说　明　书　摘　要

本发明公开了一种分布式医疗影像处理模型的训练方法及应用方法，包括：收集来自多个医疗中心经过标注的医学影像数据，对医疗影像数据进行数据预处理，得到各个医疗中心的局部数据集，根据局部数据集生成全局数据集；根据局部数据集生成局部对抗影像样本；基于变分贝叶斯框架构建初始分布式医疗影像处理模型；采用局部数据集和局部对抗影像样本对局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个局部模型进行全局聚合处理，形成全局模型；当各个局部模型的局部损失函数收敛或者迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型。本发明实施例能够训练分散大规模数据，提高了模型准确率模型的鲁棒性，可广泛应用于图像处理技术领域。

摘　要　附　图

指定图 1 为摘要附图

权　利　要　求　书

1．一种分布式医疗影像处理模型的训练方法，其特征在于，包括：

收集来自多个医疗中心经过标注的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集；

根据所述局部数据集生成局部对抗影像样本；

基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型；

采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型；

当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

2．根据权利要求 1 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述对所述医疗影像数据进行数据预处理，得到局部数据集，根据所述局部数据集生成全局数据集，包括：

对若干个医疗中心的医疗影像数据进行随机组合的形态学操作，得到局部数据集；其中，所述形态学操作包括以下至少之一：开放操作、关闭操作、随机膨胀操作或者随机侵蚀操作；

从所述局部数据集中确定若干样本，生成全局数据集；

对所述局部数据集和所述全局数据集进行数据增强。

3．根据权利要求 1 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述根据所述局部数据集生成局部对抗影像样本，包括：

配置扰动项；

对所述局部数据集中添加所述扰动项，生成第一对抗影像样本；

根据所述第一对抗影像样本对所述扰动项进行迭代处理；

采用梯度下降算法，以小步梯度下降的方式，按照预设的时间间隔重复执行所述对所述局部数据集添加所述扰动项，生成第一对抗影像样本的步骤，直至迭代次数达到预设的第一迭代次数阈值，得到最优扰动值；

对所述局部数据集添加所述最优扰动值，生成局部对抗影像样本。

4．根据权利要求 3 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述根据所述全局数据集生成全局对抗影像样本，所述对所述局部数据集中添加所述扰动项，

批注 [JQ1]:
基于发明人的补充，进一步理解方案并进行了修改，请审阅。

生成第一对抗影像样本的计算公式为：

$$x' = x + \varepsilon \cdot sign\left(\nabla_x L(\theta, x, y)\right)$$

其中，x'表示第一对抗影像样本，ε表示一个趋近于 0 的正数；sign( )表示符号函数；L( )表示原模型的损失函数，∇_x即表示损失函数关于输入 x 的梯度计算；x 表示原始样本，y 表示原始样本经过模型运算之后的样本输出。

5．根据权利要求 1 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述基于变分贝叶斯框架构建初始分布式医疗影像处理模型的步骤中，包括以下构建局部模型的步骤：

构建分割网络，用于生成通用数据的概率分布预测；其中，所述分割网络是一个卷积神经网络；

构建先验编码器和后验编码器；其中，所述先验编码器用于计算全局模型的全局损失函数；所述后验编码器用于计算局部模型的局部损失函数；

构建分布自适应网络，用于输出自适应矩阵以计算最终预测结果。

6．根据权利要求 1 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，包括：

基于梯度下降算法和对抗损失配置局部损失函数；

将所述局部训练集和所述局部对抗影像样本结合作为训练集；

采用所述训练集对所述分布式医疗影像处理模型进行局部训练，得到模型训练结果；

基于所述局部损失函数，根据所述模型训练结果计算损失值。

7．根据权利要求 6 所述的一种分布式医疗影像处理模型的训练方法，其特征在于，所述局部损失函数的表达式为：

$$loss_{new} = l_{CE} + l_{NR} + \alpha l_{TR} + \beta l_{KL} + \lambda l_{ADV}$$

其中，l_{CE}是交叉熵损失；l_{NR}是非重叠损失；l_{TR}是约束值；l_{KL}表示先验分布和后验分布之间的差异；α、β和λ均为超参数；l_{ADV}是对抗生成器的损失函数。

8．一种分布式医疗影像处理模型的应用方法，其特征在于，包括：

获取待处理医疗影像；

将所述待处理医疗影像输入采用如权利要求 1 所述的训练方法训练得到的目标分布式医疗影像处理模型进行分割预测处理，得到影像处理结果。

9．一种分布式医疗影像处理模型的训练系统，其特征在于，包括：

第一模块，用于收集来自多个医疗中心经过标注的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据

集；

第二模块，用于根据所述局部数据集生成局部对抗影像样本；

第三模块，用于基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型；

第四模块，用于采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型；还用于当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

10．一种电子设备，其特征在于，包括处理器以及存储器；

所述存储器用于存储程序；

所述处理器执行所述程序实现如权利要求 1 至 8 中任一项所述的方法。

说　明　书

一种分布式医疗影像处理模型的训练方法及应用方法

技术领域

本发明涉及图像处理技术领域，尤其涉及一种分布式医疗影像处理模型的训练方法及应用方法。

背景技术

近年来，随着医学影像诊断性能要求不断提升和深度学习的发展，大量针对医疗影像的AI辅助诊断系统都能提高诊断的准确性，并一定程度上保护患者的隐私。但它们同时存在以下缺点：

1.各医院医疗数据分散，共享程度不高，使大规模数据集中训练寸步难行。AI达到高准确率需要大量数据，但实际上可用于训练的医疗数据非常分散，且城市和边远地区的数据量不平衡。

