Modeling and Simulation 建模与仿真, 2024, 13(3), 2911-2921
Published Online May 2024 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2024.133264

Hans汉斯

对抗攻击下的高光谱图像分类

董　祥，钱海强

上海理工大学光电信息与计算机工程学院，上海

收稿日期：2024年4月24日；录用日期：2024年5月21日；发布日期：2024年5月29日

摘　要

近些年来深度学习在高光谱图像(HSI)分类领域取得了重大的进展，但是在面对对抗干扰时，神经网络所表现的脆弱性不容忽视。生成的对抗样本与干净样本相比，人眼几乎无法察觉，但是大多先进的深度学习模型可能会受对抗样本的愚弄，从而分类预测时误判。为了针对这一问题，本文提出了一种分层特征引导上下文网络(HFGCNet)。本文发现，通过利用高阶特征指导低阶特征学习的方法学习可以增强多尺度特征融合的有效性，能更好地提取出HSI所包含的全局上下文信息，为上下文网络的损失分摊模块提供一个更好的输入，显著地提高了神经网络面对对抗干扰时的鲁棒性。在两个公开HSI数据集上进行对比实验，结果表明与其他先进的深度学习模型相比，本文所提出的方法更具抵抗力。

关键词

高光谱图像，对抗攻击，深度学习，对抗样本

Hyperspectral Image Classification under Adversarial Attack

Xiang Dong, Haiqiang Qian

School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai

Received: Apr. 24th, 2024; accepted: May 21st, 2024; published: May 29th, 2024

Abstract

Deep learning has made significant progress in the field of hyperspectral image (HSI) classification in recent years, but the vulnerability exhibited by neural networks in the face of adversarial interference cannot be ignored. The generated adversarial samples are almost undetectable to the human eye compared to clean samples, but most advanced deep learning models may be fooled by the adversarial samples and thus misclassify the classification prediction. To address this problem, we propose a hierarchical feature-guided context network (HFGCNet). We find that learning by

文章引用: 董祥, 钱海强. 对抗攻击下的高光谱图像分类[J]. 建模与仿真, 2024, 13(3): 2911-2921.
DOI: 10.12677/mos.2024.133264

utilizing higher-order features to guide the learning of lower-order features enhances the effectiveness of multi-scale feature fusion, better extracts the global contextual information contained in the HSI, provides a better input to the loss apportionment module of the context network, and significantly improves the robustness of the neural network in the face of adversarial interference. Comparative experiments on two publicly available HSI datasets show that the method proposed in this paper is more resistant compared to other state-of-the-art deep learning models.

Keywords

Hyperspectral Image (HSI), Adversarial Attacks, Deep Learning, Adversarial Samples

1. 引言

图像分类是从高光谱图像中提取出重要信息方法之一[1]。过去，研究者通常使用传统算法对遥感影像进行解码与分析。虽然传统算法具有一定的可解释性，但是太过于依赖专家领域的知识和人工设计的特征提取器。这些特征提取器也无法有效的区别不同类别之间的差异，从而导致传统算法无法高效、准确的对 HSI 数据分类[2]。深度学习凭借其端到端自动学习判别特征的优势缓解了这一问题。

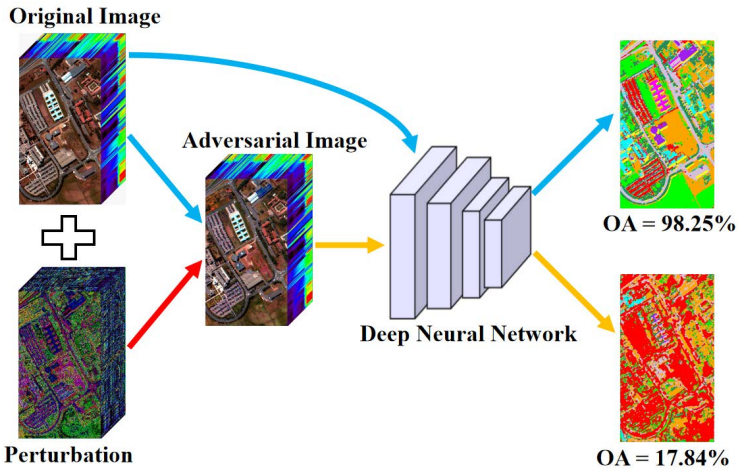


Figure 1. Examples of adversarial attacks on deep neural networks for hyperspectral image classification Tasks
图 1. 高光谱图像分类任务的深度神经网络的对抗性攻击示例

