International Journal of Computational andExperimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 952-961
http://www.ijcesen.com

ISSN:2149-9144

Research Article

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

Suneetha Madduluri[1]*, T. Kishorekumar[2]

[1]Research Scholar, Department of Electronics & Communication Engineering, NIT Warangal, Telangana, India
* **Corresponding AuthorEmail:**sunithasiva06@gmail.com - **ORCID:**0009-0009-7483-5979

[2]Professor, Department of Electronics & Communication Engineering, NIT Warangal, Telangana, India
Email:kishoret@nitw.ac.in- **ORCID:**0000-0003-0020-1702

Article Info:

DOI: 10.22399/ijcesen.565
Received : 26 October 2024
Accepted : 28 October 2024

Keywords:

Biometrics,
ECG,
VGG16,
Multimodal,
Authentication**.**

Abstract:

Unimodal or Single factor biometric systems refer to biometric systems that employ only one form of biometric data to authenticate an individual's 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 can authenticate more than once and some advantages include; highaccuracy, low error rate, and large population coverage. These biometrics systems increase integrity and privacy since it will contain several biometric features of every customer. 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 capture the intricate details of the face and ECG waveform, ensuring high accuracy in distinguishing different individuals.

1. Introduction

Biometric authentication can be considered a very important component in security practice, aiming at using physiological and behavioural characteristics of people to ascertain their identity. This technique is much superior to the conventional forms of authentication where passwords or physical tokens such as key chain token may get misplaced, forgotten or even be stolen. Finger prints, facial features, or voice structure are unique features of an individual and cannot be mimicked by others; hence such type of data serves as reliable solutions for the purpose of authentication.

The security and privacy issues have remained a worry from the time that Internet started. The most conventional techniques of the user authentication strategies mainly rely on passwords, which are also more frequently used. In the past, passwords were used to authenticate users to a central computer in an Intranet environment where the chance of getting the passwords compromised was very small due to the non-connectivity of the Intranet to other networks. However, in the present context, the devices are more connected to the Local Area Networks and the Internet is always available. Also, as a result of numerous IoT devices integration into the nowadays world, there are more and more individuals whose personal data is transmitted and stored. Consequently, implementing stringent access control policies is essential to ensure effective security and privacy [1].

Multimodal biometrics systems, which use several biometric features for persons identification, have a lot of advantages in comparison with unimodal systems as it has been characterized in several reference articles. These systems enhance the accuracy of the identification and the verification because there are lower probabilities of both false positive as well as false negative. Another advantage of integrated multiple traits is that the system becomes less variable and one or more traits can participate to ensure the reliability of the system. The security is considerably enhanced here because it would be much more difficult for the attacker to spoof or obviate several biometric measures. Multimodal biometrics deal with the problem of non- universality whereby the failure of one biometric cannot hinder the identification process. The convenience is also shifted to the users of these systems since they can offer various modes of authentication; for example, facial recognition may be used instead of fingerprints when required. Thirdly, the multimodal systems offer a higher level of protection from spoofing attacks and also the system adaptability from any specific noisy input ensuring the high degree of reliable performance even under adverse circumstances. Last of all, these systems can be more easily scaled since the recognition process can be distributed across multiple traits so that the processing speed and the efficiency of the systems in question is improved. Altogether, these seem to make the application of multimodal biometrics more secure, more accurate and more friendly systems for identification and authentication [2,3].

ECG based biometric modalities, apply the unique electrical impulses generated by the heart for the identification and authentication of persons. ECG signals are highly personal dependent on the differences in cardiac structure and function and therefore ECG based biometrics are consistent and robust across time. In contrast to the biometric algorithms like fingerprints, face recognition, ECG biometrics provides non intrusive and continuous form of authentication with least amount of interaction from the user once the signal is taken. The security of ECG-based systems can be further improved by the fact that is difficult to imitate or spoof the above said internal physiological signals which in turn makes the system safe from fraud and impersonation attacks. ECG BIs can be extended for various fields including healthcare, finance and IoT since it is highly immunes to different environment challenges. Present researches in ECG Biometric systems seek at optimizing noise reduction process, investigating variability due to physiological parameters and establishing uniform acquisition and processing methodologies so that they can make ECG biometric system more accurate and dependable. Therefore, ECG biometrics implies one of the most effective approaches toward enhancing identification while employing the physiological natures of the subject's cardiac signals [4-9].

