

Seungmin Kim

☎ 010-6641-5024 • ✉ kims0802@soongsil.ac.kr • 📄 Google Scholar

Research Interests

My research focuses on **AI Safety**, with particular interests in **Adversarial Robustness** and **Speech AI Security**. I study security vulnerabilities in **speech AI systems** by analyzing speaker identity, acoustic characteristics, and the underlying mechanisms of speech synthesis models. My research also involves developing robust **voice protection** techniques and designing **attack and defense methods** for modern speech synthesis systems. Recently, I have expanded my interests to the safety and security of **Audio Language Models (ALMs)**.

Education

Soongsil University

M.S. in Software, GPA: 4.5/4.5

Seoul, South Korea

Mar. 2025 – Feb. 2027 (Expected)

○ Research focus: AI Safety, Adversarial Robustness, Speech AI Security

Soongsil University

B.S. in Software, GPA: 3.0/4.5

Seoul, South Korea

Mar. 2021 – Feb. 2025

○ Relevant Coursework: Machine Learning, Artificial Intelligence, Algorithms, Linear Algebra

Work Experience

AI Safety Center, Soongsil University

Undergraduate Student Intern

Seoul, South Korea

Jul. 2022 – Feb. 2025

Publications

International Conference

NaVo: Natural Voice Protection against Voice Cloning Attacks via Generative Universal

Sep. 2026

Adversarial Audio

Accepted to Interspeech 2026

Seoyoung Park*, *Seungmin Kim**, Sohee Park, Dain Kim, et al.

*These authors contributed equally and are listed in alphabetical order.

RoCo: Robust Code for Fast and Effective Proactive Defense against Voice Cloning Attack

May. 2026

2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2026, *Oral*)

Seungmin Kim, Dain Kim, Sohee Park, and Daeseon Choi

Session Replication Attack Through QR Code Sniffing in Passkey CTAP Registration

Jun. 2024

39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024)

Donghyun Kim, *Seungmin Kim*, Gwonsang Ryu, and Daeseon Choi

Face Verifiable Anonymization in Video Surveillance

Aug. 2023

24th World Conference on Information Security Applications (WISA)

Sungjune Park, Hyunsik Na, *Seungmin Kim*, and Daeseon Choi

Submitted / Under Review

MUTE: Multi-Level Alignment Uncoupling Against Talking-Head Exploitation for Voice Protection

2026

Advances in Neural Information Processing Systems (NeurIPS 2026)

Donghyun Kim*, Jin Hong*, *Seungmin Kim**, Dain Kim, Junseok Kwon, and Daeseon Choi

*These authors contributed equally and are listed in alphabetical order.

RoVo: Robust Voice Protection Against Voice Cloning Attacks via Embedding-Level Adversarial Perturbations

2026

ACM International Conference on Multimedia 2026 (ACM MM 2026)

Seungmin Kim, Sohee Park, Dain Kim, Donghyun Kim, Jisu Lee, and Daeseon Choi

Domestic Journal.....

Voice Synthesis Detection Using Language Model-Based Speech Feature Extraction Jun. 2024
The Korea Institute of Information Security & Cryptology (KCI Indexed)
Seungmin Kim, Sohee Park, and Daeseon Choi

Comparison of Korean Speech De-identification Performance of Speech De-identification Model and Broadcast Voice Modulation Mar. 2023
Smart Media Journal (KCI Indexed)
Seungmin Kim, Daeul Park, and Daeseon Choi

Domestic Conference.....

Proactive Defense Against DeepVoice Misuse via Voice Codebook Perturbation Jun. 2025
Korea Information Security Society Yeongnam Branch Academic Conference
Seungmin Kim, Dain Kim, and Daeseon Choi

DeepVoice Threat Response: Current Technological Trends Jun. 2025
Korea Information Security Society Summer Academic Conference
Dain Kim, *Seungmin Kim*, and Daeseon Choi

A Study on Voice Reconstruction Methods for Defending Against AI-based Deep Voice Generation Sep. 2024
Korea Information Security Society Winter Academic Conference
Seungmin Kim, Sohee Park, and Daeseon Choi

Speech Synthesis Classification Using BERT Sep. 2023
Korea Information Security Society Chungcheong Branch Academic Conference
Seungmin Kim, Donghyun Kim, and Daeseon Choi

A Proposal for Improvement of Security Vulnerability in Broadcast Voice Modulation Using Lightweight Anonymization Model Dec. 2022
Korea Information Science Society Korea Software Comprehensive Academic Conference
Daeul Park, *Seungmin Kim*, Hyunsik Na, and Daeseon Choi

Patents and Software Copyrights.....

Patent.....

Code-Based Fast Voice Protection System and Method for Preventing Voice Cloning Attacks Jul. 2026
Application No.: 10-2026-0141478 (Korea), Pending
Seungmin Kim, Sohee Park, and Daeseon Choi

Speech Transformation Method for Defense Against Voice Cloning Attack Dec. 2025
Application No.: 19/437,589 (U.S.), Pending
Seungmin Kim and Daeseon Choi

Method and Apparatus for Classifying Generated Speech Apr. 2025
Application No.: 19/184,526 (U.S.), Pending
Seungmin Kim and Daeseon Choi

Speech Transformation Method for Synthetic Voice Attack Defense Mar. 2025
Application No.: 10-2025-0032204 (Korea), Pending
Seungmin Kim and Daeseon Choi

Generated Speech Classification Method and Apparatus Nov. 2023
Application No.: 10-2023-0151614 (Korea), Pending
Seungmin Kim and Daeseon Choi

Software Copyrights.....

Code-Based Fast Voice Protection System and Method for Preventing Voice Cloning Attacks Jul. 2026

Registration No.: 202607220009, Registered
Seungmin Kim, Sohee Park, and Daeseon Choi

Voice Reconstruction System for Defense Against AI-Based DeepVoice Generation

Nov. 2024

Registration No.: C-2024-048858, Registered
Seungmin Kim and Daeseon Choi

Research Projects

Development of Robust Real-time Deepfake Disruption Technology via Adversarial Noise Injection for Privacy Protection

Apr. 2026 – Dec. 2028

- Personal Information Protection Commission (PIPC)
- Researching proactive defense against voice cloning attacks.
- Led proposal preparation.

Development of Countermeasure Technologies for Generative AI Security Threats

Apr. 2024 – Dec. 2027

- Institute for Information & Communications Technology Planning & Evaluation (IITP)
- Researching deepfake defense technologies.
- Participated in proposal preparation.

Robust AI and Distributed Attack Detection for Edge AI Security

Apr. 2021 – Dec. 2026

- Institute for Information & Communications Technology Planning & Evaluation (IITP)
- Research on DeepVoice detection and voice deepfake security for smart speakers.
- Developed a prototype system for simulating attacks against edge AI.

Voice Modulation Service for Customer Response Data

Nov. 2023

- TimeGate (Commissioned Project)
- Performed voice modulation on customer response speech data.

Research on the Analysis of Protocols and Security Verification of Passwordless Authentication

Feb. 2023 – Nov. 2023

- Cryptography Research Group, Korea Institute of Information Security and Cryptology

Skills

Programming: Python, C, C++

Operating Systems: Windows, Linux