CHAOFEI YANG

+1(412) 944-8566 ⋄ Union City, CA
ycf418@gmail.com ⋄ LinkedIn ⋄ Google Scholar

OBJECTIVE

Machine Learning Engineer with 2+ years of experience in recommendation system.

EDUCATION

PhD of Computer Engineering, Duke University 2017 - 2020
Advisor: Yiran Chen and Hai Li
Research Interest: Machine learning security, neuromorphic computing.

Master of Computer Engineering, University of Pittsburgh 2014 - 2017
Advisor: Yiran Chen and Hai Li

Bachelor of Electronic Engineering, Tsinghua University 2010 - 2014

PROFESSIONAL EXPERIENCE

Research Scientist Aug 2020 - Present
Meta *Menlo Park, CA*

- Build large-scale recommendation models with data preparation, ML algorithms, and end-to-end evaluation.
- Explore state-of-the-art modeling techniques such as advanced data augmentation, hierarchical architecture, and multi-domain multi-task learning.
- Improve training optimization for large-scale models with massive distributed GPU clusters.

Software Engineer (ML) Intern Jun 2019 - Aug 2019
Facebook *Menlo Park, CA*

- Identify a new policy in ads. Implement an adversarial image synthesis API with various manipulation functions, based on this policy. Construct a synthetic dataset at scale.
- Explore transfer learning and end-to-end training of classification models, with the help of the synthetic data.
- Productionize the models and evaluate them on real ads images.

Deep Learning Intern May 2018 - Aug 2018
KLA-Tencor *Milpitas, CA*

- Propose the outlier-excluded adaptive clipping and mask normalization to preprocess the wafer images, in order to address the discrepancy across wafers from different fabs.
- Propose to leverage gamma correction to alter the contrast of wafer images, thus augmenting the data (which is very limited), combining with random rotation.
- Corporate with other teams to leverage the company's internal library and implement the project on Tensorflow.

RESEARCH PROJECTS

Defense against Deepfake Attack using Adversarial Faces 2019 - 2020
Advisor: Yiran Chen and Hai Li

- Explore attack techniques in Deepfake using generative adversarial networks.
- Propose to leverage transformation-aware adversarial faces against discriminator to defend Deepfake, by consistently yielding more artifacts in synthesized faces.
- Demonstrate effectiveness and through extensive experiments under various settings based on multiple metrics.

Neural Network Security Exploration, Attacks and Defenses 2016 - 2019
Advisor: Yiran Chen and Hai Li

- Explore poisoning attacks against machine learning models, specifically neural networks, by analyzing the calculation of gradients.
- Propose a generative method to accelerate the poisoned sample generation speed while maintaining reasonable attack performance.
- Explore novel offense and defense methods of adversarial attacks.

Neuromorphic Chip Design and Hardware Security 2014 - 2016
Advisor: Yiran Chen and Hai Li

- Develop and implement neural network models in neuromorphic chips, e.g., memristor-based crossbars, for designated applications, e.g., image classification.
- Cooperate with the hardware team to adapt algorithms to real device constraints.
- Identify security threats targeting on the neuromorphic computing system and develop hardware-based solutions.

SKILLS

Programming languages	Python, C/C++, Matlab, Java, Shell, SQL, Verilog
Deep learning frameworks	PyTorch, Caffe2, Tensorflow, Keras
EDA	Cadence Virtuoso, ModelSim

SELECTED PUBLICATIONS

[1] **Chaofei Yang**, Leah Ding, Yiran Chen, Hai Li, Defending against gan-based deepfake attacks via transformation-aware adversarial faces, IJCNN, 2021

[2] **Chaofei Yang**, Hai Li, Yiran Chen, Jiang Hu, Enhancing generalization of wafer defect detection by data discrepancy-aware preprocessing and contrast-varied augmentation, ASP-DAC, 2020

[3] **Chaofei Yang**, Beiye Liu, Hai Li, Yiran Chen, Wujie Wen, Mark Barnell, Qing Wu, Jeyavijayan Rajendran, Thwarting Replication Attack against Memristor-based Neuromorphic Computing System, TCAD, 2019

[4] **Chaofei Yang**, Qing Wu, Hai Li, Yiran Chen, Generative poisoning attack method against neural networks, arXiv, 2017

[5] Amr M. Hassan, **Chaofei Yang**, Chenchen Liu, Hai Li, Yiran Chen, Hybrid spiking-based multi-layered self-learning neuromorphic system based on memristor crossbar arrays, DATE, 2017

[6] **Chaofei Yang**, Beiye Liu, Hai Li, Yiran Chen, Wujie Wen, Mark Barnell, Qing Wu, Jeyavijayan Rajendran, Security of neuromorphic computing: thwarting learning attacks using memristor's obsolescence effect, ICCAD, 2016

[7] **Chaofei Yang**, Chunpeng Wu, Hai Li, Yiran Chen, Mark Barnell, Qing Wu, Security challenges in smart surveillance systems and the solutions based on emerging nano-devices, ICCAD, pp. 1-6, 2016

[8] Chenchen Liu, Bonan Yan, **Chaofei Yang**, Linghao Song, Zheng Li, Beiye Liu, Yiran Chen, Hai Li, Qing Wu, Hao Jiang, A spiking neuromorphic design with resistive crossbar, DAC, 2015