INTERNSHIP PROJECT REPORT

on

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

Submitted by

ALUVOJU VIVEK (SR UNIVERSITY/ECE / 3RD YEAR)

SATHU TEJASWI (SR UNIVERSITY /ECE/ 3RD YEAR)

GAJULA HARICHANDANA (SR UNIVERSITY /CSE /3RD YEAR)

THALLA SANJANA (KITS WARANGAL /CSO/ 3RD YEAR)

Under the guidance of

Prof. T. Kishore Kumar

Professor, Department of ECE

NIT Warangal

Centre for Training and Learning

NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

HANAMKONDA-506004, TELANGANA, INDIA

Centre for Training and Learning

NATIONAL INSTITUTE OF TECHNOLOGY

WARANGAL

HANAMKONDA-506004, TELANGANA, INDIA

BONAFIDE CERTIFICATE

This is to certify that this project report entitled **“Multimodal Biometrics Authentication System For Military Weapon Access: Face and ECG Authentication”** submitted to National Institute of Technology, Warangal, is a bonafide record of work done by **“Aluvoju Vivek, Sathu Tejaswi, Gajula Harichandana, Thalla Sanjana”** under my supervision from **“3 June 2024”** to **“16 July 2024”**

Supervisor

Prof. T. Kishore Kumar

Professor, Department of ECE

NIT Warangal

Place: Warangal

Date: 16 July 2024

DECLARATION

This is to declare that this report has been written by us. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. We aver that if any part of the report is found to be plagiarized, we are shall take full responsibility for it.

Place: Warangal

Date: 16 July 2024

Submitted by:

Aluvoju Vivek

Sathu Tejaswi

Gajula Harichandana

Thalla Sanjana

ACKNOWLEDGEMENT

We extend our sincere gratitude to the following individuals and organizations whose support and contributions were instrumental in the successful completion of this project and thesis.

First and foremost, we express our deepest gratitude to Dr. T. Kishore Kumar, Professor and Head of CTL (Center for Training and Learning), NIT Warangal. His constant motivation, guidance, and unwavering support were pivotal in helping us achieve this significant milestone.

We are profoundly thankful to the management of NIT Warangal for providing exceptional lab facilities and tools that were essential for our research.

Our heartfelt thanks go to our seniors whose valuable guidance and insights were invaluable in shaping our work.

We are deeply grateful to Dr. Kishore Kumar for providing us with the opportunity to acquire such valuable knowledge through this internship.

Special thanks are due to Boeing for their generous sponsorship, which was crucial to the success of this internship program at NIT Warangal.

In conclusion, we sincerely thank everyone involved for their invaluable support and contributions. This journey would not have been possible without you, and we are truly privileged to be part of this enriching experience.

ABSTRACT

The research focuses on developing a multimodal biometric authentication system for military applications, utilizing ECG waveform and facial recognition technologies. The methodology uses Convolutional Neural Network (CNN) models based on the VGG16 architecture for both modalities. The models achieved impressive accuracies of 92.08% for ECG waveform authentication and 95.6% for facial recognition, demonstrating their efficiency in different biometric modalities. The overall accuracy obtained after combining the modalities is 98.33%. This dual-layered authentication not only enhances security but also ensures higher accuracy and user convenience, addressing the diverse needs of military applications. ECG data has taken using AD8232 sensor from 30 individual persons, parallelly taken facial data from same persons. The research demonstrates the potential of multimodal biometric systems in high-security environments, offering a compelling alternative to traditional unimodal systems. By combining physiological and facial biometric traits, the system presents a reliable and secure authentication mechanism. This study contributes to the academic field of biometric security and paves the way for practical implementations in sensitive sectors, ultimately safeguarding national security through advanced technological advancements.

INDEX

Sl.No.	Content	Pg No.
1.	Aim	7
2.	Objectives	7
3.	Introduction	8
4.	Literature Survey	10
5.	Gaps Identified in Pre-Existing Methods	11
6.	Design Methodology	12
7.	Platforms Used	19
8.	Libraries Used	21
9.	Representation of Model Data	23
10.	Flowchart	27
11.	Results	28
12.	Model Metrics Analysis	29
13.	Conclusion	29
14.	References	29

MULTIMODAL BIOMETRICS AUTHENTICATION SYSTEM FOR MILITARY WEAPON ACCESS: FACE AND ECG AUTHENTICATION

Aim

The aim of this project is to provide better security and improved accuracy for enhance military weapons access using multimodal biometrics authentication. Compared to unimodal biometrics, multimodal biometrics authentication provides double layered security which gives the authentication accurately. In this project developed multimodal biometrics authentication combining face and ECG recognition which enhances security and accuracy by leveraging two distinct biometric modalities. Here we utilized CNN (Convolutional Neural Network) VGG-16 architecture to extract features from ECG signals and facial recognition.

Objectives

System Development: To develop the system, we used VGG-16 Convolutional Neural Network (CNN) architecture for feature extraction from both face and ECG modalities.

Facial Recognition: We used VGG-16 architecture to extract facial features from medium-resolution images. The medium resolution convolutional filters captured intricate details of the face, ensuring high accuracy in distinguishing different individuals.

ECG Recognition: For this also VGG-16 architecture is used to process and extract features from ECG signals, converting waveforms into image-like representations. It captures complex patterns in accurate individual identification which adds more accuracy and also security to the system.

Real-time Tracking: Enable real-time monitoring and capturing of individual face and as well as ecg for recognition from the database to identify the individual for providing authentication.

Feature fusion: Feature fusion combines multiple data features for improved model performance.

Database management: Establish a centralized database to store ECG and facial data as image representation securely, ensuring the access to the individual correctly.

Interface: To combine the features of ECG and face biometrics, the Flask library in Python was used to create a user-friendly frontend GUI.

Introduction

Biometrics are basically the measurements taken from human body that can be used for the authentication of that specific person. We know stuff like using fingerprints, recognizing face, or scanning eyes for iris are all the part of biometrics. Other ways to identify people are by the shape of their ear, the way they sit and walk, their special body smells, the veins in their hands, and the expressions on their face. All these things are different types of biometrics and there are many more other than these. Few of them are mentioned below:

1. Iris Recognition
2. Face Recognition
3. Fingerprint Recognition
4. DNA Matching
5. ECG Recognition

6. EEG Recognition
7. Signature Recognition
8. Hand Geometry
9. Voice identification
10. Vein Recognition etc.

Multimodal biometric authentication which is more secure and accurate compared to unimodal biometrics authentication. Multimodal biometrics can be done by combining any of the two biometric methods. Multimodal biometrics provides enhanced security which makes it almost impossible to spoof or mimic. Since two biometric modalities are used in the system it gives improved accuracy.

