YEH, CHIN-YUAN

(+886)972311499 ⋄ marrch30@gmail.com
11088 5F., No. 22, Aly. 5, Ln. 423, Sec. 5,
Zhongxiao E. Rd., Xinyi Dist., Taipei, Taiwan

SUMMARY

Pursuing PhD degree in research on Deep learning. 3 years' experience researching with Pytorch. Bilingual: English and Mandarin Chinese.

CURRENT POSITION

PhD Candidate. Advisor: Professor Chen, Ming-Syan *August 2020 - now*

Data Science Program, Graduate Institute of Communication Science, National Taiwan University

EDUCATION

National Taiwan University *January 2018 - April 2020*
Master of Science
Department of Electrical Engineering Graduate GPA: 3.74

National Taiwan University *September 2013 - June 2017*
Bachelor of Science
Department of Physics Graduate GPA: 3.86

SELECTED RESEARCH WORKS

Attack as the Best Defense: Nullifying Image-to-image Translation GANs via Limit-aware Adversarial Attack (paper accepted to ICCV 2021)
This work propose a query-based black box attack against Img2Img GAN. Compared to classifiers, Img2Img models utilize a much larger model capacity and requires more deviations in the output layer to justify a successful attack. However, with the Limit-Aware Self-Guiding Gradient Sliding Attack, we are able to effectively attack and cancel ethics-concerning functions. In addition, we are also able to distort safety-critical applications (e.g., semantic segmentation of street scenes). The techniques utilized in the methods includes: 1) limit-aware RGF, which estimates gradient that adheres to the adversarial limit; 2) a gradient sliding mechanism which accelerate the gradient descent process; 3) an effective self-guiding prior extracted solely from the threat model and the target input.

Disrupting Image-Translation-Based DeepFake Algorithms with Adversarial Attacks (paper accepted to WACV2020 DeepPAB Workshop)
This work addresses the serious challenge presented by DeepNude, a Deepfake application that undresses photography of any human being, by introducing the novel aspect of adversarially attacking the DeepFake model. Projected Gradient Descent (PGD) Attack is utilized with modifications on image translation GANs including CycleGAN, pix2pix, and pix2pixHD models trained with CelebA dataset. Two attacks are proposed, including the Nullifying Attack, which causes the attacked model to output an image similar to the input, and the Distorting Attack, which causes the model to output a distorted figure. Source code is provided in Pytorch.
Github URL: https://github.com/jimmy-academia/Adversarial-Attack-CycleGAN-and-pix2pix

TECHNICAL STRENGTHS

Programming Language	Python & Pytorch
Software & Tools	Unix System, Bash scripts, Latex, Blender

WORK EXPERIENCE

Institute of Information Science, Academia Sinica *April - August 2020*
Graduate Research Assistant

- Studied Graph Neural Network, optimization techniques to further the research on black-box adversarial attacks. Provided assistant in hosting conference (The International Conference on Database Systems for Advanced Applications, DASFAA), review papers, and proposal translation and writing.

Department of Electrical Engineering, National Taiwan University *August 2018 - April 2020*
Research Assistant

- Researched on ”Disrupting Image-Translation-Based DeepFake Algorithms with Adversarial Attacks” and ”Black-box Attack on Image-Translation GANs” under advisor, Professor Wang, Sheng-De.

Shalom Inc. 旅安資訊 *March - August 2018*
Software Engineer Intern

- On-site internship under this leading tech company dedicated to providing information infrastructures for hotel management. Completed various tasks including setting up AWS cloud server, writing scripts for automatic pricing update script via custom APIs, and fetching customer information from records.

Institute of Physics, Academia Sinica *February - July 2016*
Undergraduate Research Assistant

- Researched ”Growth and Analysis of Flexible Oxide Electronic Materials” under advisors, Professor Chang, Chia-Seng and Professor Chu, Ying-Hao.

OTHER EXPERIENCE

Mandatory military training in the Republic of China (Taiwan) Marine Corps. *June - October 2017*

One year exchange student at the University of British Columbia. *September 2016 - May 2017*

Chief editor of the 34th issue of “SpaceTime,” the department journal of the Department of Physics, National Taiwan University. *January 2013*