第 5 章

脑与自然启发的学习优化

5.1 多尺度学习

5.1.1 多尺度学习原理

多尺度的本质其实是对信号的不同粒度采样，通常可以在不同的尺度下提取不同的特征，据此完成不同的任务。为了获得更有效的特征表达，科研人员在传统图像处理算法中，往往依附于图像金字塔和高斯金字塔这一概念。

多尺度技术被广泛应用于目标检测领域。目标检测作为计算机视觉领域的核心问题之一，其目的是找出图像中的感兴趣区域，同时检测目标的位置和类别作为输出信息。随着 2012 年 ImageNet 的兴起，目标测算法所使用的特征也从传统算法的手工特征向深度神经网络的深度特征过渡。在网络结构的设计上，从两阶段到一阶段，从单一尺度网络到多尺度特征提取，学者们在网络的各个环节（特征提取、损失函数、框生成、IoU 设计等）角度出发分析短板，不断提高检测器的性能。

在目标检测中，识别不同尺寸目标（尤其是小目标）一直是难点，而构造多尺度特征金字塔可以很好地解决多尺度目标检测这一问题。

图 5.1(a)所示是一个特征图像金字塔。首先对原始图像构造金字塔，然后所在金字塔的每一层提取不同的特征，最后进行对应的预测。这种方法具有明显缺点：计算量大、内存耗费大，但可以获得较好的检测精度。计算量通常会成为整个算法的性能瓶颈，因此，当前很少有神经网络中使用这种算法。

图 5.1(b)所示是一种改进的思路。学者们发现可以利用卷积网络本身所具有的特性，即通过对原始图像进行卷积和池化操作，可以获得不同尺寸的特征图，这种操作类似于在图像的特征空间中进行金字塔构建。实验表明，浅层网络往往更关注细节信息，而高层网络则更关注语义信息，因此充分利用高层的语义信息，可以准确地检测出目标。综上，可以利用最后一个卷积层的特征图进行预测。这种方法广泛应用在大多数现有深度网络中（如

VGG、ResNet、Inception 等),即使用深度网络的最后一层特征实现分类。

上述方法需要内存少且运算速度快。但其也具有明显缺点:仅仅关注深层网络的最后一层特征,会忽略其他层的特征。由于其他层的细节信息在一定程度上也可以提升检测的精度,因此产生了如图 5.1(c)所示的架构。其设计思想就是同时利用低层特征与高层特征,在不同的层中分别进行预测。简单而言,一幅图像中往往具有多个不同大小的目标,仅仅使用浅层的特征就可以检测简单目标,而利用复杂的特征可以检测复杂目标。概述整体过程就是在原始图像上应用深度卷积的基础上,再分别在不同的特征层上预测。其优点是在不同的层上可以输出对应的目标,因为不需要经过所有的层才能输出对应的目标(即对于某些目标来说,可省略多余的前向操作)。据此,神经网络在一定程度上得以加速,同时算法的检测性能也得到保障。但是,该结构也具有明显缺点:其获得的特征不鲁棒,基本都是一些弱特征(大多是从较浅的层获得的)。

为改善这一问题,提出了 FPN,其架构如图 5.1(d)所示。首先,对输入的图像进行深度卷积,然后对第二层的特征进行降维操作(添加一层尺寸为 1×1 的卷积层),接着对第四层上的特征进行上采样,使其具有相应的尺寸,再对处理后的第二层和处理后的第四层执行加法操作(对应元素相加),获得结果作为第五层的输入。使用 FPN 可以获得一个强语义信息,从而可以提高检测性能。

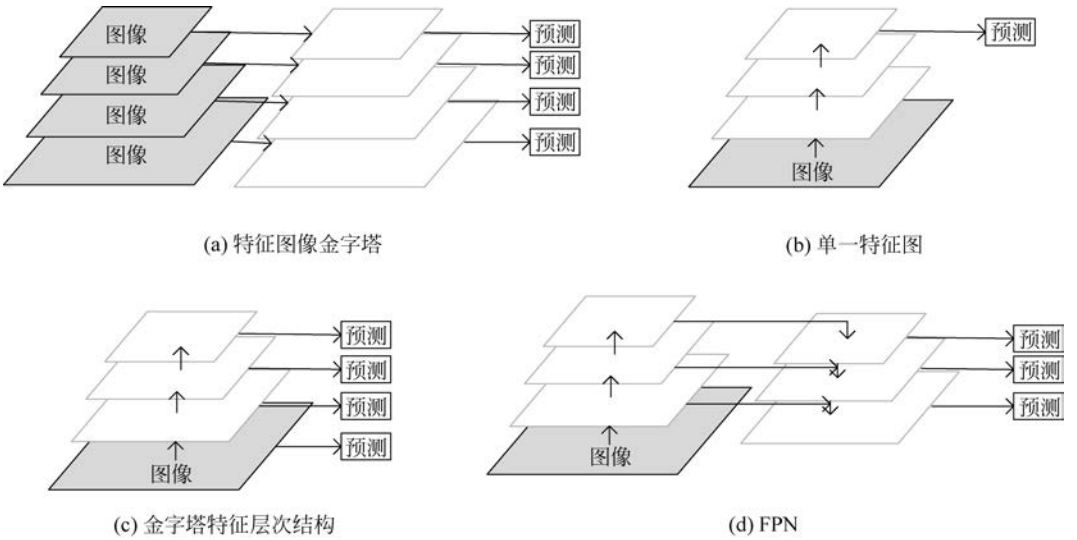

图 5.1 FPN 示意图

(https://blog.csdn.net/u013010889/article/details/78658135)

值得注意的是,使用更深的层来构造特征金字塔,可以使信息更加鲁棒。另外,因为多次的降采样和上采样操作会使深层网络的定位出现偏差,而低层特征往往可以提供较准确的位置,因此可以将处理过的低层特征和高层特征累加,构建一个更深的特征金字塔,同时

融合多层特征信息，并在不同的特征层进行输出。

5.1.2　SSD 网络

分析 FPN 的结构发展和由来可知，第三、四种结构明显优于前两种，故而也被广泛应用。在图像检测领域，One-stage SSD 就采用了图 5.1(c)金字塔形的功能层次结构，即使用分层特征预测目标，使得不同层的特征来学习同样的语义信息。

单方向的特征金字塔结构首先是在 SSD 中提出的，其主要思想是：利用图像提取的不同尺度特征构建特征金字塔，在不同的特征尺度进行预测，最后将结果进行融合。这个过程中，越深的特征具有越丰富的语义信息，且分辨率越高，从而充分提取大目标的语义信息，较浅的特征则对小目标比较友好。

SSD 以不同大小步幅的特征图作为检测层，分别检测出不同尺度的目标，用户可依据任务制定目标尺度方案。一般情况下，低层特征图步幅较小，尺寸较大，感受野较小，可以检测到小目标。高层特征图步幅较大，尺寸较小，感受野较大，可以检测到大目标。

该方式在尺度处理上简单有效，但也存在一些缺陷。

(1) 低层特征一般用于检测小目标，但低层的感受野小，且上下文信息缺乏，易造成误检。

(2) 高层虽然具有较大的感受野，但多次降采样操作可能会造成大目标的语义信息丢失。

(3) 多层特征结构，是非连续的尺度表达，即是非最优的结果。

5.1.3　FPNet

FPNet 提出了一种不同分辨率特征融合方式，既每个分辨率得到的特征图和上采样的低分辨率特征以元素的方式相加，实现不同层次的特征增强。由于此方式只在网络基础上增加了两步操作：跨层连接和元素形式相加，增加的计算量很少，对网络性能的改善卓越，故成了目标检测领域的标配。

FPNet 包括自下向上的连接、自上而下的连接和侧面连接三部分。

(1) 自下向上的连接：分层级计算出不同的分辨率特征。采用 ResNet 作为基础网络，分别提取 5 个分层特征$\{\boldsymbol{C}_1,\boldsymbol{C}_2,\boldsymbol{C}_3,\boldsymbol{C}_4,\boldsymbol{C}_5\}$。由于$\boldsymbol{C}_1$占用内存较大，故不考虑，只取$\{\boldsymbol{C}_2,\boldsymbol{C}_3,\boldsymbol{C}_4,\boldsymbol{C}_5\}$构成特征金字塔，相对于图像的分辨率下采样为$\{4,8,16,32\}$。

(2) 自上而下的连接：从$\boldsymbol{C}_5$开始，通过最近邻方法把特征图上采样 2 倍得到$\boldsymbol{C}_5'$，$\boldsymbol{C}_4$通过 1×1 卷积调整通道数得到$\boldsymbol{C}_4'$，$\boldsymbol{C}_5'$和$\boldsymbol{C}_4'$具有相同的分辨率，可以直接进行逐元素相加操作。据此迭代实现$\boldsymbol{C}_3$、$\boldsymbol{C}_2$的特征融合，该过程可以逐步增强小目标信息。

(3) 侧面连接：计算得到每个相加的特征图，再次使用 3×3 的卷积对其处理，得到最终的特征图$\{\boldsymbol{P}_2,\boldsymbol{P}_3,\boldsymbol{P}_4,\boldsymbol{P}_5\}$。

FPNet 构架了一个端到端训练的特征金字塔，通过神经网络的层级结构，实现了高效的强特征计算。通过结合自下而上与自上而下的方法来获取较强的语义特征，大幅提高了目标检测和实例分割在各数据集上的性能表现。同时，该结构灵活易推广。

Fast R-CNN 是一种基于区域的物体检测器，使用感兴趣区域池（Region-of-Interest，RoI）提取特征。Fast R-CNN 通常在单尺度特征地图上执行。为了在 FPNet 中使用它，需要将不同尺度的 RoI 分配给金字塔级别。

因为特征金字塔是从一个图像金字塔中产生的，所以当基于区域的探测器在图像金字塔上运行时，可以调整它们的分配策略。在形式上，将宽度为 w、高度为 h 的 RoI 分配给的特征金字塔的 P_k 层：

$$k = \left\lfloor k_0 + \log_2\left(\frac{\sqrt{wh}}{224}\right)\right\rfloor \tag{5-1}$$

自从 2016 年提出 FPNet 网络后，目前很多视觉任务均采用 FPNet 作为进一步研究的基础网络。FPNet 通过更为轻量的最近邻插值结合侧向连接，实现了将高层的语义信息逐渐传输到低层的功能，从而使得尺度信息更为平滑。虽然 FPNet 看似完美，但其仍然有一些明显缺陷。

（1）FPNet 在上采样过程中使用了比较粗糙的最近邻插值，导致高层的语义信息不一定得到有效传播。

（2）通过多次下采样，FPNet 的最高层的感受野虽然丰富，但可能也丢失了小目标的语义信息。

（3）FPNet 的构建过程中，只使用了基础的 4 层输出，其输出的多尺度信息不一定足够。

（4）FPNet 中虽然可以传播强语义信息给其他层，但因为其本身就提取了不同 backbone 的输出，因此对于不同尺度的表达能力可能仍然存在区别。

为了解决上述问题，科研人员提出了很多变体，简述如下。

5.1.4 PANet

PANet 是由中国香港中文大学和腾讯优图联合提出的一种实例分割框架。在该框架中，核心内容是增强 FPN 的多尺度融合信息。PANet 因为其卓越性能，在 COCO2017 挑战赛中的实例分割任务中取得了第一名的成绩，在目标检测任务中取得了第二名的成绩。

PANet 的目标检测和实例分割采用共享的网络架构如图 5.2 所示，在该框架下，两者性能均有提升。

由于 FPN 的高层级特征与低层级别之间的特征连接路径较长，如图 5.2 中虚线①所示，故而增加了访问准确定位信息时的难度。因此，在 FPN 基础上，PANet 创建了自下而上的路径增强方式，通过缩短特征信息的连接路径，PANet 利用低层级的较准确的定位信

息增强特征金字塔的性能。

PANet 创建了自适应特征池化(adaptive feature pooling)，恢复每个候选区域和所有特征层次之间被原先的较长连接所破坏的信息路径，并聚合每个特征层的每个候选区域。

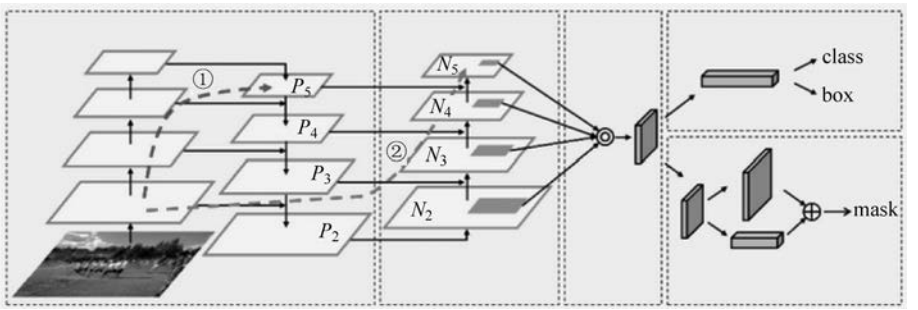

图 5.2　PANet 示意图

(https://blog.csdn.net/weixin_37993251/article/details/88245006)

5.1.5　ThunderNet

ThunderNet 是旷视提出的一种轻量型目标检测框架，有效地实现了 ARM 平台上的实时检测。ThunderNet 的整体结构如图 5.3 所示。与 FPN 相比，ThunderNet 对 FPN 结构进行了简化，只使用 C_4/C_5 层，并引入池化操作，C_4 分辨率大小的累加特征作为最终的输出。

