

(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

(43) 国际公布日  
2024 年 2 月 22 日 (22.02.2024)



(10) 国际公布号  
**WO 2024/036880 A1**

(51) 国际专利分类号:  
**G06F 21/62** (2013.01) **G06N 20/00** (2019.01)

上海市浦东新区含笑路 36 号银联大厦  
7 楼, Shanghai 200135 (CN)。

(21) 国际申请号: PCT/CN2023/071564

(22) 国际申请日: 2023 年 1 月 10 日 (10.01.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
202210975564.1 2022 年 8 月 15 日 (15.08.2022) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 张远健 (ZHANG, Yuanjian); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。周雍恺 (ZHOU, Yongkai); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。陈钟正 (CHEN, Zhongzheng); 中国

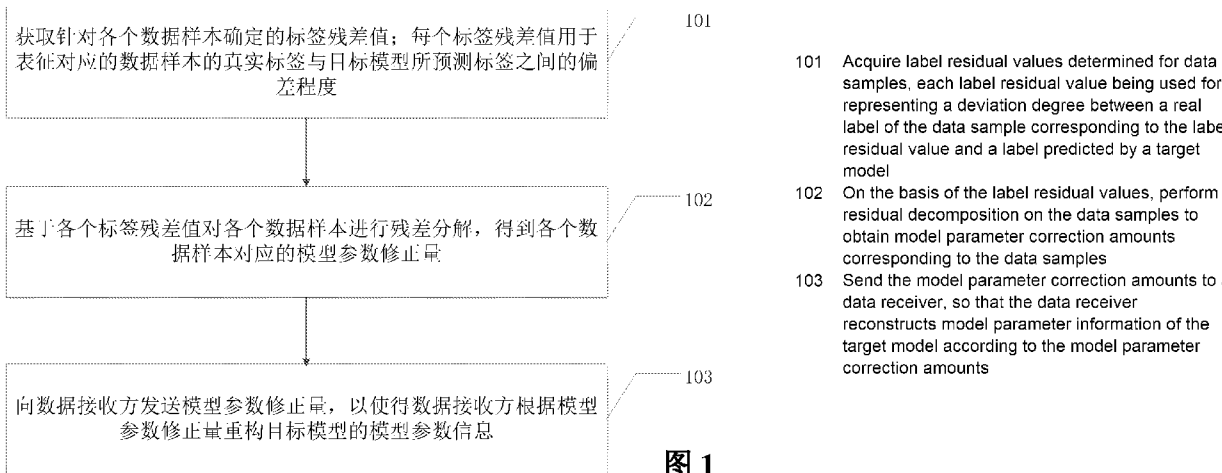
(74) 代理人: 北京市中伦律师事务所 (ZHONG LUN LAW FIRM); 中国北京市朝阳区金和东路 20 号院正大中心南塔 24 层, Beijing 100020 (CN)。

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, CV, GH, GM, KE, LR, LS, MW, MZ,

(54) Title: DATA PROCESSING METHOD AND APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 一种数据处理方法、装置、电子设备及存储介质



(57) Abstract: The present disclosure provides a data processing method and apparatus, an electronic device, and a storage medium. The method comprises: acquiring label residual values determined for data samples, each label residual value being used for representing a deviation degree between a real label of the data sample corresponding to the label residual value and a label predicted by a target model; on the basis of the label residual values, performing residual decomposition on the data samples to obtain model parameter correction amounts corresponding to the data samples; and sending the model parameter correction amounts to a data receiver, so that the data receiver reconstructs model parameter information of the target model according to the model parameter correction amounts. According to the present disclosure, a residual can be effectively disturbed by means of residual decomposition, so that a data sender can protect a real label owned thereby, and meanwhile, the data sender can transmit necessary correction information (i.e., model parameter correction amounts) to a data receiver to reconstruct accurate model parameter information, thereby further ensuring model training performance.

NA, RW, SC, 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, ME, 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))。

**(57)** 摘要: 本公开提供了一种数据处理方法、装置、电子设备及存储介质, 其中, 该方法包括: 获取针对各个数据样本确定的标签残差值; 每个标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度; 基于各个标签残差值对各个数据样本进行残差分解, 得到各个数据样本对应的模型参数修正量; 向数据接收方发送模型参数修正量, 以使得数据接收方根据模型参数修正量重构目标模型的模型参数信息。本公开通过残差分解可以有效地对残差进行扰动, 这使得数据发送方能够保护其拥有的真实标签, 与此同时, 数据发送方可以传递必要的修正信息(即模型参数修正量)给数据接收方以重构精准的模型参数信息, 进一步确保了模型的训练性能。

## 一种数据处理方法、装置、电子设备及存储介质

本申请要求于 2022 年 08 月 15 日提交的、申请号为 CN202210975564.1、  
标题为“一种数据处理方法、装置、电子设备及存储介质”的中国专利申  
5 请的优先权，该中国专利申请的公开内容以引用的方式并入本文。

### 技术领域

本公开涉及数据安全技术领域，具体而言，涉及一种数据处理方法、  
装置、电子设备及存储介质。

### 背景技术

10 随着人工智能和大数据挖掘分析等应用领域的发展，对数据量的需求  
越来越大。为了进行更大价值的挖掘，往往需要多方数据的融合。这里的  
多方数据可以是来源于不同的组织，例如，交易数据可以分散于金融结构，  
医疗诊断记录可以是来源于医疗机构，此外，还可以是来自于不同的行业，  
例如，同样是交易数据可以来自于电商还可以来自于金融。

15 多方数据要素在流通过程中受到监管部门的合规约束，使得将明细数  
据集中式收集后训练模型用于业务经营的方式并不可行，这构成了数据壁  
垒。为了打破数据壁垒，可以采用联邦学习的方法使得各个参与方在无需  
共享其隐私数据的前提下获得全局模型，这里的隐私数据可以是有关目标  
用户的标签信息，例如，目标用户是否为高净值用户。在合理挖掘数据的  
20 应用价值的同时，也需要防止出现数据滥用，实现对隐私数据的保护。在  
实际应用中，可以通过加密的方式交换模型相关信息以实现协同优化联邦  
模型。

相关技术中提供了一种残差加密方式，以标签数据作为隐私数据为例，  
有标签方可以在发送模型相关信息之前，以加法的形式作一个差分隐私，  
25 使得满足差分隐私条件后，再由有标签方以同态加密的形式发送给无标签

方。由于噪声的存在，无标签方无法根据掌握的模型相关参数重构真实的残差，从而达到保护隐私数据的目的。

然而，由于差分隐私自带噪声的原因，这使得无标签方后续在模型精度上存在一定的性能损失。

## 5 发明内容

本公开实施例至少提供一种数据处理方法、装置、电子设备及存储介质，数据发送方通过残差分解的方式对标签这一隐私数据进行加密，数据接收方基于加密得到的模型参数修正量进行模型参数重构，重构的模型精度较高。

10 第一方面，本公开实施例提供了一种数据处理方法，包括：

获取针对各个数据样本确定的标签残差值；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

基于各个所述标签残差值对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量；

15 向数据接收方发送所述模型参数修正量，以使得所述数据接收方根据所述模型参数修正量重构所述目标模型的模型参数信息。

在一种可能的实施方式中，所述基于各个所述标签残差值对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量，包括：

20 按照数据大小的排列顺序将各个所述标签残差值进行排序，得到排序的各个标签残差值；

在从所述各个数据样本中选取出需要进行残差分解的目标数据样本的情况下，对所述目标数据样本所在排序的标签残差值进行变化，得到所述各个数据样本对应的残差变化信息；

25 基于所述各个数据样本对应的残差变化信息以及所述各个数据样本的

真实标签，确定所述各个数据样本对应的模型参数修正量。

在一种可能的实施方式中，按照如下步骤从所述各个数据样本中选取需要进行残差分解的目标数据样本：

按照预设分组数量将所述排序的各个标签残差值进行分组，得到分组  
5 后的标签残差值；

从每个分组后的标签残差值中选取预设数量个目标标签残差值；

将所述目标标签残差值对应的数据样本确定为所述目标数据样本。

在一种可能的实施方式中，在所述各个数据样本对应的残差变化信息  
对应残差变化向量的情况下，所述对所述目标数据样本所在排序的标签残  
10 差值进行变化，得到所述各个数据样本对应的残差变化信息，包括：

针对每个所述数据样本，在判断出所述数据样本非所述目标数据样本  
的情况下，确定所述数据样本对应第一残差变化值；或者，

在判断出所述数据样本是所述目标数据样本，且所述数据样本的标签  
残差值大于零的情况下，确定所述数据样本对应第二残差变化值；或者，

15 在判断出所述数据样本是所述目标数据样本，且所述数据样本的标签  
残差值小于零的情况下，确定所述数据样本对应第三残差变化值；

将各个所述数据样本分别对应的残差变化值进行集合，确定所述残差  
变化向量；其中，所述残差变化向量用于表征所述各个数据样本的标签残  
差值是否发生变化。

20 在一种可能的实施方式中，所述基于所述各个数据样本对应的残差变  
化信息以及所述各个数据样本的真实标签，确定所述各个数据样本对应的  
模型参数修正量，包括：

将所述残差变化向量以及所述残差变化向量的转置结果进行点乘运  
算，确定第一算子；以及，在确定所述各个数据样本的真实标签对应的标  
25 签值的情况下，确定与所述标签值对应的第二算子；

基于所述第一算子和所述第二算子，确定所述各个数据样本对应的模型参数修正量。

在一种可能的实施方式中，在得到所述各个数据样本对应的残差变化信息之后，所述方法还包括：

- 5        基于所述各个数据样本对应的残差变化信息和所述排序的各个标签残差值之间的乘积运算，确定变化后的标签残差值；

基于所述变化后的标签残差值确定向所述数据接收方发送的模型参数信息；

向所述数据接收方发送所述模型参数信息。

- 10       在一种可能的实施方式中，所述向所述数据接收方发送所述模型参数信息，包括：

在未达到模型收敛条件的情况下，向所述数据接收方发送所述模型参数信息；

所述向数据接收方发送所述模型参数修正量，包括：

- 15       在达到模型收敛条件的情况下，向所述数据接收方发送所述模型参数修正量。

第二方面，本公开还提供了一种数据处理方法，包括：

- 接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，所述模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解  
20       确定的；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

