

AP(%)		Distance metric		
Attack method	Squeeze method	mAP	mIoU	wAP (ours)
C&W [1]	bit4	74.7	72.5	84.3
	bit5	75.3	82.4	86.8
	bit6	79.8	87.1	90.5
	bit7	80.3	88.1	90.8
DR [2]	bit4	81.5	92.6	95.4
	bit5	84.8	94.8	97.8
	bit6	86.7	95.8	98.5
	bit7	86.8	95.8	98.3
MI-FGSM [3]	bit4	77.5	89.7	93.6
	bit5	82.1	93.2	96.8
	bit6	84.4	94.8	98.2
	bit7	84.4	94.8	97.8
TI-DIM [4]	bit4	76.6	88.8	93.1
	bit5	81.7	92.9	96.5
	bit6	84.5	94.5	98.2
	bit7	84.6	94.5	97.7
DIM [5]	bit4	76.2	89.2	93.5
	bit5	80.9	92.9	96.7
	bit6	83.3	94.5	98.2
	bit7	83.4	94.5	97.8

Table 1. Using AP to evaluate the performance of different distance metric on bdd dataset in single frame setting.

1. REFERENCES

- [1] Nicholas Carlini and David Wagner, “Towards evaluating the robustness of neural networks,” in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 39–57.
- [2] Yantao Lu, Yunhan Jia, Jianyu Wang, Bai Li, Weiheng Chai, Lawrence Carin, and Senem Velipasalar, “Enhancing cross-task black-box transferability of adversarial examples with dispersion reduction,” *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 940–949, 2020.
- [3] Yinpeng Dong, Fangzhou Liao, Tianyu Pang, Xiaolin Hu, and Jun Zhu, “Discovering adversarial examples with momentum,” *CoRR, abs/1710.06081*, 2017, 2017.
- [4] Yinpeng Dong, Tianyu Pang, Hang Su, and Jun Zhu, “Evading defenses to transferable adversarial examples by translation-invariant attacks,” *arXiv preprint arXiv:1904.02884*, 2019.
- [5] Cihang Xie, Zhishuai Zhang, Jianyu Wang, Yuyin Zhou, Zhou Ren, and Alan Yuille, “Improving transferability of adversarial examples with input diversity,” *arXiv preprint arXiv:1803.06978*, 2018.