(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113780552 B
(45)授权公告日 2024.03.22

(21)申请号 202111052962.8

(22)申请日 2021.09.09

(65)同一申请的已公布的文献号
申请公布号 CN 113780552 A

(43)申请公布日 2021.12.10

(73)专利权人 浙江数秦科技有限公司
地址 311121 浙江省杭州市余杭区仓前街道鼎创财富中心2幢11层

(72)发明人 张金琳 俞学劢 高航

(51)Int.Cl.
G06N 3/098(2023.01)
G06N 3/082(2023.01)
G06N 3/045(2023.01)
G06F 7/544(2006.01)
G06F 7/548(2006.01)
G06F 7/552(2006.01)
G06F 7/556(2006.01)
G06F 21/62(2013.01)

(56)对比文件
CN 110537191 A,2019.12.03
CN 111242290 A,2020.06.05
CN 112529166 A,2021.03.19
CN 112819152 A,2021.05.18
CN 113343284 A,2021.09.03
US 2020242466 A1,2020.07.30
US 2020356858 A1,2020.11.12

何英哲 等.机器学习系统的隐私和安全问题综述.计算机研究与发展.2019,(第10期),第2049-2070页.

刘雨双.基于差分隐私和安全多方计算的模型融合隐私保护数据挖掘方案.中国优秀硕士学位论文全文数据库 信息科技辑.2018,(第12期),第1-47页.

崔建京 等.同态加密在加密机器学习中的应用研究综述.计算机科学.2018,第45卷(第04期),第46-52页.

谭作文 等.机器学习隐私保护研究综述.软件学报.2020,第31卷(第07期),第2127-2156页.

审查员 林贤旻

权利要求书2页 说明书6页 附图5页

(54)发明名称

一种双向隐私保护的安全多方计算方法

(57)摘要

本发明涉及计算机技术领域,具体涉及一种双向隐私保护的安全多方计算方法,包括:模型方建立神经网络模型拟合目标函数;将输入层神经元的连接拆分为两个连接;建立协作输入神经元和保留输入神经元;建立协作方;将协作数发送给协作方;数据方获得保留数;协作方计算协作连接的值;获得协作中间值;数据方将协作比例系数和保留比例系数发送给模型方,获得保留权系数;计算保留连接的值;将保留中间值发送给协作方;协作方获得第1层神经元的输入;模型方代入激活函数,获得第1层神经元的输出,进而获得目标神经网络模型的输出,即为安全多方计算的结果。本发明的有益效果是:扩大了安全多方计算的范围;实现隐私数据和神经网络模型的双向保密。

CN 113780552 B

1.一种双向隐私保护的安全多方计算方法,其特征在于,包括:

模型方建立神经网络模型拟合目标函数,获得目标神经网络模型;

将目标神经网络模型的输入层神经元涉及的连接拆分为两个连接,分别记为协作连接和保留连接,协作连接和保留连接的权系数分别记为协作权系数和保留权系数;

为每个协作连接建立协作输入神经元,为每个保留连接建立保留输入神经元;

建立协作方,模型方将全部协作连接及协作权系数发送给协作方;

每个数据方分别为所属的协作连接和保留连接,随机生成协作比例系数和保留比例系数,将协作连接对应的输入数与协作比例系数相乘的结果,作为协作数,发送给协作方;

数据方将输入数与保留比例系数相乘的结果,作为保留数;

协作方将协作数与协作权系数相乘,作为协作连接的值;

协作方将连接同一个第1层神经元的协作连接的值相加,作为第1层神经元的协作中间值;

数据方将协作比例系数和保留比例系数发送给模型方,模型方通过计算获得适配的保留权系数,将保留权系数反馈给数据方;

数据方将保留数与保留权系数相乘,作为保留连接的值;

将连接同一个第1层神经元的保留连接的值相加,作为第1层神经元的保留中间值,发送给协作方;

协作方将第1层神经元的协作中间值、保留中间值和偏移值相加,获得第1层神经元的输入,将第1层神经元的输入发送给模型方;

模型方将第1层神经元的输入代入激活函数,获得第1层神经元的输出,进而获得目标神经网络模型的输出,即为安全多方计算的结果;

模型方建立神经网络模型拟合目标函数的方法包括:

模型方将目标函数涉及的输入字段发送给相关的数据方;

数据方提供输入字段的输入数的取值范围和分布概率;

模型方根据分布概率在输入数的取值范围内随机生成输入数;

将输入数代入目标函数获得目标函数的结果,结果作为标签,形成样本数据;

使用样本数据训练神经网络模型,获得目标神经网络模型;

模型方为输入层神经元涉及的连接的权系数生成一个随机的干扰量,干扰量与权系数的比值小于预设阈值,根据协作权系数、协作比例系数、保留比例系数及添加干扰量后的原连接权系数,计算出保留权系数,发送给数据源方;

模型方构建神经网络模型时,执行以下步骤:

设定阈值N,N为正整数;

模型方分别计算目标函数对每个输入数的1阶偏导至N阶偏导;

对于输入数,若目标函数的m阶偏导非常数,则模型方添加所述输入数的m次方作为神经网络模型的输入神经元。

2.根据权利要求1所述的一种双向隐私保护的安全多方计算方法,其特征在于,

数据方计算输入数分布概率的方法为:数据方将输入数的取值范围划分为若干个区间,计算每个区间的分布概率。

3.根据权利要求1或2所述的一种双向隐私保护的安全多方计算方法,其特征在于,

模型方获得目标神经网络模型后,检查第1层每个神经元涉及的连接的权重值,若存在第1层的神经元仅涉及一条权重非零的连接,则丢弃该目标神经网络模型,重新构建神经网络模型并重新训练拟合目标函数。

