(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111091199 B
(45)授权公告日 2023.05.16

(21)申请号 201911335678.4
(22)申请日 2019.12.20
(65)同一申请的已公布的文献号
申请公布号 CN 111091199 A
(43)申请公布日 2020.05.01
(73)专利权人 哈尔滨工业大学(深圳)
地址 518055 广东省深圳市南山区桃源街道深圳大学城哈尔滨工业大学校区
(72)发明人 廖清 黄茜茜 柏思远 丁烨 李京竹
(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 郭浩辉 麦小婵
(51)Int.Cl.
G06N 20/00(2019.01)

审查员 燕璐

权利要求书1页 说明书8页 附图2页

(54)发明名称

一种基于差分隐私的联邦学习方法、装置及存储介质

(57)摘要

本发明公开了一种基于差分隐私的联邦学习方法、装置和存储介质。所述方法包括:S1、将预设的第一模型参数下发至用户端,使所述用户端根据所述第一模型参数,基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数;其中,所述第一模型参数包括隐私预算;S2、对所述第二模型参数进行参数平均化,得到第三模型参数,并将所述第三模型参数下发至所述用户端;S3、将步骤S1～S2的执行总次数作为模型训练轮次,并当所述模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2,反之结束模型训练。本发明能够保障数据隐私安全,并提高训练模型的精确度。

CN 111091199 B

1.一种基于差分隐私的联邦学习方法,其特征在于,包括:

S1、将预设的第一模型参数下发至用户端,使所述用户端根据所述第一模型参数,基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数;其中,所述第一模型参数包括隐私预算;

所述用户端根据所述第一模型参数,基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数,包括:

所述用户端根据所述第一模型参数,通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数;

所述用户端根据所述第一模型参数,通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数,包括:

将所述隐私预算随机分为最优步长参数和噪音梯度参数;其中,所述最优步长参数和所述噪音梯度参数均用于确定添加的高斯噪音的大小;

当剩余的所述隐私预算大于0时,沿梯度下降的方向更新所述用户端本地的深度学习模型,得到所述第二模型参数;

S2、对所述第二模型参数进行参数平均化,得到第三模型参数,并将所述第三模型参数下发至所述用户端;

S3、将步骤S1～S2的执行总次数作为模型训练轮次,并当所述模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2,反之结束模型训练。

2.一种基于差分隐私的联邦学习装置,其特征在于,包括:

第一模型参数下发模块,用于将预设的第一模型参数下发至用户端,使所述用户端根据所述第一模型参数,基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数;其中,所述第一模型参数包括隐私预算;

所述用户端根据所述第一模型参数,基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数,包括:

所述用户端根据所述第一模型参数,通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数;

所述用户端根据所述第一模型参数,通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数,包括:

将所述隐私预算随机分为最优步长参数和噪音梯度参数;其中,所述最优步长参数和所述噪音梯度参数均用于确定添加的高斯噪音的大小;

当剩余的所述隐私预算大于0时,沿梯度下降的方向更新所述用户端本地的深度学习模型,得到所述第二模型参数;

第三模型参数下发模块,用于对所述第二模型参数进行参数平均化,得到第三模型参数,并将所述第三模型参数下发至所述用户端;

模型训练轮次判断模块,用于将上述下发模块的执行总次数作为模型训练轮次,并当所述模型训练轮次未达到预设阈值时重复执行上述下发模块,反之结束模型训练。

3.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机程序,其中,在所述计算机程序运行时控制所述计算机可读存储介质所在设备执行如权利要求1所述的基于差分隐私的联邦学习方法。

一种基于差分隐私的联邦学习方法、装置及存储介质

技术领域

[0001] 本发明涉及人工智能技术领域，尤其涉及一种基于差分隐私的联邦学习方法、装置及存储介质。

背景技术

[0002] 目前，大多数用户比如企业或机构等都想要联合其他用户的数据协同训练AI模型，出于数据隐私保护和安全的考虑，各个用户无法直接进行数据交换，难以实现跨用户协同训练AI模型。而应用Google提出的联邦学习方法可解决上述问题。