2.模型鲁棒性不足，临床信任度低，模型实际部署难以推进。现有模型往往基于各类深度神经网络实现，而研究表明，这些模型在精心设计的对抗扰动下会暴露弱点。边远地区采集的数据质量问题和潜在的对抗攻击更难察觉，使得模型鲁棒性能和泛化性能未能达到要求。

3.模型的可解释性不足，无法确定模型是否依照需求进行训练。一些AI算法模型在做出预测或诊断时，往往缺乏足够的解释性，不能生成医生可以解释的合理预测。这使得医生难以理解模型的决策过程，从而对其结果产生怀疑或不信任。

发明内容

本发明旨在至少在一定程度上解决相关技术中的技术问题之一。为此，本发明提出一种适用于训练分散大规模数据的、能够提高模型准确率的分布式医疗影像处理模型的训练方法及应用方法。

一方面，本发明实施例提供了一种分布式医疗影像处理模型的训练方法，包括：

收集来自多个医疗中心经过标注的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集；

根据所述局部数据集生成局部对抗影像样本；

基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型；

采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型；

当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

可选地，所述对所述医疗影像数据进行数据预处理，得到局部数据集，根据所述局部数据集生成全局数据集，包括：

对若干个医疗中心的医疗影像数据进行随机组合的形态学操作，得到局部数据集；其中，所述形态学操作包括以下至少之一：开放操作、关闭操作、随机膨胀操作或者随机侵蚀操作；

从所述局部数据集中确定若干样本，生成全局数据集；

对所述局部数据集和所述全局数据集进行数据增强。

可选地，所述根据所述局部数据集生成局部对抗影像样本，包括：

配置扰动项；

对所述局部数据集中添加所述扰动项，生成第一对抗影像样本；

根据所述第一对抗影像样本对所述扰动项进行迭代处理；

采用梯度下降算法，以小步梯度下降的方式，按照预设的时间间隔重复执行所述对所述局部数据集添加所述扰动项，生成第一对抗影像样本的步骤，直至迭代次数达到预设的第一迭代次数阈值，得到最优扰动值；

对所述局部数据集添加所述最优扰动值，生成局部对抗影像样本。

可选地，所述根据所述全局数据集生成全局对抗影像样本，所述对所述局部数据集中添加所述扰动项，生成第一对抗影像样本的计算公式为：

$$x' = x + \varepsilon \cdot sign\left(\nabla_x L(\theta, x, y)\right)$$

其中，x'表示第一对抗影像样本，ε表示一个趋近于 0 的正数；sign( )表示符号函数；L( )表示原模型的损失函数，∇_x即表示损失函数关于输入 x 的梯度计算；x 表示原始样本，y 表示原始样本经过模型运算之后的样本输出。

可选地，所述基于变分贝叶斯框架构建初始分布式医疗影像处理模型的步骤中，包括以下构建局部模型的步骤：

构建分割网络，用于生成通用数据的概率分布预测；其中，所述分割网络是一个卷积神经网络；

构建先验编码器和后验编码器；其中，所述先验编码器用于计算全局模型的全局损失函数；所述后验编码器用于计算局部模型的局部损失函数；

构建分布自适应网络，用于输出自适应矩阵以计算最终预测结果。

可选地，所述采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，包括：

基于梯度下降算法和对抗损失配置局部损失函数；

将所述局部训练集和所述局部对抗影像样本结合作为训练集；

采用所述训练集对所述分布式医疗影像处理模型进行局部训练，得到模型训练结果；

基于所述局部损失函数，根据所述模型训练结果计算损失值。

可选地，所述局部损失函数的表达式为：

$$loss_{new} = l_{CE} + l_{NR} + \alpha l_{TR} + \beta l_{KL} + \lambda l_{ADV}$$

其中，l_{CE}是交叉熵损失；l_{NR}是非重叠损失；l_{TR}是约束值；l_{KL}表示先验分布和后验分布之间的差异；α、β和λ均为超参数；l_{ADV}是对抗生成器的损失函数。

另一方面，本发明实施例还提供了一种分布式医疗影像处理模型的训练系统，包括：

第一模块，用于收集来自多个医疗中心经过标注的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集；

第二模块，用于根据所述局部数据集生成局部对抗影像样本；

第三模块，用于基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型；

第四模块，用于采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型；还用于当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

另一方面，本发明实施例还提供了一种电子设备，包括：处理器以及存储器；存储器用于存储程序；处理器执行程序实现如上所述的方法。

另一方面，本发明实施例还提供了一种计算机存储介质，其中存储有处理器可执行的程序，处理器可执行的程序在由处理器执行时用于实现如上所述的方法。

本发明实施例具有如下有益效果：能够基于不同医疗中心各自的数据训练一个通用的全局模型，并且通过训练各医疗中心的局部模型进行全局模型预测结果的修正，适用于训练分散大规模数据的、能够提高模型准确率；同时由于不需要进行数据汇总，还能够提升训练过程中的数据隐私安全性。通过加入对抗影像样本的对抗训练，还能够提升分布式医疗影像处

理模型的鲁棒性。

附图说明

附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

图 1 是本发明实施例提供的分布式医疗影像处理模型的训练方法的步骤图；

图 2 是本发明实施例提供的分布式医疗影像处理模型的训练方法流程示意图；

图 3 是本发明实施例提供的分布式医疗影像处理模型的模型结构示意图；

图 4 是本发明实施例提供的分布式医疗影像处理模型的应用方法的步骤图；

图 5 是本发明实施例提供的分布式医疗影像处理模型的训练系统结构示意图；

图 6 是本发明实施例提供的电子设备结构示意图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

需要说明的是，虽然在系统示意图中进行了功能模块划分，在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于系统中的模块划分，或流程图中的顺序执行所示出或描述的步骤。说明书和权利要求书及上述附图中的术语“第一/S100”、“第二/S200”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

