

Metric	Clean	No Defense Attack	w/ Defense Attack
Loss	0.000641	3.93	0.00759
Accuracy	100%	16%	100%

Example Misclassifications:

```

-----
No misclassified images for stage: Clean
Attack: fgsm_cw_attack
Dataset: MNIST
Training Epochs: 10
Trained Clean Images: 64
Test Images: 140
Accuracy: 1.00
Precision: 1.00
Recall: 1.00
F1-score: 1.00
ROC AUC score is not defined for a single class.
-----

```

```

-----
Number of misclassified images for No Defense Attack: 54
Attack: fgsm_cw_attack
Dataset: MNIST
Training Epochs: 10
Adversarial Training Images: 60
Test Images: 140
Accuracy: 0.16
Precision: 0.28
Recall: 0.24
F1-score: 0.26
ROC AUC Score: 1.00
-----

```

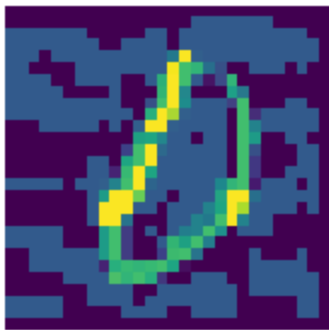
Misclassifications:

```

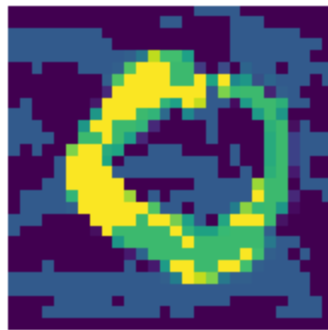
0 -> 2: 12
0 -> 9: 15
0 -> 6: 6
0 -> 5: 5
0 -> 7: 7
0 -> 8: 7
0 -> 1: 2

