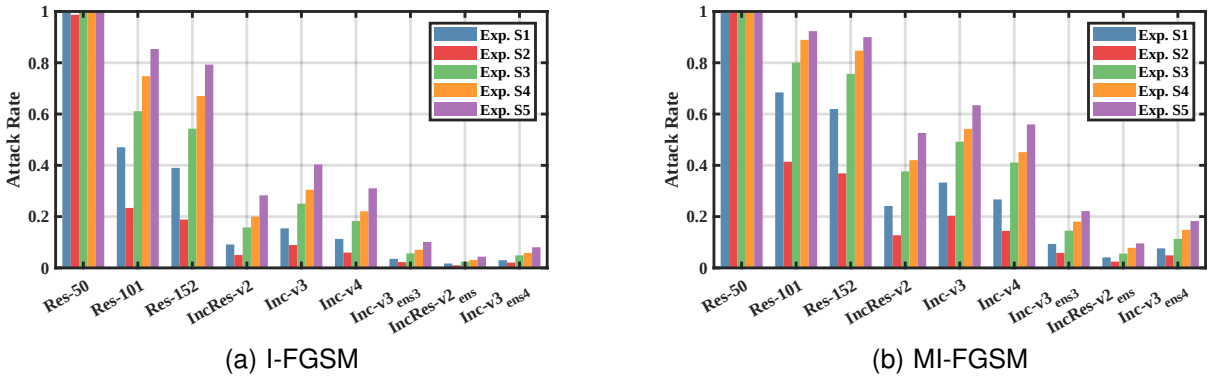
Supplementary material for "Learning Transferable Adversarial Examples via Ghost Networks"

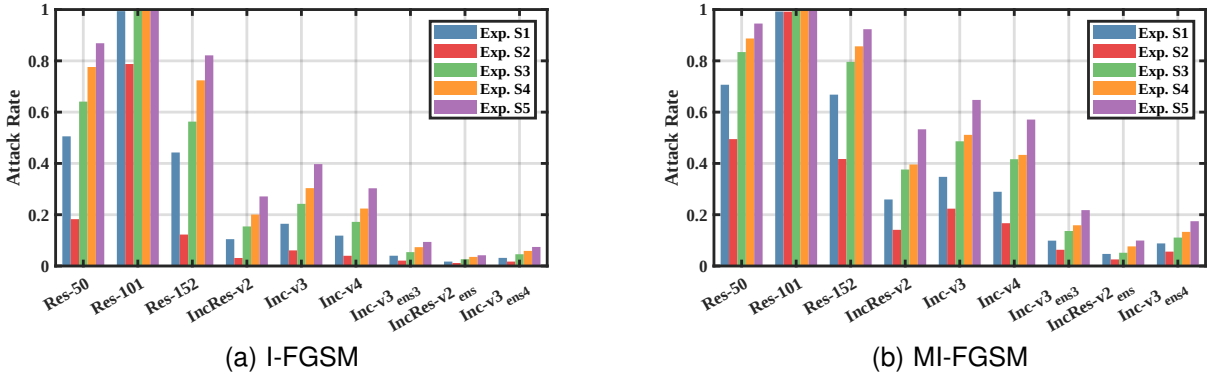
The document contains the supplementary materials for "Learning Transferable Adversarial Examples vis Ghost Networks". Due to the space limitation, the comparison of performance under the setting of single-model attack and multi-model attack has to be simplified in the main manuscript.

The goal of this document is to present a detailed comparison. Therefore, in Fig. 1, Fig. 2, Fig.3, Fig.4, Fig. 5 and Fig. 6, we present the comparison of attack rates of adversarial examples generated by a single base model (Res-50, Res-101, Res-152, IncRes-v2, Inc-v3 and Inc-v4 for each figure). Moreover, rather than reporting the average attack rate of multi-model attack, the attack rates for all nine models are reported in Table. 1.



