(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 120112920 A
(43)申请公布日 2025.06.06

(21)申请号 202280100963.1
(22)申请日 2022.11.11
(85)PCT国际申请进入国家阶段日
2025.04.10
(86)PCT国际申请的申请数据
PCT/JP2022/042101 2022.11.11
(87)PCT国际申请的公布数据
WO2024/100890 JA 2024.05.16
(71)申请人 三菱电机株式会社
地址 日本东京都
(72)发明人 中井纲人
(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 方冬梅 邓毅
(51)Int.Cl.
G06N 20/00(2006.01)

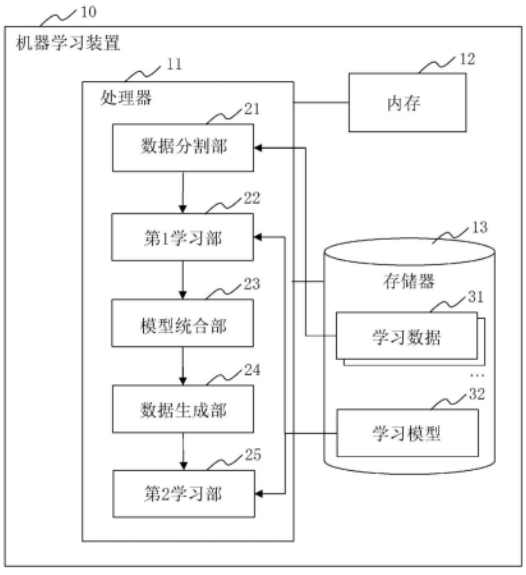
权利要求书2页 说明书8页 附图6页

(54)发明名称

机器学习装置、机器学习方法和机器学习程序

(57)摘要

第1学习部(22)将n个学习数据分别作为对象,使用对象学习数据进行训练,生成第1学习模型。模型统合部(23)对从n个第1学习模型中选择出的m个第1学习模型进行统合,生成统合模型。数据生成部(24)通过软标签对附加给对象数据的标签进行置换,生成新学习数据,该软标签是对统合模型提供对象数据作为输入而得到的结果,该对象数据是成为统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据。第2学习部(25)使用新学习数据进行训练,生成第2学习模型。



CN 120112920 A

1.一种机器学习装置,其具有:

第1学习部,其关于3以上的整数n,将附加了标签的n个学习数据分别作为对象,使用对象学习数据进行训练,生成与所述对象学习数据对应的第1学习模型,由此生成所述n个第1学习模型;

模型统合部,其关于小于n的整数m,对从由所述第1学习部生成的所述n个第1学习模型中选择出的m个第1学习模型进行统合,生成统合模型;

数据生成部,其通过软标签对附加给对象数据的标签进行置换,生成新学习数据,该软标签是对由所述模型统合部生成的统合模型提供所述对象数据作为输入而得到的结果,该对象数据是成为所述统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据;以及

第2学习部,其使用由所述数据生成部生成的新学习数据进行训练,生成第2学习模型。

2.根据权利要求1所述的机器学习装置,其中,

所述模型统合部针对能够从所述n个第1学习模型中选择的m个第1学习模型的各组合,生成所述统合模型,

所述数据生成部通过软标签对附加给对象数据的标签进行置换,生成新学习数据,该软标签是将由所述模型统合部生成的各统合模型作为对象、对对象统合模型提供所述对象数据作为输入而得到的结果,该对象数据是成为所述对象统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据。

3.根据权利要求1或2所述的机器学习装置,其中,

所述整数m为n-1。

4.根据权利要求1~3中的任意一项所述的机器学习装置,其中,

所述第2学习部使用针对所述新学习数据以基准比例附加所述学习数据而得到的数据进行训练,生成所述第2学习模型。

5.根据权利要求1~4中的任意一项所述的机器学习装置,其中,

所述机器学习装置还具有重新学习部,该重新学习部使用成为所述统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据进行所述统合模型的重新训练,

所述数据生成部使用通过所述重新学习部进行重新训练后的所述统合模型生成所述新学习数据。

6.一种机器学习方法,其中,

计算机关于3以上的整数n,将附加了标签的n个学习数据分别作为对象,使用对象学习数据进行训练,生成与所述对象学习数据对应的第1学习模型,由此生成所述n个第1学习模型,

计算机关于小于n的整数m,对从所述n个第1学习模型中选择出的m个第1学习模型进行统合,生成统合模型,

计算机通过软标签对附加给对象数据的标签进行置换,生成新学习数据,该软标签是对所述统合模型提供所述对象数据作为输入而得到的结果,该对象数据是成为所述统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据,

计算机使用所述新学习数据进行训练,生成第2学习模型。

7.一种机器学习程序,其使计算机作为机器学习装置发挥功能,该机器学习装置进行

以下处理：

第1学习处理，关于3以上的整数n，将附加了标签的n个学习数据分别作为对象，使用对象学习数据进行训练，生成与所述对象学习数据对应的第1学习模型，由此生成所述n个第1学习模型；

模型统合处理，关于小于n的整数m，对从通过所述第1学习处理生成的所述n个第1学习模型中选择出的m个第1学习模型进行统合，生成统合模型；

数据生成处理，通过软标签对附加给对象数据的标签进行置换，生成新学习数据，该软标签是对通过所述模型统合处理生成的统合模型提供所述对象数据作为输入而得到的结果，该对象数据是成为所述统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据；以及

第2学习处理，使用通过所述数据生成处理生成的新学习数据进行训练，生成第2学习模型。

机器学习装置、机器学习方法和机器学习程序

技术领域

[0001] 本公开涉及机器学习模型的训练方法。

背景技术

[0002] 作为机器学习中的隐私的课题,指出存在成员推断攻击。成员推断攻击是以下这样的攻击。对作为攻击对象的机器学习模型(以下为目标模型)提供正常的输入数据,观察从目标模型响应的推断结果。由此,确定所输入的数据是否包含在目标模型的学习数据中(=是否是成员)。

[0003] 在专利文献1和非专利文献1、2中记载了成员推断攻击的对策。

[0004] 在专利文献1中,学习数据被分割成包含隐私信息的学习数据和不包含隐私信息的学习数据。包含隐私信息的学习数据被用于机器学习模型的仅输入层的训练。不包含隐私信息的学习数据被用于机器学习模型的全部层的重新训练。重新训练后的机器学习模型具有成员推断攻击的耐性。

