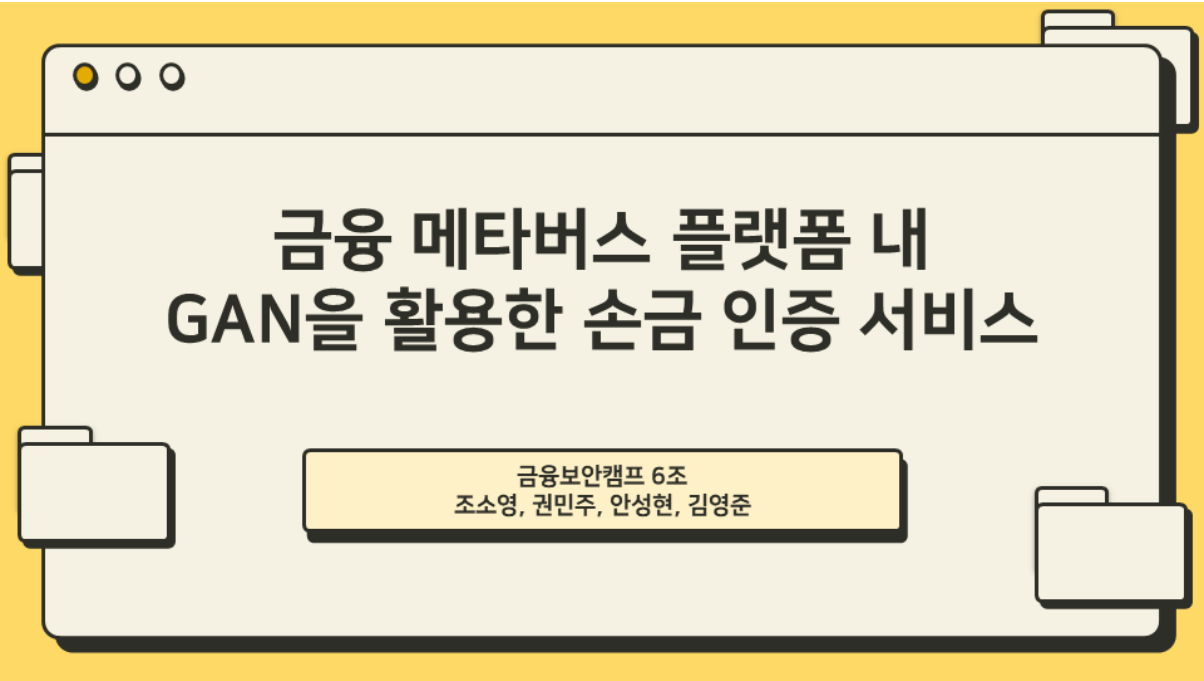
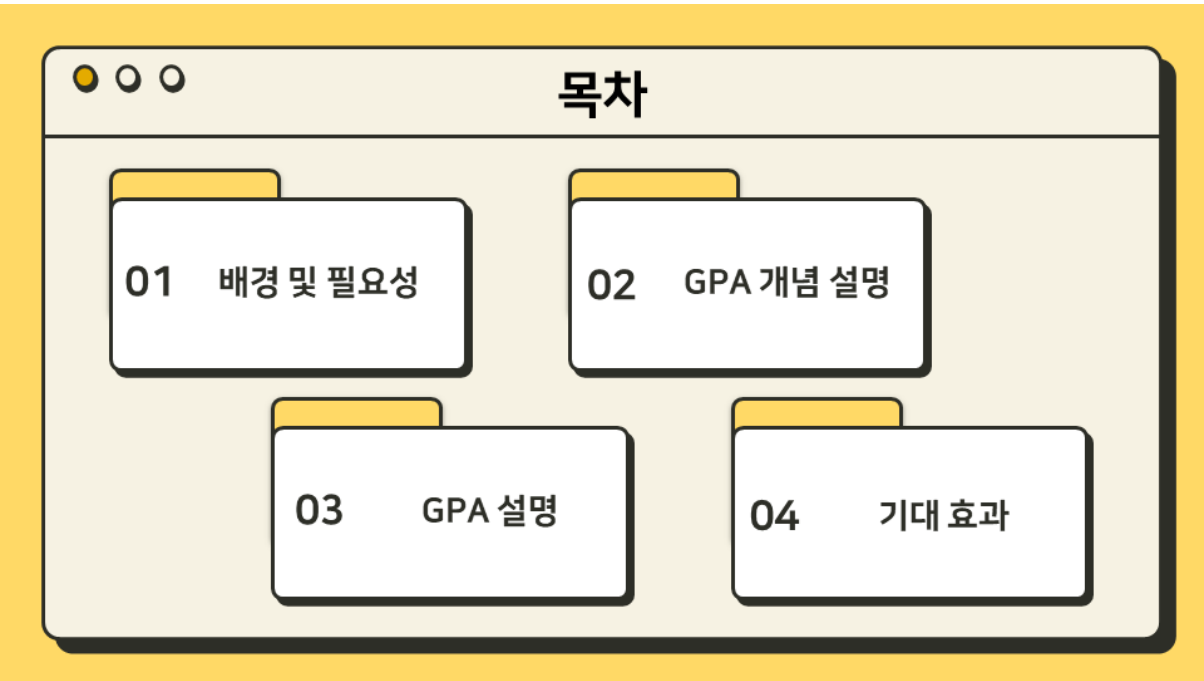


안녕하세요 '금융 메타버스 플랫폼 내 GAN을 활용한 손금 인증 서비스'를 주제로 발표하게 된 6조 안성현입니다.



목차는 다음과 같이 발표하겠습니다.

먼저 배경 및 필요성입니다.

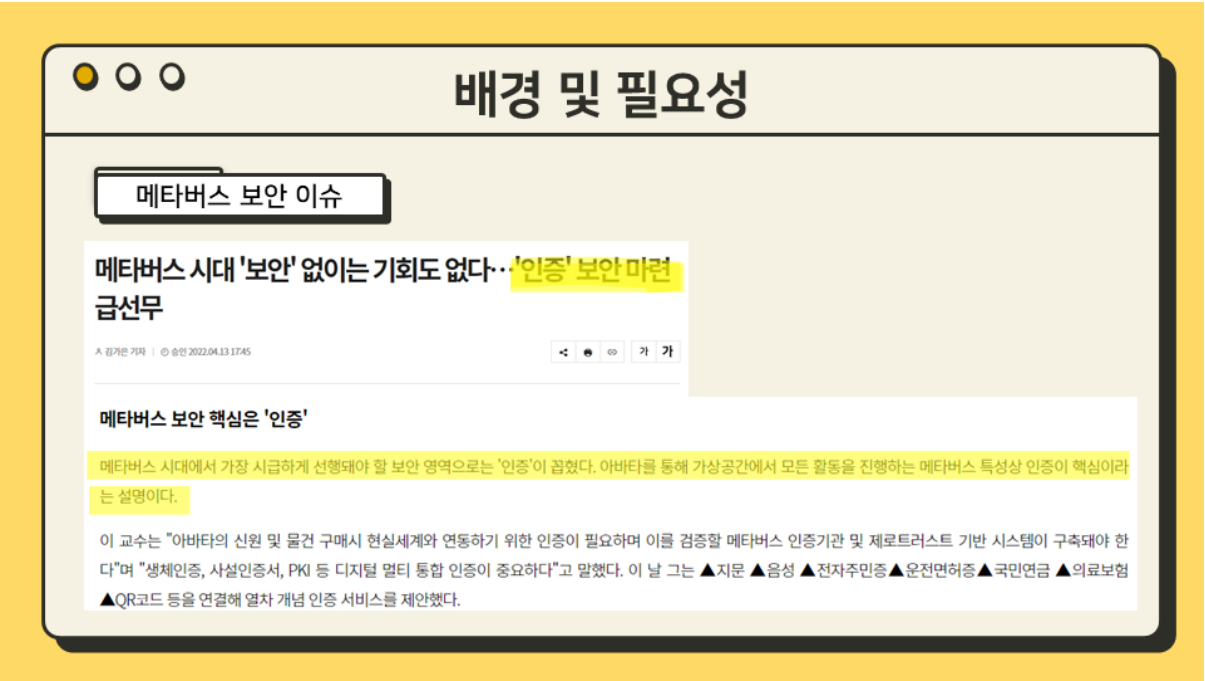
오늘날 메타버스 환경이 주목되고 있습니다.

메타버스 시장이 **급부상하게 된 계기는** 3가지가 있습니다.

첫 번째로, 코로나 19로 인해 비대면 사회가 일상화되어 MZ세대를 중심으로 가상세계가 새로운 사회적 장으로 자리를 잡았습니다.

두 번째로, 4차 산업혁명 본격화로 인해 메타버스의 핵심 인프라가 구축되었습니다.

마지막으로 AR/VR 기술은 AI 등 타 신기술 대비 높은 상용화 수준에 진입했기 때문입니다.



하지만 메타버스가 사회에 확산되면서 보안 위협이 크게 증가하고 있습니다

이 중 메타버스에서 가장 시급하게 선행되어야 할 보안 영역으로는 '인증' 이 꼽혔습니다.

아바타를 통해 가상공간에서의 모든 활동을 진행하기 때문입니다. 따라서 메타버스에서도 강력한 인증 시스템이 필요할 것으로 보입니다.

현재 '인증' 기술은 비접촉식 생체 '인식'이 강조되는 '2.0 시대'에서, 점차 보안성이 강화된 '3.0 시대'로 진입 중입니다. 3.0시대부터는 생체정보 복합 인증을 이용해서 '인증'기술의 보안성이 크게 개선되었습니다. 3.0시대에 떠오르는 기술 중 '생체 인증과 머신 러닝'에 대해 말씀드리겠습니다.

그 전에 컴퓨터 비전이라는 용어가 나옵니다.

컴퓨터 비전은 컴퓨터가 사람처럼 영상을 보고 영상 속 중요한 정보를 알아내는 분야입니다.

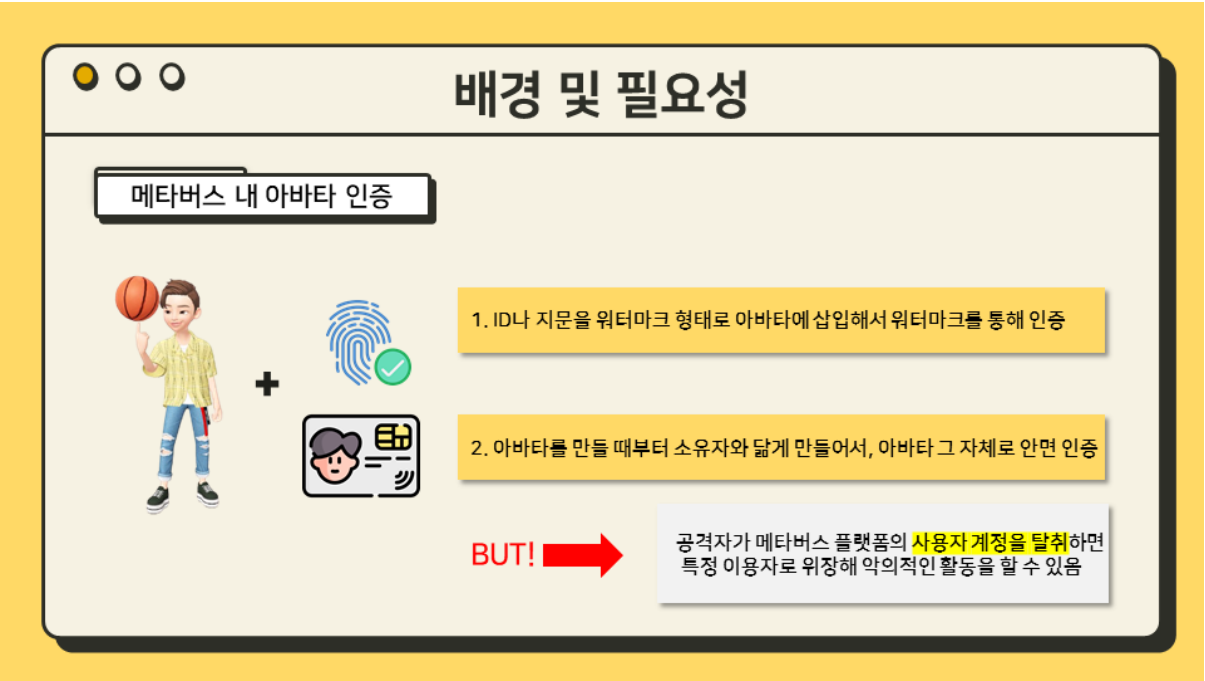
저희가 생체 인증에서 사용하는 얼굴이나 손금 등도 컴퓨터는 2D 영상을 통해 확인하고 그 영상 속에서 특징을 파악함으로써 사용자를 구분합니다.

