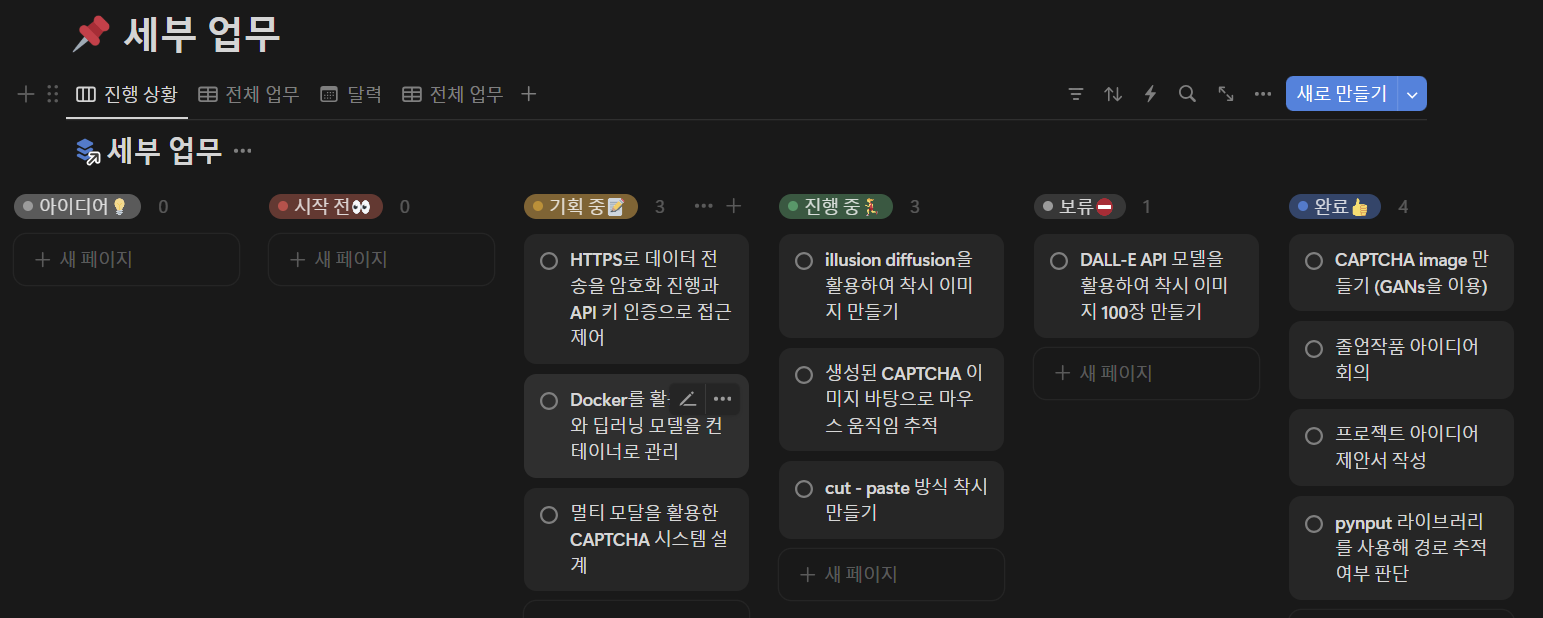
**<2차 프로그램 진행 일시 및 진행 사항 Report>**

**1분반(AI)\_[강승민,강지원,김유현]**

**<2차 프로그램 진행 일시 및 진행 사항>**

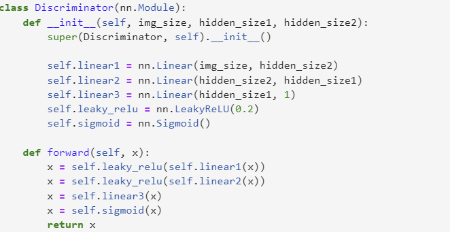
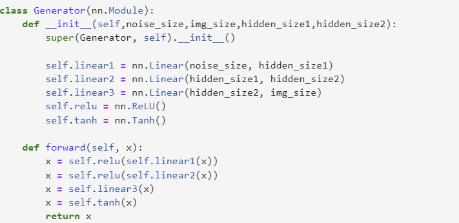


목표 : 우선적으로 시각 CAPTCHA, 행동 CAPTCHA 여러 논문에 나와 있는 방법론들을 Test를 한 다음 관련하여 사용할 수 있는 CAPTCHA Task를 생각한다.

