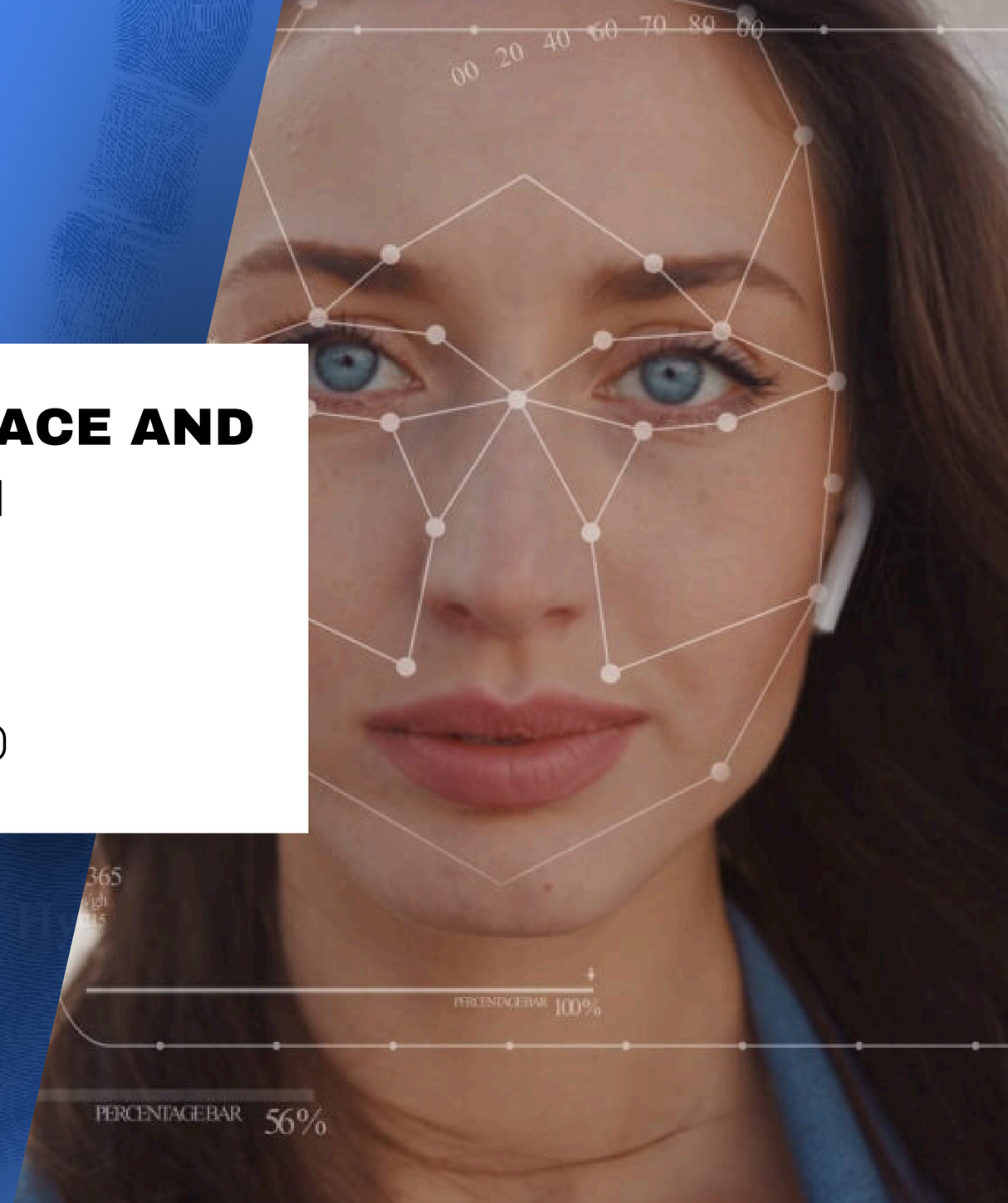
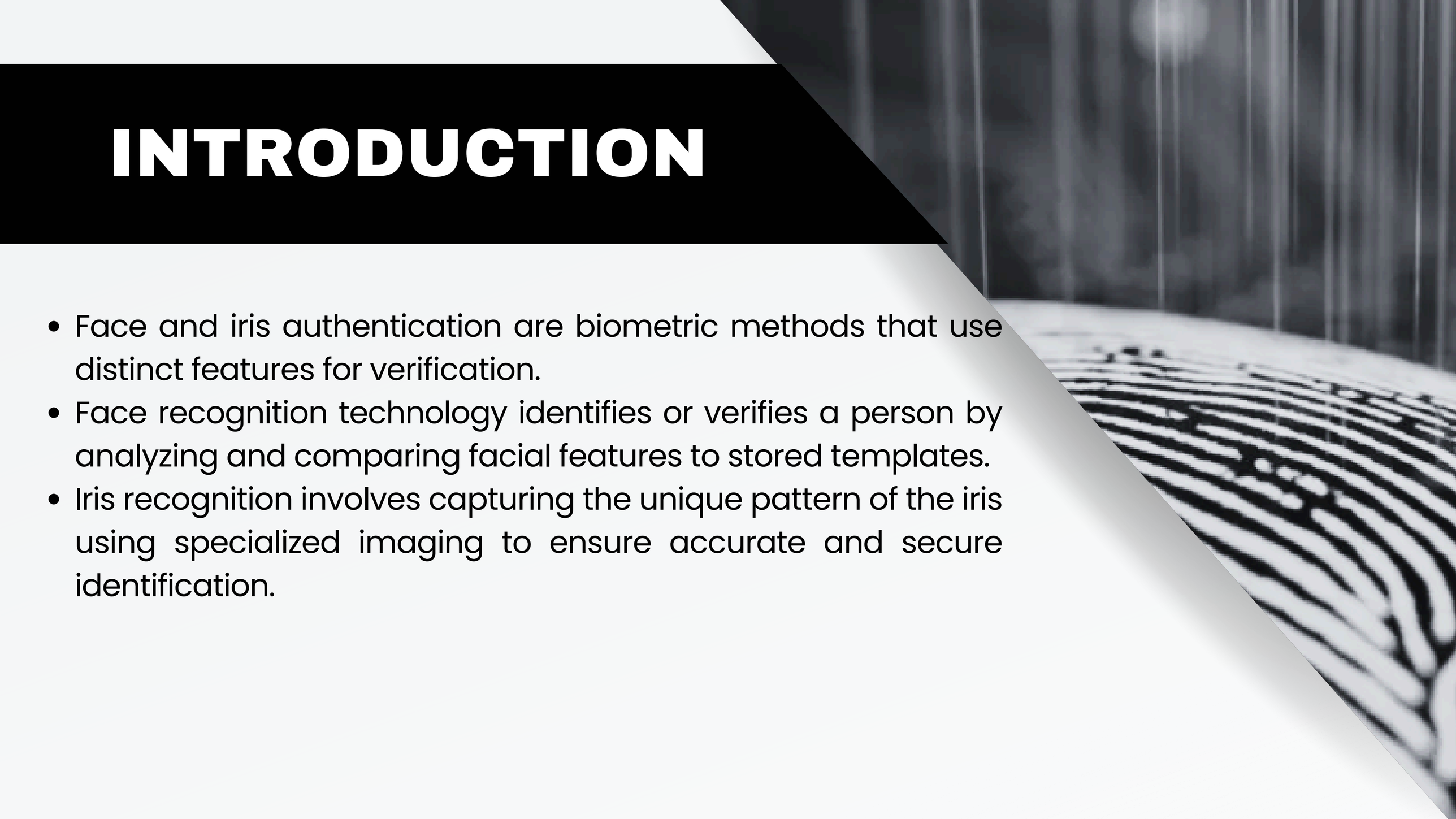
AUTHENTICATION USING FACE AND IRIS RECOGNITION

