바이스가 서로 출력한 샘플 이미지를 공유할 수 있다. 물론 더 많은 수의 디바이스가 존재하더라도 네트워크를 통해 서로 샘플 이미지를 공유하는 것이 가능하다.

[0023] 여기에서 믹스업에 적용된 믹스비율(Mixing ratio)는 제외하고 믹싱된 결과값인 샘플 이미지만을 공유한다. 즉, 믹스 비율은 각 디바이스들이 샘플 이미지를 생성하는데 사용하는 각자의 개인키(Private Key)일 수 있다. 이와 같이 공유된 샘플 이미지에 대한 예측값을 각자 측정하고 이를 서로 공유한다.

[0024] 복수의 디바이스는 자신이 공유한 샘플 이미지에 대한 다른 디바이스의 예측값을 이용한다. 각 디바이스 별로

모델이 탑재될 수 있으며 자신이 믹스업한 샘플 이미지에 대한 다른 모델들의 예측값의 평균을 계산할 수 있다. 복수의 디바이스들이 모두 이러한 방법에 따라 타 디바이스의 예측값을 수신하면 각자 자신의 믹스 비율을 이용하여 역 믹스업된 예측값을 출력할 수 있다. 즉, 모델에 예측값을 입력하여 다시 한번 믹스업된 결과값을 획득하는 것이다. 이와 같이 역 믹스업된 예측값을 구하면 이를 이미지의 라벨값으로 입력할 수 있다.

[0025] 한편, 복수의 디바이스들은 이와 같이 생성된 라벨값을 이용하여 각자의 모델을 트레이닝할 수 있다. 이러한 프로세스를 통해 라벨값이 입력되지 않은 이동체의 이미지에 실시간으로 라벨값을 입력할 수 있으며 라벨링 수행 시 발생할 수 있는 샘플 프라이버시 손실을 방지할 수 있다. 그리고 이러한 과정에서 다른 디바이스의 모델에서 출력된 예측값을 이용하기 때문에 공간 다이버시티가 증가되는 효과가 발생될 수 있다. 즉 이동체의 이동 경로와 위치에 대한 상관관계를 파악할 수 있으므로 보다 높은 정확도로 트레이닝을 수행할 수 있다.

[0026] 도 2는 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 방법에 대한 순서도이다. 도 2를 참조하면 개인정보를 보장하는 실시간 라벨링 방법(200)는 210 단계 내지 250 단계를 포함한다. 각 단계는 실시간 라벨링을 수행하는 장치들을 통해 진행될 수 있으며 각 단계들은 순차적으로 수행될 수 있다.

[0027] 210 단계에서 복수의 이동체가 카메라를 이용하여 지상에 대한 복수의 이미지를 각각 촬영하고 복수의 디바이스들에게 각각 전송한다. 복수의 이동체가 촬영한 이미지는 라벨값이 입력되지 않은 로데이터(Raw data)이고, 각 이미지는 각각의 이동체가 지나는 경로를 포함할 수 있다. 여기에서 경로는 도로의 형태일 수도 있고 도로 주변의 랜드마크나 교통표지판일 수도 있다.

[0028] 220 단계에서 복수의 디바이스가 딥러닝 모델에 복수의 이미지를 입력하여 믹스업(Mix up) 된 샘플 데이터를 출력하고 각자 출력한 샘플 데이터에서 개인정보(Privacy)를 제외한 나머지인 샘플 이미지를 서로 공유한다. 220 단계에서 출력되는 샘플 데이터는 복수의 디바이스 각각에 탑재된 딥러닝 모델의 믹스 비율에 따라서 출력된다. 예컨대, 믹스 비율은 믹스업 이미지를 생성하는데 이용하는 개인키 값일 수 있다. 즉, 각 모델의 믹스 비율은 서로 동일할 수도 있고 서로 다를 수 있다. 중요한 점은 개인정보에 해당하는 믹스 비율을 타 디바이스에 공유하지 않는다는 점이다. 즉, 모델을 통해 출력된 샘플 이미지만을 이용하여 라벨값을 생성하는데 이용할 수 있다.

[0029] 230 단계에서 복수의 디바이스가 공유된 샘플 이미지에 대한 예측값을 각자 측정하고 예측값을 서로 공유한다. 복수의 디바이스는 타 디바이스들로부터 공유된 예측값의 평균을 계산한다.