4.根据权利要求1或2所述的一种双向隐私保护的安全多方计算方法,其特征在于,

模型方建立历史记录表,历史记录表记录每对协作连接和保留连接收到的协作比例系数和保留比例系数,并记录模型方分配的协作权系数和计算所得保留权系数;

当再次收到历史表中记录的协作比例系数和保留比例系数时,为协作连接分配同样的协作权系数;

将同样的保留权系数发送给数据源方。

5.根据权利要求1或2所述的一种双向隐私保护的安全多方计算方法,其特征在于,

模型方根据目标函数,选择划分量,所述划分量为目标函数中涉及指数函数的输入数,模型方根据划分量的取值范围,为划分量设置若干个区间,为每个区间建立一个神经网络模型,并将神经网络模型关联对应的区间,进行安全多方计算时,由划分量对应的数据方选择对应的神经网络模型并通知其他数据方、协作方和模型方。

一种双向隐私保护的安全多方计算方法

技术领域

[0001] 本发明涉及大数据技术领域,具体涉及一种双向隐私保护的安全多方计算方法。

背景技术

[0002] 随着大数据时代的到来,如何保护隐私数据和防止敏感信息泄露成为当前面临的重大挑战。在具体应用中,隐私即为数据所有者不愿意被披露的敏感信息,包括敏感数据以及数据所表征的特性。为解决大数据应用中隐私保护的问题,本领域提出了安全多方计算的技术。安全多方计算主要是针对无可信第三方的情况下,如何安全地计算一个约定函数的问题。安全多方计算能够同时确保输入数的隐私和计算结果的正确性。在无可信第三方的前提下通过数学理论保证参与计算的各方成员输入信息不暴露,且同时能够获得准确的运算结果。目前的安全多方计算方案包括加密布尔电路和同态加密。加密布尔电路的执行效率非常低,难以满足需要。同态加密技术仅支持加法和乘法的计算,应用范围十分有限。因而需要研究新的安全多方计算方法。

[0003] 如中国专利CN110546642A,公开日2019年12月6日,一种不利用可信初始化器的安全多方计算,包括编码在计算机存储介质上的计算机程序,通过不利用可信初始化器的秘密共享安全协同地计算包括第一方的隐私数据的第一矩阵和包括第二方的隐私数据的第二矩阵的矩阵乘积。获得包括第一方的隐私数据的第一矩阵;生成第一随机矩阵;识别第一随机矩阵的第一子矩阵和第一随机矩阵的第二子矩阵;基于第一矩阵、第一随机矩阵、第一子矩阵和第二子矩阵计算第一方的第一加扰隐私数据;接收第二方的第二加扰隐私数据;计算矩阵乘积的第一加数;接收矩阵乘积的第二加数;以及通过对第一加数和第二加数求和来计算矩阵乘积。其技术方案使用矩阵乘积完成隐私数的计算,通过秘密共享和加饶数据保证隐私数的保密。但其采用的矩阵乘法能够实现的计算有限,仍然无法解决安全多方计算应用范围窄的技术问题。

发明内容

[0004] 本发明要解决的技术问题是:目前安全多方计算效率低或者应用范围窄的技术问题。提出了一种双向隐私保护的安全多方计算方法,本方法能够扩大安全多方计算的应用范围,同时能够保护目标函数的隐私,实现数据和函数的双向隐私保护。

[0005] 为解决上述技术问题,本发明所采取的技术方案为:一种双向隐私保护的安全多方计算方法,包括:模型方建立神经网络模型拟合目标函数,获得目标神经网络模型;将目标神经网络模型的输入层神经元涉及的连接拆分为两个连接,分别记为协作连接和保留连接,协作连接和保留连接的权系数分别记为协作权系数和保留权系数;为每个协作连接建立协作输入神经元,为每个保留连接建立保留输入神经元;建立协作方,模型方将全部协作连接及协作权系数发送给协作方;每个数据方分别为所属的协作连接和保留连接,随机生成协作比例系数和保留比例系数,将协作连接对应的输入数与协作比例系数相乘的结果,作为协作数,发送给协作方;数据方将输入数与保留比例系数相乘的结果,作为保留数;协

作方将协作数与协作权系数相乘,作为协作连接的值;协作方将连接同一个第1层神经元的协作连接的值相加,作为第1层神经元的协作中间值;数据方将协作比例系数和保留比例系数发送给模型方,模型方通过计算获得适配的保留权系数,将保留权系数反馈给数据方;数据方将保留数与保留权系数相乘,作为保留连接的值;将连接同一个第1层神经元的保留连接的值相加,作为第1层神经元的保留中间值,发送给协作方;协作方将第1层神经元的协作中间值、保留中间值和偏移值相加,获得第1层神经元的输入,将第1层神经元的输入发送给模型方;模型方将第1层神经元的输入代入激活函数,获得第1层神经元的输出,进而获得目标神经网络模型的输出,即为安全多方计算的结果。

