Student ID Authentication Using Facial Recognition

Nguyễn Bình Thành (Team leader); Đỗ Hùng Cường; Nguyễn Chí Dũng; Cao Hoàng Tùng; Cao Phạm Thành Đạt.

Advisor: Lương Trung Kiên

Abstract: This project investigates the integration of facial recognition technology into the student ID authentication process to enhance both accuracy and security in verifying student identities. The main motivation arises from the urgent need for a fast, precise, and tamper-resistant authentication method in educational settings. Our approach combines traditional student ID scanning with live facial capture, followed by the application of deep learning algorithms to compare and verify the match between the two images. The system was implemented and tested on a diverse dataset of student images, demonstrating high accuracy under various lighting conditions and environments. These results validate the feasibility of applying facial recognition technology for student ID authentication and open up potential applications in areas such as attendance management and access control within campus environments.

Keywords: Facial Recognition; Student ID Authentication; Biometric Authentication; Computer Vision

1. Introduction

In today's context, ensuring security and accurate identity verification in educational institutions is increasingly important. Traditional student IDs, although widely used, are susceptible to forgery or misuse. Therefore, integrating biometric technology—especially facial recognition—into the student identity verification process offers a promising solution to enhance both accuracy and security.

Facial recognition technology has proven effective across various fields, from security to commerce. In educational environments, its application can automate the verification process, reduce errors, and improve overall management efficiency. For instance, research by Ngonadi and Orobor developed a facial recognition service model using deep neural networks and support vector machines to verify student identities, thereby minimizing impersonation during examinations [1].

However, implementing facial recognition systems in educational settings requires careful consideration of accuracy, privacy, and student acceptance. The study by Shi and Jain introduced DocFace+, an automated system that matches ID document

photos with self-portrait images, showcasing the potential for automated identity verification [2].

Based on these studies, this project aims to develop a student ID authentication system that integrates traditional card scanning with live image capture, utilizing deep learning algorithms for comparison and identity verification. The system is designed to provide a fast, accurate, and secure authentication solution in educational environments.

2. Related Works

2.1 Real-Time Face Verification in Controlled Environments

Several studies have demonstrated robust face verification under controlled conditions using combined approaches. For instance, *Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine* [1] proposes a system that leverages deep neural networks alongside SVM to compare ID card images with live face captures. Similarly, *Hệ thống xác minh cá nhân bằng thẻ căn cước và ảnh khuôn mặt* [2] offers a solution based on a similar fusion of biometric data, while *DocFace+: ID Document to Selfie Matching* [14] utilizes deep CNNs to extract and compare features from ID documents and selfie images. These works collectively support the feasibility of real-time face verification in controlled environments, although they note challenges when image quality degrades.

2.2 Mobile and KYC-Based Face Verification Systems

The trend toward mobile authentication and KYC (Know Your Customer) processes has spurred the development of solutions tailored for on-the-go verification. For example, *Xác thực danh tính trên thiết bị di động bằng cách xác minh khuôn mặt và nhận dạng hình ảnh ID* [4] presents a system that integrates face verification with ID image recognition on mobile devices, achieving high accuracy under ideal conditions. Complementing this, *Xác minh khuôn mặt và thẻ ID để KYC* [7] provides a framework specifically designed for KYC processes, while *Identity Authentication on Mobile Devices Using Face Verification and ID Image Recognition* [16] demonstrates the practical application of these technologies. Together, these studies highlight the promise and limitations of mobile-based face verification, especially under varying environmental conditions.

