Yinpeng Dong
Department of Computer Science and Technology, Tsinghua University
FIT building 1-509, Beijing, China, 100084
http://ml.cs.tsinghua.edu.cn/~yinpeng

Contact Information

Phone: (+86) 18603303421
Email: dongyinpeng@mail.tsinghua.edu.cn; dongyinpeng@gmail.com

Work Experience

Department of Computer Science and Technology 2022.01 -
Tsinghua University, Beijing, China
Postdoctoral Researcher, collaborated with Prof. Jun Zhu

Education

Department of Computer Science and Technology 2017.09 - 2022.01
Tsinghua University, Beijing, China
Ph.D, advised by Prof. Jun Zhu

Department of Computer Science and Technology 2013.08 - 2017.06
Tsinghua University, Beijing, China
Bachelor of Engineering
***GPA*: 94.4/100; *Rank*: 2/107**

Robotic Institute 2016.06 - 2016.09
Carnegie Mellon University, Pittsburgh, US
Visiting Student

Department of Electrical Engineering and Computer Science 2015.06 - 2015.07
National Tsing Hua University, Hsinchu, Taiwan
Exchange Student

Publications

(* indicates equal contribution)

ViewFool: Evaluating the Robustness of Visual Recognition to Adversarial Viewpoints
Yinpeng Dong, Shouwei Ruan, Hang Su, Caixin Kang, Xingxing Wei, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2022*

Pre-trained Adversarial Perturbations
Yuanhao Ban and **Yinpeng Dong**
*Advances in Neural Information Processing Systems (**NeurIPS**), 2022*

Isometric 3D Adversarial Examples in the Physical World
Yibo Miao, **Yinpeng Dong**, Jun Zhu, and Xiao-Shan Gao
*Advances in Neural Information Processing Systems (**NeurIPS**), 2022*

Boosting Transferability of Targeted Adversarial Examples via Hierarchical Generative Networks
Xiao Yang, **Yinpeng Dong**, Tianyu Pang, Hang Su, and Jun Zhu
*European Conference on Computer Vision (**ECCV**), 2022*

AutoDA: Automated Decision-based Iterative Adversarial Attacks
Qi-An Fu, **Yinpeng Dong**, Hang Su, Jun Zhu, and Chao Zhang
*31st USENIX Security Symposium (**USENIX Security ’22**), 2022*

GSmooth: Certified Robustness against Semantic Transformations via Generalized

Randomized Smoothing
Zhongkai Hao, Chengyang Ying, **Yinpeng Dong**, Hang Su, Jian Song, and Jun Zhu
*International Conference on Machine Learning (**ICML**), 2022*

Two Coupled Rejection Metrics Can Tell Adversarial Examples Apart
Tianyu Pang, Huishuai Zhang, Di He, **Yinpeng Dong**, Hang Su, Wei Chen, Jun Zhu, and Tie-Yan Liu
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2022*

Exploring Memorization in Adversarial Training
Yinpeng Dong, Ke Xu, Xiao Yang, Tianyu Pang, Zhijie Deng, Hang Su, and Jun Zhu
*International Conference on Learning Representations (**ICLR**), 2022*

Query-Efficient Black-box Adversarial Attacks Guided by a Transfer-based Prior
Yinpeng Dong*, Shuyu Cheng*, Tianyu Pang, Hang Su, and Jun Zhu
*IEEE Transaction on Pattern Analysis and Machine Intelligence (**TPAMI**), 2021*

Accumulative Poisoning Attacks on Real-time Data
Tianyu Pang, Xiao Yang, **Yinpeng Dong**, Hang Su, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2021*

Black-box Detection of Backdoor Attacks with Limited Information and Data
Yinpeng Dong, Xiao Yang, Zhijie Deng, Tianyu Pang, Zihao Xiao, Hang Su, and Jun Zhu
*International Conference on Computer Vision (**ICCV**), 2021*

Towards Face Encryption by Generating Adversarial Identity Masks
Xiao Yang, **Yinpeng Dong**, Tianyu Pang, Hang Su, Jun Zhu, Yuefeng Chen, and Hui Xue
*International Conference on Computer Vision (**ICCV**), 2021*

Improving Transferability of Adversarial Patches on Face Recognition with Generative Models
Zihao Xiao, Xianfeng Gao, Chilin Fu, **Yinpeng Dong**, Wei Gao, Xiaolu Zhang, Jun Zhou, and Jun Zhu
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2021*

