캡스톤 디자인II
‘딥페이크 탐지’
중간발표

김지수, 김민지, 민지민

지난 캡스톤 회의 내용

데이터 로드 과정에서 이미지의 경로와 label을 txt 파일에 저장한 후 txt 파일에서 경로를 읽어와 real/fake를 판단함.

커리큘럼 러닝을 적용하려면, 이미지 저장없이 epoch마다 학습하는 방식임.

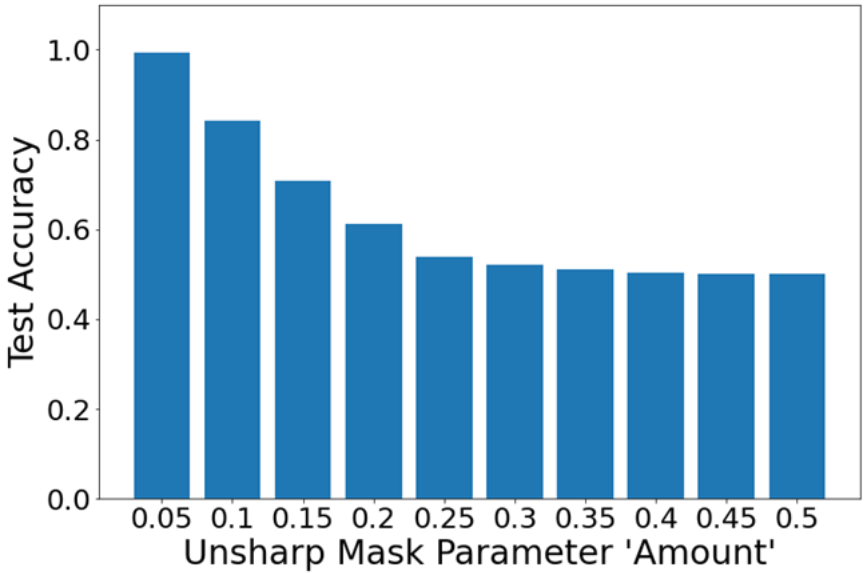
=> 따라서 커리큘럼 러닝을 하려면 코드를 다시 짜야할 듯

모든 공격의 parameter 설정 후 모델을 생성하여 inference 진행함

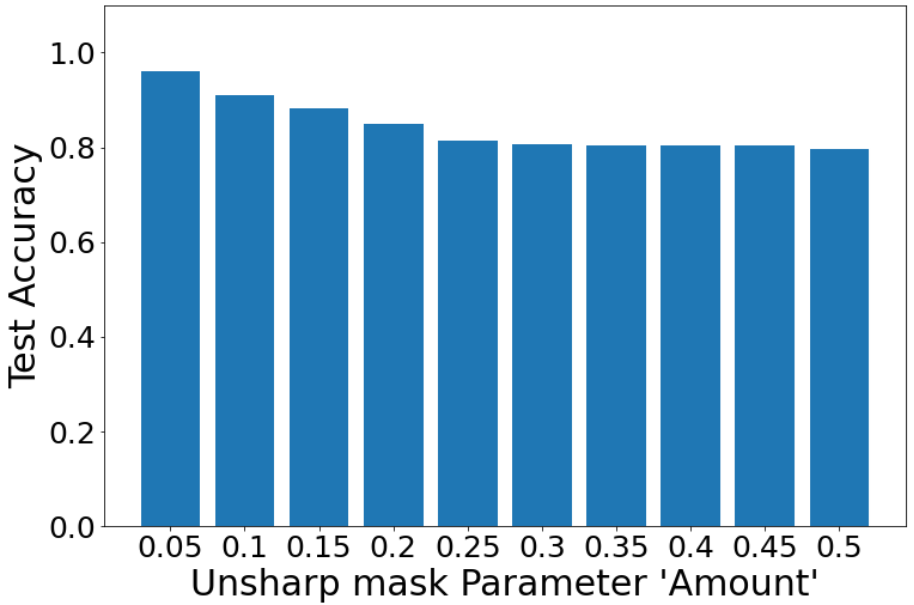
```
gaussian/medium/real/test/image_00002_real_4484.jpg 0
gaussian/medium/real/test/image_00001_real_4489.jpg 0
gaussian/medium/fake/test/image_00001_dffs_3580.jpg 1
gaussian/medium/fake/test/image_00001_dffs_3572.jpg 1
gaussian/medium/fake/test/image_00001_dffs_3581.jpg 1
```