[0006] 作为优选,模型方建立神经网络模型拟合目标函数的方法包括:模型方将目标函数涉及的输入字段发送给相关的数据方;数据方提供输入字段的输入数的取值范围和分布概率;模型方根据按照分布概率在输入数的取值范围内随机生成输入数;将输入数代入目标函数获得目标函数的结果,结果作为标签,形成样本数据;使用样本数据训练神经网络模型,获得目标神经网络模型。

[0007] 作为优选,数据方计算输入数分布概率的方法为:数据方将输入数的取值范围划分为若干个区间,计算每个区间的分布概率。

[0008] 作为优选,模型方获得目标神经网络模型后,检查第1层每个神经元涉及的连接的权重值,若存在第1层的神经元仅涉及一条权重非零的连接,则丢弃该目标神经网络模型,重新构建神经网络模型并重新训练拟合目标函数。

[0009] 作为优选,模型方建立历史记录表,历史记录表记录每对协作连接和保留连接收到的协作比例系数和保留比例系数,并记录模型方分配的协作权系数和计算所得保留权系数;当再次收到历史表中记录的协作比例系数和保留比例系数时,为协作连接分配同样的协作权系数;将同样的保留权系数发送给数据源方。

[0010] 作为优选,模型方为输入层神经元涉及的连接的权系数生成一个随机的干扰量,干扰量与权系数的比值小于预设阈值,根据协作权系数、协作比例系数、保留比例系数及添加干扰量后的原连接权系数,计算出保留权系数,发送给数据源方。

[0011] 作为优选,模型方根据目标函数,选择划分量,所述划分量为目标函数中涉及指数函数的输入数,模型方根据划分量的取值范围,为划分量设置若干个区间,为每个区间建立一个神经网络模型,并将神经网络模型关联对应的区间,进行安全多方计算时,由划分量对应的数据方选择对应的神经网络模型并通知其他数据方、协作方和模型方。

[0012] 作为优选,模型方构建神经网络模型时,执行以下步骤:设定阈值N,N为正整数;模型方分别计算目标函数对每个输入数的1阶偏导至N阶偏导;对于输入数,若目标函数的m阶偏导非常数,则模型方添加所述输入数的m次方作为神经网络模型的输入神经元。

[0013] 本发明的实质性效果是:通过神经网络模型拟合任意目标函数,扩大了安全多方计算的范围;神经网络的计算效率较高,提高了安全多方计算的计算效率;实现隐私数据和神经网络模型的双向保密。

附图说明

[0014] 图1为实施例一安全多方计算方法示意图。

[0015] 图2为实施例一拟合目标函数方法示意图。

[0016] 图3为实施例一取值分布概率示意图。

[0017] 图4为实施例一模型方历史记录表使用示意图。

[0018] 图5为实施例一建立神经网络模型方法示意图。

[0019] 图6为实施例一目标神经网络模型示意图。

[0020] 图7为实施例一目标神经网络模型拆分示意图。

[0021] 其中:10、输入数,20、输入层,30、第1层,40、输出层,21、协作连接,22、保留连接,23、保留输入神经元,24、协作输入神经元。

具体实施方式

[0022] 下面通过具体实施例,并结合附图,对本发明的具体实施方式作进一步具体说明。

[0023] 实施例一:

[0024] 一种双向隐私保护的安全多方计算方法,请参阅附图1,本方法包括以下步骤:

[0025] 步骤A01)模型方建立神经网络模型拟合目标函数,获得目标神经网络模型;

[0026] 步骤A02)将目标神经网络模型的输入层神经元涉及的连接拆分为两个连接,分别记为协作连接21和保留连接22,协作连接21和保留连接22的权系数分别记为协作权系数和保留权系数;

[0027] 步骤A03)为每个协作连接21建立协作输入神经元24,为每个保留连接22建立保留输入神经元23;

[0028] 步骤A04)建立协作方,模型方将全部协作连接21及协作权系数发送给协作方;

[0029] 步骤A05)每个数据方分别为所属的协作连接21和保留连接22,随机生成协作比例系数和保留比例系数,将协作连接21对应的输入数与协作比例系数相乘的结果,作为协作数,发送给协作方;

[0030] 步骤A06)数据方将输入数与保留比例系数相乘的结果,作为保留数;

[0031] 步骤A07)协作方将协作数与协作权系数相乘,作为协作连接21的值;

[0032] 步骤A08)协作方将连接同一个第1层神经元的协作连接21的值相加,作为第1层神经元的协作中间值;

[0033] 步骤A09)数据方将协作比例系数和保留比例系数发送给模型方,模型方通过计算获得适配的保留权系数,将保留权系数反馈给数据方;

[0034] 步骤A10)数据方将保留数与保留权系数相乘,作为保留连接22的值;

[0035] 步骤A11)将连接同一个第1层神经元的保留连接22的值相加,作为第1层神经元的保留中间值,发送给协作方;

[0036] 步骤A12)协作方将第1层神经元的协作中间值、保留中间值和偏移值相加,获得第1层神经元的输入,将第1层神经元的输入发送给模型方;

[0037] 步骤A13)模型方将第1层神经元的输入代入激活函数,获得第1层神经元的输出,进而获得目标神经网络模型的输出,即为安全多方计算的结果。

[0038] 请参阅附图2,模型方建立神经网络模型拟合目标函数的方法包括:步骤B01)模型方将目标函数涉及的输入字段发送给相关的数据方;步骤B02)数据方提供输入字段的输入数的取值范围和分布概率;步骤B03)模型方根据按照分布概率在输入数的取值范围内随机生成输入数;步骤B04)将输入数代入目标函数获得目标函数的结果,结果作为标签,形成样

