Woo Jae Kim

School of Computing
Korea Advanced Institute of Science and Technology (KAIST)
☎ *(+82) 010-4584-3490*
✉ *woojae1123@gmail.com / wkim97@kaist.ac.kr*
Personal Webpage
Github *Google Scholar*

Computer Vision · Adversarial Machine Learning

Highlights

Extensive research experience in adversarial defense.
Participated as the first author on one project; published a paper at CVPR 2023 as a highlights paper.

Extensive research experience in adversarial attack.
Participated as the first author on two projects; published a paper at ICIP 2022 as an oral paper and submitted a paper to CVPR 2024.

Research experience in computer vision and rendering fields.
Participated as a co-author on six projects related to numerous fields in computer vision and rendering.

Education

2023 – present: **Ph.D., School of Computing**, *KAIST, Daejeon, Korea*.
Advisor: Sung-Eui Yoon
Research topics: Adversarial attack & defense

2021 – 2023: **M.S., School of Computing**, *KAIST, Daejeon, Korea*.
Advisor: Sung-Eui Yoon
Research topics: Adversarial attack & defense
Thesis: Diverse Generative Perturbations on Attention Space for Transferable Adversarial Attacks

2016 – 2021: **B.S., School of Computing**, *KAIST, Daejeon, Korea*.
Minor in Electrical Engineering

Publications

First-authored

[C.5] Feature Separation and Recalibration for Adversarial Robustness.
Woo Jae Kim, Yoonki Cho, Junsik Jung, and Sung-Eui Yoon.
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2023*
Highlights paper (∼ 2.6% acceptance rate)
[Paper] [Code]

[C.3] Diverse Generative Perturbations on Attention Space for Transferable Adversarial Attacks.
Woo Jae Kim, Seunghoon Hong, and Sung-Eui Yoon.
*IEEE International Conference on Image Processing (**ICIP**), 2022*
Oral paper (∼ 10% acceptance rate)
[Paper] [Code]

Co-authored

[C.6] Towards Content-based Pixel Retrieval in Revisited Oxford and Paris.
Guoyuan An, **Woo Jae Kim**, Saelyne Yang, Rong Li, Yuchi Huo, and Sung-Eui Yoon.
*IEEE/CVF International Conference on Computer Vision (**ICCV**), 2023*
[Paper] [Code]

[C.4] Pixel-wise Guidance for Utilizing Auxiliary Features in Monte Carlo Denoising.
Kyubeom Han, Olivia G. Odenthal, **Woo Jae Kim**, and Sung-Eui Yoon.
*ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games (**i3D**), 2023*
also published at Proceedings of the ACM on Computer Graphics and Interactive Techniques (PACM-CGIT)
[Paper] [Code]

[C.2] Part-based Pseudo Label Refinement for Unsupervised Person Re-identification.
Yoonki Cho, **Woo Jae Kim**, Seunghoon Hong, and Sung-Eui Yoon.
*IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**), 2022*
[Paper] [Code]

[C.1] Deep Video Inpainting Guided by Audio-Visual Self-Supervision.
Kyuyeon Kim, Junsik Jung*, **Woo Jae Kim***, and Sung-Eui Yoon. (** equal contributions*)
*IEEE International Conference on Acoustics, Speech and Signal Processing (**ICASSP**), 2022*
[Paper] [Code]

Projects

Recalibrating Non-robust Feature Activations for Adversarial Robustness.
at Scalable Graphics, Vision, & Robotics Lab [*C.5*]
• Designed and implemented the *Feature Separation and Recalibration* module that restores discriminative cues from corrupted feature maps of adversarial examples.
• Significantly improved robustness of various adversarial training strategies with small computational overhead.

Improving the Transferability of Adversarial Attacks.
at Scalable Graphics, Vision, & Robotics Lab [*C.3*]
• Designed and implemented an adversarial attack that generates highly transferable adversarial examples across different models via stochastic exploration of adversarial vulnerability on the image attention space.
• Achieved the state-of-the-art adversarial attack transferability at the time of publication.

Implementing Scheduling Techniques for xv6 Operating System.
at Computer Architecture and Systems Lab
• Implemented and analyzed the lottery scheduling on xv6, a C-based operating system.

Designing a Parser Program for DRAM Failure Logs.
at SK Hynix
• Implemented a parser program for analyzing the faults of DRAMs based on the failure logs.

Fellowships & Awards

Nov. 2023 ***Recipient*** of the Qualcomm Innovation Fellowship.

Feb. 2022 ***Paper Award*** in the 34th Workshop on Image Processing and Image Understanding (IPIU).

Aug. 2023, Feb. 2022 ***Best TA Award*** in School of Computing, KAIST.

Feb. 2021 ***Grand Prix Award (1st place)*** in the Undergraduate Research Program (URP) in KAIST.

Invited Talks & Presentations

Jan. 2024 Invited to Qualcomm Korea to give a talk on adversarial robustness [C.5].

Feb. 2022 Invited to Korean Conference on Computer Vision (KCCV) 2023 for oral and poster presentations on adversarial robustness [C.5].

Skills

Languages	Korean Native, English Native
Programming Languages	Python, C, C++, Java, MATLAB, R
Tools	PyTorch, Tensorflow, Keras, Numpy, LaTex
Web Technologies	HTML, CSS, Javascript

Professional Service

2023 **CVPR**, Reviewer.

2023 **ICCV**, Reviewer.

Teaching Experience

2023 **Teaching Assistant, Samsung Electronics**.
AI Expert Program

2018-2019, 2021-2023 **Teaching Assistant, KAIST**.
CS101 Introduction to Programming

2021, 2023 **Teaching Assistant, KAIST**.
CS206 Data Structure