[0005] 在非专利文献1中,使用通过包含隐私信息的学习数据进行训练后的机器学习模型,对未附加标签的不包含隐私信息的学习数据赋予标签(以下称为软标签)。不包含隐私信息的学习数据例如是公开数据。通过被附加了软标签的学习数据来训练其他机器学习模型。该训练后的机器学习模型具有成员推断攻击的耐性。

[0006] 在非专利文献2中,初始的学习数据被分割成常数n个集合。关于n个集合,分别将除了该集合以外的n-1个集合设定成学习数据。即,设定具有n-1个集合的n个学习数据。分别使用n个学习数据进行训练,生成与n个学习数据分别对应的机器学习模型。将n个机器学习模型分别作为对象,对作为对象的机器学习模型提供作为对象的机器学习模型的训练中使用的学习数据中未包含的集合作为输入而取得软标签。作为输入而提供的集合的标签被置换成软标签,成为新的学习数据。然后,使用新的学习数据来训练机器学习模型。该训练后的机器学习模型具有成员推断攻击的耐性。

[0007] 现有技术文献

[0008] 专利文献

[0009] 专利文献1:日本特开2021-193533号公报

[0010] 非专利文献

[0011] 非专利文献1:Virat Shejwalkar et.al,“Membership Privacy for Machine Learning Models Through Knowledge Transfer”,AAAI2021

[0012] 非专利文献2:Rishav Chourasia et.al,“Knowledge Cross-Distillation for Membership Privacy”,PETS2022

发明内容

[0013] 发明要解决的课题

[0014] 在专利文献1和非专利文献1所记载的对策中,需要不包含隐私信息的学习数据。

在医疗和金融等领域中,有时在机器学习中使用敏感的数据,因此,很难准备不包含隐私信息的学习数据。

[0015] 在非专利文献2所记载的对策中,不需要不包含隐私信息的学习数据。但是,在非专利文献2所记载的对策中,根据学习数据的分割数n,需要追加n×(n-1)的学习数据的训练。因此,与现有的其他对策相比,基于对策的计算量多。

[0016] 本公开的目的在于,不需要不包含隐私信息的学习数据,并且抑制计算量,使得针对成员推断攻击具有耐性。

[0017] 用于解决课题的手段

[0018] 本公开的机器学习装置具有:第1学习部,其关于3以上的整数n,将附加了标签的n个学习数据分别作为对象,使用对象学习数据进行训练,生成与所述对象学习数据对应的第1学习模型,由此生成所述n个第1学习模型;模型统合部,其关于小于n的整数m,对从由所述第1学习部生成的所述n个第1学习模型中选择出的m个第1学习模型进行统合,生成统合模型;数据生成部,其通过软标签对附加给对象数据的标签进行置换,生成新学习数据,该软标签是对由所述模型统合部生成的统合模型提供所述对象数据作为输入而得到的结果,该对象数据是成为所述统合模型的基础的m个第1学习模型生成时的训练中使用的学习数据以外的学习数据;以及第2学习部,其使用由所述数据生成部生成的新学习数据进行训练,生成第2学习模型。

[0019] 发明效果

[0020] 在本公开中,对使用对象学习数据进行训练而生成的第1学习模型进行统合,生成统合模型,通过统合模型生成新学习数据。由此,能够不需要不包含隐私信息的学习数据,并且抑制计算量,使得针对成员推断攻击具有耐性。

附图说明

[0021] 图1是实施方式1的机器学习装置10的结构图。

[0022] 图2是示出实施方式1的机器学习装置10的处理的流程的流程图。

[0023] 图3是实施方式1的机器学习装置10的动作的具体例的说明图。

[0024] 图4是变形例2的机器学习装置10的结构图。

[0025] 图5是实施方式2的机器学习装置10的结构图。

[0026] 图6是示出实施方式2的机器学习装置10的处理的流程的流程图。

[0027] 图7是实施方式2的机器学习装置10的动作的具体例的说明图。

具体实施方式

[0028] 实施方式1

[0029] ***结构的说明***

[0030] 参照图1对实施方式1的机器学习装置10的结构进行说明。

[0031] 机器学习装置10是计算机。

[0032] 机器学习装置10具有处理器11、内存(memory)12和存储器(storage)13这样的硬件。处理器11经由信号线与其他硬件连接,对这些其他硬件进行控制。

[0033] 处理器11是进行处理的IC。IC是Integrated Circuit(集成电路)的缩写。作为具

体例,处理器11是CPU、DSP、GPU。CPU是Central Processing Unit(中央处理单元)的缩写。DSP是Digital Signal Processor(数字信号处理器)的缩写。GPU是Graphics Processing Unit(图形处理单元)的缩写。

[0034] 内存12是暂时存储数据的存储装置。作为具体例,内存12是SRAM、DRAM。SRAM是Static Random Access Memory(静态随机存取存储器)的缩写。DRAM是Dynamic Random Access Memory(动态随机存取存储器)的缩写。

[0035] 存储器13是保管数据的存储装置。作为具体例,存储器13是HDD。HDD是Hard Disk Drive(硬盘驱动器)的缩写。此外,存储器13也可以是SD(注册商标)存储卡、CompactFlash(注册商标)、NAND闪存、软盘、光盘、高密度盘、Blu-ray(注册商标)盘、DVD这样的移动记录介质。SD是Secure Digital(安全数字)的缩写。DVD是Digital Versatile Disk(数字多功能盘)的缩写。

[0036] 作为功能结构要素,机器学习装置10具有数据分割部21、第1学习部22、模型统合部23、数据生成部24和第2学习部25。机器学习装置10的各功能结构要素的功能通过软件来实现。

[0037] 在存储器13中存储有实现机器学习装置10的各功能结构要素的功能的程序。该程序由处理器11读入到内存12,由处理器11来执行。由此,实现机器学习装置10的各功能结构要素的功能。

[0038] 在存储器13中存储有学习模型32和多个学习数据31。各学习数据31被附加标签,包含隐私信息。

[0039] 在图1中,仅示出1个处理器11。但是,处理器11也可以是多个,多个处理器11也可以协作执行实现各功能的程序。

[0040] ***动作的说明***

[0041] 参照图2和图3对实施方式1的机器学习装置10的动作进行说明。

[0042] 实施方式1的机器学习装置10的动作步骤相当于实施方式1的机器学习方法。此外,实现实施方式1的机器学习装置10的动作的程序相当于实施方式1的机器学习程序。

[0043] 参照图2对实施方式1的机器学习装置10的处理的流程进行说明。

[0044] (步骤S11:数据分割处理)

