Journal of Wuhan Polytechnic

弱监督人工智能算法平台研究

冯琰一[1]，周　雯[2]，张　睿[1]

（1. 光控特斯联（上海）信息科技有限公司，上海 200030；
2. 武汉软件工程职业学院 信息学院，湖北 武汉 430205）

摘　要：针对目前人工智能开放平台普遍存在预训练模型开发成本高、行业数据标注成本高等问题，本文研究了一种使用弱监督训练范式且任务可解耦的人工智能算法平台（Weak Supervision & Task Decoupling AI Platform，简称为 WSTD-AP）。不同于基于传统强监督学习的人工智能算法平台，WSTP 将大规模无标签数据用于不同规模的模型训练，在有限成本情况下充分利用“扩展法则”（Scaling Law），使模型在下游任务（如图像识别、目标检测等）达到更好的效果。

关键词：人工智能；算法平台；弱监督；预训练模型

中图分类号：TP181　　文献标志码：A　　文章编号：1671-931X（2024）05-0110-05

DOI：10.19899/j.cnki.42-1669/Z.2024.05.017

一、前言

随着科技的不断进步，人工智能（AI）技术已经取得了令人瞩目的成就，成为推动社会进步和产业升级的关键引擎。其中，人工智能算法平台作为必不可少的基础设施，引起了广泛的研究兴趣和社会关注。

目前，人工智能开放平台普遍存在一些痛点。一方面，平台研发人员需要针对不同的行业应用需求开发不同的算法，导致复用性差、预训练模型开发成本高；另一方面平台用户需要标注大量行业真实数据以避免数据间分布差异过大、模型训练陷入过拟合等问题，进而增加了平台用户的计算成本和数据标注成本。

对以上问题，我们研究了一种使用弱监督训练范式且任务可解耦的人工智能算法平台，针对“预训练算法模型”部分，我们引入一种可解耦任务模型；针对“模型训练技术”部分，我们基于自监督学习和迁移学习提出了一种统一的弱监督训练范式，这个训练范式的核心在于充分利用“扩展法则”中的数据可扩展性使模型从中受益。

二、相关工作

（一）人工智能算法平台

人工智能算法平台降低了企业 AI 赋能的成本，同时也提升了效率，使 AI 能力得到快速部署且在

收稿日期：2024-03-14

基金项目：2022 年湖北省教育厅科学技术研究计划指导性项目“AIoT 教学实训平台研究”（项目编号：B2022548）。

作者简介：冯琰一（1986— ），男，广东广州人，光控特斯联（上海）信息科技有限公司技术总监，研究方向：人工智能；周雯（1983— ），女，湖北武汉人，武汉软件工程职业学院信息学院副教授，研究方向：物联网应用技术；张睿（1995— ），男，广东广州人，光控特斯联（上海）信息科技有限公司技术工程师，研究方向：算法研究。

不同行业中实现大规模应用。

人工智能算法平台的建设流程主要分为三个环节：搭建底层架构、算法研发，以及产品封装。其中前两者最为重要，首先，底层架构主要是指基于深度学习框架的底层架构，目前主流深度学习框架包括 Tensorflow、Pytorch、百度飞桨等。其次，算法研发包含了通用算法、行业定制化算法以及算法训练技术：通用技术算法包括计算机视觉、语音识别、自然语言处理等基础人工智能技术；行业定制化技术一般指行业应用算法，包括车牌识别、智能语音客服等，是通用技术算法的应用延伸；最后，算法训练技术是算法模型的建模方法，其很大程度上决定了算法的鲁棒性、准确性、复用性以及可扩展性。目前算法训练技术主要分为强监督学习和非强监督学习。

（二）自监督学习

自监督学习是一种利用未标记数据来学习有用特征表示的机器学习范式，它可以帮助提高下游任务的性能。自监督学习的主要思想是通过设计一些伪监督任务，利用数据本身的结构或属性来生成标签，从而避免人工标注的成本和限制。自监督学习在自然语言处理、计算机视觉、语音识别等领域都有广泛的应用和研究。