따라서 생체 인증 문제는 컴퓨터 비전 문제를 푸는 것으로 생각할 수 있습니다.

그런데 이 컴퓨터비전 분야가 2012년부터는 머신 러닝과 함께 하게 됩니다.

2012년 '이미지 인식' 대회에서 AlexNet이라는 머신 러닝 모델이 나오면서 이전 모델들을 압도하는 퍼포먼스를 보여준 것입니다. 그리고 2022년인 지금까지 컴퓨터비전 분야에 머신 러닝이 결합할 시 성능 향상이 된다는 연구가 계속 나오고 있습니다.

따라서 생체 인증을 머신 러닝으로 해결하였을 때 높은 정확도를 기대할 수 있습니다.



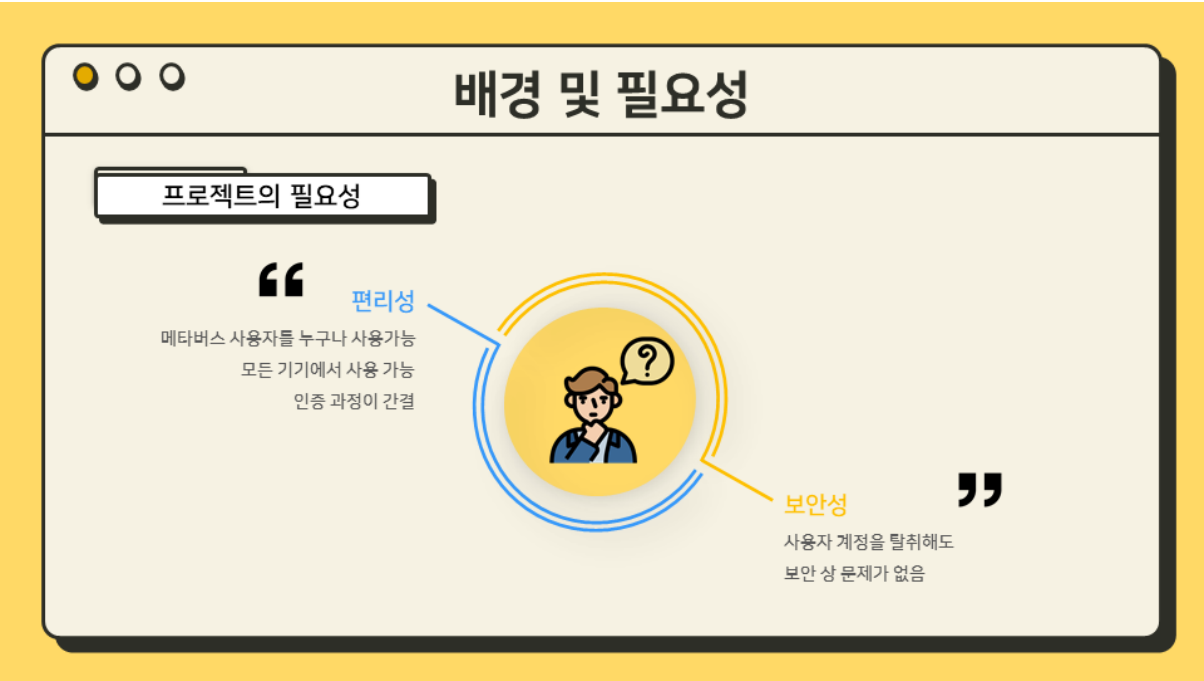
지금까지 소개해드린 생체 인증 기술을 메타버스 환경에서도 적용할 수 있습니다

바로 메타버스 내 아바타 인증을 이용하는 방식입니다. 이 방식은 크게 두 가지가 있습니다.

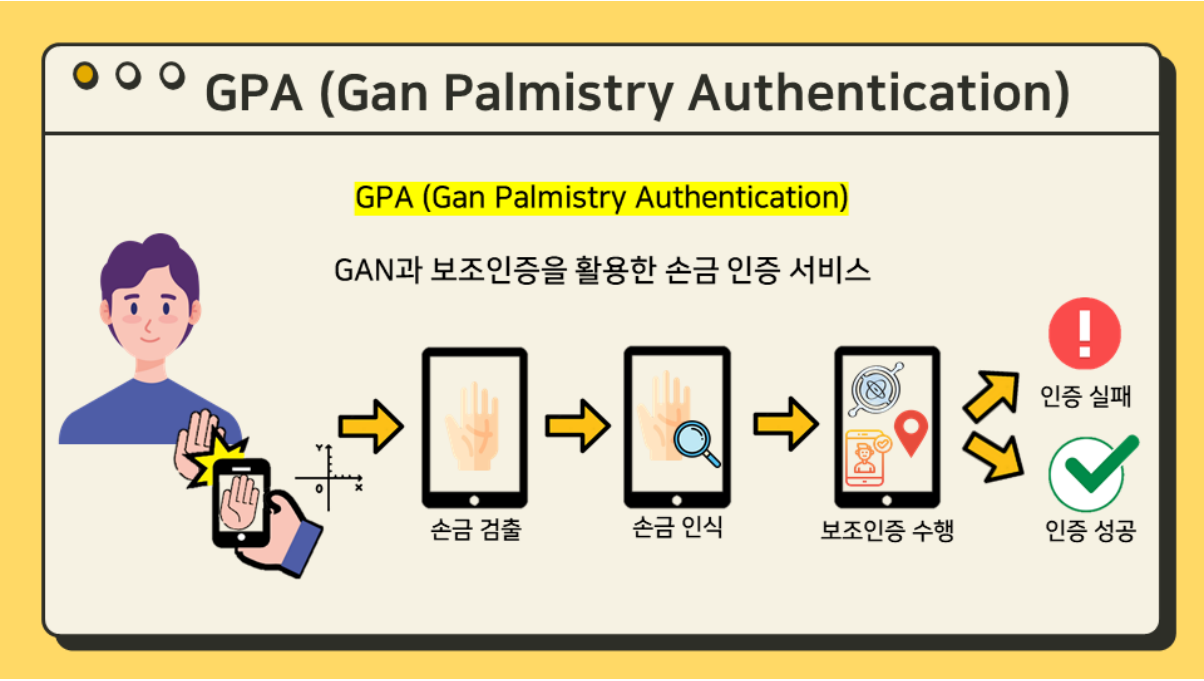
첫 번째로, ID나 지문을 워터마크 형태로 아바타에 삽입해서 워터마크를 통해 인증을 하는 방식입니다.

두 번째로, 아바타를 만들 때부터 소유자와 닮게 만들어서, 아바타 그 자체로 안면 인증을 하는 방식입니다.

그러나 이러한 아바타 인증은 메타버스 내부에서만 적용되기 때문에, 누군가 사용자의 계정을 탈취하면 해당 사용자로 위장해 악의적인 활동을 할 수 있다는 치명적인 단점이 존재합니다



따라서 저희는 아바타 인증만큼 편리하면서도, 사용자의 계정이 탈취되었을 때 보안 상 인증 문제가 없는 새로운 인증 서비스를 제안하려고 합니다

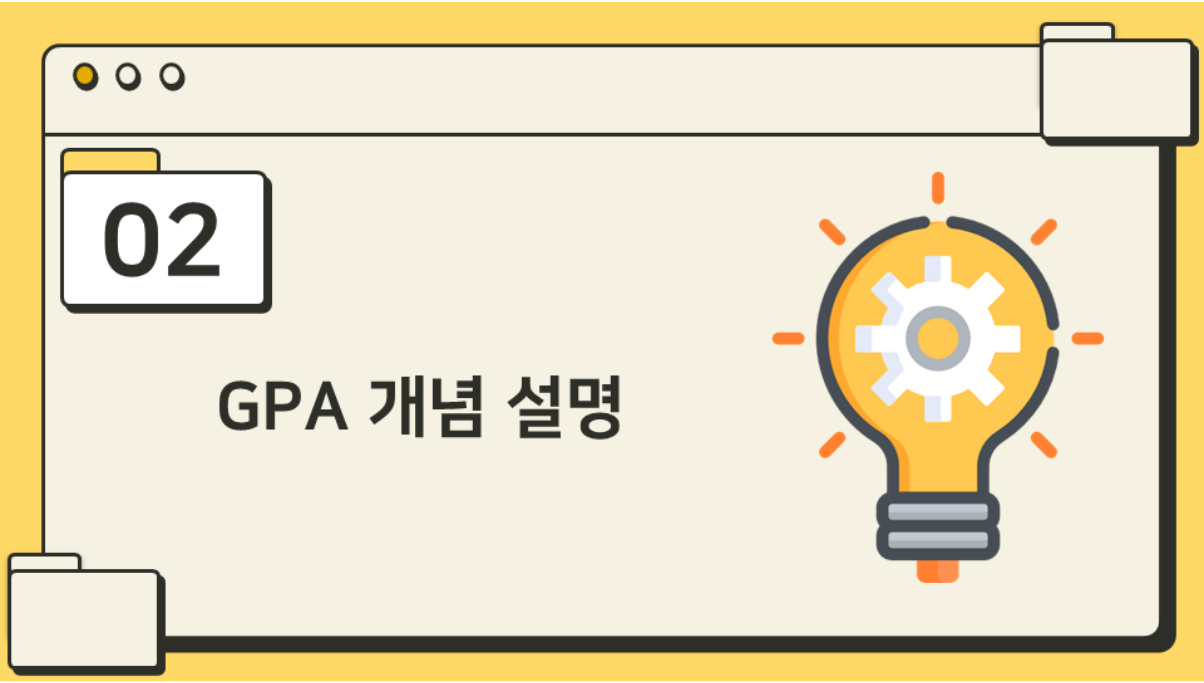


제안하는 서비스의 이름은 GPA (Gan Palmistry Authentication) 입니다.

