캡스톤디자인 I 계획서

<table>
<tr><td rowspan="2">제 목</td><td>국문</td><td colspan="4">위조 얼굴 탐지를 위한 모델 개발</td></tr>
<tr><td>영문</td><td colspan="4">Developing A Model For Face Anti-Spoofing</td></tr>
<tr><td>프로젝트 목표
(500자
내외)</td><td colspan="5">해당 프로젝트에서는 위조 얼굴을 탐지하는 딥러닝 기반 모델을 연구한다. 기존 위조 얼굴 탐지 기법들과 우리가 제안하는 위조 얼굴 탐지 모델의 성능을 비교, 분석한다. 경량화한 위조 얼굴 탐지 모델을 어플리케이션에 탑재하여 실생활에 적용할 수 있도록 한다.
[논문 투고]
SCI급 1편, KCC(컴퓨터 종합 학술대회) 수상을 목표로 한다.</td></tr>
<tr><td>프로젝트
내용</td><td colspan="5">얼굴 인식 기술은 우리가 매일 같이 사용하는 기술 중 하나이다. 기술이 널리 쓰이고 있는 만큼 보안을 위협하는 얼굴 위변조 시도 또한 다양해지고, 많은 기업과 연구소에서 위조 얼굴 탐지에 대한 연구가 활발히 진행되고 있다. 위조 얼굴 탐지는 얼굴 인식 시스템을 위협하는 다양한 공격 행위를 얼마나 잘 탐지하는지, 정상 사용자를 위조 얼굴로 오분류 하지 않는지를 평가한다.
위조 얼굴 탐지는 데이터 내의 조명, 배경과 같은 환경 요소들이 모델 성능에 큰 영향을 미친다. 모델이 훈련에 사용된 도메인 외에 새로운 도메인에서도 잘 작동하도록 하는 도메인 일반화(Domain Generalization)를 통해 강인한 모델을 만들고자 한다.
딥러닝 모델은 연산량이 많아 일상적인 어플리케이션에 직접 적용하기 어렵다. 이에, 모델을 경량화하여 실제 어플리케이션에서도 효율적으로 사용할 수 있도록 하고자 한다.
우리는 얼굴 인식 기반 본인인증 시스템들이 널리 사용되며 시스템의 보안을 위협하는 공격들에 강력하게 대응 가능한 모델을 만들고자 한다.</td></tr>
<tr><td>중심어(국문)</td><td colspan="2">딥러닝</td><td>위조 얼굴 탐지</td><td>인공지능</td><td>미세 신호 탐지</td></tr>
<tr><td>Keywords
(english)</td><td colspan="2">Deep Learning</td><td>Face
Anti-Spoofing</td><td>Artificial
intelligence</td><td>Micro-signal
detection</td></tr>
<tr><td>멘토</td><td>소
속</td><td colspan="2">㈜알체라</td><td>이름</td><td>이건우</td></tr>
<tr><td rowspan="5">팀
구성원</td><td>학년
/반</td><td>·학 번</td><td>이 름</td><td colspan="2">연락처(전화번호/이메일)</td></tr>
<tr><td>4</td><td>20191766</td><td>김동수</td><td colspan="2">010-9067-5828 / 20191766@edu.hanbat.ac.kr</td></tr>
<tr><td>4</td><td>20211915</td><td>오서연</td><td colspan="2">010-2953-7418 / 20211915@edu.hanbat.ac.kr</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="6">컴퓨터공학과의 캡스톤디자인 관리규정과 모든 지시사항을 준수하면서 본 캡스톤디자인을 성실히 수행하고자 아래와 같이 계획서를 제출합니다.
2024 년 3월 7일
책 임 자 : 김동수 (인)
희망 지도교수 : 장한얼</td></tr>
</table>

1. 캡스톤디자인의 배경 및 필요성

스마트폰 잠금해제, 모바일 결제 등 사용자 인증 및 모니터링 목적으로 폭넓게 쓰이는 얼굴 인식 기술은 일상생활에서 자주 사용하는 활용도가 높은 기술 중 하나이다. 기술이 널리 쓰이고 있는 만큼, 보안을 위협하는 얼굴 위변조 시도가 다양해지고 있다. 타인 사칭이나 신분 위장을 목적으로 고품질의 사진, 영상, 사람을 모방한 실리콘 마스크 등을 활용하게 교묘하게 시스템의 감시를 피하는 행위들이 나타난다. 특히, 사용자 인증 시 사용하는 비접촉식 얼굴 인식 기술은 위변조로 된 얼굴 데이터로 시스템을 속이는 스푸핑 공격에 취약하다. 위변조된 얼굴 데이터를 사용하여 인식 시스템을 속이는 스푸핑 공격을 방지하고, 사용자 인증 시스템이 스푸핑 시도에 대해 인증을 허용해 발생하는 피해를 최소화할 필요가 있다.

위조 얼굴 탐지는 데이터 특성상 내의 조명, 배경과 같은 환경 요소들이 모델 성능에 큰 영향을 미친다. 최근에는 다양한 센서의 개발 및 기술들의 결합으로 촬영된 기기에 따라서도 얼굴 이미지의 특징 차이가 발생한다. 데이터셋의 특성 차이로 인해 성능 하락이 발생하는 문제를 해결하기 위해 도메인 일반화(Domain Generallization)에 대한 연구가 진행되고 있다.[1][2]

우리는 위조 얼굴 탐지에서 발생할 수 있는 도메인 일반화 문제를 해결하고 위조 공격에 대응할 수 있는 딥러닝 모델을 개발할 예정이다. 또한, 개발 모델을 일상생활에서 사용할 수 있도록 경량화 후 어플리케이션을 제작하는 것이 목표이다.