```

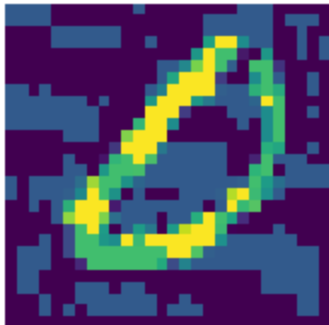
0 -> 2



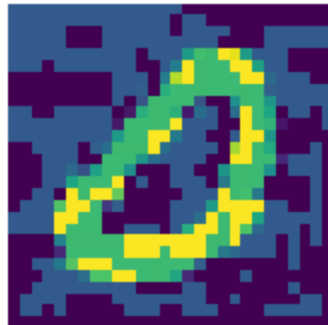
0 -> 9



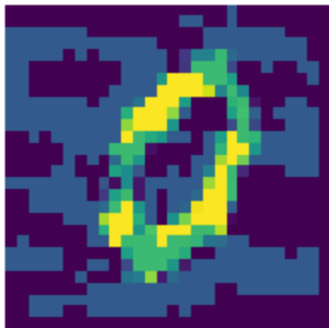
0 -> 6



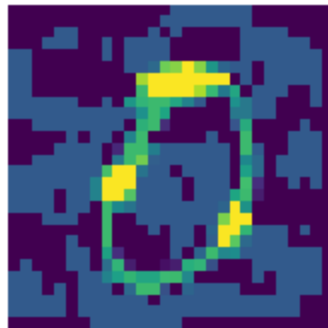
0 -> 2



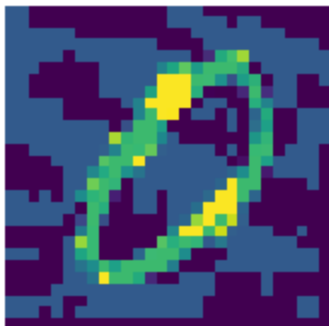
0 -> 9



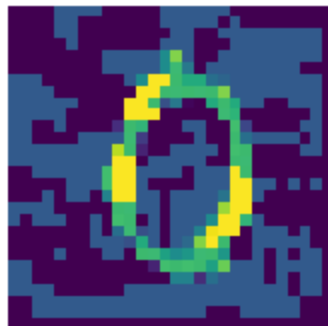
0 -> 5



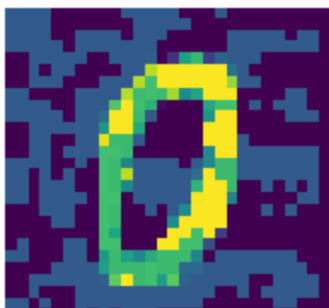
0 -> 2



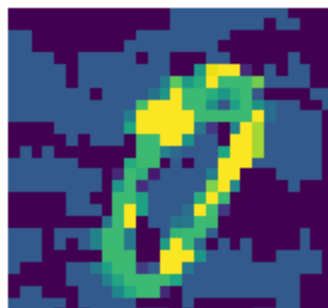
0 -> 5



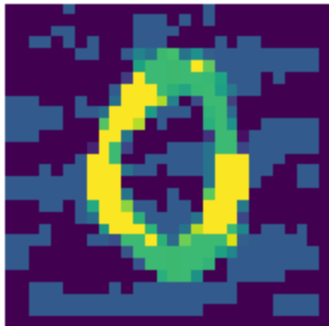
0 -> 7



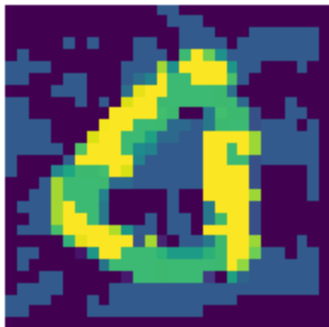
0 -> 8



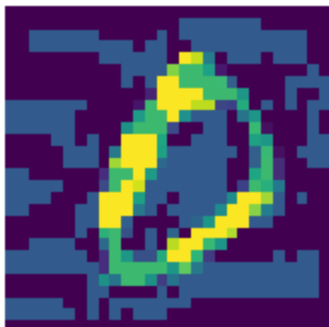
0 -> 9



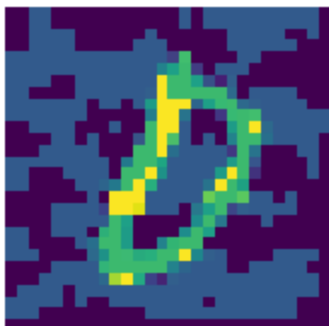
0 -> 9



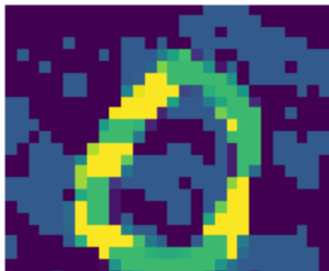
0 -> 6



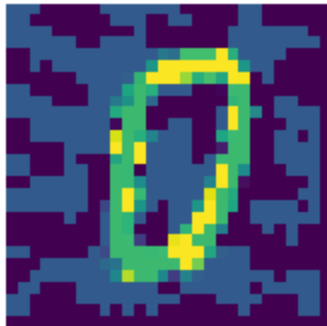
0 -> 8



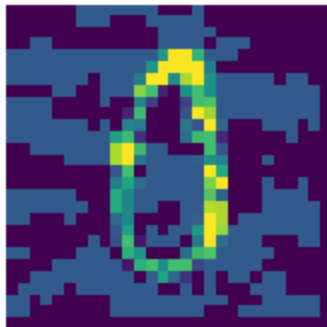
