

面向任务扩展的增量学习动态神经网络: 研究进展与展望

赵海燕¹, 马权益¹, 曹 健², 陈庆奎¹

(1. 上海理工大学光电信息与计算机工程学院, 上海 200093; 2. 上海交通大学计算机科学与技术系, 上海 200030)

摘 要: 增量学习是近年来机器学习领域的一个重要的研究方向, 它能高效地进行知识迁移却不产生遗忘. 与静态模型相比, 动态网络可以根据不同的输入调整其结构或参数, 从而在准确性、计算效率和适应性等方面具有显著的优势. 本文从动态架构角度出发, 根据动态网络中的自适应选择方式, 对当前增量学习模型中所涉及到动态神经网络进行了系统化的总结. 文中首先阐述了增量学习研究进展和定义, 归纳了增量学习的学习场景. 其次根据动态路由选择粒度的不同, 将增量学习的动态神经网络划分为基于任务的动态选择、基于模块化的动态选择、基于神经元的动态选择、基于卷积通道的动态选择和基于权重的动态选择, 并对常用的增量学习模型分类进行了阐述和比较. 最后归纳了一些常见数据集, 并对未来的研究方向进行展望.

关键词: 增量学习; 动态神经网络; 深度学习; 灾难性遗忘; 自适应选择

基金项目: 国家自然科学基金(No.62072301); 上海市科委科技创新计划(No.21511104700)

中图分类号: TP301.6

文献标识码: A

文章编号: 0372-2112(2023)06-1710-15

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.12263/DZXB.20221226

Dynamic Neural Network for Incremental Learning with Task Extended: Research Progress and Prospect

ZHAO Hai-yan¹, MA Quan-yi¹, CAO Jian², CHEN Qing-kui¹

(1. School of Optical-Electrical & Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China;

2. Department of Computer Science and Technology, Shanghai Jiaotong University, Shanghai 200030, China)

Abstract: Incremental learning is an important research direction in the field of machine learning in recent years. It can efficiently transfer knowledge without forgetting. Dynamic networks exhibit significant advantages in accuracy, computational efficiency, and adaptability compared to static models, as they can adjust their structure or parameters according to different inputs. From the perspective of dynamic architecture, this paper systematically summarizes the dynamic neural network involved in the current incremental learning model according to the adaptive selection method in the dynamic network. Firstly, this paper describes the research progress and definition of incremental learning, and summarizes the learning scenarios of incremental learning. Then, according to the granularity of dynamic routing selection, the dynamic neural network of incremental learning is divided into task-based dynamic selection, modular dynamic selection, neuron-based dynamic selection, convolution channel-based dynamic selection and weight-based dynamic selection. At last, some common datasets are summarized, and prospects for future research directions are discussed.

Key words: incremental learning; dynamic neural network; deep learning; catastrophic forgetting; adaptive selection

Foundation Item(s): National Natural Science Foundation of China (No.62072301); The Program of Technology Innovation of the Science and Technology Commission of Shanghai Municipality (No.21511104700)

1 引言

传统的神经网络往往在独立同分布 (Independently and Identically Distributed, IID) 的数据集上以离

线的方式训练模型. 增量学习 (Incremental Learning, IL) 研究从非 IID 数据流中学习知识, 能随着环境变化进行动态自适应学习. 传统的 IL 假设每次新到一个任

务,每个任务的数据分布是固定的,可以在当前任务上进行多次重复训练.而在线增量学习(Online Incremental Learning, OIL)假设一次到达一个小批量的数据,训练过程中无法访问当前或以前的任务中的批量数据.然而,用非平稳数据流增量更新神经网络会导致灾难性遗忘(Catastrophic Forgetting, CF)问题^[1]即模型适应新任务覆盖旧任务参数导致旧任务性能下降.IL一直寻求在学习稳定性和可塑性之间取得平衡,稳定性指保留过去知识的能力,而可塑性指适应新知识的能力.

增量学习所使用的技术大致可以分为三大类:网络正则化、记忆或数据重放、动态架构.网络正则化指对在损失函数引入额外的惩罚项或优化参数梯度来约束网络的参数更新;记忆或数据重放指模型允许访问有限容量的内存缓冲区或使用生成对抗网络(Generative Adversarial Network, GAN)生成伪数据进行数据重放;动态架构通常采用扩展网络体系结构或者通过动态路由选择子网络为每个任务分配不同参数来提高模型自适应能力.

本文对近年来适合于任务扩展场景的增量学习模型所涉及到的动态神经网络进行了系统化的分析与总结.文中总结了增量学习的相关概念,增量学习的动态架构研究现状,介绍了研究中常用的实验数据集、模型评价指标和增量学习中的应用场景,最后对未来的研究方向进行了展望.

2 增量学习概述

2.1 增量学习进展

灾难性遗忘^[1]一直是增量学习研究的重点,即当模型对新任务进行学习时会遗忘之前任务所学习的知识,为了克服此类问题,许多方法相继被提出.一种有效的手段是限制性地更新模型权重,文献[2]提出了一个知识蒸馏损失^[3]方法来限制权重更新,文献[4]则利用Fisher信息矩阵评估旧任务权重的重要性,依据重要程度更新权重.另一种有效手段是允许模型访问有限容量的内存缓冲区保存一部分旧样本或利用生成网络创建旧任务的伪示例.文献[5]存储少量旧样本,通过同时学习分类器和数据特征来减少遗忘.一些生成重放的策略^[6,7],利用生成网络模型准确地重放旧数据来消除灾难性遗忘.限制权重更新手段能一定程度上缓解遗忘问题,但过度约束网络参数,会导致新任务的学习受损.而访问有限内存缓冲区策略可能会因为实际数据的隐私策略导致不可访问,生成重放策略的缺点是训练生成模型需要花费大量的时间和内存,特别是在更复杂的训练集下.还有一种手段是利用动态架构,通常采用扩展网络体系结构或动态路由选择子网的方案来解决灾难性遗忘问题,其优势在于可为不同训练

任务动态分配结构或参数,进一步提高了模型可扩展性和自适应能力,这也是本篇文章研究的重点.近年来,随着研究的深入,一个流行的趋势是对上述手段进行结合,利用综合的方法来开展研究与其他相关综述研究相比,本研究将增量学习的研究进展更加具体化,侧重于对利用动态架构的相关工作展开进一步研究,并依据动态路由选择粒度对相关研究进行更细致化分类,文中所涉及的方法也更适合应用于异任务增量学习,具体可参考后续章节.

2.2 增量学习定义

目前对增量学习还没有形成明确、一致的定义,本文针对监督学习场景给出定义.在监督学习场景下,增量学习通常被定义为在来自顺序任务的非平稳数据上训练机器学习模型.假设训练数据集 $D=\{D_1, \dots, D_T\}$ 包含了 T 个任务,其中第 t 个任务的数据可表示为 $D_t=\{x_i^t, y_i^t\}_{i=1}^n$, n 表示第 t 个任务训练数据的数量,第 t 个任务包含输入样本 $x_i^t \in X$ 及其相应标签 $y_i^t \in Y$ 组成的数据.增量学习目标是训练一个由 θ 参数化的单一模型 $f_\theta: X \rightarrow Y$,使模型输入来自任意任务的不可见测试样本 x ,预测标签 $y=f_\theta(x) \in Y$.在大多数场景下都假设这些任务之间不存在明显的交集即假设任务间是有明显的任务边界的.最近几年,出现了无任务增量学习(task-free incremental learning)^[8,9],它假设各任务的数据不被人为设定的任务硬边界隔断,即样本可能来自于任意任务,并且不假定数据服从IID分布,甚至数据也可以来自不断变化的概率分布.在本文中,我们将大多数的学习场景放在有明显任务边界的条件下,不过多的涉及到无任务此类场景.

2.3 增量学习的学习场景

为了阐述学习场景,记 $X^{(t)}, Y^{(t)}$ 分别为任务 t 的数据样本集和类别标签集, $P(X^{(t)}), P(Y^{(t)})$ 分别表示任务 t 数据概率分布和标签概率分布.

根据在训练中是否提供任务标识、在推理中是否提供任务标识和在评估中是否共享类标签将增量学习的学习过程可以分为如下类别^[10,11]:任务增量学习(task-incremental learning)、域增量学习(domain-incremental learning)、类增量学习(class-incremental learning),近年来还出现了一种新的学习场景:任务不可知增量学习(task-agnostic learning)^[12].任务标识代表了增量学习过程中各个任务中的ID号,根据类标签是否在任务之间共享分为共享标签和非共享标签.在非共享的情况下,模型必须预测正确的任务ID和其中的正确类.在共享的情况下,模型只需要预测跨任务的正确共享标签,因此它不需要表示或预测数据来自哪个任务.对分类任务下的增量学习场景和描述如表1

所示.

表1 分类任务增量学习场景

学习场景	描述
任务增量学习	训练和推理阶段提供任务标识
域增量学习	训练阶段提供标识,推理阶段不提供;共享标签
类增量学习	训练阶段提供标识,推理阶段不提供;非共享标签
任务不可知增量学习	训练和推理阶段均不提供任务标识;共享标签

2.3.1 任务增量学习

任务增量学习(task-incremental learning)是最简单的增量学习场景,在该场景下,模型在训练和推理阶段都给出任务标识,不同时刻收集的数据属于不同的任务.由于总是提供任务标识,因此在此场景中可以使用特定于任务的组件来训练模型.此场景中使用的典型网络架构具有“多头”输出层,这意味着每个任务都有自己的输出单元,但网络的其余部分可以在任务之间共享.任务增量学习的基本假设可以定义为 $P(X^{(t)}) \neq P(X^{(t+1)})$; $P(Y^{(t)}) \neq P(Y^{(t+1)})$ 即不同时刻的任务数据和标签均来自于不相同的分布,与不同的任务对应.