（三）任务可解耦的预训练模型

可解耦任务模型是一类多任务学习模型，它们的特点是通过显式或隐式地将任务的特征或参数分解为任务共享的部分和任务特有的部分，从而实现任务的解耦和优化。可解耦任务模型可以分为两大类：基于特征解耦的模型和基于参数解耦的模型。前者主要思想是将原始输入的特征分解为任务共享特征和任务特有特征，然后分别用于不同的任务，例如 FDN；后者的主要思想是将模型的参数分解为任务共享的部分和任务特有的部分，然后分别用于不同的任务。例如，Task-MoE 混合专家模型。

三、方法

本文提出了一种使用弱监督训练范式且任务可解耦的人工智能算法平台 WSTD-AP。总体包含两个核心点：任务可解耦训练模型（Task Decoupling Pre-trained Model，简称 TDPM）和弱监督训练框架（Weak Supervision Training Framework）。我们将在本节中对 WSTD-AP 的各部分细节，以及平台训练模型过程进行详细介绍。

（一）WSTD-AP 算法技术

1. 可解耦任务模型

我们为 WSTD-AP 引入了两种可解耦任务模型的结构，分别是“One-to-One”结构和“One for All”结构。

首先，“One-to-One”结构采用“主干模型 + 任务头”结构（如图 1 所示）中，我们使用一个通用预训练主干模型来提取任务的特征，然后根据任务的类型，从任务头模型集（下标指的是任务 ID）中选择一个对应的任务头来完成任务。假设输入是，输出是，则可通过以下公式 1 表示此结构：

$$Y=t_*[F_b(X)] \quad (式\ 1)$$

这种范式通常用于单任务模型，即单一预训练训练模型对应单一任务。其优势在于相同数据模态下的不同任务间可以复用预训练主干模型的强大的表示能力，提高模型复用率和减少模型训练计算量和训练数据量。

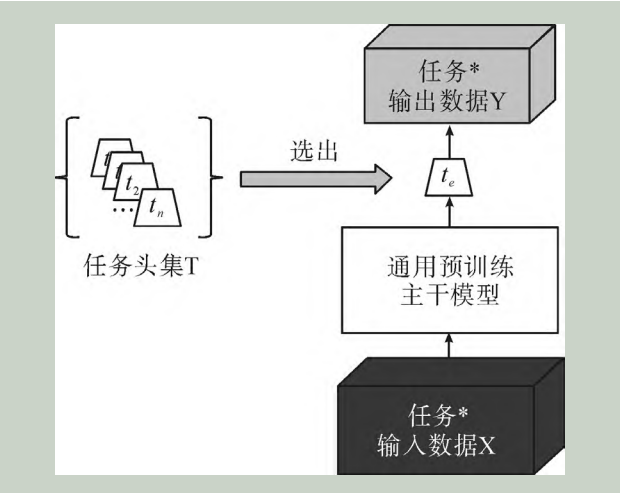

图 1　主干模型 + 任务头结构示意图

“One for All”结构采用的是“混合专家”结构（如图 2 所示），主要是为了解决多任务学习场景，即一个模型一次训练即可同时完成多个任务，进而提高模型的可扩展性和泛化能力。此结构是基于“One-to-One”结构扩展而来，不同之处在于此结构的主干模型只采用 Transformer 模型，且有一个核心部件——路由器神经网络，其作用是根据输入的任务类型为每个任务分配一个专家子网络，以及一个共享的通用子网络。路由器神经网络包括专家路由控制门和共享—专家全连接层。其中专家路由控制门的输出是一个概率分布，表示每个任务对应的专家子网络和通用子网络的权重。然后，根据这个概率分布，将输入的任务数据分发到相应的子网

