







ShengYun (Anthony) Peng

My research strengthens the generalization and safety of the generative AI, spanning vision models, LLMs, and VLMs. As steps towards this goal, I work on generalizable multimodal representation learning and safe and robust machine learning models.

 shengyun-peng.github.io
 speng65@gatech.edu
 CV PDF

 @RealAnthonyPeng
 @ShengYun-Peng
 Google Scholar

Education

- Jan. 2022 — present **Ph.D. in Computer Science**
Georgia Institute of Technology, Atlanta, GA
Advisor: Duen Horng Chau
- Jan. 2021 — Dec. 2022 **M.S. in Computer Science**
Georgia Institute of Technology, Atlanta, GA
GPA: 4.00/4.00
- Sept. 2015 — June 2020 **B.Eng. in Civil Engineering**
Tongji University, Shanghai, China
GPA: 92.37/100, Outstanding Graduates Award of Shanghai, 2020
- July 2019 — Sept. 2019 **Cross-disciplinary Scholars in Science and Technology (CSST) Program**
University of California, Los Angeles, Los Angeles, CA
GPA: 4.00/4.00

Industry Research Experience

- May 2022 — Aug. 2022 **Intel Corporation**, Hillsboro, OR
Graduate ML Security Intern, Security Solution Lab
Mentor: Weilin Xu, Jason Martin
Worked on DARPA Guaranteeing AI Robustness Against Deception (GARD) project; Investigated four key architectural components underpinning SOTA CNNs and Transformers that boost adversarial robustness.

Academic Research Experience

- May 2021 — present **Georgia Institute of Technology**, Atlanta, GA
Graduate Research Assistant, School of Computer Science
Mentor: Duen Horng Chau
Member of Polo Club of Data Science where we bridge and innovate at the intersection of data mining and human-computer interaction to synthesize scalable, interactive, and interpretable tools that amplify human's ability to understand and interact with big data.
- Sept. 2020 — Dec. 2020 **Fudan University**, Shanghai, China
Undergraduate Research Assistant, Shanghai Key Laboratory of Data Science
Mentor: Weidong Yang
Built a cockpit monitoring software that can locate the dashboard, extract the plane's status parameters, and interactively verify the correctness based on human guidance.
- Oct. 2017 — Aug. 2020 **Tongji University**, Shanghai, China
Undergraduate Research Assistant, State Key Laboratory of Disaster Reduction in Civil Engineering
Mentor: Ying Zhou
Developed a framework from the ground-up which identified structural system through a non-contact measurement method, which was widely used by multiple cities for structural health monitoring in China.
- July 2018 — Jan. 2020 **Shanghai Jiao Tong University**, Shanghai, China

Undergraduate Research Assistant, Advanced Avionics and Intelligent Information Lab

Mentor: Xingcheng Zhang, Gang Xiao

Developed visible and infrared fusion methods on both pixel and feature levels, which solved tracking challenges including partial occlusion and low illumination. The tracker ranked first on large-scale RGBT234 tracking benchmark.

July 2019 — Dec. 2019

University of California, Los Angeles, Los Angeles, CA

Undergraduate Research Assistant, Design Automation Lab

Mentor: Yunxuan Yu, Lei He

Proposed a novel anchor-free tracker that achieved SOTA performances on widely-used tracking benchmarks, e.g., OTB2015, VOT2015, VOT2016, and TrackingNet.

Apr. 2017 — Apr. 2018

Tongji University, Shanghai, China

Undergraduate Research Assistant, School of Materials Science and Engineering

Mentor: Qianrong Yang

Mechanical design and manufacture of a 3D concrete printer with automatic pulp feeding systems.

June 2017 — Aug. 2017

Chinese Academy of Sciences, Beijing, China

Undergraduate Research Assistant, Institute of Computing Technology

Mentor: Chao Liu

PID control in Matlab Simulink for cruise missile and Cessna-172 aircraft flight.

Honors and Awards

2023 BMVC 2023 Best Poster Award

Only five of the accepted papers are selected for the award

2020 Outstanding Graduates in Shanghai

For top 5% undergraduates graduating in 2020.

2017 — 2018 National Scholarship

Stipend awarded to top 2% undergraduates in all China's universities.

2017 — 2018 Tongji University Excellent Student

For top 5% undergraduates in Tongji University.

2016 — 2017 First Prize of Tongji University Scholarship of Excellence

For outstanding undergraduates in Tongji University.