By: Kausal S D (CYS21028)
Jayaraj V (CYS21026)



INTRODUCTION

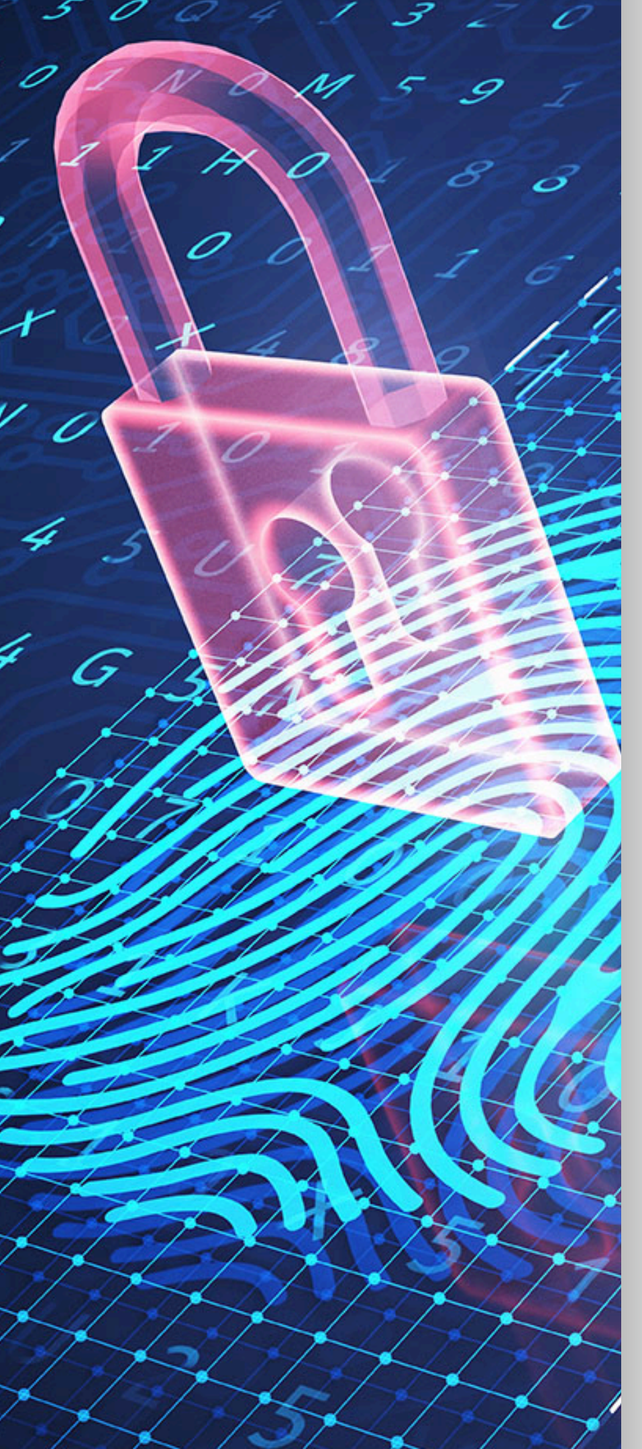


- Face and iris authentication are biometric methods that use distinct features for verification.
- Face recognition technology identifies or verifies a person by analyzing and comparing facial features to stored templates.
- Iris recognition involves capturing the unique pattern of the iris using specialized imaging to ensure accurate and secure identification.

PROBLEM STATEMENT

- Develop a biometric authentication system that integrates face and iris recognition technologies to enhance security and accuracy. The system must effectively analyze and compare facial features and iris patterns to reliably verify individual identities while minimizing the risk of false positives and negatives.

- Create a dual-authentication system combining face and iris recognition to provide a higher level of security by leveraging the unique biometric patterns of both facial features and iris structures, ensuring robust identity verification in diverse environments and conditions.



OBJECTIVE

- To design and implement a biometric authentication system that integrates face and iris recognition technologies to achieve high accuracy and security in identity verification.

- To enhance user authentication by developing a system that combines face and iris recognition, ensuring robust performance under varying environmental conditions and user scenarios, while maintaining ease of use and minimizing false authentication errors.

- The system aims to leverage the complementary strengths of both biometric modalities to provide reliable, multi-factor authentication in various operational settings.

Why Face and Iris Recognition?

Accuracy:
The combination of Iris detection and face recognition enhances accuracy by utilizing two distinct and unique biometric features, significantly reducing authentication errors.

Non-Intrusive:
Both Iris detection and face recognition are contactless methods, ensuring a hygienic and user-friendly experience, unlike fingerprint or handprint systems.

