

FS - Feature Squeezing					
TVM = Total Variance Minimization					
SS = Spatial Smoothing					
GA = Gaussian Augmentation					
Model:					
Inception V3	Attack:	No Defense:	TVM + SS	FS + TVM + SS	
	No Attack	97.49%	97.49%	97.49%	
	FGSM(eps=0.1)				
	FGSM(eps=0.3)				
	FGSM(eps=0.4)	93.11%	92.28%	92.28%	
	BIM(eps=0.4)	45.51%	90.61%	91.23%	
	PGD(eps=0.3. eps_step=0.1)	56.16%	91.02%	90.81%	
	C&W				
Squeezenet 1_1	Attack:	No Defense:	TVM + SS	FS + TVM + SS	
	No Attack	95.62%	95.62%	95.62%	
	FGSM(eps=0.1)	93.32%			
	FGSM(eps=0.3)	89.98%			
	FGSM(eps=0.4)	87.47%	87.06%	87.06%	
	BIM(eps=0.4)	53.24%	86.43%	86.64%	
	PGD(eps=0.3. eps_step=0.1)	59.50%	86.85%	86.85%	
	C&W				
Efficientnet	Attack:	No Defense:	TVM + SS	FS + TVM + SS	
	No Attack	95.41%	95.41%	95.41%	
	FGSM(eps=0.1)	93.11%			
	FGSM(eps=0.3)	92.28%			
	FGSM(eps=0.4)	91.86%	92.07%	92.07%	
	BIM(eps=0.4)	38.41%	89.35%	89.35%	

	PGD(eps=0.3. eps_step=0.1)	50.10%	90.19%	89.77%	
	C&W				
Resnet18 (Omar's Model)	Attack:	No Defense:	TVM + SS	FS + TVM + SS	
	No Attack	94.99%	94.99%	94.99%	
	FGSM(eps=0.1)				
	FGSM(eps=0.3)				
	FGSM(eps=0.4)	86.43%	86.22%	86.01%	
	BIM(eps=0.4)	38.83%	83.30%	83.09%	
	PGD(eps=0.3. eps_step=0.1)	49.27%	84.55%	84.34%	
	C&W				

	My Defenses	1. TVM(w/CG)							
		2. TVM+SS+GA							
TV - Total Variance Minimization									
FS - Feature Squeezing									
SS - Spatial Smoothing									
JC - JPEG Compression									
TVM= Total Variance Minimization, SS - Spatial Smoothing, JC - JPEG Compression, GA - Gaussian Augmentation							FS = Feature Squeezing		
Model:									
ResNet18	Attack	No Defense:	TVM(CG solver used)	TVM+SS	TVM + SS + GA	TVM + GA	TVM+GA+SS	TVM+SS+GA+JC	SS+TVM
	No Attack	96.24%	96.24%	96.24%	96.24%				
	FGSM(eps=0.2)	67.22%	82.88%	86.22%					
	FGSM(eps=0.3)								
	FGSM(eps=0.4)								
	BIM(eps=0.4)	51.14%	90.81%	89.77%	81.62%				89.35%
	PGD(eps=0.3, eps=0.1)	50.10%	91.65%	90.19%	79.96%		79.96%	80.17%	
	C&W	2.07%							
InceptionV3(Lex')	Attack	No Defense:	TVM(CG enabled)	TVM+SS	TVM+SS+GA				
	No Attack	97.49%	97.49%	97.49%	97.49%				
	FGSM(eps=0.2)								
	FGSM(eps=0.3)								
	FGSM(eps=0.4)								
	BIM(eps=0.4)	88.52%	91.23%	91.65%	90.605			80.17%	
	PGD(eps=0.3, eps=0.1)	54.49%	93.32%	92.69%	84.55%	84.34%	84.55%	83.51%	
	C&W								