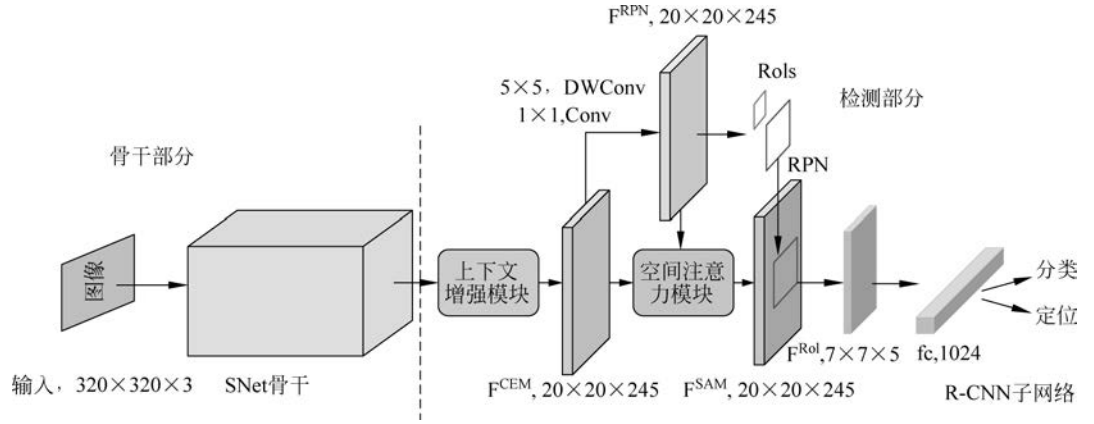

图 5.3　ThunderNet 示意图

(https://blog.csdn.net/qiu931110/article/details/88903724/)

ThunderNet 使用 320×320 像素作为网络的输入分辨率。其整体网络结构分为两部分：骨干部分和检测部分。网络骨干部分采用的是 SNet(ShuffleNetV2 修改版)。网络检

测部分采用的是压缩的 RPN 网络，即利用上下文增强模块(Context Enhancement Module，CEM)整合局部和全局特征，从而增强网络的特征表达能力。同时，ThunderNet 提出了空间注意力模块，引入来自 RPN 的前后景信息优化特征分布。

5.1.6 Libra R-CNN

Libra R-CNN 是由浙江大学、香港中文大学等联合提出的一种新颖的目标检测模型。就目标检测领域而言，无论是一阶段的还是两阶段的，都涉及候选区域的选择、特征的提取与融合、损失是否收敛等多个问题。针对目标检测的三个阶段，有学者提出了三个问题：采样的候选区域是否具有很好的代表性，不同层特征如何有效融合，损失函数如何得到更好的收敛。针对这三个问题，Libra R-CNN 中给出了三个改进方向：IoU-balanced Sampling、Balanced Feature Pyramid、Balanced L1 Loss。其中，第二个改进方向由 FPN 改造而来。为了更高效地利用 FPN 特征，对其进行重新调节、整合、提炼与加强。将$\{C_2,C_3,C_5\}$的多层特征均调节到 C_4 尺寸，并进行加权求平均值。将得到的特征再重新调整返回到$\{C_2,C_3,C_5\}$特征分辨率。同时，使用高斯非局部注意力机制增强特征。

5.1.7 遥感领域中的应用

随着对地观测技术和高分辨率光学遥感平台的逐步发展，过大的图像尺寸、复杂的图像背景、不均的训练样本以及光照和阴影等问题使目标检测与位置识别更具挑战。

在目标检测领域，现有的基于神经网络的自然影像目标检测成果显著，但对遥感影像而言，高精度、高效率的目标检测目前仍相当困难。与自然影像相比，遥感影像检测具有以下特点。

(1) 观测视角的不同：遥感影像通常是由自上而下的视角获取的，而自然图像是从不同的视角获取的，因此物体在影像上的渲染方式有很大不同。

(2) 影像尺寸的区别：遥感影像的尺寸及其覆盖范围通常均比自然影像大得多。同时，遥感影像的处理更耗时，且其占用内存更大。

(3) 类别的不平衡：这种不平衡主要体现在类别数量及目标大小。自然场景中的待检测物体一般都是均匀分布的，同时这些影像通常只含有有限个数的物体，但是遥感影像往往包含一个物体或几个物体，且这些物体的尺寸可能差异巨大。

(4) 其他因素：与自然图像相比，光照条件、图像分辨率、遮挡、阴影、背景和边界锐度等都会极大地影响遥感影像目标检测的效果。

在 2019 年，有学者提出了一种可以同时充分利用语义特征和空间分辨率特征的双多尺度特征金字塔网络(Double Multi-scale Feature Pyramid Network，DM-FPN)。该框架可以充分利用弱空间分辨率、强语义特征和高空间分辨率、弱语义的特征。

另外，为解决遥感影像尺寸过大、背景过于复杂、训练样本大小及其数量分布不均匀等

问题，还有学者提出了多尺度训练、预测和自适应类别非极大值抑制策略。通过多尺度训练和预测策略可以大幅提升检测性能。由于遥感影像的尺寸特点，在深层次的卷积中往往会丢失大量语义信息，尤其是小目标的。因此，可以将遥感影像放大 2 倍、缩小 0.5 倍，放大后的遥感影像可以增强小目标的空间分辨率特征，同时缩小后的遥感影像可以使大目标被完整地分割到单个图像块中实现训练。另外，为了增强训练样本的多样性，训练过程中可以采用多尺度的图块。在进行预测时，通过变形图像检测尽可能多的目标，变形处理包括放大、缩小、水平翻转及垂直翻转。整个过程就是先对每一幅待测试图像均进行多尺度处理，然后根据影像大小信息，将其分割成具有拥有一定重叠度的图像块，并对其进行检测，最后通过自适应类别非极大值抑制获得最终结果。

5.2　注意力学习

5.2.1　注意力学习原理

注意力机制(attention mechanism)是机器学习中的一种数据处理方法。在人工智能领域，随着神经网络在深度学习方面的进展，注意力已成为神经网络结构的重要组成部分，并在自然语言处理、统计学习、语音和计算机视觉等领域有着大量的应用。

注意力机制之所以受到广泛关注，主要是因为人们对影响人类生活的应用程序中的学习模型公平性、问责制和透明度越来越感兴趣(神经网络之前常常被视为黑盒模型)，而注意力机制利用人类视觉机制进行直观解释，可以提高神经网络的可解释性。

最早使用注意力机制的神经网络是 RNN 结构，作为 RNN 的编码器-解码器框架的一部分对长的输入语句进行编码，基于 RNN 的注意力模型如图 5.4 所示。

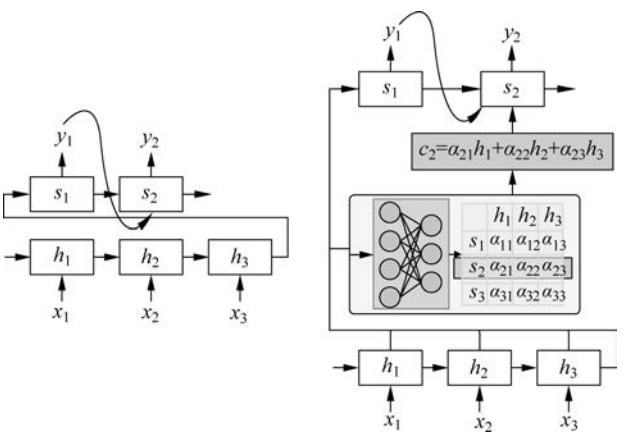

图 5.4　基于 RNN 的注意力模型

(https://arxiv.org/abs/1904.02874)

近几年来，随着注意力机制的变体越来越多，也逐渐向计算机视觉领域渗透。很多深度学习与视觉注意力机制结合的研究工作被证明是有效的。计算机视觉中注意力机制的基本思想是让模型学会专注，把注意力集中在重要的信息上而忽视不重要的信息。下面分别从空间域、通道域介绍计算机视觉中的经典的注意力机制模型。此处需要注意，由于神经网络通过梯度反向传播来学习注意力的权重，因此计算机视觉中的注意力多为可微的软注意力。

空间域的注意力机制的基本原理是将图像中的空间域信息进行对应的空间变换，从而能将关键的信息提取出来。对于 CNN 来说，每一层都会输出一个 $C\times H\times W$ 的特征图，C 表示通道维度，同时也代表卷积核的数量，H 和 W 就是原始图像经过压缩后的图的高度和宽度。针对 CNN 的空间注意力就是对于所有的通道，在二维平面上，对 $H\times W$ 尺寸的特征图中的每个像素都学习到一个权重。

下面重点介绍空间域的注意力机制模型。

5.2.2 STN

空间变换网络(Spatial Transformer Networks，STN)模型利用注意力机制，将原始图像中的空间信息变换到另一个空间中并保留了关键信息。

STN 针对 CNN 中缺乏对输入数据空间不变性的局限性，提出一种基于注意力的空间变换动态机制，主动通过为每个图像生成适当的变换来对图像(或特征图)进行空间变换输入样本，实现了包括缩放、修剪、旋转以及非刚性变形等空间不变性，空间变换遵循：

$$\begin{pmatrix} x_i^s \\ y_i^s \end{pmatrix}=\tau_\theta(G_i)=A_\theta\begin{pmatrix} x_i^t \\ y_i^t \\ 1 \end{pmatrix}=\begin{bmatrix} \theta_{11} & \theta_{12} & \theta_{13} \\ \theta_{21} & \theta_{22} & \theta_{23} \end{bmatrix}\begin{pmatrix} x_i^t \\ y_i^t \\ 1 \end{pmatrix} \tag{5-2}$$

空间变换模块的结构如图 5.5 所示，包括定位网络(localisation net)、网格生成(grid generator)和采样机制(sampler)三部分。输入特征 $\boldsymbol{U}$ 传递给定位网络用于回归转换参数 θ。通过网格生成转换为采样网格，$\tau(G)$ 应用于输入特征 $\boldsymbol{U}$ 产生输出特征图 V。定位网络和采样机制共同构成空间转换器。

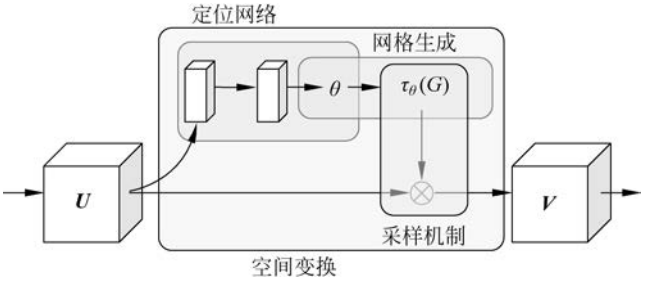

图 5.5 STN 结构图

(https://arxiv.org/abs/1506.02025)

空间变换器模块不仅可以选择图像中最相关的区域(注意力),而且还可以将这些区域转换为规范的预期姿势以简化识别接下来的几层。

5.2.3　SENet

与上述空间域的注意力机制不同,基于通道的注意力的核心思想是通过网络学习通道域上的特征权重,训练模型中有效的特征图权重大,无效或效果小的特征图权重小,从而在任务中达到更好的效果。具体来说,就是通过学习的方式自动获取每个特征通道的重要程度,然后依照这个重要程度增强有用的特征并抑制对当前任务用处不大的特征。

通常,单纯的基于通道的注意力在空间维度上权重相同,即对每一个通道内的信息直接全局平均池化,而忽略通道内的局部信息。

SENet 提出了针对特征图通道中关系的网络结构单元:SE(Squeeze-and-Excitation)模块。SENet 利用能够让网络模型对特征进行校准的门机制,使网络从全局信息出发选择性放大有价值的特征通道,并且抑制无用的特征通道,通过精确建模卷积特征各个通道之间的作用关系,学习通道之间的相关性,改善网络模型的表达能力。

SENet 模块结构如图 5.6 所示,对于任意给定的特征图块 $\boldsymbol{X}\in\boldsymbol{R}^{W'\times H'\times C'}$,进行转换操作

$$F_{\mathrm{tr}}:\boldsymbol{X}\rightarrow\boldsymbol{U},\quad \boldsymbol{U}\in\boldsymbol{R}^{W\times H\times C}$$

其中,F_{tr} 表示标准的卷积操作,将转换后的特征记作 $\boldsymbol{U}$,送入 SENet 模块分别进行挤压(squeeze)和激励(excitation)操作。

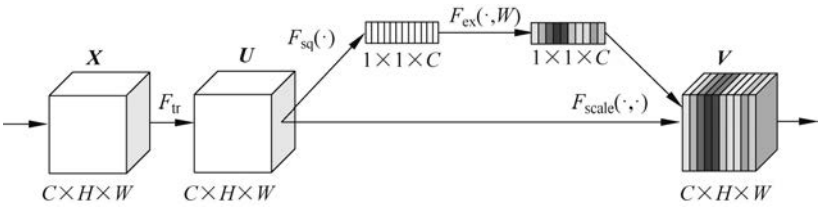

图 5.6　SENet 模块结构

(1) 挤压:全局信息嵌入(global information embedding)。由于每个学习好的卷积核都是以局部感受野的方式进行卷积,因此在经过 SE 模块转换之后的特征 U 的各个数据单元不能利用数据单元以外的纹理信息。为了解决通道之间的依赖关系问题,首先考虑在输出特征组图中各个通道的信号量本身的问题,这个问题在感受野还很小的较浅网络层中最为严重。为了解决这个问题,将特征 $\boldsymbol{U}$ 挤压全局空间信息成为一个通道描述器,挤压过程通过一个简单的全局平均池化层(global average pooling)实现,产生通道的统计信息 $\boldsymbol{z}\in\boldsymbol{R}^{C}$。此处 $\boldsymbol{z}$ 的第 c 个元素计算过程如下:

$$z_c = F_{sq}(u_c) = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} u_c(i,j) \tag{5-3}$$