Facial and Electrocardiogram (ECG) based biometric authentication to access miliary weapons, where in the ECG signals and Facial data are taken from military personnel for double authentication and then accessing superweapons. We can somehow forge Facial Data. So, for double layer of security check we are integrating ECG as well as Facial recognition system. Everyone's heart is somewhat different in size, shape, and position. Also, the electrical signals it produces are unique from person to person. This uniqueness will be used for biometric authentication.

Unlike fingerprints or features, which can be forged or copied, our heart's electrical signals stay the same. ECG biometrics is a technology that uses the electrical activity of an individual's heart to verify their identity. This method is so very secure, because it is based on differences in the sizes of people’s hearts as well as their shapes and anatomical structures. This makes it very difficult for one to forge or mimic ECG biometrics hence making it promising for use in highly accurate applications. It serves as a great tool for use in unsafe zones because it is a live data taken from individual. Convolutional Neural Network (CNN) VGG-16 model used for both Facial and ECG Recognition.

The aim is to develop a sophisticated authentication system that accurately identifies individuals based on their unique ECG patterns, reducing the need for manual operation and ensuring high security standards.

Literature Survey

Researched various biometric authentication methods. While commonly used methods like fingerprint, face recognition, and iris scanning provide security, they can be easily forged. To enhance security, especially for critical applications like military weapon access, we have chosen to explore multimodal biometric authentication. This approach combines facial recognition with electrocardiogram (ECG) authentication. Information on these methods was gathered from sources such as Wikipedia, Geek for Geeks, and YouTube to study and understand them better. Extensively reviewed numerous research papers on multimodal biometric authentication systems to gain a thorough understanding of the subject. While commonly used methods such as fingerprint, facial recognition, and iris scanning provide a certain level of security, they can be susceptible to forgery.

To enhance security, particularly for critical applications like military weapon access, we chose to explore multimodal biometric authentication. This approach integrates facial recognition with electrocardiogram (ECG) authentication. Research indicates that combining facial recognition with ECG authentication offers a significantly higher level of security. Facial recognition provides an additional layer of verification, while ECG authentication utilizes the unique electrical patterns of an individual's heartbeat, making it extremely challenging to forge. By reviewing and analyzing these academic sources, we confirmed that this combination of biometric methods enhances the robustness and reliability of the authentication process.

Gaps Identified in pre-existing methods

1. **Fingerprint Recognition:** Physical changes to the fingerprint, such as aging, injury, or temporary conditions like swelling, can affect its pattern and can be forged easily.
2. **Iris Recognition:** Poor lighting conditions can affect scan quality of the iris. Also, eyeglasses or contact lenses can obstruct the iris scan and lead to authentication failures.
3. **DNA Matching:** The primary drawback of DNA matching biometric authentication is the time and expense involved in collecting and analysing DNA samples.
4. **Signature Recognition:** Signature recognition biometric authentication has a main disadvantage as signatures can be easily forged just by practicing signature on paper. This making it less secure than other biometric systems.
5. **Vein Recognition:** Vein recognition biometric authentication is very costly. Because requires specialized equipment for capturing and analysing vein patterns.
6. **Voice Recognition:** There will be excessive noise in the environment, the system struggles to accurately capture and recognize the user's voice. This leads in authentication errors.

Design Methodology

Dataset Selection and Preprocessing:

ECG data has taken using AD8232 sensor from each individual persons, parallelly taken facial data from same persons. The dataset included 30 facial images of 30 different individuals .Coming to the ECG dataset, the dataset contains annotated recordings of ECG signals from 30 individuals capturing various heart rhythms and anomalies. The data was filtered out to ensure the integrity and clarity of the signals, and the ECG signals were segmented into manageable portions representing distinct cardiac cycles or intervals. The aim is to develop ECG biometric systems capable of accurately identifying individuals based on their unique cardiac signatures.

Model Training:

VGG-16 processes and extracts feature from ECG signals by converting the waveforms into image-like representations, enabling the network to utilize its convolutional layers effectively. This transformation allows VGG-16 to capture complex temporal and spatial patterns within the ECG data, which are crucial for accurate individual identification. By analyzing these intricate patterns, the model can distinguish unique characteristics in heartbeats, enhancing recognition accuracy. This capability, combined with facial features in a multimodal system, significantly boosts overall authentication performance, providing a more secure and reliable biometric solution.
Utilized VGG-16 to extract facial features from high-resolution images. The medium-resolution convolutional filters captured the intricate details of each face, ensuring high accuracy in distinguishing different individuals. By

focusing on small receptive fields, the network can effectively detect subtle features such as the shape of the eyes, nose, and mouth, as well as variations in skin texture. This detailed feature extraction leads to robust recognition performance, making VGG-16 highly suitable for biometric authentication systems.

Graphical user Interface:

To combine the features of ECG and face biometrics, the Flask library in Python used to create a user-friendly frontend GUI. The application prompts users to upload their ECG data and capture and upload their face data via a camera interface. The system 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, if not same it shows “Not authenticated”.

Hardware implementation:

Components used:

1. ESP32 CAM

Fig. 1. ESP32 CAM

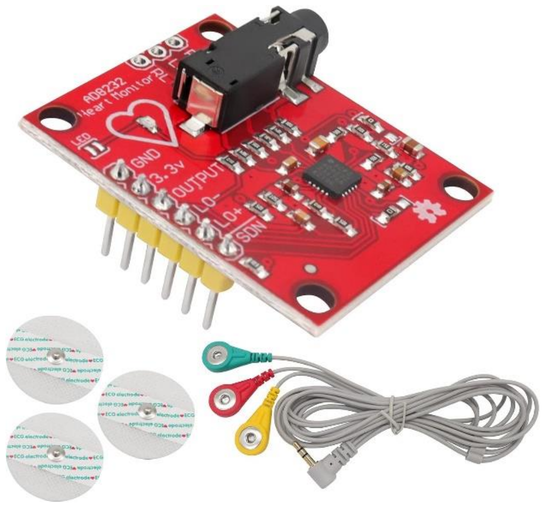

Fig. 2. AD8232 ECG sensor with Electrodes

<u>Description:</u>

The Fig.1.ESP32-CAM is a compact and versatile microcontroller module equipped with a camera. It features an ESP32-S chip with dual-core processors, integrated Wi-Fi, and Bluetooth capabilities, making it suitable for a wide range of IoT applications. The module includes a 2MP OV2640 camera, capable of capturing high-resolution images and streaming video. The ESP32-CAM has several GPIO pins for peripheral connections and supports SD card storage, allowing for image and video storage. Its small size and powerful processing capabilities make it ideal for applications like security systems, remote monitoring, and facial recognition projects.

