

Adversarial Images

Adam Spindler

February 23, 2021

1 Introduction

2 Accuracies with Perturbation

2.1 Adding Noise



YOLOv3 = 0.99987
RCNN = 0.99987



YOLOv3 = 0.99987
RCNN = 0.99993



YOLOv3 = 0.99968
RCNN = 0.99610



YOLOv3 = 0.99985
RCNN = 0

2.2 Grayscale



YOLOv3 = 0.99987
RCNN = 0.99987



YOLOv3 = 0.99988
RCNN = 0.99987



YOLOv3 = 0.99989
RCNN = 0.99986



YOLOv3 = 0.99986
RCNN = 0.99868

2.3 Contrast



YOLOv3 = 0.99987
RCNN = 0.99987



YOLOv3 = 0.99985
RCNN = 0.99994



YOLOv3 = 0.99986
RCNN = 0.99993



YOLOv3 = 0.99984
RCNN = 0.99859