[0045] 数据分割部21将存储器13中存储的多个学习数据31读入到内存12。数据分割部21将所读入的多个学习数据31分割成常数n个集合。n为3以上的整数。例如,数据分割部21以使各集合中包含的学习数据31的数量大致相等的方式对多个学习数据31进行等分。由此,生成n个学习数据的数据集(以下称为学习数据33)。数据分割部21将n个学习数据33写入内存12中。

[0046] (步骤S12:第1学习处理)

[0047] 第1学习部22从内存12读入学习模型32和在步骤S11中生成的n个学习数据33。第1学习部22将n个学习数据33分别设定成对象学习数据33。第1学习部22使用对象学习数据33对学习模型32进行训练,生成与对象学习数据33对应的第1学习模型34。由此,生成n个第1学习模型34。第1学习部22将n个第1学习模型34写入内存12中。

[0048] (步骤S13:模型统合处理)

[0049] 模型统合部23从内存12读入在步骤S12中生成的n个第1学习模型34。模型统合部

23对从n个第1学习模型34中选择出的m个第1学习模型34进行统合,生成统合模型35。m为小于n的整数。这里,模型统合部23针对能够从n个第1学习模型中选择的m个第1学习模型34的各组合生成统合模型35。模型统合部23将针对各组合的统合模型35写入内存12中。

[0050] 模型统合部23对m个第1学习模型34的参数进行合计,按照每个参数进行相加平均或加权平均等算术处理。由此,模型统合部23对m个第1学习模型34进行统合,生成统合模型35。

[0051] 在实施方式1中,设为m=n-1。从n个第1学习模型34中选择n-1个第1学习模型34的组合为n种。即,存在n个第1学习模型34中的除了第1个第1学习模型34以外的其余的n-1个第1学习模型34的组合、除了第2个第1学习模型34以外的其余的n-1个第1学习模型34的组合、……除了第n个第1学习模型34以外的其余的n-1个第1学习模型34的组合这n种组合。

[0052] 因此,模型统合部23针对n种的各组合,对该组合的第1学习模型34进行统合,生成统合模型35。其结果,生成n个统合模型35。

[0053] (步骤S14:数据生成处理)

[0054] 数据生成部24从内存12读入在步骤S13中生成的各统合模型35。数据生成部24将各统合模型35分别设定成对象统合模型35。

[0055] 数据生成部24对对象统合模型35提供对象数据36作为输入来进行推断,该对象数据36是成为对象统合模型35的基础的m个第1学习模型生成时的训练中使用的学习数据33以外的学习数据33。数据生成部24取得通过对象统合模型35进行推断而得到的结果即软标签。数据生成部24通过软标签对附加给对象数据36的标签进行置换,生成新学习数据37。数据生成部24汇集关于各统合模型35分别生成的新学习数据37,作为新学习数据37的数据集写入内存12中。

[0056] 在实施方式1中,数据生成部24读入n个统合模型35。数据生成部24将n个统合模型35分别设定成对象统合模型35。

[0057] 数据生成部24对对象统合模型35提供对象数据36作为输入来进行推断,该对象数据36是成为对象统合模型35的基础的n-1个第1学习模型生成时的训练中使用的学习数据33以外的学习数据33。例如,在根据除了第1个第1学习模型34以外的其余的n-1个第1学习模型34的组合而生成了对象统合模型35的情况下,第1个第1学习模型34成为对象数据36。同样,在根据除了第2个第1学习模型34以外的其余的n-1个第1学习模型34的组合而生成了对象统合模型35的情况下,第2个第1学习模型34成为对象数据36。数据生成部24通过软标签对附加给对象数据36的标签进行置换,生成新学习数据37。

[0058] 数据生成部24汇集关于n个统合模型35分别生成的新学习数据37,作为新学习数据37的数据集写入内存12中。

[0059] (步骤S15:第2学习处理)

[0060] 第2学习部25从内存12读入学习模型32和在步骤S14中生成的新学习数据37的数据集。第2学习部25使用新学习数据37的数据集对学习模型32进行训练,生成第2学习模型38。

[0061] 参照图3对实施方式1的机器学习装置10的动作的具体例进行说明。

[0062] 在图3中,示出分割数即n为3、m为n-1的情况下的例子。

[0063] 在步骤S11中,数据分割部21将包含隐私信息的学习数据31等分成3(=n)个。

[0064] 由此,生成学习数据33A、学习数据33B和学习数据33C。

[0065] 在步骤S12中,第1学习部22将3个学习数据33分别设定成对象学习数据33。第1学习部22使用对象学习数据33对学习模型32进行训练,生成与对象学习数据33对应的第1学习模型34。

[0066] 由此,生成通过学习数据33A进行训练后的第1学习模型34A、通过学习数据33B进行训练后的第1学习模型34B、通过学习数据33C进行训练后的第1学习模型34C这3个学习数据33。

[0067] 在步骤S13中,模型统合部23将能够从3个第1学习模型34中选择的2(=m=n-1)个第1学习模型34的各组合设定成对象组合。模型统合部23对对象组合中包含的2个第1学习模型34进行统合,生成统合模型35。

[0068] 由此,生成对第1学习模型34A和第1学习模型34B进行统合后的统合模型35A、对第1学习模型34B和第1学习模型34C进行统合后的统合模型35B、以及对第1学习模型34A和第1学习模型34C进行统合后的统合模型35C这3个统合模型35。

[0069] 在步骤S14中,数据生成部24将3个统合模型35分别设定成对象统合模型35。数据生成部24对对象统合模型35提供对象数据36作为输入,该对象数据36是成为对象统合模型35的基础的2个第1学习模型34的训练中未使用的学习数据33。对统合模型35A提供第1学习模型34A和第1学习模型34B的训练中未使用的学习数据33C作为输入。对统合模型35B提供第1学习模型34B和第1学习模型34C的训练中未使用的学习数据33A作为输入。对统合模型35C提供第1学习模型34A和第1学习模型34C的训练中未使用的学习数据33B作为输入。

[0070] 数据生成部24通过软标签对附加给对象数据36的标签进行置换,生成新学习数据37,该软标签是通过对象统合模型35进行推断而得到的结果。即,通过由统合模型35A得到的软标签对学习数据33C的标签进行置换,生成新学习数据37A。通过由统合模型35B得到的软标签对学习数据33A的标签进行置换,生成新学习数据37B。通过由统合模型35C得到的软标签对学习数据33B的标签进行置换,生成新学习数据37C。

[0071] 数据生成部24汇集新学习数据37A、新学习数据37B和新学习数据37C,生成新学习数据37的数据集。

[0072] 在步骤S15中,第2学习部25使用新学习数据37的数据集对学习模型32进行训练,生成第2学习模型38。

[0073] 这里,学习模型32的训练例如通过深度学习来进行。另外,学习模型32的训练不限于深度学习,例如也可以通过回归法、决策树学习、贝叶斯法、聚类等运算来进行。

