Wonjun **Lee**

Ph.D. Candidate in Electical Engineering, CILAB, KAIST

291, Daehak-ro, Yuseong-gu, Daejeon, 34141, Rep. of KOREA

(+82) 10-5420-3553 | dpenguin2000 [at] gmail.com | Wonjun-Lee1009 | Google Scholar

I am currently pursuing an Ph.D. degree in Electrical Engineering at KAIST. My academic journey began at Gyeonggi Science High School for the Gifted, which fostered my passion for research and innovation. I then earned my B.S. in Electrical Engineering and Computer Science at KAIST, and M.S. in Electrical Engineering at KAIST. I enjoy engaging with creative challenges and value building meaningful relationships along the way. Please feel free to explore my academic background below and contact me directly for further details.

Research Interest

As AI's role expands across various fields, building **trustworthy AI** is crucial. I am particularly interested in AI security, as vulnerabilities compromise reliability and fairness.

Additionally, as humans rely on various senses for judgment, I focus on research in **multi-modal learning** and **vision foundation models**. My goal is to help bridge the understanding between AI and humans.

My work explores the following, but not limited to:

- **Multimedia Forensics**: detecting forgeries, synthetic image, and deepfakes
- **AI Security**: adversarial attack, jailbreaking and their defense
- **Multi-Modal Learning**
- **Vision Foundation Models**

Education

Korea Advanced Institute of Science and Technology (KAIST) — *Daejeon, S.Korea*

Ph.D. in Electrical Engineering — *Mar. 2025 - Present*

Korea Advanced Institute of Science and Technology (KAIST) — *Daejeon, S.Korea*

M.S. in Electrical Engineering — *Mar. 2023 - Feb. 2025*

Korea Advanced Institute of Science and Technology (KAIST) — *Daejeon, S.Korea*

B.S. in Electrical Engineering & Computer Science (Double Major) — *Mar. 2019 - Feb. 2023*

Gyeonggi Science High School for the Gifted (GSHS) — *Suwon, Gyeonggi-do, S.Korea*

Major in Math, Physics, and Biology — *Mar. 2016 - Feb. 2019*

Publication

International

Efficient Test-Time Optimization for Depth Completion via Low-Rank Decoder Adaptation — *2026*

PREPRINT — *Depth Estimation, VFM*

Minseok Seo*, **Wonjun Lee***, Jaehyuk Jang, Changick Kim **(*: Equal Contribution)**

Generalizable Prompt Tuning for Audio-Language Models via Semantic Expansion — *2026*

PREPRINT — *Prompt Tuning*

Jaehyuk Jang*, **Wonjun Lee***, Kangwook Ko*, Changick Kim, Changick Kim **(*: Equal Contribution)**

SELFI: Selective Fusion of Identity for Generalizable Deepfake Detection — *2025*

PREPRINT — *Deepfake Detection*

Younghun Kim, Minsuk Jang, Myung-Joon Kwon, **Wonjun Lee**, Changick Kim

Benign-to-Toxic Jailbreaking: Inducing Harmful Responses from Harmless Prompts — *2025*

PREPRINT — *Multimodal LLM Jailbreak*

Hee-Seon Kim, Minbeom Kim, **Wonjun Lee**, Kihyun Kim, Changick Kim

SAFIRE: Segment Any Forged Image Region — *2025*

AAAI Conference on Artificial Intelligence (**AAAI**) — *Image Forgery Localization*

Myung-Joon Kwon*, **Wonjun Lee***, Seung-Hun Nam, Minji Son, Changick Kim **(*: Equal Contribution)**

FRIDAY: Mitigating Unintentional Facial Identity in Deepfake Detectors Gudided by Facial Recognizers *2024*

Visual Communications and Image Processing (**VCIP**) **Oral Presentation** *Deepfake Detection*

Younghun Kim, Myung-Joon Kwon, **Wonjun Lee**, Changick Kim

Domestic

Ensembling Pretrained Models for Enhanced Generalization in Synthetic Image Detection *2024*

Institute of Electronics and Information Engineers (**IEIE**) **LG Electronics Paper Award** *Synthetic Image Detection*

Myung-Joon Kwon, **Wonjun Lee**, Younghun Kim, Changick Kim

Combatting Bias: Corrective Measures Through Adversarial Training in Neural Networks *2024*

Institute of Electronics and Information Engineers (**IEIE**) **LG Electronics Paper Award** *De-Biasing, Adversarial Training*

Wonjun Lee, Myung-Joon Kwon, Younghun Kim, Changick Kim

Improving the Generalization Performance of Deepfake Detection Through a Partial Image Manipulation Augmentation Technique *2024*

Institute of Electronics and Information Engineers (**IEIE**) *Deepfake Detection*

Younghun Kim, Myung-Joon Kwon, **Wonjun Lee**, Changick Kim

Research Experience

Roen Surgical *Daejeon, S.Korea*

KAIST EE Externship Program Second Cohort *Jun.2022 – Dec.2022*

SAMSUNG Electronics CE/IM Division *Mobile Communications Unit* *Remote*

Summer Internship *Jul.2021 - Aug.2021*

SAMSUNG Electronics DS Division *Foundry Business Unit* *Hwaseong, Gyeonggi-do, S.Korea*

