Robust AI Project Team

Weekly Report

Heran Zhu

Electronic Information School, Wuhan University

Oct 9th, 2021

鲁棒模型

表 1: 干净样本测试集

训练方法	训练数据集	准确率
正常训练	原始干净样本	**92.15** %
PDG对抗训练	干净样本、重建样本	85.25 %
PDG对抗训练	对抗样本、对抗样本的重建样本	**89.30** %

表 2: PDG对抗样本测试集

训练方法	训练数据集	准确率
正常训练	原始干净样本	4.55 %
PDG对抗训练	干净样本、重建样本	78.40 %
PDG对抗训练	对抗样本、对抗样本的重建样本	83.55 %

在鲁棒模型之前加入重建

表 3: 干净样本重建测试集

训练方法	训练数据集	准确率
正常训练	原始干净样本	**90.15** %
PDG对抗训练	干净样本、重建样本	83.75 %
PDG对抗训练	对抗样本、对抗样本的重建样本	**87.00** %

表 4: 对抗样本重建测试集

训练方法	训练数据集	准确率
正常训练	原始干净样本	**75.25** %
PDG对抗训练	干净样本、重建样本	72.25 %
PDG对抗训练	对抗样本、对抗样本的重建样本	**82.05** %

Thanks!