

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2025-0079326
(43) 공개일자 2025년06월04일

(51) 국제특허분류(Int. Cl.)
G06N 3/098 (2023.01) H04L 67/10 (2022.01)
(52) CPC특허분류
G06N 3/098 (2023.01)
H04L 67/10 (2022.05)
(21) 출원번호 10-2023-0166385
(22) 출원일자 2023년11월27일
심사청구일자 2023년11월27일

(71) 출원인
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
이슬기
울산광역시 울주군 언양읍 유니스트길 50 (반연리, 울산과학기술원)
정이수
울산광역시 울주군 언양읍 유니스트길 50 (반연리, 울산과학기술원)
(74) 대리인
특허법인 수

전체 청구항 수 : 총 32 항

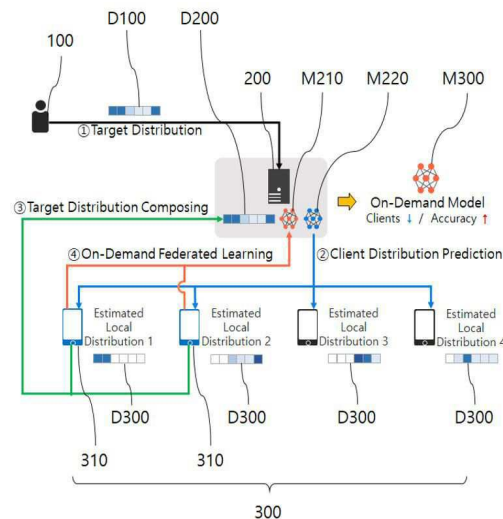
(54) 발명의 명칭 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법

(57) 요약

본 발명은 연합학습에서 필요한 클러스터링을 효율적으로 구성하고, 서버에서 필요한 만큼 클러스터링을 구성하여 요구 기반 모델의 학습을 수행할 수 있는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법에 관한 것이다.

본 발명의 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 사용자로부터 원하는 타겟 클래스 분포를 지정받아 연합학습을 수행하는 학습서버 및 타겟 클래스 분포에 맞추어 서버셋을 구성하여 학습서버와 연합학습을 수행하는 클라이언트로 이루어진다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711193983
과제번호	2020-0-01336-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	인공지능대학원지원(울산과학기술원)
기 여 율	50.00/100
과제수행기관명	울산과학기술원
연구기간	2023.01.01 ~ 2023.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711199491
과제번호	00277383
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	야생에서 학습하기: 효율적인 온-디바이스 트레이닝을 위해 무엇을, 언제, 어떻게
학습해야 하는가	
기 여 율	50.00/100
과제수행기관명	울산과학기술원
연구기간	2023.09.01 ~ 2024.02.29

명세서

청구범위

청구항 1

사용자로부터 원하는 타겟 클래스 분포를 지정받아 연합학습을 수행하는 학습서버; 및
상기 타겟 클래스 분포에 맞추어 서버셋을 구성하여 상기 학습서버와 연합학습을 수행하는 클라이언트;를 포함하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 2

제 1항에 있어서,
상기 학습서버는 상기 클라이언트의 상기 타겟 클래스 분포를 토대로 서버셋을 구성하기 위해 상기 클라이언트의 클래스 분포를 예측하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 3

제 2항에 있어서,
상기 클래스 분포를 예측하는 클래스 분포 예측 모델은 심층신경망(DNN; Deep Neural Network)을 사용하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 4

제 3항에 있어서,
상기 클래스 분포 예측 모델은 연합학습 알고리즘을 이용하여 업데이트되는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 5

제 4항에 있어서,
상기 학습서버는 상기 클래스 분포 예측 모델의 업데이트와 동시에 타스크 모델의 학습을 동시에 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 6

제 5항에 있어서,
상기 클래스 분포 예측 모델은 상기 타스크 모델의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 7

제 6항에 있어서,
상기 클래스 분포 예측 모델은 상기 타스크 모델의 학습 중에 상기 타스크 모델의 기울기(gradient)와 전체 데이터에서 일부 데이터를 추출한 미니 배치의 클래스 분포를 토대로 학습을 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 8

제 7항에 있어서,
상기 클라이언트에서 학습된 상기 클래스 분포 예측 모델은 상기 학습서버로 전송되어 다른 상기 클라이언트에서 학습된 모델과 함께 집계되는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 9

제 8항에 있어서,

상기 클라이언트는 상기 타스크 모델의 기울기(gradient)인 타스크 모델 출력을 상기 학습서버로 전송하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 10

제 9항에 있어서,

상기 학습서버는 상기 클라이언트에서 전송한 상기 타스크 모델 출력을 토대로 상기 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 11

제 10항에 있어서,

상기 학습서버는 상기 클라이언트에서 전송한 상기 타스크 모델 출력의 평균을 토대로 상기 클래스 분포를 예측하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 12

제 11항에 있어서,

상기 학습서버는 예측한 상기 클라이언트의 상기 클래스 분포를 토대로 상기 타겟 클래스 분포를 이루는 서브셋을 구성하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 13

제 12항에 있어서,

상기 타겟 클래스 분포는 예측한 상기 클라이언트의 상기 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출되는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 14

제 13항에 있어서,

상기 학습서버는 상기 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 지정하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 15

제 14항에 있어서,

상기 학습서버는 상기 서브셋으로 사용할 상기 클래스 분류된 클라이언트의 개수를 연합학습이 가능한 최소의 개수로 지정하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 16

제 15항에 있어서,

상기 학습서버는 상기 서브셋으로 사용할 상기 클래스 분류된 클라이언트와 함께 요구 기반 모델에 대한 연합학습을 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템.

