Tokyo, Japan

Futa (Kai) Waseda

futa-waseda@nii.ac.jp

Summary:

- 3rd-year Ph.D. student in Computer Science at The University of Tokyo.
- Research focus: robustness and reliability of deep learning models (adversarial robustness, calibration, vision-language security).
- Publications: **WACV'23, ICML'23, ICIP'24, ICLR'25, ACL'25 Main, ACMMM'25, WACV'26**.
- Awards/Scholarships: **NII Inose Outstanding Student Award (2025)**; **JSPS DC2** (acceptance rate: **17.9%**).
- Collaboration: Technical University of Munich (TUM), NEC, CyberAgent AI Lab, SB Intuitions, Turing Inc., and Ollo Inc.
- English: TOEFL iBT **96**/120.

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 (expected)**

- Information Science and Technology | Supervisor: Prof. Isao Echizen
- Research: robustness and reliability of deep learning models.

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

- Informatics | Hosted by Prof. Daniel Cremers; supervised by Christian Tomani.
- Research outcome (international collaboration): robust uncertainty calibration under distribution shift; accepted at **ICML 2023**.
- Coursework: Novel Challenges on Deep Learning; Biologically-inspired Methods; Cognitive Neuroscience.
- Scholarship (selective): **UTokyo–TOYOTA Study Abroad Scholarship 2021**.

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

- M.Sc. in Information Science and Technology (March 2023) | Supervisor: Prof. Isao Echizen | **GPA: 3.93/4.00**.
- Research outcome (core contribution): theory on adversarial example transferability; accepted at **WACV 2023**.
- 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**.
- Research outcome (industry-academia): auto-bidding agent for peer-to-peer electricity trading under uncertainty; accepted at **IEEE EEEIC 2020** (with TOYOTA).
- Coursework: Mathematics; Programming; Statistical Machine Learning; Image Media Technologies; Strength of Materials; Fluid Mechanics; Economics; Multi-Agent System; Engineering Simulation.

Employment

Research Internship | **Turing Inc., Japan** | **April 2025 – present**

- Research on reliable vision-language models.

Research Internship | **SB Intuitions, Japan** | **Aug. 2024 – Aug. 2025**

- Research on IP protection for large language models (**ACL 2025 Main**).

Research Internship **CyberAgent AI Lab, Japan** **Feb. 2024 – Jan. 2026**

- Research on adversarial robustness of vision-language models (**MIRU 2024 Oral (Top 31%)**; **WACV 2026**).

Research Internship **NEC Corporation, Japan** **Aug. 2023 – Dec. 2023**

- Research on domain generalization for computer vision models (Secure System Platform team).
- Resulted in a filed patent (details to be disclosed).

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

- Built a core behavior-recognition algorithm for factory operations (Python/PyTorch), contributing to a **20% efficiency improvement** in deployed sites.
- Promoted to *Senior Researcher* (Oct. 2023); led technical direction-setting and mentorship within the algorithm team.

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

- Conducted research on robustness and reliability in computer vision, leading to publications at **WACV 2023, ICML 2023, ICLR 2025, ACMMM 2025, WACV 2026, etc**.
- Mentored a 6-month international intern; initiated a project on defending infrared human detection against adversarial patches (**ICIP 2024**).

Publications (First-authored)

- Futa Waseda, Antonio Tejero-de-Pablos, and Isao Echizen. "Multimodal Adversarial Defense for Vision-Language Models by Leveraging One-To-Many Relationships", **WACV 2026**.
- 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

- CVPR('26), NeurIPS('23,'25), ICML('24,'25), ICLR('24,'25,'26), IEEE TIFS('24), APSIPA('23)

Awards

- **NII Inose Outstanding Student Award, 2025**—NII's top student award for Ph.D. graduates supervised by NII (National Institute of Informatics, Japan).
- **Outstanding Performance Award**—Top 2/20 teams, "Advanced Artificial Intelligence Theory" (The University of Tokyo). Built an image-to-text model that generates humor-aware social media captions (link).
- **Special Prize**—Top 2/18 teams, The Analytics Hackathon 2019 (SAS Institute Japan). Developed an AI model to predict machinery failures from operational data (link).

- **First-Place Award**—Top 1/7 teams, MDS Data Science Contest 2018 (The University of Tokyo). Identified a new insight in the food industry using large-scale lifestyle data (link).

Scholarships

- **PhD Research Fellowship (DC2)** from The Japan Society for the Promotion of Science (JSPS). 1,300$/month. Acceptance rate: 17.9%. (April 2024 – March 2026)
- **SPRING GX** from Support for Pioneering Research Initiated by Next Generation (SPRING) of Japan Science and Technology Agency (JST). 1,200$/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