Chen Liu

+41 78 838 33 84 • chen.liu@epfl.ch • Birth: 21st,Jan,1993

Education

- **École polytechnique fédérale de Lausanne(EPFL)** **Lausanne, Switzerland**
  PhD in Computer Science *2017-*
  Topic: adversarial robustness in deep learning. Supervisors: Prof. Sabine Süsstrunk, Dr. Mathieu Salzmann
- **École polytechnique fédérale de Lausanne(EPFL)** **Lausanne, Switzerland**
  M.S in Computer Science *2015-2017*
  GPA: 5.73/6.00 Transcript
- **Tsinghua University** **Beijing, China**
  B.ENG in Computer Science and Technology *2011-2015*
  GPA: 91.34/100.00 Rank 9/123 Transcript Graduated with Distinction

Research & Work Experiences

- **Swisscom Digital Lab** **Feb, 2017–Aug,2017**
  Lausanne Switzerland *Internship*
  - Automatic document summarization by sequence-to-sequence model with attention mechanism.
- **Siemens Research (USA)** **Jul,2016–Feb,2017**
  Princeton, New Jersey, USA *Research Intern*
  - Deep metric learning by triplet neural networks to automatically tune parameters of a 3D medical imaging renderer to obtain images of consistent visual effect.

Publications

- Chen Liu, Zhichao Huang, Mathieu Salzmann, Tong Zhang, Sabine Süsstrunk. "Hard Adversarial Instances Lead to Overfitting in Adversarial Training". *Under submission*.
- Zhichao Huang, Chen Liu, Mathieu Salzmann, Sabine Süsstrunk, Tong Zhang. "Improving Adversarial Defense with Self-supervised Test-time Fine-tuning". *Under submission*.
- Chen Liu, Mathieu Salzmann, Sabine Süsstrunk. "Training Provably Robust Models by Polyhedral Envelope Regularization". *IEEE Transactions on Neural Networks and Learning Systems 2021*.
- Chen Liu, Mathieu Salzmann, Tao Lin, Ryota Tomioka, Sabine Süsstrunk. "On the Loss Landscape of Adversarial Training: Identifying Challenges and How to Overcome Them". *Neural Information Processing Systems (NeurIPS) 2020*.
- Chen Liu, Ryota Tomioka, Volkan Cevher. "On Certifying Non-uniform Bounds against Adversarial Attacks". In *International Conference on Machine Learning (ICML) 2019*.
- Ya-Ping Hsieh, Chen Liu, Volkan Cevher. "Finding the Mixed Nash Equilibria of Generative Adversarial Networks". In *International Conference on Machine Learning (ICML) 2019*. Oral Presentation in *Smooth Games Optimization and Machine Learning Workshop in NeurIPS 2018*.
- Chen Liu, Shun Miao, Kaloian Petkov, Sandra Sudarsky, Daphne Yu, Tommaso Mansi. "Consistent 3D Rendering in Medical Imaging". *European Patent No. 18160956.1 - 1208*.

Professional Service

Reviewer: ICML, NeurIPS, ICLR

Awards & Honors

- Qualcomm Innovation Fellowship Europe 2020 Finallist (15 in Europe)
- ICML Travel Award (2019)
- Microsoft Research Scholarship.(MSR sponsored student 2017 - 2019)
- Outstanding Undergraduate Students in Department of Computer Science and Technology in Tsinghua University.(2015)
- Scholarship of Academic Excellence in Tsinghua University.(2014)
- Scholarship of Social Work in Tsinghua University.(2013)
- Scholarship of Academic Excellence in Tsinghua University.(2013)
- First Prize in Beijing College Student Physics Competition. (2012)

Mentorship

EPFL Mater student:
Ningwei Ma. "Adversarial Robustness for Neural Ordinary Differential Equations."
Yulun Jiang. "Adversarial Robustness for Multiple Threat Models".
Ziqi Zhao. "Network Pruning in Adversarial Training".
EPFL Bachelor student:
Majdouline Ait Yahia. "Robust Binary Network".

Skills

- Programming Language: Python, C/C++, Matlab, Java.
- Deep Learning Tools: Pytorch, Tensorflow, Keras, Theano.
- Natural Language: Mandarin(Native), English(Fluent).

External Links

- Github: Codes. https://github.com/liuchen11
- Homepage: Projects. https://liuchen11.github.io