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发明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。

在进行介绍之前，首先介绍鲁棒优化的含义：

鲁棒优化（Robust Optimization）：鲁棒优化是一个目的是求出适用于所有约束条件，使得在最坏情况下的目标函数最优的一种规划方法。数学规划需要输入数据在准确知道的情况下建立模型，并利用已有的数学规划方法得到最优解，这些方法没有考虑到数据不确定性的影响。鲁棒优化针对规划中出现的不确定性变量建立不确定集合，利用相关的优化理论如对偶理论对其进行转化，使得不确定性问题转化为可解的鲁棒对应问题，并给出鲁棒最优解。

参照图 1 和图 2，该方法包括以下步骤：

S100、收集多个医疗中心的医学影像数据，对所述医疗影像数据进行数据预处理，得到

各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集。

可选地，所述步骤 S100 包括以下步骤 S110~S130。

S110、对若干个医疗中心的医疗影像数据进行随机组合的形态学操作，得到局部数据集；其中，所述形态学操作包括以下至少之一：开放操作、关闭操作、随机膨胀操作或者随机侵蚀操作。

侵蚀操作是通过使用结构元素（也称为核）来缩小图像中的物体。该操作将结构元素与原图像进行卷积，并将卷积后的图像像素值设为结构元素内的最小像素值。侵蚀操作可以用于去除图像中的噪声、缩小物体的大小、分离相连的物体或者检测边界。它通过消除物体的边缘来使物体变细或缩小。

而膨胀操作与侵蚀操作相反，通过使用结构元素来扩大图像中的物体。该操作卷积后将像素值设为结构元素内的最大像素值。膨胀操作通过在物体边缘扩展像素来使物体变粗或扩大，可以用于连接不完整的物体或者增大物体的大小。

基于此，本发明实施例对医疗影像数据进行的形态学操作可以为：

开放操作：一种先由侵蚀操作而后再接上膨胀操作的组合。它主要用于去除图像中的小噪点或细小的不连续区域，并且可以平滑图像的边界。

关闭操作：一种先由膨胀操作而后再接上侵蚀操作的组合。它主要用于填充图像中的小孔洞或连接不完整的物体。

随机膨胀操作：一种对膨胀操作引入随机性的变体。通常的膨胀操作会使用固定大小的结构元素来扩展图像中的物体，而随机膨胀操作会随机选择结构元素的大小和形状来进行膨胀，这样可以在一定程度上模拟物体的自然形状变化或噪声的影响。随机侵蚀操作与随机膨胀操作类似，是对侵蚀操作引入随机性的变体，两者功能也相似。

可以从以上至少之一的形态学操作中随机组合，并根据随机组合的操作对医疗影像数据进行形态学处理，以模拟不同医疗中心之间标注常见的偏差和变化。

S120、从所述局部数据集中确定若干样本，生成全局数据集。

每个局部数据集都对应着一个医疗中心，数据量可能非常庞大，因此本发明实施例从局部数据集选取确定若干样本，形成全局数据集，用于验证全局模型的性能。

S130、对所述局部数据集和所述全局数据集进行数据增强。

在一些实施例中，可以先对所有处理后的医学影像数据重新采样至一定的分辨率，例如 0.6×0.6×1.25mm，并以待分割区域为中心裁剪为适宜的尺寸，例如可以为 256×256；再对裁剪后的影像数据进行 Z-score 归一化处理。而在训练过程中本发明实施例采用随机旋转、翻转、弹性变形和添加高斯噪声等方法对数据进行数据增强。

S200、根据所述局部数据集生成局部对抗影像样本。

具体而言，步骤 S200 可以包括以下步骤 S210~S240。

S210、配置扰动项。

在一些实施例中，配置的扰动项可以为：

$$\eta = \varepsilon \cdot sign\left(\nabla_x L(\theta, x, y)\right) \tag{1}$$

其中，η 即为添加的扰动项。ε 表示一个趋近于 0 的正数；sign( )表示符号函数，当自变量输入≥0 时，函数输出为 1，否则输出为-1；L( )表示原模型的损失函数，∇_x 即表示损失函数关于输入的原始样本x的梯度计算。

为了让后续生成的对抗影像样本不被机器所识别，η 应该足够小，这里使用无穷阶范数来表述 η 足够小这一限制，如下式所示：

$$\left|\left|\eta\right|\right|_\infty < \varepsilon \tag{2}$$

S220、对所述局部数据集中添加所述扰动项，生成第一对抗影像样本。

设x是原始样本，即各医疗中心的原始影像数据；x' 是第一对抗影像样本，则生成第一对抗影像样本的计算公式为：

$$x' = x + \varepsilon \cdot sign\left(\nabla_x L(\theta, x, y)\right) \tag{3}$$

步骤 S210~S220 生成对抗影像样本的方式可以解释为内部期望最大化的单步攻击，但从鲁棒性的提升角度来说，多步攻击会更加有效提升模型的鲁棒性，因为本发明实施例后续所构建的分布式训练框架是复杂的非线性映射。

因此，本发明实施例在样本训练中添加对抗样本之后，采用 PGD 算法，以小步梯度下降的方式来探索损失函数的大部分情况，以一个拟定的时间间隔为单位逐步多次迭代，以找到最合适的对抗样本。

