控制与决策
Control and Decision

基于分类特征约束变分伪样本生成器的类增量学习

莫建文， 陈瑶嘉

引用本文:
莫建文, 陈瑶嘉. 基于分类特征约束变分伪样本生成器的类增量学习[J]. 控制与决策, 2021, 36(10): 2475−2482.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2020.0228

基于分类特征约束变分伪样本生成器的类增量学习

莫建文[1,2†], 陈瑶嘉[2]

(1. 桂林电子科技大学 认知无线电与信息处理省部共建教育部重点实验室，广西 桂林 541004；
2. 桂林电子科技大学 信息与通信学院，广西 桂林 541004)

摘 要: 针对神经网络模型进行类增量训练时产生的灾难性遗忘问题,提出一种基于分类特征约束变分伪样本生成器的类增量学习方法. 首先,通过构造伪样本生成器记忆旧类样本来训练新的分类器及新的伪样本生成器. 伪样本生成器以变分自编码器为基础,用分类特征进行约束,使生成的样本更好地保留旧类在分类器上的性能. 然后,用旧分类器的输出作为伪样本的精馏标签,进一步保留从旧类获得的知识. 最后,为了平衡旧类样本的生成数量,采用基于分类器分数的伪样本选择,在保持每个旧类伪样本数量平衡的前提下选择一些更具代表性的旧类伪样本. 在MNIST、FASHION、E-MNIST和SVHN数据集上的实验结果表明,所提出的方法能有效减少灾难性遗忘的影响,提高图像的分类精度.

关键词: 类增量学习；灾难性遗忘；分类特征约束；变分自编码器；精馏标签；伪样本选择

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2020.0228 **开放科学(资源服务)标识码(OSID):**

引用格式: 莫建文,陈瑶嘉. 基于分类特征约束变分伪样本生成器的类增量学习[J]. 控制与决策, 2021, 36(10): 2475-2482.

Class incremental learning based on variational pseudo-sample generator with classification feature constraints

MO Jian-wen[1,2†], *CHEN Yao-jia*[2]

(1. Ministry of Education Key Lab. of Cognitive Radio and Information Processing, Guilin University of Electronic Technology，Guilin 541004，China；2. School of Information and Communication，Guilin University of Electronic Technology，Guilin 541004，China)

Abstract: Aiming at the catastrophic forgetting problem caused by the class incremental training of neural network models, a class incremental learning method based on a variational pseudo-sample generator with classification feature constraints is proposed. Firstly, a new classifier and a new pseudo sample generator are trained by constructing a pseudo-sample generator to memorize old class samples. The pseudo sample generator is based on the variational autoencoder and uses classification features to constrain the generated samples to better retain the performance of the old class on the classifier. Then, the output of the old classifier is used as the distillation label of the pseudo sample to further retain the knowledge obtained from the old class. Finally, in order to balance the number of samples generated by the old class, pseudo sample selection based on the score of the classifier can be used to select some more representative samples of the old class while maintaining the balance of the number of pseudo samples of each old class. Experimental results on MNIST, FASHION, E-MNIST and SVHN datasets show that the proposed method can effectively reduce the impact of catastrophic forgetting and improve the accuracy of image classification.

Keywords: class incremental learning; catastrophic forgetting; classification feature constraints; variational autoencoder; distillation label; pseudo sample selection

0 引 言

近年来深度学习方法因其最先进的成果而引人注目,但深度模型的经典训练范例仍无法用于类增量学习. 这是因为在旧类训练样本不可用的情况下,使用随机梯度下降仅在新类的数据上直接微调现有模型会导致灾难性遗忘[1]效应,即仅用新类数据训练神

收稿日期: 2020-03-02；**修回日期:** 2020-05-22.

基金项目: 国家自然科学基金项目(61661017, 61967005, U1501252)；广西自然科学基金项目(2017GXNSFBA198212)；广西科技基地和人才专项(桂科AD19110060)；中国博士后科学基金面上项目(2016M602923XB)；认知无线电教育部重点实验室项目(CRKL150103, CRKL190107, CRKL160104)；桂林电子科技大学研究生创新项目(2019YCXS020).

责任编委: 侯忠生.

†通讯作者. E-mail: mo_jianwen@126.com.

经网络会导致它覆盖,从而忘记它在旧类数据学到的知识. 若保留所有旧类的训练样本,则每当遇到新类时,从头开始重新训练模型是非常昂贵的,这是因为保留所有旧类的训练样本需要巨大的数据存储需求.

最近的文献中,改善类增量学习中存在的灾难性遗忘现象的方法大致可分为4大类: 正则化方法、网络扩展方法、精馏方法和重放方法. 正则化方法[2-5]的模型可以限制可学习参数的变化,以防止覆盖以前优化的网络参数. 文献[2]提出的弹性权重合并(elastic weight consolidation, EWC)能保护某些对前一任务重要的权重来缓解其性能损失. 网络扩展方法[6-10]的模型通过修改网络架构本身以适应新的任务. 文献[7]提出的网络扩展方法一方面保留了原始网络的过滤器,另一方面在卷积层和全连接层上增加了额外的过滤器来适应新的任务.

