### **BoYang ZHENG**

Undergraduate of Computer Science and Technology

in Shanghai Jiao Tong University (SJTU)

**2003** April.

Shanghai https://bytetriper.com.cn/

with good foundations of math. Passionate about deep learning. Currently research interests are Computer Vision, Generative Models, Multi-modal models and Adversarial Attacks.

# Competences & Languages

90.22/100, rank 9/33 in ACM Honor Class 2021

#### **Education**

present ACM Honor Class 2021, Shanghai Jiao Tong University September 2021 Undergraduate in Computer Science and Technology

# </> Experiences & Projects

> AI-related experiences: **Hands-on experience** with:

- PEFT(parameter efficient fine-tuning) Diffusion Models (Stable-Diffusion specifically).
- PEFTing LLMs (Llama2 specifically) on vision tasks.
- Building and training CNN, RNN, LSTM, Transformer, ViT etc. (implemented by pure PyTorch).
- > CPU: (Verilog) A CPU with tomasulo algorithm, branch prediction and out-of-order execution. Written with verilog and runs on an actual FPGA.
- > Compiler: (java) An OO level, graph-coloring based compiler for a self-defined language called Mx\*, which resembles Java much.

### Papers

- > Improved AdvDM: <Understanding and Improving Adversarial Attacks on Latent Diffusion Model>: A research about crafting general and strong adversarial examples against latent diffusion models (especially Stable Diffusion). This paper is under review of ICLR 2024. [Co-first Author]
- > [Course Work] Latent Magic: <Latent Magic: An Investigation into Adversarial Examples Crafted in the Semantic Latent Space>: A reseach into adversarial attacks crafted in latent space, which purposed the FIRST evaluation metric in this field. This paper served as the project of machine learning class. [Only Author

## Selected Courses

> Computer Programming: 94/100

> Data Structure: **94/100** 

> Machine Learning: **95/100** (top one paper award)

> Algorithm: **99/100**.

> Data Mining: **97.6/100** (top one in kaggle contest)

> Mathematical Analysis: 96/100