[0030] 240 단계에서 복수의 디바이스가 공유된 예측값을 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력한다. 복수의 디바이스들은 타 디바이스에서 예측된 자신의 샘플 데이터에 대한 예측값 및 자신이 샘플 데이터를 생성하는데 이용한 믹스 비율을 토대로 공유된 예측값을 역 믹스업한다.

[0031] 250 단계에서 복수의 디바이스가 역 믹스업된 예측값을 복수의 이미지에 대한 라벨값으로 입력한다. 250 단계에서 복수의 디바이스들은 210 내지 240 단계에 따라 생성한 라벨값을 각자의 모델에 입력하여 트레이닝하는 단계를 더 수행할 수 있다.

[0032] 도 3은 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 장치에 대한 블록도이다. 도 3을 참조하면 라벨링 장치(300)는 안테나(310), 저장장치(320) 및 연산장치(330)를 포함한다.

[0033] 안테나(310)는 복수의 이동체로부터 전송되는 복수의 이미지를 수신한다. 안테나는 일반적은 V2X 통신에 이용하는 방향성 안테나를 이용할 수 있다. 안테나(310)는 V2X 통신에 따른 주파수를 이용하여 네트워크 상의 복수의 이동체들로부터 이미지를 수신할 수 있다.

[0034] 저장장치(320)는 딥러닝 모델을 저장한다. 딥러닝 모델은 복수의 이미지를 믹스업(Mix up)하기 위한 것으로 각자의 믹스 비율로 복수의 이미지를 믹싱할 수 있다.

[0035] 연산장치(330)는 딥러닝 모델에 복수의 이미지를 입력하여 믹스업 된 샘플 데이터를 출력한다. 상술한 바와 같이 믹스 비율에 따른 샘플 데이터가 출력될 수 있다. 그리고 샘플 데이터에서 개인정보를 제외한 샘플 이미지를 타 디바이스에 전송한다. 그리고 타 디바이스들로부터 샘플 이미지에 대한 예측값을 획득하고 이를 딥러닝 모델에 다시 입력하여 역 믹스업(Inverse Mix up) 된 예측값을 출력한다. 이와 같이 역 믹스업된 예측값을 복수의 이미지에 대한 라벨값으로 입력할 수 있다.

[0036] 한편, 상술한 라벨링 장치(300)는 컴퓨터와 같은 디바이스에서 실행될 수 있는 실행가능한 알고리즘을 포함하는 프로그램(또는 어플리케이션)으로 구현될 수 있다. 상기 프로그램은 일시적 또는 비일시적 판독 가능 매체(non-

transitory computer readable medium)에 저장되어 제공될 수 있다.

[0037] 비일시적 판독 가능 매체란 레지스터, 캐쉬, 메모리 등과 같이 짧은 순간 동안 데이터를 저장하는 매체가 아니라 반영구적으로 데이터를 저장하며, 기기에 의해 판독(reading)이 가능한 매체를 의미한다. 구체적으로는, 상술한 다양한 어플리케이션 또는 프로그램들은 CD, DVD, 하드 디스크, 블루레이 디스크, USB, 메모리카드, ROM (read-only memory), PROM (programmable read only memory), EPROM(Erasable PROM, EPROM) 또는 EEPROM(Electrically EPROM) 또는 플래시 메모리 등과 같은 비일시적 판독 가능 매체에 저장되어 제공될 수 있다.

[0038] 일시적 판독 가능 매체는 스태틱 램(Static RAM, SRAM), 다이내믹 램(Dynamic RAM, DRAM), 싱크로너스 디램(Synchronous DRAM, SDRAM), 2배속 SDRAM(Double Data Rate SDRAM, DDR SDRAM), 증강형 SDRAM(Enhanced SDRAM, ESDRAM), 동기화 DRAM(Synclink DRAM, SLDRAM) 및 직접 램버스 램(Direct Rambus RAM, DRRAM) 과 같은 다양한 RAM을 의미한다.

