금융 메타버스 플랫폼 내 GAN을 활용한 손금 인증 서비스

금융보안캠프 6조
조소영, 권민주, 안성현, 김영준

목차

01 배경 및 필요성

02 GPA 개념 설명

03 GPA 설명

04 기대 효과

01

배경 및 필요성

배경 및 필요성

메타버스 환경 주목

MZ 세대 중심의 가상세계 발달

코로나19로 인한 비대면 사회가 일상화
새로운 사회적 장으로 자리잡음

메타버스의 핵심 인프라 구축

자율주행차 등 신산업의 발전에 따라
DNA(Data, Network, AI)를 촉진

메타버스 기술의 상용화

AR/VR 기술은 AI 등 타 신기술 대비
높은 상용화 수준에 진입

배경 및 필요성

메타버스 보안 이슈

메타버스 시대 '보안' 없이는 기회도 없다…'인증' 보안 마련 급선무

김가은 기자 | 승인 2022.04.13 17:45

가 가

메타버스 보안 핵심은 '인증'

메타버스 시대에서 가장 시급하게 선행돼야 할 보안 영역으로는 '인증'이 꼽혔다. 아바타를 통해 가상공간에서 모든 활동을 진행하는 메타버스 특성상 인증이 핵심이라는 설명이다.

이 교수는 "아바타의 신원 및 물건 구매시 현실세계와 연동하기 위한 인증이 필요하며 이를 검증할 메타버스 인증기관 및 제로트러스트 기반 시스템이 구축돼야 한다"며 "생체인증, 사설인증서, PKI 등 디지털 멀티 통합 인증이 중요하다"고 말했다. 이 날 그는 ▲지문 ▲음성 ▲전자주민증▲운전면허증▲국민연금 ▲의료보험 ▲QR코드 등을 연결해 열차 개념 인증 서비스를 제안했다.

배경 및 필요성

생체인증 기술 현황

비접촉식 생체 '인식' 강조

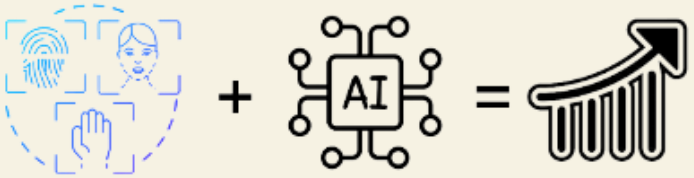
1.0 시대 → 2.0 시대 → 3.0 시대

머신러닝의 생체인증 복합화를 이용

(출처. LDB미래전략연구소)

배경 및 필요성

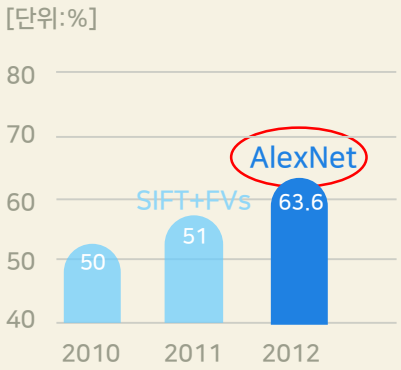
컴퓨터 비전과 머신러닝



생체 인증
(컴퓨터 비전)

머신러닝

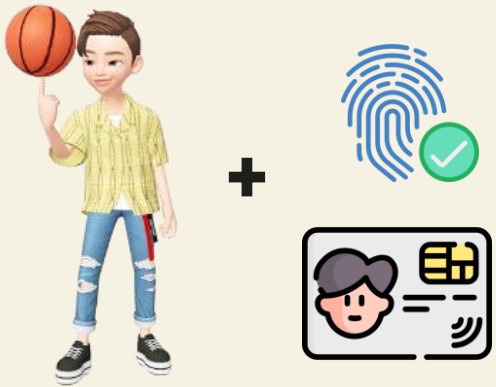
성능 향상



- 컴퓨터 비전: 컴퓨터가 사람처럼 영상을 보고 영상 속 중요한 정보를 알아내는 분야
- 생체 인증에서 사용하는 얼굴이나 손금 등도 컴퓨터는 2D 영상을 통해 확인하고 그 영상 속에서 특징을 파악함으로써 사용자를 구분함
- 2012년 '이미지 인식' 대회에서 AlexNet이라는 머신러닝 모델이 나오면서 이전 모델들을 압도하는 퍼포먼스를 보여주었음 (51% → 63%)

배경 및 필요성

메타버스 내 아바타 인증



1. ID나 지문을 워터마크 형태로 아바타에 삽입해서 워터마크를 통해 인증

2. 아바타를 만들 때부터 소유자와 닮게 만들어서, 아바타 그 자체로 안면 인증

BUT!

공격자가 메타버스 플랫폼의 사용자 계정을 탈취하면
특정 이용자로 위장해 악의적인 활동을 할 수 있음

배경 및 필요성

프로젝트의 필요성

편리성

메타버스 사용자들 누구나 사용가능

모든 기기에서 사용 가능

인증 과정이 간결

보안성

사용자 계정을 탈취해도

보안 상 문제가 없음

GPA (Gan Palmistry Authentication)

GPA (Gan Palmistry Authentication)