知识精馏[11]一开始提出的目的是为了实现知识迁移,其主要思想是将复杂网络得到的软目标作为总损失的一部分,诱导简单网络的训练,使得简单网络能达到复杂网络的性能. 文献[12]提出了一种新的尝试,利用精馏损失和标准交叉熵损失来保持旧任务的性能,虽然这种方法在某种程度上减少了遗忘,特别是在简单的场景中,旧样本和新样本来自不同的数据集,它们之间几乎没有混淆,但因其旧类的知识表示较弱,其性能远非理想. 文献[13]基于文献[12]的方法,使用自动编码器而不是精馏损失来保留旧任务的知识,该方法还在一个限制性场景中进行了评估,其中旧网络和新网络在不同的数据集上进行训练,结果类似于文献[12]. 文献[14]将精馏损失应用到增量目标检测器的学习中,并在目标检测方面取得了较好的效果,但是这种特定体系结构不太适用于更一般的分类场景.

重放方法的模型不再保留关键滤波器或权重,它主要分两类. 一类是直接将一小部分原始数据集保存到内存缓冲区中,如文献[15]中提出的增量分类器与表示学习,该方法仅需要保留少量旧类的训练数据,并且可以逐步添加新类,且可以同时学习分类器和学习表示. 文献[16]在文献[15]的基础上进行了改进,提出了端到端的增量学习,主要改进文献[15]中存在的新旧类的训练样本数量不均衡问题. 另一类是通过训练生成器模拟旧类的数据和标签来估计旧类数据的分布,如文献[17]中,通过使用递归神经网络生成代表旧类的随机图像来实现类增量学习. 但生成模型要求为每个学习的类别存储每个像素的平均值和标准差,这导致模型的存储需求随所学习的类的数量而增加. 文献[18]提出的深度生成重放(deep generative replay, DGR)方法对每个任务都训练一个无条件的GAN来累积生成和区分图像,提出的GAN是无条件的,因此DGR使用了一个额外的分类器,该分类器经过并行训练对生成的图像进行分类并分配相应的标签. 文献[19]提出一种记忆重放GAN(memory replay GANs, MeRGAN)方法通过对DGR框架进行修改,将无条件的GAN替换为ACGAN,从而消除了额外分类器的需要. 文献[20]结合这两个方面提出了一种闭环记忆GAN(closed-loop memory GAN, CloGAN)方法将非常小的内存缓冲区与训练生成器结合使用,用内存缓冲区中的真实样本充当生成器的外部正则化,以降低生成器生成的图像随类增量次数增多引起的生成图像退化问题.

尽管有越来越多的解决方案,但灾难性遗忘并不是一个已经解决的问题. 正则化方法在类增量类学习中表现不佳,例如EWC[2]方法,文献[20]中的实验验证了这一局限性. 另一方面,网络扩展的方法虽然通常能为约束的增量问题提供简洁的解决方案,但很快就会变得不可持续,因为参数或网络层数量的快速增加导致大量内存占用. 同样,重放方法也会遇到可扩展性问题. 随着类增量学习次数的增多,单纯的生成重放会出现生成图像质量下降问题,结合一定的内存缓冲区虽然在一定程度上缓解了这种下降的趋势,但同样随着类增量学习次数的增多,内存缓冲区中每类图像的样本数量减少,还是会出现生成图像质量下降的问题.

本文针对现有方法不能完全舍弃旧类样本数据、内存占用大且最终分类性能较低等问题,提出一种基于分类特征约束变分伪样本生成器的类增量学习方法. 首先,构造一种基于分类特征约束的变分伪样本生成器,确保生成的伪样本能更好地保留旧类在分类器上的性能. 然后,结合知识精馏[11]的思想,为伪样本生成器生成的伪样本打上精馏标签,进一步保留从旧类中获得的知识. 最后,采用基于分类分数的伪样本选择策略,在平衡每个旧类伪样本的数量的基础上选择更具代表性的伪样本. 该方法能在完全不保留旧类样本数据的前提下,有效减少灾难性遗忘的影响,提高图像分类精度.

1 基于分类特征约束变分伪样本生成器的类增量学习

1.1 类增量学习系统结构

基于分类特征约束变分伪样本生成器(variational auto-encoder based on classification feature

constraint, CF-VAE) 的类增量学习方法用旧分类器、旧伪样本生成器、新类样本来训练生成新的分类器及伪样本生成器,不需要记忆旧类样本及标签,过程如图1所示,主要分为3个阶段.

第1阶段:利用当前的旧伪样本生成器ψ_t生成旧类的伪样本,并基于旧分类器G_t为每个生成的伪样本打上精馏标签;

第2阶段:根据伪样本在G_t上的分类分数为每个旧类选择一定数量有代表性的伪样本,并与新类的样本数据$S_{\rm new}$一起构建增量训练数据集$S_{\rm train}$;

第3阶段:以带标签的增量训练数据集训练新分类器G_{t+1},以不带标签的增量训练数据集训练新伪样本生成器ψ_{t+1}.