本数据;步骤B05)使用样本数据训练神经网络模型,获得目标神经网络模型。请参阅附图3,数据方计算输入数分布概率的方法为:数据方将输入数的取值范围划分为若干个区间,计算每个区间的分布概率。将区间划分边界和数值的分布概率发送给模型方。

[0039] 理论上神经网络模型能够拟合任意函数。对多个输入数的一次方进行加法运输的拟合效果最好,甚至能实现精准拟合。对于三角函数等取值范围有限的函数的拟合也具有较高的拟合精度和训练效率。然而对于如2次方、3次方、幂函数、指数函数等,达到较高拟合精度会造成神经网络模型较为复杂。采用将输入数的取值范围划分区间的方式,能够提高神经网络模型拟合的精度,加快神经网络模型训练的效率。

[0040] 模型方获得目标神经网络模型后,检查第1层每个神经元涉及的连接的权重值,若存在第1层的神经元仅涉及一条权重非零的连接,则丢弃该目标神经网络模型,重新构建神经网络模型并重新训练拟合目标函数。若仅存在一条权重非零的连接,则说明在神经网络模型训练过程中出现了权重消失的错误。需要重新进行神经网络模型的训练,通常需要修改梯度函数还避免权重消失。

[0041] 请参阅附图4,本实施例中模型方执行以下步骤:步骤C01)模型方建立历史记录表,历史记录表记录每对协作连接21和保留连接22收到的协作比例系数和保留比例系数,并记录模型方分配的协作权系数和计算所得保留权系数;步骤C02)当再次收到历史表中记录的协作比例系数和保留比例系数时,为协作连接21分配同样的协作权系数;步骤C03)将同样的保留权系数发送给数据源方。

[0042] 模型方为输入层神经元涉及的连接的权系数生成一个随机的干扰量,干扰量与权系数的比值小于预设阈值,根据协作权系数、协作比例系数、保留比例系数及添加干扰量后的原连接权系数,计算出保留权系数,发送给数据源方。使用干扰量能够进一步提升模型的隐私性。

[0043] 模型方根据目标函数,选择划分量,划分量为目标函数中涉及指数函数的输入数,模型方根据划分量的取值范围,为划分量设置若干个区间,为每个区间建立一个神经网络模型,并将神经网络模型关联对应的区间,进行安全多方计算时,由划分量对应的数据方选择对应的神经网络模型并通知其他数据方、协作方和模型方。

[0044] 请参阅附图5,模型方构建神经网络模型时,执行以下步骤:步骤D01)设定阈值N,N为正整数;步骤D02)模型方分别计算目标函数对每个输入数的1阶偏导至N阶偏导;步骤D03)对于输入数,若目标函数的m阶偏导非常数,则模型方添加输入数的m次方作为神经网络模型的输入神经元。如目标函数为y=x1^2+3*x2,则目标函数对于x1的一阶偏导、二阶偏导非0,三阶偏导为0,对x2的一阶偏导非0,二阶偏导为0,则为x1建立1次方输入神经元和2次方输入神经元,对x2建立1次方输入神经元。将幂运算转换为加法运算,降低神经网络的复杂度,节省神经网络的训练时长。值得注意的是,即使不建立x1的2次方输入神经元,神经网络模型也能够通过大量样本数据的训练,获得拟合x1的平方的结果。

[0045] 其大致原理为,与x1输入神经元连接的多个隐藏层神经元分别具有不同的权重。当x1的取值与权重相当时,x1与权重的乘积即接近x1的2次方。当这样的隐藏层神经元足够多时,其计算精度将满足要求。同样的,对于x1的3次方,当权重与x1的平方相当时,权重与x1的乘积即接近x1的3次方。

[0046] 同样的,对于指数函数、三角函数、对数函数等较为复杂的函数。当隐藏层神经元

数量足够多时,使得输入数在其取值范围内,总存在某个隐藏层神经元连接的权重与输入数的乘积与对应函数值接近。其他不接近的神经元可以通过激活函数的抑制而不再传播。虽然会导致神经网络模型庞大复杂,但能够实施。

[0047] 同时也意味着,未增加m次方作为神经网络模型的输入神经元时,该方案适合输入数的数量多,而目标函数涉及的计算较为简单的情况。增加m次方作为神经网络模型的输入神经元的技术方案时,由于增加了输入数的高次项,则能够计算更为复杂的目标函数。包括含高次项的加权和计算。实际上,对应能够进行泰勒展开的函数,本方案都能够具有较高效率的进行拟合。如e^x、lnx的泰勒展开式中,包括x的1次方至N次方,当N足够大时,能够使误差低于阈值。从而本实施例大幅的扩大了神经网络模型能够高效率拟合的目标函数的范围。扩大了本方案高效率实施的范围。

[0048] 请参阅附图6,神经网络模型通常包括一个输入层、一个输出层和若干个隐藏层,隐藏层也称为中间层,在一些简单的神经网络模型中,也可以没有隐藏层。输出层可以有一个神经元,也可以有多个神经元。较为典型的神经网络模型为全连接神经网络。即每层的神经元与上一层的神经元均连接。输入层也被称为第0层,相应的隐藏层被依次称为第1层、第2层等。图6中所示神经网络模型具有一个输入层20、一个输出层40和一个隐藏层,即第1层30。输入层10的神经元的输出即为输入数10,用于将输入数10导入神经网络模型。图6所示的神经网络模型的目标函数为x1、x2和x3的加权和。使用的激活函数ReLU在输入数为正数时,是能够根据输出反推出输入数的。因而需要多个输入数才能保证输入数的隐私。