Bag of Tricks for Adversarial Training
Tianyu Pang, Xiao Yang, **Yinpeng Dong**, Hang Su, Jun Zhu
*International Conference on Learning Representations (**ICLR**), 2021*

Adversarial Distributional Training for Robust Deep Learning
Yinpeng Dong*, Zhijie Deng*, Tianyu Pang, Hang Su, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2020*

Understanding and Exploring the Network with Stochastic Architectures
Zhijie Deng, **Yinpeng Dong**, Shifeng Zhang, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2020*

Boosting Adversarial Training with Hypersphere Embedding
Tianyu Pang*, Xiao Yang*, **Yinpeng Dong**, Kun Xu, Hang Su, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2020*

Benchmarking Adversarial Robustness on Image Classification (**Oral**)
Yinpeng Dong, Qi-An Fu, Xiao Yang, Tianyu Pang, Hang Su, Zihao Xiao, and Jun Zhu
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2020*

Rethinking Softmax Cross-Entropy Loss for Adversarial Robustness
Tianyu Pang, Kun Xu, **Yinpeng Dong**, Chao Du, Ning Chen, and Jun Zhu
*International Conference on Learning Representations (**ICLR**), 2020*

Improving Black-box Adversarial Attacks with a Transfer-based Prior
Shuyu Cheng*, **Yinpeng Dong***, Tianyu Pang, Hang Su, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2019*

Evading Defenses to Transferable Adversarial Examples by Translation-Invariant Attacks (**Oral**)
Yinpeng Dong, Tianyu Pang, Hang Su, and Jun Zhu
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2019*

Efficient Decision-based Black-box Adversarial Attacks on Face Recognition
Yinpeng Dong, Hang Su, Baoyuan Wu, Zhifeng Li, Wei Liu, Tong Zhang, and Jun Zhu
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2019*

Stochastic Quantization for Learning Accurate Low-bit Deep Neural Networks
Yinpeng Dong, Renkun Ni, Jianguo Li, Yurong Chen, Hang Su, and Jun Zhu
*International Journal of Computer Vision (**IJCV**), 2019*

Composite Binary Decomposition Networks
You Qiaoben, Zheng Wang, Jianguo Li, **Yinpeng Dong**, Yu-Gang Jiang, and Jun Zhu
*The Thirty-Third AAAI Conference on Artificial Intelligence (**AAAI**), 2019*

Towards Robust Detection of Adversarial Examples (**Spotlight**)
Tianyu Pang, Chao Du, **Yinpeng Dong**, and Jun Zhu
*Advances in Neural Information Processing Systems (**NeurIPS**), 2018*

Boosting Adversarial Attacks with Momentum (**Spotlight**)
Yinpeng Dong, Fangzhou Liao, Tianyu Pang, Hang Su, Jun Zhu, Xiaolin Hu, and Jianguo Li
*IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2018*

Defense against Adversarial Attacks Using High-Level Representation Guided Denoiser
Fangzhou Liao*, Ming Liang*, **Yinpeng Dong**, Tianyu Pang, Jun Zhu, and Xiaolin Hu
*IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2018*

Learning Visual Knowledge Memory Networks for Visual Question Answering
Zhou Su, Chen Zhu, **Yinpeng Dong**, Dongqi Cai, Yurong Chen, and Jianguo Li
*IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2018*

Learning Accurate Low-Bit Deep Neural Networks with Stochastic Quantization (**Oral, Best Paper Nomination**)
Yinpeng Dong, Renkun Ni, Jianguo Li, Yurong Chen, Jun Zhu, and Hang Su
*British Machine Vision Conference (**BMVC**), 2017*

Forecast Plausible Paths in Crowd Scenes
Hang Su, Jun Zhu, **Yinpeng Dong**, and Bo Zhang
*International Joint Conference on Artificial Intelligence (**IJCAI**), 2017*

Improving Interpretability of Deep Neural Networks with Semantic Information
Yinpeng Dong, Hang Su, Jun Zhu, and Bo Zhang
*IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2017*

Efficient and Robust Semi-supervised Learning over a Sparse-Regularized Graph
Hang Su, Jun Zhu, Zhaozheng Yin, **Yinpeng Dong**, and Bo Zhang
*European Conference on Computer Vision (**ECCV**), 2016*

Crowd Scene Understanding with Coherent Recurrent Neural Networks
Hang Su, **Yinpeng Dong**, Jun Zhu, Haibin Ling, and Bo Zhang
*International Joint Conference on Artificial Intelligence (**IJCAI**), 2016*

