

Cihang Xie

CONTACT INFORMATION

Department of Computer Science (424) 320-1038
3400 North Charles Street cihangxie306@gmail.com
Baltimore, Maryland 21218, USA <https://cihangxie.github.io/>

EDUCATION

Johns Hopkins University (JHU) 09/2016 - present
Ph.D. in Department of Computer Science
Advisor: Alan Yuille

University of California, Los Angeles (UCLA) 09/2014 - 12/2015
M.S. in Electrical Engineering

Huazhong University of Science and Technology (HUST) 09/2010 - 06/2014
B.S. in Telecommunications Engineering

ACADEMIC EXPERIENCE

Google Brain 11/2019 - present
Student Researcher
Mentors: Dr. Quoc Le, Dr. Mingxing Tan and Dr. Boqing Gong

Google 06/2019 - 11/2019
Research Intern
Mentors: Dr. Quoc Le, Dr. Mingxing Tan, Dr. Boqing Gong and Dr. Jiang Wang

Facebook AI Research 11/2018 - 04/2019
Visiting Researcher
Mentors: Dr. Kaiming He, Dr. Laurens van der Maaten and Dr. Judy Hoffman

Facebook AI Research 06/2018 - 11/2018
Research Intern
Mentors: Dr. Kaiming He and Dr. Laurens van der Maaten

TEACHING

Johns Hopkins University (JHU) Fall 2019
Role: Guest Lecturer
Course: EN.600.485 *Probabilistic Models of the Visual Cortex*
Instructor: Alan Yuille

University of California, Merced (UCM) Fall 2019
Role: Guest Lecturer
Course: EECS 286 *Advanced Topics in Computer Vision*
Instructor: Ming-Hsuan Yang

Johns Hopkins University (JHU) Spring 2018
Role: Teaching Assistant
Course: EN.601.783 *Vision as Bayesian Inference*
Instructor: Alan Yuille

PUBLICATIONS

[1] **Cihang Xie**, Mingxing Tan, Boqing Gong, Jiang Wang, Alan Yuille, Quoc Le. Adversarial Examples Improve Image Recognition. In Proceedings of *Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2020.

- [2] Yingwei Li, Xiaojie Jin, Jieru Mei, Xiaochen Lian, Linjie Yang, **Cihang Xie**, Qihang Yu, Yuyin Zhou, Song Bai, Alan Yuille. When Self-Attention Meets Mobile Networks: Manual Design and AutoSearch. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2020.
- [3] Lifeng Huang, Chengying Gao, Yuyin Zhou, Changqing Zou, **Cihang Xie**, Alan Yuille, Ning Liu. UPC: Learning Universal Physical Camouflage Attacks on Object Detectors. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2020.
- [4] **Cihang Xie**, Alan Yuille. Intriguing Properties of Adversarial Training at Scale. In *International Conference on Learning Representations (ICLR)*, 2020.
- [5] Yingwei Li, Song Bai, Yuyin Zhou, **Cihang Xie**, Zhishuai Zhang, Alan Yuille. Learning Transferable Adversarial Examples via Ghost Networks. In *Proceedings of The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI)*, AAAI Press, 2020.
- [6] **Cihang Xie**, Yuxin Wu, Laurens van der Maaten, Alan Yuille, Kaiming He. Feature Denoising for Improving Adversarial Robustness. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2019.
- [7] **Cihang Xie**, Zhishuai Zhang, Yuyin Zhou, Song Bai, Jianyu Wang, Zhou Ren, Alan Yuille. Improving Transferability of Adversarial Examples with Input Diversity. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2019.
- [8] Zhishuai Zhang, Siyuan Qiao, **Cihang Xie**, Wei Shen, Bo Wang, Alan Yuille. Single-Shot Object Detection with Enriched Semantics. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2018.
- [9] Zhishuai Zhang, **Cihang Xie**, Jianyu Wang, Lingxi Xie, Alan Yuille. DeepVoting: A Robust and Explainable Deep Network for Semantic Part Detection under Partial Occlusion. In *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, 2018.
- [10] **Cihang Xie**, Jianyu Wang, Zhishuai Zhang, Ren Zhou, Alan Yuille. Mitigating Adversarial Effects Through Randomization. In *International Conference on Learning Representations (ICLR)*, 2018.
- [11] Jianyu Wang, Zhishuai Zhang, **Cihang Xie**, Yuyin Zhou, Vittal Premachandran, Jun Zhu, Lingxi Xie, Alan Yuille. Visual Concepts and Compositional Voting. In *Annals of Mathematical Sciences and Applications*, 2018.
- [12] Alexey Kurakin, Ian Goodfellow, Samy Bengio, Yinpeng Dong, Fangzhou Liao, Ming Liang, Tianyu Pang, Jun Zhu, Xiaolin Hu, **Cihang Xie**, Jianyu Wang, Zhishuai Zhang, Zhou Ren, Alan Yuille, Sangxia Huang, Yao Zhao, Yuzhe Zhao, Zhonglin Han, Junjiajia Long, Yerkebulan Berdibekov, Takuya Akiba, Seiya Tokui, Motoki Abe. Adversarial Attacks and Defences Competition. In *the NeurIPS’17 Competition: Building Intelligent Systems*, 2018.
- [13] **Cihang Xie**, Jianyu Wang, Zhishuai Zhang, Yuyin Zhou, Lingxi Xie, Alan Yuille. Adversarial Examples for Semantic Segmentation and Object Detection. In *Proceedings of International Conference on Computer Vision (ICCV)*, IEEE, 2017.
- [14] Jianyu Wang, **Cihang Xie**, Zhishuai Zhang, Jun Zhu, Lingxi Xie, Alan Yuille. Detecting Semantic Parts on Partially Occluded Rigid Objects. In *Proceedings of British Machine Vision Conference (BMVC)*, 2017.