[0049] 请参阅附图7,输入层的神经元有3个,输入数分别为x1、x2和x3,其中x1和x2属于数据方甲,x3属于数据方乙。以第1层的第1个神经元为例,分别将x1、x2和x3拆分为对应的协作数和保留数。如输入数x1记为协作数x1_c和保留数x1_r,相应的协作权系数wc111和保留权系数xr111。对输入数x2和x3做同样操作。

[0050] 协作权系数由模型方分配并发送给协作节点。数据方甲和数据方乙随机生成协作比例系数和保留比例系数。将协作比例系数和保留比例系数发送给模型方。模型方根据协作权系数、原连接权系数、协作比例系数和保留比例系数,计算获得保留权系数。计算等式为:原连接权系数=协作比例系数*协作权系数+保留比例系数*保留权系数。模型方保留有原连接的权系数,因而能够计算获得保留权系数。协作方因不知晓保留权系数,因而无法计算获得原连接的权系数。数据方因不知晓协作权系数,也无法计算获得原连接的权系数。

[0051] 其中数据方甲和数据方乙分别将协作数x1_c、x2_c和x3_c发送给协作方。数据方甲保留保留数x1_r和x2_r,数据方乙保留保留数x3_r,数据方甲计算保留中间值Temp_r_1=x1_r*wr111+x2_r*wr112,数据方乙计算保留中间值Temp_r_2=x3_r*wr113,Temp_r_1和Temp_r_2发送给协作方。协作方计算协作中间值Temp_c= x1_c*wc111+x2_c*wc112+x3_c*wc113,协作方获得第1层的第1个神经元对应的保留中间值Temp_r_1和保留中间值Temp_r_2后,将保留中间值Temp_r_1、保留中间值Temp_r_2和协作中间值Temp_c求和,结果等于x1_r*wr111+x2_r*wr112+x3_r*wr113+x1_c*wc111+x2_c*wc112+x3_c*wc113,即等于x1、x2和x3分别与原连接权系数的乘积的和。再加上偏移值b1后,即获得第1层的第1个神经元的输入。将输入发送给模型方,模型方将输入代入激活函数即可获得第1层的第1个神经元的输出。进而继续获得目标神经网络模型的输出。

[0052] 本实施例的有益技术效果是:通过神经网络模型拟合任意目标函数,扩大了安全

多方计算的范围;神经网络的计算效率较高,提高了安全多方计算的计算效率;实现隐私数据和神经网络模型的双向保密。

[0053] 以上的实施例只是本发明的一种较佳的方案,并非对本发明作任何形式上的限制,在不超出权利要求所记载的技术方案的前提下还有其它的变体及改型。


模型方建立神经网络模型拟合目标函数，获得目标神经网络模型
A01
将目标神经网络模型的输入层神经元涉及的连接拆分为两个连接
A02
为每个协作连接建立协作输入神经元，为每个保留连接建立保留输入神经元
A03
建立协作方，模型方将全部协作连接及协作权系数发送给协作方
A04
数据方随机生成协作比例系数和保留比例系数，将输入数与协作比例系数相乘的结果作为协作数，发送给协作方
A05
数据方将输入数与保留比例系数相乘的结果，作为保留数
A06
协作方将协作数与协作权系数相乘，作为协作连接的值
A07
协作方将连接同一个第1层神经元的协作连接的值相加，作为第1层神经元的协作中间值
A08
数据方将协作比例系数和保留比例系数发送给模型方，模型方通过计算获得适配的保留权系数，将保留权系数反馈给数据方
A09
数据方将保留数与保留权系数相乘，作为保留连接的值
A10
将连接同一个第1层神经元的保留连接的值相加，作为第1层神经元的保留中间值，发送给协作方
A11
协作方将第1层神经元的协作中间值、保留中间值和偏移值相加，获得第1层神经元的输入，将第1层神经元的输入发送给模型方
A12
模型方将第1层神经元的输入代入激活函数，获得第1层神经元的输出，进而获得目标神经网络模型的输出，即为安全多方计算的结果
A13