2.3.2 域增量学习

域增量学习(domain-incremental learning)是指不同时刻到达的数据属于同一任务的相同类别,但输入数据的分布发生了变化,不同时间片上的数据属于不同的域.在该场景下,在训练阶段提供任务标识,推理阶段不提供任务标识,并且提供共享标签.域增量学习的基本假设定义为 $P(X^{(t)}) \neq P(X^{(t+1)})$; $Y^{(t)} = Y^{(t+1)}$ 即不同时刻的任务数据和标签均来自于相同的分布,与不同的任务对应.

2.3.3 类增量学习

在类增量学习(class-incremental learning)的训练过程中,在不同时间段所收集的数据均属于同一分类任务的不同类别,且类别没有交叉.在该场景下,任务

标识只在训练阶段给出,在推理阶段不提供,因此类增量模型不仅要推断输入属于哪个任务,还要进一步推断任务中的类别,这就要求模型在学习过程中能够自适应地增加新分类的类别,其基本假设可以表示为 $P(X^{(t)}) \neq P(X^{(t+1)})$; $P(Y^{(t)}) \neq P(Y^{(t+1)})$; $Y^{(t)} \subset Y^{(t+1)}$.

2.3.4 任务不可知增量学习

任务不可知增量学习(task-agnostic learning)^[12]是一种泛化能力最强,也是最有挑战性的增量学习场景.在该场景下,在训练和推理阶段都不提供任务标识,仅提供共享标签.不同时刻收集的训练数据和标签分布不一致,在推理阶段,测试数据以及对应的分类标签也不同于任意一个时刻的训练数据的场景.因此,这种学习方式要求模型学到的特征能够容易地泛化到任意新场景上,并且不会降低在先前任务上的训练表现.任务不可知增量学习可以表示为 $P(X^{(t)}) \neq P(X^{(t+1)})$; $P(Y^{(t)}) \neq P(Y^{(t+1)})$; $P(X_{(\text{test})}^{(t)}) \neq P(X_{(\text{train})}^{(t+1)})$; $Y_{(\text{test})} \neq Y_{(\text{train})}$.

3 增量学习中的动态架构

目前研究的增量学习方法中,存在着诸多的动态架构模型.根据动态网络中的路由选择粒度,将增量学习中的动态架构分为:基于任务的动态选择、基于模块化的动态选择、基于神经元的动态选择、基于卷积通道的动态选择和基于权重的动态选择.依据此分类策略,图1对近年来流行的面向增量学习的动态神经网络架构做了总结,并分类介绍一些经典方法模型和后续的优化方法.

模型适用的增量学习场景,主要取决于模型自身的框架设计以及数据的处理方式.本文在参考了部分模型原文的实验步骤后,对分类任务下部分经典模型适用的增量学习场景进行了总结,主要包括了任务增量、域增量和类增量场景,不过多涉及到任务不可知增量场景,如表2所示.

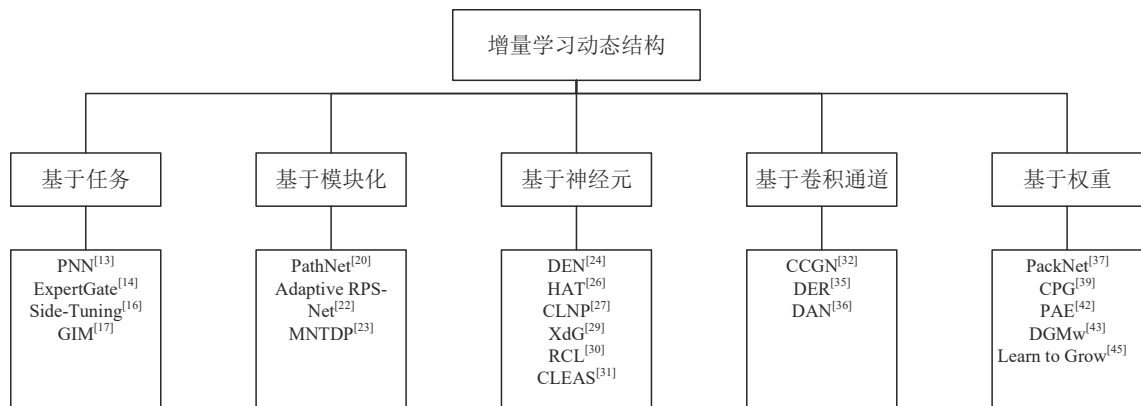


图1 增量学习动态结构分类示意图

表 2 部分经典模型适用的增量学习场景

分类策略	模型名称	适用增量学习场景
基于任务	PNN ^[13]	任务增量
	ExpertGate ^[14]	任务增量
	Side-Tuning ^[16]	任务增量
	GIM ^[17]	任务增量/类增量
基于模块化	PathNet ^[20]	域增量
	Adaptive RPS-Net ^[22]	类增量
	MNTDP ^[23]	域增量/类增量
基于神经元	DEN ^[24]	域增量/类增量
	CLNP ^[27]	任务增量/域增量/类增量
	RCL ^[30]	域增量/类增量
	CLEAS ^[31]	域增量/类增量
基于卷积通道	CCGN ^[32]	任务增量/类增量
	DER ^[35]	类增量
基于权重	PackNet ^[37]	域增量/类增量
	CPG ^[39]	域增量/类增量
	PAE ^[42]	域增量/类增量

3.1 基于任务的动态选择

基于任务的动态选择策略通常采用扩展基础网络的方式为新任务分配新的任务网络. 各个任务网络间以并列方式相互排列, 可根据任务标识动态选择对应网络进行训练或推理. 因此基于此类策略的网络参数往往会随着任务数量呈线性增长, 此类网络也在早年应用较多.

3.1.1 渐进式网络

Rusu 等人提出了渐进式网络 (Progressive Neural Network, PNN)^[13], 通过为新任务分配固定数量的神经元 (滤波器) 和网络层来扩展神经网络体系结构. 为了减少灾难性遗忘和使网络具备一定的迁移能力, PNN 冻结了网络权重参数和在旧任务权重与新任务权重中采用非线性横向连接的适配器来共享权重. 这种非线性横向连接在稠密层中采用包含单个隐藏层的多层感知机 (MultiLayer Perceptron, MLP) 来实现, 而在卷积层中, 则使用 1×1 卷积进行处理, 两者的作用都是为了降维来保持输入的维度统一.

假设一个渐进式网络总共有 L 层, 第 $i (i \leq L)$ 层隐藏层表示为 $\mathbf{h}_i^{(t)}$, t 为当前需要学习的任务. 当训练第 t 个任务参数 $\theta^{(t)}$ 时, 前一个网络参数 $\theta^{(t-1)}$ 被“冻结”, 并将第 t 个任务隐藏层 $\mathbf{h}_i^{(t)}$ 以非线性横向连接方式连接到扩展到前面网络中. 第 t 个任务隐藏层表示如式 (1) 所示:

$$\mathbf{h}_i^{(t)} = f \left(\mathbf{W}_i^{(t)} \mathbf{h}_{i-1}^{(t)} + \sum_{j < t} \mathbf{U}_i^{(t,j)} \mathbf{h}_{i-1}^{(j)} \right) \quad (1)$$

其中, $\mathbf{W}_i^{(t)}$ 为第 t 个任务网络第 i 层的权重矩阵, $\mathbf{U}_i^{(t,j)}$ 为

第 j 个任务网络第 $i-1$ 层到第 t 个任务网络第 i 层的非线性横向连接.

3.1.2 专家门控

Aljundi 等人提出了专家门控 (expert gate)^[14] 模型, 专家门控利用自编码器 (AutoEncoder, AE), 为每个任务网络学习与其输入类似的输出. 这种自编码器首先对输入 x 进行包含标准化和 Sigmoid 函数的预处理操作, 随后将数据传入到一个由全连接层和修正线性单元 (Rectified Linear Unit, ReLU)^[15] 层组成的编码器和由一个全连接层和 Sigmoid 函数组成的解码器中. 根据输入与输出之间的重构误差, 衡量输入与任务特征间的相关性. 当训练一个新任务 t 时, 利用任务间相关性, 选择最相关的专家任务网络采用微调 (fine-tune) 或者不遗忘 (Learning Without Forgetting, LWF)^[2] 等方法来扩展和训练新网络. 式 (2) 用于计算两个任务之间相关性:

$$\text{Rel}(T_t, T_a) = 1 - \left(\frac{\text{Er}_a - \text{Er}_t}{\text{Er}_t} \right) \quad (2)$$

其中, Er_t 和 Er_a 表示当前任务 t 和另一任务 $a (a < t)$ 平均重构误差, 该任务关系系数越大, 代表任务之间越相关. 在推理阶段时, 在不同任务的自动编码器后, 添加了一个带有温度系数的 Softmax 层^[3], 通过传入测试数据, 加载最有置信度的专家模型, 从而对输入进一步分类.