[0003] 联邦学习在用户各自数据不出本地的前提下，通过加密机制或扰动机制下的参数交换与优化，建立一个共有模型。这要求用户用自身数据训练得到用户模型，并将用户模型的模型参数上传至服务器，由服务器根据多个用户上传的模型参数进行模型优化后基于差分隐私进行数据隐私保护，建立一个共有模型。

[0004] 但在现有的联邦学习方法中，仍存在以下技术难点：

[0005] 1、用户将模型参数直接上传至服务器，使得模型参数暴露在数据传输通道及服务器中，无法充分保障数据隐私安全；

[0006] 2、数据量较大或数据量较小的用户均使用相同的模型构建方法和训练轮次，难以保证模型的精确度；

[0007] 3、差分隐私随机梯度下降算法(DP-SGD)和自适应的Laplace机制(AdLM)等差分隐私深度学习算法给模型加入的噪音较大且较为固定，难以针对不同的训练过程优化调整噪音，难以保证模型的精确度。

发明内容

[0008] 本发明提供一种基于差分隐私的联邦学习方法、装置及存储介质，以克服现有的联邦学习方法面对的技术难点，本发明能够保障数据隐私安全，并提高训练模型的精确度。

[0009] 为了解决上述技术问题，本发明一实施例提供一种基于差分隐私的联邦学习方法，包括：

[0010] S1、将预设的第一模型参数下发至用户端，使所述用户端根据所述第一模型参数，基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数；其中，所述第一模型参数包括隐私预算；

[0011] S2、对所述第二模型参数进行参数平均化，得到第三模型参数，并将所述第三模型参数下发至所述用户端；

[0012] S3、将步骤S1～S2的执行总次数作为模型训练轮次，并当所述模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2，反之结束模型训练。

[0013] 进一步地，所述用户端根据所述第一模型参数，基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数，包括：

[0014] 所述用户端根据所述第一模型参数，通过差分隐私-卷积神经网络算法更新所述

用户端本地的深度学习模型并返回所述第二模型参数。

[0015] 进一步地，所述用户端根据所述第一模型参数，通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数，包括：

[0016] 将所述隐私预算随机分为最优步长参数和噪音梯度参数；其中，所述最优步长参数和所述噪音梯度参数均用于确定添加的高斯噪音的大小；

[0017] 当剩余的所述隐私预算大于0时，沿梯度下降的方向更新所述用户端本地的深度学习模型，得到所述第二模型参数。

[0018] 本发明另一实施例提供一种基于差分隐私的联邦学习装置，包括：

[0019] 第一模型参数下发模块，用于将预设的第一模型参数下发至用户端，使所述用户端根据所述第一模型参数，基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数；其中，所述第一模型参数包括隐私预算；

[0020] 第三模型参数下发模块，用于对所述第二模型参数进行参数平均化，得到第三模型参数，并将所述第三模型参数下发至所述用户端；

[0021] 模型训练轮次判断模块，用于将上述下发模块的执行总次数作为模型训练轮次，并当所述模型训练轮次未达到预设阈值时重复执行上述下发模块，反之结束模型训练。

[0022] 进一步地，所述用户端根据所述第一模型参数，基于差分隐私技术更新所述用户端本地的深度学习模型并返回第二模型参数，包括：

[0023] 所述用户端根据所述第一模型参数，通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数。

[0024] 进一步地，所述用户端根据所述第一模型参数，通过差分隐私-卷积神经网络算法更新所述用户端本地的深度学习模型并返回所述第二模型参数，包括：

[0025] 将所述隐私预算随机分为最优步长参数和噪音梯度参数；其中，所述最优步长参数和所述噪音梯度参数均用于确定添加的高斯噪音的大小；

[0026] 当剩余的所述隐私预算大于0时，沿梯度下降的方向更新所述用户端本地的深度学习模型，得到所述第二模型参数。

[0027] 本发明还提供一种计算机可读存储介质，所述计算机可读存储介质包括存储的计算机程序，其中，在所述计算机程序运行时控制所述计算机可读存储介质所在设备执行如上所述的基于差分隐私的联邦学习方法。