PREPRINTS

- [1] Yingwei Li, Song Bai, **Cihang Xie**, Zhenyu Liao, Xiaohui Shen, Alan Yuille. Regional Homogeneity: Towards Learning Transferable Universal Adversarial Perturbations Against Defenses, in Arxiv
- [2] Nicolas Papernot, Fartash Faghri, Nicholas Carlini, Ian Goodfellow, Reuben Feinman, Alexey Kurakin, **Cihang Xie**, Yash Sharma, Tom Brown, Aurko Roy, Alexander Matyasko, Vahid Behzadan, Karen Hambardzumyan, Zhishuai Zhang, Yi-Lin Juang, Zhi Li, Ryan Sheatsley, Abhibhav Garg, Jonathan Uesato, Willi Gierke, Yinpeng Dong, David Berthelot, Paul Hendricks, Jonas Rauber, Rujun Long, Patrick McDaniel. Technical Report on the Cleverhans v2.1.0 Adversarial Examples Library, in Arxiv
- [3] Jianyu Wang, Zhishuai Zhang, **Cihang Xie**, Vittal Premachandran, Alan Yuille. Unsupervised learning of object semantic parts from internal states of cnns by population encoding, in Arxiv

TALKS

- Adversarial Examples Improve Image Recognition**
Google BrainDec 2019
- Towards Robust Defense Against Adversarial Examples & Beyond**
University of Maryland, College ParkDec 2019
- Intriguing Adversarial Examples & How To Defend Against Them**
University of California, BerkeleySep 2019
University of California, San DiegoSep 2019
University of California, DavisSep 2019
Stanford UniversitySep 2019
Google BrainAug 2019
- Towards Transferable Adversarial Attacks & Robust Adversarial Defense**
Princeton UniversityMay 2019
- Feature Denoising for Improving Adversarial Robustness**
VALSE WebinarSep 2019
Google Ph.D. Intern Research ConferenceJul 2019
1st JHU Computer Vision WorkshopApr 2019
- An Introduction to Adversarial Attacks and Defenses**
Facebook AI ResearchJun 2018
- Mitigating Adversarial Effects Through Randomization**
NIPS 2017 Workshop on Adversarial Attacks and Defences CompetitionDec 2017

SELECTED AWARDS

- Facebook Fellowship**2020
- Finalist** of Facebook Fellowship2019
- No.1** in the defense track of the Competition on Adversarial Attacks and Defenses2018
Teammates: **Cihang Xie**, Yuxin Wu, Laurens van der Maaten, Alan Yuille and Kaiming He
- No.1** in the Competition on Adversarial Attacks and Defenses CTF SHANGHAI 20182018
Teammates: Yuxin Wu, **Cihang Xie**
- Snap Research University Collaboration Scholarship**2017

No.2 in the defense track of NIPS'17 Competition: Defending against Adversarial Attacks 2017
Teammates: **Cihang Xie**, Jianyu Wang, Zhishuai Zhang, Zhou Ren and Alan Yuille

WORKSHOP

Adversarial Machine Learning in Computer Vision, CVPR 2020

Organizers: **Cihang Xie**, Xinyun Chen, Song Bai, Bo Li, Kaiming He, Fei-Fei Li, Luc Van Gool, Philip Torr, Dawn Song, Alan Yuille

Website: <https://adv-workshop-2020.github.io/>

Adversarial Robustness in the Real World, ECCV 2020

Organizers: Adam Kortylewski, **Cihang Xie**, Song Bai, Zhaowei Cai, Yingwei Li, Andrei Barbu, Wieland Brendel, Nuno Vasconcelos, Andrea Vedaldi, Philip Torr, Rama Chellappa, Alan Yuille

ACADEMIC SERVICES

Conference Reviewer

- Computer Vision and Pattern Recognition (CVPR)
- European Conference on Computer Vision (ECCV)
- International Conference on Computer Vision (ICCV)
- Conference on Neural Information Processing Systems (NeurIPS)
- International Conference on Machine Learning (ICML)
- Winter Conference on Applications of Computer Vision (WACV)
- AAAI Conference on Artificial Intelligence (AAAI)
- Conference on Uncertainty in Artificial Intelligence (UAI)
- British Machine Vision Conference (BMVC)

Journal Reviewer

- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
- International Journal of Computer Vision (IJCV)
- IEEE Transactions on Neural Networks and Learning Systems (TNNLS)
- IEEE Transactions on Signal Processing (TSP)
- The Journal of Artificial Intelligence (AIJ)
- IEEE Transactions on Circuits and Systems for Video Technology (TCSVT)

OPEN SOURCES

Contributor to **tensorflow/cleverhans**

Codes and models on GitHub: <https://github.com/cihangxie>