Point of Image Fragmentation: The attack with tuned parameters s.t. the image retains as much of the perceptible image data while minimizing accuracy. Must be evaluated manually by humans as “perception” can not be automated.

Accuracy at Point of Image Fragmentation

	Clean	FGSM	PGD	DeepFool	CW	JSMA	Square
MNIST	99.52%	91.00%	2.34%	0.0%	0%	0.39%	59.38%
CIFAR10	75.71%	3.10%	4.30%	0.0%	6.25%	0.0%	47.65%
SVHN	93.20%	22.65%	16.02%	0.0%	1.95%	0.0%	26.95%

Tuned Parameters

MNIST:
FGSM - [epsilon = 0.05]
DeepFool - [overshoot =0.02, max_iterations=50]
PGD - [epsilon = 0.25, alpha = 0.1]
JSMA - [theta = 0.1]
CW - [alpha = 0.01, kappa = 0, c=0.75]
Square - [epsilon:]

CIFAR10:
FGSM - [epsilon = 0.025]
DeepFool - [overshoot =0.02, max_iterations=50]
PGD - [epsilon = 0.25, alpha = 0.00625]
JSMA - [theta = 0.000625]
CW - [alpha = 0.01, kappa = 0, c= 0.65]

SVHN:
FGSM - [epsilon = 0.025]
DeepFool - [overshoot =0.02, max_iterations=50]
PGD - [epsilon = 0.25, alpha = 0.00625]
JSMA - [theta = 0.0025]
CW - [alpha = 0.01, kappa = 0, c=0.75]

Accuracy of Robust Models (Same Parameters)

FGSM:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
FGSM Augmented MNIST	99.46%	90.63%	7.03%	0.0%	0.0%	0.0%
FGSM Augmented CIFAR10	76.19%	3.51%	6.25%	0.0%	7.34%	0.0%
FGSM Augmented SVHN	92.87%	24.6%	20.70%	0.0%	1.94%	0.39%

Deepfool:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
Deepfool Augmented MNIST	99.53%	89.06%	7.03%	0.0%	2.88%	0.0%
Deepfool Augmented CIFAR10	76.67%	3.13%	4.69%	0.0%	2.88%	0.0%
Deepfool Augmented SVHN	93.06%	23.44%	20.31%	0.0%	1.94%	0.39%

PGD:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
PGD Augmented MNIST	99.51%	89.06%	7.81%	0.0%	5.60%	0.0%
PGD Augmented CIFAR10	75.99%	3.91%	7.42%	0.0%	4.71%	0.39%
PGD Augmented SVHN	92.93%	30.47%	20.31%	0.0%	1.94%	0.39%

JSMA

	Clean	FGSM	PGD	DeepFool	CW	JSMA
JSMA Augmented MNIST	99.44%	91.80%	11.33%	0.0%	0.0%	0.39%
JSMA Augmented CIFAR10	75.59%	3.51%	5.47%	0.0%	4.71%	0.39%
JSMA Augmented SVHN	93.04%	26.56%	21.88%	0.0%	0.98%	0.39%

CW:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
CW Augmented MNIST	99.51%	90.23%	6.25%	0.0%	0.0%	0.0%
CW Augmented CIFAR10	76.56%	3.91%	6.25%	0.0%	4.71%	0.0%
CW Augmented SVHN	92.93%	23.44%	19.92%	0.0%	1.94%	0.0%

Fully Augmented:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
Fully Augmented MNIST	99.44%	92.58%	13.28%	0.0%	6.48%	0.0%
Fully Augmented CIFAR10	76.45%	3.51%	5.86%	0.0%	4.71%	0.0%
Fully Augmented SVHN	92.48%	24.21%	19.53%	0.0%	4.71%	1.17%

Example Table:

	Clean	FGSM	PGD	DeepFool	CW	JSMA
____ Augmented MNIST	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
____ Augmented CIFAR10	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
____ Augmented SVHN	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%