Siyuan "Cyan" Huang

shuan124@jhu.edu, siyuanhuang@gwu.edu, (571) 507-4326

3978 Edgehill Ave E7, Baltimore, MD, US, 21211

Profile

Programming Languages, Tools & Skills: Python, PyTorch, Linux, LaTeX, Mathematica.

Current Research Area: Person Re-identification / Body Recognition, Computer Vision, Deep Learning, Cognitive Machine Learning.

Past Research Area: Efficient Neural Network, Physical Adversarial Attack, Trajectory, Data Mining.

Educational Background

- Johns Hopkins University (JHU), Baltimore, MD, USA   Predicted May 2026

   PhD in Electronical & Computer Engineering.

   Master of Science in Engineering. GPA: 3.7 / 4.0

   Relevant Coursework: Deep Learning, Machine Perception, Machine Learning.

- The George Washington University (GWU), Washington, DC, USA   May 2020

   Thesis Master of Science in Computer Science. GPA: 3.8 / 4.0

   Relevant Coursework: Machine Learning, Design & Analysis of Algorithms, Artificial Intelligence, Intro. To Statistical NLP.

   Thesis: Low Rank Approximations for Efficient DNN Training

- Wuhan University of Technology (WUT), Wuhan., Hubei, China   June 2018

   Bachelor of Engineering in Software Engineering. GPA: 3.6 / 4.0

   Relevant Coursework: Introduction to Artificial Intelligence, Technology & Application of Big Data, Algorithm Design & Analysis, Data Structure.

Selected Projects

Artificial Intelligence for Engineering and Medicine Lab, Johns Hopkins University, *Graduate Research Assistant*.

Supervisor: Prof. Rama Chellappa.   09/2022-Present

- **Biometric Recognition and Identification at Altitude and Range (BRIAR).** This project aims to recognize identity in very challenging scenarios, e.g., 1,000m and UAV. So far, I designed two models.
   - BRIARNet is an end-to-end detection-to-recognition model, that can detect identities from raw videos and then recognize them. BRIARNet leverages 3D bottleneck (inflated ResNet) and clothes-adversarial loss to handle both cropped images and frames. BRIARNet achieves a rank-20 recognition accuracy of 75.13% and a TAR@1%FAR of 54.09% on a protocol of 100 subjects with 444 distractors, both are SOTA results.
   - SemReID is a self-supervised ReID pre-training model that leverages Segment Anything Model for adaptive part-based semantic extraction. SemReID can automatically generate local semantics for a raw image, e.g, face, upper body, lower body. SemReID demonstrates SOTA performance on 10+ metrics, 13 protocols, 4 datasets, in various fields, including standard ReID, clothes-change ReID, and BRIAR.
   - Both BRIARNet and SemReID are successfully delivered to IARPA (Manager: Dr. Lars Ericson).

Alternative Computing Group, National Institute of Standards and Technology, *Associate Researcher*.

Adaptive Devices and Microsystems Lab, The George Washington University, *Graduate Research Assistant*.

Supervisor: Dr. Jabez J. McClelland, Dr. Mark D. Stiles, Prof. Gina C. Adam, Dr. Brian D. Hoskins.   18/2018-11/2022

- **Efficient Deep Neural Network (DNN) Training.** This project aims to minimize DNN accelerator overhead, especially on the calculation of gradient that cannot be efficiently contained in accelerators. I designed three algorithms.
   - SBE combined low-rank approximations and streaming methods to compute the contribution of each input and error vector pair to the update as they arrive requires no further information about them for subsequent processing. This approach minimizes storage and computational requirements while preserving the advantages of batch updates.

- Rank-sum and Rank-seq are SGD-based gradient descent methods used to reconstruct the memristor array. They use stochastic rounding to avoid vanishing weight updates, and decomposition methods to keep the memory overhead low. Rank-sum/-seq + NMF can achieve near SGD accuracy in memristor-based DNN at significant memory savings.
- SBPCA uses stochastic power iterations to generate a stochastic rank-k approximation of the gradient. The approximation is made in an expanded vector form that can efficiently be applied to the rows and columns of crossbars for array-level updates. SBPCA can effectively train DNN with performance comparable to standard SGD.
- Published five papers in top conferences and journals, including Frontiers in Neuroscience, AAAI, and JETCS.

