Zhipeng Wei

Ph.D. Student in the School of Computer Science
Fudan University, China

✉ zpwei21@m.fudan.edu.cn
zhipeng-wei.github.io
Google Scholar

EDUCATION

Fudan University Shanghai, China
Ph.D. in Computer Science 2021-Expected June 2024
Advisor: Prof. Chen Jingjing and Jiang Yu-Gang

National University of Singapore Singapore
Visiting Student 2018-2019
Advisor: Prof. Chua Tat Seng

Jilin University Changchun, China
M.S. in Computer Science 2017-2020
Advisor: Prof. Zhou Fengfeng

Jilin University Changchun, China
B.S. in Biological Science 2013-2017

RESEARCH EXPERIENCE

Fudan University Shanghai, China
Ph.D. Candidate, Advisor: Prof. Chen Jingjing and Jiang Yu-Gang Sep.2021 – Present

- Developed a transfer-based targeted attack method that optimizes adversarial perturbations on global and local inputs by maximizing feature similarity between the two inputs.
- Analyzed feature similarity between image and video models for cross-modal attack, which leverages adversarial perturbations crafted from image models to attack video models.
- Explored the vulnerability of Vision Transformers by the proposed Pay No Attention and PatchOut attacks.

Fudan University Shanghai, China
Research Assistant, Advisor: Prof. Chen Jingjing and Jiang Yu-Gang Sep.2020 – Aug.2021

- Introduced a temporal translation method to augment adversarial inputs, consequently improving adversarial transferability across various video models.
- Grouped video frames by feature similarity to boost the efficiency of black-box attacks on video models.

National University of Singapore Singapore
Visiting Research Scholar, Advisor: Prof. Chua Tat Seng Oct.2018 – Jun.2019

- Employed a heuristic-based algorithm to select partial regions in video inputs, enhancing the efficiency of black-box attacks on video models.
- Developed graphs representing ingredient hierarchy, attributes, and co-occurrences in food images using a multi-relational Graph Convolutional Network (GCN) for zero-shot ingredient recognition.
- Employed GPS location data to improve the performance of food photo recognition.

TEACHIING EXPERIENCE

Fudan University Shanghai, China
Teaching Assistant 2021 - 2023

- Taught over 50 undergraduate students in the computer vision course, delivering 135-minute sessions twice per semester, which included OpenCV and PyTorch tutorials.

Fudan University Shanghai, China
Mentoring 2021 - 2023

- Assisted in mentoring a team focused on adversarial attacks and defenses, where Kai Chen and Yiqiang Lv have published papers in AAAI, ACM MM, and ICME.

HONORS & AWARDS

Outstanding Master's Thesis of Jilin Province Dec. 2022
China National Scholarship of Fudan University Oct. 2022
Outstanding Graduates of Jilin University Jun. 2020
Outstanding Master's Thesis of Jilin University Jun. 2020

ACADEMIC SERVICE

Reviewer for IEEE TNNLS; TCSVT; TDSC; ACM MM 2022; AAAI 2023, 2024; CVPR 2023; IJCAI 2023; ICCV 2023; NIPS2023; ICLR 2024.

PUBLICATIONS

1. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang, "Adaptive Cross-Modal Transferable Adversarial Attacks from Images to Videos". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence.* doi: 10.1109/TPAMI.2023.3347835.
2. **Zhipeng Wei**, Jingjing Chen, Micah Goldblum, Zuxuan Wu, Tom Goldstein, Yu-Gang Jiang and Larry S. Davis, "Towards Transferable Adversarial Attacks on Image and Video Transformers". In: *IEEE Transactions on Image Processing*. vol. 32, pp. 6346-6358, 2023.
3. Kai Chen, **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang. "GCMA: Generative Cross-Modal Transferable Adversarial Attacks from Images to Videos." In: *Proceedings of the 31th ACM International Conference on Multimedia*. 2023
4. Jingjing Chen*, Linhai Zhuo*, **Zhipeng Wei**, Hao Zhang, Huazhu Fu, and Yu-Gang Jiang. "Knowledge driven weights estimation for large-scale few-shot image recognition." In: *Pattern Recognition 142 (2023)*, p. 109668

5. Yiqiang Lv, Jingjing Chen, **Zhipeng Wei**, Kai Chen, Zuxuan Wu, and Yu-Gang Jiang. "Downstream Task-agnostic Transferable Attacks on Language-Image Pre-training Models." In: *2023 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE. 2023, pp. 2831–2836
6. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang. "Enhancing the Self-Universality for Transferable Targeted Attacks." In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2023, pp. 12281–12290
7. Kai Chen, **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang. "Attacking video recognition models with bullet-screen comments." In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. 1. 2022, pp. 312–320
8. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang. "Cross-modal transferable adversarial attacks from images to videos." In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2022, pp. 15064–15073
9. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang. "Boosting the transferability of video adversarial examples via temporal translation." In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. 3. 2022, pp. 2659–2667
10. **Zhipeng Wei**, Jingjing Chen, Micah Goldblum, Zuxuan Wu, Tom Goldstein, and Yu-Gang Jiang. "Towards transferable adversarial attacks on vision transformers." In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. 3. 2022, pp. 2668–2676
11. **Zhipeng Wei**, Jingjing Chen, Hao Zhang, Linxi Jiang, and Yu-Gang Jiang. "Adaptive Temporal Grouping for Black-box Adversarial Attacks on Videos." In: *Proceedings of the 2022 International Conference on Multimedia Retrieval*. 2022, pp. 587–593
12. **Zhipeng Wei**, Jingjing Chen, Xingxing Wei, et al. "Heuristic black-box adversarial attacks on video recognition models." In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 34. 07. 2020, pp. 12338–12345
13. Jingjing Chen, Liangming Pan, **Zhipeng Wei**, Xiang Wang, Chong-Wah Ngo, and Tat-Seng Chua. "Zero-shot ingredient recognition by multi-relational graph convolutional network." In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 34. 07. 2020, pp. 10542–10550
14. **Zhipeng Wei**, Jingjing Chen, Zhaoyan Ming, Chong-Wah Ngo, Tat-Seng Chua, and Fengfeng Zhou. "DietLens-eout: Large scale restaurant food photo recognition." In: *Proceedings of the 2019 on International Conference on Multimedia Retrieval*. 2019, pp. 399–403

Ongoing manuscripts:

15. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang, "Dynamic Linear Augmentation and Dilated Attention for Transferable Targeted Attacks". In submission.
16. **Zhipeng Wei**, Jingjing Chen, Zuxuan Wu, and Yu-Gang Jiang, "Flattening the Loss Landscape for Free to Enhance Adversarial Transferability". In submission.

INVITED TALKS

1. Spotlight, Vision And Learning Seminar (VALSE). August 2022.
2. Speaker, AI TIME PHD-CVPR. August 2022.
3. Speaker, AI TIME PHD-AAAI. May 2022.