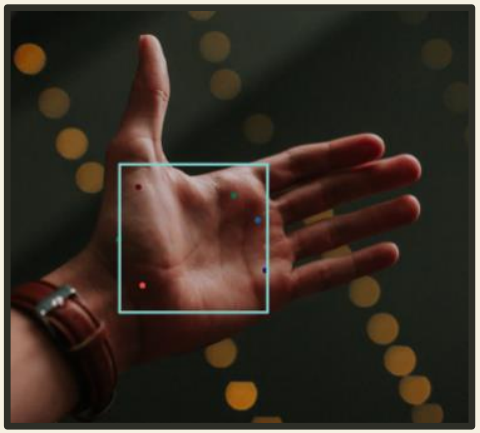
GAN과 보조인증을 활용한 손금 인증 서비스

02

GPA 개념 설명

GPA 개념 설명

YOLO 모델



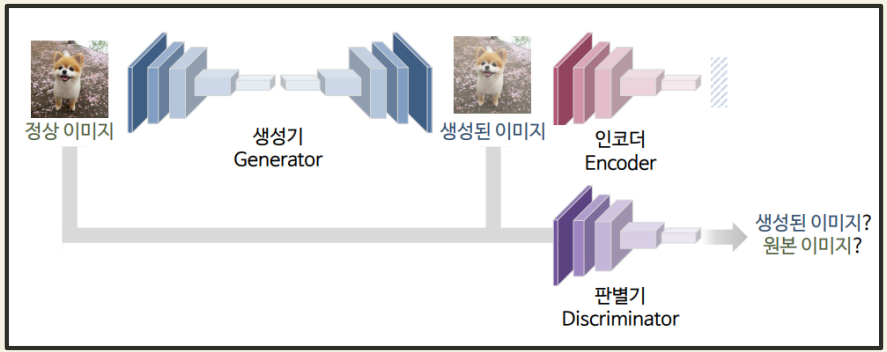
YOLOv5

- YOLO 모델
  - 입력 이미지가 손이 아닌 손금이 되려면 객체 검출이 사전에 필요함
  - 손에서 손금 영역을 잘 검출하도록 YOLO 모델을 학습함
  - YOLO: 객체 검출 문제에서 매우 높은 성능을 보이는 딥 러닝 모델

GPA 개념 설명

GANomaly

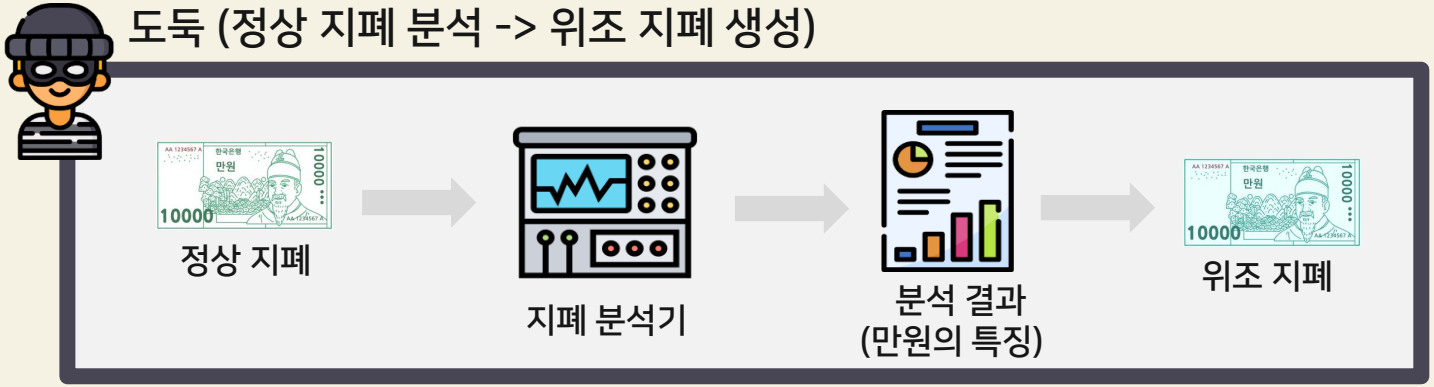
- GAN 기반 이상치 탐지
  - 이상치 탐지: 불량 검출, 이상 감지 등 비정상 여부를 탐지하는 기술
  - GAN: 머신러닝을 이용한 이미지 생성 모델
  - GANomaly: 대표적인 GAN 기반 이상치 탐지 모델



GPA 개념 설명

GANomaly

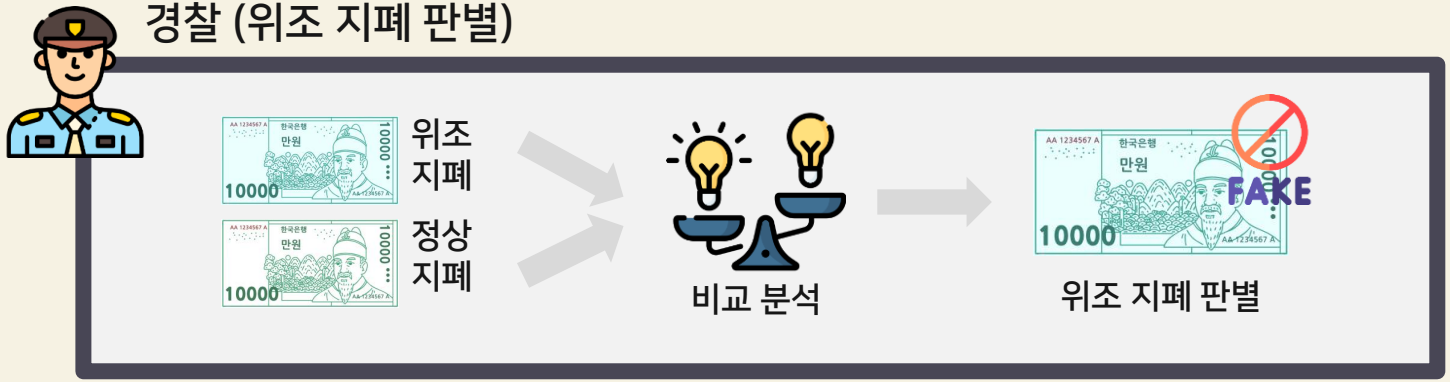
- 생성기 (도둑)
  - 위조 지폐를 생성하는 역할
  - 자신에게 들어온 지폐를 분석 -> 지폐의 특징 파악
    -> 특징을 이용해서 위조 지폐 생성



