

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 Baltimore, MD, USA 21218 Dept. Electrical and Computer Engineering, Whiting School of Engineering <i>Ph.D. Electrical and Electronics Engineering</i> 08/2021 - Current <i>Advisor: Vishal M. Patel</i>	
INTERESTS	<ul style="list-style-type: none">Deep Learning, Computer Vision, and Multi-modality ModelsArtificial Intelligence Security, Robustness and TrustworthinessLinux Operating System Development and Administration	
EXPERIENCE	<ul style="list-style-type: none">Google Research, Computational Imaging Team Mountain View, CA 94043 Student Researcher (Computer Vision) 05/2024 - 08/2025 <i>Mentor: Hossein Talebi, Keren Ye, Mauricio Delbracio, Peyman Milanfar</i>Microsoft Research, Applied Sciences Group Redmond, WA 98052 Research Intern (Deep Learning) 05/2023 - 08/2023 <i>Mentor: Kazuhito Koishida, Saeed Amizadeh</i>Wormpex AI Research LLC Bellevue, WA 98004 Research Intern (Computer Vision) 05/2022 - 08/2022 <i>Mentor: Haoxiang Li, Yiding Yang, Gang Hua</i>Xi'an Jiaotong University Xi'an, Shaanxi 710049 Institute of Artificial Intelligence and Robotics (IAIR) Research Assistant (Computer Vision) 07/2020 - 06/2021 <i>Supervisor: Le Wang, Sanping Zhou</i>	
EDUCATION	<ul style="list-style-type: none">Xidian University Xi'an, Shaanxi, China 710071 <i>M.Eng. Pattern Recognition and Intelligent Systems.</i> July, 2020 09/2017 - 06/2020 <i>Thesis: Coherent Visual-Semantic Embedding for Cross-Modal Retrieval</i> <i>Advisor: Zhenxing Niu</i>Xidian University Xi'an, Shaanxi, China 710126 <i>B.Eng. Electromagnetic Field and Wireless Technology.</i> July, 2017 09/2013 - 07/2017 <i>Advisor: Zhenxing Niu</i>	
PUBLICATIONS	Google Scholar Profile: scholar.google.com/citations?user=BVIO95UAAAAJ (Aug. 10 2025) Citations: 1704 H-Index: 11 i10-Index: 11 Other Identifiers: [ORCID] [Publons] [Semantic Scholar] [Web of Science] [DBLP]	
	JOURNAL ARTICLES:	(1 TPAMI, 1 TMLR, 1 TMM)
[Openreview] [arXiv]	[J01] Yatong Bai, <u>Mo Zhou</u> , Vishal M. Patel, Somayeh Sojoudi, “ <i>MixedNUTS: Training-Free Accuracy-Robustness Balance via Nonlinearly Mixed Classifiers</i> ,” Transactions on Machine Learning Research (TMLR), 2024.	

- [PDF] [arXiv] [Github] [J02] Mo Zhou, Le Wang, Zhenxing Niu, Qilin Zhang, Nanning Zheng, Gang Hua, “*Adversarial Attack and Defense in Deep Ranking*,” IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2024. DOI: 10.1109/TPAMI.2024.3365699
- [PDF] [J03] Le Wang, Mo Zhou, Zhenxing Niu, Qilin Zhang, Nanning Zheng, “*Adaptive Ladder Loss for Learning Coherent Visual-Semantic Embedding*,” IEEE Transactions on Multimedia (TMM), 2021. DOI: 10.1109/TMM.2021.3139210

CONFERENCE PAPERS: (3 CVPR, 3 ICCV, 1 ECCV, 1 NeurIPS, 1 ICLR, 1 AAAI)

