

Mo Zhou

CONTACT	3400 North Charles Street Baltimore, MD 21218 United States	Tel: (+1) ***** Email: cdluminate@gmail.com Website: cdluminate.github.io
STATUS	Chinese citizen	
CURRENT	<ul style="list-style-type: none">Johns Hopkins University Dept. Electrical and Computer Engineering, Whiting School of Engineering <i>Ph.D.</i> Electrical and Electronics Engineering	Baltimore, MD, USA 21218 08/2021 - Current
INTERESTS	<ul style="list-style-type: none">Machine Learning, Deep Learning, and Computer VisionObject Recognition and Detection, Vision-Language ModelsAdversarial Defense and Robustness for AI SecurityLarge Language Models and ApplicationsLinux Operating System Development and Administration	
EXPERIENCE	<ul style="list-style-type: none">Google Research, Computational Imaging Team Student Researcher (Computer Vision)Microsoft Research, Applied Sciences Group Research Intern (Deep Learning)Wormpex AI Research LLC Research Intern (Computer Vision)Xi'an Jiaotong University Institute of Artificial Intelligence and Robotics (IAIR) Research Assistant (Computer Vision)	Mountain View, CA 94043 05/2024 - 10/2024 Redmond, WA 98052 05/2023 - 08/2023 Bellevue, WA 98004 05/2022 - 08/2022 Xi'an, Shaanxi 710049 07/2020 - 06/2021
EDUCATION	<ul style="list-style-type: none">Xidian University <i>M.Eng.</i> Pattern Recognition and Intelligent Systems. July, 2020 <i>Thesis:</i> Coherent Visual-Semantic Embedding for Cross-Modal RetrievalXidian University <i>B.Eng.</i> Electromagnetic Field and Wireless Technology. July, 2017	Xi'an, Shaanxi, China 710071 09/2017 - 06/2020 Xi'an, Shaanxi, China 710126 09/2013 - 07/2017
PUBLICATIONS	Google Scholar Profile: scholar.google.com/citations?user=BVIO95UAAAAJ (Mar. 30 2024) Citations: 1205 H-Index: 8 i10-Index: 8 Other Identifiers: [ORCID] [Publons] [Semantic Scholar] [Web of Science] [DBLP]	
	JOURNAL ARTICLES:	(1 TPAMI, 1 TMM)
[PDF] [arXiv] [Github]	[J01] <u>Mo Zhou</u> , Le Wang, Zhenxing Niu, Qilin Zhang, Nanning Zheng, Gang Hua, “ <i>Adversarial Attack and Defense in Deep Ranking</i> ,” IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2024. DOI: 10.1109/TPAMI.2024.3365699	
[PDF]	[J02] Le Wang, <u>Mo Zhou</u> , Zhenxing Niu, Qilin Zhang, Nanning Zheng, “ <i>Adaptive Ladder Loss for Learning Coherent Visual-Semantic Embedding</i> ,” IEEE Transactions on Multimedia (TMM), 2021. DOI: 10.1109/TMM.2021.3139210	

CONFERENCE PAPERS:

(3 CVPR, 2 ICCV, 1 ECCV, 1 NeurIPS, 1 AAAI)

- [PDF] [Github] [C01] Yiqun Mei, Pengfei Guo, Mo Zhou, Vishal M. Patel, “*Resource-Adaptive Federated Learning with All-In-One Neural Composition*,” Advances in Neural Information Processing Systems (NeurIPS), 2022.
- [PDF] [arXiv] [Github] [C02] Mo Zhou, Vishal M. Patel, “*Enhancing Adversarial Robustness for Deep Metric Learning*,” in Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2022.
- [PDF] [arXiv] [Github] [C03] Mo Zhou, Le Wang, Zhenxing Niu, Qilin Zhang, Yinghui Xu, Nanning Zheng, Gang Hua, “*Practical Order Attack in Deep Ranking*,” in Proc. IEEE International Conf. on Computer Vision (ICCV), 2021.
- [PDF] [arXiv] [Github] [C04] Liushuai Shi, Le Wang, Chengjiang Long, Sanping Zhou, Mo Zhou, Zhenxing Niu, Gang Hua, “*SGCN: Sparse Graph Convolution for Pedestrian Trajectory Prediction*,” In Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2021.
- [PDF] [arXiv] [Github] [C05] Mo Zhou, Zhenxing Niu, Le Wang, Qilin Zhang, Gang Hua, “*Adversarial Ranking Attack and Defense*,” in Proc. European Conf. on Computer Vision (ECCV), 2020.
- [PDF] [arXiv] [Github] [C06] Mo Zhou, Zhenxing Niu, Le Wang, Zhanning Gao, Qilin Zhang, Gang Hua, “*Ladder Loss for Coherent Visual-Semantic Embedding*,” in Proc. AAAI Conf. on Artificial Intelligence (AAAI), 2020.
- [PDF] [C07] Zhenxing Niu, Mo Zhou, Le Wang, Xinbo Gao, Gang Hua, “*Hierarchical Multimodal LSTM for Dense Visual-Semantic Embedding*,” in Proc. IEEE International Conf. on Computer Vision (ICCV), 2017.
- [PDF] [Dataset] [C08] Zhenxing Niu, Mo Zhou, Le Wang, Xinbo Gao, Gang Hua. “*Ordinal Regression with Multiple Output CNN for Age Estimation*,” in Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2016.