2.3 Multi-Factor and Two-Factor Authentication Approaches

To enhance security, researchers have explored multi-factor authentication methods that incorporate additional biometric elements. For instance, *Nghiên cứu và phát triển hệ thống xác thực khuôn mặt hai yếu tố sử dụng mã F-QR vô hình trên thẻ căn cước bằng laser 1064 nm và camera AI* [8] introduces a two-factor system where an

invisible F-QR code is embedded in the ID card and verified alongside the facial image. In addition, *Nghiên cứu các phương pháp bảo mật tài liệu nhận dạng bằng cách lưu trữ các mẫu sinh trắc học khuôn mặt dưới dạng mã có thể đọc được bằng máy* [17] investigates secure storage and verification of biometric templates using machine-readable codes. Further reinforcing these approaches, the open-source project *Phần mềm sử dụng tính năng phát hiện khuôn mặt dựa trên deep learning và thư viện nhận dạng khuôn mặt* [20] demonstrates practical implementations of deep learning techniques for multi-factor verification. These studies collectively underline the enhanced security benefits—and inherent complexity—of two-factor authentication systems.

2.4 Challenges and Future Directions in Uncontrolled Scenarios

Despite promising results in controlled environments, several works highlight challenges when face verification systems are deployed in uncontrolled or diverse scenarios. For instance, *Face Verification With Challenging Imposters and Diversified Demographics* [18] examines the impact of imposter attacks and demographic diversity on system performance, revealing reduced accuracy in certain populations. In a similar vein, *Nghiên cứu về việc ứng dụng công nghệ nhận dạng khuôn mặt trong quy trình xác minh an ninh sân bay* [19] discusses the application of face recognition technology in airport security, noting that real-world variables such as lighting, pose, and occlusion continue to challenge these systems. Additionally, *Xác thực sinh trắc học khi chuyển trên 10 triệu đồng chỉ bằng ảnh tĩnh* [12] highlights practical issues encountered in financial applications, where even minor deviations in image quality can lead to significant verification errors. Collectively, these studies stress the need for further research into robust algorithms and adaptive preprocessing techniques to improve system performance in diverse, real-world scenarios.

Overall, these grouped studies—from controlled real-time systems and mobile/KYC solutions to multi-factor approaches and challenges in uncontrolled environments—offer a comprehensive view of the current state of face and ID verification research. They provide valuable insights into both the strengths and limitations of existing technologies, guiding future efforts to enhance security and reliability in biometric authentication systems.

3. Data Preparation

This project utilizes a pre-trained InsightFace model for face verification and the ORB (Oriented FAST and Rotated BRIEF) algorithm for ID card detection. Therefore, data preparation does not involve constructing a large training dataset from scratch. Instead, the primary data consists of a single reference image and real-time data collected from a webcam during system operation.

3.1 Reference Image

The reference image serves as a template of a standard Citizen Identification Card (CCCD) used to detect the ID card in the video feed from the webcam. This image is captured using a high-resolution camera with the following specifications:

- Original Size**:** 1280x720 pixels
- Format: JPEG
- Content: A clear ID card layout including a face photo, logo, and textual information

The reference image is crucial for extracting ORB features (keypoints and descriptors) to match against ID cards appearing in the video feed. The preprocessing steps include:

- Resizing: Downscaling to 600x380 pixels to optimize processing speed while maintaining the aspect ratio (1.58).
- Grayscale Conversion: Converting to grayscale using OpenCV (`cv2.cvtColor`) to reduce computational complexity.
- Feature Extraction: Using ORB (`cv2.ORB_create`) with 2000 features to generate reference descriptors, stored in `reference_features`.

3.2 Real-Time Data Collection

The primary verification data is collected directly from the webcam during system operation. This includes two types:

- ID card images: Captured from the webcam when a user places their ID card within the frame, detected and cropped using the `detect_id_card` function.
- Live face images: Captured from the user's face when looking at the webcam, detected using the `detect_faces` function.

Data Preprocessing for Webcam Input

Each video frame (640x480 resolution) undergoes processing to detect both the ID card and the user's face.

Cropping and Alignment:

- For ID cards: After detection using ORB, the detected region is warped using a perspective transform to a standard size of 600x380 pixels.
- For faces: Faces are cropped from frames using the OpenCV DNN face detector and resized to 112x112 pixels (the required input size for InsightFace).