Efficiency:
Because fingerprint has high false acceptance and false rejection rates, this could be replaced by Iris recognition because it have low false acceptance and false rejection rates.

Convenience:
Users benefit from a seamless experience, as there’s no need for physical tokens like cards or fobs, eliminating the risk of loss or misplacement.

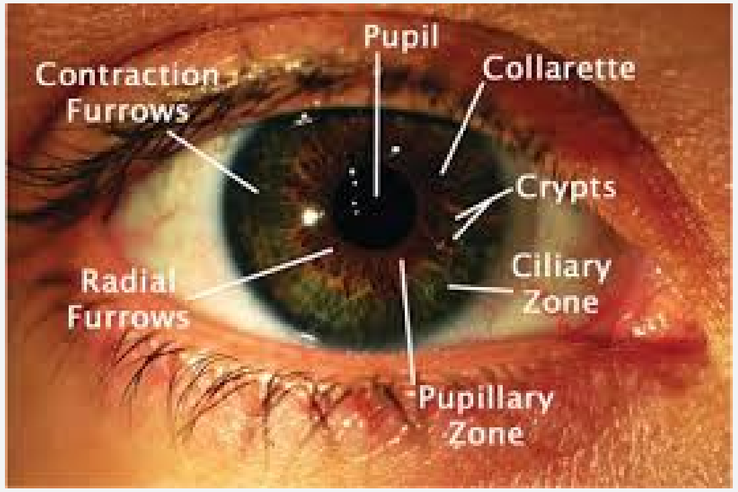
Security:
Combining Iris detection and face recognition provides greater security than single-method systems like RFID cards or fingerprints.

