

Defense Implemented: Randomization

Randomization Approach: Random Resizing

Metric	Clean	No Defense Attack	w/ Defense Attack
Loss	0.00105	3.76	0.000564
Accuracy	100%	14%	100%

Example Misclassifications:

No misclassified images for stage: Clean
Attack: fgsm_bim_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_bim_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 -> 3: 3
- 0 -> 2: 16
- 0 -> 5: 11
- 0 -> 6: 12
- 0 -> 9: 7
- 0 -> 8: 4
- 0 -> 4: 2

No misclassified images for stage: w/ Defense Attack

Attack: fgsm_bim_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.