청구항 17

학습서버에서 사용자로부터 원하는 타겟 클래스 분포를 지정받는 타겟 클래스 분포 지정 단계;

상기 학습서버에서 클라이언트의 클래스 분포를 예측하는 클래스 분포 예측 단계;

상기 클라이언트에서 상기 타겟 클래스 분포에 맞추어 상기 클라이언트의 서브셋을 구성하는 서브셋 구성 단계;

및

상기 학습서버에서 상기 서브셋과 요구 기반 모델의 학습을 수행하는 요구 기반 모델 학습 단계;를 포함하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 18

제 17항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클라이언트의 상기 타겟 클래스 분포를 토대로 서브셋을 구성하기 위해 상기 클라이언트의 클래스 분포를 예측하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 19

제 18항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클래스 분포를 예측에 사용되는 클래스 분포 예측 모델은 심층신경망(DNN; Deep Neural Network)을 사용하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 20

제 19항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클래스 분포 예측 모델은 연합학습 알고리즘을 이용하여 업데이트되는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 21

제 20항에 있어서,

상기 클래스 분포 예측 단계에서 상기 학습서버는 상기 클래스 분포 예측 모델의 업데이트와 동시에 타스크 모델의 학습을 동시에 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 22

제 21항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클래스 분포 예측 모델은 상기 타스크 모델의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 23

제 22항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클래스 분포 예측 모델은 상기 타스크 모델의 학습 중에 상기 타스크 모델의 기울기(gradient)와 전체 데이터에서 일부 데이터를 추출한 미니 배치의 클래스 분포를 토대로 학습을 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 24

제 23항에 있어서,

상기 클래스 분포 예측 단계에서는 상기 클라이언트에서 학습된 상기 클래스 분포 예측 모델을 상기 학습서버로 전송하여 상기 학습서버에서 다른 상기 클라이언트에서 학습된 모델과 함께 집계하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 25

제 24항에 있어서,

상기 클래스 분포 예측 단계에서 상기 클라이언트는 상기 타스크 모델의 기울기(gradient)인 타스크 모델 출력을 상기 학습서버로 전송하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 26

제 25항에 있어서,

상기 클래스 분포 예측 단계에서 상기 학습서버는 상기 클라이언트에서 전송한 상기 타스크 모델 출력을 토대로 상기 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 27

제 26항에 있어서,

상기 클래스 분포 예측 단계에서 상기 학습서버는 상기 클라이언트에서 전송한 상기 타스크 모델 출력의 평균을 토대로 상기 클래스 분포를 예측하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 28

제 27항에 있어서,

상기 서브셋 구성 단계에서 상기 학습서버는 예측한 상기 클라이언트의 상기 클래스 분포를 토대로 상기 타겟 클래스 분포를 이루는 서브셋을 구성하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 29

제 28항에 있어서,

상기 서브셋 구성 단계에서 상기 타겟 클래스 분포는 예측한 상기 클라이언트의 상기 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출되는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 30

제 29항에 있어서,

상기 서브셋 구성 단계에서 상기 학습서버는 상기 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 지정하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 31

제 30항에 있어서,

상기 서브셋 구성 단계에서 상기 학습서버는 상기 서브셋으로 사용할 상기 클래스 분류된 클라이언트의 개수를 연합학습이 가능한 최소의 개수로 지정하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

청구항 32

제 31항에 있어서,

상기 요구 기반 모델 학습 단계에서 상기 학습서버는 상기 서브셋으로 사용할 상기 클래스 분류된 클라이언트와 함께 상기 요구 기반 모델에 대한 연합학습을 수행하는 것을 특징으로 하는 임의의 타겟 클래스 분포에 최적화된 연합학습 방법.

발명의 설명

기술 분야

본 발명은 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법에 관한 것으로, 상세하게는, 서버와 다수의 클라이언트 간 연관성 있는 클라이언트만 클러스터링하여 연합학습을 수행하는 것이다.

[0001]

[0002] 또한, 본 발명은 서버와 연관성 있는 클라이언트만 클러스터링하여 저렴한 비용으로 클라이언트를 관리할 수 있는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법에 관한 것이다.

배경 기술

[0003] 연합학습(Federated Learning)은 다수의 로컬 클라이언트들의 데이터가 탈 중앙화 된 상태에서, 서버와 클라이언트들이 협력하여 데이터를 학습하는 알고리즘이다.

[0004] 클라이언트는 로컬 데이터로 로컬 태스크 모델을 학습시키고, 서버에 로컬 태스크 모델을 전송한다. 서버는 여러 클라이언트들의 태스크 모델을 집계하여 단일 글로벌 태스크 모델을 생성한다.

[0005] 데이터를 전송하지 않고, 태스크 모델만을 전송하므로, 개인정보 보호에 이점이 있다. 그러나, 단일 글로벌 태스크 모델을 생성하기 때문에 특히 불균형하게 분포된(non-IID) 로컬 클라이언트 데이터 분포에서 잘 일반화되기 어려운 단점이 있다.

[0006] 이러한 단점을 보완하기 위해 개인화된연합학습(Personalized Federated Learning)이 연구 되었는데, 이는 하나의 글로벌 태스크 모델이 아니라, 로컬 클라이언트에 최적화된 태스크 모델을 학습시키는 알고리즘이다.

[0007] 로컬 클라이언트의 데이터 분포에 한정되어, 제한적인 데이터 분포에 최적화된 태스크 모델을 학습시킨다. 그러나 학습 데이터가 적어 신뢰성이 떨어지는 단점이 있다.

[0008] 한편, 클러스터연합학습(Clustered Federated Learning)은 이러한 단점을 보완하기 위해 태스크 모델 학습 방향이 비슷한 로컬 클라이언트들끼리 묶어, 클러스터를 만들고, 클러스터 당 태스크 모델을 생성하는 알고리즘이다.

