

No	Defence
1	Mask Gradient [MaskedGradient]
2	JPEG Compression* [das2018shield]
3	Randomisation[croce2021mind]
4	Mustafa, Super-Resolution
5	Image Denoising [Mustafa`2020]
6	One Hot [buckman2018thermometer]
7	Data Sanitizing [Cretu2008] *
8	High dimensional robust estimation[diakonikolas2019sever]
9	Regularization[brendel2018decisionbased]
10	PixelDefend, Defensive Distillation
11	Gradient Masking [boenisch2021gradient]
12	VectorDefence [kabilan2018vectordefense]
13	Stochastic Elements [brendel2018decisionbased]
14	RobustScaling [Image-Scaling29]
15	Logit Squeezing* [shafahi2019label]
16	Super resolution [Mustafa`2020]
17	Image Denoising [fan2019brief]
18	Thermometer Encoding [buckman2018thermometer]
19	BAT [worzyk2021broad]
20	Data Augmentation[shorten2019survey]
21	Data Sanitizing[Cretu2008]
22	Adversarial Training*[chakraborty2018adversarial]
23	Pixel Defend[song2018pixeldefend]
24	Defensive Distillation[carlini2016defensive]
25	Regularization[jakubovitz2018improving]
26	Filter (Gaussian, AVerage, Median)[yu2020attention]
27	PGD-AdvT[madry2017towards]
28	Ensemble-AdvT[Tramer-2017]
29	PAT[laidlaw2021perceptual]
30	Vector Defence[kabilan2018vectordefense]
31	Mustafa[Mustafa`2020]
32	BAT [worzyk2021broad]
33	Data Sanitizing [Cretu2008]
34	Augmented Adv Training [brendel2018decisionbased]
35	Augmented Adv Training [brendel2018decisionbased]
36	JPEG Compression [JPEG-Compression-aydemir2018effects]
37	Augmented Adv Training [brendel2018decisionbased]
38	Guided Denoiser[cheng2019improving]
39	Stochastic Element [dhillon2018stochastic],
40	Adversarial Training[chakraborty2018adversarial]
41	Adversarial Purification[Yoon2021]
42	Shardped Edges [dhillon2018stochastic]
43	Adversarial Training[chakraborty2018adversarial]
44	Stochastic Element [dhillon2018stochastic], Shardped Edges [dhillon2018stochastic]
45	Stochastic Element [dhillon2018stochastic], Shardped Edges [dhillon2018stochastic]
46	Termometer Enconding[buckman2018thermometer]
47	JPEG Compression [das2018shield]
48	Adversarial Training[chakraborty2018adversarial]
49	BAT [worzyk2021broad]

50	Pixel Defend [shafahi2019label]
51	Certified Robustness [lecuyer2019certified]
52	DBSCAN Preprocessing Sanitizing [Crussell2015]
53	Preprocessing,
54	Image denoising
55	Certified Robustness
56	Non-convex Guarantee
57	Byzantine-Robust Distribution[pmlr-v97-yin19a]