特征 $\boldsymbol{U}$ 可以看作一组局部描述器集合对整幅通道图的描述信息，为了简化运算，使用了简单的全局平均池化。

(2) 激励：自适应校准(adaptive recalibration)。在挤压操作获得的信息 $\boldsymbol{z} \in \boldsymbol{R}^C$ 的基础上，进行第二步激励操作以捕捉通道的依赖关系。为了达到期望，第二步的函数应该满足两个标准：能够捕捉通道之间的非线性相互作用的关系；能够在多个通道在经过多次激活函数情况下学习多个通道之间非互斥的关系。因此激励模块借助激活函数 Sigmoid，使用简单的门机制进行操作，对数据的具体运算如下：

$$s = F_{ex}(\boldsymbol{z},\boldsymbol{w}) = \sigma[g(\boldsymbol{z},\boldsymbol{w})] = \sigma[\boldsymbol{w}_2\delta(\boldsymbol{w}_1\boldsymbol{z})] \tag{5-4}$$

其中，δ 是进行线性激活函数操作，$\boldsymbol{w}_1 \in \boldsymbol{R}^{\frac{C}{r}\times C}$ 以及 $\boldsymbol{w}_2 \in \boldsymbol{R}^{\frac{C}{r}\times C}$。为了防止模型变得复杂并且考虑到泛化因素，设置了两层全连接层作为瓶颈对门机制进行参数化。最终整个网络模块的输出经过尺度变换操作，具体操作为：

$$\tilde{\boldsymbol{x}}_c = F_{scale}(\boldsymbol{u}_c, \boldsymbol{s}_c) = \boldsymbol{s}_c \cdot \boldsymbol{u}_c \tag{5-5}$$

其中，$\widetilde{\boldsymbol{X}} = [\tilde{\boldsymbol{x}}_1, \tilde{\boldsymbol{x}}_2, \cdots, \tilde{\boldsymbol{x}}_c]$；$F_{scale}(\boldsymbol{u}_c, \boldsymbol{s}_c)$表示特征图 $\boldsymbol{u}_c \in \boldsymbol{R}^{W\times H}$ 和 $\boldsymbol{s}_c$ 的通道域的乘积。

因为输出是由所有通道之和产生的，通道之间的依赖关系隐藏在 v_c 中，但这些依赖关系也和卷积核捕捉的特征图组空间关系相纠缠。因此应确保网络能够利用增加网络本身对有价值信息的敏感性，使这些有价值的信息在之后的网络层中能得到利用，而无用的特征信息则被舍弃。

SENet 的单元内部结构如图 5.7 所示，其易于实现，并且很容易可以加载到现有的网络模型框架中。整个 SENet 模型通过不断堆叠 SENet 模块进行构造，SENet 模块能够在一个网络模型中的任意深度位置进行插入替换，并可以随着在网络层任意插入而自动适应网络模型的需求。SENet 模块能够以一种未知的方式对特征组进行权重奖惩，加强了所在位置的特征图组的表达能力，在整个网络模型中，特征组图的调整的优点能够通过 SENet 模块不断地累计。

5.2.4 SKNet

SKNet(Selective Kernel Networks)是 SENet 的加强版，它采用与 SE 类似的 SK 模块，并可以自适应调节自身的感受野模块。SK 模块核心思想是用多尺度特征汇总的信息在通道域智能地指导如何分配，侧重使用哪个核的表征。该模块对超分辨率任务有一定的提升，并且实验证实了在分类任务上有很好的表现。

SKNet 启发自皮质神经元根据不同的刺激可动态调节其自身的感受野的原理，结合 SENet 中的挤压和激励操作，合并与运行映射(merge-and-run mappings)操作，以及注意力

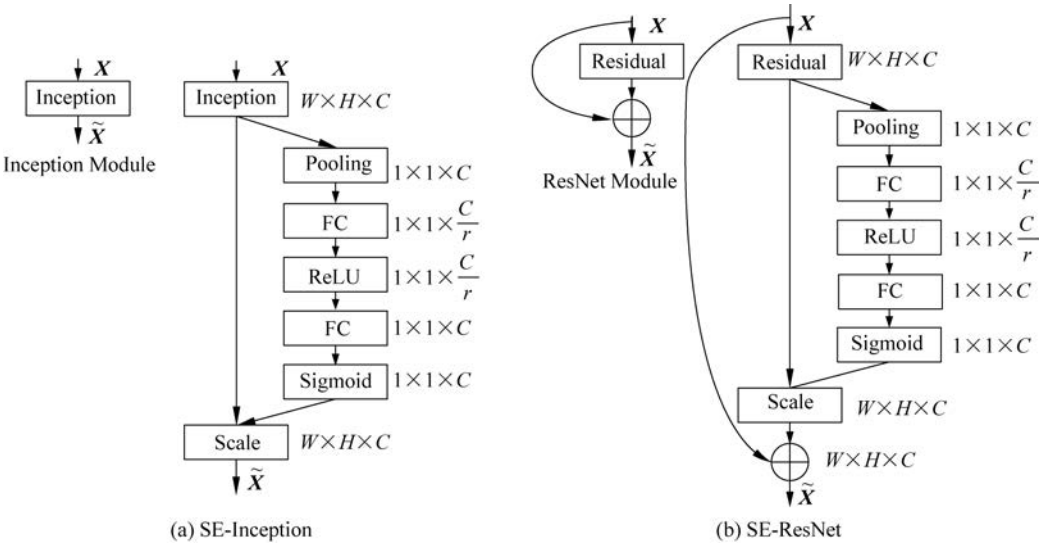

图 5.7　SENet 单元内部结构

初始块(attention on inception block)思想,对所有的卷积核大于 1 的 Kernel 进行 SK(selective kernel)操作,充分利用组卷积/深度卷积带来的较小的理论参数和触发器的优势,使增加多路与动态选择的设计也不会带来很大的负担。这样的设计使任何网络进行 SK 操作变得非常容易,网络整体结构如图 5.8 所示。

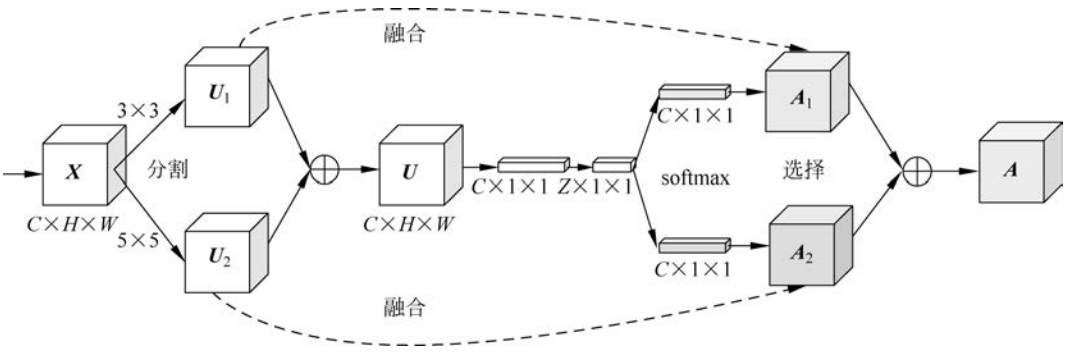

图 5.8　SKNet 网络结构图

(https://arxiv.org/pdf/1903.06586.pdf)

SKNet 的结构使得它可以简单便捷地移植到多分支网络中。以三分支为例,图 5.9 给出了网络为三分支时的 SKNet 模型(分支数量也是 SK 模块的一个可选参数)。

原始特征图 $\boldsymbol{X}$ 经过不同尺度的卷积核后得到 $\boldsymbol{U}_1$、$\boldsymbol{U}_2$、$\boldsymbol{U}_3$ 三个特征图,然后相加得到了 $\boldsymbol{U}$,$\boldsymbol{U}$ 中融合了多个感受野的信息。得到的 $\boldsymbol{U}$ 是维度为 $C\times H\times W$ 的特征图,沿着 H 和 W 维度求平均值,最终得到的是与通道信息相关的 $C\times 1\times 1$ 的一维向量,代表各个通道的信

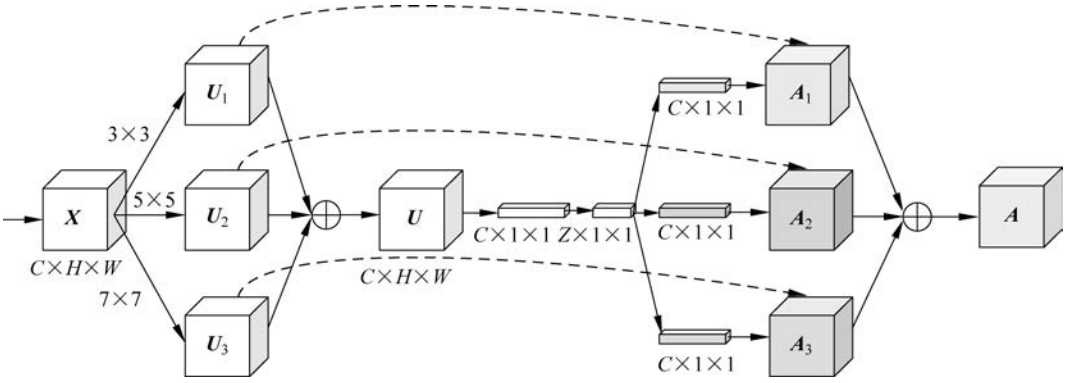

图 5.9 三分支 SKNet 结构图

(https://www.163.com/dy/article/G36IT8BJ0531D9VR.html)

息的重要程度。

之后再用了一个线性变换,将原来的 C 维映射成 Z 维的信息,然后分别使用了 3 个线性变换,从 Z 维变为原来的 C,这样完成了针对通道维度的信息提取,然后使用 softmax 进行归一化,此时每个通道对应一个分数,代表其通道的重要程度,这相当于一个掩膜(mask)。将 3 个得到的 Selective Kernel 分别乘以对应的 $\boldsymbol{U}_1$、$\boldsymbol{U}_2$、$\boldsymbol{U}_3$,得到 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$。然后 3 个模块相加,进行信息融合,得到最终模块 $\boldsymbol{A}$,相比于最初的 $\boldsymbol{X}$,模块 $\boldsymbol{A}$ 经过了信息的提炼,融合了多个感受野的信息。

通道域注意力的基本思想给每个通道上的信号都增加一个权重,来代表该通道与关键信息的相关度,这个权重越大,则表示相关度越高。

5.2.5 遥感领域中的应用

遥感领域的众多任务中,运用注意力机制增强目标特征或感兴趣区域,有效解决了分类、分割、检测等多种遥感任务中的痛点问题。

举例来说,在极化 SAR 图像分类任务中,基于注意力机制的 Attention Ladder Network(ALN),在梯形网络中分别设计了注意力编码器和注意力解码器,使模型在学习的过程中自动筛选出对当前任务有用信息,从而提取有注意力感知的特征,提高模型的学习效率。在高光谱图像分类任务中,传统 CNN 难以提取高光谱图像局部特征,为了加强对高光谱图像的空间域和光谱域中局部关键性特征的学习,引入基于空间-光谱注意力的高光谱图像特征提取方法,提高了高光谱图像特征的表征能力。在雷达点云数据分类任务中,基于时间空间多尺度注意力神经网络,利用双通道空间、光谱和多尺度注意卷积,学习频谱和空间增强的特征表示,并表示不同类的多尺度信息,在雷达数据集上实现更具竞争力的分类性能。

注意力机制同样成功应用于遥感图像处理的核心问题——遥感检测中。遥感图像目标检测旨在定位并识别遥感图像中的感兴趣目标。针对遥感影像小目标难以检测的问题，为了增加网络的辨识能力，更多地关注网络中提取的高频特征，在目标检测网络 Faster-RCNN、RetinaNet 等基础上，引入空间-通道注意力机制网络，在特征提取网络中加入注意力机制模块可以获取更多需要关注目标的信息，抑制其他无用信息，以适应遥感图像视野范围大导致的背景复杂和小目标问题，提高检测器性能。使用旋转锚点框实现任意方向目标的检测，改善了自然图像检测网络对小目标检测准确度低的问题，解决了遥感影像中密集分布、任意方向的小目标检测识别问题。

5.3　Siamese 协同学习

5.3.1　Siamese 协同学习原理

在单输入网络分类中，不同类别的样本不均衡会导致对样本较少的类别无法充分训练。为解决这个问题，Chopra 等提出了 Siamese 网络，神经网络的“孪生(Siamese)”是通过共享权重实现的，如图 5.10 所示。

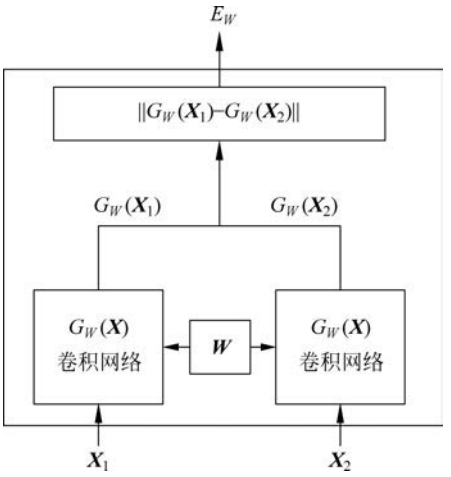

图 5.10　Siamese 网络的结构示意图

(https://blog.csdn.net/sxf1061926959/article/details/54836696)

