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

Dr. Prof. T. Kishore Kumar[#], Suneetha Sivakrishna[#], Aluvoju Vivek[*], G Hari Chandana[$], T Sanjana[@], Sathu Tejaswi[*]

[#]*Department of Electronics and Communication Engineering, NIT, Warangal, Telangana, India.*

[*]*Department of Electronics and Communication Engineering, SR University, Warangal, Telangana, India.*

[$]*Department of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

[@]*Department of Computer Science and Engineering (IoT), KITS, Warangal, Telangana, India.*

Abstract—Unimodal biometric systems use a single source of biometric data, such as fingerprints or facial features, to verify identity. These kinds of biometrics are susceptible to higher error rates and security vulnerabilities because it relays on a single trait for authentication. To overcome this, multimodal biometrics method is proposed. Multi-modal biometric system authenticates more than once and has various benefits such as high accuracy, low error rate and larger population coverage. These biometrics systems enhance integrity and privacy, as it stores different biometric characteristics of every user. So, here designed a multimodal biometrics project utilizing deep learning to enhance authentication security by combining face and Electrocardiogram (ECG) signals. VGG-16 model, a deep learning architecture used to capture complex patterns in accurate individual identification with both ECG and Facial data. The high-resolution convolutional filters captured intricate details of the face and ECG waveform, ensuring high accuracy in distinguishing different individuals.

***Keywords*— Biometrics, ECG, Facial, VGG16, Multimodal, Unimodal, Security, Dataset, Authentication.**

I. INTRODUCTION

Biometric authentication is a crucial aspect of security, leveraging unique physiological and behavioural characteristics to verify individuals' identities. This form of authentication offers significant advantages over traditional methods like passwords or tokens, which can be easily lost, forgotten, or stolen. Biometric data, such as fingerprints, facial features, or voice patterns, are inherently tied to the individual and are difficult to replicate, making them a robust choice for secure authentication.

Security and privacy management have been challenging since the inception of the Internet. Traditional user authentication methods primarily depend on passwords, which are often reusable. Originally, passwords were used to authenticate users to a central computer within an Intranet, where the risk of password exposure was minimal due to the lack of external network access. However, in the current landscape, devices are connected to local networks and the Internet is accessible ubiquitously. Additionally, the widespread adoption of the Internet of Things (IoT) has led to a significant increase in the transmission and storage of sensitive personal data. Consequently, implementing stringent access control policies is essential to ensure effective security and privacy [1].

Multimodal biometrics systems, which utilize multiple biometric traits for person recognition, offer numerous advantages over unimodal systems, as highlighted by several reference articles. These systems enhance accuracy by reducing the chances of false positives and false negatives, leading to more reliable identification and verification processes. The integration of multiple traits also improves the system's overall reliability, as it can compensate for the variability or unavailability of individual traits. Security is significantly heightened, as attackers would find it considerably more challenging to spoof or circumvent multiple biometric traits simultaneously. Multimodal biometrics address the issue of non-universality, ensuring that the absence of one biometric trait does not impede the authentication process. User convenience is also improved, as these systems provide flexible authentication options, allowing, for instance, facial recognition to substitute for fingerprint verification when necessary. Additionally, multimodal systems exhibit greater resilience to spoofing attacks and mitigate the impact of noisy data from any single source, ensuring consistent and reliable performance under various conditions. Finally, these systems can be more effectively scaled by distributing the recognition process across multiple traits, enhancing processing speed and overall system efficiency. Collectively, these advantages make multimodal biometrics a more secure, accurate, and user-friendly approach to identity verification and authentication.[3]

Electrocardiogram (ECG) biometric modalities utilize the distinctive electrical signals produced by the heart for person identification and verification. ECG signals are inherently unique to individuals due to variations in cardiac anatomy and physiology, making them stable and reliable biometric markers over time. Unlike traditional biometric methods, such as fingerprints or facial recognition, ECG biometrics offer non-intrusive and continuous authentication capabilities, requiring minimal user interaction once the initial signal is captured. The security of ECG-based systems is bolstered by the difficulty in replicating or spoofing these internal physiological signals, which enhances their resistance to fraud and impersonation attacks. Applications of ECG biometrics span various sectors including healthcare, finance, and Internet of Things (IoT), benefiting from its robustness and adaptability in diverse environments. Ongoing research focuses on improving noise reduction techniques, addressing variability due to physiological conditions, and standardizing acquisition and processing methodologies to enhance the accuracy and reliability of ECG biometric systems. In summary, ECG biometrics represent a promising avenue for secure and seamless identification, leveraging the physiological uniqueness of cardiac signals for enhanced authentication processes. [4-9]

