Haekyu Park

haekyu@gatech.edu · haekyu.com · Curriculum Vitae · Google Scholar

My research goal is to enhance **machine learning interpretability**, to enable:

- **Confident use of machine learning**, by helping people interpret and trust the models
- **Effective model debugging and improvement**, by promoting practitioners' understanding of why a model would not work well and providing insights into how to fix it
- **Broadening access to machine learning**, by encouraging people of diverse backgrounds to easily learn and leverage the technologies.

Specifically, I design and develop interactive visualization systems to interpret machine learning models. I am a member of the Polo Club of Data Science at Georgia Tech. I have been fortunate to work with amazing researchers, engineers, and scientists at NVIDIA and Intel.

Education

Georgia Institute of Technology
Ph.D., Computer Science
Advisor: Dr. Polo Chau
Aug 2018 - Present

Seoul National University
B.S., Computer Science and Engineering
Graduated with honors (Cum Laude)
Mar 2012 - Aug 2017

Research Experience

AI Infrastructure Software Intern May 2020 - Jul 2020
NVIDIA, Santa Clara, CA
Mentor: Joe Eaton, Brad Rees, Bartley Richardson
Developed a visual graph analytics, allowing for interactively running multiple graph algorithms in real-time on large graphs. Leveraged GPU acceleration for both data analysis and rendering side.

Data Science Intern May 2019 - Aug 2019
NVIDIA, Austin, TX
Mentor: Bartley Richardson, Brad Rees, Joe Eaton
Internship results are integrated into NVIDIA RAPIDS team's cybersecurity usecase notebook, presented at KDD 2019 NVIDIA RAPIDS tutorial.

Graduate Research Assistant Aug 2018 - Present
Georgia Institute of Technology, Atlanta, GA

Undergraduate Research Assistant June 2016 - Aug 2017
Seoul National University, Seoul, Republic of Korea

Awards & Honors

"Thank a Teacher" Award 2019
Center of Teaching & Learning (CTL), Georgia Institute of Technology

Moon-Jung Chung Scholarship 2019
KOCSEA (The Korean Computer Scientists and Engineers Association in America)

National Scholarship for Science and Engineering 2015
National Scholarship for Science and Engineering

Grants & Funding

WiML Travel Funding 2019
$550 Travel Funding
Women in Machine Learning Workshop, co-located with NeurIPS

Amazon AWS Research Grant 2018
Funded $5,000 in AWS cloud credits
Co-PIs: Nilaksh Das, Scott Freitas, Duen Horng Chau

Publication

SkeletonVis: Interactive Visualization for Understanding Adversarial Attacks on Human Action Recognition Models

Haekyu Park, Zijie J. Wang, Nilaksh Das, Anindya S. Paul, Pruthvi Perumalla, Zhiyan Zhou, and Duen Horng Chau
AAAI, Demo, Virtual, 2021.

Bluff: Interactively Deciphering Adversarial Attacks on Deep Neural Networks

Nilaksh Das*, Haekyu Park*, Zijie J. Wang, Fred Hohman, Robert Firstman, Emily Rogers, and Duen Horng Chau
IEEE Visualization Conference, (VIS), Salt Lake City, UT, USA, 2020.
* Authors contributed equally.
▶ Demo PDF arXiv

CNN Explainer: Learning Convolutional Neural Networks with Interactive Visualization

Zijie J. Wang, Robert Turko, Omar Shaikh, Haekyu Park, Nilaksh Das, Fred Hohman, Minsuk Kahng, Duen Horng Chau
IEEE Conference on Visual Analytics Science and Technology, (VAST), Salt Lake City, UT, USA, 2020.
▶ Demo PDF

A Comparative Analysis of Industry Human-AI Interaction Guidelines

Austin P. Wright, Zijie J. Wang, Haekyu Park, Grace Guo, Fabian Sperrle, Mennatallah El-Assady, Alex Endert Daniel Keim Duen Horng Chau
IEEE Visualization Conference, Workshop on Trust and Expertise in Visual Analytics (TREX), Salt Lake City, UT, USA, 2020.
PDF