Face characteristics refer to multiple physical features of the face that are utilized in biometrics where specific faces characteristics are used in identification as well as verification purposes. The facial recognition techniques define and analyse facial properties like distances of the eyes, length and breadth of the nose and the Jaws line amongst others to form face template for persons. This modality is used because it does not involve any physical touch which entails the use of cameras only to capture images and is used in facials recognition such as unlocking mobile phones, airport security among others. New trends in deep learning especially CNN has improved the recognition system over other systems, making it possible to recognize faces in real time and with high levels of reliability even in changing environment. However, it is not without its problems like its weakness to change in light, pose, and even facial expressions of subject persons. Current studies seek to optimize these factors in addition to ethical issues of privacy and consent with regard to facial traits on biometric authentication systems. Altogether, facial traits as the biometric modalities represent a powerful set of the opportunities, which has a high potential of development in the context of advances noticed in the field of the computer vision and machine learning [10-14].

The major theme of this study is to establish new multi-modal biometric ECG (electrocardiogram) and face recognition to boost security access measures in different hazardous fields. Through the identification of the electrical activity profiles each person's heart possesses, with the aid of this study, this research intends to devise an exceptionally safe, accurate, and non- invasive way for identification. Coming up with ways of obtaining ECG signals at high quality during diverse exercises and in order to eliminate or reduce the noise and additional artifacts to acquire better results. Employing current generation data processing methods and computer algorithms, including pattern matching and machine learning, to analyse ECG data and ascertain the uniqueness of the feature and enhance the speed and reliability of the identity recognition process. Securing ECG biometric system from spoofing and other attendant cyber threats through multi-factor authentication and encryption. Proactively identifying and meeting the customers' needs by creating easily-navigation interfaces and ensuring that the system can be used by heart disease or physically impaired persons. Carrying out extensive experimental and operational trials of ECG biometric systems in practice in order to prove their efficiency and stability when integrating in the preexisting security systems. And bring the development of advanced biometric face recognition systems to increase the security measures in the access and authorization of different regions. Thus, rendering the specifically identified and localized facial features, this work is going to offer a highly accurate, trusted and contactless approach to identity confirmation. Building complex methods of obtaining sharp and clear pieces of facial images in various lighting, orientation of the face and its position, and facial expressions. Also applying the modern algorithms of the facial identification and the machine learning to analyse the biometric data of faces, eliminating the mistakes, such as false positive or false negative. Enhancing the system's ability to counter such spoofs such as photo and video by integrating liveness detection and anti-spoofing mechanisms into the system. It covers the protection of the data from third parties and in some jurisdictions it complies with some prescribed standards that create confidence with the user. Exploring solutions to continue to have elegance and integration with interfaces and experiences unobtrusively while catering for everyone but especially those with facial abnormalities and/or any form of disability. The most significant methodology which can be used to define how effective face recognition systems are and to compare them with the existing security systems is the usage of tests and integrating the systems into the already existing security systems (table 1). Here 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.

2. Literature review existing biometric authentication

Biometric authentication systems are increasingly used for security because they can verify individuals based on unique biological traits.

Table 1. *Overview of the most common systems.*

SI. No.	Authentication Method	Advantage	Disadvantage
1	Fingerprint Recognition	• High accuracy • Cost effective • Easy to use	• Can be affected by cuts, dirt, or wear • Potential for spoofing with h- 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

2.1 Research on Face-Based Authentication

Multi-user active authentication means a need to authenticate multiple subjects; this is problematic for traditional systems. This is addressed by the Extremal Open set Rejection whereby there is a process of identification which uses spare representation followed by a verification process. It employs Extreme Value Theory to build distribution and the primary focus is on the sparsity vector, probability distribution and their overlap for a decision. On three investigated public face-based mobile authentication datasets, the method's applicability in addressing these issues is key[15-21]. A technique that incorporates the user biometrics data with a secret word that is personal to the user. This approach entails discretised random orthonormal projection of the biometric features, eliminating any possibility of error; it also produces non-invertible templates which can be revoked. Another scheme that has not been discretized is also described together with the help of mathematical modeling. The efficiency of both methods is justified on face verification tasks using ORL and GT database, proving the effectiveness of the proposed methods compared to the existing methods[22]. Traditional methods like PINs and short passwords used for smartphone security are increasingly vulnerable to compromise.

