Rey Reza Wiyatno

: rrwiyatn.github.io | : Google Scholar | : rrwiyatn | : reywiyatno@gmail.com | : (226) 989-8495

RESEARCH INTERESTS

- **Robotic Learning**: learning from physical interaction, meta-continual learning, learning-based control, and sim-to-real
- **Robotic Vision**: real world adversarial examples for robotics, object pose estimation, and object tracking

RESEARCH EXPERIENCE

Research Intern (supervised by Dr. Anqi Xu) — Jan 2018-Present

Element AI, Montréal QC

- Currently part of the **robotics team** within the Applied Research Lab (May 2019-Present)
- Conducted research on the applications of **adversarial examples in robotics** (fundamental research)
- Implemented deep learning based **autonomous drone tracking** software with **ROS**
- Investigated state of the art **adversarial attack and defense** methods in machine learning

Research Assistant — Sep 2017-Dec 2017

Neurocognitive Computing Lab at the University of Waterloo, Waterloo ON

- Researched various **biologically inspired learning algorithms** for neural networks with Professor Jeff Orchard

PUBLICATIONS

Refereed Conference Publications

- Maximal Jacobian-based Saliency Map Attack. Rey Wiyatno and Anqi Xu, in *Montréal Artificial Intelligence Symposium (MAIS'18)*, 5 pages, 2018, arXiv:1808.07945.
- Style Memory: Making a Classifier Network Generative. Rey Wiyatno and Jeff Orchard, in *IEEE International Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC'18)*, 6 pages, 2018, arXiv:1803.01900.

Manuscripts in Preparation

- Adversarial Examples in Modern Machine Learning: A Review. Rey Wiyatno, Anqi Xu, Ousmane Dia, and Archy de Berker, *work in progress*, 89 pages.
- CCATN: Class Conditional Adversarial Transformation Networks. Rey Wiyatno, *to be submitted to a relevant conference*, 11 pages.

Non-refereed Scientific Articles

- Securing Machine Learning Models Against Adversarial Attacks. Rey Wiyatno, in *Element AI Lab Blog*, 2019.
- Tricking a Machine into Thinking You're Milla Jovovich. Rey Wiyatno, in *Element AI Lab Blog*, 2018.

PRESENTATIONS

- **Guest Lecture (CS489/698 - Neural Networks): Adversarial Examples for Neural Networks** — Mar 2019
  David R. Cheriton School of Computer Science at the University of Waterloo, Waterloo ON
- **Science Talk: Adversarial Examples in Machine Learning** — Dec 2018
  Neurocognitive Computing Lab at the University of Waterloo, Waterloo ON
- **Science Talk: Physical Adversarial Examples for Drone Tracking** — Aug 2018
  Mobile Robotics Lab at McGill University, Montréal QC
- **Conference Talk: Style Memory - Making a Classifier Network Generative** — Jul 2018
  IEEE International Conference on Cognitive Informatics and Cognitive Computing 2018, Berkeley CA
- **Guest Lecture (CS489/698 - Neural Networks): Long Short-Term Memory** — Mar 2018
  David R. Cheriton School of Computer Science at the University of Waterloo, Waterloo ON

ROBOTICS AND MACHINE LEARNING KNOWLEDGE

- **Machine Learning**: CNN, RNN, LSTM, autoencoders, GAN, adversarial domain adaptation, adversarial attacks, adversarial defenses, explainability, meta learning, reinforcement learning (basics)
- **Robotic Vision**: object detection, object tracking, image segmentation, object pose estimation, human pose estimation, camera relocalization, classical vision algorithms (e.g., edge detectors, Hough transform, optical flow, etc.), stereo geometry
- **Control Theory**: proportional-integral-derivative (PID) controller, controller/plant discretization, controller emulation, pole placement designs, state-space models, direct design of digital controller, system identification

EDUCATION

BASc., Honours, Mechatronics Engineering, Co-operative Program — University of Waterloo
Graduation Awards: Dean's Honours List, With Distinction — Class of 2019