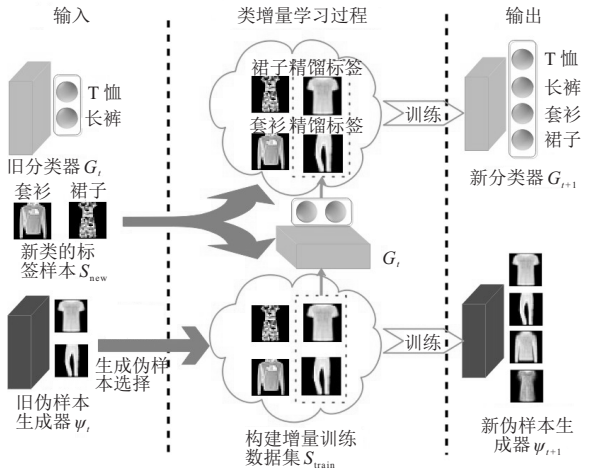


图1　基于CF-VAE的类增量学习过程

1.2　旧类伪样本的生成及其精馏标签

如图1所示,每次进行类增量学习时,首先需要用训练好的旧伪样本生成器ψ_t为旧类生成伪样本$X_{\rm old}^{\rm gen}$,即

$$X_{\rm old}^{\rm gen}=\{x_1',\dots,x_n'\}=\{x_j'|x_j'=\psi_t(\varepsilon_j)\}. \quad (1)$$

其中:$\varepsilon_j\in N(0,1)$;x_j'为ψ_t生成的旧类的伪样本,$j\in 1\sim n$,n为ψ_t每次生成的伪样本数量.

接着,为了尽可能地保留分类器在旧类上的性能,采用知识精馏的思想为生成的旧类伪样本打上精馏标签. 知识精馏[11]一开始提出的目的是为了实现知识迁移,其主要思想是将复杂网络得到的软目标作为总损失的一部分,诱导简单网络的训练,使得简单网络能达到复杂网络的性能. 文献[11]分析表明,当软目标具有较高的熵时,它们在每个训练样本中提供的信息比硬目标更多,并且训练样本之间的梯度差异较小. 因此,相比于原始的复杂网络,简单网络通常可以在少得多的数据上进行训练. 本文中伪样本通过旧分类器得到的输出作为伪样本的精馏标签,能在使用伪样本及其精馏标签与新类标签样本训练新分类器时诱导网络在它们之间学习更细粒度的分离,使得新分类器网络学习了类的更具辨别力的表示. 具体地,首先将生成的伪样本$X_{\rm old}^{\rm gen}$输入当前的旧分类器G_t的特征提取网络φ中得到用于分类的特征,然后将特征输入G_t的Softmax层得到分类器的输出,即

$$Y_{\rm old}=\{\boldsymbol{y}_1,\dots,\boldsymbol{y}_n\}=\{\boldsymbol{y}_j|\boldsymbol{y}_j=G_t[\varphi(x_j')]\}. \quad (2)$$

其中$\boldsymbol{y}_j$为对应的x_j'的精馏标签,这个旧分类器G_t的输出$Y_{\rm old}$就是生成的伪样本的精馏标签集.

1.3　生成伪样本的选择及构建增量训练数据集

因为采用的CF-VAE是无监督模型,且样本的生成是随机的,随着旧类数目的增加,仅靠着CF-VAE模型的随机生成很难准确地把控每个旧类的样本生成数量及其质量. 拒绝抽样[21]是对难以直接抽样的目标分布进行抽样的一种方法,文献[22]提出的鉴别器拒绝抽样(discriminator rejection sampling, DRS)方法将拒绝抽样应用到GAN,通过从训练好的GAN中生成样本,并将鉴别器的输出概率作为拒绝抽样的依据,概率合格的生成样本保存,不合格的拒绝. 文献[22]分析了以输出概率作为拒绝抽样的依据的有效性,并通过在ImageNet数据上的实验验证了该方法能有效地使GAN生成样本的概率分布更接近于真实样本. 本文采用拒绝抽样的思想,在DRS的基础上,提出了基于分类分数的伪样本选择策略,通过使用分类器代替DRS中的鉴别器为生成的伪样本进行预测,根据预测的分类分数来精确选择每个类的伪样本数量及保证其质量. 具体地,设C为数据集总的类别数,每次增量两个类,c表示$t+1$时刻观察到的类的数量,即$1\sim c-2$类为t时刻观察到的旧类的数量,$c-1\sim c$为$t+1$时刻观察到的新类,则每个旧类的伪样本$x_j'\in X_{\rm old}^{\rm gen}$在$G_t$上的预测所属类别与分类分数分别为

$$k=\arg\max_{m\in(1,C)} y_{j,m}, \quad (3)$$

$$s_j=y_{j,k}, \quad (4)$$

其中$\boldsymbol{y}_j=[y_{j,1},\dots,y_{j,C}]^{\rm T}$为一个$C$维向量.

随着类增量学习次数的增多,分类器要区分的类数目随之增多,训练旧分类器G_t与旧伪样本生成器ψ_t用到的大部分训练样本将由$t-1$时刻的伪样本生成器ψ_{t-1}提供,少部分由t时刻数据集中$c-2$与$c-3$类的训练样本提供. 即在训练旧分类器G_t时用到的是数据集中$c-2$与$c-3$类的训练样本,而要预测的

却是旧伪样本生成器ψ_t生成的$c-2$与$c-3$类的伪样本,这会使得旧伪样本生成器ψ_t生成的$c-2$与$c-3$类的伪样本通过旧分类器G_t很难得到较高的预测分数. 针对这问题,设计一个伪样本选择策略,对不同的旧类类别采用两种不同的方案.