PGD（Projected Gradient Descent）是在对抗训练中的一种梯度下降算法。在深度学习中，神经网络在精心训练后，其分类准确性可以非常出色，但其的鲁棒性却可能很差，可能会轻易被对抗攻击打破。即通过对输入图片进行微小扰动，就可以在几乎肉眼看不出差距的前提下，让神经网络的分类准确率大幅下降。对抗训练算法采用小步多走的策略进行对抗，旨在找到一个最优解，使得模型能够在对抗环境下更加稳健。其核心思想是通过在每个训练步骤中对输入数据添加一小部分扰动，以使其对原始模型产生最大的干扰或误判，这些扰动是基于模型的梯度计算而产生的。PGD 算法通过迭代地更新扰动来最大化对抗性的影响，目标是在训练过程中增加模型对于对抗性样本的鲁棒性，从而提高模型的安全性和可信度。通过不断地使模型面对对抗性样本并进行优化训练，PGD 算法可以帮助模型更好地识别和处理具

有一定扰动的输入数据，使模型更好地应对具有一定攻击性的输入数据。

于是得到步骤 S230~S240。

S230、根据所述第一对抗影像样本对所述扰动项进行迭代处理。

本发明实施例的扰动迭代表达式为：

$$x_{t+1} = \prod_{x+S}\left\{x_t + \varepsilon \cdot sign\left(\nabla_{x_t} L(\theta, x_t, y_t)\right)\right\} \tag{4}$$

其中，$t+1$ 时刻的输入根据 t 时刻的输入以及 $t+1$ 时刻与 t 时刻之间的损失函数关于 x 的梯度 ∇_{x_t} 求出。$\prod_{x+S}$ 的意思是：先计算原始影像样本的损失梯度得到对抗影像样本，对抗影像样本减去原始影像样本得到扰动值；如果扰动值超过一定的范围，就要映射回规定的范围 S 内。经过多步迭代之后对抗影像样本 x' 的生成就可以达到最优解，也就是达到最强的攻击效果，有利于提高模型训练后的鲁棒性。

S240、采用梯度下降算法，以小步梯度下降的方式，按照预设的时间间隔重复执行所述对所述局部数据集添加所述扰动项，生成第一对抗影像样本的步骤，直至迭代次数达到预设的迭代阈值，得到最优扰动值。

S250、对所述局部数据集添加所述最优扰动值，生成局部对抗影像样本。

S300、基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型。

数据非独立同分布（Non-identically Distributed Data）指的是在一个系统或数据集中的数据并不满足相同的概率分布或数据生成过程。这意味着不同的数据样本之间可能存在不同的概率分布特征，例如数据的统计特性、分布形态、数据生成方式等可能不同。这对于机器学习和数据分析等任务可能带来挑战，因为传统的基于独立同分布数据假设的方法可能不再适用，需要考虑数据的非独立同分布性。

解耦预测（Decoupling prediction）旨在将复杂的预测问题分解为多个子问题，并独立地对每个子问题进行建模和预测。其目的是通过解除各个子问题之间的依赖性，提高预测模型的灵活性和整体性能。在解耦预测中，首先需要定义多个相关但相互独立的子问题，然后针对每个子问题建立独立的模型。每个模型可以使用不同的机器学习算法、特征选择方法或参数设置，以最好地，好地解决特定的子问题。这些模型可以并行训练，互不干扰。在预测阶段，解耦预测方法会将新的输入样本传递给每个子模型，分别生成一个或多个预测结果，最后将这些预测结果组合以产生最终的整体预测。解耦预测的优势在于，它能够有效解决复杂问题中的耦合和依赖性，通过将问题分解为独立的子问题，可以提高模型的可解释性和稳定

性，并且更容易地调整和优化每个子模型。

本发明实施例基于变分贝叶斯框架构建了一种分布式医疗影像处理模型，该模型是一种分布式学习解耦预测模型，它连通了全局方法和个性化方法，可以用于非 IDD（即 NDD，不满足独立同分布假设）的医疗影像数据的分割。变分贝叶斯框架通过将变分散度最小化来衡量拟合分布与真实后验分布之间的差异；变分散度是两个概率分布之间的距离度量，常用的变分散度包括 KL 散度和海森斯坦距离等；为了最小化变分散度，我们定义一个优化问题，通过调整变分分布的参数来使变分散度最小化，这个优化问题通常可以通过迭代算法来求解。全局方法是指在分布式学习中，将所有医疗中心的数据汇集到一起，训练一个全局模型，然后将该模型应用于所有医疗中心的医疗影像处理；个性化方法则指的是在每个医疗中心训练一个本地模型，该模型只使用该医疗中心的本地数据进行训练，并且只应用于该医疗中心的图像处理。本发明实施例的分布式医疗影像处理模型具有分布条件自适应网络，能够在训练时将预测样本和与该预测样本相对应的标注进行解耦，在测试时根据局部分布情况进行自适应预测。

批注 [JQ2]: 请简要介绍“变分贝叶斯框架”。

基于此，参照图 3，本发明实施例构建的初始分布式医疗影像处理模型可以包括与医疗中心一一对应的若干个局部模型，而全局模型在模型的训练过程中通过全局聚合操作产生。图 3 中，虚线左侧为学习任务，右侧为局部模型的学习框架。

在图 5 的学习任务中，任务 1 是对于来自多医疗中心的非 IDD 数据，聚合训练一个全局模型$f(\theta)$；任务 2 是寻找每个医疗中心的局部模型。本发明实施例的全局模型实现对通用数据分布$p(x,y)$的统一分割，即对于并未用于训练的医疗中心的医疗影像也能被有效分割；另一方面，局部模型能够修改全局模型的预测结果，使得该预测结果更倾向于局部分布，例如第 k 个中心的$p(x_k,y_k)$。

局部模型的构建步骤可以包括以下步骤 a~c。

a) 构建分割网络，用于生成通用数据的概率分布预测；其中，分割网络是一个卷积神经网络。

分割网络用于生成通用数据的预测。它是一个卷积神经网络，它将x作为输入，输出一个概率分布$p(y|x)$。该概率分布表示给定输入x时，输出y出现的概率分布。

在本发明实施例中，通用数据是可以应用于不同本地模型以及全局模型训练的数据，这些数据具有广泛的适用性，通常是由对多个中心里的某个医疗中心数据进行选取形成的，即通用数据是从某个医疗中心抽取出来的数据。

卷积神经网络（Convolutional Neural Network）卷积神经网络是一种具有局部连接、权值共享等特点的深层前馈神经网络，擅长处理图像特别是图像识别等相关机器学习问题，比如

图像分类、目标检测、图像分割等各种视觉任务中都有显著的提升效果，是目前应用最广泛的模型之一。其具有表征学习能力，能够按其阶层结构对输入信息进行平移不变分类，可以进行监督学习和非监督学习，其隐含层内的卷积核参数共享和层间连接的稀疏性使得卷积神经网络能够以较小的计算量对格点化特征，例如像素和音频进行学习、有稳定的效果且对数据没有额外的特征工程要求。

b) 构建先验编码器和后验编码器，其中，所述先验编码器用于计算全局模型的全局损失函数；所述后验编码器用于计算局部模型的局部损失函数。

在本发明实施例中，联合数据是指来自不同中心的数据集合。这些数据分散存储在不同的位置，可能无法集中在一个地方进行处理，因此将这类数据特称为联合数据，即联合数据是指所有医疗中心的数据。

先验编码器和后验编码器可以通过潜在表示 z_k 对联合数据分布 $p(x_k, y_k)$ 和 $q(x_k, y_k)$，即图中的 p_{ψ_k} 和 q_{φ_k} 进行建模。这两种编码器是神经网络的一种，功能都是将输入 x 和输出 y 作为输入，输出一个潜在变量 z；该潜在变量 z 表示输入 x 和输出 y 之间的关系。先验编码器与后验编码器不同的是，前者的输出结果用于计算全局模型的损失函数，后者的结果用于计算个性化模型（即局部模型）的损失函数。

c) 构建分布自适应网络模型，用于输出自适应矩阵以计算最终预测结果。

以上步骤 a 和步骤 b 的输出结果均可用作 DA 网络（分布自适应网络）的输入。根据这些新的参数和局部数据的分布，DA 网络可以输出自适应矩阵 W_k。最终，对局部数据的预测是通过自适应矩阵 W_k 与全局数据的预测相乘得到的。

S400、采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型。

本发明实施例基于群体学习对分布式医疗影像处理模型进行训练，包括根据一定周期而进行的模型全局聚合和局部模型训练。

群体学习（Swarm Learning）：群体学习是一种分布式的、去中心化的机器学习方法，通过边缘设备之间的协作和信息共享来完成模型的训练和预测任务，具有保护隐私和避免数据集中化的优势。在群体学习中，每个边缘设备都是一个学习节点，拥有自己的数据集和计算能力。首先，所有设备在本地独立地进行模型的初始化和训练；然后，各边缘设备通过网络交流彼此的模型参数，并结合本地的数据进行合并更新。这种参数的交流和合并可以通过加密和去隐私化技术来保护数据的安全性，这使得模型能够在设备之间进行分布式的学习，避免了数据集中在一个地方的问题，并且由于数据不需要离开设备进行集中存储和处理，所以群体学习拥有在充分利用各个节点数据集的基础上保护用户隐私的优势。

批注 [JQ3]: 请问本发明提出的“分布自适应网络”是怎样的结构？

批注 [24R3]: 它的结构由一个多层感知器（Multi-Layer Perceptron, MLP）组成，它的输入是先验编码器和后验编码器的输出结果，以及分割网络生成的通用数据的预测结果。MLP 的输出是自适应矩阵 W，用于将通用数据的预测结果适应到本地数据的分布上。W 是根据本地数据的分布和通用数据的预测结果之间的关系来计算的。

在全局聚合中，每个医疗中心 k 从其他医疗中心收集全局模型的局部更新参数$\{(\theta_k)\}_{k=1}^{K}$，并从每个医疗中心的训练规模(n_k)加权进行模型聚合，全局聚合的具体表达式为：

$$\theta = \sum_{k=1}^{K}\left(\frac{n_k}{N}\theta_k\right), N = \sum_{k=1}^{K}(n_k) \tag{5}$$

其中，$\{\theta_k^p\}$表示局部模型，在全局聚合的阶段保持在局部中。而在局部训练时，每个医疗中心训练自己的局部模型，此时全局模型初始化为聚合结果θ。

而步骤 S400 中，采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练的步骤可以包括以下步骤 S410~S440。

S410、基于梯度下降算法和对抗损失配置局部损失函数。

可以预先确定加入对抗训练算法时的传统损失函数：

$$loss = l_{CE} + l_{NR} + \alpha l_{TR} + \beta l_{KL} \tag{6}$$

其中，l_{CE}是交叉熵损失，被应用于训练分割网络和 DA 网络，用于计算两个网络的输出的乘积与标签之间的交叉熵损失。

l_{NR}是非重叠损失，作用在局部模型：在每个医疗中心的数据集中，将分割偏差视为噪声，并将其视为伪标签添加到训练数据中，这样可以增加训练数据量，并平衡噪声容忍度和收敛速度，从而提高局部模型在多个中心数据集上的泛化能力和鲁棒性。