[0028] 本发明的实施例，具有如下有益效果：

[0029] 通过将预设的第一模型参数，包括隐私预算下发至用户端，使用户端可根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，进而通过对用户端上传的第二模型参数进行参数平均化，向用户端下发得到的第三模型参数。同时，将上述操作作为一轮模型训练，通过累计模型训练轮次，在模型训练轮次未达到预设阈值时重复执行上述操作，反之结束模型训练。本发明通过使各个用户端基于差分隐私技术更新其本地的深度学习模型后再上传第二模型参数，有利于保障数据隐私安全，并提高训练模型的精确度；通过对第二模型参数进行参数平均化，能够对第二模型参数进行整合得到第三模型参数，使用户端根据第三模型参数进行下一轮模型训练，有利于提高训练模型的精确度；通过对模型训练轮次设置阈值，使得只有当模型训练轮次达到预设阈值时才结束模型训练，有利于进一步提高训练模型的精确度。

附图说明

[0030] 图1为本发明第一实施例中的一种基于差分隐私的联邦学习方法的流程示意图；

[0031] 图2为本发明第一实施例中的基于差分隐私的联邦学习框架的结构示意图；

[0032] 图3为本发明第一实施例中的差分隐私-卷积神经网络算法的流程示意图；

[0033] 图4为本发明第二实施例中的一种基于差分隐私的联邦学习装置的结构示意图。

具体实施方式

[0034] 下面将结合本发明中的附图，对本发明中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0035] 需要说明的是，文中的步骤编号，仅为了方便具体实施例的解释，不作为限定步骤执行先后顺序的作用。本实施例提供的方法可以由相关的服务器执行，且下文均以服务器作为执行主体为例进行说明。

[0036] 第一实施例。请参阅图1-3。

[0037] 如图1所示，第一实施例提供一种基于差分隐私的联邦学习方法，所述方法包括步骤S1～S3：

[0038] S1、将预设的第一模型参数下发至用户端，使用户端根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数；其中，第一模型参数包括隐私预算。

[0039] S2、对第二模型参数进行参数平均化，得到第三模型参数，并将第三模型参数下发至用户端。

[0040] S3、将步骤S1～S2的执行总次数作为模型训练轮次，并当模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2，反之结束模型训练。

[0041] 在步骤S1中，用户端根据服务器下发的第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型，以向服务器返回第二模型参数，即用户端在上传第二模型参数之前已对第二模型参数进行差分隐私处理。差分隐私(differential privacy)是密码学中的一种手段，旨在提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其记录的机会。本实施例先对第二模型参数进行差分隐私处理后再上传至服务器，能够避免第二模型参数直接暴露在数据传输过程和服务器中，有利于保障数据隐私安全。

[0042] 其中，服务器可根据各个用户端的训练数据集数据量的大小预先设置隐私预算，使得用户端可根据相应的隐私预算，利用其训练数据集训练其本地的深度学习模型，有利于提高训练模型的精确度。例如，对于训练数据集数据量较小的用户端，为降低噪音水平需设置较大的隐私预算；对于训练数据集数据量较大的用户端，因全局敏感性较小可设置较小的隐私预算。本实施例通过使不同数据量的用户端进行不同程度的差分隐私处理，有利于提高训练模型的精确度。

[0043] 在步骤S2中，服务器对用户端上传的第二模型参数进行参数平均化，即整合该用户端多次训练其本地的深度学习模型得到的所有第二模型参数，有利于提高训练模型的精

确度。

[0044] 在步骤S3中，将步骤S1～S2的执行总次数作为模型训练轮次，并当模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2，相当于通过用户端和服务器不断交互用于训练模型的模型参数直至模型训练轮次达到预设阈值，有利于提高训练模型的精确度。

[0045] 基于差分隐私的联邦学习框架如图2所示，以数据量不等的K个用户端进行联邦学习为例。

[0046] ①各个用户端通过训练其本地的深度学习模型，在梯度更新上进行差分隐私处理得到权重参数，比如第k个用户得到权重参数w_{t+1}^{k}。

[0047] ②服务器在所有用户端中随机选取部分用户端作为子集Z_t，并获取子集Z_t中的用户端在当前轮次训练其本地深度学习模型得到的模型参数，以计算模型参数差值$\Delta w_{t+1}^{k} = w_{t+1}^{k} - w_{t}^{k}$。其中，$w_{t}^{k}$为上一轮次的模型参数。

