작 품 명

팀　　명: 봇듀오

지도교수: 장한얼

참여학생: 김동수, 오서연

작품 개요

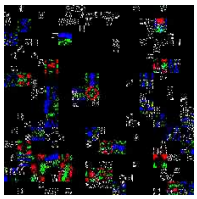
- 데이터에 비밀리에 삽입된 악성 데이터(스테고)로 보안 문제 발생 가능
- 스테고 이미지를 탐지하는 스테그어날리시스 모델의 성능을 개선하여 악성 데이터를 탐지하고자함

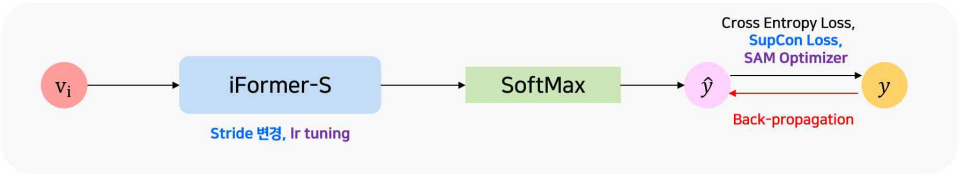
최종 목표

- 학습에 사용된 도메인뿐만 아니라, 사용되지 않은 도메인에서도 성능을 측정하여 실제 환경에서의 성능 개선을 도모

작품의 구성

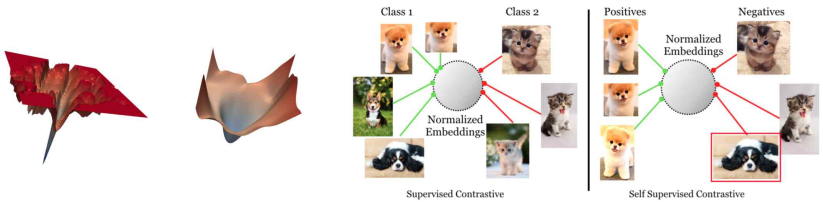
[데이터 예시 및 모델 개요]

커버 (원본)	스테고 (비밀 메시지 삽입)	잔차 (메세지 위치)
		



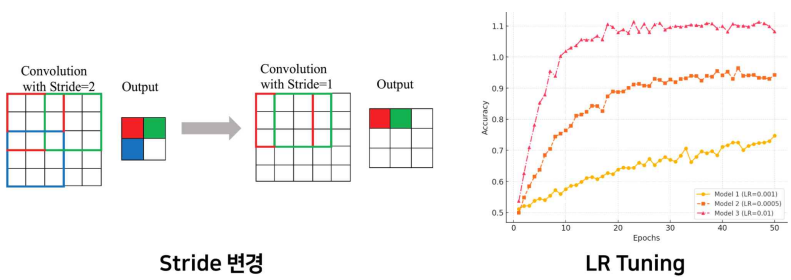
기대효과 및 활용방안

- 데이터에 삽입되어 있는 스테고 정보를 효과적으로 탐지하여 악성 코드, 해킹 등의 보안 문제를 해결할 수 있음
- 학습에 사용하지 않은 도메인에 대한 성능 개선을 통해 학습에 사용한 환경뿐만 아니라 다른 촬영 환경에서도 스테고 정보를 효과적으로 탐지할 수 있음



SAM Optimizer **SupCon Loss**

[SAM Optimizer과 Supcon Loss를 활용한 학습]



Stride 변경 **LR Tuning**

[Stride 변경과 LR tuning을 활용한 학습]