

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号

WO 2021/179720 A1

(43) 国际公布日

2021 年 9 月 16 日 (16.09.2021)

(51) 国际专利分类号:

G06F 16/28 (2019.01)

(21) 国际申请号:

PCT/CN2020/135588

(22) 国际申请日:

2020 年 12 月 11 日 (11.12.2020)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202011085715.3 2020 年 10 月 12 日 (12.10.2020) CN

(71) 申请人: 平安科技 (深圳) 有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];

中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 王健宗 (WANG, Jianzong); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

肖京 (XIAO, Jing); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

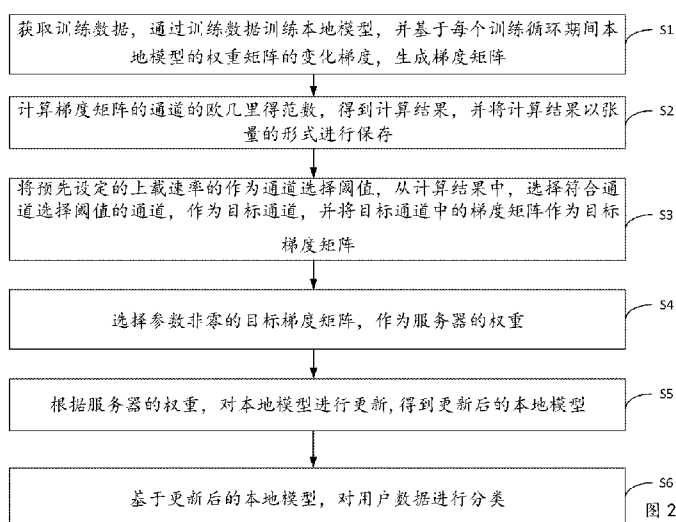
何安珣 (HE, Anxun); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市世联合知识产权代理有限公司 (SL INTELLECTUAL PROPERTY CO., LTD.);

中国广东省深圳市福田区沙头街道天安社区泰然四路 29 号天安创新科技广场一期 A 座 805E, Guangdong 518000 (CN)。

(54) Title: FEDERATED-LEARNING-BASED USER DATA CLASSIFICATION METHOD AND APPARATUS, AND DEVICE AND MEDIUM

(54) 发明名称: 基于联邦学习的用户数据分类方法、装置、设备及介质



S1 Acquire training data, train a local model by means of the training data, and generate a gradient matrix on the basis of a change gradient of a weight matrix of the local model during each training cycle
S2 Calculate the Euclidean norm of a channel of the gradient matrix to obtain a calculation result, and save the calculation result in the form of a tensor
S3 Take a preset upload rate as a channel selection threshold value, select, from the calculation result, a channel conforming to the channel selection threshold value to serve as a target channel, and take a gradient matrix in the target channel as a target gradient matrix
S4 Select a target gradient matrix with a non-zero parameter as the weight of a server
S5 Update the local model according to the weight of the server to obtain an updated local model
S6 Classify user data on the basis of the updated local model

图 2

(57) Abstract: A federated-learning-based user data classification method and apparatus, and a device and a medium, which relate to the technical field of information security. The method comprises: acquiring training data, training a local model by means of the training data, and generating a gradient matrix on the basis of a change gradient of a weight matrix of the local model during each training cycle; taking a preset upload rate as a channel selection threshold value, selecting, from a calculation result, a channel conforming to the channel selection threshold value to serve as a target channel, and taking a gradient matrix in the target channel as a target gradient

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布(细则48.2(h))。
- 根据申请人的请求, 在条约第21条(2)(a)所规定的期限届满之前进行。

matrix; selecting a target gradient matrix with a non-zero parameter as the weight of a server; updating the local model according to the weight of the server; and classifying user data according to an updated local model. The present invention also relates to blockchain technology. The training data is stored in a blockchain. By generating an updated local model, the security of private data of a user is protected during user data classification.

(57) 摘要: 一种基于联邦学习的用户数据分类方法、装置、设备及介质, 涉及信息安全技术领域, 该方法包括: 获取训练数据, 并通过训练数据训练本地模型, 并基于每个训练循环期间本地模型的权重矩阵的变化梯度, 生成梯度矩阵, 将预先设定的上载速率作为通道选择阈值, 从计算结果中, 选择符合所述通道选择阈值的通道, 作为目标通道, 并将目标通道中的梯度矩阵作为目标梯度矩阵; 选择参数非零目标梯度矩阵, 作为服务器的权重; 根据服务器的权重, 对本地模型进行更新, 并根据更新后的本地模型对用户数据进行分类。还涉及区块链技术, 训练数据存储于区块链中。通过生成更新后的本地模型, 实现在用户数据分类时, 保护用户隐私数据安全。

基于联邦学习的用户数据分类方法、装置、设备及介质

本申请要求于 2020 年 10 月 12 日提交中国专利局、申请号为 202011085715.3，发明名称为“基于联邦学习的用户数据分类方法、装置、设备及介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及信息安全技术领域，尤其涉及一种基于联邦学习的用户数据分类方法、装置、设备及介质。

背景技术

一方面随着法律法规的不断完善以及监控的不断加强，数据的集中式处理将面临巨大的法律风险；另一方面各个数据拥有方之间出于安全、经济利益等因素不愿意共享原始数据。这些因素都会导致数据以孤岛的形式存在。为了打破数据孤岛，联邦学习应运而生。联邦学习无须各数据拥有方共享原始数据，可以在保证安全性的条件下，充分地利用各数据拥有方的原始数据进行模型训练，有效解决了人工智能时代的数据孤岛问题。

目前基于联邦学习的用户数据分类方法为：通过服务器节点将待训练模型下发至多个工作节点，各工作节点基于各自所拥有的数据对接收到的待训练模型进行训练，并将训练好的模型参数回传至服务器节点，服务器节点根据接收到的各工作节点的模型参数对待训练模型进行更新，然后重复上述过程直至待训练模型满足预设的性能指标，再通过符合预设性能指标的训练模型对用户数据进行分类。但是，发明人意识到，在这种分类方法过程中，训练数据都共享给执行分析的中央服务器，而提供数据的用户则无法对其进行控制，这样存在用户数据泄露的风险。现亟需一种在对用户数据进行分类时，能够保护用户隐私数据安全的方法。

发明内容

本申请实施例的目的在于提出一种基于联邦学习的用户数据分类方法，在进行用户数据分类时，以提高用户隐私数据的安全性。

为了解决上述技术问题，本申请实施例提供一种基于联邦学习的用户数据分类方法，包括：

获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量的形式进行保存；

将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

选择参数非零的所述目标梯度矩阵，作为服务器的权重；

根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

基于所述更新后的本地模型，对用户数据进行分类。

为了解决上述技术问题，本申请实施例提供一种基于联邦学习的用户数据分类装置，包括：

梯度矩阵获取模块，用于获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算结果获取模块，用于计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量的形式进行保存；

梯度矩阵更新模块，用于将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

服务器的权重模块，用于选择参数非零的所述目标梯度矩阵，作为服务器的权重；

本地模型更新模块，用于根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

用户数据分类模块，用于基于所述更新后的本地模型，对用户数据进行分类。

为了解决上述技术问题，本申请实施例还提供一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量的形式进行保存；

将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

选择参数非零的所述目标梯度矩阵，作为服务器的权重；

根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

基于所述更新后的本地模型，对用户数据进行分类。

为了解决上述技术问题，本申请实施例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存储有计算机可读指令，所述计算机可读指令被处理器执行时实现如下步骤：

