SHENG-YEN CHOU

@ unaxultraspaceos5@gmail.com ⚲ Hsinchu, Taiwan in Sheng-Yen Chou ⚙ FrankCCCCC ⚲ Blog ⚲ Google Scholar

PUBLICATION

How to Backdoor Diffusion Models?

Sheng-Yen Chou, Pin-Yu Chen, and Tsung-Yi Ho
- CVPR 2023, ICLR'23 BANDS Workshop Best Paper

VillanDiffusion: A Unified Backdoor Attack Framework for Diffusion Models

Sheng-Yen Chou, Pin-Yu Chen, and Tsung-Yi Ho
- Under Submission

Single-level Adversarial Data Synthesis based on Neural Tangent Kernels

Yu-Rong Zhang, Ruei-Yang Su, Sheng Yen Chou, and Shan-Hung Wu
- ArXiv

EDUCATION

B.S. Computer Science
National Tsing Hua University
- 📅 2017 – 2022   ⚲ Hsinchu, Taiwan

Change major from Power Mechanical Engineering in 2019

RESEARCH EXPERIENCE

Research Internship
🏛 Carnegie Mellon University   📅 Jun 2023 – Present
- Collaborate with Safe AI Lab
- Apply diffusion models to augment tiny image-caption dataset.

Research Assistant
🏛 The Chinese University of Hong Kong   📅 Jul 2022 – Present   ⚲ Hong Kong
- Supervised by Prof. Tsung-Yi Ho and Pin-Yu Chen
- Propose a new attack to backdoor diffusion model, called BadDiffusion. We can backdoor DDPM with only 5% poison rate on CIFAR10 dataset.
- Propose a generalized attack to backdoor various diffusion model, called VillanDiffusion.

Research Assistant
🏛 National Ting Hua University   📅 Feb 2020 – Jun 2022   ⚲ Hsinchu, Taiwan
- Supervised by Prof. Shan-Hung Wu
- Engage in **machine learning** and **distributed database** researches.
- **Machine Learning**
  - We derive a new **single level objective from the bilevel optimization problem of GANs** to stabilize the training process based on the Neural Tangent Kernels (NTKs), which formulate a closed-form approximation.
  - I **derive the convergence guarantee** of out method, GA-NTK.
  - Our method GA-NTK can **generate competitive images with only 64 ~256 training images in comparison to SOTA GANs.**
- **Distributed Database**
  - Implement the **prototype of the "DependencyAnalyzer" component for the open source database projects: VanillaCore**
  - **Reproduce some experiments of the paper MB2: Decomposed Behavior Modeling for Self-Driving Database Management Systems in the open source database project: ElaSQL.**
  - Survey the papers that apply reinforcement learning and machine learning on the database system.
- AAAI'21 Paper Review
- CS565600: Deep Learning Teaching Assistant

PROJECTS

EfficientDet
- An **EfficientDet implementation in TF2.0** based on the paper EfficientDet: Scalable and Efficient Object Detection on CVPR'20.
- Project Page

DRL Collection
- A collection of implements of classical DRL algorithms. It contain modular **implementations of A3C, A2C, DDQN, and REINFORCE(naive) with Tensorflow2.0.**
- Project Page

ML Collection

- Implemetation and derivation of ML algorithms, including **SVM and VBGMM in Python.**
- Project Page

SKILLS

C++   Tensorflow/PyTorch/Jax   Python   Java   React/React Native   Diffusion Model

WORKING EXPERIENCE

Project Leader

🏛 Campus Delivery Project   📅 Sep 2018 - Dec 2018   📍 Hsinchu, Taiwan

- Build a delivery service with reusable containers with business associate Ching Piao.
- I lead an 8 people execution team and the project became the Green Pepper Delivery and **it served 100 people every day.**
- Project Demo

IT Internship / Expatriate Maintaining Engineer / Project Manager

🏛 ChingPiao   📅 Aug 2018 – Jul 2019   📍 Taipei, Taiwan

- Build an online rental service running at Liu-Qui island for Pingtung County Government. Communicate with partner IT company.
- **We've achieved the 1000 membership within 1.5 months and predict to achieve 200 daily usages.**
- **Create an APP(Ching Piao Rental Service POS) and double the speed of the service.**
- Official page

Co-founder / Software Engineer / Business Development

🏛 LEAFHOPPER.IO   📅 May 2019 - Dec 2020   📍 Hsinchu, Taiwan

- **Cooperate with the Lu-Gu township government** and **create immutable traceability for Dong Ding Oolong tea**. We've **invited to hold a open tender valued 2 million NTD**.
- I lead a team of 7 people and negotiated with local farmers. I also built up a tea traceability system with **Postgres, React and, Ethereum.**
- Official Page