Normalization:

- Pixel values are normalized to the [0,1] range by dividing by 255 to ensure compatibility with the pretrained model.

3.4 Data Pairing (ID-Face Pairs)

The system automatically generates ID-face pairs for comparison:

- Positive pairs**:** The face image extracted from the ID card (`photo_area`) is paired with the live face image of the same person.

- Negative pairs**:** Not generated automatically due to limited data; instead, manual testing is conducted by pairing an ID card image with a live face image of a different person.

For example, in a single test run, the system captures:

- One ID card image (`warped_card.jpg`)

- One live face image (`live_face.jpg`)

This pair is processed by InsightFace to extract embeddings and compute a similarity score.

3.5 Performance Evaluation

Due to the absence of a large dataset, performance evaluation is conducted qualitatively by testing with five real-world data pairs:

- Sample size**:** 5 ID card images and 5 corresponding live face images from 5 different individuals.

Methodology**:**

- Running the system for each pair and recording the similarity score from

`compare_face_embeddings`.

- Observing the ID card detection success rate (`detect_id_card`) and face verification accuracy (using a default similarity threshold of 0.3).

Results**:** Documented in the "Results" section, with an average success rate recorded.

4. Methods

4.1 Overview

The code implements a face verification system that compares a face on an ID card with a live face captured via webcam. It uses computer vision techniques to detect the ID card, locate faces, and compare their features in real-time. The process operates through a state-based workflow with three stages: detecting the ID card, detecting the live face, and verifying the match.

