

# 1 page Term-project topic submission Assignment

📅 날짜	@2025년 5월 7일
⚙️ 상태	완료

## Term-project topic submission

과제 제출 시작

마감 월요일 기준 오후 11:59    배점 5    제출물 유형 파일 업로드  
이용 가능 5월 6일 오전 12:00-5월 12일 오후 11:59 7일

1 page term-project topic submission

1. **문제 설정** – 문제가 얼마나 타당하고 잘 정의되어 있는가?
2. **동기** – 왜 이 문제를 해결할 가치가 있으며, 왜 제안된 방법으로 접근해야 하는가?
3. **방법** – 접근 방식에 대한 간략한 설명.
4. **결과** – 성능 및 성과.

**제출 요구사항** 5월 11일까지 (방법론 제외) **1페이지 분량의 워드 문서를** 제출해 주세요.  
포함 내용:

- **2~3문장으로 구성된 명확한 문제 설정**
- **동기의 일부 – 특히, 이 문제를 해결하는 것이 왜 중요한지**

[VicLab\\_onepage.docx](#)

- 직접 확인해야 한다는 사람 리소스 문제 + 비대면에 있어서 신분증 도용 문제 +
- Reference
- <https://news.mt.co.kr/mtview.php?no=2024022714025715344>
- <https://news.kbs.co.kr/news/pc/view/view.do?ncd=8030725>

- <https://www.fsc.go.kr/no010101/74052?srchCtgr=&curPage=75&srchKey=&srchText=&srchBeginDt=&srchEndDt=>
- Reference - 디지털 취약계층
  - <https://www.yna.co.kr/view/AKR20241122137500004>
  - [https://www.khan.co.kr/article/201411232147195/?utm\\_source=livere&utm\\_medium=social\\_share](https://www.khan.co.kr/article/201411232147195/?utm_source=livere&utm_medium=social_share)

비대면 인증이 확산되면서 신분증 도용을 통한 부정 사용 사례가 증가하고 있지만, 이를 막기 위해 사람의 눈으로 직접 확인하는 방식은 시간과 인력이 많이 소모됩니다. 이러한 수동 검증 방식은 대규모 사용자 대응에 한계가 있으며, 동시에 인증 정확성과 보안성을 확보하기 어렵습니다.

## 인공지능을 활용한 주민등록증 본인 판별 시스템

재윤) 최근 개인정보 유출과 기술 악용으로 인해 타인의 명의를 도용한 금융 사기가 급증하고 있으며, 기존의 신분증 사진만으로는 정확한 본인 확인이 어려워 보다 정밀한 인증 방식이 요구되고 있습니다. 특히 고령자나 디지털 취약계층은 사기의 주요 대상이 되기 쉬워 보안 강화가 시급한 상황입니다. 기존의 수동 본인 확인 방식은 시간과 비용이 많이 들어 AI 기반 얼굴 비교 기술을 활용한 자동 인증 시스템이 필요합니다. 이 기술은 인증 정확도와 속도를 높이고 운영 효율성까지 개선할 수 있어, 금융사기 예방과 디지털 소외계층의 접근성 향상 측면에서 매우 중요한 해결책이 됩니다.

<정유현>

문제 설정 version 1)

**최근 신분증 도용 및 비대면 금융 사기가 증가하면서, 신분증 사진만으로는 본인 여부를 판별하기에 한계가 드러나고 있습니다.** 본 프로젝트는 신분증에서 얼굴을 자동으로 탐지하고, 사용자의 실시간 얼굴 영상과의 유사도를 정량적으로 비교하며, 영상 속 인물이 실제 사람인지까지 검증하는 기술을 결합하여 **AI 기반의 신뢰도 높은 본인 인증 시스템**을 구현하는 것을 목표로 합니다.

문제 설정

현재 얼굴 이미지와 주민등록증에 포함된 얼굴 사진 간의 유사도를 판단하여 본인 여부를 확인하는 기술은 점점 중요해지고 있습니다. 이 프로젝트는 두 이미지 간의 특징을 비교함으로써 실제 사용자가 본인인지 확인하는 문제를 다룹니다.

## 동기

최근 비대면 인증 시스템은 다양한 생활 영역에서 필수적으로 사용되고 있으며, 이는 신분증을 기반으로 한 본인 확인 절차와 밀접하게 연결되어 있습니다. 그러나 단순히 신분증 사진을 제출하고 이를 수동으로 비교하거나 OCR 정보만을 확인하는 방식은 위·변조된 이미지나 타인의 신분증을 이용한 대리 인증과 같은 보안 위협에 취약합니다. 이러한 위험은 특히 금융 서비스에서의 계좌 개설, 대출 신청, 공공기관의 행정 서비스 접근, 그리고 온라인에서의 실명 인증과 같은 민감한 분야에서 심각한 문제를 야기할 수 있습니다.