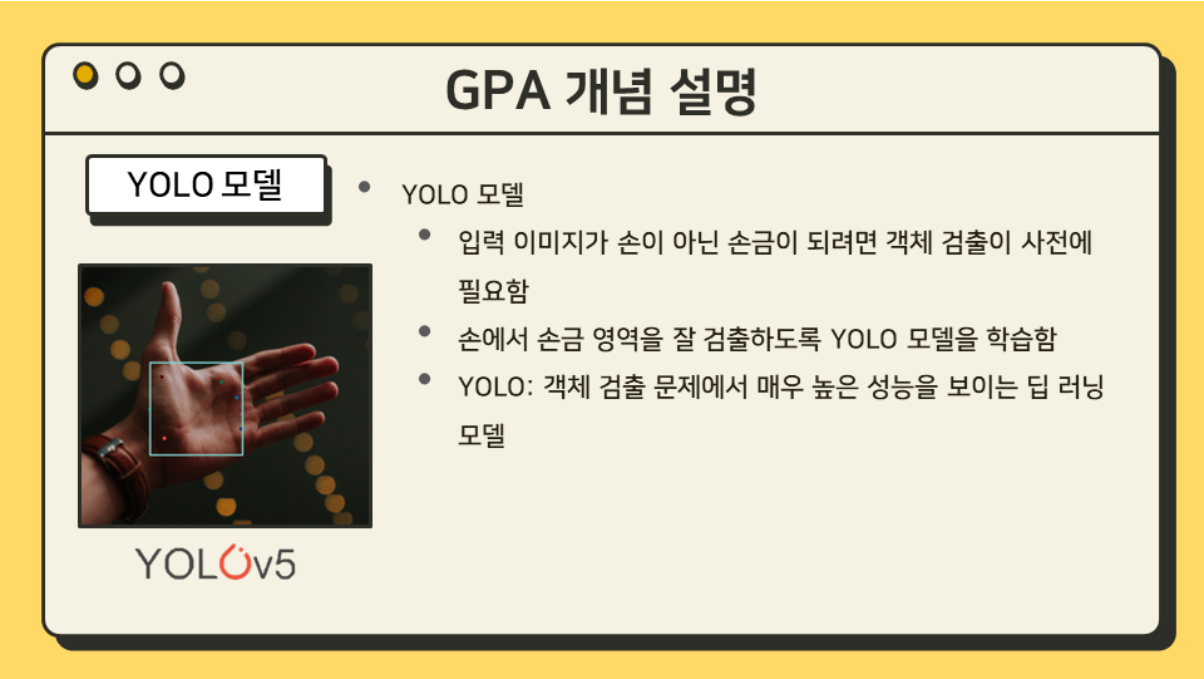
GPA는 머신 러닝 모델인 GAN과 보조인증을 활용한 손금 인증 서비스 의미합니다.

간단히 설명하자면 카메라와 영상 처리 기법을 이용해서 손금을 검출하고 GAN 모델로 손금을 인식합니다.

그리고 보안성을 강화하기 위해 보조 인증을 수행하면 인증 여부가 판별나게 됩니다.



GPA를 설명하기 앞서, 이해를 돕고자 개념 설명을 먼저 하고 넘어가겠습니다.

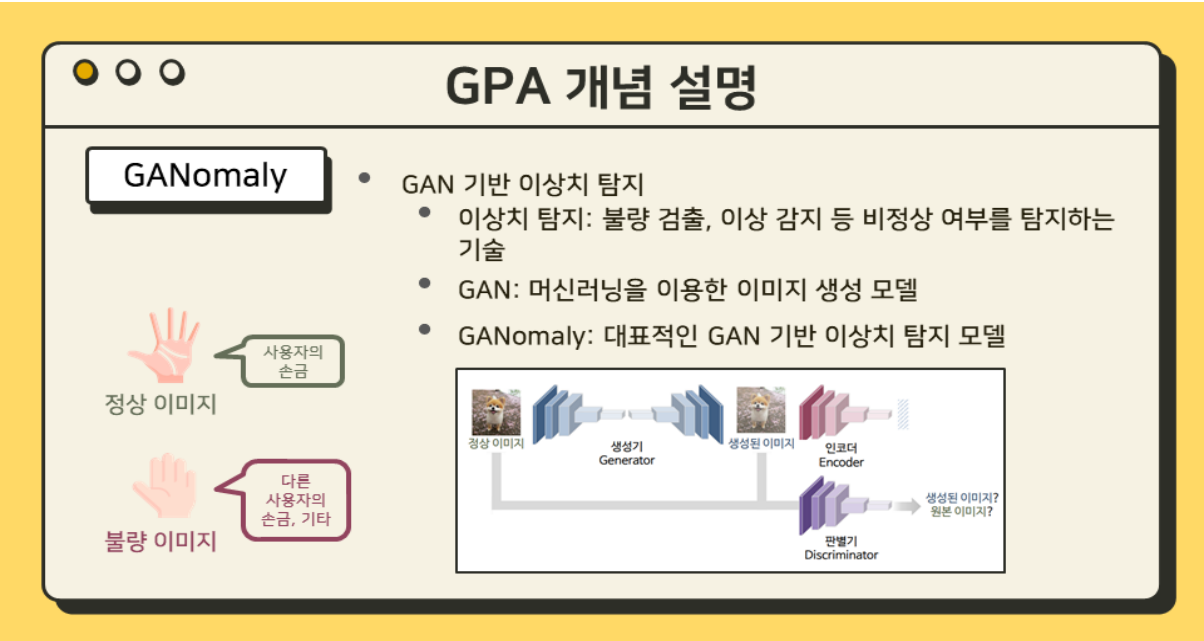


GPA 서비스에서 사용한 YOLO 모델에 대해 말씀드리겠습니다.

YOLO 모델은 객체 검출 문제에서 매우 높은 성능을 보이는 딥 러닝 모델입니다.

입력 이미지가 손이 아닌 손금이 되려면 객체 검출이 사전에 필요합니다.

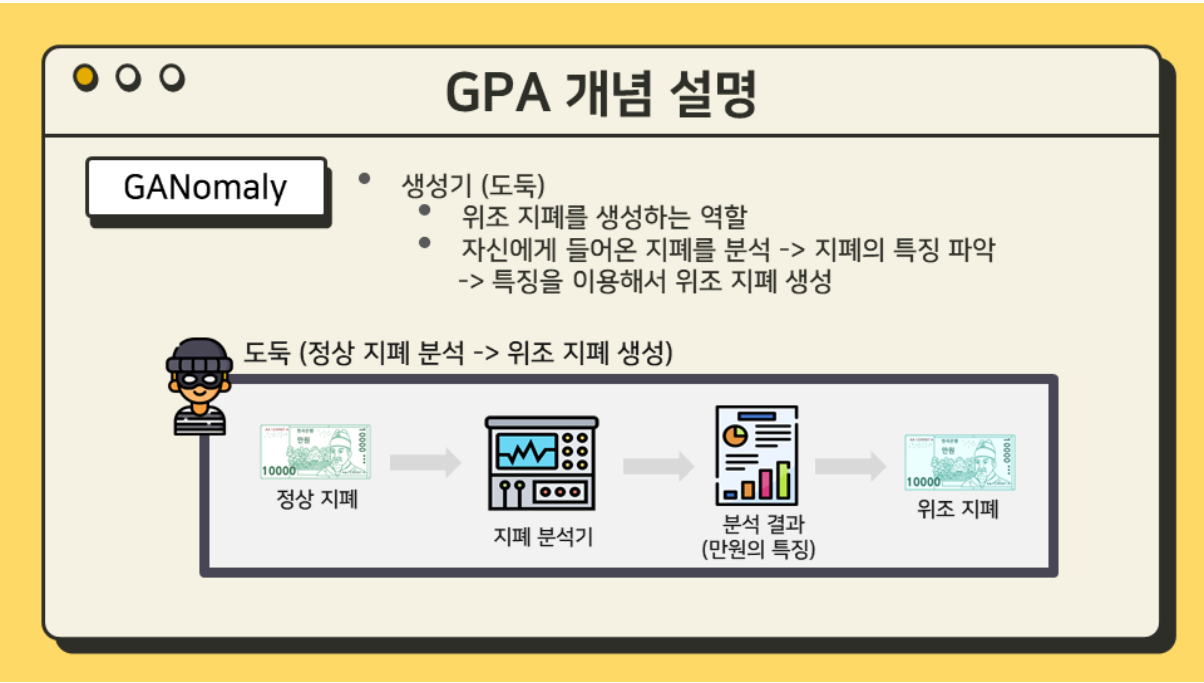
그래서 손에서 손금 영역을 잘 검출하도록 이 모델을 이용하여 학습할 필요성이 있습니다.



또한 GAN 기반 이상치 탐지기술인 GANomaly를 사용했습니다.

'이상치 탐지'란 불량 검출, 이상 감지 등 비정상 여부를 탐지하는 기술을 뜻하며 'GAN'은 머신러닝을 이용한 이미지 생성 모델을 의미합니다.

GANomaly 모델은 아래 그림과 같이 생성기, 인코더, 판별기로 이루어져 있습니다.

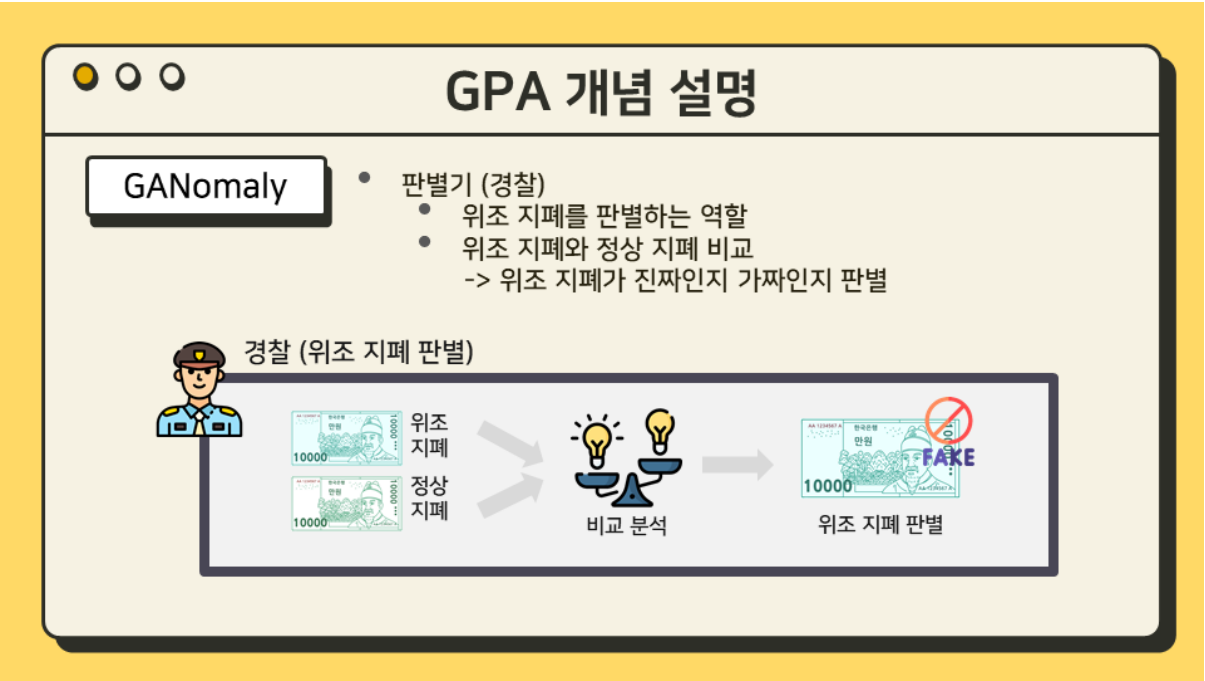


GANomaly를 좀 더 자세히 설명하기 위해 예시를 하나 들어보겠습니다.