Face traits serve as versatile biometric modalities, leveraging distinct facial features for identification and authentication purposes. Facial recognition technology analyses facial characteristics such as the distance between eyes, nose shape, and jawline contours to create unique templates for each individual. This modality is widely adopted due to its non-intrusive nature, requiring only visual capture via cameras, making it suitable for various applications from smartphone unlocking to airport security. Recent advancements in deep learning algorithms, particularly convolutional neural networks (CNNs), have significantly enhanced the accuracy and robustness of facial recognition systems, allowing for real-time and reliable identification even in diverse environmental conditions. Despite its popularity, facial recognition technology faces challenges such as sensitivity to variations in lighting, pose, and facial expressions, which can affect its performance and reliability. Ongoing research focuses on improving these aspects, alongside addressing ethical concerns regarding privacy and consent, to further enhance the usability and acceptance of facial traits in biometric authentication systems. In summary, facial traits as biometric modalities offer a potent combination of accessibility, accuracy, and adaptability, continuing to evolve with advancements in computer vision and machine learning technologies. [10-14]

II. OBJECTIVES AND CONTRIBUTIONS OF THE RESEARCH

The objective of this research is to explore and develop advanced multimodal biometric ECG (electrocardiogram) recognition systems and face recognition to enhance security access protocols in various high-risk sectors. By leveraging the unique electrical activity patterns of the heart, which are distinct to each individual, this study aims to establish a highly reliable, accurate, and non-intrusive method for identity verification. Developing innovative techniques for capturing high-quality ECG signals under different conditions and minimizing noise and artifacts to ensure accurate readings. Utilizing advanced pattern recognition algorithms and machine learning techniques to analyse ECG data, identifying unique features and improving the accuracy and speed of identity verification. Ensuring the robustness of the ECG biometric system against potential spoofing and cyber-attacks by integrating multi-factor authentication and encryption technologies. Enhancing user experience by designing user-friendly interfaces and ensuring the system is accessible to individuals with diverse needs, including those with heart conditions or disabilities. Conducting comprehensive testing and integration of ECG biometric systems within existing security infrastructures in real-world scenarios to validate their effectiveness and reliability. And advance biometric face recognition systems to enhance security access protocols across various sectors. By harnessing the distinct facial features unique to each individual, this study aims to develop a highly reliable, accurate, and non-intrusive method for identity verification. Developing sophisticated techniques for capturing high-quality facial images under diverse conditions, ensuring clarity, and minimizing the effects of lighting, angles, and expressions. Utilizing advanced facial recognition algorithms and machine learning techniques to analyse facial features, improve accuracy, and reduce false positives and negatives. Enhancing the system's resilience against spoofing attacks, such as photo and video forgery, by integrating liveness detection and anti-spoofing technologies. Ensuring robust data encryption and compliance with privacy regulations to protect user information and maintain trust. Designing intuitive interfaces that provide a seamless user experience while ensuring accessibility for individuals with diverse needs, including those with facial differences or disabilities. Conducting comprehensive testing and integration of face recognition systems within existing security infrastructures to validate their effectiveness and reliability in real-world scenarios.

These are some prior objectives:

- To advance the security technology in military area.
- To implement double layer security instead of single security check.
- Enhances system's resilience against spoofing attacks by integrating more than one authentication and anti-spoofing technologies.
- Improve user experience by designing user-friendly interfaces.

III. LITERATURE REVIEW EXISTING BIOMETRIC AUTHENTICATION

Biometric authentication systems are increasingly used for security due to their ability to verify individuals based on unique biological traits.

