

面向通信信号调制识别的半监督生成对抗网络框架*

周华吉^{1,2}, 徐杰¹, 郑仕链¹, 沈伟国¹, 王巍¹, 楼财义¹

(1. 电磁空间安全全国重点实验室, 浙江嘉兴 314033; 2. 西安电子科技大学人工智能学院, 陕西西安 710071)

摘要:针对只有少量标签数据的弱监督条件下现有调制信号识别模型准确率较低的问题,提出基于生成对抗网络的半监督学习框架。该方法通过对通信信号进行冗余空域变换,使其在适应生成对抗网络模型的同时保留丰富的信号相邻特征;通过梯度惩罚 Wasserstein 生成对抗网络的引入,构建适宜电磁信号处理的半监督学习框架,实现对无标签信号样本的有效利用。为了验证所提算法的有效性,在 RADIOML 2016.04C 数据集上进行测试。实验结果表明,该方法在半监督条件下能训练出高效的分类器,获得优异的调制识别结果。

关键词:生成对抗网络;半监督学习框架;通信信号;调制识别

中图分类号:TN92 文献标志码:A 文章编号:1001-2486(2023)06-078-06

Semi-supervised generative adversarial network framework for modulation recognition of communication signals

ZHOU Huaji^{1,2}, XU Jie¹, ZHENG Shilian¹, SHEN Weiguo¹, WANG Wei¹, LOU Caiyi¹

(1. National Key Laboratory of Electromagnetic Space Security, Jiaxing 314033, China;

2. School of Artificial Intelligence, Xidian University, Xi'an 710071, China)

Abstract: Aiming at the problem that the accuracy of the existing modulation signal recognition model was low under the condition of weak supervision with only a small amount of labeled data, a semi supervised learning framework based on generated countermeasure network was proposed. By performing a redundant spatial transformation on the communication signals, the method can adapt to the generative adversarial network model and retain rich signal adjacent features. Through the introduction of Wasserstein generative adversarial network-gradient penalty, a semi-supervised learning framework suitable for electromagnetic signal processing was constructed to realize the effective utilization of unlabeled signal samples. In order to verify the effectiveness of the proposed algorithm, sufficient experiments were conducted on the RADIOML 2016.04C dataset. Experimental results show that the proposed method can train an efficient classifier under semi-supervised conditions and obtain excellent modulation recognition results.

Keywords: generative adversarial network; semi-supervised learning framework; communication signal; modulation recognition

通俗来说,通信信号调制识别,就是挖掘通信信号特征,以最大可能区分信号的调制类型。其在认知无线电^[1-4]、频谱监测^[5-6]、网络安全^[7-8]等领域都有广泛的应用。通信信号调制识别主要采用模式识别方法。支持向量机对于调制识别有较好的效果,但是,核函数的选择直接影响着最终的识别结果,且算法不具有自适应能力^[9]。人工神经网络自适应能力较强,但是在信噪比较低条件下,调制识别效果不好,同时因为需要对信号的特征进行训练,计算复杂度较高^[10]。近年来,深度学习技术迅猛发展,卷积神经网络(convolutional neural network, CNN)是将人工神经网络和深度学习技术相结合而产生的深度神经

网络,因其强大的特征提取能力,且具备稀疏连接、权重共享等特性,有较好的调制识别效果^[11-15]。然而,利用卷积神经网络进行调制识别的一个特点是需要大量带标签数据进行全监督学习。而在实际作战场景下,很多重要信号转瞬即逝,要大量获取十分困难;再则,由于电磁环境日益复杂,各种信号互相干扰,要给信号数据打上正确的标签更是难上加难,这就意味着当前几乎最优的卷积神经网络面对只有少量标签数据的弱监督条件下的调制信号识别问题,显得有些束手无策。而如何解决弱监督条件下的调制信号识别问题,也成为当前研究的一个热点和难点。

生成对抗网络^[16-17] (generative adversarial

* 收稿日期:2021-11-26

基金项目:国家自然科学基金资助项目(61772401, U19B2015, U19B2016, 61871398)