0 -> 9



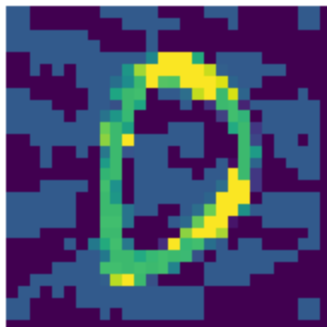
0 -> 2



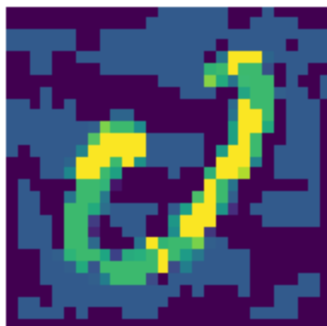
0 -> 1



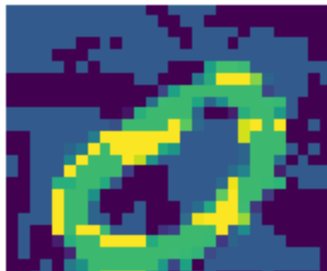
0 -> 2



0 -> 2

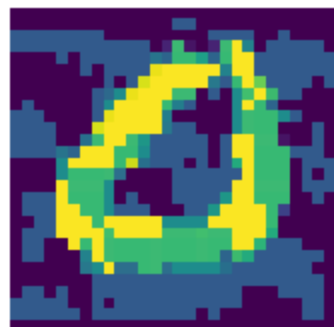


0 -> 2

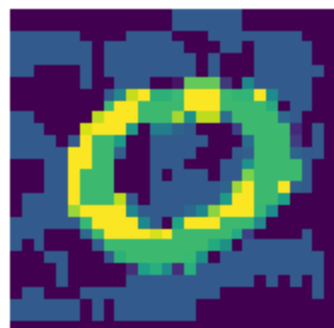




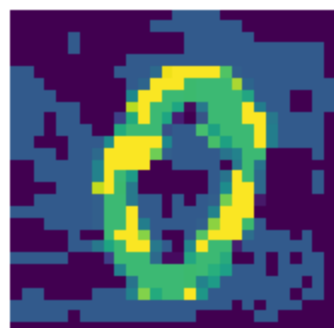
0 -> 9



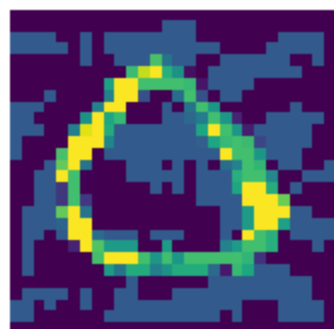
0 -> 9



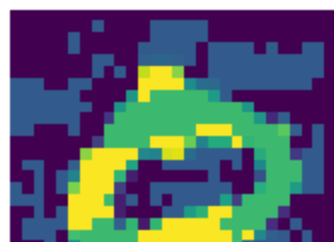
0 -> 7



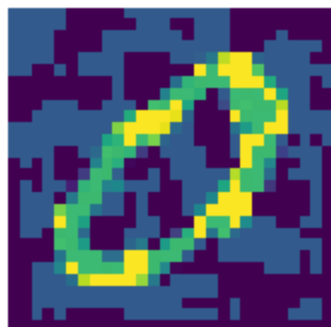
0 -> 9



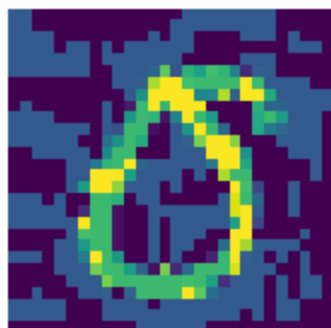
0 -> 6



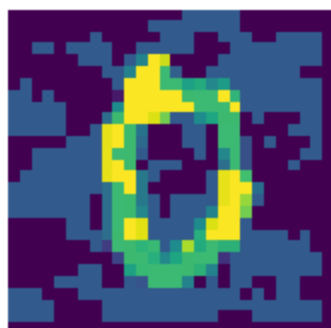
0 -> 2



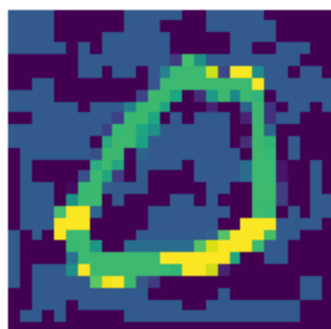
0 -> 8



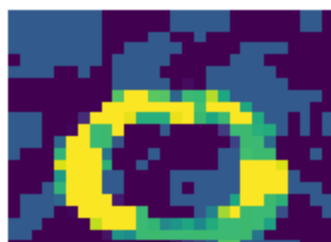
0 -> 7



0 -> 2

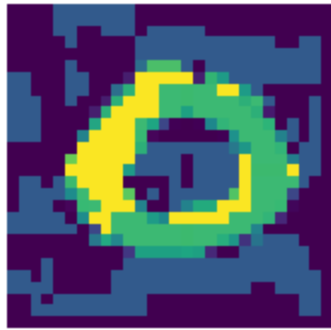


0 -> 9

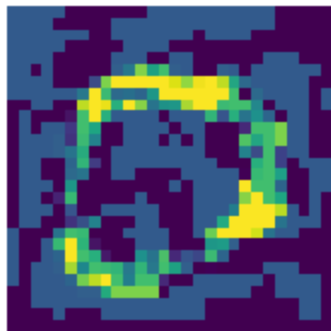