Siamese 网络的目的是从数据中去学习一个相似性度量，然后用这个学习的度量去比较和匹配新的未知类别的样本。这个方法可应用于类别数多或者整个训练样本无法用于之前方法训练的分类问题。以图像处理任务为例，Siamese 网络的输入样本($\boldsymbol{x}_1$，$\boldsymbol{x}_2$，$\boldsymbol{x}_3$)由一对图像和一个标签组成。输入数据是一对图像($\boldsymbol{x}_1$，$\boldsymbol{x}_2$)，输入标签 $\boldsymbol{y}$ 为 0 或 1，0 代表输入数据为同一类，1 代表输入数据为不同类。输入图像 $\boldsymbol{x}_1$、$\boldsymbol{x}_2$ 分别送入双支路网络得到输出

$G(\boldsymbol{x}_1)$和$G(\boldsymbol{x}_2)$。损失函数定义为：

$$L(\boldsymbol{w})=\sum_{i=1}^{P} l(\boldsymbol{w},(\boldsymbol{y},\boldsymbol{x}_1,\boldsymbol{x}_2)^i)$$

$$l(\boldsymbol{w},\boldsymbol{y},\boldsymbol{x}_1,\boldsymbol{x}_2)=(1-\boldsymbol{y})-L_G(E_W)+YL_1(E_W)=(1-\boldsymbol{y})\frac{2}{Q}(E_W)^2+(Y)2Q\mathrm{e}^{\frac{2.77}{Q}E_W}$$

$$E_W(\boldsymbol{x}_1,\boldsymbol{x}_2)=\|G_W(\boldsymbol{x}_1)-G_W(\boldsymbol{x}_2)\| \tag{5-6}$$

其中，L_G 计算相同类别的图像对的损失函数，L_1 计算不同类别的图像对的损失函数。P 为训练的样本数，Q 为常数，$\boldsymbol{w}$ 为双支路网络的共享参数。最后对损失函数进行梯度反向传播以更新网络共享的权重 $\boldsymbol{w}$。

Siamese 网络与单输入网络的主要区别如下。

(1) 输入不再是单个样本，而是一对样本，不再给单个的样本确切的标签，而且给定一对样本是否来自同一个类的标签，如果是则为 0，否则为 1。

(2) 设计了两个一模一样的网络并且网络共享权重，对输出进行了距离度量。

(3) 针对输入的样本对是否来自同一个类别设计了损失函数，损失函数形式类似交叉熵损失。

Siamese 网络主要的优点是淡化了标签，可以对那些没有训练过的类别进行分类，使网络具有很好的扩展性。而且对一些小数据量的数据集也适用，变相地增加了整个数据集的大小，使数据量相对较小的数据集也能用深度网络训练出不错的效果。

Siamese 网络奠定了双支路网络的基础，越来越多的工作将双支路网络应用于图像处理领域，接下来分别介绍双支路网络在图像匹配和目标跟踪任务中的应用。

5.3.2 MatchNet

Siamese 协同学习在图像匹配领域应用广泛。图像匹配(image matching)旨在将两幅图像中具有相似属性的内容或结构进行像素上的识别与对齐。一般而言，待匹配的图像通常取自相同或相似的场景或目标，或者具有相同形状或语义信息的其他类型图像对，从而具有一定的可匹配性。

MatchNet 作为深度学习在图像匹配应用的鼻祖，由特征提取网络和度量网络组成，其具体结构和网络参数如图 5.11 所示。

其中特征提取网络由图 5.11(a)的深度卷积网络完成，每个 patch 输入卷积网络，生成一个固定维度的特征。用于特征比对的度量网络由图 5.11(b)的三层全连接层组成。图 5.11(c)为 MatchNet 的训练架构，在训练阶段，首先对图像块进行采样平均，特征网络组成了与 Siamese 网络相似的双支路网络(之间共享参数)，采样后的图像块分别输入双支路特征网络进行特征提取；将双支路网络的输出串联在一起作为度量网络的输入进行相似度学习；最后，对特征和度量网络进行联合训练，利用 SGD 算法优化下面的交叉熵损失函数：

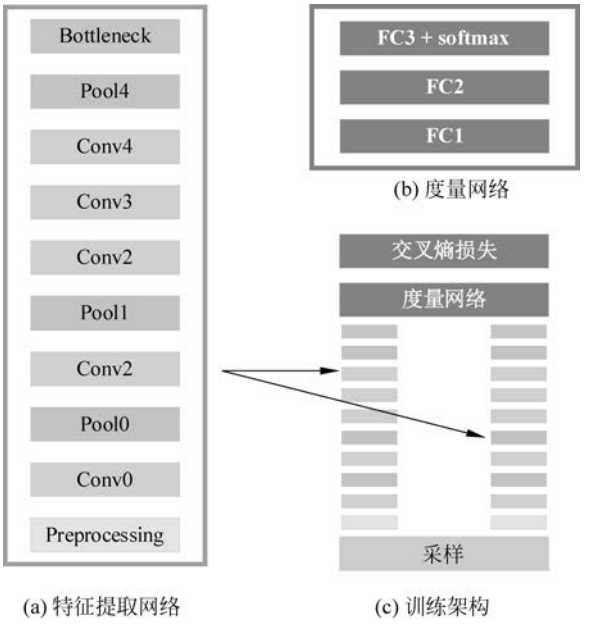

图 5.11　MatchNet 结构

(https://ieeexplore.ieee.org/document/7298948)

$$E=-\frac{1}{n}\sum_{i=1}^{n}[y_i\log(\hat{\boldsymbol{y}}_i)+(1-y_i)\log(1-\hat{\boldsymbol{y}}_i)] \tag{5-7}$$

其中，y_i 表示输入图像 x_i 的标签，$y_i\in\{0,1\}$，1 代表匹配，否则为 0。$\hat{\boldsymbol{y}}_i$ 表示损失函数中预测标签为 1 的概率，其计算公式如下：

$$\hat{\boldsymbol{y}}_i=\frac{e^{v_1(x_i)}}{e^{v_0(x_i)}+e^{v_1(x_i)}} \tag{5-8}$$

其中，$v_0(x_i)$和 $v_1(x_i)$是全连接层 FC3 的两个输出值，这两个值非负且和为 1，表示两个图像块匹配或者不匹配的可能性。

在目标跟踪任务中，视频的第一帧给定模板，算法将后续帧的候选框与模板进行相似度匹配，以确定每帧的目标所在位置。

5.3.3　Siamese FC 网络

将一个全卷积 Siamese 网络嵌入跟踪算法中，通过相似性学习解决搜索区域与目标模板的匹配问题。它采用离线学习的 CNN 克服了深度学习在跟踪任务中时效性差的缺点，开辟了利用 CNN 进行目标跟踪的新篇章。

Siamese FC 网络的框架如图 5.12 所示。其中，$\boldsymbol{z}$ 代表模板图像，算法中使用的是第一帧的真实标签；$\boldsymbol{x}$ 为待跟踪帧中的候选框搜索区域；ϕ 代表特征映射操作，即将原始图像映

射到特征空间(一般采用的是 CNN 的卷积层和池化层)；6×6×128 代表 z 经过 ϕ 得到 128 通道 6×6 大小的特征，同理，22×22×128 是 x 经过 ϕ 得到的特征；* 代表相关操作，具体是将 6×6×128 的模板特征当做卷积核，对 22×22×128 大小的搜索区域特征图进行卷积操作，得到 17×17 的响应图，它表示搜索区域的各个位置与模板相似度值，图上最大值对应的点就是算法认为的目标中心所在位置。需要注意的是，由两个 ϕ 表示的网络结构是一样的，是只包含卷积层和池化层是典型的全卷积神经网络，并且它们之间共享权重。

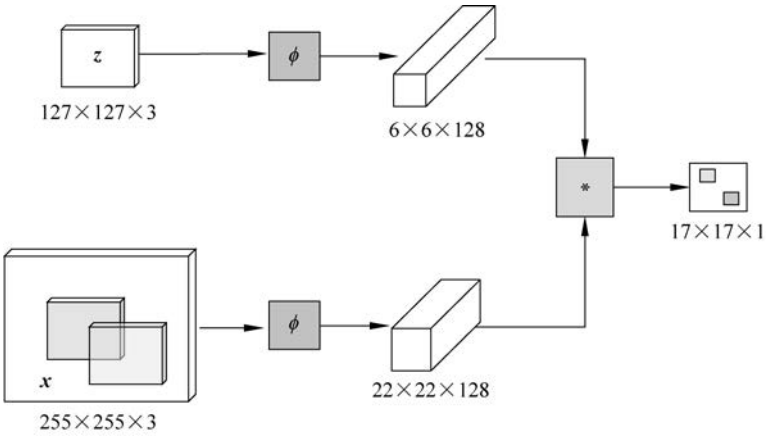

图 5.12 Siamese FC 网络框架

(https://arxiv.org/abs/1606.09549)

为了构造损失函数，算法对搜索区域的位置点进行了正负样本的区分，即目标一定范围内的点作为正样本，这个范围外的点作为负样本。采用 Logistic loss 计算响应图(score map)中的每个点的损失，具体的损失函数为：

$$\ell(y,v)=\log[1+\exp(-yv)] \tag{5-9}$$

其中，v 为响应图中每个点的真实值，$y\in\{+1,-1\}$ 代表这个点所对应的标签，正样本的标签为 1，负样本的标签为 −1。这样，当 v 较大且 $y=1$ 时，认为跟踪正确，损失函数 ℓ 很小，相反，当 v 较大且 $y=-1$ 时，表示跟踪到了错误的位置，此时 ℓ 很大。利用 SGD 算法最小化损失函数，训练得到最优的网络参数。

5.3.4 CFNet

Siamese FC 网络的速度很快，但是全卷积结构缺少特定目标的判别性信息，因此精度不太好。为解决这个问题，在 Siamese FC 的结构上加入了相关滤波器(Correlation Filter，CF)层，得到了 CFNet。相关滤波器判别性比较好，可以求解岭回归(ridge regression)问题；同时利用循环矩阵的性质提高了傅里叶域计算，可以实现在线跟踪。CFNet 首次将相关滤波融入深度神经网络的架构，可以端到端的训练，比 SiamFC 使用的网络更浅但不降低

精度。CFNet 网络结构如图 5.13 所示。

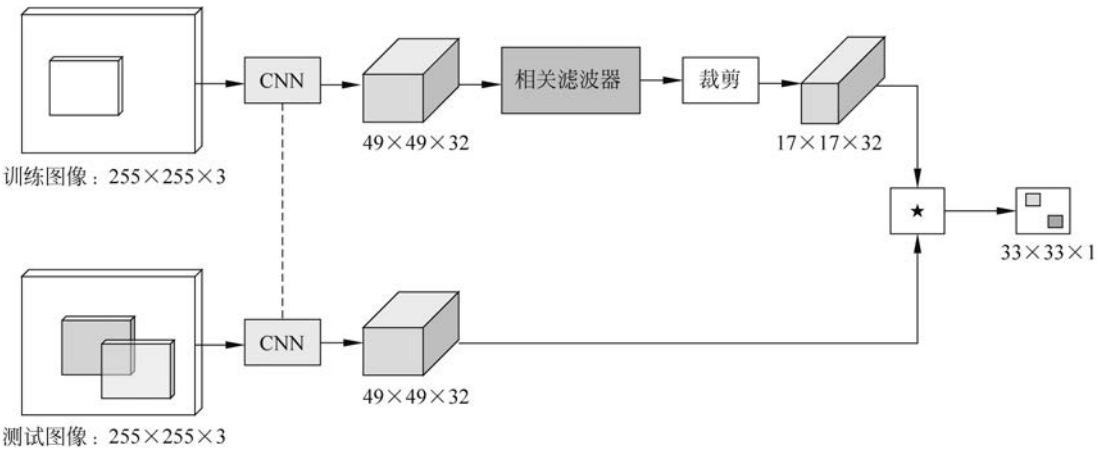

图 5.13　CFNet 网络结构

(https://arxiv.org/abs/1704.06036)

对比 Siamese FC 网络的结构图，CFNet 在 Siamese 卷积网提取的特征后增加了 CF 层，核心就是将相关滤波器可微，把其作为网络的一层，使之可以反向传播，以至于整个网络可以端到端训练。跟踪任务可建模为：

$$\arg\min_{w}\frac{1}{2n}\|\boldsymbol{w}\star\boldsymbol{x}-\boldsymbol{y}\|^2+\frac{\lambda}{2}\|\boldsymbol{w}\|^2 \tag{5-10}$$

其中，$\boldsymbol{w}$ 是相关滤波器；$\boldsymbol{y}$ 是 $\boldsymbol{x}$ 位置的高斯响应；$\star$代表互相关。推导过程将式(5-10)转化为拉格朗日对偶问题，再进行微分，从而使 CF 层可以通过反向传播优化。

5.3.5　Siamese RPN

Siamese RPN 也是在 Siamese FC 的基础上进一步改进，将 Siamese FC 中的全连接层改为区域候选网络(Region Proposal Network，RPN)层，RPN 来自目标检测算法 Faster R-CNN。RPN 的多尺度锚点(anchor)让算法更适应目标的尺寸变化，同时 RPN 的坐标回归可以让跟踪框更加准确。Siamese RPN 网络结构如图 5.14 所示。

Siamese RPN 的双支路网络和 Siamese FC 一样，都是先通过权重共享的 Siamese 全卷积网络对模板和检测帧分别进行特征提取。但 Siamese RPN 将特征输入 RPN 结构。与 Siamese FC 一样，★代表相关操作。

