

Hyper-parameters of attack methods

dataset	attack method	model family	parameter	success rate
MNIST	FGSM	LeNet	0.2, 0.3, 0.4	0.94
		VGG		0.81
		ResNet		0.83
		GoogLeNet		0.71
	CW	LeNet	9, 10, 11	0.91
		VGG		0.81
		ResNet		0.91
		GoogLeNet		0.90
	JSMA	LeNet	0.09, 0.1, 0.11	0.89
		VGG		0.25
		ResNet		0.75
		GoogLeNet		0.52
CIFAR	FGSM	VGG	0.01, 0.02, 0.03	0.76
		ResNet		0.65
		GoogLeNet		0.75
	CW	VGG	0.1, 0.2, 0.3	0.88
		ResNet		0.90
		GoogLeNet		0.90
	JSMA	VGG	0.09, 0.1, 0.11	0.80
		ResNet		0.79
		GoogLeNet		0.75