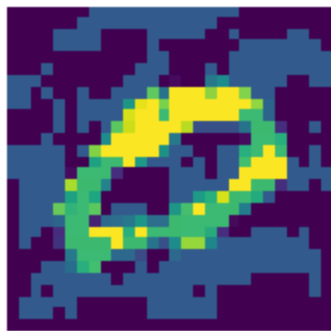
0 -> 9



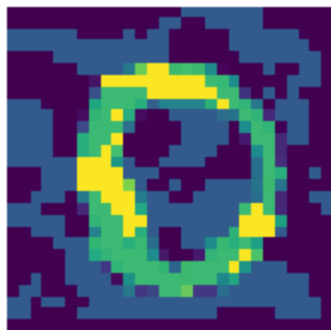
0 -> 2



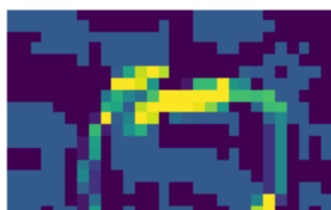
0 -> 7



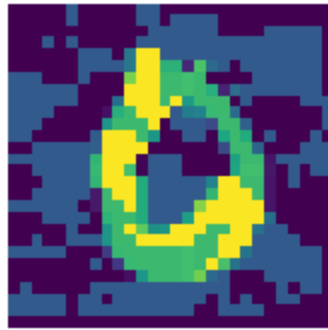
0 -> 8



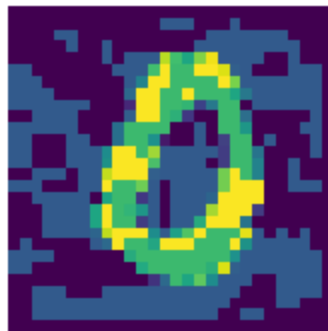
0 -> 5



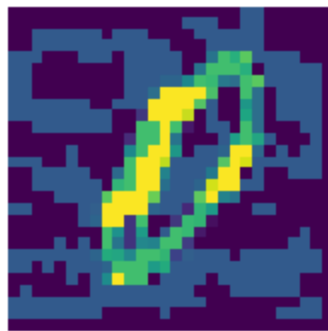
0 -> 6



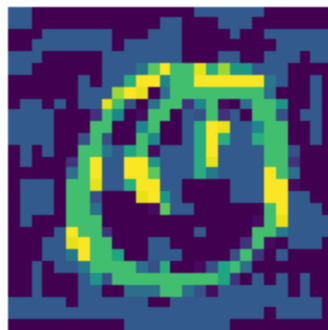
0 -> 9



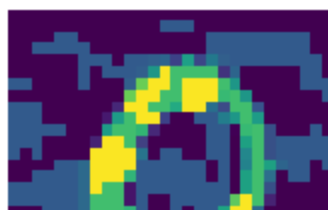
0 -> 8



0 -> 8

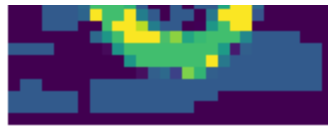


0 -> 9

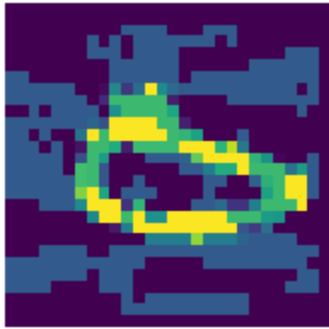




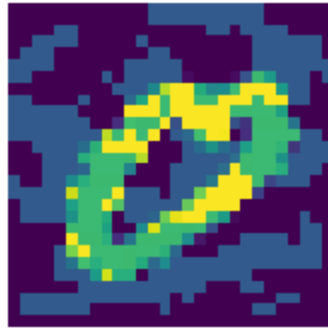
0 -> 5



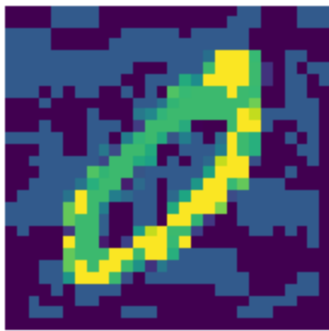
0 -> 7



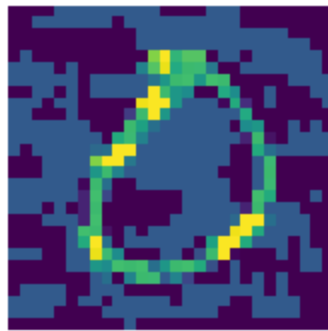
0 -> 2



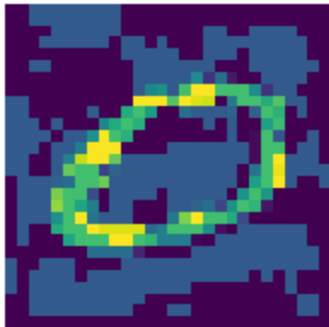
0 -> 1



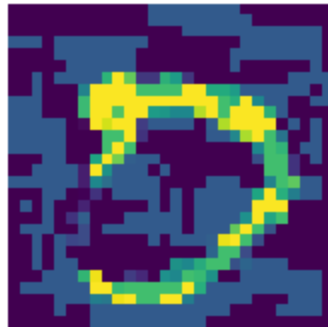