[0048] ③在计算模型参数差值后，服务器对各个模型参数差值直接进行平均化$\Delta w_{t+1} \leftarrow w_t + \frac{1}{m}\left(\sum_{k=1}^{K} \Delta w_{t+1}^{k}\right)$。其中，在服务器无差分隐私处理。

[0049] ④服务器将经参数平均化的模型参数下发给子集Z_t中的用户端，使接收到用户端进行下一轮模型训练。其中，子集Z_t中的各个用户端收到的参数都相同。

[0050] 本实施例通过将预设的第一模型参数，包括隐私预算下发至用户端，使用户端可根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，进而通过对用户端上传的第二模型参数进行参数平均化，向用户端下发得到的第三模型参数。同时，将上述操作作为一轮模型训练，通过累计模型训练轮次，在模型训练轮次未达到预设阈值时重复执行上述操作，反之结束模型训练。

[0051] 通过使各个用户端基于差分隐私技术更新其本地的深度学习模型后再上传第二模型参数，有利于保障数据隐私安全，并提高训练模型的精确度；通过对第二模型参数进行参数平均化，能够对第二模型参数进行整合得到第三模型参数，使用户端根据第三模型参数进行下一轮模型训练，有利于提高训练模型的精确度；通过对模型训练轮次设置阈值，使得只有当模型训练轮次达到预设阈值时才结束模型训练，有利于进一步提高训练模型的精确度。

[0052] 在优选的实施例当中，用户端根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，包括用户端根据第一模型参数，通过差分隐私-卷积神经网络算法更新用户端本地的深度学习模型并返回第二模型参数。

[0053] 在本实施例的一种优选实施方式当中，所述用户端根据第一模型参数，通过差分隐私-卷积神经网络算法更新用户端本地的深度学习模型并返回第二模型参数，包括：将隐私预算随机分为最优步长参数和噪音梯度参数；其中，最优步长参数和所述噪音梯度参数均用于确定添加的高斯噪音的大小；当剩余的隐私预算大于0时，沿梯度下降的方向更新用户端本地的深度学习模型，得到第二模型参数。

[0054] 差分隐私-卷积神经网络(DPAGD-CNN)算法的算法流程图如图3所示。

[0055] 在本实施例中，第一模型参数包括损失函数、隐私预算、梯度裁剪阈值、预算增长率和训练数据集批大小。预算增长率表示最优步长参数和噪音梯度参数的变化速度。最优

步长参数用于确定向模型参数添加的高斯噪声的大小,噪音梯度参数用于确定给梯度添加的高斯噪声的大小。模型/步长变更概率参数用于判断优化模型参数,还是优化最优步长参数和噪音梯度参数。

[0056] 用户端在获取服务器下发的第一模型参数之后,将未由服务器分配的剩余差分隐私深度学习的过程参数进行初始化,比如对深度学习模型的模型参数随机赋初值,初始模型训练轮次为0。

[0057] 用户端将隐私预算随机分为最优步长参数和噪音梯度参数,并判断剩余的隐私参数是否大于0。当剩余的隐私预算不大于0时,向服务器返回第二模型参数。

[0058] 当剩余的隐私预算大于0时,初始化模型/步长变更概率参数为0,计算当前模型参数的梯度值,并依据梯度裁剪阈值进行裁剪,向裁剪后的梯度加入高斯噪音,以此减少隐私预算中相应的量,继而依据用户端的训练数据集中的最差数据(损失函数值最大),向模型/步长变更概率参数添加高斯噪声,以此减少隐私预算相应的量。

[0059] 用户端判断模型/步长变更概率参数是否大于0。当模型/步长变更概率参数大于0时,在剩余的隐私预算不大于0时向服务器返回第二模型参数,在剩余的隐私预算大于0时更新优化自适应差分隐私卷积神经网络中的参数,并重新判断剩余的隐私预算是否大于0。

[0060] 当模型/步长变更概率参数不大于0时,更新最优步长参数和噪音梯度参数,并重新判断剩余的隐私预算是否大于0。

[0061] 在此过程中,最优步长参数越小,用户端数据越符合训练模型,用户端数据添加的高斯噪声分布越集中在大于0的部分,高斯噪音为负的概率越小,则进行最优步长参数、噪音梯度参数优化的概率也越小,反之则越大。