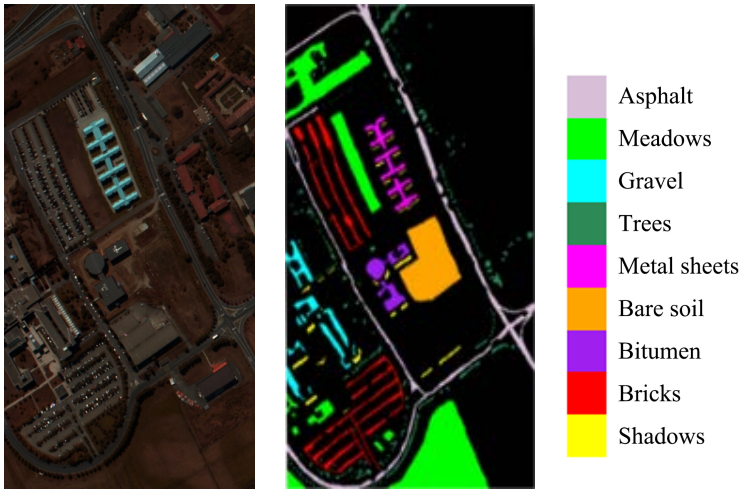
Chen 等人首次在 HSI 分类中使用了深度学习，提出了一种基于无监督学习和自动编码器分层训练的光谱－空间信息联合分类网络[3]。鉴于 HSI 分类任务中标记样本数量，Zhu 等人首次将对抗生成网络(GAN)引入到 HSI 分类任务中，更高效的扩展样本数量。同时设计针对空间和光谱特征的 1D-GAN 和 3D-GAN 模型作为相应的分类器[4]。Feng 等人分别设计了生成器，用于生成包含空间和光谱信息的样本。他们还设计了一种通过提取光谱特征进行多重分类的判别器[5]。Zhang 等人将 Progressive GAN 与 wasserstein 梯度惩罚概念相结合，实现了平滑稳定的训练[6]。尽管深度学习模型在遥感领域表现优异[7]，

但是在面对对抗干扰时，极易做出错误的判断。Szegedy 等人首次发现，在干净样本中加入对抗扰动会降低模型分类的准确性[8]。如图 1 所示，在原始干净图像上添加此快速符号梯度法(FGSM)后生成的对抗图像，人类视觉系统几乎无法辨别。本文使用 Ghostnet [9]作为深度学习示意模型。虽然 Ghostnet 在原始图像上可以实现 98.25%的 OA，但在对抗图像上却只有 17.84%。这种落差无疑展现了对抗干扰会对用于 HSI 分类的深度学习模型构成巨大威胁。

针对该问题，本文提出了一种分层特征引导上下文网络的对抗防御方法。该方法在骨干网络中使用特征编码与远程编码模型。在连接方式中，为了更好的让高阶特征指导低阶特征学习，本文借鉴了 U-Net 的连接方法[10]。将最终学习到的特征输入到上下文网络中，利用上下文网络的损失共享机制增强模型内在的鲁棒性。最后通过设计的顺序特征融合模块进行多尺度拼接，增强融合特征的表征能力。该网络能更好的辨别不同类别之间的差异，同时增强模型的泛化能力。本文的模型在两个不同数据集上均取得了超过 95%的总体准确率(OA)。

2. 高光谱数据集介绍

本文所用的数据集均为公开可用的。第一个数据集为 Pavia University。该数据集由 ROSIS 传感器在意大北部帕维亚上空拍摄得到的。空间分辨率为 1.3 米，共有 115 个波段，空间维度大小为 610 × 340，处理 12 个噪声波段后剩余 103 个波段，有 9 个特征类别可供分类。Pavia University 数据集的真实遥感影像和地面实况图如图 2 示，各个地物样本数量如表 1 所示。



(a) 原始图像　　(b) 地面实况图

Figure 2. Pavia university dataset
图 2. 帕维亚大学数据集

Table 1. Number of training and testing samples used University of Pavia dataset
表 1. 帕维亚大学数据集中使用的训练和测试样本数帕维亚大学数据集

类别序号	类名	训练数量	测试数量
1	Asphalt	100	6531
2	Meadows	100	18549
3	Gravel	100	1999

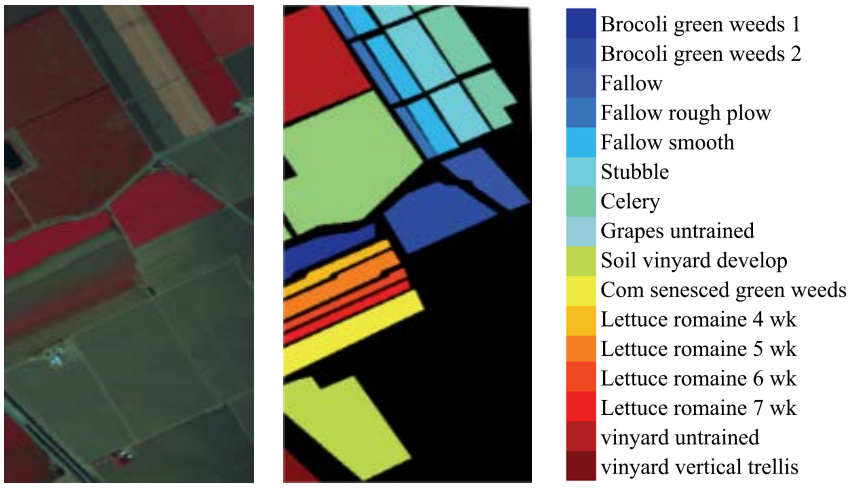
续表

4	Trees	100	2964
5	Metal sheets	100	1245
6	Bare soil	100	4929
7	Bitumen	100	1230
8	Bricks	100	3582
9	Shadows	100	847
	Total	900	41876

