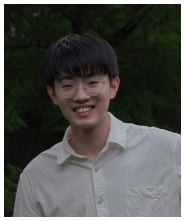
大连理工大学 DALIAN UNIVERSITY OF TECHNOLOGY



赵梦楠

出生时间：1995.11.15　出生地：山东济宁　专业：计算机（AI安全）

15822843520　dlutzmn@mail.dlut.edu.cn

教育背景

大连理工大学（2021年9月-至今）　导师：尹宝才教授和张立和教授

博士研究生　计算机（AI安全）　论文题目：从爬取图像训练扩散模型的安全问题研究

大连理工大学（2018年9月 – 2021年6月）　导师：王波教授

硕士研究生　信息与通信工程（AI安全）　论文题目：基于对抗样本的攻防研究

天津理工大学（2014年9月 – 2018年7月）

本科　电子信息工程　高考 620+；绩点 3.7+；免修数学（均分95+）、英语等。

实习经历

- **中科院自动化所**（2021年2-6月）导师王伟教授

已发表论文

1 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, "Catastrophic Overfitting: A Potential Blessing in Disguise ," in European Conference on Computer Vision (ECCV), 2024 **(清华A，CCF-B)**.

2 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, "Fast adversarial training with smooth convergence," in Proceedings of the International Conference on Computer Vision (ICCV), 2023 **(CCF-A)**.

3 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, "Adversarial attacks on scene graph generation," IEEE Transactions on Information Forensics and Security, 2024 **(SCI1-Top; CCF-A)**.

4 **M. n. Zhao**, B. Wang, W. Wang, Y. q. Kong, T. h. Zheng, and K. Ren, "Guided erasable adversarial attack (geaa) toward shared data protection," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2468–2482, 2022 **(SCI1-Top; CCF-A)**.

5 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, "Class correlation correction for unbised scene graph generation," Pattern Recognition, 2024 **(SCI1-Top; CCF-B)**.

6 B. Wang **(导师), M. n. Zhao**, W. Wang, F. Wei, Z. Qin, and K. Ren, "Are you confident that you have successfully generated adversarial examples?" IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 6, pp. 2089–2099, 2020 **(SCI1-Top; CCF-B)**.

7 B. Wang **(导师), M. n. Zhao**, W. Wang, X. r. Dai, Y. Li, and Y. q. Guo, "Adversarial analysis for source camera identification," IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 11, pp. 4174–4186, 2021 **(SCI1-Top; CCF-B)**.

8 **M. n. Zhao**, B. Wang, W. k. Guo, and W. Wang, "Protecting by attacking: A personal information protecting method with cross-modal adversarial examples," Neurocomputing, vol. 551, 2023 **(SCI2-Top; CCF-C)**.

9 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, "Temporal knowledge graph reasoning triggered by memories," Applied Intelligence, 2023 **(SCI2; CCF-C)**.

10 **M. n. Zhao**, B. Wang, F. Wei, M. n. Zhu, and X. Sui, "Source camera identification based on coupling coding and adaptive filter," IEEE Access, vol. 8, pp. 54 431–54 440, 2019 **Direct Accept; Cite 10+; SCI3**.

11 **M. n. Zhao**, X. r. Dai, B. Wang, F. Yu, and F. Wei, "Further understanding towards sparsity adversarial attacks," in International Conference on Artificial Intelligence and Security, Springer, 2022, **(EI)**

已录专利

1 **赵梦楠**，王波。一种基于深度学习用于源相机识别的合理对抗分析方法与流程。CN112381149A

2 **赵梦楠**，王波。一种基于自适应滤波与耦合性编码的图像来源鉴别方法。ZL201910871685.X; CN110659679

3 **赵梦楠**，王波。一种基于权重谱生成对抗样本的点攻击方法。ZL201911050075.X; CN110866287B

4 王波**(导师)**，**赵梦楠**，。一种基于欺骗攻击者的对抗样本防御方法。ZL201911050099.5; CN110852363B

5 **赵梦楠**，王波。一种针对共享数据保护的定向对抗下毒攻击方法。CN113821770A

在审论文

1 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, Eipformer: Emphasizing instance positions in 3d instance segmentation, in IEEE Transactions on Neural Networks and Learning Systems **(SCI1 Top; CCF-B)**

2 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, Forget All That Should Be Forgotten: Separable, Recoverable, and Sustainable Multi-Concept Erasure from Diffusion Models, in IEEE Symposium on Security and Privacy，IEEE S&P, **CCF-A**

3 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, Catastrophic overfitting: A potential blessing in disguise, in European Conference on Computer Vision, ECCV2024, **CCF-A**

4 **M. n. Zhao**, L. h. Zhang, Y. q. Kong, and B. c. Yin, Advprompt: Enhancing the reliability of erasing concept, ready for AAAI2024, **CCF-A**

专业服务：审稿人

- ACM Multimedia - MM, CCF-A
- IEEE Transactions on Neural Networks and Learning Systems, SCI1-Top
- IEEE Transactions on Multimedia, SCI1-Top
- IEEE Transactions on Circuits and Systems for Video Technology, SCI1-Top
- European Conference on Computer Vision - ECCV, CCF-B
- IEEE Transactions on Network Science and Engineering, SCI1
- Journal of King Saud University-Computer and Information Sciences SCI2
- International Journal of Machine Learning and Cybernetics, SCI3

其他论文

1 S. q. Wu, B Wang, J. x. Zhao, **M. n. Zhao**, K Zhong, Y. q. Guo. “Virtual sample generation and ensemble learning based image source identification with small training samples”, International Journal of Digital Crime and Forensics (IJDCF) 13 (3), 34-46

2 王波，代晓蕊，王伟，于菲，魏飞，**赵梦楠**，面向联邦学习的对抗样本投毒攻击。中国科学：信息科学, CCF-A

3 C. Jiang, Y. q. Kong, **M. n. Zhao**, L. h. Zhang, B. c. Yin. “CollabLearn: Propelling Weakly-Supervised Referring Image Segmentation through Collaboration of Semantics and Details”, under review in ACM Multimedia, ACMM2024, CCF-A

其他

- 英语：六级；多邻国：105
- 奖励：大连理工大学优秀研究生；大学生数学建模天津市市奖等
- 参加项目：
  1. 国家重点研发计划项目：2018AAA0102003
  2. 国家自然科学基金：U19B2039, 62276046, U1936117, 61772111, U1736119 , 61972395, 62106037
  3. 大连市科技创新：2021JJ12GX018
  4. 中央大学基础研究基金：DUT21GF303，DUT20TD110，DUTRC（3）088