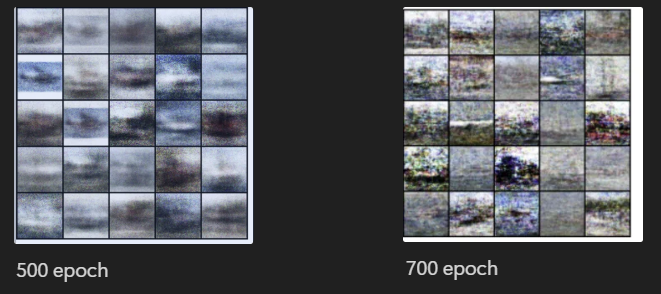
* 1차 Report 주요 논문 혹은 Methodology 내용
  + 시각 CAPTCHA
    - GANs , DCGAN, Distance – DCGAN, Composite – DCGAN
    - Stable Diffusion model
  + 행동 CAPTCHA
    - 웹 페이지를 이용하여 이미지를 로드하고 마우스 Detect을 하여 백엔드 서버로 데이터를 전송을 한 다음, 마우스 데이터 확보
  + CAPTCHA Tasks, Problem Setting
    - 이미지를 제시하여 어떠한 Image인 지 맞추는 것
    - 이미지를 제시하여 어떠한 Image를 추론할 수 있는 지 서술
    - 마우스 이동을 통해 이미지를 그려 몇 퍼센트 안에 그릴 수 있는 지 Check

 ex) Toss Bank 동그라미 그리기 Challenge

1. **시스템 설계 – CAPTCHA 구성 요소 설계**
2. **시각 기반 CAPTCHA**
   1. **목표 : CAPTCHA image를 수정하거나, 새롭게 만들어 Human은 인지할 수 있게, Computer는 인지하지 못하게 만든다.**
   2. **실행 방법**
      1. CAPTCHA image 훈련데이터로 사용을 하여 Synthesize 데이터를 만든다.
         1. **GANs**
            1. MLP 신경망을 거쳐 Generator는 생성을 하고, Discriminator는 Generator가 생성한 Image에 대한 판단을 한다.



* + - * 1. Hyperparameter : {Noisy\_dimention = 100, hidden\_size1 = 256, hidden\_size2 = 512, image\_size = 64 \* 64, learning\_rate = 2e-4, Optimizer = adam}
        2. Synthesize Image

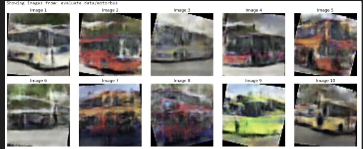


결과 : GANs 모델은 사람도 구분하기 힘든 Image를 생성한다

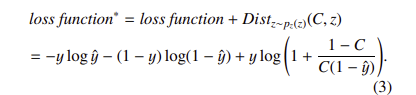
* + - 1. **DCGAN**
         1. Deep Convolution Network를 GANs 적용한 DCGAN
         2. 논문에서 제공된 모델 Architecture, weight\_init을 Generator에게만 적용, discriminator적용X(image set resolution이 적기 때문에 선명하지 못하는 이유)
         3. Hyperparameter : {Noisy\_dimention = 100, learning\_late = 2e-4, input\_size = 64\*64}
         4. 데이터 augmentation을 통해 데이터 수 증강

(RandomRotation, RandomHorizontalFlip, Normalize)