unsharp

<이전 모델>

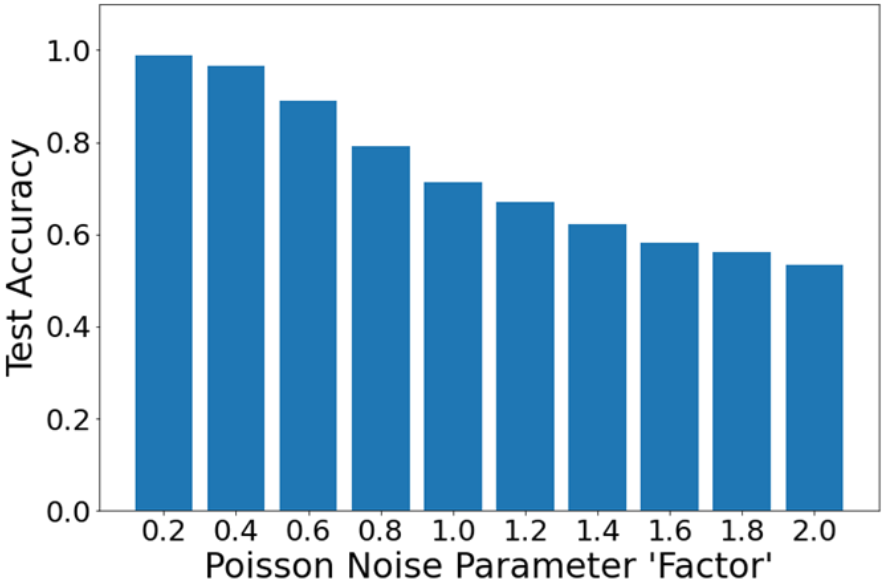


<new 모델>

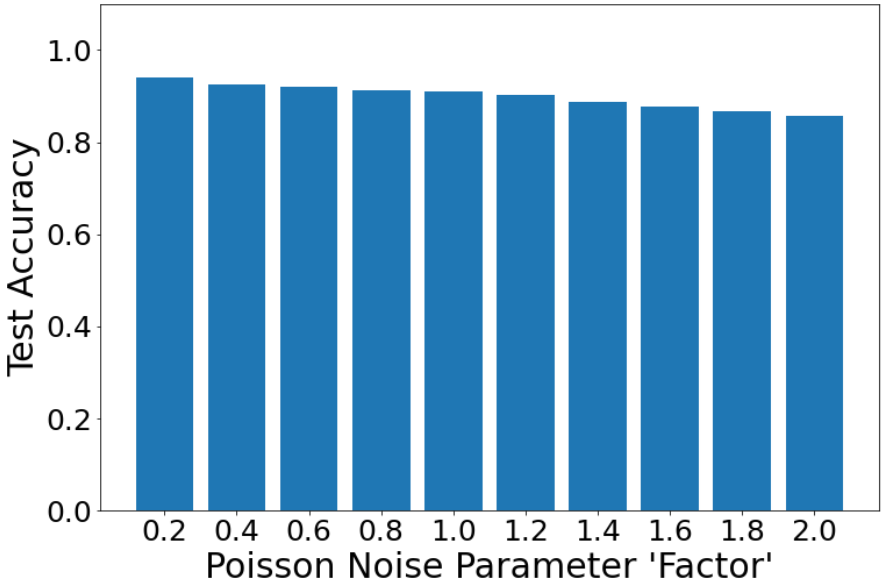


poisson

<이전 모델>

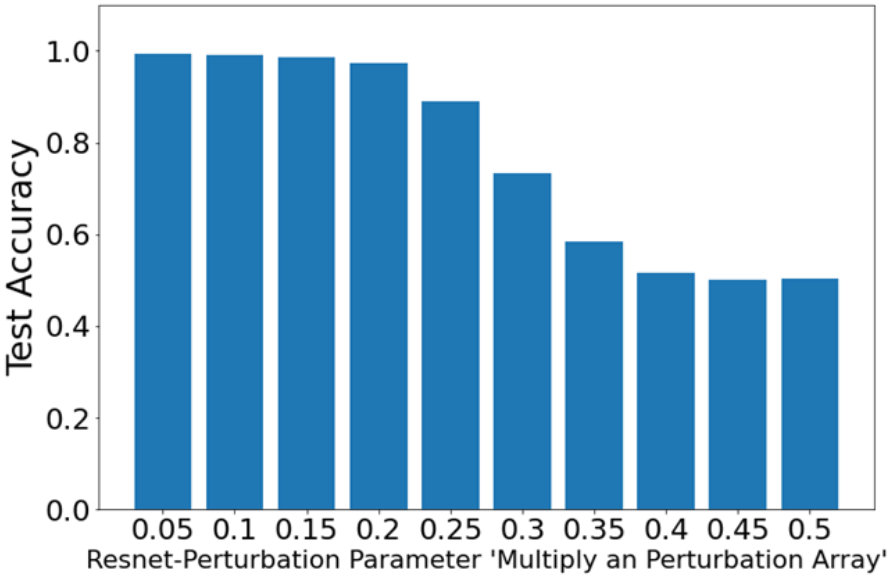


