Tokyo, Japan

Futa (Kai) Waseda

futa-waseda@g.ecc.u-tokyo.ac.jp

Summary:

- I am a 3rd-year PhD student at The University of Tokyo, Japan, majoring in Computer Science.
- I have papers on **robustness and reliability of deep learning models** (**WACV'23**, **ICML'23**, **ICIP'24**, **ICLR'25**, **ACL'25 Main**, **ACMMM'25**), showcasing sufficient research capability and expertise.
- **Proficient in English communication and collaboration**, evidenced by the successful collaboration with the Technical University of Munich (TUM), leading to acceptance at **ICML2023**.
- **Many Collaboration experiences** with various teams, including research experience with **NEC Corporation**, **TUM**, **CyberAgent AI Lab**, and **SB Intuitions**, and Research & Development experience at **Ollo Inc.**.

Personal Info

- Nationality: Japan / USA *(Dual nationality.* ***No VISA required to work in the USA)***
- Language: Japanese (Native), English (Advanced; *TOEFL: 96/120)*
- Website: https://futa-waseda.netlify.app | Github: https://github.com/futakw
- Google scholar: https://scholar.google.co.jp/citations?user=aBQ2en8AAAAJ&hl=en

Education

PhD candidate **The University of Tokyo, Japan** **April 2023 – (March 2026)**

- Information Science and Technology | Supervisor: Prof. Isao Echizen *(Expected graduation: March 2026)*
- Researching on the robustness and reliability of deep learning models.

Exchange Student **Technical University of Munich, Germany** **April 2021 – March 2022**

- Informatics | Joined Prof. Daniel Cremers's lab, supervised by Christian Tomani.
- Developed a state-of-the-art method for robustly calibrating the uncertainty estimation of computer vision models in distribution-shift scenarios, accepted at **ICML2023**, highlighting strong English communication and collaboration skills.
- Coursework: Novel Challenges on Deep Learning; Biologically-inspired Methods; Cognitive Neuroscience.
- Received **UTokyo-TOYOTA Study Abroad Scholarship 2021**, as a top-level AI researcher.

M.Sc. **The University of Tokyo, Japan** **April 2020 – March 2023**

- M.Sc. of Information Science and Technology (March 2023) | Supervisor: Prof. Isao Echizen | **GPA: 3.93/4.00**.
- Developed a novel theory on adversarial example transferability between models, accepted at **WACV2023**, marking a novel direction in my lab and showcasing my strong passion and curiosity.
- Coursework: Artificial Intelligence; Computer Vision; Neurointelligence; Cognitive Science.

B.Eng. **The University of Tokyo, Japan** **April 2016 – March 2020**

- B.Eng. in Systems Innovation (March 2020) | Supervisor: Prof. Kenji Tanaka | **Major GPA: 3.52/4.00**.
- Developed an auto-bidding agent in multi-agent systems for the peer-to-peer electricity trading market, addressing uncertainties. Accepted at **IEEE EEEIC2020**, in collaboration with TOYOTA, showing strong industry collaboration skills.
- Coursework: Mathematics; Programming; Statistical Machine Learning; Image Media Technologies; Strength of Materials; Fluid Mechanics; Economics; Multi-Agent System; Engineering Simulation.

Employment

Research Internship **SB Intuitions, Japan** **Aug. 2024 – (current)**

- Research on protecting IP of Large Language Models (Accepted at **ACL'25 Main**).

Research Internship **CyberAgent AI Lab, Japan** **February 2024 – (current)**

- Research on adversarial robustness of vision-language models (Accepted to **MIRU2024 Oral (Top 31%)**.

Research Internship (4 month) **NEC Corporation, Japan** **August 2023 – December 2023**

- Research on domain generalization of computer vision models, joining the Secure System Platform team.
- The proposed method was patented (To be announced).