RPN 有 2 个分支：分类和回归。如果设置 k 个锚点 RPN 网络需要为分类分支输出通道数为 $2k$ 的特征图，为回归分支输出通道数为 $4k$ 的特征图。因此在进行相关操作前，算法需要提升通道数。

对分类和回归分支进行相关操作后，损失函数的设置与 Faster R-CNN 一样，为分类损

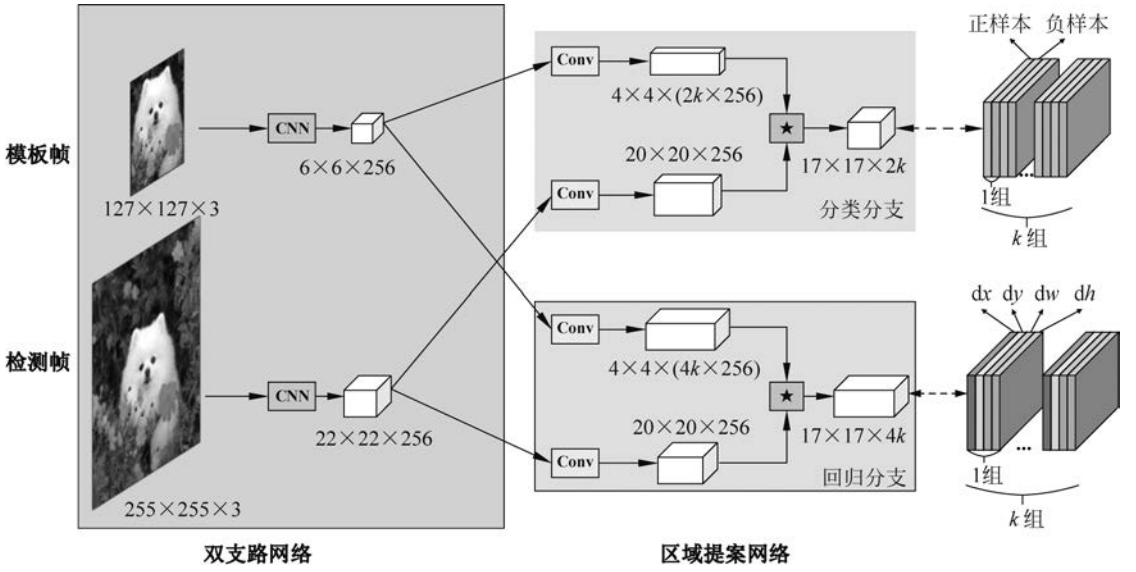

图 5.14 Siamese RPN 网络结构

(https://openaccess.thecvf.com/content_cvpr_2018/papers/Li_High_Performance_Visual_CVPR_2018_paper.pdf)

失和回归损失两部分。分类损失用到的是交叉熵,回归损失则为带归一化的平滑 L_1 损失。

5.3.6 遥感领域中的应用

在遥感领域,许多工作采用了 Siamese 结构进行图像处理任务。例如,Siam-CRNN 网络将 Siamese 卷积网络和 RNN 结合用于多时相 VHR 图像中的变化检测任务。它由三个子网组成:深度 Siamese 卷积神经网络(Deep Siamese Convolutional Neural Networks,DSCNN)、多层 RNN(MRNN)和全连接层。其中 DSCNN 用于从同质或异质 VHR 图像块中提取空间光谱特征。由 LSTM 单元堆叠的 MRNN 负责将 DSCNN 提取的空间光谱特征映射到新的特征空间,并挖掘它们之间的变化信息。此外,Siam-CRNN 的全连接层用于预测变化概率。

Liu 等提出了 Siamese AM-Net 框架,在双支路网络中引入了注意力机制,用于地面摄像机图像和无人驾驶航空器(UAV)三维模型渲染图像的匹配任务,是一种间接建立二维空间和三维空间之间空间关系的方法。它将带有注意力机制的自动编码器嵌入到双支路网络中。

Fang 等提出了基于 GAN 的 Siamese 框架 GSF,用于滑坡清单制图等变化探测任务。GSF 包括两个级联模块:域适应和滑坡检测。域适应模块采用对抗性学习,对滑坡前和滑坡后图像之间进行跨域映射,然后将配对图像转换为同一域,以抑制双时空遥感影像的域差异。滑坡检测模块利用双支路网络进行像素级滑坡检测,此方法不仅能有效区分滑坡与未

变化区域，还能有效区分其他变化区域。

最新的工作将图卷积网络融入双支路框架，对空间和语义进行相似性学习用于遥感影像任务。例如，Tian 等提出了一种新型的连体图嵌入网络，利用空间和语义信息共同提取高层次特征表示对遥感高分辨图像进行物体检测。具体地，首先从空间依赖性和语义对应性方面设计了一种新型的对比损失，用于图相似度量学习；然后通过训练新型的对比损失函数，采用 SGEN 架构进行空间和语义相似度学习；最后这些提取的具有高空间和语义辨识度的特征被用于提高物体检测的性能。

Chaudhuri 等提出了新型连体图卷积网络（SGCN）用于极高分辨率遥感图像检索（CBIR）任务。它从局部区域的角度论证了基于区域邻接图的图像表征对极高分辨率遥感场景的有效性。然而，标准 GCN 特征缺乏对细粒度类的判别性能，这些特征可能不是 CBIR 任务的最佳选择。为克服这个问题，给定 RAG 表示，SGCN 架构的目的是学习一个嵌入空间，将语义上一致的图像拉近，同时将不一致的样本推远，利用对比损失函数进行训练，从而评估一对图形之间的相似性。

5.4　强化学习

5.4.1　强化学习原理

深度强化学习（Deep Reinforcement Learning，DRL）是深度学习与强化学习相结合的产物，它集成了深度学习在视觉等感知问题上强大的理解能力以及强化学习的决策能力，实现了端到端学习。DRL 的出现使强化学习技术真正走向实用，可以解决现实场景中的复杂问题。

在遥感领域，利用 DRL，遥感数据可以设定每个像素都有自己的状态和动作，并且可以基于与环境的交互修改其动作，设计奖励功能，探索数据信息，进行更准确的任务结果。

强化学习是一类特殊的机器学习算法，借鉴于行为主义心理学。与有监督学习和无监督学习的目标不同，算法要解决的问题是智能体（agent）即运行强化学习算法的实体，在环境中怎样执行动作以获得最大的累计奖励。

$<A,S,R,P>$是强化学习中经典的四元组，A 代表的是智能体的所有动作；S 是智能体所能感知的世界的状态；R 是一个实数值，代表奖励或惩罚；P 则是智能体所交互世界，也被称为模型。具体来说，策略是指智能体则是在状态 S 时，所要做出动作的选择。奖励信号定义了智能体学习的目标。价值函数定义的是评判一次交互中的回报好坏。模型是对真实世界的模拟，模型建模的是智能体采样后环境的反应。

5.4.2　面向值函数的深度强化学习

Q-learning 是强化学习的经典算法，但它是一种表格方法，只是根据过去出现的状态统

计和迭代 Q 值。为了使 Q-learning 能够带有预测能力，2013 年 DeepMind 提出了深度 Q 网络(Deep Q-Network，DQN)，DQN 使用 CNN 作为价值函数拟合 Q-learning 中的动作价值，这是第一个直接从原始像素中成功学习控制策略的 DRL 算法。DQN 模型的核心就是 CNN，使用 Q-learning 训练，其输入为原始像素，输出为价值函数。在不改变模型的架构和参数的情况下，DQN 在 7 个 Atari2600 游戏中击败了之前所有的算法，并在其中 3 个游戏中击败了人类最佳水平。2015 年，DeepMind 针对上述 2013 年模型添加目标网络并改进了 DQN 的学习性能。

1. Q-learning

Q-learning 算法的核心是贝尔曼(Bellman)最优化方程，即更新 Q 的函数为：

$$Q_*(s,a)=E[R_{t+1}+\gamma\max_{a'}Q(s_{t+1},a')\mid S_t=s,A_t=a] \tag{5-11}$$

其中，γ 为学习速率。显然，γ 越大，保留之前学习的结果越少。

Q-learning 的过程是不断更新的。首先，给定参数 γ 和奖励矩阵 $\boldsymbol{R}$；将 Q 初始化为 0。随机选择一个初始状态 s。若未达到目标状态，则执行以下几步：在当前状态 s 的所有行为中选取一个行为 a；利用选定的行为 a，得到下一个状态 S'；按照式(5-11)计算 $Q(s,a)$；令 $s:=S'$，直到状态 s 终止。

在 Q-learning 中，需要维护 Q 值表，表的维数为：状态数 $S\times$动作数 A，表中每个数代表在当前状态 s 下可以采用动作 a 可以获得的未来收益的折现和。不断迭代 Q 值表使其最终收敛，根据 Q 值表就可以在每个状态下选取一个最优策略。

2. DQN

在 DQN 出现之前，当用神经网络逼近强化学习中的动作值函数时，会出现不稳定甚至不收敛的问题。为了解决此问题，DQN 使用了两个技术：经验回放机制和目标网络。DQN 训练过程如图 5.15 所示。

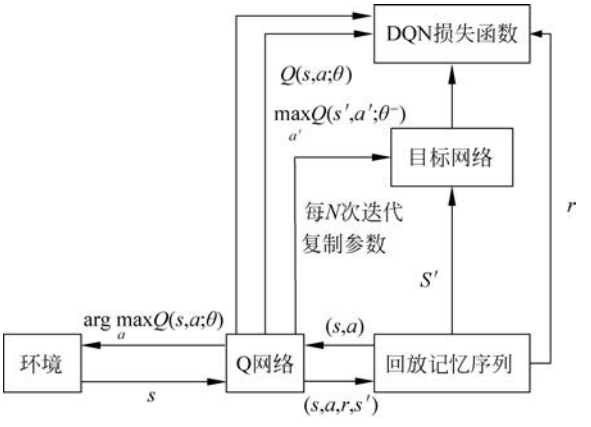

图 5.15 DQN 训练过程

(http://cjc.ict.ac.cn/online/onlinepaper/42-6-15-201968180907.pdf)

DQN 对 Q-Learning 的修改主要有两方面：利用 DCNN 逼近值函数；利用经验回放训练强化学习的学习过程。在训练神经网络时，一般假设训练数据是独立同分布的，但如果采取当前参数的网络获得的样本更新当前的网络参数，那么这些顺序数据之间存在很强的关联性，网络的训练会很不稳定。DQN 利用经验回放的方法，在更新当前时刻参数时会随机用到不同时刻参数下获得的样本，样本之间的关联性相对来说比较小。直接训练 Q-Network 的好处是，只要 Q 值收敛了，则每个状态对应的最大动作也就确定了，也就是确定性的策略已经确定了。

5.4.3　面向策略梯度的深度强化学习

DQN 适用范围还是在低维、离散动作空间。DQN 是求每个离散动作的 $\max\limits_{a} Q(s,a)$，在连续空间就不适用了。于是引入了策略梯度方法解决连续动作空间问题。基于策略梯度的 DRL 分为深度确定性策略梯度(Deep Deterministic Policy Gradient，DDPG)、信赖域策略优化(Trust Region Policy Optimization，TRPO)和异步优势行动者-评价者(Asynchronous Advantage Actor Critic，A3C)等三类方法。

1. 策略梯度和 actor-critic 算法

策略梯度方法中，参数化策略 π 为 π_θ，然后计算得到动作上策略梯度，沿着梯度方法，一点点地调整动作，逐渐得到最优策略。

随机性 actor-critic 算法中，策略网络由行动者(actor)网络和输出动作网络组成。价值网络是评价者(critic)，可以评价行动者网络所选动作的好坏，并生成 TD_error 信号并指导行动者网络评价者网络的更新。图 5.16 为 actor-critic 算法架构图。

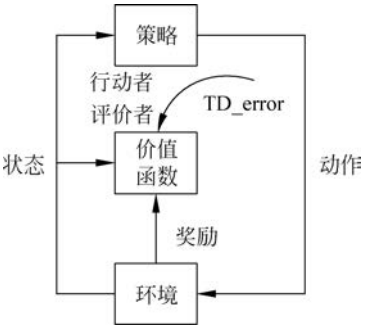

图 5.16　actor-critic 算法架构图
(http://cjc.ict.ac.cn/online/onlinepaper/42-6-15-201968180907.pdf)

2. DDPG

DDPG 结合了 DQN 和 DPG，把 DRL 推向了连续动作空间控制。DDPG 借鉴 DQN 技术，采用经验回放机制和单独的目标网络，减少数据之间的相关性，增加算法的稳定性和鲁棒性。虽然 DDPG 借鉴了 DQN 的思想，但要直接将 Q-learning 应用到连续动作空间是不可能的，因此 DDPG 采用的是基于 DPG 算法的 actor-critic 方法。DDPG 采用的经验回放机制和 DQN 完全相同，但目标网络的更新方式和 DQN 相比略有差异。DDPG 中的行动者网络和评价者网络的两个目标网络以小步长滞后更新，而非隔 C 步更新。

DQN 的目标网络是隔 N 步和 Q 网络同步一次，DDPG 中行动者和评价者各自的目标网络参数 θ^- 和 ω^- 则是通过变化较慢的方式更新，而不是直接复制参数，以此进一步增加