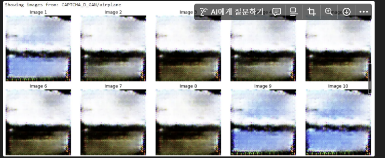
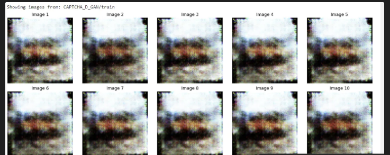
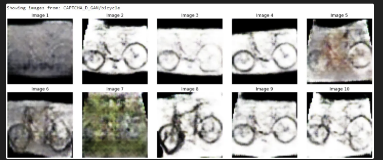
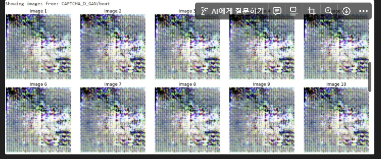
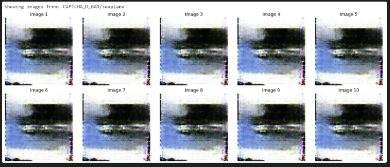
E. Synthesize Image



* + - 1. **Distance – GANs**
         1. DCGAN architecture에서 Generator loss Function에 distance(C,z)를 추가함으로써 생성되는 image 모든 pixel값에 distance값이 더해진다.



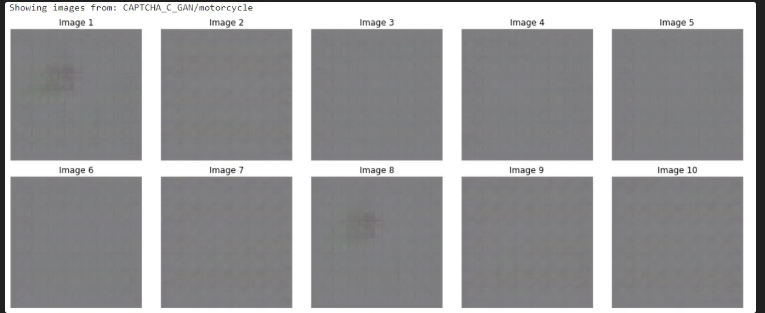
* + - * 1. Hyperparameter : {Noisy\_dimention = 100, learning\_late = 2e-4, input\_size = 64\*64, distance\_factor = 0.1, C = 1.2}
        2. Synthesize image



* + - 1. **Composite – GANs**
         1. DCGAN으로 생성한 이미지와, batch내에 있는 original image를 결합한 데이터를 토대로 Generator, discriminator를 학습



* + - * 1. Hyperparameter : {Noisy\_dimention = 100, learning\_late = 2e-4, input\_size = 64\*64, alpha = 0.5}
        2. Synthesize Image



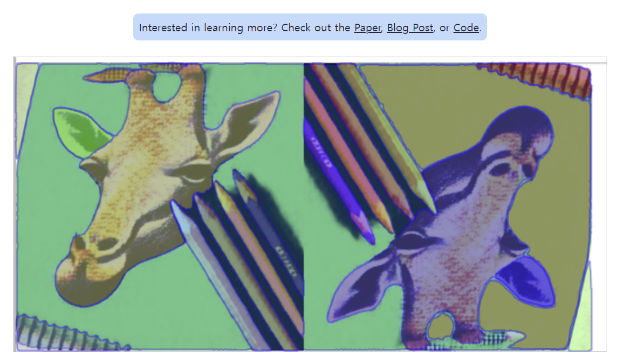
* + 1. **() Image 데이터를 Stable Diffusion 모델에 적용을 하여 새로운 데이터로 만든다.** 
       1. **FLIP illusion : 한 이미지를 뒤집으면 다른 이미지가 되는 것**
          1. 초기 단계에서 Prompt를 입력받아 Condition으로 사용을 하여 이미지를 생성한다.



* + - * 1. 학습이 진행되면서 Diffusion Model은 Noisy를 제거하고 Condition을 바탕으로 Image를 만들게 된다.



* + - * 1. Segmentation Anything Model을 통한 결과



SAM(Computer 구분) : Left\_image는 (기린,연필), Right\_image는 (펭귄, 연필)

* + - * 1. 관련 Tasks

왼쪽 image를 180도로 뒤집으면 어떤 동물이 보일까?