获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量的形式进行保存；

将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

选择参数非零的所述目标梯度矩阵，作为服务器的权重；

根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

基于所述更新后的本地模型，对用户数据进行分类。

以上方案中的一种基于联邦学习的用户数据分类方法，通过获取训练数据，并通过训练数据训练本地模型，得到梯度矩阵，并计算梯度矩阵的通道的欧几里得范数，得到计算结果，并将计算结果以张量的形式进行保存，便于后续对计算结果进行筛选更新，然后根据预先设定的上载速率的作为通道选择阈值，从计算结果中，选择符合通道选择阈值的通道，作为目标通道，并将目标通道中的梯度矩阵作为目标梯度矩阵，便于从本地模型向服务器上载了渐变中的一部分通道，并在数据集上上传了部分的通道而不是全部通道获得了更好的性能，在保护隐私的同时减少了梯度的冗余性；最后选择参数非零的目标梯度矩阵，作为服务器的权重，并根据服务器的权重，对本地模型进行更新，得到更新后的本地模型，最后基于更新后的本地模型，对用户数据进行分类。实现在联邦学习训练过程中，将部分权重上传到服务器，而无需将全部权重上传，使得更新后的本地模型在进行用户分类时，减少对用户数据的访问，进而有利于保护用户隐私数据的安全。

附图说明

为了更清楚地说明本申请中的方案，下面将对本申请实施例描述中所需要使用的附图作一个简单介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1是本申请实施例提供的基于联邦学习的用户数据分类方法的应用环境示意图；

图2是根据本申请实施例提供的基于联邦学习的用户数据分类方法的一实现流程图；

图3是本申请实施例提供的基于联邦学习的用户数据分类方法中步骤S3的一实现流程图；

图4是本申请实施例提供的基于联邦学习的用户数据分类装置示意图；

图5是本申请实施例提供的计算机设备的示意图。

具体实施方式

除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同；本文中在申请的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本申请；本申请的说明书和权利要求书及上述附图说明中的术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。本申请的说明书和权利要求书或上述附图中的术语“第一”、“第二”等是用于区别不同对象，而不是用于描述特定顺序。

在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

为了使本技术领域的人员更好地理解本申请方案，下面将结合附图，对本申请实施例中的技术方案进行清楚、完整地描述。

下面结合附图和实施方式对本申请进行详细说明。

请参阅图 1，系统架构 100 可以包括终端设备 101、102、103，网络 104 和服务器 105。网络 104 用以在终端设备 101、102、103 和服务器 105 之间提供通信链路的介质。网络 104 可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

用户可以使用终端设备 101、102、103 通过网络 104 与服务器 105 交互，以接收或发送消息等。终端设备 101、102、103 上可以安装有各种通讯客户端应用，例如网页浏览器应用、搜索类应用、即时通信工具等。

终端设备 101、102、103 可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

服务器 105 可以是提供各种服务的服务器，例如对终端设备 101、102、103 上显示的页面提供支持的后台服务器。

需要说明的是，本申请实施例所提供的一种基于联邦学习的用户数据分类方法一般由服务器执行，相应地，一种基于联邦学习的用户数据分类装置一般设置于服务器中。

应该理解，图 1 中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器的。

请参阅图 2，图 2 示出了基于联邦学习的用户数据分类方法的一种具体实施方式。

需注意的是，若有实质上相同的结果，本申请的方法并不以图 2 所示的流程顺序为限，该方法包括如下步骤：

S1：获取训练数据，通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成梯度矩阵。

具体的，对于联邦学习而言，其过程分为自治和联合两部分。其自治的部分：首先，两个或两个以上的参与方们在各自终端安装初始化的模型，每个参与方拥有相同的模型，之后参与方们可以使用当地的数据训练模型。由于参与方们拥有不同的数据，最终终端所训练的模型也拥有不同的模型参数。联合的部分：不同的模型参数将同时上传到服务器，服务器将完成模型参数的聚合与更新，并且将更新好的参数返回到参与方的终端，各个终端开始下一次的迭代。以上的步骤会一直重复，直到整个训练过程的收敛。在本实施例中，上述参与方为本实施例的本地模型，所以在本地模型的训练过程中，首先会获取各自的训练数据，进行本地模型的训练。

具体的，每一个本地模型在获取到训练数据后，进行训练本地模型，每个本地模型都会生成一个梯度矩阵，该梯度矩阵用以显示每个训练循环期间权重矩阵的变化。例如，将

梯度矩阵表示为 G ，并且与权重矩阵 W 具有相同的形状。由于与权重矩阵相比，偏差矩阵的影响微不足道，因此出于效率考虑，省略了偏差的变化。由于是忽略了偏差矩阵的影响，故而在本实施例中，通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成梯度矩阵。

S2：计算梯度矩阵的通道欧几里得范数，得到计算结果，并将计算结果以张量的形式进行保存。

具体的，考虑到通道必须穿过每一层的神经元并与包含这些神经元索引的 L 维向量相关，因此，计算结果可以以张量的形式进行保存，其中，每个元素其中等于通道规范。

其中，欧几里得度量 (euclidean metric) (也称欧氏距离) 是一个通常采用的距离定义，指在 m 维空间中两个点之间的真实距离，或者向量的自然长度 (即该点到原点的距离)。在二维和三维空间中的欧氏距离就是两点之间的实际距离。向量的范数可以简单形象的理解为向量的长度，或者向量到零点的距离，或者相应的两个点之间的距离。所以欧几里得范数为欧几里得度量相关联的范数，简称 $L2$ 范数。在本实施例中，通过计算通道的欧几里得范数，便于后续对通道的筛选，进而获取到更新后的梯度矩阵。

其中，计算结果为梯度矩阵的每个通道的欧几里得范数。

其中，张量 (Tensor) 是一个定义在一些向量空间和一些对偶空间的笛卡儿积上的多重线性映射，其坐标是 $|n|$ 维空间内，有 $|n|$ 个分量的一种量，其中每个分量都是坐标的函数，而在坐标变换时，这些分量也依照某些规则作线性变换。不同维度的张量代表这不同的含义，0 维张量表示一个标量，标量是一个数字；1 维张量代表向量，1 维张量称为“向量”；2 维张量表示为矩阵；3 维张量表示公用数据存储在张量，如时间序列数据、股价、文本数据 彩色图片 (RGB)。在本实施例中，通过将通道的欧几里得范数以张量的形式进行保存，此时的张量是一个 2 维张量，其可以将梯度矩阵的欧几里得范数以矩阵的形式进行保存，这种形式的张量便于后续通过对张量进行拉直，调整为一维的矢量形式，便于将通道的梯度进行排序，从而便于对目标梯度的筛选。

S3：将预先设定的上载速率的作为通道选择阈值，从计算结果中，选择符合通道选择阈值的通道，作为目标通道，并将目标通道中的梯度矩阵作为目标梯度矩阵。

具体的，预先设定上载速率 α ，本实施例可以将梯度矩阵以张量拉直的方式，将其转化为一维张量的矢量形式并将其排序，再计算上载速率 α 的分位数 q_α ，将计算上载速率 α 分位数 q_α 作为通道选择阈值。然后，根据该通道选择的阈值，从计算结果中，选择符合该阈值的通道，作为目标通道，再获取目标通道中的梯度矩阵，并将其作为目标梯度。

