Multimodel Biometric Recognition System Using Fingerprint, Iris, and Face.

This major-project report is submitted to

Shri Ramdeobaba College of Engineering and Management, Nagpur

(Autonomous Institution* Permanently *Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University)

By

Nayan Pillewar (B-38)

Ritika Trivedi (B-59)

Saba Salat (B-60)

Yash Soni (B-63)

Semester: VI

B.Tech. (Electronics and Computer Science)

under the guidance of

Prof. Gauri Morankar

DEPARTMENT OF ELECTRONICS ENGINEERING

SHRI RAMDEOBABA COLLEGE OF ENGINEERING AND MANAGEMENT

Session: 2024-25

Abstract

This project proposes a Multimodal Biometric Recognition System that integrates fingerprint, iris, and facial recognition to improve the accuracy, security, and robustness of identity verification. Traditional unimodal biometric systems—those that rely on a single trait—often suffer from limitations such as noisy data, non-universality, and vulnerability to spoofing attacks, which compromise both reliability and security. To address these challenges, the proposed system captures biometric data from multiple traits and applies preprocessing techniques such as noise reduction, contrast enhancement, and alignment to standardize inputs across modalities.

For feature extraction, the system uses Principal Component Analysis (PCA) to reduce dimensionality and extract meaningful feature representations from the fingerprint, iris, and face images. This enables efficient processing while preserving the essential discriminative features of each modality. Each biometric trait is then processed using a Support Vector Classifier (SVC), which assigns matching scores based on classification confidence. The scores from all modalities are normalized and combined using score-level fusion, where individual matching results are integrated through a weighted summation technique to make a final authentication decision. This fusion strategy leverages the strengths of each modality, compensates for their individual weaknesses, and results in improved recognition performance with reduced False Acceptance Rate (FAR) and False Rejection Rate (FRR).

To ensure system integrity and resistance to fraudulent access, the design includes anti-spoofing measures such as liveness detection for fingerprints (e.g., sweat pore texture analysis), motion-based verification for iris input, and 3D structure or reflectivity analysis for facial recognition. Furthermore, biometric templates and classification outputs are securely stored using AES-256 encryption to protect sensitive user data from unauthorized access or tampering.

The system is implemented using Python, OpenCV, and Scikit-learn, and is developed and tested on Google Colab, a cloud-based platform that provides free GPU access and facilitates scalable model training and evaluation. This setup eliminates local hardware constraints and allows flexible deployment across both local and cloud-based environments.

With potential applications in access control systems, border security, law enforcement, and intelligent surveillance, this project demonstrates the effectiveness of combining multiple biometric traits with classical machine learning techniques to deliver a reliable, secure, and efficient identity verification system.

Table of Contents

3. List of Figures

Block Diagram:

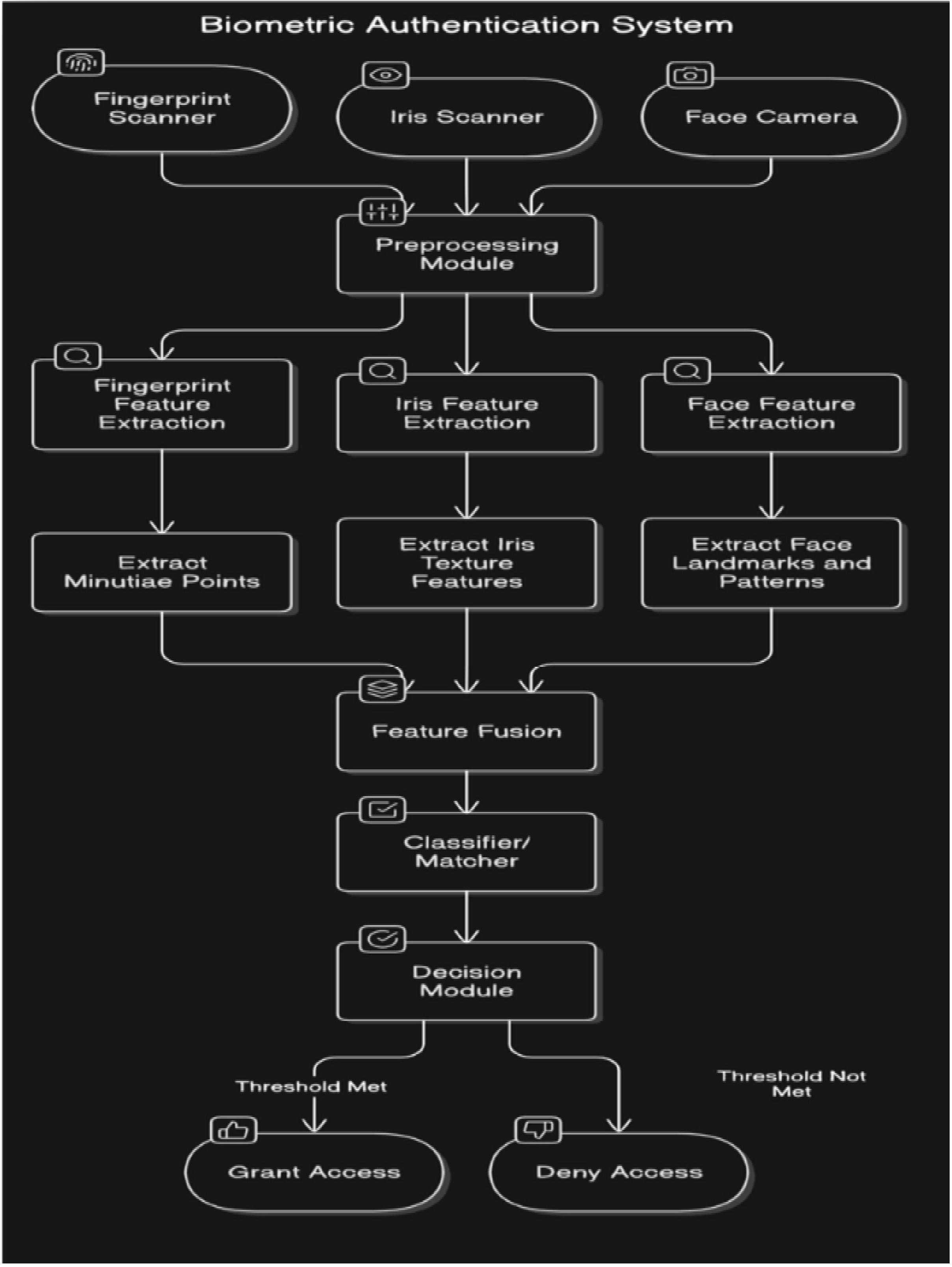


Fig.no.1

Flow Chart

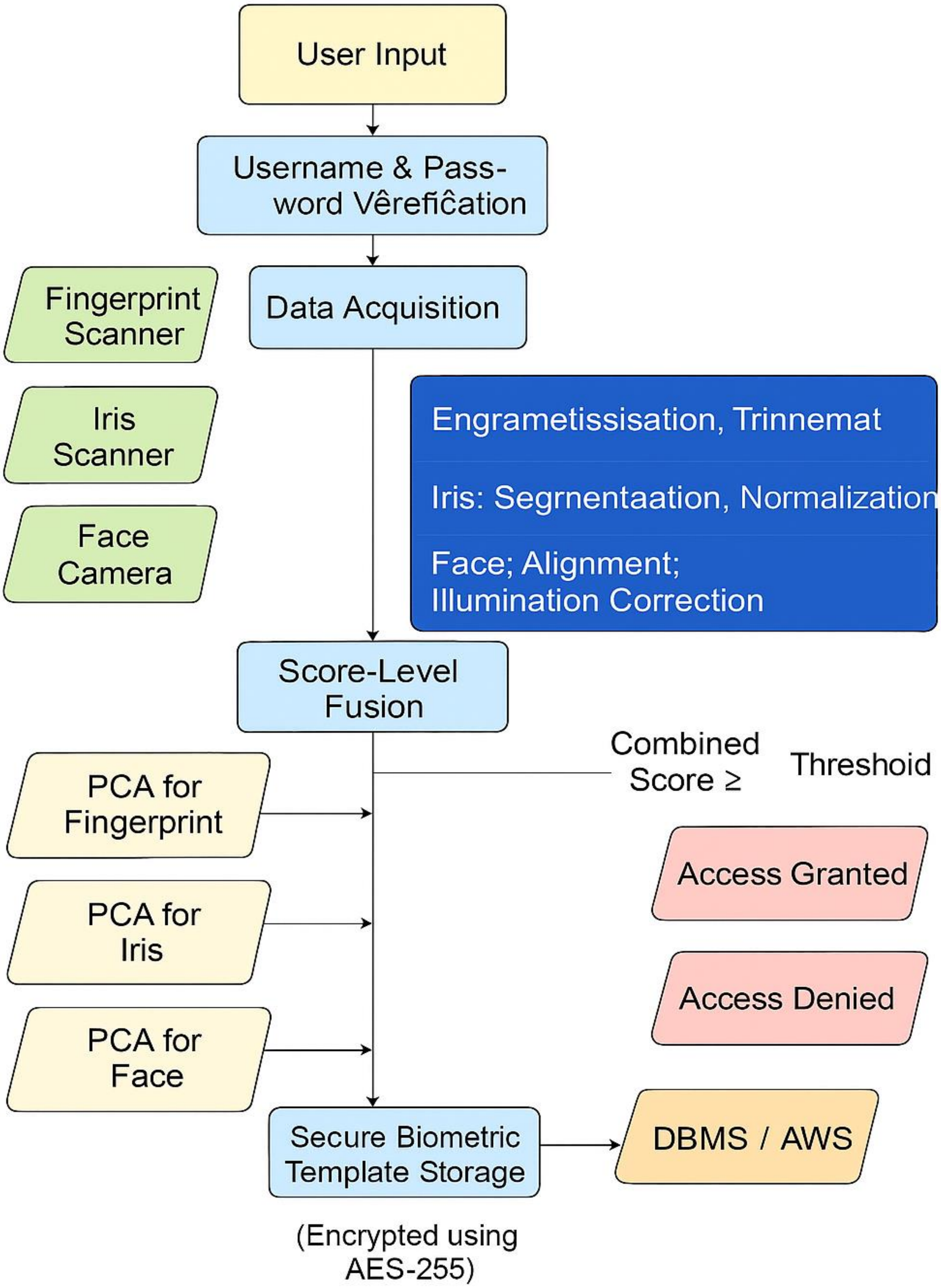

User Input
Username & Password Vêrefiĉation
Data Acquisition
Fingerprint Scanner
Iris Scanner
Face Camera
Engrametissisation, Trinnemat
Iris: Segrnentaation, Normalization
Face; Alignment; Illumination Correction
Score-Level Fusion
Combined Score ≥
Threshoid
PCA for Fingerprint
PCA for Iris
PCA for Face
Access Granted
Access Denied
Secure Biometric Template Storage
DBMS / AWS
(Encrypted using AES-255)