TABLE 1: Overview of the most common systems

Sl. No.	Authentication method	Advantage	Disadvantages
1.	Fingerprint Recognition	• High accuracy • Cost-effective • Easy to use	• Can be affected by cuts, dirt, or wear • Potential for spoofing with high-quality fake fingerprints
2.	Iris Recognition	• Extremely high accuracy • Stable over a person's lifetime	• Requires specialized equipment • Can be perceived as intrusive
3.	Voice Recognition	• Non-intrusive • Can be used remotely	• Can be affected by background noise and illness • Susceptible to voice imitation and recording attacks
4.	Hand Geometry Recognition	• Quick and easy to use • Suitable for environments where hands are dirty or gloves are worn	• Less accurate than other biometric methods • Not unique enough for high-security applications
5.	Retina Scanning	• Extremely high accuracy • Difficult to spoof	• Highly intrusive • Requires specialized and expensive equipment

6.	Behavioural Biometrics	• Non-intrusive • Can be used continuously	• Less mature technology

A. Research on Face-Based Authentication

Multi-user active authentication requires verifying multiple subjects, which poses challenges for traditional methods. Extremal Open set Rejection addresses this with a sparse representation-based identification step and a verification step. It uses Extreme Value Theory to model distributions, focusing on sparsity vector concentration and distribution overlap for decision-making. Tested on three public face-based mobile authentication datasets, the method demonstrates effectiveness in handling these challenges [21]. a method that combines biometric data with a user-specific secret key for human verification. This approach involves discretized random orthonormal transformation of biometric features, ensuring zero error rate and generating non-invertible templates that can be revoked. Another scheme without discretization is also presented, supported by mathematical analysis. The feasibility of both methods is demonstrated on face verification tasks using ORL and GT databases, showing their effectiveness compared to existing approaches [22]. Traditional methods like PINs and short passwords used for smartphone security are increasingly vulnerable to compromise.

B. Research On ECG-Based Authentication

There are many previously worked ECG-based researches. In that we have gone through few papers like: Authentication is key for securing communication between sensor nodes in wireless body sensor networks (WBSNs). The electrocardiogram (ECG) data collected by these nodes offer continuous availability and inherent liveness detection, making them ideal for authentication. While much research has focused on ECG-based intranode authentication in WBSNs, the protection of sensitive ECG data has been less explored. This article introduces a privacy-preserving ECG-based authentication system using a noninvertible transformation called the manipulatable Haar transform (MHT). This system not only ensures secure intranode authentication but also protects sensitive ECG data from exposure [18]. ECG has emerged as a robust biometric for human recognition, providing continuous identification that is hard to intercept or duplicate. However, many current algorithms require long ECG data, limiting practical use. This study introduces a two-phase authentication method using neural networks (NN) for fast, 3-second authentication with reliable performance. Tested on 50 subjects using mobile-collected finger ECG signals under various conditions, the first phase employs a "General" NN model for initial screening, followed by "Personal" NN models for detailed identification. The algorithm shows strong performance across the full dataset and subsets of various sizes [19]. Patients use medical IoT devices for health monitoring, sending personal health records to hospitals for diagnosis. However, security and privacy issues arise due to the sensitive nature of health data. Traditional cryptographic methods and passwords are inadequate for health monitoring's privacy and security demands. Biometric authentication, especially using ECG signals, verifies human characteristics effectively. Despite ECG's suitability, practical ECG-based authentication often fails due to data noise and privacy concerns.

C. Research on Multimodal Biometric Authentication

Multimodal biometrics, including fingerprint, palmprint, and finger knuckle print biometrics, are widely used for authentication. The Automatic Fingerprint Identification System (AFIS) uses techniques based on minutiae points, while Finger Knuckle print features lines and creases on the outer surface of the finger. These rich texture information makes them powerful means for personal identification. Artificial Neural Networks (ANN) is one of the Soft Computing techniques used for multimodal biometric identification. These biometrics are considered popular, reliable, and leading biometrics. [20]. Secure smartphone authentication is crucial for financial transactions, and traditional methods like PIN and passwords are vulnerable. A multi-modal biometric system, utilizing face, periocular, and iris characteristics [23]. Multimodal biometrics involves fusion of various biometrics, classified into sensor level, decision level, and score level fusion. The fusion classifier can be categorized into rank level, abstract level, and measurement level fusion. This proposal proposes integrating fingerprint and Iris biometrics with fuzzy vault to form a multimodal biometric crypto system, examining it using score level fusion. [25-26]

IV. METHODOLOGY

A. Face Image Data Collection:

Facial data is collected from by recording 8-9 second videos from 30 different people. We Used ESP32 CAM for this procedure. The resolution we selected is 'XGA 1024 X 768 p x'. This method includes capturing various angles and expressions, ensuring a diverse and comprehensive dataset. From these videos, we extracted multiple images and further process.