第二个数据集为 Salinas。该数据集由 AVIRIS 传感器获取，空间分辨率为 3.7 米，空间维度大小为 512 × 217。原始数据包含 224 个波段，剔除水汽吸收严重的波段后，剩下 204 个波段，有 16 个特征类别可供分类。Salinas 数据集的真实遥感影像和地面实况图如图 3 示，各个地物样本数量如表 2 所示。

Table 2. Number of training and testing samples used Salinas dataset
表 2. 萨利纳斯山谷数据集中使用的训练和测试样本数

类别序号	类名	训练数量	测试数量
1	Brocoli-green weeds 1	100	1909
2	Brocoli-green weeds 2	100	3623
3	Fallow	100	1876
4	Fallow rough plow	100	1294
5	Fallow smooth	100	2578
6	Stubble	100	3859
7	Celery	100	3479
8	Grapes untrained	100	11,971
9	Soil ineyard develop	100	6103
10	Corn senesced geeen weeds	100	3178
11	Lettuce romaine 4wk	100	968
12	Lettuce romaine 5wk	100	1827
13	Lettuce romaine 6wk	100	816
14	Lettuceromaine 7wk	100	970
15	Vinyard untrained	100	7168
16	Vinyard vertical trellis	100	1707
	Total	1600	52,529



(a) 原始图像　　(b) 地面实况图

Figure 3. Salinas dataset
图 3. 萨利纳斯数据集

3. 方法原理

3.1. 对抗攻击

假定深度神经网络函数为 $f:x\in\mathbb{R}^m\to y\in\{1,\cdots,k\}$，其中 k 为类别标签数，y 为相应的正确标签，对于给定图像 x 和相应标签 y' (本文希望网络预测错的结果)，可通过求解下面的盒式约束优化问题生成。

$$\min_{\rho}\|\rho\|_2,\text{Subject to}:\begin{cases}f(x+\rho)=y'\\ x+\rho\in[0,1]^m\end{cases},\tag{1}$$

式中，ρ 代表干扰值。精确计算公式(1)一般来说较困难。因此 Szegedy 等人使用公式(2)来获得近似解。

$$\min_{\rho}c\|\rho\|_2+J(f(x+\rho,\theta),y'),\tag{2}$$

其中 J 为损失函数，θ 为神经网络参数。由于在实际应用中公式(2)方法耗时较长，导致优化困难。针对这一问题，Goodfellow 等人提出了快速梯度符号法(FGSM)。快速梯度符号法是一种一步攻击方法，对抗实例 x_{adv} 的生成计算如式(3)所示：

$$x_{adv}=clip\left(x-\varepsilon sign\left(\nabla_x J\left(f(x,\theta),y'\right)\right)\right),\tag{3}$$

式中 $\tilde{N}_x J\left(f(x,\theta),y'\right)$ 为 $J\left(f(x,\theta)\right)$ 的梯度，$sign(\cdot)$为 sign 函数，$clip(\cdot)$确保最终生成的对抗范例的像素值被限定在一个特定的范围内。ε 是控制扰动的标量系数。Kurakin 等人通过引入∞规范来调整生成的扰动，改进了 FSGM。

$$\varsigma_\infty:x_{adv}=clip\left(x-\varepsilon\frac{\nabla_x J\left(f(x,\theta),y'\right)}{\left\|\nabla_x J\left(f(x,\theta),y'\right)\right\|_\infty}\right),\tag{4}$$

3.2. 网络模型设计

整个网络由骨干网络、上下文编码模块、顺序特征融合模块这三部分组成。骨干网络由四个 2D 卷积层、一个 6 × 6 的平均池化层和四对特征编码和远程特征编码模块构成。前四个卷积层采用不同扩张率的扩张卷积来扩大感受野。特征编码模块(如图 4 所示)由用于空间特征交互的 ConvNeXt 轻量级深度卷积

层和用于加速模型收敛的批量归一化(BN)层组成。远程特征编码模块(如图 4 所示)以特征编码模块为基础，加入了深度扩张卷积(扩张率为 3)，并配有两个跳转连接。其中特征编码只包括实线元素，而远程特征编码则包括实线和虚线元素。DW Conv 是深度卷积层。

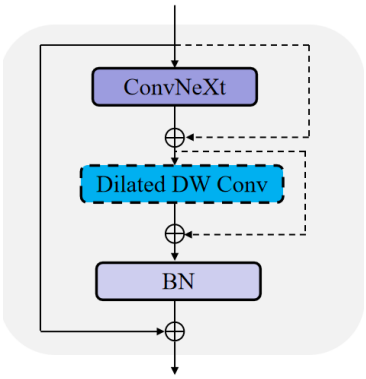


Figure 4. The structure of feature encoding and remote feature encoding
图 4. 特征编码和远程特征编码的结构