[0062] 在用户端的模型更新中,应用具有自适应梯度下降的差分隐私-卷积神经网络(DPAGD-CNN)算法,即在深度学习模型的迭代训练过程中,通过自适应的方法给梯度加入不同大小的噪音,但总体不改变原有的差分隐私预算。在模型优化过程的开始,使用不容易影响梯度下降正确方向的较大的噪声值,随着模型的优化,梯度下降的方向变得精确,从而有利于提高训练模型的精确度。

[0063] 第二实施例。请参阅图4。

[0064] 如图4所示,第二实施例提供一种基于差分隐私的联邦学习装置,包括:第一模型参数下发模块21,用于将预设的第一模型参数下发至用户端,使用户端根据第一模型参数,基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数;其中,第一模型参数包括隐私预算;第三模型参数下发模块22,用于对第二模型参数进行参数平均化,得到第三模型参数,并将第三模型参数下发至用户端;模型训练轮次判断模块23,用于将上述下发模块(21、22)的执行总次数作为模型训练轮次,并当模型训练轮次未达到预设阈值时重复执行上述下发模块(21、22),反之结束模型训练。

[0065] 通过第一模型参数下发模块21,使用户端根据服务器下发的第一模型参数,基于差分隐私技术更新用户端本地的深度学习模型,以向服务器返回第二模型参数,即用户端在上传第二模型参数之前已对第二模型参数进行差分隐私处理。差分隐私(differential privacy)是密码学中的一种手段,旨在提供一种当从统计数据库查询时,最大化数据查询的准确性,同时最大限度减少识别其记录的机会。本实施例通过第一模型参数下发模块21使用户端先对第二模型参数进行差分隐私处理后再上传至服务器,能够避免第二模型参数

直接暴露在数据传输过程和服务器中，有利于保障数据隐私安全。

[0066] 其中，服务器可根据各个用户端的训练数据集数据量的大小预先设置隐私预算，使得用户端可根据相应的隐私预算，利用其训练数据集训练其本地的深度学习模型，有利于提高训练模型的精确度。例如，对于训练数据集数据量较小的用户端，为降低噪音水平需设置较大的隐私预算；对于训练数据集数据量较大的用户端，因全局敏感性较小可设置较小的隐私预算。本实施例通过使不同数据量的用户端进行不同程度的差分隐私处理，有利于提高训练模型的精确度。

[0067] 通过第三模型参数下发模块22，由服务器对用户端上传的第二模型参数进行参数平均化，即整合该用户端多次训练其本地的深度学习模型得到的所有第二模型参数，有利于提高训练模型的精确度。

[0068] 通过模型训练轮次判断模块23，将上述下发模块(21、22)的执行总次数作为模型训练轮次，并当模型训练轮次未达到预设阈值时重复执行上述下发模块(21、22)，相当于通过用户端和服务器不断交互用于训练模型的模型参数直至模型训练轮次达到预设阈值，有利于提高训练模型的精确度。

[0069] 本实施例通过第一模型参数下发模块21将预设的第一模型参数，包括隐私预算下发至用户端，使用户端可根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，进而通过第三模型参数下发模块22对用户端上传的第二模型参数进行参数平均化，向用户端下发得到的第三模型参数。同时，通过模型训练轮次判断模块23将上述下发模块(21、22)执行的操作作为一轮模型训练，通过累计模型训练轮次，在模型训练轮次未达到预设阈值时重复执行上述下发模块(21、22)，反之结束模型训练。

[0070] 通过第一模型参数下发模块21使各个用户端基于差分隐私技术更新其本地的深度学习模型后再上传第二模型参数，有利于保障数据隐私安全，并提高训练模型的精确度；通过第三模型参数下发模块22对第二模型参数进行参数平均化，能够对第二模型参数进行整合得到第三模型参数，使用户端根据第三模型参数进行下一轮模型训练，有利于提高训练模型的精确度；通过模型训练轮次判断模块23对模型训练轮次设置阈值，使得只有当模型训练轮次达到预设阈值时才结束模型训练，有利于进一步提高训练模型的精确度。