3.1.3 分析比较

渐进式神经网络^[13]为新任务分配固定数量的神经元 (滤波器) 和网络层来扩展体系结构, 并利用非线性横向连接到先前网络共享权重. 这种渐进式扩展方案和专家门控^[14]一样, 会造成任务数量与模型结构复杂度成正比, 最终可能会生成一个具有高冗余的过于复杂的网络, 缺乏一定的可扩展性. 而且在训练和推理阶段都需要提供任务标识, 只适用于任务增量的场景. 2019 年提出了一种侧调 (side-tuning)^[16] 网络, 该方法训练一个轻量级的侧网络来适应一个预训练的基础网络. 在给定预训练的基模型 $B(x)$ 的情况下, 侧调以求和的方式将侧模型 $S(x)$ 与 $B(x)$ 相结合, 目标任务的表示形式为 $B(x) \oplus S(x) = \alpha B(x) + (1 - \alpha) S(x)$, 其中 α 为一个与任务相关性的可学习参数. 侧调消除了 PNN 中的横向连接, 使其更加简单, 适用于更多的问题. 在增量学习的场景下, 每一个任务对应一个侧网络, 由于侧调与任务顺序无关, 所以训练不会随着训练的进行而减慢. (Gated Incremental Memories, GIM)^[17] 将渐进式网络与专家门控进行结合, 提出一种增量学习下的循环神经网络.

3.2 基于模块化的动态选择

基于此类策略的模型, 在网络中使用模块化的设

计理念. 模块可以是任何小型神经网络, 如常见的残差网络 (Residual Network, ResNet)^[18] 块、稠密连接网络 (Dense convolutional Network, DenseNet)^[19] 块等, 每一个任务网络通常由诸多神经模块组合而成, 这些模块可以从过去的任务中迁移知识, 也可以为新任务训练新知识. 学习一个任务可以简化为要重用哪些过去的模块, 以及要实例化哪些新模块来解决当前的任务.

3.2.1 PathNet

Fernando 等人于 2017 年提出的 PathNet^[20]. 假设 PathNet 网络有 L 层, 每层有 M 个模块, 每个模块为一个小型神经网络 (如卷积层、全连接层、激活函数等), 各个层之间以一种模块求和机制将该层模块输出传递到下一层的活动模块上. 此模型可以应用于强化学习和监督学习场景, 下面以监督学习的场景为例.

首先对神经网络进行随机初始化, 先随机选择一组路径, 每个路径为 $N \times L$ 矩阵, 用来描述被激活的模块, 其中 N 表示每层最多包含的模块数 ($N < M$), L 表示网络的层数. 然后使用二元锦标赛遗传算法^[21]来选择优化路径, 方式为将一个随机路径与另一个随机路径比较误差, 误差小的路径以 $1/(N \times L)$ 概率产生突变, 为避免陷入局部最优点, 利用局部邻域在 $N \times L$ 矩阵中选择一个元素为每一个基因型元素加上一个范围为 $[-2, 2]$ 的整数. 当学习下一任务时, 固定当前任务选择到的路径, 即该路径上的模块权重和偏差被冻结, 然后初始化一组新的路径, 同样采用锦标赛选择遗传算法进行路径的选择.

3.2.2 Adaptive RPS-Net

Adaptive RPS-Net (Adaptive Random Path Selection Network)^[22] 采用了一种随机路径选择方法, 通过路径共享和重用, 为新任务自适应选择最优路径. Adaptive RPS-Net 网络以模块化形式构造路径, 网络中的每一层中包含了相同数量的模块, 每个模块可以是单个 ResNet^[18] 块. 同时利用并行残差设计, 使用一个跳过连接使这些模块与其并行堆叠, 目的是支持多个任务同时进行增量训练而互不干扰. 在每层后面使用元素加法将所有模块化输出和跳过连接输出组成在一起, 以聚合从不同路径获得的互补的特定于任务的特征. 同时引入一种新的路径饱和度量方法, 用路径饱和系数作为一个简单的度量来决定是否需要切换当前路径. 对于给定的阈值 th , 在对一个任务进行训练后, 我们简单地计算当前路径配置中的饱和系数. 如果网络饱和度高于阈值 th , 则随机采样一组 N 条新路径, 同时固定旧路径参数, 然后为下一个任务并行训练 N 个模型并选择最优的一条路径训练模型.

3.2.3 分析比较

PathNet^[20] 利用遗传算法为任务选择模块来规划路径, 而 Adaptive RPS-Net^[22] 则采用了随机路径选择方法. PathNet 以简单的前馈方式添加所有模块, 而 Adaptive RPS-Net 将模块作为残差连接添加到标识路径上, 即使所有模块都饱和, 该标识路径也可以随时学习特征. 而 MNTDP (Modular Networks With Task Driven Prior)^[23] 则利用任务驱动先验优先于指数搜索空间的所有可能的方式来组合模块, 该先验只允许前一任务体系结构最好特征的局部扰动.

3.3 基于神经元的动态选择

此类选择策略侧重给模型提供神经元级别的控制, 通过扩展或舍弃任务相关神经元来达到扩展网络和剪枝网络的目的. 值得注意的是, 此类模型往往也适用于卷积网络, 此节侧重于神经元级别动态网络说明, 而有关 CNN 场景会在 3.4 节说明.

3.3.1 动态可扩展网络 DEN

Yoon 等人提出一种深度网络体系结构动态可扩展网络 (Dynamically Expandable Net-work, DEN)^[24], 它可以在训练一系列任务时动态决定网络容量, 学习任务间紧凑的重叠知识共享结构. 学习任务时, DEN 依次执行选择性再训练、动态拓展网络以及分裂与复制三个阶段以在线方式有效地训练网络. 在增量学习场景下, 当对当前任务 t 进行训练时, 当前模型参数 \mathbf{w}' 的求解如式 (3) 将转化为最优化问题:

$$\min_{\mathbf{w}'} L(\mathbf{w}'; \mathbf{w}^{t-1}, D_t) + \lambda R(\mathbf{w}'), t = 1, 2, \dots, T \quad (3)$$

其中, $D_t = \{x_i, y_i\}_{i=1}^{N_t}$ 表示任务训练集, L 表示当前任务的损失函数, \mathbf{w}' 是任务 t 的模型参数, λ 是正则化参数, $R(\mathbf{w}')$ 是正则化项.

动态可扩展网络 DEN 架构如图 2 所示, 当前任务 t 的任务网络神经元以红线相连. 在训练过程中, 首先对模型进行选择性再训练, 使用 L1 正则化训练第 1 个任务网络, 以构建模型稀疏连接, 在增量学习的过程中, 将始终保持 \mathbf{w}^{t-1} 的稀疏性. 利用这种稀疏连接, 可以使用广度优先搜索识别到受训练影响的神经元进行选择再训练. 在完成选择性再训练后, 若网络损失值 L_t 仍低于超参数阈值 τ , 此时需要引入额外的神经元扩展网络. 动态拓展网络预先在每一网络层中扩展 k 个神经元, 再利用组稀疏正则化 (group sparse regularization)^[25] 来动态决定在层中丢弃一些不必要的神经元, 以最大限度地利用网络容量. 在分裂与复制阶段, 可以计算每个神经元的语义漂移量 ρ'_i , 若该值高于超参数阈值 σ 时, 通过分裂和复制神经元, 进一步防止因为引入新的神经元引起的语义漂移.

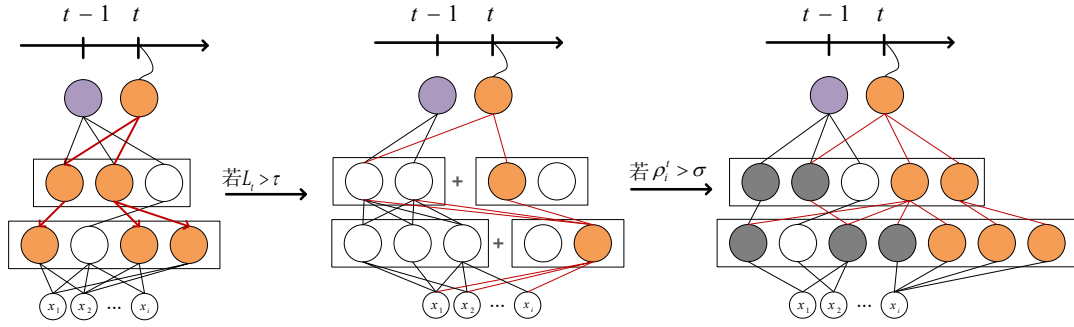


图2 DEN架构图

3.3.2 面向任务的硬注意力机制

Serra 等人提出一种面向任务的硬注意力机制 (Hard Attention to the Task, HAT)^[26],来解决任务增量场景下的灾难性遗忘问题. 模型采用一种分层注意力机制来学习当前的任务 t . 除了最后一层 L 使用二进制硬编码之外,其余的网络层 $l \in \{1, \dots, L-1\}$ 采用相同的学习过程. 当给定 l 层的输出单元 \mathbf{h}_l ,按顺序与 \mathbf{a}_l^t 进行同或运算 $\mathbf{h}_l' = \mathbf{a}_l^t \odot \mathbf{h}_l$, \mathbf{a}_l^t 是单层任务嵌入 \mathbf{e}_l^t 的门控形式,形式为 $\mathbf{a}_l^t = \sigma(\mathbf{s} \mathbf{e}_l^t)$. 其中 $\sigma(x) \in [0, 1]$ 是一个 Sigmoid 门函数, s 为正标度参数. 通过这种的门控机制可以形成二元注意力掩码 (binary attention masks),来选择性地激活或禁用每层神经元的输出. 在训练过程中,模型根据之前所有任务学习的硬注意力机制来约束梯度更新. 因此,为了获得直到当前任务的注意力机制向量,在学习了任务 t 并且获得 \mathbf{a}_l^t 之后,递归地计算 $\mathbf{a}_l^{\leq t} = \max(\mathbf{a}_l^t, \mathbf{a}_l^{\leq t-1})$. 为了对第 $t+1$ 任务训练,同时不遗忘之前的任务知识,使用当前层和之前层的累积注意力的最小值来对第 l 层参数进行更新,如式(4):

$$\mathbf{g}_{l,ij}' = \left[1 - \min(\mathbf{a}_{l,i}^t, \mathbf{a}_{l-1,j}^{\leq t}) \right] \mathbf{g}_{l,ij} \quad (4)$$

其中下标 i, j 分别表示第 l 层的输入和第 $l-1$ 层的输出. HAT 采用一种注意力机制可学习掩码实现神经元级别的动态选择,顺序学习一系列任务.

