캡스톤 디자인 I 최종결과 보고서

프로젝트 제목(국문): 위조 얼굴 탐지를 위한 모델 개발
프로젝트 제목(영문): Developing models for Face Anti-spoofing

프로젝트 팀(원): 학번: 20191766 이름: 김동수
프로젝트 팀(원): 학번: 20211915 이름: 오서연

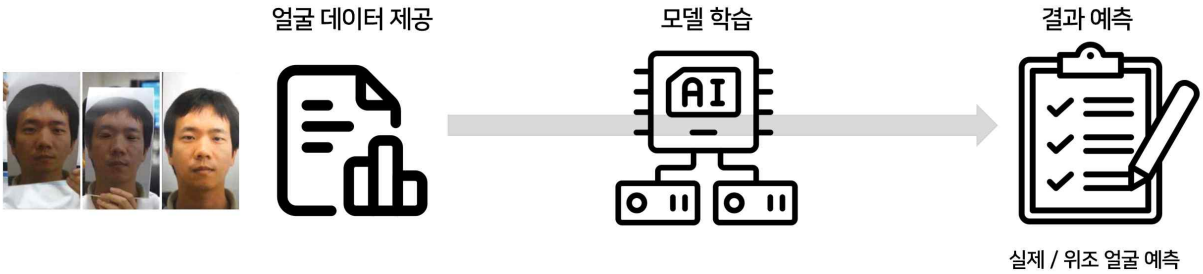
1. 중간보고서의 검토결과 심사위원의 '수정 및 개선 의견'과 그러한 검토의견을 반영하여 개선한 부분을 명시하시오.
없음.

2. 기능, 성능 및 품질 요구사항을 충족하기 위해 본 개발 프로젝트에서 적용한 주요 알고리즘, 설계방법 등을 기술하시오.

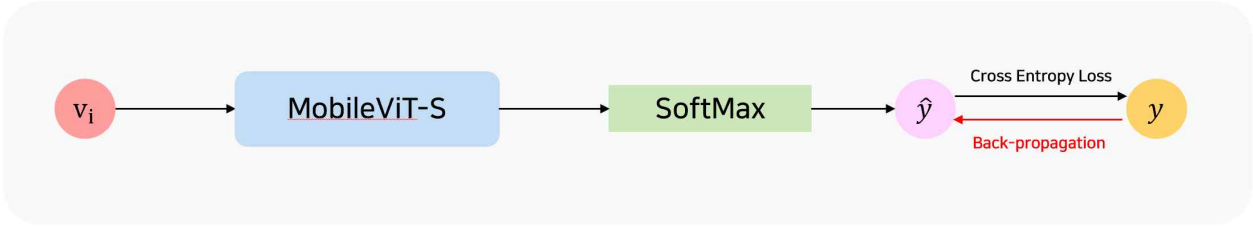
2-1) Face Anti-Spoofing 모델의 기본 구조로 MobileViT-S를 활용하였다. MobileViT-S는 경량화된 비전 트랜스포머 모델로, 모바일 및 임베디드 장치에 적합한 고효율 모델이다.
2-2) Baseline 모델의 성능을 향상시키기 위해 Supervised Contrastive Learning(SupCon) Loss를 적용하였다. SupCon Loss는 같은 클래스에 속한 샘플들 간의 거리를 최소화하고, 다른 클래스에 속한 샘플들 간의 거리를 최대화하는 방식으로 학습을 진행한다. 이를 통해 모델이 더욱 강인한 특징 표현을 학습할 수 있다.
2-3) 모델 최적화를 위해 Sharpness-Aware Minimization(SAM) Optimizer를 사용하였다. SAM Optimizer는 손실 함수의 민감도를 고려하여 매개변수 업데이트를 수행한다. 이는 일반화 성능을 향상시키고, 모델이 더욱 평탄한 loss-landspace에 수렴하도록 유도한다.
2-4) 모델의 특징 추출 능력을 강화하기 위해 Convolutional Layer의 Stride를 1로 설정하였다. Stride를 1로 설정함으로써, 더 세밀한 특징 정보를 유지할 수 있으며, 이는 Face Anti-Spoofing 성능 향상에 기여한다.
2-5) 데이터 증강(Data Augmentation) 기법을 적용하여 모델의 일반화 능력을 향상시켰다. 회전, 크기 조절, 밝기 변화 등 다양한 변환을 통해 학습 데이터의 다양성을 높였으며, 이는 모델이 다양한 환경에서도 강인한 성능을 발휘할 수 있도록 돕는다.