Preprints & Workshops

BadDet: Backdoor Attacks on Object Detection
Shih-Han Chan, **Yinpeng Dong**, Jun Zhu, Xiaolu Zhang, Jun Zhou
ECCV 2022 workshop on Adversarial Robustness in the Real World, 2022

Adversarial Vision Challenge
Wieland Brendel, Jonas Rauber, Alexey Kurakin, Nicolas Papernot, Behar Veliqi, Sharada P. Mohanty, Florian Laurent, Marcel Salathé, Matthias Bethge, Yaodong Yu, Hongyang Zhang, Susu Xu, Hongbao Zhang, Pengtao Xie, Eric P. Xing, Thomas Brunner, Frederik Diehl, Jérôme Rony, Luiz Gustavo Hafemann, Shuyu Cheng, **Yinpeng Dong**, Xuefei Ning, Wenshuo Li, Yu Wang
NeurIPS 2018 Competition Chapter, 2019

Batch Virtual Adversarial Training for Graph Convolutional Networks
Zhijie Deng, **Yinpeng Dong**, and Jun Zhu
ICML 2019 Workshop on Learning and Reasoning with Graph-Structured Representation, 2019

Towards Interpretable Deep Neural Networks by Leveraging Adversarial Examples
Yinpeng Dong, Hang Su, Jun Zhu, Fan Bao, and Bo Zhang
AAAI 2019 Workshop on Network Interpretability for Deep Learning, 2019

Adversarial Attacks and Defences Competition
Alexey Kurakin, Ian Goodfellow, Samy Bengio, **Yinpeng Dong**, Fangzhou Liao, Ming Liang, Tianyu Pang, Jun Zhu, Xiaolin Hu, et al.
NeurIPS 2017 Competition Chapter, 2018

Feature Engineering and Ensemble Modeling for Paper Acceptance Rank Prediction
Yujie Qian*, **Yinpeng Dong***, Ye Ma*, Hailong Jin, and Juanzi Li
KDD Workshop KDDCUP, 2016

Selected Awards

National Postdoctoral Innovative Talents Support Program	2022.06
Shuimu Tsinghua Scholar Program	2022.01
Beijing Outstanding Graduates	2022.01
ByteDance Scholars Program	2020.11

Tsinghua-HUAWEI Scholarship 2020.10

Baidu Fellowship 2020.01

‘84’ Future Innovation Scholarship 2019.12

Microsoft Research Asia (MSRA) Fellowship 2019.11

China National Scholarship 2019.10

VALSE Annual Outstanding Student Paper Award 2019.04

CCF-CV Academic Emerging Award 2018.11

China National Scholarship 2018.10

Tsinghua University Future PhD Fellowship 2017.09

Challenges

The 1st palce in GeekPwn DeepFake competition (Shanghai) 2020.10

The 1st palces in GeekPwn CAAD CTF and Adversarial Patch competitions (Shanghai) 2019.10

The 2nd place in the Untargeted Attack track of NeurIPS 2018 Adversarial Vision Challenge 2018.11

The 2nd places in Targeted Attack track, Defense track, and the 3rd place in Non-targeted Attack track of GeekPwn CAAD competition 2018.9

The 1st palce in GeekPwn CAAD CTF competition (Las Vegas) 2018.8

The 1st places in NeurIPS 2017 Adversarial Attacks and Defenses 2017.10

The 2nd place in KDDCUP 2016 2016.7

Services

Organizer for:
ECCV 2022 Workshop on Adversarial Robustness in the Real World
AAAI 2022 Workshop on Adversarial Machine Learning and Beyond
ICML 2021 Workshop on A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning
ICCV 2021 Workshop on Adversarial Robustness in the Real World
CVPR 2021 Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems and Online Challenges (AML-CV)

Reviewer for:
TPAMI 2019, 2020, 2021, 2022
IJCV 2021, 2022
TIP 2019, 2020, 2021
TNNLS 2019, 2020
NeurIPS 2016, 2019, 2020, 2021, 2022
ICML 2019, 2021, 2022
CVPR 2019, 2020, 2021, 2022
ICLR 2020, 2021, 2022, 2023

ICCV 2019, 2021
ECCV 2020
AAAI 2019, 2020, 2021
IJCAI 2019, 2020

Teaching

2019 Spring, **Head TA** in *Statistical Machine Learning*, instructed by Prof. Jun Zhu