(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
2021 年 9 月 30 日 (30.09.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/189907 A1

(51) 国际专利分类号:
G16H 50/70 (2018.01) *G16H 50/20* (2018.01)
G16H 50/50 (2018.01)

(21) 国际申请号: PCT/CN2020/131987

(22) 国际申请日: 2020 年 11 月 27 日 (27.11.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011127805.4 2020年10月20日 (20.10.2020) 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: 李泽远 (LI, Zeyuan); 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)。 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)。

(74) 代理人: 深圳市沃德知识产权代理事务所（普通合伙） (SHENZHEN WORLD INTELLECTUAL PROPERTY AGENCY (GENERAL PARTNERSHIP)); 中国广东省深圳市福田区梅林街道中康路128号卓越城1期2栋301B于志光, Guangdong 518000 (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, 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,

(54) **Title:** ELECTRONIC DEVICE, DISEASE TYPE DETECTION METHOD AND APPARATUS, AND MEDIUM

(54) **发明名称**: 电子设备、疾病类型检测方法、装置及介质

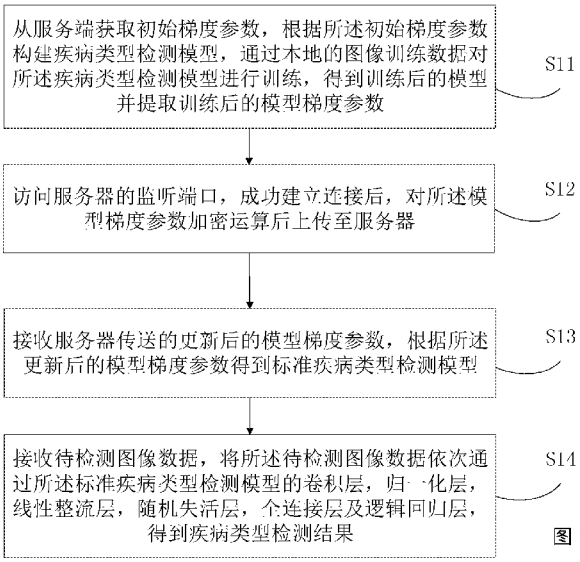

图 1

S11 Acquire an initial gradient parameter from a server, construct a disease type detection model according to the initial gradient parameter, train the disease type detection model by means of local image training data so as to obtain a trained model, and extract a model gradient parameter after training

S12 Access a monitoring port of the server, after a connection is successfully established, perform an encryption operation on the model gradient parameter, and then upload the model gradient parameter subjected to the encryption operation to the server

S13 Receive the updated model gradient parameter transmitted by the server, and obtain a standard disease type detection model according to the updated model gradient parameter

S14 Receive image data to be subjected to detection, and successively make said image data pass through a convolutional layer, a normalization layer, a rectified linear units layer, a dropout layer, a fully connected layer and a logistic regression layer of the standard disease type detection model so as to obtain a disease type detection result

(57) **Abstract:** The present application relates to data processing technology. Disclosed are an electronic device, an apparatus, a storage medium and a disease type detection method. The method comprises: a client encrypting a model gradient parameter after training using local data, and uploading the encrypted model gradient parameter to a server; the server decrypting the encrypted model gradient parameter and performing a joint operation to obtain updated model gradient data; and the client receiving the updated model gradient parameter returned by the server, obtaining a standard disease type detection model according to the updated model gradient parameter, and performing detection on image data to be subjected to detection by using the standard disease type detection model so as to obtain a disease type detection result. The present application further relates to blockchain technology, and the updated model gradient parameter can be stored in a blockchain node. By means of the present application, the accuracy of a disease type detection model can be improved.

WO 2021/189907 A1

[见续页]

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。

(57) 摘要：本申请涉及数据处理技术，揭露一种电子设备、装置、存储介质及疾病类型检测方法。所述方法包括：客户端将利用本地数据训练后的模型梯度参数加密后上传至服务端，服务端对所述加密后的模型梯度参数进行解密并进行联合运算，得到更新后的模型梯度数据，客户端接收到服务端返回更新后的模型梯度参数并根据所述更新后的模型梯度参数得到标准疾病类型检测模型，利用标准疾病类型检测模型对待检测图像数据进行检测，得到疾病类型检测结果。本申请还涉及区块链技术，所述更新后的模型梯度参数可以存储在区块链节点中。本申请可以提高疾病类型检测模型的准确性。

电子设备、疾病类型检测方法、装置及介质

本申请要求于 2020 年 10 月 20 日提交中国专利局、申请号为 CN202011127805.4、名称为“电子设备、疾病类型检测方法、装置及介质”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

本申请涉及数据处理技术，尤其涉及一种电子设备、疾病类型检测方法、装置及计算机可读存储介质。

背景技术

疾病的检测与判断对于降低病人的死亡率尤其重要。例如，当今，心脏病成为人们生活中一种常见疾病，心脏病具体细分包括众多种类，实现对心脏病种类快速且准确的检测可以降低心脏病患者死亡率。目前检测心脏病种类主要采用心电图检测手段，对心脏疾病进行诊断。

由于医疗数据的隐私性，发明人意识到目前用于对心电图进行检测的模型准确率不够高，用于训练模型的心电图数据局限于几个医院中，各个医院所拥有的心电图数据仍存在数据壁垒，使得大量的心电图数据无法有效利用，从而无法准确根据心电图判断出心脏疾病种类。

发明内容

本申请提供的一种电子设备，所述电子设备包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器能够执行如下步骤：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

本申请还提供一种电子设备，其中，所述电子设备包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器执行如下步骤：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

