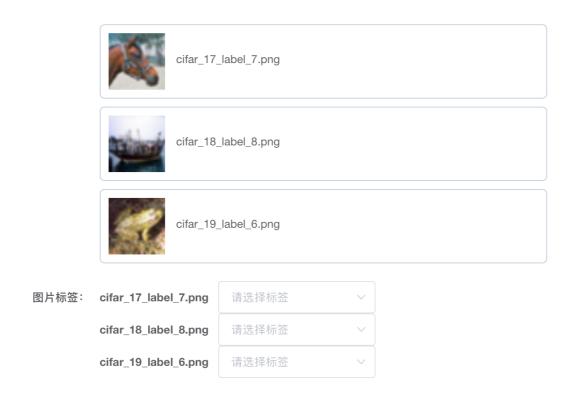
Deepcert 工具使用说明

第一步:选择网络模型的数据集,目前 Deepcert 工具支持在 cifar-10 与 mnist 两种数据集上进行验证工作。

第二步:上传需要验证的网络模型文件,Deepcert 对于网络模型有着如下限制: {{模型文件限制}}

第三步:上传需要进行验证的测试图片,Deepcert 对于测试图片有着如下限制:对于基于 mnist 数据集的网络模型,测试图片要求为 28*28 的灰度图,并且为 png 格式;对于基于 cifar-10 数据集的网络模型,测试图片要求为 32*32*3 的彩色图,并且为 png 格式。

上传图片时支持多选,在完成上传图片选择后,需要提供每一张测试图片的标签(即在网络中该图片的正确分类结果),如果文件名中包含'label_',则其后的数字会被作为默认标签。图片含义与标签序号的关系参见表 1 与表 2 例:



第四步:是选择扰动半径度量标准,目前 Deepcert 工具支持在 L1, L2,以及无穷范数下计算测试图片的最小对抗扰动半径。

| 标签序号 | 含义 |
|------|------------|
| 0 | airplane |
| 1 | automobile |
| 2 | bird |
| 3 | cat |
| 4 | deer |
| 5 | dog |
| 6 | frog |
| 7 | horse |
| 8 | ship |
| 9 | truck |

表 1 测试图片标签与含义关系表: cifar-10

| 标签序号 | 含义 |
|------|--------|
| 0 | 手写数字 0 |
| 1 | 手写数字 1 |
| 2 | 手写数字 2 |
| 3 | 手写数字3 |
| 4 | 手写数字 4 |
| 5 | 手写数字 5 |
| 6 | 手写数字 6 |
| 7 | 手写数字7 |
| 8 | 手写数字 8 |
| 9 | 手写数字 9 |

表 2 测试图片标签与含义关系表: mnist