위와 같은 방법들을 단계적으로 적용하여 Face Anti-Spoofing 모델의 성능을 향상시켰다. Baseline 모델인 MobileViT-S에 SupCon Loss, SAM Optimizer, Stride 1, 그리고 Data Augmentation을 순차적으로 적용하며 실험을 진행하였다. 이를 통해 각 기법이 모델의 성능에 미치는 영향을 분석하고, 최적의 조합을 찾아내었다.

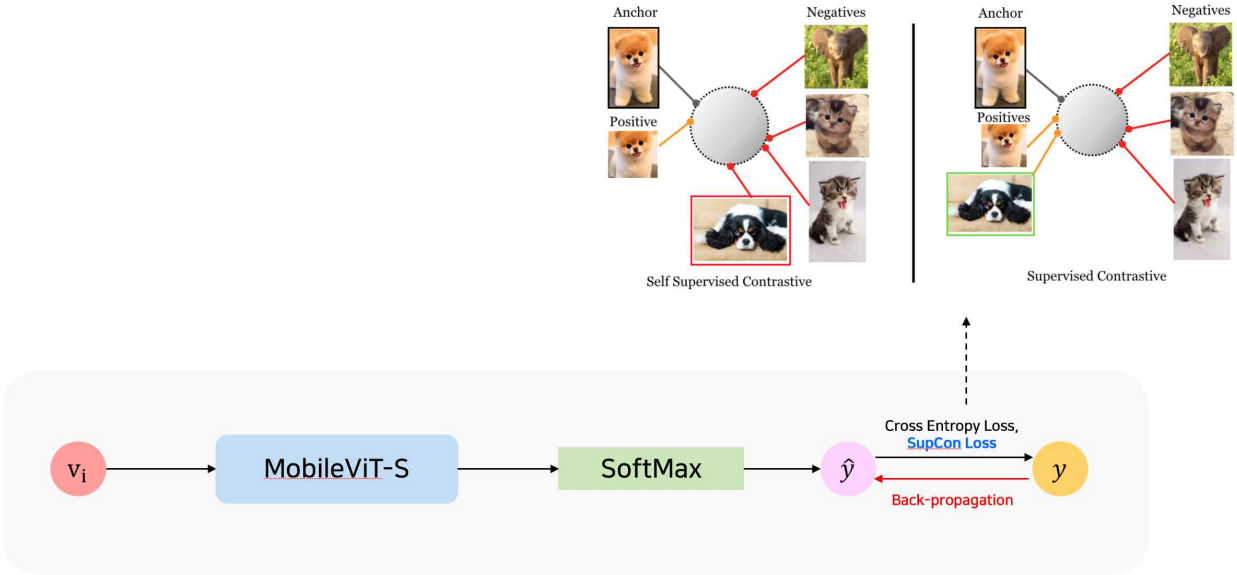
3. 요구사항 정의서에 명세된 기능 및 품질 요구사항에 대하여 최종 완료된 결과를 기술하시오.
3-1) 전체 프로세스