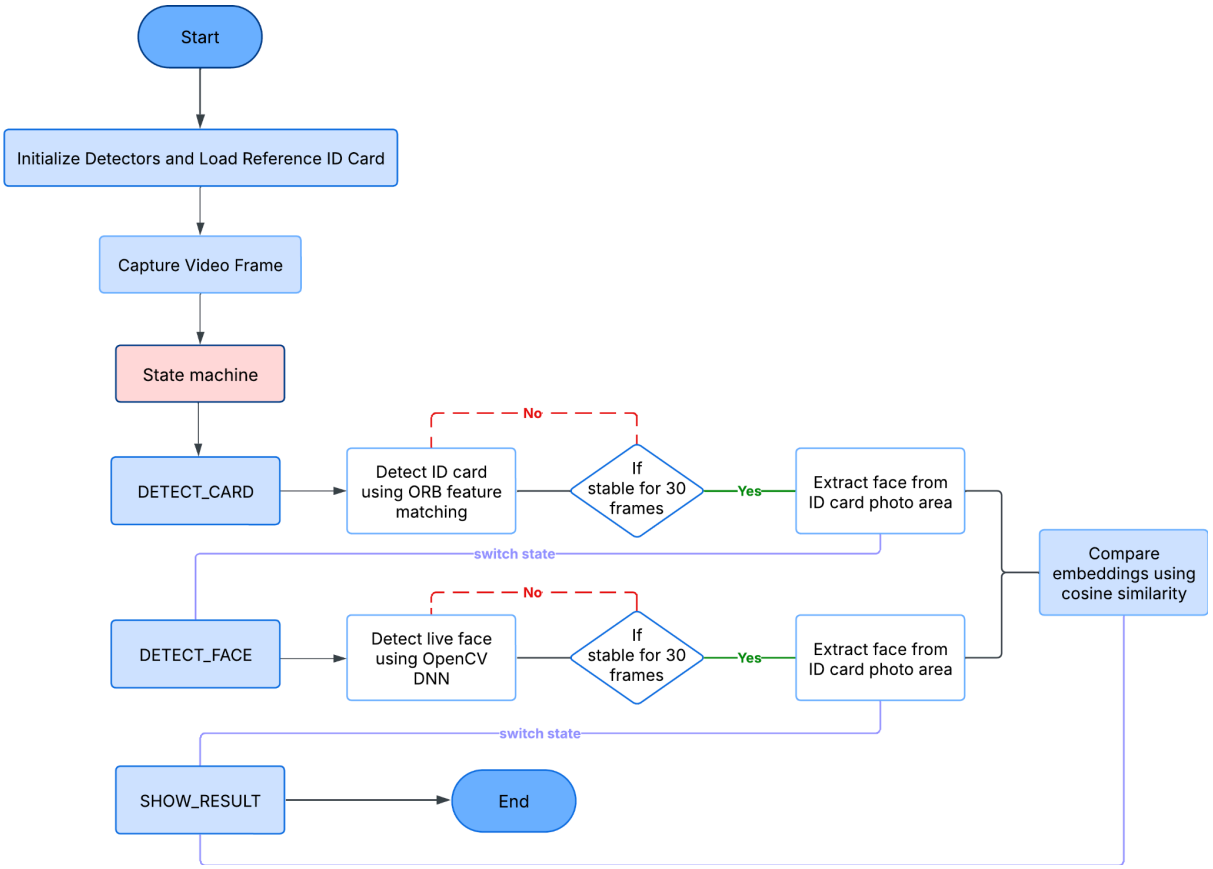

Figure 1: This diagram shows the sequence from frame capture to result display, with state transitions based on consistent detections.

4.2 Detailed Methodology

4.2a ID Card Detection

Overview

This section of the face verification system is responsible for automatically detecting an ID card (like a student ID or citizen ID) in the live video feed from a webcam. It compares each frame from the camera to a reference image of an ID card (e.g., reference_id_card.jpg) to find a match. The process uses the **ORB (Oriented FAST and Rotated BRIEF)** algorithm—a fast and reliable tool for spotting unique features in images—and includes several checks to ensure the detection is accurate. If successful, it draws a green outline around the card and creates a straightened (warped) view of it for further processing.

Key Steps and Important Parts

1. **Preparing the Reference Image**
   - The system starts with a reference image of an ID card, loaded from a file like reference_id_card.jpg. This image acts as the "template" of what the card should look like.
   - The image is converted to grayscale (black and white) to simplify processing, and ORB identifies "keypoints"—distinct spots like corners, logos, or text edges. These keypoints come with "descriptors," which are like unique fingerprints describing each spot.
2. **Analyzing the Camera Frame**
   - Each frame from the webcam is also turned into grayscale and processed with ORB to find its own keypoints and descriptors.
   - ORB is tuned with settings like nfeatures=2000 (looking for up to 2000 keypoints) and scaleFactor=1.2 (checking multiple sizes of the image) to handle different angles and distances.
   - A trick called histogram equalization is applied to adjust brightness and contrast, making keypoints easier to spot even if the lighting changes.
3. **Matching Keypoints (KNN Matching)**
   - The system compares keypoints from the reference image to those in the camera frame using **KNN matching** (K-Nearest Neighbors). For each reference keypoint, it finds the two most similar keypoints in the frame (the "closest" and "second-closest" matches).
   - It then applies **Lowe's Ratio Test**: if the closest match is much better than the second-closest (distance ratio < 0.75), it's considered a "good match." For example, if the closest match has a distance of 5 and the second-closest is 20, the ratio is 5/20 = 0.25, which passes.
   - The code needs at least 15 good matches to proceed (**Figure 2**).

Figure 2: If enough good matches are found (≥15), the code will draw a green outline around the detected card and show a corrected perspective view.