GPA 개념 설명

GANomaly

- 판별기 (경찰)
  - 위조 지폐를 판별하는 역할
  - 위조 지폐와 정상 지폐 비교
    -> 위조 지폐가 진짜인지 가짜인지 판별



GPA 개념 설명

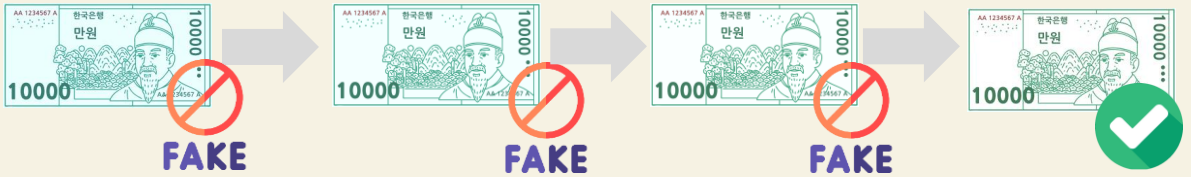
GANomaly

- 도둑(생성기)은 진짜 같은 위조 지폐를 만들기 위해 학습함
- 경찰(판별기)은 위조 지폐를 잘 구분해내기 위해 학습함
- 경찰이 위조 지폐를 구분해내지 못 할 때 까지 학습을 진행함

도둑
(위조 지폐 생성)

첫 번째 시도 두 번째 시도 세 번째 시도 네 번째 시도

경찰
(위조 지폐 판별)



GPA 개념 설명

GANomaly

- 천 원짜리 위조하기
  - 도둑은 지금까지 만 원으로 위조 만 원을 생성하는 일 밖에 하지 않음
  - 도둑의 보스가 나타나 천 원으로 위조 천 원을 생성하는 것을 요구

천 원도 한번 위조해봐!!

보스

넵.. 만들어보겠습니다..

도둑

GPA 개념 설명

GANomaly

- 천 원으로 만 원 생성
  - 도둑은 지폐의 특징으로 위조 지폐를 생성하는 일을 잘 함
  - 그러나 도둑은 만 원짜리만 생성하도록 학습했으므로

    위조 만 원만 만들 수 있음

도둑 (정상 지폐 분석 -> 위조 지폐 생성)

정상 천 원

지폐 분석기

분석 결과
(천 원의 특징)

위조 만 원

GPA 개념 설명

GANomaly

- 천 원으로 만 원 생성
  - 보스는 천 원으로 위조 만 원을 생성해낸 도둑을 믿지 못함

이게 가능하다고??

보스

위조 지폐

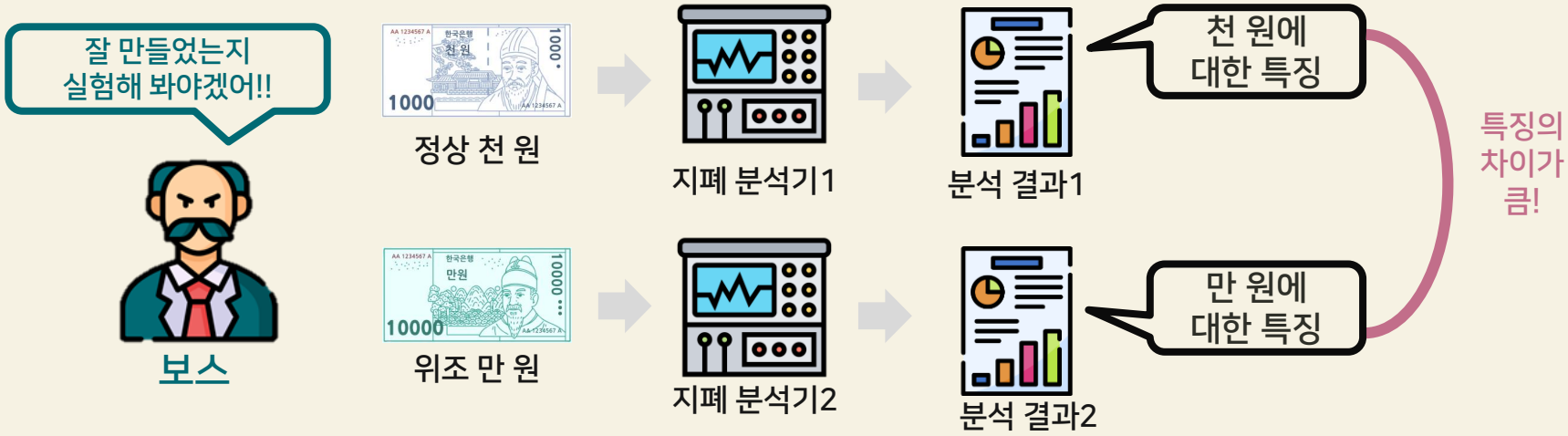
만 원밖에 못만들겠어요..