进一步的，本实施例中的通道中对应每个元素的处理，并且对应每个训练数据处理 (即每个元素的处理) 后得到的梯度矩阵。

需要说明的是，预先设定的上载速率根据实际情况而定，此处不做限定。

进一步的，处理梯度有两种处理的方法。负选择：丢弃其通道的欧几里得范数低于上载速率 α 分位数 q_α 的通道，并选择其余参数进行更新。正向选择：选择标准高于上载速率 α 分位数 q_α 且其余参数设置为零的通道。在本实施例中，两种选择方法都可以实行。

但考虑到不同的神经通道可能包含相同的神经元，通过优先选择上传具有相同更新速率的更多参数，正选择往往比负选择表现更好，故而优选选择正选择的方式进行梯度的处理。

S4：选择参数非零的目标梯度矩阵，作为服务器的权重。

具体的，由于目标梯度矩阵存在着数值为零的梯度，该部分梯度矩阵对本地模型的更新并无作用，故而对更新后的梯度进行筛选，得到服务器的权重。

在一具体实施例中，若给定输入梯度矩阵 X ，普通的网络会把梯度矩阵 X 乘上服务器的权重，加上偏差之后传入到下一个隐藏层，但是，在本申请中，由于偏差矩阵与权重矩阵相比，偏差矩阵的影响微不足道，因此出于效率考虑，省略了偏差的变化。所以，在本实施例中，在本地模型中，会忽略偏差的影响，通过服务器的权重进行更新。

S5：根据服务器的权重，对本地模型进行更新，得到更新后的本地模型。

具体的，将服务器的权重传送到本地模型，在本地模型中，根据服务器的权重，对梯度矩阵进行参数的更新，以达到对本地模型进行更新。

在一具体实施例中，服务器更新的伪代码要求：训练集 (X, y) ，更新率 α ，本地模型，服务器在训练集 (X, y) 上训练本地模型并保存梯度 ΔW ；计算每个通道的欧几里得范数，并将结果以张量的形式进行保存；将张量调直为矢量并计算其 α 分位数 t_α ；根据 t_α 从梯度 ΔW 中选择通道，并得到处理后的梯度 $\Delta W_{\sim}$ ；将 $\Delta W_{\sim}$ 的非零部分更新为服务器的权重。返回更新的服务器模型，服务器更新算法在每个全局循环中执行，实现对本地模型的更新。

S6：基于更新后的本地模型，对用户数据进行分类。

具体的，由于在得到更新后的本地模型过程中，只是将部分权重上传到服务器，而无需将全部权重上传，使得更新后的本地模型在进行用户分类时，减少对用户数据的访问，进而有利于保护用户隐私数据的安全。

在本实施例中，通过获取训练数据，并通过训练数据训练本地模型，得到梯度矩阵，并计算梯度矩阵的通道的欧几里得范数，得到计算结果，并将计算结果以张量的形式进行保存，便于后续对计算结果进行筛选更新，然后将预先设定的上载速率的作为通道选择阈值，从计算结果中，选择符合通道选择阈值的通道，作为目标通道，并将目标通道中的梯度矩阵作为目标梯度矩阵，便于从本地模型向服务器上载了渐变中的一部分通道，并在数据集上上传了部分的通道而不是全部通道获得了更好的性能，在保护隐私的同时减少了梯度的冗余性；最后选择更新后的梯度矩阵的非零部分，作为服务器的权重，并根据服务器的权重，对本地模型进行更新，得到更新后的本地模型，最后基于更新后的本地模型，对用户数据进行分类。实现在联邦学习训练过程中，将部分权重上传到服务器，而无需将全部权重上传，使得更新后的本地模型在进行用户分类时，减少对用户数据的访问，进而有利于保护用户隐私数据的安全。。

进一步的，在步骤 S1 中，获取训练数据，通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成梯度矩阵包括：

获取用户数据，并对用户数据进行解析，得到本地模型的通用用户，并获取通用用户

的对应数据，作为训练数据。

具体的，在获取到用户数据后，在对用户数据进行解析时，为了保护用户数据的隐私，会对用户数据进行加密。该加密过程中，存在加密密钥和解密密钥，服务器通过对加密过程中的编号对比，解析出各个本地模型中，存在的相同编码的样本，该相同编码的样本即为本地模型的通用用户。再获取该通用用户的对应数据，将其作为训练数据。进一步的，由于本地模型的用户群体并非完全重合，服务器利用基于户样本对齐技术，在各个本地模型不公开各自数据的前提下确认本地模型间的通用用户，并且不暴露不互相重叠的用户。以便联合这些用户的特征进行建模。

进一步的，在本实施中，样本对齐技术是采用加密的用户样本对齐技术。其中，加密的用户样本对齐技术优选 RSA 加密算法。RSA 加密算法是 1977 年由罗纳德·李维斯特 (Ron Rivest)、阿迪·萨莫尔 (Adi Shamir) 和伦纳德·阿德曼 (Leonard Adleman) 一起提出的。RSA 加密算法通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA 密钥至少为 500 位长，一般推荐使用 1024 位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的 DES 或 IDEA 对话密钥加密，然后使用 RSA 密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成得到梯度矩阵。

具体的，由于忽略了偏差矩阵的影响，所以在每个训练循环期间本地模型的权重矩阵的变化梯度，生成得到梯度矩阵，实现梯度矩阵的获取，有利于后续对目标梯度矩阵的筛选，进而将部分权重上传服务器中，达到保护用户隐私数据安全的目的。

本实施例，通过基于样本对齐技术，获取本地模型共有用户的数据，作为训练数据，再通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成得到梯度矩阵。

请参阅图 3，图 3 示出了步骤 S3 的一种具体实施方式，步骤 S3 中将预先设定的上载速率的作为通道选择阈值，从计算结果中，选择符合通道选择阈值的通道，作为目标通道，并将目标通道中的梯度矩阵作为目标梯度矩阵的具体实现过程，详叙如下：

S31：将计算结果转化为一阶张量的形式，并将计算结果进行排序，得到排序结果。

具体的，由于上述步骤是将梯度矩阵的欧几里得范数以 2 维张量的形式进行保存，所以在本步骤中，将计算结果拉直转化为一阶张量的形式，由一阶张量的表现形式为矢量。故而，通过计算其适量的模，并可以把计算结果按照大小的形式进行排列，得到排列结果。

S32：计算预先设定的上载速率的分位数，得到上载速率的分位数。

具体的，由于要将部分权重上传到服务器，而上传时考虑到具有相同更新速率的参数，其表现会更好，所以需要根据上载速率的分位数作为通道选择阈值。所以要计算预先设定的上载速率的分位数，得到上载速率的分位数。

S33: 将上载速率的分位数作为通道选择阈值, 选择排序结果中符合通道选择阈值的通道, 作为目标通道。

具体的, 在排序结果中, 由于排序结果对应着相应的通道, 故而将符合通道选择阈值的通道, 作为目标通道。

S34: 获取目标通道中的梯度矩阵, 并将目标通道中的梯度矩阵作为目标梯度矩阵。

具体的, 目标通道中有对应的梯度矩阵, 通过获取目标通道中的梯度矩阵, 得到目标梯度矩阵。

本实施例中, 通过将计算结果转化为一阶张量的形式, 并将计算结果进行排序, 得到排序结果, 并计算预先设定的上载速率的分位数, 得到上载速率的分位数, 再将上载速率的分位数作为通道选择阈值, 选择排序结果中符合通道选择阈值的通道, 作为目标通道, 获取目标通道中的梯度矩阵, 并将目标通道中的梯度矩阵作为目标梯度矩阵, 有利于对梯度矩阵的筛选, 并实现减少梯度矩阵的冗余, 减少数据量, 使得上传服务器的梯度更少, 有效的保护用户的隐私数据。

