```
Defense Implemented: Randomization

Randomization Approach: Combined Randomization

+----------+---------+---------------------+---------------------+
| Metric   | Clean   | No Defense Attack   | w/ Defense Attack   |
+==========+=========+=====================+=====================+
| Loss     | 0.00883 | 4.87                | 0.00229             |
+----------+---------+---------------------+---------------------+
| Accuracy | 100%    | 6%                  | 100%                |
+----------+---------+---------------------+---------------------+

Example Misclassifications:

--------------------------------------------------------
No misclassified images for stage: Clean
Attack: fgsm_pgd_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: 60
Attack: fgsm_pgd_attack
Dataset: MNIST
Training Epochs: 10
Adversarial Training Images: 27105
Test Images: 140
Accuracy: 0.06
Precision: 0.12
Recall: 0.10
F1-score: 0.11
ROC AUC Score: 1.00
--------------------------------------------------------

Misclassifications:
0 -> 7: 5
0 -> 2: 17
0 -> 5: 3
0 -> 6: 20
0 -> 4: 2
0 -> 9: 11
0 -> 8: 2

--------------------------------------------------------
```

```
No misclassified images for stage: w/ Defense Attack
Attack: fgsm_pgd_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.
---------------------------------------------------------
```