도둑

GPA 개념 설명

GANomaly

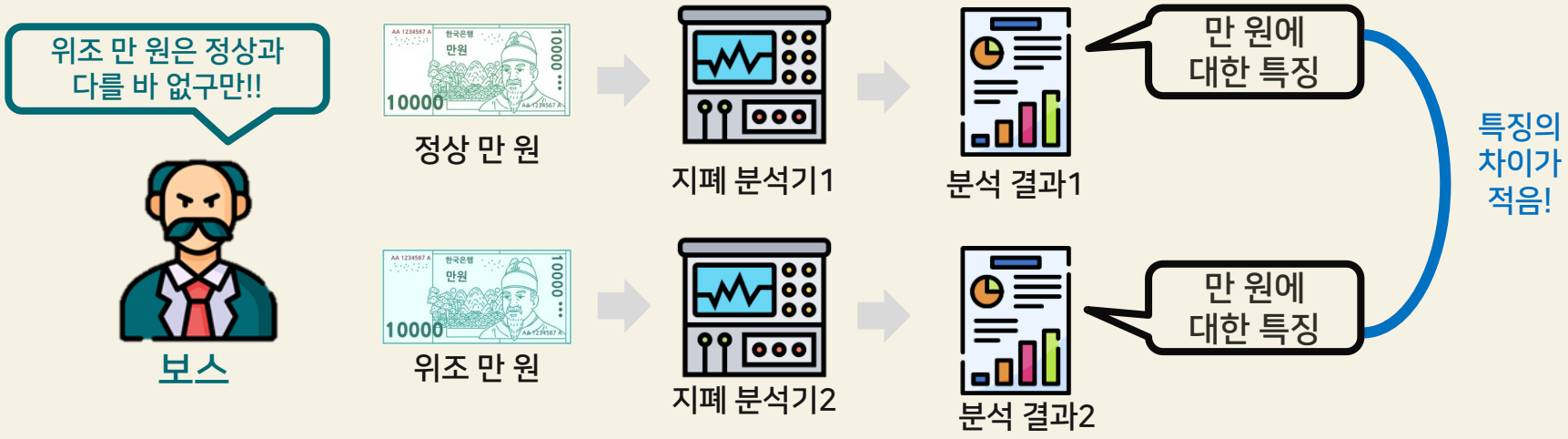
- 위조 지폐 실험
  - 정상 천 원의 분석 결과와 위조 만 원의 분석 결과가 다른지 실험해 봄
  - 분석 결과, 두 특징의 차이가 매우 컸음



GPA 개념 설명

GANomaly

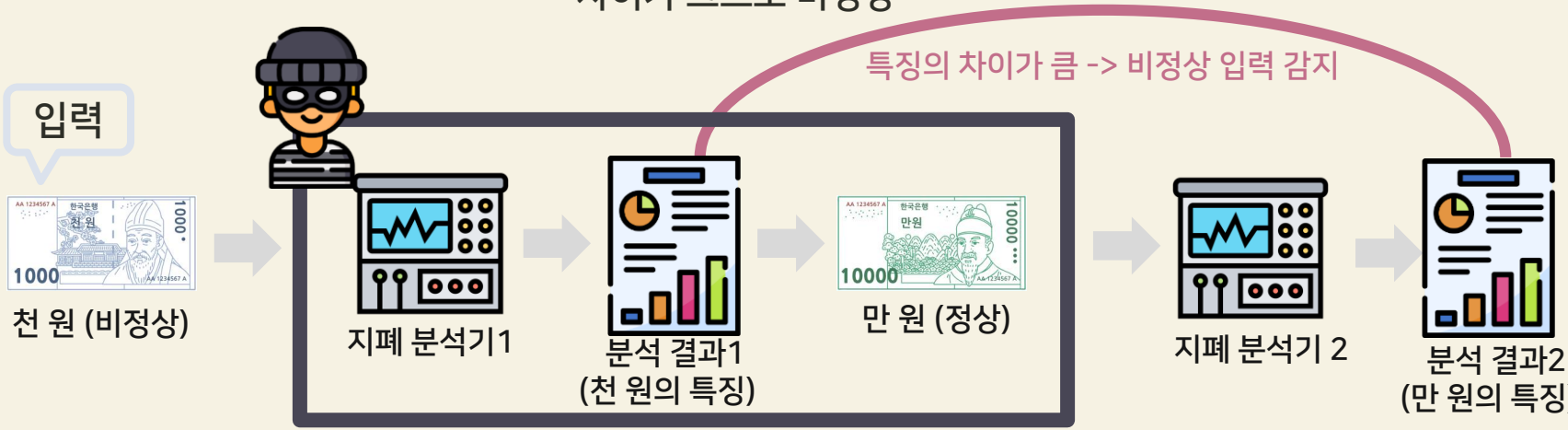
- 위조 지폐 실험
  - 정상 만 원의 분석 결과와 위조 만 원의 분석 결과가 다른지 실험해 봄
  - 분석 결과, 두 특징의 차이가 거의 없었음



GPA 개념 설명

GANomaly

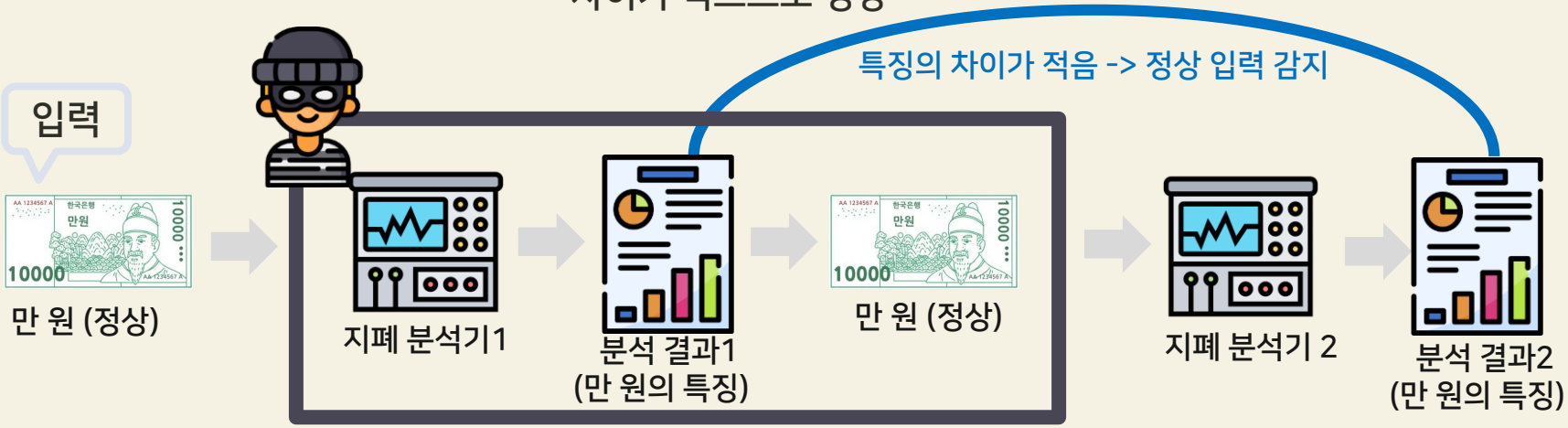
- 이상치 탐지
  - 분석 결과1과 분석 결과2의 차이가 이상치 탐지의 핵심 아이디어
  - 천 원을 비정상, 만 원을 정상이라고 간주 -> 입력이 천 원 -> 특징의 차이가 크므로 비정상



