

강의개요

생성형 AI 기술의 이해

최근 몇 년간 생성형 인공지능(Generative AI)은 다양한 산업과 일상생활에 깊이 스며들며 혁신을 이끌고 있습니다. 생성형 AI는 텍스트, 이미지, 음악, 영상 등 인간이 만들어내던 콘텐츠를 자동으로 생성할 수 있는 기술로, 특히 트랜스포머(Transformer)와 같은 딥러닝 기술의 발전 덕분에 빠르게 성장해 왔습니다. 이 강의에서는 생성형 AI의 개념과 이를 가능하게 하는 핵심 기술을 쉽게 이해할 수 있도록 소개합니다.

본 강의의 목표는 다음과 같습니다.

- 텍스트 생성형 AI의 중심 기술인 트랜스포머(Transformer) 구조의 이해
- 챗GPT와 같은 LLM의 개념, 신경망 구성, 학습 방법을 이해
- 연구를 위한 ChatGPT 활용 사례 소개
- 이미지 생성 기술인 디퓨전 (diffusion) 모델의 원리를 소개

* 강의 난이도: 초급

* 강의: 이상근 교수 (고려대학교 정보보호학과)

Curriculum Vitae

Speaker Name: Sangkyun Lee, Ph.D.



► Personal Info

Name Sangkyun Lee
Title Associate professor
Affiliation Korea University

► Contact Information

Address 145, Anam-ro, Seongbuk-gu, Seoul, 02841, Korea
Email sangkyun@korea.ac.kr

Research interest : Trustworthy AI, Robust deep learning methods, AI for security, Data analysis.

Educational Experience

2003 B.S., Seoul National University
2005 M.S., Seoul National University
2011 Ph.D., University of Wisconsin-Madison, USA

Professional Experience

2011-2014 Post-doc Researcher, SFB 876, TU Dortmund University, Germany
2015-2017 Principal Investigator, SFB 876, TU Dortmund University, Germany
2017-2019 Assistant Professor, Department of Computer Science, Hanyang University ERICA
2020-2021 Assistant Professor, School of Cybersecurity, Korea University
2022-current Associate Professor, School of Cybersecurity, Korea University

Selected Publications (3 maximum)

1. SwiftThief: Enhancing Query Efficiency of Model Stealing by Contrastive Learning, Jeonghyun Lee, Sungmin Han, Sangkyun Lee, IJCAI, 2024
2. Libra-CAM: An Activation-Based Attribution Based on the Linear Approximation of Deep Neural Nets and Threshold Calibration, Sangkyun Lee, Sungmin Han, IJCAI, 2022
2. Model Stealing Defense against Exploiting Information Leak Through the Interpretation of Deep Neural Nets, Jeonghyun Lee, Sungmin Han, Sangkyun Lee, IJCAI, 2022