본 프로젝트는 이러한 보안 취약점을 해결하고 인증 시스템의 신뢰도를 높이기 위한 기술적 해법으로, 사용자의 실제 얼굴 이미지와 신분증에 포함된 얼굴 사진 간의 정교한 유사도 비교를 통해 본인 여부를 자동으로 판별하는 시스템을 제안합니다. 이 기술은 대리 인증을 차단하고, 신분증 위조 여부를 간접적으로 판단할 수 있는 수단이 되며, 나아가 전체 비대면 인증 과정의 보안성을 크게 향상시킬 수 있습니다.

더불어, 본인 확인의 정확성과 신속성을 동시에 확보할 수 있는 이 시스템은 사용자 편의성을 저해하지 않으면서도 고신뢰 인증을 제공할 수 있다는 점에서, 향후 디지털 행정과 전자 금융 서비스, 원격 의료 등 다양한 분야로의 확장 가능성도 높습니다.

김민종

### Problem Setting:

금융기관에서는 사용자가 제출한 신분증 사진만으로는 본인 여부를 정확히 판단하기 어렵습니다. 특히 비대면 상황에서 신분증을 도용한 대출 신청이나 계정 개설 등의 사기 사례가 증가하고 있어, 신분증 사진과 실시간 얼굴 영상을 비교해 신원을 정확히 검증할 수 있는 기술이 필요합니다.

### Motivation:

최근 고령자나 디지털 취약 계층을 대상으로 한 **신분증 도용 및 사기 피해**가 증가하고 있습니다. 현재 일부 금융기관에서는 전화 통화 후 고객이 **카메라 앞에 얼굴을 비추면 직원이 수작업으로 대조**하는 방식으로 본인 여부를 확인하고 있지만, 이 방식은 **시간이 오래 걸리고 인건비가 높으며 오판 가능성도** 존재합니다.

본 프로젝트는 **신분증 사진과 실시간 얼굴 영상을 자동 매칭**하여 본인 여부를 빠르고 정확하게 판단할 수 있는 **AI 기반 자동 인증 시스템**을 구현하고자 합니다. 이를 통해:

- **보안성을 향상**시켜 도용 및 사기 위험을 낮추고,

- 업무 자동화 및 비용 절감을 달성하며,
- KYC/AML 규제 준수를 효과적으로 지원할 수 있습니다.

또한, 이 기술은 모바일 뱅킹과 같은 비대면 금융 서비스의 기반 기술로 활용될 수 있으며, 고객 온보딩, 공유경제, 디지털 자산 계좌 개설, 온라인 시험 등 다양한 분야에 확장이 가능합니다.

김형래

Motivation:OT

#### ▼ 문제 설명

보안 문제 관련 현황 자료:

[https://www.koreatimenews.com/news/article.html?no=749250&utm\\_source=chatgpt.com](https://www.koreatimenews.com/news/article.html?no=749250&utm_source=chatgpt.com)

—> 개인정보위, 2024년 개인정보 유출 신고 동향 분석결과

<https://www.prnewswire.com/apac/news-releases/sumsub-apac-sees-121-increase-in-identity-fraud-with-deepfakes-becoming-a-growing-threat-302312092.html>

—> 딥페이크 기반 금융사기 증가 관련 뉴스

<https://mobileidworld.com/toss-leads-facial-recognition-adoption-in-south-korean-financial-services/>

→ Toss 얼굴 인식 기술 도입

<https://www.chosun.com/economy/industry-company/2025/04/23/F2ZBUOBEEFA5BO5YPGYSUND3JU>

<한글>

최근 개인정보 유출 사고(예: SKT 유출 사건) 이후, 금융거래에서 타인의 명의로 계정을 만들거나 대출을 신청하는 **사기 피해**가 증가하고 있습니다. 특히 고령자나 정보 취약 계층은 사기 대상을 삼기 쉬워 보안이 더욱 중요합니다. 기존의 ID 카드 사진만으로는 신원 확인이 충분하지 않기 때문에, **실시간 얼굴 영상과의 매칭 기술**이 필요합니다.