学习过程的稳定性：

$$\theta^{-}=\tau\theta+(1-\tau)\theta^{-} \tag{5-12}$$

$$\omega^{-}=\tau\omega+(1-\tau)\omega^{-} \tag{5-13}$$

但都是为了解决模型训练稳定性问题。同时，在连续动作空间中学习的主要挑战是有效地实现冒险探索，考虑到 DDPG 是离策略算法。DDPG 中通过在动作基础上增加噪声(noise)的方式解决这个问题：

$$\mu'(s_t)=\mu(s\mid\theta)+\mathcal{N} \tag{5-14}$$

和 DQN 相比，DDPG 的网络结构除值网络之外还多了一个策略网络。同时 DQN 输入仅是视频帧而不需要额外输入动作，每个离散动作都有一个单独的输出单元，其价值网络的输出是每个动作所对应的 Q 值。而 DDPG 的值网络则是输入视频帧后再通过 CNN 得到特征，再输入动作 a，最后输出 Q 值。

5.4.4 遥感领域中的应用

在强化学习通过 agent 进行一系列观察，其中动作和相应的奖励与环境交互，完成任务。在遥感领域，强化学习通过与环境的互动，通过最大化累积特征奖励决定顺序动作。

尤其是当只有很少的标记像素可用时，强化学习还可以无须使用任何标记的训练数据集，可以获得比较高的精度。这很适合数据量较少的遥感任务，如在 SPRL 中，利用基于强化学习方法用于极化 SAR 数据分类。将像素按照强化学习设置状态和动作，通过与环境的交互来修改其动作。从本地邻域设计空间极化奖励功能，以探索空间和极化信息，进行更准确的分类。这样就可以得到自演化和无模型的分类器，它具有简单的原理，对数据中存在的斑点噪声具有鲁棒性。通过与环境的互动，当只有很少的标记像素可用时，SPRL 网络可以获得很高的分类精度。

同样地，对于少样本的遥感数据，Schulman John 提出了一种用于 PolSAR 图像分类的改进的 DQN 方法，该方法可以通过使用 ε-贪心策略与 agent 进行交互生成大量有效数据。在网络中，多层特征图像和分类动作分别表示为环境状态和 agent 动作。模型预测结果以一些标准给出了奖励。使用带有注释的样本集来反馈 agent 所做的操作。如果 agent 预测与标记值一致，则将奖励标记为 1；否则，将奖励标记为 −1。在 DQN 算法中，网络使用学习值 Q 更新具有随机梯度的权重，并使用经验重播机制缓解相关数据和非平稳分布的问题。

除了对数据进行扩充和加强，为了解决遥感影像背景复杂以及船舶密集的泊车场景检测任务困难问题。Mnih Volodymyr 提出了一种基于特征融合金字塔网络的深度强化学习(FFPN-RL)的船舶旋转检测模型，将深度强化学习应用于倾斜的船舶检测任务。通过操作集的三个操作：行动 1、行动 2 和行动 3 完成角度预测。通过在动作集中使用不同的旋转角度，可以实现更高的预测精度并减少决策动作的数量。奖励功能通过选定的动作来鼓励或

惩罚角度预测代理。agent 积累了以上奖励的经验，从中学习并最终在每个决定中选择适当的行动。使得该检测网络可以有效地生成用于船舶的倾斜矩形箱。

深度强化学习可以根据环境需要，设计动作、状态和奖励机制，使得模型结果趋于期望结果。并且，强化学习在小样本量和环境复杂的情况下，会有比较优秀的性能，这使得强化学习在遥感领域十分具有前景。

5.5　迁移学习

深度学习在各个领域取得了优异的成绩，深度迁移学习应运而生。利用深度神经网络进行有效的知识迁移成了研究热点，即深度迁移学习。在介绍深度迁移学习之前，首先介绍传统的迁移学习(Transfer Learning，TL)。

5.5.1　迁移学习原理

在机器学习中，迁移学习已成为研究热点之一。机器学习中表现优异的监督学习，往往需要大量的标注数据。然而，在实际进行标注数据时需要花费大量的人力、物力与财力。而迁移学习可以很好地解决这一问题，人们可以在使用部分标注数据的前提下，对监督学习的机器学习方法进行训练，减少了对大量标注数据的依赖。当前迁移学习发展的主要趋势是使用大量的标记分类数据对基准网络进行预训练，然后使用少量带注释的检测数据微调网络进行检测。迁移学习是一种重要的机器学习方法，它主要将解决一个问题时获得的知识应用于另一个不同但存在一定联系的问题中去。传统的机器学习在训练不同任务且不同域的模型时，需要分别使用标记数据对模型 A 和模型 B 分别训练，以达到期望的效果，其学习模式如图 5.17 所示。

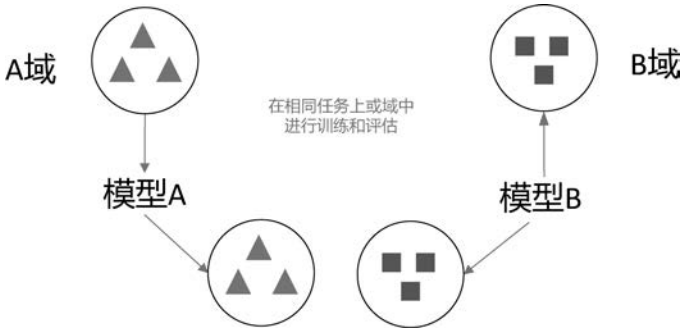

图 5.17　传统的机器学习模式

(https://my.oschina.net/u/876354/blog/1614883)

在实际应用中，由于模型继承了训练数据的偏差，不能直接进行新数据集测试，常常会

出现性能下降或崩溃的情况。因为任务(甚至标签)不同,导致能直接利用现有模型。然而,迁移学习可以利用一些相关任务或域的已有标记数据处理这些场景,如图 5.18 所示。

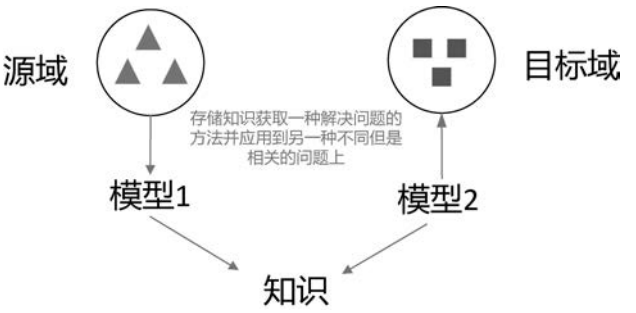

图 5.18 迁移学习模式

(https://my.oschina.net/u/876354/blog/1614883)

使用迁移学习的益处有以下 3 点。

(1) 微调前,源模型的初始性能比不使用迁移学习到的模型更高。

(2) 在训练的过程中,源模型学习效果提升的速率比不使用迁移学习更快。

(3) 训练得到的模型的收敛性能比不使用迁移学习更好。

在使用迁移学习时,需要注意新数据集的大小以及与原始数据集的相似性。迁移学习中应遵循以下常见经验规则。

(1) 新数据集较小,与原始数据集相似。数据集过小会造成过拟合问题,此时微调网络是存在问题的。同时,由于数据与原始数据相似,希望 ConvNet 中的高级特性也与此数据集相关。因此,最好的办法是在 CNN 上训练一个线性分类器。

(2) 新数据集很大,与原始数据集相似。当数据集较大时,可以对整个网络进行微调,不会存在过拟合问题。

(3) 新数据集很小,但与原始数据集差异较大。由于数据集很小,最好只训练一个线性分类器。数据集差异较大,网络的顶部训练分类器可能不是最好的,因为网络的顶部包含了更多特定于数据集的特性。

(4) 新数据集很大,与原始数据集差异较大。由于数据集较大,从头开始训练 ConvNet 的代价较大。然而,在实践中使用预先训练的模型中的权重初始化仍然非常有益。可以通过微调达到较好的模型性能。

在进行迁移学习时,预训练模型的约束以及设置适当的学习率是比较重要的。若使用预先训练的网络,可能会在新数据集可以使用的体系结构方面受限制。与计算新数据集的新线性分类器的(随机初始化)权重相比,通常对正在微调的卷积网络权重使用较小的学习速率。利用源域数据可以训练得到一个效果良好的分类器。但是,因源域和目标域数据之间存在细微差异,源域模型无法很好地对目标域数据进行分类。常用的一种方法就是将目

标域和源域数据的特征分布对齐，利用源域数据训练得到的模型就可以对目标域数据进行分类。

在迁移学习中，当源域和目标域的数据分布不同但两个任务相同时，这种特殊的迁移学习叫作域适应(domain adaptation)。域适应目前是迁移学习的一大研究热点，它的任务是学习一个能将源域和目标域映射到一个共同特征空间的映射，同时再学习一个对共同特征空间的映射，使得复合映射可以拟合只在源域学到的映射，并且非常靠近只在目标域学到的映射。图 5.19 便是迁移学习中常用到的域适应模型。

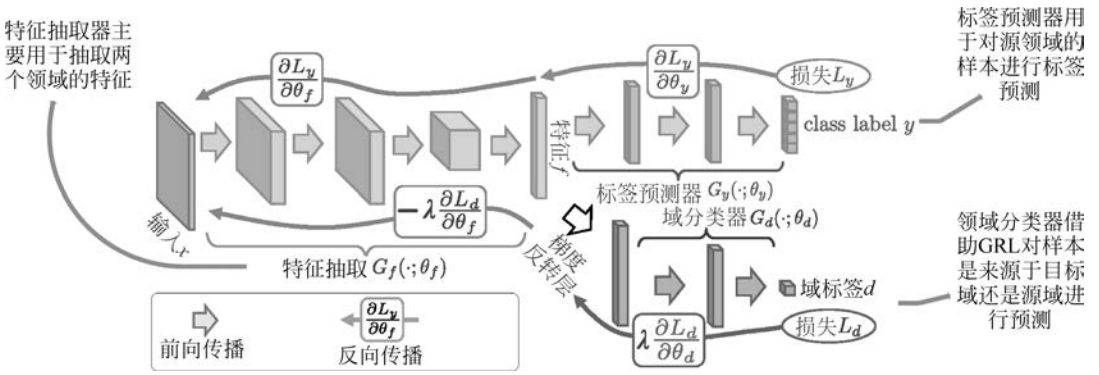

图 5.19　域适应模型

(https://arxiv.org/abs/1505.07818)

5.5.2　迁移学习分类

随着深度神经网络在各个领域的广泛应用，大量的深度迁移学习方法被提出。基于深度迁移学习的技术，本节主要将介绍 4 类深度迁移学习：基于实例的深度迁移学习、基于映射的深度迁移学习、基于网络的深度迁移学习和基于对抗的深度迁移学习。

1. 基于实例的深度迁移学习

基于实例的深度迁移学习是指采用一种特定的权重调整策略，从源域中选择部分实例作为目标域训练集的补充，并为这些选择的实例分配适当的权重。它主要是基于“两个域之间存在差异，但源域中的部分实例可以被具有适当权重的目标域利用”的假设。在训练数据集中，排除源域与目标域含义不一致的实例。同时，在具有适当权重的训练数据集中，包含了与目标域含义相似的源域实例。

TrAdaBoost 使用基于插件的技术过滤出与源域中的目标域不同的情况。在源域中重新加权实例，组成类似于目标域的分布。最后，通过使用来自源域和来自目标域的重新加权实例训练模型。该算法在保证算法性能的前提下，减小了不同分布域的加权训练误差。TaskTrAdaBoost 是一种快速算法，可以促进对新目标的快速再训练。TrAdaBoost 主要是

为分类问题而设计的，而 R2（ExpBoost. R2 和 TrAdaBoost. R2）是为解决回归问题而提出的。双权域自适应算法（BIW）则可以将两个域的特征空间对齐到公共坐标系中，然后为源域的实例分配适当的权重。

2. 基于映射的深度迁移学习

基于映射的深度迁移学习是指将实例从源域和目标域映射到新的数据空间。在这个新的数据空间中，来自两个域的实例是相似的，适合于联合深度神经网络。它基于“两个源域之间即使存在差异，但它们在一个复杂的新数据空间中可能更相似”的假设。基于实例的深度迁移学习提出，来自源域和目标域的实例映射到一个新的数据空间，其中将新数据空间中的所有实例视为神经网络的训练集。

迁移成分分析（Transfer Component Analysis，TCA）在传统迁移学习的许多应用中得到了广泛的应用。将 TCA 方法推广到深度神经网络是一种自然的思路。将最大平均偏差（Maximum Mean Deviation，MMD）扩展到比较深度神经网络中的分布，通过引入适应层和额外的域混淆损失来学习语义上有意义和域不变的表示。该工作中使用了多核 MMD 距离代替 MMD 距离。将 CNN 中与学习任务相关的隐藏层映射到重构核希尔伯特空间（Reproducing Kernel Hilbert Space，RKHS）中，利用多核优化方法最小化不同域之间的距离。联合最大平均偏差（Joint Maximum Mean Deviation，JMMD）度量联合分布的关系。利用 JMMD 方法对 DNN 的传输学习能力进行推广，以适应不同领域的数据分布，并对已有的工作进行改进。还可以应用 Wasserstein 距离作为一种新的域距离度量方法寻找更好的映射。

3. 基于网络的深度迁移学习

基于网络的深度迁移学习是指将源领域中预先训练好的部分网络，包括其网络结构和连接参数，重新利用，将其转换为用于目标领域的深度神经网络的一部分。基于“神经网络类似于人脑的处理机制，是一个迭代的、连续的抽象过程”的假设，该网络的前端层可以看作一个特征提取器，所提取的特征是通用的。在学习过程中，首先利用大规模训练数据集对网络进行源域训练。其次，将对源域进行预处理的部分网络迁移到为目标域设计的新网络中。最后，可以对所传输的子网络进行微调策略的更新。