3.3.3 分析比较

DEN 在保持原有体系结构参数不变的情况下,动态扩展网络以适应新的任务. 并使用组稀疏正则化技术^[25]保证神经元模型的稀疏性,通过策略性地选择一些旧的神经元进行再训练,只在必要时才添加新的神经元. 然而,由于旧神经元的再训练,也会出现遗忘问题并且 DEN 的性能对各种超参数非常敏感,包括正则化参数和阈值系数. Golkar 等人提出的 CLNP (Continual Learning via Neural Pruning)^[27]在固定容量的模型中,基于神经元模型的稀疏化提出了一种终身学习方法,该方法使用一种基于激活的神经剪枝稀疏化方案来训练使用一小部分的模型. Masse 等人提出了上下文相关选通门 (context-dependent gating)^[28],使得稀疏的、

大部分不重叠的单元集对任何一个任务都是有效的,算法由一个额外的信号组成,该信号对每个任务都是唯一的,以门控形式随机选择的 $X\%$ 隐藏单元的活动乘以 0,而保持其余 $(1-X\%)$ 的活动不变. 将上下文相关选通门一些突触稳定方法,如 SI (Synaptic Intelligence)^[29]、EWC (Elastic Weight Consolidation)^[4] 配合使用,将会变得更有效. RCL (Reinforced Continual Learning)^[30] 和 CLEAS (Continual Learning with Efficient Architecture Search)^[31] 都设计使用网络结构搜索 (Neural Architecture Search, NAS) 提供神经元水平控制,通过重用部分旧神经元和添加适当的新神经元优化新的架构.

3.4 基于卷积通道的动态选择

此类方法可以根据样本自适应地激活不同的卷积通道,基于门函数、特征激活等方法动态执行通道级别的控制.

3.4.1 CCGN

Abati 等人提出了 CCGN (Conditional Channel Gated Networks)^[32],算法提供一种通道级的门控方法来选择性激活通道,通过学习任务专用的选通模块,有效应对任务增量和类增量场景. 在任务增量的场景下, \mathbf{h}^l 和 \mathbf{h}^{l+1} 为第 l 层和第 $l+1$ 层卷积层的输入. 训练任务 t 的通道级的门控可表示为 $\hat{\mathbf{h}}^{l+1} = G_c^l(\mathbf{h}^l) \odot \mathbf{h}^{l+1}$, 其中 $G_c^l(\mathbf{h}^l) = (g_1^l, \dots, g_{c_{out}}^l)$, 其中 $g_i^l \in \{0, 1\}$, \odot 为通道上的乘法, c_{out}^l 表示第 l 层的输出通道数. 为解决二进制掩码在反向传播过程中不可微问题,利用 Gumbel-Softmax^[33] 抽样和直通估计器^[34] 得到梯度的有偏估计. 而在类增量场景下,使用所有选通模块 $(G_1^l, \dots, G_{c_{out}}^l)$, 前向传播得到选通层输出 $(\hat{\mathbf{h}}_1^{l+1}, \dots, \hat{\mathbf{h}}_{c_{out}}^{l+1})$, 这样依次传递. 利用该机制在网络中生成并行计算流,共享相同的层,为每个层激活选择不同的通道,最后通过任务分类器选择到对应的任务输出头.

当学习一系列任务 $T = \{T_1, \dots, T_N\}$, 为了同时应对任务增量和类增量的场景,可将对类和任务预测进行联合优化,如式(5)所示:

$$\max_{\theta} E_{t \sim T} \left\{ E_{(\mathbf{x}, \mathbf{y}) \sim T_t} [\log p_{\theta}(\mathbf{y}, t | \mathbf{x})] \right\} = E_{t \sim T} \left\{ E_{(\mathbf{x}, \mathbf{y}) \sim T_t} [\log p_{\theta}(\mathbf{y} | \mathbf{x}, t) + \log p_{\theta}(t | \mathbf{x})] \right\} \quad (5)$$

其中, T_t 表示第 t 个任务, θ 为网络的参数, \mathbf{x} , \mathbf{y} 和 t 分别是样本的数据、标签和与任务 t 相关联的随机变量. $\log p(\mathbf{y} | \mathbf{x}, t)$ 表示根据任务进行类别分类, $\log p(t | \mathbf{x})$ 依赖于任务分类器, 预测观察到的样本属于哪个任务.

3.4.2 DER

DER (Dynamically Expandable Representation)^[35] 将基于内存回放和基于动态网络扩展结合来解决类增量问题. 模型由超特征提取器 Φ 和分类器 H_t 组成, 采用将特征学习和分类器学习进行解耦以提升模型的稳定性和可塑性. 为了降低类别增加带来的参数增量, 模型采用了一种可微通道级掩码剪枝方法, 根据特征的复杂性实现动态剪枝. 在每一个增量步骤中, 用一个新的特征提取器 F_t 扩展超特征提取器 Φ_t 网络, 同时保持以前特征提取器的参数不变. 通道级剪枝表示为 $\mathbf{f}_i' = \mathbf{f}_i \odot \mathbf{m}_i$, 其中 \mathbf{f}_i 为输入在特征提取器 F_t 经过卷积层 l 的输出, \mathbf{m}_i 为第 l 层卷积的掩码, 掩码中的第 i 个值表示为 $m_i' \in [0, 1]$, \mathbf{f}_i' 为经过掩码后的特征图, \odot 为通道级乘法. 为了使 \mathbf{m}_i 的值落入区间 $[0, 1]$, 采用了门控函数 $\mathbf{m}_i = \sigma(\mathbf{s} \mathbf{e}_i)$, σ 使用了 Sigmoid 门控函数, \mathbf{e}_i 是可学习的掩码参数, s 为正标度参数, 这点上与 HAT (Hard Attention to the Task)^[26] 很相似.

所有特征提取器产生的特征级联合并在一起, 并被送入分类器进行类预测. 同时为了使网络学习新类的多样性和判别性特征, 设计了一个区分新旧类的辅助损失 $L_{\text{ER}} = L_{H_t} + \lambda_a L_{H_t^a}$ 其中 H_t^a 用来鉴别新旧类的辅助分类器, λ_a 为控制辅助分类效果的超参数. 分类器学习阶段, 为了以减少不平衡训练引入的分类器权重的偏差, 首先用随机权重重新初始化分类器, 然后从当前可用的数据中采样一个类平衡子集, 并只用交叉熵损失训练分类器.

3.4.3 分析比较

CCGN^[32] 利用一个可学习门控掩码, 根据输入动态特征动态激活通道. DER^[35] 也采用了类似的学习方法, 通过由超特征提取器和线性分类器组成的网络进行特征提取和分类, 同时为了去除模型冗余并学习新类的紧凑特征, 采用了一种可微分的基于通道级掩码的剪枝方法来动态剪枝网络. 在 CCGN 中, 由于只有部分层的参数被冻结, 学习后的特征表示可能会在步骤中缓慢退化. 而 DER 保持之前学习的表示不变同时使用新的特征提取器参数化新特征来扩充. 这使得模型能够在之前学习的表示的子空间中保留旧概念的内在结

构, 并通过最终的分器重用该结构以减少遗忘. 深度自适应网络 (Deep Adaptation Networks, DAN)^[36] 扩展了每个新任务的体系结构, 新任务模型中的每一层都是基模型相应层中原始过滤器的稀疏线性组合.

3.5 基于权重的动态选择

此类模型以一种细粒度的选择策略, 实现权重级别的模型剪枝和网络容量拓展.

3.5.1 PackNet

Mallya 等人提出的 PackNet (Pack Networks)^[37], 当向单个深度神经网络顺序添加任务时, 利用基于权重的网络剪枝方法来释放网络中的冗余参数. 这些冗余参数将会被重用学习训练新任务, 冻结上一任务网络权重参数以减缓灾难性遗忘. 在训练阶段, 首先初始化任务参数, 依据 DSD (Dense Sparse Dense)^[38] 剪枝策略, 将卷积层或全连通层的权重按绝对值大小排序, 然后按比例去掉最小的一组权重值即通过权重剪枝释放冗余参数. 剪枝完成后, 重新训练旧任务网络来保证网络性能. 当学习新任务时, 这些释放的参数被重新使用用来训练新网络. PackNet 将每一个任务对应权重矩阵存储进一个用二进制表示的稀疏掩码中, 在推理阶段, 这种稀疏掩码与过滤器权重参数执行矩阵乘法操作, 动态激活或舍弃相应权重. 图 3 展示了顺序学习两个任务 PackNet 的模型流程, 其中灰色圆圈表示任务的初始化网络参数权重, 白色圆圈为释放的冗余权重, 蓝色和橙色圆圈为被重用于训练新任务网络权重. PackNet 模型是与任务训练顺序相关, 并且模型容量相对固定.

3.5.2 CPG

Hung 等人提出的 CPG (Compacting, Picking and Growing)^[39] 模型结合了权重剪枝、临界权重选择和权重网络扩展的思想学习新任务. 首先, 保持旧任务权重不变, 对新任务权重使用逐步剪枝 (gradual pruning)^[40] 来压缩模型, 逐步剪枝技术并不是按比例去掉权重而是以先修剪小部分权重后重新训练剩余权重的方式来迭代恢复性能, 直到满足剪枝条件为止. 接下来, 参照 Piggyback^[41] 方法学习一个实数掩码 \hat{M} , 并应用一个阈值函数构造二进制掩码 $M \in \{0, 1\}$. 通过掩码 M 选择和重用一些对新任务至关重要的旧任务权重 (临界权重), 这些临界权重与释放的冗余权重会一起用来训练新任务. 如果新任务的训练没有达到精度和性能要求, 可以通过在模型中额外的权重, 如在卷积层中添加新滤波器或在全连通层中添加新的神经元来扩展体系结构, 然后依次使用逐步剪枝和重新训练使直至模型收敛. 因此, 在学习一系列任务时, CPG 通过压缩模型 \rightarrow 挑选权重 \rightarrow 扩展权重的循环方式来学习紧凑模型结构.

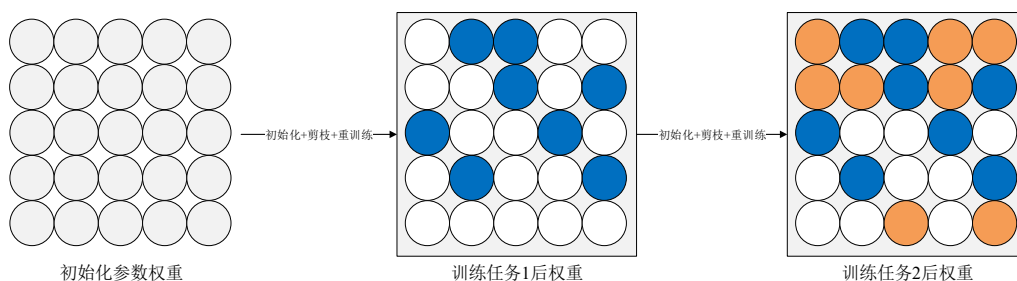


图3 PackNet流程图

3.5.3 分析比较

PackNet^[37]与CPG^[39]都利用了权重剪枝释放冗余权重.不同的是,PackNet对权重使用固定比例的剪枝策略,并将所有旧任务固定权重和剪枝释放的冗余权重联合用于新任务训练,并无模型拓展,因此模型容量相对固定.CPG做了改进,使用了逐步剪枝^[40]技术来压缩模型和拓展权重来增加模型容量,这与Hung等人提出的PAE(Pack And Expand)^[42]较为相似.除此之外,受Piggyback^[43]的启发,CPG通过学习一个可微掩码从旧参数中挑选一部分关键的权重,将挑选出的旧权重和新添加的新权重都用来学习新任务.Ostapenko等人提出动态生成记忆DGM(Dynamic Generative Memory)^[43],依赖于条件生成网络^[44],通过存储以往数据分布,将先前任务的合成样本和新任务的真实样本

一起训练模型.而DGMw(Dynamic Generative Memory weights)^[44]利用在生成器的权值上学习一组二进制掩码,从而在训练过程中逐步学习新的信息,同时为了保持层中用于每个任务训练的自由权重数量不变,通过动态扩展权重来保证足够的模型容量.Li等人提出Learn to Grow^[45]框架将模型结构学习和参数估计分离,利用网络体系结构搜索来学习网络结构.

4 实验数据集和评价准则

4.1 实验数据集介绍

考虑到增量学习大多数应用场景为图像分类,因此下面列举增量学习中用于图像分类的常见数据集.同时结合增量学习的不同学习场景,对这些常见数据集进一步的分类介绍,参数如表3所示.

表3 增量学习常见分类数据集介绍

数据集	图像尺寸	训练集数量	测试集数量	类数量	适用场景
CUB-200 Birds	-	5 994	5 794	200	任务增量
OxfordFlowers_102	-	-	-	102	任务增量
Split CIFAR100	32×32×3	50 000	10 000	100	类增量
Split MiniImageNet	84×84×3	50 000	10 000	100	类增量
CORe50-NC	128×128×3	-	-	50	类增量
Rotation MNIST	28×28×3	55 000	10 000	10	域增量
Permutation MNIST	28×28×3	55 000	10 000	10	域增量
CORe50-NI	128×128×3	120 000	44 972	50	域增量
Label-Permuted MNIST	28×28×3	55 000	10 000	10	任务不可知增量

(1) 任务增量数据集

CUB-200 Birds 200^[46]是一个细粒度图像数据集,包含200种鸟类的照片.该数据集共11788张鸟类图像,包含200类鸟类子类,其中训练数据集有5994张图像,测试集有5794张图像,每张图像均提供了图像类标记信息.

OxfordFlowers_102^[47]数据集由102类产自英国的花卉组成.每类由40-258张图片组成.

(2) 类增量数据集

Split CIFAR-100是通过将CIFAR100^[48]数据集拆分成20个具有不相交类的任务来构造的,每个任务有5个类.每个任务有2 500幅32×32×3图像用于训练,

500幅图像用于测试.

Split MiniImageNet基于MiniImageNet^[49]数据集,有100个类,分成20个不相交的任务.每个任务包含5个类,每个类由500幅用于训练的84×84×3图像和100幅用于测试的图像组成.

CORe50-NC^[50]是一个为9个任务和50个类的类增量学习而设计的数据集,第一个任务中有10个类,随后的8个任务中有5个类.

(3) 域增量数据集

Rotation MNIST^[51]和Permutation MNIST^[4]是基于MNIST^[52]用于域增量学习的常用数据. Permutation MNIST是参考某个固定的排列,通过重新排列像素来

创建任务,而 Rotation MNIST 则通过对数字旋转固定的角度创建任务.

CORe50-NI^[50]是一个广泛评估领域增量学习的数据集,有8个任务,每个任务有50个类的大约15 000个训练图像,具有不同类型的非平稳性,包括光照、背景、遮挡、姿态和尺度.所有任务只有一个测试集,其中包含44 972个图像.

(4)任务不可知增量数据集

Label-Permuted MNIST 是通过固定的置换对 MNIST 中标签中的类进行洗牌来创建一个新的任务,而非图像中的像素.这一变化的原因是为了确保不可能简单地根据图像来猜测当前的任务.

4.2 实验评价准则

对于增量学习算法的性能可以从以下几个方面进行评估:

4.2.1 准确性

文献[53]提出一种称为平均准确性的估计方法,假设 $a_{i,j} \in [0,1]$ 是模型在任务 i 上训练后,模型在任务 j 上的分类准确性能.任务 T 的平均精确度定义为

$$A_T = \frac{1}{T} \sum_{j=1}^T a_{T,j} \quad (6)$$

文献[54]给定训练测试样本精度矩阵 I ,其中每个元素 $I_{i,j} \in \mathbf{R}^{T \times T}$ 为观察任务 i 的最后一个样本得到的模型在任务 j 上的测试分类精度.模型的准确性是通过考虑矩阵 I 的对角元素,实现对训练集和测试集的平均精度进行考虑.准确性 A 为

$$A = \sum_{i>j}^T I_{i,j} / \frac{T(T+1)}{2} \quad (7)$$

文献[53]主要是为了在最后一个任务结束时评估模型的性能,而在文献[54]中,该准确性准则考虑到模型在每一时间步的性能的准确性指标,这样能够更好地考虑连续学习模型的动态性能.

