(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년07월13일
(11) 등록번호 10-2420895
(24) 등록일자 2022년07월11일

(51) 국제특허분류(Int. Cl.)
G06N 3/04 (2006.01) *G06N 3/08* (2006.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
G06N 3/0454 (2013.01)
G06N 3/08 (2013.01)
(21) 출원번호 10-2019-0179049
(22) 출원일자 2019년12월31일
심사청구일자 2019년12월31일
(65) 공개번호 10-2021-0085702
(43) 공개일자 2021년07월08일
(56) 선행기술조사문헌
JP2019215512 A
(뒷면에 계속)
전체 청구항 수 : 총 5 항

(73) 특허권자
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
김성륜
서울특별시 용산구 한강대로 26, 101동 2407호(한강로3가, 한강대우트럼프월드3차)
오승은
제주특별자치도 제주시 대원길 13, 101동 104호(아라일동, 영도그린힐)
(74) 대리인
민영준

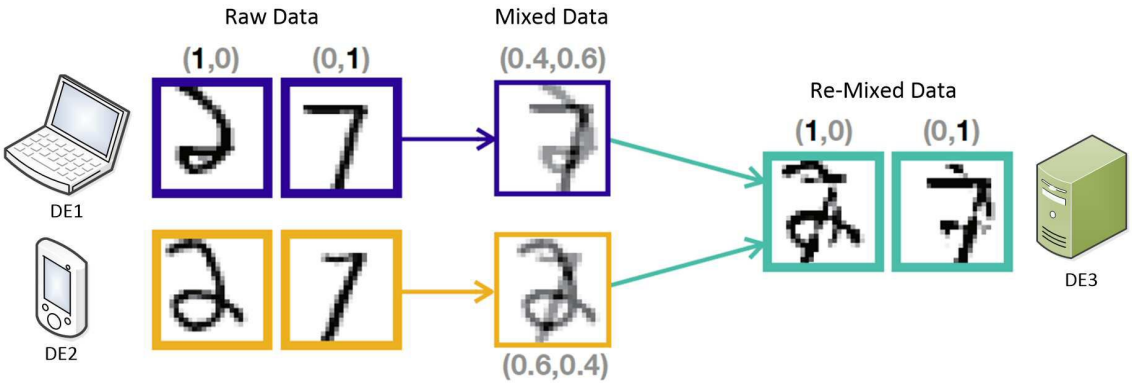
심사관 : 이준상

(54) 발명의 명칭 **다중 경로 혼합 기반 학습 데이터 획득 장치 및 방법**

(57) 요 약

본 발명은 다수의 단말 각각으로부터 다수의 학습 데이터가 혼합 비율에 따라 혼합된 혼합 데이터를 전송받고, 다수의 단말 각각으로부터 전송된 혼합 데이터를 포함된 레이블에 따라 구분하고 구분된 각 레이블을 혼합 데이터를 전송한 단말의 개수에 대응하여 구성된 재혼합 비율에 따라 재혼합하여 미리 저장된 학습 모델을 학습시키기 위한 재혼합 학습 데이터를 획득하므로, 다수의 단말 각각에서 데이터 혼합 방식으로 전송된 혼합 데이터를 재혼합하여 학습 성능을 향상시킬 수 있으며 보안성을 향상시킬 수 있는 학습 데이터 획득 장치 및 방법을 제공할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 67/10 (2022.05)

(56) 선행기술조사문헌
JP2019220114 A
KR101979115 B1
US20190087689 A1
US20190354867 A1

이 발명을 지원한 국가연구개발사업
과제고유번호 2016-0-00208
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기술진흥센터
연구사업명 방송통신산업기술개발(R&D)사업
연구과제명 (창조씨앗-2단계) 차세대 5G V2X서비스 실현을 위한 정밀 측위탐색 연계 고효율 다중안테나 정보전송 및 네트워크 기술 연구
기 여 율 1/1
과제수행기관명 연세대학교 산학협력단
연구기간 2019.01.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

다수의 단말에 의해 수행되는 학습 데이터 획득 방법에 있어서,

상기 다수의 단말 각각이 다수의 샘플 데이터를 획득하고, 획득된 상기 다수의 샘플 데이터 각각에 샘플 데이터를 분류하기 위한 레이블을 레이블링하며, 획득된 다수의 학습 데이터를 혼합 비율에 따라 혼합하여 다른 단말로 혼합 데이터를 전송하는 단계; 및

다수의 단말 각각으로부터 전송된 다수의 혼합 데이터를 상기 다수의 혼합 데이터 각각에 포함된 레이블에 따라 구분하고, 구분된 각 레이블을 혼합 데이터를 전송한 단말의 개수에 대응하여 구성된 재혼합 비율에 따라 재혼합하여 미리 저장된 학습 모델을 학습시키기 위한 재혼합 학습 데이터를 획득하는 단계를 포함하는 학습 데이터 획득 방법.

청구항 8

삭제

청구항 9

제7 항에 있어서, 상기 혼합 데이터를 획득하는 단계는

다수의 학습 데이터(x_1, x_2, …, x_n) 각각에 대응하는 개별 혼합 비율(λ_1, λ_2, …, λ_n)의 가중합($\tilde{x} = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$)으로 상기 혼합 데이터를 획득하는 학습 데이터 획득 방법.