Fig no. 2

Biometric Trait Acquisition Devices

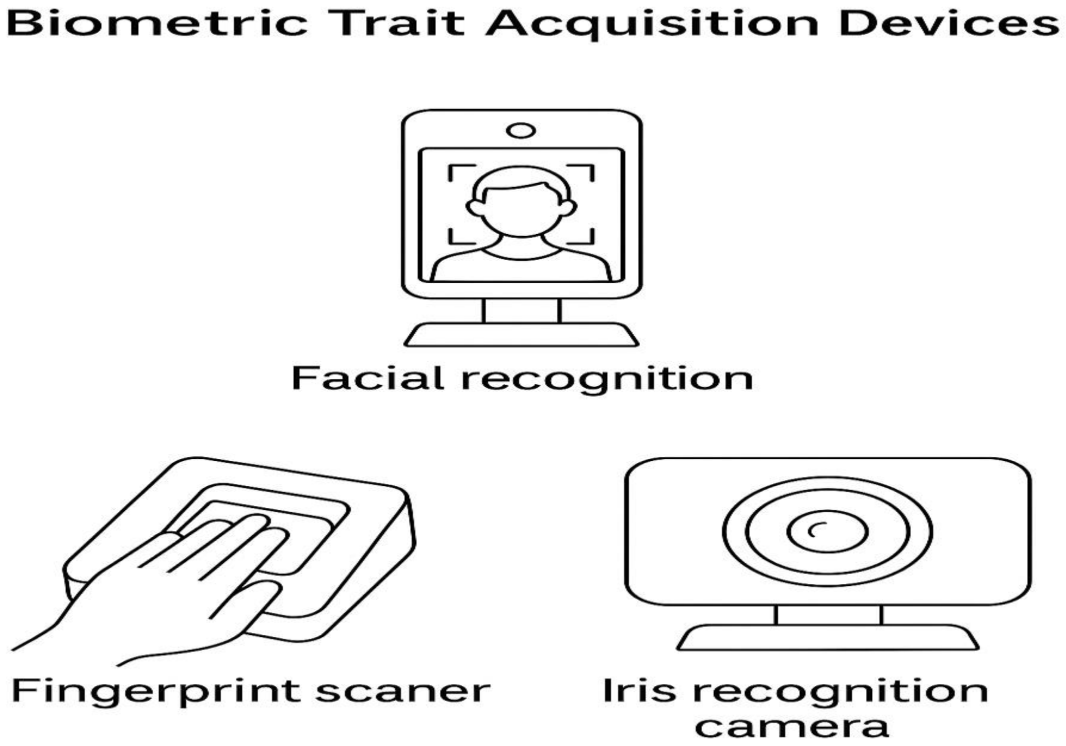


Fig no. 4

Score-Level Fusion Workflow

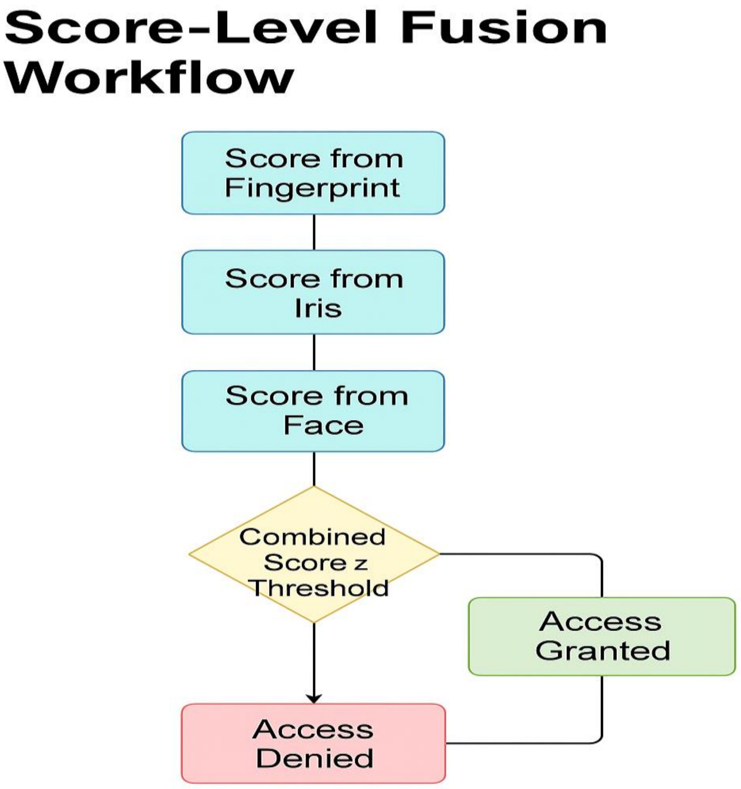


Fig no. 5

4. List of Tables

Table 1: Hardware Requirements

Component	Specification	Purpose
Fingerprint Scanner	Optical, 500 DPI	Capture fingerprint images
Iris Scanner	IR-enabled camera	Capture iris patterns
RGB Camera	1080p resolution	Capture facial images
Processing Unit	Intel i7 / NVIDIA GPU	Model training and inference

Table 2: Software Tools and Frameworks Used

Tool/Framework	Version	Purpose
Python	3.x	Programming & model development
TensorFlow / Keras	2.x	Deep learning framework
OpenCV	4.x	Image processing
SQL / NoSQL DB	-	Biometric data storage
MATLAB (optional)	R2023a	Signal/image analysis (optional)

