

Zhang, Xiao (张潇)

BCI & ML Lab
School of Artificial Intelligence & Automation
Huazhong University of Science & Technology (HUST)

PHONE: +86 189-9551-1421
EMAIL: xiao_zhang@hust.edu.cn
WEB: zhangxiao96.github.io

RESEARCH EXPERIENCE

My research interests include generalization/memorization of DNNs, AI security, and brain-computer interfaces (BCIs). My ultimate goal is to understand the basic rules of our brain through AI research, and, if I am lucky enough, capture a glimmer of hope to construct AGI.

Current Apr 2019	Analysis of DNN's Prediction Landscape BCI & ML Lab, HUST <ul style="list-style-type: none">Study the influence of different optimization techniques (e.g., Batch Normalization, Dropout,...) on the linear regions of DNNs.Explore generalization and memorization of DNNs from the perspective of geometric analysis on prediction landscape.Through the analysis of DNN's prediction landscape, monitor test behaviors without any validation set.
Dec 2019 Sep 2018	Security in Brain-Computer Interfaces BCI & ML Lab, HUST <ul style="list-style-type: none">Construct adversarial noise on some popular CNN classifiers in EEG-based BCIs, and analyze its influence on the learned features.Construct adversarial noise on traditional approaches (e.g., Riemann-based pipeline, CCA, ...) used in EEG-based BCI spellers (e.g., P300 speller, SSVEP speller,...).Consider the causality of constructing adversarial noise for time series.

EDUCATION

Jun 2021 Sep 2018	M.Eng. - School of Artificial Intelligence & Automation, HUST GPA: 90.3/100, Rank: 12/188 Supervisor: Prof. Dongrui Wu
Jun 2018 Sep 2014	B.Eng. - School of Optical & Electronic Information, HUST GPA: 3.91/4.0, Rank: 5/318 Supervisor: Prof. Danhua Cao

PUBLICATIONS

DEEP LEARNING	<ul style="list-style-type: none">X. Zhang and D. Wu, "Rethink the Connections among Generalization, Memorization and the Spectral Bias of DNNs," in Proc. The Thirty-Fifth AAAI Conf. on Artificial Intelligence, 2020, <i>submitted</i>.X. Zhang and D. Wu, "Empirical Studies on the Properties of Linear Regions in Deep Neural Networks," in Proc. Int'l Conf. on Learning Representations (ICLR), Addis Ababa, Ethiopia, April 2020.
BCI & SECURITY	<ul style="list-style-type: none">X. Zhang, D. Wu, L. Ding, H. Luo, C-T Lin, T-P Jung and R. Chavarriaga, "Tiny Noise, Big Mistakes: Adversarial Perturbations Induce Errors in Brain-Computer Interface Spellings," National Science Review, 2020, <i>Accepted</i>.

- Z. Liu*, **X. Zhang***, D. Wu, "Universal Adversarial Perturbations for CNN Classifiers in EEG-Based BCIs ," IEEE Trans. on Neural Systems and Rehabilitation Engineering, 2020, *Submitted*.
- **X. Zhang** and D. Wu, "On the Vulnerability of CNN Classifiers in EEG-Based BCIs," IEEE Trans. on Neural Systems and Rehabilitation Engineering, vol. 27, no. 5, pp. 814-825, 2019.
- X. Jiang, **X. Zhang**, D. Wu, "Active Learning for Black-Box Adversarial Attacks in EEG-Based Brain-Computer Interfaces ," IEEE Symposium Series on Computational Intelligence, Xiamen, China, December 2019.

HONORS

2020	Goodix Scholarship for Technology
2019	National Scholarship for Postgraduates
2019	1 st Place - China Brain-Computer Interface Competition
2018	"Outstanding Graduate" of HUST
2018	"Honor College Student" of Qiming College of HUST
2015	2 nd Place - The 7 th Mathematics Competition of Chinese College Students
2015	National Encouragement Scholarship