곽현정 HYEONJEONG KWAK

kwakrhkr59@gmail.com (2171003@ewhain.net)
https://github.com/kwakrhkr59

학력사항

2021.3. ~ 이화여자대학교 재학

- 컴퓨터공학과 주전공
- 수학과 복수전공
- GPA: 4.25/4.3

스택

- C/C++
- Python
  - Keras
  - Tensorflow
- Java

💼 경력

2022.7. ~ 2024.2. 이화여자대학교 AISec 학부생 인턴

인공지능을 활용한 네트워크 보안 연구 진행 및 논문 작성

📚 논문

- DeepCoAST: Unveiling Split Trace Correlation to Counter Traffic Splitting Defense
  - IEEE Access* (To appear), 2024 (SCI-E)
- 딥러닝 기반 분할 데이터 상관관계 탐지를 통한 WF 방어 모델의 취약점 탐색
  - 한국정보보호학회 영남지부 학술대회 2023

📜 특허

- 토르 웹사이트 핑거프린팅 방어기법에서 추출한 분할 트래픽 대상 딥러닝 기반 상관관계 탐지 시스템 및 방법

🏆 수상내역

- 이화여자대학교 교내 프로그래밍 대회 E-PPER 22회 대상
- 2023 한국정보보호학회 영남지부 학술대회 학회장상
- 신촌 연합 대학 프로그래밍 대회 SUAPC 2023 Summer 학교 1등상

🌐 어학 능력

- TOEIC: 895 (LC 460, RC 435)

곽현정 HYEONJEONG KWAK

kwakrhkr59@gmail.com (2171003@ewhain.net)
https://github.com/kwakrhkr59

반갑습니다, 6G를 선도할 머신러닝 연구자입니다

저는 머신러닝에 매료되어 네트워크 환경에서 머신러닝을 연구하고 있는 곽현정입니다. 현재 컴퓨터공학을 심화 전공하면서 컴퓨터 공학 뿐만 아니라 과학적 이해도 함께 넓혀가고 있습니다. 동시에 수학을 복수 전공하여 머신러닝 모델을 수학적 언어로 표현하고 자유롭게 다룰 수 있는 기반을 닦아가고 있습니다.

최근에는 6G 기술에 큰 관심을 가지고 LLaMA 모델을 기반으로 SpaceX의 Starlink 네트워크 트래픽을 분석하여 사용자의 검색 기록을 추정하는 웹사이트 핑거프린팅(Website Fingerprinting) 연구를 진행 중입니다.

동아리

2024.9. ~	RCY	|	대한적십사 산하 대학생봉사단 어르신 디지털 교육 및 보이스피싱 예방 교육 진행
2024.2. ~ 2024.9.	EURON	|	이화여자대학교 인공지능 학술 동아리 최신 AI 논문 스터디 및 세미나 진행
2023.3. ~ 2023.8.	ECC	|	이화여자대학교 중앙 컴퓨터 동아리 kaggle을 기반 데이터 분석 프로젝트 진행
2021.12. ~ 2022.12.	EDOC	|	이화여자대학교 소프트웨어학부 프로그래밍 동아리
2021.3. ~ 2023.8.	EPOXI	|	이화여자대학교 농구동아리

교내·외 활동

2023.9. ~ 2023.12. 자료구조 튜터
자료구조 강의 수강생 대상 자료구조 보충 수업 및 실시간 질의 응답 진행

2022.9. ~ 2023.12. 원스탑 튜터
코딩테스트 대비 알고리즘 강의 및 튜터링 진행

2023.7. ~ 2023.8. EPITA Summer School
프랑스 단기 해외 연수. AI course 수강 및 diffusion 모델 활용 프로젝트 진행

2022.9. ~ 2022.12. OpenPose를 활용한 실시간 자세 교정 애플리케이션 Poever 개발
Node.js를 이용하여 OpenPose API를 활용한 관절 각도 계산 로직 개발

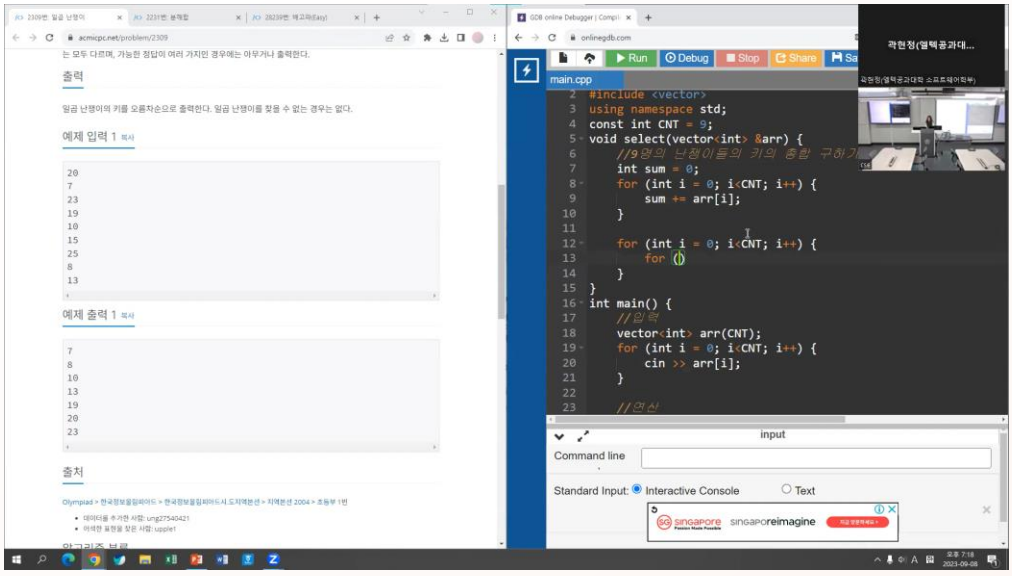
2022.9
~ 2023.12

자료구조 및 알고리즘 튜터링

2학년 1학기, 자바 프로그래밍 수업에서 성실히 프로젝트 과제와 프로그래밍 시험을 수행한 모습을 눈여겨보신 교수님의 추천으로 소프트웨어학부생을 대상으로 한 알고리즘 튜터링을 진행해왔습니다.