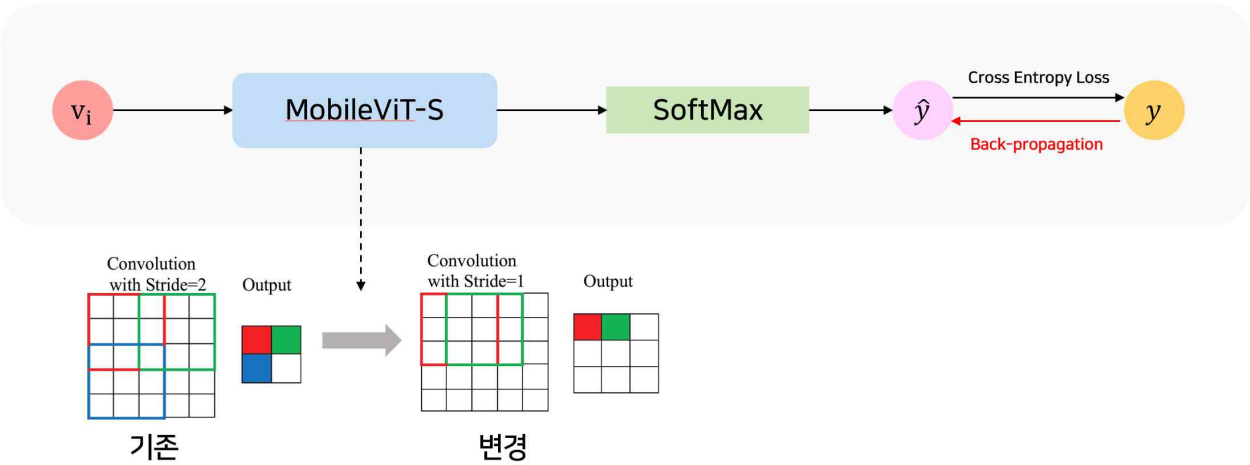
3-2) 베이스라인 모델 구조



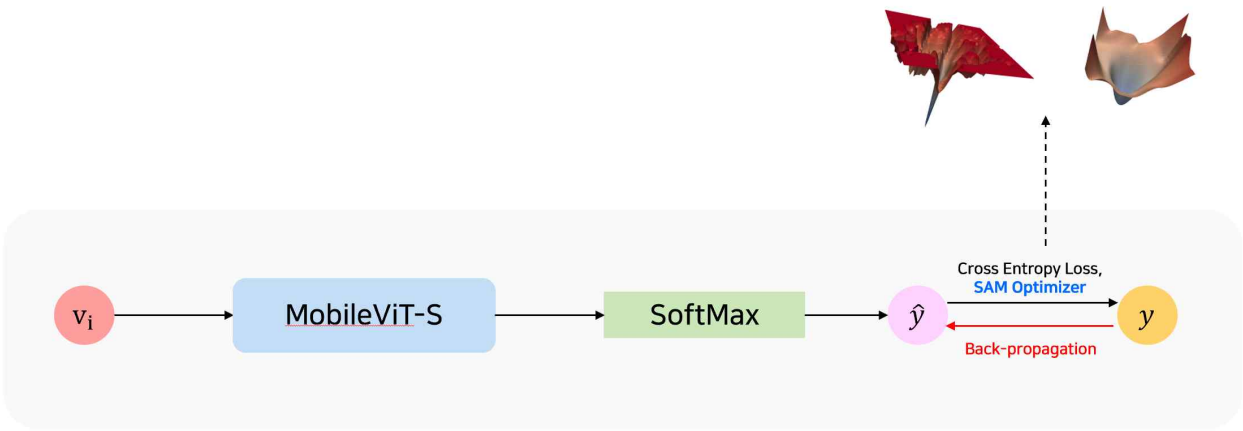
3-3) SupCon Loss 모델 구조



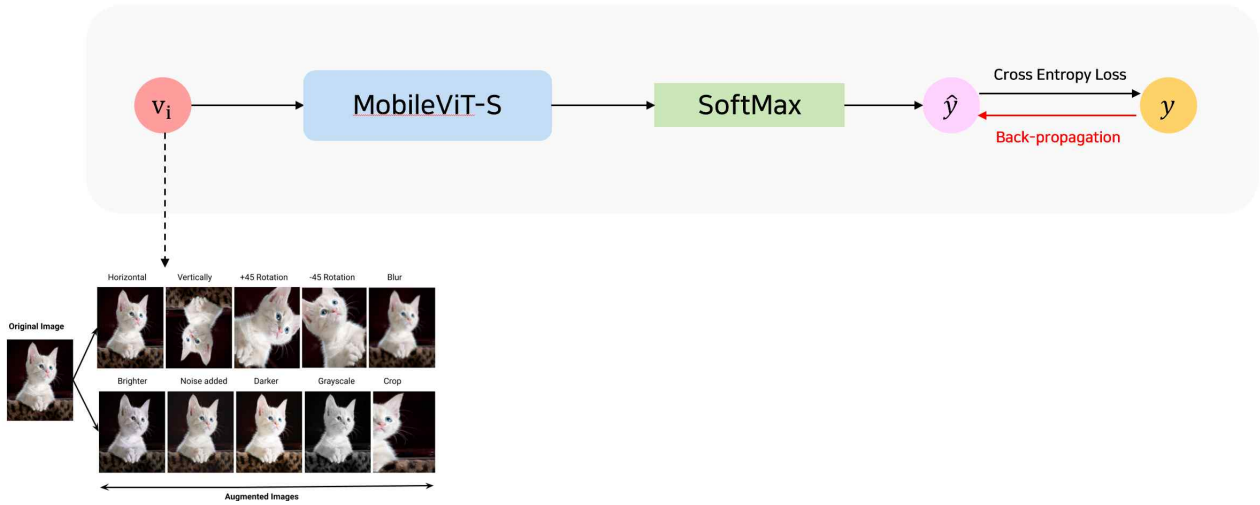
3-4) Stride 1 모델 구조



3-5) SAM 모델 구조



3-6) Data Augmentation 모델 구조



4. 구현하지 못한 기능 요구사항이 있다면 그 이유와 해결방안을 기술하시오,

최초 요구사항	구현 여부(미구현, 수정, 삭제 등)	이유(일정부족, 프로젝트 관리미비, 팀원변동, 기술적 문제 등)
		해당사항 없음

5. 요구사항을 충족시키지 못한 성능, 품질 요구사항이 있다면 그 이유와 해결방안을 기술하시오.