进一步的, 在步骤 S33 中, 将上载速率的分位数作为通道选择阈值, 选择排序结果中符合通道选择阈值的通道, 作为目标通道包括:

在排序结果中, 选择高于上载速率的分位数且其他参数为零的通道, 作为目标通道。

具体的, 由于考虑到不同的神经通道可能包含相同的神经元, 通过优先选择上传具有相同更新速率的更多参数, 所以选择高于上载速率的分位数且其他参数为零的通道, 作为目标通道。

本实施例中, 在排序结果中, 选择高于上载速率的分位数且其他参数为零的通道, 作为目标通道, 有利于提高通道的上传速率, 使得模型的训练更加迅速。

进一步的, 在步骤 S5 中, 根据服务器的权重, 对本地模型进行更新包括:

将服务器的权重传送到本地模型中, 并通过服务器的权重对梯度矩阵进行更新, 得到更新矩阵。

具体的, 通过服务器的权重对本地模型的梯度矩阵更新, 要增加本地模型的梯度矩阵的原始重量, 得到更新矩阵。

通过更新矩阵对本地模型进行更新。

具体的, 由于服务器的权重对本地模型的梯度矩阵的更新, 使得本地模型的参数发生了改变, 进而实现对本地模型的更新。

本实施例中, 通过将服务器的权重传送到本地模型中, 并通过服务器的权重对梯度矩阵进行更新, 得到更新矩阵, 并通过更新矩阵对本地模型进行更新, 实现了本地模型的更新, 并且在对用户数据分类时, 实现了对用户隐私数据的保护。

进一步的, 在步骤: 将服务器的权重传送到本地模型中, 并通过服务器的权重对梯度矩阵进行更新, 得到更新矩阵之前基于联邦学习的用户数据分类方法还包括:

通过线性整流函数对本地模型的隐藏层进行激活, 与 S 形函数对本地模型的输出层进行激活, 构建人工神经网络。

具体的，使用线性整流函数对本地模型的隐藏层进行激活，与 S 形函数对本地模型的输出层进行激活，构建一个神经网络，用于对 3 个完全连接的层以及相应层中的 64、32、1 个神经元进行死亡率的二进制预测。实现对服务器的权重的更新。

其中，神经网络 (Artificial Neural Network, ANN) 简称神经网络 (NN)，是基于生物学中神经网络的基本原理，在理解和抽象了人脑结构和外界刺激响应机制后，以网络拓扑知识为理论基础，模拟人脑的神经系统对复杂信息的处理机制的一种数学模型。该模型以并行分布的处理能力、高容错性、智能化和自学习等能力为特征，将信息的加工和存储结合在一起，以其独特的知识表示方式和智能化的自适应学习能力，引起各学科领域的关注。它实际上是一个有大量简单元件相互连接而成的复杂网络，具有高度的非线性，能够进行复杂的逻辑操作和非线性关系实现的系统。

其中，线性整流函数和 S 形函数为神经网络中的激活函数。

通过神经网络对连接层的神经元进行死亡率的预测，其中，每两个神经元间的连接都代表一个对于通过连接层的服务器的权重。

具体的，由于神经网络是一种运算模型，由大量的节点（或称神经元）之间相互联接构成。每个节点代表一种特定的输出函数，称为激活函数。每两个节点间的连接都代表一个对于通过该连接信号的加权值，称之为权重 (weight)，神经网络就是通过这种方式来模拟人类的记忆。故而通过神经网络对连接层的神经元进行死亡率的预测，进而对服务器的权重的预测与更新。

本实施例中，通过线性整流函数对本地模型的隐藏层进行激活，与 S 形函数对本地模型的输出层进行激活，构建神经网络，通过神经网络对连接层的神经元进行死亡率的预测，实现对服务器的权重的预测与更新，有利于后续对本地模型的更新，在对用户数据分类时，实现保护用户隐私数据的安全。

进一步的，该基于联邦学习的用户数据分类方法还包括：将训练数据存储于区块链中。

需要强调的是，为进一步保证上述训练数据的私密和安全性，上述训练数据还可以存储于一区块链的节点中。

本申请中基于联邦学习的用户数据分类方法涉及人工智能领域中的神经网络、机器学习以及聚类分析。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，该计算机可读指令可存储于一计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory, ROM) 等非易失性存储介质，或随机存储记忆体 (Random Access Memory, RAM) 等。

请参考图 4，作为对上述图 2 所示方法的实现，本申请提供了一种基于联邦学习的用户数据分类装置的一个实施例，该装置实施例与图 2 所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

如图 4 所示，本实施例的基于联邦学习的用户数据分类装置包括：梯度矩阵获取模块

61、计算结果获取模块 62、梯度矩阵更新模块 63、服务器的权重模块 64、本地模块更新模块 65 及用户数据分类模型 66，其中：

梯度矩阵获取模块 61，用于获取训练数据，通过训练数据训练本地模型，并基于每个训练循环期间本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算结果获取模块 62，用于计算梯度矩阵的通道欧几里得范数，得到计算结果，并将计算结果以张量的形式进行保存；

梯度矩阵更新模块 63，用于将预先设定的上载速率的作为通道选择阈值，从计算结果中，选择符合通道选择阈值的通道，作为目标通道，并将目标通道中的梯度矩阵作为目标梯度矩阵，其中，通道对应有训练数据的处理生成后的梯度矩阵；

服务器的权重模块 64，用于选择参数非零的目标梯度矩阵，作为服务器的权重；

本地模块更新模块 65，用于根据服务器的权重，对本地模型进行更新，得到更新后的本地模型；

用户数据分类模型 66，用于基于更新后的本地模型，对用户数据进行分类。

进一步的，梯度矩阵获取模块包括：

训练单元获取单元，用于获取用户数据，并对用户数据进行解析，得到本地模型的通用用户，并获取通用用户的对应数据，作为训练数据；

本地模型训练单元，用于通过训练数据训练本地模型，得到梯度矩阵。

进一步的，梯度矩阵更新模块 63 包括：

排序结果获取单元，用于将计算结果转化为一阶张量的形式，并将计算结果进行排序，得到排序结果；

分位数计算单元，用于计算预先设定的上载速率的分位数，得到上载速率的分位数；

通道选择单元，用于将上载速率的分位数作为通道选择阈值，选择排序结果中符合通道选择阈值的通道，作为目标通道；

梯度矩阵确定单元，用于获取目标通道中的梯度矩阵，并将目标通道中的梯度矩阵作为目标梯度矩阵。

进一步的，通道选择单元包括：

目标通道确定子单元，用于在排序结果中，选择高于上载速率的分位数且其他参数为零的通道，作为目标通道。

进一步的，本地模块更新模块 65 包括：

服务器的权重传送单元，用于将服务器的权重传送到本地模型中，并通过服务器的权重对梯度矩阵进行更新，得到更新矩阵；

本地模型更新单元，用于通过更新矩阵对本地模型进行更新。

进一步的，在服务器的权重传送单元之前，基于联邦学习的用户数据分类装置还包括：

人工神经网络构建子单元，用于通过线性整流函数对本地模型的隐藏层进行激活，与 S 形函数对本地模型的输出层进行激活，构建人工神经网络；

死亡率的预测子单元，用于通过人工神经网络对连接层的神经元进行死亡率的预测，

其中，每两个神经元间的连接都代表一个对于通过连接层的服务器的权重。

进一步的，该基于联邦学习的用户数据分类装置还包括：

区块链存储模块，用于将训练数据存储于区块链中。

需要强调的是，为进一步保证上述训练数据的私密和安全性，上述训练数据还可以存储于一区块链的节点中。

为解决上述技术问题，本申请实施例还提供计算机设备。具体请参阅图 5，图 5 为本实施例计算机设备基本结构框图。

计算机设备 7 包括通过系统总线相互通信连接存储器 71、处理器 72、网络接口 73。需要指出的是，图中仅示出了具有三种组件存储器 71、处理器 72、网络接口 73 的计算机设备 7，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。其中，本技术领域技术人员可以理解，这里的计算机设备是一种能够按照事先设定或存储的指令，自动进行数值计算和/或信息处理的设备，其硬件包括但不限于微处理器、专用集成电路 (Application Specific Integrated Circuit, ASIC)、可编程门阵列 (Field-Programmable Gate Array, FPGA)、数字处理器 (Digital Signal Processor, DSP)、嵌入式设备等。