根据所述模型参数修正量重构所述目标模型的模型参数信息。

在一种可能的实施方式中，所述根据所述模型参数修正量重构所述目标模型的模型参数信息，包括：

获取针对目标模型输入的数据特征信息；

基于所述数据特征信息和所述模型参数修正量，确定所述目标模型的模型参数信息。

5 在一种可能的实施方式中，在所述数据特征信息包括数据特征向量的情况下，所述基于所述数据特征信息和所述模型参数修正量，确定所述目标模型的模型参数信息，包括：

将所述数据特征向量以及所述数据特征向量的转置结果进行点乘运算，确定第三算子；以及，将所述数据特征向量的转置结果以及所述数据特征向量进行点乘运算，确定第四算子；

10 基于所述第三算子、所述第四算子以及所述模型参数修正量，确定所述目标模型的模型参数信息。

第三方面，本公开还提供了一种数据处理装置，包括：

15 获取模块，用于获取针对各个数据样本确定的标签残差值；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

分解模块，用于基于各个所述标签残差值对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量；

发送模块，用于向数据接收方发送所述模型参数修正量，以使得所述数据接收方根据所述模型参数修正量重构所述目标模型的模型参数信息。

20 第四方面，本公开还提供了一种数据处理装置，包括：

接收模块，用于接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，所述模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解确定的；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

25 重构模块，用于根据所述模型参数修正量重构所述目标模型的模型参

数信息。

第五方面，本公开还提供了一种电子设备，包括：处理器、存储器和总线，所述存储器存储有所述处理器可执行的机器可读指令，当电子设备运行时，所述处理器与所述存储器之间通过总线通信，所述机器可读指令被所述处理器执行时执行如第一方面及其各种实施方式、第二方面及其各种实施方式任一项所述的数据处理方法。

第六方面，本公开还提供了一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行如第一方面及其各种实施方式、第二方面及其各种实施方式任一项所述的数据处理方法。

采用上述数据处理方法、装置、电子设备及存储介质，在获取到针对各个数据样本确定的标签残差值的情况下，可以基于各个所述标签残差值对所述各个数据样本进行残差分解，而后可以将残差分解得到的各个数据样本对应的模型参数修正量发送给数据接收方，数据接收方则可以根据模型参数修正量重构模型参数信息。本公开中，数据发送方（即有标签方）在进行残差分解的过程中，可以有效地对残差进行扰动，使得数据接收方（即无标签方）仅能构造带错误标签信息的模型，这使得数据发送方能够保护其拥有的真实标签，与此同时，有标签方可以传递必要的修正信息（即模型参数修正量）给无标签方，使得无标签方可以按照修正信息重构精准的模型参数信息，进一步确保了模型的训练性能。

本公开的其他优点将配合以下的说明和附图进行更详细的解说。

应当理解，上述说明仅是本公开技术方案的概述，以便能够更清楚地了解本公开的技术手段，从而可依照说明书的内容予以实施。为了让本公开的上述和其它目的、特征和优点能够更明显易懂，以下特举例说明本公开的具体实施方式。

## 附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，此处的附图被并入说明书中并构成本说明书中的一部分，这些附图示出了符合本公开的实施例，并与说明书一起用于说明本公开的技术方案。应当理解，以下附图仅示出了本公开的某些实施例，因此不应被看作是对范围的限定，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相关的附图。而且在整个附图中，用相同的标号表示相同的部件。在附图中：

图 1 示出了本公开实施例所提供的一种数据处理方法的流程图；

图 2 示出了本公开实施例所提供的数据处理方法中，确定残差变化信息具体方法的流程图；

图 3 示出了本公开实施例所提供的一种数据处理方法的时序流程图；

图 4 示出了本公开实施例所提供的一种数据处理方法的应用示意图；

图 5 示出了本公开实施例所提供的另一种数据处理方法的流程图；

图 6 示出了本公开实施例所提供的一种数据处理装置的示意图；

图 7 示出了本公开实施例所提供的另一种数据处理装置的示意图；

图 8 示出了本公开实施例所提供的一种电子设备的示意图。

## 具体实施方式

下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

在本公开实施方式的描述中，应理解，诸如“包括”或“具有”等术语旨在指示本说明书中所公开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不旨在排除一个或多个其他特征、数字、步骤、行为、

部件、部分或其组合存在的可能性。

除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本文中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。

术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”等的特征可以明示或者隐含地包括一个或者更多个这一特征。在本公开实施方式的描述中，除非另有说明，“多个”的含义是两个或两个以上。

经研究发现，相关技术中可以通过加密的方式交换模型相关信息以实现协同优化联邦模型。

相关技术中提供了一种残差加密方式，以标签数据作为隐私数据为例，有标签方可以在发送模型相关信息之前，以加法的形式作一个差分隐私，使得满足差分隐私条件后，再由有标签方以同态加密的形式发送给无标签方。

其中，在进行差分隐私的过程，也即是给残差  $r_i$  增加噪声的过程，使得差分隐私  $\tilde{r}_i = r_i + noise$ ，其中所增加的噪声满足条件  $noise \sim Lap(2\epsilon^{-1})$ （即，噪声来自于标准差为  $2\epsilon^{-1}$  产生的拉普拉斯随机变量）。由于噪声的存在，无标签方无法根据掌握的模型相关参数重构真实的残差  $r_i$ ，从而达到保护隐私数据的目的。

另外一种加密方式是本地化差分隐私随机响应。其思想为通过随机扰动批（batch）的组成，使得交互的残差在形式上维度不变，但是实际的秩小于批中样本的个数，从而得到的残差不唯一。

具体来说，有标签方根据双方商定的 batch 大小，从有标签方样本选择一个子集  $C$ ，以标签的类别分布生成一个关于标签  $y \in \{0,1\}$  的随机响应向量

$m$ ，并将差分隐私处理得到  $m_r$  发送给无标签方。当无标签方根据特征  $x^b$  构建局部模型后，有标签方将随机响应得到的  $m_i=1$  残差给出真实的残差值  $r_i$ ，而对于不在批中的样本则置 0，在保证交互的残差维度仍然为批的大小 ( $|B|$ ) 下，所构造的残差矩阵经同态加密后发送给无标签方。发送的内容  $D$  的组成形式化表示为：

$$\langle r_i \rangle = \begin{cases} \langle \sigma(l_i) \rangle & i \in D \\ 0 & i \notin D \end{cases}$$

其中  $D \subset \{i: m_i=1\} \wedge |D|=|B|$ ， $\sigma(\bullet)$  为 sigmoid 函数， $\langle \bullet \rangle$  为同态加密。该方法称为差分隐私和同态加密混合的标签保护策略，且在满足如下条件下能实现  $\varepsilon$  差分隐私：

$$\frac{q \exp(\varepsilon)}{1 + \exp(\varepsilon)} + \frac{1-q}{1 + \exp(\varepsilon)} < 1, \quad 0 < q < \frac{1}{2}$$

$q$  为  $m$  中标注为 1 的比例。通过有标签方的上述操作，使得无标签方无法构造关于残差的线性方程组。

然而，上述方式虽然实现了标签保护，而且分类的精度损失相比第一种加密方式而言有所下降，但是由于差分隐私和随机置零的存在，没有充分利用批中的样本信息，因而相对于明文计算而言依然有性能损失，且分类精度损失的减小以增加训练成本为代价，暂不具备短期内投入生产使用的可能性。

为了至少部分地解决上述问题以及其他潜在问题中的一个或者多个，本公开提供了至少一种数据处理方案，有标签方通过残差分解的方式对标签这一隐私数据进行加密，无标签方基于加密得到的模型参数修正量进行模型参数重构，重构的模型精度较高。

需要说明的是，本公开实施例中的有标签方和无标签方均需要进行本地计算，并协作式交互修正信息，计算开销并没有显著增加。这里的有标签方对应的是数据发送方，无标签方对应的是数据接收方，残差分解是在有标签方进行，参数重构则在无标签方完成。

在实际应用中，这里的数据发送方指的是具有真实标签的发起方及其用于执行包括残差分解操作在内的处理设备，这里的数据接收方指的是具有模型输入特征，但不具备真实标签的响应方及其用于执行参数重构操作在内的处理设备。

5 为便于对本实施例进行理解，首先对本公开实施例所公开的一种数据处理方法进行详细介绍，本公开实施例所提供的数据处理方法的执行主体一般为具有一定计算能力的电子设备，该电子设备例如包括：终端设备或其它处理设备，终端设备可以为用户设备（User Equipment, UE）、移动设备、用户终端、蜂窝电话、个人数字助理（Personal Digital Assistant, PDA）、  
10 手持设备等。在一些可能的实现方式中，该数据处理方法可以通过处理器调用存储器中存储的计算机可读指令的方式来实现。

参见图 1 所示，为本公开实施例提供的数据处理方法的流程图，该方法主要是在数据发送方执行，具体包括步骤 S101~S103，其中：

S101：获取针对各个数据样本确定的标签残差值；每个标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；  
15

S102：基于各个标签残差值对各个数据样本进行残差分解，得到各个数据样本对应的模型参数修正量；

S103：向数据接收方发送模型参数修正量，以使得数据接收方根据模型参数修正量重构目标模型的模型参数信息。  
20

为了便于理解本公开实施例提供的数据处理方法，接下来首先对该方法的应用场景进行具体说明。本公开实施例中的数据处理方法主要可以应用于联邦学习领域，这里的联邦学习对应的可以是多方数据的融合学习方式，例如，可以是来源于金融结构的交易数据以及医疗机构的医疗诊断记录所形成的融合数据。  
25

在相关技术中，大多采用纵向逻辑回归方法来构建联合模型。而由于

纵向逻辑回归方法本身的特性约束，导致一方的隐私数据很可能被另一方反推得到。例如，金融机构内产生的有关一个用户是否为高净值用户的标签数据很可能随着模型参数信息的共享而泄漏到医疗机构，在这种情况下，将对用户隐私带来一定的不安全因素。