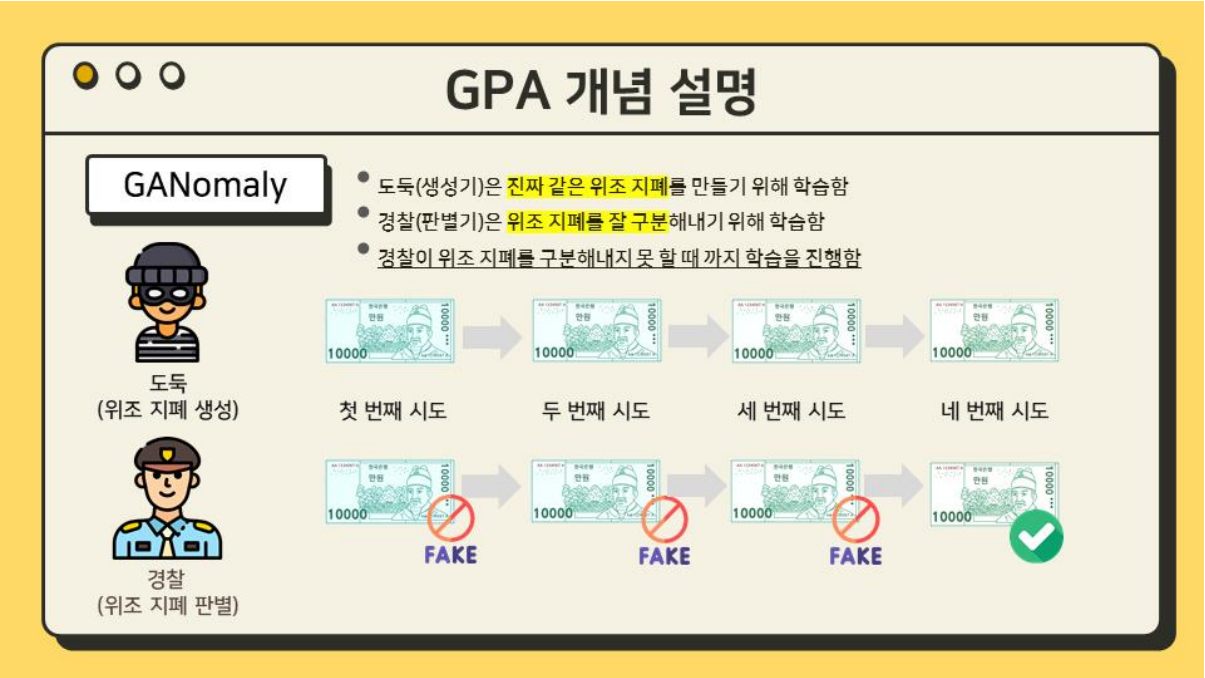
GANomaly에서 사용되는 생성기는 위조 지폐를 생성하는 도둑의 역할을 하게 됩니다.

도둑은 자신에게 들어온 지폐를 분석하고 지폐의 특징을 파악합니다.

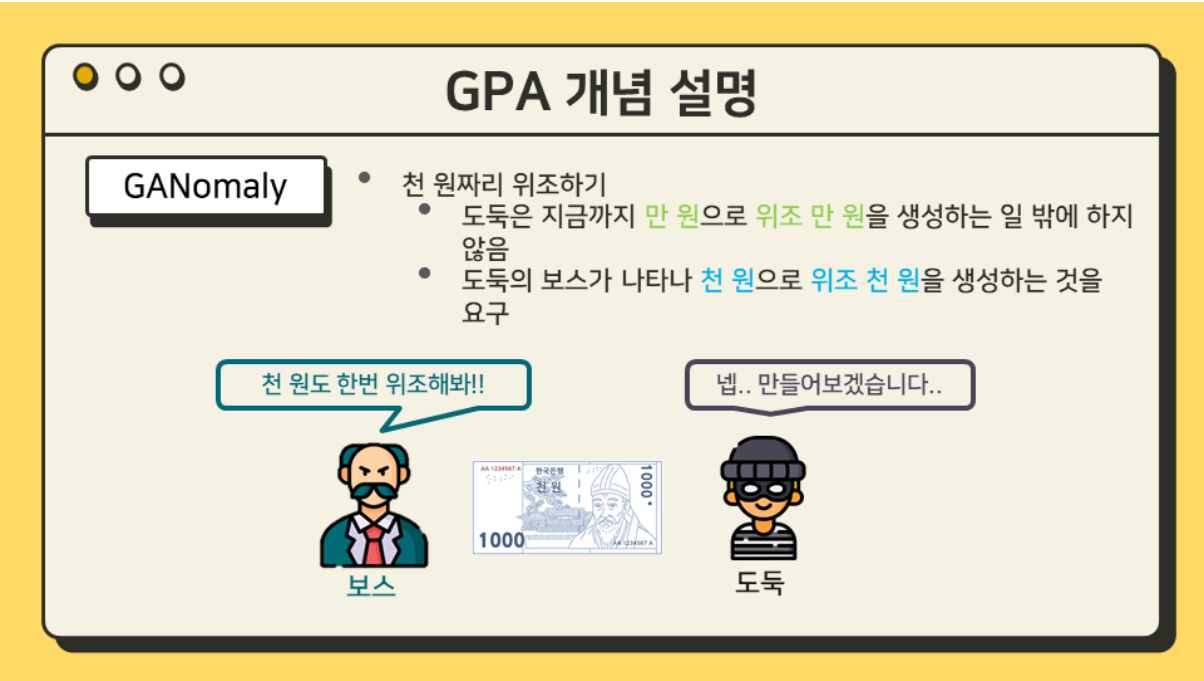
그리고 파악한 특징을 이용해서 위조 지폐를 생성하게 됩니다.



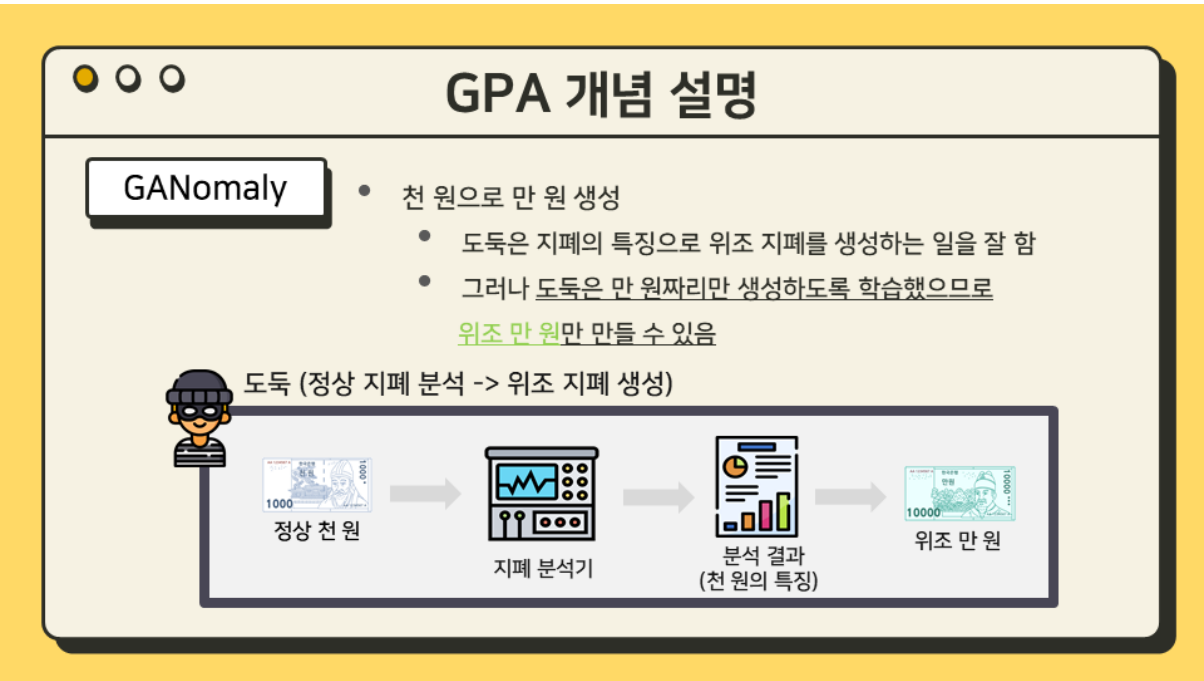
GANomaly에서 사용되는 판별기는 지폐가 진짜인지 가짜인지 판별하는 경찰의 역할을 하게 됩니다. 즉, 경찰은 위조지폐와 정상 지폐를 비교 분석하여 위조 지폐를 판별합니다.



도둑은 진짜 같은 위조 지폐를 만들기 위해 학습하고, 경찰은 위조 지폐를 잘 구분해내기 위해 학습을 진행합니다. 이 둘은 경찰이 위조 지폐를 구분해내지 못할 때까지 학습을 진행하게 됩니다.

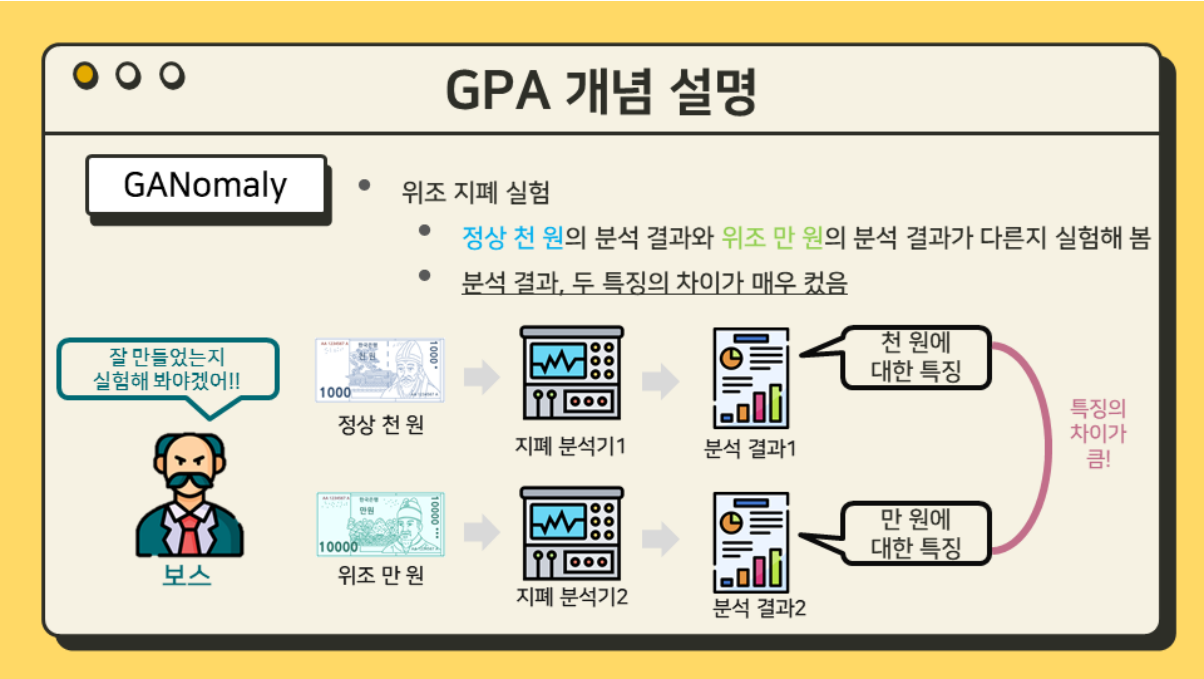


이 때 만 원만 위조할 수 있었던 도둑에게 천 원을 위조하라는 보스의 요구가 있다면 어떻게 될까요?