[0071] 在优选的实施例当中，所述用户端根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，包括用户端根据第一模型参数，通过差分隐私-卷积神经网络算法更新用户端本地的深度学习模型并返回第二模型参数。

[0072] 在优选的实施例当中，所述用户端根据第一模型参数，通过差分隐私-卷积神经网络算法更新用户端本地的深度学习模型并返回第二模型参数，包括：将隐私预算随机分为最优步长参数和噪音梯度参数；其中，最优步长参数和噪音梯度参数均用于确定添加的高斯噪音的大小；当剩余的隐私预算大于0时，沿梯度下降的方向更新用户端本地的深度学习模型，得到第二模型参数。

[0073] 差分隐私-卷积神经网络(DPAGD-CNN)算法的算法流程具体如下。

[0074] 在本实施例中，第一模型参数包括损失函数、隐私预算、梯度裁剪阈值、预算增长率和训练数据集批大小。预算增长率表示最优步长参数和噪音梯度参数的变化速度。最优步长参数用于确定向模型参数添加的高斯噪声的大小，噪音梯度参数用于确定给梯度添加的高斯噪声的大小。模型/步长变更概率参数用于判断优化模型参数，还是优化最优步长参

数和噪音梯度参数。

[0075] 用户端在获取服务器下发的第一模型参数之后，将未由服务器分配的剩余差分隐私深度学习的过程参数进行初始化，比如对深度学习模型的模型参数随机赋初值，初始模型训练轮次为0。

[0076] 用户端将隐私预算随机分为最优步长参数和噪音梯度参数，并判断剩余的隐私参数是否大于0。当剩余的隐私预算不大于0时，向服务器返回第二模型参数。

[0077] 当剩余的隐私预算大于0时，初始化模型/步长变更概率参数为0，计算当前模型参数的梯度值，并依据梯度裁剪阈值进行裁剪，向裁剪后的梯度加入高斯噪音，以此减少隐私预算中相应的量，继而依据用户端的训练数据集中的最差数据(损失函数值最大)，向模型/步长变更概率参数添加高斯噪声，以此减少隐私预算相应的量。

[0078] 用户端判断模型/步长变更概率参数是否大于0。当模型/步长变更概率参数大于0时，在剩余的隐私预算不大于0时向服务器返回第二模型参数，在剩余的隐私预算大于0时更新优化自适应差分隐私卷积神经网络中的参数，并重新判断剩余的隐私预算是否大于0。

[0079] 当模型/步长变更概率参数不大于0时，更新最优步长参数和噪音梯度参数，并重新判断剩余的隐私预算是否大于0。

[0080] 在此过程中，最优步长参数越小，用户端数据越符合训练模型，用户端数据添加的高斯噪声分布越集中在大于0的部分，高斯噪音为负的概率越小，则进行最优步长参数、噪音梯度参数优化的概率也越小，反之则越大。

[0081] 在用户端的模型更新中，应用具有自适应梯度下降的差分隐私-卷积神经网络(DPAGD-CNN)算法，即在深度学习模型的迭代训练过程中，通过自适应的方法给梯度加入不同大小的噪音，但总体不改变原有的差分隐私预算。在模型优化过程的开始，使用不容易影响梯度下降正确方向的较大的噪声值，随着模型的优化，梯度下降的方向变得精确，从而有利于提高训练模型的精确度。

[0082] 第三实施例。

[0083] 第三实施例提供一种计算机可读存储介质，所述计算机可读存储介质包括存储的计算机程序，其中，在所述计算机程序运行时控制所述计算机可读存储介质所在设备执行如第一实施例所述的基于差分隐私的联邦学习方法，并达到与之相同的有益效果。

