

Metric	Clean	No Defense Attack	w/ Defense Attack
Loss	0.00164	4.33	0.00218
Accuracy	100%	12%	100%

#### Example Misclassifications:

```

-----
No misclassified images for stage: Clean
Attack: fgsm_cw_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: 56
Attack: fgsm_cw_attack
Dataset: EMNIST
Training Epochs: 10
Adversarial Training Images: 60
Test Images: 625
Accuracy: 0.12
Precision: 0.58
Recall: 0.14
F1-score: 0.22
ROC AUC Score: 1.00
-----

```

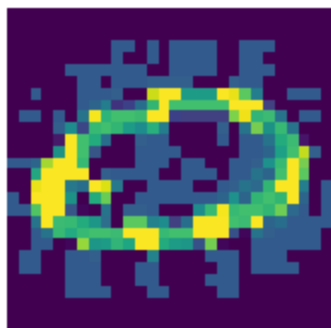
#### Misclassifications:

```

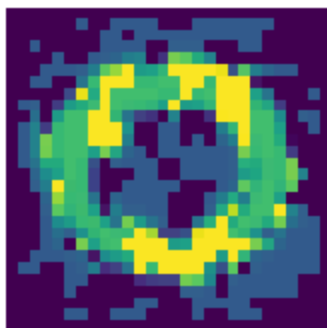
0 -> 8: 3
0 -> 9: 8
0 -> 2: 23
0 -> 6: 15
0 -> 7: 2
0 -> 5: 2
0 -> 3: 1
0 -> 4: 2

