2020 04 20 智能对抗组会

Spencer Woo

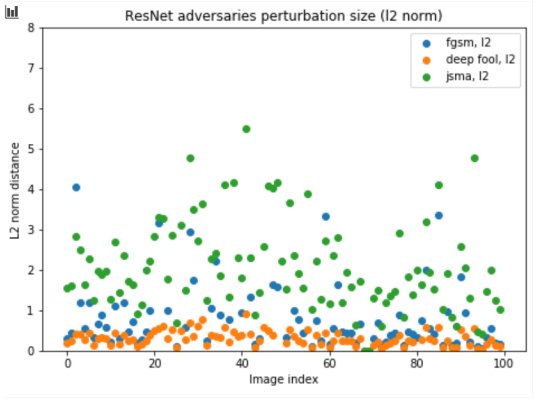
Data Security and Artificial Intelligence Security Laboratory
School of Computer Science and Technology, BIT

2020 年 4 月 20 日

北京理工大學

</> 第一部分的一个大标题

第一部分 第一个实验的实验结果



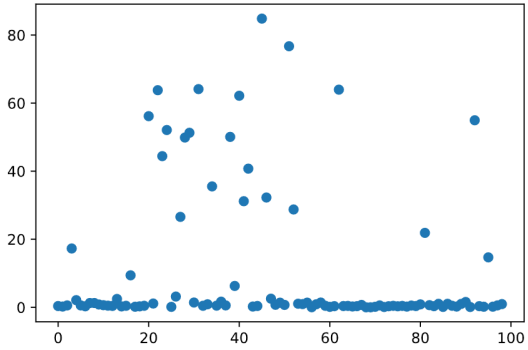
✔ 100% fooling rate

北京理工大學

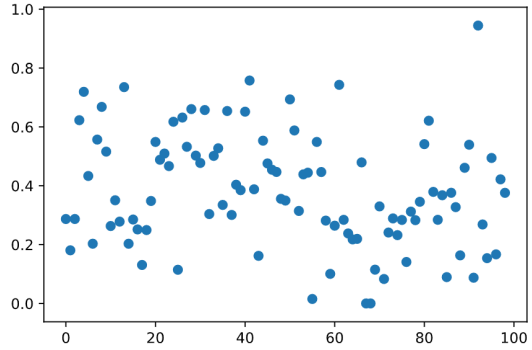
之后部分实验的实验结果

实验二 巴啦啦小魔仙实验

左右分栏的左侧部分



左右分栏的右侧部分



最后总结和计划

一个相关的公式：

$$x_{adv} = x + \varepsilon * \text{sign}(\nabla_x J(\theta, x, y))$$

之后的任务重点：

- 完成某某任务的某某阶段，记录分析某阶段性成果
- 整理、收集并分析第一实验数据
- 对第二实验进行重新构思、规划和设计