Multimodal Biometric Authentication System for Military Weapon Access: Face and ECG Authentication

Summer internship program on “AIoT and it’s Applications”
Center for Training and Learning, NIT Warangal

Abstract

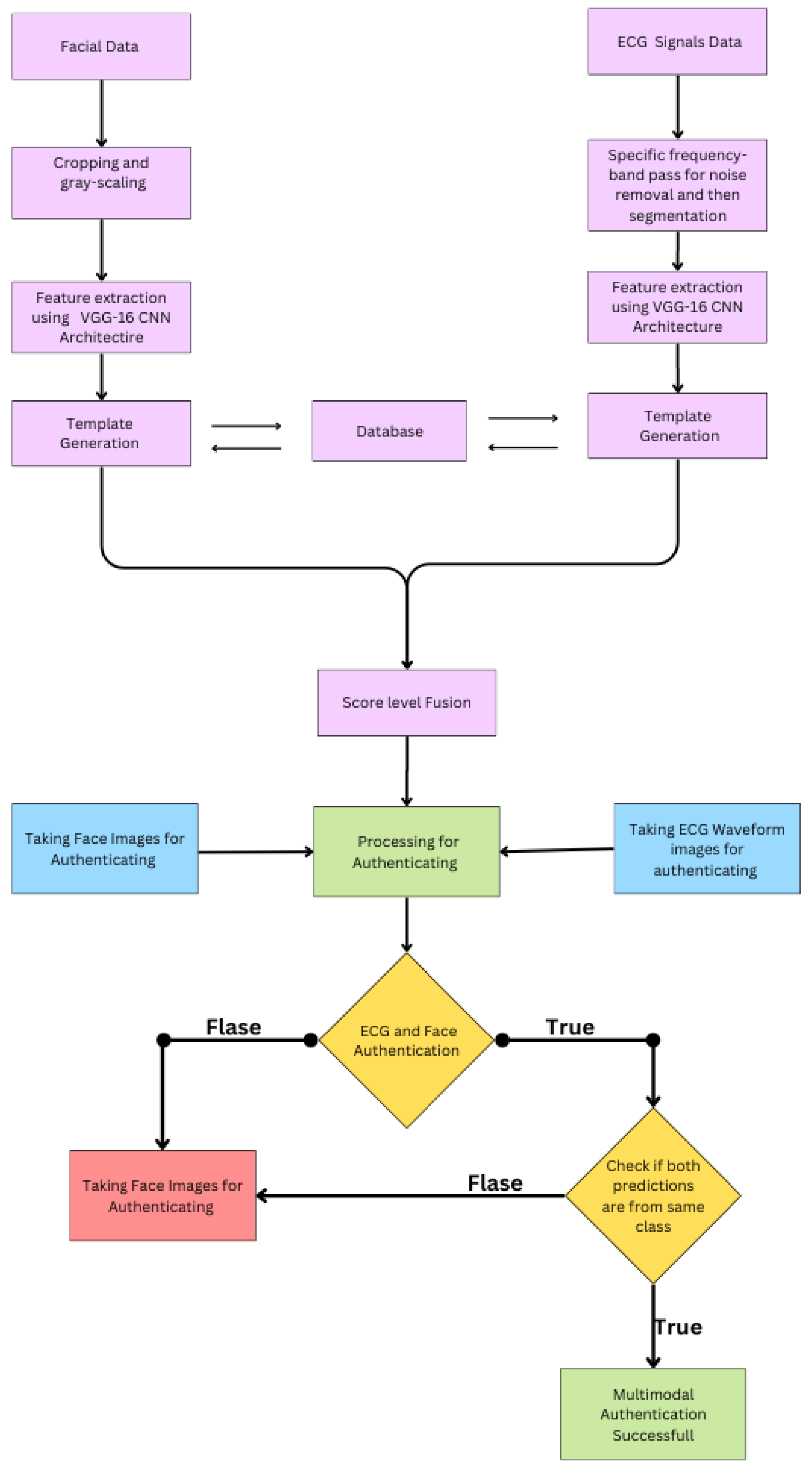
Unimodal biometric systems rely on a single source of biometric data, like fingerprints or facial features, which can lead to higher error rates and security vulnerabilities. A multimodal biometric system, which authenticates multiple times, offers high accuracy, low error rates, and larger population coverage. This system enhances integrity and privacy by storing different biometric characteristics for each user. A multimodal biometric project uses deep learning to enhance authentication security by combining face and electrocardiogram (ECG) signals. The VGG-16 model captures complex patterns in individual identification, while high-resolution convolutional filters capture intricate details, ensuring high accuracy in distinguishing individuals.