컴퓨터는 왼쪽이미지를 180도 회전 시킬 수는 있는 다음 시각적 해석이 필요한 부분은 어려움을 느낀다.

두 개의 Image는 같은 이미지일까?

컴퓨터가 Pixel단위로 계산을 하는 알고리즘만 사용하면 불가능

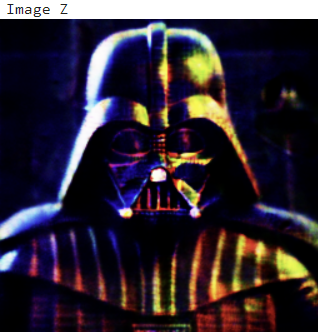
Multimodal, CNN모델이 변형된 데이터까지 학습을 한 상태이면 가능하다.

왼쪽 이미지에 있는 연필들은 동물과 어떤 연관성이 있을까?

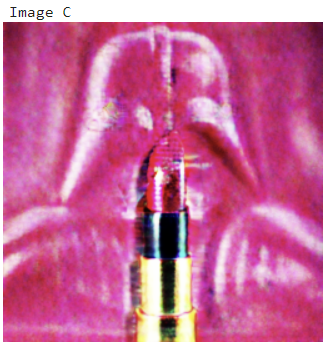
추상적 설명을 요구하는 것은 컴퓨터에게 어려움을 준다.

* + - 1. **Hidden Overlays illusion : 여러 이미지를 합쳐 특징 이미지를 숨기는 방법**
         1. 초기 단계에서 Prompt를 입력받아 Conditon으로 이미지 생성, 숨길 Text Prompt 선택

숨길 Text Prompt 결과 이미지



여러 특징 Condition 결과 이미지



* + - * 1. 관련 Tasks

Image 안에서 숨겨져 있는 Character의 이름은?

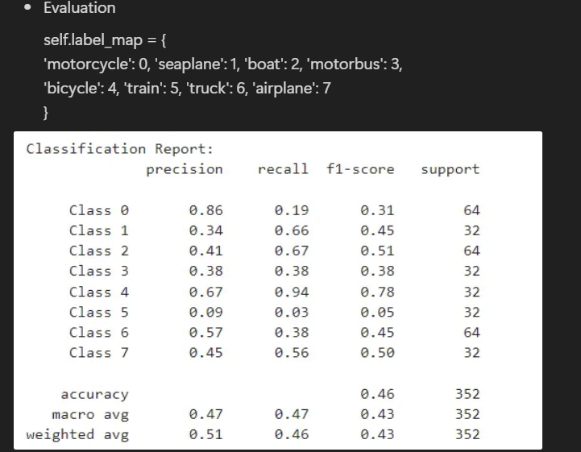
* 1. **Synthesize or Augmented Data Evaluation**
     1. **ResNet18 Fine-Tuning Evaluation**
        1. Pre – trained ResNet18 모델에서 Fully Connected layer (weight,Bias)만 학습을 하고 나머지 부분은 Freeze한다. 새롭게 만들어 둔 데이터를 Confusion – matrix, F1-score를 메겨 잘 학습된 Computer가 어느 정도 인 지 할 수 있는 지 파악한다.
           1. GANs Evaluation 결과

Human : 생성된 image 208장 중에서 160장 분류 (80%)

Model : 생성된 image 208장 중에서 150장 분류 (~80%)

-> 따라서 GANs의 경우 시각 CAPTCHA Method로는 부적합하다.