[0084] 综上所述，本发明的实施例具有如下有益效果：

[0085] 通过将预设的第一模型参数，包括隐私预算下发至用户端，使用户端可根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数，进而通过对用户端上传的第二模型参数进行参数平均化，向用户端下发得到的第三模型参数。同时，将上述操作作为一轮模型训练，通过累计模型训练轮次，在模型训练轮次未达到预设阈值时重复执行上述操作，反之结束模型训练。本实施例通过使各个用户端基于差分隐私技术更新其本地的深度学习模型后再上传第二模型参数，有利于保障数据隐私安全，并提高训练模型的精确度；通过对第二模型参数进行参数平均化，能够对第二模型参数进行整合得到第三模型参数，使用户端根据第三模型参数进行下一轮模型训练，有利于提高训练模型的精确度；通过对模型训练轮次设置阈值，使得只有当模型训练轮次达到预设阈值时才结束模型训练，有利于进一步提高训练模型的精确度。

[0086] 以上所述是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员

来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也视为本发明的保护范围。

[0087] 本领域普通技术人员可以理解实现上述实施例中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。


将预设的第一模型参数下发至用户端，使用户端根据第一模型参数，基于差分隐私技术更新用户端本地的深度学习模型并返回第二模型参数；其中，第一模型参数包括隐私预算
S1
对第二模型参数进行参数平均化，得到第三模型参数，并将第三模型参数下发至用户端
S2
将步骤S1~S2的执行总次数作为模型训练轮次，并当模型训练轮次未达到预设阈值时重复执行步骤S1和步骤S2，反之结束模型训练
S3

图1

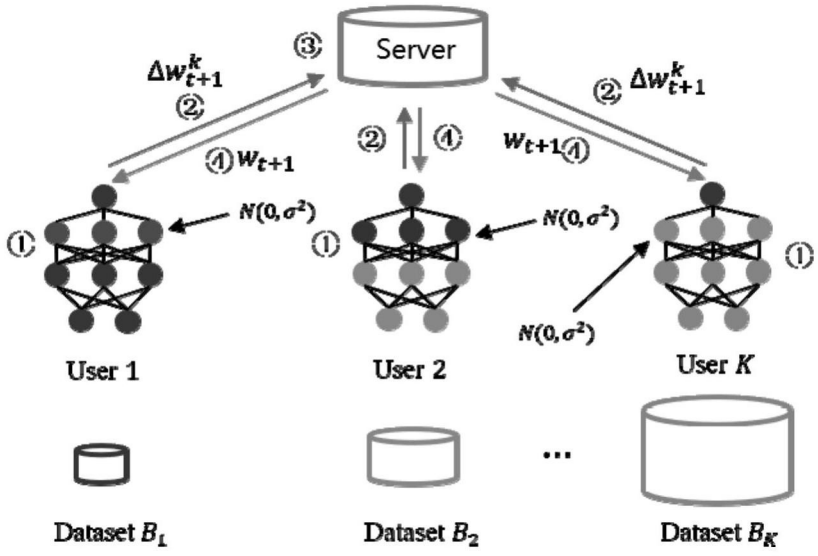
Server
③
Δw_{t+1}^k
②
④ W_{t+1}
$N(0,\sigma^2)$
①
User 1
User 2
User K
Dataset B_1
Dataset B_2
Dataset B_K