络中进行处理，最后将子网络的输出加权求和，得　到最终的任务结果。

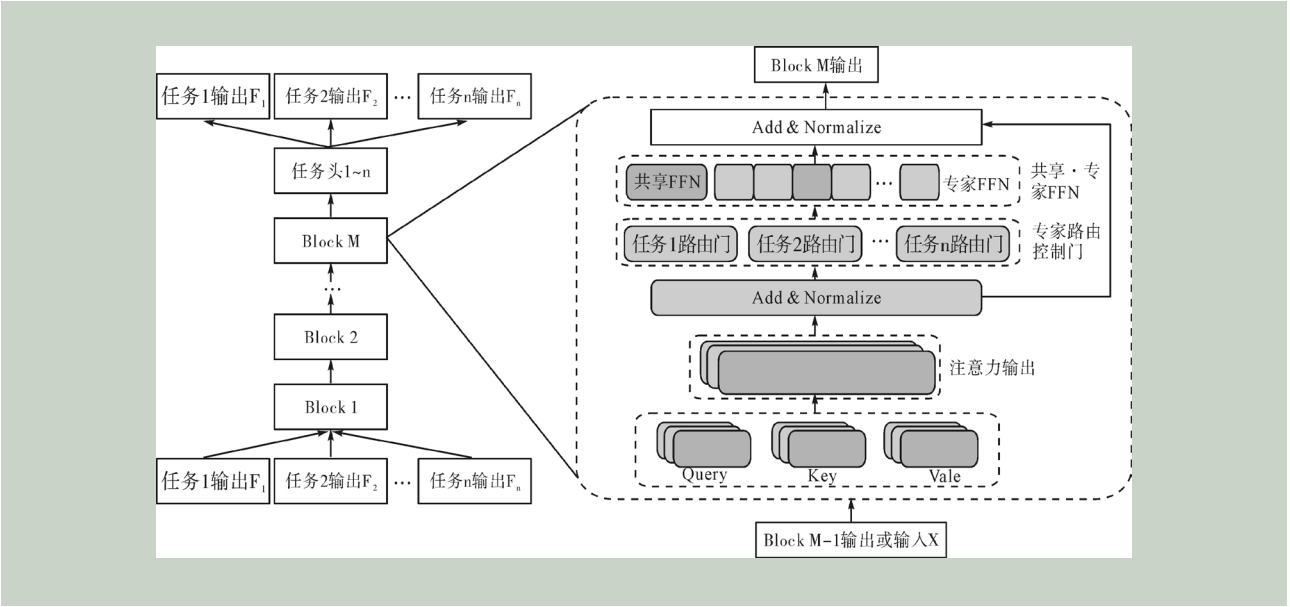

图2　“混合专家”结构示意图

2. 弱监督训练框架

从上述 WSTD-AP 的两种预训练模型结构和原理可知，模型十分依赖于通用主干模型的表示能力，且解耦后任务器（即任务头或专家子网络）较为灵活，因此需要一种灵活且统一的训练框架用于平台的模型训练。本文所提训练框架主要分成两部分：基于自监督的通用主干模型预训练和基于迁移学习的任务模型训练。

（1）基于自监督学习的通用主干模型预训练

通用主干模型是可解耦任务模型非常重要的一部分，具有更好表示能力和推理能力的通用主干模型能更好地促使任务模型完成下游任务。基于“扩展法则”，下游任务测试损失值会随着“计算”“数据规模”和“模型参数量”的增加呈现可预测的下降模式。同时，我们知道若在有限数据规模和模型规模下仅对“计算”扩增是会导致过拟合结果，所以我们主要对“数据规模”和“模型规模”上进行扩增。

首先，“模型规模”代表了模型复杂度和推理知识存储空间大小，即在不陷入过拟合的情况下，“模型规模”是越大能力越强。因此，我们所使用的通用主干模型规模最小不低于 25M 参数量，常用规模为 86M 参数量。其次，在“数据规模”上，我们收集了大量公开无标签数据，例如我们私有大规模视觉数据集有将近 3000 万张不同场景的图片数据。