本申请还提供一种应用于客户端的疾病类型检测装置，所述装置包括：

加密模块，用于从服务端端获取疾病类型检测模型，通过本地的图像数据训练数据对所述疾病类型检测模型进行训练，得到训练后的模型梯度参数，访问服务端的监听端口，成功建立连接后，对所述模型梯度参数进行加密后上传至服务端；

模型更新模块，用于接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

分类模块，用于接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

本申请还提供一种应用于服务端的疾病类型检测装置，所述装置包括：

解密模块，用于开启 K 个监听端口，其中，K 为客户端的数量，利用所述监听端口接收多个客户端发送的加密后的模型梯度参数，对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

参数更新模块，用于对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，将所述更新后的模型梯度参数分发给每个客户端。

本申请还提供一种计算机可读存储介质，包括存储数据区和存储程序区，存储数据区存储创建的数据，存储程序区存储有计算机程序；其中，所述计算机程序被处理器执行时实现：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到训练后的模型并提取训练后的模型梯度参数；

访问服务端的监听端口，成功建立连接后，对所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

本申请还提供一种计算机可读存储介质，包括存储数据区和存储程序区，存储数据区存储创建的数据，存储程序区存储有计算机程序；其中，所述计算机程序被处理器执行时实现：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

本申请还提供一种疾病类型检测方法，所述方法包括：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

本申请还提供一种疾病类型检测方法，所述方法包括：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

附图说明

图1为本申请第一实施例提供的电子设备的内部结构示意图；

图2为本申请第二实施例提供的疾病类型检测方法的流程示意图；

图3为本申请第三实施例提供的疾病类型检测方法的流程示意图；

图4为本申请第四实施例提供的疾病类型检测装置的模块示意图；

本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本申请实施例提供一种电子设备。所述电子设备可以是，例如服务端、终端等的至少一种。所述服务端包括但不限于：单台服务端、服务端集群、云端服务端或云端服务端集群等。

如图 1 所示，为本申请一实施例提供的电子设备的内部结构示意图。

所述电子设备 1 可以包括处理器 10、存储器 11 和总线，还可以包括存储在所述存储器 11 中并可在所述处理器 10 上运行的计算机程序，如疾病类型检测程序 12。

其中，所述存储器 11 至少包括一种类型的可读存储介质，所述可读存储介质包括闪存、移动硬盘、多媒体卡、卡型存储器（例如：SD 或 DX 存储器等）、磁性存储器、磁盘、光盘等。所述存储器 11 在一些实施例中可以是电子设备 1 的内部存储单元，例如该电子设备 1 的移动硬盘。所述存储器 11 在另一些实施例中也可以是电子设备 1 的外部存储设备，例如电子设备 1 上配备的插接式移动硬盘、智能存储卡（Smart Media Card， SMC）、安全数字（Secure Digital， SD）卡、闪存卡（Flash Card）等。进一步地，所述存储器 11 还可以既包括电子设备 1 的内部存储单元也包括外部存储设备。所述存储器 11 不仅可以用于存储安装于电子设备 1 的应用软件及各类数据，例如疾病类型检测程序 12 的代码等，还可以用于暂时地存储已经输出或者将要输出的数据。

所述处理器 10 在一些实施例中可以由集成电路组成，例如可以由单个封装的集成电路所组成，也可以是由多个相同功能或不同功能封装的集成电路所组成，包括一个或者多个中央处理器（Central Processing unit，CPU）、微处理器、数字处理芯片、图形处理器及各种控制芯片的组合等。所述处理器 10 是所述电子设备的控制核心（Control Unit），利用各种接口和线路连接整个电子设备的各个部件，通过运行或执行存储在所述存储器 11 内的程序或者模块（例如执行疾病类型检测程序等），以及调用存储在所述存储器 11 内的数据，以执行电子设备 1 的各种功能和处理数据。

所述总线可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。该总线可以分为地址总线、数据总线、控制总线等。所述总线被设置为实现所述存储器 11 以及至少一个处理器 10 等之间的连接通信。

图 1 仅示出了具有部件的电子设备，本领域技术人员可以理解的是，图 1 示出的结构

并不构成对所述电子设备 1 的限定，可以包括比图示更少或者更多的部件，或者组合某些部件，或者不同的部件布置。

例如，尽管未示出，所述电子设备 1 还可以包括给各个部件供电的电源（比如电池），优选地，电源可以通过电源管理装置与所述至少一个处理器 10 逻辑相连，从而通过电源管理装置实现充电管理、放电管理、以及功耗管理等功能。电源还可以包括一个或一个以上的直流或交流电源、再充电装置、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。所述电子设备 1 还可以包括多种传感器、蓝牙模块、Wi-Fi 模块等，在此不再赘述。

进一步地，所述电子设备 1 还可以包括网络接口，可选地，所述网络接口可以包括有线接口和/或无线接口（如 WI-FI 接口、蓝牙接口等），通常用于在该电子设备 1 与其他电子设备之间建立通信连接。

可选地，该电子设备 1 还可以包括用户接口，用户接口可以是显示器（Display）、输入单元（比如键盘（Keyboard）），可选地，用户接口还可以是标准的有线接口、无线接口。可选地，在一些实施例中，显示器可以是 LED 显示器、液晶显示器、触控式液晶显示器以及 OLED（Organic Light-Emitting Diode，有机发光二极管）触摸器等。其中，显示器也可以适当的称为显示屏或显示单元，用于显示在电子设备 1 中处理的信息以及用于显示可视化的用户界面。