청구항 10

제9 항에 있어서, 상기 혼합 데이터를 획득하는 단계는

상기 개별 혼합 비율(λ_1, λ_2, …, λ_n)이 학습 데이터(x_1, x_2, …, x_n) 구성하는 샘플 데이터(s_1, s_2, …, s_n)

및 벡터 형식을 갖는 레이블(l_1, l_2, …, l_n)에 각각 가중되는 학습 데이터 획득 방법.

청구항 11

제10 항에 있어서, 상기 재혼합 학습 데이터를 획득하는 단계는

다수의 단말 각각에서 전송된 혼합 데이터($\widetilde{x_1}$, $\widetilde{x_2}$, …, $\widetilde{x_m}$) 각각의 레이블(l_1, l_2, …, l_n)에 대해, 개별 재혼합 비율($\widetilde{\lambda_1}$, $\widetilde{\lambda_2}$, …, $\widetilde{\lambda_m}$)을 조절하면서 재혼합하여 다수의 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득하는 학습 데이터 획득 방법.

청구항 12

제11 항에 있어서, 상기 학습 데이터 획득 방법은

상기 재혼합 학습 데이터(x_1', x_2', … x_n')에 포함된 재혼합 샘플 데이터(s_1', s_2', … s_n')와 대응하는 재혼합 레이블(l_1', l_2', … l_n') 중 재혼합 샘플 데이터(s_1', s_2', … s_n')를 상기 학습 모델을 학습시키기 위한 입력값으로 입력하고, 재혼합 레이블(l_1', l_2', … l_n')을 진리값으로 이용하여 상기 학습 모델의 오차를 판별하고 역전파하여 상기 학습 모델을 학습시키는 단계를 더 포함하는 학습 데이터 획득 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 학습 데이터 획득 장치 및 방법에 관한 것으로, 다중 경로 혼합 기반 학습 데이터 획득 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 인공 신경망을 학습시키기 위해서는 대량의 학습 데이터를 필요로 하지만, 개별 단말이 생성하거나 획득할 수 있는 학습 데이터의 수는 매우 제한적이다. 또한 개별 단말에서 획득되는 학습 데이터는 독립 항등 분포(independent identically distributed: 이하 iid)를 따르지 않고, 각 단말의 서로 상이한 연산 능력으로 인해, 학습할 수 있는 학습 데이터의 크기가 제한되므로 높은 정확도의 학습을 수행하기 어렵다는 한계가 있다.

[0003] 이러한 한계를 극복하기 위해 최근에는 다수의 단말 및/또는 서버로 이루어진 분산네트워크를 이용하여 인공 신경망을 학습시키는 방안이 제안되었다. 분산 네트워크를 이용하면 다수의 단말에서 획득된 학습 데이터를 수집하여 단말간 혹은 단말-서버 간 데이터 교환을 통해 대량의 학습 데이터를 용이하게 획득할 수 있다. 뿐만 아니라, iid를 따르는 학습 데이터를 획득할 수 있으므로 높은 정확도로 학습을 수행할 수 있다는 장점이 있다.

[0004] 단말간 혹은 단말-서버 간 데이터 교환 방식에는 각 단말이 획득한 학습 데이터의 직접 교환 방식, 학습 모델을 교환하는 방식 또는 학습 모델의 출력 분포를 교환하는 방식 등이 있다.

[0005] 그러나 각 단말이 학습 데이터를 직접 교환하는 경우, 학습 데이터에 포함될 수 있는 개인 정보 등과 같은 보호되어야 하는 각종 정보가 유출될 수 있다는 우려가 있다. 그리고 학습 모델을 교환하는 방식의 경우, 학습 데이터를 전송하지 않으므로 정보 유출 문제를 해소할 수 있으나, 학습 모델의 용량으로 인해 전송해야 하는 데이터 크기가 매우 크다. 따라서 단말의 제한된 전송 요량으로 인해 전송이 용이하지 않다. 한편 학습 모델의 출력 분포를 교환하는 방식 또한 정보 유출 문제를 해소할 수 있으며, 전송해야 하는 데이터 크기 또한 작아 전송 제약을 해소할 수 있다. 반면 학습 시에 정확도가 요구되는 수준으로 향상되지 않는다는 문제가 있다.

[0006] 이에 학습 데이터를 직접 교환하는 방식을 이용하여 전송 용량을 줄이고 학습 정확도를 높이면서도 정보 유출을 방지하기 위한 다양한 방법이 제안되었다. 이러한 정보 유출을 방지하기 위한 방법으로는 랜덤 노이즈를 추가하는 방법과 양자화 레벨을 조절하는 방식 및 데이터 혼합 방식 등이 잘 알려져있다. 그러나 이러한 정보 유출을 방지하기 위한 방법을 적용하는 경우, 데이터 량이 증가되거나 학습 정확도가 낮아지는 문제가 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국 공개 특허 제10-2019-0032433호 (2019.03.27 공개)

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 분산네트워크의 다수의 단말에서 인공 신경망 학습을 위한 데이터 전송 시에 개인 정보 유출을 방지할 수 있으면서 학습 정확도를 향상시킬 수 있도록 하는 학습 데이터 획득 장치 및 방법을 제공하는데 있다.

[0009] 본 발명의 다른 목적은 다수의 단말 각각에서 데이터 혼합 방식으로 전송된 혼합 데이터를 재혼합하여 학습 성능을 향상시킬 수 있는 학습 데이터 획득 장치 및 방법을 제공하는데 있다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 학습 데이터 획득 장치는 다수의 단말 각각으로부터 다수의 학습 데이터가 혼합 비율에 따라 혼합된 혼합 데이터를 전송받고, 다수의 단말 각각으로부터 전송된 혼합 데이터를 포함된 레이블에 따라 구분하고 구분된 각 레이블을 혼합 데이터를 전송한 단말의 개수에 대응하여 구성된 재혼합 비율에 따라 재혼합하여 미리 저장된 학습 모델을 학습시키기 위한 재혼합 학습 데이터를 획득한다.