l_{TR}用于约束自适应矩阵W_k的大小和稀疏性，以避免模型过拟合，从而使全局模型更加符合局部数据集的分布特征。

l_{KL}用于学习先验分布$p(z)$和后验分布$q(z|(x_k, y_k))$之间的差异，以便更好地建模数据分布。

而α和β是超参数，用于平衡适应矩阵正则化和KL散度损失对于$loss$的影响。

进一步地，基于添加的 PGD 算法对损失函数 loss 进行优化，以进一步评估模型的鲁棒性能。上述优化方法可以为：使用对抗生成网络（GAN）中的判别器损失函数l_{ADV}来鼓励模型学习提升鲁棒性的能力，本发明实施例假设$D(x)$表示判别器网络对输入x的输出，则对抗损失可以确定为：

$$l_{ADV} = -\log\left(D(x')\right) \tag{7}$$

通过最小化l_{ADV}，可以使得对抗样本更难以被判别器网络区分出来，从而提高模型的鲁棒性。

基于此，优化后的损失函数$loss_{new}$的表达式为：

$$loss_{new} = l_{CE} + l_{NR} + \alpha l_{TR} + \beta l_{KL} + \lambda l_{ADV} \tag{8}$$

其中 λ 是超参数，用于平衡对抗损失和其他损失之间的权重。

S420、将所述局部训练集和所述局部对抗影像样本结合作为训练集。

S430、采用所述训练集对所述分布式医疗影像处理模型进行局部训练，得到模型训练结果。

在进行模型训练之前，除了正则化参数之外，还需要设置其他一些必要的超参数使得模型能够运行，设置的超参数例如：迭代次数、学习率、扰动梯度下降步长。

S440、基于所述局部损失函数，根据所述模型训练结果计算损失值。

S500、当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

根据本发明实施例的添加模型鲁棒性提升策略的分布式训练框架以及优化后的损失函数，可以对该框架性能进行评估；在一些实施例中，将相同的样本输入本发明实施例的模型和其他传统框架模型，分别在任务 1 和任务 2 中进行评估比较。

本发明训练方法训练得到的分布式医疗影像处理模型具体可以应用于各种医疗影像处理场景，例如分割医疗影像、根据医疗影像识别目标对象等，具体可以根据实际需求输入的不同训练数据集和训练任务而确定。

本发明实施例具体以下有益效果：

1、本发明实施例的训练方法能够基于不同医疗中心各自的数据训练一个通用的全局模型，并且通过训练各医疗中心的局部模型进行全局模型预测结果的修正，适用于训练分散大规模数据的、能够提高模型准确率；同时由于不需要进行数据汇总，还能够提升训练过程中的数据隐私安全性。

2、本发明实施例的训练方法有利于打破医院间的数据孤岛，促进数据的协作。通过整合多个边远地区医院的医学影像数据，能够更全面地进行病理诊断，提高医学影像辅助诊断平台在病理诊断方面的可靠性和可应用性。这为患者的转诊提供了方便，使得医疗资源能够更加合理地分配和利用。

3、提升了鲁棒性和可靠性：通过群体学习技术和对抗训练框架，提升了医疗影像处理模型的鲁棒性和临床信任度。群体学习技术允许多个节点在本地学习后将知识进行聚合和共享，扩大了模型训练的数据规模，提高了模型的鲁棒性和可靠性。对抗训练框架则进一步提升了模型的鲁棒性和泛化性能。

4、个性化和泛化性能的平衡：本发明实施例考虑了不同边远地区人群的健康状况具有地方特殊性。通过数据预处理过程中随机组合形态学操作等方法，本发明实施例平衡了模型对泛化性和个性化的要求，有利于训练后模型在不同地区的适用性和准确性。

下面结合具体用于对胸部磁共振成像（MRI）医学影像进行处理的应用场景进一步介绍本发明实施例的训练方法的实例：

（1）收集多个医疗中心的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集。

首先从不同医疗中心收集对胸部磁共振成像（MRI）的医学影像，这些影像需要由医疗专家标注好左心房分割区域。为便于理解，示例性地，本发明实施例以收集三个医疗中心的MRI医学影像数据为例，在实际情况中，医疗中心可以为若干个。

将其中两个中心命名为中心A和中心B，对于中心A和B，选择15个样本进行模型训练，选择5个样本作为局部的测试数据。对于其中一个中心的数据集，随机选择两组，每组35个样本，分别作为中心C和中心D，它们的训练和测试比例分割为6:1。

在本发明实施例中，为了模拟不同中心之间的标注常见的偏差和变化，对C中心的训练标签进行了形态学操作，即对中心C的训练标签进行了开放和随机侵蚀操作；对中心D的训练标签进行了封闭和随机扩张操作；对于C、D中心的局部测试数据进行了开放和关闭操作。

此外，示例性地，本发明实施例从每个医疗中心分别挑选了10个病例样本数据，生成了一个全局的数据测试集。此处的局部测试数据用于验证个性化方法的性能；全局的数据测试集用于验证全局模型的性能。

接着将所有MRI医学影像数据重新采样至0.6×0.6×1.25mm的分辨率，并以心脏区域为中心裁剪为256×256的尺寸，再进行Z-score归一化处理。而在训练过程中应用随机旋转、翻转、弹性变形和添加高斯噪声等方法对数据进行数据增强。

需要说明的是，以上样本数量仅作为示例，本发明实施例不对此进行限制。

（2）根据所述局部数据集生成局部对抗影像样本。

采用步骤S200的方法生成，此处不再赘述。

（3）构建分布式医疗影像处理模型；其中，所述医疗影像处理模型包括一个全局模型、若干个与所述医疗中心一一对应的局部模型和一个基于变分贝叶斯框架构建的分布式学习解耦预测模型。

