YITAO XU

study0098@gmail.com ◇ Homepage ◇ Google Scholar ID

EDUCATION

M.Sc. Computer Science, Exchange, École Polytechnique Fédérale de Lausanne, EPFL 2022-Present

M.Sc. Machine Learning, KTH Royal Institute of Technology 2021-Present

B.Eng. Computer Science, Beihang University 2016-2020

RESEARCH EXPERIENCE

-Research Intern, Image and Visual Representation Lab, EPFL 06.2022 - Present

-Advisor: Ehsan Pajouheshgar, Prof. Sabine Süsstrunk

Topic: Real-time Dynamic Texture Synthesis using Neural Cellular Automata

- Proposed DyNCA to synthesize dynamic texture videos of arbitrary size and infinite length in real time, while all current SOTA methods can only synthesize a short, fixed-size video in a few hours.
- Devised multi-scale perception and positional encoding to enhance performance of the vanilla NCA on texture learning.
- DyNCA can synthesize more realistic texture videos than current methods, as shown by an extensive user study on 150 persons, each required to assess the realism of nearly 60 videos.
- Built an interactive demo, providing many real-time interaction tools with DyNCA.

-Research Assistant, Tsinghua Laboratory of Brain and Intelligence, Tsinghua University

-Advisor: Prof. Jia Liu 11.2020 - 05.2021

Topic: Towards Machines Understanding Physics: Block Tower Stability Inference

- Developed the algorithm to make machines infer the stability of block towers like humans using shape-bias-enhanced CNN.
- Demonstrated the consistency of DNN and humans at the computational level of probabilistic judgments of block-tower stability, through an extensive user study on more than 50 people and 100 block towers.
- Developed a platform for physical event simulation.

-Research Intern, State Key Laboratory of Software Development Environment,Beihang University

-Advisor: Prof. Xianglong Liu 04.2019 - 05.2020

Topic 1: Interpreting Convolutional Neural Networks (CNN) with Neuron Sensitivity

- Proposed a new method for interpreting various popular CNN via analyzing sensitive neurons by segmenting the input images, and proved their criticalness for CNN via neuron ablation study.
- Developed a new method to train robust CNN against adversarial attacks by stabilizing sensitive neurons, achieving SOTA defense performance against adversarial attacks.

Topic 2: Adversarial Attack against the Agent in Embodied Question Answering

- Developed the algorithm to perform adversarial attacks against the embodied agent, with SOTA attacking performance.
- Proposed spatially contextual attack and helped develop temporal attention method to improve the attacking efficiency.

Topic 3: Analysis and Rectification of Texture Bias in Convolutional Neural Networks

- Analyzed texture and shape bias in CNN and validate the texture bias of trained CNN.
- Proposed the algorithm to obtain shape-related and texture-related feature maps inside a CNN via distorting the shape or texture of the input images.
- Proposed the new loss function to enhance the shape bias of a CNN via minimizing the cosine distance between shape-related feature maps and the original ones, improving the SOTA adversarial training methods.

PUBLICATIONS

PUBLISHED

- Chongzhi Zhang, Aishan Liu, Xianglong Liu, **Yitao Xu**, et al. (2020). Interpreting and improving adversarial robustness of deep neural networks with neuron sensitivity. IEEE Transactions on Image Processing, 30, 1291-1304.
- Aishan Liu, Tairan Huang, Xianglong Liu, **Yitao Xu**, et al. (2020, August). Spatiotemporal attacks for embodied agents. In European Conference on Computer Vision (pp. 122-138). Springer, Cham.
- Tianlin Li, Aishan Liu, Xianglong Liu, **Yitao Xu**, et al. (2021). Understanding adversarial robustness via critical attacking route. Information Sciences, 547, 568-578.

PREPRINT

- Ehsan Pajouheshgar*, **Yitao Xu***,Tong Zhang, and Sabine Süsstrunk. DyNCA: Real-time Dynamic Texture Synthesis Using Neural Cellular Automata. arXiv preprint arXiv:2211.11417, 2022.

*: Equal contribution.

WORK EXPERIENCE

-Machine Learning Intern, DiDi AI Labs, DiDi Global Inc. 06.2020 - 11.2020

-Group Leader: Dr. Zhengping Che, Prof. Jian Tang

Project 1: Embedded Real-time UAV Pedestrian Detection

- Developed an interpolation-based framework for pedestrian detection in 2K UAV videos using EfficientDet in TensorRT.
- The proposed method works 3 times faster than the vanilla EfficientDet on a real-world dataset without losing performance (84.4 mAP and $\sim$ 10 FPS on Nvidia Jetson TX2 platform). Patent granted.

Project 2: 3D LiDAR Point Cloud Object Detection on nuScenes Dataset

- Used Gaussian pyramid and multi-model fusion to boost the performance of 3d LiDAR object detection. Ranked 1/42 on nuScences detection leaderboard, team PVC-ensemble, 09/12/2020.

HONOURS AND AWARDS

- **Outstanding Undergraduate** of Beihang University, 11.2019
- **Outstanding Undergraduate** of Beihang University, 11.2018
- **Outstanding Undergraduate** of Beihang University, 11.2017
- **Scholarship for Academic Merit**, Beihang University, 09.2016

TEACHING

-Department of Psychology, Tsinghua University

Course: Advances in Cognitive Science 02.2021 - 05.2021

- Gave a 2-hour lecture on the development of Symbolism, based on chapter 3.2-3,4 in "Mind, body, world: foundations of cognitive science". slides.

VOLUNTEERING

-Volunteer tutor for junior students at Beihang University. 09.2017 - 06.2018

Mentor junior students on core courses, including "Principles of Computer Organization", "Algorithmic Design and Analysis", "Probability and Statistics".