首先,令$S_k^{\rm gen}=\varnothing, S_{\rm old}^{\rm gen}=\varnothing$,其中$S_k^{\rm gen}$为$k$类伪样本数据集,$S_{\rm old}^{\rm gen}$为所有旧类的伪样本集,$\varnothing$为一个空集,则对于一个属于$X_{\rm old}^{\rm gen}$的样本$x'_j$,根据式(3)和(4)分别计算所属类别$k$和分类分数$s_j$,即:

1) 当$k\in[c-3,c-2]$时,将伪样本和标签放入对应的数据集,即$S_k^{\rm gen}=S_k^{\rm gen}\bigcup\{(x'_j,\boldsymbol{y_j})\}$;

2) 当$k\in(1,c-4)$,且$s_j>T$,即$S_k^{\rm gen}=S_k^{\rm gen}\bigcup\{(x'_j,\boldsymbol{y_j})\}$时,舍弃小于等于$T$的伪样本,其中$T$为分类分数的阈值,且$0<T<1$.

伪样本的选择算法流程如下所示.

算法1 伪样本的选择.

输入:旧的分类器G_t,伪样本生成器ψ_t;

输出: 所有旧类的伪样本集$S_{\rm old}^{\rm gen}=\{S_1^{\rm gen},\dots,S_{c-2}^{\rm gen}\}$.

初始化:$S_k^{\rm gen}=\varnothing, S_{\rm old}^{\rm gen}=\varnothing$.

step 1: 通过式(1)利用ψ_t生成旧类的伪样本x'_j;

step 2: 通过式(2)将x'_j输入G_t得到x'_j的Softmax输出值$\boldsymbol{y_j}$;

step 3: 通过式(3)和(4)分别计算x'_j的所属类别k和分类分数s_j;

step 4: 当$k\in[c-3,c-2]$时,$S_k^{\rm gen}=S_k^{\rm gen}\bigcup\{(x'_j,\boldsymbol{y}_j)\}$;

step 5: 当$k\in(1,c-4)$,且$s_j>T$时,$S_k^{\rm gen}=S_k^{\rm gen}\bigcup\{(x'_j,\boldsymbol{y}_j)\}$;

step 6: 当$k>c-2$时,舍弃伪样本x'_j;

step 7: 重复step 1 ~ step 6,直到每个类的伪样本数量都达到数据集每个类训练样本的数量为止.

最后,将经过样本选择的所有旧类的伪样本集$S_{\rm old}^{\rm gen}$同新类的标签样本集$S_{\rm new}$一起构建增量训练数据集$S_{\rm train}=S_{\rm old}^{\rm gen}\bigcup S_{\rm new}$,为接下来的类增量学习训练新的分类器$G_{t+1}$与伪样本生成器$\psi_{t+1}$.

1.4 分 类 器

分类器基于多层全连接神经网络,由特征提取网络和最后的Softmax分类层组成. 首先,特征提取网络由输入层与隐藏层组成,作为一个可训练的特征提取网络将输入的训练样本x_j映射为一组具有D维的特征,即$\varphi: x_j\to R^D$.

接下来为一个全连接的Softmax分类层,具有与数据集总的类别数C一致的输出节点,对应的权值为$w_1,\dots,w_C\in R^D$,则对于任何$k\in\{1,\dots,C\}$类得到的Softmax分类层的输出为

$$G_k(x_j)=\frac{{\rm e}^{w_k^{\rm T}\cdot\varphi(x_j)+\boldsymbol{b_k}}}{\sum\limits_{i=1}^{C}{\rm e}^{w_i^{\rm T}\cdot\varphi(x_j)+\boldsymbol{b}_i}}. \tag{5}$$

其中:$\boldsymbol{b_k}$与$\boldsymbol{b_j}$为偏置项向量,$\varphi(x_j)$为x_j通过特征提取网络φ得到的一组D维的特征.

在这里,增量训练数据集中新类训练样本为one-hot标签,旧类生成的伪样本为精馏标签,所以分类器由两种损失函数构成,一种是新类的交叉熵损失L_E,另一种是旧类的精馏损失L_K,令分类器的总损失为L_G,设每次增量2个类,$1\sim c-2$类为旧类,$c-1\sim c$为新类,则新类的交叉熵损失L_E为

$$L_E=-\frac{1}{2N}\sum_{j=1}^{2N}\sum_{m=1}^{C}p_{j,m}\cdot\log q_{j,m}. \tag{6}$$

其中:N为每类的样本数量,$\boldsymbol{p}_i$为新类样本的one-hot标签,$\boldsymbol{q}_i$为Softmax层的输出值.