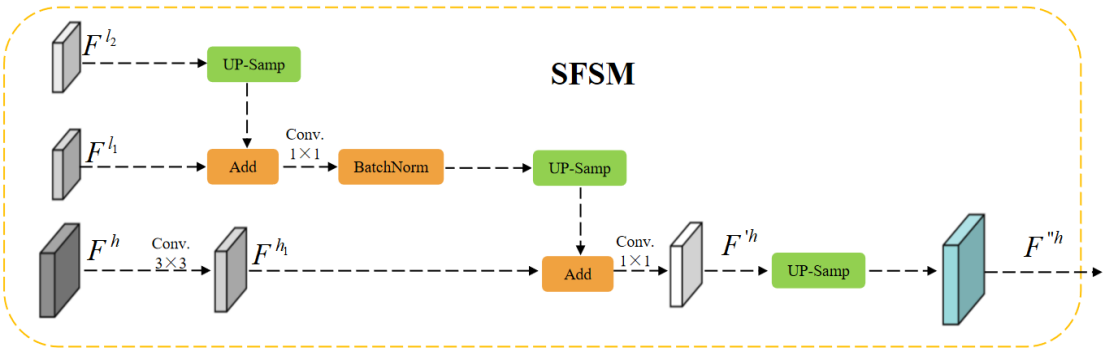


Figure 5. Sequential feature fusion module
图 5. 顺序特征编码模块

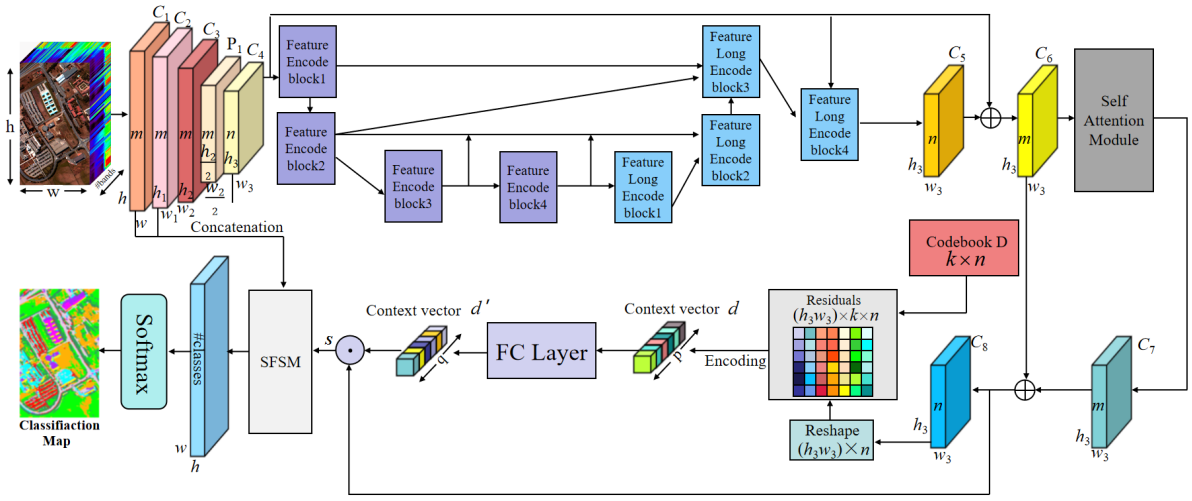


Figure 6. Hierarchical feature-guided context network
图 6. 分层特征引导上下文网络

为了更好地捕捉全局特征信息，提取的高层次特征 C_6 以建立全局空间依赖关系。注意力块中所有卷积核的大小均为 1 × 1，m 和 n 分别代表通道数，分别为 64 和 48。输出特征 C_7 的尺寸为 $m \times h_3 \times w_3$。然后通过残差连接与 C_6 连接，以降低过拟合风险。最后，通过 1 × 1 卷积层减少特征维度，输出大小为 $n \times h_3 \times w_3$ 的 C_8。本文将 C_8 重塑为 $(h_3 w_3) \times n$。紧接着将其送入到上下文网络中将给定像素点与整个图像所有相关像素点建立残差关系。设计一个可学习字典 D，大小为 $k \times n$，其中 $k = n = 48$，

$$e_{ij} = \frac{\exp\left(-s_j \left\| r_{ij} \right\|^2\right)}{\sum_{l=1}^{k} \exp\left(-s_l \left\| r_{il} \right\|^2\right)} r_{ij}, \tag{5}$$

式中 r_{ij} 代表 D 中每第 i 行元素(即 D 中第 i 个码本)与输入到上下文网络的 C_8 中第 j 特征点的残差，s_j 为第 j 个码本的缩放因子。全局上下向量 $e \in \mathbb{R}^n$，再将其输入到一个全连接层，输出特征为 $m \times 1 \times 1$ 的特征，和输入特征 C_8 做通道乘法输出为 S。最后将 S、C_1、C_2 输入到顺序特征融合模块中完成最后的拼接。顺序特征融合模块如图 5 所示，该模块可以减少融合特征图中边界信息的损失，这种高分辨率和低分辨率特征图之间的持续信息交互，可以将丰富的语义信息和精细的细节特征结合起来，实现对边界信息和相互干扰目标的更精确检测。整个网络如图 6 所示

4. 实验与分析

4.1. 实验设计和细节

本文在实验中使用的对抗样本都是通过公式(4)生成，其中 ε 的值设置为 0.06。实验是在相同扰动强度下，比较不同模型在相同对抗测试集上的分类结果。本研究中的所有实验结果都是通过重复 20 次随机训练和测试数据获得的。所有实验结果均通过计算 20 次结果的平均值和标准偏差得出。实验所需的训练集包括从相应数据集中为每个类别随机抽取的 100 个样本，而测试集则由其余样本组成。本文使用总体准确率(OA)、卡帕系数(k)、平均准确率(AA)和每个类别的准确率来评估不同的模型。本文中的所有实验均使用 Pytorch 框架进行。每个模型训练周期设置为 1000。实验在 A100-PCIE-40GB GPU 上进行。

