Jie Li

Third-year Ph.D student · Xiamen University
Address: Room 701, Administration Building #B, Haiyun Park, Xiamen University, 361005
E-mail: lijie.32@outlook.com
Person Homepage: https://m0re.fun

RESEARCH INTEREST

Machine Learn and Computer Vision.
Adversarial examples and robust deep learning.

EDUCATION

M.S-Ph.D. candidate of Artificial Intelligence 2019.09 - PRESENT
Xiamen University (XMU), Xiamen, China
Advisor: Rongrong Ji

Master of Artificial Intelligence 2017.09 - 2019.06
Xiamen University (XMU), Xiamen, China
Advisor: Rongrong Ji

Bachelor of Computer Science 2013.09 - 2017.06
Xiamen University (XMU), Xiamen, China

PUBLICATION

Yixu Wang, **Jie Li**, Hong Liu, Yan Wang, Yongjian Wu, Feiyue Huang, Rongrong Ji. *Black-Box Dissector: Towards Erasing-based Hard-Label Model Stealing Attack.* In European Conference on Computer Vision (ECCV 2022).

Shuman Fang, **Jie Li**, Xianming Lin, Rongrong Ji. *Learning to Learn Transferable Attack.* In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI 2022).

Jie Li, Rongrong Ji, Peixian Chen, Baochang Zhang, Xiaopeng Hong, Ruixin Zhang, Shaoxin Li, Jilin Li, Feiyue Huang, Yongjian Wu. *Aha! Adaptive History-driven Attack for Decision-based Black-box Models.* In Proceedings of the International Conference on Computer Vision 2021 (ICCV 2021).

Jie Li, Rongrong Ji, Hong Liu, Jianzhuang Liu, Bineng Zhong, Cheng Deng, Qi Tian. *Projection & Probability-Driven Black-Box Attack.* In Proceedings of the Conference on ComputerVision and Pattern Recognition 2020 (CVPR 2020).

Hong Liu, Rongrong Ji, **Jie Li**, Baochang Zhang, Yue Gao, Yongjian Wu, Feiyue Huang. *Universal Adversarial Perturbation via Prior Driven Uncertainty Approximation.* In Proceedings of the International Conference on Computer Vision 2019 (ICCV 2019). (Oral).

Jie Li, Rongrong Ji, Hong Liu, Xiaopeng Hong, Yue Gao, Qi Tian. *Universal Perturbation Attack Against Image Retrieval.* In Proceedings of the International Conference on Computer Vision 2019 (ICCV 2019).

Hong Liu, **Jie Li**, Rongrong Ji, and Yongjian Wu. *Learning Neural Bag-of-Matrix-Summarization with Riemannian Network.* In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI 2019).

Xianming Lin, **Jie Li**, Hualin Zeng, Rongrong Ji. *Font generation based on least*

squares conditional generative adversarial nets. Multimedia Tools and Applications, 2019.

RESEARCH EXPERIENCE

Research Intern 2020.06 - 2020.08
Youtu Lab, Tencent Technology (Shanghai) CO.,Ltd, China
- Decision-based Black-box Adversarial Attack (Published at ICCV'21)

AWARDS

Xiamen University Scholarship 2020

ACTIVITIES

Reviewer: TIP, CVPR, ICCV, ECCV, AAAI, IJCAI, ACM MM, ACCV, WACV, MM Asia.