旧类的精馏损失L_K为

$$L_K=-\frac{1}{N\times(c-2)}\sum_{j=1}^{N\times(c-2)}\sum_{m=1}^{C}y_{j,m}\cdot\log q_{j,m}, \tag{7}$$

其中$\boldsymbol{y}_j$为生成的旧类伪样本的精馏标签,则分类器的总损失L_G为

$$L_G=L_E+L_K=-\Big(\frac{1}{N\times 2}\sum_{j=1}^{2N}\sum_{m=1}^{C}p_{j,m}\cdot\log q_{j,m}+\frac{1}{N\times(c-2)}\sum_{j=1}^{N\times(c-2)}\sum_{m=1}^{C}y_{j,m}\cdot\log q_{j,m}\Big). \tag{8}$$

1.5 伪样本生成器

伪样本生成器(CF-VAE)是由变分自编码器结合分类器中的特征提取网络组成,旨在生成的伪样本不仅能尽可能地拟合训练样本,而且还能做到尽可能地拟合训练样本在分类器上的性能表现,以此来保证生成的伪样本能更为有效地保留分类器对旧类的分类性能. CF-VAE的总体结构如图2所示.

传统的VAE如图2虚线框中所示. VAE本身只有两个损失函数,一个重构损失L_R和一个KL散度损失$L_{\rm KL}$. 其中重构损失L_R是为了使解码出来的重构样本x'_j与训练样本x_j尽可能的一致,即

$$L_R=(x_j-x'_j)^2. \tag{9}$$

对于KL散度,描述的是两个概率分布间的差异,

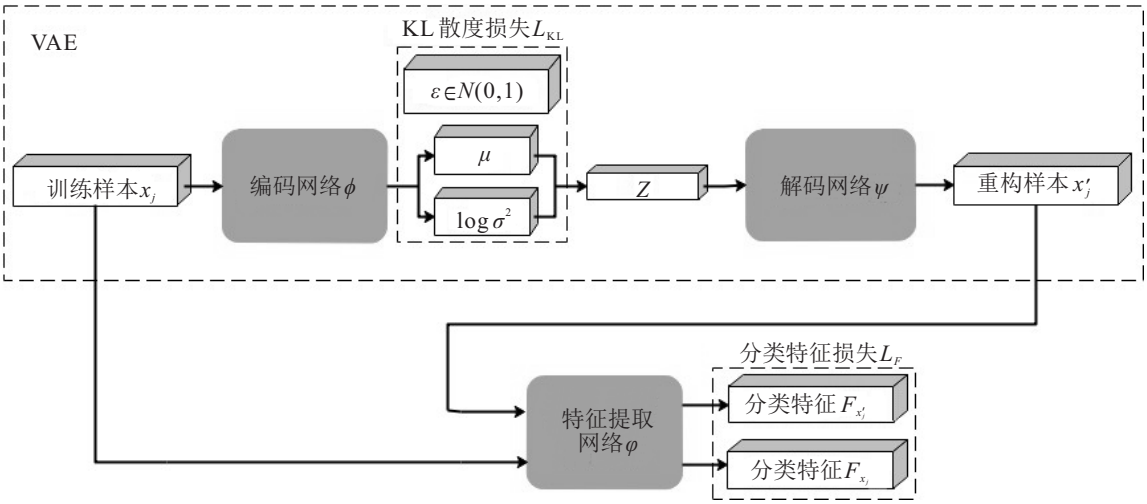


图 2　CF-VAE总体结构

在这里的目的是为了使通过解码网络ϕ得到的Z_j向标准正态分布$N(0,1)$看齐,即

$$L_{\mathrm{KL}} = \mathrm{KL}(N(\mu_j,\sigma_j^2)|N(0,1)) = -\frac{1}{2}(1+\log\sigma_j^2-\mu_j^2-\sigma_j^2). \tag{10}$$

其中: $Z_j = \mu_j + \varepsilon\cdot\sigma_j$, μ_j和$\log\sigma_j^2$分别为训练样本x_j通过编码网络ϕ得到的均值和方差的对数, ε为均值为0、方差为1的标准正态分布.

CF-VAE总体结构如图2所示,通过结合分类器中的特征提取网络φ为传统VAE构建新的损失项. 它在训练好当前分类器后,将分类器的特征提取网络冻结,只作为一个提取特征的模块,训练样本x_j通过特征提取网络φ后能得到一组用于分类的特征,记为F_{x_j},即

$$F_{x_j} = \varphi(x_j). \tag{11}$$

同样地,通过解码网络ψ重构的样本x'_j也通过特征提取网络得到一组特征$F_{x'_j}$,则新的损失函数L_F为

$$L_F = (F_{x_j} - F_{x'_j})^2. \tag{12}$$

最终,通过最小化3个损失的加权和L_{ALL}来训练伪样本生成器,即

$$L_{\mathrm{ALL}} = L_R + L_{\mathrm{KL}} + L_F = (x_j - x'_j)^2 - \frac{1}{2}(1+\log\sigma_j^2 - \mu_j^2 - \sigma_j^2) + (F_{x_j} - F_{x'_j})^2. \tag{13}$$

总体而言,提出的基于分类特征约束变分伪样本生成器的类增量学习方法在进行类增量学习时,旧类的所有训练数据不再可用,而在完成类增量学习后只需保留单一的分类器与生成器,即能完成对目前观测到的类进行多分类和对新类进行类增量学习,且分类器与生成器的参数规模保持不变.

基于分类特征约束变分伪样本生成器的类增量学习过程如下所示.

算法2　基于CF-VAE的类增量学习.

输入: 新类数据集S_{new},旧分类器G_t与伪样本生成器ψ_t;

输出: 新分类器G_{t+1}与新伪样本生成器ψ_{t+1}.

初始化: $S_{\mathrm{old}}^{\mathrm{gen}} = \varnothing$, $S_{\mathrm{train}} = \varnothing$.

step 1: 通过式(1)利用伪样本生成器ψ_t生成旧类的伪样本$X_{\mathrm{old}}^{\mathrm{gen}}$;

step 2: 通过式(2)为每个旧类的伪样本打上精馏标签$Y_{\mathrm{old}} = G_t\{\varphi(X_{\mathrm{old}}^{\mathrm{gen}})\}$;

step 3: 根据算法1精确选择每个类的伪样本数量与其精馏标签构建伪样本集$S_{\mathrm{old}}^{\mathrm{gen}} \leftarrow$伪样本选择$(G_t,\psi_t)$;

step 4: 通过新类标签数据集S_{new}和旧类的伪样本集$S_{\mathrm{old}}^{\mathrm{gen}}$共同构建增量训练数据集$S_{\mathrm{train}} = S_{\mathrm{old}}^{\mathrm{gen}} \bigcup S_{\mathrm{new}}$;

step 5: 通过增量训练数据集S_{train}训练新分类器G_{t+1}与伪样本生成器ψ_{t+1}.

2　实验结果及分析

在这里,以类的平均分类精度评估类增量学习,每次类增量学习都是来自整个数据集的类的一个不相交子集. 在4个数据集中评估类增量学习: MNIST、FASHION、SVHN和E-MNIST. 所有数据集在进行类增量学习时被细分为独立的子集,前3个数据集每个子集有2个类,总共5个子集覆盖数据集所有的类. E-MNIST是一个较大的数据集,以每个子集3个类将它划分为8个子集,在8个连续的子集中覆盖了24个不同的类.

2.1 类增量学习的对比实验

为验证所提出的类增量学习方法的优势,与文献[20]提出的CloGAN分别在MNIST、FASHION、SVHN以及E-MNIST数据集上进行比较,以平均分类精度作为衡量标准. 为了更好地对比,分别评估了CF-VAE与CloGAN的分类器与生成器. 分类器方面,CloGAN的分类器使用一个6层的卷积神经网络,通过实验,发现一个3层的全连接神经网络就能很好地对这些数据集进行分类,所以CF-VAE的分类器使用一个3层的全连接神经网络. 对比CF-VAE与CloGAN的分类器在各个数据集上的分类性能,结果如表1所示,CF-VAE与CloGAN的分类器在各个数据集上具有相似的平均分类精度,其中CloGAN的分类器在E-MNIST数据集上较CF-VAE的分类器有更好的分类性能. 表2比较了CF-VAE与CloGAN生成器的网络结构. CloGAN的生成器采用AC-GAN,由判别网络与生成网络构成,其中判别网络与生成网络的隐藏层分别为5层与4层卷积层. CF-VAE采用与ACGAN相似的网络结构,即CF-VAE的编码网络与解码网络的隐藏层都是4层的卷积层.

表1 分类器在各个数据集上的平均分类精度 %

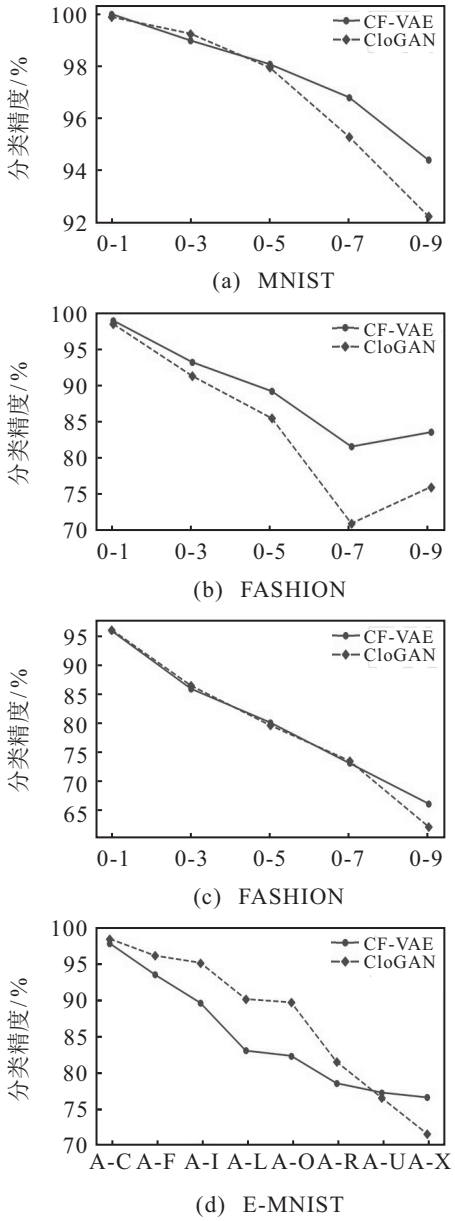
分类器	MNIST	FASHION	SVHN	E-MNIST
CloGAN	98.29	86.48	84.43	89.41
CF-VAE	97.99	86.8	84.33	86.14

表2 生成器的网络结构

网络结构	编码网络/判别网络	解码网络/生成网络
AC-GAN	5层卷积层	4层卷积层
CF-VAE	4层卷积层	4层卷积层

设CloGAN在MNIST、FASHION、SVHN以及E-MNIST数据集上的预留图像缓冲区分别为数据集训练样本数量的0.16%、0.1%、0.8%以及0.8%,CF-VAE与CloGAN在各个数据集上完成所有类的增量训练得到的平均分类精度结果如图3所示.

