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。

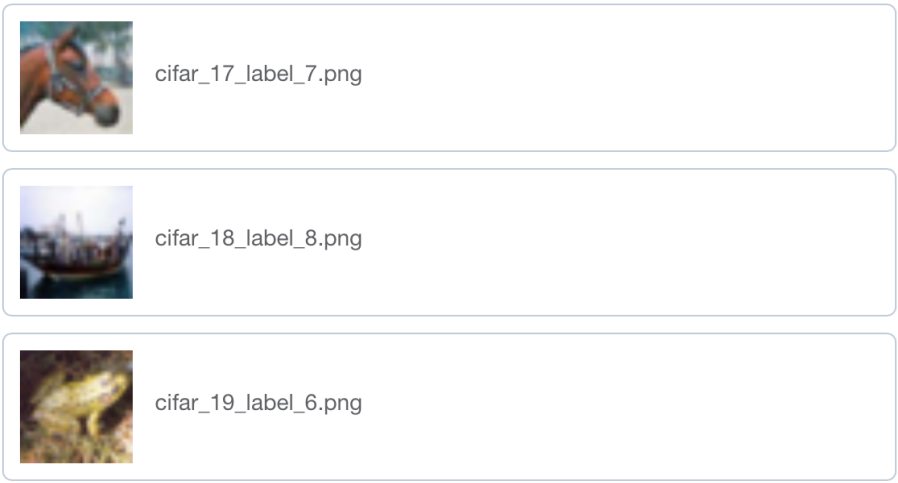
第二步：上传需要验证的网络模型文件，Deepcert 对于网络模型有着如下限制：网络文件格式为.h5，网络只支持“卷积层+全连接层”或“卷积层+池化层/残差层+全连接层”，暂时不支持仅包含全连接层的网络。

Deepcert 对于网络模型文件名有着如下限制：对于“卷积层+全连接层”的网络，文件名为*数据集名称(cifar/mnist)*_cnn_*层数* layer_*filter 数*_*kernal 数*_*激活函数(sigmoid/tanh/arctan)*，例如 cifar_cnn_5layer_5_3_tanh；对于卷积层+池化层/残差层+全连接层”的网络，文件名为*数据集名称(cifar/mnist)*_cnn/resnet_*网络层数/结构特征*_*激活函数(sigmoid/tanh/arctan)*，例如 mnist_resnet_5_sigmoid

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