在本实例中，基于变分贝叶斯框架搭建用于左心房分割的分布式学习框架，它作为桥梁连通了全局方法和个性化方法，可以用于非IDD（即不满足独立同分布假设）的MRI影像数据的分割。全局方法是指在分布式学习中，将所有中心的数据汇集到一起，训练一个全局模型，然后将该模型应用于所有医疗中心的测试数据；个性化方法则是指在每个医疗中心训练一个本地模型，该模型只使用本地数据进行训练，并且只应用于该医疗中心的测试数据。

本发明实施例还提出了一种分布条件自适应网络，在训练时将预测样本和与它相对应的标注进行解耦，在测试时根据局部分布情况进行自适应的预测。

（4）通过所述分布式学习解耦预测模型将预测样本与标注进行解耦，采用所述全局数据集对所述全局模型进行全局聚合处理。

具体地，采用步骤 S400 进行全局聚合处理。

（5）采用所述局部数据集和所述局部对抗影像样本对所述分布式医疗影像处理模型进行局部训练，当损失函数收敛或者达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型。

具体地，采用步骤 S400~500 进行模型训练。

另一方面，参照图 4，本发明实施例提供了一种分布式医疗影像处理模型的应用方法，包括以下步骤 S600~S700。

S600、获取待处理医疗影像。

S700、将所述待处理医疗影像输入采用如权利要求 1 所述的训练方法训练得到的目标分布式医疗影像处理模型进行分割预测处理，得到影像处理结果。

具体地，所得到的影像结果根据实际需求训练得到的目标分布式医疗影像处理模型确定。

另一方面，如图 5 所示，本发明实施例提供了一种分布式医疗影像处理模型的训练系统，包括：

第一模块，用于收集来自多个医疗中心经过标注的医学影像数据，对所述医疗影像数据进行数据预处理，得到各个所述医疗中心的局部数据集，根据所述局部数据集生成全局数据集；

第二模块，用于根据所述局部数据集生成局部对抗影像样本；

第三模块，用于基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，所述初始医疗影像处理模型包括若干个与所述医疗中心一一对应的局部模型；

第四模块，用于采用所述局部数据集和所述局部对抗影像样本对所述局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个所述局部模型进行全局聚合处理，形成所述全局模型；还用于当各个所述局部模型的局部损失函数收敛或者所述迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，所述目标医疗影像处理模型包括一个全局模型和若干个与所述医疗中心一一对应的局部模型。

另一方面，如图 6 所示，本发明实施例还提供了一种电子设备，包括：处理器以及存储器；存储器用于存储程序；处理器执行程序实现如上所述的方法。

另一方面，本发明实施例还提供了一种计算机存储介质，其中存储有处理器可执行的程

序，处理器可执行的程序在由处理器执行时用于实现如上所述的方法。

在一些可选择的实施例中，在方框图中提到的功能/操作可以不按照操作示图提到的顺序发生。例如，取决于所涉及的功能/操作，连续示出的两个方框实际上可以被大体上同时地执行或所述方框有时能以相反顺序被执行。此外，在本发明的流程图中所呈现和描述的实施例以示例的方式被提供，目的在于提供对技术更全面的理解。所公开的方法不限于本文所呈现的操作和逻辑流程。可选择的实施例是可预期的，其中各种操作的顺序被改变以及其中被描述为较大操作的一部分的子操作被独立地执行。

在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备（如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统）使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。

计算机可读介质的更具体的示例（非穷尽性列表）包括以下：具有一个或多个布线的电连接部（电子装置）、便携式计算机盘盒（磁装置）、随机存取存储器（RAM）、只读存储器（ROM）、可擦除可编辑只读存储器（EPROM 或闪速存储器）、光纤装置以及便携式光盘只读存储器（CDROM）。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同物限定。

以上是对本发明的较佳实施进行了具体说明，但本发明并不限于所述实施例，熟悉本领域的技术人员在不违背本发明精神的前提下还可做出种种的等同变形或替换，这些等同的变形或替换均包含在本发明权利要求所限定的范围内。

说　明　书　附　图

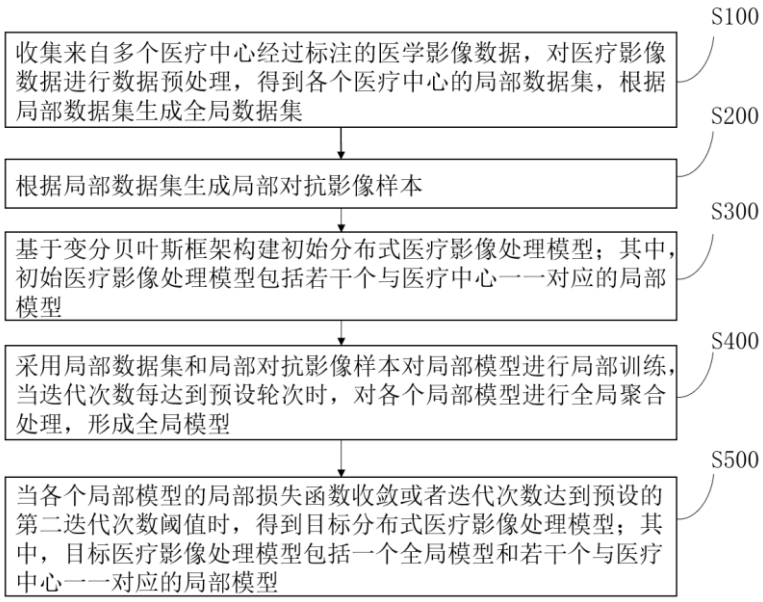
S100
收集来自多个医疗中心经过标注的医学影像数据，对医疗影像数据进行数据预处理，得到各个医疗中心的局部数据集，根据局部数据集生成全局数据集
S200
根据局部数据集生成局部对抗影像样本
S300
基于变分贝叶斯框架构建初始分布式医疗影像处理模型；其中，初始医疗影像处理模型包括若干个与医疗中心一一对应的局部模型
S400
采用局部数据集和局部对抗影像样本对局部模型进行局部训练，当迭代次数每达到预设轮次时，对各个局部模型进行全局聚合处理，形成全局模型
S500
当各个局部模型的局部损失函数收敛或者迭代次数达到预设的第二迭代次数阈值时，得到目标分布式医疗影像处理模型；其中，目标医疗影像处理模型包括一个全局模型和若干个与医疗中心一一对应的局部模型