Argo Lite: Open-Source Interactive Graph Exploration and Visualization in Browsers

Siwei Li, Zhiyan Zhou, Anish Upadhayay, Omar Shaikh, Scott Freitas, Haekyu Park, Zijie J. Wang, Susanta Routray, Matthew Hull, and Duen Horng Chau
ACM International Conference on Information and Knowledge Management, (CIKM), Resource Track, Online, 2020.
Demo

Massif: Interactive Interpretation of Adversarial Attacks on Deep Learning

Nilaksh Das*, Haekyu Park*, Zijie J. Wang, Fred Hohman, Robert Firstman, Emily Rogers, and Duen Horng Chau
ACM CHI Conference on Human Factors in Computing Systems (CHI), Late-Breaking Works, Honolulu, Hawaii, USA, 2020.
* Authors contributed equally.
PDF arXiv

CNN 101: Interactive Visual Learning for Convolutional Neural Networks

Zijie J. Wang, Robert Turko, Omar Shaikh, Haekyu Park, Nilaksh Das, Fred Hohman, Minsuk Kahng, and Duen Horng Chau
ACM CHI Conference on Human Factors in Computing Systems (CHI), Late-Breaking Works, Honolulu, Hawaii, USA, 2020.
PDF arXiv

Summit: Scaling Deep Learning Interpretability by Visualizing Activation and Attribution Summarizations

Fred Hohman, Haekyu Park, Caleb Robinson, and Duen Horng Chau
IEEE Transactions on Visualization and Computer Graphics (TVCG), Vancouver, BC, Canada, 2020.
Demo PDF arXiv

Visual Analytics for Interpretability on Deep Neural Networks

Haekyu Park, Fred Hohman, Nilaksh Das, Caleb Robinson, and Duen Horng Chau
Women in Machine Learning Workshop (WiML), co-located with NeurIPS 2019, Vancouver, BC, Canada, 2019.

MLsploit: A Framework for Interactive Experimentation with Adversarial Machine Learning Research

Nilaksh Das, Siwei Li, Chanil Jeon, Jinho Jung, Shang-Tse Chen, Carter Yagemann, Evan Downing, Haekyu Park, Evan Yang, Li Chen, Michael Kounavis, Ravi Sahita, David Durham, Scott Buck, Duen Horng Chau, Taesoo Kim, and Wenke Lee
ACM SIGKDD Conference on Konwledge Discovery and Data Mining (KDD), KDD Project, Anchorage, Alaska, USA, 2019.
Demo PDF

MLsploit: A Cloud-Based Framework for Adversarial Machine Learning Research

Nilaksh Das, Siwei Li, Chanil Jeon, Jinho Jung, Shang-Tse Chen, Carter Yagemann, Evan Downing, Haekyu Park, Evan Yang, Li Chen, Michael Kounavis, Ravi Sahita, David Durham, Scott Buck, Duen Horng Chau, Taesoo Kim, and Wenke Lee
Black Hat Asia - Arsenal, 2019.
Demo Abstract Video

NeuralDivergence: Exploring and Understanding Neural Networks by Comparing Activation Distributions

Haekyu Park Fred Hohman, and Duen Horng Chau
IEEE Pacific Visualization Symposium (PacificVis), Bangkok, Thailand, 2019.
Demo PDF arXiv

SIDE: Representation Learning in Signed Directed Networks

Junghwan Kim, Haekyu Park, Ji-Eun Lee, and U Kang
The Web Conference (Previously known as WWW, World Wide Web Conference), Lyon, France, 2018.
Project PDF

A Comparative Study of Matrix Factorization and Random Walk with Restart in Recommender Systems