[0074] ***实施方式1的效果***

[0075] 如上所述,实施方式1的机器学习装置10使用对包含隐私信息的学习数据31进行分割后的学习数据33生成多个第1学习模型34,对第1学习模型34进行统合,生成统合模型35。而且,机器学习装置10通过由统合模型35得到的软标签生成新学习数据37,通过新学习数据37对学习模型32进行训练,生成第2学习模型38。即,使用去掉原来的学习数据31的隐私信息后的新学习数据37对学习模型32进行训练,生成第2学习模型38。

[0076] 由此,实施方式1的机器学习装置10能够生成针对成员推断攻击具有耐性的第2学习模型38。即,机器学习装置10不用如专利文献1和非专利文献1那样准备不包含隐私信息的学习数据,就能够生成针对成员推断攻击具有耐性的第2学习模型38。

[0077] 此外,实施方式1的机器学习装置10关于对学习数据31进行分割后的多个学习数据33,分别生成第1学习模型34,对第1学习模型34进行统合,生成统合模型35。即,机器学习装置10不是如非专利文献2那样进行追加的学习,而是对第1学习模型34进行统合。由此,与非专利文献2的技术相比,能够抑制计算量,生成针对成员推断攻击具有耐性的第2学习模型38。

[0078] 具体而言,为了针对成员推断攻击具有耐性,机器学习装置10需要(1)追加1次训练、以及(2)作为轻量处理的第1学习模型34的参数的平均计算和软标签的赋予。追加进行的1次训练是与学习数据31的分割数n对应的n个学习数据33的训练。第1学习模型34的参数的平均计算是第1学习模型34的统合处理中的计算。

[0079] ***其他结构***

[0080] <变形例1>

[0081] 在步骤S15中,第2学习部25也可以使用针对新学习数据37的数据集以基准比例附加学习数据31而得到的数据进行训练。

[0082] 由此,可预见到学习精度的提高。但是,学习数据31相对于新学习数据37的比率越高,则第2学习模型38的成员推断攻击耐性越低。因此,需要根据必要的成员推断攻击耐性,事先设定基准比例。

[0083] <变形例2>

[0084] 在实施方式1中,各功能结构要素通过软件来实现。但是,作为变形例2,各功能结构要素也可以通过硬件来实现。在该变形例2中,对与实施方式1不同之处进行说明。

[0085] 参照图4对变形例2的机器学习装置10的结构进行说明。

[0086] 在各功能结构要素通过硬件来实现的情况下,机器学习装置10代替处理器11、内存12和存储器13而具有电子电路15。电子电路15是实现各功能结构要素、内存12和存储器13的功能的专用的电路。

[0087] 作为电子电路15,设想单一电路、复合电路、程序化的处理器、并行程序化的处理器、逻辑IC、GA、ASIC、FPGA。GA是Gate Array(门阵列)的缩写。ASIC是Application Specific Integrated Circuit(专用集成电路)的缩写。FPGA是Field-Programmable Gate Array(现场可编程门阵列)的缩写。

[0088] 可以通过1个电子电路15实现各功能结构要素,也可以使多个电子电路15分散实现各功能结构要素。

[0089] <变形例3>

[0090] 作为变形例3,也可以是,一部分的各功能结构要素通过硬件来实现,其他的各功能结构要素通过软件来实现。

[0091] 将处理器11、内存12、存储器13和电子电路15称作处理电路。即,各功能结构要素的功能通过处理电路来实现。

[0092] 实施方式2

[0093] 实施方式2与实施方式1的不同之处在于,进行统合模型35的重新训练。在实施方式2中,对该不同之处进行说明,省略相同之处的说明。

[0094] ***结构的说明***

[0095] 参照图5对实施方式2的机器学习装置10的结构进行说明。

[0096] 机器学习装置10与图1所示的机器学习装置10的不同之处在于,作为功能结构要素而具有重新学习部26。与其他功能结构要素同样,重新学习部26通过软件或硬件来实现。

[0097] ***动作的说明***

[0098] 参照图6对实施方式2的机器学习装置10的处理的流程进行说明。

[0099] 步骤S21～步骤S23的处理与图2的步骤S11～步骤S13的处理相同。步骤S25和步骤S26的处理与图2的步骤S14和步骤S15的处理相同。

[0100] 但是,在步骤S25中,使用在步骤S24中进行重新训练后的统合模型35生成新学习数据37。

[0101] (步骤S24:重新学习处理)

[0102] 重新学习部26从内存12读入在步骤S23中生成的各统合模型35。重新学习部26将各统合模型35分别设定成对象统合模型35。

[0103] 重新学习部26使用成为对象统合模型35的基础的m个第1学习模型34生成时的训练中使用的学习数据33,进行对象统合模型35的重新训练。各第1学习模型34使用1个学习数据33来生成。因此,重新学习部26使用m个第1学习模型34生成时使用的m个学习数据33进行训练。

[0104] 参照图7对实施方式2的机器学习装置10的动作的具体例进行说明。

[0105] 在图7中,与图3的例子同样,示出分割数即n为3、m为n-1的情况下的例子。

[0106] 通过步骤S21～步骤S23的处理,与图3的例子同样,生成统合模型35A～统合模型35C这3个统合模型35。

[0107] 在步骤S24中,重新学习部26将3个统合模型35分别设定成对象统合模型35。数据生成部24使用成为对象统合模型35的基础的2个第1学习模型34的训练中使用的学习数据33,对对象统合模型35进行重新训练。

[0108] 使用第1学习模型34A和第1学习模型34B的训练中使用的学习数据33A和学习数据33B对统合模型35A进行重新训练。由此,生成统合模型35A'。使用第1学习模型34B和第1学习模型34C的训练中使用的学习数据33B和学习数据33C对统合模型35B进行重新训练。由此,生成统合模型35B'。使用第1学习模型34A和第1学习模型34C的训练中使用的学习数据33A和学习数据33C对统合模型35C进行重新训练。由此,生成统合模型35C'。

[0109] 在步骤S25中,数据生成部24将重新训练后的3个统合模型35分别设定成对象统合模型35。即,数据生成部24将统合模型35A'、统合模型35B'和统合模型35C'分别设定成对象统合模型35。然后,与图3的例子同样,数据生成部24通过对象统合模型35生成新学习数据37。