```

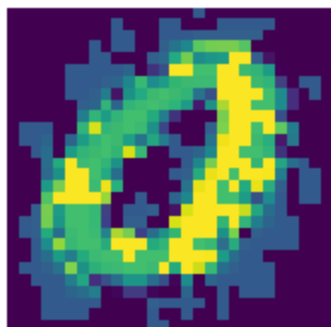
0 -&gt; 8



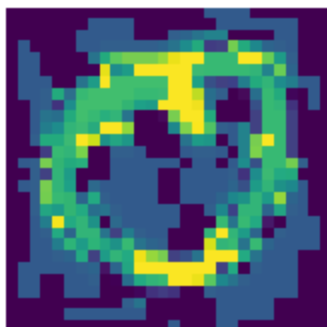
0 -&gt; 9



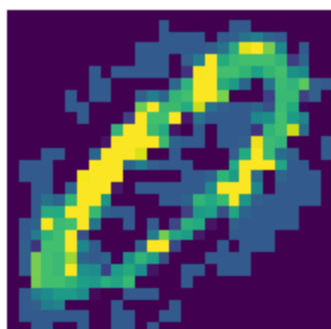
0 -&gt; 2



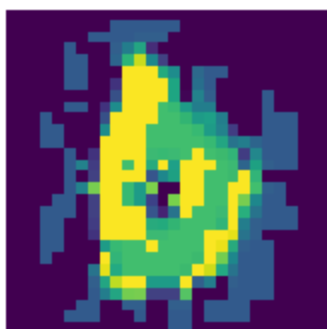
0 -&gt; 9



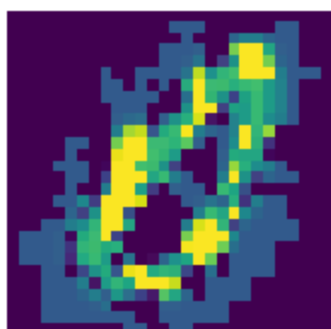
0 -&gt; 6



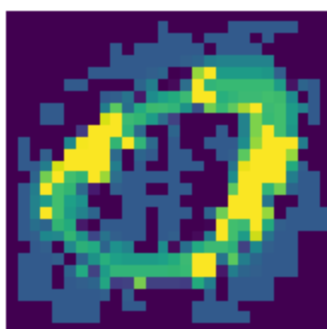
0 -&gt; 7



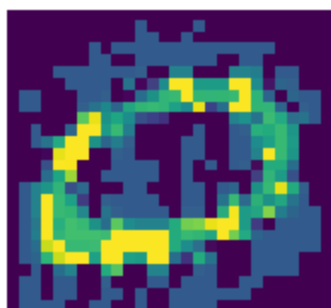
0 -&gt; 2



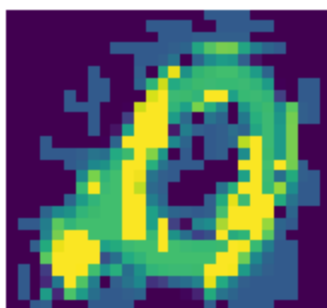
0 -&gt; 2



0 -&gt; 9

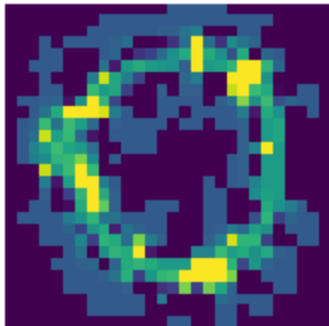


0 -&gt; 6

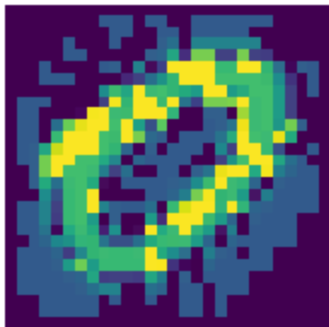




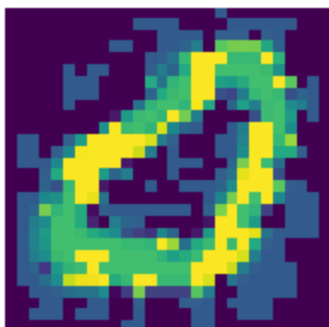
0 -&gt; 5



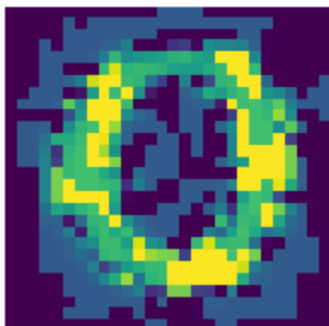
0 -&gt; 6



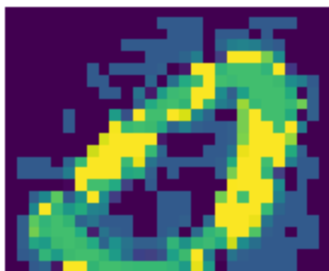
0 -&gt; 2



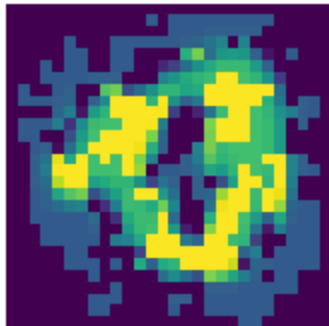
0 -&gt; 2



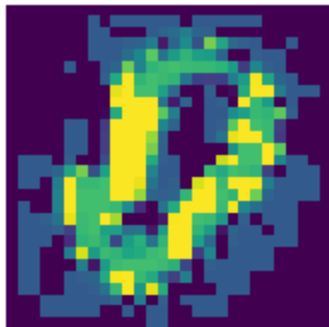