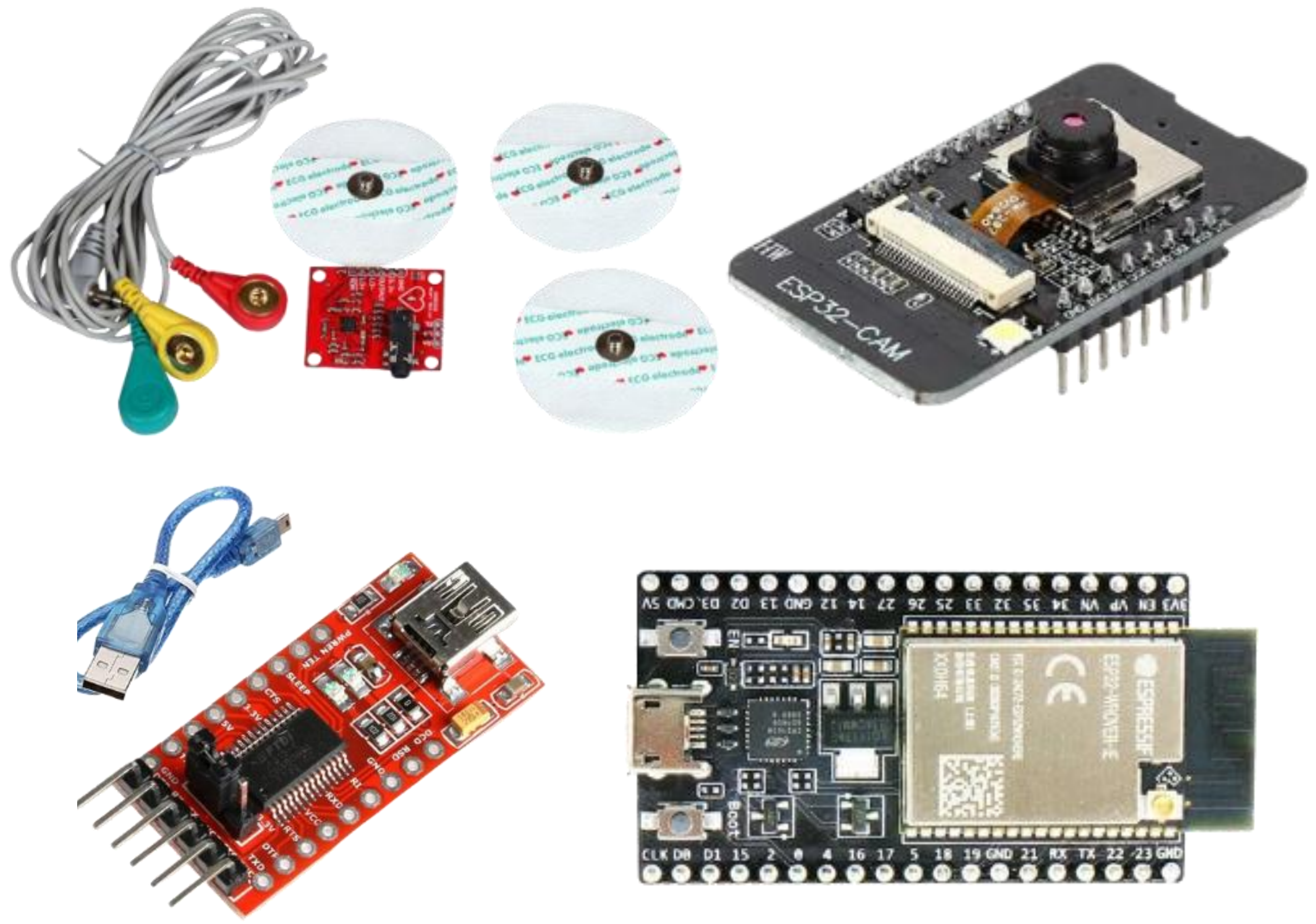
Introduction

The project aims to develop a military biometric system using ECG waveforms and facial recognition. This system enhances security by identifying individuals and preventing unauthorized access and identity theft. It creates a reliable two-step verification process, making it harder for fake identities to succeed. The goal is to provide secure access to resources for military personnel while protecting sensitive information. The research aims to advance biometric technology for military needs, demonstrating the commitment to enhancing security in military settings. This project represents a significant step forward in protecting military forces worldwide.