图2

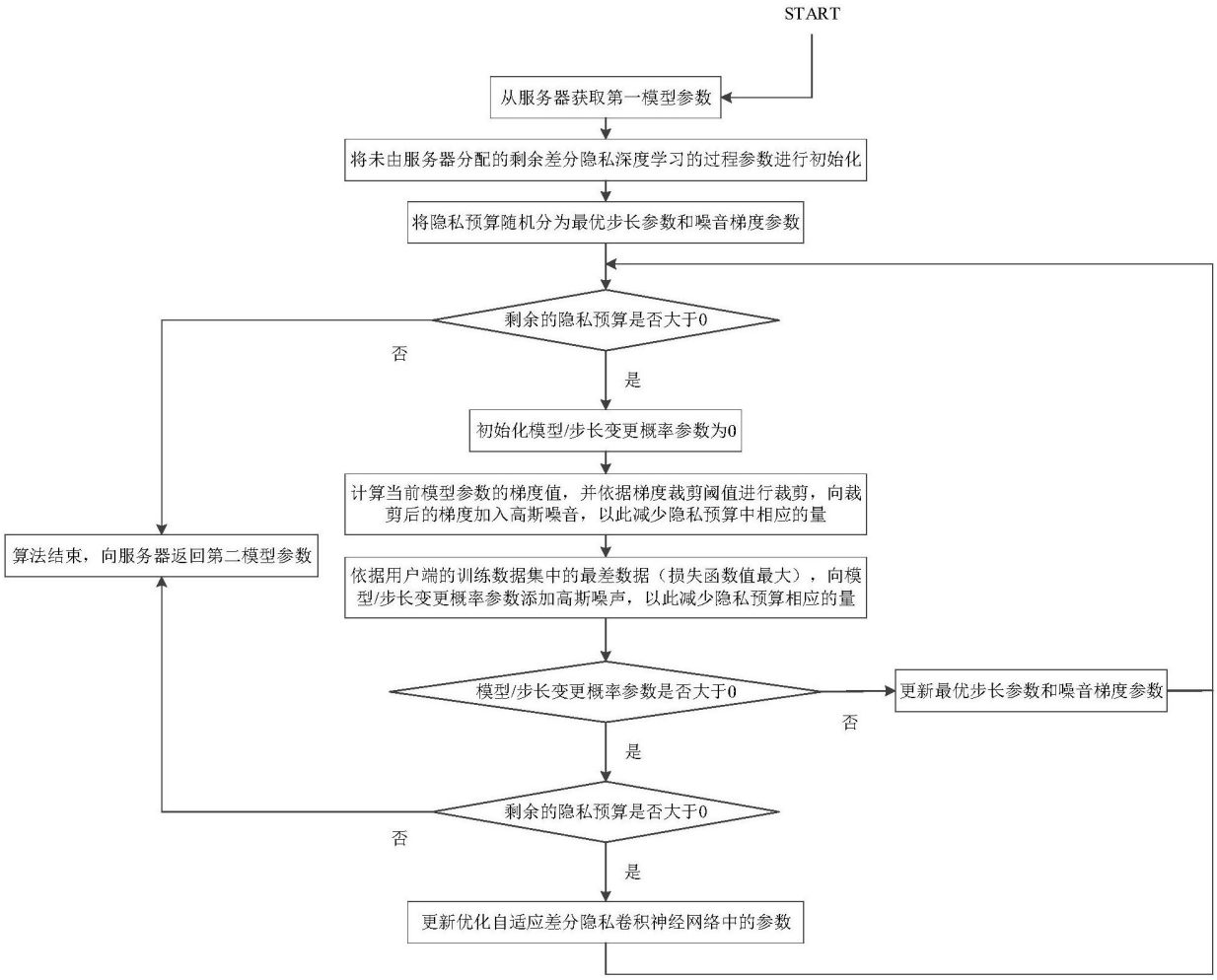
START
从服务器获取第一模型参数
将未由服务器分配的剩余差分隐私深度学习的过程参数进行初始化
将隐私预算随机分为最优步长参数和噪音梯度参数
剩余的隐私预算是否大于0
否
是
初始化模型/步长变更概率参数为0
计算当前模型参数的梯度值，并依据梯度裁剪阈值进行裁剪，向裁剪后的梯度加入高斯噪音，以此减少隐私预算中相应的量
算法结束，向服务器返回第二模型参数
依据用户端的训练数据集中的最差数据（损失函数值最大），向模型/步长变更概率参数添加高斯噪声，以此减少隐私预算相应的量
模型/步长变更概率参数是否大于0
更新最优步长参数和噪音梯度参数
否
是
剩余的隐私预算是否大于0
否
是
更新优化自适应差分隐私卷积神经网络中的参数

图3

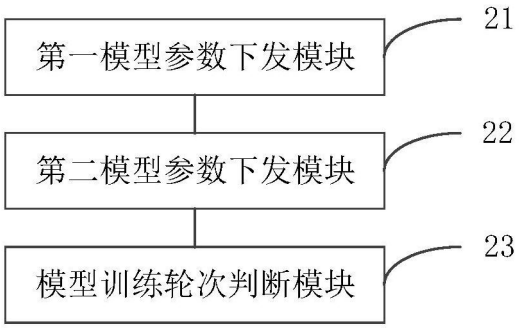
第一模型参数下发模块
21
第二模型参数下发模块
22
模型训练轮次判断模块
23

图4