图1

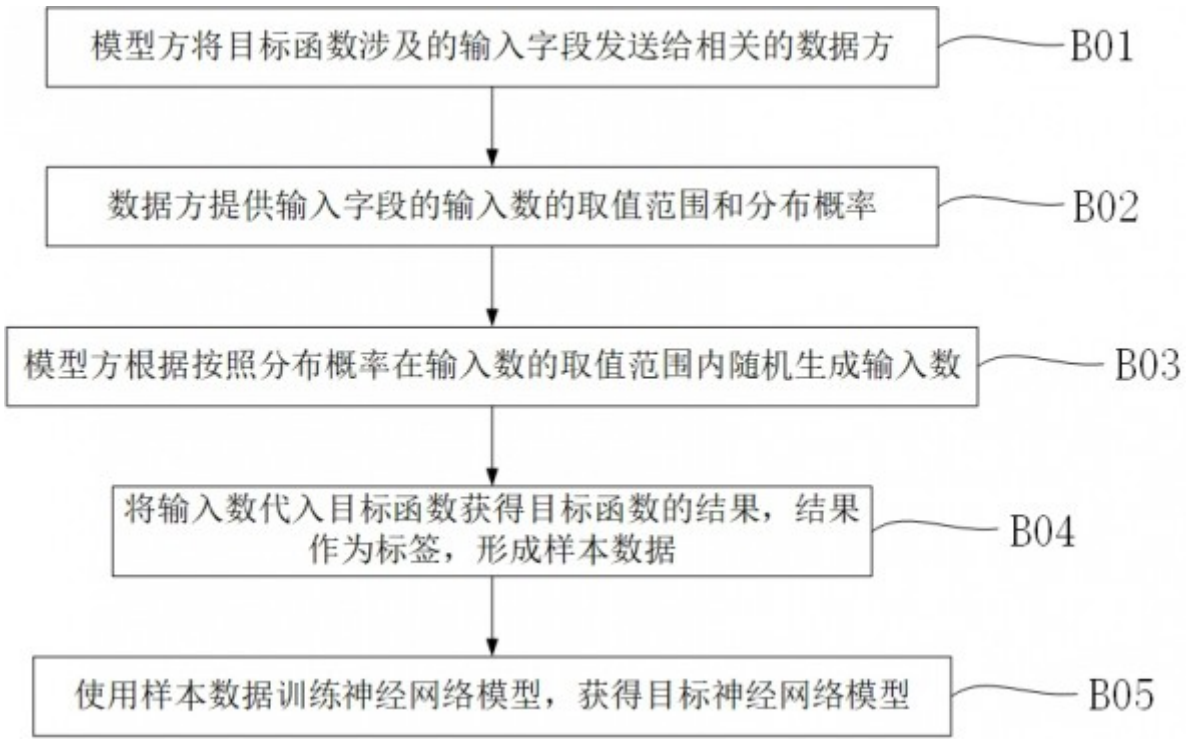
模型方将目标函数涉及的输入字段发送给相关的数据方
B01
数据方提供输入字段的输入数的取值范围和分布概率
B02
模型方根据按照分布概率在输入数的取值范围内随机生成输入数
B03
将输入数代入目标函数获得目标函数的结果，结果作为标签，形成样本数据
B04
使用样本数据训练神经网络模型，获得目标神经网络模型
B05