作者简介:周华吉(1988—),男,浙江金华人,高级工程师,硕士, E-mail:472376253@qq.com

network, GAN)自2014年由Goodfellow提出以来,向人们展示了从无到有的神奇能力,并且已经在工业界有着广泛的应用。生成对抗网络是一种基于博弈论的学习模型,它包含两个主要成分:生成器和判别器,生成器通过接收噪声产生尽可能真实的伪数据,判别器则去分辨输入的是真实数据还是生成器产生的伪数据。双方在训练中相互博弈,训练的终点是达到纳什均衡,产生以假乱真的信号样本。虽然生成对抗网络具有强大的特征映射及逼真样本生成能力,而且在图像领域,如图像生成、分类、风格迁移等方面已经有了极广泛的应用,但由于电磁信号和图像之间存在天然的差异,因此其在调制信号识别领域的应用还极少。Tu等^[18]设计了一种半监督生成对抗网络,并将调制信号以星座图的形式输入到网络中,获得了较好的调制识别效果。但是他们并没有真正实现调制信号的端到端识别,本质上还是对图像进行处理;同时半监督生成对抗网络中使用的是原始GAN,网络训练稳定性较差。

在本文中,首先提出了一种将调制信号数据进行冗余空域变换的方法,之后利用冗余空域变换之后的数据训练出一个基于梯度惩罚 Wasserstein 生成对抗网络^[19](Wasserstein generative adversarial network-gradient penalty,

WGAN-GP)的无监督训练模型,利用其稳定的训练能力对生成器和判别器进行预训练。在获得预训练参数的基础上,设计并训练出一种二维信号半监督生成对抗网络(semi-supervised generative adversarial network for 2-dimensional signal, SSGAN-2D)模型,能将少量有标签数据和大量无标签数据都很好地利用起来。

1 信号冗余空域变换

生成对抗网络近年来取得了多方向的突破,例如从损失函数上改进使其训练更加平稳可控,从训练方式上改进使其可以从低分辨率的图像平滑过渡到高分辨率图像,从功能上拓展使其可以进行图像分类任务。这些改进方法大多集中于图像处理领域,电磁信号作为一种区别于图像的数据,如果直接套用上述的方法、模型或框架,很难取得一个令人满意的结果。因此,为了使电磁信号数据可以更有效地对应生成对抗模型,同时保持丰富的信号相邻特征,提出了一种信号冗余空域变换的方法。

假设一段电磁信号序列为 $A(n) = \{x_1, x_2, x_3, \dots, x_n\}$, 本文对信号序列做出如图1所示的空域变换。即,将长度为 n 的一维电磁信号转换成 $k \cdot k$ 的二维信号,其中 $k = \lfloor n/2 \rfloor$ 。

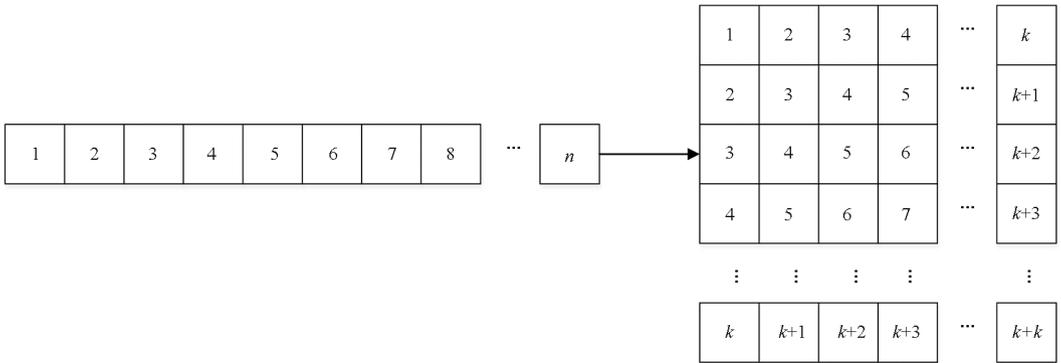


图1 信号冗余空域变换

Fig. 1 Signal redundancy spatial transformation

而传统的电磁信号空域变换,如图2所示。即,将长度为 n 的一维电磁信号转换成 $k \cdot k$ 的二维信号,其中 $k = \lfloor \sqrt{n} \rfloor$ 。