Methodology

The study focuses on developing ECG biometric systems that accurately identify individuals based on their unique cardiac signatures. ECG data has taken using AD8232 sensor from 30 individual persons, parallelly taken facial data from same persons. The Database contains annotated recordings of ECG signals capturing various heart rhythms and anomalies. VGG-16 is used to process and extract features from ECG signals, converting waveforms into image-like representations. This allows the network to capture complex temporal and spatial patterns, enhancing recognition accuracy. VGG-16 is also used to extract facial features from high-resolution images, capturing intricate details such as the shape of the eyes, nose, and mouth, as well as variations in skin texture. The Flask library in Python is used to create a user-friendly frontend GUI that processes these inputs by loading the respective pre-trained models API for ECG authentication and face recognition. If both models predict the same class, the system declares "Authentication successful" and logs the result.


Facial Data
Cropping and gray-scaling
Feature extraction using VGG-16 CNN Architectire
Template Generation
Database
ECG Signals Data
Specific frequency-band pass for noise removal and then segmentation
Feature extraction using VGG-16 CNN Architecture
Template Generation
Score level Fusion
Taking Face Images for Authenticating
Processing for Authenticating
Taking ECG Waveform images for authenticating
ECG and Face Authentication
Flase
True
Taking Face Images for Authenticating
Flase
Check if both predictions are from same class
True
Multimodal Authentication Successfull

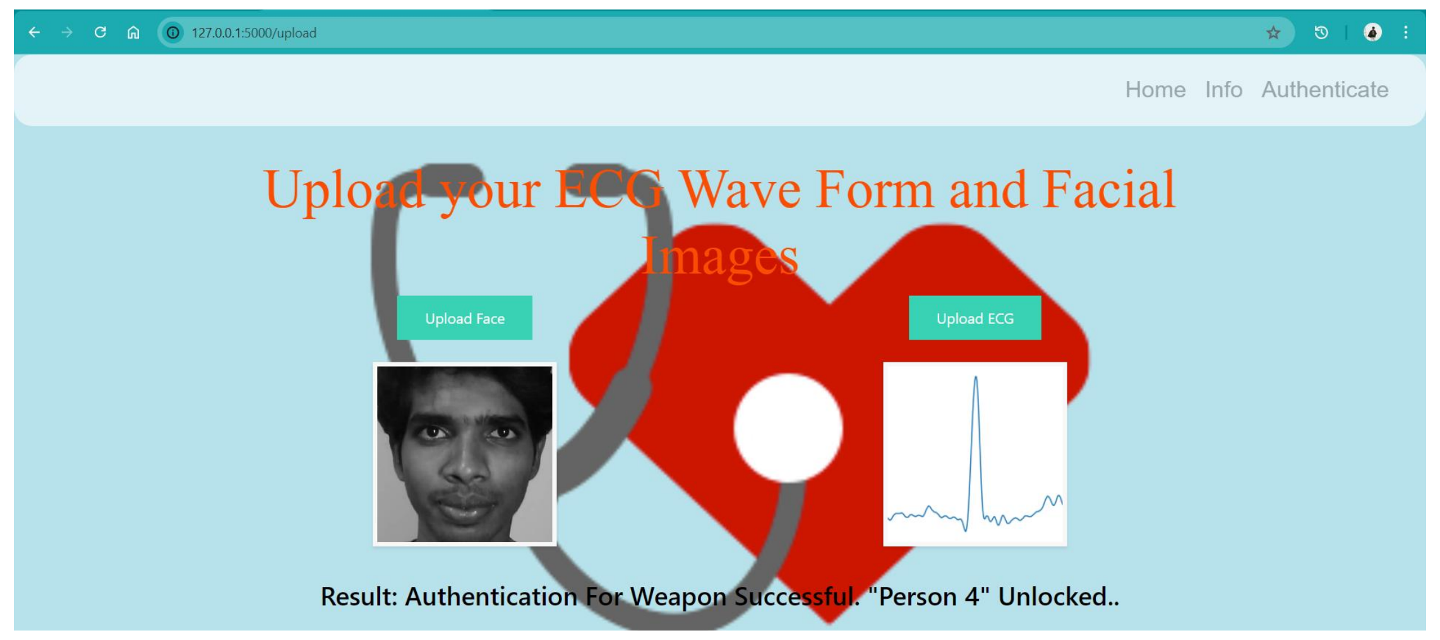


Devices used for IoT Implementation used

VGG16 Model	Face Authentication	ECG Authentication	Fusion
Accuracy	95.6%	92.08%	98.33%
Recall	94.37%	90.83%	98.36%
Precision	95.35%	91.9%	98.33%
F1 score	94.3%	92.24%	98.33%