[0009] 그러나, 클러스터링에 많은 계산 비용이 요구되어 이를 극복하기 위한 연구가 지속되어 왔다.

[0010] 그 일례로, 미국 공개특허공보 제2022-709237호에서는 명령을 인스턴스화하거나 실행하는 프로세서 회로에서 다른 노드로부터의 컨텍스트 데이터를 기초로 기계 학습 모델의 일부를 재학습하는 컨텍스트 데이터를 사용한 클러스터화된 연합 학습 장치에 관해 개시하고 있다.

[0011] 그러나, 이 경우에도 업데이트에 일부 컨텍스트 데이터를 사용할 뿐 여전히 클러스터링에 많은 계산 비용이 요구되며, 이를 저장하기 위한 많은 메모리가 필요한 단점이 있다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 미국 공개특허공보 제2022-709237호(2022.07.14.)

발명의 내용

해결하려는 과제

[0013] 본 발명의 목적은, 연합학습에서 필요한 클러스터링을 효율적으로 구성하는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법을 제공하는 것이다.

[0014] 본 발명은 서버에서 필요한만큼 클러스터링을 구성하여 요구 기반 모델의 학습을 수행할 수 있는 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법을 제공하는데 또 다른 목적이 있다.

과제의 해결 수단

[0015] 본 발명에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 사용자로부터 원하는 타겟 클래스 분포를 지정받아 연합학습을 수행하는 학습서버 및 타겟 클래스 분포에 맞추어 서브셋을 구성하여 학습서버와 연합학습을 수행하는 클라이언트를 포함할 수 있다.

[0016] 여기서, 학습서버는 클라이언트의 타겟 클래스 분포를 토대로 서브셋을 구성하기 위해 클라이언트의 클래스 분포를 예측할 수 있다.

- [0017] 또한, 클래스 분포를 예측하는 클래스 분포 예측 모델은 심층신경망(DNN Deep Neural Network)을 사용할 수 있다.
- [0018] 여기서, 클래스 분포 예측 모델은 연합학습 알고리즘을 이용하여 업데이트될 수 있다.
- [0019] 또한, 학습서버는 클래스 분포 예측 모델의 업데이트와 동시에 타스크 모델의 학습을 동시에 수행할 수 있다.
- [0020] 여기서, 클래스 분포 예측 모델은 타스크 모델의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 할 수 있다.
- [0021] 또한, 클래스 분포 예측 모델은 타스크 모델의 학습 중에 타스크 모델의 기울기(gradient)와 전체 데이터에서 일부 데이터를 추출한 미니 배치의 클래스 분포를 토대로 학습을 수행할 수 있다.
- [0022] 여기서, 클라이언트에서 학습된 클래스 분포 예측 모델은 학습서버로 전송되어 다른 클라이언트에서 학습된 모델과 함께 집계될 수 있다.
- [0023] 또한, 클라이언트는 타스크 모델의 기울기(gradient)인 타스크 모델 출력을 학습서버로 전송할 수 있다.
- [0024] 여기서, 학습서버는 클라이언트에서 전송한 타스크 모델 출력을 토대로 클래스 분포를 예측한 뒤에 해당 예측값들을 평균할 수 있다.
- [0025] 또한, 학습서버는 클라이언트에서 전송한 타스크 모델 출력의 평균을 토대로 클래스 분포를 예측할 수 있다.
- [0026] 여기서, 학습서버는 예측한 클라이언트의 클래스 분포를 토대로 타겟 클래스 분포를 이루는 서브셋을 구성할 수 있다.
- [0027] 또한, 타겟 클래스 분포는 예측한 클라이언트의 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출된다.
- [0028] 여기서, 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 지정할 수 있다.
- [0029] 또한, 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 연합학습이 가능한 최소의 개수로 지정할 수 있다.
- [0030] 한편, 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트와 함께 요구 기반 모델에 대한 연합학습을 수행할 수 있다.
- [0031] 본 발명의 다른 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 방법은 학습서버에서 사용자로부터 원하는 타겟 클래스 분포를 지정받는 타겟 클래스 분포 지정 단계, 학습서버에서 클라이언트의 클래스 분포를 예측하는 클래스 분포 예측 단계, 클라이언트에서 타겟 클래스 분포에 맞추어 클라이언트의 서브셋을 구성하는 서브셋 구성 단계, 및 학습서버에서 서브셋과 요구 기반 모델의 학습을 수행하는 요구 기반 모델 학습 단계를 포함할 수 있다.
- [0032] 여기서, 클래스 분포 예측 단계에서 클라이언트의 타겟 클래스 분포를 토대로 서브셋을 구성하기 위해 클라이언트의 클래스 분포를 예측할 수 있다.
- [0033] 또한, 클래스 분포 예측 단계에서 클래스 분포를 예측에 사용되는 클래스 분포 예측 모델은 심층신경망(DNN Deep Neural Network)을 사용할 수 있다.
- [0034] 여기서, 클래스 분포 예측 단계에서 클래스 분포 예측 모델은 연합학습 알고리즘을 이용하여 업데이트될 수 있다.
- [0035] 또한, 클래스 분포 예측 단계에서 학습서버는 클래스 분포 예측 모델의 업데이트와 동시에 타스크 모델의 학습을 동시에 수행할 수 있다.
- [0036] 여기서, 클래스 분포 예측 단계에서 클래스 분포 예측 모델은 타스크 모델의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 할 수 있다.
- [0037] 또한, 클래스 분포 예측 단계에서 클래스 분포 예측 모델은 타스크 모델의 학습 중에 타스크 모델의 기울기(gradient)와 전체 데이터에서 일부 데이터를 추출한 미니 배치의 클래스 분포를 토대로 학습을 수행할 수 있다.
- [0038] 여기서, 클래스 분포 예측 단계에서는 클라이언트에서 학습된 클래스 분포 예측 모델을 학습서버로 전송하여 학습서버에서 다른 클라이언트에서 학습된 모델과 함께 집계할 수 있다.