* + - * 1. DCGANs Evaluation 결과

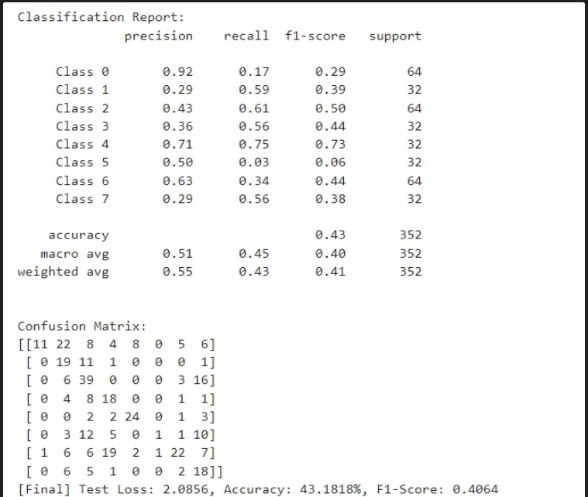


Human : 생성 image 352장 중에서 340장 분류(96%)

모델 f1-score = 43%

-> DCGAN을 사용하는 것이 시각 CAPTCHA Method로써 적합하다.

* + - * 1. Distance-GANs결과

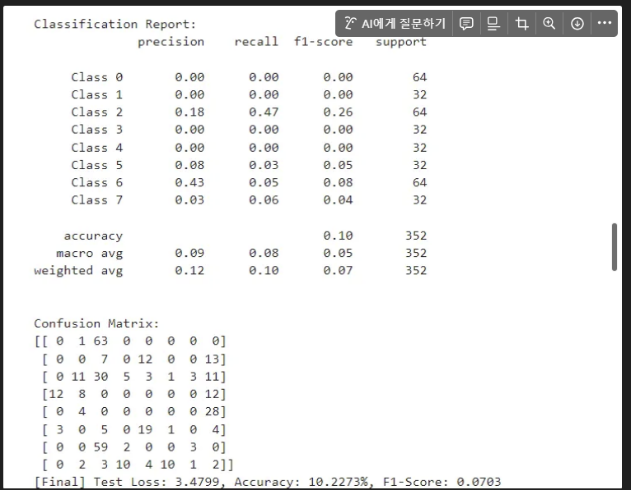


Human : 생성 image 352장 중에서 40장 분류(11%)

Model f1 – score = 40%

->Distance를 추가하는 것은 시각 CAPTCHA Method로써 적합하지 않다.

* + - * 1. Composite-GANs결과

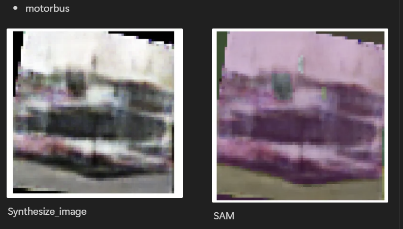
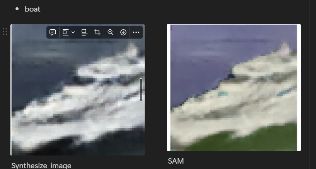
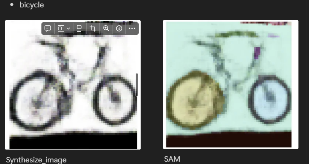
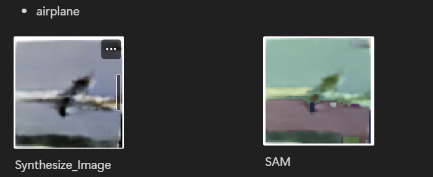


Human : 생성 image 352장 중 0장 분류(0%)

Model f1 – marco : 0.07

->Composite – DCGANs은 시각 CAPTCHA Method로써 적합하지 않다.

* + 1. **Image Segmentation Model SAM**
       1. Segmentation Anything Model을 사용하여 Synthesized Image, Noisy 적용된 Image를 SAM 모델을 통해 컴퓨터가 Segmentation 할 수 있는 정도를 시각화 한다.
          1. **DCGAN**



1. **프론트엔드 & 백엔드**

: **GAN을 통해 생성된 CAPTCHA 이미지를 프론트엔드로 전송받아 팝업창을 통해 출력. 정답 데이터로 설정된 이미지와 사용자가 선택한 이미지의 일치 여부를 판단하여 결과 도출. 성공 시 개인정보를 서버로 전달하여 저장하고 팝업창에서 알림창을 통해 메시지 제공. 실패 시 개인정보를 저장하지 않고 새롭게 문제를 해결해야함. 최종적으로 검증 결과를 사용자에게 반환**