B. ECG Data Collection

Coming to the ECG biometric authentication dataset we took the MIT-BIH Arrhythmia Database. The MIT-BIH Arrhythmia Database is a collection of 48 half-hour excerpts of two-channel ambulatory ECG recordings from 47 subjects studied by the BIH Arrhythmia Laboratory between 1975 and 1979. The recordings were digitized at 360 samples per second per channel with 11-bit resolution over a 10-mV range. Two or more cardiologists independently annotated each record, with disagreements resolved to obtain computer-readable reference annotations for each beat. The entire MIT-BIH Arrhythmia Database is available in this directory, with about half of the database available since PhysioNet's inception in 1999.

C. Face Image Preprocessing

As we recorded 8-9 second videos, we carefully extracted multiple frames to gather a wide-ranging collection of facial images from different angles. Each frame underwent a cropping procedure to isolate the face, prioritizing key features while minimizing background interference. Following this, the cropped images were converted to grayscale to simplify computation and aid the model in focusing on essential facial characteristics without the complexity of colour information. This preprocessing step facilitated the development of a diverse and resilient dataset, encompassing nuanced facial expressions and orientations crucial for reliable facial authentication.

D. ECG Signal Extracting.

The MIT-BIH Arrhythmia Database was used to collect ECG data. Aim is to enhance signal clarity by removing unwanted noise. This involved applying a bandpass filter technique, which allowed us to isolate specific frequency ranges of the signal that are crucial for accurate analysis. By focusing on these targeted frequency bands, effectively filtered out irrelevant noise that could otherwise obscure important details in the ECG waveform. After noise reduction, segmentation of the cleaned signals into distinct sections representing different phases or events within the cardiac cycle is done. These segmented images were then saved for further analysis or visualization, providing clearer insights into the ECG data without the interference of unwanted noise. This method of approach not only improves the accuracy of ECG signal interpretation but also ensures that the extracted data is reliable and useful for medical diagnostics or research purposes.

E. Deep Learning Algorithm – VGG16:

The VGG16 model is a deep learning algorithm used for image recognition. It consists of multiple layers, including convolutional, pooling, and fully connected layers. VGG16 is inspired by the visual processing in the human brain and is effective in capturing hierarchical patterns and spatial dependencies within images. The construction of VGG16 involves assembling unseen layers in a specific order, allowing it to learn hierarchical attributes. The pre-processing in VGG16 is similar to the human brain.

1) VGG16 Architecture

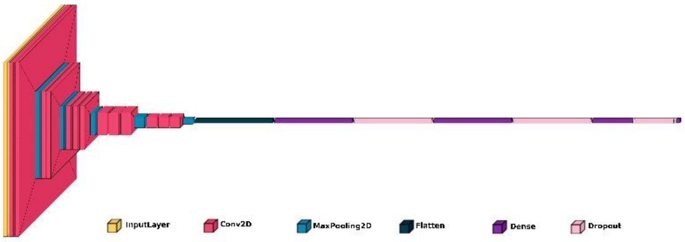


Fig. 1. VGG16 Architecture which we used for both Face and ECG

The VGG model modification aims to optimize training efficiency for specific classification tasks by learning for feature extraction. Fig. 1 is the visual representation of our model. Here, the base model, VGG16, is initially used without its top layers, allowing for custom classifier layers. By freezing all layers except for critical feature extraction layers, computational resources are optimized while retaining the ability to extract complex visual features from images.

Further, the VGG16 architecture has been modified with custom classifier layers to improve its adaptability. The model consists of three dense layers with rectified linear unit activation functions, interleaved with dropout layers to prevent overfitting. The dense layers have 4096 neurons each, followed by 2048 neurons, and a final SoftMax layer with 30 output classes tailored to specific classification tasks. This design preserves the deep learning model's ability to capture hierarchical patterns in visual data and aligns with best practices in model regularization and task-specific output optimization.

F. Input Data for evaluation

For capturing input data, we utilize the ESP32-CAM module to collect live facial images and ECG waveforms from advanced medical equipment to ensure precise waveform acquisition. Presently, the ESP32-CAM is employed for live face capture, providing real-time facial data for authentication purposes. This integration of the ESP32-CAM allows us to gather high-quality facial images directly from the source, enhancing the accuracy and reliability of our face authentication model. Future work will focus on extending the capabilities of the ESP32-CAM to include real-time ECG data capture, further improving the robustness and applicability of our multimodal biometric authentication system.