- [0039] 또한, 클래스 분포 예측 단계에서 클라이언트는 타스크 모델의 기울기(gradient)인 타스크 모델 출력을 학습서버로 전송할 수 있다.
- [0040] 여기서, 클래스 분포 예측 단계에서 학습서버는 클라이언트에서 전송한 타스크 모델 출력을 토대로 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균할 수 있다.
- [0041] 또한, 클래스 분포 예측 단계에서 학습서버는 클라이언트에서 전송한 타스크 모델 출력의 평균을 토대로 클래스 분포를 예측할 수 있다.
- [0042] 여기서, 서브셋 구성 단계에서 학습서버는 예측한 클라이언트의 클래스 분포를 토대로 타겟 클래스 분포를 이루는 서브셋을 구성할 수 있다.
- [0043] 또한, 서브셋 구성 단계에서 타겟 클래스 분포는 예측한 클라이언트의 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출된다.
- [0044] 여기서, 서브셋 구성 단계에서 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 지정할 수 있다.
- [0045] 또한, 서브셋 구성 단계에서 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트의 개수를 연합학습이 가능한 최소의 개수로 지정할 수 있다.
- [0046] 여기서, 요구 기반 모델 학습 단계에서 학습서버는 서브셋으로 사용할 클래스 분류된 클라이언트와 함께 요구 기반 모델에 대한 연합학습을 수행할 수 있다.

발명의 효과

- [0047] 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법은 연합학습에서 필요한 클러스터링을 효율적으로 구성하는 장점이 있다.
- [0048] 또한, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법은 서버에서 필요한 만큼 클러스터링을 구성하여 요구 기반 모델의 학습을 수행할 수 있는 장점이 있다.

도면의 간단한 설명

- [0049] 도 1은 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템을 나타낸 개략구성도이다.
- 도 2는 도 1의 클라이언트가 클래스 분포를 출력하는 구성을 상세히 나타낸 도면이다.
- 도 3은 도 1의 학습서버가 클래스 분포를 평균내는 구성을 상세히 나타낸 도면으로서, 도 3(a)는 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 것을 나타내며, 도 3(b)는 클라이언트에서 전송한 타스크 모델 출력의 평균을 토대로 클래스 분포를 예측하는 것을 나타낸다.
- 도 4는 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 방법을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0050] 이하, 본 발명의 실시를 위한 구체적인 실시예를 첨부된 도면들을 참조하여 설명한다.
- [0051] 본 발명을 설명함에 있어서 제 1, 제 2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 용어들에 의해 한정되지 않을 수 있다. 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 된다. 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.
- [0052] 어떤 구성요소가 다른 구성요소에 연결되어 있거나 접속되어 있다고 언급되는 경우는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해될 수 있다.
- [0053] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다.
- [0054] 본 명세서에서, 포함하다 또는 구비하다 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부

품 또는 이들을 조합한 것이 존재함을 지정하려는 것으로서, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해될 수 있다.

- [0055] 또한, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.
- [0056] 이하, 첨부된 도면을 참조하여 본 발명에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법에 대해 상세히 설명한다.
- [0058] 도 1은 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템을 나타낸 개략구성도이며, 도 2 및 도 3은 도 1을 상세히 설명하기 위한 세부 도면이다.
- [0059] 이하, 도 1 내지 도 3을 참조하여 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템을 설명한다.
- [0060] 먼저, 도 1을 참조하면, 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 사용자(100)로부터 원하는 타겟 클래스 분포를 지정받아 연합학습을 수행하는 학습서버(200) 및 타겟 클래스 분포로 분류되어 학습서버(200)와 연합학습을 수행하는 클라이언트(300)로 이루어진다.
- [0061] 기존 연합학습 알고리즘들은 글로벌 태스크 모델(global task model)을 생성하거나, 특정 로컬 클라이언트(local client)에 맞춤형 된 로컬 태스크 모델을 학습시킨다.
- [0062] 반면, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 사용자(100)로부터 원하는 타겟 클래스 분포를 지정받아 임의의 타겟 클래스 분포에 맞춰진 태스크 모델(M210)을 생성하기 위해 연합학습을 수행한다.
- [0063] 즉, 클라이언트(300) 중 일부를 골라 서버셋을 구성하여, 적은 수의 클래스 분류된 클라이언트(310)로 더 좋은 성능을 보이는 요구 기반 모델(M300)을 학습시킨다.
- [0064] 이때, 학습서버(200)는 클라이언트(300)의 타겟 클래스 분포를 토대로 서버셋을 구성하기 위해 클라이언트(300)의 클래스 분포 예측 모델(M220)을 연합학습으로 학습하여 클래스 분포를 예측한다.
- [0065] 클래스 분포 예측 모델(M220)로 추정된 클라이언트(300)의 클래스 분포를 조합하여 타겟 클래스를 구성한다. 타겟 클래스를 구성하는데 쓰인 클래스 분류된 클라이언트(310)들이 서버셋에 해당한다.
- [0066] 따라서, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 클래스 분포를 사용하므로 직관적이고 사용자 친화적이며, 적은 수의 클래스 분류된 클라이언트(310)를 사용하므로 학습서버(200)의 클라이언트(300)에 대한 관리 비용이 줄어드는 장점이 있다.
- [0067] 또한, 산업사물인터넷(IIOT; Industrial Internet of Things) 시스템 분야에서는 수 많은 센서가 산업 환경을 모니터링하고 공정 환경을 제어한다.
- [0068] 여기서, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 초기 통신 라운드 후 임의의 타겟 클래스 분포를 구성하는 클라이언트(300)의 하위 집합을 구성하여 연합 학습에 필요한 장치 수를 줄일 수 있으며, 이로써 모든 클라이언트(300)와 통신할 필요성이 없고, 통신 비용을 절감하면서 원하는 클래스 분포에 대한 모델을 학습시킬 수 있는 장점이 있다.
- [0069] 한편, 공유 경제 분야에서는 사람들이 자원을 소유하지 않고 공유하기 때문에, 해당 서비스에 포함된 스마트 기기의 사용자는 자주 바뀌며, 한 명의 사용자에게 최적화된 모델을 학습시키는 것은 어렵다.
- [0070] 이때, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템에서 신규로 서비스를 대여하는 사용자(100)는 디바이스에 축적된 데이터가 아닌 자신의 사용 패턴을 반영한 데이터에 최적화된 서비스를 요청할 수 있으며, 따라서 클래스 분포가 직관적이기 때문에 사용자는 원하는 데이터 클래스에 대해 훈련된 홈 장치를 쉽게 사용할 수 있는 장점이 있다.
- [0072] 도 2는 도 1의 클라이언트(300)가 클래스 분포를 출력하는 구성을 상세히 나타낸 도면이다.
- [0073] 도 2에서 볼 수 있는 바와 같이, 클래스 분포를 예측하는 클래스 분포 예측 모델(M220)은 심층신경망(DNN Deep

