Defense Implemented: Randomization

Randomization Approach: Random Cropping

```
+----------+---------+--------------------+--------------------+
| Metric   | Clean   | No Defense Attack   | w/ Defense Attack   |
+==========+=========+====================+====================+
| Loss     | 0.00383 | 5.17               | 4.37e-05           |
+----------+---------+--------------------+--------------------+
| Accuracy | 100%    | 14%                | 100%               |
+----------+---------+--------------------+--------------------+
```

Example Misclassifications:

No misclassified images for stage: Clean
Attack: fgsm_cw_attack
Dataset: MNIST
Training Epochs: 10
Trained Clean Images: 54210
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: 55
Attack: fgsm_cw_attack
Dataset: MNIST
Training Epochs: 10
Adversarial Training Images: 27105
Test Images: 140
Accuracy: 0.14
Precision: 0.26
Recall: 0.22
F1-score: 0.24
ROC AUC Score: 1.00

Misclassifications:
0 -> 8: 6
0 -> 6: 10
0 -> 5: 11
0 -> 9: 10
0 -> 2: 14
0 -> 4: 2
0 -> 7: 2

No misclassified images for stage: w/ Defense Attack
Attack: fgsm_cw_attack
Dataset: MNIST
Training Epochs: 10
Retrained Clean and Adversarial Images: 81315
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.