[0039] 도 4는 믹스업 샘플을 생성하는 것을 나타낸 도면이다. 도 4를 참조하면 단말이 갖는 임의의 두 데이터에 대하여 믹스업된 샘플을 생성하는 것이 가능하다. 여기에서 임의의 두 데이터는 이미지 샘플 및 레이블의 페어일 수 있다. 믹스업된 샘플 데이터는 $\tilde{x} = \lambda x_1 + (1-\lambda)x_2$ 과 같은 형태가 될 수 있다. 여기에서 λ 가 믹스 비율(Mixing ratio)를 의미한다. 믹스업 알고리즘을 통해 출력된 샘플 데이터 $\tilde{x}$ 를 데이터 교환에 사용함으로써 개인정보의 유출 문제를 일정수준 해결할 수 있고 테스트의 정확도 향상 또한 기대할 수 있다.

[0040] 한편, 개시된 기술에서 제안하는 믹스업 방식과 역 믹스업 방식은 다음과 같다. 먼저 분산 네트워크 내의 단일 혹은 복수의 디바이스가 복수의 이동체들로부터 수신한 복수개의 이미지 $x_1, x_2, \cdots, x_n$ 에 대해 mixup 알고리즘을 적용시켜 샘플 이미지를 생성한다. 샘플 이미지 $\tilde{x}$ 는 아래 수학식 1과 같이 정의된다.

[0042] [수학식 1]

[0043] $$\tilde{x} = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$$

[0044] 여기에서 각 디바이스의 믹싱 비율의 합은 1이 될 수 있다. 즉, $\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$ 을 만족한다.

[0045] 다음으로 샘플 이미지 $\tilde{x}$ 를 다른 디바이스들과 공유한다. 그리고 다른 디바이스들로부터 공유받은 데이터셋 $\tilde{x_1}, \tilde{x_2}, \cdots, \tilde{x_m}$ 을 각자의 모델에 다시 입력하여 역 믹스업(inverse mixup) 된 데이터를 출력한다. 즉, 샘플 이미지를 생성한 믹스업 알고리즘에 한번 더 통과시키는 것이다. 역 믹스업된 데이터는 아래 수학식 2와 같이 정의된다.

[0047] [수학식 2]

[0048] $$x' = \tilde{\lambda_1}\tilde{x_1} + \tilde{\lambda_2}\tilde{x_2} + \cdots + \tilde{\lambda_m}\tilde{x_m}$$

[0049] 여기에서 $(\tilde{\lambda_1}, \tilde{\lambda_2}, \cdots, \tilde{\lambda_m})$ 는 $\tilde{\lambda_1} + \tilde{\lambda_2} + \cdots + \tilde{\lambda_m} = 1$ 을 만족함과 동시에 $l' = l_k \quad (k \epsilon \{1,2,\cdots,m\})$를 만족하는 값을 사용한다. n=m=2인 special case에 대하여 $\tilde{\lambda_1}$ 과 $\tilde{\lambda_2}$ 을 계산하면 아래 수학식 3과 같이 정의할 수 있다.

[0051] [수학식 3]