4.2.2 遗忘率

为了评估模型的遗忘程度,HAT^[26]引入遗忘率概念. f_j^i 表示是在任务 i 上训练模型后对任务 j 的遗忘程度,文献[53]对遗忘率的定义如下:

$$f_j^i = \max_{l \in \{1, \dots, i-1\}} (a_{l,j} - a_{i,j}) \quad (8)$$

其中 $a_{i,j}$ 为模型在任务 i 上训练后,在任务 j 上的分类准确率.任务 T 的平均遗忘率 F_T 度量定义为

$$F_T = \frac{1}{T-1} \sum_{j=1}^{T-1} f_j^T \quad (9)$$

4.2.3 知识正向与反向迁移能力

Lopez 等人^[51]在对增量学习的评估中,引入正向迁移与反向迁移能力概念,用来衡量对模型的知识迁移性能.知识正向迁移(ForWard Transfer, FWT)是衡量学

习任务对未来任务的影响.根据之前文献[51]对准确性的度量准则,文献[53]进一步修改了训练-测试准确度,其中 $I_{i,j}$ 的平均准确性高于准确率矩阵 I 的主对角线.因此定义 f_{FWT} 为

$$f_{\text{FWT}} = \frac{\sum_{i<j}^T I_{i,j}}{\frac{T(T-1)}{2}} \quad (10)$$

反向迁移能力(BackWard Transfer, BWT)是衡量模型学习了一个新的任务后对先前任务的影响.当需要在多任务或流数据背景下进行学习时,往往就需要模型对其反向迁移性能的评估.式 f_{BWT} 定义在学习了任务 i 之后,在同一测试集的最后一个任务结束时,对任务 j ($j < i$) 计算准确度.在此,与准确性的度量准则类似,将其扩展到对每个任务的后向迁移求平均值:

$$f_{\text{BWT}} = \frac{\sum_{i=2}^T \sum_{j=1}^{i-1} (I_{i,j} - I_{j,j})}{\frac{T(T-1)}{2}} \quad (11)$$

4.2.4 内存规模度量

根据每个任务 i 的参数 θ 的数量来量化每个模型的存储器的大小,记为 $\text{Mem}(\theta_i)$,相对于第1个任务内存大小 $\text{Mem}(\theta_1)$,随着时间推移,模型对任务不断地学习,内存规模大小不应该增长过快.因此,将模型的内存规模大小(Memory Size, MS) f_{MS} 定义^[54]为

$$f_{\text{MS}} = \min(1, \frac{1}{T} \sum_{i=1}^T \frac{\text{Mem}(\theta_i)}{\text{Mem}(\theta_1)}) \quad (12)$$

4.2.5 计算效率

文献[54]定义任务之间的平均计算效率 f_{CE} 为

$$f_{\text{CE}} = \min \left(1, \frac{1}{T} \sum_{i=1}^T \frac{\text{Ops} \uparrow \downarrow (D_i) \times \varepsilon}{\text{Ops}(D_i)} \right) \quad (13)$$

其中, $\text{Ops}(D_i)$ 是指在 D_i 进行训练时所需要的乘法和加法运算总次数;而 $\text{Ops} \uparrow \downarrow (D_i)$ 是指 D_i 进行一次正向和反向传播所需要的运算次数.为了避免 $\text{Ops} \uparrow \downarrow (D_i)$ 过小,我们通常对其统一乘以一个大于1的缩放因子 ε ,它与学习 D_i 所需要的 epoch 次数相关.该指标本质上反应了运算中有多少是直接用以进行正向和反向传播的.

4.3 对比实验总结

鉴于不同的模型方法在数据集选取、学习场景选择、超参数选择、实验环境等方面具有一定的差异,很难以一种直观的角度对不同的模型方法进行对比,因此本文对一些方法的实验效果进行了总结.

在 MNTDP^[23] 实验中, MNTDP 相比, PNN^[13] 展现了较好的平均准确率,但同时需要较多的内存和计算量, RCL^[30] 和 HAT^[26] 的平均准确率较低,计算量也较大.

在 CLEAS^[31] 实验中比较了 CLEAS, RCL, DEN^[24] 等方法, 在准确率上 CLEAS 取得了比较明显的优势. 实验中又详细比较了 CLEAS 和 RCL 在神经元复用和神经元分配方面的表现, CLEAS 相对于 RCL 的优势在于使用了更少的神经元对模型进行扩展, 以及对旧神经元的选择复用更加的合理. DER^[35] 实验中展示了与基线模型相比, 得益于通道级的剪枝策略, 可以使用更少的参数来提高平均准确率, 并在知识正向与反向迁移能力取得优势. CCGN^[32] 实验中对不同增量场景下的实验效果. 在任务增量下, CCGN 和 HAT 都能取得不错的平均准确率, 在类增量场景下, DGMw^[43] 利用生成记忆进行类增量, 在简单数据集下有非常好的平均准确率, 但随着数据集复杂度的增加会造成生成样本的质量下降, 因而 CCGN 优势逐渐变大. CPG 实验中比较了 PackNet 和 PAE 的区别, 三者都是权重级的选择策略. 从准确率方面观察, 三者训练任务量少时取得效果相近, 但 PackNet 不允许模型扩展, 因此会随着任务数增多造成性能下降, CPG^[39] 对比 PAE^[42] 优势在于可将扩展后的冗余权重应用于未来任务的学习中, 在模型训练中更加紧凑.

文献中各种实验的结果表明, 上述模型都具备一定程度的抗遗忘能力, 往往路由选择粒度越小, 模型的参数规模相对会越小, 但不能根据路由选择粒度来单一评判实验准确率, 模型的平均准确率还受诸多其他因素的影响.

5 增量学习应用

增量学习大部分研究都主要在计算机视觉上, 包括图像分类、语义分割、目标检测等, 其中应用于图像分类场景最为普遍, 本文涉及的大部分模型都主要用来解决图像分类问题, 因此不再详细赘述. 此外, 增量学习也开始在自然语言处理和推荐系统等领域展开研究.

(1) 语义分割

深度语义分割模型需要大量训练图像的集合, 这些训练图像具有密集的像素级标注. 然而, 在像素级对大量图像进行标注的代价很高, 希望在不需要大量图像的情况下向分割模型中添加新的类, 目前已有部分相关文献实现了这一目标. 文献[55]则认为背景移位问题加剧了语义分割中的灾难性遗忘, 因此他们提出了传统交叉熵的一个改进版本, 引入了两个新的损失项来正确地解释背景类中的语义分布转移问题. 文献[56]提出了基于原型的增量少镜头分割 (Prototype-based Incremental Few-Shot Segmentation, PIFSS), 它将原型学习和知识提取结合起来, 利用原型来初始化新类的分类器, 微调网络以细化其特征表示. 最近的一项

研究提出了一个弱增量学习的语义分割框架^[57], 扩展了一个标准的编码器-解码器, 通过在编码器上引入定位器, 它增量地训练一个从图像级标签生成在线伪监督的分割模型, 并利用已有的知识增量更新模型.

(2) 目标检测

监督对象检测范式依赖于访问预定义的标记数据, 这种学习范式通常假设数据分布是固定的或静止的, 而来自真实世界的的数据是连续动态的, 其分布是非平稳的. 为了应对这一场景, 目前已有研究将增量学习应用于目标检测当中. 文献[58]提出了一种适用于增量学习场景的双记忆自组织体系结构, 该模型结构主要包括一个深度卷积特征提取模块和 2 个分层排列的递归自组织网络, 实现在增量学习场景下的视频序列中的目标对象识别. 文献[59]认为到当下最先进的有关食物识别的深度神经网络模型不能实现数据的增量学习, 经常在增量学习场景中出现灾难性遗忘问题. 因此, 提出一种新的自适应简化类增量核值学习机方法 (Adaptive Reduced Class Incremental Kernel Extreme Learning Machine, ARCIKELM), 进而完成目标食物对象的识别. 最近的工作提出了一种基于响应的增量蒸馏方法, 称为弹性响应蒸馏 (Elastic Response Distillation, ERD)^[60], 它侧重于从分类头和回归头弹性学习响应, 来解决增量目标检测中的灾难性遗忘问题.

(3) 自然语言处理

在文献[61]介绍了一种增量学习背景下的自然语言学习模型, 该模型实现了对在线文本数据的有效学习. 而文献[62]则提出了一个新的增量学习场景, 它处理自然语言学习中常见的序列到序列的学习任务. 文献[63]对个性化在线语言学习的问题展开研究, 它涉及到将个性化语言模型拟合到随时间变化的用户群体中. 在此基础上, 提出一个简单的连续梯度下降算法 (Continual Gradient Descent, ConGraD), 利用部分在线数据来衡量泛化程度, 对模型进行调整优化.

(4) 推荐系统

增量学习也有一部分研究应用于在推荐系统领域. ADER (Adaptively Distilled Exemplar Replay)^[64] 提出了利用自适应蒸馏损失和回放技术处理基于会话推荐中的遗忘问题. Graph-SAIL (Graph Structure Aware Incremental Learning)^[65] 被引入到基于图神经网络的推荐系统中, 利用局部结构蒸馏、全局结构蒸馏和自嵌入蒸馏来保持用户在增量模型更新过程中的长期偏好.

6 未来研究方向

增量学习作为机器学习领域中的一个极具潜力的研究方向, 近几年一直被广大学者研究. 随着人工智能及机器学习不断的发展, 增量学习在图像分类、目标

检测、自然语言处理等领域得到许多应用. 在这一节中,我们将讨论增量学习中的一些新兴方向,这些方向已经引起了人们的兴趣,并有望在未来获得更多的关注.

(1) 自监督和无监督增量学习

在任何学习系统中,能够从无监督的数据流中增量地学习表示是一个理想的情况. 到目前为止将自监督学习应用于增量学习的关注较少,是个很好的探索方向. 无监督增量学习仍处于起步阶段,预计未来将会有更多的研究.

(2) 特征排练

伪排练是存储示例的一个很好的替代方法. 它学习一个单独的网络,生成以前任务的图像. 然而,目前最先进的图像生成方法难以逼真地生成复杂的图像数据,因此这种方法被应用于简单的数据集,但在复杂的数据集上得到的结果并不令人满意. 为了解决这个问题,一些工作已经提出执行特征重放而不是图像重放^[6,66],因此基于排练的方法也可以应用于复杂的数据集.