0 -&gt; 2



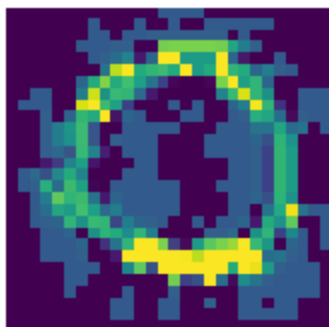
0 -&gt; 6



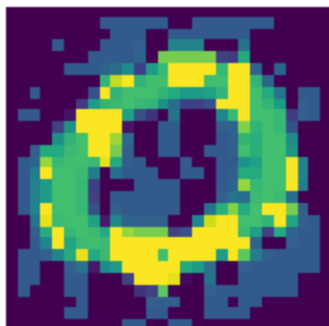
0 -&gt; 2



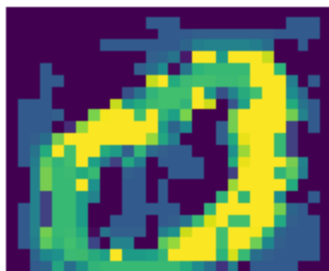
0 -&gt; 9



0 -&gt; 9

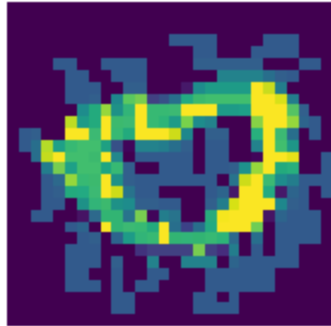


0 -&gt; 2

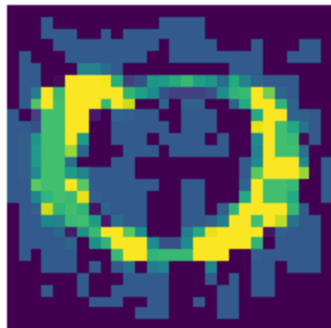




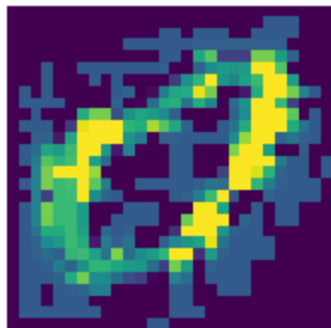
0 -&gt; 2



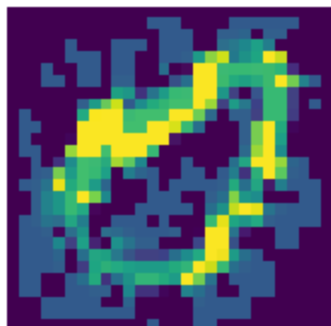
0 -&gt; 2



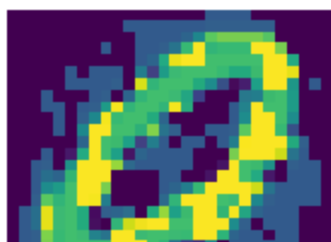
0 -&gt; 2



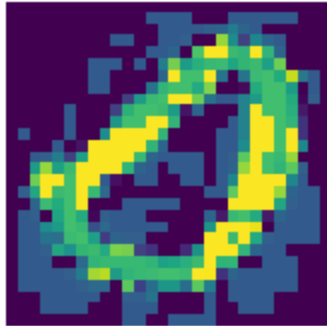
0 -&gt; 2



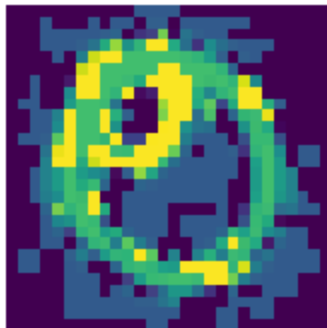
0 -&gt; 2



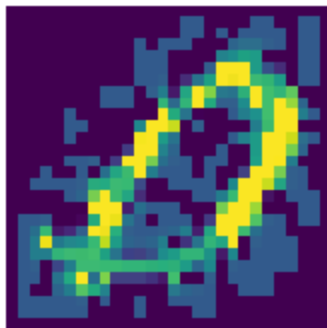
0 -&gt; 2



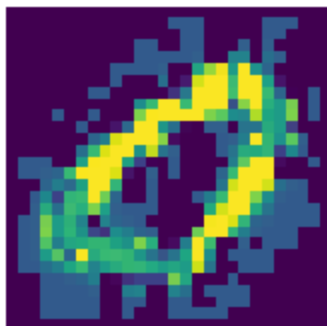
0 -&gt; 8



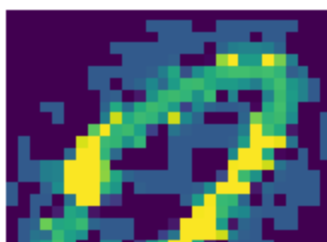
0 -&gt; 6



0 -&gt; 6

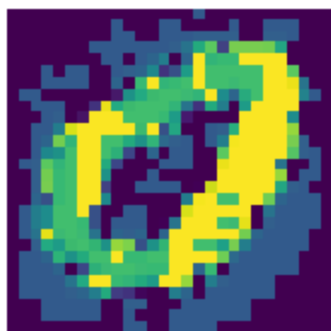


0 -&gt; 2