G. Flow Chart

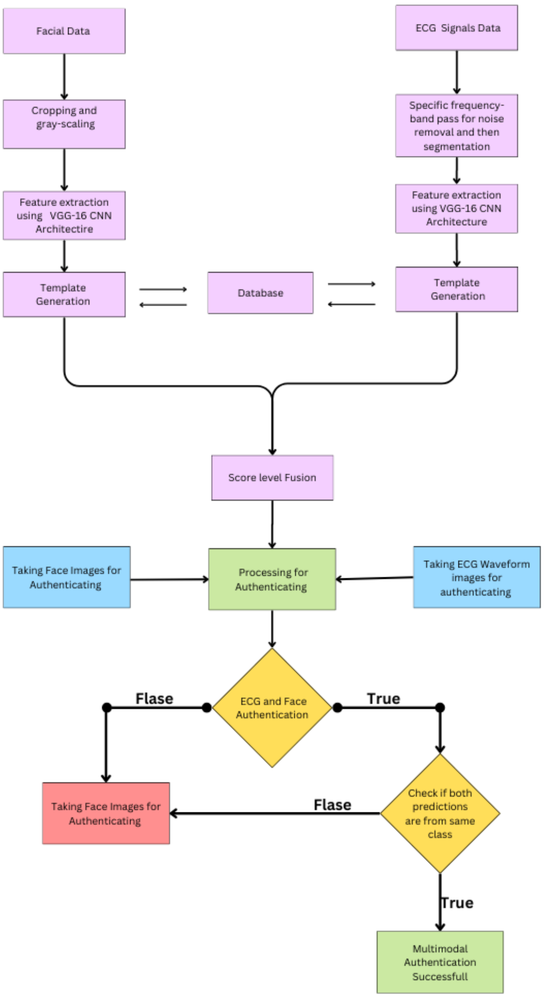

Facial Data
Cropping and gray-scaling
Feature extraction using VGG-16 CNN Architectire
Template Generation
Database
ECG Signals Data
Specific frequency-band pass for noise removal and then segmentation
Feature extraction using VGG-16 CNN Architecture
Template Generation
Score level Fusion
Taking Face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

Fig. 2. Complete flowchart of project

H. Method for Authentication.

By analysing the fig. 2, it is clear data preprocessing process for face and ECG are unique. For facial data we cropped up to faces and grayscale whereas for ECG data we cleared out the noise and then segmented the signals. Then feature extraction done with VGG16 architecture. To combine and access ECG and face biometrics models, we employed logical ‘and’ operator. The application prompts users to upload their ECG data and capture their face data via a camera interface. The system then processes these inputs by loading the respective pre-trained models: one for ECG authentication and another for face recognition. The ECG and the face model analyse the uploaded ECG signal and facial for authentication with the help of threshold score. Then after that, if both models predict the same class, indicating that the ECG and face data belong to the same individual, the system declares “Authentication for Weapon successful. ‘Person (no.) Unlocked.” and logs the result. Otherwise, it returns "Authentication Failed”. This integrated approach ensures an efficient biometric authentication process, leveraging the unique advantages of both ECG and facial recognition technologies.

V. Results and Discussions

A. Performance Evaluation

To comprehensively evaluate the performance of our trained models, we assessed the ECG authentication model, the face authentication model, and their fusion model using key performance metrics. Specifically, we measured Accuracy, Recall, Precision, and F1 score, as these metrics provide a holistic understanding of each model's effectiveness in correctly identifying and classifying instances.

Recall: It measures the proportion of true positives correctly identified.

$$Recall = \frac{True\ Positive\ (TP)}{True\ Positive\ (TP) + False\ Negative(FN)}$$

Precision: It measures the proportion of true positives among predicted positives.

$$Precition = \frac{True\ Positive\ (TP)}{True\ Positive\ (TP) + False\ Positive(FP)}$$

F1: This score balances precision and recall for a single performance metric.

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Accuracy: It measures the proportion of correct predictions among all predictions.

$$Accuracy = \frac{True\ Positive\ (TP) + True\ Negative(TN)}{All\ Samples}$$

TABLE 2: Comparative Metrics Evaluations

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%

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. (fig. 3, fig. 7)

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. (fig. 4, fig. 8)

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. (fig. 5, fig. 9, fig. 11)

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. (fig. 6, fig. 10, fig. 12)

The following graphs shows these evaluations, showcasing the effectiveness of our models in various dimensions.