4. **Locating the Card (Homography)**
   - With enough good matches (≥15), the system uses a mathematical trick called **homography** (cv2.findHomography with RANSAC) to figure out where the card is in the frame. Homography maps the reference card's corners to their positions in the camera image.
   - RANSAC (a robust fitting method) ensures the mapping is accurate even if some matches are slightly off, requiring at least 70% of matches to fit the model (inliers).
   - The result is a set of four corners defining the card's outline in the frame.
5. **Validation Checks**
   - **Aspect Ratio**: The detected card's width-to-height ratio must be close to the reference's (1.58), within 20% tolerance. This ensures it's shaped like a real card.
   - **Size**: The card can't be too small (<50 pixels) or too big (>90% of the frame), so it's realistic in the scene.
   - **Shape**: The four corners must form a convex quadrilateral (no weird dents or overlaps).
   - If any check fails, the detection is rejected.

4.2b Face Detection

The system uses OpenCV's DNN-based face detector initialized with pre-trained models, based on SSD (Single Shot MultiBox Detector) architecture with backbone ResNet.

The detection process works by:

1. Converting the image to a normalized blob
2. Passing the blob through a pre-trained neural network
3. Processing the network output to extract face bounding boxes

4.2c Face Comparison

In this face verification system, the face comparison model used is InsightFace's buffalo_l model, a highly accurate face recognition model based on ArcFace, using a ResNet-50 backbone architecture.

The model is initialized with a 640x640 detection size, loading only the detection and recognition modules for efficiency. Facial embeddings are extracted from both the ID card and live face, with a warning triggered if the detection score drops below 0.5, indicating potential quality issues. These embeddings are normalized to unit length, and their similarity is calculated using cosine similarity (dot product), producing a score between -1 and 1. A match is confirmed if the score exceeds 0.3, a threshold selected to balance accuracy and robustness.

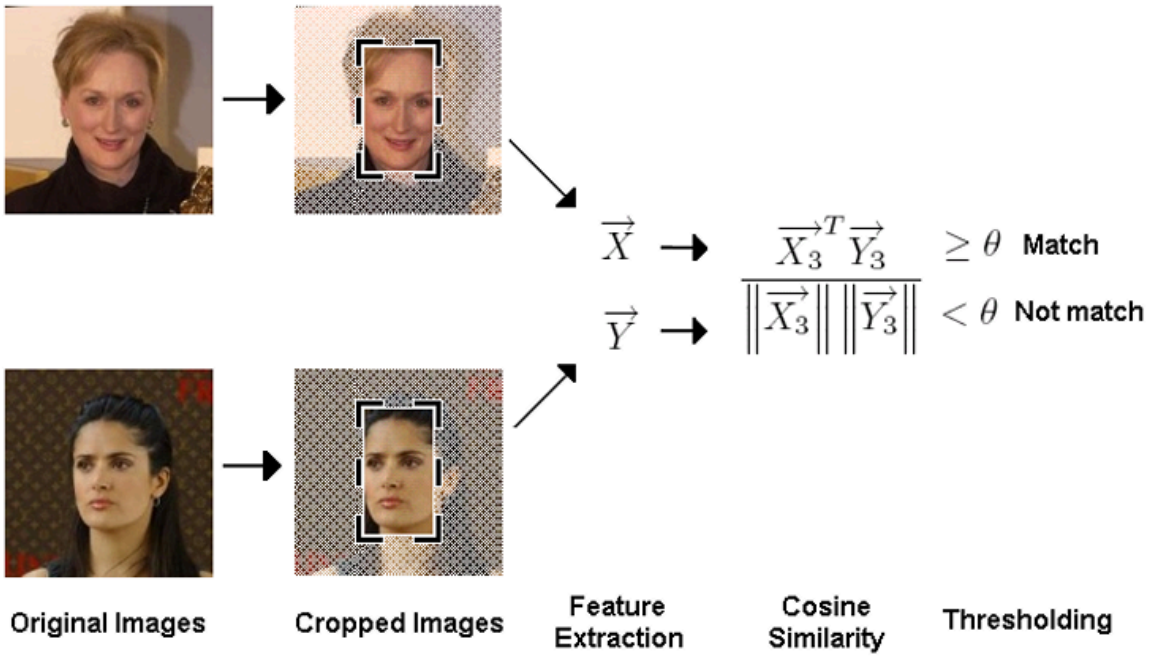

Figure 2: Example of Face comparison.