또한 현재 신한은행 등 일부 금융기관에서는, 고객이 전화를 통해 본인 확인 요청을 받으면, **카메라 앞에서 얼굴을 보여주고 직원이 수작업으로 신원을 확인하는 절차**를 진행하고

있습니다.

이 방식은 고객 수가 많을 경우 **시간이 오래 걸리고 인건비가 많이 들며**, 사람에 따라 **오 판 가능성**도 존재합니다.

이 프로젝트는 이러한 인증 과정을 **AI 기반 얼굴 인식 기술로 자동화**하여, 고객의 **신분증 사진과 실시간 얼굴 영상**을 비교해 **본인 여부를 즉시 판단**할 수 있도록 합니다.

이를 통해 금융기관은

- **운영 비용을 줄이고,**
- **인증 속도를 높이며,**
- **보안성과 일관성을 동시에 확보**할 수 있습니다.

특히 대규모 고객을 상대하는 은행에서는 **확장성과 효율성 면에서 큰 이점**을 가질 수 있습니다.

## Motivation (동기)

이 프로젝트는 **신분증 사진과 실시간 촬영된 얼굴을 비교**하여 실제 사용자 본인인지 판단하는 시스템입니다.

- 위·변조된 신분증 사용을 차단하고
- 본인의 얼굴이 아니면 즉시 경고 메시지를 출력해 **금융사기 예방**에 도움을 줄 수 있습니다.
- 기술적으로는 얼굴 인식(Face Detection & Verification), 유사도 측정(Cosine Similarity), DeepFace나 FaceNet 기반 모델 등이 활용됩니다.

이 시스템은 특히 비대면 계좌 개설, 대출, 주식 앱 가입 시 **간편하고 강력한 인증 방식**으로 적용될 수 있으며,

고령자나 시력 약자 등 **입력 어려움을 겪는 금융소외계층에게도 유용**합니다.

<영어>



## Problem Setting

Following recent personal data leakage incidents (e.g., the SKT data breach), there has been a growing number of **fraud cases** involving the creation of accounts or loan applications under someone else's name.

This issue is particularly serious for the elderly and digitally vulnerable populations, who are more likely to become targets of fraud.

Since ID card photos alone are no longer sufficient for accurate identity verification, **a matching system using real-time facial video** is increasingly necessary.

In current banking procedures, such as at **Shinhan Bank**, customers are often asked to confirm their identity by speaking on the phone and then showing their face through a camera, which is **manually verified by a human staff member**.

This process is **time-consuming, labor-intensive, and costly**, especially when applied to a large number of customers.

This project aims to **automate the identity verification process** using AI-based facial recognition, allowing the system to compare a customer's **live facial image with their ID photo** in real-time.

By doing so, banks can **significantly reduce operational costs**, minimize human error, and **speed up the verification process**, while maintaining or even enhancing the level of security.

This also ensures **scalability and consistency**, which is difficult to achieve with manual checks.

---

## Motivation

This project proposes a system that **compares the face extracted from an ID card with a real-time facial image** to determine whether the user is truly the account holder.

- It helps **prevent the use of forged or stolen IDs**,
- and can immediately trigger a warning message if the face does not match, assisting in **preventing financial fraud**.
- From a technical perspective, the system utilizes face detection and verification, **similarity measurement** (e.g., Cosine Similarity), and models such as **DeepFace** or **FaceNet**.

This system can be applied as a **simple yet secure authentication method** for non-face-to-face account openings, loan applications, or stock trading apps.

It is also highly beneficial for the **financially marginalized**, including **older adults or those with visual impairments**, who may struggle with manual input processes.

---

워드 기준 2~3문장

<한국어>

### ◆ 문제 설정 (Problem Setting)

최근 SKT 개인정보 유출 사건 등으로 인해, 타인의 명의를 도용해 계좌를 개설하거나 대출을 신청하는 **금융 사기**가 증가하고 있습니다.

기존의 신분증 사진만으로는 정확한 신원 확인이 어려워졌으며,

이를 대체할 **보다 신뢰도 높은 본인 확인 방법**이 절실한 상황입니다.

---

### ◆ 동기 (Motivation)

현재 일부 은행에서는 전화 또는 영상통화를 통해 **직원이 직접 얼굴을 확인하는 방식**으로 본인 여부를 판단하고 있지만, 이 방식은 **시간과 인력이 많이 소모되고 오차 발생 가능성도 존재**합니다.