由于数据量的指数级扩增，我们无法对那些数据进行一一标注，因此，我们使用了两种自监督学习范式：对比学习建模和掩码建模。

完成通用主干模型的自监督预训练后，即可将预训练通用主干模型用于下游任务的可解耦任务模型。

（2）基于迁移学习的特定任务知识获取

在此部分，我们根据不同下游任务和需求，使用预训练通用主干模型构建任务模型（即可解耦任务模型），并使用迁移学习完成特定任务知识获取。

在迁移学习上，我们有三种模式：任务器强监督训练、任务模型强监督训练，以及任务模型不完全监督训练。

“任务器强监督训练”是指用带标签任务数据集训练任务器，同时预训练通用主干模型不会发生参数调整。这种模式主要用于下游任务数据规模小的情况，其优势在于可以减少模型的参数量和计算资源，避免过拟合和欠拟合的问题；

“任务模型强监督训练”是指用带标签任务数据集训练任务模型，此时预训练通用主干模型也需要参与训练。这种模式主要用于中大规模下游任务数据集情况；

“任务模型不完全监督训练”指用带部分标签任务数据集训练任务模型，此时预训练通用主干模型也需要参与训练。若有大规模无标签任务数据且同时有部分任务数据带有标签，即可使用此模式。此模式会先用无标签任务数据对通用主干模

型再次进行自监督训练，然后再用部分带标签任务数据对任务模型进行强监督训练，接着用完成强监督训练的任务模型自动标注无标签任务数据，得到新的带标签数据集，用于下一轮强监督训练，如此循环直至任务模型在任务测试集的性能不再提升，即可停止。

四、实验

（一）数据集

为了验证本文所提方案可行，我们分别在CIFAR10数据集、TSL Gesture Dataset私有手势识别数据集和NLP花呗公开数据集上进行测试。CIFAR10数据集是一个用于图像分类的数据集，它包含了10个类别的60000张32×32的彩色图像。此数据集主要用于验证此论文所提技术对小分辨率公开数据集的分类效果。TSL Gesture Dataset是自有特定任务数据集，包含7万多张图片数据，共有5个手势类别。为了验证此论文所提技术对小规模数据的分类效果，将分配3990张图片为训练集，剩余70000多张图片数据为验证集。NLP花呗公开数据集是一个用于问题相似度计算的数据集，也属于NLP句子对分类任务。该数据集包含了10万对的标注数据，每一对数据由两个句子和一个标注组成，标注为1表示两个句子是同义的，标注为0表示两个句子是不同义的。

（二）评价指标

本文对分类任务使用Acc@1准确率作为实验评价指标，即分类正确的样本数量除以所有样本数量即可得到。

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

（三）实验结果

本文首先以ImageNet-1k数据完成通用主干模型自监督预训练，然后再用上述其余数据集完成任务模型的迁移学习训练。其中表1和2是对3种不同迁移学习训练模式（模式1为“任务器强监督训练”，模式2为“任务模型强监督训练”，模式3为“任务模型不完全监督训练”，TFS指的是“Train from scratch”，即主干模型未被预训练，整个模型参数均随机初始化，从头开始训练）的对比，表3是WSTD-AP和其他算法平台在NLP句子对分类上的性能对比：

表1　CIFAR10实验结果

模型	预训练方式	训练模式	自监督训练轮次	强监督训练轮次	Acc@1(%)
ResNet50 (FP32)	对比学习	模式1	/	90	91.37
		模式1	/	30	91.19
		模式2	/	30	96.68
		模式3	30	90	97.00
		模式3	30	30	96.06
ViT-Small(FP16)	对比学习	模式1	/	90	92.81
		模式1	/	30	93.11
		模式2	/	30	无法训练
		模式3	30	90	97.77
		模式3	100	30	97.87

