
ECCV'20
ONLINE
23-28 AUGUST 2020
16TH EUROPEAN CONFERENCE ON
COMPUTER VISION
WWW.ECCV2020.EU

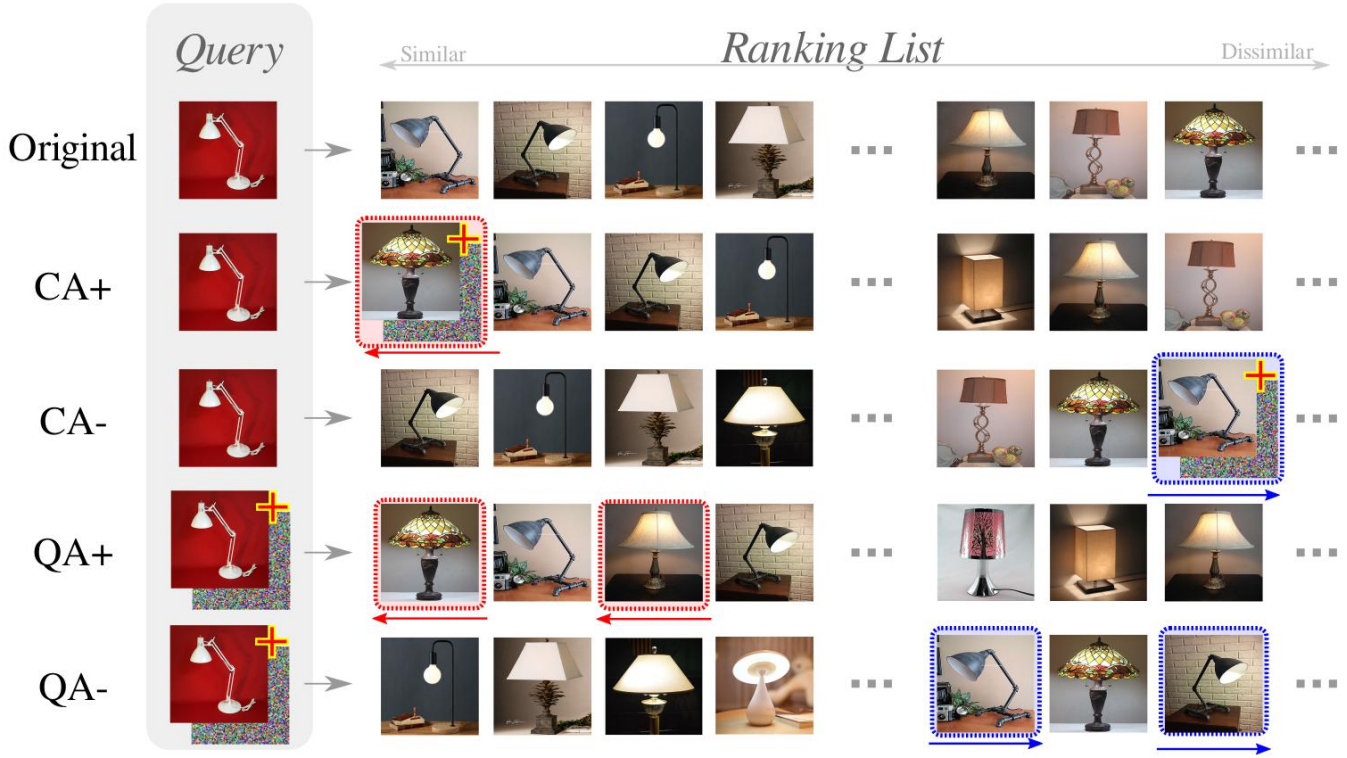
Adversarial Ranking Attack and Defense

Mo Zhou, Zhenxing Niu, Le Wang, Qilin Zhang, Gang Hua

Adversarial Ranking Attack: Raise or lower the ranks of some chosen candidates with respect to a set of specific queries.

- **Candidate Attack (CA):** Raise (CA+) or lower (CA-) the ranks by perturbing the candidate.
- **Query Attack (QA):** Raise (QA+) or lower (QA-) the ranks by perturbing the query.

Defense against the Attacks: Improve the ranking model robustness and mitigate all the proposed attacks simultaneously.



Arxiv: https://arxiv.org/abs/2002.11293 Github: