2021 SW CAPSTONE DESIGN
| 빅데이터 캡스톤디자인

팀　　명 : 5인이상집합금지
지도교수 : 임성훈

Deepfake Spear and Shield

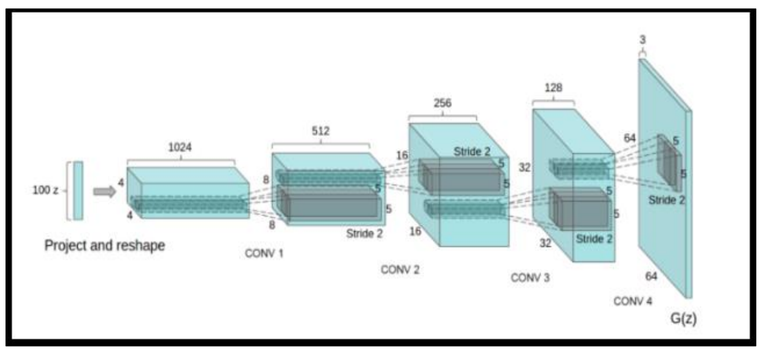
과제목적

현재 AI(인공지능)는 기술이 발전하고 대중화 되면서 인공지능을 기반으로 딥페이크(deepfake)라는 사람 얼굴 이미지 합성 기술이 발달하고 있다. 이는 초상권 보호를 위해 사용될 수도 있지만, 악의적인 사용을 하는 경우가 비일비재하다. 본 프로젝트에서는 2가지의 모델을 제시하며, deepfake를 더욱 실제 이미지 같이 만드는 네트워크의 발전을 하는 것과 동시에 deepfake의 악의적인 사용을 사전에 차단하며 초상권을 보호하는 시스템을 구성하는 것이 주 목적이다.

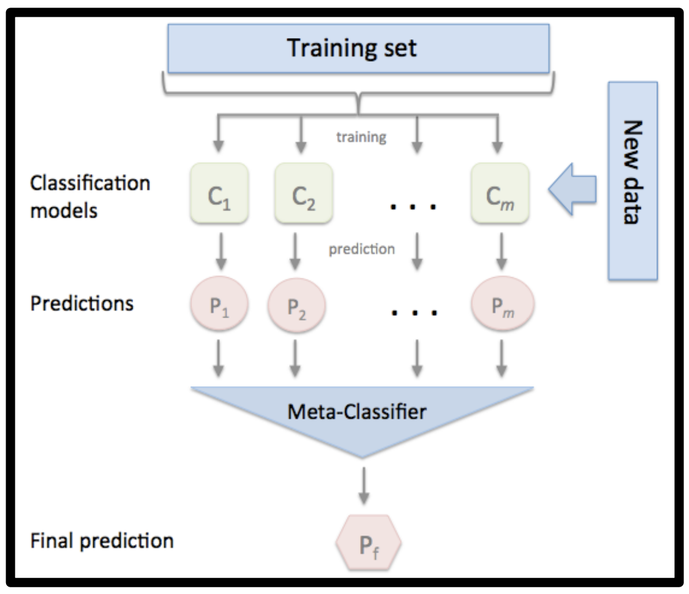
과제내용

– Team A
- 생성적 적대 신경망(GAN)기술을 사용하여 가짜이미지 생성
- 본 프로젝트는 실제이미지를 학습하여 noise를 이용해 deepfake이미지를 만드는 기술을 제안한다.
- Generator로 가짜 개체 생성. 학습된 Discriminator에 가짜 이미지 학습시켜 Generator에 업데이트

– Team B
- CNN(convolutional neural network)을 사용하여 실제이미지와 가짜 이미지 판별
- 여러 개의 사전 학습 모델을 사용하여 정확도가 높은 판별기 생성
- 훈련을 통해 얻은 모델들을 이용해 앙상블(Ensemble)을 하여 성능을 향상시킨다.



TeamA



TeamB

활용방안 및 기대효과

프로젝트에서는 앞으로 발전해 나아가는 인공지능 분야 중 Deepfake의 발전된 데이터 생성을 이루었다. 또 제안하는 두 모델의 적대적인 경쟁을 통해 Deepfake를 악용하는 범죄를 예방하고, 초상권 침해의 문제를 개선할 것으로 기대된다.
더 나아가 TeamB에서 개발된 기술을 사용해 실시간으로 가짜 이미지를 판별하고 범죄에 사용되는 가짜 이미지를 TeamA에서 만든 가짜 이미지로 대체하여 익명성을 보장할 수 있게 된다.