[0011] 상기 다수의 단말 각각은 상기 학습 모델을 학습시키기 위한 다수의 샘플 데이터를 획득하고, 획득된 다수의 샘플 데이터 각각에 샘플 데이터를 분류하기 위한 레이블을 레이블링하여 상기 다수의 학습 데이터를 획득하며, 획득된 상기 다수의 학습 데이터를 혼합 비율에 따라 혼합하여 상기 혼합 데이터를 획득할 수 있다.

[0012] 상기 다수의 단말 각각은 다수의 학습 데이터(x_1, x_2, …, x_n) 각각에 대응하는 개별 혼합 비율(λ_1, λ_2, …, λ_n)(여기서 개별 혼합 비율(λ_1, λ_2, …, λ_n)의 총합은 1($\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$))의 가중합 ($\tilde{x} = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$)으로 상기 혼합 데이터를 획득할 수 있다.

[0013] 상기 개별 혼합 비율은 학습 데이터(x_1, x_2, …, x_n) 구성하는 샘플 데이터(s_1, s_2, …, s_n) 및 레이블(l_1, l_2, …, l_n) 각각에 가중될 수 있다.

[0014] 상기 학습 데이터 획득 장치는 다수의 단말 각각에서 전송된 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$) 각각의 레이블(l_1, l_2, …, l_n)에 대해, 개별 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)(여기서 개별 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)의 총합은 1($\tilde{\lambda_1} + \tilde{\lambda_2} + \cdots + \tilde{\lambda_m} = 1$))을 조절하면서 재혼합하여 다수의 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득할 수 있다.

[0015] 상기 학습 데이터 획득 장치는 상기 재혼합 학습 데이터(x_1', x_2', … x_n')에 포함된 재혼합 샘플 데이터(s_1', s_2', … s_n')와 대응하는 재혼합 레이블(l_1', l_2', … l_n') 중 재혼합 샘플 데이터(s_1', s_2', … s_n')를 상기 학습 모델을 학습시키기 위한 입력값으로 입력하고, 재혼합 레이블(l_1', l_2', … l_n')을 상기 학습 모델의 오차를 판별하여 역전파하기 위한 진리값으로 이용할 수 있다.

[0016] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 학습 데이터 획득 방법은 다수의 단말 각각이 다수의 학습 데이터가 혼합 비율에 따라 혼합된 혼합 데이터를 전송하는 단계; 및 다수의 단말 각각으로부터 전송된 혼합 데이터를 포함된 레이블에 따라 구분하고 구분된 각 레이블을 혼합 데이터를 전송한 단말의 개수에 대응하여 구성된 재혼합 비율에 따라 재혼합하여 미리 저장된 학습 모델을 학습시키기 위한 재혼합 학습 데이터를 획득하는 단계를 포함한다.

발명의 효과

[0017] 따라서, 본 발명의 실시예에 따른 학습 데이터 획득 장치 및 방법은 분산네트워크의 다수의 단말에서 인공 신경망 학습을 위한 데이터 전송 시에 개인 정보 유출을 방지할 수 있으면서 학습 정확도를 향상시킬 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 학습 데이터 획득 장치를 위한 분산 네트워크의 일예를 나타낸다.

도 2는 본 발명의 일 실시예에 따른 학습 데이터 획득 장치가 다중 경로 혼합 방식을 기반으로 학습 데이터를 획득하는 개념을 설명하기 위한 도면이다.

도 3은 본 실시예에 따른 재혼합 학습 데이터를 이용하여 학습을 수행하는 경우, 학습 정확도를 평가한 결과를 나타낸다.

도 4는 본 발명의 일 실시예에 따른 학습 데이터 획득 방법을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0020] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 그러나, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 설명하는 실시예에 한정되는 것이 아니다. 그리고, 본 발명을 명확하게 설명하기 위하여 설명과 관계없는 부분은 생략되며, 도면의 동일한 참조부호는 동일한 부재임을 나타낸다.

[0021] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0022] 도 1은 본 발명의 일 실시예에 따른 학습 데이터 획득 장치를 위한 분산 네트워크의 일예를 나타낸다.

[0023] 도 1을 참조하면, 본 실시예에 따른 분산 네트워크는 다수의 단말(DE1 ~ DE3)을 포함한다. 다수의 단말(DE1 ~ DE3) 각각은 기지정된 학습 데이터를 획득한다. 여기서 다수의 단말(DE1 ~ DE3) 각각은 학습 데이터로 이용 가능한 샘플 데이터를 수집하고, 수집된 샘플 데이터가 무엇을 학습시키기 위한 데이터인지 레이블링하여 학습 데이터를 획득한다. 그리고 획득된 학습 데이터를 그대로 전송하지 않고, 데이터 혼합 방식에 따라 기지정된 방식으로 혼합하여 전송한다. 데이터 혼합 방식에서 다수의 단말(DE1 ~ DE3)은 서로 다른 데이터를 분류하는 학습을 위해 수집된 샘플 데이터에 대해 서로 다르게 레이블링되어 획득된 다수의 학습 데이터를 미리 지정된 비율로 혼합하여 혼합 데이터를 획득하고, 획득된 혼합 데이터를 전송한다.