Samsung Talent Internship Program (STIP) *Jul.2020 - Aug.2020*

Patent

A Universal Image-Generation Framework for Jailbreaking Large Vision–Language Models by Bypassing Safety Alignment *2025*

KR Patent 10-2025-0157353

- Participated as a Key Developer in Patent Development
- Participated through the Project with ETRI

Method and System for Generating Universal Adversarial Perturbations Using High-Sensitivity Components of Vision Encoders in Large-Scale Vision-Language Models *2025*

KR Patent 10-2025-0194468

- Participated as a Key Developer in Patent Development
- Participated through the Project with IITP

Stone size estimation method *2023*

KR Patent 10-2023-0031846

- Participated as a Key Developer in Patent Development
- Participated through the KAIST EE Externship

Honors & Awards

2024 **LG Electronics Paper Award**, Summer Annual Conference of IEIE *Jeju, S.Korea*

2023 **Certificate**, KAIST Leadership and Volunteer Excellence Award Certificate *Daejeon, S.Korea*

2022 **Certificate**, KAIST CS348 Certificate of Appreciation *Daejeon, S.Korea*

2018 **Bronze Award**, SAMSUNG Humantech Paper Award Biology Division — *Seoul, S.Korea*
2017 **3rd Place**, Mathematics Education Joint Academic Conference R&E Poster Presentation Competition — *S.Korea*
2017 **1st Place (Minister of Oceans and Fisheries Award)**, Marine Biology Research Competition — *Incheon, S.Korea*
2017 **Bronze Award**, Korean Mathematics Competition (KMC) — *S.Korea*
2017 **4th Place**, Korean Mathematics Olympiad (KMO) — *S.Korea*
2017 **Award Certificate**, President of Korean Earth Science Society — *S.Korea*

Project

Development of AI Technology with Robust and Flexible Resilience Against Risk Factors — *Jan. 2025 - Dec. 2028*

Electronics and Telecommunications Research Institute (ETRI)

- Team Leader

Penetration Security Testing of ML Model Vulnerabilities and Defense — *Jan. 2025 - Dec. 2027*

Institute for Information & communication Technology Planning & evaluation (IITP)

Scene Text Recognition with Visual Contexts — *Sep. 2024 - Dec. 2024*

Center for Security Technology Research, KAIST

Bypass Techniques for Identifying Vulnerabilities in CAPTCHA — *Mar. 2023 - Dec. 2023*

Center for Security Technology Research, KAIST

Practical Adversarial Attacks of AI Facial Recognition Technology Using Physical Patterns — *Mar. 2023 - Dec. 2023*

Center for Security Technology Research, KAIST

Presentation

KAIST EE Career Concert 2024 — *Daejeon, S.Korea*

Presenter — *May. 2024*

- This program is for undergraduate students in EE who are struggling to decide on their career path
- Present about my undergraduate years, what led me to pursue graduate studies, and what research I am currently conducting

KAIST EE Career Concert 2022 — *Daejeon, S.Korea*

Presenter — *Nov. 2022*

- Shared experiences at the KAIST EE Externship Program

Extracurricular Activity

KAIST Electrical Engineering TA — *Daejeon, S.Korea*

Member — *Sep. 2023 - Present*

- Signals and Systems - Fall 2023
- Introduction to Electronics Design Lab - Fall 2023, Fall 2024, Spring 2025
- Digital Image Processing - Spring 2024
- EE Career Development I - Spring 2025, Spring 2026
- Introduction to Machine Learning - Fall 2025

KAIST Student Counseling Assistant (CA) — *Daejeon, S.Korea*

Member — *Mar. 2024 - Feb. 2025, Sep. 2025 - Present*

- The CA (Counseling Assistant) program aims to expand counseling support opportunities for students and graduate students to ensure a smooth academic/school life and career planning.
- Participants work autonomously with peers to enhance their development skills and foster personal growth.

MadCamp 11th Cohort Hosted by KAIST CS — *Daejeon, S.Korea*

Member — *Sep. 2019*

- MadCamp is an intensive program in collaboration with KAIST, focused on app, web, and game development for undergraduate students in South Korea.
- Participants work autonomously with peers to enhance their development skills and foster personal growth.

KAIST Electrical Engineering Student Council — *Daejeon, S.Korea*

Vice Department Representative — *Feb. 2020 - Feb.2022*

KAIST Dance Crew Illusion *Daejeon, S.Korea*

President *Jan. 2020 - Feb.2022*

Awarded the Best Team Title in the Outstanding Freshman *Daejeon, S.Korea*

Member *Sep. 2019*

Awarded the Outstanding Freshman *Daejeon, S.Korea*

Member *Sep. 2019*

Vice Class Leader of KAIST Freshman Class 6 *Daejeon, S.Korea*

Vice Class Leader *Mar. 2019 - Feb. 2020*