The Fig.2. AD8232 sensor captures the electrical activity of the heart via a single lead. The AD8232 chip provides amplification and filtering, making it easier to capture clear ECG signals. Typically, three disposable electrodes are used to capture the ECG signal. These are placed on the body to detect the electrical activity of the heart. Connects the electrodes to the AD8232 module.

Red electrodes are placed on the right upper arm or the right side of the chest. Acts as the positive electrode. This placement helps in capturing the electrical signals generated by the heart as they travel through the body.

Yellow electrode is placed on the left upper arm or the left side of the chest. Serves as the negative electrode. This position forms the main lead for measuring the potential difference caused by the heart's electrical activity. Green electrode is placed on the right lower torso, near the stomach, or on the right leg. Acts as the ground electrode. It stabilizes the signal and reduces electrical noise by providing a common ground for the other two electrodes. The positioning of the electrodes is designed to capture the heart's electrical activity from different angles, providing a comprehensive view of the heart's function. Placing electrodes on the arms and stomach is practical and comfortable for users, making it suitable for continuous and long-term monitoring.

Usage in project:

1.ESP32-CAM module

Fig.3. ESP32-CAM

The ESP32-CAM module was utilized for capturing live facial images for our face recognition system. Its 2MP OV2640 camera provided high-quality images for accurate recognition. Connecting the camera to a Wi-Fi network enabled real-time image streaming and processing, ensuring efficient biometric authentication. The compact size and wireless capabilities made it an ideal choice.

2. FTDI Module

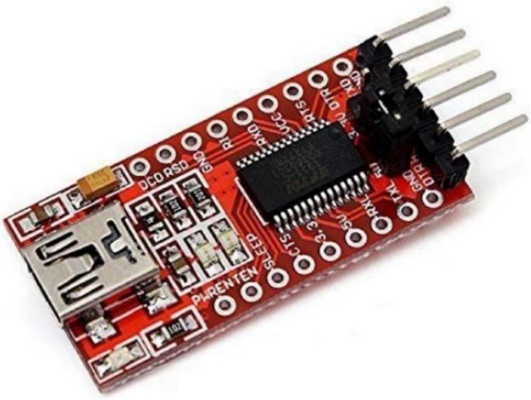

Fig. 4. FTDI Module

The FTDI (Future Technology Devices International) module is a versatile and widely-used tool in the realm of electronics and embedded systems. It serves as a bridge between USB (Universal Serial Bus) and UART (Universal Asynchronous Receiver-Transmitter) communication interfaces, facilitating seamless data transfer between a computer and a microcontroller or other peripheral devices. This module is particularly valued for its simplicity, reliability, and ease of integration, making it an essential component in many projects involving serial communication.

3. USB Cable

The USB cable is a universal protocol that ensures compatibility across devices and platforms, allowing data transfer rates ranging from standard to high-speed. It also delivers varying levels of electrical power, from a few watts for small devices to higher for laptops and other power-hungry electronics.

4. Jumper wires

Jumper wires are essential components in electronics prototyping and circuit assembly, used to establish connections between various points on a breadboard or between components on a circuit board. They are flexible, insulated wires with connectors at each end, facilitating easy and temporary electrical connections during testing and development phases.

Circuit Diagram:

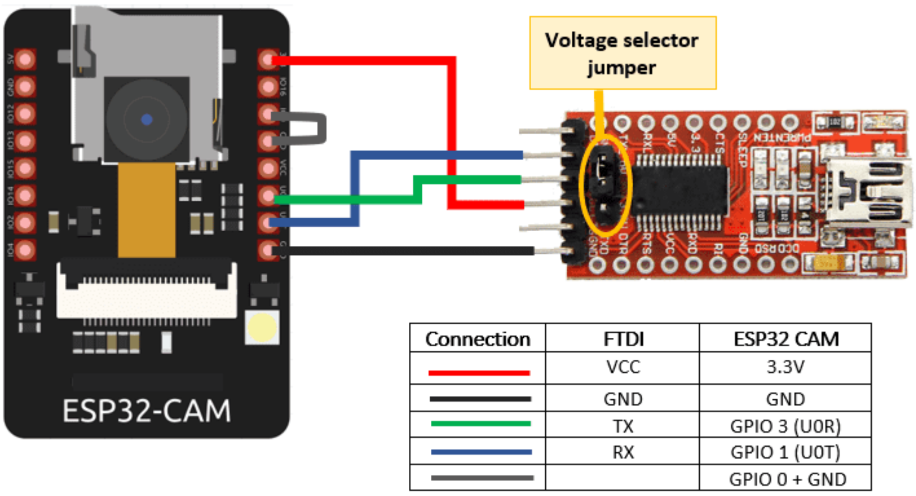

Fig. 5. ESP32 Cam and FTDI Module Connections

5. AD8232

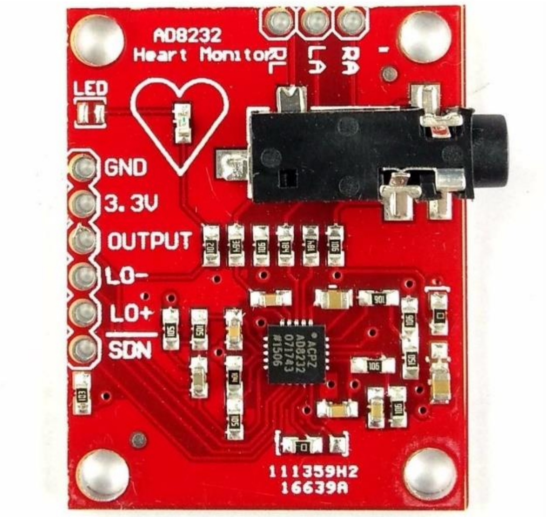

Fig.6. AD8232

The AD8232 is a specialized sensor module designed to capture the electrical activity of the heart, known as an electrocardiogram (ECG). It features the AD8232 chip, which provides integrated signal conditioning by amplifying and filtering the ECG signals, ensuring clear and accurate output.