이에 따라, **신분증의 얼굴 사진과 실시간 촬영된 얼굴 이미지를 AI로 비교하는 자동 본인 인증 시스템**은 운영 비용 절감은 물론, **인증 정확도와 처리 속도**를 동시에 개선할 수 있습니다.

또한, 이 방식은 **입력이 어려운 고령자나 디지털 소외계층**에게도 더 나은 접근성을 제공합니다.

<영어>

### ◆ Problem Setting

Due to recent data breaches in South Korea, such as the SKT incident, financial fraud involving stolen identities—like unauthorized account openings and loan applications—has significantly increased.

Traditional methods that rely solely on ID card photos are no longer sufficient to confirm a user's identity with high accuracy.

This situation demands a more reliable and automated approach to verifying that the person requesting access is indeed the rightful owner of the ID.

---

## ◆ Motivation

Manually verifying facial identity through phone and video calls, as commonly practiced in banks, is labor-intensive, time-consuming, and error-prone.

By implementing AI-based facial verification—matching a live facial image with an ID photo—financial institutions can reduce operational costs, improve efficiency, and enhance security.

This solution is especially beneficial for the elderly and digitally vulnerable individuals, who may struggle with conventional input-based authentication methods.

### ▼ 해결 방법

주민등록증 사진과 실시간 사용자의 얼굴이 일치함을 확인해서 주민등록증 도용을 방지  
본인이 아니면 주민등록증을 활용한 서비스 사용 제한

To prevent the misuse of resident registration cards, the system verifies whether the user's real-time face matches the face on the ID card.

If the user is not the legitimate holder, access to services using the resident registration card will be restricted.

주민등록증 사진을 받고 얼굴 추출

실시간 사용자의 얼굴을 인식해서 주민등록증에서의 사진과 일정 이상 유사도를 보이면  
본인으로 판정

사진으로 인증하는 것을 방지하기 위해 여러 각도에서 완벽하게 동일한 이미지로 판정  
되면 기각처럼 사용자가 실시간으로 얼굴을 촬영하고 있음을 확인

First, the system receives the resident registration card photo and extracts the facial region.

Then, the user's live face is captured through real-time camera input.

If the extracted face from the ID photo and the live face show a similarity above a predefined threshold, the user is authenticated as the legitimate holder.



To prevent fraud using static images (such as holding up a photo to the camera), the system requires the user to move their head in various angles during the live capture.

If the system detects identical images across multiple angles without natural variation, the authentication attempt is rejected, ensuring the user is physically present and interacting in real time.

#### ▼ 구현 방법

1. 주민등록증 얼굴 검출 → RetinaFace 등 활용하여 얼굴 추출
2. 영상에서 선별 프레임 추출 → blur score, pose 기준으로 key-frame 확인 후 추출
3. 사람이 맞는지 확인 여부. → 깊게하려면 깊게 할 수 있고, 단순 frame 흔들림 비교도 가능.
4. ID 사진 - 실시간 얼굴 1:1 매칭 확인 → Arcface 임베딩 코사인 유사도 확인.

#### ▼ 기대 효과 및 효용

##### **보안성 향상**

- 얼굴 인식과 신분증 이미지 분석을 동시에 수행해 **이중 인증**이 가능하며, **도용/사기**의 위험을 줄일 수 있습니다.

##### **비대면 금융 서비스 확대**

- 고객은 **지점 방문 없이 온라인에서 신원 인증**을 완료할 수 있으므로, 모바일 뱅킹, 디지털 자산 계좌 개설 등 비대면 금융 서비스에 필수적인 기반 기술이 됩니다.

##### **업무 효율화 및 비용 절감**

- 신분증 확인 업무를 자동화함으로써 **인건비를 줄이고, 처리 속도를 향상**시켜 전반적인 운영 효율성을 높입니다.

##### **규제 준수 (KYC/AML)**

- 은행과 금융기관은 **KYC(Know Your Customer)** 및 **AML(Anti-Money Laundering)** 요구사항을 충족하기 위해 고객의 신원을 정확히 확인해야 합니다. 이 서비스를 통해 그 기준을 자동화된 방식으로 충족할 수 있습니다.

##### **추가 기대효과**

- **KYC(본인 인증)를 필요로 하는 B2B 시장**은 거의 모든 산업에 걸쳐 있고, 수요가 급성장 중
- **코로나19 이후** 비대면 수요가 폭발, 오프라인 인증 과정을 없애려는 흐름 강세
- **“신뢰성”** 과 **“빠른 전환”** 이 필요한 곳(고객 온보딩, 대여 서비스, 시험 등)에서 필수적인 기술