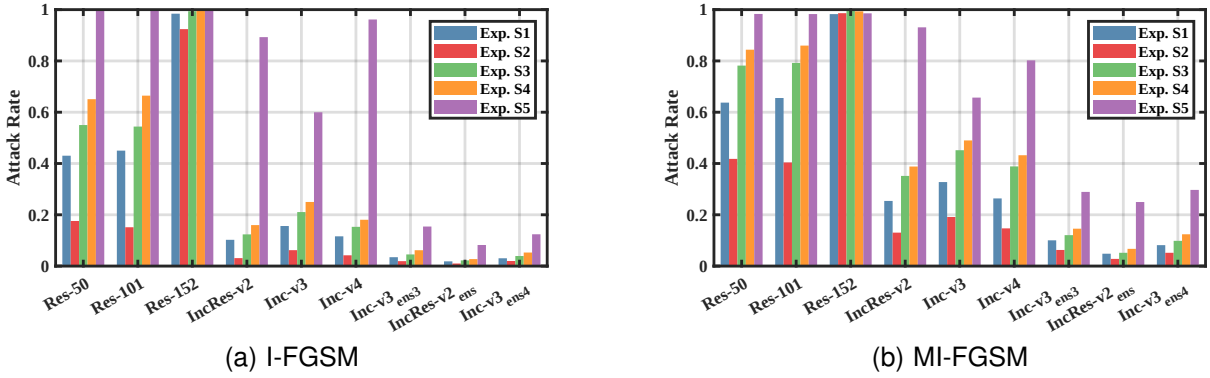
(a) I-FGSM (b) MI-FGSM

Figure 1: The attack rate comparison when attacking Res-50, and testing on all the base models.



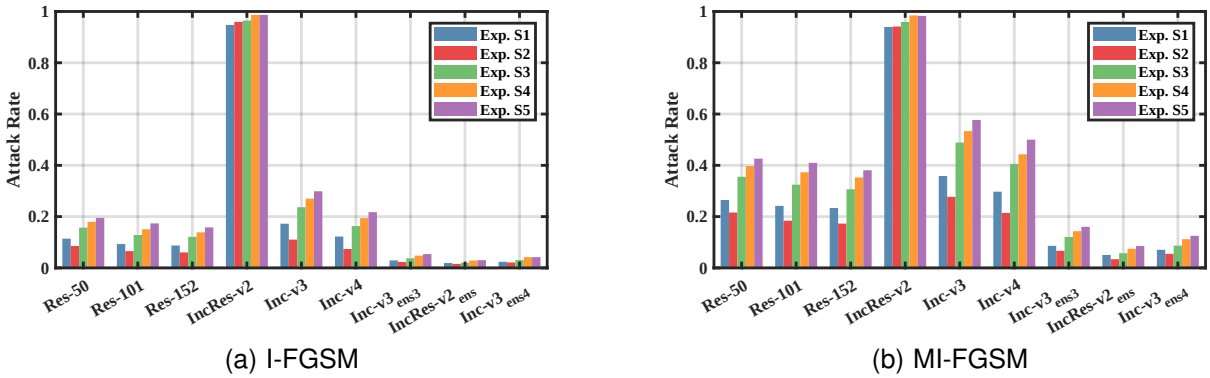
(a) I-FGSM (b) MI-FGSM

Figure 2: The attack rate comparison when attacking Res-101, and testing on all the base models.



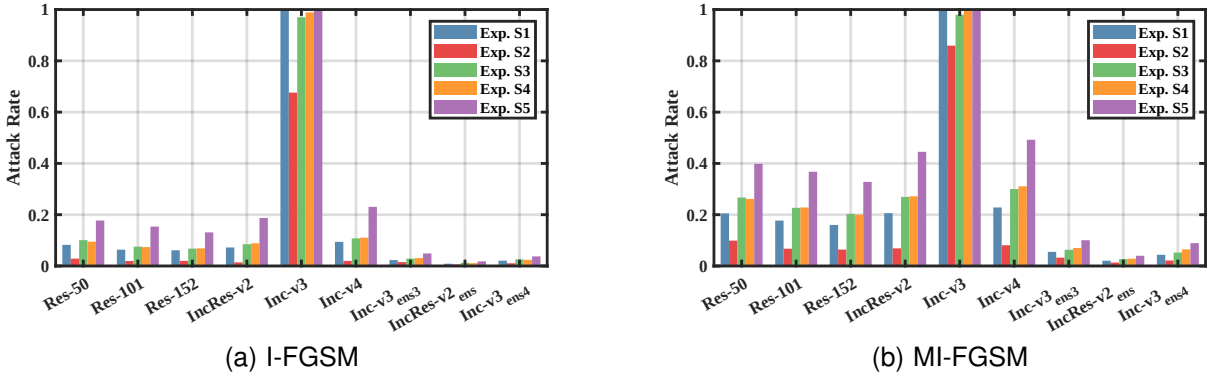
(a) I-FGSM (b) MI-FGSM

Figure 3: The attack rate comparison when attacking Res-152, and testing on all the base models.