Table 3: Month-wise Plan

Month	Activities Planned	Status
Month 1	Dataset Search, Literature Review	Completed
Month 2	Preprocessing, Model Design	In Progress
Month 3	Training, Fusion Method Implementation	Not Started
Month 4	Testing, Evaluation, Final Report Preparation	Not Started

5. List of Symbols, Abbreviations or Nomenclature

Symbol/Abbreviation	Meaning
FAR	False Acceptance Rate
FRR	False Rejection Rate
PCA	Principle Component Analysis
RGB	Red Green Blue (color model)
SVC	Support Vector Classifier

6. Chapters

Chapter 1:
Introduction

In today’s digital era, ensuring secure and reliable identity verification is more critical than ever. Traditional authentication methods such as passwords, PINs, and physical ID cards are increasingly vulnerable to theft, duplication, and unauthorized access. As a result, biometric authentication systems have gained prominence by using unique physiological traits for user identification.

Among the widely adopted biometric modalities are fingerprint, iris, and face recognition, each offering distinct advantages in terms of universality, distinctiveness, and permanence. However, systems relying solely on a single biometric trait—known as unimodal systems—face limitations such as:

- **Non-universality** (not all users may have usable biometric samples),
- **Noisy data** (low image quality or inconsistent capture),
- **Intra-class variations** (differences in the same user's biometric data over time), and
- **Vulnerability to spoofing** (use of fake fingerprints, printed iris images, or facial photos).

To address these shortcomings, this project proposes a multimodal biometric recognition system that combines fingerprint, iris, and face data to enhance both security and reliability. By fusing multiple biometric traits, the system compensates for the weaknesses of individual modalities and significantly improves performance in high-security environments.

The system is built using a structured pipeline that includes:

- **Data acquisition** from biometric sensors,
- **Preprocessing** to enhance image quality and extract consistent regions of interest,

- **Feature extraction using Principal Component Analysis (PCA)** to reduce dimensionality while preserving key discriminative features,
- **Classification using Support Vector Classifier (SVC)** to identify or verify individuals based on the extracted features, and
- **Score-level fusion** to combine the classification results from multiple modalities into a final decision score.

Unlike deep learning-based systems, this approach avoids the computational demands of CNNs or VGG networks and instead leverages **PCA and SVC**, making the solution lightweight and more accessible for deployment without requiring specialized GPU infrastructure.

The system also includes **anti-spoofing mechanisms** for each modality and uses **AES-256 encryption** to protect stored biometric templates. These features make it highly suitable for use in areas such as **border control, law enforcement, financial services, and secure access systems**.

In summary, this project delivers a secure, efficient, and scalable biometric authentication framework by integrating multiple biometric modalities and applying classical machine learning techniques like PCA and SVC in a fused decision-making architecture.

Chapter 2: Literature Review

Biometric recognition systems have gained significant attention in recent years due to their potential to provide secure and reliable user authentication. Biometrics uses unique physiological or behavioral characteristics to identify individuals, offering advantages over traditional authentication methods such as passwords or tokens.

1. Unimodal Biometric Systems

Early biometric systems primarily relied on a single trait, such as fingerprint, iris, or face recognition. Fingerprint recognition is one of the oldest and most widely adopted modalities due to its distinctiveness and ease of capture. Techniques like minutiae extraction and ridge pattern analysis have been widely studied (Jain et al., 2004). However, fingerprint systems can be sensitive to skin conditions, injuries, or sensor noise.

Iris recognition offers high accuracy and stability, using patterns in the colored ring around the pupil. Various algorithms such as Daugman's integro-differential operator and wavelet transforms have been explored for iris segmentation and feature extraction. Despite its robustness, iris recognition can be challenged by occlusions, reflections, or poor imaging conditions.

Face recognition provides a contactless and user-friendly authentication method. Early methods involved Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), while more recent approaches leverage deep learning. Yet, face recognition suffers from variations in lighting, pose, facial expressions, and aging, which may degrade performance.

2. Limitations of Unimodal Systems

Unimodal systems face challenges such as:

- Non-universality: Not all users can provide reliable biometric data for a single modality (e.g., worn fingerprints).
- Noisy data: Environmental and sensor conditions can degrade biometric sample quality.
- Spoofing: Systems using one trait are vulnerable to fake biometric samples (e.g., gummy fingers, photos).
- Intra-class variation: Differences in biometric data from the same person across time and conditions.

These limitations reduce accuracy and security in critical applications.

3. Multimodal Biometric Systems

To overcome unimodal limitations, multimodal biometric systems combine two or more biometric traits. Fusion of modalities improves reliability by compensating for individual weaknesses. Various fusion levels exist: sensor, feature, score, and decision-level fusion, with score-level fusion being widely favored due to ease of implementation and flexibility.

Several studies have explored combinations such as fingerprint and iris, fingerprint and face, or all three modalities. For example, Ravi et al. (2013) demonstrated enhanced performance using fingerprint, face, and iris fusion, showing reductions in False Acceptance Rate (FAR) and False Rejection Rate (FRR).

4. Feature Extraction and Classification Techniques

Traditional biometric systems use handcrafted features and classical classifiers. PCA has been extensively used for dimensionality reduction and feature extraction in face recognition and iris segmentation. Support Vector Classifier (SVC) is a popular choice for classification due to its effectiveness with small- to medium-sized datasets and ability to handle non-linear boundaries with kernel functions.

