Bao Huynh Thai

Student https://github.com/tbaro19 *(July 2025)*

Education

University of Information Technology, Ho Chi Minh City

- *Bachelor of Science in Artificial Intelligence* *2023 – 2027*
  GPA: 3.06/4.00

Research Experience

- **Evolutionary Learning & Optimization** Oct 2024 - Present
  Research Student
  - **Adversarial Attack**: Conducted research on black-box and white-box adversarial attacks targeting OCR systems, vision-language models (VLMs), and similar AI models to evaluate and improve their robustness.
  - First author, Paper: Adversarial Robustness Evaluation of a Vietnamese Handwriting OCR System. PGD variants used to evaluate VietOCR robustness on handwriting data.
- **Multimedia Laboratory** Feb 2025 - Present
  Research Student
  - **Large Language Models**: Research and development of multimodal systems and pipelines for educational question answering tasks with explainability capabilities.
  - **3D Objects Retrieval**: Research on systems for 3D object retrieval and reconstruction from images and masked 2D inputs.
  - Co-author, Paper: Explainable Large Language Models for Educational Question-Answering: A Multi-Model Ensemble Approach with Structured Reasoning
  - Co-author, Paper: ROOMELSA: Retrieval of Optimal Objects for Multi-modal Enhanced Language and Spatial Assistance
- **Stubborn Strawberries team** Jan 2025 - Present
  Research Student
  - **Text to 3D models**: Research and improvement of text-to-3D models; developed pipelines integrating multiple models.
  - **ARM64 CPU Architecture**: Researched performance and addressed emerging issues in ARM64 CPU architecture.

Projects

- **AdvRE-ViHandOCR**: Evaluated the adversarial robustness of a Vietnamese handwriting OCR model against PGD white-box attacks. https://github.com/tbaro19/AdvRE-ViHandOCR
- **VNOID**: Scripts to benchmark the performance of large language models (LLMs) using vLLM. Help you measure throughput, latency, and the effect of CPU offloading on inference. https://github.com/tbaro19/VNOID

Skills / Experience

- **Languages**: Python (scikit-learn, NumPy, Pandas, PyTorch, ...), C++ (Arduino IDE).
- **Technical Skills**: Linux, Arduino/Raspberry Pi/Jetson Nano, ARM64 CPU Architecture, Adversarial Attack, Computer Vision, NLP, Genetic Algorithm, ...
- **Teaching Skills**: Lecture Designing, Presentation, Mentoring, Hosting & Reviewing.

Hobbies

- Research computer science & ARM64 CPU Architecture topics. Play football, table tennis

Social activities

- Mentor of Science Lab programs: ELECTRAHACK 2023, SIP 2024, ICOHACK 2024, SOFTHACK 2025
- Organizer/Volunteer of Arduino Day Vietnam 2023
- Speak about ARM64 CPU Architecture at Arduino Day Vietnam 2025, HCMC AI Meetup #1 - Menlo Research, OpenInfra & Cloud Native Day Vietnam 2025