GPA 개념 설명

GANomaly

- 이상치 탐지
  - 분석 결과1과 분석 결과2의 차이가 이상치 탐지의 핵심 아이디어
  - 천 원을 비정상, 만 원을 정상이라고 간주 -> 입력이 만 원 -> 특징의 차이가 적으므로 정상



GPA 개념 설명

GANomaly

- 손금 인증과 이상치 탐지
  - 정상 이미지로 간주한 만 원을 ' 사용자의 손금 ' 으로 대체
  - 불량 이미지로 간주한 천 원을 ' 기타 모든 이미지 ' 로 대체
  - 사용자의 손금만으로 학습이 되므로 기타 모든 이미지는 불량으로 간주 됨

정상 이미지

불량 이미지

03

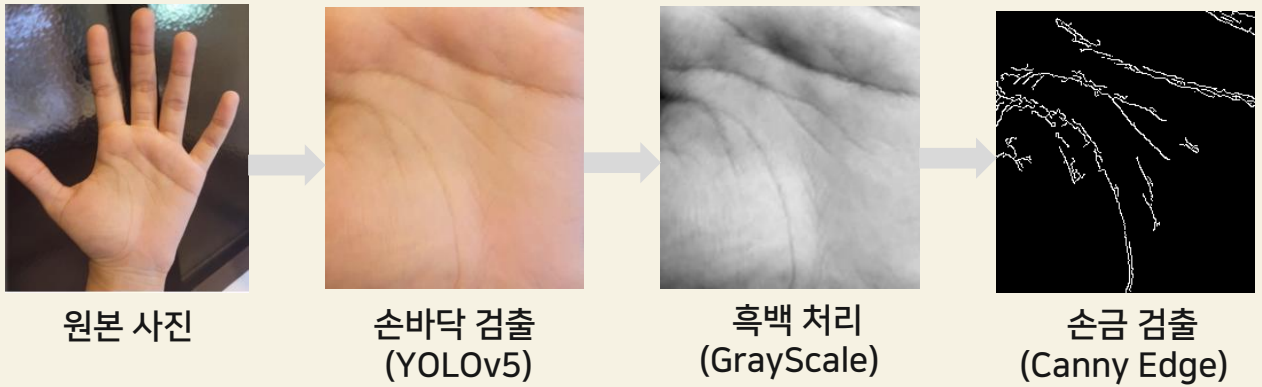
GPA 설명

GPA 설명

손금 검출

- 영상 처리
  - YOLO가 손금 영역(손바닥)을 검출하면 영상 처리를 진행함
  - 흑백 처리를 해서 연산량을 낮춤

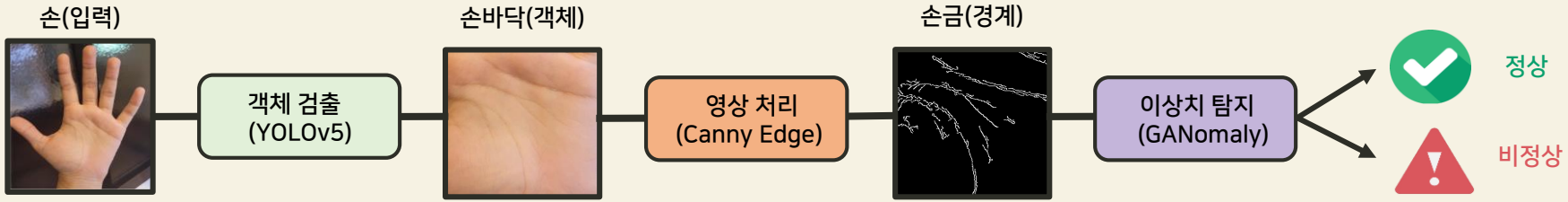
  -> 경계 검출 알고리즘 (Canny Edge Detection)으로 손금을 검출 함

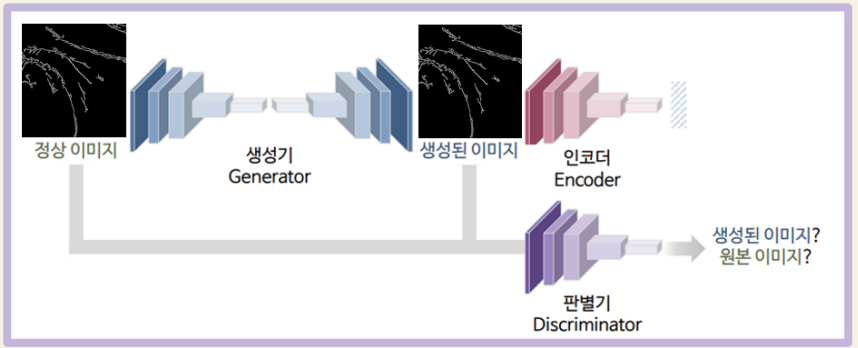


원본 사진 | 손바닥 검출 (YOLOv5) | 흑백 처리 (GrayScale) | 손금 검출 (Canny Edge)