可以清晰地看出,当对冗余空域变换之后的信号进行卷积操作时,能充分提取信号相邻特征。而如果对通信信号序列直接进行粗暴地二维转换,则会损失很多相邻特征。

2 基于 WGAN-GP 的半监督分类模型

本文中,设计了一个基于 WGAN-GP 的无监

督预训练模型,利用其稳定的训练能力对生成器和判别器参数进行预训练。之后在 WGAN-GP 的基础上,构建了一个 SSGAN-2D 模型,不仅保留了 WGAN-GP 利用无类别标签数据学习提取特征的能力,又使其获得信号分类能力。

2.1 WGAN-GP 结构

WGAN-GP 是一个无监督模型,和原始 GAN 相比, WGAN-GP 主要在损失函数上进行了改进,使得训练更加稳定有效。原始 GAN 中生成器和判别器的对抗关系为:

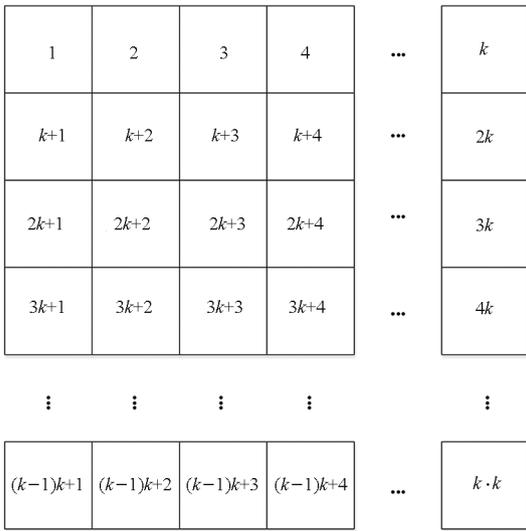


图 2 传统信号空域变换

Fig. 2 Traditional signal spatial transformation

$$\min_G \max_D V(G, D) = E_{x \sim p_{\text{data}}(x)} [\lg D(x)] + E_{z \sim p_z(z)} (\lg \{1 - D[G(z)]\}) \quad (1)$$

式中, p_{data} 是真实数据分布, p_z 是噪声数据分布。 $D(x)$ 表示判别器 D 判断真实数据是否真实的概率, 而 $D[G(z)]$ 则是 D 判断生成器 G 生成的数据是否真实的概率。

因此判别器的损失函数为:

$$J_D = -E_{x \sim p_{\text{data}}(x)} [\lg D(x)] - E_{z \sim p_z(z)} (\lg \{1 - D[G(z)]\}) \quad (2)$$

实际应用中生成器的损失函数常为:

$$J_G = -E_{z \sim p_z(z)} (\lg \{1 - D[G(z)]\}) \quad (3)$$

标准生成式对抗网络定义的损失函数会导致如下两个主要问题: ①训练 GAN 需要达到纳什均衡, 有时候可以用梯度下降法做到, 但有时候做不到。所以训练 GAN 相比变分自编码器 (variational auto-encoder, VAE) 或者像素递归神经网络 (pixel recurrent neural networks, PixelRNN) 是不稳定的^[20]; ②生成器和判别器的 loss 无法指示训练进程, 而且生成式对抗网络存在模式崩溃 (model collapse) 的问题, 具体表现为训练阶段的梯度消失使得生成的样本非常差, 即使长时间训练也无法得到很好的改善。

针对上述问题, Wasserstein 生成对抗网络^[20]首先提出原始 GAN 用来衡量两个分布距离和差异的延森 - 香农 (Jensen-Shannon, JS) 散度所存在的问题。当两个分布不存在重叠时, JS 散度不能为生成器提供连续有效的梯度而导致模型失效。因此采用 Wasserstein 距离去衡量生成数据分

布和真实数据分布之间的距离, 以解决训练不稳定的问题。此时损失函数变为:

$$\min_G \max_{D \in L} V(G, D) = E_{x \sim p_{\text{data}}(x)} [D(x)] - E_{z \sim p_z(z)} \{D[G(z)]\} \quad (4)$$

其中, L 是 1-Lipschitz 函数。则判别器损失函数改写为:

$$J_D = -E_{x \sim p_{\text{data}}(x)} [D(x)] + E_{z \sim p_z(z)} \{D[G(z)]\} \quad (5)$$