(3) 元学习

元学习(Meta-Learning)是一种新兴的学习领域,目的是在解决相关任务的同时,利用积累的信息学习新的任务. 近年来,基于元学习的在线增量学习方法有了一定进展,并将元学习应用于无明显任务边界的增量^[12]场景中. MER(Meta-Experience Replay)^[67]将经验重放与基于优化的元学习相结合,以最大限度地转移和最小化基于未来梯度的干扰. OML(Online-aware Meta-Learning)^[68]定义一个元目标,用它来学习加速未来任务和避免灾难性干扰的表示. 最近,iTAML(Incremental Task-Agnostic Meta-Learning)^[69]提出学习一个任务不可知模型,该模型自动预测任务,并通过元更新快速适应预测的任务.

(4) 在线增量学习

在线增量学习(online-IL)是增量学习的一个分支,更适用于更接近实际的应用场景. 离线增量学习(offline-IL)假设新数据一次到达一个任务,每个任务的数据分布通常固定的,而在线增量学习假设每次数据一次到达一个小批量大小的数据块,新模型依据前一模型和最新的新数据块进行调整. 近年来,有相关文献对该领域开展研究. 文献[70]通过引入改进的交叉蒸馏损失函数和两步学习技术,能够以在线方式对新类数据和旧类的新分布数据流进行训练. 文献[71]利用增量学习的约束优化思想,在线场景下,将样本选择问题归结为一个约束项化简问题. 另一项研究,PuriDiver(Purity and Diversity aware Episode Replay)^[72]结合记忆采样和半监督学习方法,可以从带有损坏标签的模

糊数据流中进行在线学习.

(5) 无任务边界设置

许多实际应用程序不能很好地适应具有非重叠任务的实验设置. 无任务(task-free)是一个更现实的场景,指没有明确的任务边界,在类上的分布逐渐发生改变. 在这项研究中,CN-DPM(Continual Neural Dirichlet Process Mixture)采用基于扩展的无任务 IL 方法,在贝叶斯非参数框架下有原则地扩展专家数量. 模型由一组专家组成,每个专家负责一个数据流中的一个子集. 文献[8]扩展 MAS(Memory Aware Synapses)^[73]通过一个协议来确定何时更新没有任务定义的重要性权重. GMED(Gradient based Memory EDiting)^[74]是针对无任务学习的基于内存的 IL 框架,它可以通过一个小的梯度更新直接“编辑”存储在回放内存中的示例,更有效地缓解灾难性遗忘.

7 总结

增量学习是近年来机器学习领域的一个重要的研究方向,其目的在于高效地转化和利用已经学过的知识来学习一系列新任务,并且能够极大程度地解决灾难性遗忘等诸多问题. 而动态神经网络处理不同样本时,能动态地调节自身的结构或参数,从而在推理效率、表达能力、自适应性等方面展现出卓越的优势. 因此,本文对增量学习领域涉及到动态网络架构做了综述. 介绍了增量学习和动态网络的基本概念,分析当前研究现状,阐述了增量学习中不同的学习场景. 文中分别从粗粒度到细粒度等角度详细分析了增量学习中的动态网络模型,文中也列出了常用的实验数据集和评价指标. 最后,对近年来的应用和未来的可研究方向做了分析.

参考文献

- [1] MCCLOSKEY M, COHEN N J. Catastrophic interference in connectionist networks: The sequential learning problem [M]//Psychology of Learning and Motivation. Amsterdam: Elsevier, 1989: 109-165.
- [2] LI Z, HOIEM D. Learning without forgetting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 40(12): 2935-2947.
- [3] HINTON G, VINYALS O, DEAN J. Distilling the knowledge in a neural network[J]. Computer Science, 2015, 14(7): 38-39.
- [4] KIRKPATRICK J, PASCANU R, RABINOWITZ N, et al. Overcoming catastrophic forgetting in neural networks[J]. Proceedings of the National Academy of Sciences, 2017, 114(13): 3521-3526.

- [5] REBUFFI S A, KOLESNIKOV A, SPERL G, et al. iCaRL: Incremental classifier and representation learning [C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2017: 5533-5542.
- [6] LIU X L, WU C S, MENTA M, et al. Generative feature replay for class-incremental learning[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Piscataway: IEEE, 2020: 915-924.
- [7] KIM J H, LEE S W, KWAK D, et al. Multimodal residual learning for visual QA[J]. *Advances in Neural Information Processing Systems*, 2016: 361-369.
- [8] ALJUNDI R, KELCHTERMANS K, TUYTELAARS T. Task-free continual learning[C]//2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 11246-11255.
- [9] WORTSMAN M, RAMANUJAN V, LIU R, et al. Supermasks in superposition[J]. *Advances in Neural Information Processing Systems*, 2020, 33: 15173-15184.
- [10] VAN DE VEN G M, TOLIAS A S. Three scenarios for continual learning[EB/OL]. (2019-04-15) [2023-04-12]. <https://arxiv.org/abs/1904.07734>.
- [11] DE LANGE M, ALJUNDI R, MASANA M, et al. A continual learning survey: Defying forgetting in classification tasks[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2022, 44(7): 3366-3385.
- [12] HE X, SYGNOWSKI J, GALASHOV A, et al. Task agnostic continual learning via meta learning [EB/OL]. (2019-06-12)[2023-04-12]. <https://arxiv.org/abs/1906.05201>.
- [13] RUSU A A, RABINOWITZ N C, DESJARDINS G, et al. Progressive neural networks[EB/OL]. (2016-10-22)[2023-04-15]. <https://arxiv.org/abs/1606.04671>.
- [14] ALJUNDI R, CHAKRAVARTY P, TUYTELAARS T. Expert gate: Lifelong learning with a network of experts [C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2017: 7120-7129.
- [15] ZEILER M D, RANZATO M, MONGA R, et al. On rectified linear units for speech processing[C]//2013 IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway: IEEE, 2013: 3517-3521.
- [16] ZHANG J O, SAX A, ZAMIR A, et al. Side-tuning: A baseline for network adaptation via additive side networks [C]//2020 European Conference on Computer Vision. Glasgow: ECCV, 2020: 698-714.
- [17] COSSU A, CARTA A, BACCIU D. Continual learning with gated incremental memories for sequential data processing[C]//2020 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE, 2020: 1-8.
- [18] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2016: 770-778.
- [19] HUANG G, LIU Z, VAN DER MAATEN L, et al. Densely connected convolutional networks[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2017: 2261-2269.
- [20] FERNANDO C, BANARSE D, BLUNDELL C, et al. PathNet: Evolution channels gradient descent in super neural networks[EB/OL]. (2017-01-15) [2023-04-12]. <https://arxiv.org/abs/1701.08734>.
- [21] HARVEY I. The microbial genetic algorithm[EB/OL]. (2016-10-22)[2023-04-15]. https://doi.org/10.1007/978-3-642-21314-4_16.
- [22] RAJASEGARAN J, HAYAT M, KHAN S, et al. An adaptive random path selection approach for incremental learning[EB/OL]. (2019-06-03) [2023-04-15]. <https://arxiv.org/abs/1906.01120>.
- [23] VENIAT T, DENOYER L, RANZATO M. Efficient continual learning with modular networks and task-driven priors[EB/OL]. (2020-12-23)[2023-04-15]. <https://arxiv.org/abs/2012.12631>.
- [24] YOON J, YANG E, LEE J, et al. Lifelong Learning with dynamically expandable networks[C/OL]//6th International Conference on Learning Representations. Vancouver: ICLR, (2018)[2023-04-12]. <https://openreview.net/forum?id=Sk7KsfW0->.
- [25] SCARDAPANE S, COMMINELO D, HUSSAIN A, et al. Group sparse regularization for deep neural networks [J]. *Neurocomputing*, 2017, 241: 81-89.
- [26] SERRA J, SURIS D, MIRON M, et al. Overcoming catastrophic forgetting with hard attention to the task[C]//Proceedings of the 36th International Conference on Machine Learning. New York: ACM, 2019: 4555-4564.
- [27] GOLKAR S, KAGAN M, CHO K. Continual learning via neural pruning[EB/OL]. (2019-03-11)[2023-04-15]. <https://arxiv.org/abs/1903.04476>.
- [28] MASSE N Y, GRANT G D, FREEDMAN D J. Alleviating catastrophic forgetting using context-dependent gating and synaptic stabilization[J]. *Proceedings of the National Academy of Sciences of the United States of America*