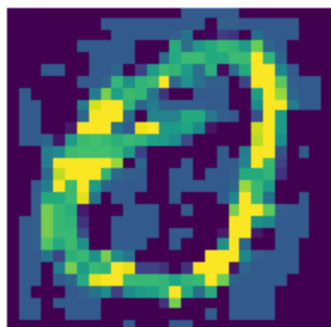




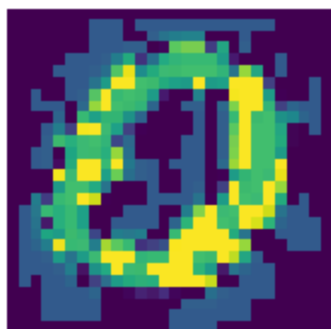
0 -&gt; 2



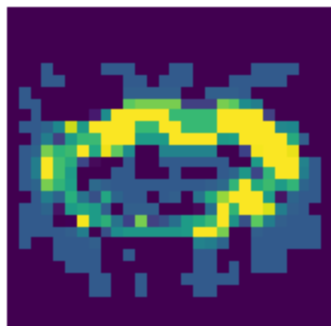
0 -&gt; 2



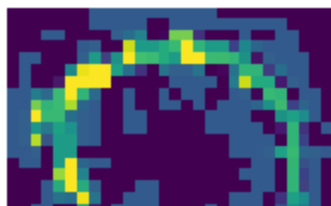
0 -&gt; 9



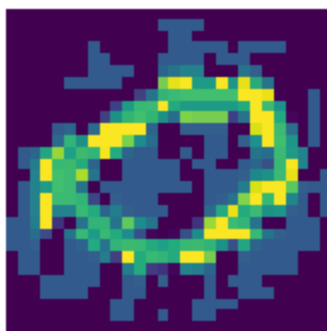
0 -&gt; 6



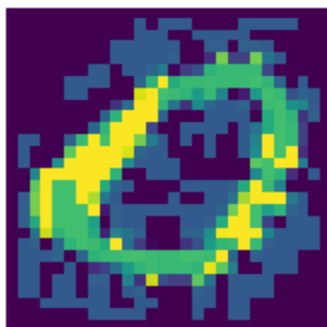
0 -&gt; 5



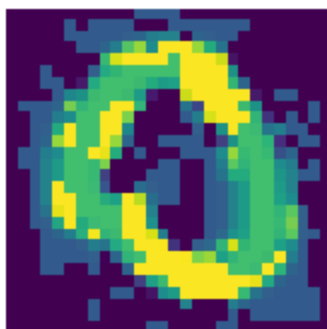
0 -&gt; 6



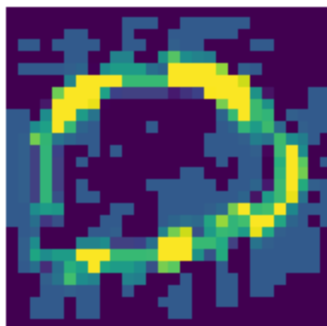
0 -&gt; 2



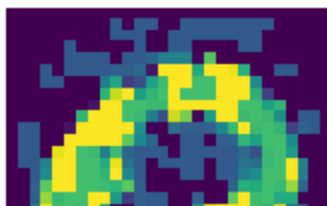
0 -&gt; 3

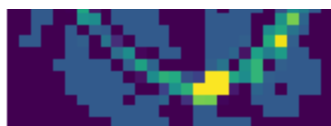


0 -&gt; 4



0 -&gt; 9





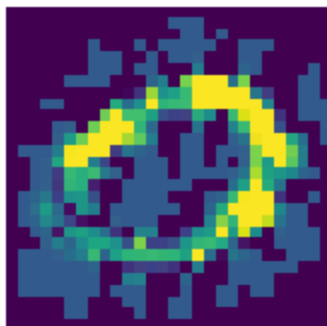
0 -&gt; 6



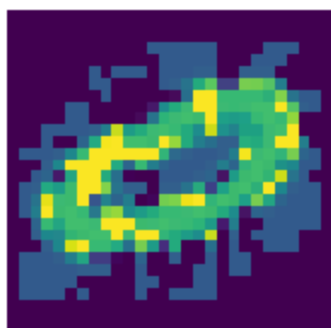
0 -&gt; 6



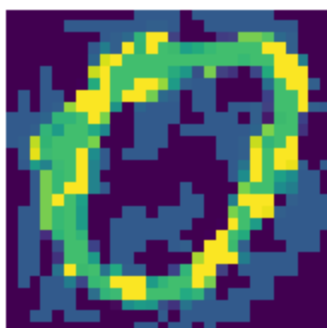
0 -&gt; 8



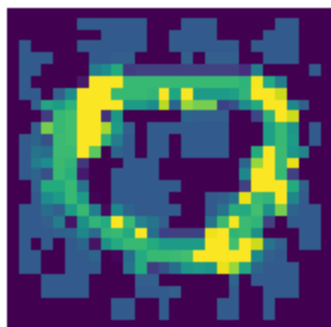
0 -&gt; 2



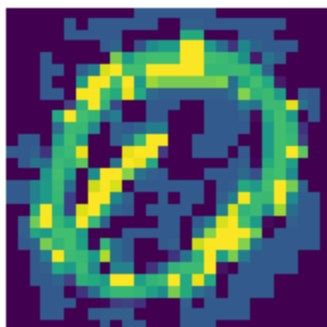