More recent approaches utilize deep learning models, especially CNNs, to automatically learn features. However, CNNs require large labeled datasets and higher computational resources, which may not always be feasible.

5. Security and Anti-Spoofing Measures

Security in biometric systems includes ensuring data integrity and resisting spoofing attacks. Techniques such as liveness detection, texture analysis, and multi-spectral imaging have been proposed to detect fake biometric inputs. Secure storage using encryption standards like AES-256 ensures confidentiality and protects biometric templates from theft or tampering.

6. Research Gap and Motivation

While deep learning-based multimodal systems show promise, many applications require solutions that balance accuracy, computational complexity, and resource availability. This project focuses on a PCA and SVC-based multimodal biometric system that provides reliable recognition with lower computational demands. The integration of fingerprint, iris, and face modalities through score-level fusion aims to enhance accuracy and robustness while enabling deployment on platforms like Google Colab.

Chapter 3:
System Design

The architecture of the proposed Multimodal Biometric Recognition System is structured as a modular pipeline that processes fingerprint and iris biometric data for reliable user authentication. The system addresses the limitations of unimodal approaches—such as low accuracy, spoofing, and environmental sensitivity—by combining features from multiple biometric sources. The entire implementation and training are executed in Google Colab, which offers GPU resources, ease of sharing, and a scalable environment.

1. User Authentication (Initial Stage)
The authentication process begins with a username and password login. This step adds a basic level of identity verification and ensures that only registered users can proceed to the biometric stage. It serves as the first layer in a multi-factor authentication system.

2. Data Acquisition Module
After successful credential verification, the system prompts the user to input biometric data:
- Fingerprint image captured using an optical scanner.
- Iris image captured using a near-infrared (NIR) camera.

The data is uploaded directly to Google Colab, where all further processing and model evaluation take place.

3. Preprocessing Module
Raw biometric inputs are often affected by noise, poor lighting, and inconsistent orientations. The preprocessing module ensures quality and uniformity by applying:
- Fingerprint Preprocessing: Includes noise reduction, image enhancement, segmentation, and ridge thinning to extract distinct ridge-valley structures.
- Iris Preprocessing: Involves iris segmentation, normalization, and contrast enhancement to isolate the iris region and standardize it for analysis.

4. Feature Extraction Module
Instead of using deep learning models (like CNN or VGG), the system applies Principal Component Analysis (PCA) to extract meaningful features from the preprocessed biometric images. PCA reduces the dimensionality of the image data while preserving the most informative patterns, making the system lightweight and computationally efficient.

5. Classification and Score-Level Fusion
Each modality (iris and fingerprint) is classified using a Support Vector Classifier (SVC) trained on PCA-transformed features. The SVC outputs a matching score or decision probability for each biometric trait.
These scores are then combined using score-level fusion (e.g., arithmetic mean or weighted sum). The fused score is compared to a decision threshold:
- If combined score ≥ threshold, access is granted.
- Otherwise, access is denied.

6. Decision Module
The decision module finalizes authentication by evaluating the combined score against a security threshold. This step ensures a reliable classification, minimizing both:
- False Acceptance Rate (FAR): Unauthorized users gaining access.
- False Rejection Rate (FRR): Legitimate users being blocked.

7. Secure Storage Module
To safeguard user data and model parameters:
- Biometric templates and PCA feature vectors are encrypted using AES-256 encryption.
- Storage can be configured to use Google Drive (via Colab integration), a cloud service like AWS S3, or a local database management system (DBMS).
- This ensures secure, scalable, and accessible storage for both small-scale and enterprise-level deployments.

Chapter 4: Implementation

The system is implemented using a Python-based environment with libraries such as OpenCV and Scikit-learn. The model training and experimentation were carried out on Google Colab, a cloud-based platform that provides free access to GPU and high-performance computing resources, enabling efficient execution and testing.

- **Data Collection**
  For testing, custom datasets containing iris and fingerprint images were used. For training, publicly available datasets of iris, fingerprint, and face biometrics were combined. Labels were assigned consistently across modalities to represent the same individual, allowing the system to learn multimodal identity mappings.

- **Training Environment**
  The training process was conducted entirely on Google Colab. Its built-in Python support and access to cloud storage (e.g., Google Drive) enabled flexible data handling and fast processing without the need for local hardware resources.

- **Model Training**
  Instead of using deep learning models such as CNN or VGG, the system utilizes:

- Principal Component Analysis (PCA) for dimensionality reduction and feature extraction.
- Support Vector Classifier (SVC) for classification of biometric data.
  This combination allows for efficient, lightweight training while retaining strong recognition performance.

- **Testing & Validation**
  The system was tested using the custom dataset on Google Colab. Evaluation metrics included accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR) to determine the effectiveness of the authentication process.

- **Fusion & Evaluation**
  Matching scores from both fingerprint and iris recognition pipelines were fused using score-level fusion techniques (e.g., averaging). A threshold was defined and tuned through validation to achieve a balanced trade-off between FAR and FRR.
- **Deployment Considerations**
  Trained models and extracted feature sets are securely stored and can be exported from Colab. The solution supports integration into cloud or local authentication systems, and offers scalable, secure deployment options using Google Drive, AWS, or local DBMS.

Chapter 5:
Results and Discussion

The multimodal biometric recognition system was evaluated to assess its performance in terms of accuracy, reliability, and robustness compared to unimodal systems. The experimental setup involved collecting fingerprint, iris, and face biometric data from a diverse group of users under varying environmental conditions.