6. Electrodes

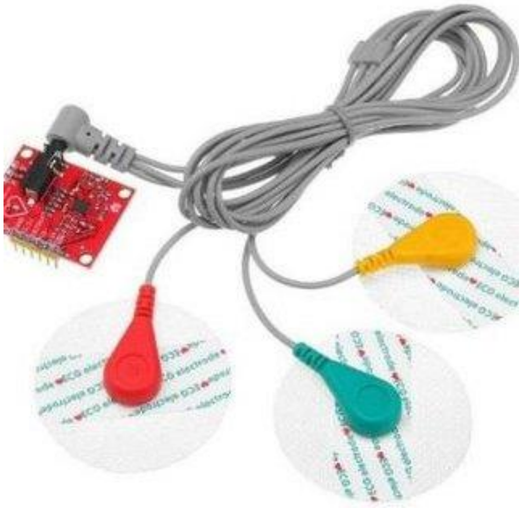

Fig.7. Electrodes

ECG electrodes are crucial in capturing heart electrical activity in an ECG sensor system. Made of conductive materials, they detect biopotential signals from the heart. Placed on the skin at specific locations, they transmit electrical impulses to the ECG sensor module, amplifying and filtering them for heart health assessment. Proper placement and secure attachment are essential for accurate readings.

7. ESP-32

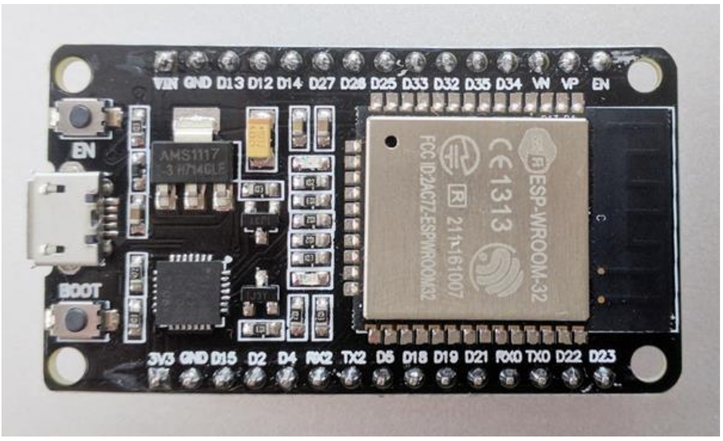

Fig.8.ESP-32

The ESP-32 is a versatile microcontroller with integrated Wi-Fi and Bluetooth capabilities, a dual-core processor, and low power consumption, making it ideal for various applications like IoT devices and wearable electronics. Its community support and development resources ensure ease of use, and its advanced security features, including secure boot and flash encryption, make it suitable for secure applications.

Circuit Diagram:

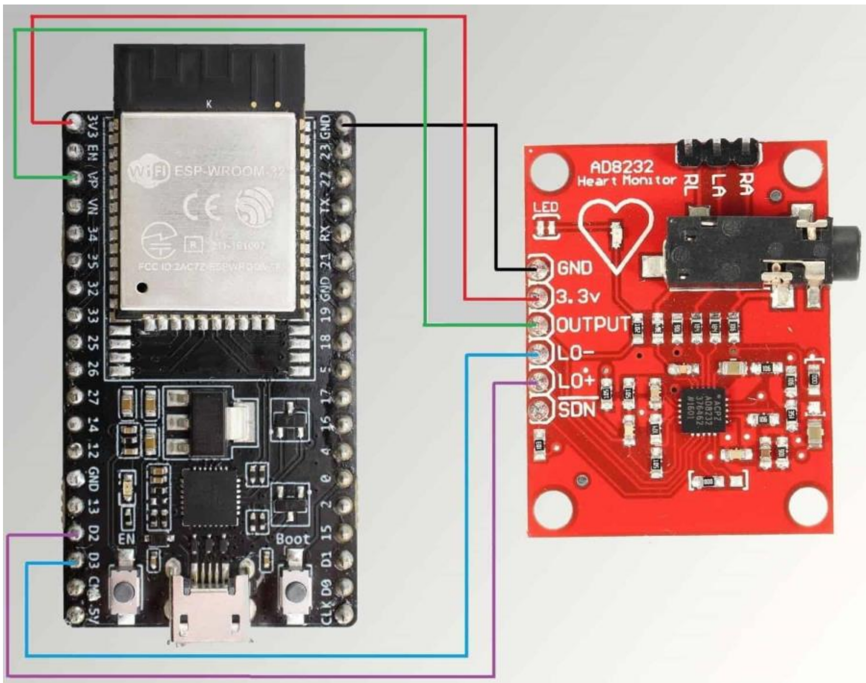

Fig.9. ESP-32 and AD8232 Connections

Platforms Used:

1. Google Colab, short for Google Colaboratory, is a cloud-based platform provided by Google for Python programming and machine learning. It offers a Jupyter notebook environment that allows users to write and execute Python code directly in their web browser without requiring any setup or installation. Colab supports collaborative work, providing access to GPUs and TPUs for accelerated computation, making it popular among researchers, educators, and developers for data analysis, machine learning, and AI research.