4.2. 分类结果

分析表 3、表 4，本文可以看出，本文设计的模型在两个数据集上的表现均优于其余四个比较模型。在两个数据集上，SACNet 均远超其余 3 个对比模型 28%的 OA。这一现象表明，仅仅提取光谱和空间信息可能无法有效解决网络易受恶意攻击的问题。通过对比两个表中数据，可以发现现有的基于深度学习的先进方法极易受到对抗性干扰。以 CNN-LS^{2}CM [11]和 SSFCN [12]为例，它们在干净数据集上均取得了出色的成绩，然而在对抗测试集上的性能却严重下降。此外，本文还观察到，在 SACNet [13]的基础上加入特征编码和远程特征编码组合模块，以及顺序特征融合模块后，HFGCNet 在性能上明显优于 SACNet。这进一步证明了这两个模块的加入对增强模型内在的对抗防御能力是有效的。

进一步分析图 7、图 8 分类图像。在帕维亚大学数据集上，本文可以发现图像右下角明显属于“Meadows”类别的区域，其余四个模型均在这一区域表现出不同程度的误判，而本文 HFGCNet 模型对该类别的分类与地面实况基本一致。在萨利纳斯数据集上，本文还观察到图像左下角明显属于“Soil vinyard develop”的类别区域，其余四种对比模型都明显出严重的分类错误。相比之下，本文所提出的 HFGCNet 对对抗攻击具有更强的鲁棒性，且分类图更接近地面实况标注。这是因为基于 FGSM 算法的对抗干扰是在原始输入样本的基础上沿着损失函数的梯度方向生成干扰的，这就意味着攻击者根据训练模型的梯度信息来调整生成的对抗样本，而在本文对比的四个方法中有三个是单纯的基于空谱信息特征的

网络并不能很好处理图像中各像素点产生的有害梯度的影响，而 SACNet 是利用将像素点之间产生关联性，从而将各像素点产生的有害梯度由该图像中其他相关像素共同分担，所以性能相较于其余 3 个模型较优，但是其在主干网络的特征提取和网络末端特征融合部分并未学习到的语义信息，从而导致分类结果相较于本文较差。

Table 3. Adversarial classification results on the Pavia dataset, with best results in bold
表 3. 帕维亚数据集上的对抗分类结果，最佳结果以粗体显示

类别	SACNet	SSFCN	CNN-LS^{2}CM	Ghostnet	HFGCNet
1	90.48 ± 2.42	96.34 ± 0.74	96.46 ± 2.49	96.39 ± 3.32	96.10 ± 0.61
2	89.42 ± 4.64	5.84 ± 5.44	2.83 ± 4.55	61.14 ± 16.58	**92.86 ± 2.45**
3	91.71 ± 4.01	3.09 ± 3.17	3.53 ± 6.01	27.33 ± 33.81	**99.07 ± 0.96**
4	92.73 ± 4.19	**98.33 ± 0.37**	73.65 ± 26.36	92.43 ± 4.80	94.45 ± 1.32
5	98.24 ± 0.98	99.66 ± 0.2	95.45 ± 12.62	**100 ± 0.00**	99.85 ± 0.21
6	87.83 ± 22.09	64.70 ± 18.14	5.67 ± 7.00	24.11 ± 9.90	**98.77 ± 1.73**
7	83.16 ± 21.00	17.24 ± 11.69	0.02 ± 0.06	17.36 ± 16.25	**97.98 ± 1.08**
8	90.36 ± 3.73	74.30 ± 9.94	10.25 ± 11.34	42.03 ± 24.13	**96.52 ± 0.93**
9	97.45 ± 1.83	**99.90 ± 0.13**	92.75 ± 18.67	99.03 ± 2.10	98.43 ± 0.50
OA (%)	90.10 ± 3.60	44.22 ± 3.59	27.97 ± 3.27	61.42 ± 9.32	**95.30 ± 1.05**
K (%)	87.02 ± 3.70	36.99 ± 3.60	18.21 ± 3.60	51.61 ± 10.48	**93.82 ± 1.34**
AA (%)	91.26 ± 4.34	62.15 ± 2.53	42.29 ± 5.21	62.20 ± 7.39	**97.11 ± 0.37**

Table 4. Adversarial classification results on the Pavia dataset, with best results in bold
表 4. 萨利纳斯数据集上的对抗分类结果，最佳结果以粗体显示