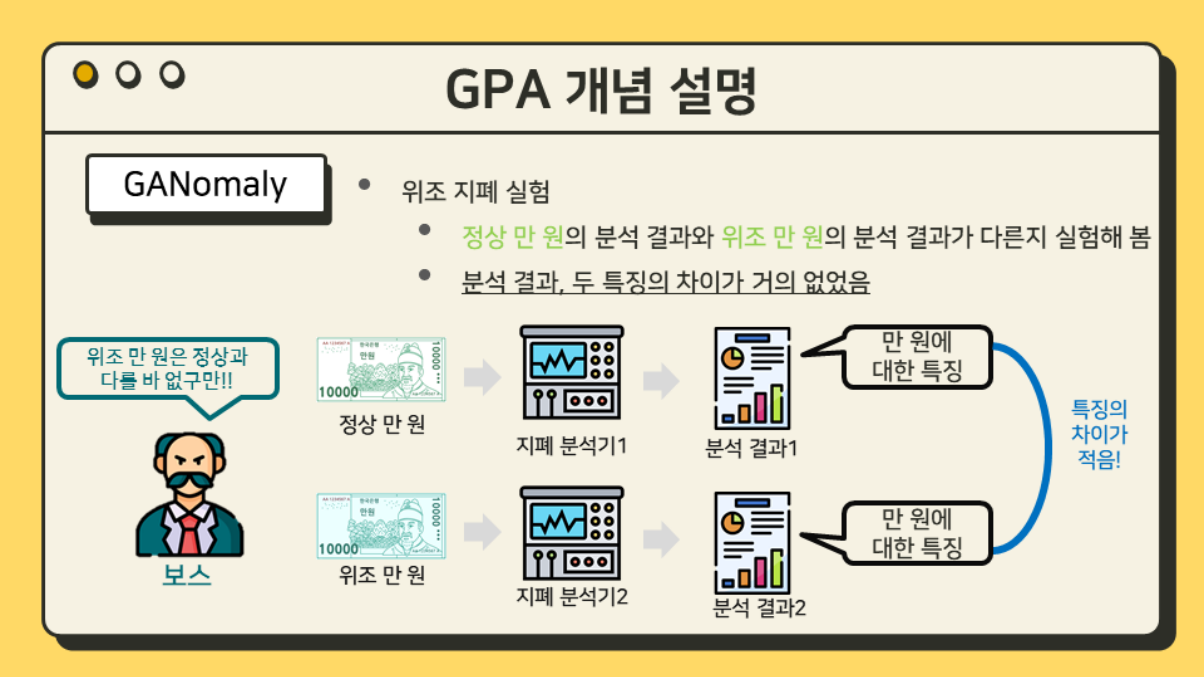
도둑은 지폐의 특징을 이용해서 위조 만원을 생성하는 일은 잘합니다. 하지만
위조 만 원 지폐만 생성하도록 학습을 했으므로 정상 지폐 천원을 위조 만원으로 만들게 됩니다.

보스는 천 원으로 위조 만 원을 생성해낸 도둑을 당연히 믿지 못합니다.



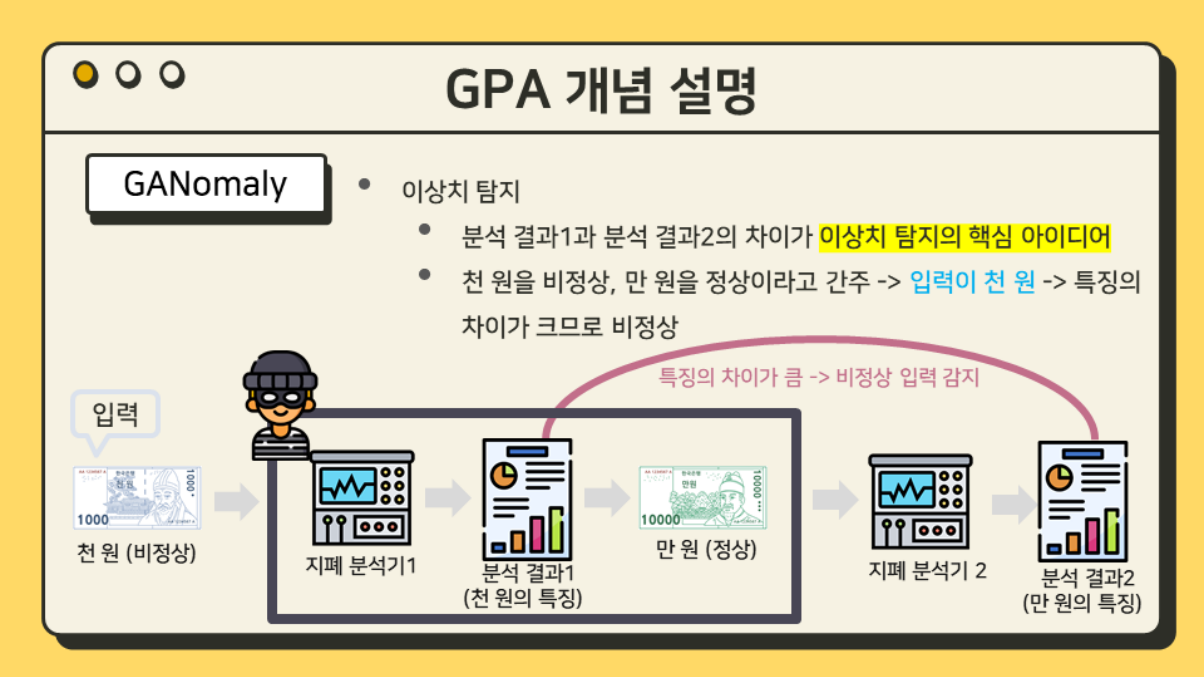
따라서 보스는 도둑이 위조 지폐를 잘 만들었는지 확인하기 위해 정상 천원과 위조된 만원을 지폐 분석기에 넣어 차이점을 알아보는 실험을 해보았습니다.

분석 결과, 두 지폐의 특징 차이가 매우 크게 나왔습니다.



이번에는 정상 만 원과 위조 만 원을 지폐 분석기에 넣어 차이점을 알아보는 실험을 해보았습니다.

분석 결과, 두 지폐의 특징 차이가 거의 없습니다.



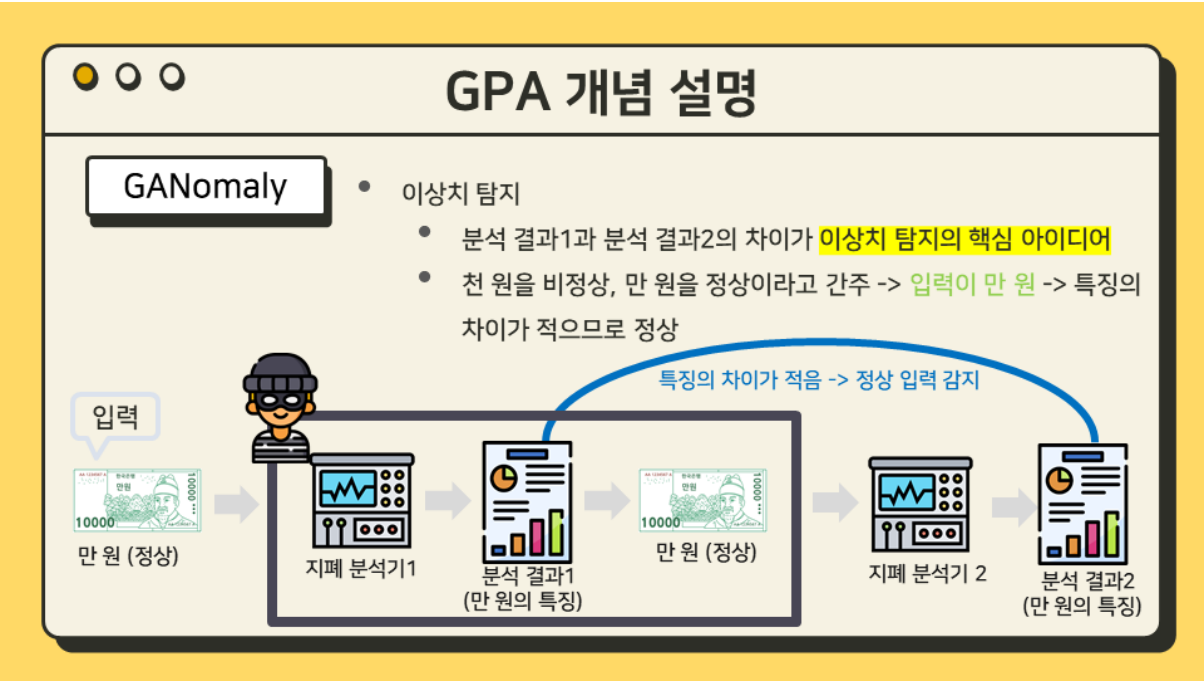
분석 결과1과 분석 결과2의 차이가 이상치 탐지의 핵심 아이디어입니다.

천 원을 비정상, 만 원을 정상이라고 간주하겠습니다.

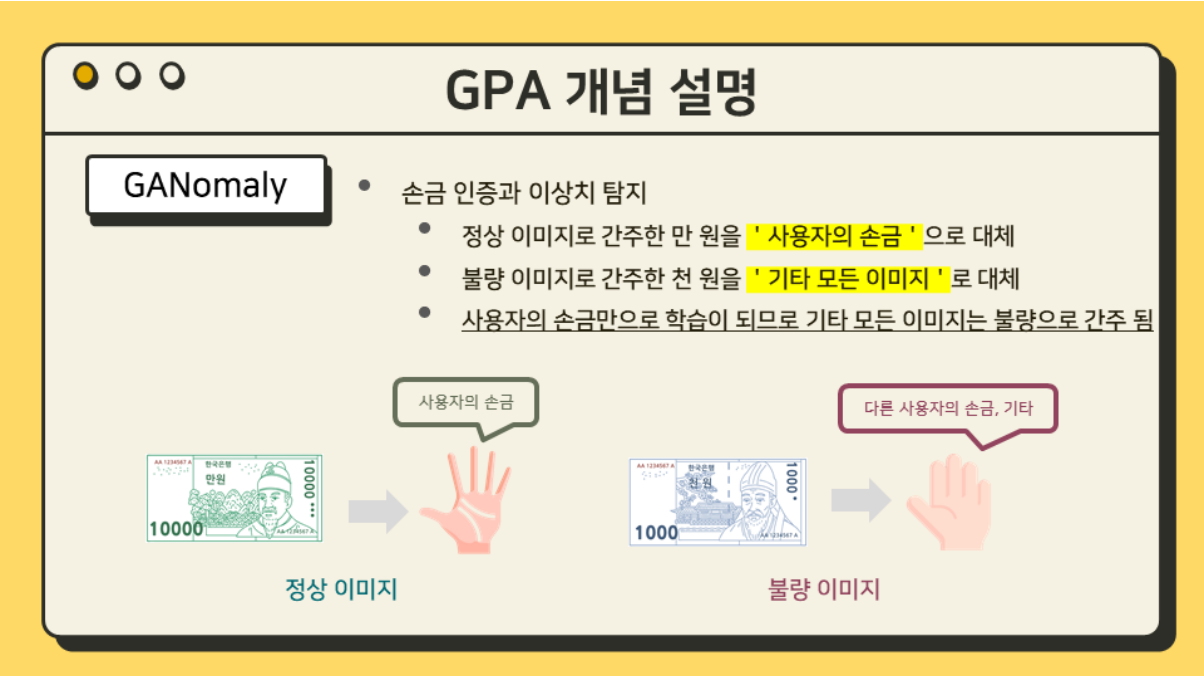
모델의 입력에 비정상인 천 원이 들어오면 생성자인 도둑에 의해 만 원이 생성되게 됩니다.