0 -> 9



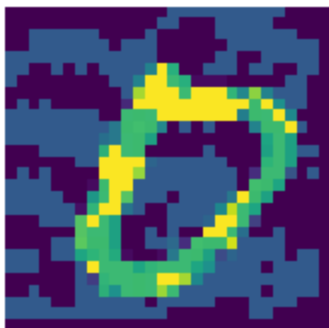
0 -> 7



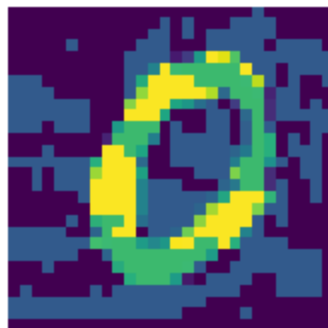
0 -> 8



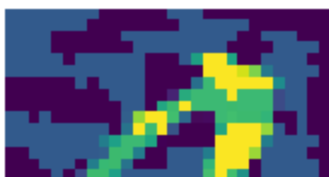
0 -> 6

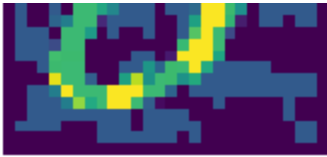


0 -> 2

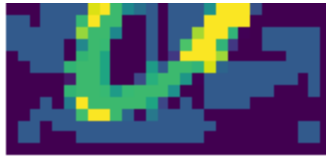


0 -> 7

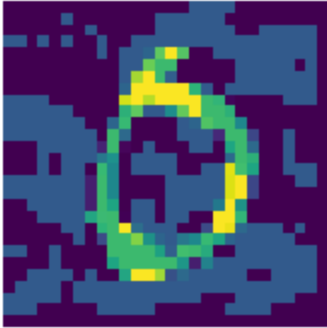




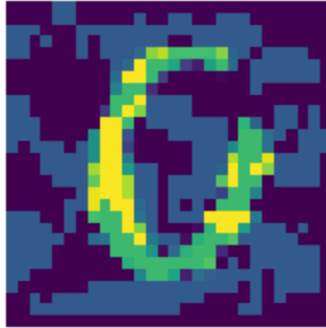
0 -> 5



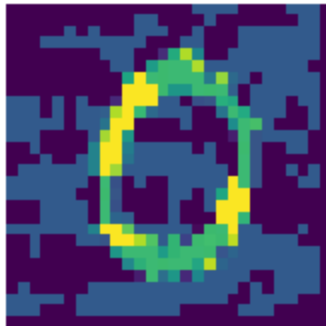
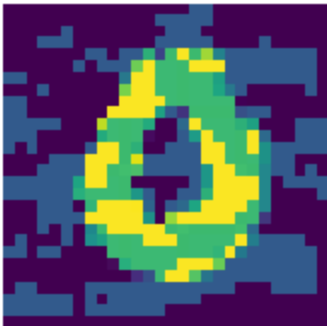
0 -> 6



0 -> 9



0 -> 9



No misclassified images for stage: w/ Defense Attack

Attack: fgsm_cw_attack

Dataset: MNIST

Training Epochs: 10

Retrained Clean and Adversarial Images: 124

Test Images: 140

Accuracy: 1.00

Precision: 1.00

Recall: 1.00

F1-score: 1.00

ROC AUC score is not defined for a single class.