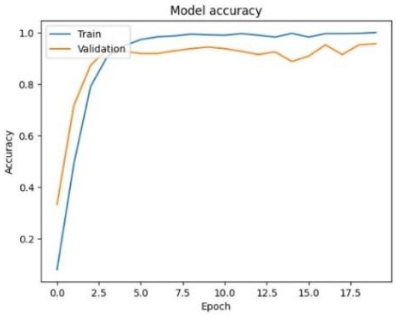


Fig 3. Model Accuracy curve for face recognition

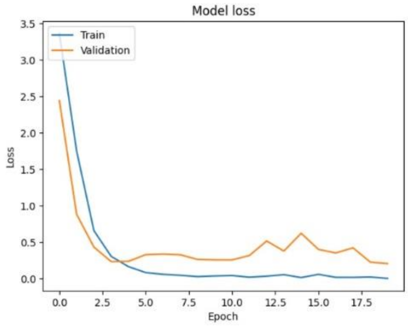


Fig 4. Model Loss curve for face recognition

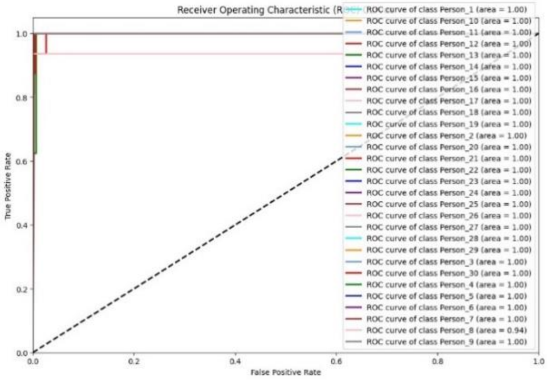


Fig 5. ROC for face recognition

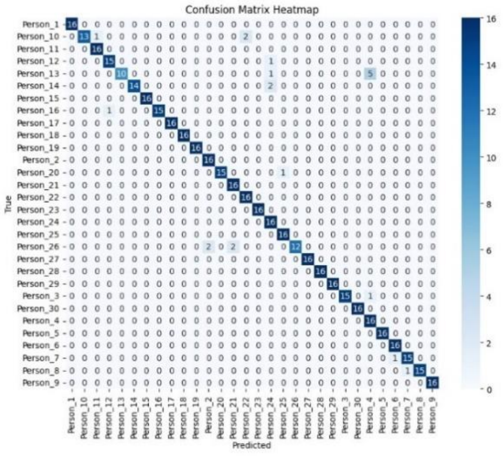


Fig 6. Confusion Matrix for face recognition

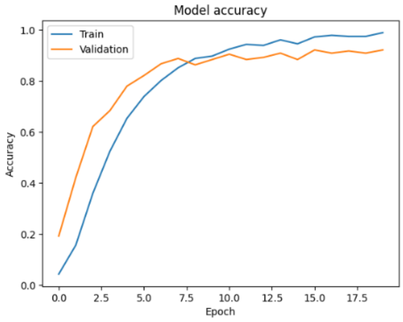


Fig 7. Model Accuracy curve for ECG recognition

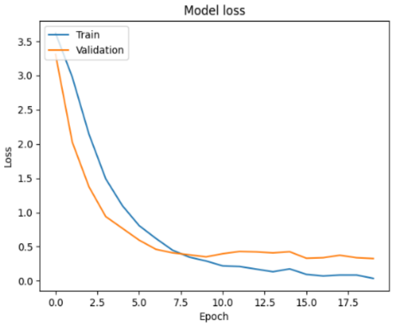


Fig 8. Model Loss curve for ECG recognition

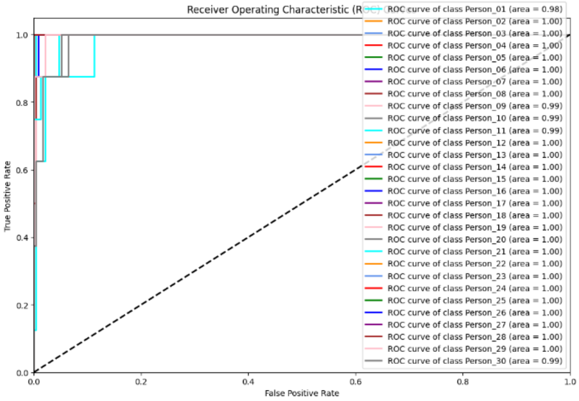


Fig 9. ROC for ECG recognition

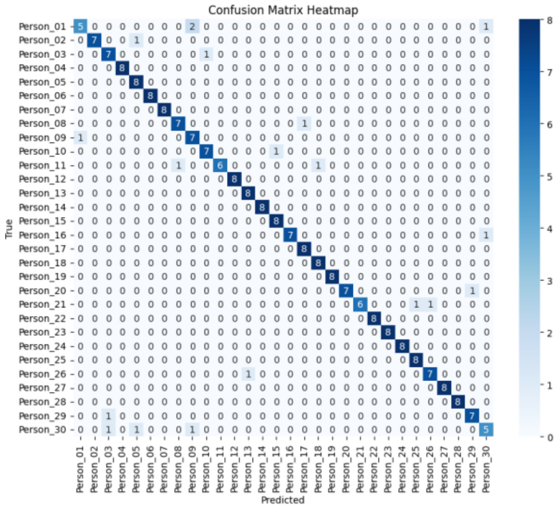


Fig 10. Confusion Matrix for ECG recognition