生成器的损失函数改为:

$$J_G = -E_{z \sim p_z(z)} \{D[G(z)]\} \lambda \quad (6)$$

WGAN 极大地优化了 GAN 中出现的问题, 但是为了使用 Wasserstein 距离, WGAN 需要对判别器权重 W_D 进行裁剪, 使它在一定的范围 $(-c, c)$ 内。其对权重进行裁剪的做法过于粗暴, 这一操作间接限制了其梯度信息发生, 并且对训练的稳定性造成伤害。针对这一问题, WGAN-GP 提出用梯度惩罚机制代替权重裁剪, 将判别器的损失函数更改为:

$$J_D = E_{z \sim p_z(z)} \{D[G(z)]\} - E_{x \sim p_{\text{data}}(x)} [D(x)] + \lambda E_{\hat{x} \sim p_{\hat{x}}(\hat{x})} \{[\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1]^2\} \quad (7)$$

式中, $p_{\hat{x}}$ 为生成样本和真实样本之间采样点的概率分布。

WGAN-GP 进一步稳定了 GAN 的训练过程, 而且保证了结果质量, 因此本文采用 WGAN-GP 的损失函数设计预训练网络。

WGAN-GP 的结构如图 3 所示。其中 fc 是全连接层, 将 200 维的噪音输入映射为 256 维。

本文采用所有的无标签样本用来训练 WGAN-GP 网络, 得到训练好的生成器和判别器参数模型。

2.2 半监督调制信号识别模型

WGAN-GP 网络具有良好的训练稳定性, 但它是无监督模型, 其判别器部分是一个二分类器, 只判断输入数据的真假, 并不能直接用于多种信号的调制识别。为此需要对网络结构进行改进, 使其既保留 WGAN-GP 利用无类别标签数据学习提取特征的能力, 又能获得信号分类能力。

在 WGAN-GP 的基础上, 本文设计了一种半监督模型架构, 即 SSGAN-2D, 如图 4 所示。SSGAN-2D 的分类器将接收三种数据, 分别是由 WGAN-GP 中生成器接收噪音生成的伪数据、有类别标签的真实数据和无类别标签的真实数据。