- 5        为了在更好的推进联邦学习的同时，提升隐私数据的保护力度，本公开实施例提供了一种协作式的数据处理方案，该方案主要对应两个阶段，一个是模型训练阶段，另一个是模型修正阶段。

针对模型训练阶段，主要是在有标签方执行残差分解的过程。分解后仅有一部分残差相关的混淆信息在同态加密保护下与无标签方交换，而另一部分残差保留信息由有标签方单独持有，不参与模型训练过程，使得无标签方即使按照相关标签泄露攻击方式（满足列满秩条件）解出残差，也会因为该残差与真实标签对应关系不再具备一一对应关系，使得其关于有标签方标签推测的精度与随机猜测二分类结果相当，无法根据已知标签泄露攻击方式获得的残差的符号反推有标签方的真实标签，从而确保了隐私数据的  
10        安全性。  
15        数据的真实性。

针对模型修正阶段，主要是在无标签方执行参数重构的过程。在有标签方模型训练收敛后，由有标签方发起，无标签方响应，仅需要有标签方和无标签方额外进行一轮次关于无标签方权重信息的交互即可完成无标签方每个特征权值的修正。由于有标签方提供的额外信息无法通过模型训练阶段获得，且该信息系真实标签与保护标签所实施的残差保留的整体，无标签方在重构出高精度的模型的前提下，也无法在模型修正阶段获得有标签方的标签信息，从而进一步确保了隐私数据的安全性。  
20        数据的真实性。

本公开实施例中的数据发送方，在获取到针对各个数据样本确定的标签残差值的情况下，可以基于各个标签残差值对各个数据样本进行残差分解，得到各个数据样本对应的模型参数修正量，最后向数据接收方发送模型参数修正量。这里的模型参数修正量即是有标签方向无标签方提供的额外信息，该额外信息是在对残差进行分解后确定的。  
25        数据的真实性。

有标签方根据无标签方对自身标签的拟合程度在本地随机执行残差分解，以达到随机化替换标签信息的效果，使得无标签方不能根据有标签方处理后的残差信息反推真实标签。

5 可知的是，本公开实施例中，通过扰动残差使得无标签方仅能构造带错误标签信息的模型，而所包含的错误信息系有标签方本地对残差信息作分解产生，无标签方对此无法区分；然后，有标签方传递必要的修正信息给无标签方，使得无标签方可以修正特征的权值，但不能获得有标签方的标签。

10 无标签方在有标签方的配合下修正存在偏差的特征权值，得到正确的模型参数信息。由于该信息由有标签方的标签及对标签的扰动信息组成，其中扰动信息与模型训练阶段无标签方已知的信息无关，使得无标签方无法获得有标签方的标签信息。

15 考虑到模型参数修正量的确定对于无标签方重构模型参数的关键作用，接下来可以重点说明有关确定模型参数修正量的过程，具体可以通过如下步骤来实现：

步骤一、按照数据大小的排列顺序将各个标签残差值进行排序，得到排序的各个标签残差值；

20 步骤二、在从各个数据样本中选取需要进行残差分解的目标数据样本的情况下，对目标数据样本所在排序的标签残差值进行变化，得到各个数据样本对应的残差变化信息；

步骤三、基于各个数据样本对应的残差变化信息以及各个数据样本的真实标签，确定各个数据样本对应的模型参数修正量。

这里，首先可以对各个标签残差值进行排序，并得到残差变化信息，而后基于残差变化信息以及真实标签确定模型参数修正量。

25 其中，上述残差变化信息用于指示标签残差值是否发生变化，对于变化的标签残差值可以进行第一标记，对于未变化的标签残差值可以进行第

二标记，从而可以达到随机替换真实标签的目的，又考虑到有关模型参数修正量是结合残差变化信息和真实标签得到的，也即，无标签方获得的并非直接的真实标签而是经过标签映射后的修正量，基于这一修正量以及对应的输入特征即可以构建出模型参数信息。

- 5       需要说明的是，有标签方在模型收敛后才需要将真实的标签和所作的标签映射在本地做运算合成后再发送给无标签方。

10       为了达到随机替换真实标签的目的，在进行残差变化之前，需要通过分组、选取等一系列操作选择出目标样本。具体地，首先可以按照预设分组数量将排序的各个标签残差值进行分组，得到分组后的标签残差值，而后从每个分组后的标签残差值中选取预设数量个目标标签残差值，最后将目标标签残差值对应的数据样本确定为目标数据样本。这里的分组可以是预设好的，例如，可以分为两组、四组等，在此不做具体的限制，目的在于使得无标签方无法根据特征之间的相似性获得关于有标签方标签信息的额外信息。与此同时，在从各分组中选取需要进行残差变化的数据样本的过程中，可以是随机定量的抽取，以确保标签替换的随机性，进一步提升数据的安全性。

20       本公开实施例中的残差变化信息可以指向的是残差变化向量，每个向量对应一个数据样本的残差变化情况。其中，在判断出一个数据样本非目标数据样本的情况下，可以确定数据样本对应第一残差变化值；在判断出一个数据样本是目标数据样本，且数据样本的标签残差值大于零的情况下，可以确定数据样本对应第二残差变化值；在判断出一个数据样本是目标数据样本，且数据样本的标签残差值小于零的情况下，确定数据样本对应第三残差变化值。而后，可以将各个数据样本分别对应的残差变化值进行集合，确定残差变化向量。

- 25       基于上述残差变化向量，可以确定模型参数修正量，具体通过如下步骤来实现：

步骤一、将残差变化向量以及残差变化向量的转置结果进行点乘运算，确定第一算子；以及，在确定各个数据样本的真实标签对应的标签值的情况下，确定与标签值对应的第二算子；

5 步骤二、基于第一算子和第二算子，确定各个数据样本对应的模型参数修正量。

这里可以基于第一算子和第二算子确定模型参数修正量。该模型参数修正量也可以是一个多维向量，每一个维度指向的是一个数据样本的修正量，继而实现针对目标模型的整体修正。

10 在确定残差变化信息的过程中，还可以基于各个数据样本对应的残差变化信息和排序的各个标签残差值之间的乘积运算，确定变化后的标签残差值，而后可以基于变化后的标签残差值确定向数据接收方发送的模型参数信息，并向数据接收方发送模型参数信息。

其中，上述有关变化后的标签残差值的计算过程可以是在模型收敛之前仅需要执行一次的步骤，例如，有标签方可以是在首轮执行上述步骤，15 改变随机选择样本的残差值，其效果相当于改变了样本真实标签，在确保了标签安全性的前提下，还降低了计算成本。

需要说明的是，这里的模型参数信息可以是训练中间过程，也即未达到模型收敛条件的情况下，有标签方向无标签方发送的，由于这里发生了残差变化，即使无标签方接收到了模型参数信息，也无法反推出真实标签。20 在完成模型训练，也即达到模型收敛条件的情况下，有标签方则可以向无标签方发送修正量以便于无标签方重构出准确的模型参数信息。

在实际应用中，有关模型收敛可以是与训练批次相关联的，在一个批次内的所有数据样本都完成一轮参数更新的情况下，可以判定模型是否满足收敛条件，若收敛则按照上述方式发送修正量，否则继续执行模型训练。

25 为了便于理解上述有关模型参数修正量的确定过程，可以结合如下实施例进一步进行说明。

首先，前提条件示例如下：

1) 建模需在两方之间完成，A 方承担数据应用方(Guest)的角色，B 方承担数据提供方(Host)和协作者(Arbiter)的角色。标签在 A 方(即有标签方)，特征在 B 方(即无标签方)；

5        2) A 方的标签为二分类(0/1)；

3) B 方仅已知 A 方的标签为二分类 0/1 形式，A 方标签的其他信息 B 方未知，但任一类别的标签均为 B 方感兴趣(即 B 方希望了解 A 方任何一个样本的标签信息)；

4) 双方约定按照纵向逻辑回归的基本步骤完成联合建模，B 方仅可对  
10    A 方发起半诚实攻击。

这里，有标签方和无标签方以某种安全方式约定双方联合建模均采用纵向逻辑回归，确定每轮建模的批  $B$  的大小  $|B|$  及组成、模型参数学习率  $\eta$ ，且通过安全求交确定对齐样本。其中 B 方已知对齐样本的特征  $\{(\mathbf{x}_i)\}$ ，A 方已知对齐样本的标签  $\{y_i\}$ 。每一轮由 B 方发起，A 方响应，以 B 方更新局  
15    部模型  $\mathbf{w}_b^{B(t)}$  的参数结束。同时 A 方和 B 方约定当模型收敛(flag=1)后，双方协作式完成 B 方真实权值  $\mathbf{W}$  的重构。

在模型训练阶段，当模型未达到收敛条件(此时 flag=0)时，执行以下步骤：

在一个批  $B$  中，B 方根据自有的模型参数  $\mathbf{w}_b^{B(t)}$  以及特征集合  $\{(\mathbf{x}_i^B)\}$  构造局  
20    部模型  $\{l_i^{B(t)}\}$  (计算方式为  $l_i^{B(t)} = \mathbf{x}_i^B \mathbf{w}_b^{B(t)}$ )，然后将  $\{l_i^{B(t)}\}$  以同态加密(例如 paillier 算法)发送给 A 方。

当模型达到收敛条件(此时 flag=0)时，此时双方已完成关于带错误标签的模型训练，并执行如下操作：

A 方将模型参数修正量  $\frac{\mathbf{y}+1}{2} \mathbf{S}^T (\mathbf{S}^T)^{-1}$  发送给 B 方，B 方按照如下方式  
25    重构真实的模型参数  $\mathbf{w}$ ：

$$\mathbf{w} = \frac{\mathbf{X}^T (\mathbf{X}\mathbf{X}^T)^{-1} + (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \left( \frac{\mathbf{y}+1}{2} \mathbf{S}\mathbf{S}^T (\mathbf{S}\mathbf{S}^T)^{-1} \right)}{2}$$