5. Limitations and Future Improvements

Existing problems of the current implementation:

- The algorithm isn't optimal and doesn't accurately detect the card's corners.

→ **Suggestion for improvement**: Use contours combined with perspective transform (identify the 4 corners of the card and warp the perspective).

- The photo on the ID card is often significantly different from the live photo, making direct image processing result in low accuracy and impracticality.

→ **Recommendation**: Use the ID number to map to a student's photo from a recent period (e.g., within the last month – allowing students to periodically update

their facial information on the system) and compare this recent database photo with the live image of the student captured by the software for verification.

- To build an effective system for verifying faces and ID cards, careful consideration must be given to the organization of stored data: ID codes, student personal information, and facial information stored as vectors, ensuring fast and accurate retrieval. Furthermore, the vector extraction method needs to be researched based on reputable publications to guarantee recognition accuracy and prevent misidentification from phone images (presentation attacks).

  → It's necessary to consult existing research on face-based attendance systems and combine them with traditional OCR methods for ID cards to develop a better approach.

- Revisiting the questions: Will students check in via one camera or multiple cameras? If multiple cameras are used, multiple object tracking (MOT) methods would be required to monitor several students simultaneously (tracking how long students are in the classroom versus how long they are away).

- The current method only addresses the technical aspects and still has many process-related loopholes. Specifically: If a student checks in and then leaves, are they counted as present? How long must a student be physically in the classroom to be considered 'attending'? And does the system prevent cases of using deepfakes, phone images, videos, or someone else's student ID card for 'buddy punching' (checking in for others)?

6. Conclusion and Perspectives

This project successfully developed and implemented a student ID authentication system that integrates traditional ID card scanning with live facial recognition, leveraging computer vision and deep learning techniques to enhance security and accuracy in educational environments. The combination of the ORB algorithm for ID card detection and the InsightFace buffalo_l model for face comparison proved effective in achieving reliable real-time verification. ORB’s ability to detect keypoints and match them robustly across varying angles and lighting conditions, paired with InsightFace’s high-precision facial embeddings and cosine similarity scoring, enabled the system to accurately distinguish between matching and non-matching ID-face pairs. The state-based workflow—detecting the ID card, capturing the live face, and verifying the match—streamlined the process, making it both user-friendly and efficient for practical deployment.

References

[1] Ngonadi, I. V., & Orobor, A. I. (2020). Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine (SVM). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(4), 11-20. Available from https://www.researchgate.net/publication/342866546_Face_Recognition_Service_Model_for_Student_Identity_Verification_Using_Deep_Neural_Network_and_Support_Vector_Machine_SVM

[2] Shi, Y., & Jain, A. K. (2018). DocFace+: ID Document to Selfie Matching. *arXiv preprint arXiv:1809.05620*. Available from https://arxiv.org/abs/1809.05620

[3] Folego, G., Angeloni, M. A., Stuchi, J. A., Godoy, A., & Rocha, A. (2016). Cross-Domain Face Verification: Matching ID Document and Self-Portrait Photographs. *arXiv preprint arXiv:1611.05755*. Available from https://arxiv.org/abs/1611.05755

[4] Identity Authentication on Mobile Devices Using Face Verification and ID Image Recognition. Available at: https://www.sciencedirect.com/science/article/pii/S1877050919320812

[5] How Selfies and ID Card Photos Can Be Used to Verify Identity. Available at: https://usesmileid.com/blog/how-selfies-and-id-card-photos-can-be-used-to-verify-identity

[6] Face Authentication on Banking Apps: Why Many Users Still Struggle? Available at: https://vnbusiness.vn/ngan-hang/xac-thuc-khuon-mat-tren-app-ngan-hang-vi-sao-nhieu-nguoi-van-chua-thuc-hien-duoc-1100590.html