图2

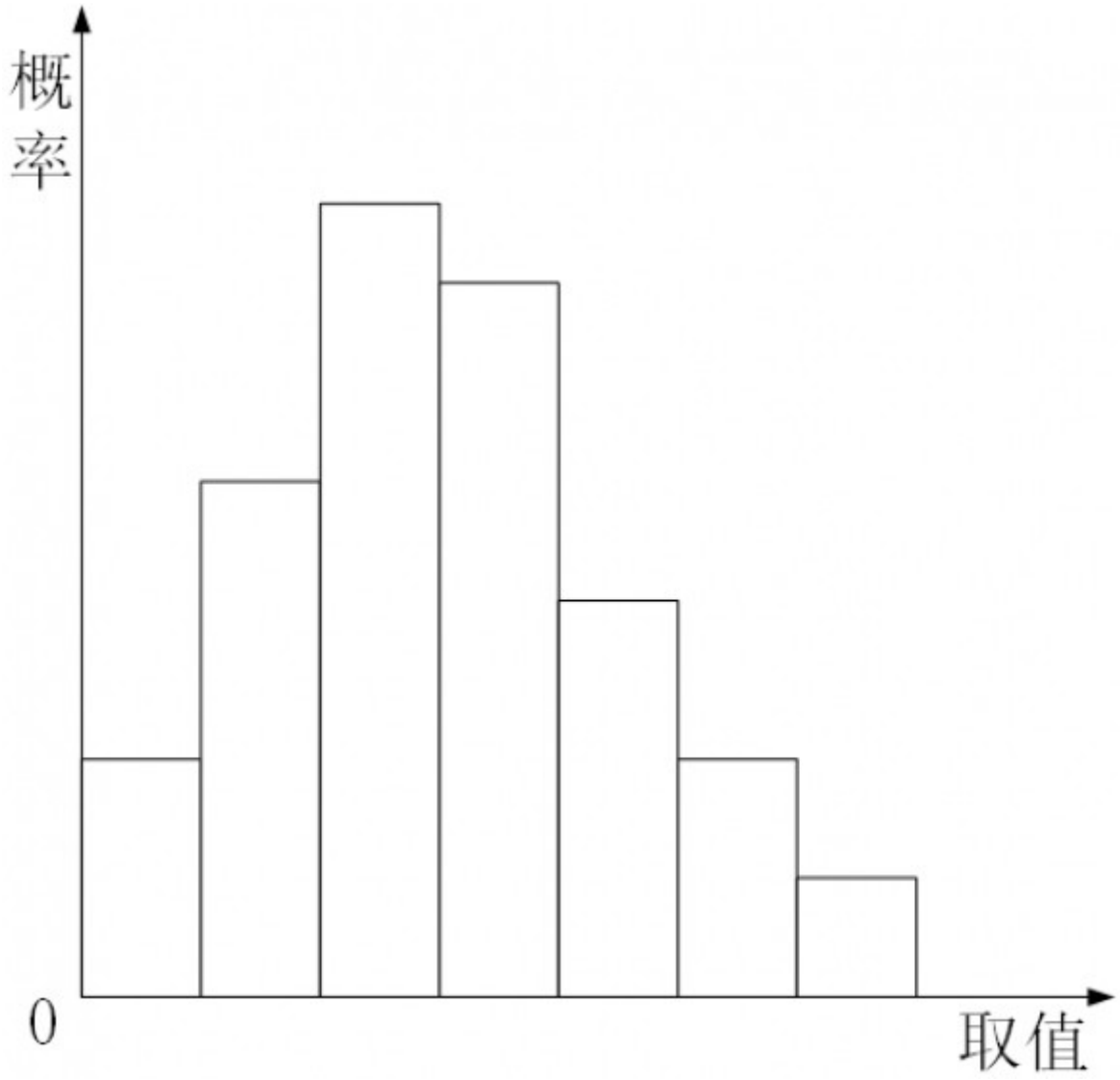
概率
0
取值

图3

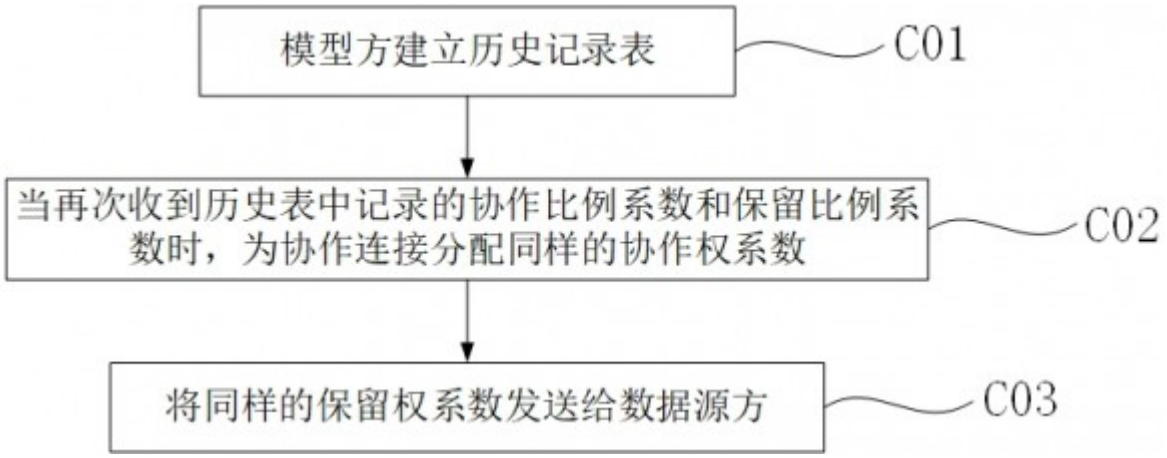
模型方建立历史记录表
C01
当再次收到历史表中记录的协作比例系数和保留比例系数时，为协作连接分配同样的协作权系数
C02
将同样的保留权系数发送给数据源方
C03

图4

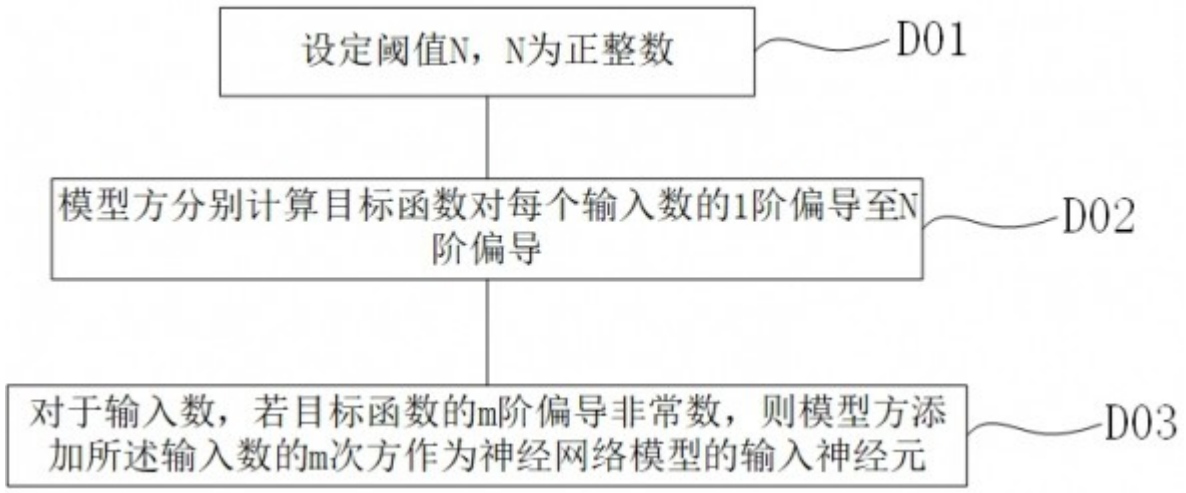
设定阈值N，N为正整数
D01
模型方分别计算目标函数对每个输入数的1阶偏导至N阶偏导
D02
对于输入数，若目标函数的m阶偏导非常数，则模型方添加所述输入数的m次方作为神经网络模型的输入神经元
D03