2016 — 2017 Excellent Worker in the ASCE-Tongji-ISG of the Instructional Innovation

For my work at ASCE-Tongji-ISG club.

2017 National Undergraduate Innovative Programs Certificate

For our research in "3D Printing of Concrete Structures and Sample Strength Tests".

2017 3rd Prize in Contemporary Undergraduate Mathematical Contest in Modeling

We worked on the second problem, which was creating a price model for a specific photo service.

2016 1st Prize in Mathematics Competition of Chinese College Students

The competition examines advanced calculus and linear algebra knowledge.

Publications

UniTable: Towards a Unified Framework for Table Structure Recognition via Self-Supervised Pretraining

ShengYun Peng, Seongmin Lee, Xiaojing Wang, Raji Balasubramaniyan, Duen Horng Chau
preprint. 2024.

[Project](#) [BibTeX](#)

Self-supervised Pre-training for Table Structure Recognition Transformer

ShengYun Peng, Seongmin Lee, Xiaojing Wang, Raji Balasubramaniyan, Duen Horng Chau
Association for the Advancement of Artificial Intelligence (AAAI) SDU Workshop. 2024.

[Project](#) [BibTeX](#)

High-Performance Transformers for Table Structure Recognition Need Early Convolutions

ShengYun Peng, Seongmin Lee, Xiaojing Wang, Raji Balasubramaniyan, Duen Horng Chau
Neural Information Processing Systems (NeurIPS) TRL Workshop. 2023.

[Project](#) [PDF](#) [Code](#) [BibTeX](#) [Oral](#)

Robust Principles: Architectural Design Principles for Adversarially Robust CNNs

ShengYun Peng, Weilin Xu, Cory Cornelius, Matthew Hull, Kevin Li, Rahul Duggal, Mansi Phute, Duen Horng Chau, Jason Martin

British Machine Vision Conference (BMVC). 2023.

[Project](#) [PDF](#) [Video](#) [Poster](#) [Code](#) [BibTeX](#) [🏆 Best Poster Award](#)

Diffusion Explainer: Visual Explanation for Text-to-image Stable Diffusion

Seongmin Lee, Benjamin Hoover, Hendrik Strobelt, Zijie J. Wang, ShengYun Peng, Austin Wright, Kevin Li, Haekyu Park, Haoyang Yang, Duen Horng Chau

IEEE Visualization Conference (VIS). 2023.

[Project](#) [Demo](#) [PDF](#) [Recording](#) [Code](#) [BibTeX](#)

SkeleVision: Towards Adversarial Resiliency of Person Tracking with Multi-Task Learning

Nilaksh Das, ShengYun Peng, Duen Horng Chau

European Conference on Computer Vision (ECCV) AROW Workshop. 2022.

[Project](#) [PDF](#) [Code](#) [BibTeX](#)

DetectorDetective: Investigating the Effects of Adversarial Examples on Object Detectors

Sivapriya Vellaichamy, Matthew Hull, Zijie J. Wang, Nilaksh Das, ShengYun Peng, Haekyu Park, Duen Horng Chau

CVPR Demo. 2022.

[Project](#) [PDF](#) [BibTeX](#)

A novel DNN tracking algorithm for structural system identification

ShengYun Peng, LingFeng Yan, Bin He, Ying Zhou

Smart Structures and Systems. 2021.

[Project](#) [PDF](#) [Video](#) [BibTeX](#) [DOI](#)

DSiamMFT: An RGB-T fusion tracking method via dynamic Siamese networks using multi-layer feature fusion

Xingchen Zhang, Ping Ye, ShengYun Peng, Jun Liu, Gang Xiao

Signal Processing, Image Communication. 2020.

[Project](#) [PDF](#) [BibTeX](#) [DOI](#)

Anti-occlusion object tracking based on correlation filter

Jun Liu, Gang Xiao, Xingchen Zhang, Ping Ye, Xingzhong Xiong, ShengYun Peng

Signal, Image and Video Processing. 2019.

[Project](#) [PDF](#) [BibTeX](#) [DOI](#)

SiamFT: An RGB-Infrared Fusion Tracking Method via Fully Convolutional Siamese Networks

Xingchen Zhang, Ping Ye, ShengYun Peng, Jun Liu, Ke Gong, Gang Xiao

IEEE Access. 2019.