应该了解，所述实施例仅为说明之用，在专利申请范围上并不受此结构的限制。

所述电子设备 1 中的所述存储器 11 存储的疾病类型检测程序 12 是多个指令的组合，在所述处理器 10 中运行时，可以实现一种疾病类型检测方法。详细地，所述疾病类型检测方法可参照下述关于图 2 所示的流程图中的描述。

参照图 2 所示，为本申请第二实施例提供的一种疾病类型检测方法的流程示意图。本实施例第二实施例中所述的疾病类型检测方法应用于客户端中，包括：

S11、从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型训练后的模型梯度参数。

本申请实施例中，所述本地的图像训练数据包括医院的数据库中所保存的病人的心电图像。

本申请实施例利用所述本地的图像训练数据对从服务端端获取到的疾病类型检测模型进行训练，得到训练后的模型梯度参数。

S12、访问服务端的监听端口，成功建立连接后，将训练后的所述模型梯度参数进行加密后上传至服务端。

本申请实施例中，所述对所述模型梯度参数进行加密，包括：

随机选取大质数p，q，使得pq与$(p-1)(q-1)$的最大公倍数为 1；

计算$n=p\times q$，且满足$\lambda(n)=lcm(p-1,q-1)$，其中，lcm 为最小公倍数，λ 为卡迈克尔函数；

随机选择一个小于n^2的正整数g，并计算$\mu=(L(g^{\lambda}modn^2))^{-1}modn$；

根据所述 n、g、λ,和μ，得到公钥为(n,g)，私钥为(λ,μ)；

利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

其中，质数是指在大于 1 的自然数中，除了 1 和它本身以外不再有其他因数的自然数，所述大质数则是指满足质数定义的自然数中最大的一个或者多个。

进一步地，本申请实施例将所述公钥传输给服务端，利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

本申请实施例在多个客户端，如多个医院，执行所述疾病类型检测模型的训练，得到每个客户端对应的模型梯度参数。例如，所述多个医院可以包括 A 医院、B 医院和 C 医院

等，A 医院对应的模型梯度参数为w_1，B 医院对应的模型梯度参数为w_2，C 医院对应的模型梯度参数为w_3等，以此类推。本申请实施例利用所述私钥对所述模型梯度参数进行加密，方便后续上传更新，达到了拓展数据样本并保护病人隐私的目的。

进一步地，本申请实施例利用 http 协议通过服务端开的监听端口将加密后的模型梯度参数上传至所述服务端。

S13、接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型。

本申请实施例利用服务端传送的更新后的模型梯度参数对所述疾病类型检测模型进行更新，得到标准疾病类型检测模型。

S14、接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

本申请实施例中，接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

其中，所述卷积层用于对所述待检测图像数据进行特征提取，所述归一化层用于防止梯度爆炸和梯度消失，所述线性整流层用于提高梯度下降和反向传播过程的效率，所述随机失活层用于实现所述标准疾病类型检测模型的正则化，降低其结构风险，所述全连接层用于将特征提取出的局部特征进行组装，以及所述逻辑回归层用于进行预测。

进一步地，所述待检测图像数据以及对应的注释数据包括心电图像与其对应的包含了心脏病专家的注释数据的 json 文件。

例如，本申请实施例获取病人的心电图数据，将所述心电图数据输入至所述标准疾病类型检测模型中，通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到诊断结果。其中，所述诊断结果是心脏疾病的具体分类，包括但不限于心房纤颤和扑动，房室传导阻滞，二联律，异位心房节律，交接性心律，窦性心律，室上性心动过速。

图 3 所示的流程示意图描述了本申请第三实施例提供的疾病类型检测方法。本实施例第三实施例所述的疾病类型检测方法应用于服务端，包括：

S21、开启 K 个监听端口，其中，K 为客户端的数量。

本申请实施例中，所述服务端根据客户端的数量开启 K 个监听端口，以便与每一个客户端之间执行数据传输。

S22、利用所述监听端口接收多个客户端发送的加密后的模型梯度参数。

S23、对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数。

本申请实施例利用所述公钥(n, g)对所述加密后的模型梯度参数进行解密处理，得到每个客户端对应的模型梯度参数。

具体地，所述对所述加密后的模型梯度参数进行解密，包括：

根据下述解密公式对所述加密后的模型梯度参数进行解密：

$$m = L\left(c^{\lambda} mod n^2\right) * \mu mod n$$

$$L\left(c^{\lambda} mod n^2\right) = \frac{(c^{\lambda} mod n^2 - 1)}{n}$$

其中，m 是解密后的模型梯度参数，c 是指加密后的模型梯度参数，mod 是指取模运算符，$n = p \times q$，其中，p，q为满足pq与$(p-1)(q-1)$的最大公倍数为 1 的大质数，λ 为卡迈克尔函数，μ为预设参数。

例如，所述各个客户端包括但不限于 A 医院、B 医院、C 医院，各个客户端对所述加密后的模型梯度参数进行解密处理，得到每个客户端对应的模型梯度参数。

S24、对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数。

本申请实施例中，所述对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，包括：

采用下述方法执行联合运算，得到更新后的模型梯度参数：

$$f(w)=\sum_{k=1}^{K}\frac{n_k}{n}F_k(w)$$

$$F_k(w)=\frac{1}{n_k}\sum_{i\in P_k}f_i(w)$$

其中，$f(w)$为更新后的模型梯度参数，$f_i(w)$为模型梯度参数，$F_k(w)$表示中间参数，K 为所述客户端数量，P_k代表存储在第 k 个客户端中的训练数据，n_k为训练数据的数量。

