# Sy-Tuyen Ho (Tuyen)

UMD PhD Student

**Research Interests.** Safety and Security AI, Multimodality Models, Agents.
**Contact:** stho@umd.edu, hosytuyen99@gmail.com

## Education

**University of Maryland, College Park (UMD)** United State
Doctor of Philosophy in Computer Science 2025–present
Supervisor: Prof. Furong Huang
Research Topics: Safety and Security AI, Multimodality Models, Agents

**Singapore University of Technology and Design (SUTD)** Singapore
Master of Engineering (Research) 2024–2025
Supervisor: Prof. Ngai Man Cheung
Research Topics: Safety and Security AI, Multimodality Models

**University of Information Technology** Vietnam
**Vietnam National University HCMC (VNU-HCM)** 2017–2021
Bachelor of Science in Computer Science, Honour program
*Salutatorian* of the intake 2017
Supervisor: Prof. Tam Nguyen

## Experience

**University of Maryland, College Park (UMD)** United State
Teaching Assistant 2025–present

**Temasek Lab @ SUTD** Singapore
Research Assistant & Senior Research Assistant 2022–2025
Worked on research projects funded by DSO National Laboratories
DSO Collaborator: Dr. Lionel Heng

**Viettel Group** Vietnam
Internship 2020–2021

## Selected Publications

1. **Sy-Tuyen Ho**, Yaseema Rusiru Ariyarathna Epa, Yasoda Lasiru Ariyarathna Epa, Andrew Mendez, Kecheng Liu, Xudong Jiang, Alex Kot, Furong Huang, Ngai-Man Cheung, "Don't Trust the Memory: Understanding and Mitigating Data Poisoning in LVLMs". Under Review at ICLR 2026

2. Khoa Duong, Tien-Phat Nguyen, Tri Cao, **Sy-Tuyen Ho**, Ngai-Man Cheung, "Don't Trust the Memory: Understanding and Mitigating Data Poisoning in LVLMs". Under Review at ICLR 2026

3. Ngoc-Bao Nguyen, **Sy-Tuyen Ho**, Jun Hao Koh, Ngai-man Cheung, "Model Inversion Attacks on Vision-Language Models: Do They Leak What They Learn?". Under Review at ICLR 2026

4. **Sy-Tuyen Ho**, Jun Hao Koh, Ngoc-Bao Nguyen, Alexander Binder, Ngai-man Cheung, "Revisiting Model Inversion Evaluation: From Misleading Standards to Reliable Privacy Assessment". Under Review at ICLR 2026

5. **Sy-Tuyen Ho***, Tuan Van Vo*, Somayeh Ebrahimkhani*, Ngai-man Cheung, "Vision Transformer Neural Architecture Search for Out-of-Distribution Generalization: Benchmark and Insights". **NeurIPS 2024**

6. Jun Hao Koh*, **Sy-Tuyen Ho***, Ngoc-Bao Nguyen, Ngai-man Cheung, "On the Vulnerability of Skip Connections to Model Inversion Attacks". **ECCV 2024** (* indicates equal contributions)

7. **Sy-Tuyen Ho**, Koh Jun Hao, Keshigeyan Chandrasegaran, Ngoc-Bao Nguyen, Ngai-man Cheung, "Model Inversion Robustness: Can Transfer Learning Help?". **CVPR 2024**

## Awards and Honors

- [2025] UMD Graduate School Dean's Fellowships
- [2025] UMD PhD Scholarship
- [2024] Temasek Lab Research Quality Award
- [2023] SUTD Master's Scholarship
- [2021] Salutatorian of the 2017 intake at UIT, VNU-HCM

## Skills

- **Pytorch/LLMs**
- **High-performance computing**
- **Python/C++**

## Services

- **Journal Reviewer:** TMM 2023-2025
- **Conference Reviewer** NeurIPS 2024/2025, ICLR 2025/2026, AISTATS 2025, ICML 2025, ACM MM 2025, AAAI 2026

## Referees

1. **Associate Professor Furong Huang - Department of Computer Science**
   Affiliation: University of Maryland College Park, The United State
   E-mail: furongh@cs.umd.edu

2. **Associate Professor Ngai-Man Cheung - Associate Head of Pillar**
   Affiliation: Singapore University of Technology and Design, Singapore
   E-mail: ngaiman_cheung@sutd.edu.sg

3. **Dr Lionel Heng - Principal Member of Technical Staff and Director of the Robotics Autonomy Lab**
   Affiliation: DSO National Laboratories, Singapore
   E-mail: lionel.heng@ieee.org

4. **Associate Professor Tam Nguyen - Head of Vision and Mixed Reality Lab**
   Affiliation: University of Dayton, The United State
   E-mail: tamnguyen@udayton.edu