WiNR 工具使用说明

第一步：选择网络模型的数据集，目前 WiNR 工具支持在 cifar-10 ，fashion_mnist 和 gtsrb 三种数据集上进行验证工作。

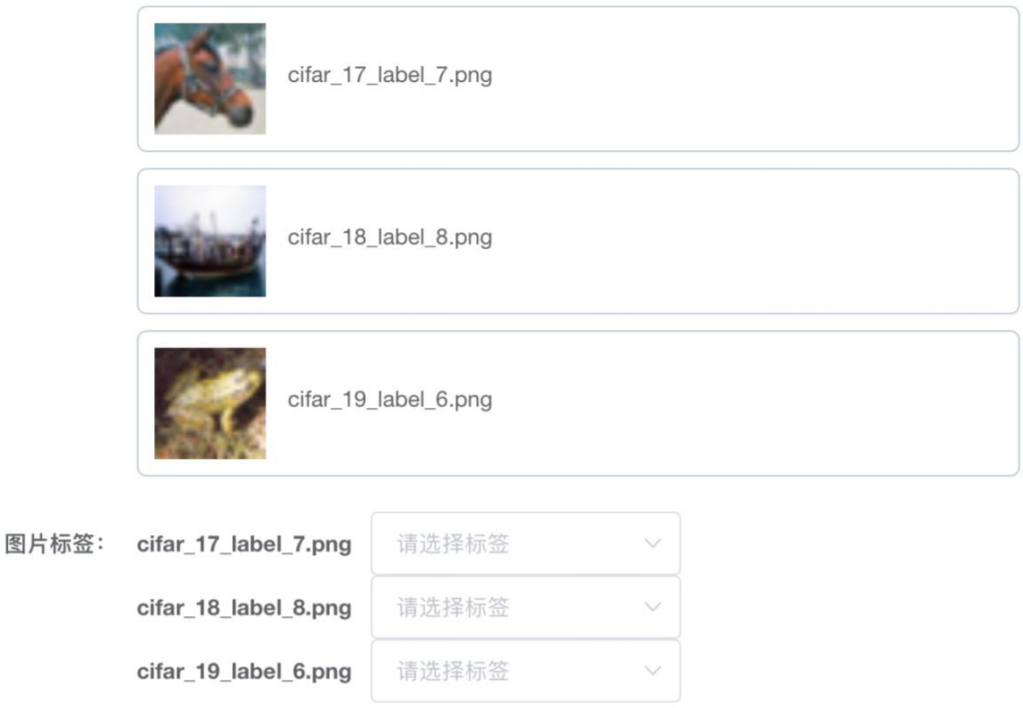
第二步：上传需要验证的网络模型文件，WiNR 对于网络模型有着如下限制：文件格式要求为 .h5 ，激活函数目前要求为 sigmoid ，网络要求为“卷积层”或“卷积层 + 池化层”。

第三步：选择扰动值，调整步长为 0.005，也可通过手动输入。

第四步：上传需要进行验证的测试图片，WiNR 对于测试图片有着如下限制：图片格式要求为 .jpg ，对于基于 fashion_mnist 数据集的网络模型，测试图片要求为 28*28 的灰度图；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；对于基于 gtsrb 数据集的网络模型，测试图片要求为 43*43*3 的彩色图。

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，表 2，表 3。

例：



标签序号	含义
0	T-shirt
1	Trouser
2	Pullover
3	Dress
4	Coat
5	Sandal
6	Shirt
7	Sneaker
8	Bag
9	Ankle boot

表 1 测试图片标签与含义关系表 fashion_mnist

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 2 测试图片标签与含义关系表. cifar-10

标签序号	含义
0	Speed limit (20km/h)
1	Speed limit (30km/h)
2	Speed limit (50km/h)
3	Speed limit (60km/h)
4	Speed limit (70km/h)
5	Speed limit (80km/h)
6	End of speed limit (80km/h)
7	Speed limit (100km/h)
8	Speed limit (120km/h)
9	No passing
10	No passing for vehicles over 3.5 metric tons
11	Right-of-way at the next intersection
12	Priority road
13	Yield
14	Stop
15	No vehicles
16	Vehicles over 3.5 metric tons prohibited
17	No entry
18	General caution
19	Dangerous curve to the left
20	Dangerous curve to the right
21	Double curve
22	Bumpy road
23	Slippery road
24	Road narrows on the right
25	Road work

26	Traffic signals
27	Pedestrians
28	Children crossing
29	Bicycles crossing
30	Beware of ice/snow
31	Wild animals crossing
32	End of all speed and passing limits
33	Turn right ahead
34	Turn left ahead
35	Ahead only
36	Go straight or right
37	Go straight or left
38	Keep right
39	Keep left
40	Roundabout mandatory
41	End of no passing
42	End of no passing by vehicles over 3.5 metric tons

表 3 测试图片标签与含义关系表 gtsrb