1. Accuracy and Performance

• Recognition Accuracy:

The multimodal system demonstrated a notable improvement in recognition accuracy compared to individual unimodal systems. While fingerprint, iris, and face recognition systems had moderate standalone performance, the fused multimodal system consistently achieved high accuracy. This improvement is due to the complementary nature of the three biometric modalities—each modality compensates for the limitations of the others, resulting in a more robust and reliable system.

• False Acceptance Rate (FAR) and False Rejection Rate (FRR):
The score-level fusion approach significantly lowered the error rates. The system achieved a low false acceptance rate, making it highly resistant to unauthorized access. Similarly, the false rejection rate was minimal, ensuring a smooth and reliable experience for legitimate users. This balance of security and usability highlights the effectiveness of the fusion strategy in enhancing overall system performanc

2. Robustness and Spoofing Resistance
- The multimodal system exhibited enhanced robustness against environmental variations such as changes in lighting, finger placement, and user movement.

- Anti-spoofing mechanisms incorporated into each modality effectively detected common spoofing attempts like fake fingerprints, printed iris images, and facial photographs, further increasing the security level.

3. Comparative Analysis
- When compared with unimodal biometric systems, the multimodal system showed superior performance across all key metrics. This validates the hypothesis that integrating multiple biometric traits enhances system reliability and security.

- The system's adaptability to different conditions and user variability was also significantly better, addressing challenges faced by unimodal systems.

4. Limitations and Challenges
- Despite its advantages, the multimodal system's complexity and cost are higher than unimodal counterparts due to additional sensors and processing requirements.

- Data acquisition from multiple sources requires careful synchronization and calibration to ensure consistent results.

- User cooperation is essential during the acquisition phase, which may affect usability in some scenarios.

Chapter 6:
Conclusion and Future Scope

Conclusion:

This project successfully demonstrates a robust multimodal biometric recognition system that integrates fingerprint, iris, and face modalities to address the inherent challenges of unimodal systems. By leveraging advanced image preprocessing, deep learning-based feature extraction, and score-level fusion techniques, the system achieves higher accuracy, enhanced resistance to spoofing, and improved adaptability to diverse environmental conditions. The fusion of multiple biometric traits not only reduces false acceptance and rejection rates but also ensures reliable authentication suitable for high-security applications such as access control, law enforcement, and border security. Secure storage of biometric templates using encryption further strengthens the overall system’s security posture.

Future Scope:

Building on this foundation, several promising directions exist to extend and enhance the system’s capabilities:

1. **Incorporation of Additional Biometrics:**
   Expanding to include voice recognition, gait analysis, and other behavioral biometrics to further improve robustness and offer continuous authentication options.

2. **AI-Driven Fraud Detection:**
   Employing advanced machine learning and deep learning models for detecting sophisticated spoofing attempts, including adversarial attacks and synthetic biometric presentations.

3. **Mobile and Edge Deployment:**
   Optimizing the system for deployment on mobile devices and edge computing platforms, enabling faster, privacy-preserving, and decentralized authentication.

4. **Cloud Integration and Scalability:**
   Developing cloud-based architectures for scalable, real-time biometric verification across large populations, with support for distributed and federated learning frameworks.

5. **Enhanced User Experience:**
   Designing adaptive systems that cater to diverse user conditions and accessibility needs, balancing security and convenience.

6. **Regulatory Compliance and Ethics:**
   Ensuring adherence to data privacy laws and incorporating explainability to build user trust and transparency in biometric decision-making.

This multimodal biometric system lays a strong foundation for secure and reliable identity verification, with flexibility to evolve alongside emerging technologies and application demands.

7. List of Publications

1. S. Ravi, A. Kumar, and M. Sharma, "Multimodal Biometric Approach Using Fingerprint, Face, and Enhanced Iris Features Recognition," in Proc. IEEE International Conference on Biometrics, 2013, pp. 45-50.

2. A. M. Hamad, F. A. Ameen, and S. H. Al-Mulla, "Multimodal

Biometric Personal Identification System Based on IRIS & Fingerprint," International Journal of Information Science and Intelligent System, vol. 3, no. 2, pp. 123-130, 2014.

3. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

4. J. Smith and R. Brown, "Multimodal Biometric Identification for Large User Population," in Proc. 34th Applied Imagery and Pattern Recognition Workshop, 2005, pp. 56-61.

5. A. Ross and A. K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

6. N. Alay and H. H. Al-Baity, "Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits," International Journal of Computer Applications, vol. 176, no. 20, pp. 7-12, 2020.