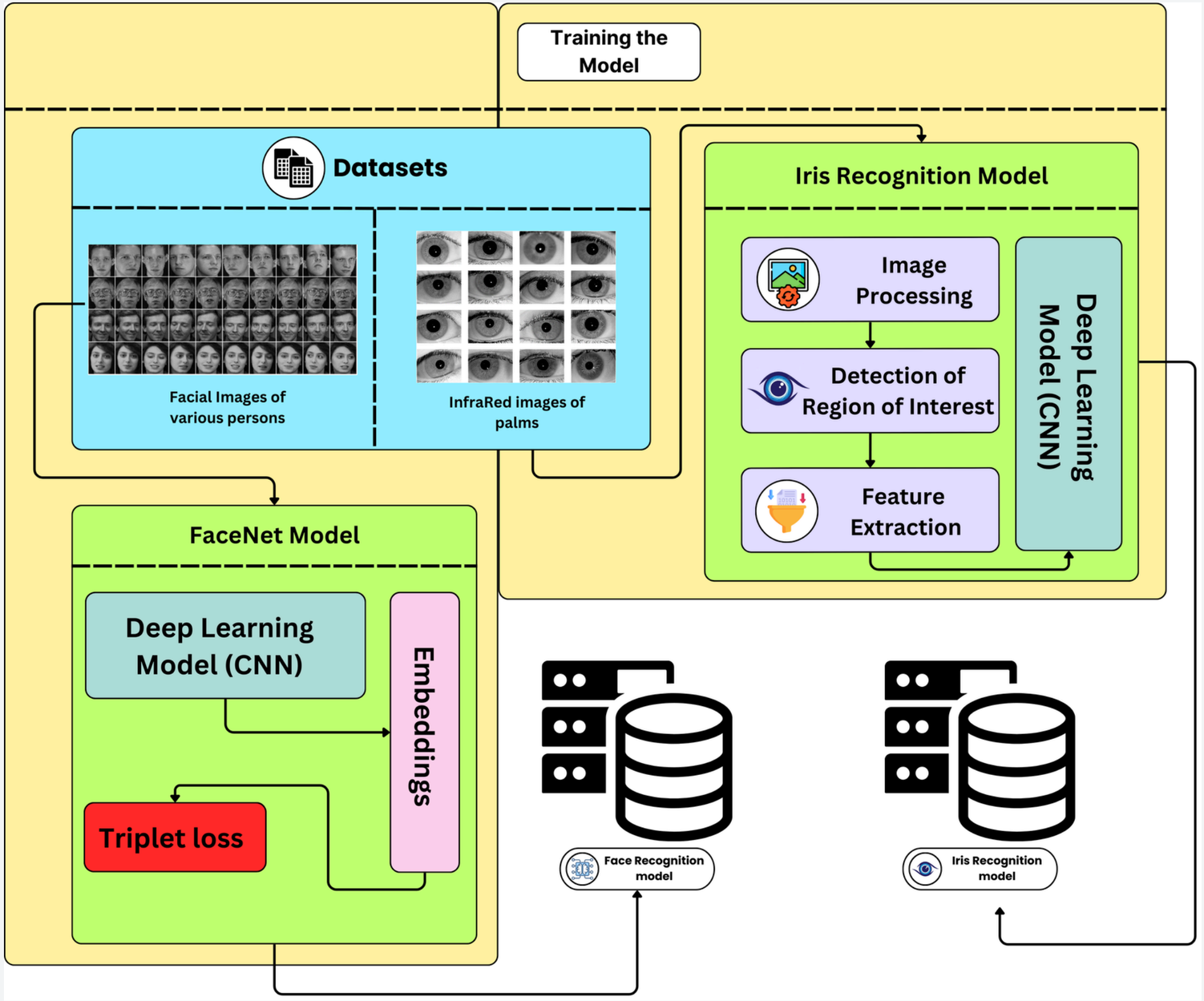
METHODOLOGY

- **Data Collection and Preprocessing:** Collect a large dataset of facial images with various expressions and lighting conditions.
- **Feature Extraction:** Use FaceNet's CNN architecture to extract facial features and generate embeddings that represent unique facial characteristics.
- **Triplet Loss Training:** Minimize distances between embeddings of the same person, maximize distances between different individuals.
- **Real-Time Comparison:** Compare live facial embeddings with stored embeddings for identification and verification.

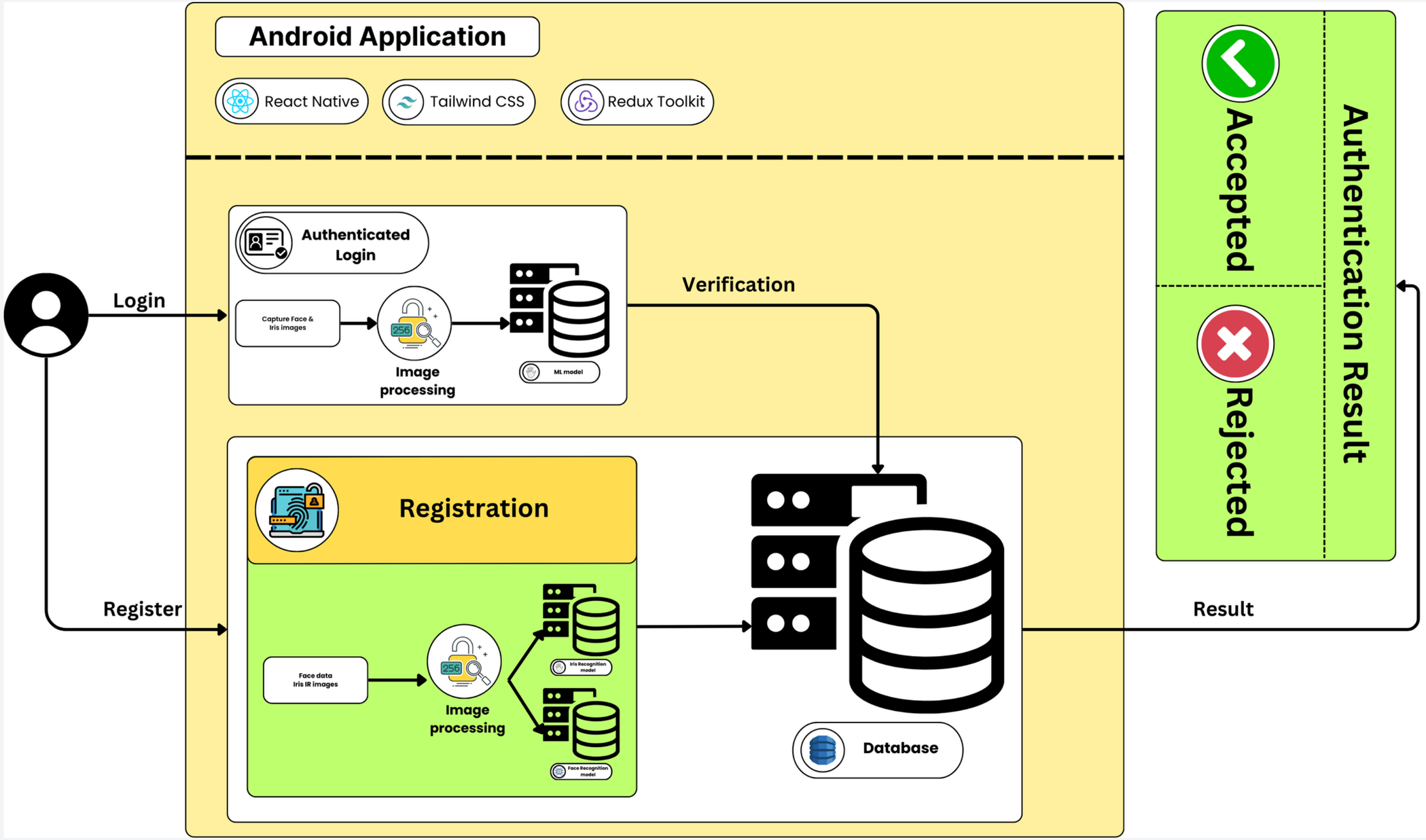
- **Dataset Preparation:** Load and preprocess iris images from the dataset directory. Extract labels based on directory structure and store image paths and labels in a DataFrame.
- **Image Preprocessing:** Resize and normalize images, convert them to NumPy arrays, and reshape them for model input. Split the dataset into training, validation, and test sets.
- **Model Construction:** Define a CNN architecture with convolutional, batch normalization, max pooling, and dropout layers. Use fully connected layers with a softmax output for classification. Compile the model with an appropriate loss function and optimizer.
- **Model Training:** Train the model using the training set, validate with the validation set, and use callbacks for early stopping, model checkpointing, and learning rate adjustments. Track performance metrics throughout.
- **Model Evaluation and Visualization:** Evaluate the model on the test set to determine accuracy. Visualize training and validation accuracy and loss curves to assess model performance and convergence.