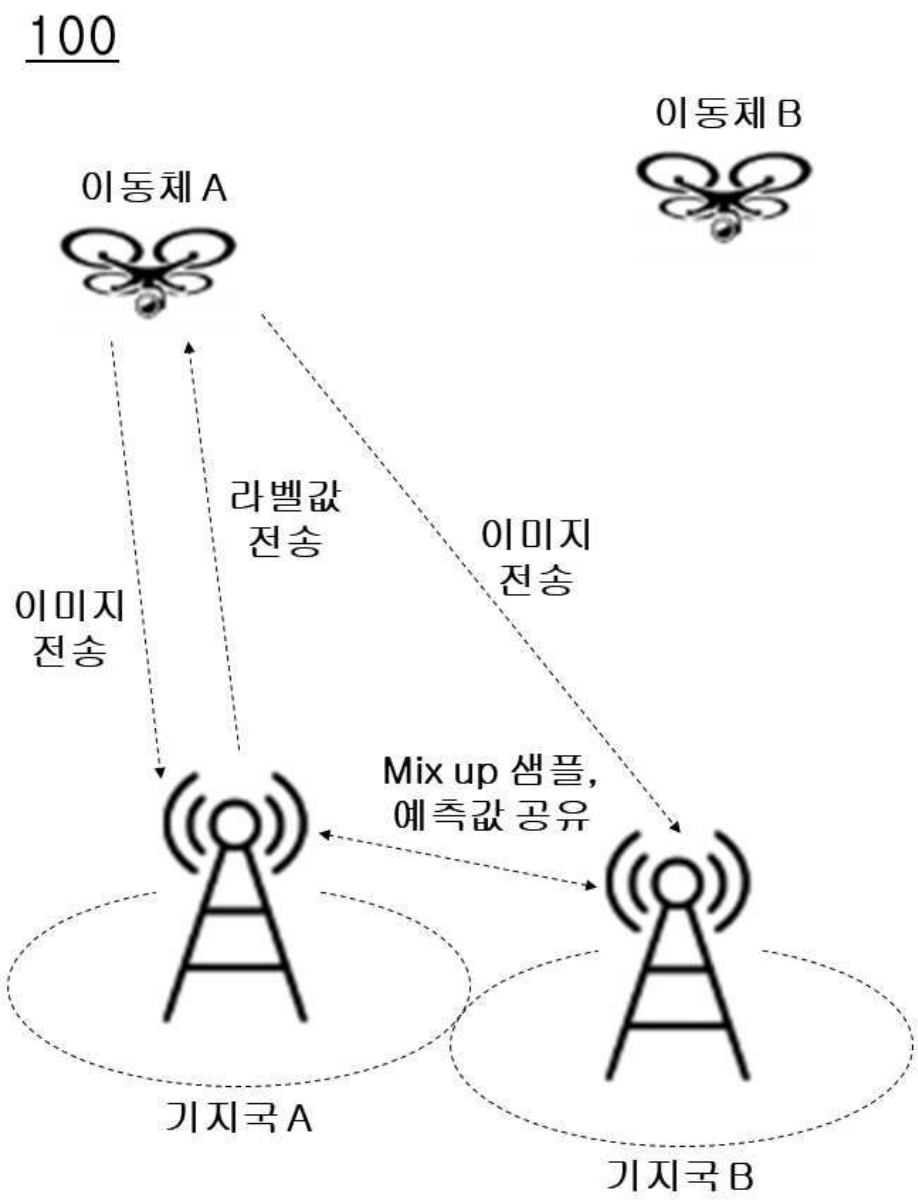
[0052] 1. $\widetilde{\lambda_1} = 1 - \widetilde{\lambda_2} = \frac{\lambda_1}{2\lambda_1 - 1}$, then $l' = l_1$.
2. $\widetilde{\lambda_1} = 1 - \widetilde{\lambda_2} = 1 - \frac{\lambda_1}{2\lambda_1 - 1}$, then $l' = l_2$.

[0054] 이때, $\lambda_1 x_1 + \lambda_2 x_2$ 과 $\lambda_1 x_2 + \lambda_2 x_1$ 모두 공유가 된 상태로 믹스업 알고리즘에 통과시킬 경우, $\widetilde{\lambda_1} = 1 - \widetilde{\lambda_2} = \frac{\lambda_1}{2\lambda_1 - 1}$ 에 대하여 $l' = l_1$ 을 만족함과 동시에 $s' = s_1$ 을 만족시킨다. $\cdot \widetilde{\lambda_1} = 1 - \widetilde{\lambda_2} = 1 - \frac{\lambda_1}{2\lambda_1 - 1}$ 인 경우에 대해서도 마찬가지로 $l' = l_2$ 과 $s' = s_2$ 이 동시에 성립한다. 이는 레이블 뿐만 아니라 이미지 샘플 자체도 기존에 다른 단말이 가지고 있던 형태 그대로 복원 가능하다는 것을 의미하고 이러한 경우 프라이버시 보호가 적용이 안되기 때문에 샘플 데이터를 전송할 때 $\lambda_1 x_1 + \lambda_2 x_2$ 이 공유가 되는 경우, $\lambda_1 x_2 + \lambda_2 x_1$ 과 같은 mixup 데이터는 공유가 되지 않도록 유의해야 한다. 복수의 디바이스들은 이와 같이 처리된 역 믹스업 데이터 $x'_1, x'_2, \cdots$를 라벨값으로 활용하여 트레이닝을 진행한다. 따라서 개인정보를 유출하지 않고 트레이닝 정확도를 향상시킬 수 있다.