GPA 설명

손금 검출 및 인식





GPA 설명

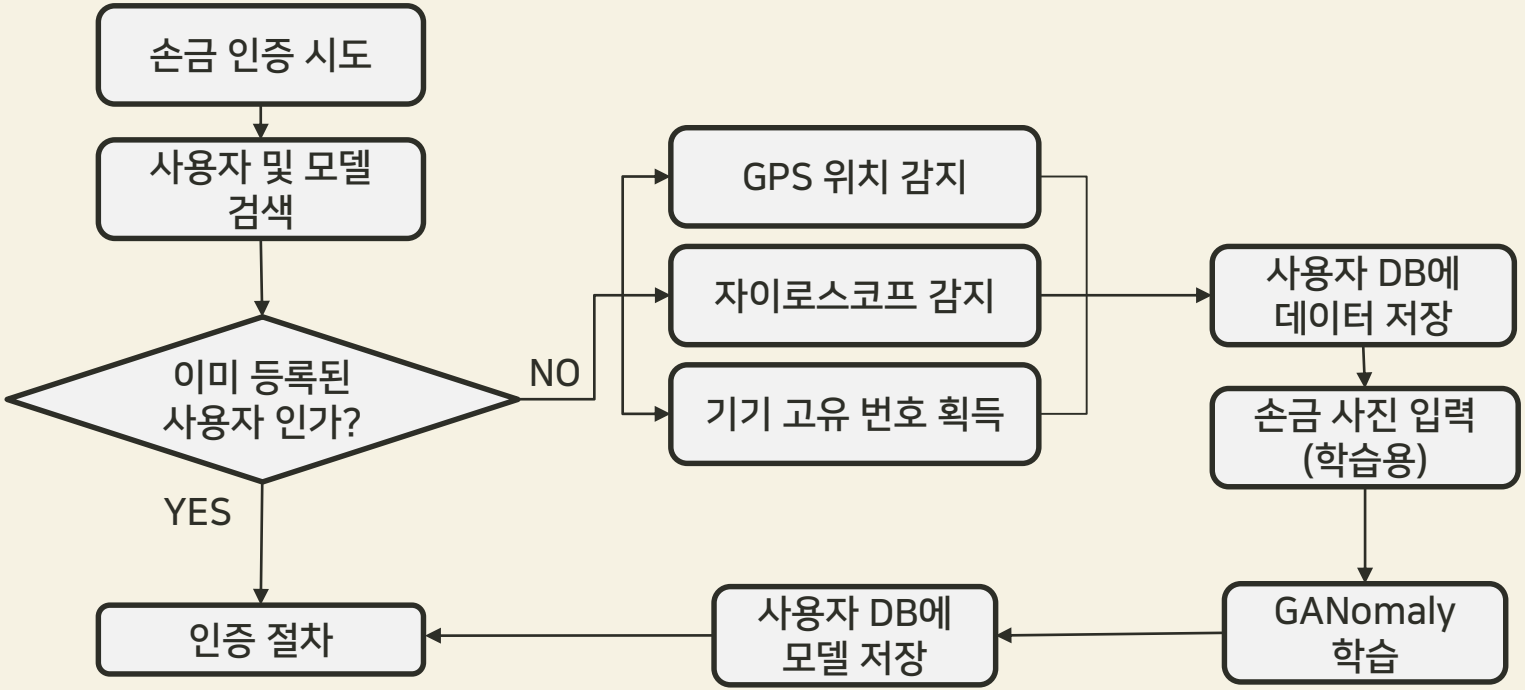
보안 강화

- 학습하기 전 (위치, 등록 기기, 자이로스코프 회전 정보)를 저장함
- 손금 인증 과정에서 저장한 세 정보 중 하나라도 다르면
  사용자 패턴이 다르다고 판단하여 인증 실패함