SELECTED PROJECTS PLEASE VISIT REYREZAWIYATNO.COM FOR MORE DETAILS

Physical Adversarial Examples for Drone Tracking — Aug 2018-Mar 2019

- Developed and implemented the algorithm to generate physical adversarial examples for drone tracking
- Implemented and evaluated the effectiveness of **Expectation over Transformation** (Athalye et al., 2018) in generating physically realizable adversarial examples

Intelligent Manufacturing Visual Inspection Tool — Oct 2018-Feb 2019

- Designed and built a **low-cost solution for high quality visual inspection tool** that incorporates an enclosure, a four degrees-of-freedom robot arm, and a camera attached at the end effector of the arm, with Mask R-CNN (He et al., 2017) as the defect detector
- Winner of Autodesk Canada Capstone Design Award

Autonomous Drone Tracking — Jul 2018

- Implemented object detection and tracking models which include **Single Shot Multibox Detector** (Liu et al., 2015), **GOTURN** (Held et al., 2016), and **SiamFC** (Bertinetto et al., 2016)
- Developed autonomous drone tracker software with **exponential filter** and **PID controller** using **ROS**

Deep Learning Papers Reproducibility — Jun 2017-Sep 2017

- Implemented and evaluated **Adversarial Transformation Networks** (Baluja et al., 2017), **Photo Image Synthesis with Cascaded Refinement Networks** (Chen et al., 2017), **The One Hundred Layers Tiramisu** (Jégou et al., 2016), **Generative Adversarial Nets (GAN)** (Goodfellow et al., 2014), **DCGAN** (Radford et al., 2015), **WGAN** (Arjovsky et al., 2017), **Super Resolution with Perceptual Losses** (Johnson et al., 2016), **Neural Style Transfer** (Gatys et al., 2015), **Fast Gradient Sign Method** (Goodfellow et al., 2014), and **DenseNet** (Huang et al., 2016)

Auto Photo Enhancing and Dehazing — Jul 2017

- Experimented and trained neural networks for **image enhancing and dehazing using L_2 loss in feature space as perceptual similarity objective** on MIT-Adobe FiveK and NYU Dehazing datasets

Suitcase Robot — Aug 2015

- Designed and built a RaspberryPi-powered **person-following suitcase using color-based tracking**

SKILLS

- **Software Tools**: Python, C++, Lua, Keras, TensorFlow, ROS, Gazebo, NumPy, SciPy, OpenCV, Scikit-Learn, Arduino, Processing, Docker, Flask, MATLAB, Linux, LabVIEW, LaTeX
- **Hardware Tools**: Autodesk Inventor, OpenSCAD, SolidWorks, ANSYS AIM, Eagle, Altium Designer, LTSpice
- **Firmware/Electrical**: Microcontrollers & SoC (e.g., Arduino, RaspberryPi, NVIDIA Jetson, etc.), Wi-Fi microcontrollers, circuits design, PCB layout, electronics troubleshooting, SMD soldering, rework
- **Mechanical**: CAD, product design, design for manufacturing, design for assembly, finite element analysis, injection molding, rapid prototyping, additive manufacturing, laser cutting

INDUSTRIAL EXPERIENCE

Backend and Deep Learning Engineer — May 2017-Aug 2017
Canon Innovation Lab, Waterloo ON

- Designed and implemented backend and algorithms using **Docker, Flask, OpenCV, Keras, and TensorFlow** for various photography and printing services prototypes

Mechatronics Engineer — May 2016-Dec 2016
OpenROV, Berkeley CA

- Designed the mechanical, electrical, and software of an **underwater drone external payload**
- Conducted rapid prototype and tested various parts of Trident ROV for production purpose

Computer Vision, Human Machine Interface, and Test Engineer — May 2015-Aug 2015 & Jan 2016-Apr 2016
Flex (formerly Flextronics) - Automotive Division, Toronto ON

- Designed and evaluated various **computer vision vision algorithms for advanced driving assistance systems**
- Characterized and tested various cameras and other optical sensors