S25、将所述更新后的模型梯度参数分发给每个客户端。

本申请实施例中，对所述客户端与所述服务端进行安全连接，得到成功建立连接的所述客户端和所述服务端，将所述更新后的模型梯度参数分发给每个客户端。

如图 4 所示，是本申请第四实施例提供的疾病类型检测装置的模块示意图。

本申请所述疾病类型检测装置可以被划分为第一疾病类型检测装置 100 以及第二疾病类型检测装置 200。其中，所述第一疾病类型检测装置 100 可以安装于客户端中以及所述第二疾病类型检测装置 200 可以安装在服务端中。

根据实现的功能，所述第一疾病类型检测装置 100 可以包括加密模块 101、模型更新模块 102 及分类模块 103；以及所述第二疾病类型检测装置 200 可以包括解密模块 201 及参数更新模块 202。

本申请所述模块也可以称之为单元，是指一种能够被电子设备处理器所执行，并且能够完成固定功能的一系列计算机程序段，其存储在电子设备的存储器中。

在本实施例中，所述第一疾病类型检测装置 100 中和所述第一疾病类型检测装置 200 各模块的功能如下：

所述加密模块 101，用于从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数，访问服务端的监听端口，成功建立连接后，将训练后的所述模型梯度参数进行加密后上传至服务端；

所述解密模块 201，用于开启 K 个监听端口，其中，K 为客户端的数量，利用所述监听端口接收多个客户端发送的加密后的模型梯度参数，对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

所述参数更新模块 202，用于对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，将所述更新后的模型梯度参数分发给每个客户端。

所述模型更新模块 102，用于接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

所述分类模块 103，用于接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

详细地，所述第一疾病类型检测装置 100 各模块在客户端中执行下述操作：

步骤一、所述加密模块 101 从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所

述疾病类型检测模型训练后的模型梯度参数；本申请实施例中，所述本地的图像训练数据包括医院的数据库中所保存的病人的心电图像。

本申请实施例利用所述本地的图像训练数据对从服务端端获取到的疾病类型检测模型进行训练，得到训练后的模型梯度参数。

步骤二、所述加密模块 101 访问服务端的监听端口，成功建立连接后，

对所述模型梯度参数进行加密后上传至服务端。

本申请实施例中，所述加密模块 101 对所述模型梯度参数进行加密，包括：

随机选取大质数p，q，使得pq与$(p-1)(q-1)$的最大公倍数为 1；

计算$n=p\times q$，且满足$\lambda(n)=lcm(p-1,q-1)$，其中，lcm 为最小公倍数，λ 为卡迈克尔函数；

随机选择一个小于n^2的正整数g，并计算$\mu=(L(g^{\lambda}modn^2))^{-1}modn$；

根据所述 n、g、λ,和μ，得到公钥为(n,g)，私钥为(λ,μ)；

利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

其中，质数是指在大于 1 的自然数中，除了 1 和它本身以外不再有其他因数的自然数，所述大质数则是指满足质数定义的自然数中最大的一个或者多个。

进一步地，本申请实施例将所述公钥传输给服务端，利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

本申请实施例在多个客户端，如多个医院，执行所述疾病类型检测模型的训练，得到每个客户端对应的模型梯度参数。例如，所述多个医院可以包括 A 医院、B 医院和 C 医院等，A 医院对应的模型梯度参数为w_1，B 医院对应的模型梯度参数为w_2，C 医院对应的模型梯度参数为w_3等，以此类推。本申请实施例利用所述私钥对所述模型梯度参数进行加密，方便后续上传更新，达到了拓展数据样本并保护病人隐私的目的。

进一步地，本申请实施例利用 http 协议通过服务端开的监听端口将加密后的模型梯度参数上传至所述服务端。

步骤三、所述模型更新模块 102 接收服务端传送的更新后的梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型。

本申请实施例所述模型更新模块 102 利用服务端传送的更新后的模型梯度参数对所述疾病类型检测模型进行更新，得到标准疾病类型检测模型。

步骤四、所述分类模块 103 接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

其中，所述卷积层用于对所述待检测图像数据进行特征提取，所述归一化层用于防止梯度爆炸和梯度消失，所述线性整流层用于提高梯度下降和反向传播过程的效率，所述随机失活层用于实现所述标准疾病类型检测模型的正则化，降低其结构风险，所述全连接层用于将特征提取出的局部特征进行组装，以及所述逻辑回归层用于进行预测。

本申请实施例中，所述分类模块 103 接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

进一步地，所述待检测图像数据以及对应的注释数据包括心电图像与其对应的包含了心脏病专家的注释数据的 json 文件。

例如，本申请实施例获取病人的心电图数据，将所述心电图数据输入至所述标准疾病类型检测模型中，通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到诊断结果。其中，所述诊断结果是心脏疾病的具体分类，包括但不限于心房纤颤和扑动，房室传导阻滞，二联律，异位心房节律，交接性心律，窦性心律，室上性心动过速。