将网络分为两部分，第一部分是语言无关的特征变换，第二部分是语言相关分类器。语言无关的特征变换可以在多种语言之间进行转换。在 ImageNet 数据集上重用 CNN 训练的前层来计算其他数据集中图像的中间图像表示，CNN 被训练来学习图像表示，这些图像表示可以在有限的训练数据下有效地迁移到其他视觉识别任务中。

联合学习源域标记数据和目标域未标记数据的自适应分类器和可迁移特征，通过将多个层次插入到深度网络中，参照目标分类器显式学习残差函数。学习域自适应和深度哈希特性是在 DNN 中同时存在的一种新的多尺度卷积稀疏编码方法。该方法能在不同尺度下自动学习滤波器组，并与学习模式的强制尺度特异性相结合，为学习可迁移的基础知识并针

对目标任务进行微调提供了一种无监督的解决方案。在无监督聚类方法中，DNN 可以作为优秀的特征提取器。它在不使用任何标记实例的情况下，根据形态学特征识别新类。

另一个非常值得注意的是网络结构和可迁移性之间的关系。结果表明，某些模块可能不会影响域内的精度，但会影响可移植性。Yosinski 等明确了深层网络中哪些特征是可迁移的，哪些类型的网络更适合迁移。同时，他们得出结论：LeNet、AlexNet、VGG、Inception、ResNet 是基于网络的深度迁移学习的较好选择。

4. 基于对抗的深度迁移学习

基于对抗性的深度迁移学习是指在 GAN 的启发下，引入对抗性技术，寻找既适用于源域又适用于目标域的可迁移表达。它基于假设：为了有效地迁移，良好的表征应该是对主要学习任务的区别性，以及对源域和目标域的不加区分。

近两年，研究者将对抗思想引入了迁移学习，提出了域对抗神经网络(DANN)。DANN 将“域适应”嵌入特征表示的学习过程中。同时，在 DANN 优化特征映射参数时采取最小化标签分类器的损失函数 L_y，最大化域分类器的损失函数 L_d。这样使得最终训练得到的模型可以提取出具有区分力的特征，同时可以提取出对域变换具有不变性的特征。在源域为大规模数据集的训练过程中，将网络的前端层作为特征提取器。它从两个域中提取特征并将其送到对抗层，然后在对抗层区别特征的来源。如果对抗网络的性能较差，则意味着这两类特征之间的差异较小，可迁移性较好，反之亦然。在接下来的训练过程中，将考虑对抗性层的性能，迫使迁移网络发现更具有可迁移性的一般特征。

5.5.3　遥感领域中的应用

迁移学习的目的是通过迁移在不同但相关的源域中的知识来提高目标学习者在目标域上的学习表现。这样可以减少对大量目标域数据的依赖，构建目标学习者。由于其广泛的应用前景，迁移学习已经成为机器学习中一个热门和有发展前景的领域。在实际应用中，因为不需要大量完备的标注数据，所以迁移学习使得深度学习的落地应用变得简单。吴恩达在 NIPS 2016 教程也提出迁移学习将成为下一个机器学习商业成功的驱动者。

目前，将迁移学习与遥感数据结合的相关研究也较多。发展中国家缺乏可靠的数据是可持续发展、粮食安全和救灾的主要障碍。遥感数据是高度非结构化的，目前还没有技术能够自动提取有用的信息，同时遥感训练数据非常稀少，使得很难应用 CNN 等现代技术。Xie Michael 等提出使用迁移学习方法丰富夜间光强度数据，并训练一个完全卷积的 CNN 模型预测白天图像中的夜间灯光，同时学习对贫困预测有用的特征。Chen Zhong 等主要利用迁移学习解决遥感影像中的飞机检测问题，采用单一的 DCNN 和有限的训练样本实现端到端的可训练飞机检测，在一定程度上提高了遥感数据中飞机检测的精度。Begüm Demir 提出了一种基于变化检测驱动的迁移学习方法，通过对同一区域不同时间(即图像时间序列)的遥感影像进行分类来更新土地覆盖图。该方法旨在利用源域的已有知识，为目标域定

义一个可靠的训练集，这是通过对目标域和源域应用无监督的变化检测方法，并将检测到的未更改训练样本的类标签从源域迁移到目标域来初始化目标域训练集来实现的。Yuan Yuan 等提出了一种利用自然图像知识提高高光谱图像分辨率的新框架。该框架利用 DCNN 学习低分辨率和高分辨率图像之间的映射，并借鉴迁移学习的思想将其转化为高光谱图像。有限标记的 SAR 目标数据成为训练深层 CNN 的障碍，为了解决这个问题，有学者提出了一种基于传递学习的方法，从足够多的未标记 SAR 场景图像中学习到的知识可以传递给标记的 SAR 目标数据。实验结果表明，在标记训练数据较少的情况下，迁移学习能获得较好的学习效果。

针对遥感数据，首先从拍摄上来讲并不容易获得，因拍摄设备限制以及存在各种干扰，因此数据源质量和数量都无法得到较好的保证。其次，针对遥感数据标注，因为遥感数据不同于普通的自然场景，所以在标注时需要良好的专业知识以及丰富的标注经验，所以大量遥感数据标注存在较多的困难。如果仅使用少量标注数据，就能够借助监督学习进行训练学习，可以给遥感数据研究工作带来一定的便利。

从以上研究工作中可以看出，迁移学习能够有效缓解遥感数据稀缺问题，并减少标记工作量。对于自然场景的深度学习模型，研究者通过域适应将自然数据特征与遥感数据特征对齐，然后进行遥感数据任务。

5.6 联邦学习

2016 年，谷歌提出了联邦学习(Federated Learning，FL)，这是一种新的机器学习技术，主要在多个分散的边缘设备或服务器上进行训练算法。联邦学习在一定程度上保证了数据隐私以及数据传输安全。而隐私与安全对一些需要高度保密的行业具有十分重要的作用，如国防、医药、互联网等，因此联邦学习的研究源源不断。

5.6.1 联邦学习原理

传统的做法是将所有数据上传至一台服务器上并进行训练学习，而联邦学习是在多个设备或服务器上保存数据样本，并且它们之间并不进行数据交换操作。用通俗的话来说，我们可以使用联邦学习调用多个参与者的数据进行训练学习，但是并不共享这些数据。这在一定程度上保证了数据隐私以及限制数据访问权限等问题。在物理层面上，联邦学习系统一般由数据持有方和中心服务器组成。具体的客户端-服务器架构的联邦学习框架如图 5.20 所示。具体的学习流程如下。

(1) 系统初始化。首先由中心服务器发送建模任务，寻求参与客户端。客户端数据持有方根据自身需求，提出联合建模设想。在与其他合作数据持有方达成协议后，联合建模设想被确立，各数据持有方进入联合建模过程。由中心服务器向各数据持有方发布初始参数。

（2）局部计算。联合建模任务开启并初始化系统参数后，各数据持有方将被要求首先在本地根据己方数据进行局部计算，计算完成后，将本地局部计算所得梯度脱敏后进行上传，以用于全局模型的一次更新。

（3）中心聚合。在收到来自多个数据持有方的计算结果后，中心服务器对这些计算值进行聚合操作，在聚合的过程中需要同时考虑效率、安全、隐私等多方面问题。

（4）模型更新。中心服务器根据聚合后的结果对全局模型进行一次更新，并将更新后的模型返回给参与建模的数据持有方。数据持有方更新本地模型，并开启下一次局部计算，同时评估更新后的模型性能，当性能足够好时，训练终止，联合建模结束。建立好的全局模型将会被保留在中心服务器端，以进行后续的预测或分类工作。

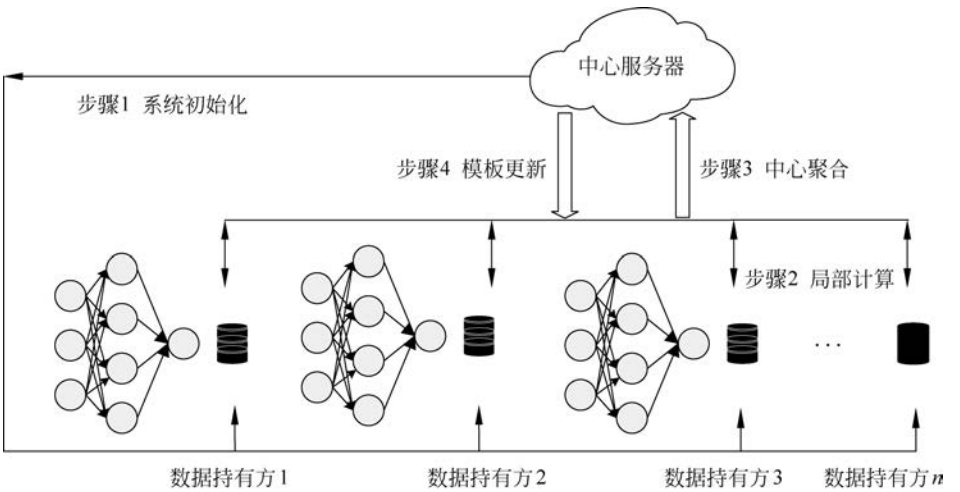

图 5.20　客户端-服务器架构的联邦学习框架

（http://www.infocomm-journal.com/bdr/article/2020/2096-0271/2096-0271-6-6-00064.shtml）

联邦学习的学习过程主要有：服务器向客户端发送公钥→客户端间交换中间的训练结果→加密汇总后的梯度与损失数据→更新模型。联邦迁移学习是指在两个数据集的用户与用户特征重叠都较少的情况下，不对数据进行切分，而是利用迁移学习克服数据或标签不足的情况。如何能够在不交换数据的前提下进行迁移学习，这是联邦迁移学习解决的问题。其学习过程分为 4 个步骤：双方交换公钥→双方分别计算加密和交换中间训练结果→双方计算加密后的梯度，加上混淆码发给对方→双方解密梯度并交换，反混淆并更新本地的模型。它有效地解决了数据隐私问题，同时能够充分利用现有算力，所以得到了广泛的应用。

5.6.2　联邦学习分类

联邦学习的孤岛数据有不同的分布特征。对于每一个参与方来说，自己所拥有的数据可以用一个矩阵来表示。现有的联邦学习主要可以根据数据集分布情况与根据场景进行分类。

首先，联邦学习可以按照训练数据在不同参与方之间的数据特征空间和样本 ID 空间的分布情况进行划分为 3 类：横向联邦学习、纵向联邦学习与联邦迁移学习。以上 3 类学习按照特征维度与用户维度的划分如图 5.21 所示。

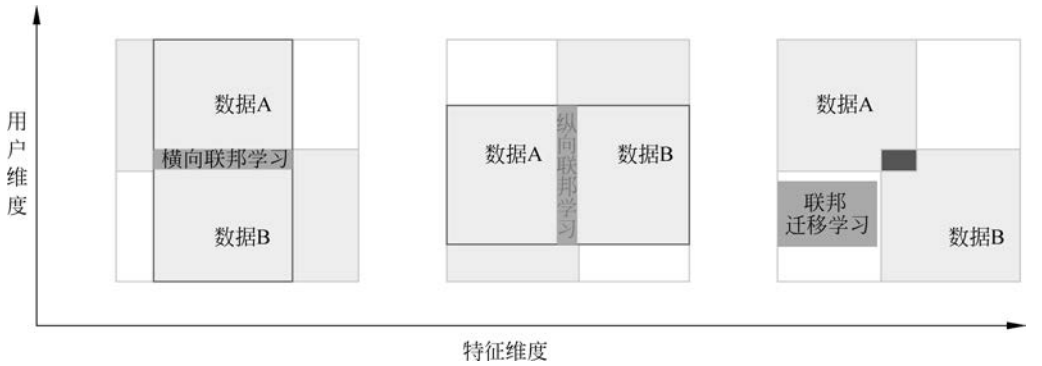

图 5.21 横向联邦学习、纵向联邦学习与联邦迁移学习

(https://www.cnblogs.com/wt869054461/p/12375011.html)

横向联邦学习(Horizontal Federated Learning，HFL)是指在两个数据集的用户特征重叠较多而用户重叠较少的情况下，把数据集按照横向(即特征维度)切分，并取出双方特征相同而用户不完全相同的那部分数据进行训练。简而言之，横向联邦学习是指将训练数据进行横向划分，也就是数据矩阵或者表格的按行(横向)划分。不同行的数据有相同的数据特征，即数据特征是对齐的。

纵向联邦学习(Vertical Federated Learning，VFL)是指在两个数据集的用户重叠较多而用户特征重叠较少的情况下，按照用户维度对数据集进行切分，并取出双方用户相同而用户特征不完全相同的那部分数据进行训练。简而言之，纵向联邦学习是指将训练数据“纵向划分”，也就是数据矩阵或者表格的按列(纵向)划分。不同列的数据有相同的样本 ID，即训练样本是对齐的。

联邦迁移学习(Federated Transfer Learning，FTL)适用于参与方的数据样本和数据特征重叠都很少的情况。目前大部分的研究是基于横向联邦学习和纵向联邦学习的，联邦迁移学习领域的研究相对较少。

除了上述按照数据集分布进行分类，联邦学习还可以按照场景进行分类，主要分为跨设备(cross-device)和跨孤岛(cross-silo)。其中，跨设备类型着重于整合大量移动端和边缘设备应用程序，例如，Google 的 Gboard 移动键盘，Apple 在 iOS 13 中使用跨设备用于 QuickType 键盘和“Hey Siri”的人声分类器等。跨孤岛类型可能只涉及少量相对可靠的客户端应用程序(如多个组织合作训练一个模型)，常见的跨孤岛实例包括再保险的财务风险预测、药物发现、电子健康记录挖掘、医疗数据细分和智能制造等。两种类型间的差异如表 5.1 所示。