<new 모델>

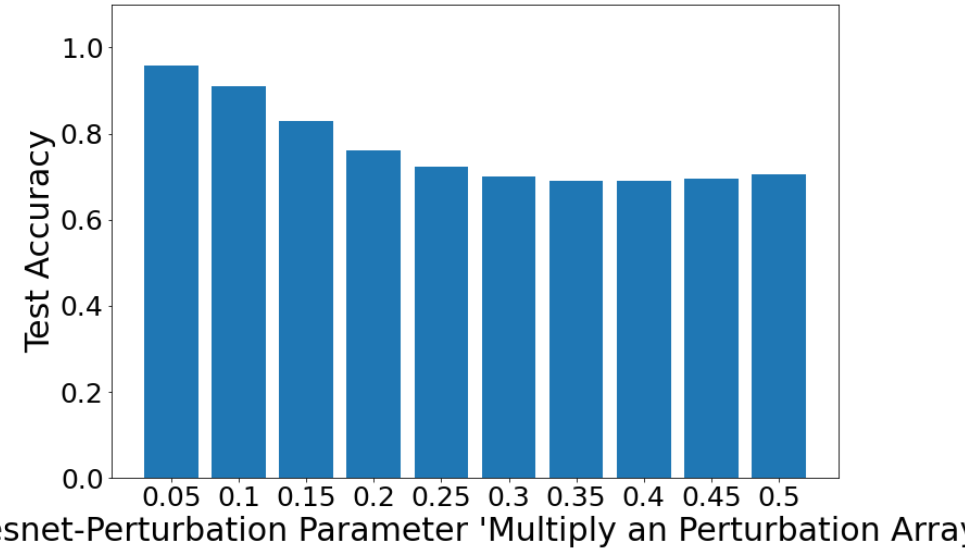


resnet perturbation

<이전 모델>

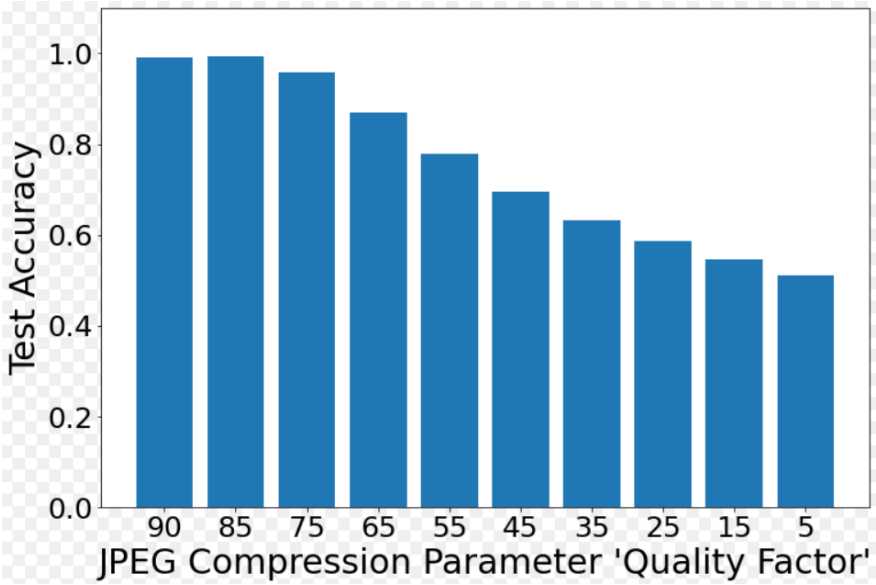


<new 모델>