생성된 만원을 지폐 분석기2에 넣게 되면 분석 결과1과 분석 결과2의 차이는 크게 발생합니다.

따라서 비정상인 1,000원이 입력으로 들어왔다고 예측할 수 있습니다.

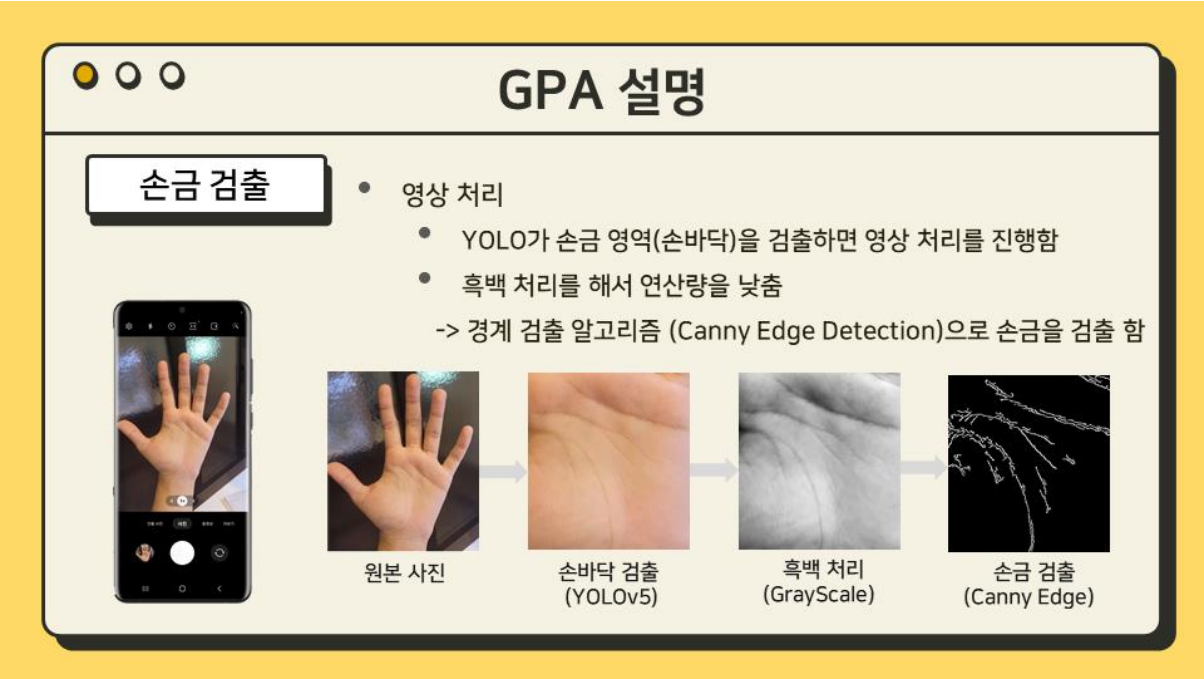


이번에는 모델의 입력으로 정상인 만 원을 넣어보겠습니다.
그럼 생성자인 도둑에 의해 만 원이 생성되게 됩니다.
생성된 만원을 지폐 분석기2에 넣게 되면 분석 결과1과 분석 결과2의 차이는 적게 발생합니다.
따라서 정상인 10,000원이 입력으로 들어왔다고 예측할 수 있습니다.



앞에서 살펴본 이상치 탐지가 손금 인증에 적용되면 다음과 같습니다.
정상 이미지로 간주한 만 원은 '사용자의 손금' 으로 대체되고
불량 이미지로 간주한 천 원은 '기타 모든 이미지'로 대체됩니다.
사용자의 손금만으로 학습이 되므로 기타 다른 모든 이미지는 불량으로 간주됩니다.

이제 저희의 GPA에 대해 말씀드리겠습니다.

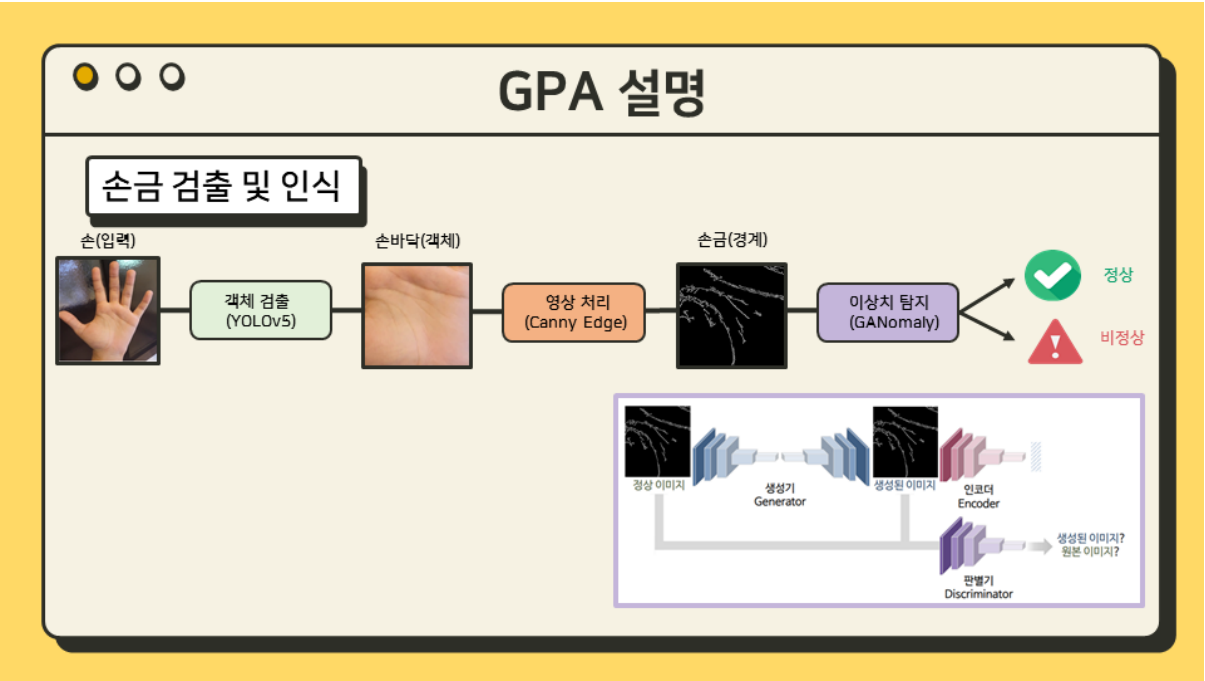


손금 검출을 하는 Task부터 말씀드리겠습니다.

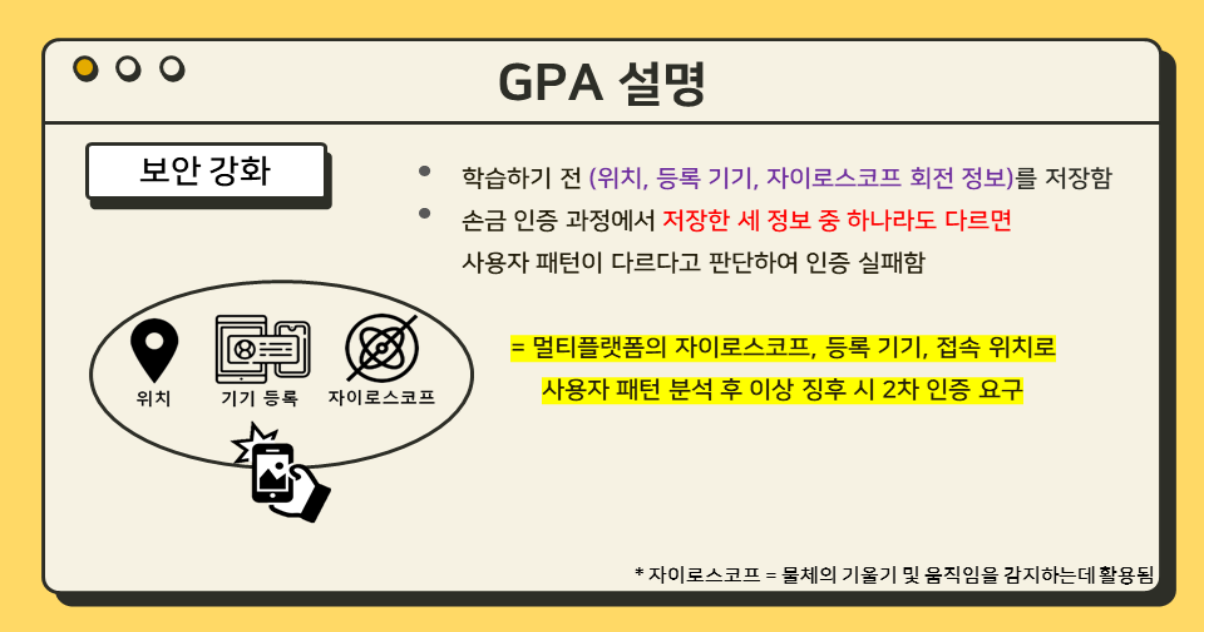
먼저 사용자가 카메라로 손을 찍습니다. 그럼 YOLO 모델을 이용해서 손금 영역인 손바닥을 검출할 수 있습니다.

이후 흑백 처리를 통해 연산을 낮추어 인식이 좀 더 빨리 될 수 있도록 하였습니다.

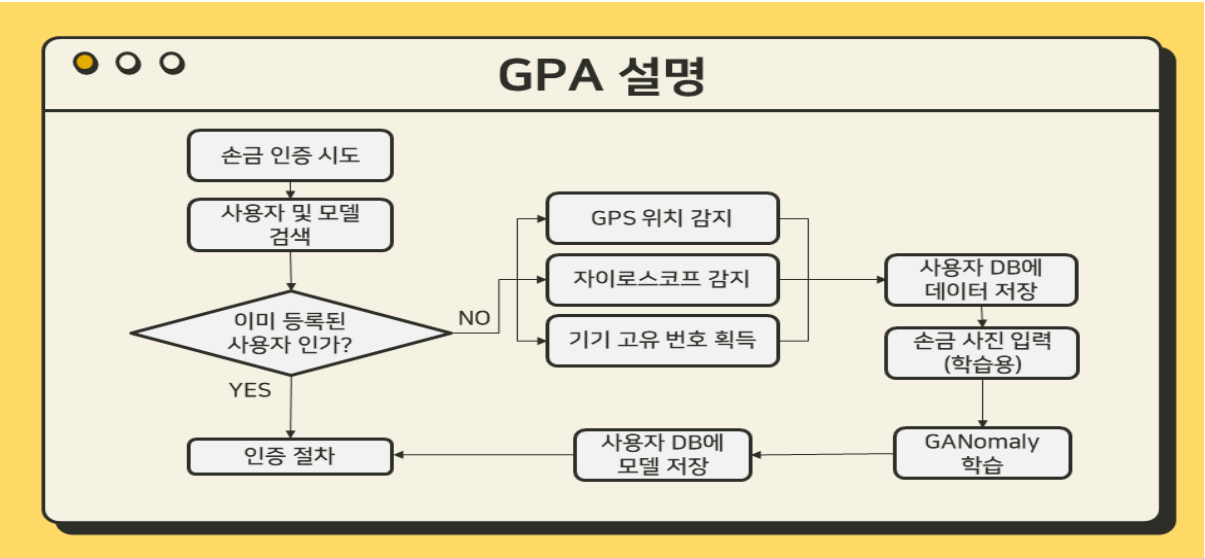
마지막으로 경계 검출 알고리즘 (Canny Edge Detection)을 이용하여 손금을 검출합니다.