其中,  $\mathbf{X}$  对应的是数据特征向量,  $\mathbf{y}$  对应的是真实标签的值,  $\mathbf{S}$  是  $\mathbf{S}_B$  按批拼接得到的标签映射向量, 对应的是残差变化信息。

需要说明的是, 上述残差变化信息对应的可以是本批样本残差的保留信息  $\neg r_i^B$ , 且该保留信息可以是在训练的第一轮确定的。具体可以按照如下步骤来实现:

1) A 方根据残差  $r_i^{B(t)}$  排序 (从小到大或从大到小均可) 所有批内的样本。

2) A 方对本批样本的残差按如下方式作随机化残差分解。随机选择一个数  $m \in \{2, 4\}$  作为本批内由样本构成的组大小。

对于排序后的样本序列, 从第一个样本起, 每  $m$  个样本形成一个组  $G_i, i=1, 2, \dots, \lceil |B|/m \rceil$ , 其中符号  $\lceil |B|/m \rceil$  代表不小于  $|B|/m$  的最小整数。对于所形成的任意一个组  $G_j$ , 随机从组内选择  $\lceil |G_j|/2 \rceil$  个样本形成候选集  $C^B$ , 且  $C^B \triangleq f(B, m)$ , 且对于所有在  $C^B$  内的样本, 按照以下方式确定对应的保留信息  $\neg r_i^B$ 。

其中, 若  $r_i^{B(t)} > 0$ , 则  $\neg r_i^B = 1$ ; 若  $r_i^{B(t)} < 0$ , 则  $\neg r_i^B = -1$ , 不管是 1 还是 -1, 后续均将会执行残差变化。对于所有不在  $C^B$  内的样本  $x_i$ , 有  $\neg r_i^B = 0$ , 后续不会执行残差变化。具体可以按照如下公式来确定:

$$\neg r_i^B = \begin{cases} 1 & \text{sort}(i) \in C^{B(t)} \wedge r_i^{B(t)} > 0 \\ 0 & \text{sort}(i) \notin C^{B(t)} \\ -1 & \text{sort}(i) \in C^{B(t)} \wedge r_i^{B(t)} < 0 \end{cases}$$

其中  $\text{sort}(i)$  为按照残差  $\Delta r_i^B$  排序得到的第  $i$  个样本在批中的顺序。这里, 为了防止 B 方反推, 可以按照 B 方针对数据样本的原始顺序进行重排。

为了便于进一步说明有关重排操作所对应的残差分解, 可以结合图 2 所示的残差分解示意图进一步进行说明。

如图 2 所示, 批大小  $|B|=8$ , 按残差值由小到大顺序排列后, 第二列和

第四列的粗体分别为  $\neg r_i^{B(t)}$  在  $m=2$  和  $m=4$  下按组随机选择的样本非零表示，相应的随机化残差分解可见第三列和第五列的 1/-1 部分。

这里，基于标签保留信息  $\neg r_i^{B(t)}$  可以确定残差变化向量  $\mathbf{S}^B$ 。 $\mathbf{S}^B$  中的每个元素体现样本在首轮残差分解时残差信息是否发生变化。当残差发生变化时， $S_i^B = -1$ ；否则  $S_i^B = 1$ 。即：

$$S_i^B = \begin{cases} -1 & \neg r_i^B \neq 0 \\ 1 & \neg r_i^B = 0 \end{cases}$$

在确定残差变化向量  $\mathbf{S}^B$  的情况下，可以将残差变化向量以及残差变化向量的转置结果进行点乘运算，确定第一算子  $\mathbf{SS}^\top$ ；以及，在确定各个数据样本的真实标签对应的标签值的情况下，确定与标签值对应的第二算子  $\frac{\mathbf{y}+1}{2}$ ，而后确定模型参数修正量  $\left(\frac{\mathbf{y}+1}{2} \mathbf{SS}^\top (\mathbf{SS}^\top)^{-1}\right)$ 。

需要说明的是，上述模型参数修正量可以是在结束模型训练之后 A 方向 B 方发送的，在模型训练过程中，A 方发送给 B 方的伪残差可以按下式计算：

$$\tilde{r}_i^{B(t)} = r_i^{B(t)} - \neg r_i^B$$

这样，B 方在密态下更新本方的模型参数  $\mathbf{w}_b^{B(t)}$ ，计算方式为：

$$\mathbf{w}_b^{B(t)} = \mathbf{w}_b^{B(t)} - \eta \tilde{\mathbf{g}}_b^{B(t)}$$

其中， $\tilde{\mathbf{g}}_b^{B(t)}$  为 B 方根据身份信息求解得的关于参数  $\mathbf{w}_b^B$  的梯度信息，该信息等价于 A 方按照特征及对应的伪残差在每个样本上乘积得到的伪梯度信息  $\{x_i \tilde{r}_i^{B(t)}\}$ 。

对每一个批  $B$  重复以上步骤，直至所有样本都完成一轮参数更新，然后判定模型是否满足收敛条件，若收敛则置  $\text{flag}=1$ ，否则继续。主要操作的时序图如图 3 所示。

可知的是，本公开实施例在有标签方进行了一次残差分解（仅联合建模的第一轮）和一次模型参数重构信息发送这两个步骤，同时，在无标签方需进行一次权值构造，具体可以参照图 4 进行说明。

如图 4 所示，在完成批初始化之后，无标签方可以基于有标签方给予的模型参数建立局部模型，而后由有标签方判断是否处于首轮训练，若是，有标签方可以按照上述步骤构造保留残差以及标签变换，无标签方则可以基于伪残差进行更新。而后，在确定达到模型收敛的情况下，有标签方可以发送额外信息给无标签方以便无标签方重构权值。

需要说明的是，本公开实施例不限制批初始化和达到收敛条件两个模块的具体实现方式，批初始化前的双方样本对齐亦不限定实现方式。本公开实施例的重点在于有标签方实施针对无标签方的残差分解和与无标签方协作式实现权值重构，其他在模型训练阶段的步骤计算可以采用经典的梯度下降法求解。

此外，有关数据安全性可以从模型训练和模型修正两部分分析。模型训练过程中，残差保留信息由有标签方单独持有，不参与模型训练过程。无标签方无法根据已知的信息判定有标签方对特定的示例标签是否修改。

对有标签方而言，这种安全是信息论级别，其效果使得无标签方无法通过增加算力获得本方的标签，且仅需执行一轮本地操作，额外计算开销相对于整个联合建模开销而言可以忽略不计。因此无标签方无法依据半诚实攻击获取有标签方的真实标签  $\mathbf{y}$ 。

而权值重构部分，理论依据为等式  $\mathbf{XWS} = \mathbf{YS}$ 。由于真实标签及其变换信息整体  $\left(\frac{\mathbf{y}+1}{2}\mathbf{SS}^T(\mathbf{SS}^T)^{-1}\right)$  发送给无标签方，该过程不涉及梯度信息交互，与已知标签泄露方式无关。这使得无标签方也无法计算有标签方对标签所作的标签映射  $\mathbf{S}$  以及实际标签  $\mathbf{Y}$ 。因此，若攻击者沿用已知的标签泄露攻击方式，则自始至终无法消除残差与标签之间的随机对应性。换言之，不论无标签方获得的结果为正的残差值还是负的残差值，其对应的真实标签可能为正类（1）也可能为负类（0）。

再者，有关模型可用性可从权值重构的角度分析。鉴于问题的背景可以限定为二分类，因此若在首轮有标签方改变了随机选择样本的残差值，

其效果相当于改变了样本真实标签，从正类（负类）变化为负类（正类）。其中排序的意义在于对抗无标签方因随机初始化参数的差异泄露更多有标签方标签信息。因而在真实标签  $\mathbf{Y}$  上施加  $\mathbf{S}$  或  $\{\neg r_i^B\}$  没有明显的信息差异，而且最终得到的结果在有标签方发送前并未对信息作包括差分隐私在内的混淆化处理，理论上权值对样本类别的区分能力可以达到更佳效果。

参见图 5 所示，为本公开实施例提供的数据处理方法的流程图，该方法主要是在数据接收方执行，具体包括步骤 S501~S502，其中：

S501：接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解确定的；每个标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

S502：根据模型参数修正量重构目标模型的模型参数信息。

这里，基于接收的模型参数修正量可以实现有关目标模型的参数重构，由于这里的模型参数修正量是基于数据发送方的真实标签以及对应的残差变化信息确定的，因而可以标记对应的标签替换情况，且基于修正量无法解析出真实标签，因而可以在对数据发送方的真实标签进行保护的前提下，实现模型参数的准确重构。

其中，有关模型参数修正量的确定过程可以参照上述实施例的相关描述，在此不做赘述。

在重构模型参数信息的过程中，除了需要依赖于上述模型参数修正量，还需要考虑针对目标模型输入的数据特征信息，具体可以通过如下步骤来实现：

步骤一、将数据特征向量以及数据特征向量的转置结果进行点乘运算，确定第三算子；以及，将数据特征向量的转置结果以及数据特征向量进行点乘运算，确定第四算子；

步骤二、基于第三算子、第四算子以及模型参数修正量，确定目标模

型的模型参数信息。

本公开实施例中有关模型参数信息的确定过程可以参照上述模型参数  $w$  的公式：

$$w = \frac{\mathbf{x}^T (\mathbf{X}\mathbf{X}^T)^{-1} + (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{x}^T \left( \frac{y+1}{2} \mathbf{S}\mathbf{S}^T (\mathbf{S}\mathbf{S}^T)^{-1} \right)}{2}$$

5 这里的  $\mathbf{x}\mathbf{x}^T$  对应的是第三算子， $\mathbf{x}^T \mathbf{x}$  对应的是第四算子， $\left( \frac{y+1}{2} \mathbf{S}\mathbf{S}^T (\mathbf{S}\mathbf{S}^T)^{-1} \right)$  对应的是修正量，继而可以确定出模型参数。

在本说明书的描述中，参考术语“一些可能的实施方式”、“一些实施方式”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施方式或示例描述的具体特征、结构、材料或者特点包含于本公开的至少一个  
10 实施方式或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施方式或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施方式或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施方式或示例以及不同实施方式或示例的特征进行结合和组合。

