

# 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

---

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

## EDUCATION

---

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

## PUBLICATIONS

---

<b>DEEP LEARNING</b>	<ul style="list-style-type: none"><li>• <b>X. Zhang</b>, D. Wu, H. Xiong and B. Dai, "Optimization Variance: Exploring Generalization Properties of DNNs," in Proc. Int'l Conf. on Learning Representations (ICLR), 2021, <i>submitted</i>.</li><li>• <b>X. Zhang</b>, D. Wu and H. Xiong, "Rethink the Connections among Generalization, Memorization and the Spectral Bias of DNNs," in Proc. The Thirty-Fifth AAAI Conf. on Artificial Intelligence, 2021, <i>submitted</i>.</li><li>• <b>X. Zhang</b> 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. (Poster)</li></ul>
<b>BCI &amp; SECURITY</b>	<ul style="list-style-type: none"><li>• <b>X. Zhang</b>, 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>. (IF=16.69)</li></ul>

- 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*. (IF=3.34)
- **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. (IF=3.34)

## HONORS

---

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