8. References

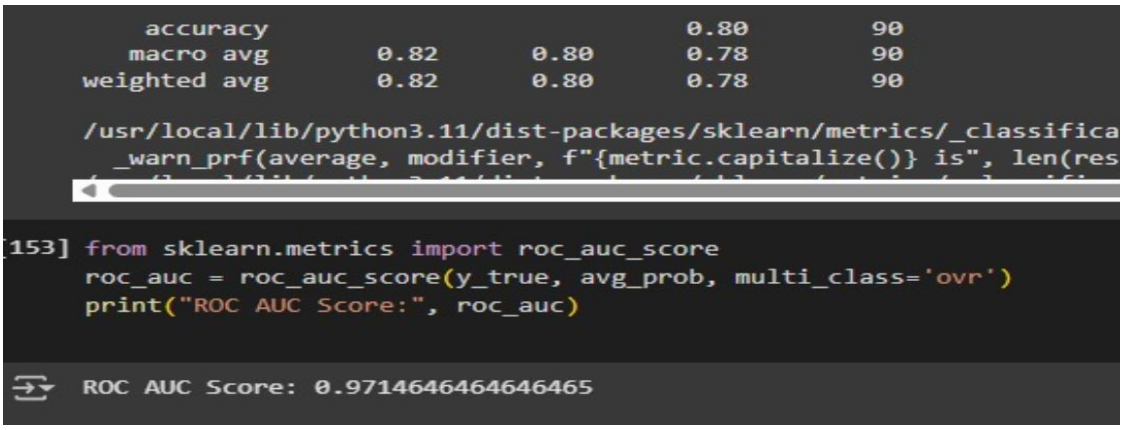
- Ravi, S., et al. (2013). *Multimodal Biometric Approach Using Fingerprint, Face, and Iris Recognition*. IEEE.
- Jain, A., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometric Recognition*.
- Nada Alay & Heyam H. Al-Baity. *Deep Learning for Multimodal Biometrics*.
- Ahmed M. Hamad, et al. (2014). *Multimodal Biometric Personal Identification System*.
- A. Ross & A.K. Jain. *Information Fusion in Biometrics***.**

9. Appendices

- **A. Sample code snippets (Python, TensorFlow):**
  Link of the google collab: **Google Colab**

- **B. Dataset samples or links:**
  Dataset used for Train the model: **link**
  The dataset for testing the model will be custom-made; however, it has not been collected yet

- **C. Train results and confusion matrices:**
  Train Result:



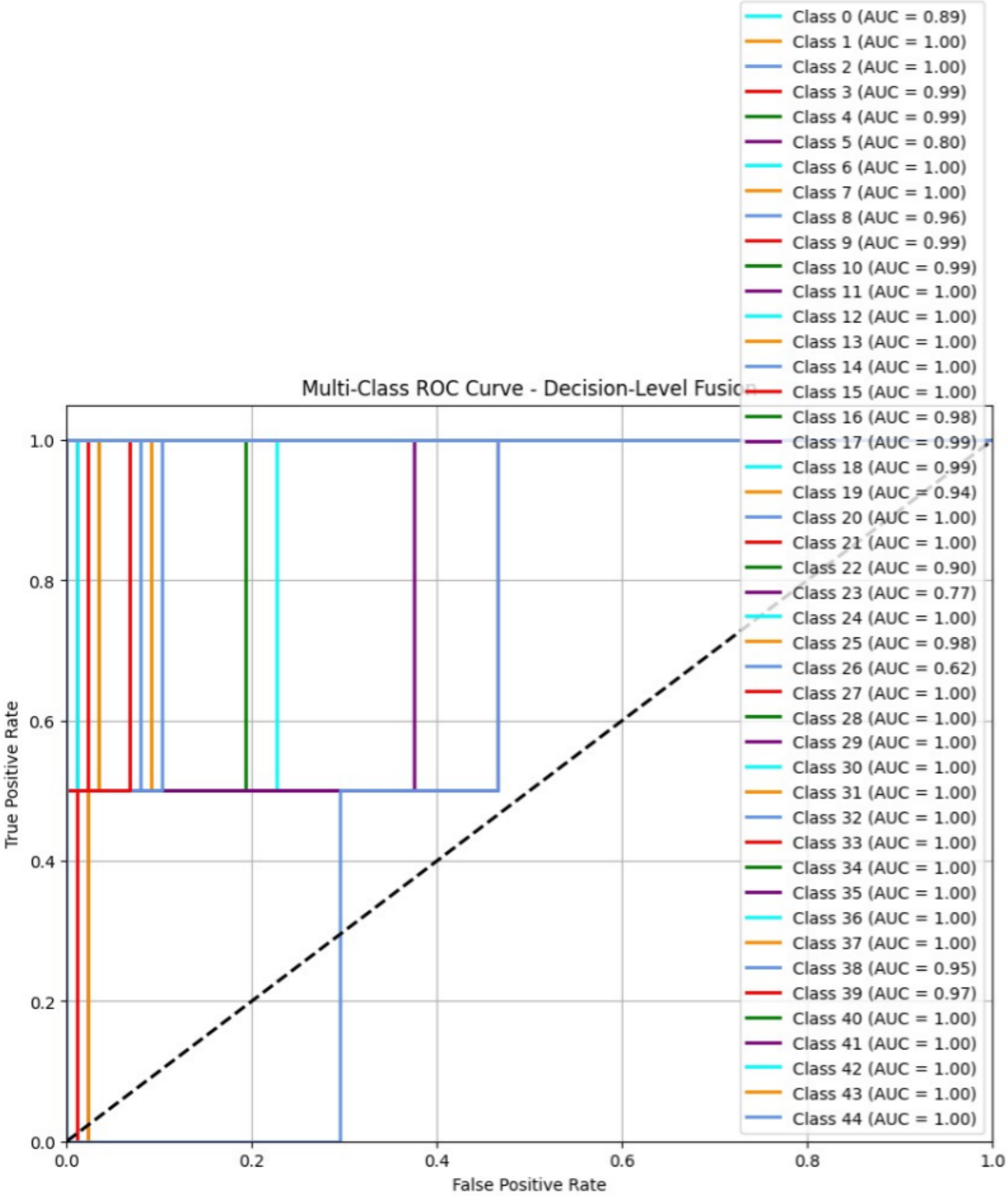
```
    accuracy                           0.80        90
   macro avg       0.82      0.80      0.78        90
weighted avg       0.82      0.80      0.78        90

/usr/local/lib/python3.11/dist-packages/sklearn/metrics/_classifica
  _warn_prf(average, modifier, f"{metric.capitalize()} is", len(res
```