15 关于本公开实施方式的方法流程图，将某些操作描述为以一定顺序执行的不同的步骤。这样的流程图属于说明性的而非限制性的。可以将在本文章中所描述的某些步骤分组在一起并且在单个操作中执行、可以将某些步骤分割成多个子步骤、并且可以以不同于在本文中所示出的顺序来执行某些步骤。可以由任何电路结构和/或有形机制(例如，由在计算机设备上运行的  
20 的软件、硬件(例如，处理器或芯片实现的逻辑功能)等、和/或其任何组合)以任何方式来实现现在流程图中所示出的各个步骤。

本领域技术人员可以理解，在具体实施方式的上述方法中，各步骤的撰写顺序并不意味着严格的执行顺序而对实施过程构成任何限定，各步骤的具体执行顺序应当以其功能和可能的内在逻辑确定。

25 基于同一发明构思，本公开实施例中还提供了与数据处理方法对应的

数据处理装置，由于本公开实施例中的装置解决问题的原理与本公开实施例上述数据处理方法相似，因此装置的实施可以参见方法的实施，重复之处不再赘述。

参照图 6 所示，为本公开实施例提供的一种数据处理装置的示意图，  
5 装置包括：获取模块 601、分解模块 602、发送模块 603；其中，

获取模块 601，用于获取针对各个数据样本确定的标签残差值；每个标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

10 分解模块 602，用于基于各个标签残差值对各个数据样本进行残差分解，得到各个数据样本对应的模型参数修正量；

发送模块 603，用于向数据接收方发送模型参数修正量，以使得数据接收方根据模型参数修正量重构目标模型的模型参数信息。

采用上述数据处理装置，在获取到针对各个数据样本确定的标签残差值的情况下，可以基于各个标签残差值对各个数据样本进行残差分解，而  
15 后可以将残差分解得到的各个数据样本对应的模型参数修正量发送给数据接收方，数据接收方则可以根据模型参数修正量重构模型参数信息。本公开中，数据发送方（即有标签方）在进行残差分解的过程中，可以有效地对残差进行扰动，使得数据接收方（即无标签方）仅能构造带错误标签信息的模型，这使得数据发送方能够保护其拥有的真实标签，与此同时，有  
20 标签方可以传递必要的修正信息（即模型参数修正量）给无标签方，使得无标签方可以按照修正信息重构精准的模型参数信息，进一步确保了模型的训练性能。

在一种可能的实施方式中，分解模块 602，用于按照如下步骤基于各个标签残差值对各个数据样本进行残差分解，得到各个数据样本对应的模型  
25 参数修正量，包括

将各个标签残差值进行排序，得到排序的各个标签残差值；

在从各个数据样本中选取需要进行残差分解的目标数据样本的情况下，对目标数据样本所在排序的标签残差值进行变化，得到各个数据样本对应的残差变化信息；

5 基于各个数据样本对应的残差变化信息以及各个数据样本的真实标签，确定各个数据样本对应的模型参数修正量。

在一种可能的实施方式中，分解模块 602，用于按照如下步骤从各个数据样本中选取需要进行残差分解的目标数据样本：

按照预设分组数量将排序的各个标签残差值进行分组，得到分组后的标签残差值；

10 从每个分组后的标签残差值中选取预设数量个目标标签残差值；

将目标标签残差值对应的数据样本确定为目标数据样本。

在一种可能的实施方式中，在各个数据样本对应的残差变化信息对应残差变化向量的情况下，分解模块 602，用于按照如下步骤对目标数据样本所在排序的标签残差值进行变化，得到各个数据样本对应的残差变化信息：

15 针对每个数据样本，在判断出数据样本非目标数据样本的情况下，确定数据样本对应第一残差变化值；或者，

在判断出数据样本是目标数据样本，且数据样本的标签残差值大于零的情况下，确定数据样本对应第二残差变化值；或者，

20 在判断出数据样本是目标数据样本，且数据样本的标签残差值小于零的情况下，确定数据样本对应第三残差变化值；

将各个数据样本分别对应的残差变化值进行集合，确定残差变化向量；其中，残差变化向量用于表征各个数据样本的标签残差值是否发生变化。

在一种可能的实施方式中，分解模块 602，用于按照如下步骤基于各个数据样本对应的残差变化信息以及各个数据样本的真实标签，确定各个数据样本对应的模型参数修正量：

25

将残差变化向量以及残差变化向量的转置结果进行点乘运算，确定第一算子；以及，在确定各个数据样本的真实标签对应的标签值的情况下，确定与标签值对应的第二算子；

基于第一算子和第二算子，确定各个数据样本对应的模型参数修正量。

5 在一种可能的实施方式中，发送模块 603，还用于：

在得到各个数据样本对应的残差变化信息之后，基于各个数据样本对应的残差变化信息和排序的各个标签残差值之间的乘积运算，确定变化后的标签残差值；

基于变化后的标签残差值确定向数据接收方发送的模型参数信息；

10 向数据接收方发送模型参数信息。

在一种可能的实施方式中，发送模块 603，用于按照如下步骤向数据接收方发送模型参数信息：

在未达到模型收敛条件的情况下，向数据接收方发送模型参数信息；

发送模块 603，用于按照如下步骤向数据接收方发送模型参数修正量：

15 在达到模型收敛条件的情况下，向数据接收方发送模型参数修正量。

参照图 7 所示，为本公开实施例提供的另一种数据处理装置的示意图，装置包括：接收模块 701、重构模块 702；其中，

接收模块 701，用于接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解确定的；每个标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

20

重构模块 702，用于根据模型参数修正量重构目标模型的模型参数信息。

在一种可能的实施方式中，重构模块 702，用于按照如下步骤根据模型

参数修正量重构目标模型的模型参数信息：

获取针对目标模型输入的数据特征信息；

基于数据特征信息和模型参数修正量，确定目标模型的模型参数信息。

5 在一种可能的实施方式中，在数据特征信息包括数据特征向量的情况下，重构模块 702，用于按照如下步骤基于数据特征信息和模型参数修正量，确定目标模型的模型参数信息：

将数据特征向量以及数据特征向量的转置结果进行点乘运算，确定第三算子；以及，将数据特征向量的转置结果以及数据特征向量进行点乘运算，确定第四算子；

10 基于第三算子、第四算子以及模型参数修正量，确定目标模型的模型参数信息。

需要说明的是，本申请实施方式中的装置可以实现前述方法的实施方式的各个过程，并达到相同的效果和功能，这里不再赘述。

本公开实施例还提供了一种电子设备，如图 8 所示，为本公开实施例  
15 提供的电子设备结构示意图，包括：处理器 801、存储器 802、和总线 803。存储器 802 存储有处理器 801 可执行的机器可读指令（比如，图 6 中的装置中获取模块 601、分解模块 602、发送模块 603 对应的执行指令等；再如图 7 中的装置中接收模块 701、重构模块 702 对应的执行指令等），当电子设备运行时，处理器 801 与存储器 802 之间通过总线 803 通信，机器可读  
20 指令被处理器 801 执行时执行如图 1 或者如图 5 所示的数据处理方法的步骤。

本公开实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行上述方法实施例中所述的数据处理方法的步骤。其中，该存储介质可以是易失性或非易  
25 失的计算机可读取存储介质。

本公开实施例还提供一种计算机程序产品，该计算机程序产品承载有程序代码，所述程序代码包括的指令可用于执行上述方法实施例中所述的数据处理方法的步骤，具体可参见上述方法实施例，在此不再赘述。

其中，上述计算机程序产品可以具体通过硬件、软件或其结合的方式实现。在一个可选实施例中，所述计算机程序产品具体体现为计算机存储介质，在另一个可选实施例中，计算机程序产品具体体现为软件产品，例如软件开发包（Software Development Kit，SDK）等等。

本申请中的各个实施方式均采用递进的方式描述，各个实施方式之间相同相似的部分互相参见即可，每个实施方式重点说明的都是与其他实施方式的不同之处。尤其，对于装置、设备和计算机可读存储介质实施方式而言，由于其基本相似于方法实施方式，所以其描述进行了简化，相关之处可参见方法实施方式的部分说明即可。

本申请实施方式提供的装置、设备和计算机可读存储介质与方法是一一对应的，因此，装置、设备和计算机可读存储介质也具有与其对应的方法类似的有益技术效果，由于上面已经对方法的有益技术效果进行了详细说明，因此，这里不再赘述装置、设备和计算机可读存储介质的有益技术效果。

本领域内的技术人员应明白，本公开的实施方式可提供为方法、装置（设备或系统）、或计算机可读存储介质。因此，本公开可采用完全硬件实施方式、完全软件实施方式、或结合软件和硬件方面的实施方式的形式。而且，本公开可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机可读存储介质的形式。

本公开是参照根据本公开实施方式的方法、装置（设备或系统）、和计算机可读存储介质的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和

/ 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁

盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。此外，尽管在附图中以特定顺序描述了本公开方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。

- 5 附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个步骤执行。

虽然已经参考若干具体实施方式描述了本公开的精神和原理，但是应该理解，本公开并不限于所公开的具体实施方式，对各方面的划分也不意味着这些方面中的特征不能组合以进行受益，这种划分仅是为了表述的方便。本公开旨在涵盖所附权利要求的精神和范围内所包括的各种修改和等  
10 同布置。

## 权 利 要 求 书

1、一种数据处理方法，包括：

获取针对各个数据样本确定的标签残差值；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

5       基于各个所述标签残差值对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量；

向数据接收方发送所述模型参数修正量，以使得所述数据接收方根据所述模型参数修正量重构所述目标模型的模型参数信息。

2、根据权利要求1所述的方法，其中，所述基于各个所述标签残差值  
10       对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量，包括：

按照数据大小的排列顺序将各个所述标签残差值进行排序，得到排序的各个标签残差值；

在从所述各个数据样本中选取需要进行残差分解的目标数据样本的  
15       情况下，对所述目标数据样本所在排序的标签残差值进行变化，得到所述各个数据样本对应的残差变化信息；