[0024] 그리고 분산 네트워크에는 적어도 하나의 서버(SV)가 더 포함될 수 있다. 적어도 하나의 서버(SV)는 다수의 단말(DE1 ~ DE3)에서 전달되는 혼합 데이터를 인가받고, 전달된 혼합 데이터를 기반으로 학습을 수행할 수 있다. 즉 본 실시예에서 서버(SV)는 혼합 데이터를 기반으로 학습을 수행할 수 있는 성능을 갖는 장치이다.

[0025] 즉 다수의 단말(DE1 ~ DE3) 중 적어도 하나가 서버(SV)로 동작할 수도 있으며, 획득된 학습 데이터를 상호 교환할 수 있다. 그리고 다수의 단말(DE1 ~ DE3) 각각은 상호 교환된 혼합 데이터를 기반으로 각각 개별적으로 학습을 수행할 수 있다.

[0026] 한편 다수의 단말(DE1 ~ DE3)과 적어도 하나의 서버(SV)는 적어도 하나의 기지국(BS)을 통해 통신을 수행할 수 있다.

[0027] 특히 본 실시예에서 다수의 단말(DE1 ~ DE3) 또는 적어도 하나의 서버(SV)는 다른 단말에서 전송되는 혼합 데이터를 기지정된 방식으로 다시 혼합하여 재혼합 학습 데이터를 생성하고, 생성된 재혼합 학습 데이터를 이용하여 학습을 수행함으로써 학습 성능을 향상시킬 수 있다.

[0028] 다수의 단말(DE1 ~ DE3)이 혼합 데이터를 획득하는 방법과 전송된 혼합 데이터를 재혼합하는 방법에 대한 상세한 설명은 후술한다.

[0029] 도 2는 본 발명의 일 실시예에 따른 학습 데이터 획득 장치가 다중 경로 혼합 방식을 기반으로 학습 데이터를 획득하는 개념을 설명하기 위한 도면이다.

[0030] 도 2에서는 설명의 편의를 위하여, 다수의 단말(DE1 ~ DE3) 중 제1 및 제2 단말(DE1, DE2)이 혼합 데이터를 생성하여 전송하고, 제3 단말(DE3)이 제1 및 제2 단말(DE1, DE2)로부터 전송된 혼합 데이터를 기반으로 재혼합 학습 데이터를 생성하는 경우를 가정하여 도시하였다.

[0031] 다수의 단말(DE1 ~ DE3) 중 제1 및 제2 단말(DE1, DE2) 각각은 학습 데이터를 획득하고, 획득된 학습 데이터를 제3 단말(DE3)로 전송한다. 이때 다수의 단말(DE1, DE2) 각각은 획득된 다수의 학습 데이터를 그대로 전송하지 않고, 다수의 학습 데이터를 기지정된 방식으로 서로 혼합하여 혼합 데이터를 전송한다. 이는 상기한 바와 같이, 학습 데이터에 포함될 수 있는 정보가 유출되는 것을 방지하기 위해서이다.

[0032] 제1 및 제2 단말(DE1, DE2) 각각은 학습 데이터로 이용될 기지정된 분류를 학습하기 위한 샘플 데이터를 획득하며, 도 2에서는 일예로 각각의 단말이 "2" 및 "7"의 숫자를 샘플 데이터(s_1, s_2)로 획득하는 경우를 도시하였다. 도 2에서와 같이 단말(DE1, DE2)이 2 종류의 숫자를 샘플 데이터로 획득하는 경우, 각 단말(DE1, DE2)은 획득된 각각의 샘플 데이터가 무엇을 분류하기 위한 샘플 데이터인지를 나타내는 레이블을 종류별로 서로 다르게 레이블링하여 학습 데이터를 획득한다.

[0033] 각 단말(DE1, DE2)이 "2" 및 "7"의 2 종류의 숫자를 샘플 데이터(s_1, s_2)로 획득하므로, 획득하는 샘플 데이터의 분류 수에 따라 숫자 "2"에 대한 샘플 데이터(s_1)에는 레이블(l_1 = (1, 0))을 레이블링하고, 숫자 "7"에 대한 샘플 데이터(s_2)에는 레이블(l_2 = (0, 1))을 레이블링하였다. 그러나 다른 예로 0 ~ 9까지의 10개의 숫자를 샘플 데이터(s_0 ~ s_9)로 획득하는 것으로 가정하는 경우, 각 단말(DE1, DE2)은 획득된 샘플 데이터(s_2 ~ s_7) "2" 및 "7"에 대한 레이블(l_2, l_7)을 각각 (0, 0, 1, 0, 0, 0, 0, 0, 0, 0) 및 (0, 0, 0, 0, 0, 0, 0, 1, 0, 0)로 레이블링 할 수도 있다. 즉 각각의 단말(DE1, DE2)은 획득하도록 지정된 샘플 데이터의 분류 개수에 따라 획득된 샘플 데이터에 대응하는 레이블을 레이블링하여, 샘플 데이터와 레이블이 쌍을 이루는 학습 데이터를 획득한다.

[0034] 여기서는 각 단말(DE1, DE2)이 "2" 및 "7"의 2 종류의 숫자를 샘플 데이터(s_1, s_2)로 획득하여 대응하는 레이블(l_1, l_2)을 레이블링하므로, 샘플 데이터와 레이블이 쌍을 이루는 학습 데이터(x_1, x_2)는 각각 x_1 = (s_1, l_1), x_2 = (s_2, l_2)로 획득될 수 있다.