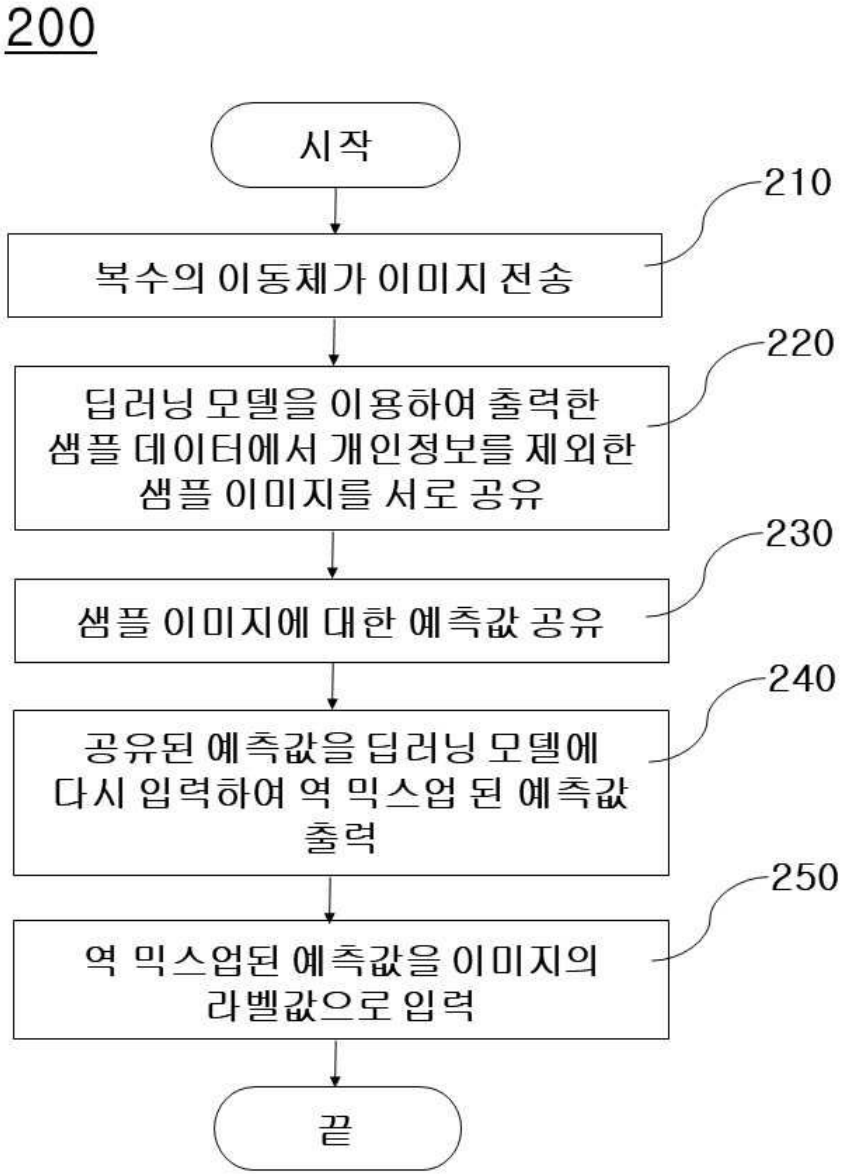
[0055] 개시된 기술의 일 실시예에 따른 개인정보를 보장하는 실시간 라벨링 방법 및 장치는 이해를 돕기 위하여 도면에 도시된 실시 예를 참고로 설명되었으나, 이는 예시적인 것에 불과하며, 당해 분야에서 통상적 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 개시된 기술의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해 정해져야 할 것이다.