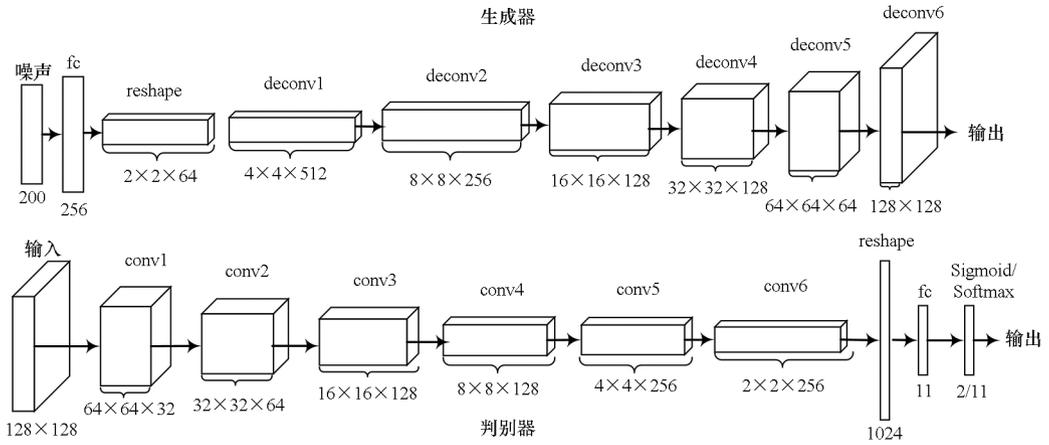


图 3 WGAN-GP 网络结构
Fig. 3 WGAN-GP network structure

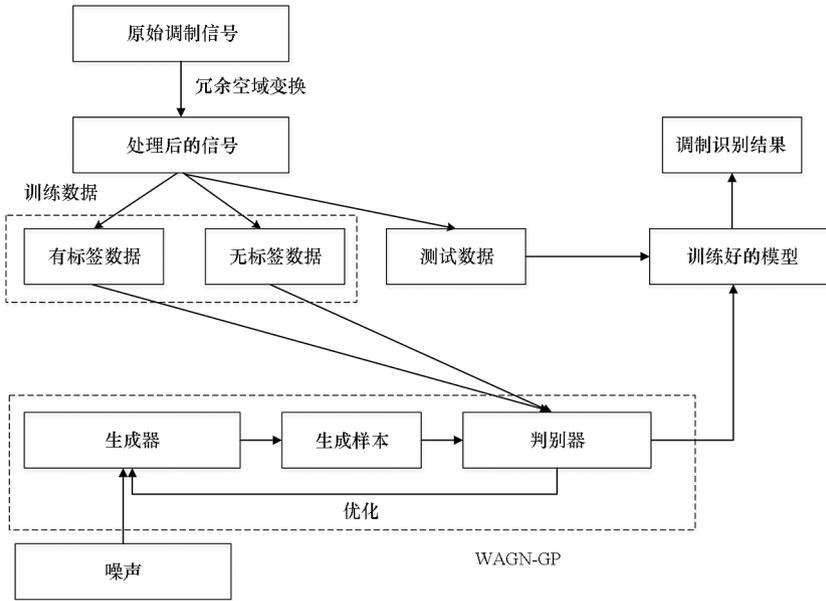


图 4 半监督调制信号识别模型: SSGAN-2D
Fig. 4 Semi-supervised modulation signal recognition model: SSGAN-2D

假设数据共 k 类,将输入判别器数据的真伪看成第 $k + 1$ 类,是为 1,不是则为 0。这样,将 Generator 生成的伪数据的标签设置为 $unlabel_f = \{0,0,0,\dots,1\}$ (前 k 项为 0, $k + 1$ 项为 1),无标记的真实数据的标签设置为 $unlabel_r = \{1,1,1,\dots,0\}$,有标记的真实数据的标签为 $label_r = \{y_1, y_2, y_3, \dots, 0\}$ (前 k 项表示真实的类别标签)。这样,所有数据的标签都变成 $k + 1$ 维。在 Softmax 分类器判别时,由生成器产生的伪数据 $unlabel_f = \{0,0,0,\dots,1\}$ 和无标记真实数据 $unlabel_r = \{1,1,1,\dots,0\}$ 仍是一个二分类问题(标签前 k 维看作一部分,第 $k + 1$ 维看作一部分,就是简单的 0, 1 二分类标签),从而得以实现原始 GAN 无监督提取特征的能力。而对有标记的真实数据来说,其标签第 $k + 1$ 维添加的 0 并不影响其分类。这样则统

一了无监督模式和监督模式的分类器输出。

SSGAN-2D 中,生成器损失函数和 WGAN-GP 是一样的,即:

$$L_G = -E_{z \sim p_z(z)} (\lg \{D[G(z)]\}) \quad (8)$$

而 SSGAN-2D 中的判别器的损失函数既包括有监督损失又包括无监督损失。在接收有标记样本时,优化有监督损失 $L_{supervised}$,在接收无标记真实样本时,优化无监督损失 $L_{unsupervised}$,总损失函数 $L_D = L_{supervised} \cdot (1 - flag) \cdot 10 + L_{unsupervised}$, $flag$ 是一个表征输入数据是有类别标注(取 0)或无类别标注(取 1)的标志符。取 0 时, $L_D = L_{supervised} \times 10 + L_{unsupervised}$,其中 $L_{supervised}$ 乘以 10 后远大于 $L_{unsupervised}$,从而主要优化的就是无监督损失部分;取 1 时, $L_D = L_{unsupervised}$,优化无监督损失部分。这两部分的具体函数分别为:

$$L_{\text{supervised}} = -E_{x,y \sim p_{\text{data}}(x,y)} \lg[p_x(y = i | x, y < k + 1)] \quad (9)$$

$$L_{\text{unsupervised}} = -\{E_{x \sim p_{\text{data}}(x)} \lg[1 - p_x(y = k + 1 | x)] + E_{x \sim G} \lg[p_x(y = k + 1 | x)]\} \quad (10)$$

其中, $p_x(y = i | x, y < k + 1)$ 为真实数据被判为第 i 类的概率, $E_{x \sim p_{\text{data}}(x)} \lg[1 - p_x(y = k + 1 | x)]$ 为真实数据判为真的期望, $E_{x \sim G} \lg[p_x(y = k + 1 | x)]$ 为生成的虚假样本判为假的期望。