详细地，所述第二疾病类型检测装置 200 各模块在服务端中执行下述操作：

步骤一、所述解密模块 201 开启 K 个监听端口，其中，K 为客户端的数量。

本申请实施例中，所述服务端根据客户端的数量开启 K 个监听端口，以便与每一个客户端之间执行数据传输。

步骤二、所述解密模块 201 利用所述监听端口接收多个客户端发送的加密后的模型梯度参数。

步骤三、所述解密模块 201 对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数。

本申请实施例所述解密模块 201 利用所述公钥(n, g)对所述加密后的模型梯度参数进行解密处理，得到每个客户端对应的模型梯度参数。

具体地，所述对所述加密后的模型梯度参数进行解密，包括：

根据下述解密公式对所述加密后的模型梯度参数进行解密：

$$m = L\left(c^{\lambda} mod n^2\right) * \mu mod n$$

$$L\left(c^{\lambda} mod n^2\right) = \frac{(c^{\lambda} mod n^2 - 1)}{n}$$

其中，m 是解密后的模型梯度参数，c 是指加密后的模型梯度参数，mod 是指取模运算符,$n = p \times q$，其中，p，q为满足pq与$(p-1)(q-1)$的最大公倍数为 1 的大质数，λ 为卡迈克尔函数，μ为预设参数。

例如，所述各个客户端包括但不限于 A 医院、B 医院、C 医院，各个客户端对所述加密后的模型梯度参数进行解密处理，得到每个客户端对应的模型梯度参数。

步骤四、所述参数更新模块 202 对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数。

本申请实施例中，所述参数更新模块 202 对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，包括：

采用下述方法执行联合运算，得到更新后的模型梯度参数：

$$f(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w)$$

$$F_k(w) = \frac{1}{n_k} \sum_{i \in P_k} f_i(w)$$

其中，$f(w)$为更新后的模型梯度参数，$f_i(w)$为模型梯度参数，$F_k(w)$表示中间参数，K 为所述客户端数量，P_k代表存储在第 k 个客户端中的训练数据，n_k为训练数据的数量。

步骤五、所述参数更新模块 202 将所述更新后的模型梯度参数分发给每个客户端。

本申请实施例中，所述参数更新模块 202 对所述客户端与所述服务端进行安全连接，得到成功建立连接的所述客户端和所述服务端，将所述更新后的模型梯度参数分发给每个客户端。

进一步地，所述疾病类型检测装置的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中，所述计算机可读存储介质可以是易失性，也可以是非易失性。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U 盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM，Read-Only Memory）。

进一步地，所述计算机可用存储介质可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序等；存储数据区可存储根据区块链节点的使用所创建的数据等。

所述计算机可读存储介质的存储程序区存储有计算机程序；其中，所述计算机程序被

处理器执行时实现如下步骤：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

进一步的，所述计算机可读存储介质的存储程序区存储有计算机程序；其中，所述计算机程序被处理器执行时实现如下步骤：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能模块的形式实现。

对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。

因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附关联图表记视为限制所涉及的权利要求。

此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第二等词语用来表示名称，而并不表示任何特定的顺序。

最后应说明的是，以上实施例仅用以说明本申请的技术方案而非限制，尽管参照较佳实施例对本申请进行了详细说明，本领域的普通技术人员应当理解，可以对本申请的技术方案进行修改或等同替换，而不脱离本申请技术方案的精神和范围。

权利要求书

1、一种电子设备，其中，所述电子设备包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器执行如下步骤：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

2、如权利要求 1 所述的电子设备，其中，所述对所述模型梯度参数进行加密后上传至服务端，包括：

随机选取大质数p，q，使得pq与$(p-1)(q-1)$的最大公倍数为 1；

计算$n=p\times q$，且满足$\lambda(n)=lcm(p-1,q-1)$，其中，lcm 为最小公倍数，λ 为卡迈克尔函数；

随机选择一个小于n^2的正整数g，并计算$\mu=(L(g^{\lambda}modn^2))^{-1}modn$；

根据所述 n、g、λ,和μ，得到公钥为(n,g)，私钥为(λ,μ)；

利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

3、如权利要求 1 所述的电子设备，其中，所述待检测图像数据以及对应的注释数据包括心电图像与其对应的包含了心脏病专家的注释数据的 json 文件。

4、一种电子设备，其中，所述电子设备包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器执行如下步骤：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

5、如权利要求 4 所述的电子设备，其中，所述对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，包括：

采用下述方法执行联合运算，得到更新后的模型梯度参数：

$$f(w)=\sum_{k=1}^{K}\frac{n_k}{n}F_k(w)$$

$$F_k(w)=\frac{1}{n_k}\sum_{i\in P_k}f_i(w)$$

其中，$f(w)$为更新后的模型梯度参数，$f_i(w)$为模型梯度参数，$F_k(w)$表示中间参数，K 为所述客户端数量，P_k代表存储在第 k 个客户端中的训练数据，n_k为训练数据的数量。

6、如权利要求 4 所述的电子设备，其中，所述对所述加密后的模型梯度参数进行解密，包括：

根据下述解密公式对所述加密后的模型梯度参数进行解密：

$$m = L\left(c^{\lambda} mod n^2\right) * \mu mod n$$

$$L\left(c^{\lambda} mod n^2\right) = \frac{(c^{\lambda} mod n^2 - 1)}{n}$$

其中，m 是解密后的模型梯度参数，c 是指加密后的模型梯度参数，mod 是指取模运算符，$n = p \times q$，其中，p，q为满足pq与$(p-1)(q-1)$的最大公倍数为 1 的大质数，λ 为卡迈克尔函数，μ为预设参数。

7、一种疾病类型检测装置，其中，所述装置应用于客户端电子设备，所述装置包括：

加密模块，用于从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数，访问服务端的监听端口，成功建立连接后，将训练后的所述模型梯度参数进行加密后上传至服务端；

模型更新模块，用于接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

分类模块，用于接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

8、一种疾病类型检测装置，其中，所述装置应用于服务端电子设备，所述装置包括：

解密模块，用于开启 K 个监听端口，其中，K 为客户端的数量，利用所述监听端口接收多个客户端发送的加密后的模型梯度参数，对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

