

Adversarial MRI Defense System Report

MRI Adversarial Attack Classification Report

Generated on: 2025-04-19 19:18:03

Image: fgsm_fgsm_2a9db457-d9ae-4597-bc87-d33db757e7e4_mri_healthy_6.jpg

Original Image

Error adding image: '_io.BytesIO' object has no attribute 'startswith'

Classification Results

Predicted Class: PGD

Confidence Scores:

Clean	0.00%
FGSM	0.16%
BIM	19.50%
PGD	80.34%

Error adding image: '_io.BytesIO' object has no attribute 'startswith'

Interpretation:

The image shows signs of Projected Gradient Descent attack, which is an iterative attack with random initialization that typically creates stronger adversarial examples.

Recommendations:

Consider running the image through our purification system to remove adversarial perturbations.