图 1

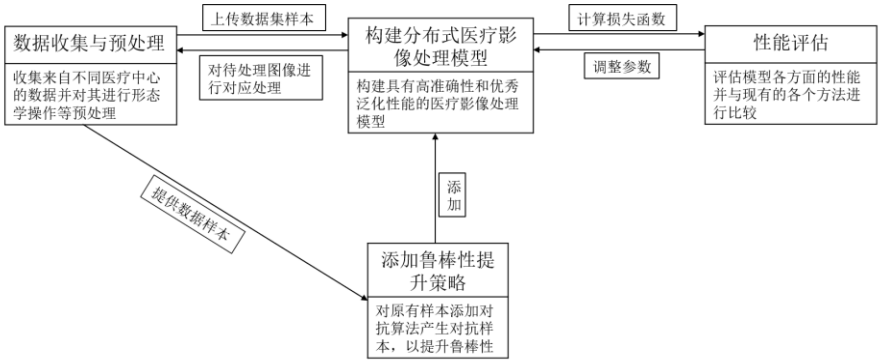
数据收集与预处理
收集来自不同医疗中心的数据并对其进行形态学操作等预处理
上传数据集样本
对待处理图像进行对应处理
构建分布式医疗影像处理模型
构建具有高准确性和优秀泛化性能的医疗影像处理模型
计算损失函数
调整参数
性能评估
评估模型各方面的性能并与现有的各个方法进行比较
提供数据样本
添加
添加鲁棒性提升策略
对原有样本添加对抗算法产生对抗样本，以提升鲁棒性

图 2

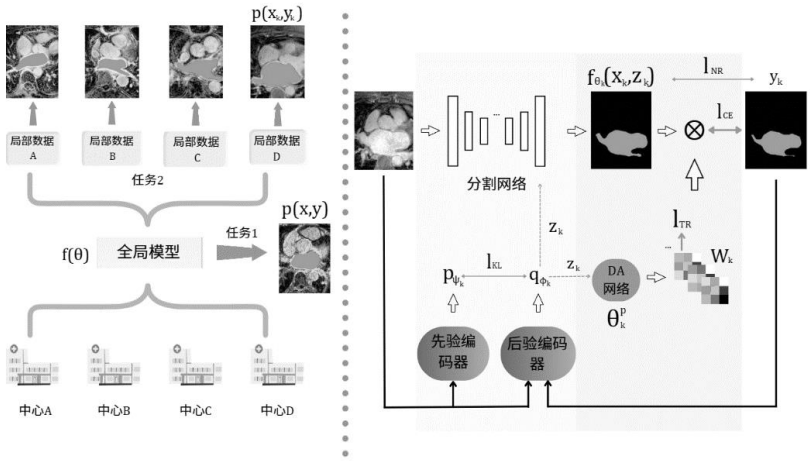
局部数据 A
局部数据 B
局部数据 C
局部数据 D
任务2
全局模型
f(θ)
任务1
中心A
中心B
中心C
中心D
分割网络
先验编码器
后验编码器
DA 网络

图 3

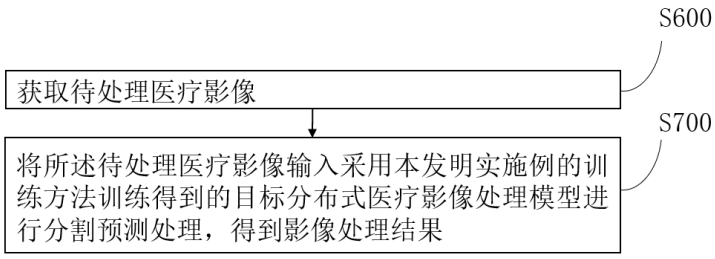
S600
获取待处理医疗影像
S700
将所述待处理医疗影像输入采用本发明实施例的训练方法训练得到的目标分布式医疗影像处理模型进行分割预测处理，得到影像处理结果

图 4

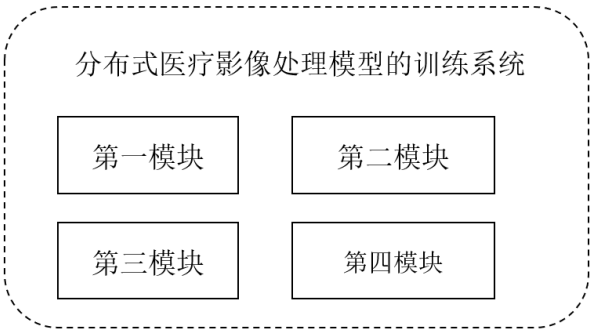
分布式医疗影像处理模型的训练系统
第一模块
第二模块
第三模块
第四模块

图 5

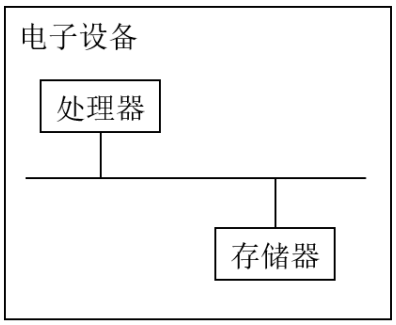

图 6