

Buu Truong Phan

Website: truongbuu.github.io - Email: truongbuu94@gmail.com
[Google Scholar](#) - [LinkedIn](#)

RESEARCH INTERESTS

My research interest lies at the intersection of information theory and deep learning. Currently, deep models encounter various challenges, including adversarial attacks, privacy concerns, and issues of memorization. Interestingly, similar problems are also observed in large-scale communication systems, which can be analyzed using information-theoretic tools. By leveraging these tools, my goal is to explore the limitations of deep models and develop strategies for improvement.

Previously, I worked on projects focused on adversarial attacks, approximate inference, out-of-distribution detection and safety architecture for systems with neural networks.

ACADEMIC BACKGROUND

Ph.D. Electrical and Computer Engineering 2022 - Present
University of Toronto, Canada

- Research in information theory & machine learning with Prof. [Ashish Khisti](#). Currently focusing on fundamental limits in neural compression and reverse channel coding.

MASc. Electrical and Computer Engineering 2017-2019
University of Waterloo, Canada

- Research in deep learning, uncertainty alignment and out-of-distribution detection with Prof. [Krzysztof Czarnecki](#).

BEng. Electrical Engineering 2012-2016
Vietnam National University, Vietnam.

RESEARCH EXPERIENCE

Vector Institute for AI, Canada June 2023 - Present
Faculty Affiliate Researcher (Information Theory & Deep Learning).
Advisor: Prof. Ashish Khisti.

LG Electronics AI Lab, Canada 2021 - 2022
Research Engineer (Continual Learning & Computer Vision).

[Algolux](#) (acquired by Torc Robotics), Canada 2019 - 2021
Research Scientist (Adversarial Attack and Efficient Deep Learning)
Collaborators: Dr. Felix Heide and Dr. Fahim Mannan.

HIGHLIGHTED PAPERS

Salehkalaibar Sadaf*, **Buu Phan***, Jun Chen, Wei Yu, and Ashish Khisti: *On the Choice of Perception Loss Function for Learned Video Compression*. arXiv preprint arXiv:2305.19301 (2023). Accepted as spotlight paper in Neural Compression and Information Theory workshop in ICML 2023.

- *Contributions:* develop deep learning experiments and idea discussion.
- *Paper summary:* We show a counter-intuitive phenomenon in perceptual neural video compression.

Buu Phan*, Fahim Mannan, and Felix Heide: *Adversarial imaging pipelines*. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 16051-16061. 2021.

- *Contributions:* theoretical and experimental development, idea discussion.
- *Paper summary:* We develop a gradient based adversarial attack method on camera optics and ISPs.

Buu Phan*, Samin Khan, Rick Salay, and Krzysztof Czarnecki. "Bayesian uncertainty quantification with synthetic data." In Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops. Received a best paper award.

- *Contributions:* theoretical and experimental development, idea proposal.
- *Paper summary:* We show that uncertainty estimates from neural network are surprisingly aligned spatially with human perception.

Denouden, Taylor, Rick Salay, Krzysztof Czarnecki, Vahdat Abdelzad, **Buu Phan**, and Sachin Vernekar. *Improving reconstruction autoencoder out-of-distribution detection with Mahalanobis distance*. arXiv preprint arXiv:1812.02765 (2018).

- *Contributions:* idea proposal.
- *Paper summary:* We show why Mahalanobis distance is important for reconstruction-based OOD detection and vice versa.

OTHER PUBLICATIONS

Best viewed at my [Google Scholar](#).

AWARDS

Ontario Graduate Scholarship 2023
Award for top students in Ontario, Canada.

Best paper award 2019
Received at the Workshop on Artificial Intelligence Safety Engineering for the paper "Bayesian uncertainty quantification with synthetic data."

Toyota Canada Graduate Scholarship 2018
Scholarship for graduate students working in AI Safety.

Faculty of Engineering Awards, University of Waterloo 2018, 2019
Scholarship for top-performing graduate students.

International Master's Student Awards, University of Waterloo 2017-2019
Valedictorian, International University 2016

ACADEMIC SERVICES

- Reviewer - ICML 2023 Neural Compression Workshop 2023
- Reviewer- Conference on Computer Vision and Pattern Recognition (CVPR) 2022

SOFTWARE SKILLS

Programming: PyTorch, Tensorflow, Matlab, PyThon, C/C++.
System: Unix, Docker.