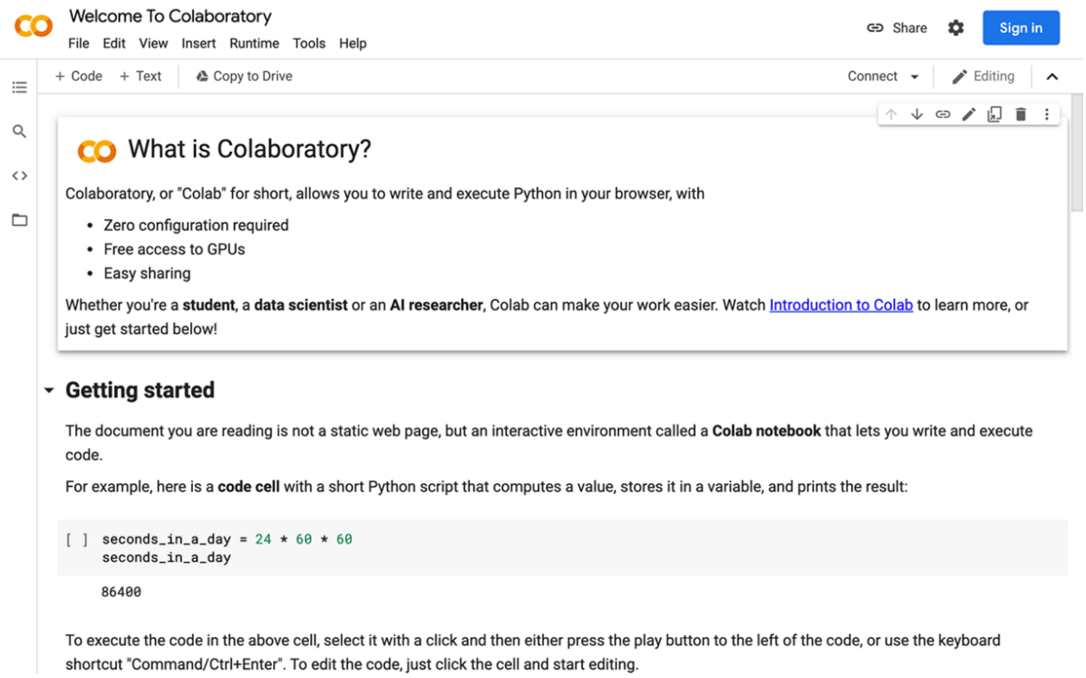

Fig. 10. Google Colab Interface

2. Thonny: Thonny is a user-friendly integrated development environment (IDE) for Python beginners. It features a simple and clean interface designed to help new programmers learn Python programming concepts efficiently. Thonny offers essential tools like an interactive Python shell, debugger, and syntax highlighting, making it an ideal choice for educational settings and early-stage development projects.

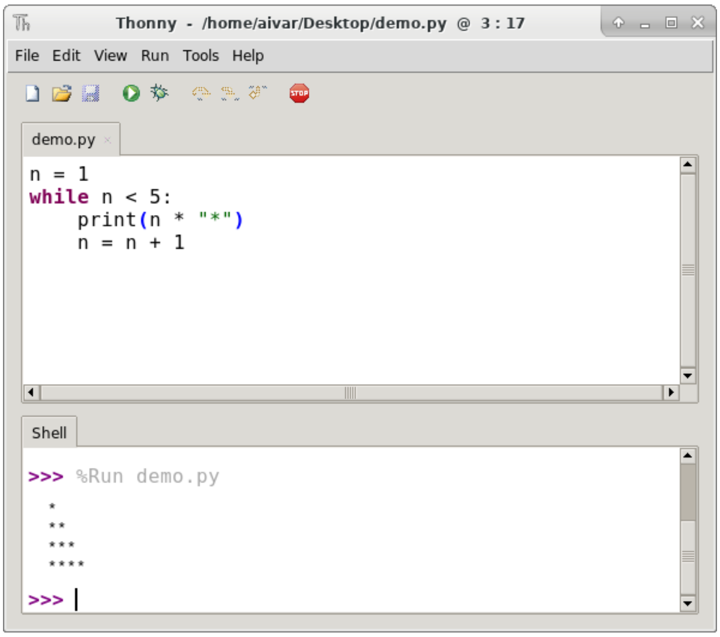

Fig. 11. Thonny Interface

3. Arduino IDE is an open-source platform used for creating interactive projects and prototypes. It allows users to program microcontrollers for tasks like LED controls and sensor integrations. In our project, we used Arduino to program the ESP32-CAM module, enabling camera functionalities and integrating them into our application.

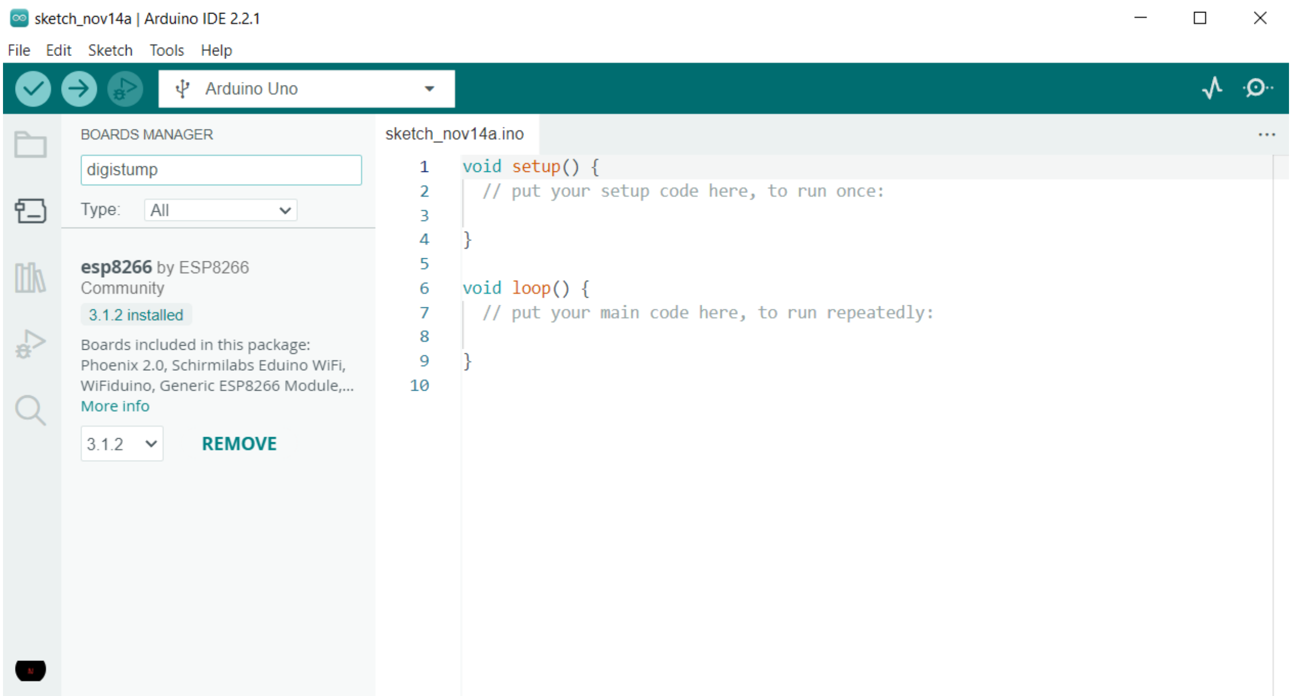

Fig. 12. Arduino IDE Interface

Libraries used:

1. glob: The Python glob library is a useful tool for retrieving files and directories that match specific wildcard patterns, enabling efficient search for files based on complex criteria like file extensions or partial names, making it ideal for batch processing or data collection.

2. wfdb: The WFDB Python package is a tool for reading, writing, and processing physiologic signals and annotations in the PhysioBank format, enabling efficient handling of complex waveform data, signal filtering, annotation extraction, and visualization within Python environments.

3. biosppy: BioSPPy is a Python library for biosignal processing, offering tools for ECG, EEG, and physiological signal analysis. It simplifies complex tasks and provides a user-friendly interface for both novice and expert users.

4. Matplotlib is a Python library used for creating static, animated, and interactive visualizations. It offers a MATLAB-like interface and supports various plots like line, scatter, bar, and histograms. Its customizable nature makes it a popular choice for scientific computing, data analysis, and machine learning applications.