[7] Face and ID Card Verification for KYC. Available at: https://iapp.co.th/docs/ekyc/face-and-id-card-verification-for-kyc

[8] Research and Development of a Two-Factor Face Authentication System Using an Invisible F-QR Code on ID Card by 1064 nm Laser and AI Camera. Available at: https://www.researchgate.net/publication/364586284

[9] Facial Recognition Will Replace Keys, Passports, and Tickets in the Next 5 Years – But Is This a Privacy Violation? Available at: https://www.thesun.co.uk/tech/30731964/facial-recognition-replace-keys-passports-tickets/

[10] AI Face Recognition: 6 Key Applications in Practice. Available at: https://lacviet.vn/ai-face-recognition/

[11] How Does the Facial Recognition System Work? Explaining Benefits, Usage Scenarios, and Precautions. Available at: https://www.alsok.com.vn/vi/column/how-does-the-facial-recognition-system-work-explaining-the-benefits-usage-scenarios-and-precautions/

[12] Biometric Authentication for Transactions Over 10 Million VND Using Static Images. Available at: https://vnexpress.net/dung-anh-tinh-qua-mat-xac-thuc-sinh-trac-hoc-tren-app-ngan-hang-4765838.html

[13] ID Photo Verification by Face Recognition.

[14] Shi, Y. & Jain, A.K. (2018). DocFace+: ID Document to Selfie Matching. arXiv preprint. Available at: https://arxiv.org/abs/1809.05620

[15] Face Recognition for Identification and Verification in Attendance System: A Systematic Review.

[16] Identity Authentication on Mobile Devices Using Face Verification and ID Image Recognition. Available at: https://www.researchgate.net/publication/338283772_Identity_authentication_on_mobile_devices_using_face_verification_and_ID_image_recognition

[17] Research on Secure ID Document Storage Using Machine-Readable Facial Biometric Templates. Available at: https://www.mdpi.com/2076-3417/11/13/6134

[18] Popescu, A. et al. (2022). Face Verification With Challenging Imposters and Diversified Demographics. WACV Conference Paper. Available at: https://openaccess.thecvf.com/content/WACV2022/papers/Popescu_Face_Verification_With_Challenging_Imposters_and_Diversified_Demographics_WACV_2022_paper.pdf

[19] Feasibility Study of a New Security Verification Process Based on Face Recognition Technology at Airports. Available at: https://www.researchgate.net/publication/341574148

[20] Software Utilizing Deep Learning-Based Face Detection and Facial Recognition Libraries. Available at: https://github.com/acs-unitartucs/idcard_face_match

Appendix A. Project Plan management

Task Name	Priority	Owner	Start date	End date	Status	Issues
Find documents	High	Group	14/3/2025	20/3/2025	Finished	
Write Report & Slide	High	Group	21/3/2025	28/3/2025	Finished	
Review related papers	Medium	Cao Phạm Thành Đạt	16/3/2025	21/3/2025	Finished	
Review and analyze public dataset	Low	Nguyễn Chí Dũng	17/3/2025	20/3/2025	Finished	
Write code and monitor project	High	Nguyễn Bình Thành	15/3/2025	20/3/2025	Finished	
Evaluate potential method	Medium	Nguyễn Bình Thành	15/3/2025	26/3/2025	Finished	
Experiment and improve code	Medium	Đỗ Thành Cường	20/3/2025	27/3/2025	Finished	
Test and report errors	Low	Đỗ Thành Cường	28/03/2025	28/03/2025	Finished	
Limitations and Future Improvements	Medium	Nguyễn Hoàng Tùng	20/3/2025	25/3/2025	Finished	

Writing appendix	Low	Cao Phạm Thành Đạt	26/3/2025	27/3/2025	Finished	

Appendix B. Source code & Data

Code + Dataset: Face and id verify