

	CIFAR10		CIFAR100	
	ResNet18	WRN-3410	ResNet18	WRN-3410
Vanilla Training	≈ 15.3 s	≈ 90.2 s	≈ 15.7 s	≈ 101.3 s
Adversarial Training	≈ 108.6 s	≈ 1047.2 s	≈ 110.9 s	$1197.2 \approx$ s
MID [1]	2530 ± 10 s	-	3460 ± 20 s	-
NAT (ours)	≈ 129.8 s	≈ 1165.8 s	≈ 127.3 s	≈ 1328.2 s

References

[1] Zhang L, Zhou Y, Yang Y, et al. Meta invariance defense towards generalizable robustness to unknown adversarial attacks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2024.