基于所述各个数据样本对应的残差变化信息以及所述各个数据样本的真实标签，确定所述各个数据样本对应的模型参数修正量。

3、根据权利要求2所述的方法，其中，按照如下步骤从所述各个数据  
20       样本中选取需要进行残差分解的目标数据样本：

按照预设分组数量将所述排序的各个标签残差值进行分组，得到分组后的标签残差值；

从每个分组后的标签残差值中选取预设数量个目标标签残差值；

将所述目标标签残差值对应的数据样本确定为所述目标数据样本。

4、根据权利要求 2 或 3 所述的方法，其中，在所述各个数据样本对应的残差变化信息对应残差变化向量的情况下，所述对所述目标数据样本所在排序的标签残差值进行变化，得到所述各个数据样本对应的残差变化信息，包括：

5 针对每个所述数据样本，在判断出所述数据样本非所述目标数据样本的情况下，确定所述数据样本对应第一残差变化值；或者，

在判断出所述数据样本是所述目标数据样本，且所述数据样本的标签残差值大于零的情况下，确定所述数据样本对应第二残差变化值；或者，

10 在判断出所述数据样本是所述目标数据样本，且所述数据样本的标签残差值小于零的情况下，确定所述数据样本对应第三残差变化值；

将各个所述数据样本分别对应的残差变化值进行集合，确定所述残差变化向量；其中，所述残差变化向量用于表征所述各个数据样本的标签残差值是否发生变化。

15 5、根据权利要求 4 所述的方法，其中，所述基于所述各个数据样本对应的残差变化信息以及所述各个数据样本的真实标签，确定所述各个数据样本对应的模型参数修正量，包括：

将所述残差变化向量以及所述残差变化向量的转置结果进行点乘运算，确定第一算子；以及，在确定所述各个数据样本的真实标签对应的标签值的情况下，确定与所述标签值对应的第二算子；

20 基于所述第一算子和所述第二算子，确定所述各个数据样本对应的模型参数修正量。

6、根据权利要求 2 至 5 任一项所述的方法，其中，在得到所述各个数据样本对应的残差变化信息之后，所述方法还包括：

25 基于所述各个数据样本对应的残差变化信息和所述排序的各个标签残差值之间的乘积运算，确定变化后的标签残差值；

基于所述变化后的标签残差值确定向所述数据接收方发送的模型参数信息；

向所述数据接收方发送所述模型参数信息。

7、根据权利要求 6 所述的方法，其中，所述向所述数据接收方发送所述模型参数信息，包括：

在未达到模型收敛条件的情况下，向所述数据接收方发送所述模型参数信息；

所述向数据接收方发送所述模型参数修正量，包括：

在达到模型收敛条件的情况下，向所述数据接收方发送所述模型参数修正量。

8、一种数据处理方法，包括：

接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，所述模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解确定的；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

根据所述模型参数修正量重构所述目标模型的模型参数信息。

9、根据权利要求 8 所述的方法，其中，所述根据所述模型参数修正量重构所述目标模型的模型参数信息，包括：

获取针对目标模型输入的数据特征信息；

基于所述数据特征信息和所述模型参数修正量，确定所述目标模型的模型参数信息。

10、根据权利要求 9 所述的方法，其中，在所述数据特征信息包括数据特征向量的情况下，所述基于所述数据特征信息和所述模型参数修正量，确定所述目标模型的模型参数信息，包括：

将所述数据特征向量以及所述数据特征向量的转置结果进行点乘运算，确定第三算子；以及，将所述数据特征向量的转置结果以及所述数据特征向量进行点乘运算，确定第四算子；

5 基于所述第三算子、所述第四算子以及所述模型参数修正量，确定所述目标模型的模型参数信息。

11、一种数据处理装置，包括：

获取模块，用于获取针对各个数据样本确定的标签残差值；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

10 分解模块，用于基于各个所述标签残差值对所述各个数据样本进行残差分解，得到所述各个数据样本对应的模型参数修正量；

发送模块，用于向数据接收方发送所述模型参数修正量，以使得所述数据接收方根据所述模型参数修正量重构所述目标模型的模型参数信息。

12、一种数据处理装置，包括：

15 接收模块，用于接收数据发送方发送的各个数据样本对应的模型参数修正量；其中，所述模型参数修正量是基于各个数据样本确定的标签残差值进行残差分解确定的；每个所述标签残差值用于表征对应的数据样本的真实标签与目标模型所预测标签之间的偏差程度；

20 重构模块，用于根据所述模型参数修正量重构所述目标模型的模型参数信息。

13、一种电子设备，包括：处理器、存储器和总线，所述存储器存储有所述处理器可执行的机器可读指令，当电子设备运行时，所述处理器与所述存储器之间通过总线通信，所述机器可读指令被所述处理器执行时执行如权利要求 1 至 10 任一项所述的数据处理方法。