0 -&gt; 2



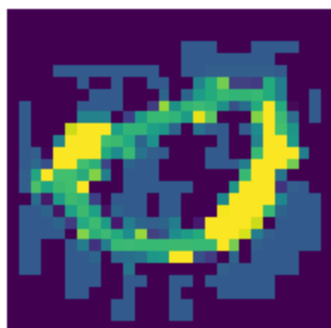
0 -&gt; 9



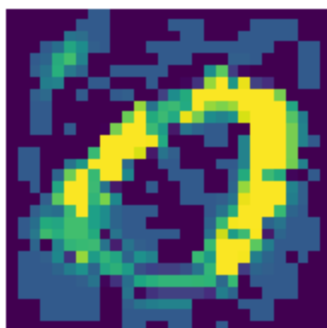
0 -&gt; 2



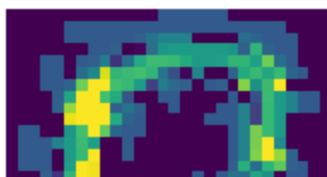
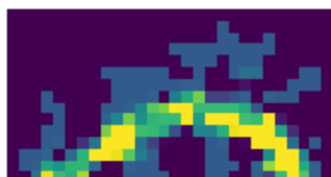
0 -&gt; 6

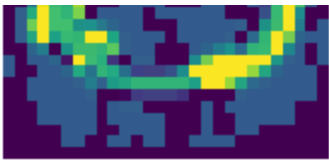


0 -&gt; 6

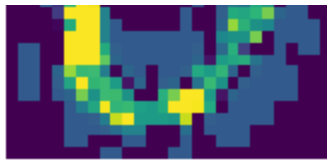


0 -&gt; 7

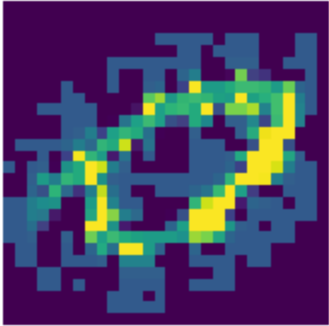




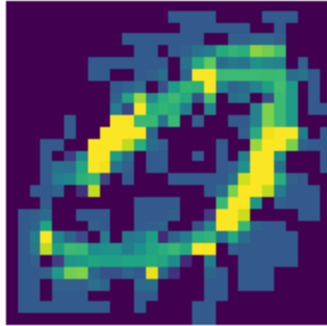
0 -&gt; 6



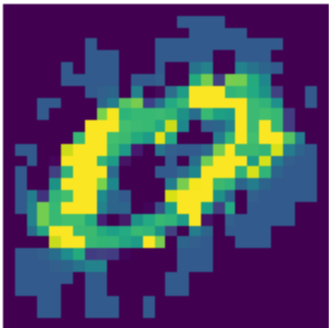
0 -&gt; 2



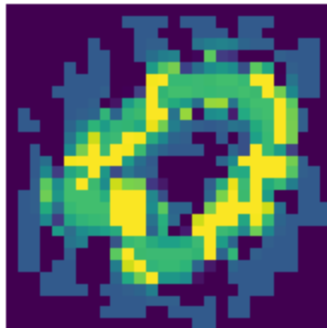
0 -&gt; 2



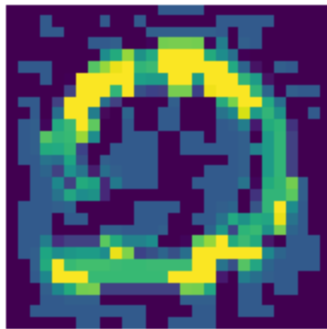
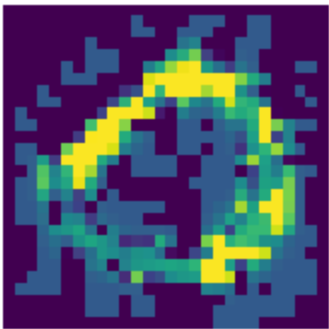
0 -&gt; 6



0 -&gt; 6



0 -&gt; 4



-----  
No misclassified images for stage: w/ Defense Attack

Attack: fgsm\_cw\_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.