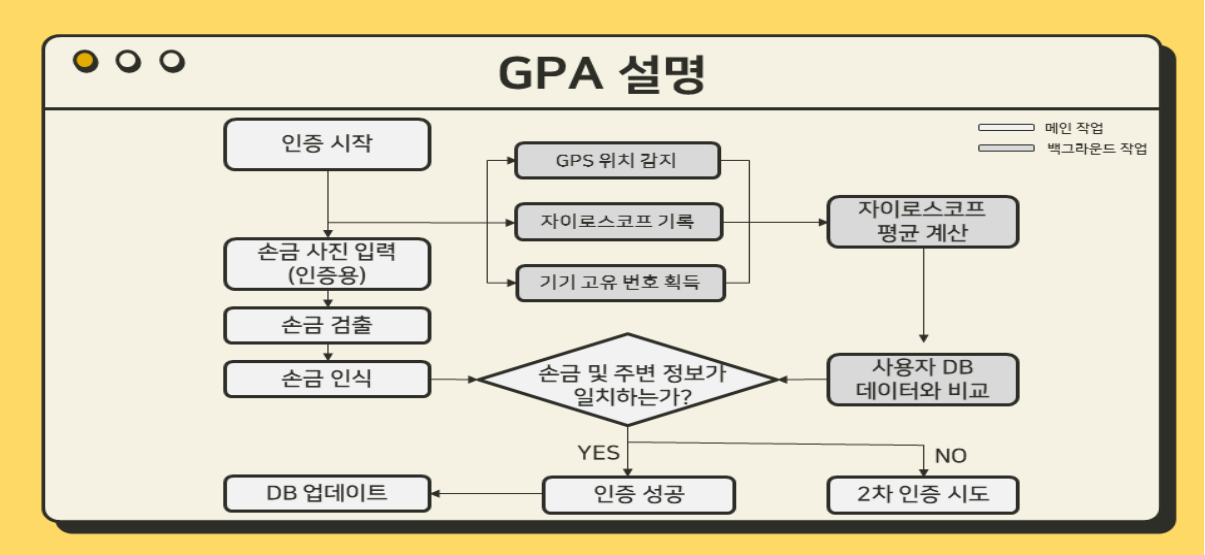
이렇게 객체 검출과 영상 처리가 끝나면 앞서 소개해드린 GANomaly 모델을 이용해서 정상 손금인지 비정상 손금인지를 판별하게 됩니다.



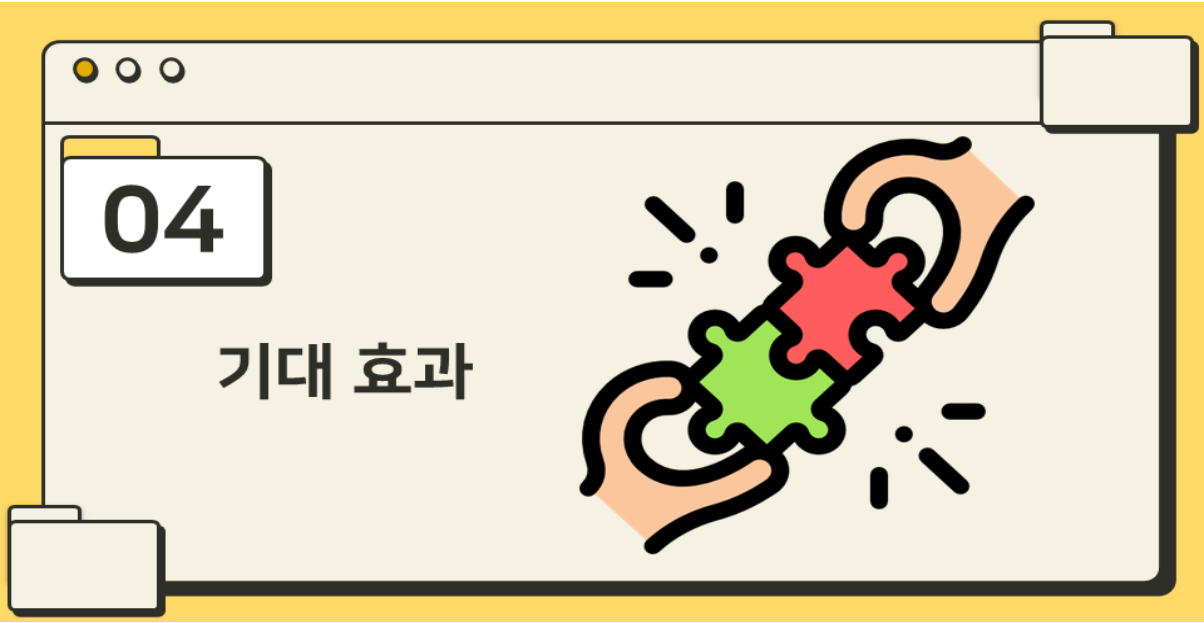
또한 GPA의 보안을 강화하기 위해 학습하기 전,
위치, 등록 기기, 자이로스코프 회전 정보를 저장합니다.
이 때, 자이로스코프는 물체의 기울기 및 움직임을 감지하는데 활용합니다.
따라서 사용자가 인증을 하는 동안 스마트폰 기울기 정보를 저장합니다.
이후 손금 인증 과정에서 저장한 세 정보 중 사용자패턴과 하나라도 다르면 인증이 실패하게 되며 2차인증을 요구합니다.



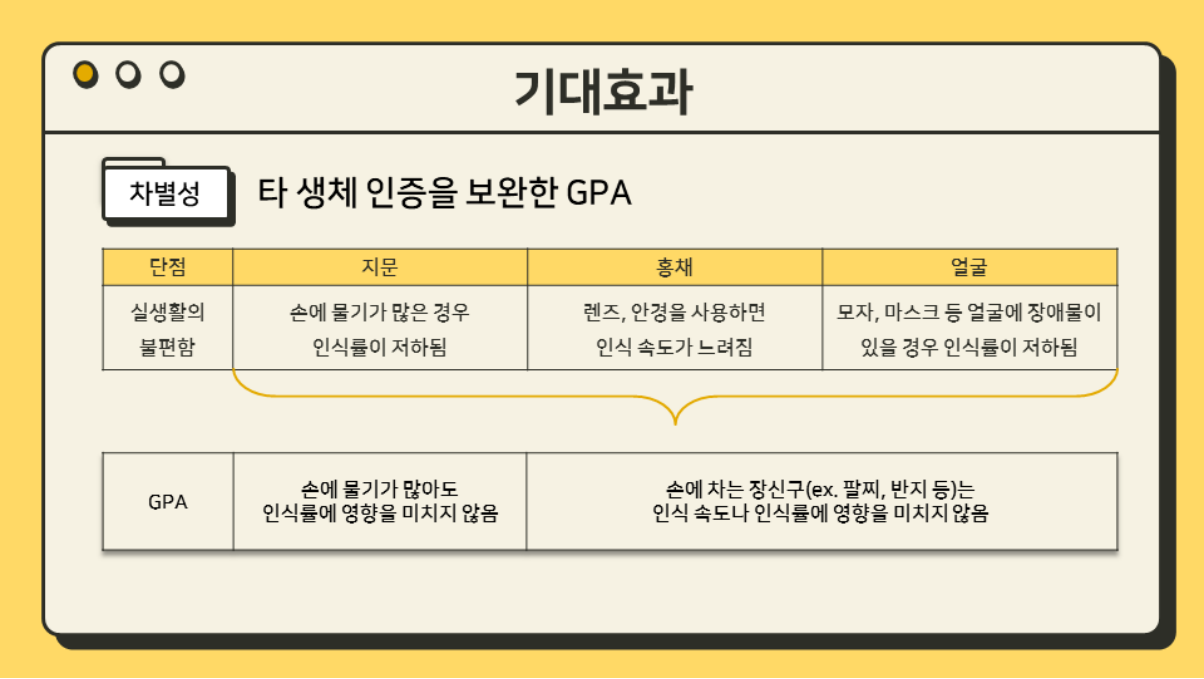
다음은 저희 서비스의 동작 과정에 대해 말씀드리겠습니다.
손금 인증이 시작되면 사용자 및 모델을 검색합니다.
이 때, 데이터베이스에 이미 등록된 사용자인지를 판단합니다.
만약 등록된 사용자가 아니라면 보조 인증을 위해 GPS 위치, 자이로스코프, 기기고유 번호 정보를 사용자 데이터베이스에 저장합니다.
이후 학습을 위한 손금 사진을 입력하고 GANomaly 학습을 진행합니다.
그리고 사용자 데이터베이스에 모델이 저장된 후에는 인증을 진행할 수 있습니다.
만약 이미 등록된 사용자라면 바로 인증 절차로 넘어가게 됩니다.



인증이 시작되면 백그라운드 작업에서 보조 인증이 수행됩니다.
사용자가 메인 작업에서 손금 인증을 하는 동안, GPS 위치, 자이로스코프 정보, 기기 정보를 확인하는 것입니다.
이후 손금 및 주변 정보가 일치하는지 확인을 해서 만약 모두 일치한다면 인증이 성공되고 일치하지 않다면 2차 인증을 시도합니다.
인증이 성공되면 데이터베이스를 업데이트해서 사용자의 최신 패턴을 기록합니다.



다음은 기대효과입니다.



GPA는 타 생체 인증을 보완한 차별성을 가지고 있습니다.

현재 다른 생체인증들은 실생활에서의 불편한 점들을 찾아볼 수 있습니다.

지문 인증의 경우 손에 물기가 많다면 인식률이 저하되며, 홍채 인증의 경우 렌즈나 안경을 사용하면 인식 속도가 느려집니다.

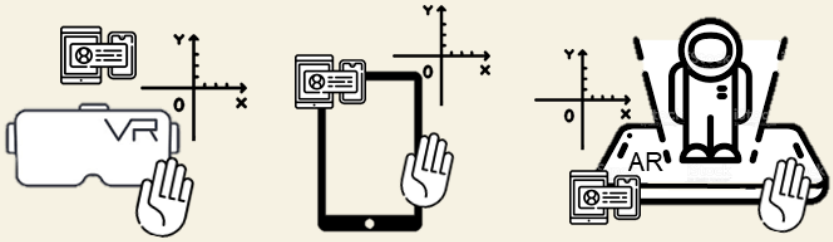
얼굴인증을 하는 경우에는 모자, 마스크 등 얼굴에 장애물이 있을 경우 인식률이 저하되는 불편함이 있습니다.

하지만 GPA는 손에 물기가 많아도 인식률에 영향을 미치지 않으며,

손에 차는 팔찌, 반지와 같은 장신구는 인식 속도나 인식률에 영향을 미치지 않습니다.

기대효과

범용성 금융 메타버스 인증을 기기 제약 없이 활용 가능

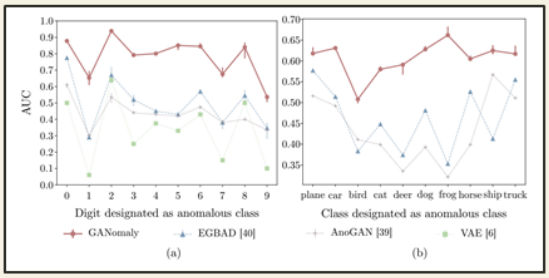


- 카메라가 내장되어 있는 모든 스마트기기(ex. 스마트폰, VR기기)에서 인증 서비스 사용 가능

두 번째로, 금융 메타버스 인증을 기기 제약 없이 활용 가능합니다.
카메라만 내장되어 있다면 모든 스마트기기에서 인증 서비스를 사용할 수 있습니다.

