Group - 18 **Midterm Project Report** **Aishwarya Rao Kallepu**
Shashidhar Reddy Kamatham
Anil Reddy Vangala

CIS 6930 Trustworthy AI Systems – Spring 2025
Submitted to Professor Guangjing Wang, Department of Computer Science
University of South Florida
10th March 2025

Project Title: Multimodal Biometric Authentication System

1. Introduction:

In today's digital world keeping our accounts and data safe is very important. Traditional passwords are not always secure as they can be hacked or forgotten. A better way is to use biometric authentication which means using unique human features like the face or voice to confirm identity.

But using only one type of biometric like just the face or just the voice can have problems. For example, bad lighting can make it hard for face recognition to work and a noisy place can make voice recognition fail. Also, some people may try to trick the system by using photos or recorded voices.

To fix these issues this project introduces a **Multimodal Biometric Authentication System** which uses both face and voice together. This makes the system more secure and accurate compared to using only one method.

This project is being developed as part of a midterm AI application. The final project will test how fair private strong and understandable the system is.

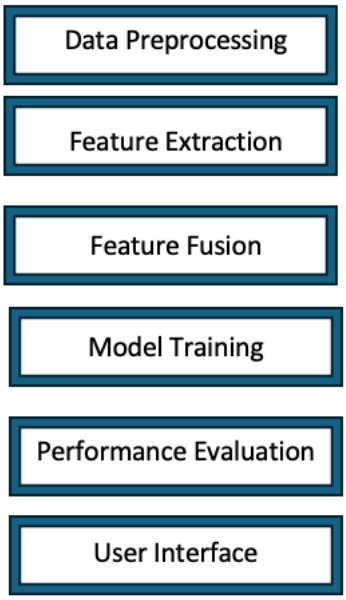
2. Project Objective:

The main goals of this project are:

- Developing an AI-based biometric authentication system that integrates face and voice recognition.
- Improving authentication accuracy by using multiple biometric features instead of a single feature.
- Training and evaluating machine learning models such as Random Forest, SVM, k-NN, and deep learning models like CNNs and LSTMs.
- Ensuring privacy and security through encryption and fairness testing.
- Providing a simple and efficient user interface for authentication.

3. System Architecture:

This system is designed in a structured manner, covering all essential stages: Data Preprocessing, Feature Extraction, Feature Fusion, Model Training, Performance Evaluation and User Interface Development.



3.1 Key Components of the System

1. **Data Collection**
   - Face images and voice recordings are sourced from publicly available biometric datasets.
2. **Preprocessing & Feature Extraction**
   - **Face Processing:** Images are resized, normalized, and edge features are extracted for better accuracy.
   - **Voice Processing:** Audio recordings are resampled, and features such as Mel-Frequency Cepstral Coefficients (MFCCs) and spectral contrast are extracted to capture key speech characteristics.
3. **Feature-Level Fusion**
   - The extracted face and voice features are merged into a single feature vector for each user, leading to improved recognition accuracy.
4. **Model Training & Performance Evaluation**
   - The system is trained using Random Forest, SVM, and k-NN classifiers for machine learning and CNNs & LSTMs for deep learning-based authentication.

- Performance is evaluated using metrics such as Confusion Matrix, ROC Curve, Equal Error Rate (EER), and d-prime calculations.

5. **User Interface & Deployment**
   - A Tkinter-based graphical interface allows real-time authentication through face and voice input.
   - The system is API-ready for seamless integration into real-world applications.

4. Implementation Details:

4.1 Technologies & Tools Used

- Programming Language: Python
- Libraries Used: Scikit-learn, TensorFlow, OpenCV, Librosa
- Data Processing: Pandas, NumPy, Seaborn, Matplotlib
- User Interface Development: Tkinter
- Security Measures: Encryption, fairness testing, explainability tools like SHAP & LIME

4.2 Data Processing & Model Training

- Face and voice datasets are aligned to maintain consistency in identity mapping.
- SMOTE (Synthetic Minority Oversampling Technique) is used to handle class imbalances and improve model performance.
- The dataset is split into training and testing sets, with models trained using Stratified k-Fold Cross Validation (k=5).
- Evaluation criteria include:
  - Accuracy
  - Receiver Operating Characteristic (ROC) AUC
  - Equal Error Rate (EER)
  - D-prime value (to distinguish between genuine and impostor users)

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 performed significantly better than unimodal systems.
- SVM delivered the highest accuracy, followed by Random Forest.
- Lower Equal Error Rate (EER) in the multimodal system ensures better security and fewer false positives.

6. Trustworthiness & Ethical Considerations (Final Project Focus):

In the **Final Project**, we will assess and enhance the **trustworthiness** of the system, focusing on:

- **Fairness & Bias Mitigation:**
  - Evaluating model performance across different demographics to ensure fair recognition.
  - Implementing bias-mitigation techniques if discrepancies are found.
- **Privacy & Security Measures:**
  - Encrypting biometric data to prevent unauthorized access.
  - Exploring differential privacy to safeguard user data.
- **Explainability & Transparency:**
  - Using SHAP and LIME to provide transparency in model decisions.
- **Robustness & Reliability:**
  - Conducting adversarial attack testing to ensure resistance to spoofing and external threats.

7. Future Enhancements:

- **Enhancing Deep Learning Models:** Implementing transformers and GANs for more accurate biometric feature extraction.
- **Exploring Different Fusion Techniques:** Comparing feature-level, score-level, and decision-level fusion approaches.
- **Dataset Expansion:** Using real-world biometric samples to improve model generalization.
- **Better UI & Deployment:** Making the user interface more interactive with real-time authentication testing.
- **Building a Full-Scale Trustworthy AI Framework:** Incorporating fairness, privacy, and security best practices into the authentication system.

8. Conclusion:

This project shows that using both face and voice for authentication is much safer and more reliable than using just one of them. By combining these two biometrics the system becomes more accurate secure and strong.

In the future we will work on making the system fair, private (privacy) and secure (security), so that it stays trustworthy and free from bias while being strong enough for real-world use.

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.