3 实验和分析

为了验证提出的基于 SSGAN-2D 模型的调制信号识别方法, 在公开数据集 RADIOML 2016.04C. 上进行实验验证, 并和卷积神经网络方法进行比较。该数据集包含 11 类调制样式: 8PSK, AM-DSB, AM-SSB, BPSK, CPFSK, GFSK, PAM4, QAM16, QAM64, QPSK, WBFM。信噪比范围为 $[-20, 18]$ dB, 间隔为 2 dB, 信号为双通道

2×128 维度, 每种信噪比包含 8 103 个样本。

3.1 实验 1: 不同带标签样本个数对半监督识别结果的影响

针对不同带标签样本个数的数据集分别进行算法验证:

选择信噪比为 12 dB 的信号进行试验, 随机选择 50% 的数据作为训练样本, 另外 50% 的数据作为测试样本。为了挑战所提算法的能力, 本文从训练样本中随机挑选数量从 110 ~ 1 100 (11 类信号, 每类信号数目相同) 的多组数据作为有标签数据, 剩余数据作为无标签数据, 来开展试验。

利用有标签数据进行识别模型训练的卷积神经网络方法作为对比。为了保证对比效果的客观性, 卷积神经网络结构和 SSGAN-2D 中的判别器基本一致, 不同的是, 输出为 11 类。具体识别准确率实验结果如表 1 所示。

表 1 不同带标签样本数量条件下的识别准确率实验结果

Tab. 1 Experimental results of recognition accuracy under different numbers of labeled sample

方法	样本数量									
	110	220	330	440	550	660	770	880	990	1 100
SSGAN-2D 方法	0.834	0.866	0.892	0.907	0.918	0.928	0.929	0.930	0.933	0.936
CNN 方法	0.721	0.818	0.859	0.885	0.895	0.920	0.922	0.926	0.927	0.930

实验结果表明: 在不同带标签样本个数条件下, 本文所提的 SSGAN-2D 方法能很好地利用无标签数据, 辅助特征提取, 从而获得比 CNN 方法更好的识别效果。进一步地, 当带标签数据较少时, SSGAN-2D 方法的优势较大, 而随着带标签数据的增多, SSGAN-2D 方法的优势会逐渐减少, 这个现象是可以理解的。当带标签数据较少时, CNN 不能很好地训练, 无法得到较好的信号特征, 而半监督模型可以利用大量无标签数据辅助完成信号特征的提取; 当带标签相对较多时, CNN 方法本身就能提取较好的、用于准确识别的信号特征, 半监督模型能利用无标签数据的优势反而不明显。

3.2 实验 2: 不同信噪比对半监督识别结果的影响

针对不同信噪比的数据集分别进行算法验证:

选取了 0 dB, 8 dB, 10 dB, 12 dB, 14 dB, 16 dB, 18 dB 共 7 种信噪比的信号数据分别进行实验。每种信噪比的信号数据中随机选择 50% 的数据作为训练样本, 另外 50% 的数据作为测试样本, 半监督算法的主要兴趣是针对小样本数据进行处理, 所以本文把有标签数据样本的数量设定为 440 (每类样本数量均为 40), 剩余数据作为无标签数据, 开展实验。

具体识别准确率实验结果如表 2 所示。从表 2

表 2 不同信噪比条件下的识别准确率实验结果

Tab. 2 Experimental results of recognition accuracy under different SNRs

方法	信噪比						
	0 dB	8 dB	10 dB	12 dB	14 dB	16 dB	18 dB
SSGAN-2D 方法	0.838	0.872	0.885	0.907	0.895	0.898	0.904
CNN 方法	0.756	0.824	0.863	0.885	0.874	0.880	0.882

中可以看出,在有标签样本数量极端少,每类只有40个时,SSGAN-2D方法同样表现出了强大的性能。在信噪比为12 dB时,SSGAN-2D方法达到最高的识别准确度为90.7%,在不同信噪比条件下,SSGAN-2D方法和CNN方法相比,都有明显的优势。

在实验过程中发现,当有标签样本数量较少时,信号识别率和样本选择强相关,如果选择的样本较好地反映了样本集分布,则识别率较高,反之,识别率较低。而这也是符合常理的。所以,为了反映算法效果的客观性,上述两个实验中,针对同一标签数量,均随机选择样本进行10次识别实验,并取识别率均值,作为最终识别结果。