Architecture Diagram

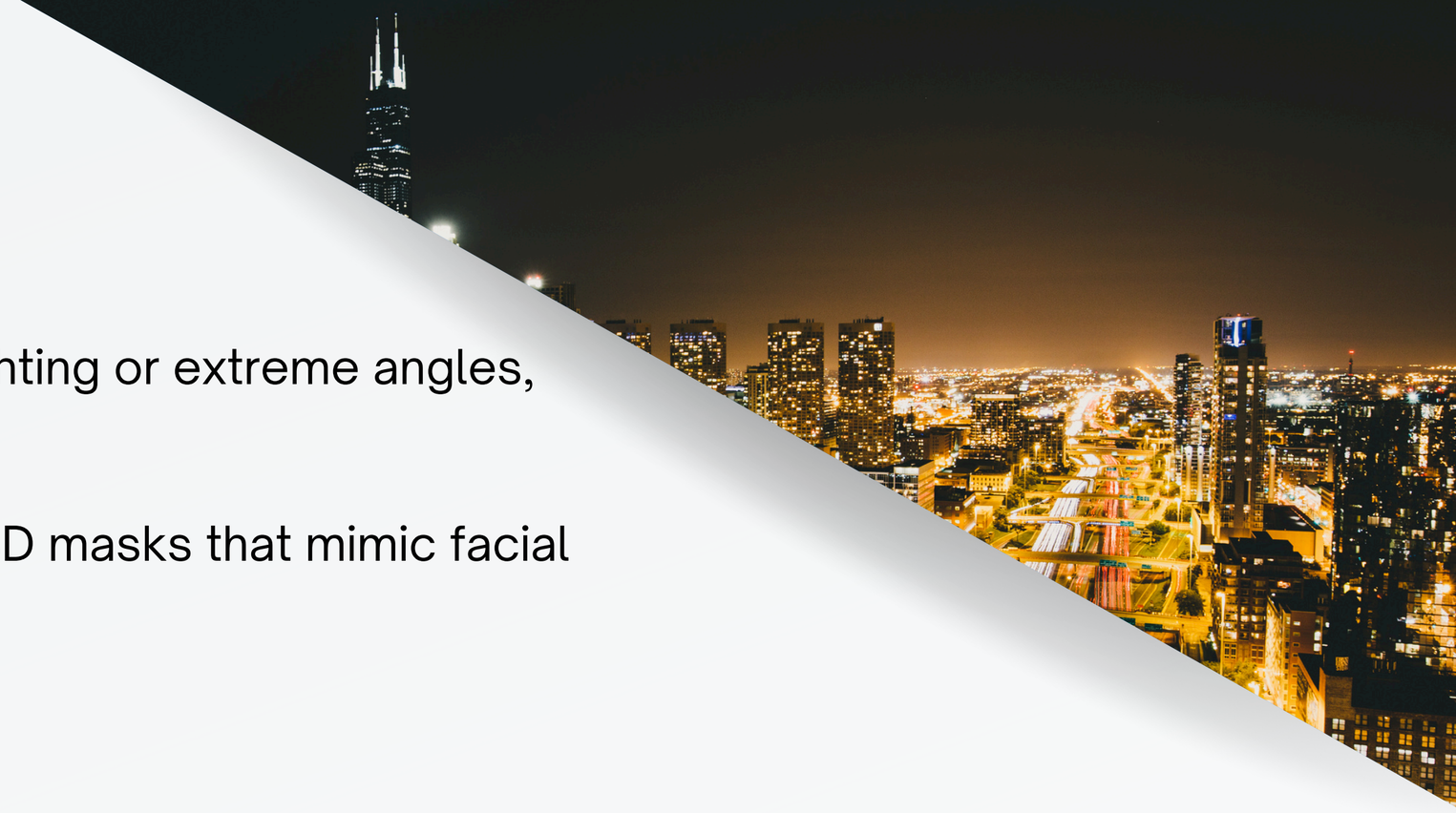




Architecture Diagram



SHOWSTOPPERS



Face Recognition

- Performance can degrade with poor lighting or extreme angles, affecting accuracy.
- Vulnerable to attacks using photos or 3D masks that mimic facial features.