Neural Network)을 사용하며, 학습서버(200)와 클라이언트(300) 간 연합학습 알고리즘을 이용하여 업데이트된다.

[0074] 또한, 학습서버(200)는 클래스 분포 예측 모델(M220)의 업데이트와 동시에 타스크 모델(M210)의 학습을 동시에 수행할 수 있다.

[0075] 상세하게는, 클래스 분포 예측 모델(M220)은 타스크 모델(M210)의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 한다.

[0076] 즉, 타스크 모델(M210)의 학습 중에 타스크 모델(M210)의 기울기(gradient)와 전체 데이터(D400)에서 일부 데이터를 추출한 미니 배치(D410)의 클래스 분포를 토대로 학습을 수행한다.

[0077] 한편, 클라이언트(300)에서 학습된 클래스 분포 예측 모델(M220)은 학습서버(200)로 전송되어 다른 클라이언트(300)에서 학습된 클래스 분포 예측 모델(M220)과 함께 집계되며, 이러한 집계 방법은 도 3에서 상세히 설명한다.

[0079] 도 3은 도 1의 학습서버(200)가 클래스 분포를 평균내는 구성을 상세히 나타낸 도면으로서, 도 3(a)는 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 것을 나타내며, 도 3(b)는 클라이언트(300)에서 전송한 타스크 모델 출력(D500)의 평균을 토대로 클래스 분포를 예측하는 것을 나타낸다.

[0080] 도 3에서 알 수 있는 바와 같이, 클라이언트(300)는 타스크 모델(M210)의 기울기(gradient)인 타스크 모델 출력(D500)을 학습서버(200)로 전송하고 학습서버(200)는 클라이언트(300)에서 전송한 타스크 모델 출력(D500)을 토대로 평균을 수행하는 방법은 두 가지로 할 수 있다.

[0081] 즉, 도 3(a)와 같이 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 방법과, 도 3(b)와 같이 클라이언트(300)에서 전송한 타스크 모델 출력(D500)의 평균을 토대로 클래스 분포를 예측하는 방법이다.

[0082] 이후, 학습서버(200)는 예측한 클라이언트(300)의 클래스 분포를 토대로 타겟 클래스 분포를 이루는 서브셋을 구성한다.

[0083] 아래 수학적 식 1에서 $r_{cn} > 0$ 인 클라이언트들이 서브셋에 속하게 되며, 수학적 식 1은 가중치(weight)가 음수가 되는 것을 허용하지 않는 수학적 최적화 기술인 음수없는 최소자승법(NNLS: Non-Negative Least Squares)을 이용하여 푼다.

[0084] 또한, 몇 개의 클라이언트를 선택할 지 지정할 수 있으며, 즉 적은 클라이언트들을 선택하여 서브셋을 구성 가능하다.

[0085] [수학적 식 1]

$$\begin{bmatrix} d_t^1 \\ \vdots \\ d_t^n \end{bmatrix} = \begin{bmatrix} d_{c_1}^1 & d_{c_2}^1 & \cdots & d_{c_m}^1 \\ \vdots & \vdots & \ddots & \vdots \\ d_{c_1}^n & d_{c_2}^n & \cdots & d_{c_m}^n \end{bmatrix} \begin{bmatrix} r_{c_1} \\ \vdots \\ r_{c_m} \end{bmatrix},$$

[0086] 여기서, d_t 는 타겟 클래스 분포, d_c 는 예측한 클라이언트의 클래스 분포,

[0088] r 은 서브셋 구성을 위한 가중치.

[0090] 또한, 타겟 클래스 분포는 예측한 클라이언트(300)의 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출된다.

[0091] 여기서, 학습서버(200)는 서브셋으로 사용할 클래스 분류된 클라이언트(310)의 개수를 지정할 수 있으며, 연합학습이 가능한 최소의 개수로 지정하는 것이 바람직하다.

[0092] 한편, 학습서버(200)는 서브셋으로 사용할 클래스 분류된 클라이언트(310)와 함께 요구 기반 모델(M300)에 대한

연합학습을 아래 수식식 2와 같이 수행할 수 있다.

[0093] [수식식 2]

$$w \leftarrow \sum_c r^c \frac{n^c}{n},$$

[0095] 여기서, c 는 각 클라이언트의 인덱스, w 는 모델의 파라미터 (가중치), n 은 전체 클라이언트의 데이터 개수, n^c 는 해당 클라이언트의 데이터 개수.