Haekyu Park, Jinhong Jung, and U Kang

IEEE International Conference on Big Data (BigData), Boston, MA, USA, 2017.
Project PDF arXiv

Open-Source Research Projects

CNN Explainer: Learning Convolutional Neural Networks with Interactive Visualization 2020

Keywords: Deep Learning Education, Interactive Visualization, Interactive Animation
Interactive visual system for learning Convolutional Neural Networks.
It was published at IEEE VIS (VAST, TVCG), 2020.
Zijie Jay Wang, Robert Turko, Omar Shaikh, Haekyu Park, Nilaksh Das, Fred Hohman, Minsuk Kahng, Duen Horng (Polo) Chau
Demo Top of Github Trending ★ 4,905 Github stars (as of Oct 2020)

Bluff: Interactively Deciphering Adversarial Attacks on Deep Neural Networks 2020

Keywords: Adversarial Attacks, Neural Network Interpretability, Activation Pathways, Interactive Visual Analytics
Interactive system for visualizing, characterizing, and deciphering adversarial attacks on vision-based neural networks.
It was published at IEEE VIS, 2020.
Nilaksh Das*, Haekyu Park*, Zijie Jay Wang, Fred Hohman, Robert Firstman, Emily Rogers, Duen Horng Chau
(* Equal Contribution)
Demo

Summit: Scaling Deep Learning Interpretability by Visualizing Activation and Attribution Summarizations 2019

Keywords: Neural Network Interpretability, Attribution Graph, Interactive Visual Analytics
Interactive visualization that scalably summarizes what features a deep learning model has learned and how those features interact to make predictions.
It was published at IEEE VIS (VAST, TVCG), 2019.
Fred Hohman, Haekyu Park, Caleb Robinson, Duen Horng Chau
Demo

MLsploit: A Framework for Interactive Experimentation with Adversarial Machine Learning Research 2019

Keywords: Adversarial Attacks and Defenses for Machine Learning Models, Interactive Experimentation
User-friendly, cloud-based system that enables researchers and practitioners to rapidly evaluate and compare state-of-the-art adversarial attacks and defenses for machine learning (ML) models.
It was published at a KDD 2019 Project Showcase.
Demo

SIDE: Representation Learning in Signed Directed Networks 2018

Keywords: Network Embedding, Signed Weighted Directed Graph
General network embedding method that represents both sign and direction of edges in the embedding space.
It was published at the Web Conference (WWW), 2018.
Project

A Comparative Study of Matrix Factorization and Random Walk with Restart in Recommender Systems 2017

Keywords: Recommender System, Matrix Factorization, Random Walk with Restart
We provide a comparative study of matrix factorization and RWR, which are the most representative recommender systems.
It was published at IEEE Big Data, 2017.
Project

Other Projects

DARPA Guaranteeing AI Robustness against Deception (GARD) 2020

Keywords: Defenses for Adversarial Examples, Robustness, Defense using Semantic Coherence
We develop defenses for adversarial attacks on object detector for both RGB images and single-camera video. We augment this object detector to support spatial, temporal, semantic coherence in videos.

RAPIDS and Cybersecurity: A Network Use Case 2019

Keywords: RAPIDS, NVIDIA, GPU-acceleration, Graph, Personalized Page Rank
We showcase an approach to flagging anomalous network communications in a large graph using a combination of structural graph features and graph analytics, running end-to-end in RAPIDS.
Presented at KDD 2019 NVIDIA RAPIDS tutorial with the cybersecurity use case notebook.