[Project](#) [PDF](#) [BibTeX](#) [DOI](#)

Object Fusion Tracking Based on Visible and Infrared Images Using Fully Convolutional Siamese Networks

Xingchen Zhang, Ping Ye, Dan Qiao, Junhao Zhao, ShengYun Peng, Gang Xiao

22th International Conference on Information Fusion (FUSION). 2019.

[Project](#) [PDF](#) [BibTeX](#) [DOI](#)

Preprint

LLM Self Defense: By Self Examination, LLMs Know They Are Being Tricked

Mansi Phute, Alec Helbling, Matthew Hull, ShengYun Peng, Sebastian Szyller, Cory Cornelius, Duen Horng Chau

arXiv. 2023.

[Project](#) [PDF](#) [BibTeX](#)

RobArch: Designing Robust Architectures against Adversarial Attacks

ShengYun Peng, Weilin Xu, Cory Cornelius, Kevin Li, Rahul Duggal, Duen Horng Chau, Jason Martin

arXiv. 2023.

[Project](#) [PDF](#) [BibTeX](#)

IMB-NAS: Neural Architecture Search for Imbalanced Datasets

Rahul Duggal, ShengYun Peng, Hao Zhou, Duen Horng Chau

arXiv. 2022.

Accurate Anchor Free Tracking

ShengYun Peng, Yunxuan Yu, Kun Wang, Lei He
arXiv. 2020.

Invited Talks and Presentations

UniTable: Towards a Unified Table Foundation Model

Mar. 2024 ADP AI Community of Practice Meetup

Self-supervised Pre-training for Table Structure Recognition Transformer

Feb. 2024 AAI 2024 Scientific Document Understanding Workshop

High-Performance Transformers for Table Structure Recognition Need Early Convolutions

Dec. 2023 NeurIPS 2023 2nd Table Representation Workshop

Robust Principles

Oct. 2023 DARPA GARD PI Meeting (Evaluation 7)

Exploration of Robust Model Architectures

May 2023 DARPA GARD PI Meeting (Evaluation 6)

In Search of Robust Architectures against Adversarial Attacks

Aug. 2022 Intel Labs (Internship Report)

A New Siamese-based Tracking for Structural Health Monitoring

June 2019 International Workshop on Data Science in Civil Engineering

Grants and Funding

2024 — 2026 **Physical Adversarial Attack and Defense for Aerial Imagery**

Co-authored \$1.1M awarded research proposal from Technology Innovation Institute (TII)
PIs: Duen Horng Chau, Wenke Lee

2022 — 2023 **Document Understanding**

Co-authored \$250k awarded research proposal from Automatic Data Processing (ADP), Inc.
PIs: Duen Horng Chau, Chao Zhang, Srijan Kumar

Service

Program Committee

SIAM International Conference on Data Mining (**SDM**) 2024

Reviewer

Scientific Reports 2023
ICCV Workshop on Adversarial Robustness In the Real World 2023
IEEE Transactions on Cybernetics 2023
ICML Workshop on AdvML-Frontiers 2023
Signal Processing: Image Communication 2022
SN Applied Sciences 2022
Pattern Recognition 2020
IEEE Access 2020

Member

2016 — 2017 American Society of Civil Engineers - Tongji (**ASCE**)

Mentoring

Apr. 2023 — present

Mansi Phute

M.S. in Computer Science, Georgia Institute of Technology

Aug. 2022 — May 2023

Kevin Li

B.S. in Computer Science, Georgia Institute of Technology

Now: ML Ph.D. at Carnegie Mellon University

May 2022 — May 2023

Chakravarthy RVK

M.S. in Analytics - Data Science, Georgia Institute of Technology

Oct. 2021 — May 2022

Sivapriya Vellaichamy

M.S. in Computational Data Analytics, Georgia Institute of Technology

Now: AI Research Tech - Senior Associate at JPMorgan Chase

References

Dr. Polo Chau, Associate Professor

School of Computational Science and Engineering

Georgia Institute of Technology

faculty.cc.gatech.edu/~dchau

Dr. Lei He, Professor

School of Electrical and Computer Engineering

University of California, Los Angeles

eda.ee.ucla.edu/people/faculty.html

Dr. Ying Zhou, Professor

College of Civil Engineering

Tongji University

<https://www.journals.elsevier.com/resilient-cities-and-structures/editorial-board/ying-zhou>