Mao Po-Yuan

+81-80-9649-6720 mao.kyushu@gmail.com Mao Po-Yuan

Educational Background and Awards

Master of Science, *(Information Science) GPA : 3.7/4* **Fukuoka, Japan** *Kyushu University*
10/2022 - 09/2024
Global Program (Taught in English)
Graduation thesis: Understanding Robustness and Safety of Diffusion Model
Awarded:
Third Place in "Generative AI and LLMs Hackathon" organized by US-JAPAN Collaborative Workshop: Accelerating IC Design Phase II

Bachelor of Science, *(Mechanical Engineering)* **Taichung, Taiwan** *National Chung Hsing University*
09/2016 - 06/2020
Graduation project: Nano-scale Stereolithography 3D Printer
Awarded :
Best Innovation "2019 National University Industry and Academic Innovation Competition"
Honorable Mention "2019 Taiwan Precision Engineering Technology Symposium Hanmin University Project Competition"

Work Experience

Research Assistant, *(Academia Sinica)* **Taipei, Taiwan** *10/2024 - now*

- Research in Diffusion Model security and applications

Student Research Intern, *(Sony R&D)* **Tokyo, Japan** *02/2024 - 03/2024*

- Contributed to a commercial **image recognition** model by leveraging **synthetic data** generated through **pose, edge, and depth-controlled diffusion models**.
- Implemented unreleased Diffusion Models and trained them from scratch.
- Designed losses to optimize image quality and controllability of controllable diffusion model.

Research Assistant, *(LIS, Kyushu University)* **Fukuoka, Japan** *10/2022 - 03/2024*

- Built up an authentication and payment subscription system by integrating **Firebase** with **Strip**.
- Developed and deployed a comprehensive Python and deep learning instructional website.

Selected Publications

Published

- "MaXsive: High-Capacity and Robust Training-Free Generative Image Watermarking in Diffusion Models ". Published at **ACM MM** 2025.
  Mao Po-Yuan, Cheng-Chang Tsai and Chun-Shien Lu.
- "VSC: Visual Search Compositional Text-to-Image Diffusion Model ". Published at **ICCV** 2025 .
  Dat DoHuu, Nam Hyeonu, **Mao Po-Yuan** and Tae-Hyun Oh.
- "HOPE: A Memory-Based and Composition-Aware Framework for Zero-Shot Learning with Hopfield Network and Soft Mixture of Experts". Published at **WACV (Oral)** 2025 .
  Dat DoHuu*, **Mao Po-Yuan***, Nguyen TienHoang, Buntine Wray and Bennamoun Mohammed.
- "Magnum: Tackling high-dimensional structures with self-organization". Published in 2023 at **Neurocomputing**.
  Mao Po-Yuan, Tham Yikfoong, Zhang Heng and Danilo Vasconcellos Vargas.
- "Preliminary results on Chunking with Recurrent Neural Networks". Published in **SICE** 2021.
  Mao Po-Yuan and Danilo Vasconcellos Vargas.

In Submission/Revision

- "Breaking Free: How to Hack Safety Guardrails in Black-Box Diffusion Models!". In submission.
  Shashank Kotyan*, **Mao Po-Yuan***, Pin-Yu Chen and Danilo Vasconcellos Vargas.
- "Synthetic Shifts to Initial Seed Vector Exposes the Brittle Nature of Latent-Based Diffusion Models". In submission.
  Mao Po-Yuan*, Shashank Kotyan*, Tham YikFoong and Danilo Vasconcellos Vargas.
- "The Challenges of Image Generation Models in Generating Multi-Component Images". In submission.
  Tham YikFoong, Shashank Kotyan, **Mao Po-Yuan**, and Danilo Vasconcellos Vargas.

Full List at Google Scholar

* These authors contributed equally to the work

Skills

Research

- **Research Area:** Generative Model, Computer Vision, Deep Learning, Adversarial Machine Learning.
- **Programming Languages:** Python (Advanced).
- **Tools:** PyTorch, Distributed Computing, TensorFlow, Plotly Dashboard, Pandas, Sklearn

Software Engineering

- **Programming Languages:** Python (Advanced), Javascript (Intermediate).
- **Tools:** Linux, FireBase, Stripe, AWS, FastAPI library

Selected Research Projects

Improve the Adaptive Machine Learning Algorithm

- Proposed **Magnum**, enhancing the scalability of adaptive representation algorithms for **time series unsupervised** task.
- Proposed a physics-inspired machine learning algorithm, **Inertia-SyncMap**, to enhance learning stability.
- Migrated bio-inspired chunking algorithm into **Deep Recursive Neural Networks**.
- Assisted in the development of **Xenovert** to address **covariance shift** issues.
  Research Output : Four articles published/in submission.

Understanding Limitation of Generative Models

- Studied the **latent space** of state-of-the-art diffusion model and proposed simple **synthetic shifts** to break the image generation.
- Evaluated the robustness of **diffusion** models, highlighting their dependence on the **diffusion strategy**.
- Studied and evaluated the impact of **complex multi-component prompts** in various generative models.
- Shawn the risk that employing **NSFW detectors** to constrain diffusion models.
  Research Output : Two articles in submission.

Understanding Adversarial Attack and Neural Network Robustness

- Proposed **EvoSeed**, a framework integrated **CMA-ES** with Text-to-Image Diffusion Models, to produce **Natural Adversarial Samples**.
- Revealed the **transferability** of **Natural Adversarial Samples** across robust classifiers.
  Research Output : A article in submission.

Building Nano-Scale Stereolithography 3D Printing

- Developed a **second-order control system** to improve precision from the millimeter to the nanometer scale.
- Developed a single-chip control system using **Arduino** and **C**$^{++}$.
- Implement a user-machine interface by **C**$^{\#}$.
  Research Output : Two National Awards

Languages

- **Chinese** [Native]
- **Japanese** [N1]
- **English** [Proficient]