[0035] 그리고 제1 및 제2 단말(DE1, DE2)은 샘플 데이터(s_1, s_2)와 레이블(l_1, l_2) 쌍으로 구성된 학습 데이터(x_1, x_2)를 기지정된 방식으로 혼합하여 혼합 데이터를 생성한다. 여기서 제1 및 제2 단말(DE1, DE2)은 서로 다른 다수의 학습 데이터(x_1, x_2)를 혼합 비율(mixing ratio)(λ = (λ_1, λ_2))에 따라 수학식 1과 같이 혼합하여 혼합 데이터를 획득한다.

수학식 1

[0036] $$\tilde{x} = \lambda_1 x_1 + \lambda_2 x_2$$

[0037] 여기서 개별 혼합 비율(λ_1, λ_2)의 총합은 1(λ_1 + λ_2 = 1)이다. 따라서 수학식 1은 수학식 2로 표현될 수 있다.

수학식 2

[0038] $$\tilde{x} = \lambda_1 x_1 + (1 - \lambda_1) x_2$$

[0039] 도 2에서는 제1 단말(DE1)이 2개의 학습 데이터(x_1, x_2)에 대한 혼합 비율(λ_1, λ_2)을 각각 0.4, 0.6으로 설정하여 혼합하고, 제2 단말(DE2)은 2개의 학습 데이터(x_1, x_2)에 대한 혼합 비율(λ_1, λ_2)을 각각 0.6, 0.4으로 설정하여 혼합한 경우를 도시하였다. 즉 숫자 "2"와 "7"의 이미지가 각각 0.6, 0.4의 혼합 비율(λ_1, λ_2)에 따라 혼합되어 나타난다.

[0040] 혼합 비율(λ = (λ_1, λ_2))은 학습 데이터(x_1, x_2)의 샘플 데이터(s_1, s_2)를 합성할 때, 각 샘플 데이터의 비중을 조절하기 위한 가중치이다. 그리고 혼합 비율을 샘플 데이터(s_1, s_2)뿐만 아니라 샘플 데이터(s_1, s_2)에 대응하는 레이블(l_1, l_2)에도 가중된다. 즉 레이블(l_1, l_2)에도 혼합 비율(λ_1, λ_2)이 가중되어 제1 단말(DE1)에서 가중된 레이블($\lambda_1 l_1$, $\lambda_2 l_2$)은 각각 (0.4, 0), (0, 0.6)이 되고 제2 단말(DE2)에서 가중된 레이블($\lambda_1 l_1$, $\lambda_2 l_2$)은 각각 (0.6, 0), (0, 0.4)이 된다. 그리고 혼합 데이터($\tilde{x}$)에서는 가중된 레이블들이 결합되어 제1 단말(DE1)의 혼합 데이터($\tilde{x_1}$)의 혼합 비율(λ_1, λ_2)이 가중된 레이블은 (0.4, 0.6)가 되고, 제2 단말(DE2)의 혼합 데이터($\tilde{x_2}$)의 혼합 비율(λ_1, λ_2)이 가중된 레이블은 (0.6, 0.4)가 된다.

[0041] 상기에서는 각 단말이 2 종류의 샘플 데이터를 획득하는 것으로 가정하여, 혼합 데이터($\tilde{x}$)를 수학식 1과 같이 생성하는 것으로 설명하였으나, 단말(DE1, DE2)이 n가지 종류의 학습 데이터(x_1, x_2, … x_n)를 획득하도록 지정된 경우, 혼합 데이터($\tilde{x}$)는 수학식 3과 같이 일반화된 방식으로 획득될 수 있다.

수학식 3

[0042] $$\tilde{x} = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$$

[0043] 여기서 개별 혼합 비율(λ_1, λ_2, …, λ_n)의 총합은 1($\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$)이다.

[0044] 제3 단말(DE3)은 제1 및 제2 단말(DE1, DE2) 각각으로부터 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$)를 인가받고, 인가된 다수의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$)를 기지정된 방식으로 재혼합(Re-Mixed)하여, 재혼합 학습 데이터(x')를 획득한다.

[0045] 제3 단말(DE3)은 m개의 단말로부터 m개의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$)가 전송되면, 전송된 m개의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$) 각각에 대해 m개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)을 적용하여 수학식 4와 같이 재혼합한다.

수학식 4

[0046] $$x' = \tilde{\lambda_1}\tilde{x_1} + \tilde{\lambda_2}\tilde{x_2} + \cdots + \tilde{\lambda_m}\tilde{x_m}$$

[0047] 여기서 m개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)의 총합은 1($\tilde{\lambda_1} + \tilde{\lambda_2} + \cdots + \tilde{\lambda_m} = 1$)이다. 이때, 제3 단말(DE3)은 수학식 4에 따른 하나의 재혼합 학습 데이터(x')를 획득하는 것이 아니라, 각각의 단말(DE1, DE2)가 혼합 데이터를 생성하는데 적용하는 학습 데이터(x_1, x_2, … x_n)의 개수(n)에 대응하는 개수의 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득할 수 있다.

[0048] 그리고 재혼합 학습 데이터(x')의 재혼합 레이블(l')은 m개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)에 대응하여 재혼합 레이블(l' = l_k(여기서 k ∈ {1, 2, …, m}))을 만족한다.

[0049] 즉 전송된 m개의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$) 각각의 레이블(l_1, l_2, …, l_n)에 따라, m개의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$) 각각의 레이블(l_1, l_2, …, l_n)을 변경하면서 m개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)의 재혼합 레이블(l_k)을 적용하여 n개의 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득한다.

