

## Mo Zhou

---

CONTACT	3400 North Charles Street Baltimore, MD 21218 United States	Tel: (+1) ***** Email: <a href="mailto:cdluminate@gmail.com">cdluminate@gmail.com</a> Website: <a href="https://cdluminate.github.io">cdluminate.github.io</a>
STATUS	Chinese citizen	
CURRENT	<ul style="list-style-type: none"><li>Johns Hopkins University Dept. Electrical and Computer Engineering, Whiting School of Engineering <i>Ph.D.</i> Electrical and Electronics Engineering</li></ul>	Baltimore, MD, USA 21218 08/2021 - Current
INTERESTS	<ul style="list-style-type: none"><li>Machine Learning, Deep Learning, and Computer Vision</li><li>Object Recognition and Detection, Vision-Language Models</li><li>Adversarial Defense and Robustness for AI Security</li><li>Large Language Models and Applications</li><li>Linux Operating System Development and Administration</li></ul>	
EXPERIENCE	<ul style="list-style-type: none"><li>Google Research, Computational Imaging Team Student Researcher (Computer Vision)</li><li>Microsoft Research, Applied Sciences Group Research Intern (Deep Learning)</li><li>Wormpex AI Research LLC Research Intern (Computer Vision)</li><li>Xi'an Jiaotong University Institute of Artificial Intelligence and Robotics (IAIR) Research Assistant (Computer Vision)</li></ul>	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"><li>Xidian University <i>M.Eng.</i> Pattern Recognition and Intelligent Systems. July, 2020 <i>Thesis:</i> Coherent Visual-Semantic Embedding for Cross-Modal Retrieval</li><li>Xidian University <i>B.Eng.</i> Electromagnetic Field and Wireless Technology. July, 2017</li></ul>	Xi'an, Shaanxi, China 710071 09/2017 - 06/2020 Xi'an, Shaanxi, China 710126 09/2013 - 07/2017
PUBLICATIONS	Google Scholar Profile: <a href="https://scholar.google.com/citations?user=BVIO95UAAAAJ">scholar.google.com/citations?user=BVIO95UAAAAJ</a> (June. 6 2024) Citations: 1263 H-Index: 9 i10-Index: 8 Other Identifiers: <a href="#">[ORCID]</a> <a href="#">[Publons]</a> <a href="#">[Semantic Scholar]</a> <a href="#">[Web of Science]</a> <a href="#">[DBLP]</a>	
	JOURNAL ARTICLES:	(1 TPAMI, 1 TMM)
<a href="#">[PDF]</a> <a href="#">[arXiv]</a> <a href="#">[Github]</a>	[J01] <a href="#">Mo Zhou</a> , 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	
<a href="#">[PDF]</a>	[J02] Le Wang, <a href="#">Mo Zhou</a> , 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 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 – 2024
  - 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"> <li>◦ AAAI Conf. on Artificial Intelligence (AAAI) 2021 – 2022</li> <li>◦ Winter Conf. on Applications of Computer Vision (WACV) 2021 – 2024</li> <li>◦ Asian Conf. on Computer vision (ACCV) 2018 – 2024</li> <li>◦ International Conf. on Pattern Recognition (ICPR) 2024</li> </ul>
	<ul style="list-style-type: none"> <li>• Reviewer of International Journals <ul style="list-style-type: none"> <li>◦ IEEE Trans. on Pattern Analysis and Machine Intelligence (TPAMI) 2021 – 2023</li> <li>◦ IEEE Trans. on Neural Networks and Learning Systems (TNNLS) 2022</li> <li>◦ IEEE Trans. on Multimedia (TMM) 2023</li> <li>◦ IEEE Trans. on Dependable and Secure Computing (TDSC) 2022</li> <li>◦ Elsevier Journal of Neural Networks (NeuNet) 2022</li> <li>◦ Elsevier Journal of Neurocomputing (NeuComp) 2021</li> <li>◦ Elsevier Journal of Image and Vision Computing (IMAVIS) 2023 – 2024</li> <li>◦ Elsevier Journal of Computers &amp; Security (COSE) 2024</li> <li>◦ Springer Journal: International Journal of Computer Vision (IJCV) 2023 – 2024</li> <li>◦ Springer Journal of Machine Vision and Application (MVA) 2020 – 2023</li> <li>◦ Springer Journal of Complex &amp; Intelligent Systems (CAIS) 2021 – 2023</li> <li>◦ Oxford University Press: The Computer Journal (COMPJ) 2023</li> </ul> </li> <li>• Organizer of International Workshops <ul style="list-style-type: none"> <li>◦ 4th Workshop on Adversarial Robustness In the Real World ICCV 2023</li> <li>◦ 4th Workshop of Adversarial Machine Learning on Computer Vision CVPR 2024</li> </ul> </li> <li>• Volunteer in Free and Open-Source Software Communities <ul style="list-style-type: none"> <li>◦  <b>Official Developer</b> for Debian GNU/Linux 08/2018 – Current</li> <li>◦  <b>Contributor</b> for Gentoo GNU/Linux 06/2019 – 08/2019</li> </ul> </li> </ul>
[Website] [Website]	
HONORS	<ul style="list-style-type: none"> <li>• <b>Outstanding Reviewer</b> for CVPR 2024 2024</li> <li>• <b>Outstanding Reviewer</b> for ICCV 2021 2021</li> <li>• Open Source Promotion Plan (OSPP) with Tsinghua University TUNA Association 2020 Project: <i>Integrating Data Science Software into Debian</i> (<b>Best Quality Award</b>)</li> <li>• Google Summer of Code (GSoC) with Debian Project 2020 Project: <i>BLAS/LAPACK Ecosystem Enhancement for Debian</i></li> <li>• Google Summer of Code (GSoC) with Gentoo Foundation 2019 Project: <i>BLAS and LAPACK Runtime Switching</i></li> <li>• Xidian University Secondary School Scholarship.<sup>+</sup> 2017-2018</li> <li>• Interdisciplinary Contest in Modeling (ICM) 2016 Meritorious Winner. Advisor: Youlong Yang (Xidian University)</li> </ul>
AFFLIATION	<ul style="list-style-type: none"> <li>• Student Member, IEEE Aug 2021 – Dec 2024</li> </ul>
REFERENCES	AVAILABLE UPON REQUEST.