图3中各个折线图的纵坐标为分类精度,横坐标为类名,FASHION数据集中各种服饰的标签以数字0～9代替. 图3中各图的结果表明了在各个数据集中CF-VAE比起CloGAN具有更好的分类效果,即使是不使用旧类的图像作为缓冲区,也能有效地降低灾难性遗忘的影响. 从E-MNIST数据集上的实验结果可以看出,GloGAN方法在前几次增量中具有较大的优势,但后劲不足,究其原因则是在缓冲区大小不变的情况下,前几次类增量学习中每类能保留的旧类样本数量较多,而经过多次类增量后每类保留的样本数迅速减少,则CloGAN的性能也随之骤降.



(a) MNIST (b) FASHION (c) FASHION (d) E-MNIST

图3 平均分类精度对比

表3比较了近两年的基于重放的类增量学习方法在完成每个数据集的所有类增量训练后的最大平均分类精度. 在MNIST数据集中,CF-VAE的平均分类精度为94.40%,分类效果比MeRGAN的98.25%与DGR的94.90%略差,但是对于其他比MNIST数据集困难得多的数据集,CF-VAE比起DGR和MeRGAN更具优越性.

表3 分类器在各个数据集上的平均分类精度 %

方法	MNIST	FASHION	SVHN	E-MNIST
CF-VAE	94.40	83.71	66.23	76.46
CloGAN	92.26	76.15	62.33	71.45
MeRGAN	98.25	65.62	31.94	61.92
DGR	94.90	62.11	46.83	42.35

2.2　高、低分类分数伪样本对分类性能的影响

为了表明基于分类分数的样本选择策略对生成的伪样本在分类性能上的影响,通过生成E-MNIST数据集中的类A、B、C的伪样本进行说明.根据实验,将分类分数的阈值设置为0.9能得到最佳的结果,生成的A、B、C类的伪样本如图4所示。

(a)　分类分数≤0.9

(b)　分类分数 >0.9

图 4　生成的ABC类伪样本

从图4可以看出,高分类分数的伪样本的图像质量比低分类分数的伪样本好.进一步地,为了更好地说明高、低分类分数伪样本对分类性能的影响,将高、低分类分数的伪样本通过特征提取网络得到分类特征,并将这些分类特征降到2维,降维后的高、低分类分数的伪样本的分类特征表示如图5所示,其中A_H、B_H、C_H、A_L、B_L、C_L分别对应ABC类伪样本分类分数大于0.9与小于等于0.9的分类特征

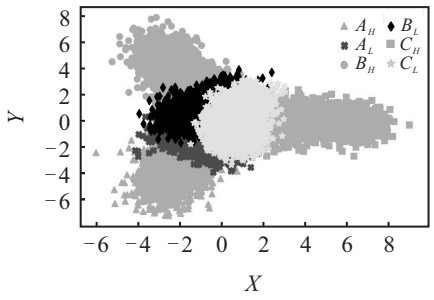


图 5　生成的ABC类伪样本的分类特征在2维上的表示

从图5可以看出:低分类分数的伪样本的分类特征类与类之间没有明显的区分间隔,类与类之间相互包含;而高分类分数的伪样本的分类特征类与类之间有着明显的区分间隔,即高分类分数的伪样本在分类器上更具可分性.

2.3　各个模块对分类器性能的影响

为了进一步说明所提出的类增量学习方法的有效性,在E-MNIST上进行了额外的实验,在实验中分离了算法的各个模块,其中包含:

1)使用精馏标签来保留更多的旧类的知识;

2)基于分类特征约束变分伪样本生成器CF-VAE;

3)基于分类分数的伪样本选择.

创建4种混合设置:

第1种设置为基于传统VAE + one-hot标签;

第2种设置为基于传统VAE + 精馏标签;

第3种设置为基于CF-VAE + 精馏标签;

第4种设置为基于CF-VAE + 精馏标签 + 伪样本选择.

以平均分类精度作为衡量标准,实验结果如图6所示.

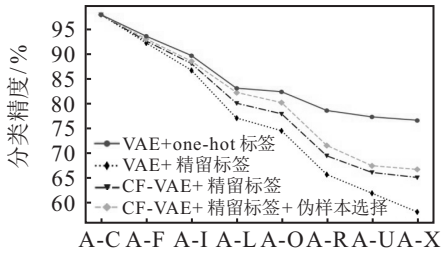


图 6　4种混合设置的平均分类精度

如图6所示,VAE+one-hot标签模型的平均分类精度为58.11 %,使用精馏标签能将平均分类精度提升到65 %,在此基础上将VAE替换为CF-VAE能使平均分类精度上升到66.61 %,最后经过伪样本选择后平均精度达到最大值76.46 %.图6表明,每增加一种模块性能都有所提升,即提出的类增量学习方法的各个模块都可以为其良好的性能做出贡献,所有这些模块结合能够获得最优的结果.

