

강의개요

Introduction to Deep Learning

딥러닝은 이미지/영상 처리, 시계열 예측 등 다양한 분야에서 다량의 데이터를 기반으로 분류 등 문제를 해결하기 위한 기계학습 기법이다. 본 과정에서는 기계학습과 딥러닝의 개념적 이해를 바탕으로, 최근 많이 활용되고 있는 CNN (Convolutional Neural Network), RNN (Recurrent Neural Network)의 구조와 활용 방법에 대해 소개한다. 또한 GAN 등 생성 모델과 최근 각광받고 있는 XAI (eXplainable AI) 기술에 대해 간단히 소개한다. 본 과정은 각 기법의 개념적 이해와 직관적인 수학적 이해를 통해 수강생이 각 기법의 동작 원리와 장단점에 대해 파악할 수 있도록 하며, 또한 구글의 딥러닝 소프트웨어인 Tensorflow를 이용한 실습을 통해 딥러닝 기법 적용을 위한 기초 소양을 다지고자 한다.

강의는 다음의 내용을 포함한다:

- 기계학습 및 딥러닝의 기초
- DNN (Deep Neural Network), CNN (Convolutional Neural Network), RNN (Recurrent Neural Network) 이해
- GAN 등 생성 기법 소개
- XAI 기법 소개

*참고강의교재:

Deep learning, Goodfellow, Bengio & Courville, MIT Press, 2016

*교육생준비물:

노트북 (메모리 8GB 이상, 디스크 여유공간 30GB 이상), 구글 크롬 웹 브라우저
실습 시 구글 Colaboratory 사용 예정 (설치 필요 없음, 구글 개인 계정 생성 필수)
<https://colab.research.google.com/notebooks/welcome.ipynb>

* 강의 난이도: 초급~중급

* 강의: 이상근 교수 (고려대학교 정보보호대학원)

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
Phone Number 02-3290-4890

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 (5 maximum)

1. 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
3. Hunt for Unseen Intrusion: Multi-Head Self-Attention Neural Detector, Seongyun Seo, Sungmin Han, Janghyeon Park, Shinwoo Shim, Han-Eul Ryu, Byoungmo Cho, and Sangkyun Lee, IEEE Access, 2021
4. Fast Saddle-Point Algorithm for Generalized Dantzig Selector and FDR Control with the Ordered l_1 -Norm, Sangkyun Lee, Damian Brzyski and Malgorzata Bogdan, AISTATS, 2016

5. Co-author, Mutational dynamics between primary and relapse neuroblastomas. In *Nature Genetics*, Vol. 47, No. 8, pages 872-877, 2015.

강의 시간표

시 간	발 표 내 용	연 자
09:00-09:20(20)	등 록	
09:20-09:30(10)	공지사항 전달	
9:30-10:50(80)	Introduction to ML & DNN (이론)	이상근 교수
10:50-11:00(10)	휴 식	
11:00-12:10(70)	CNN (이론)	이상근 교수
12:10-13:40(90)	점 심	
13:40-15:10(90)	RNN, GAN, XAI (이론)	이상근 교수
15:10-15:20(10)	휴 식	
15:20-16:50(90)	AI 모델 구조 정의, 학습 알고리즘 적용, 성능 평가, 시각화 방법 (Tensorflow 실습)	이정현, 한성민 조교