25 14、一种计算机可读存储介质，该计算机可读存储介质上存储有计算

机程序，该计算机程序被处理器运行时执行如权利要求 1 至 10 任一项所述的数据处理方法。

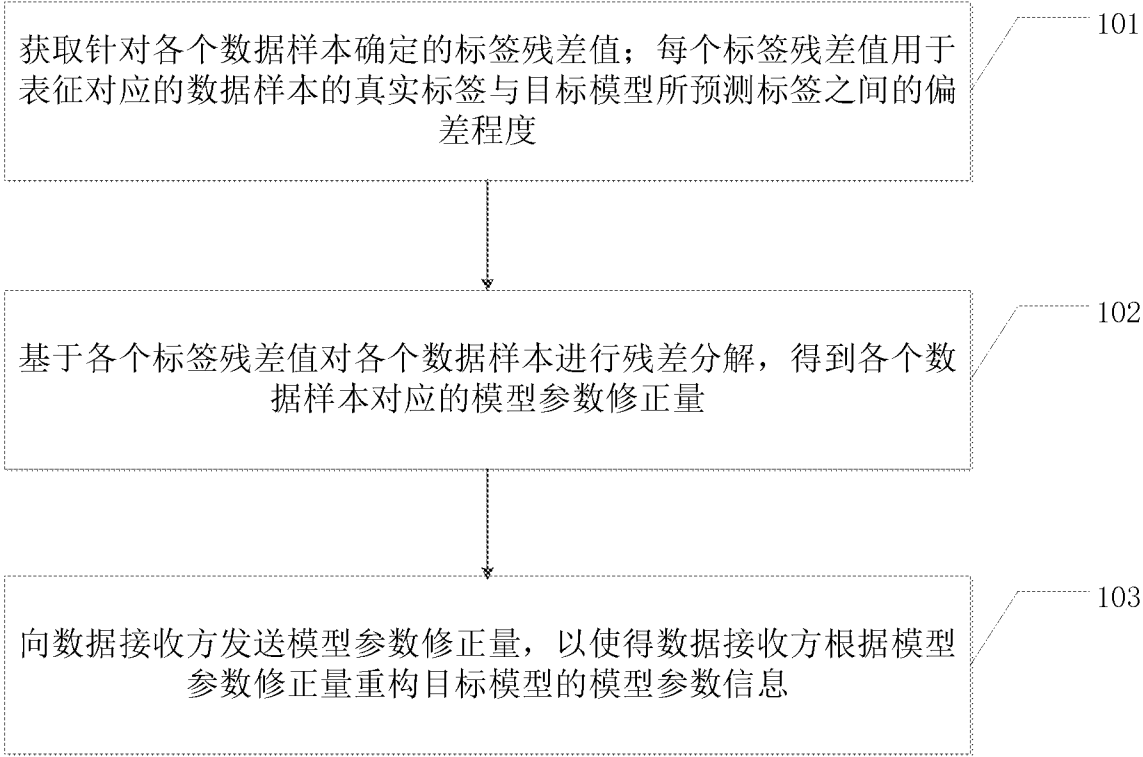


图 1

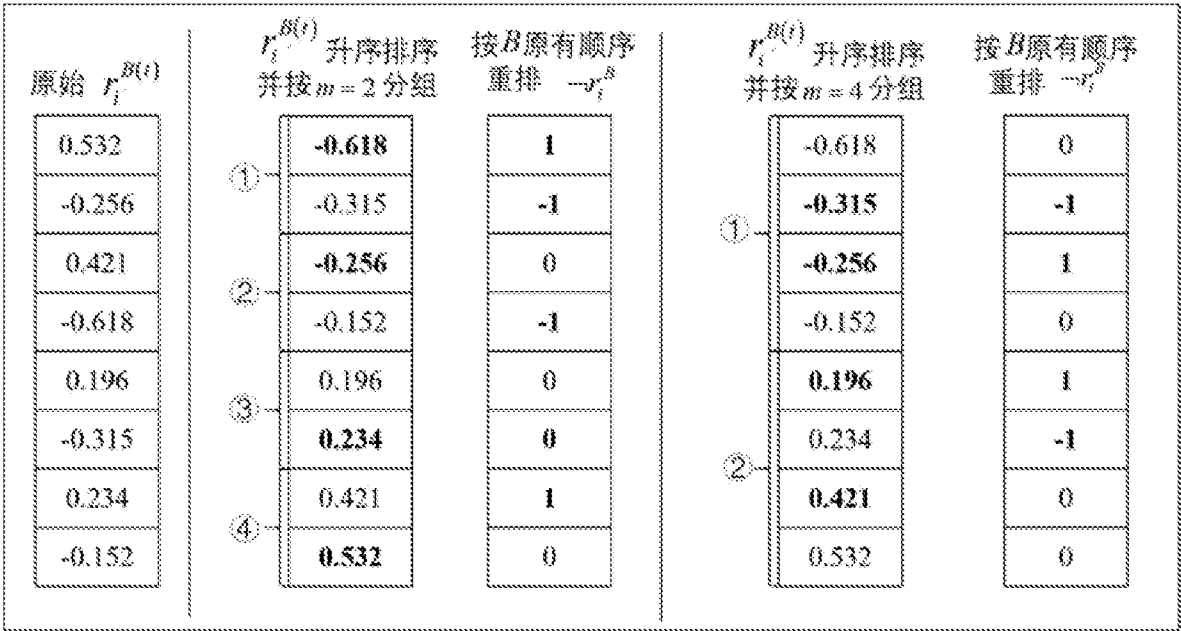


图 2

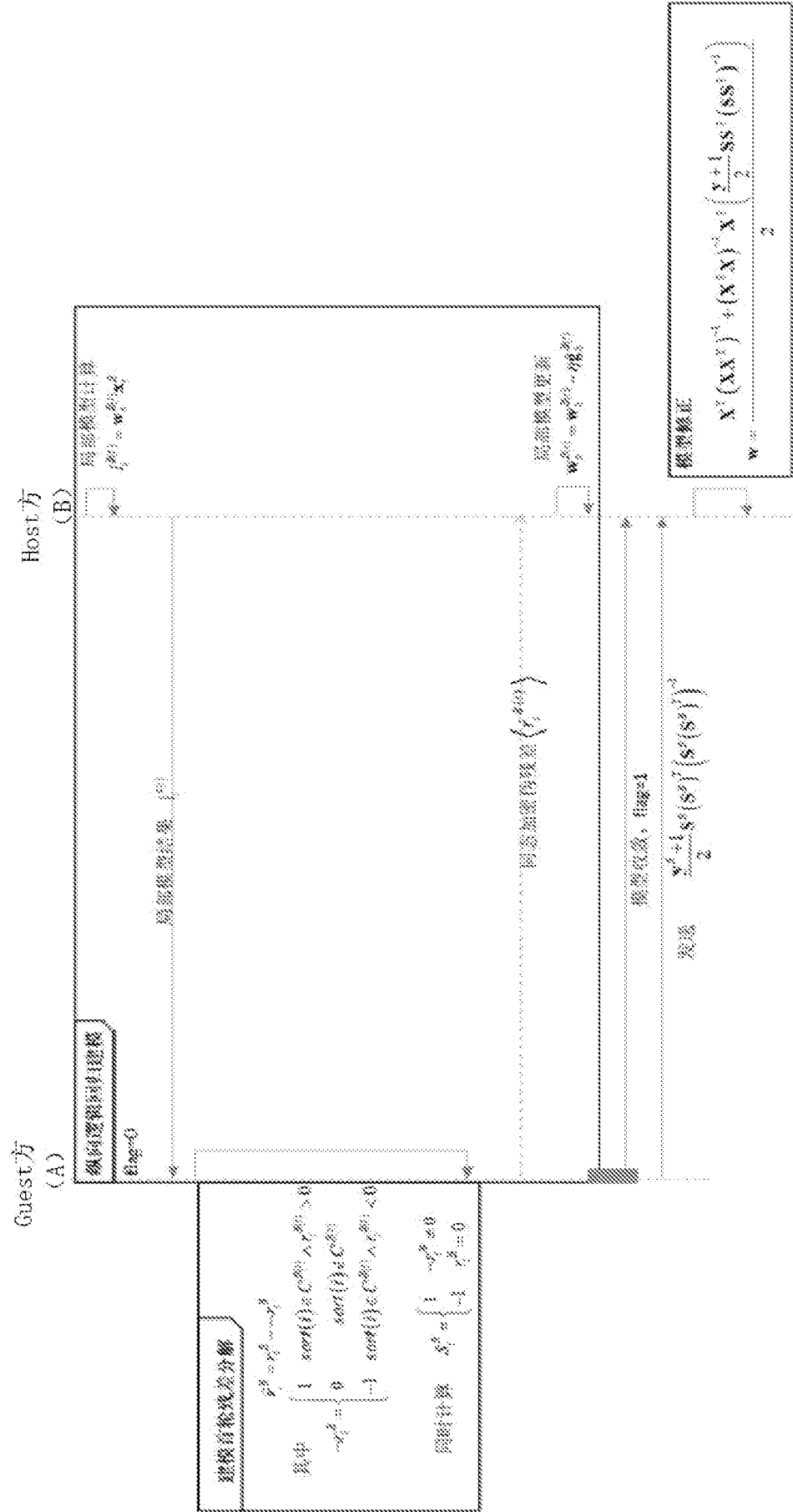


图3

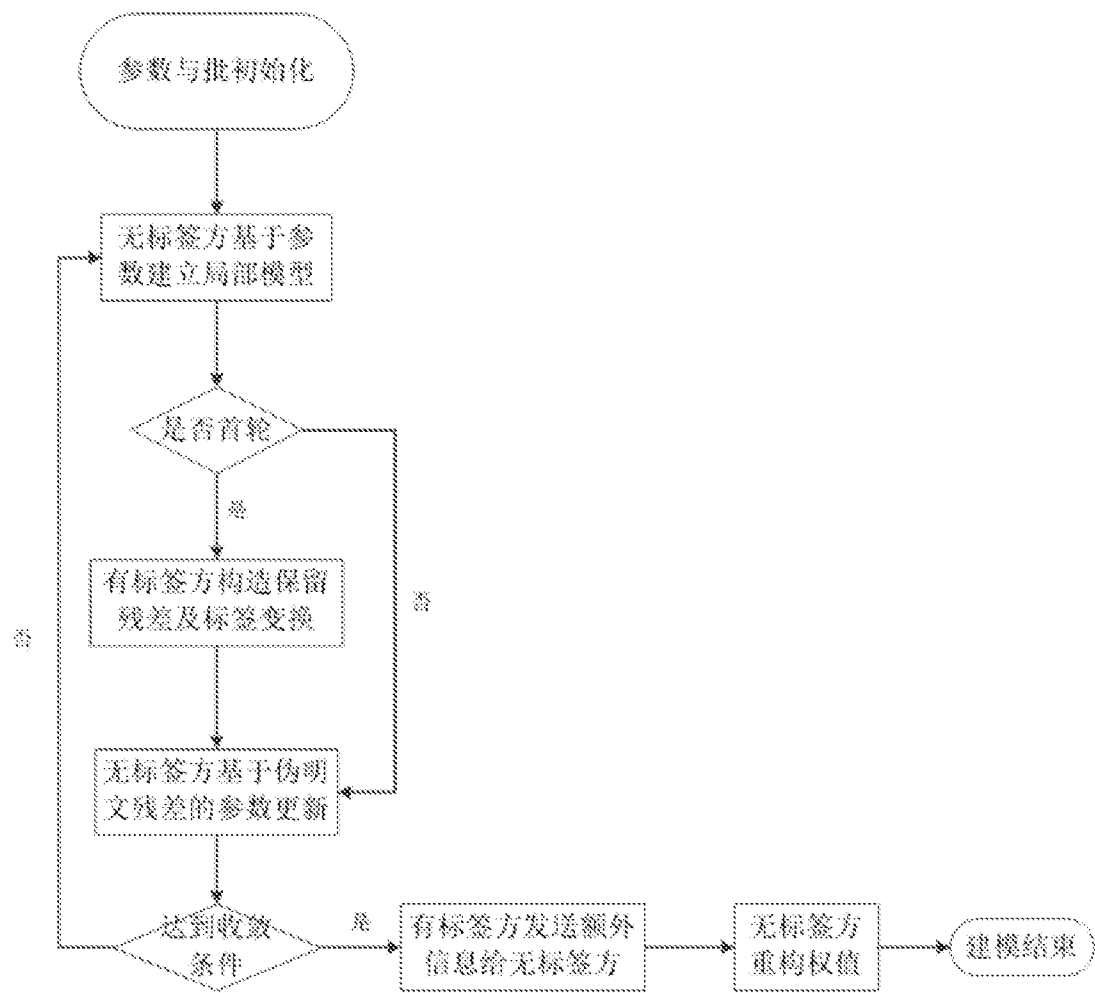


图 4

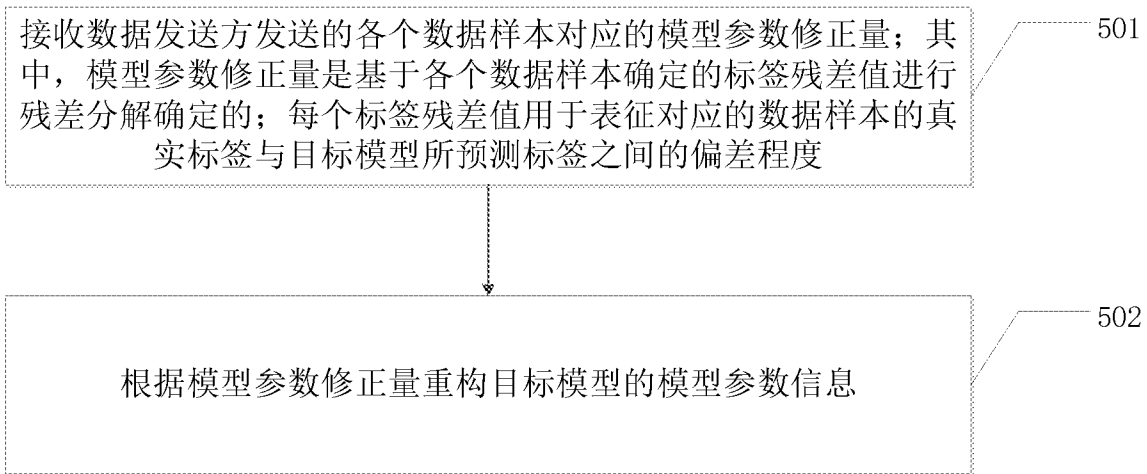


图 5

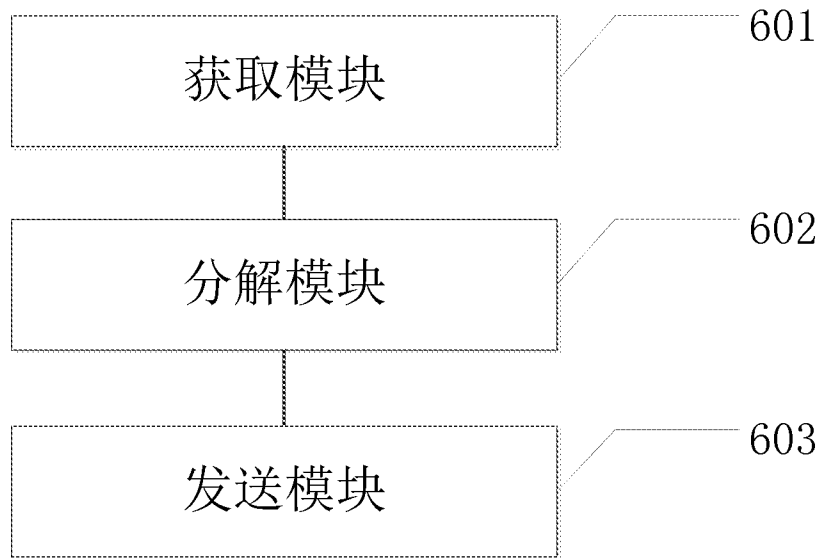


图 6

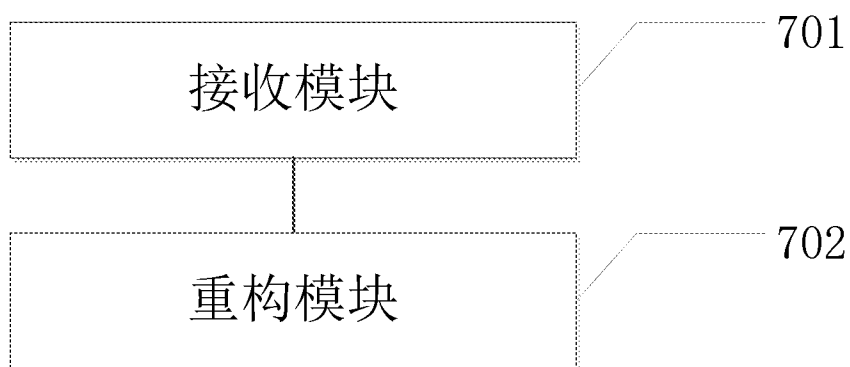


图 7

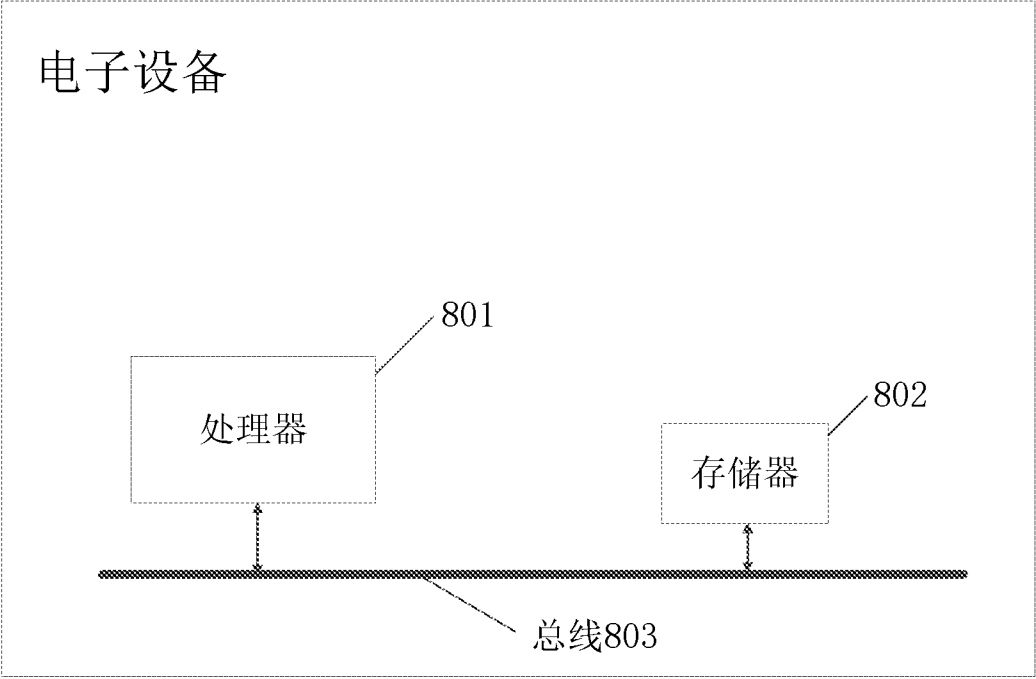


图 8

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/071564

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F21/62(2013.01)i;G06N20/00(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)

IPC:G06F,G06N

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)

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 联邦, 模型, 标签, 残差, 偏差, 误差, 预测, 分解, 参数, 修正, 变化, 变换, 排序, 分组, 向量, 算子, federal, model, label, residual, bias, error, prediction, decomposition, parameter, revision, variation, transformation, sorting, grouping, vector, operator

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                | Relevant to claim No. |
|-----------|-------------------------------------------------------------------------------------------------------------------|-----------------------|
| PX        | CN 115422574 A (CHINA UNIONPAY CO., LTD.) 02 December 2022 (2022-12-02)<br>claims 1-14                            | 1-14                  |
| X         | CN 112347476 A (FACEMON CO., LTD.) 09 February 2021 (2021-02-09)<br>claims 1-8                                    | 1, 8-14               |
| A         | CN 111435452 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 21 July 2020 (2020-07-21)<br>entire document | 1-14                  |
| A         | CN 114611128 A (BEIJING BYTEDANCE NETWORK TECHNOLOGY CO., LTD.) 10 June 2022 (2022-06-10)<br>entire document      | 1-14                  |
| A         | CN 114723068 A (JDT TECHNOLOGY HOLDING CO., LTD.) 08 July 2022 (2022-07-08)<br>entire document                    | 1-14                  |
| A         | US 2020143080 A1 (ADVANCED NEW TECHNOLOGIES CO., LTD.) 07 May 2020 (2020-05-07)<br>entire document                | 1-14                  |



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

“D” document cited by the applicant in the international application

“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

13 April 2023

Date of mailing of the international search report

18 April 2023

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2023/071564**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |             |    | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|-------------|----|--------------------------------------|
| CN                                        | 115422574  | A  | 02 December 2022                     | None                    |             |    |                                      |
| CN                                        | 112347476  | A  | 09 February 2021                     | WO                      | 2022103330  | A1 | 19 May 2022                          |
| CN                                        | 111435452  | A  | 21 July 2020                         | None                    |             |    |                                      |
| CN                                        | 114611128  | A  | 10 June 2022                         | None                    |             |    |                                      |
| CN                                        | 114723068  | A  | 08 July 2022                         | None                    |             |    |                                      |
| US                                        | 2020143080 | A1 | 07 May 2020                          | SG                      | 11201912390 | YA | 30 January 2020                      |
