Benchmark Result

Succeeded Adversarial examples

Top-5 Accuracy against attacks

Vanilla	20%			
attacks	FGSM	CW	PGD	DeepFool
default	60%	60%	64%	22%
targeted	60%	60%	unsupported	unsupported

Attack Results with graph
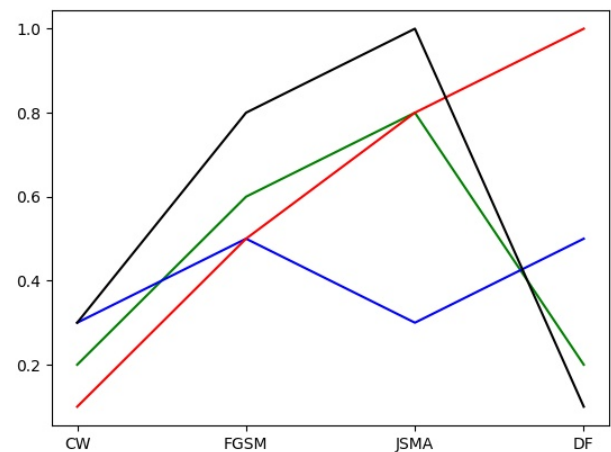
Advise for your model robustness

robustness about your model can vary considering your data sets complexity. Your Model cannot defend againstNone1 Your model is hardly robust to given attacks. Is this properly trained?

This weakness can be caused from setting hyper parameters, matbe input bias, or input capacity and so many more.If you think none of this are your issues we recommend adversarial training with our adverarial examples provided.

Try again with adversarilly trained model and check out the result. See more info in the attached papers and linked tensorboard.