5. OpenCV is a Python-based library for computer vision and image processing tasks, renowned for its object detection, face recognition, and image transformation capabilities, and its extensive collection of optimized algorithms is utilized in robotics, artificial intelligence, and augmented reality.

6. **NumPy** is a crucial Python library for numerical computing, offering powerful tools for manipulating large arrays and matrices. It offers efficient mathematical functions for data analysis, machine learning, and scientific computing, and its optimized array operations ensure high-performance computing.

7. TensorFlow is an open-source library for machine learning and numerical computation, offering a flexible framework for building and training various models, suitable for research and production environments across multiple platforms and devices. It is Developed by Google Brain.

8. Flask is a Python web framework that simplifies the creation of web applications with minimal boilerplate code, making it suitable for beginners and experienced developers. It supports extensions for efficient application customization.

9. Visual Keras is a Python library that simplifies the visualization of deep learning models, offering intuitive tools for creating detailed representations of model architectures, layer configurations, connections, and parameter details.

10. The Arduino `esp_camera.h` library enables the integration of ESP32 microcontrollers with cameras, allowing for the capture and processing of images and video streams within projects. It includes functions for setting camera settings, capturing frames, and accessing image data, making it ideal for applications like surveillance, image recognition, and IoT devices.

11. The WiFi.h library in Arduino enables connecting your board to a Wi-Fi network, facilitating wireless communication and internet access for projects. It simplifies network management, data transmission, and management, making it particularly useful for IoT applications, allowing Arduino to interact with web services and other networked devices.

Representation of model data

To thoroughly assess our classification models, we have included several key metrics and visualizations. The modal accuracy graph illustrates the classifier's performance based on the most frequently predicted class, offering insights into its baseline accuracy. The model loss graph depicts the error function's behaviour during training, highlighting the convergence of the model and the reduction of errors over time. Additionally, the Receiver Operating Characteristic (ROC) curves are presented to demonstrate the diagnostic ability of our binary classifier systems across different discrimination thresholds, providing a visual measure of sensitivity versus specificity. Lastly, the confusion matrix offers a detailed view of the classification outcomes, presenting the counts of true positives, true negatives, false positives, and false negatives, thereby enabling a deeper understanding of the model's performance. The following graphs shows these evaluations, showcasing the effectiveness of our models in various dimensions.