PREPRINT / UNDER-REVIEW PAPERS:



- [arXiv] [X01] Yatong Bai, Mo Zhou, Vishal M. Patel, Somayeh Sojoudi, “*MixedNUTS: Training-Free Accuracy-Robustness Balance via Nonlinearly Mixed Classifiers*,” 2024, Under Reivew.
- [arXiv] [X02] Kangfu Mei, Mo Zhou, Vishal M. Patel, “*T1: Scaling Diffusion Probabilistic Fields to High-Resolution on Unified Visual Modalities*,” 2023, Under Review.
- [arXiv] [Github] [X03] Yu Zeng*, Mo Zhou*, Yuan Xue, Vishal M. Patel, “*Securing Deep Generative Models with Universal Adversarial Signature*,” 2023, Under Review.
- [arXiv] [X04] Mo Zhou, Yiding Yang, Haoxiang Li, Vishal M. Patel, Gang Hua, “*Deployment Prior Injection for Run-time Calibratable Object Detection*,” 2022, Under Review.
- [arXiv] [X05] Mo Zhou, Vishal M. Patel, “*On Trace and Characterization of PGD-Like Adversarial Attacks*,” 2022, Under Review.

PATENTS

- [P01] Le Wang, Mo Zhou, Sanping Zhou, Shitao Chen, Jingmin Xin, Nanning Zheng, “A Practical Relative Order Adversarial Attack Method”. Chinese Patent No. 202110998691.9.
- [P02] Zhenxing Niu, Wei Xue, Mo Zhou, Bo Yuan, Xinbo Gao, Gang Hua, “Age estimation method based on multi-output convolution neural network and ordered regression”. Chinese Patent No. 201610273524.7.

ACTIVITIES

- Reviewer of International Conferences
 - IEEE Conf. on Computer Vision and Pattern Recognition (CVPR) 2020 – 2024
 - Annual Conf. on Neural Information Processing Systems (NeurIPS) 2022 – 2023
 - International Conf. on Computer Vision (ICCV) 2021 – 2023
 - European Conf. on Computer Vision (ECCV) 2020 – 2024
 - International Conf. Learning Representations (ICLR) 2022 – 2024
 - International Conf. of Machine Learning (ICML) 2023 – 2024

	<ul style="list-style-type: none"> ◦ AAAI Conf. on Artificial Intelligence (AAAI) 2021 – 2022 ◦ Winter Conf. on Applications of Computer Vision (WACV) 2021 – 2024 ◦ Asian Conf. on Computer vision (ACCV) 2018 – 2024 ◦ International Conf. on Pattern Recognition (ICPR) 2024
	<ul style="list-style-type: none"> • Reviewer of International Journals <ul style="list-style-type: none"> ◦ IEEE Trans. on Pattern Analysis and Machine Intelligence (TPAMI) 2021 – 2023 ◦ IEEE Trans. on Neural Networks and Learning Systems (TNNLS) 2022 ◦ IEEE Trans. on Multimedia (TMM) 2023 ◦ IEEE Trans. on Dependable and Secure Computing (TDSC) 2022 ◦ Elsevier Journal of Neural Networks (NeuNet) 2022 ◦ Elsevier Journal of Neurocomputing (NeuComp) 2021 ◦ Elsevier Journal of Image and Vision Computing (IMAVIS) 2023 – 2024 ◦ Elsevier Journal of Computers & Security (COSE) 2024 ◦ Springer Journal: International Journal of Computer Vision (IJCV) 2023 – 2024 ◦ Springer Journal of Machine Vision and Application (MVA) 2020 – 2023 ◦ Springer Journal of Complex & Intelligent Systems (CAIS) 2021 – 2023 ◦ Oxford University Press: The Computer Journal (COMPJ) 2023 • Organizer of International Workshops <ul style="list-style-type: none"> ◦ 4th Workshop on Adversarial Robustness In the Real World ICCV 2023 ◦ 4th Workshop of Adversarial Machine Learning on Computer Vision CVPR 2024 • Volunteer in Free and Open-Source Software Communities <ul style="list-style-type: none"> ◦  Official Developer for Debian GNU/Linux 08/2018 – Current ◦  Contributor for Gentoo GNU/Linux 06/2019 – 08/2019
HONORS	<ul style="list-style-type: none"> • Outstanding Reviewer for ICCV 2021 2021 • Open Source Promotion Plan (OSPP) with Tsinghua University TUNA Association 2020 Project: <i>Integrating Data Science Software into Debian</i> (Best Quality Award) • Google Summer of Code (GSoC) with Debian Project 2020 Project: <i>BLAS/LAPACK Ecosystem Enhancement for Debian</i> • Google Summer of Code (GSoC) with Gentoo Foundation 2019 Project: <i>BLAS and LAPACK Runtime Switching</i> • Xidian University Secondary School Scholarship. ⁺ 2017-2018 • Interdisciplinary Contest in Modeling (ICM) 2016 Meritorious Winner. Advisor: Youlong Yang (Xidian University)
AFFLIATION	<ul style="list-style-type: none"> • Student Member, IEEE Aug 2021 – Dec 2024
REFERENCES	AVAILABLE UPON REQUEST.