[0110] 在步骤S26中,与图3的例子同样,第2学习部25使用新学习数据37的数据集,对学习模型32进行训练,生成第2学习模型38。

[0111] ***实施方式2的效果***

[0112] 如上所述,实施方式2的机器学习装置10对统合模型35进行重新训练。由此,与实施方式1相比,能够提高统合模型35的推断的精度。当统合模型35的推断的精度提高时,能够高精度地对新学习数据37附加软标签。其结果,能够生成推断的精度高的第2学习模型38。

[0113] 另外,也可以将以上的说明中的"部"改写成"电路"、"工序"、"步骤"、"处理"或"处

理电路”。

[0114] 以上说明了本公开的实施方式和变形例。也可以组合实施这些实施方式和变形例中的若干个实施方式和变形例。此外,也可以实施任意1个或若干个实施方式和变形例的一部分。另外,本公开不限于以上的实施方式和变形例,能够根据需要进行各种变更。

[0115] 标号说明

[0116] 10:机器学习装置;11:处理器;12:内存;13:存储器;15:电子电路;21:数据分割部;22:第1学习部;23:模型统合部;24:数据生成部;25:第2学习部;26:重新学习部;31:学习数据;32:学习模型;33:学习数据;34:第1学习模型;35:统合模型;36:对象数据;37:新学习数据;38:第2学习模型。

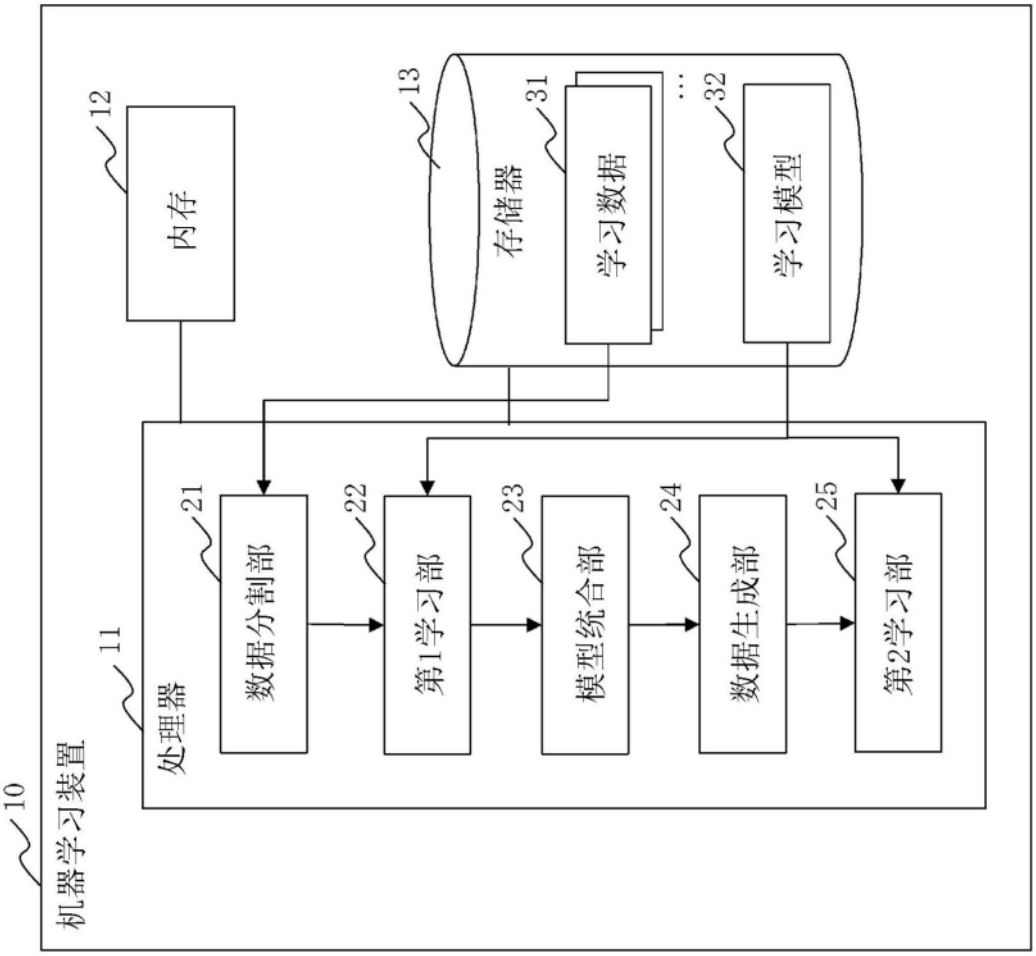

10
机器学习装置
11
处理器
21
数据分割部
22
第1学习部
23
模型统合部
24
数据生成部
25
第2学习部
12
内存
13
存储器
31
学习数据
…
32
学习模型

图1

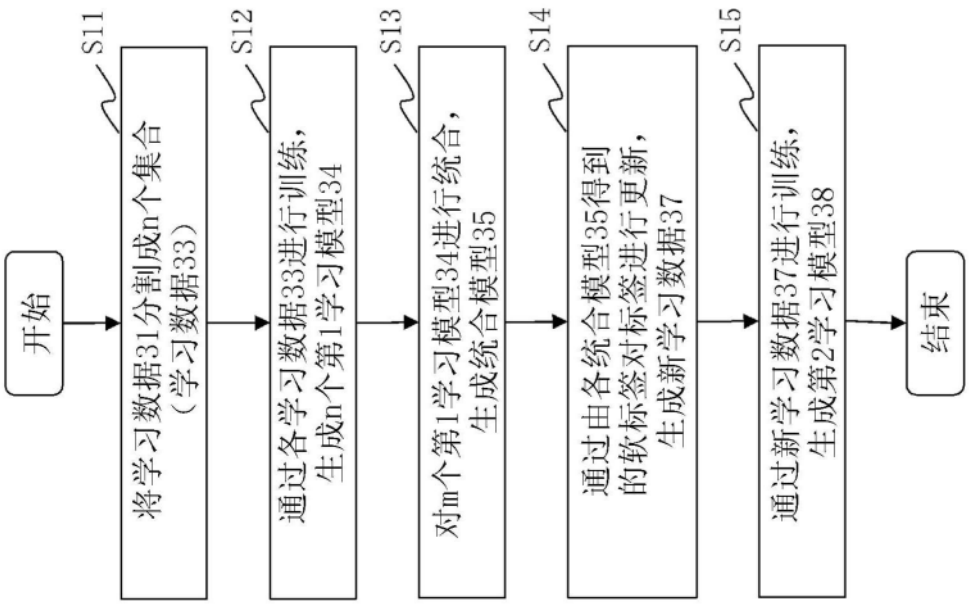

开始
S11
将学习数据31分割成n个集合
（学习数据33）
S12
通过各学习数据33进行训练，
生成n个第1学习模型34
S13
对m个第1学习模型34进行统合，
生成统合模型35
S14
通过由各统合模型35得到
的软标签对标签进行更新，
生成新学习数据37
S15
通过新学习数据37进行训练，
生成第2学习模型38
结束

