Multimodal Biometric Authentication System: Project Report

1. Introduction

In today's digital world, security and authentication have become major concerns. Traditional password-based authentication systems have several vulnerabilities, including the risk of being hacked, forgotten, or stolen. Biometric authentication provides a more secure and convenient alternative, as it relies on unique biological traits like fingerprints, facial features, or voice patterns. However, single biometric systems (unimodal) have their own set of limitations, such as poor recognition under challenging environmental conditions or susceptibility to spoofing attacks.

To overcome these drawbacks, we have developed a **Multimodal Biometric Authentication System** that integrates **Face and Voice Biometrics** using **feature-level fusion**. By combining two biometric modalities, the system improves overall authentication accuracy, robustness, and security.

This project is part of the **Midterm AI Application Requirement**, and for the **Final Project**, we will be evaluating various **trustworthiness aspects**, such as **fairness, privacy, robustness, and explainability**, to ensure our system is not only efficient but also ethical and reliable.

2. Project Objectives

The primary objectives of this project are:

- **Developing an AI-powered biometric authentication system** that combines face and voice recognition for better security.
- **Enhancing authentication accuracy** by fusing multiple biometric features.
- **Training and evaluating different machine learning models** such as **Random Forest, SVM, k-NN** and advanced deep learning techniques like **CNNs and LSTMs**.
- **Ensuring security and privacy** by incorporating encryption techniques and fairness testing.
- **Providing a functional and user-friendly interface** for real-time authentication.

3. System Architecture

The project follows a **structured and modular design**, consisting of various stages such as data preprocessing, feature extraction, feature fusion, model training, performance evaluation, and user interface development.

3.1 Major Components of the System

1. **Data Collection**
    - Face images and voice samples are collected from publicly available biometric datasets.
2. **Preprocessing & Feature Extraction**
    - **Face Processing:** Images are resized, normalised, and edge features are extracted using computer vision techniques.
    - **Voice Processing:** Audio samples are resampled, and features like **Mel-Frequency Cepstral Coefficients (MFCCs) and spectral contrast** are extracted.
3. **Feature-Level Fusion**
    - The extracted face and voice features are combined into a single vector for each user to improve recognition accuracy.
4. **Model Training & Performance Evaluation**
    - The system is trained using **Random Forest, SVM, and k-NN classifiers** for traditional ML models and **CNNs & LSTMs** for deep learning-based authentication.
    - The model performance is evaluated using various metrics such as **Confusion Matrix, ROC Curve, Equal Error Rate (EER), and d-prime calculations**.
5. **User Interface & Deployment**
    - A **Tkinter-based graphical interface** is implemented, allowing users to authenticate themselves using face and voice biometrics in real-time.
    - The system is designed to be **API-ready** for future integration with other applications.

4. Implementation Details

4.1 Technologies & Tools Used

- **Programming Language:** Python
- **Machine Learning Libraries:** Scikit-learn, TensorFlow, OpenCV, Librosa

- **Data Processing:** Pandas, NumPy, Seaborn, Matplotlib
- **User Interface:** Tkinter
- **Security & Trustworthy AI Methods:** Data encryption, fairness checks, and explainability models like SHAP & LIME

4.2 Data Processing & Model Training

- The face and voice datasets are aligned to maintain consistency across user identities.
- **SMOTE (Synthetic Minority Oversampling Technique)** is applied to handle class imbalances and improve generalisation.
- The dataset is split into **training and testing sets**, and models are trained using **Stratified k-Fold Cross Validation (k=5)**.
- Performance evaluation includes:
    - **Accuracy**
    - **Receiver Operating Characteristic (ROC) AUC**
    - **Equal Error Rate (EER)**
    - **D-prime value for measuring separability between classes**

5. Experimental Results & Performance Evaluation

5.1 Performance Metrics Comparison

Metric	Face-Only	Voice-Only	Multimodal
Accuracy	99%	95%	99%
ROC AUC	1.00	0.99	1.00
EER	0.0001	0.0149	0.0001
d-prime	11.98	4.93	12.22

- **The multimodal system outperformed unimodal systems, proving that integrating face and voice biometrics leads to better authentication.**
- **SVM provided the highest accuracy, followed closely by Random Forest.**

- **Lower Equal Error Rate (EER) in the multimodal system indicates fewer authentication errors, enhancing security.**

6. Trustworthiness & Ethical Considerations (Final Project Focus)

For the **final phase**, we will be evaluating and improving the **trustworthiness aspects** of the system to ensure fairness, privacy, and robustness.

- **Fairness & Bias Mitigation:**
    - We will analyse whether the model performs equally well across different demographics and implement bias-mitigation techniques if required.
- **Privacy & Security Measures:**
    - Implement encryption techniques to protect biometric data.
    - Explore differential privacy methods for securing sensitive data.
- **Explainability & Transparency:**
    - Integrate explainable AI methods such as **SHAP and LIME** to interpret model decisions and improve trustworthiness.
- **Robustness & Resilience:**
    - Conduct adversarial attack simulations to test system robustness against spoofing and noisy inputs.

7. Future Scope & Enhancements

- **Deep Learning Expansion:** Implement advanced deep learning models such as **transformers and GANs** for better feature extraction.
- **Exploring Alternative Fusion Techniques:** Compare **feature-level, score-level, and decision-level fusion**.
- **Dataset Expansion:** Incorporate **real-world biometric samples** for increased generalisation.
- **Enhanced UI & Deployment:** Improve UI interactivity and integrate **real-time authentication testing**.
- **Full-Scale Trustworthy AI Framework:** Implement fairness, privacy, and security best practices for future biometric systems.

8. Conclusion

This project successfully demonstrates that **multimodal biometric authentication is a more secure and accurate approach** compared to traditional unimodal methods. The integration of **face and voice biometrics** significantly improves **authentication performance, security, and reliability**.

Moving forward, we will focus on **evaluating the system's fairness, privacy, and security aspects**, ensuring that our biometric system is **trustworthy and ethically sound** for real-world applications.

9. References

1. Jain, A., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer.
2. Viola, P., & Jones, M. (2001). Rapid Object Detection Using a Boosted Cascade of Simple Features. IEEE CVPR.
3. Chen, L., et al. (2020). Privacy and Bias in Biometric Systems. IEEE Transactions on Information Forensics and Security.

Developed by:

- **Aishwarya Rao Kallepu**
- **Anil Reddy Vangala**
- **Shashidhar Reddy Kamatham**