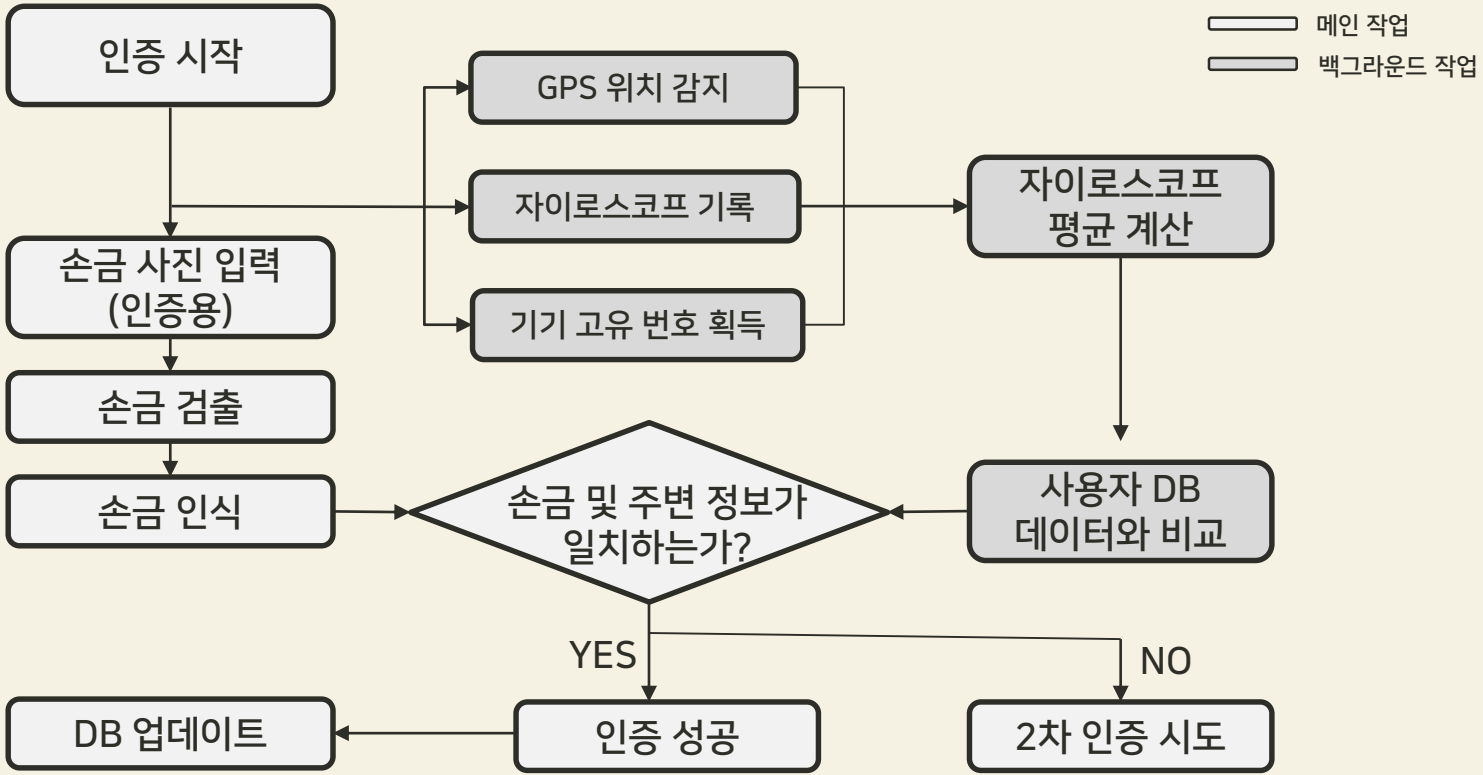
= 멀티플랫폼의 자이로스코프, 등록 기기, 접속 위치로
사용자 패턴 분석 후 이상 징후 시 2차 인증 요구

* 자이로스코프 = 물체의 기울기 및 움직임을 감지하는데 활용됨

GPA 설명

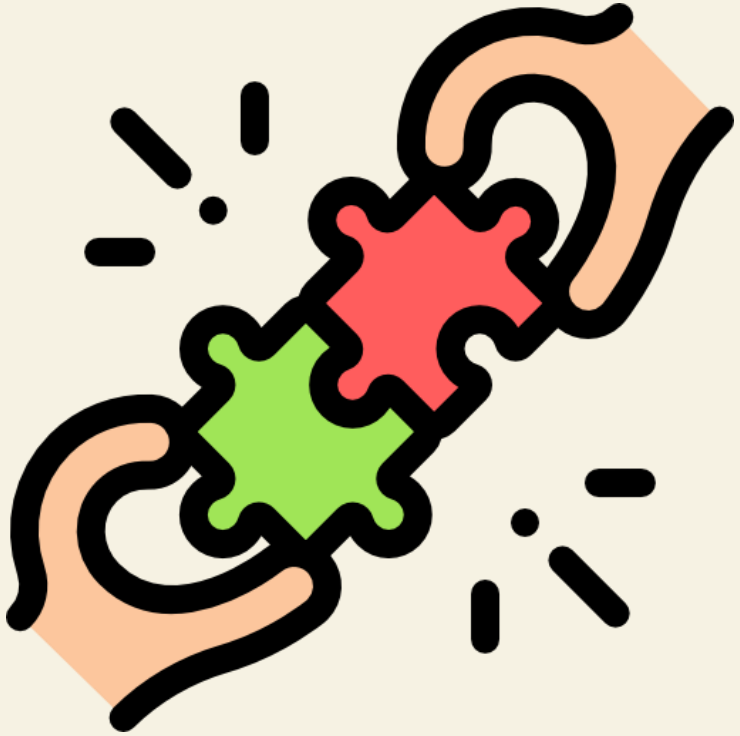

손금 인증 시도
사용자 및 모델 검색
이미 등록된 사용자 인가?
NO
YES
GPS 위치 감지
자이로스코프 감지
기기 고유 번호 획득
사용자 DB에 데이터 저장
손금 사진 입력 (학습용)
GANomaly 학습
사용자 DB에 모델 저장
인증 절차

GPA 설명


메인 작업
백그라운드 작업
인증 시작
GPS 위치 감지
자이로스코프 기록
기기 고유 번호 획득
자이로스코프 평균 계산
손금 사진 입력 (인증용)
손금 검출
손금 인식
손금 및 주변 정보가 일치하는가?
사용자 DB 데이터와 비교
YES
NO
DB 업데이트
인증 성공
2차 인증 시도