图2

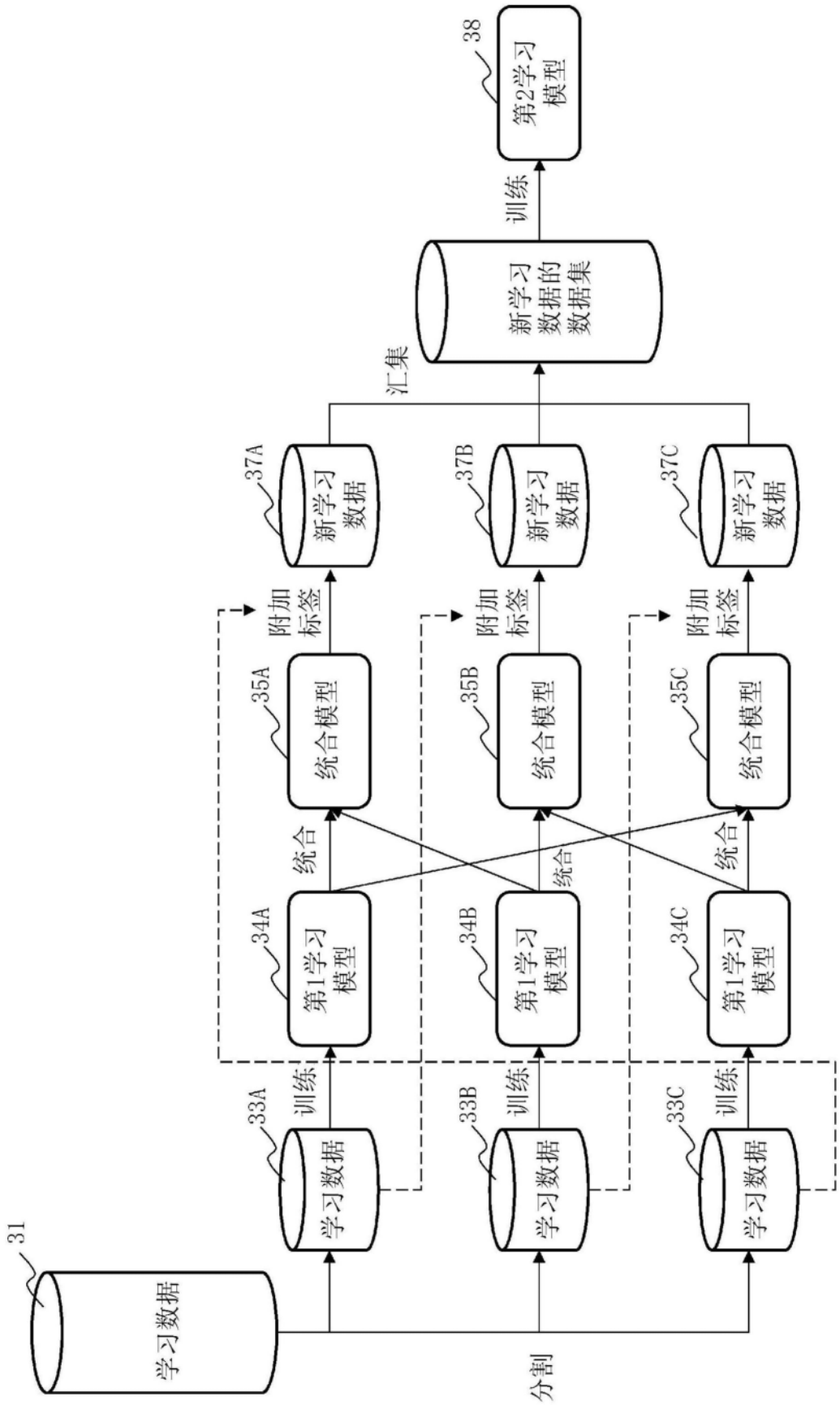

31
学习数据
分割
33A
学习数据
33B
学习数据
33C
学习数据
训练
训练
训练
34A
第1学习模型
34B
第1学习模型
34C
第1学习模型
统合
统合
统合
35A
统合模型
35B
统合模型
35C
统合模型
附加标签
附加标签
附加标签
37A
新学习数据
37B
新学习数据
37C
新学习数据
汇集
新学习数据的数据集
训练
38
第2学习模型