计算机设备可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。计算机设备可以与用户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互。

存储器 71 至少包括一种类型的计算机可读存储介质，所述计算机可读存储介质可以是非易失性，也可以是易失性，计算机可读存储介质包括闪存、硬盘、多媒体卡、卡型存储器 (例如，SD 或 DX 存储器等)、随机访问存储器 (RAM)、静态随机访问存储器 (SRAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、可编程只读存储器 (PROM)、磁性存储器、磁盘、光盘等。在一些实施例中，存储器 71 可以是计算机设备 7 的内部存储单元，例如该计算机设备 7 的硬盘或内存。在另一些实施例中，存储器 71 也可以是计算机设备 7 的外部存储设备，例如该计算机设备 7 上配备的插接式硬盘，智能存储卡 (Smart Media Card, SMC)，安全数字 (Secure Digital, SD) 卡，闪存卡 (Flash Card) 等。当然，存储器 71 还可以既包括计算机设备 7 的内部存储单元也包括其外部存储设备。本实施例中，存储器 71 通常用于存储安装于计算机设备 7 的操作系统和各类应用软件，例如基于联邦学习的用户数据分类方法的计算机可读指令等。此外，存储器 71 还可以用于暂时地存储已经输出或者将要输出的各类数据。

处理器 72 在一些实施例中可以是中央处理器 (Central Processing Unit, CPU)、控制器、微控制器、微处理器、或其他数据处理芯片。该处理器 72 通常用于控制计算机设备 7 的总体操作。本实施例中，处理器 72 用于运行存储器 71 中存储的计算机可读指令或者处理数据，例如运行一种基于联邦学习的用户数据分类方法的计算机可读指令。

网络接口 73 可包括无线网络接口或有线网络接口，该网络接口 73 通常用于在计算机设备 7 与其他电子设备之间建立通信连接。

本申请还提供了另一种实施方式，即提供一种计算机可读存储介质，计算机可读存储

介质存储有服务器维护计算机可读指令，服务器维护计算机可读指令可被至少一个处理器执行，以使至少一个处理器执行如上述的一种基于联邦学习的用户数据分类方法的步骤。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，空调器，或者网络设备等）执行本申请各个实施例的方法。

本申请所指区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain)，本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层等。

显然，以上所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例，附图中给出了本申请的较佳实施例，但并不限制本申请的专利范围。本申请可以以许多不同的形式来实现，相反地，提供这些实施例的目的是使对本申请的公开内容的理解更加透彻全面。尽管参照前述实施例对本申请进行了详细的说明，对于本领域的技术人员来而言，其依然可以对前述各具体实施方式所记载的技术方案进行修改，或者对其中部分技术特征进行等效替换。凡是利用本申请说明书及附图内容所做的等效结构，直接或间接运用在其他相关的技术领域，均同理在本申请专利保护范围之内。

权利要求书

1、一种基于联邦学习的用户数据分类方法，包括：

获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

5 计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量的形式进行保存；

将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

10 选择参数非零的所述目标梯度矩阵，作为服务器的权重；

根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

基于所述更新后的本地模型，对用户数据进行分类。

2、根据权利要求1所述的基于联邦学习的用户数据分类方法，其中，所述获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩
15 阵的变化梯度，生成梯度矩阵包括：

获取用户数据，并对所述用户数据进行解析，得到本地模型的通用用户，并获取所述通用用户的对应数据，作为所述训练数据；

通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成得到梯度矩阵。

20 3、根据权利要求1所述的基于联邦学习的用户数据分类方法，其中，所述将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵包括：

将所述计算结果转化为一阶张量的形式，并将所述计算结果进行排序，得到排序结果；

计算所述预先设定的上载速率的分位数，得到上载速率的分位数；

25 将所述上载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道；

获取所述目标通道中的梯度矩阵，并将所述目标通道中的梯度矩阵作为所述目标梯度矩阵。

4、根据权利要求3所述的基于联邦学习的用户数据分类方法，其中，所述将所述上
30 载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道包括：

在所述排序结果中，选择高于所述上载速率的分位数且其他参数为零的通道，作为所述目标通道。

5、根据权利要求1至4任一项所述的基于联邦学习的用户数据分类方法，其中，所
35 述根据所述服务器的权重，对所述本地模型进行更新包括：

将所述服务器的权重传送到本地模型中，并通过服务器的权重对所述梯度矩阵进行更

新, 得到更新矩阵;

通过所述更新矩阵对所述本地模型进行更新。

6、根据权利要求5所述的基于联邦学习的用户数据分类方法, 其中, 在所述将所述服务器的权重传送到本地模型中, 并通过服务器的权重对所述梯度矩阵进行更新, 得到更新矩阵之前, 所述方法包括:

通过线性整流函数对本地模型的隐藏层进行激活, 与S形函数对本地模型的输出层进行激活, 构建人工神经网络;

通过所述人工神经网络对连接层的神经元进行死亡率的预测, 其中, 每两个神经元间的连接都代表一个对于通过所述连接层的服务器的权重。

7、根据权利要求1所述的基于联邦学习的用户数据分类方法, 其中, 将所述训练数据存储于区块链中。

8、一种基于联邦学习的用户数据分类装置, 包括:

梯度矩阵获取模块, 用于获取训练数据, 通过所述训练数据训练本地模型, 并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度, 生成梯度矩阵;

计算结果获取模块, 用于计算所述梯度矩阵的通道的欧几里得范数, 得到计算结果, 并将所述计算结果以张量的形式进行保存;

梯度矩阵更新模块, 用于将预先设定的上载速率的作为通道选择阈值, 从所述计算结果中, 选择符合所述通道选择阈值的通道, 作为目标通道, 并将所述目标通道中的梯度矩阵作为目标梯度矩阵, 其中, 所述通道对应有所述训练数据的处理生成后的梯度矩阵;

服务器的权重模块, 用于选择参数非零的所述目标梯度矩阵, 作为服务器的权重;

本地模块更新模块, 用于根据所述服务器的权重, 对所述本地模型进行更新, 得到更新后的本地模型;

用户数据分类模块, 用于基于所述更新后的本地模型, 对用户数据进行分类。

9、一种计算机设备, 包括存储器和处理器, 所述存储器中存储有计算机可读指令, 所述处理器执行所述计算机可读指令时实现如下步骤:

获取训练数据, 通过所述训练数据训练本地模型, 并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度, 生成梯度矩阵;

