

Metric	Clean	No Defense Attack	w/ Defense Attack
Loss	0.00453	0.374	0.00453
Accuracy	100%	88%	100%

Example Misclassifications:

```

-----
No misclassified images for stage: Clean
Attack: cw_pgd_attack
Dataset: EMNIST
Training Epochs: 10
Trained Clean Images: 64
Test Images: 625
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: 8
Attack: cw_pgd_attack
Dataset: EMNIST
Training Epochs: 10
Adversarial Training Images: 60
Test Images: 625
Accuracy: 0.88
Precision: 0.99
Recall: 0.88
F1-score: 0.93
ROC AUC Score: 1.00
-----

```

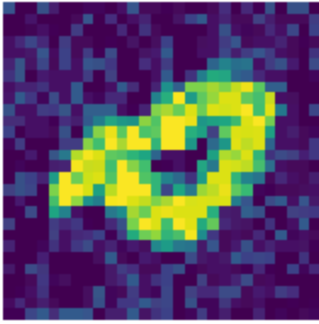
Misclassifications:

```

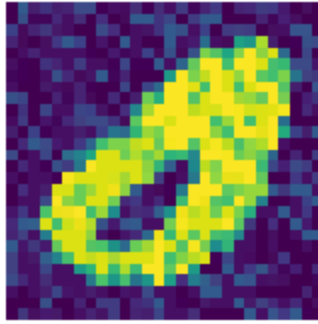
0 -> 8: 4
0 -> 6: 3
0 -> 4: 1

```

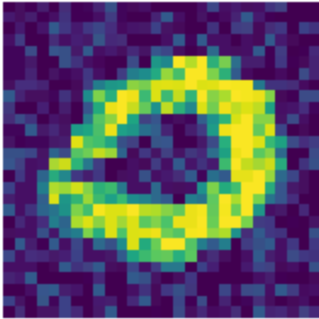
0 -> 8



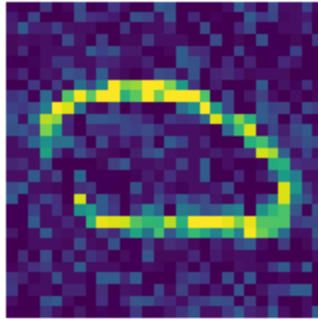
0 -> 6



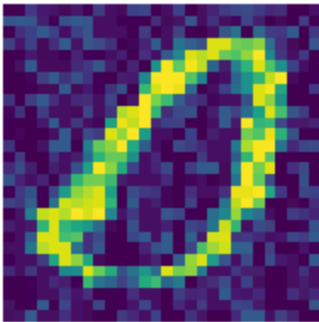
0 -> 4



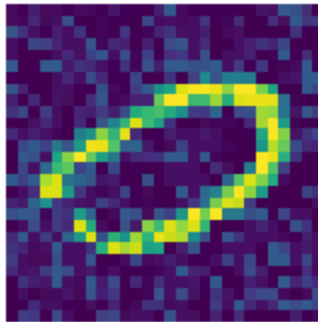
0 -> 8



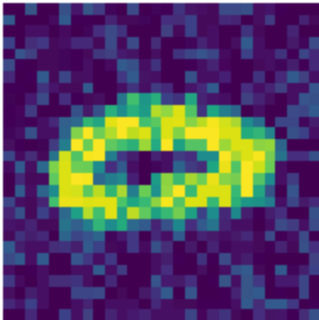
0 -> 6



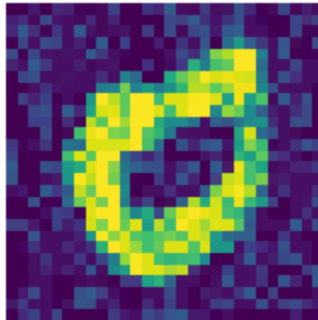
0 -> 6



0 -> 8



0 -> 8



No misclassified images for stage: w/ Defense Attack

Attack: cw_pgd_attack

Dataset: EMNIST

Training Epochs: 10

Retrained Clean and Adversarial Images: 124

Test Images: 625

Accuracy: 1.00

Precision: 1.00

Recall: 1.00

F1-score: 1.00

ROC AUC score is not defined for a single class.