분류(성능, 속도 등) 및 최초 요구사항	충족 여부(현재 측정결과 제시)	이유(일정부족, 프로젝트 관리미비, 팀원변동, 기술적 문제 등)
		해당사항 없음

6. 최종 완성된 프로젝트 결과물(소프트웨어, 하드웨어 등)을 설치하여 사용하기 위한 사용자 매뉴얼을 작성하시오.

학습 환경

Ubuntu 20.04.4 LTS
Python 3.8.16
CUDA 11.8
GPU : NVIDIA A6000 48G x 2
CPU : AMD EPYC 7642 48-Core Processor
Memory : 40G

학습 사용 데이터셋

SiW-Mv2(https://cvlab.cse.msu.edu/siw-mv2-dataset.html) 벤치마크 데이터셋 이용
Leave-one-out Test 진행 - 데이터셋의 AttackType 중 하나를 Test 데이터, 이외의 AttatckType을 학습 데이터로 사용하는 Test 기법

모델 학습 및 추론 방법(스크립트 사용)

스크립트 사용 시 기본적으로는 모든 AttackType에 대한 학습 스크립트가 작성되어있음
필요에 따라 원하는 AttackType에 대해서만 학습 및 추론하도록 수정 가능
1. git clone https://github.com/HBNU-SWUNIV/come-capstone24-botduo.git
2. pip install requirements.txt
3. sh scripts/train1.sh
4. sh scripts/train2.sh
4. 실행 시 학습 및 추론을 동시 진행하여 성능평가를 진행함
4. 학습이 완료되면 기본설정으로 ./ckpt/Capstone_Design_to_{Test 진행 AttackType}/ 폴더에 iteration 별 학습모델(iter_{n}.pth.tar)과, 최고성능 모델(model_best.pth.tar)을 저장함

모델 학습 및 추론 방법(스크립트 미사용)

2. git clone https://github.com/HBNU-SWUNIV/come-capstone24-botduo.git
2. pip install requirements.txt
3. python train.py --max_iter 100 —test_attack_type {Test를 원하는 AttackType} --save_model
4. 실행 시 학습 및 추론을 동시 진행하여 성능평가를 진행함
4. 학습이 완료되면 기본설정으로 ./ckpt/Capstone_Design_to_{Test 진행 AttackType}/ 폴더에 iteration 별 학습모델(iter_{n}.pth.tar)과, 최고성능 모델(model_best.pth.tar)을 저장함

학습 세팅

Backbone: MobileViT_S
Iteration: 100
BatchSize: 데이터로더 당 8
LearningRate: 1e-4(0.0001)
Optimizer: AdamW(weight decay = 1e-6)

7. 캡스톤디자인 결과의 활용방안

외부 지식을 활용하는 Face Anti-Spoofing 모델은 얼굴 인식 기술이 널리 사용되는 환경에서 사용자 인증의 정확성과 보안성을 크게 향상시킬 수 있다. 특히 금융 기관, 국가 중요 시설 출입 등 다양한 분야에서 활용 가치가 높아지고 있으며, 사람들의 일상 생활에서 접하는 보안 및 인증 상황에서 중요한 역할을 할 것으로 기대된다. 개인 사용자 측면에서도 Face Anti-Spoofing 모델의 중요성이 커지고 있다. 모바일 기기의 얼굴 인식 잠금 해제 기능에 이 모델을 적용하면 스푸핑 공격으로부터 사용자의 개인정보를 보다 안전하게 보호할 수 있다. 이는 사용자가 자신의 기기를 안심하고 사용할 수 있게 해주며, 개인정보 유출의 위험을 최소화한다.

본 프로젝트에서 제안하는 Face Anti-Spoofing 모델로 소비자들은 보안성이 한층 강화된 얼굴 인식 시스템을 통해 제품이나 서비스를 이용할 수 있게 되며, 기업들은 모델을 활용하여 고객 인증 과정의 정확도를 높이고 사기 및 부정 사용을 효과적으로 예방할 수 있다. 이는 일상생활을 보다 안전하고 편리하게 만드는 동시에 새로운 산업 기회를 창출하는 기반이 될 수 있다.