计算所述梯度矩阵的通道的欧几里得范数, 得到计算结果, 并将所述计算结果以张量的形式进行保存;

将预先设定的上载速率的作为通道选择阈值, 从所述计算结果中, 选择符合所述通道选择阈值的通道, 作为目标通道, 并将所述目标通道中的梯度矩阵作为目标梯度矩阵, 其中, 所述通道对应有所述训练数据的处理生成后的梯度矩阵;

选择参数非零的所述目标梯度矩阵, 作为服务器的权重;

根据所述服务器的权重, 对所述本地模型进行更新, 得到更新后的本地模型;

基于所述更新后的本地模型, 对用户数据进行分类。

10、根据权利要求9所述的计算机设备, 其中, 所述获取训练数据, 通过所述训练数

据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵包括：

获取用户数据，并对所述用户数据进行解析，得到本地模型的通用用户，并获取所述通用用户的对应数据，作为所述训练数据；

- 5 通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成得到梯度矩阵。

11、根据权利要求 9 所述的计算机设备，其中，所述将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵包括：

- 10 将所述计算结果转化为一阶张量的形式，并将所述计算结果进行排序，得到排序结果；
计算所述预先设定的上载速率的分位数，得到上载速率的分位数；

将所述上载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道；

- 15 获取所述目标通道中的梯度矩阵，并将所述目标通道中的梯度矩阵作为所述目标梯度矩阵。

12、根据权利要求 11 所述的计算机设备，其中，所述将所述上载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道包括：

在所述排序结果中，选择高于所述上载速率的分位数且其他参数为零的通道，作为所述目标通道。

- 20 13、根据权利要求 9-12 任一项所述的计算机设备，其中，所述根据所述服务器的权重，对所述本地模型进行更新包括：

将所述服务器的权重传送到本地模型中，并通过服务器的权重对所述梯度矩阵进行更新，得到更新矩阵；

通过所述更新矩阵对所述本地模型进行更新。

- 25 14、根据权利要求 13 所述的计算机设备，其中，在所述将所述服务器的权重传送到本地模型中，并通过服务器的权重对所述梯度矩阵进行更新，得到更新矩阵之前，所述方法包括：

通过线性整流函数对本地模型的隐藏层进行激活，与 S 形函数对本地模型的输出层进行激活，构建人工神经网络；

- 30 通过所述人工神经网络对连接层的神经元进行死亡率的预测，其中，每两个神经元间的连接都代表一个对于通过所述连接层的服务器的权重。

15、一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现如下步骤：

- 35 获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵；

计算所述梯度矩阵的通道的欧几里得范数，得到计算结果，并将所述计算结果以张量

的形式进行保存；

将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵，其中，所述通道对应有所述训练数据的处理生成后的梯度矩阵；

5 选择参数非零的所述目标梯度矩阵，作为服务器的权重；

根据所述服务器的权重，对所述本地模型进行更新，得到更新后的本地模型；

基于所述更新后的本地模型，对用户数据进行分类。

16、根据权利要求 15 所述的一种计算机可读存储介质，其中，所述获取训练数据，通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成梯度矩阵包括：

获取用户数据，并对所述用户数据进行解析，得到本地模型的通用用户，并获取所述通用用户的对应数据，作为所述训练数据；

通过所述训练数据训练本地模型，并基于每个训练循环期间所述本地模型的权重矩阵的变化梯度，生成得到梯度矩阵。

15 17、根据权利要求 15 所述的一种计算机可读存储介质，其中，所述将预先设定的上载速率的作为通道选择阈值，从所述计算结果中，选择符合所述通道选择阈值的通道，作为目标通道，并将所述目标通道中的梯度矩阵作为目标梯度矩阵包括：

将所述计算结果转化为一阶张量的形式，并将所述计算结果进行排序，得到排序结果；

计算所述预先设定的上载速率的分位数，得到上载速率的分位数；

20 将所述上载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道；

获取所述目标通道中的梯度矩阵，并将所述目标通道中的梯度矩阵作为所述目标梯度矩阵。

25 18、根据权利要求 17 所述的一种计算机可读存储介质，其中，所述将所述上载速率的分位数作为通道选择阈值，选择所述排序结果中符合所述通道选择阈值的通道，作为目标通道包括：

在所述排序结果中，选择高于所述上载速率的分位数且其他参数为零的通道，作为所述目标通道。

30 19、根据权利要求 15-18 任一项所述的一种计算机可读存储介质，其中，所述根据所述服务器的权重，对所述本地模型进行更新包括：

将所述服务器的权重传送到本地模型中，并通过服务器的权重对所述梯度矩阵进行更新，得到更新矩阵；

通过所述更新矩阵对所述本地模型进行更新。

35 20、根据权利要求 19 所述的一种计算机可读存储介质，其中，在所述将所述服务器的权重传送到本地模型中，并通过服务器的权重对所述梯度矩阵进行更新，得到更新矩阵之前，所述方法包括：