参数更新模块，用于对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，将所述更新后的模型梯度参数分发给每个客户端。

9、一种计算机可读存储介质，包括存储数据区和存储程序区，存储数据区存储创建的数据，存储程序区存储有计算机程序；其中，所述计算机程序被处理器执行时实现如下步骤：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

10、如权利要求 9 所述的计算机可读存储介质，其中，所述对所述模型梯度参数进行加密后上传至服务端，包括：

随机选取大质数p，q，使得pq与$(p-1)(q-1)$的最大公倍数为 1；

计算$n = p \times q$，且满足$\lambda(n) = lcm(p-1, q-1)$，其中，lcm 为最小公倍数，λ 为卡迈克尔函数；

随机选择一个小于n^2的正整数g，并计算$\mu = (L(g^{\lambda} mod n^2))^{-1} mod n$；

根据所述 n、g、λ,和μ，得到公钥为(n, g)，私钥为(λ, μ)；

利用所述私钥(λ, μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

11、如权利要求 9 所述的计算机可读存储介质，其中，所述待检测图像数据以及对应的注释数据包括心电图像与其对应的包含了心脏病专家的注释数据的 json 文件。

12、一种计算机可读存储介质，包括存储数据区和存储程序区，存储数据区存储创建的数据，存储程序区存储有计算机程序；其中，所述计算机程序被处理器执行时实现如下步骤：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

13、如权利要求 12 所述的计算机可读存储介质，其中，所述对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，包括：

采用下述方法执行联合运算，得到更新后的模型梯度参数：

$$f(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w)$$

$$F_k(w) = \frac{1}{n_k} \sum_{i \in P_k} f_i(w)$$

其中，$f(w)$为更新后的模型梯度参数，$f_i(w)$为模型梯度参数，$F_k(w)$表示中间参数，K 为所述客户端数量，P_k代表存储在第 k 个客户端中的训练数据，n_k为训练数据的数量。

14、如权利要求 12 述的计算机可读存储介质，其中，所述对所述加密后的模型梯度参数进行解密，包括：

根据下述解密公式对所述加密后的模型梯度参数进行解密：

$$m = L(c^{\lambda} mod n^2) * \mu mod n$$

$$L(c^{\lambda} mod n^2) = \frac{(c^{\lambda} mod n^2 - 1)}{n}$$

其中，m 是解密后的模型梯度参数，c 是指加密后的模型梯度参数，mod 是指取模运算符，$n = p \times q$，其中，p，q为满足pq与$(p-1)(q-1)$的最大公倍数为 1 的大质数，λ 为卡迈克尔函数，μ为预设参数。

15、一种疾病类型检测方法，其中，所述方法包括：

从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到所述疾病类型检测模型的训练后的模型梯度参数；

访问服务端的监听端口，与所述服务端成功建立连接后，将训练后的所述模型梯度参数加密运算后上传至服务端；

接收服务端传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型；

接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果。

16、如权利要求 15 所述的疾病类型检测方法，其中，所述对所述模型梯度参数进行加密后上传至服务端，包括：

随机选取大质数p，q，使得pq与$(p-1)(q-1)$的最大公倍数为 1；

计算$n=p\times q$，且满足$\lambda(n)=lcm(p-1,q-1)$，其中，lcm 为最小公倍数，λ 为卡迈克尔函数；

随机选择一个小于n^2的正整数g，并计算$\mu=(L(g^{\lambda}modn^2))^{-1}modn$；

根据所述 n、g、λ,和μ，得到公钥为(n,g)，私钥为(λ,μ)；

利用所述私钥(λ,μ)对所述模型梯度参数进行加密处理，得到加密后的模型梯度参数。

17、如权利要求 15 所述的疾病类型检测方法，其中，所述待检测图像数据以及对应的注释数据包括心电图像与其对应的包含了心脏病专家的注释数据的 json 文件。

18、一种疾病类型检测方法，其中，所述方法包括：

开启 K 个监听端口，其中，K 为客户端的数量；

利用所述监听端口接收多个客户端发送的加密后的模型梯度参数；

对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数；

对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数；

将所述更新后的模型梯度参数分发给每个客户端。

19、如权利要求 18 所述的疾病类型检测方法，其中，所述对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数，包括：

采用下述方法执行联合运算，得到更新后的模型梯度参数：

$$f(w)=\sum_{k=1}^{K}\frac{n_k}{n}F_k(w)$$

$$F_k(w)=\frac{1}{n_k}\sum_{i\in P_k}f_i(w)$$

其中，$f(w)$为更新后的模型梯度参数，$f_i(w)$为模型梯度参数，$F_k(w)$表示中间参数，K 为所述客户端数量，P_k代表存储在第 k 个客户端中的训练数据，n_k为训练数据的数量。

20、如权利要求 18 所述的疾病类型检测方法，其中，所述对所述加密后的模型梯度参数进行解密，包括：

根据下述解密公式对所述加密后的模型梯度参数进行解密：

$$m=L(c^{\lambda}modn^2)*\mu modn$$

$$L(c^{\lambda}modn^2)=\frac{(c^{\lambda}modn^2-1)}{n}$$

其中，m 是解密后的模型梯度参数，c 是指加密后的模型梯度参数，mod 是指取模运算符，$n=p\times q$，其中，p，q为满足pq与$(p-1)(q-1)$的最大公倍数为 1 的大质数，λ 为卡迈克尔函数，μ为预设参数。