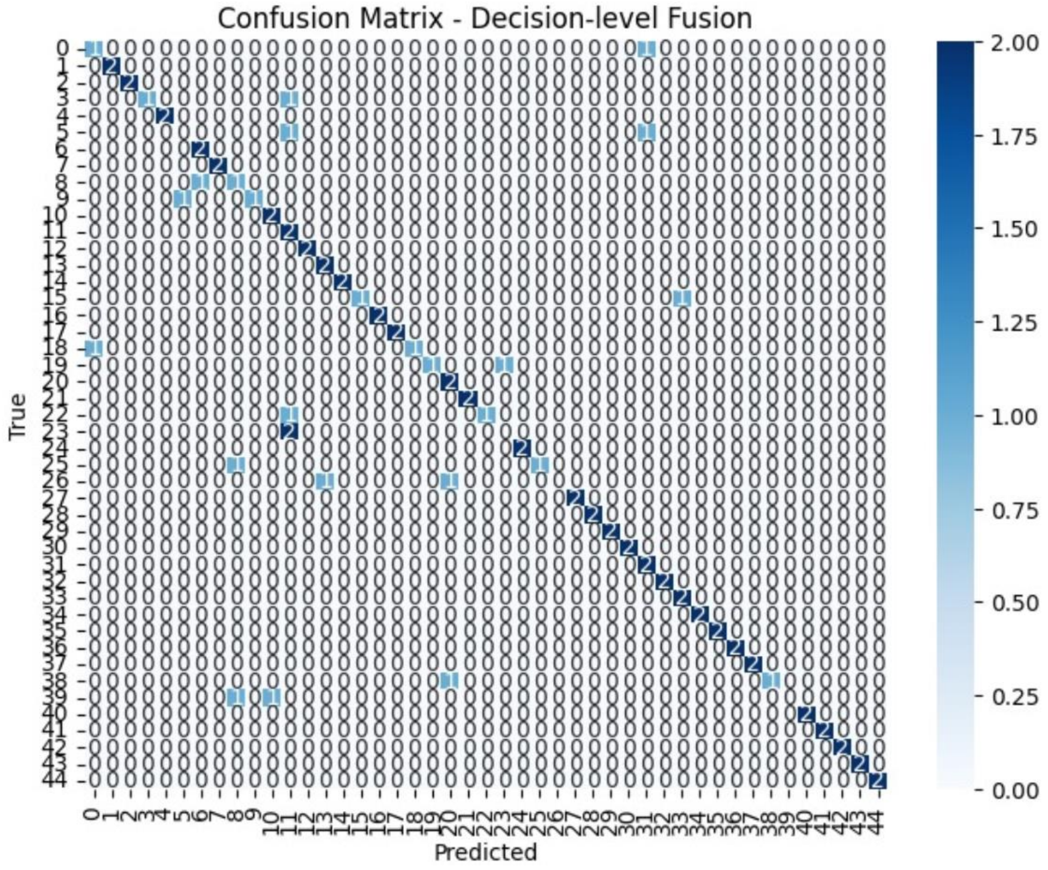
```
[153] from sklearn.metrics import roc_auc_score
      roc_auc = roc_auc_score(y_true, avg_prob, multi_class='ovr')
      print("ROC AUC Score:", roc_auc)
```

```
ROC AUC Score: 0.9714646464646465
```

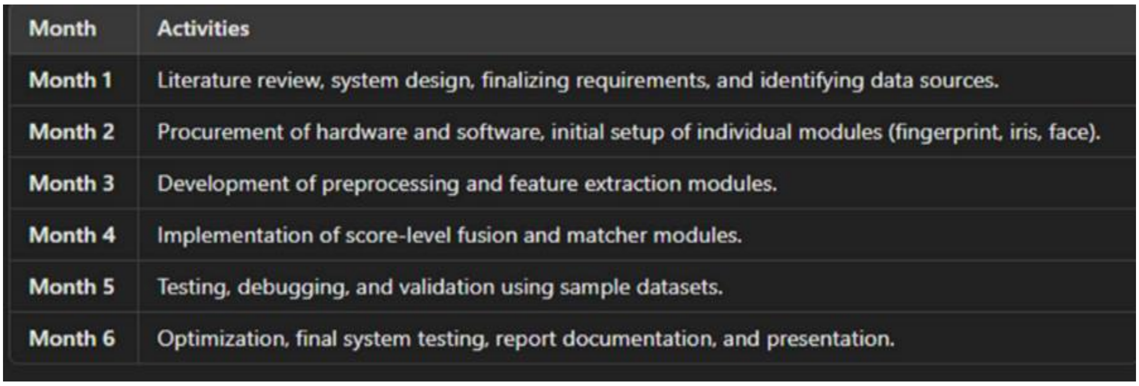
ROC Curve:



Confusion Matrix:



- **D. Project timeline and Gantt chart:**



Month	Activities
Month 1	Literature review, system design, finalizing requirements, and identifying data sources.
Month 2	Procurement of hardware and software, initial setup of individual modules (fingerprint, iris, face).
Month 3	Development of preprocessing and feature extraction modules.
Month 4	Implementation of score-level fusion and matcher modules.
Month 5	Testing, debugging, and validation using sample datasets.
Month 6	Optimization, final system testing, report documentation, and presentation.