通过线性整流函数对本地模型的隐藏层进行激活，与 S 形函数对本地模型的输出层进行激活，构建人工神经网络；

通过所述人工神经网络对连接层的神经元进行死亡率的预测，其中，每两个神经元间的连接都代表一个对于通过所述连接层的服务器的权重。

5

10

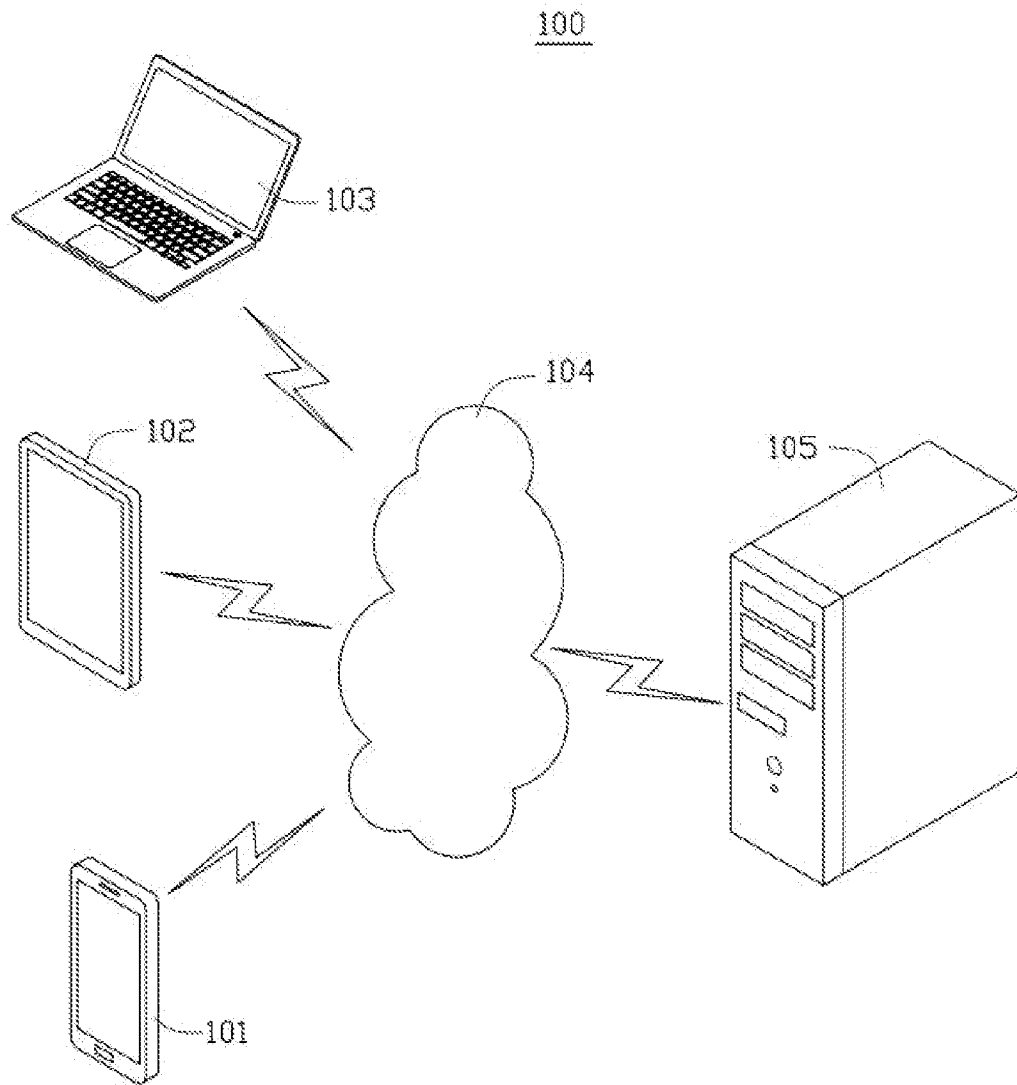
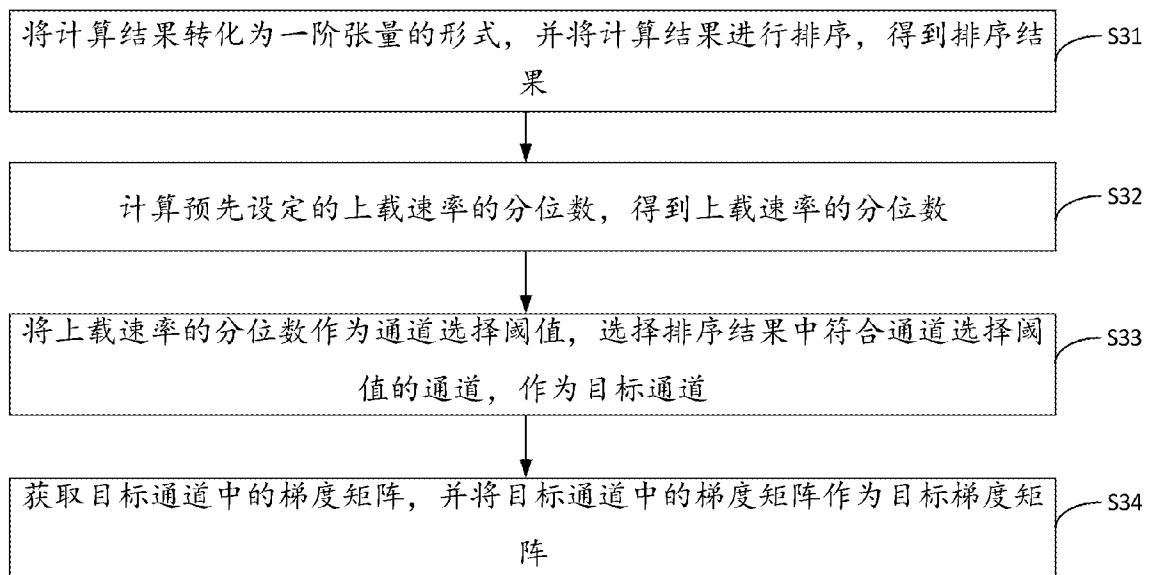
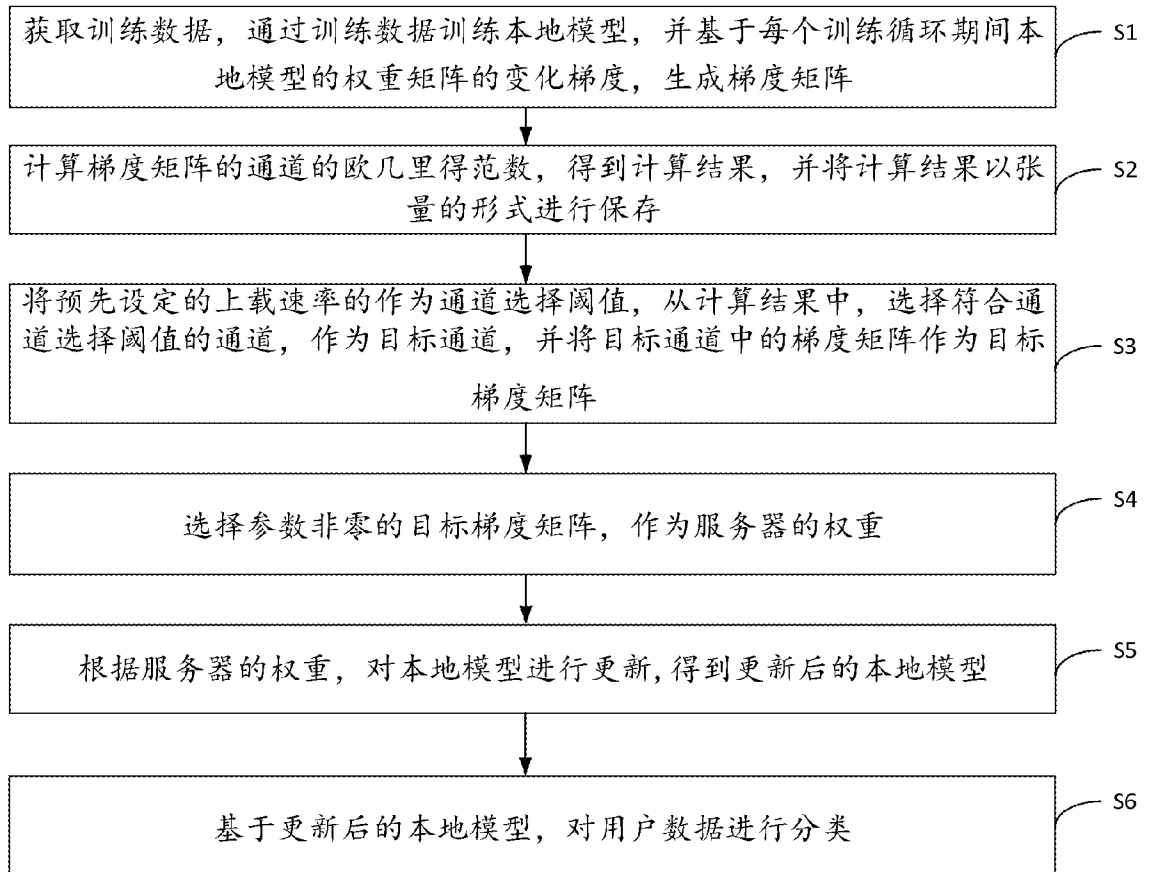