[0050] 즉 m개의 단말 각각이 획득하는 샘플 데이터의 개수가 n개로 가정하는 경우, 제3 단말(DE3)은 n개의 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득할 수 있다.

[0051] 도 2에서와 같이 2개(m = 2)의 단말(DE1, DE2)가 각각 2개(n = 2)의 학습 데이터(x_1, x_2)를 혼합하여, 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$)를 전송하는 경우, 2개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$)은 레이블이 1인 경우와 2인 경우 각각에 대해, 수학식 3을 이용하여 수학식 5 및 6으로 계산될 수 있다.

수학식 5

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

수학식 6

[0053] $$\tilde{\lambda_1} = 1 - \tilde{\lambda_2} = 1 - \frac{\lambda_1}{2\lambda_1 - 1}, then\ l' = l_2$$

[0054] 상기한 재혼합은 실질적으로 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$)를 각 레이블에 따라 다시 구분하는 것과 유사한 결과를 도출한다. 즉 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$)에 대해 역혼합하는 것과 유사하게 동작하며, 따라서 재혼합 학습 데이터(x_1', x_2', … x_n')는 역혼합 학습 데이터라고도 볼 수 있다.

[0055] 그리고 제3 단말(DE3)은 획득된 n개의 재혼합 학습 데이터(x_1', x_2', … x_n')를 기반으로 인공 신경망으로 구현되는 학습 모델을 학습시킬 수 있다.

[0056] 획득된 n개의 재혼합 학습 데이터(x_1', x_2', … x_n')는 각각 재혼합 샘플 데이터(s_1', s_2', … s_n')와 재혼합 샘플 데이터(s_1', s_2', … s_n')에 대응하는 재혼합 레이블(l_1', l_2', … l_n')의 조합으로 구성된다. 여기서 재혼합 샘플 데이터(s_1', s_2', … s_n')는 학습 모델의 입력값으로 이용되고, 재혼합 레이블(l_1', l_2', … l_n')은 학습 모델의 오차를 판별하여 역전파하기 위한 진리값으로 이용될 수 있다.

[0057] 도 3은 본 실시예에 따른 재혼합 학습 데이터를 이용하여 학습을 수행하는 경우, 학습 정확도를 평가한 결과를 나타낸다.

[0058] 도 3에서 (a)는 업링크와 다운 링크 채널 용량이 비대칭인 경우를 나타내고, (b)는 업링크와 다운 링크 채널 용량이 대칭인 경우를 나타낸다. 그리고 도 3에서Mix2FlD는 본 실시예에 따른 재혼합 학습 데이터(x_1', x_2', … x_n')를 이용하여 학습을 수행한 결과를 나타내고, MixFLD는 단말로부터 전송되는 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …,

$\tilde{x}_m$)를 이용하여 학습을 수행한 결과를 나타내며, FL, FD는 각각 학습 모델 교환 방식과 학습 모델의 출력 분포를 교환 방식에 따른 학습 결과를 나타낸다.

[0059] 도 3에 도시된 바와 같이, 본 실시예와 같이, 단말로부터 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$)를 전송받고, 전송된 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$)를 재혼합하여 생성된 재혼합 학습 데이터(x_1', x_2', … x_n')를 이용하여 학습을 수행하는 경우가, 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$)를 그대로 이용하는 경우나, 학습 모델 교환 방식과 학습 모델의 출력 분포를 교환 방식에 비해 학습 성능이 매우 우수함을 알 수 있다.

표 1

[0060]

Dataset	Sample Privacy Under Mixing Ratio λ					
	λ = 0	0.1	0.2	0.3	0.4	0.5
MNIST	2.163	4.465	5.158	5.564	5.852	**6.055**
FMNIST	1.825	4.127	4.821	5.226	5.514	**5.717**
CIFAR-10	2.582	4.884	5.577	5.983	6.270	**6.473**
CIFAR-100	2.442	4.744	5.438	5.843	6.131	**6.334**

표 2

[0061]

Dataset	Sample Privacy Under Mixing Ratio λ					
	λ = 0	0.1	0.2	0.3	0.4	0.499
MNIST	2.557	4.639	5.469	6.140	7.007	**9.366**
FMNIST	2.196	4.568	5.410	6.143	6.925	**9.273**
CIFAR-10	2.824	5.228	6.076	6.766	7.662	**10.143**
CIFAR-100	2.737	5.151	6.050	6.782	7.652	**10.104**

[0062] 표 1과 표 2는 각각 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$)를 이용하는 경우와 본 실시예에 따른 재혼합 학습 데이터(x_1', x_2', … x_n')를 이용하는 경우에 프라이버시와 같은 보안성에 대한 보장 정보를 계산한 결과를 나타낸다.

[0063] 표 1 및 표 2에서는 각 단말이 획득한 샘플 데이터(s_1, s_2)와 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$) 또는 재혼합 학습 데이터(x_1', x_2', … x_n') 사이의 최소 유클리안 거리(Minimum Euclidean Distance)에 로그(log)를 취하여 계산한 결과이다.

[0064] 표 1 및 표 2를 비교하면, 혼합 데이터($\tilde{x}_1$, $\tilde{x}_2$, …, $\tilde{x}_m$)를 이용하는 경우보다 재혼합 학습 데이터(x_1', x_2', … x_n')를 이용하는 경우에 보안성이 크게 향상됨을 알 수 있다.

[0065] 도 4는 본 발명의 일 실시예에 따른 학습 데이터 획득 방법을 나타낸다.