类别	SACNet	SSFCN	CNN-LS^{2}CM	Ghostnet	HFGCNet
1	98.92 ± 1.90	100 ± 0.00	100 ± 0.00	99.99 ± 0.03	**100 ± 0.00**
2	89.43 ± 22.65	42.31 ± 18.57	11.60 ± 19.47	98.39 ± 2.36	**100 ± 0.00**
3	97.14 ± 4.74	0.26 ± 0.53	10.63 ± 12.00	15.24 ± 18.36	**99.25 ± 2.21**
4	91.52 ± 12.88	35.14 ± 35.31	40.72 ± 39.73	51.98 ± 33.27	**99.20 ± 0.77**
5	93.54 ± 11.07	8.69 ± 22.26	27.03 ± 28.99	44.57 ± 38.37	**99.31 ± 0.45**
6	99.15 ± 0.62	92.73 ± 11.75	73.16 ± 35.22	99.87 ± 0.33	**99.98 ± 0.06**
7	96.80 ± 3.72	23.43 ± 26.27	19.81 ± 27.30	86.43 ± 14.84	**99.78 ± 0.16**
8	85.78 ± 10.13	83.09 ± 24.85	12.76 ± 15.17	24.52 ± 14.4	**94.91 ± 5.39**
9	92.28 ± 12.83	14.05 ± 30.19	45.91 ± 22.75	53.28 ± 29.29	**100 ± 0.00**
10	98.27 ± 1.26	77.58 ± 19.13	33.36 ± 21.73	58.15 ± 29.07	**98.86 ± 1.40**

续表

11	98.72 ± 1.84	35.76 ± 29.42	43.14 ± 29.77	59.72 ± 35.74	**99.42 ± 1.04**
12	99.77 ± 0.55	19.83 ± 25.86	9.45 ± 19.64	40.15 ± 24.87	**99.96 ± 0.08**
13	98.06 ± 3.42	96.40 ± 4.58	36.76 ± 23.83	56.46 ± 29.43	**100 ± 0.00**
14	99.84 ± 0.24	86.62 ± 29.65	37.43 ± 30.42	80.29 ± 18.08	**99.97 ± 0.09**
15	65.11 ± 25.74	14.53 ± 27.38	3.03 ± 5.34	33.37 ± 32.91	**95.42 ± 4.69**
16	96.48 ± 3.99	21.76 ± 13.57	44.43 ± 31.50	87.09 ± 20.08	**99.64 ± 0.54**
OA (%)	89.37 ± 4.40	45.79 ± 2.34	27.91 ± 7.64	54.79 ± 9.95	**98.13 ± 1.05**
K (%)	88.12 ± 4.96	39.77 ± 2.24	21.91 ± 8.04	49.61 ± 11.8	**97.91 ± 1.17**
AA (%)	93.94 ± 3.86	47.01 ± 2.12	34.32 ± 7.06	61.84 ± 11.44	**99.10 ± 0.04**