[0097] 이와 같은 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템은 이와 같이 타겟 클래스 분포를 구성하는 서버셋에 한정하여 연합학습을 통해 요구 기반 모델(M300)을 학습시킴으로써, 적은 수의 클래스 분류된 클라이언트(310)를 사용하여 학습서버(200)의 클라이언트(300)에 대한 관리 비용이 줄어드는 장점이 있다.

[0099] 다음, 도 4는 본 발명의 일 실시예에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 방법을 나타낸 순서도이다.

[0100] 도 4에서 볼 수 있는 바와 같이, 임의의 타겟 클래스 분포에 최적화된 연합학습 방법은 학습서버(200)에서 사용자(100)로부터 원하는 타겟 클래스 분포를 지정받는 타겟 클래스 분포 지정 단계(S100), 학습서버(200)에서 클라이언트(300)의 클래스 분포를 예측하는 클래스 분포 예측 단계(S200), 클라이언트(300)에서 타겟 클래스 분포에 맞추어 클라이언트(300)의 서버셋을 구성하는 서버셋 구성 단계(S300), 및 학습서버(200)에서 서버셋과 요구 기반 모델(M300)의 학습을 수행하는 요구 기반 모델 학습 단계(S400)로 이루어진다.

[0101] 기존 연합학습 알고리즘들은 글로벌 태스크 모델(global task model)을 생성하거나, 특정 로컬 클라이언트(local client)에 맞춤형 된 태스크 모델을 학습시킨다.

[0102] 반면, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 방법은 타겟 클래스 분포 지정 단계(S100)에서 사용자(100)로부터 원하는 타겟 클래스 분포를 지정받아 임의의 타겟 클래스 분포에 맞춰진 태스크 모델(M210)을 생성하기 위해 연합학습을 수행한다.

[0103] 즉, 클라이언트(300) 중 일부를 골라 서버셋을 구성하여, 적은 수의 클래스 분류된 클라이언트(310)로 더 좋은 성능을 보이는 요구 기반 모델(M300)을 학습시킬 수 있는 장점이 있다.

[0104] 이때, 클래스 분포 예측 단계(S200)에서는 학습서버(200)는 클라이언트(300)의 타겟 클래스 분포를 토대로 서버셋을 구성하기 위해 클라이언트(300)의 클래스 분포 예측 모델(M220)을 연합학습으로 학습하여 클래스 분포를 예측한다.

[0105] 서버셋 구성 단계(S300)에서는 클래스 분포 예측 모델(M220)로 추정된 클라이언트(300)의 클래스 분포를 조합하여 타겟 클래스를 구성한다. 타겟 클래스를 구성하는데 쓰인 클래스 분류된 클라이언트(310)들이 서버셋에 해당하며, 최종적으로 요구 기반 모델 학습 단계(S400)에서 클래스 분류된 클라이언트(310)와 함께 요구 기반 모델(M300)에 대한 연합학습을 수행한다.

[0106] 따라서, 본 발명에 의한 임의의 타겟 클래스 분포에 최적화된 연합학습 방법은 클래스 분포를 사용하므로 직관적이고 사용자 친화적이며, 적은 수의 클래스 분류된 클라이언트(310)를 사용하므로 학습서버(200)의 클라이언트(300)에 대한 관리 비용이 줄어드는 장점이 있다.

[0107] 한편, 클래스 분포 예측 단계(S200)에서는 클라이언트(300)의 타겟 클래스 분포를 토대로 서버셋을 구성하기 위해 클라이언트(300)의 클래스 분포를 예측하는데, 이때, 클래스 분포를 예측에 사용되는 클래스 분포 예측 모델(M220)은 심층신경망(DNN Deep Neural Network)을 사용하며, 학습서버(200)와 클라이언트(300) 간 연합학습 알고리즘을 이용하여 업데이트된다.

[0108] 또한, 클래스 분포 예측 단계(S200)에서 학습서버(200)는 클래스 분포 예측 모델(M220)의 업데이트와 동시에 태스크 모델(M210)의 학습을 동시에 수행할 수 있는데, 상세하게는 클래스 분포 예측 모델(M220)은 태스크 모델(M210)의 마지막 레이어의 기울기(gradient)를 입력값으로 하고 클래스 분포를 출력값으로 한다.