2. 캡스톤디자인 목표 및 비전

스마트폰 잠금 해제, 모바일 결제 등 실생활에서 폭넓게 사용되는 얼굴인식 과정에서 발생 가능한 위변조 공격에 대응하는 모델을 개발한다. 실제 어플리케이션에서도 적용하기 위해 모델을 경량화하여 적은 연산자원으로도 위변조 얼굴 탐지를 가능하도록 한다.

3. 캡스톤디자인 내용

주요기능

	내용
데이터 분석	- opencv-python 라이브러리를 활용하여 데이터 시각화 및 전처리 - pytorch transforms, MTCNN[3] 알고리즘 등을 활용하여 데이터 전처리
특징 추출 모델	- pytorch 기반의 CNN, ViT 계열모델 사용[4][5] - 다양한 촬영환경에 대해 강인하도록 추가 데이터셋을 구축하여 Fine-tuning
위조 얼굴 탐지 어플리케이션	- 학습된 모델을 적용한 어플리케이션을 제작하여 실제 위조 얼굴 탐지 수행을 진행할 수 있도록 함

비기능적 요구사항

	내용
성능	- 적은 연산자원을 사용해도 다양한 촬영 환경에서 사용 가능한 모델을 개발
유지보수성	- 널리 사용되는 모델의 구조를 사용하여 모델 학습을 진행해 제3자가 본 프로젝트에서 학습된 모델을 쉽게 불러와 사용이 가능
결과	- 경량화된 위조 얼굴 탐지 모델을 이용해 적은 하드웨어 자원으로 사용 가능한 위조 얼굴 탐지 모델 개발 - 연구 결과를 토대로 논문 작성

4. 캡스톤디자인 추진전략 및 방법

인공지능 학습용 데이터, 소프트웨어 등의 구축 및 배포를 플랫폼인 AI Hub에 공개되어 있는 'Liveness Detection을 위한 영상' 데이터셋은 2,000명에 해당하는 사람에 대해 Real, Fake데이터를 생성해 훈련 데이터 약 1,000,000장, 검증 및 테스트 데이터 200,000장으로 구성된 대용량 데이터셋이다. 해당 데이터셋을 이용하여 모델을 사전학습(Pretrain) 시킨 뒤 추가적인 얼굴 이미지 데이터셋을 구축하여 미세조정(Fine-tune)을 진행한다.

설명된 학습 과정을 진행하면서 크게 두 가지 문제가 발생할 수 있다.

1. 이미지마다 다른 촬영 환경(조명, 배경, 각도)으로 인한 모델 성능 하락

2. 주로 얼굴인식 기술을 사용하는 환경의 연산 자원은 제한되어 있음

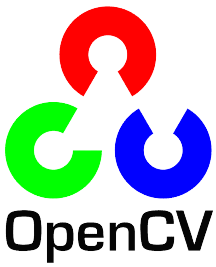
2024 CVPR Face Anti-Spoofing Challenge 참여 및 '인공지능' 과목 수강 중 진행한 텀프로젝트(위조얼굴탐지) 등의 참여를 통해 FAS모델 성능 개선 및 경량화에 대한 이해가 있으며, 이를 토대로 본 프로젝트의 목표인 FAS 모델 성능 개선 및 경량화를 달성할 수 있다.

프로젝트 멘토로는 얼굴, 영상인식 Visual AI 분야에 대한 서비스를 제공하는 회사인 알체라의 이건우 연구원을 멘토로 섭외하였다.

프로젝트와 관련된 코드는 깃허브 https://github.com/berandaNuguri(김동수) 및 https://github.com/stella08312(오서연)에 업로드한다.

	팀 구성	성명	주 역할
1	팀장	김동수	논문 및 자료조사, 모델 코드 작성, 데이터셋 구축
2	팀원	오서연	논문 및 자료조사, 모델 코드 작성, 데이터셋 구축

사용 프레임워크



5. 참고문헌

[1] Yuchen Liu, Yabo Chen, Mengran Gou, Chun-Ting Huang, Yaoming Wang, Wenrui Dai, Hongkai Xiong; Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 2023, pp. 20654-20664

[2] Chen-Hao Liao, Wen-Cheng Chen, Hsuan-Tung Liu, Yi-Ren Yeh, Min-Chun Hu, Chu-Song Chen; Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2023, pp. 6098-6107

[3] Zhang, Kaipeng, et al. "Joint face detection and alignment using multitask cascaded convolutional networks." IEEE signal processing letters 23.10 (2016): 1499-1503.

[4] Chen-Hao Liao, Wen-Cheng Chen, Hsuan-Tung Liu, Yi-Ren Yeh, Min-Chun Hu, Chu-Song Chen; Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2023, pp. 6098-6107

[5] Chien-Yi Wang, Yu-Ding Lu, Shang-Ta Yang, Shang-Hong Lai; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2022, pp. 20281-20290