[0066] 도 2를 참조하여 도 4의 학습 데이터 획득 방법을 설명하면, 본 실시예에 따른 학습 데이터 획득 방법은 크게 분산 네트워크 상의 다수의 단말 각각이 학습 모델을 학습시키기 위한 샘플 데이터를 획득하고, 획득된 샘플 데이터로부터 보안성을 강화한 혼합 데이터를 생성하여 전송하는 혼합 데이터 획득 단계(S10) 및 다수의 단말에서 전송된 다수의 혼합 데이터를 다수의 샘플 데이터로부터 혼합 데이터를 생성하는 과정과 유사하게 다시 재혼합

하여 재혼합 학습 데이터를 획득하는 재혼합 학습 데이터 획득 단계(S20) 로 구성될 수 있다.

[0067] 혼합 데이터 획득 단계(S10)에서는 우선 분산 네트워크 상의 다수의 단말(DE_1, DE_2, …, DE_m) 각각이 학습 모델을 학습시키기 위한 다수의 샘플 데이터(s_1, s_2, …, s_n)를 획득한다(S11). 이때 다수의 단말(DE_1, DE_2, …, DE_m) 각각은 기지정된 서로 다른 종류의 학습을 위해 서로 다른 종류의 샘플 데이터(s_1, s_2, …, s_n)를 획득할 수 있다. 그리고 다수의 샘플 데이터(s_1, s_2, …, s_n)가 획득되면, 획득된 샘플 데이터(s_1, s_2, …, s_n) 각각의 종류에 대응하여 레이블(l_1, l_2, …, l_n)을 각 샘플 데이터에 레이블링 함으로써, 다수의 학습 데이터(x_1, x_2, …, x_n)를 획득한다(S12).

[0068] 각각의 단말(DE_1, DE_2, …, DE_m)은 획득된 다수의 학습 데이터(x_1, x_2, …, x_n)에 대해 혼합 비율($\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_n)$)에 따라 혼합하여 혼합 데이터($\tilde{x}$)를 획득한다(S13). 각각의 단말($DE_1$, DE_2, …, DE_m)은 서로 다르게 기지정된 또는 임의의 혼합 비율($\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_n)$)에 따라 다수의 학습 데이터($x_1$, x_2, …, x_n)를 혼합하여, 각 단말(DE_1, DE_2, …, DE_m)에 대응하는 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$)를 획득할 수 있다.

[0069] 그리고 각 단말(DE_1, DE_2, …, DE_m)은 획득된 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$)를 다른 단말 또는 적어도 하나의 서버로 전송한다(S14).

[0070] 한편, 재혼합 학습 데이터 획득 단계(S20)에서는 우선 단말 또는 서버가 다른 단말(DE_1, DE_2, …, DE_m)에서 전송된 다수의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$)를 수신한다(S21). 그리고 수신된 다수의 혼합 데이터($\tilde{x_1}$, $\tilde{x_2}$, …, $\tilde{x_m}$)를 레이블(l_1, l_2, …, l_n)에 따라 구분하고, 구분된 각 레이블 단위로 m개의 재혼합 비율($\tilde{\lambda_1}$, $\tilde{\lambda_2}$, …, $\tilde{\lambda_m}$)을 적용하여 재혼합하여 재혼합 학습 데이터(x_1', x_2', … x_n')를 획득한다(S22).

[0071] 재혼합 학습 데이터(x_1', x_2', … x_n')가 획득되면, 획득된 재혼합 학습 데이터(x_1', x_2', … x_n')를 기지정된 학습 모델에 대한 학습 데이터로 이용하여 학습 모델을 학습시킨다. 이때 재혼합 학습 데이터(x_1', x_2', … x_n')의 레이블은 재혼합 학습 데이터(x_1', x_2', … x_n')가 학습시키는 종류에 대한 분류값으로, 학습 모델을 지도 학습 방식으로 학습될 수 있다.

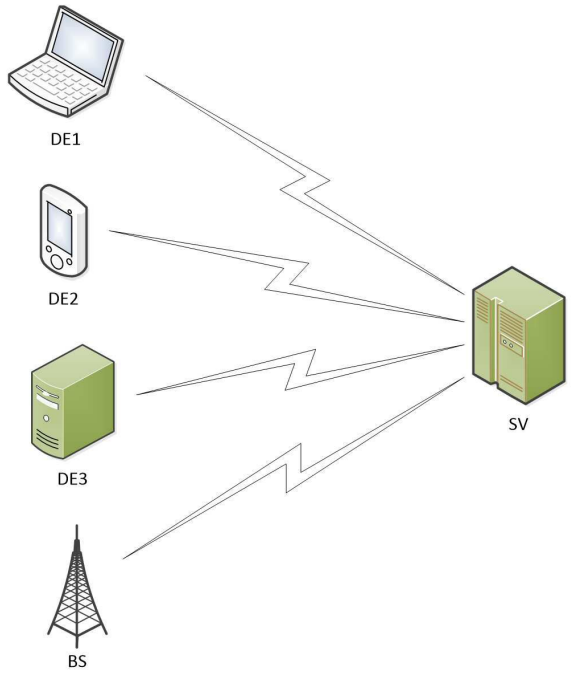
[0072] 본 발명에 따른 방법은 컴퓨터에서 실행시키기 위한 매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다. 여기서 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스 될 수 있는 임의의 가용 매체일 수 있고, 또한 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함하며, ROM(판독 전용 메모리), RAM(랜덤 액세스 메모리), CD(컴팩트 디스크)-ROM, DVD(디지털 비디오 디스크)-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등을 포함할 수 있다.