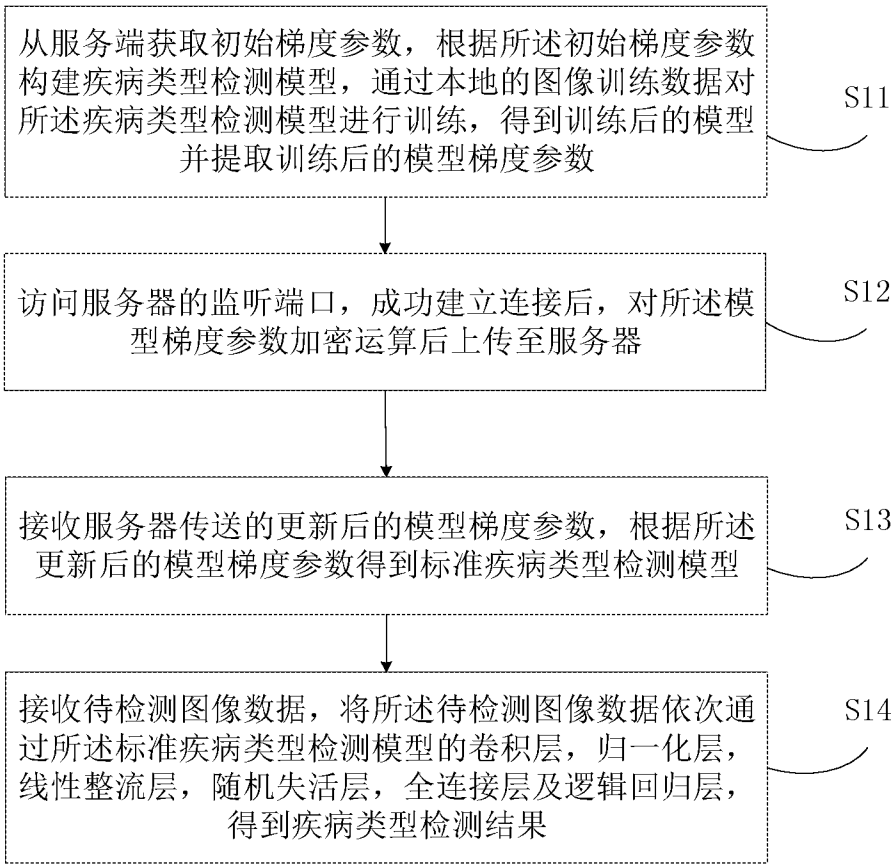
从服务端获取初始梯度参数，根据所述初始梯度参数构建疾病类型检测模型，通过本地的图像训练数据对所述疾病类型检测模型进行训练，得到训练后的模型并提取训练后的模型梯度参数
S11
访问服务器的监听端口，成功建立连接后，对所述模型梯度参数加密运算后上传至服务器
S12
接收服务器传送的更新后的模型梯度参数，根据所述更新后的模型梯度参数得到标准疾病类型检测模型
S13
接收待检测图像数据，将所述待检测图像数据依次通过所述标准疾病类型检测模型的卷积层，归一化层，线性整流层，随机失活层，全连接层及逻辑回归层，得到疾病类型检测结果
S14

图 1

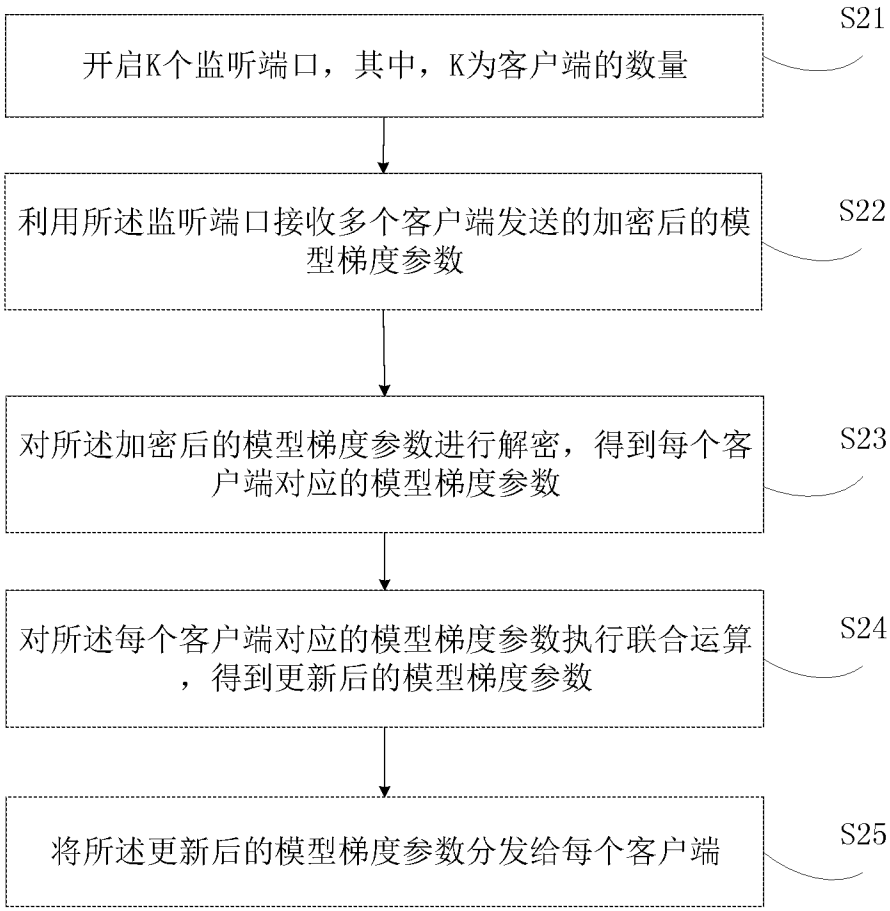
开启K个监听端口，其中，K为客户端的数量
S21
利用所述监听端口接收多个客户端发送的加密后的模型梯度参数
S22
对所述加密后的模型梯度参数进行解密，得到每个客户端对应的模型梯度参数
S23
对所述每个客户端对应的模型梯度参数执行联合运算，得到更新后的模型梯度参数
S24
将所述更新后的模型梯度参数分发给每个客户端
S25