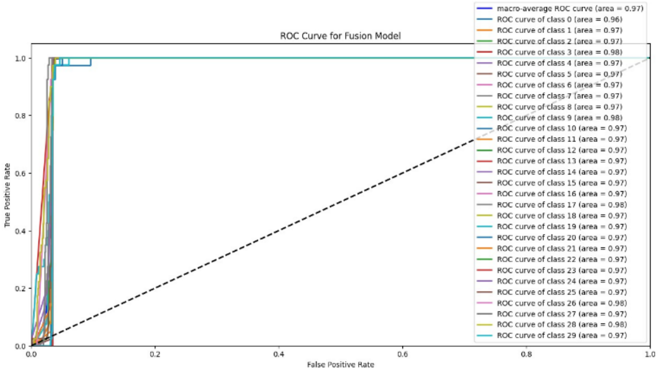


Fig 11. ROC for Fusion

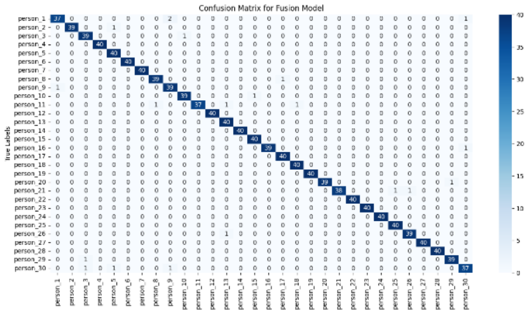
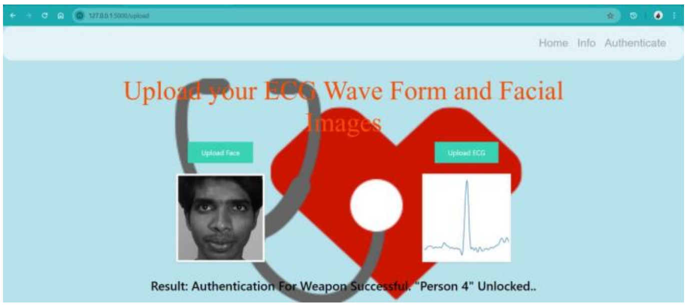


Fig 12. Confusion Matrix for fusion

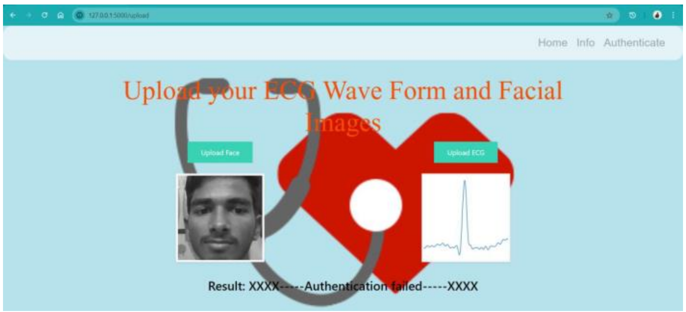
The system uses facial and ECG data to preprocess information and feed it into VGG16. The VGG16 compares the data against a database to check for matches in facial features and ECG signals. If both match, the system grants access to an individual for military weapon access, displaying "Authentication For Weapon successful. 'Person (no.) Unlocked..” (Fig. 13) If not, the system displays "Authentication Failed" (Fig. 14).