图3

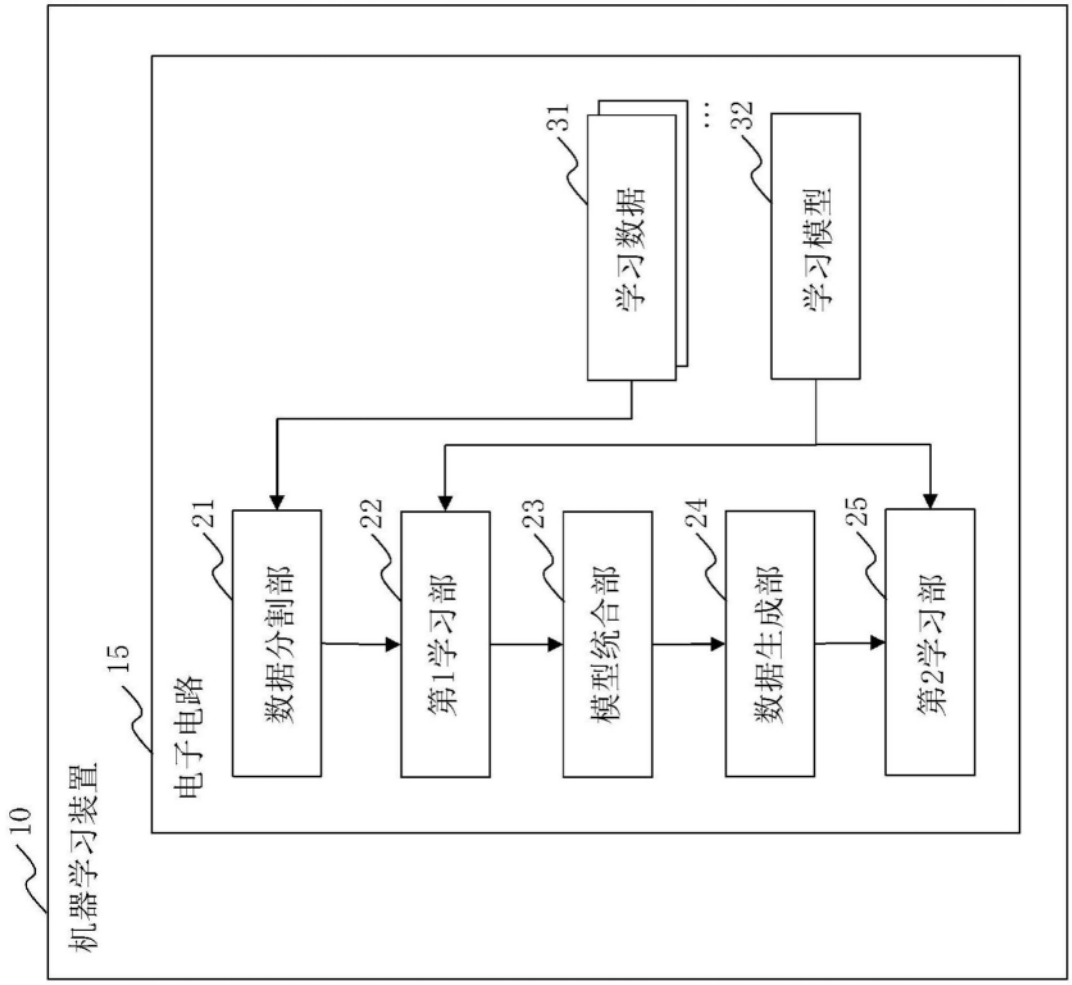

10
机器学习装置
15
电子电路
21
数据分割部
22
第1学习部
23
模型统合部
24
数据生成部
25
第2学习部
31
学习数据
…
32
学习模型

图4

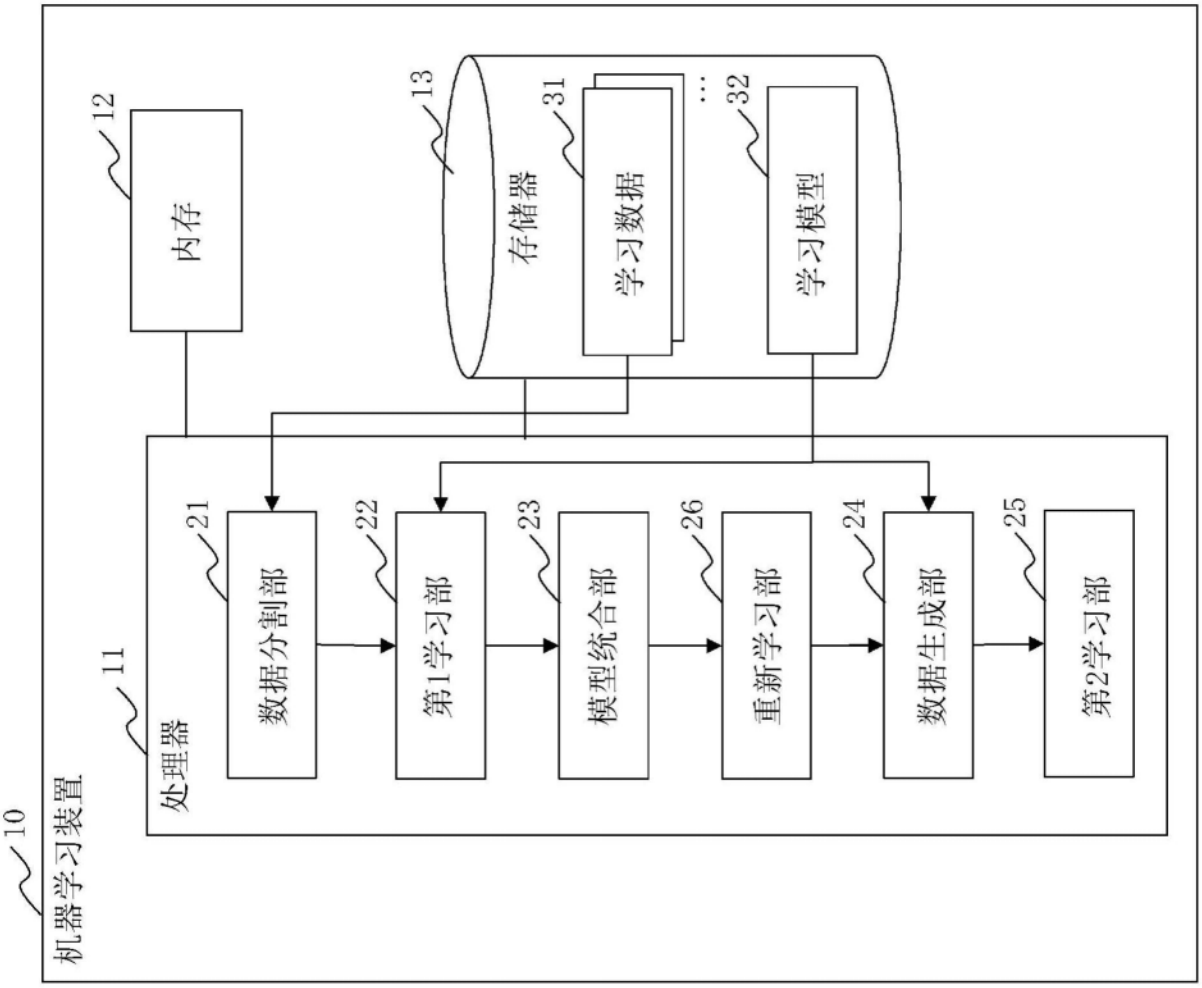

10
机器学习装置
11
处理器
12
内存
13
存储器
31
学习数据
32
学习模型
21
数据分割部
22
第1学习部
23
模型统合部
26
重新学习部
24
数据生成部
25
第2学习部