도면

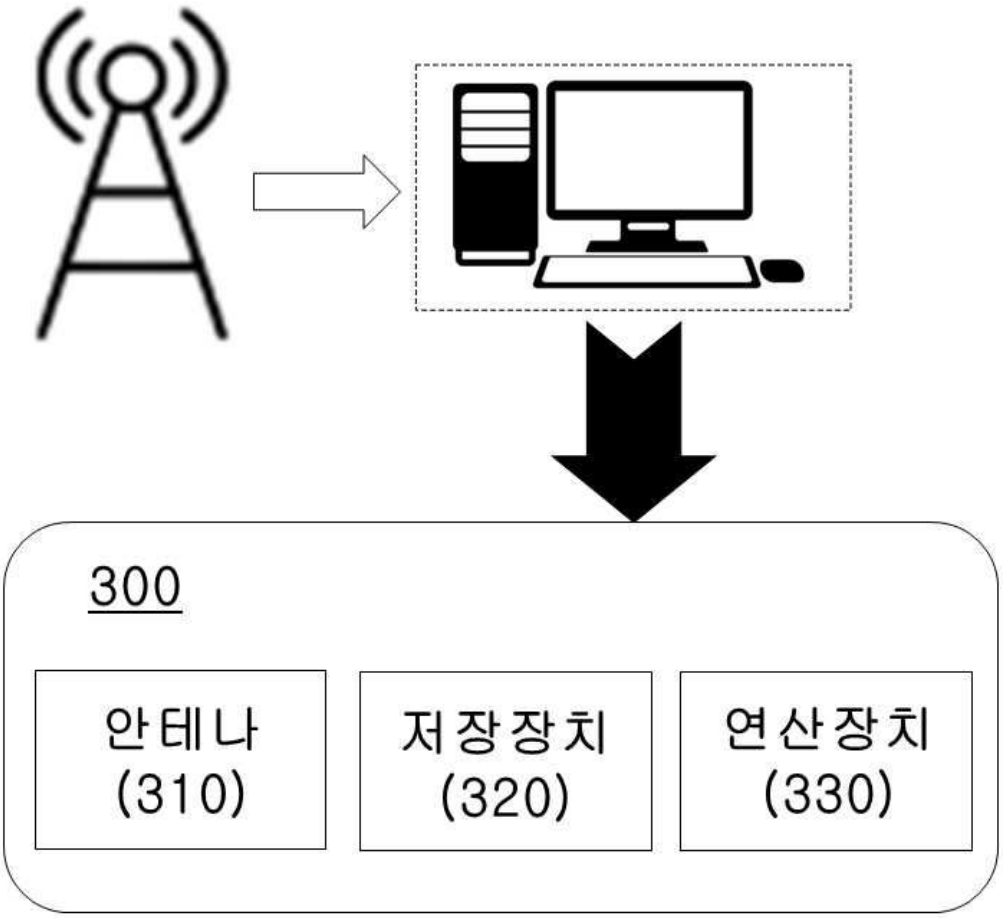
도면1



도면2

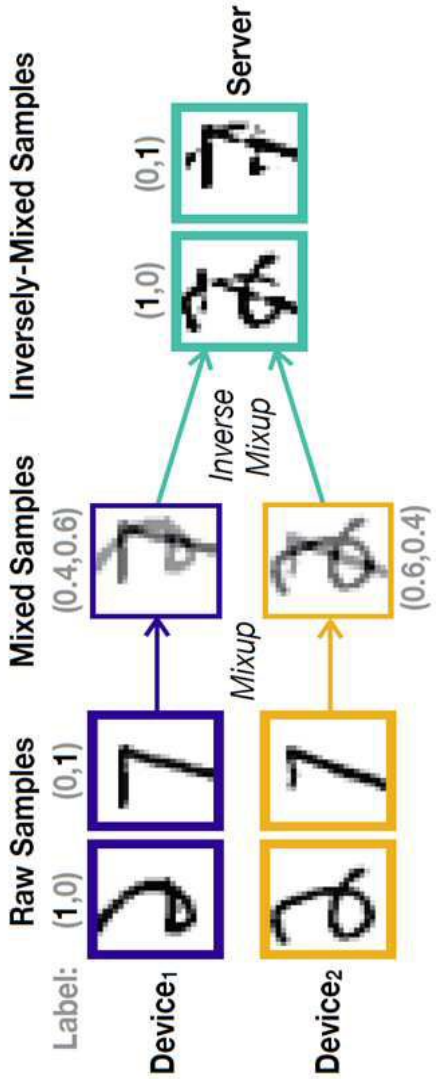

200
시작
210
복수의 이동체가 이미지 전송
220
딥러닝 모델을 이용하여 출력한 샘플 데이터에서 개인정보를 제외한 샘플 이미지를 서로 공유
230
샘플 이미지에 대한 예측값 공유
240
공유된 예측값을 딥러닝 모델에 다시 입력하여 역 믹스업 된 예측값 출력
250
역 믹스업된 예측값을 이미지의 라벨값으로 입력
끝

도면3



도면4

400


Server
Inversely-Mixed Samples
(0,1)
(1,0)
Inverse Mixup
Mixed Samples
(0.4,0.6)
(0.6,0.4)
Mixup
Raw Samples
(0,1)
(1,0)
Label:
Device1
Device2