图 1



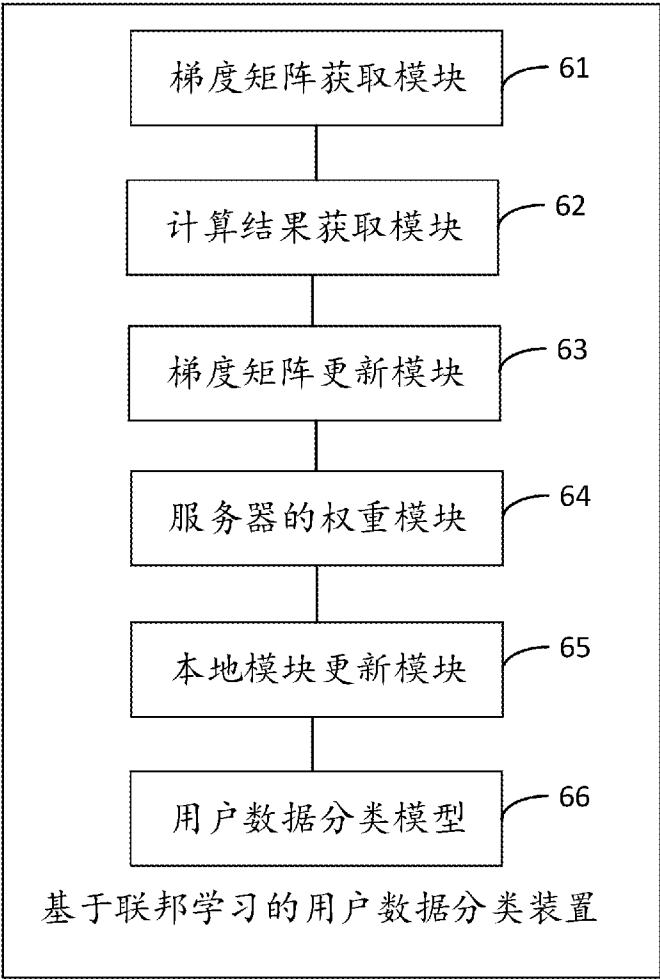


图 4

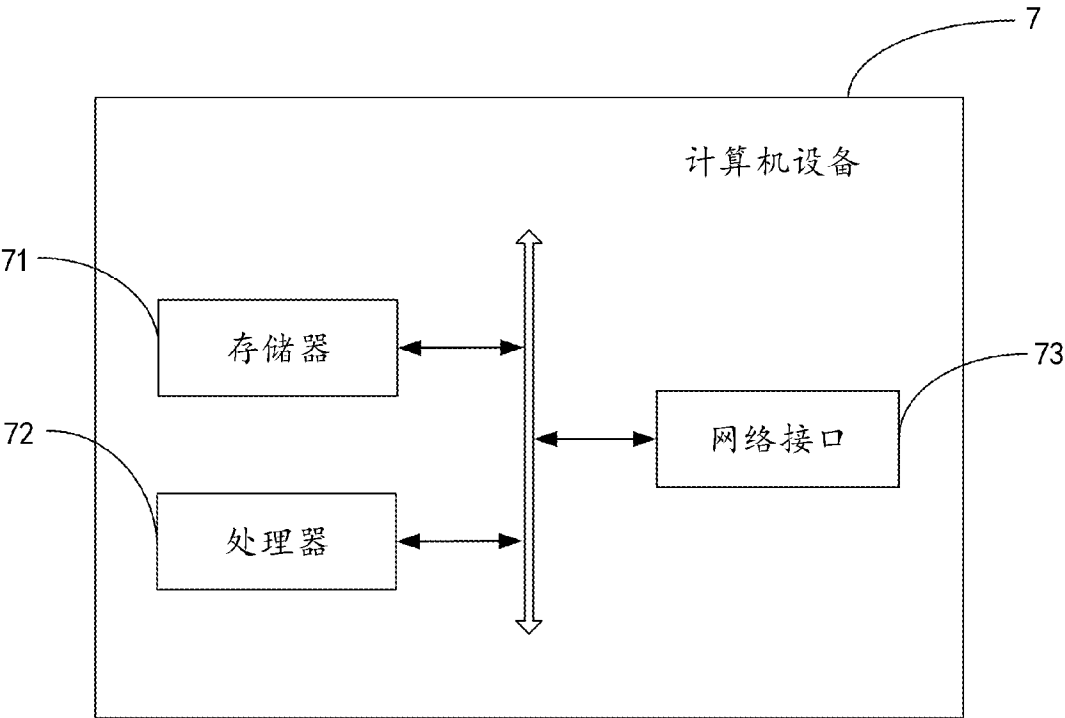


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/135588

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/28(2019.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: 联邦学习, 梯度, 矩阵, 权重, 权值, 通道, 分类, 模型, 训练, 张量, classify+, study, matrix, federal, learn+, model, train+, gradient

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 111460528 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 28 July 2020 (2020-07-28) description, paragraphs [0042]-[0131]	1-20
A	CN 110569227 A (ALIBABA GROUP HOLDING LIMITED) 13 December 2019 (2019-12-13) entire document	1-20
A	CN 110288094 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 27 September 2019 (2019-09-27) entire document	1-20
A	US 2017011280 A1 (XEROX CORPORATION) 12 January 2017 (2017-01-12) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

28 June 2021

Date of mailing of the international search report

09 July 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/135588

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111460528	A	28 July 2020	None			
CN	110569227	A	13 December 2019	WO	2021027258	A1	18 February 2021
				US	2020177364	A1	04 June 2020
				HK	40018826	A0	09 October 2020
CN	110288094	A	27 September 2019	None			
US	2017011280	A1	12 January 2017	None			

国际检索报告

国际申请号

PCT/CN2020/135588

A. 主题的分类 G06F 16/28 (2019.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																	
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) WPI, EPDOC, CNPAT, CNKI: 联邦学习, 梯度, 矩阵, 权重, 权值, 通道, 分类, 模型, 训练, 张量, classify+, study, matrix, federal, learn+, model, train+, gradient																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 111460528 A (支付宝杭州信息技术有限公司) 2020年 7月 28日 (2020 - 07 - 28) 说明书第[0042]-[0131]段</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 110569227 A (阿里巴巴集团控股有限公司) 2019年 12月 13日 (2019 - 12 - 13) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 110288094 A (深圳前海微众银行股份有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2017011280 A1 (XEROX CORPORATION) 2017年 1月 12日 (2017 - 01 - 12) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 111460528 A (支付宝杭州信息技术有限公司) 2020年 7月 28日 (2020 - 07 - 28) 说明书第[0042]-[0131]段	1-20	A	CN 110569227 A (阿里巴巴集团控股有限公司) 2019年 12月 13日 (2019 - 12 - 13) 全文	1-20	A	CN 110288094 A (深圳前海微众银行股份有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文	1-20	A	US 2017011280 A1 (XEROX CORPORATION) 2017年 1月 12日 (2017 - 01 - 12) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
A	CN 111460528 A (支付宝杭州信息技术有限公司) 2020年 7月 28日 (2020 - 07 - 28) 说明书第[0042]-[0131]段	1-20															
A	CN 110569227 A (阿里巴巴集团控股有限公司) 2019年 12月 13日 (2019 - 12 - 13) 全文	1-20															
A	CN 110288094 A (深圳前海微众银行股份有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文	1-20															
A	US 2017011280 A1 (XEROX CORPORATION) 2017年 1月 12日 (2017 - 01 - 12) 全文	1-20															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件													
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																
国际检索实际完成的日期	国际检索报告邮寄日期																
2021年 6月 28日	2021年 7月 9日																
ISA/CN的名称和邮寄地址	受权官员																
中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	田晶																
传真号 (86-10)62019451	电话号码 86-(10)-53961334																

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/135588

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	111460528	A	2020年 7月 28日	无			
CN	110569227	A	2019年 12月 13日	WO	2021027258	A1	2021年 2月 18日
				US	2020177364	A1	2020年 6月 4日
				HK	40018826	A0	2020年 10月 9日
CN	110288094	A	2019年 9月 27日	无			
US	2017011280	A1	2017年 1月 12日	无			