[0109] 즉, 태스크 모델(M210)의 학습 중에 태스크 모델(M210)의 기울기(gradient)와 전체 데이터(D400)에서 일부 데이

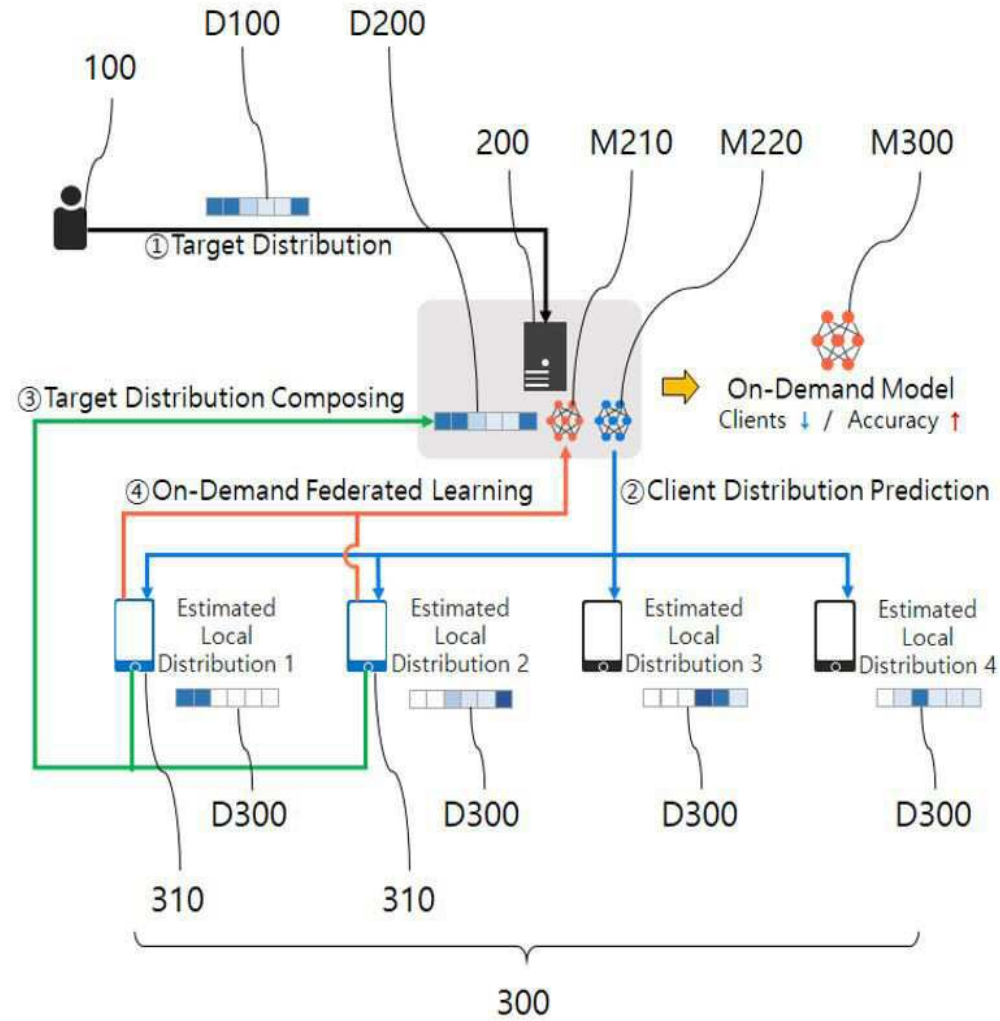
터를 추출한 미니 배치(D410)의 클래스 분포를 토대로 학습을 수행한다.

- [0110] 한편, 클라이언트(300)에서 학습된 클래스 분포 예측 모델(M220)은 학습서버(200)로 전송되어 다른 클라이언트(300)에서 학습된 클래스 분포 예측 모델(M220)과 함께 집계된다.
- [0111] 또한, 클래스 분포 예측 단계(S200)에서 클라이언트(300)는 타스크 모델(M210)의 기울기(gradient)인 타스크 모델 출력(D500)을 학습서버(200)로 전송하고 학습서버(200)는 클라이언트(300)에서 전송한 타스크 모델 출력(D500)을 토대로 평균을 수행하는 방법은 두 가지로 할 수 있다.
- [0112] 즉, 상술한 도 3(a)와 같이 클래스 분포를 예측한 뒤에 해당 예측 값들을 평균하는 방법과 도 3(b)와 같이 클라이언트(300)에서 전송한 타스크 모델 출력(D500)의 평균을 토대로 클래스 분포를 예측하는 방법이다.
- [0113] 이후, 서브셋 구성 단계(S300)에서 학습서버(200)는 예측한 클라이언트(300)의 클래스 분포를 토대로 타겟 클래스 분포를 이루는 서브셋을 구성한다.
- [0114] 예측한 클라이언트의 클래스 분포를 기반으로 타겟 클래스 분포를 이루는 서브셋을 구성하는 것은 상기 수학적식 1에서 상세히 설명하였으므로, 이에 대한 설명은 생략한다.
- [0115] 또한, 서브셋 구성 단계(S300)에서 타겟 클래스 분포는 예측한 클라이언트(300)의 클래스 분포에 서브셋 구성을 위한 가중치를 곱하여 도출된다.
- [0116] 여기서, 학습서버(200)는 서브셋으로 사용할 클래스 분류된 클라이언트(310)의 개수를 지정할 수 있으며, 연합학습이 가능한 최소의 개수로 지정한다.
- [0117] 한편, 학습서버(200)는 서브셋으로 사용할 클래스 분류된 클라이언트(310)와 함께 요구 기반 모델(M300)에 대한 연합학습을 상술한 수학적식 2와 같이 수행할 수 있으며, 앞서 설명한 바가 있으므로 이에 대한 설명은 생략한다.
- [0119] 이상과 같이, 본 발명에 따른 임의의 타겟 클래스 분포에 최적화된 연합학습 시스템 및 그 방법은 연합학습에서 필요한 클러스터링을 효율적으로 구성하는 장점이 있으며, 서버에서 필요한만큼 클러스터링을 구성하여 요구 기반 모델의 학습을 수행할 수 있는 장점이 있다.
- [0121] 본 발명의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 소프트웨어로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 발명의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 발명의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.
- [0122] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조물품(article)으로 구현될 수 있다. 용어 제조물품은 임의의 컴퓨터-판독가능 저장장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트림, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 또한, 여기서 제시되는 다양한 저장 매체는 정보를 저장하기 위한 하나 이상의 장치 및/또는 다른 기계-판독가능한 매체를 포함한다.
- [0123] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 설계 우선순위들에 기반하여, 본 발명의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.
- [0124] 제시된 실시예들에 대한 설명은 임의의 본 발명의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 이용하거