表2 TSL Gesture Dataset实验结果

模型	训练模式	自监督轮次	强监督轮次	Acc@1(%)
ResNet50 (FP32)	TFS	/	90	61.60
	模式1	/	90	88.92
	模式2	/	90	98.80
	模式3	30	90	91.10
	模式3	100	90	94.86

表3　花呗公开数据集实验结果

算法平台	主干模型	任务模型	模式	Acc@1(%)
WSTP-AP	BERT	BERT	模式1	75.6
Bai* 平台	未知	未知	未知	70.4

表1展示了CNN类模型和Transformer类模型的区别、不同计算量对性能的影响和不同迁移学习模式对性能的影响。从结果可见对CNN类模型

采用模式2和模式3均比模式1有更好的性能，而Transformer类模型采用模式3比模式1有更好的性能，进而验证了在数据量充足的情况下，让主干模型参与训练是能起到增益效果。从表2可看到，本文所提训练模式均比TFS训练方式具有更高的准确率，进而表明了本文所提训练技术比传统TFS方式具有明显优势。另外，由于手势数据集是一个小规模数据集，数据量不足以支持自监督训练，因此其采用模式3反而会给模型性能带来负面影响，但提高自监督训练阶段的计算量还是会带来增益效果。表3均表明了WSTP-AP所训练模型在NLP领域均比另一个人工智能算法开放平台有更好的表现。

五、总结

本文提出了一种使用弱监督训练范式且任务可解耦的人工智能算法平台WSTD-AP，其中包含了两个先进底层算法技术。最后，我们通过多种数据测试，也证明了WSTD-AP底层算法技术和所输出的模型的性能是优于其他算法技术和平台的。

参考文献：

[1] 李冰锋,段鑫鑫,杨艺,等.基于特征增强和损失优化的弱监督目标检测算法[J].兵器装备工程学报,2023(6):196-203.

[2] 高辉,邓淼磊,赵文君,等.基于弱监督的改进Transformer在人群定位中的应用[J].计算机工程与应用,2023(19):92-98.

[3] 林呈宇,王雷,薛聪.标签语义增强的弱监督文本分类模型[J].计算机应用,2023(2):335-342.

[4] Bin Zhang,Yiming Huang,Tingting Zhao.Comparison of Coarse Graining DEM Models Based on Exact Scaling Laws[J].工程与科学中的计算机建模(英文),2021(6):1133-1150.

[5] 唐晓彬,沈童.深度学习框架发展综述[J].调研世界,2023(4):83-88.

[6] 薛晨兴.国内外深度学习框架分析与研究[J].电子元器件与信息技术,2023(5):66-87.

[7] 马骏,马淑萍,胡晓光,等.深度学习框架:算法集成和产业基础[J].发展研究,2023(7):32-36.

[8] 梁宇.基于深度神经网络的数字图像取证关键技术研究[D].西安:西安电子科技大学,2020:1-80.

[责任编辑：胡大威]

Research on Weak Supervised Artificial Intelligence Algorithm Platform

Feng Yanyi[1], Zhou Wen[2], Zhang Rui[1]

(1.Optic Control Teslian (Shanghai) Information Technology Co., Ltd., Shanghai 200030,China;
2.School of Information, Wuhan Vocational College of Software Engineering, Wuhan , Hubei , 430205,China))

Abstract: In view of the high cost of pre-training model development and industry data annotation in the current open platform of artificial intelligence, In this paper, an artificial intelligence algorithm platform (Weak Supervision & Task Decoupling AI Platform, WSTD-AP) is studied, which uses weak supervision training paradigm and can decouple tasks. Unlike the traditional artificial intelligence algorithm platform based on strong supervised learning, WSTP uses large-scale unlabeled data for model training of different scales, and makes full use of the "expansion rule23" in the case of limited cost(Scaling Law), so that the model can achieve better results in downstream tasks (such as image recognition, target detection, etc.).

Key words: AI algorithm platform, weak supervision, pre-training model