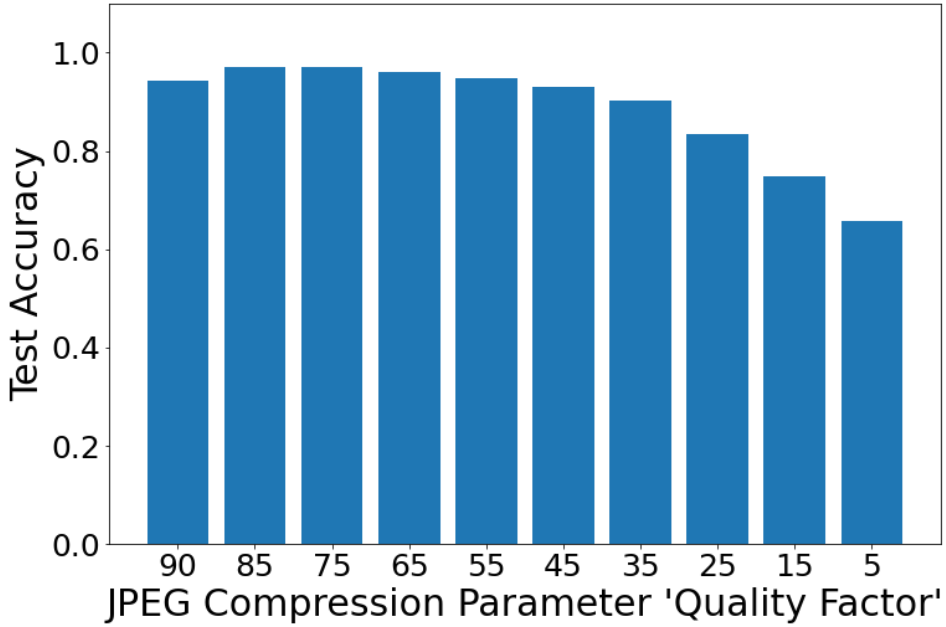


jpeg compression

<이전 모델>

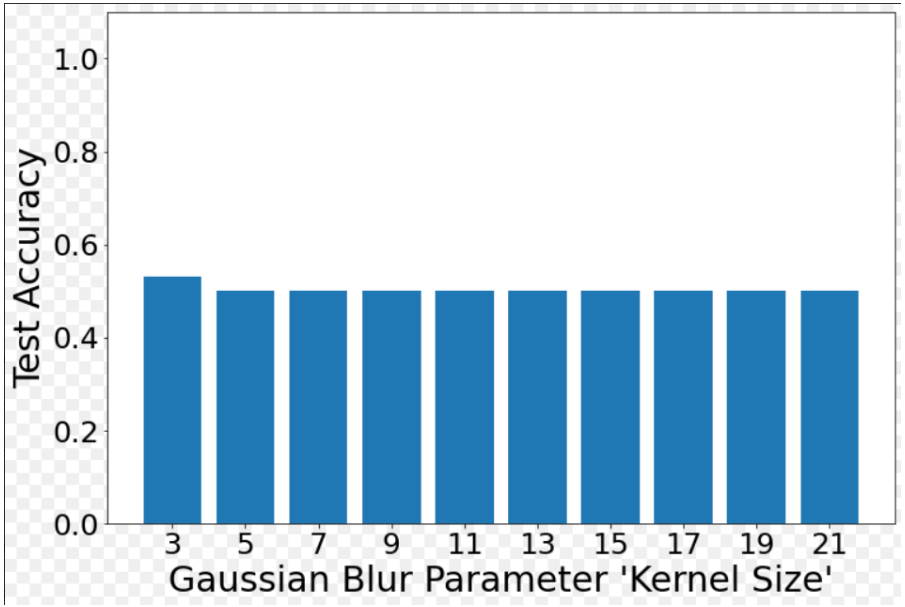


<new 모델>



gaussian blur

<이전 모델>



<new 모델>