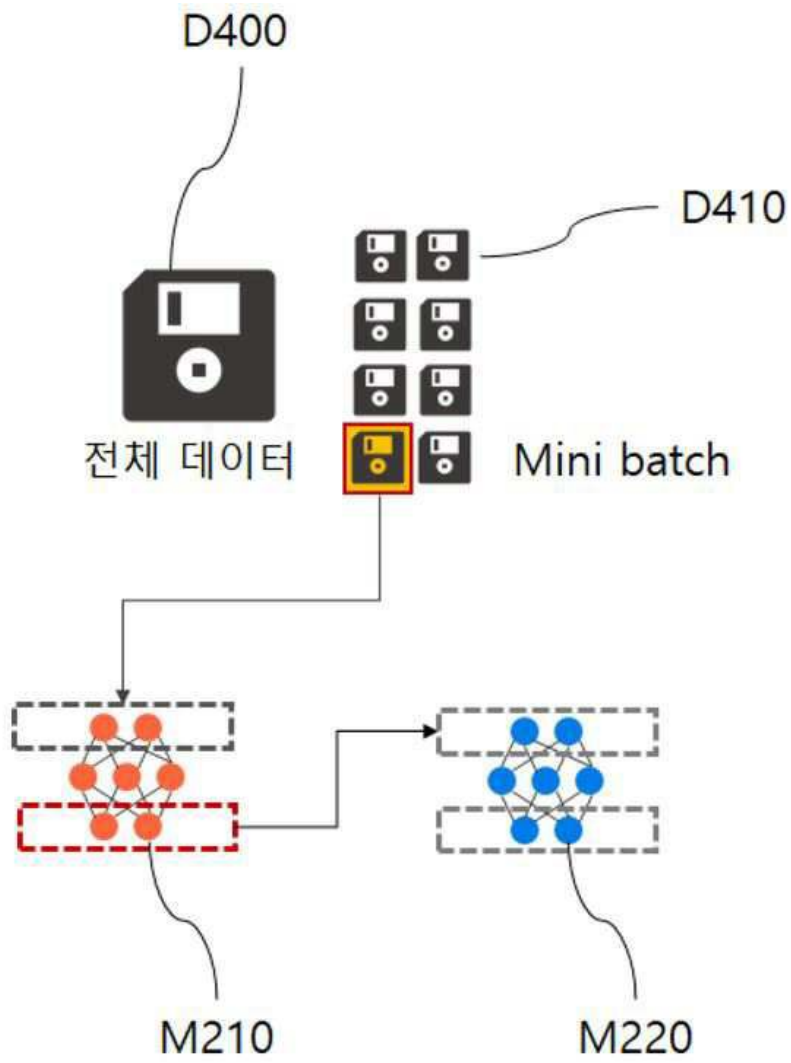
나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 발명의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

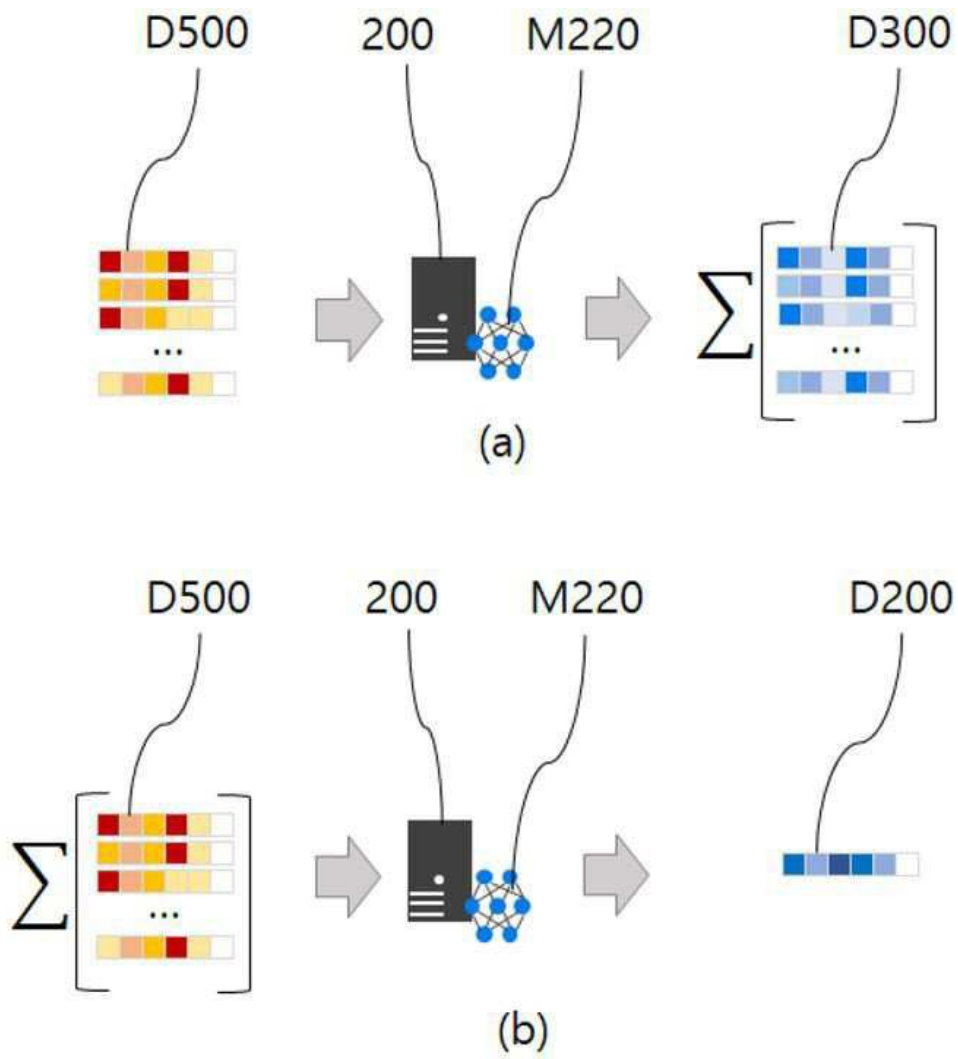
도면1



도면2



도면3



도면4

