

Left Image = Clean Image Right Image = Image after adding adversarial noise

FGSM:

1) Epsilon = 0.1

True Label: horse Predicted Label: horse Predicted Label after Attack: cat
True Label: bird Predicted Label: bird Predicted Label after Attack: cat

pred: 7, adv:3

pred: 2, adv:3



True Label: plane Predicted Label: plane Predicted Label after Attack: bird
True Label: car Predicted Label: car Predicted Label after Attack: truck

pred: 0, adv:2

pred: 1, adv:9



2) Epsilon = 0.15

True Label: plane Predicted Label: plane Predicted Label after Attack: ship
True Label: ship Predicted Label: ship Predicted Label after Attack: car

pred: 0, adv:8

pred: 8, adv:1



True Label: ship Predicted Label: ship Predicted Label after Attack: plane
True Label: bird Predicted Label: bird Predicted Label after Attack: plane

pred: 8, adv:0

pred: 2, adv:0




Epsilon = 0.2

True Label: dog Predicted Label: dog Predicted Label after Attack: bird
True Label: car Predicted Label: car Predicted Label after Attack: truck

pred: 5, adv:2

pred: 1, adv:9





True Label: ship	Predicted Label: ship	Predicted Label after Attack: plane
True Label: deer	Predicted Label: deer	Predicted Label after Attack: bird
pred: 8, adv:0	pred: 4, adv:2	
		



2. Iterative FGSM

All the images are for 10 iterations.



Left image = clean image , Middle image = Image after adding adversarial noise, Right = Adversarial Noise

1) Epsilon = 0.075

True Label: deer	Predicted Label: deer	Predicted Label after Attack: bird
True Label: dog	Predicted Label: dog	Predicted Label after Attack: bird
pred: 4, adv:2	pred: 5, adv:2	
		

True Label: frog	Predicted Label: frog	Predicted Label after Attack: car
True Label: dog	Predicted Label: dog	Predicted Label after Attack: bird
pred: 6, adv:1	pred: 5, adv:2	
		

2) Epsilon = 0.1

True Label: deer	Predicted Label: deer	Predicted Label after Attack: frog
True Label: cat	Predicted Label: cat	Predicted Label after Attack: frog
pred: 4, adv:6	pred: 3, adv:6	
		

True Label: deer	Predicted Label: deer	Predicted Label after Attack: truck
True Label: horse	Predicted Label: horse	Predicted Label after Attack: dog
pred: 4, adv:9	pred: 7, adv:5	



3) Epsilon = 0.15

True Label: deer	Predicted Label: deer	Predicted Label after Attack: bird
pred: 4, adv:2		



True Label: plane	Predicted Label: plane	Predicted Label after Attack: ship
pred: 0, adv:8		