04

기대 효과



기대효과

차별성

타 생체 인증을 보완한 GPA

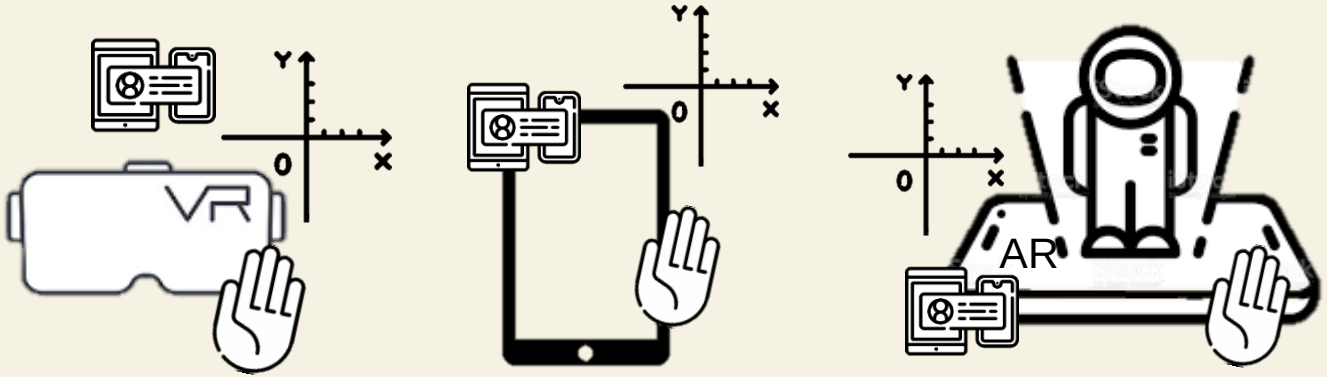
단점	지문	홍채	얼굴
실생활의 불편함	손에 물기가 많은 경우 인식률이 저하됨	렌즈, 안경을 사용하면 인식 속도가 느려짐	모자, 마스크 등 얼굴에 장애물이 있을 경우 인식률이 저하됨

GPA	손에 물기가 많아도 인식률에 영향을 미치지 않음	손에 차는 장신구(ex. 팔찌, 반지 등)는 인식 속도나 인식률에 영향을 미치지 않음

기대효과

범용성

금융 메타버스 인증을 기기 제약 없이 활용 가능

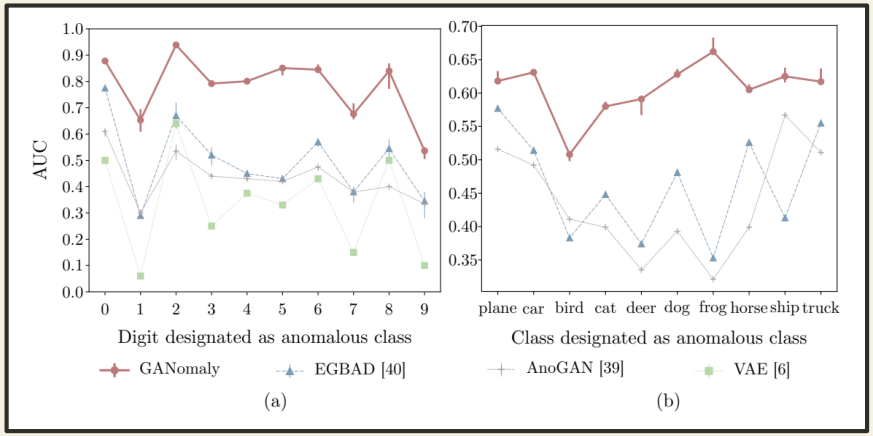


- 카메라가 내장되어 있는 모든 스마트기기(ex. 스마트폰, VR기기)에서 인증 서비스 사용 가능

기대효과

보안성

GAN의 알고리즘으로 높은 정확도



- 이상치 탐지를 하는 기존 알고리즘보다 훨씬 높은 정확도
(MAX AUC 95%)를 보여줌으로써 손금 인증에도 안정적으로 활용 가능

기대효과

보안성

3.0 인증체계에서 생체 정보 유출에 대한 인증 문제 해소

셀카 찍을 때 V 하면 해킹 위험 올라간다? - YTN 사이언스

홍채도 복사한다…생체인증 보안성 위기 맞나

'셀카에서 지문추출 外'… 5가지 최신 개인정보 위협요인

- 사용자 활동 과정에서 손바닥은 다른 신체(얼굴, 손가락 등)보다 노출이 적어 보안 활용에 더 뛰어남

기대효과

보안성

손금 인증 시, 주변정보를 보조 인증으로 사용하여 보안성 강화

- 위치 정보, 기기 정보, 기기 회전 정보(자이로스코프)를 사용자 모르게 감지하여 평소 패턴과 다를 시 2차인증을 요구

기대효과

보안성

금융 메타버스 인증에 대한 신뢰성 향상

- 금융 메타버스에서 사용할 수 있는 GPA을 제시함으로써 인증으로 인가 되지 않는 사람을 걸러내어 신뢰가 높은 금융 메타버스로 자리 매김할 수 있음

참고 문헌

- GAN 논문: https://arxiv.org/pdf/1406.2661.pdf
- GANomaly 논문: https://arxiv.org/pdf/1805.06725.pdf
- Introduction to Anomaly Detection (고려대 DMQA LAB) : http://dmqm.korea.ac.kr/activity/seminar/339
- GANomaly 핵심 리뷰 : https://ffighting.tistory.com/entry/GANomaly-%ED%95%B5%EC%8B%AC-%EB%A6%AC%EB%B7%B0
- 셀카 찍을 때 V 하면 해킹 위험 올라간다? (YTN) : https://m.science.ytn.co.kr/view.php?s_mcd=0082&key=201701231143461724
- 홍채도 복사한다…생체인증 보안성 위기 맞나 (서울경제): https://www.sedaily.com/NewsView/1OG2MMV3V7
- '셀카에서 지문추출 外'… 5가지 최신 개인정보 위협요인: https://www.ciokorea.com/news/32996#csidx360f1fd55288936b8a54d1fb0a05212
- 애플 글래스, 2025년 출시 전망..."안경으로 메시지 볼 수 있다?" (글로벌) : https://www.techm.kr/news/articleView.html?idxno=92957
- 삼성·애플·구글 참전…AR글래스 시장 '판 커진다' : https://news.g-enews.com/article/ICT/2022/06/202206081552265538 6fbbc3c26_1?md=20220608155548_U
- 본격화된 메타버스 금융, 법적 고려사항은? (한스경제): http://www.sporbiz.co.kr/news/articleView.html?idxno=612938
- 금융 메타버스 서비스 '보안 사각지대' (전자신문) : https://www.etnews.com/20211119000147

Thanks!