图5

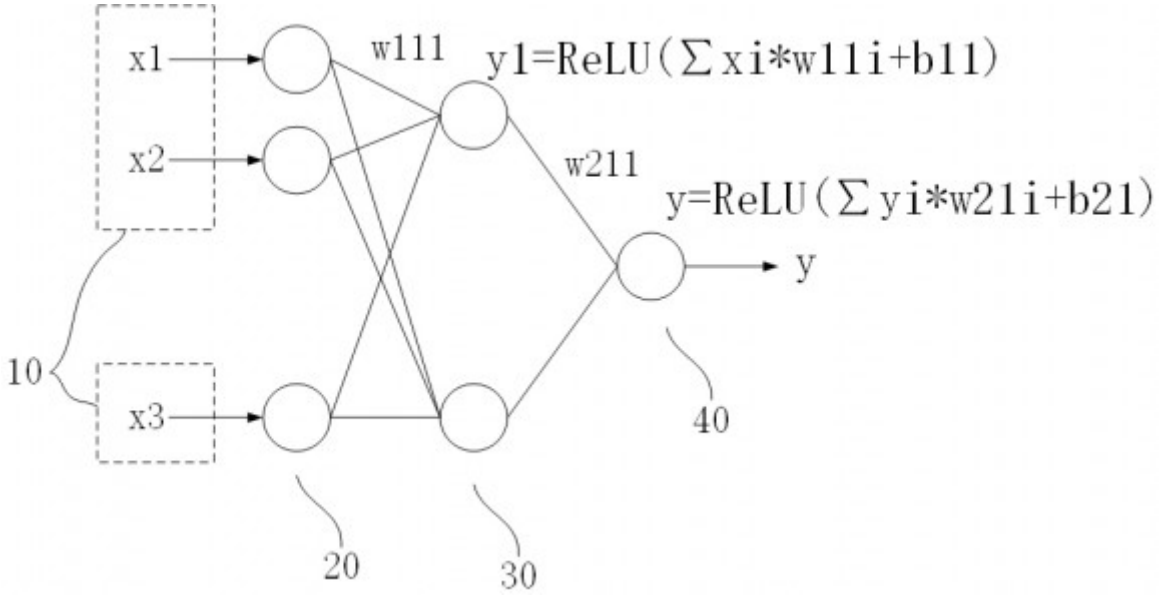
x1
x2
x3
10
w111
y1=ReLU(∑xi*w11i+b11)
w211
y=ReLU(∑yi*w21i+b21)
y
20
30
40

图6

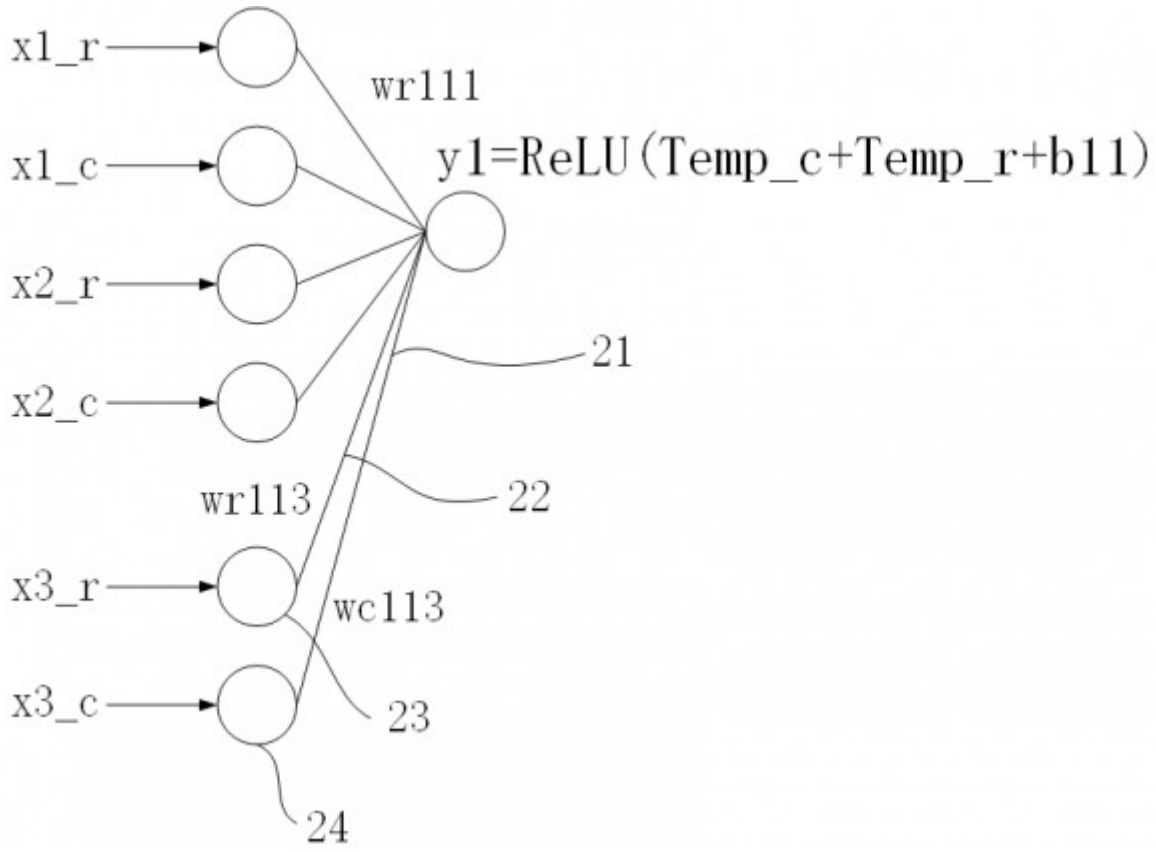
x1_r
x1_c
x2_r
x2_c
x3_r
x3_c
wr111
wr113
wc113
y1=ReLU(Temp_c+Temp_r+b11)
21
22
23
24

图7