图 2

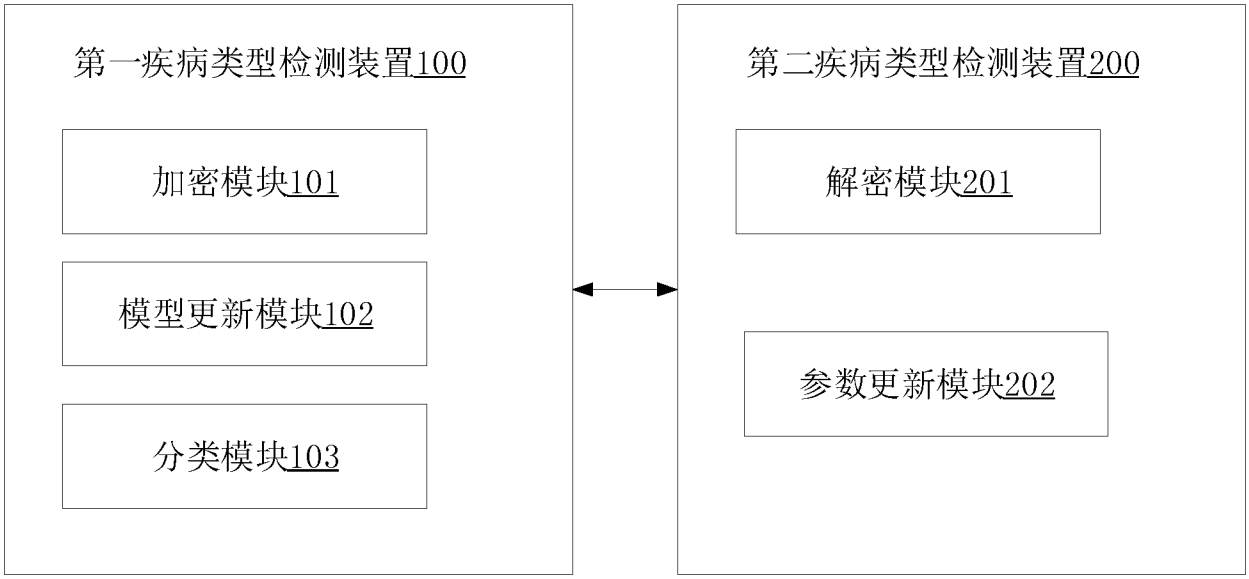
第一疾病类型检测装置100
加密模块101
模型更新模块102
分类模块103
第二疾病类型检测装置200
解密模块201
参数更新模块202

图 3


电子设备 1
处理器 10
存储器 11
疾病类型检测程序 12

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/131987

A. CLASSIFICATION OF SUBJECT MATTER

G16H 50/70(2018.01)i; G16H 50/50(2018.01)i; G16H 50/20(2018.01)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)

G16H

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)

CNPAT, CNKI, WPI, EPODOC: 病, 模型, 训练, 梯度, 更新, 调整, 修正, 加密, 解密, 服务器, 服务端, 参数, 参量, 数据, disease, model, training, grad+, update, adjustment, revis+, encrypt+, decrypt+, serv+, parameter, data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111180061 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 19 May 2020 (2020-05-19) claims 1-6, description paragraphs [0026]-[0060]	1-20
A	CN 109545385 A (ZHOU, Liguang) 29 March 2019 (2019-03-29) entire document	1-20
A	US 2019324856 A1 (EMC IP HOLDING COMPANY LLC.) 24 October 2019 (2019-10-24) 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	Date of mailing of the international search report
25 June 2021	**21 July 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/131987

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111180061 A	19 May 2020	None	
CN 109545385 A	29 March 2019	None	
US 2019324856 A1	24 October 2019	None	

国际检索报告

国际申请号
PCT/CN2020/131987

A. 主题的分类

G16H 50/70(2018.01)i; G16H 50/50(2018.01)i; G16H 50/20(2018.01)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)

G16H

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）)

CNPAT, CNKI, WPI, EPODOC: 病，模型，训练，梯度，更新，调整，修正，加密，解密，服务器，服务端，参数，参量，数据，disease, model, training, grad+, update, adjustment, revis+, encrypt+, decrypt+, serv+, parameter, data

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
X	CN 111180061 A (广东工业大学) 2020年 5月 19日 (2020-05-19) 权利要求1-6，说明书第[0026]-[0060]段	1-20
A	CN 109545385 A (周立广) 2019年 3月 29日 (2019-03-29) 全文	1-20
A	US 2019324856 A1 (EMC IP HOLDING COMPANY LLC) 2019年 10月 24日 (2019-10-24) 全文	1-20

☐ 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
“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 25日	2021年 7月 21日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 王怡轩 电话号码 86-10-53961621

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/131987

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 111180061 A	2020年 5月 19日	无	
CN 109545385 A	2019年 3月 29日	无	
US 2019324856 A1	2019年 10月 24日	无	