图5

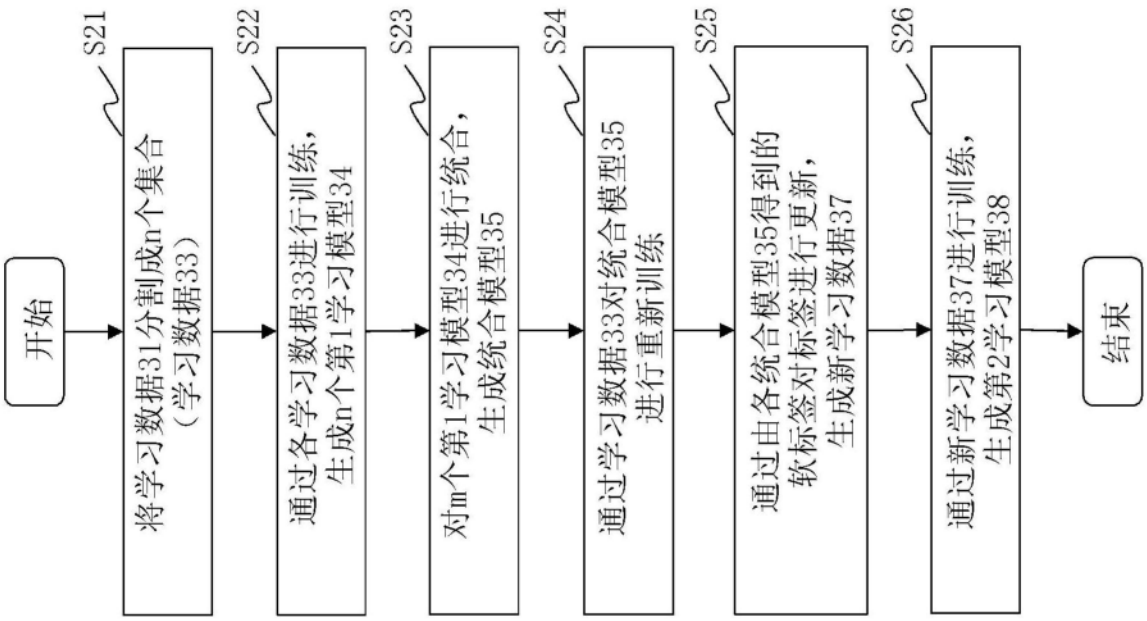

开始
S21
将学习数据31分割成n个集合
（学习数据33）
S22
通过各学习数据33进行训练，
生成n个第1学习模型34
S23
对m个第1学习模型34进行统合，
生成统合模型35
S24
通过学习数据33对统合模型35
进行重新训练
S25
通过由各统合模型35得到的
软标签对标签进行更新，
生成新学习数据37
S26
通过新学习数据37进行训练，
生成第2学习模型38
结束

图6

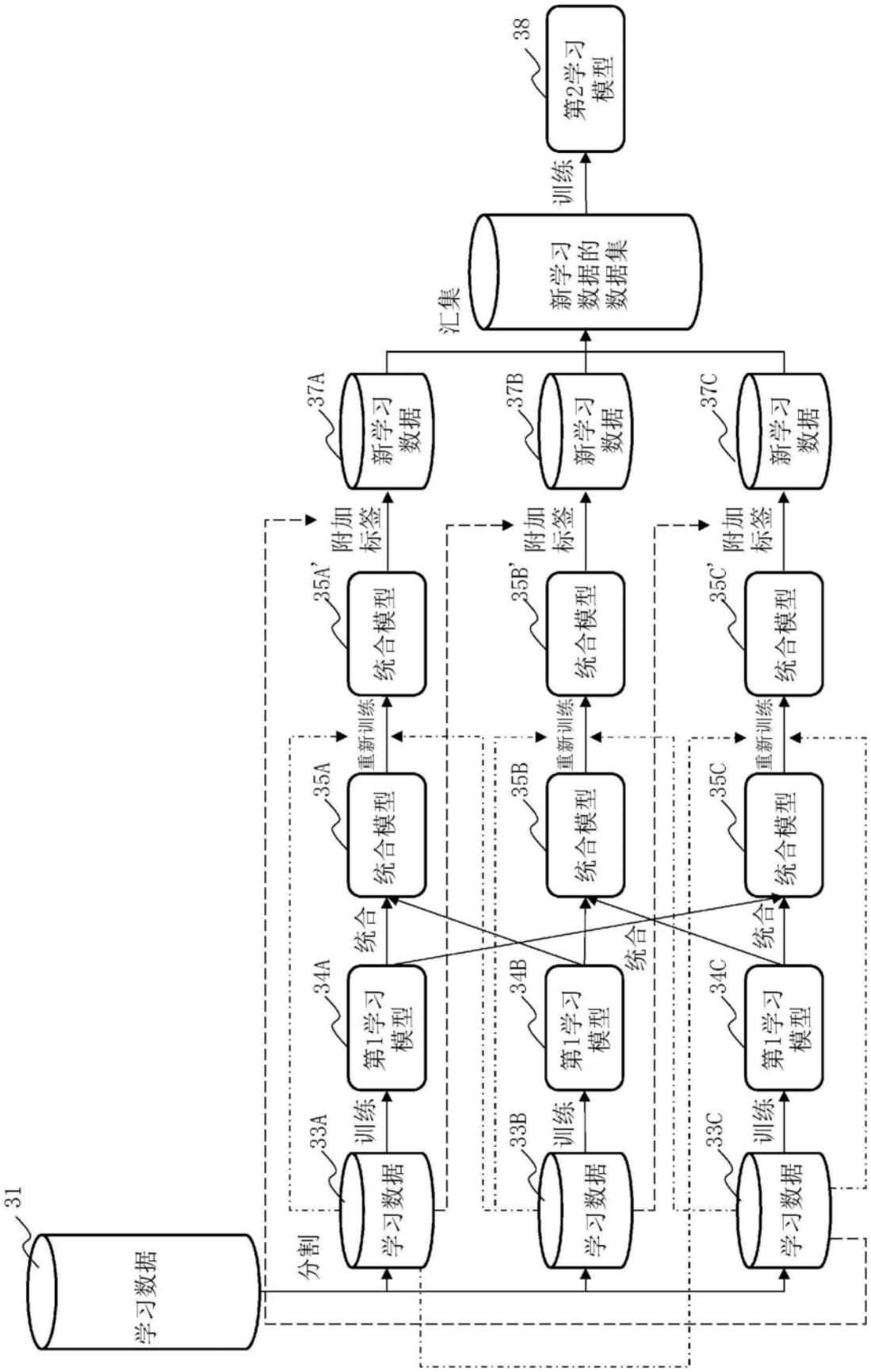

31
学习数据
分割
33A
学习数据
训练
34A
第1学习模型
统合
35A
统合模型
重新训练
35A'
统合模型
附加标签
37A
新学习数据
33B
学习数据
训练
34B
第1学习模型
统合
35B
统合模型
重新训练
35B'
统合模型
附加标签
37B
新学习数据
33C
学习数据
训练
34C
第1学习模型
统合
35C
统合模型
重新训练
35C'
统合模型
附加标签
37C
新学习数据
汇集
新学习数据的数据集
训练
38
第2学习模型

图7