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: dyp17@mails.tsinghua.edu.cn; dongyinpeng@gmail.com

Education

Department of Computer Science and Technology — 2017.09 -
Tsinghua University, Beijing, China
Ph.D. Student, 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

Computer Skills

Languages: C, C++, Python, Cuda.
Mathematical Computation: Matlab
Deep Learning Tools: Theano, Tensorflow, Caffe, Pytorch.
Operating Systems: Linux, Mac OSX, Windows.

Publications

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

Towards Robust Detection of Adversarial Examples (**Spotlight**)
Tianyu Pang, Chao Du, **Yinpeng Dong**, and Jun Zhu

*Advances in Neural Information Processing Systems (**NeurIPS**), Montreal, Canada, 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**), Salt Lake City, USA, 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**), Salt Lake City, USA, 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**), Salt Lake City, USA, 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**), London, UK, 2017*

Forecast Plausible Paths in Crowd Scenes
Hang Su, Jun Zhu, **Yinpeng Dong**, and Bo Zhang
*International Joint Conference on Artificial Intelligence (**IJCAI**), Melbourne, Australia, 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**), Honolulu, Hawaii, USA, 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**), Amsterdam, The Netherlands, 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**), New York, USA, 2016*

Preprints & Workshops

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.
NIPS 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 (* indicates equal contribution)
KDD Workshop KDDCUP, 2016

Selected Awards

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

Tsinghua Outstanding Graduates 2017.06

Beijing Outstanding Graduates 2017.06

Outstanding Thesis 2017.06

Zhong Shimo Scholarship 2016.12

Zhong Shimo Scholarship 2015.12

The CCF Outstanding Undergraduate Award 2015.06

ST Engineering Overseas Scholarship 2015.05

China National Scholarship 2014.10

Challenges

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

Reviewer: TIP, TPAMI, NeurIPS 2019, ICCV 2019, IJCAI 2019, ICML 2019, CVPR 2019, AAAI 2019, NeurIPS 2016, UAI 2016