Supplemental Material for MetaAttack

Fengxiang Yang[1], Zhun Zhong[2], Hong Liu[3], Zheng Wang[4], Zhiming Luo[6*], Shaozi Li[1*], Nicu Sebe[2,5], Shin'ichi Satoh[3,4]

[1]Artificial Intelligence Department, Xiamen University, China
[2]Department of Information Engineering and Computer Science, University of Trento, Italy
[3]National Institute of Informatics, Japan [4]The University of Tokyo, Japan [5] Huawei Research, Ireland
[6]Post Doctoral Mobile Station of Information and Communication Engineering, Xiamen University, China

Further Experiments about Using PersonX

PersonX (Sun and Zheng 2019) is a synthetic pedestrian dataset with nearly $35,000$ images while the two real datasets (Duke and Market) in previous experiments contain nearly $15,000$ images. To make sure that the advantage of PersonX is not obtained by training with more images, we conduct experiments by randomly sampling $15,000$ images from PersonX for training our method. Results are reported in Tab. 1. For Duke $\rightarrow$ MSMT, we note that using less PersonX samples may slightly reduce the attacking performance. However, with the same number of training samples, using PersonX still achieves better performance than using Real dataset (Market in this experiment). This verifies the effectiveness of using virtual data during meta-learning.

Similar superiority of using virtual dataset over real one is also verified in "Market $\rightarrow$ MSMT". It is interesting that, in "Market $\rightarrow$ MSMT", using only $15,000$ training samples achieves better attacking results than using all training samples. We conjecture that this phenomenon is because the diversity of samples is more important than the number of samples in our MetaAttack. In the PersonX, $15,000$ samples include most variation factors in this dataset, so that using more samples may not bring further improvement.

Table 1: Experiments on the scale of PersonX dataset.

Duke $\rightarrow$ MSMT		Market $\rightarrow$ MSMT		Extra Data	
mAP	rank-1	mAP	rank-1	Real	PersonX
4.8	9.8	6.1	9.5	✓	×
3.9	8.1	4.8	8.4	×	✓ $(15,000)$
3.5	7.9	5.5	8.7	×	✓ (Full)

Experiments of Only Using Label-wise or Pair-wise Constraints

For vanilla UAP attack in person re-ID, we adopt pair-wise and label-wise constraints during optimization based on (Li et al. 2019). In this part, we evaluate the performance of using single constraint. The results are listed in Tab. 2

Table 2: Ablation on attacking loss functions.

Duke $\rightarrow$ Market		Market $\rightarrow$ Duke		Used Constraint(s)	
mAP	rank-1	mAP	rank-1	Pair-wise	Label-wise
5.3	8.1	12.1	16.3	✓	×
6.4	9.8	12.3	16.4	×	✓
4.9	7.0	11.2	15.2	✓	✓

As a conclusion, we find that using one of these two constraints alone will bring performance degradation, and considering both of them together helps improve the attacking performance, which has also been verified in (Li et al. 2019). Therefore, we used both loss functions in our optimization.

References

Li, J.; Ji, R.; Liu, H.; Hong, X.; Gao, Y.; and Tian, Q. 2019. Universal perturbation attack against image retrieval. In *ICCV*.

Sun, X.; and Zheng, L. 2019. Dissecting person re-identification from the viewpoint of viewpoint. In *CVPR*.

*Corresponding author: {zhiming.luo, szlig}@xmu.edu.cn.