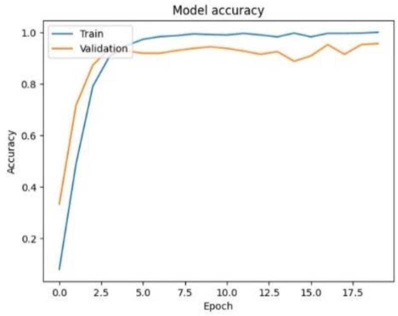

Fig.13. Model Accuracy curve for face recognition

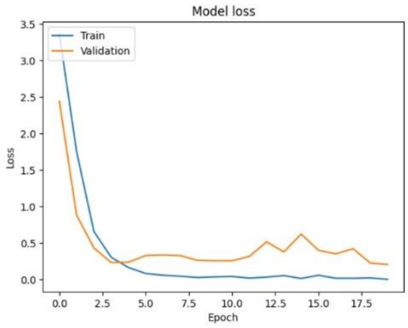

Fig.14. Model Loss curve for face recognition

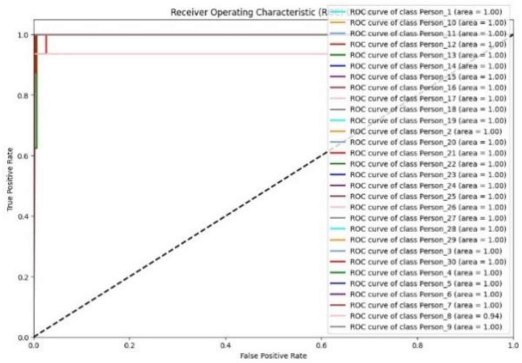

Fig.15. ROC for face recognition

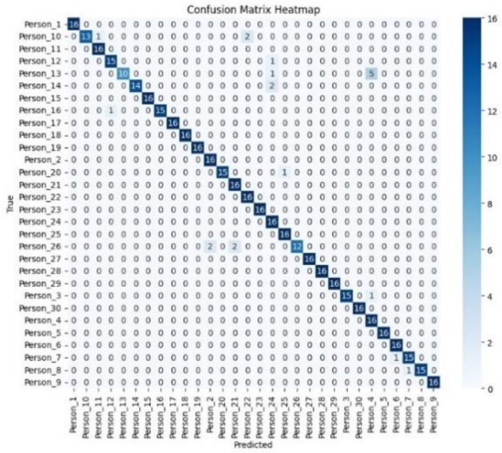

Fig.16. Confusion Matrix for face recognition

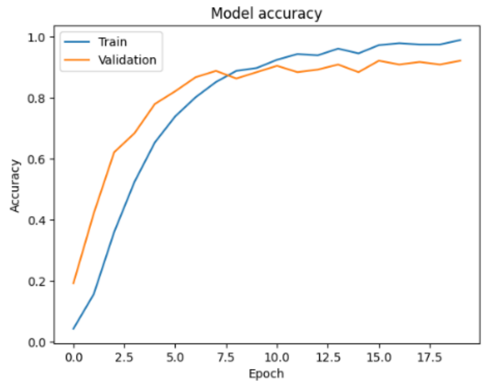

Fig.17. Model Accuracy curve for ECG recognition

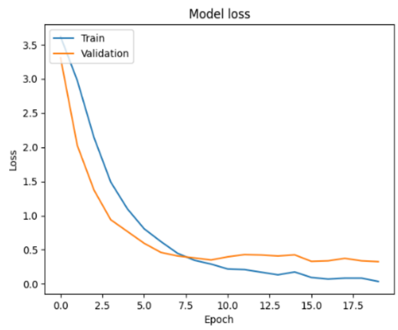

Fig.18. Model Loss curve for ECG recognition

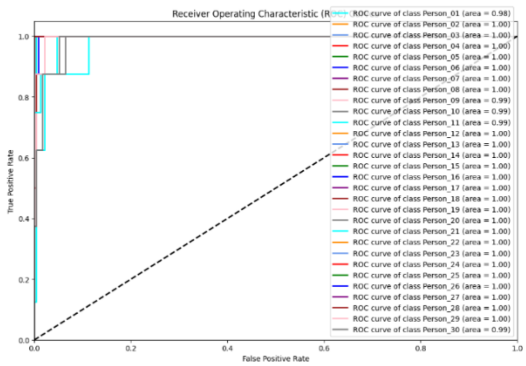

Fig.19. ROC for ECG recognition

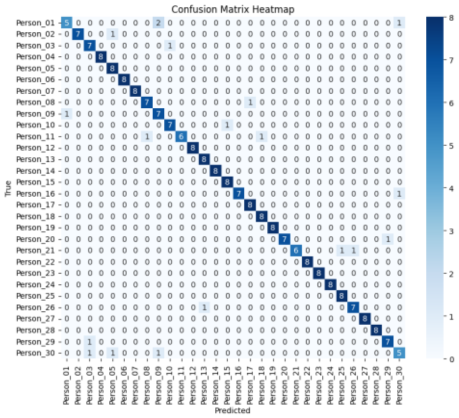

Fig.20. Confusion Matrix for ECG recognition

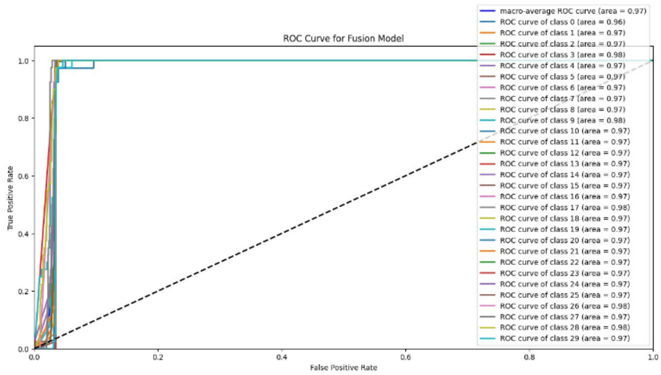

Fig.21. ROC for Fusion

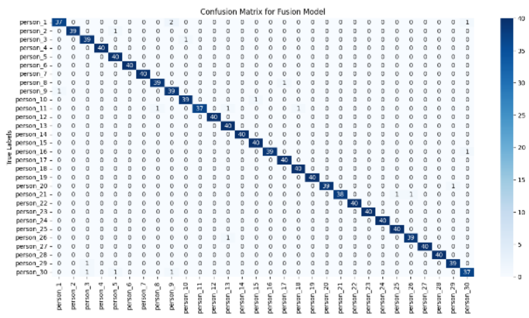

Fig.22. Confusion Matrix for fusion

Flowchart:

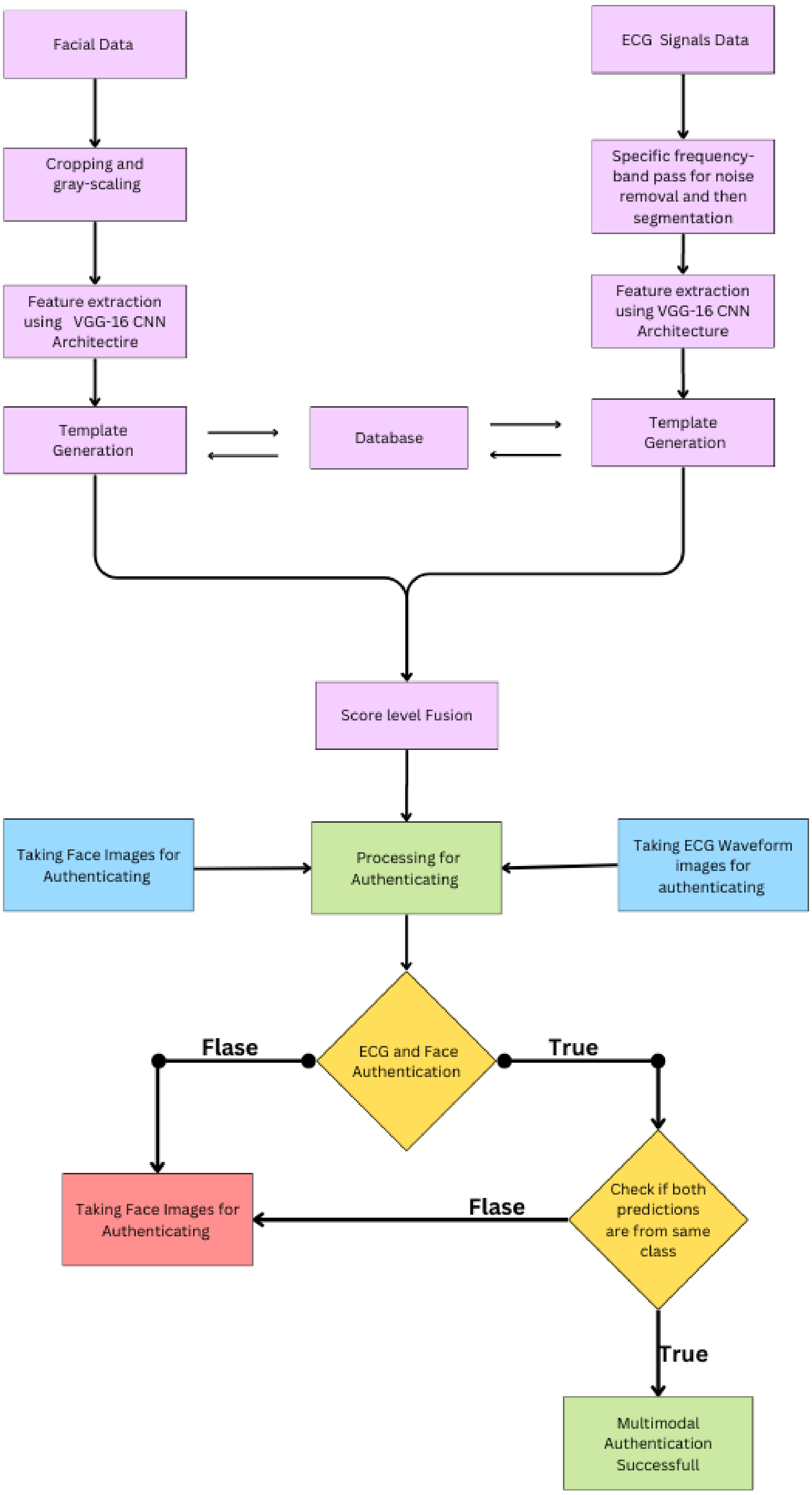

Fig. 23. Flow chart

Results:

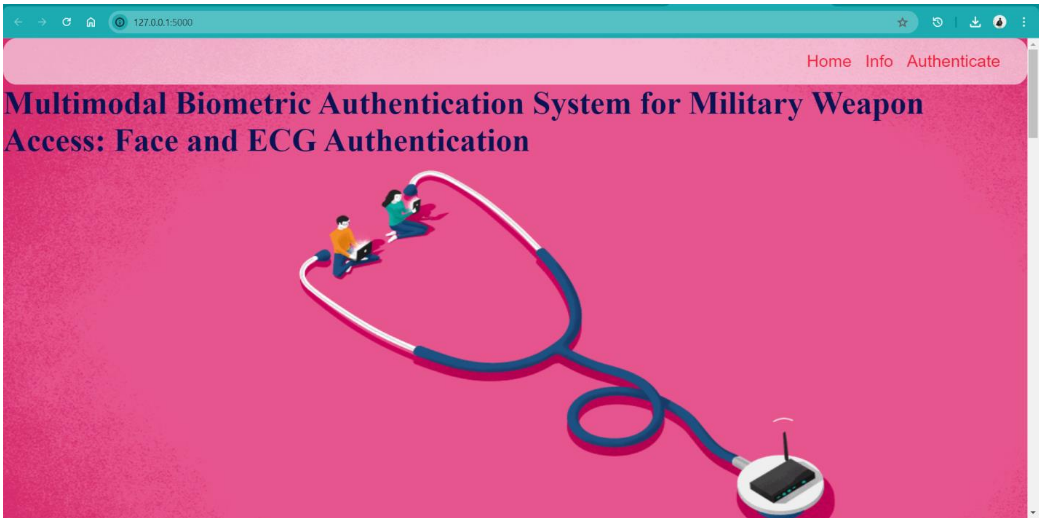

Fig.24. Homepage

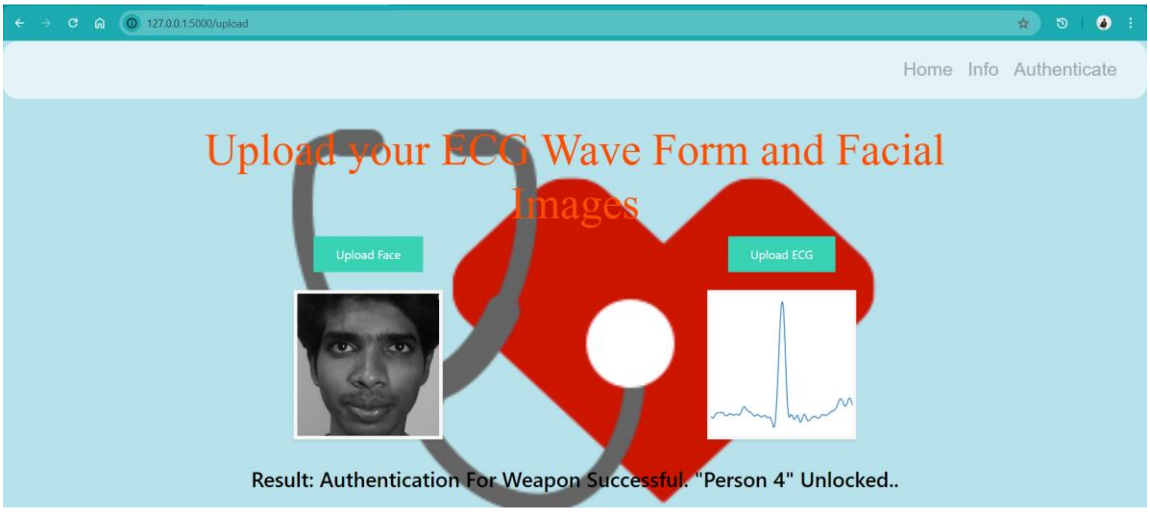

Fig. 25. Authentication Success

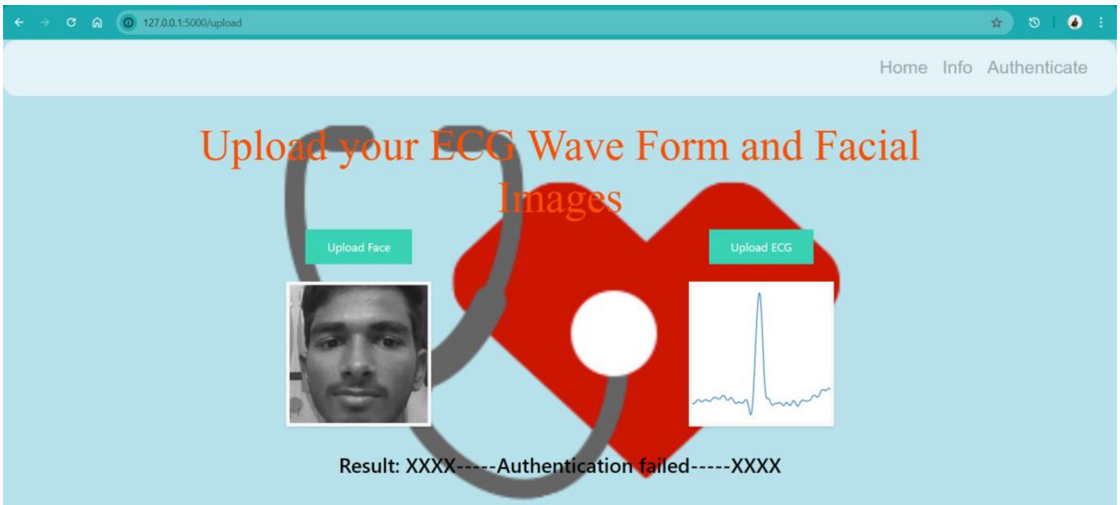

Fig.26. Authentication Failure

Model metrics analysis:

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%

Conclusion

Using the obtained facial and ECG data, the system preprocesses the information to feed into a Convolutional Neural Network (CNN). The CNN 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 "XXXX-----Authentication Failed-----XXXX" . In this work, with CNN VGG16 architecture we got accuracy of 95.6% for face recugnition,92.08 % for ECG recognition to classify 30 different people.

References:

- Facial image recognition for biometric authentication systems using a combination of geometrical feature points and low-level visual features M. Vasanthi a , K. Seetharaman b,
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
- Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115-2125.

- Karmakar, C., Khandoker, A. H., Palaniswami, M., & Jelinek, H. F. (2013). Understanding cardiovascular signals in the context of multiscale entropy. *IEEE Reviews in Biomedical Engineering, 6*, 108-119.
- Jain, A. K., Ross, A., & Prabhakar, S. (2016). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1)*, 4-20.