

Supplementary Materials: Cascaded Adversarial Attack: Simultaneously Fooling Rain Removal and Semantic Segmentation Networks

Anonymous Authors

Algorithm 1: Cascaded Adversarial Attack from Rain to Task and Cascaded Adversarial Attack from Task to Rain

Input: rainy image X_{rain} , clean image X_{clean} , deraining network f_{rain} , semantic segmentation network f_{task} , iterations T_{RRA} and T_{TA} , y is the ground label of the semantic segmentation task, perturbation bound ϵ , step size α , binary rain mask $Mask$

Output: adversarial example \hat{X}_{rain}

```

1 sample  $\delta_{RRA}$  from  $U(-\epsilon, \epsilon)$ ,  $\delta_{TA} \leftarrow 0$ ;
2 if attack is 'CAA-RT' then
3   for  $i = 1$  to  $T_{RRA}$  do
4     Calculate  $\mathcal{L}_{RRA}$  using Equation (6);
5      $\delta_{RRA} \leftarrow Proj(\delta_{RRA} - \alpha \text{sgn}(\nabla_{\delta_{RRA}} \mathcal{L}_{RRA}(X_{rain}, \delta_{RRA})))$ ;
6      $\delta_{RRA} \leftarrow \delta_{RRA} \cdot Mask$ ;
7   end
8   for  $i = 1$  to  $T_{TA}$  do
9      $\delta_{TA} \leftarrow \epsilon \text{sgn}(\nabla_{X_{clean}} \mathcal{L}_{TA}(f_{task}(X_{clean} + \delta_{RRA}), y))$ ;
10     $\delta_{TA} \leftarrow \delta_{TA} \cdot (1 - Mask)$ ;
11     $\delta_{TA} \leftarrow \text{clip}(\delta_{TA}, -\epsilon, \epsilon)$ ;
12  end
13 else
14   for  $i = 1$  to  $T_{TA}$  do
15      $\delta_{TA} \leftarrow \epsilon \text{sgn}(\nabla_{X_{clean}} \mathcal{L}_{TA}(f_{task}(X_{clean}), y))$ ;
16      $\delta_{TA} \leftarrow \delta_{TA} \cdot (1 - Mask)$ ;
17      $\delta_{TA} \leftarrow \text{clip}(\delta_{TA}, -\epsilon, \epsilon)$ ;
18   end
19   for  $i = 1$  to  $T_{RRA}$  do
20     Calculate  $\mathcal{L}_{RRA}$  using Equation (6);
21      $\delta_{RRA} \leftarrow Proj(\delta_{RRA} - \alpha \text{sgn}(\nabla_{\delta_{RRA}} \mathcal{L}_{RRA}(X_{rain} + \delta_{TA}, \delta_{RRA})))$ ;
22      $\delta_{RRA} \leftarrow \delta_{RRA} \cdot Mask$ ;
23   end
24 end
25  $\hat{X}_{rain} \leftarrow X_{rain} + \delta_{RRA} + \delta_{TA}$ ;
26  $\hat{X}_{rain} \leftarrow \text{clip}(\hat{X}_{rain}, 0, 1)$ ;

```

1 THE PSEUDO-CODES OF CAA-TR AND CAA-RT

The pseudo-codes of Cascaded Adversarial Attack from Rain to Task (CAA-RT) and Cascaded Adversarial Attack from Task to Rain (CAA-TR) are illustrated in Algorithm 1.

Table 1: The impact of rain removal networks on adversarial perturbations. For brevity, we only provide the mIoU metric. TA is implemented based on FGSM [1].

Settings	SSeg[5]	PIDNet[2]
Clean image	0.7161	0.5730
TA	0.0718	0.0673
TA + MPRNet[4]	0.2829	0.2670
TA + ARDNet[3]	0.4235	0.3689

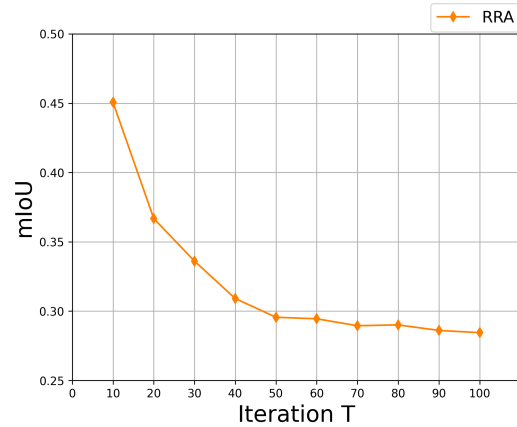


Figure 1: The attack performance of RRA under different iterations on SSeg [5] and ARDNet [3].

2 THE IMPACT OF ITERATIONS ON RRA

The performance of Remain Rain Attack (RRA) improves gradually with increasing iterations, eventually converging at around 100 iterations (see Fig. 1). Considering the balance between computational cost and performance, we chose 100 iterations as the optimal setting for our experiment.

3 THE IMPACT OF DERAINING NETWORKS ON ADVERSARIAL PERTURBATIONS.

When adversarial perturbations, which act as a form of noise, are introduced in the integrated system, they are affected by the rain removal network. In Table 1, we use clean images as inputs for Task Attack (TA) and preprocess the adversarial examples generated from TA by applying the rain removal network before feeding them into the semantic segmentation network. Additionally, we present the results of the semantic segmentation network when processing clean images, as well as the results when feeding the adversarial examples into the semantic segmentation network.

REFERENCES

[1] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. 2014. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572* (2014).

[2] Jiacong Xu, Zixiang Xiong, and Shankar P Bhattacharyya. 2023. PIDNet: A real-time semantic segmentation network inspired by PID controllers. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 19529–19539.

[3] Yi Yu, Wenhan Yang, Yap-Peng Tan, and Alex C Kot. 2022. Towards robust rain removal against adversarial attacks: A comprehensive benchmark analysis and beyond. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 6013–6022.

[4] Syed Waqas Zamir, Aditya Arora, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Ming-Hsuan Yang, and Ling Shao. 2021. Multi-stage progressive image restoration. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 14821–14831.

[5] Yi Zhu, Karan Sapra, Fitsum A Reda, Kevin J Shih, Shawn Newsam, Andrew Tao, and Bryan Catanzaro. 2019. Improving semantic segmentation via video propagation and label relaxation. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 8856–8865.