VIET QUOC VO

vietvo89@gmail.com **|** +61 474429320 **|** www.linkedin.com/in/viet-vo-75097835/
https://vietvo89.github.io/

EDUCATION

2019 - 2023 **Ph.D., Computer Science, The University of Adelaide, South Australia**

Topic: Trustworthy and Reliable Machine Learning (AI Safety & Ethics)

2012 - 2014 **Master of Engineering, Electronic and Computer Engineering, RMIT Vietnam University, Ho Chi Minh City**

Major: Computer Engineering

2007 - 2012 **Bachelor of Engineering, Electrical and Electronic Engineering, Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City**

Major: Electrical and Electronic Engineering

EXPERIENCE

2019 – Present **Researcher, The University of Adelaide**

Defense mechanism against Black-box Adversarial Attacks: Developed a diverse set of models which allows the response from models to be less informative to be exploited by black-box attacks and maintain high accuracy.

Sparse Black-box Adversarial Attack: Designed a query-based attack that perturbs a few pixels to fool Deep Learning models with only access to the model’s score output.

- Proposed a Bayesian-based attack that can obtain a 5% higher attack success rate.
- Published in *International Conference on Learning Representations (ICLR), 2024.*

Query Efficient Adversarial Attack: Developed a query-efficient attack that manipulates a few pixels to mislead Deep Learning models by exploiting solely predicted labels.

- Proposed SparseEvo attack, which is able to achieve 10x fewer queries than the current state-of-the-art method in a large-scale search space.
- Published in *International Conference on Learning Representations (ICLR), 2022.*

Deep Learning Robustness: Investigated the robustness of Deep Neural Networks against dense but imperceptible adversarial attacks with only access to the model’s output.

- Proposed RamBoAttack, which can achieve a 20% higher attack success rate.
- Employed an explainable AI technique (GradCAM) to demonstrate insights and understand the success of the proposed method.
- Published in *Network and Distributed System Security Symposium (NDSS), 2022.*

2014 - 2019 **Senior Process and Equipment Engineer, Intel Vietnam**

- Coffee Lake Transfer: Led the transfer of the first high-end desktop processor on a new chip assembly process in eight weeks (standards).
- Collaborate with counterparts and stakeholders in different Intel factories and leading module engineers to install and qualify a new assembly line.

2011 - 2012 **Undergraduate Student, IC Design Lab & Speech Recognition Research Group (HCMUT)**

- FPGA Architecture of HMM-based Decoder: Design an Architecture of HMM-based Decoder of Speech Recognizer on FPGA. The application of this design is the first design aimed at Vietnamese.
- Published in *International Conference on Control, Automation and Information Sciences (ICCAIS)*, 2012

PAPERS

2024

- Quoc Viet Vo, Ehsan Abbasnejad, and Damith Ranasinghe. “BruSLeAttack: Query-Efficient Score-Based Sparse Adversarial Attack”, International Conference on Learning Recognition(ICLR).

2022

- Quoc Viet Vo, Ehsan Abbasnejad, and Damith Ranasinghe. “Query efficient decision based sparse attacks against black-box deep learning models”, International Conference on Learning Recognition(ICLR).

2022

- Quoc Viet Vo, Ehsan Abbasnejad, and Damith Ranasinghe. “RamBoAttack: A Robust Query Efficient Deep Neural Network Decision Exploit”, Network and Distributed Systems Security (NDSS) Symposium.

AWARDS

2022 **NDSS Student travel Grant** is provided by Network and Distributed System Security Symposium for emerging security researchers who could contribute to the published content at future NDSS.

2019 **Postgraduate Research Scholarship** is provided by the Faculty of Engineering, Computer & Mathematical Sciences Divisional for talented students worldwide who want to carry out cutting-edge research and make a real impact on the world.

2012 **Intel Scholarship** is provided by Intel Vietnam for the brightest and best students and is preordained to be the core technical resource for Intel Vietnam in particular and of the high-tech industry of Vietnam in general.

SKILLS AND INTERESTS

· **Machine learning and Data**: PyTorch, Numpy, Pandas, Scikit-Learn, Python, Jupyter Lab, Hugging Face.

· **Others:** AWS Sagemaker.

· **Interests:** Trustworthy and Reliable Machine Learning, Bayesian Optimization, Evolution Algorithm, Generative AI, Large Language Model.