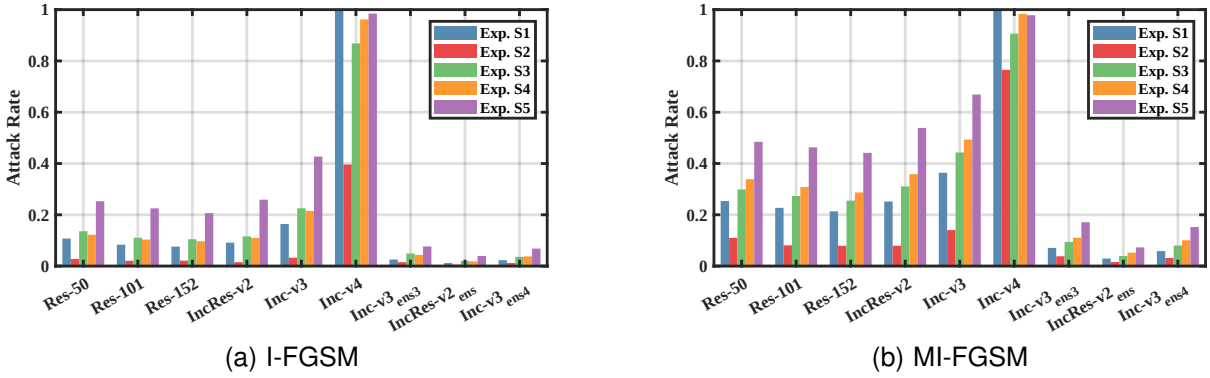
(a) I-FGSM (b) MI-FGSM

Figure 4: The attack rate comparison when attacking IncRes-v2, and testing on all the base models.



(a) I-FGSM (b) MI-FGSM

Figure 5: The attack rate comparison when attacking Inc-v3, and testing on all the base models.



(a) I-FGSM (b) MI-FGSM

Figure 6: The attack rate comparison when attacking Inc-v4 with, and testing on all the base models.

Attack	Methods	Res-50	Res-101	Res-152	IncRes-v2	Inc-v3	Inc-v4	Inc-v3$_{ens3}$	Inc-v3$_{ens4}$	IncRes-v2$_{ens}$
I-FGSM	Exp. M1	99.48	47.04	39.00	9.14	15.42	11.30	3.54	3.00	1.70
	Exp. M2	**99.90**	57.12	49.84	20.58	32.90	28.26	6.10	5.36	2.64
	Exp. M3	93.34	40.20	34.68	13.64	23.72	20.20	4.32	4.36	2.06
	Exp. M4	99.68	56.06	47.48	11.88	19.44	13.72	5.12	4.40	2.18
	Exp. M5	99.66	**76.22**	**69.34**	22.50	33.58	24.98	8.10	6.80	3.42
	Exp. M6	99.18	69.32	63.72	**31.82**	**45.96**	**41.14**	**8.26**	**7.36**	**3.52**
MI-FGSM	Exp. M1	99.38	68.44	61.96	24.12	33.28	26.70	9.34	7.62	4.10
	Exp. M2	**99.92**	73.76	68.50	42.88	53.90	50.44	14.18	11.44	6.44
	Exp. M3	98.08	63.72	57.68	33.74	46.62	42.14	11.00	9.42	4.72
	Exp. M4	99.62	69.04	62.30	23.58	33.86	25.70	9.60	7.72	3.66
	Exp. M5	99.66	**88.68**	**85.32**	46.90	59.06	50.76	**18.96**	**15.32**	8.08
	Exp. M6	99.30	82.36	78.86	**55.36**	**66.76**	**63.94**	18.54	**15.32**	**8.16**

Table 1: The comparison of attack rate (%) of multi-model attack, which is a detailed version of Table 2 in the main manuscript. We report the performance on the 9 base networks described in Sec. 4.1 of the main manuscript.