3　结　论

类增量学习是现今人工智能领域的研究热点和难点,其中主要的挑战是如何有效地解决灾难性遗忘.针对这个问题,本文提出了一种全新的类增量学习算法,首先该算法使用CF-VAE来保证生成的伪样本能更好地保留旧类在分类器上的性能;其次以知识精馏的思想为CF-VAE生成的伪样本打上精馏标签,进一步保留从旧类中获得的知识;最后采用基于分类器分数的伪样本选择策略,能在保持每个旧类伪样本数量平衡的前提下选择一些更具代表性的旧类的伪样本.该类增量学习方法能在完全不保留旧类样本数据的前提下,有效减少灾难性遗忘的影响,提高图像分类精度.

参考文献(References)

[1]　Mccloskey M, Cohen N J. Catastrophic interference in connectionist networks: The sequential learning problem[J]. Psychology of Learning and Motivation, 2016, 24: 109-165.

[2] 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.

[3] Lee S W, Kim J H, Jun J, et al. Overcoming catastrophic forgetting by incremental moment matching[C]. Advances in Neural Information Processing Systems. Curran Associates: New York, 2017: 4652-4662.

[4] Zenke F, Poole B, Ganguli S. Continual learning through synaptic intelligence[C]. International Conference on Machine Learning. Lille: International Machine Learning Society, 2017: 3987-3995.

[5] Chaudhry A, Dokania P K, Ajanthan T, et al. Riemannian walk for incremental learning: Understanding forgetting and intransigence[C]. European Conference on Computer Vision. Berlin: Springer, 2018: 556-572.

[6] 刘培磊, 唐晋韬, 谢松县, 等. 增量式神经网络聚类算法[J]. 国防科技大学学报, 2016, 38(5): 137-142.
(Liu P L, Tang J T, Xie S X, et al. Incremental neural network clustering algorithm[J]. Journal of National University of Defense Technology, 2016, 38(5): 137-142.)

[7] Cai S, Xu Z, Huang Z, et al. Enhancing CNN incremental learning capability with an expanded network[C]. Proceedings of the IEEE International Conference on Multimeia and Expo. California: IEEE, 2018: 1-6.

[8] Mallya A, Davis D, Lazebnik S. Piggyback: Adapting a single network to multiple tasks by learning to mask weights[C]. European Conference on Computer Vision. Berlin: Springer, 2018: 67-82.

[9] Mallya A, Lazebnik S. PackNet: Adding multiple tasks to a single network by iterative pruning[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Computer Society, 2018: 7765-7773.

[10] 邹国锋, 傅桂霞, 王科俊, 等. 自适应深度卷积神经网络模型构建方法[J]. 北京邮电大学学报, 2017, 40(4): 98-103.
(Zou G F, Fu G X, Wang K J, et al. Construction method of adaptive deep convolutional neural network model[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(4): 98-103.)

[11] Hinton G, Vinyals O, Dean J. Distilling the knowledge in a neural network[J]. Computer Science, 2015, 14(7): 38-39.

[12] Li Z Z, Hoiem D. Learning without forgetting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 40(12): 2935-2947

[13] Rannen A, Aljundi R, Blaschko M B, et al. Encoder based lifelong learning[C]. Proceedings of the IEEE International Confenerce on Computer Vision. Piscataway: IEEE, 2017: 1329-1337.

[14] Shmelkov K, Schmid C, Alahari K. Incremental learning of object detectors without catastrophic forgetting[C]. Proceedings of the IEEE International Conference on Computer Vision. Piscataway: IEEE, 2017: 3400-3409.

[15] Rebuffi S A, Kolesnikov A, Sperl G, et al. iCaRL: Incremental classifier and representation learning[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Computer Society, 2017: 5533-5542.

[16] Castro F M, Marin-Jimenez M J, Guil N, et al. End-to-end incremental learning[C]. European Conference on Computer Vision. Berlin: Springer, 2018: 233-248.

[17] Mellado D, Saavedra C, Chabert S, et al. Pseudorehearsal approach for incremental learning of deep convolutional neural networks[C]. Latin American Workshop on Computational Neuroscience. Berlin: Springer, 2017: 118-126.

[18] Shin H, Lee J K, Kim J, et al. Continual learning with deep generative replay[C]. Advances in Neural Information Processing Systems. Curran Associates: New York, 2017: 2991-3000.

[19] Wu C S, Herranz L, Liu X L, et al. Memory replay GANs: Learning to generate images from new categories without forgetting[C]. Advances in Neural Information Processing Systems. Curran Associates: New York, 2018: 5962-5972.

[20] Rios A, Itti L. Closed-Loop memory GAN for continual learning[C]. International Joint Conference on Artificial Intelligence. California: Macau, 2019: 3332-3338.

[21] Yuhong Yang. Information theory, inference, and learning algorithms[J]. Publications of the American Statal Association, 2005, 100(472): 1461-1462.

[22] Azadi S, Olsson C, Darrell T, et al. Discriminator rejection sampling[J]. STAT PAP, 2019, 1050: 11-26.

作者简介

莫建文 (1972–), 男, 副教授, 博士, 从事机器视觉、图像识别、智能信号处理等研究, E-mail: mo_jianwen@126.com;

陈瑶嘉 (1994–), 男, 硕士生, 从事机器视觉、图像识别的研究, E-mail: 982776090@qq.com.

(责任编辑：齐 霁)