[0073] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다.

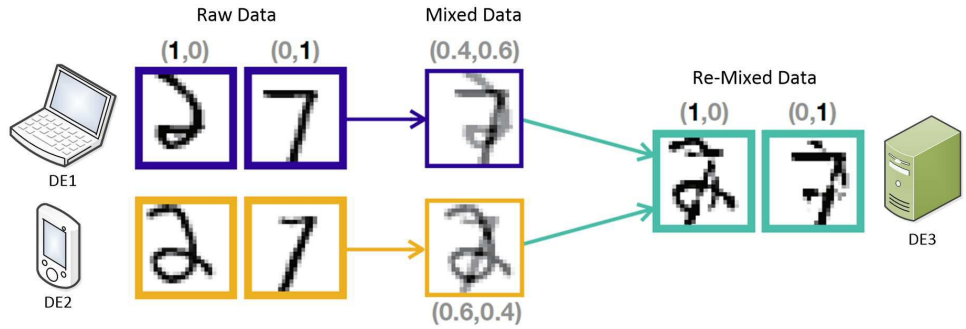
[0074] 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

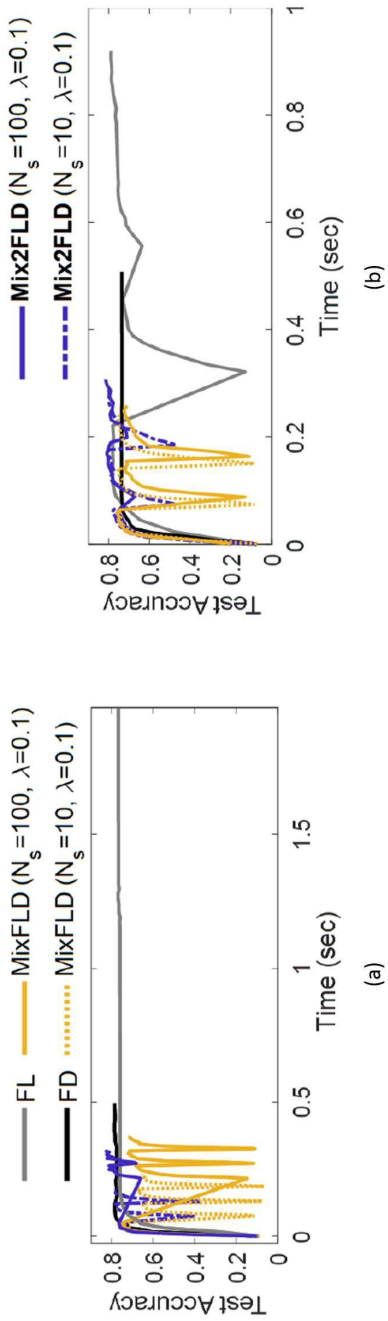
도면1


DE1
DE2
DE3
BS
SV

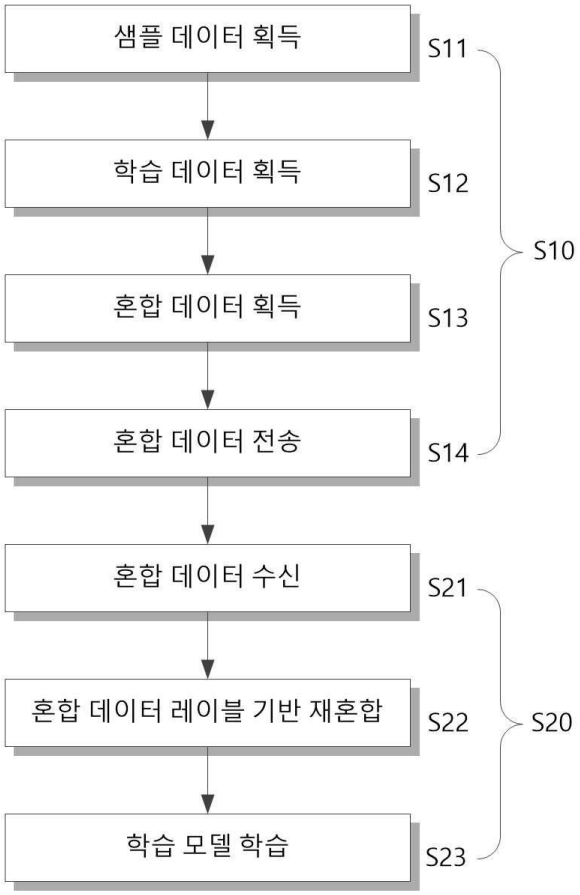
도면2


Raw Data
Mixed Data
(1,0)
(0,1)
(0.4,0.6)
(0.6,0.4)
Re-Mixed Data
(1,0)
(0,1)
DE1
DE2
DE3

도면3


Mix2FLD (N_s=100, λ=0.1)
Mix2FLD (N_s=10, λ=0.1)
Test Accuracy
Time (sec)
(b)
FL
FD
MixFLD (N_s=100, λ=0.1)
MixFLD (N_s=10, λ=0.1)
Test Accuracy
Time (sec)
(a)

도면4


샘플 데이터 획득
S11
학습 데이터 획득
S12
혼합 데이터 획득
S13
혼합 데이터 전송
S14
S10
혼합 데이터 수신
S21
혼합 데이터 레이블 기반 재혼합
S22
학습 모델 학습
S23
S20