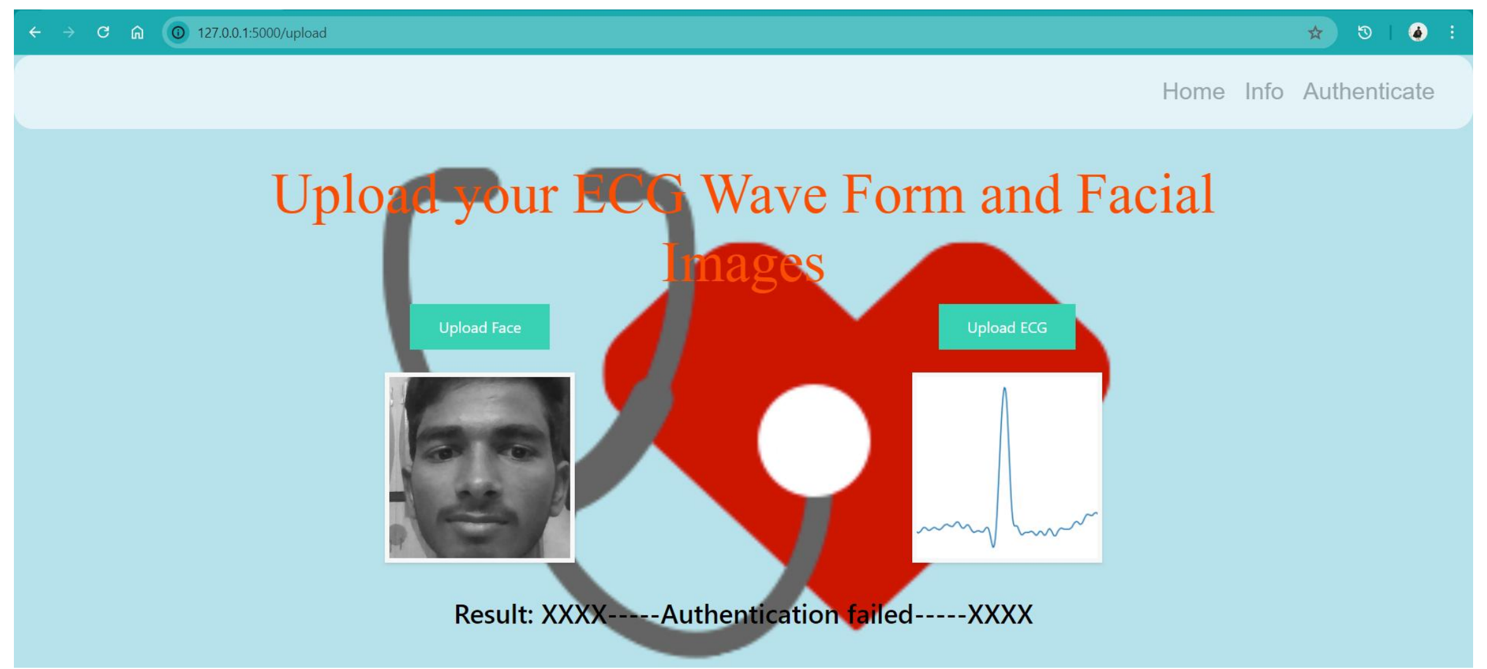
Model Metric Analysis

Results



Upload your ECG Wave Form and Facial Images

Result: Authentication For Weapon Successful. "Person 4" Unlocked..



Upload your ECG Wave Form and Facial Images

Result: XXXX-----Authentication failed-----XXXX

Conclusion

Using the obtained facial and ECG data, the system preprocesses the information to feed into a VGG16. The VGG16 then compares this data against the existing database to check for matches in both the facial features and ECG signals. If both the facial recognition and ECG graphs match the records in the database, the system grants access to the individual for military weapon access, displaying “Authentication For Weapon successful. Person (no.) Unlocked”. If either the facial features or ECG signals do not match the database records, the system displays “Authentication Failed”. In this work, with VGG16 architecture we got accuracy of 95.6% for face recognition, 92.08% for ECG recognition and fusion model accuracy is 98.33% to classify 30 different people.