- [arXiv] [C1] Mo Zhou, Keren Ye, Mauricio Delbracio, Peyman Milanfar, Vishal M. Patel, Hossien Talebi, “*UniRes: Universal Image Restoration for Complex Degradations*,” in Proc. IEEE International Conf. on Computer Vision (ICCV), 2025.
- [PDF] [arXiv] [C2] Kangfu Mei, Mo Zhou, Vishal M. Patel, “*Field-DiT: Diffusion Transformer on Unified Video, 3D, and Game Field Generation*,” in Proc. International Conference on Learning Representations (ICLR), 2025.
- [PDF] [arXiv] [Github] [C3] Mo Zhou, Vishal M. Patel, “*On Trace of PGD-Like Adversarial Attacks*,” in Proc. International Conference on Pattern Recognition (ICPR), 2024.
- [PDF] [Github] [C4] 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] [C5] 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] [C6] 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] [C7] 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] [C8] 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] [C9] 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] [C10] 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] [C11] 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] Mo Zhou, Keren Ye, Viraj Shah, Kangfu Mei, Mauricio Delbracio, Peyman Milanfar, Vishal M. Patel, Hossien Talebi, “*Reference-Guided Identity Preserving Face Restoration*,” 2025, Under Review.
- [arXiv] [Github] [X02] Yu Zeng*, Mo Zhou*, Yuan Xue, Vishal M. Patel, “*Securing Deep Generative Models with Universal Adversarial Signature*,” 2023, Under Review.
- [arXiv] [X03] Mo Zhou, Yiding Yang, Haoxiang Li, Vishal M. Patel, Gang Hua, “*Deployment Prior Injection for Run-time Calibratable Object Detection*,” 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 – 2025
 - Annual Conf. on Neural Information Processing Systems (NeurIPS) 2022 – 2025
 - International Conf. on Computer Vision (ICCV) 2021 – 2025
 - European Conf. on Computer Vision (ECCV) 2020 – 2024
 - International Conf. Learning Representations (ICLR) 2022 – 2025
 - International Conf. of Machine Learning (ICML) 2023 – 2024
 - AAAI Conf. on Artificial Intelligence (AAAI) 2021 – 2022
 - Winter Conf. on Applications of Computer Vision (WACV) 2021 – 2025
 - Asian Conf. on Computer vision (ACCV) 2018 – 2024
 - International Conf. on Pattern Recognition (ICPR) 2024
- Reviewer of International Journals
 - 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 – 2025
 - 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 Workshop and Competition
 - Erasing the Invisible: A Stress-Test Challenge for Image Watermarks NeurIPS 2024
 - 4th Workshop of Adversarial Machine Learning on Computer Vision CVPR 2024
 - 4th Workshop on Adversarial Robustness In the Real World ICCV 2023
- Volunteer in Free and Open-Source Software Communities
 -  **Official Developer** for Debian GNU/Linux 08/2018 – Current
 -  **Contributor** for Gentoo GNU/Linux 06/2019 – 08/2019

[Website]

[Website]

[Website]

TEACHING

- Deep Learning (EN . 520 . 638 . 01 . SP25) Spring 2025
 Johns Hopkins University
Teaching Assistant for Prof. Vishal M. Patel

HONORS

- Outstanding Reviewer for CVPR 2024 2024
- Outstanding Reviewer for ICCV 2021 2021
- Google Summer of Code (GSoC) as Mentor with Debian Project 2025
 Project: *Packaging LLM Inference Libraries* (Student: Kohei Sendai)
- Open Source Promotion Plan (OSPP) with Tsinghua University TUNA Association 2020
 Project: *Integrating Data Science Software into Debian* (**Best Quality Award**)
- Google Summer of Code (GSoC) as Student with Debian Project 2020
 Project: *BLAS/LAPACK Ecosystem Enhancement for Debian*

- Google Summer of Code (GSoC) as Student with Gentoo Foundation 2019
Project: *BLAS and LAPACK Runtime Switching*
- Xidian University Secondary School Scholarship.⁺ 2017-2018
- Interdisciplinary Contest in Modeling (ICM) 2016
Meritorious Winner. Advisor: Youlong Yang (Xidian University)

AFFILIATION • Student Member, IEEE Aug 2021 – Dec 2024

REFERENCES AVAILABLE UPON REQUEST.