4 结论

GAN因为其强大的逼真样本生成能力已被成功应用到众多领域,本文将其在调制信号识别问题上。对通信信号进行了一种冗余空域变换,使其在适应生成对抗网络模型的同时保留丰富的信号相邻特征;设计了一种基于生成对抗网络且适宜电磁信号处理的半监督学习框架,实现了弱监督条件下调制信号的端到端调制识别。结果表明,所提方法在有标签数据较少的情况下,能很好地利用无标签数据辅助特征提取,获得比当前几乎最优的卷积神经网络方法更好的识别效果。

后期,还将对SSGAN-2D中生成器及判别器结构设计、计算复杂度降低、训练稳定性增强、损失函数优化等方面进行进一步探索,以期获得更好的表现。

参考文献(References)

- [1] 刘明骞,李兵兵,曹超凤,等. 认知无线电中非高斯噪声下数字调制信号识别方法[J]. 通信学报, 2014, 35(1): 82-88.
- [2] 胡宗恺,熊刚. 一种改进的认知无线电调制识别方法研究[J]. 通信技术, 2018, 51(5): 1036-1040.
- [3] WANG Y, LIU M, YANG J, et al. Data-driven deep learning for automatic modulation recognition in cognitive radios[J]. IEEE Transactions on Vehicular Technology, 2019, 68(4): 4074-4077.
- [4] ZHENG S L, CHEN S C, QI P H, et al. Spectrum sensing based on deep learning classification for cognitive radios[J]. China Communications, 2020, 17(2): 138-148.
- [5] WEST N E, O'SHEA T. Deep architectures for modulation recognition [C]//Proceedings of IEEE International Symposium on Dynamic Spectrum Access Networks, 2017.
- [6] 高迎帅. 一种基于特征提取的调制识别方法[J]. 无线电通信技术, 2015, 41(2): 89-91.
- [7] 葛娟,李一兵,林云. 一种新的混合信号调制识别方法[J]. 火箭与制导学报, 2011, 31(6): 183-186.
- [8] 曾勇虎,陈翔,林云,等. 射频指纹识别的研究现状及趋势[J]. 电波科学学报, 2020, 35(3): 305-315.
- [9] WU Z L, WANG X X, GAO Z Z, et al. Automatic digital modulation recognition based on support vector machines [C]//Proceedings of International Conference on Neural Networks and Brain, 2005.
- [10] NANDI A K, AZZOUEZ E E. Modulation recognition using artificial neural networks [J]. Signal Processing, 1997, 56(2): 165-175.
- [11] CHEN S C, ZHENG S L, YANG L F, et al. Deep learning for large-scale real-world ACARS and ADS-B radio signal classification[J]. IEEE Access, 2019, 7: 89256-89264.
- [12] WU Z L, ZHAO Y L, YIN Z D, et al. Jamming signals classification using convolutional neural network [C]//Proceedings of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2017.
- [13] DONG Y H, JIANG X H, ZHOU H J, et al. SR2CNN: zero-shot learning for signal recognition[J]. IEEE Transactions on Signal Processing, 2021, 69: 2316-2329.
- [14] ZHENG S L, YE L H, WANG X Y, et al. Primary user adversarial attacks on deep learning-based spectrum sensing and the defense method[J]. China Communications, 2021, 18(12): 94-107.
- [15] ZHOU H J, JIAO L C, ZHENG S L, et al. Weight-variable scattering convolution networks and its application in electromagnetic signal classification[J]. IEEE Access, 2019, 7: 175889-175896.
- [16] GOODFELLOW I J, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial nets [C]//Proceedings of the 27th International Conference on Neural Information Processing Systems, 2014.
- [17] ZHOU H J, JIAO L C, ZHENG S L, et al. Generative adversarial network-based electromagnetic signal classification: a semi-supervised learning framework [J]. China Communications, 2020, 17(10): 157-169.
- [18] TU Y, LIN Y, WANG J, et al. Semi-supervised learning with generative adversarial networks on digital signal modulation classification [J]. Computers, Materials & Continua, 2018, 55(2): 243-254.
- [19] GULRAJANI I, AHMED F, ARJOVSKY M, et al. Improved training of Wasserstein GANs [C]//Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017.
- [20] ARJOVSKY M, CHINTALA S, BOTTOU L. Wasserstein GAN[EB/OL]. (2017-12-06) [2021-11-01]. <https://arxiv.org/abs/1701.07875>.