

Modell	Akkuranz (%)	Loss
ResNet18	94,89	0,2491
ResNet18 + Pixle-Attack	25,16	0,9077
ResNet18 + Gauß Smoothing (original data)	93,75	0,2018
ResNet18 + Gauß Smoothing (adv. data)	85,51	0,3832
ResNet18 + Adversarial Training (original data)	93,18	0,3037
ResNet18 + Adversarial Training (adv. data)	73,26	0,4889
ResNet18 + Gauß Smoothing + Adversarial Training (original data)	95,17	0,2568
ResNet18 + Gauß Smoothing + Adversarial Training (adv. data)	91,89	0,3174
ResNet50	95,17	0,2490
ResNet50 + Pixle-Attack	23,04	0,9258
ResNet50 + Gauß Smoothing (original data)	83,93	0,4616
ResNet50 + Gauß Smoothing (adv. data)	71,59	0,6311
ResNet50 + Adversarial Training (original data)	94,60	0,2354
ResNet50 + Adversarial Training (adv. data)	84,22	0,3717
ResNet50 + Gauß Smoothing + Adversarial Training (original data)	94,57	0,5184
ResNet50 + Gauß Smoothing + Adversarial Training (adv. data)	93,72	0,5434