Dang Minh Nguyen

Contact Information
Email: dang.nguyen.bkit@gmail.com
Homepage: dangne.github.io

Research Interests
I am broadly interested in demystifying deep learning and developing reliable machine learning systems. Currently, I am focusing on explaining the adversarial examples phenomenon and improving adversarial robustness.

Education

Ho Chi Minh City University of Technology (HCMUT) Ho Chi Minh, Vietnam
B.Eng. in Computer Engineering Sep 2017 - Nov 2021

- **Advisor**: Prof. Tho Thanh Quan
- **Thesis**: Towards Adversarial Attack against Embedded Face Recognition Systems
- **CPA: 9.22/10.0; Rank: 5/382; Thesis: 9.9/10.0**

Research Experience

VinAI Research Ha Noi, Vietnam
AI Research Resident Aug 2020 - Present

- **Advisor**: Prof. Anh Tuan Luu, Research Scientist
- **Project**: "COMBAT: Alternated Training for Near-Perfect Clean-Label Backdoor Attacks"
  - Improve the effectiveness of clean-label backdoor attacks by developing a training scheme where a trigger generator is jointly trained with and poisons a surrogate model. The proposed attack achieves a near-perfect transferred attack success rate and is highly extendable to satisfy various constraints (e.g., imperceptibility, input awareness, and multi-target attack).
  - **Keywords**: Backdoor Attack, Clean-label Backdoor Attack, Computer Vision.
- **Project**: "Textual Manifold-based Defense Against Natural Language Adversarial Examples"
  - Validate an important conjecture that textual adversarial examples tend to have their contextualized embeddings diverge from the manifold of natural ones. Propose a state-of-the-art defense to project adversarial examples onto the manifold before classification and effectively defend against NLP attacks.
  - **Keywords**: Adversarial Defense, Manifold Approximation, Generative Modeling, Off-manifold Conjecture, Natural Language Processing.

AI Engineer (Applied Rotation Program) Feb 2021 - May 2021

- **Advisor**: Dr. Thien Hai Nguyen, Senior Research Engineer
- **Project**: "Vietnamese Grammatical Error Correction"
  - Develop a rule-based generative model to create synthetic grammatically-incorrect sentences and a Transformer-based sequence tagging model for correcting grammatical errors in Vietnamese documents.
  - **Keywords**: Grammatical Error Correction, Sequence Tagging, Synthetic Data Generation.

Publications

Conference papers:

COMBAT: Alternated Training for Near-Perfect Clean-Label Backdoor Attacks
Dang Minh Nguyen*, Tran Ngoc Huynh*, Tung Pham, Anh Tuan Tran
*Under review at International Conference on Learning Representations (**ICLR**), 2023*

Textual Manifold-based Defense Against Natural Language Adversarial Examples
Dang Minh Nguyen, Anh Tuan Luu
*Empirical Methods in Natural Language Processing (**EMNLP**), 2022*

Physical Transferable Attack against Black-box Face Recognition Systems
Dang Minh Nguyen, Anh Nguyen, Hieu Tran, Nhan Le, Tho Thanh Quan
*Multimedia Analysis and Pattern Recognition (**MAPR**), 2021*

Books:

Artificial Neural Networks: From Regression to Deep Learning
Tho Thanh Quan, Duy Cong Tran Nguyen, Dang Minh Nguyen, Duc Quang Nguyen, Khoi Minh Le, Long Hoang Ngo Bui, Mao Xuan Nguyen, Tam Bao Ngoc Bang, Thinh Gia Nguyen, Thong Thanh Nguyen, Trang Nguyen, Trung Duc Mai, Tuan Cong Bui
Vietnam National University Ho Chi Minh City Press, 2021

Awards

Vallet Fellowship - *Rencontres du Vietnam* 2021
Outstanding Academic Performance Scholarships - *HCMUT* 2017 - 2021
Gold Medal in Informatics - *Vietnam Southern Regional Olympiad* 2016

Talks

Textual Manifold-based Defense Nov 2022
VinAI Winter Workshop. Slides, Video

Improve Your Model Performance with Adversarial Training Mar 2022
VinAI Research. Slides

Services

Reviewer for: CVPR 2023

Technical Skills

Languages: Python, C/C++
ML Frameworks: PyTorch, TensorFlow
Libraries & Tools: NumPy, Pandas, Git, Docker
Operating Systems: Linux, Mac OS, Windows

References

Dr. Anh Tuan Luu
- Assistant Professor
- School of Computer Science and Engineering
- Nanyang Technological University
- Email: anhtuan.luu@ntu.edu.sg

Dr. Tho Thanh Quan
- Associate Professor
- Department of Computer Science and Engineering
- Ho Chi Minh City University of Technology
- Email: qttho@hcmut.edu.vn

Dr. Anh Tuan Tran
- Senior Research Scientist
- VinAI Research
- Email: v.anhtt152@vinai.io