1. **프론트엔드**

: 사용자에게 CAPTCHA 이미지를 표시하고 마우스 움직임 데이터를 추적하여 백엔드로 수집된 데이터를 전송

* **CAPTCHA 이미지 로드**
* 서버에서 제공하는 CAPTCHA 이미지와 중앙부 이미지를 url을 주소로 입력 받아 이미지 로드
* ‘generated\_captcha.png’: CAPTCHA 이미지 저장
* ‘answer\_captcha\_{index}\_correct.png’: 정답 이미지 저장
* ‘answer\_captcha\_{index}-fake.png’: 오답 이미지 저장

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

* 개인정보를 입력한 뒤 ‘개인정보 활용에 동의합니다.’ 체크박스를 클릭하는 경우에만 회원가입 버튼이 눌린다.

텍스트, 스크린샷, 직사각형, 라인이(가) 표시된 사진

자동 생성된 설명

* **서버로 데이터 제출 및 submit 버튼 생성**
* 사용자가 클릭한 이미지와 정답으로 설정된 이미지 간의 데이터 간의 일치 여부를 검증하여 검증 결과를 반환 및 서버로 전달

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

1. **백엔드**

: CAPTCHA 이미지 및 검증을 위한 9개의 이미지를 제공받고 정답 이미지를 클릭할 시 회원가입을 성공시키고 실패 시 이미지를 새로고침하여 새로운 이미지를 제공받는다

* **상단부 이미지 및 중앙부 9개 이미지 로드**
* 검증을 위한 상단부 이미지와 중앙부 9개 이미지 로드

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

자동 생성된 설명

* **CAPTCHA 이미지와 정답 데이터 제공**
* 생성된 CAPTCHA 이미지와 설정된 정답 데이터 제공
* 사용자가 클릭한 이미지들이 정답 이미지로 설정된 이미지와 일치 여부를 검증

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

1. **CNN 모델 학습**

: 마우스 이동 데이터와 정답 경로의 히트맵을 학습 데이터로 받아 CNN 모델 학습하여 사용자가 경로를 따라갔는지 여부를 판단

* 마우스 움직임 데이터를 기반으로 히트맵 생성
* 라벨링을 진행하여 정답 경로일 경우 ‘1’ 출력, 정답 경로가 아닐 경우 ‘0’ 부여
* CNN 모델 생성 함수를 통해 모델 형성
* 학습을 위한 데이터 셋 구축 후 모델 학습 및 저장
* 테스트 데이터를 생성하여 학습된 모델의 정확도 평가

스크린샷이(가) 표시된 사진

자동 생성된 설명

1. **진행중**
   1. 새로운 프론트엔드 & 백엔드 양식

* 다양한 상황에 대비한 프론트엔드 양식 구상
* 이미지를 로드해왔을 때 중앙부 이미지를 다른 이미지로 설정하거나 마우스 움직임을 포착 가능하게 양식 구상
* 이미지에 맞는 다양한 질문 프롬프트 구성
* 더 많은 데이터셋 확보를 통한 다양한 이미지 바탕의 질문으로 구성

1. **기획중**
   1. 마우스 움직임 포착

* DCGAN을 통해 생성되는 이미지 finetuning하기
* 현재 이미지에 블러 처리 및 물체 식별에 어려움이 있어 이미지의 파라미터를 미세 조정하여 더 품질이 좋은 이미지 데이터로 추출 필요
* 사용자 or 봇 여부 검증 방식 확립
* 현재 사용자와 봇을 구별하는 방법으로 테두리 따라 그리기인데 이를 생성 이미지에서의 사람과 봇 구별과 어떤 방식으로 통합하여 구성할지 또는 별개의 인증 수단으로 사용할 지에 대한 논의 필요
* 마우스 움직임과 결합할 이미지 생성

야외, 사람이(가) 표시된 사진

자동 생성된 설명