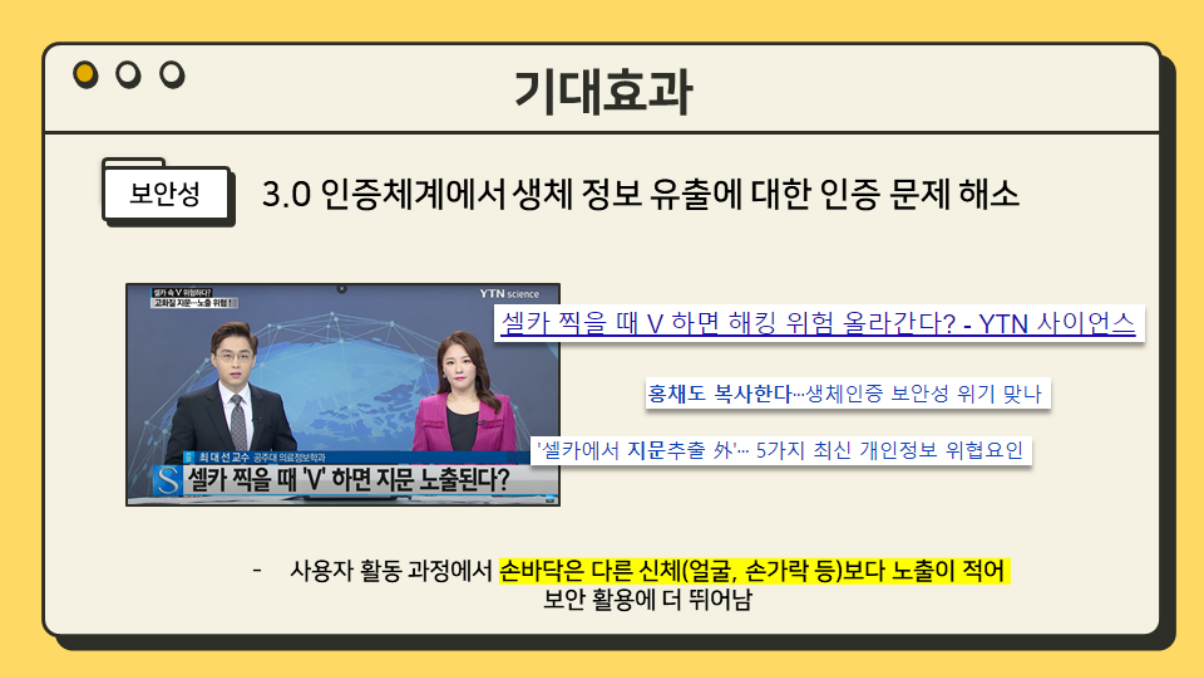
기대효과

보안성 GAN의 알고리즘으로 높은 정확도



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

세 번째로, 저희가 사용하는 GAN은 이상치 탐지를 하는 기존 알고리즘보다 훨씬 높은 정확도를 보이고 있습니다. 따라서 손금 인증에도 안정적으로 활용될 수 있습니다.



네 번째로, 생체 정보 유출에 대한 인증 문제를 해소합니다.
생활 활동 과정에서 손바닥은 얼굴, 손가락과 같은 다른 신체보다 노출이 적어 보안 활용에 더 뛰어나다고 말씀드릴 수 있습니다.

다섯 번째로, 위치-기기-회전 정보를 보조 인증으로 사용하였기 때문에 보안성이 강화되었습니다.
또한 사용자 모르게 백그라운드 환경에서 감지하는 것이기 때문에 편리하다고 말씀드릴 수 있습니다

기대효과

보안성 금융 메타버스 인증에 대한 신뢰성 향상

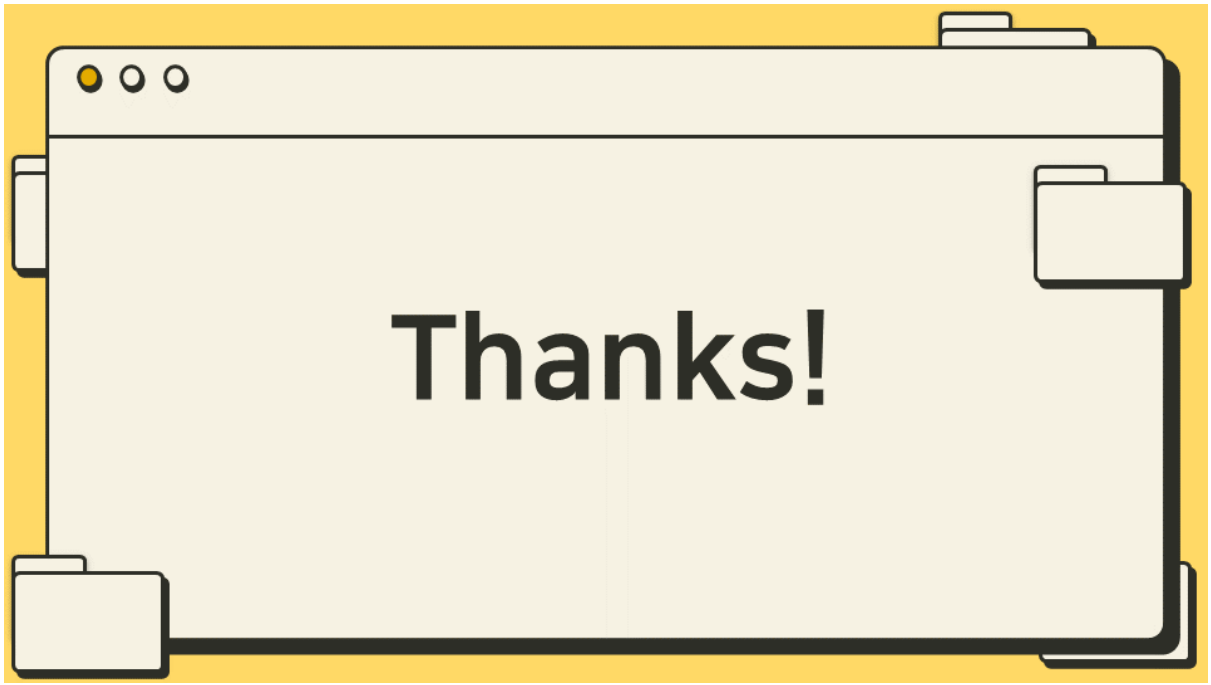
- 금융 메타버스에서 사용할 수 있는 GPA을 제시함으로써 인증으로 인가 되지 않는 사람을 걸러내어 신뢰가 높은 금융 메타버스로 자리 매김할 수 있음

마지막으로 저희 GPA를 제시함으로써, 인가되지 않는 사람을 걸러내어,
신뢰도가 높은 금융 메타버스로 자리 매김을 할 수 있습니다.

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

참고문헌은 다음과 같습니다.



이상으로 발표를 마치겠습니다. 감사합니다.

질문 사항이 있다면 받도록 하겠습니다.

★**기존에 제시되었던 손금 인증과 다른 점이 뭐냐 ?**

: 정맥 인증을 이용하는 손금 인증이 있는 것으로 알고 있습니다. 이 방식은 정밀한 센서를 이용하므로 저희 방식보다 더 보안성이 좋다고 말씀드릴 수 있습니다. 그러나 저희 손금 인증은 카메라가 있는 모든 스마트 기기에서 사용될 수 있으므로 범용성 면에서는 저희 방식이 더 좋다고 생각합니다.

★**생체 인증으로 금융 메타버스에서 어떻게 활용할 수 있는가?**

: 입금 . 송금, 결제 등의 금융 서비스를 진행할 때 활용할 수 있습니다.

★**실제 손바닥이 아닌 손바닥 사진만으로 인증이 되는가? (page.35)**

-그렇다. 컴퓨터는 2D 영상을 보고 처리하는 것이기 때문에 실제나 사진이나 처리하는 데 차이가 없다. 그러나 현재 우리가 사용하고 있는 얼굴 인식도 마찬가지이다. 그래서 얼마나 노출이 덜 되는지가 더 중요하다고 생각했고, 상대적으로 노출이 적은 손바닥을 택하였다.

-얼굴 인식의 경우 sns나 포털 검색을 통해 쉽게 도용당할 수 있다. 하지만 손바닥의 경우 손바닥이 정확하게 나와있는 사진은 상대적으로 구하기가 힘들기 때문에 도용 가능성이 낮다.

메타버스 인증에 생체 인증으로 해야하는 이유는 무엇인가?

: 앞서 말씀드렸듯이 아바타 인증을 이용하는 방식이 적용되고 있습니다.
이러한 아바타 인증은 메타버스 내부에서만 적용되기 때문에, 누군가 사용자의 계정을 탈 취하면 해당 사용자로 위장해 악의적인 활동을 할 수 있습니다.

그리고 모든 스마트기기에서 카메라를 탑재하고 있기 때문에 사용성이 좋다고 생각하였습니다.

-카메라 화질이 손금인증을 할 수 없을정도로 안좋다면 ?

: 현재 사용자가 사용하는 대부분의 핸드폰은 준수한 카메라 성능을 가지고 있기 때문에 문제 없을 것이라고 생각합니다.

AUC 가 무엇인가? (page.34)

분류 문제를 푸는 머신러닝 모델의 평가 지표 중 하나이다. AUC 가 높다는 것은 기계가 분류를 잘했다는 의미가 되므로 정확도가 높다고 표현할 수 있다.

우리가 제시한 모델은 총 10 개의 클래스(숫자 0~9)에 대한 AUC 를 나타내었고 그 중 최고 AUC 는 95 였다. (중간 값은 80 정도) 다만 GPA 에서는 클래스를 한 개(손금)만 사용하므로 더 학습 난이도가 적어 성능이 더 오를 것으로 예상한다.

학습은 어떤 방식으로 진행되는가? (page.29)

우리가 지문 인식을 사용하기 위해 지문 등록을 할 때는 여러 방향으로 많이 등록을 해야한다. 따라서 손금 등록을 할 때도 사용자가 어떤 각도를 취할지 모르므로 여러 각도에 대한 손 데이터를 취득할 예정이다. 이 과정은 사용자마다 비디오를 통해 녹화를 하고 프레임을 쪼개서 학습 이미지로 구축하면 될 것이다. 또한 사용자의 손이 아닌 모든 이미지는 불량으로 간주해야 되므로, 사용자마다 개별 학습을 해서 모델을 한 개씩 구축하는 것으로 구상하였다.

(학습 시간은?: 논문에서 한 데이터 셋에 대해 25 회 정도만 반복해서 학습하였으므로 다른 Task 에 비해 매우 짧게 학습했다고 말할 수 있다. GPU 에 따라 다르겠지만 평균적으로 3 분 이내일 것으로 예측된다.)

DB 업데이트는 왜 진행되는가? (page.30)

보조 정보로 사용되는 자이로스코프 정보, 즉 회전 정보는 최대한 많은 데이터를 수집해야 사용자의 패턴을 찾을 수 있을 것이라 생각하였다. 따라서 초기에 등록을 할 때 뿐 만아니라 인증을 하는 과정에서 매번 데이터를 수집해서 DB 를 업데이트하는 것으로 구상하였다.