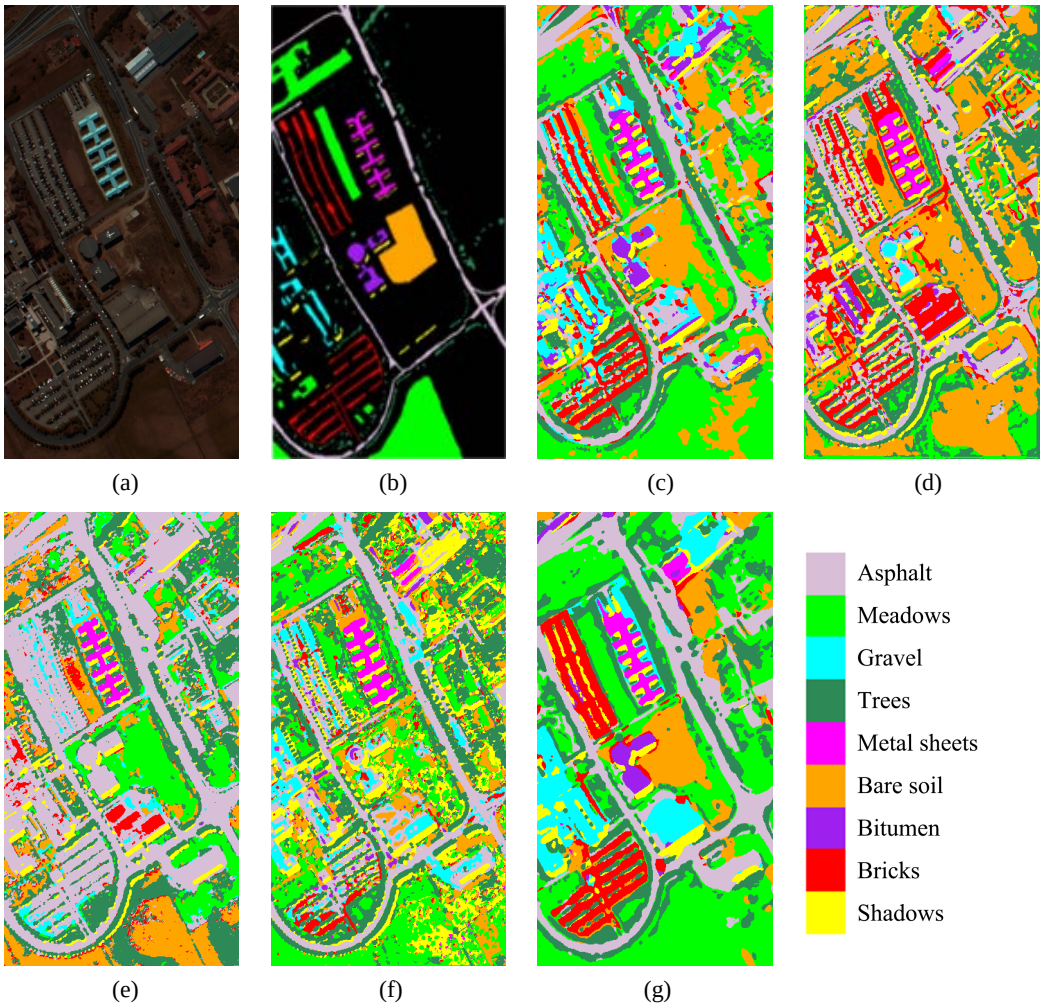


Figure 7. Classification maps of Pavia University dataset on the adversarial test set with $\varepsilon = 0.06$. (a) The false color image, (b) Ground-truth map, (c) SACNet, (d) SSFCN, (e) CNN-LS^{2}CM, (f) Ghostnet, (g) HFGCNet

图 7. 帕维亚大学数据集在 $\varepsilon = 0.06$ 的对抗测试集上的分类图。(a) 伪彩色图，(b) 地面实况图，(c) SACNet，(d) SSFCN，(e) CNN-LS^{2}CM，(f) Ghostnet，(g) HFGCNet

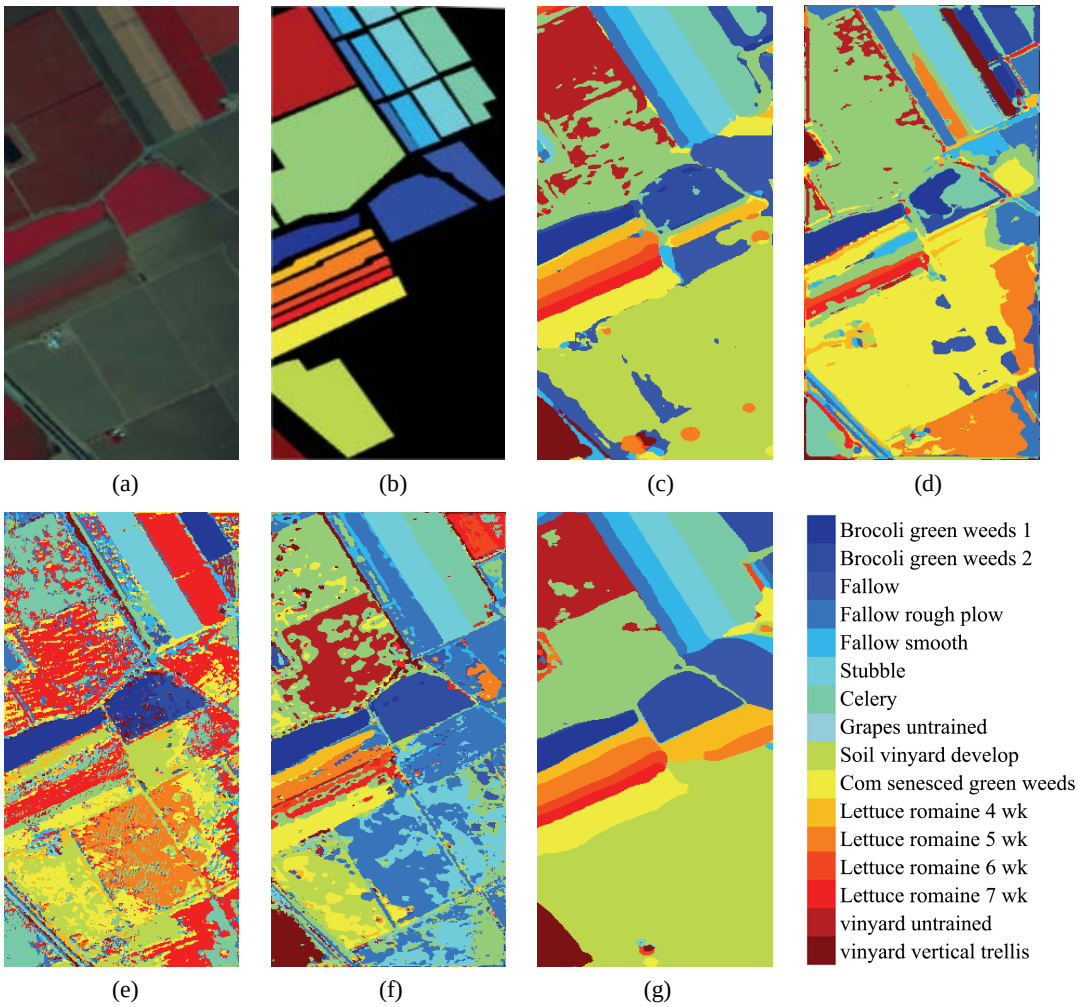


Figure 8. Classification maps of Salinas dataset on the adversarial test set with $\varepsilon = 0.06$. (a) The false color image, (b) Ground-truth map, (c) SACNet, (d) SSFCN, (e) CNN-LS^{2}CM, (f) Ghostnet, (g) HFGCNet

图 8. 萨利纳斯数据集在 $\varepsilon = 0.06$ 的对抗测试集上的分类图。(a) 伪彩色图，(b) 地面实况图，(c) SACNet，(d) SSFCN，(e) CNN-LS2CM，(f) GhostNet，(g) HFGCNet