이 튜터링에서 저는 실시간으로 브루트포스, 정수론부터 투포인터, 이분 탐색 등 초~중급 알고리즘 수업을 진행했습니다. 또한 git을 이용해 수강생들의 과제를 관리하고, 클린 코드 가이드에 따라 코드리뷰까지 진행하였습니다.

아래 이미지를 누르면 연결된 유튜브 링크에서 제가 진행한 튜터링 수업 영상을 시청하실 수 있습니다.



2022.9
~ 2022.12

OpenPose를 활용한 실시간 자세 교정 애플리케이션 개발

OpenPose API를 활용하여 실시간 자세 교정 애플리케이션을 개발했습니다. 이 애플리케이션은 2초 간격으로 스마트폰 카메라로부터 이미지를 입력 받아 사용자 관절 위치를 분석합니다.

OpenPose의 관절 검출 기능을 통해 사용자 신체의 주요 관절 좌표를 파악하고, 그 중 3개의 관절 좌표를 선택해 arctan 함수를 적용하여 각도를 계산합니다. 계산된 관절의 각도가 가동 범위를 벗어난 경우, 구체적인 자세 교정 메시지를 출력하여 사용자에게 자세 개선을 유도합니다.
정상 각도에 대한 정의는 이대목동병원 척추센터 교수님들께 자문을 받아 결정하였습니다.

저는 이 프로젝트에서 Node.js를 이용해 API로 2초 간격으로 이미지에서 관절 좌표가 담긴 json 파일을 받아 관절 사이 각도를 계산해 정상 범위 이내인지 판별하는 로직을 구현하였습니다.
https://polar-reward-a8a.notion.site/RexT-b7af591dc70b4e4fb1123b75fff6af3d

2022.7
~ 2024.2

Network Security AI Lab 학부연구생

약 1년 반 동안의 학부연구생 기간 동안, 저는 네트워크 트래픽을 분석해 유저의 방문 기록을 추적하는 보안 공격 기법인 핑거프린팅(Fingerprinting) 공격 및 방어 기법을 연구하였습니다.

이 연구실에서 근무하면서 저는 단순히 논문을 읽고 세미나에 참석하는 수준으로 그치지 않았습니다. 직접 데이터셋을 수집, 전처리하고 여러 모델 아키텍처를 설계하며 주도적으로 연구를 진행하였고, 국내 학술대회 1편, 국외 SCIE 저널 1편, 총 2편의 논문을 작성하는 성과를 이뤄냈습니다.

지속 학습(Continual Learning) 기법을 이용한 웹사이트 핑거프린팅

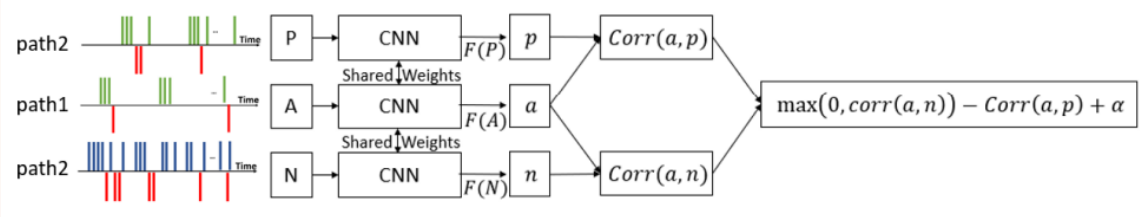
해당 연구에서는 다중 클래스 분류 작업에서 훈련 데이터 셋을 랜덤하게 고루 석지 않고, 순차적으로 학습시켰을 때 정확도가 감소하는 catastrophic forgetting 현상을 방지하기 위한 기법을 연구했습니다.

핑거프린팅 데이터셋을 순차적으로 학습시켰을 때는 최대 5%의 정확도가 나왔지만, iCaRL 모델을 이용해 다시 학습시켰을 때는 약 40%대로 정확도를 크게 향상시킬 수 있었습니다. 이를 통해 핑거프린팅 분야에서의 지속 학습 가능성을 제시했습니다.

Triplet loss를 이용한 분할 트래픽의 상관관계 분석

이 연구에서는 네트워크 트래픽을 여러 경로로 분할하여 개별 TCP/IP 패킷에서 얻을 수 있는 정보량을 줄이고, 패턴을 숨겨 핑거프린팅 공격을 방어하는 기법의 취약점을 분석했습니다.

타깃 웹사이트에서 추출되는 네트워크 패킷을 2개의 각기 다른 패킷으로 분할하고, 이들을 각각 Anchor, Positive로 설정하고, 다른 웹사이트에서 추출된 네트워크 패킷을 Negative로 설정하여 triplet loss를 계산했습니다. 이를 바탕으로 embedding vector를 만들고 모델을 학습시켜, 최종적으로 cosine similarity를 이용해 패킷 간 pairwise 상관관계를 계산하여 top k를 선정하였습니다.



이로써 학습된 Triplet model로부터 최종 0.98에 이르는 AUC 결과를 얻었습니다.

이 연구를 바탕으로 총 2편의 논문을 작성하여 2023년 한국정보보호학회(KIISC) 영남지부 학술대회에서 학회장상을 수여하였고, 최근 IEEE Access에 논문 publishing 승인을 받았습니다.