Tsinghua Laboratory of Brain and Intelligence, Tsinghua University, *Graduate Research Assistant*.
Supervisor: Prof. Bo Zhang, Prof. Jun Zhu, Prof. Xiaolin Hu.   08/2020-08/2021

- **Symmetry in Music** (in progress). This project aims to discover whether humans perceive mathematical symmetry in music, e.g., Translation (Repetition), Step (Sequence), Reflection (Retrograde), etc.
  - A behavioral test is designed to let volunteers discern symmetry types while listening to the extracted pieces.
  - Machine learning models are used to automatically analyze music of famous composers and historical eras.
  - Experiments revealed that both nowadays people and historical composers have preference in reacting/composing symmetry in music. Repetition and Sequence are two compositions that people react to most, usually are the reasons that they feel melodious of a music.
- **Physical Adversarial Attack**. This project aims to reveal the vulnerability of AI systems. Deliberately designed patterns can deceive AI in the real world. I designed three methods.
  - TC-EGA is a generative Toroidal-Cropping-based model to craft AdvTexture with repetitive structures. AdvTexture can cover clothes with arbitrary shapes so that people wearing them can hide from detectors from different viewing angles. We also made several true T-shirts, skirts, and dresses with AdvTexture in the physical world.
  - Adversarial QR code is a pattern that can be expanded periodically, and make the clothes based on it have infrared adversarial effectiveness. We then made the infrared adversarial shirt with aerogel. It lowered the AP of YOLOv3 by 64.6%, which is SOTA.
  - Carbon fiber heaters can be optimized more flexible and is lighter compared to aerogel. We improved the infrared adversarial shirt with heaters. With ensemble attack techniques, our shirt has good attack transferability to unseen CNN models and successfully attacked five typical defense methods.
  - Published three papers in top conferences and journals. Two CVPR papers are orals.

Selected Publications (Google Scholar)

[1] (in review) **Huang, Siyuan**, Yifan Zhou, Ram Prabhakar Kathirvel, Rama Chellappa, and Chun Pong Lau. "SAM-PASS: Prompt-based Self-Supervised Learning for General Person Re-Identification." *CVPR 2024*. (paper)

[2] (in review) **Huang, Siyuan**, Ram Prabhakar Kathirvel, Chun Pong Lau, and Rama Chellappa. " Whole-body Detection, Recognition and Identification at Altitude and Range." *Journal of T-BIOM 2024*. (paper)

[3] **Huang, Siyuan**, Brian D. Hoskins, Matthew W. Daniels, Mark D. Stiles, and Gina C. Adam. "Low-Rank Gradient Descent for Memory-Efficient Training of Deep In-Memory Arrays." *ACM Journal on Emerging Technologies in Computing Systems* 19, no. 2 (2023): 1-24. (paper)

[4] Hu, Zhanhao, **Siyuan Huang**, Xiaopei Zhu, Fuchun Sun, Bo Zhang, and Xiaolin Hu. "Adversarial Texture for Fooling Person Detectors in the Physical World." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 13307-13316. 2022. (paper)

[5] **Huang, Siyuan**, Junyun Zhao, Yousuf Osama, Yutong Gao, Brian Hoskins, and Gina Adam. "Gradient Decomposition Methods for Training Neural Networks with Non-Ideal Synaptic Devices." *Frontiers in neuroscience 2021*. (paper)

[6] **Huang, Siyuan**, Brian D. Hoskins, Matthew W. Daniels, Mark D. Stiles, and Gina C. Adam. "Streaming Batch Gradient Tracking for Neural Network Training." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 10, pp. 13813-13814. 2020. (paper)

Activities & Honors

- Reviewer, CVPR 2024   02/2024

- Presenter, IARPA BRIAR Program 2nd Annual PI Review Meeting   12/2023
- Presenter, JHU WSE Research Poster Showcase   11/2022
- Reviewer, ECCV 2022   05/2022
- Reviewer, CVPR 2022   02/2022
- Conference Manager Assistant, AAAI 2020   02/2020
- Presenter, GWU ECE Research Blitz   11/2019
- Presenter, GWU SEAS R&D Showcase   11/2019
- Nominee, Graduate Award for Excellence   04/2019
- Nominee, Excellence in Student Life   04/2019
- Graduate Student Professional Development Fund   02/2019
- Merit Student, Wuhan University of Technology   09/2017
- Scholarship, Wuhan University of Technology   09/2017