|  |  |
| --- | --- |
| **文章信息** | **内容** |
| **阅读程度**：  精读  **文章标题：**  Revisiting Residual Networks for Adversarial Robustness: An Architectural Perspective  **中文标题：**  重新审视残差网络的对抗性稳健性：一个架构的视角  **发表于：**  CVPR2023  **作者：**  Shihua Huang1 Zhichao Lu2\*  **单位：**  陆智超，中山大学的带三个密歇根州立大学的，爱了爱了，叫超的都好强。  真的是很完善的实验设计和很有耐心的工作方案 | 本文真的是条理清晰： |
| **摘要** |  |
| 提高卷积神经网络的对抗性鲁棒性的努力主要集中在开发更有效的对抗性训练方法上。相比之下，很少有人关注分析架构元素（如拓扑结构、深度和宽度）对对抗性鲁棒性的作用。  本文试图弥合这一差距，并提出了一个关于架构设计对对抗性稳健性的影响的整体研究。我们关注残差网络，并考虑块级别的架构设计，即拓扑结构、内核大小、激活和规范化，以及网络缩放级别，即网络中每个块的深度和宽度。  在这两种情况下，我们首先通过系统的消融实验来获得见解。然后，我们设计了一个鲁棒性残差块，称为鲁棒残差块，以及一个复合缩放规则，称为鲁棒缩放，以在所需的FLOP计数下分布深度和宽度。  最后，我们结合了鲁棒块和鲁棒缩放，并提出了一个对抗性鲁棒残差网络组合，鲁棒残差网络，涵盖了多种模型容量。  实验验证跨多个数据集和对抗性攻击表明，健壮的ResNets始终优于标准网络和其他现有的健壮的架构，实现最先进的自动攻击的61.1%（没有额外的数据）和63.7%（有500K外部数据）而2×更紧凑的参数。  简介部分：  第一段介绍了一个观点，即网络结构的变更所带来的鲁棒性改变与寻找不同的对抗训练策略所带来的改变几乎相当，为了描述这个观点，提供了一个变化量图：    左，以wrn-28-10为基线，研究了块结构，核尺寸，宽度深度等因素造成的鲁棒性改善，而最右边的灰条是不同的对抗训练策略产生的鲁棒性改善。  四个贡献写的特别好：  第一个贡献是一个简单但有效的SE变体，这是在网络组件探究中的创新点（其余的网络组件没有创新，只是研究了他们对鲁棒性的贡献）  第二个贡献是基于对这些网络组件的研究，提出了鲁棒性残差块，这是基于实验得到的。  第三个贡献是提出了鲁棒性缩放规则，在提高鲁棒精度的同时，减少了网络的可训练参。  第四个贡献是结合上述内容，使用鲁棒性残差块与鲁棒性缩放规则，实现了一波sota。 |  |