|                                           |            |    |                                      | EP                      | 3644231     | A1 | 29 April 2020                        |
|                                           |            |    |                                      | TW                      | 201907318   | A  | 16 February 2019                     |
|                                           |            |    |                                      | WO                      | 2019007417  | A1 | 10 January 2019                      |
|                                           |            |    |                                      | CN                      | 109214404   | A  | 15 January 2019                      |
|                                           |            |    |                                      | HK                      | 40003201    | A0 | 09 April 2020                        |

## 国际检索报告

国际申请号

PCT/CN2023/071564

## A. 主题的分类

G06F21/62 (2013.01) i; G06N20/00 (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)

IPC: G06F, G06N

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))

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 联邦, 模型, 标签, 残差, 偏差, 误差, 预测, 分解, 参数, 修正, 变化, 变换, 排序, 分组, 向量, 算子, federal, model, label, residual, bias, error, prediction, decomposition, parameter, revision, variation, transformation, sorting, grouping, vector, operator

## C. 相关文件

| 类 型* | 引用文件, 必要时, 指明相关段落                                                                       | 相关的权利要求 |
|------|-----------------------------------------------------------------------------------------|---------|
| PX   | CN 115422574 A (中国银联股份有限公司) 2022年12月2日 (2022 - 12 - 02)<br>权利要求1-14                     | 1-14    |
| X    | CN 112347476 A (脸萌有限公司) 2021年2月9日 (2021 - 02 - 09)<br>权利要求1-8                           | 1, 8-14 |
| A    | CN 111435452 A (百度在线网络技术 (北京) 有限公司 ) 2020年7月21日 (2020 - 07 - 21)<br>全文                  | 1-14    |
| A    | CN 114611128 A (北京字节跳动网络技术有限公司) 2022年6月10日 (2022 - 06 - 10)<br>全文                       | 1-14    |
| A    | CN 114723068 A (京东科技控股股份有限公司) 2022年7月8日 (2022 - 07 - 08)<br>全文                          | 1-14    |
| A    | US 2020143080 A1 (ADVANCED NEW TECHNOLOGIES CO., LTD.) 2020年5月7日 (2020 - 05 - 07)<br>全文 | 1-14    |

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

\* 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

“D” 申请人在国际申请中引证的文件

“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

“&amp;” 同族专利的文件

国际检索实际完成的日期

2023年4月13日

国际检索报告邮寄日期

2023年4月18日

ISA/CN的名称和邮寄地址

中国国家知识产权局

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

邱爽

电话号码 (+86) 010-53961362

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2023/071564

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |             |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|-------------|----|----------------|
| CN          | 115422574  | A  | 2022年12月2日     | 无    |             |    |                |
| CN          | 112347476  | A  | 2021年2月9日      | WO   | 2022103330  | A1 | 2022年5月19日     |
| CN          | 111435452  | A  | 2020年7月21日     | 无    |             |    |                |
| CN          | 114611128  | A  | 2022年6月10日     | 无    |             |    |                |
| CN          | 114723068  | A  | 2022年7月8日      | 无    |             |    |                |
| US          | 2020143080 | A1 | 2020年5月7日      | SG   | 11201912390 | YA | 2020年1月30日     |
|             |            |    |                | EP   | 3644231     | A1 | 2020年4月29日     |
|             |            |    |                | TW   | 201907318   | A  | 2019年2月16日     |
|             |            |    |                | WO   | 2019007417  | A1 | 2019年1月10日     |
|             |            |    |                | CN   | 109214404   | A  | 2019年1月15日     |
|             |            |    |                | HK   | 40003201    | A0 | 2020年4月9日      |