Senior Researcher **Ollo Inc., Japan** **April 2020 – Present**

- Developed the central algorithm for behavior recognition in factories (when I was an *Algorithm Engineer*), resulting in a remarkable 20% efficiency boost in factories, demonstrating strong coding skills (Python, PyTorch) and real-world problem-solving abilities.
- Promoted to *Senior Researcher* in October 2023, providing the algorithm team with guidance based on current research trends and my expertise as an AI researcher.

Research Assistant **National Institute of Informatics, Japan** **April 2020 – Present**

- Focused research on computer vision model robustness and reliability, which led to accepted papers at **WACV2023** and **ICML2023**, demonstrating strong research capabilities.
- Supervised a 6-month international intern in our lab, proposed the first technique for safeguarding infrared human detection against adversarial patches (under review), which demonstrates my ability to plan research to fit the timeline, align tasks with students' abilities, and provide expert guidance.

Publications (First-authored)

- Futa Waseda, Saku Sugawara, and Isao Echizen. "Quality Text, Robust Vision: The Role of Language in Enhancing Visual Robustness of Vision-Language Models", **ACMMM 2025**.
- Shojiro Yamabe*, Futa Waseda*, Tsubasa Takahashi, and Koki Wataoka. "MergePrint: Merge-Resistant Fingerprints for Robust Black-box Ownership Verification of Large Language Models", **ACL 2025 Main**. (*Equal-contribution co-first author)
- Futa Waseda, Ching-Chun Chang and Isao Echizen "Rethinking Invariance Regularization in Adversarial Training to Improve Robustness-Accuracy Trade-off", **ICLR 2025**.
- Lukas Strack* and Futa Waseda* et al. "Defending Against Physical Adversarial Patch Attacks on Infrared Human Detection.", **ICIP 2024**. (*Equal-contribution co-first author)
- Tomani, Christian* and Futa Waseda* et al. "Beyond In-Domain Scenarios: Robust Density-Aware Calibration." **ICML 2023**. (*Equal-contribution co-first author)
- Futa Waseda et al. "Closer Look at the Transferability of Adversarial Examples: How They Fool Different Models Differently." **WACV 2023**.
- Futa Waseda, and Kenji Tanaka. "Bidding agent for electric vehicles in peer-to-peer electricity trading market considering uncertainty." **EEEIC/I&CPS Europe. IEEE, 2020**.

Reviewer Experience

- NeurIPS'25, ICML'25, ICLR'25, ICML'24, IEEE TIFS'24, ICLR'24, APSIPA'23, NeurIPS'23

Awards

- **Outstanding Performance Award** (top 2/20 teams) in course "Advanced Artificial Intelligence Theory" from The University of Tokyo (link). Developed an image-to-text model capable of understanding humor and generating humorous social media posts, highlighting my creative application of expertise.
- **Special Prize** (top 2/18 teams) at The Analytics Hackathon 2019 hosted by SAS Institute Japan Inc. Developed a high-performance AI for predicting machinery malfunctions using operational data, showcasing real-world problem-solving abilities with machine learning.
- **First-Place Award** (top 1/7 teams) at the MDS Data Science Contest 2018 at The University of Tokyo. Discovered a new insight into the food industry by analyzing large-scale lifestyle data, demonstrating my fundamental data science capabilities.

Scholarships

- **PhD Research Fellowship (DC2)** from Japan Science and Technology Agency (JST). 1,300$/month. Acceptance rate: 18%. (April 2024 – March 2026)
- **SPRING GX** from Support for Pioneering Research Initiated by Next Generation (SPRING) of Japan Science and Technology Agency (JST). 1,200$/month. Acceptance rate: 25%. (April 2023 – March 2024)
- **Special Research Assistant 2023** at Information, Science and Technology Department, The University of Tokyo. Selected as A+ prioritized research assistant (declined after the SPRING GX acceptance).
- **UTokyo-TOYOTA Study Abroad Scholarship 2021**. 1,920$/month. Top 2 students in the university. (April 2021 – March 2022)

Research Fund

- **AIP Challenge Program** from Japan Science and Technology Agency (JST). 7,000$. (April 2023 – March 2024)

Skills

- **Programming:** Python; Java; HTML; CSS; JavaScript;