Upload your ECG Wave Form and Facial Images

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

Fig. 13. Authentication Success



Upload your ECG Wave Form and Facial Images

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

Fig. 14. Authentication Failure

VI. CONCLUSION

In conclusion, our research underscores the limitations of unimodal biometric systems, which rely on single sources of data like fingerprints or facial features. These systems are vulnerable to higher error rates and security risks due to their dependency on a singular trait for authentication. To address these challenges, we advocate for multimodal biometric approaches. By integrating multiple biometric characteristics such as ECG waveforms and facial features. Our proposed multimodal system achieves significant improvements in accuracy and reliability. Specifically, our VGG16 model-based approach yielded 92.08% accuracy for ECG data, 95.6% accuracy for facial data, and a combined accuracy of 98.33% when integrating both modalities. This demonstrates the efficacy of multimodal biometrics in enhancing authentication reliability, ensuring better integrity, and safeguarding user privacy across diverse applications.

VII. REFERENCES

- [1]K.K. Coelho et al., "A Security Management Tool for Federated Learning-Based Biometric Authentication Using Vital Signs," *Biomedical Signal Processing and Control*, vol. 85, 2023, pp. 105022.
- [2]A secure multi-modal biometrics using deep ConvGRU neural networks based hashing Sasikala T.S
- 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,
- [3]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.
- [4]Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115-2125.
- [5]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.
- [6]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.
- [7]Girard, J. M., Wu, T. Y., Chen, H. S., & Penders, J. (2017). Cardiac biometric recognition: The influence of forgery on ECG-based authentication systems. *IEEE Transactions on Information Forensics and Security, 12(10)*, 2341-2351.
- [8]Saeed, A., Ahmed, M. U., & Khattak, H. A. (2019). A comprehensive review on ECG biometric systems. *Sensors, 19(6)*, 1370.
- [9]Ghose, S., Kozma, R., & Messer, K. (2020). Advances and challenges in ECG biometric recognition. *Pattern Recognition Letters, 131*, 314-321.
- [10]Li, S. Z., Zhu, J., & Zhang, L. (2020). Handbook of face recognition (2nd ed.). Springer.
- [11]Jain, A. K., Dass, S. C., & Nandakumar, K. (2020). Handbook of biometrics. Springer.
- [12] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2018). Face recognition: A literature survey. *ACM Computing Surveys (CSUR), 50(6)*, Article 83.
- [13] Damer, N., Ouellette, D., & Richardson, S. (2019). Privacy and facial recognition: A primer. *Journal of Information Technology Education: Research, 18*, 345-358.
- [14]Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) Part 3: Demographic effects. National Institute of Standards and Technology (NIST).
- **[15]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.
- **[16]Ratha, N.K., & Bolle, R.M.** (2004). Automatic Fingerprint Recognition Systems. Springer.
- **[17]Bowyer, K.W., Hollingsworth, K., & Flynn, P.J.** (2008). A Survey of Iris Biometrics Research: 2008-2010. Handbook of Iris Recognition, 15-54.
- **[18] A privacy-preserving ECG-based authentication system for securing wireless body sensor networks W Yang, S Wang**
- **[19] Finger ECG-based authentication for healthcare data security using artificial neural network Y Chen, W Chen**
- **P.Mahalakshmi, K.Gunasekaran, D.Saravanan, 2014, Implementation of Multimodal Biometric Authentication using Soft Computing Techniques, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCICCT – 2014 (Volume 2 – Issue 05),**
- **Galoh Rashidah Haron; Dharmadharshni Maniam; Latifah Mat Nen; Nor Izyani Daud**
- **[21]**Face-based **multiple user active** authentication **on mobile devices** P Perera, VM Patel
- **[22]**Face based **biometric** authentication **with changeable and privacy preservable templates** Y Wang, KN Plataniotis
- [23]Multi-modal authentication system for smartphones using face, iris and periocular Kiran B. Raja; R. Raghavendra; Martin Stokkenes; Christoph Busch
- [24].Pinto JR, Cardoso JS, Lourenço A (2018) Evolution, current challenges, and future possibilities in ECG biometrics. IEEE Access 6:34746–34776
- [25] MuthuKumar .A, Kasturi .C and Kannan .S, Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris, ICTACT Journal on Image and Video Processing, Vol.02, No.03, Feburary 2012.
- [26] Anil Jain, Karthik Nandakumar and Arun Ross, “Score normalization in multimodal biometric systems”, Journal of Pattern Recognition society, Vol. 38, No.12, pp. 2270 –2285, 2005