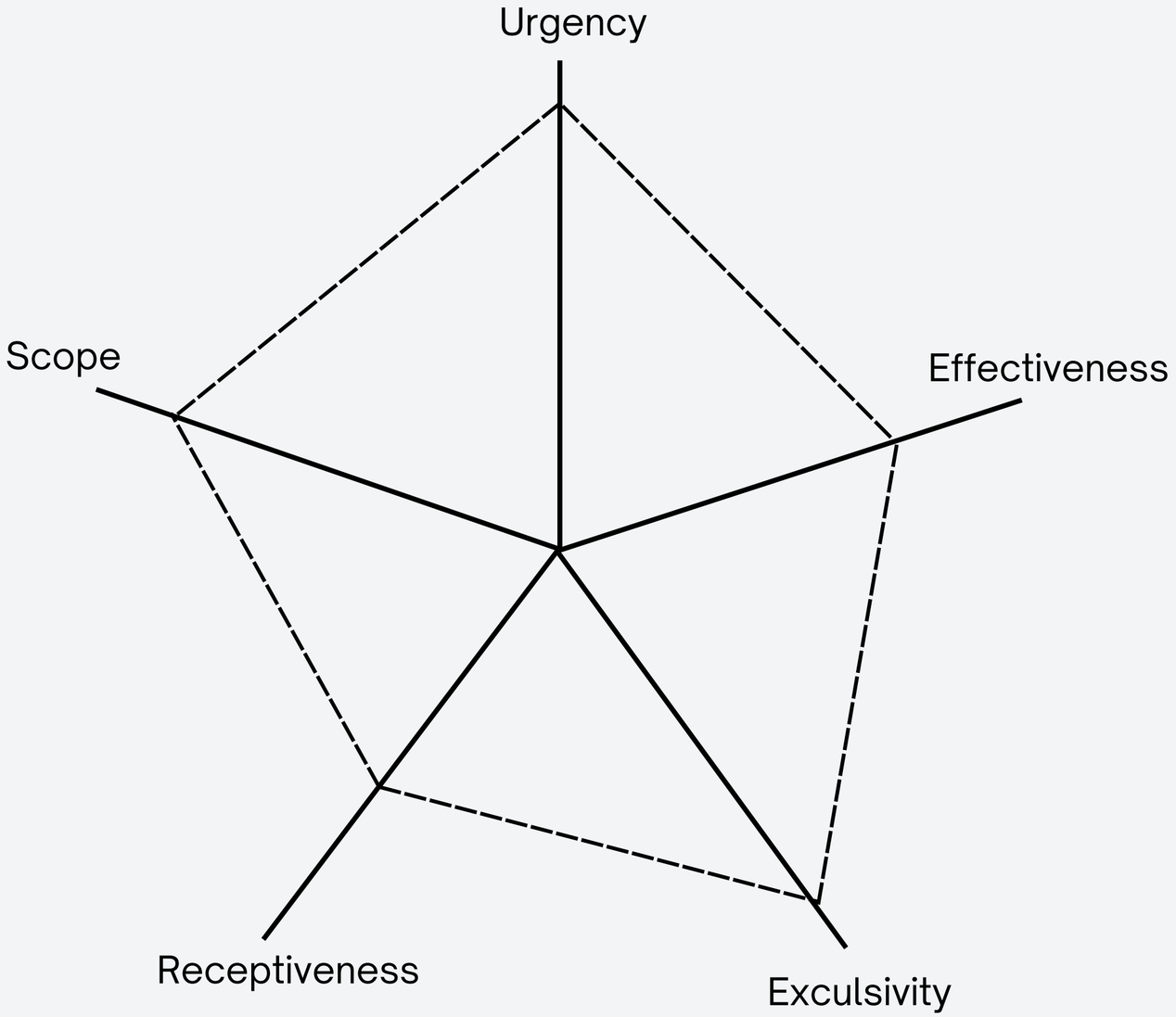
Iris Recognition

- Computational demands may hinder real-time performance.
- Poor or inconsistent image quality can impact model performance.
- Model may overfit to training data or be biased due to uneven class representation.

REFERENCE

	Projects	AUTHOR	PROBLEM STATEMENT	METHODS USED AND RESULTS
	Iris Recognition with Image Segmentation Employing Retrained Off-the-Shelf Deep Neural Networks	Daniel Kerrigan, Mateusz Trokielewicz, Adam Czajka, Kevin Bowyer	Traditional iris segmentation methods face limitations when dealing with irregular segmentation masks and diverse datasets, affecting recognition accuracy.	The authors propose three deep learning-based iris segmentation methods and evaluate them on a range of datasets. Deep learning-based segmentation outperforms conventional methods
	DeepIris: Iris Recognition Using A Deep Learning Approach	Shervin Minaee, Amirali Abdolrashidi	Previous iris recognition systems have struggled to jointly learn feature representation and perform recognition in an end-to-end manner.	This framework leverages a deep residual CNN to jointly learn features and perform iris recognition and shows promising results using only a few training images
	Resist: Reconstruction of Irises from Templates	Sohaib Ahmad, Christopher Geiger, Benjamin Fuller	Stored iris recognition templates are vulnerable to attacks aimed at reconstructing original iris images from these templates.	The RESIST method reconstructs iris images from templates using a CNN architecture integrated into a GAN. The approach is tested on multiple recognition systems, achieving high accuracy.
	Face-Recognition-using-FaceNet	Ankur Goswami	Develop an FaceNet based image processing system using machine learning for real-time face recognition.	FaceNet enhances computer vision and image processing, supporting both Live recognition & Image recognition
	Face Recognition Technology	Sagar Deshmukh et al	Improving face recognition tech for security, addressing challenges like changes in expression, aging, hairstyles, and occlusions.	Face recognition, despite limitations, is advancing rapidly in security and technology, becoming more accurate and promising better future techniques.

https://www.kaggle.com/code/sondosaabed/iris-eye-recognition-endtoend-93


Urgency
Effectiveness
Exculsivity
Receptiveness
Scope


THANK
YOU