表 5.1　“跨设备”和“跨孤岛”两者差异对比

比　较　项	跨　设　备	跨　孤　岛
实例	手机端应用	医疗机构
节点数量	$1\sim10^{10}$	1～100
节点状态	大部分节点不在线	节点几乎稳定运行
主要瓶颈	Wi-Fi 速度，设备不在线	计算瓶颈和通信瓶颈
按数据类型分类	横向	横向/纵向

5.6.3　联邦学习与神经网络学习之间的差异

针对目前的深度神经网络来说，可以通过局部训练数据样本，然后将局部模型以一定的频率交换参数，最终生成全局模型。虽然已有的分布式学习也是在多台服务器上训练同一个模型，但其与联邦学习存在的差异在于：①分布式学习主张获得并行计算力；联邦学习主张在异构数据上进行训练；②在分布式学习中假设的本地数据集分布相同，大小基本相同；在联邦学习中的数据集通常是异构的，其大小差异较大。

深度学习训练主要依赖于 SGD 的变量，其中梯度是在整个数据集的随机子集上计算的，然后用于梯度下降。在使用联邦学习方法进行深度学习训练时，服务器根据每个节点上的训练样本数按比例平均梯度，并用于进行梯度下降操作。

联邦学习在一定程度上给深度学习的训练带来了便利，但是其存在一定的技术限制与挑战。在联邦学习中，虽然不需要进行数据通信，但多台服务器之间需要进行频繁的通信来交换学习模型的参数。这对于本地计算力和内存都有着一定的要求，高宽带连接是必要的。联邦方法进行机器学习的主要优点是确保数据隐私或数据保密。在本地不进行数据存储，而且所有的数据会被切割，这样使入侵获得所有数据存在一定的困难。联邦学习只交换机器学习参数，它适用于在多任务学习框架中同时生成两个模型。

5.6.4　联邦学习与分布式学习之间的差异

联邦学习并不只是使用分布式的方式解决优化问题。联邦学习和分布式学习均是在多个计算节点上进行模型运算，其主要区别如表 5.2 所示。

表 5.2　联邦学习与分布式学习差异

比较项	联邦学习	分布式学习
数据分布	分散存储且固定，数据无法互通、可能存在数据的非独立同分布(Non-IID)	集中存储不固定，可以任意打乱并平衡地分配给所有客户端
节点数量	1～1010	1～100
节点状态	节点可能不在线	所有节点稳定运行

联邦学习是面向隐私保护的机器学习框架，原始数据分散保存在各个设备上并进行训

练，节点间数量较多且质量严重不均，服务器聚合各个本地计算的模型更新。分布式学习利用多个计算节点进行机器学习或者深度学习的算法和系统，旨在提高性能，并可扩展至更大规模的训练数据和更大的模型。各节点间数据共享，任务由服务器统一分配，各节点比较均衡。数据集中式分布式学习与跨孤岛/跨设备联邦学习的综合对比如表 5.3 所示。

表 5.3 数据集中式分布式学习与跨孤岛/跨设备联邦学习的综合对比

	数据集中式的分布式学习	跨孤岛的联邦学习	跨设备的联邦学习
设置	在大型但“扁平”的数据集上训练模型。客户端是单个群集或数据中心中的计算节点	在数据孤岛上训练模型。客户是不同的组织（如医疗或金融）或地理分布的数据中心	客户端是大量的移动或物联网设备
数据分布	数据被集中存储，可以在客户端之间进行混洗和平衡。任何客户端都可以读取数据集的任何部分	数据在本地生成，并保持分散化。每个客户端都存储自己的数据，无法读取其他客户端的数据。数据不是独立或相同分布的	数据在本地生成，并保持分散化。每个客户端都存储自己的数据，无法读取其他客户端的数据。数据不是独立或相同分布的
编排方式	中央式编排	中央编排服务器/服务负责组织培训，但从未看到原始数据	中央编排服务器/服务负责组织培训，但从未看到原始数据
广域通信	无（在一个数据中心/群集中完全连接客户端）	中心辐射型拓扑，中心代表协调服务提供商（通常不包含数据），分支连接到客户端	中心辐射型拓扑，中心代表协调服务提供商（通常不包含数据），分支连接到客户端
数据可用性	所有客户端都是可用的	所有客户端都可用	在任何时候，只有部分客户可用，通常会有日间或其他变化
数据分布范围	通常 1～1000 个客户端	通常 2～1000 个客户端	大规模并行，最多 10^{10} 个客户端
主要瓶颈	假设在网络非常快的情况下，计算通常是数据中心的瓶颈	可能是计算和通信量	通信是主要的瓶颈，尽管这取决于任务。通常跨设备联邦学习使用 Wi-Fi 或更慢的连接
可解决性	每个客户端都有一个标识或名称，该标识或名称允许系统专门访问它	每个客户端都有一个标识或名称，该标识或名称允许系统专门访问它	无法直接为客户建立索引（即不对用户进行标记）
客户状态	有状态的——每个客户都可以参与到计算的每一轮中，不断地传递状态	有状态的——每个客户都可以参与到计算的每一轮中，不断地传递状态	高度不可靠，预计有 5%或更多客户端参与一轮计算会失败或退出（例如，由于违反了电池、网络或闲置的要求而导致设备无法使用）

续表

	数据集中式的分布式学习	跨孤岛的联邦学习	跨设备的联邦学习
客户可靠性	相对较少的失败次数	相对较少的失败次数	无状态的——每个客户在一个任务中可能只参与一次，因此通常假定在每轮计算中都有一个从未见过的客户的新样本
数据分区轴	数据可以在客户端之间任意分区/重新分区	固定分区。能够根据样本分区（横向）或者特征分区（纵向）	根据样本固定分区（横向）

5.6.5　遥感领域中的应用

联邦学习应用领域广泛。Google 的研究人员致力于在 Gboard 应用程序上从用户生成的数据增强语言建模。其他人发现联邦学习非常适合医疗保健领域，可以通过在医院保留患者数据来平衡患者隐私和机器学习。物联网设备也在联邦学习上获得了关注。此外，联邦学习也进入了许多其他领域，如边缘计算、网络、机器人、网格、联邦学习增强、推荐系统、网络安全、在线零售商、无线通信和电动汽车等。本节主要介绍了遥感领域中联邦学习的应用。

针对深度学习中数据源稀缺或者有限这一挑战，联邦学习就可以很好地解决这一问题。遥感数据因获取难度高，获取到的数据质量无法保证而稀缺，以及较多数据涉及国防安全等，因此存在一定的数据壁垒问题。联邦学习在遥感数据学习过程中，可以对一些保密数据加以利用和扩展。在不接触保密的原数据源的条件下，依旧可以学习到自己的参数，在后续的实际应用使用。当然，联邦学习可以实现某种意义上的数据共享，成为打破数据壁垒的突破口。

参考文献

[1] Wang F, Tax D M J. Survey on the attention based RNN model and its applications in computer vision [EB/OL]. https://arxiv.org/abs/1601.06823v.

[2] Jaderberg M, Simonyan K, Zisserman A, et al. Spatial transformer networks[EB/OL]. https://arxiv.org/abs/1506.02025.

[3] Hu J, Shen L, Sun G. Squeeze-and-excitation networks [C]//IEEE Conference on Computer Vision and Pattern Recognition, 2018.

[4] Li X, Wang W, Hu X, et al. Selective kernel networks[C]//IEEE Conference on Computer Vision and Pattern Recognition, 2019.

[5] Itti L, Koch C. Computational modelling of visual attention[J]. Nature Reviews Neuroscience, 2001, 2(3): 194-203.

[6] Lin T Y,Dollár P,Girshick R,et al. Feature pyramid networks for object detection[C]//IEEE Conference on Computer Vision and Pattern Recognition,2017.

[7] Liu W,Anguelov D,Erhan D,et al. Ssd: Single shot multibox detector[C]//European Conference on Computer Vision,2016.

[8] Liu S,Qi L,Qin H,et al. Path aggregation network for instance segmentation[C]//IEEE Conference on Computer Vision and Pattern Recognition,2018.

[9] Qin Z,Li Z,Zhang Z,et al. Thundernet: towards real-time generic object detection on mobile devices [C]//IEEE/CVF International Conference on Computer Vision,2019.

[10] Pang J,Chen K,Shi J,et al. Libra r-cnn: towards balanced learning for object detection[C]//IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019.

[11] Seferbekov S,Iglovikov V,Buslaev A,et al. Feature pyramid network for multi-class land segmentation[C]//IEEE Conference on Computer Vision and Pattern Recognition,2018.

[12] Chopra S,Hadsell R,LeCun Y. Learning a similarity metric discriminatively,with application to face verification[C]//IEEE Conference on Computer Vision and Pattern Recognition, 2005.

[13] Norouzi M,Fleet D,Salakhutdinov R,et al. Hamming distance metric learning[J]. Advances in Neural Information Processing Systems,2012,2: 1061-1069.

[14] Chen H,Wu C,Du B,et al. Change detection in multisource VHR images via deep Siamese convolutional multiple-layers recurrent neural network[J]. IEEE Transactions on Geoscience and Remote Sensing,2019,58(4): 2848-2864.

[15] Liu W,Wang C,Bian X,et al. Learning to match ground camera image and uav 3-d model-rendered image based on siamese network with attention mechanism[J]. IEEE Geoscience and Remote Sensing Letters,2019,17(9): 1608-1612.

[16] Fang B,Chen G,Pan L,et al. GAN-based siamese framework for landslide inventory mapping using Bi-temporal optical remote sensing images[J]. IEEE Geoscience and Remote Sensing Letters,2020.

[17] Tian S,Kang L,Xing X,et al. Siamese graph embedding network for object detection in remote sensing images[J]. IEEE Geoscience and Remote Sensing Letters,2020.

[18] Chaudhuri U,Banerjee B,Bhattacharya A. Siamese graph convolutional network for content based remote sensing image retrieval[J]. Computer Vision and Image Understanding,2019,184: 22-30.

[19] Wang M,Wang Z,Yang C,et al. Polarimetric SAR data classification via reinforcement learning[J]. IEEE Access,2019,7: 137629-137637.

[20] Huang K,Nie W,Luo N. Fully polarized SAR imagery classification based on deep reinforcement learning method using multiple polarimetric features[J]. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing,2019,12(10): 3719-3730.

[21] Fu K,Li Y,Sun H,et al. A ship rotation detection model in remote sensing images based on feature fusion pyramid network and deep reinforcement learning[J]. Remote Sensing,2018,10(12): 1922.

[22] Mnih V,Kavukcuoglu K,Silver D,et al. Human-level control through deep reinforcement learning [J]. Nature,2015,518(7540): 529-533.

[23] Lillicrap T P,Hunt J J,Pritzel A,et al. Continuous control with deep reinforcement learning[EB/OL]. https://arxiv.org/abs/1509.02971.

[24] Schulman J,Levine S,Abbeel P,et al. Trust region policy optimization[C]//International Conference on Machine Learning,2015.

[25] Mnih V,Badia A P,Mirza M,et al. Asynchronous methods for deep reinforcement learning[C]//

International Conference on MachineLearning,2016.

[26] 刘建伟,高峰,罗雄麟.基于值函数和策略梯度的深度强化学习综述[J].计算机学报,2019,42(6):1406-1438.

[27] Xie M,Jean N,Burke M,et al. Transfer learning from deep features for remote sensing and poverty mapping[C]//Proceedings of the AAAI Conference on Artificial Intelligence,2016.

[28] Chen Z,Zhang T,Ouyang C. End-to-end airplane detection using transfer learning in remote sensing images[J]. Remote Sensing,2018,10(1): 139.

[29] Demir B,Bovolo F,Bruzzone L. Updating land-cover maps by classification of image time series: A novel change-detection-driven transfer learning approach[J]. IEEE Transactions on Geoscience and Remote Sensing,2012,51(1): 300-312.

[30] Demir B,Bovolo F,Bruzzone L. Updating land-cover maps by classification of image time series: A novel change-detection-driven transfer learning approach[J]. IEEE Transactions on Geoscience and Remote Sensing,2012,51(1): 300-312.

[31] Huang Z,Pan Z,Lei B. Transfer learning with deep convolutional neural network for SAR target classification with limited labeled data[J]. Remote Sensing,2017,9(9): 907.

[32] Persello C,Bruzzone L. Kernel-based domain-invariant feature selection in hyperspectral images for transfer learning[J]. IEEE Transactions on Geoscience and Remote Sensing, 2015, 54(5): 2615-2626.

[33] Li T,Sahu A K,Talwalkar A,et al. Federated learning: Challenges, methods, and future directions [J]. IEEE Signal Processing Magazine,2020,37(3): 50-60.

[34] Konečný J,McMahan B,Ramage D. Federated optimization: Distributed optimization beyond the datacenter[J]. arXiv preprint arXiv: 1511.03575,2015.

[35] Pan S J,Yang Q. A survey on transfer learning[J]. IEEE Transactions on Knowledge and Data Engineering,2009,22(10): 1345-1359.

[36] heu 御林军.深度迁移学习综述[EB/OL]. https://zhuanlan.zhihu.com/p/89951541.

[37] cheerful090.联邦学习分类及前景应用[EB/OL]. https://blog.csdn.net/cheerful090/article/details/113180606.