Recommender System for Videos on Oksusu Application 2017

Keywords: Deep Learning, Sequence/Word Embedding, Approx. k-NN, Heterogeneous Features
Our system recommends videos to users of Oksusu application, handling massive data on users' behaviors and heterogeneous information of videos.
SK Telecom, Seoul, Republic of Korea

A Fast Data Compression with Shared Virtual Memory in Heterogeneous System Architecture 2017

Keywords: OpenCL, GPGPU, SVM, HSA
I used general purpose computing on graphics processing units (GPGPU) and Shared Virtual Memory (SVM) in Heterogeneous System Architecture (HSA) for fast data deduplication methods. GPGPU and HSA provide a powerful basis for parallel computing in an easy programmable and efficient way.
Undergraduate thesis

Personalized Recommendation for Credit Card Rewards 2016

Keywords: Coupled Matrix Factorization, Time Series Data
We provide personalized recommendations for credit card rewards to customers using various side information of users and items. The main algorithm is TCMF (Time Coupled Matrix Factorization).
Hyundai Card, Seoul, Republic of Korea
News article (in Korean)

Talks & Presentation

Bluff: Interactively Deciphering Adversarial Attacks on Deep Neural Networks

Nilaksh Das*, Haekyu Park*, Zijie Jay Wang, Fred Hohman, Robert Firstman, Emily Rogers, Duen Horng Chau
(* Equal Contribution)
Oct 2020, Oral Presentation, IEEE VIS
Oct 2020, Presentation, Michigan Institute for Data Science (MIDAS) Consortium for researchers in Training

Accelerated Data Science in the Classroom: Teaching Analytics and Machine Learning with RAPIDS

Polo Chau and Haekyu Park
Mar 2020, Talk, NVIDIA's GPU Technology Conference (GTC)

NeuralDivergence: Exploring and Understanding Neural Networks by Comparing Activation Distributions

Apr 2019, Poster Presentation, PacificVis

A Comparative Study of Matrix Factorization and Random Walk with Restart in Recommender Systems
Dec 2017, Oral Presentation, IEEE Big Data

Tutorial

RAPIDS and Cybersecurity: A Network Use Case
Keywords: RAPIDS, NVIDIA, GPU-acceleration, Graph, Personalized Page Rank
Presented at KDD 2019 NVIDIA RAPIDS tutorial with the cybersecurity use case notebook

Teaching

Graduate Teaching Assistant
Georgia Institute of Technology, Atlanta, GA — Fall 2019
Data and Visual Analytics (CSE 6242)
Instructor: Polo Chau

Mentoring

Zhiyan Zhou
B.S. in Computer Science, Georgia Institute of Technology — Fall 2020 - Present
Visualization for Graph Exploration
AI Robustness against Adversarial Attacks

Megan Dass
B.S. in Computer Science, Georgia Institute of Technology — Fall 2020 - Present
AI Robustness against Adversarial Attacks

Omar Shaikh
B.S. in Computer Science, Georgia Institute of Technology — Fall 2019 - Present
Visualization for natural language processing
Received Outstanding Freshman Award

Rob Firstman
B.S. in Computer Science, Georgia Institute of Technology — Fall 2019 - Spring 2020
Visualization for deep learning interpretability

Robert Turko
B.S. in Computer Science, Georgia Institute of Technology — Fall 2019 - Spring 2020
Visualization for machine learning education

Licenses and Certifications

NVIDIA DLI Certificate – DLI Platform Course for Instructors, NVIDIA Deep Learning Institute
NVIDIA DLI Certificate – Fundamentals of Deep Learning for Computer Vision, NVIDIA Deep Learning Institute

Professional Service

Reviewer

CIKM 2020
VIS 2020
WiML 2019
KDD 2019
ICML 2019

Professional Membership

The Institute of Electrical and Electronics Engineers (IEEE). Since 2019.

Technical Skills

Programming Languages

Python, JavaScript, HTML, R, Matlab, Java, C, C++, Ocaml, Scheme

Machine Learning / Deep Learning / Data Science

TensorFlow, PyTorch, Keras, scikit-learn, OpenCV, Numpy, Pandas, SciPy, NetworkX

GPU-accelerated Data Science

cuGraph, cuDF, cuML, BlazingSQL, OpenCL

Data Visualization

D3.js, Three.js, WebGL, HoloViews, Matplotlib, WebGL, ggplot