- ica, 2018, 115(44): 10467-10475
- [29] ZENKE F, POOLE B, GANGULI S. Continual learning through synaptic intelligence[C]//Proceedings of the 34th International Conference on Machine Learning. New York: ACM, 2017: 3987-3995.
- [30] XU J, ZHU Z. Reinforced continual learning[J]. *Advances in Neural Information Processing Systems*, 2018, 31: 907-916.
- [31] GAO Q, LUO Z P, KLABJAN D, et al. Efficient architecture search for continual learning[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2022, PP (99): 1-11.
- [32] ABATI D, TOMCZAK J, BLANKEVOORT T, et al. Conditional channel gated networks for task-aware continual learning[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 3930-3939.
- [33] JANG E, GU S, POOLE B. Categorical reparameterization with gumbel-softmax[C/OL]//5th International Conference on Learning Representations. Toulon: ICLR. (2017) [2023-04-15]. <https://openreview.net/forum?id=rkE3y85ee>.
- [34] BENGIO Y, LÉONARD N, COURVILLE A. Estimating or propagating gradients through stochastic neurons for conditional computation[EB/OL]. (2013-08-15) [2023-04-15]. <https://arxiv.org/abs/1903.04476>.
- [35] YAN S P, XIE J W, HE X M. DER: Dynamically expandable representation for class incremental learning[C]//2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2021: 3013-3022.
- [36] ROSENFELD A, TSOTSOS J K. Incremental learning through deep adaptation[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020, 42(3): 651-663.
- [37] MALLYA A, LAZEBNIK S. PackNet: Adding multiple tasks to a single network by iterative pruning[C]//2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2018: 7765-7773.
- [38] HAN S, POOL J, NARANG S, et al. DSD: Dense-sparse-dense training for deep neural networks[C/OL]//5th International Conference on Learning Representations. Toulon: ICLR, (2019) [2023-04-15]. <https://openreview.net/forum?id=HyoST\9xl>.
- [39] HUNG S C Y, TU C H, WU C E, et al. Compacting, picking and growing for unforgetting continual learning[J]. *Advances in Neural Information Processing Systems*, 2019, 32: 13647-13657.
- [40] ZHU M, GUPTA S. To prune, or not to prune: exploring the efficacy of pruning for model compression [EB/OL]. (2017-10-05) [2023-04-15]. <https://arxiv.org/abs/1710.01878>.
- [41] MALLYA A, DAVIS D, LAZEBNIK S. Piggyback: Adapting a single network to multiple tasks by learning to mask weights[C]//2018 European Conference on Computer Vision. Munich: ECCV, 2018: 67-82.
- [42] HUNG S C Y, LEE J H, WAN T S T, et al. Increasingly packing multiple facial-informatics modules in A unified deep-learning model via lifelong learning[C]//Proceedings of the 2019 on International Conference on Multimedia Retrieval. New York: ACM, 2019: 339-343.
- [43] OSTAPENKO O, PUSCAS M, KLEIN T, et al. Learning to remember: A synaptic plasticity driven framework for continual learning[C]//2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 11313-11321.
- [44] MIRZA M, OSINDERO S. Conditional generative adversarial nets[EB/OL]. (2014-11-06) [2023-04-15]. <https://arxiv.org/abs/1411.1784>.
- [45] LI X, ZHOU Y, WU T, et al. Learn to grow: A continual structure learning framework for overcoming catastrophic forgetting[C]//Proceedings of the 36th International Conference on Machine Learning. New York: ACM, 2019: 3925-3934.
- [46] WELINDER P, BRANSON S, MITA T, et al. Caltech-UCSD birds 200[EB/OL]. (2011-10-26) [2023-04-15]. <https://authors.library.caltech.edu/27468/>.
- [47] NILSBACK M E, ZISSERMAN A. Automated flower classification over a large number of classes[C]//2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing. Piscataway: IEEE, 2009: 722-729.
- [48] KRIZHEVSKY A, HINTON G. Learning multiple layers of features from tiny images[J]. *Handbook of Systemic Autoimmune Diseases*, 2009, 1(4): 110.
- [49] VINYALS O, BLUNDELL C, LILLICRAP T, et al. Matching networks for one shot learning[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems. New York: ACM, 2016: 3637-3645.
- [50] LOMONACO V, MALTONI D. Core50: A new dataset and benchmark for continuous object recognition [EB/OL]. (2017-05-09) [2023-04-15]. <https://arxiv.org/abs/1705.03550>.

- [51] LOPEZ-PAZ D, RANZATO M. Gradient episodic memory for continual learning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: ACM, 2017: 6470-6479.
- [52] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.
- [53] CHAUDHRY A, ROHRBACH M, ELHOSEINY M, et al. On tiny episodic memories in continual learning[EB/OL]. (2019-02-27)[2023-04-15]. <https://arxiv.org/abs/1902.10486>.
- [54] DÍAZ-RODRÍGUEZ N, LOMONACO V, FILLIAT D, et al. Don't forget, there is more than forgetting: New metrics for Continual Learning[EB/OL]. (2018-10-31)[2023-04-15]. <https://arxiv.org/abs/1810.13166>.
- [55] CERMELLI F, MANCINI M, ROTA BULÒ S, et al. Modeling the background for incremental learning in semantic segmentation[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 9230-9239.
- [56] CERMELLI F, MANCINI M, XIAN Y, et al. Prototype-based incremental few-shot semantic segmentation[EB/OL]. (2020-11-30)[2023-04-15]. <https://arxiv.org/abs/2012.01415>.
- [57] CERMELLI F, FONTANEL D, TAVERA A, et al. Incremental learning in semantic segmentation from image labels[C]//2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2022: 4361-4371.
- [58] PARISI G I, JUN T N, WEBER C, et al. Lifelong learning of spatiotemporal representations with dual-memory recurrent self-organization[J]. Frontiers in Neurobotics, 2018, 12: 78.
- [59] TAHIR G A, LOO C K. An open-ended continual learning for food recognition using class incremental extreme learning machines[J]. IEEE Access, 2020, 8: 82328-82346.
- [60] FENG T, WANG M, YUAN H J. Overcoming catastrophic forgetting in incremental object detection via elastic response distillation[C]//2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2022: 9417-9426.
- [61] DE MASSON D'AUTUME C, RUDER S, KONG L, et al. Episodic memory in lifelong language learning[J]. Advances in Neural Information Processing Systems, 2019, 32: 13122-13131.
- [62] LI Y, ZHAO L, CHURCH K, et al. Compositional language continual learning[C/OL]//8th International Conference on Learning Representations. Addis Ababa: ICLR, 2020[2023-04-12]. <https://openreview.net/forum?id=rklnDgHtDS>.
- [63] HU H X, SENER O, SHA F, et al. Drinking from a firehose: Continual learning with web-scale natural language[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(5): 5684-5696.
- [64] MI F, LIN X Y, FALTINGS B. ADER: Adaptively distilled exemplar replay towards continual learning for session-based recommendation[C]//Proceedings of the 14th ACM Conference on Recommender Systems. New York: ACM, 2020: 408-413.
- [65] XU Y S, ZHANG Y X, GUO W, et al. GraphSAIL: Graph structure aware incremental learning for recommender systems[C]//Proceedings of the 29th ACM International Conference on Information & Knowledge Management. New York: ACM, 2020: 2861-2868.
- [66] ISCEN A, ZHANG J, LAZEBNIK S, et al. Memory-efficient incremental learning through feature adaptation[C]//2020 European Conference on Computer Vision. Glasgow: ECCV, 2020: 699-715.
- [67] RIEMER M, CASES I, AJEMIAN R, et al. Learning to learn without forgetting by maximizing transfer and minimizing interference[EB/OL]. (2018-10-29) [2023-04-15]. <https://arxiv.org/abs/1810.11910>.
- [68] JAVED K, WHITE M. Meta-learning representations for continual learning[J]. Advances in Neural Information Processing Systems, 2019, 32: 1818-1828.
- [69] RAJASEGARAN J, KHAN S, HAYAT M, et al. iTAML: An incremental task-agnostic meta-learning approach[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 13585-13594.
- [70] HE J P, MAO R Y, SHAO Z M, et al. Incremental learning in online scenario[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2020: 13923-13932.
- [71] ALJUNDI R, LIN M, GOUJAUD B, et al. Gradient based sample selection for online continual learning[J]. Advances in neural information processing systems, 2019, 32: 11816-29205.
- [72] BANG J, KOH H, PARK S, et al. Online continual learning on a contaminated data stream with blurry task boundaries[C]//2022 IEEE/CVF Conference on Computer Vi-

sion and Pattern Recognition (CVPR). Piscataway: IEEE, 2022: 9265-9274.

- [73] ALJUNDI R, BABILONI F, ELHOSEINY M, et al. Memory aware synapses: learning what (not) to forget [C]//2018 European Conference on Computer Vision. Munich: ECCV, 2018: 139-154.
- [74] JIN X, SADHU A, DU J, et al. Gradient-based editing of memory examples for online task-free continual learning [J]. Advances in Neural Information Processing Systems, 2021, 34: 29193-29205.

作者简介



赵海燕 女, 1975年11月出生于河南省焦作市。现为上海理工大学光电信息与计算机工程学院副教授。主要研究方向为智能数据分析, 推荐系统。

E-mail: zhaohaiyan1992@foxmail.com



马权益 男, 1996年9月出生于浙江省金华市。现为上海理工大学光电信息与计算机工程学院硕士研究生。主要研究方向为神经网络, 增量学习。

E-mail: mannel22@163.com



曹 健(通讯作者) 男, 1972年9月出生, 出生于江苏省宜兴市。现为上海交通大学计算机系教授, 主要方向为分布式人工智能, 智能数据分析, 服务计算。中国电子学会会员编号: E190007047S。

E-mail: cao-jian@cs.sjtu.edu.cn



陈庆奎 男, 1966年1月出生于黑龙江哈尔滨。现任上海理工大学光电信息与计算机工程学院教授、博士生导师。主要研究方向: 并行处理技术, 智能计算, 物联网技术。

E-mail: chenqingkui@usst.edu.cn