5. 结束语

迄今为止，大多数基于深度学习的高光谱成像(HSI)研究都取得了巨大成功。然而，这些研究大多建立在干净的数据集上。很少有人考虑过将数据应用到不同的场景下进行准确分类。在本研究中，本文将HSI 应用于对抗攻击场景下，并通过对比实验证明了深度学习模型在面对对抗攻击时的脆弱性。

通过几组模型对比，本文发现，在分类中综合空间特征与光谱特征并不能很好的防御通过训练网络损失函数梯度生成的对抗干扰的威胁。同时本文也发现，通过将图像中的给定像素点与其余像素点建立关联性可在一定程度上防御对抗干扰，但是通过对比 SACNet 与 HFGCNet 两者的分类结果，发现这种关系的构建需要提取更全面的上下文信息才能有更好效果。鉴于此，本文提出了一种基于分层特征引导上下文网络模型。用于端到端处理高光谱成像(HSI)中的对抗防御问题。本文的方法主要侧重在如何使得输入到上下文网络的全局信息特征更加优质，从而让给定像素与其余像素特征更好地建立非线性关系，以达成损失共享最大化，增强模型内在的鲁棒性。本文在两个公开的数据集上测试了所提出的方法。实验结果表明，与其他先进的深度分类模型相比，本文的方法在对抗防御具有更显著的优势。

参考文献

[1] Pal, M. (2024) Deep Learning Algorithms for Hyperspectral Remote Sensing Classifications: An Applied Review. *International Journal of Remote Sensing*, **45**, 451-491. https://doi.org/10.1080/01431161.2023.2297178

[2] Li, S., Song, W., Fang, L., Chen, Y., Ghamisi, P. and Benediktsson, J.A. (2019) Deep Learning for Hyperspectral Image Classification: An Overview. *IEEE Transactions on Geoscience and Remote Sensing*, **57**, 6690-6709. https://doi.org/10.1109/TGRS.2019.2907932

[3] Chen, Y., Lin, Z., Zhao, X., Wang, G. and Gu, Y. (2014) Deep Learning-Based Classification of Hyperspectral Data. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, **7**, 2094-2107. https://doi.org/10.1109/JSTARS.2014.2329330

[4] Zhu, L., Chen, Y., Ghamisi, P. and Benediktsson, J.A. (2018) Generative Adversarial Networks for Hyperspectral Image Classification. *IEEE Transactions on Geoscience and Remote Sensing*, **56**, 5046-5063. https://doi.org/10.1109/TGRS.2018.2805286

[5] Feng, J., Yu, H., Wang, L., Cao, X., Zhang, X. and Jiao, L. (2019) Classification of Hyperspectral Images Based on Multiclass Spatial—Spectral Generative Adversarial Networks. *IEEE Transactions on Geoscience and Remote Sensing*, **57**, 5329-5343. https://doi.org/10.1109/TGRS.2019.2899057

[6] Zhang, F., Bai, J., Zhang, J., Xiao, Z. and Pei, C. (2020) An Optimized Training Method for GAN-Based Hyperspectral image Classification. *IEEE Geoscience and Remote Sensing Letters*, **18**, 1791-1795. https://doi.org/10.1109/LGRS.2020.3009017

[7] Zhang, L., Zhang, L. and Du, B. (2016) Deep Learning for Remote Sensing Data: A Technical Tutorial on the State of the Art. *IEEE Geoscience and Remote Sensing Magazine*, **4**, 22-40. https://doi.org/10.1109/MGRS.2016.2540798

[8] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I. and Fergus, R. (2013) Intriguing Properties of Neural Networks. arXiv:1312.6199.

[9] Paoletti, M.E., Haut, J.M., Pereira, N.S., Plaza, J. and Plaza, A. (2021) Ghostnet for Hyperspectral Image Classification. *IEEE Transactions on Geoscience and Remote Sensing*, **59**, 10378-10393. https://doi.org/10.1109/TGRS.2021.3050257

[10] Ronneberger, O., Fischer, P. and Brox, T. (2015) U-net: Convolutional Networks for Biomedical Image Segmentation. *Medical Image Computing and Computer-Assisted Intervention—MICCAI* 2015: 18*th International Conference*, Munich, 5-9 October 2015, 234-241. https://doi.org/10.1007/978-3-319-24574-4_28

[11] Meng, Z., Jiao, L., Liang, M. and Zhao, F. (2021) A Lightweight Spectral-Spatial Convolution Module for Hyperspectral Image Classification. *IEEE Geoscience and Remote Sensing Letters*, **19**, 1-5. https://doi.org/10.1109/LGRS.2021.3069202

[12] Xu, Y., Du, B. and Zhang, L. (2019) Beyond the Patchwise Classification: Spectral-Spatial Fully Convolutional Networks for Hyperspectral Image Classification. *IEEE Transactions on Big Data*, **6**, 492-506. https://doi.org/10.1109/TBDATA.2019.2923243

[13] Xu, Y., Du, B. and Zhang, L. (2021) Self-Attention Context Network: Addressing the Threat of Adversarial Attacks for Hyperspectral Image Classification. *IEEE Transactions on Image Processing*, **30**, 8671-8685. https://doi.org/10.1109/TIP.2021.3118977