2.2 Research on ECG –Based Authentication

There are many previously worked ECG-based researches exist. In that we have gone through few papers like: Security concerns are also relevant in Wireless BSNs especially where_instance, authentication is paramount for the secure communication between the sensor nodes existing in the network. As discussed in the previous subsection, ECG generated by these nodes has real time readout and therefore has inherent liveness. While there are extensive works on the ECG based intranode authentication in WBSNs, privacy preservation of ECG-sensitive data has received more consideration. The present paper presents an ECG-Based Authentication System with Privacy Preservation Assume a noninvertible transform called the manipulable Haar transform (MHT). This system also protects the intranode authentication as well as the rather sensitive ECG data from disclosure [18]. ECG has proven to be a reliable biometric for human identification as it provides seamless and none stop identification without much possibility of imitation. In many cases, however, many of the current algorithms necessitate long data of ECG, making its applicability a bit restricted. In this paper, a two-phase of authentication using the neural network which we named 3 seconds-user-authentication-NN with a reliable performance is proposed. In the first phase applied and tested on 50 subjects using mobile collected finger ECG signals with general condition the general NN model and then the personal NN model is used. By analyzing the results shown in the graph, one can conclude that the algorithm is effective when applied on the whole set of products as well as on the subgroups of various sample size [19]. Some of the medical IoT applications are used by patients for health monitoring whereby they allow physical examination through sending their own health records to the hospitals. However, security and privacy concerns emanates from the fact that health information is sensitive. Widgets and insufficiently protective in the context of health monitoring's privacy and security requirements. Biometric authentication particularly using ECG signal is therefore an effective method of human characteristic verification. Nevertheless, ECG seems to be highly appropriate for biometric applications, it is in most cases even usable practical realization of ECG-based authentication which encounter such problems as data noise and concern for privacy.

2.3 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. [24-26].

3. Methodology

3.1 Facial Image Data Collection:

Facial data is collected from by taking 8-9 seconds of video from 30 different individuals. As for this procedure, We Used ESP32 CAM. The resolution we decided to go with is 'XGA 1024 X 768 p x'. This of course involves taking different poses, and facial expressions, to capture as many poses and expressions as possible. From these videos we had multiple image extracts and further process.

3.2 ECG Data Collection:

For the ECG biometric authentication dataset, we considered the MIT-BIH Arrhythmia Database. MIT-BIH Arrhythmia Database comprises 48 half-hour excerpts from two-channel resting ECG recordings of 47 patients examined at the BIH Arrhythmia Laboratory between 1975 and 1979. The recordings were digitized at 360 samples per second per channel at 11 bits resolution within delta mode of 10 mV range. Two or more cardiologists did label each record and disagreement reached a consensus so as to get computer readable reference annotation for each beat. All the records of the MIT-BIH Arrhythmia Database are kept in this directory and around 50% of the data since the inception of PhysioNet in 1999.

3.3 Face Image preprocessing

We shot videos that lasted 8-9 seconds, we took several frames so as to get a diversity of views of faces. Every frame passed through cropping where the subject's face was extracted with focus on the important facial parts devoid of any unnecessary background elements. Subsequently, the cropped images were converted to grayscale in order to reduce the computational demands on the model, and in addition to help the model filter out unnecessary detail in facial images such as the colour detail. This preprocessing step helped in generation of a fascinating and robust dataset to include different facial expressions and orientations which are so vital for correct facial authentication.

3.4 Electro Cardiogram Signal Extracting:

ECG data was collected from MIT-BIH Arrhythmia Database. Signal restoration goal is to improve signal clarity through reduction of interference. This involved using a bandpass filter technique in which it became easier to select a certain frequency of the signal that is most appropriate for analysis. Thus, by confining interest to these specific frequency bands—While functionally comparable in some aspects of the signal filtering methodology, the use of the mathematical Fourier Transform has major advantages in later analysis.—the system was able to filter out response components that were of little use in analysing the ECG waveform for the medical diagnostics application in this paper. Following noise removal, the signals are then divided into different regions representing different phases or events in the cardiac cycle. These segmented images were then stored for more analysis and visualization to get clearer view of ECG data without any noises that were not needed. It is not only enhancing the performance of ECG signal interpretation, but also guarantees that the extracted data from ECG signal are useful and contain meaningful information for medical diagnosing or further researches.

3.5 Deep Learning Algorithm – VGG16:

The VGG16 engine is a computational tool which can be used to identify various objects or pictures in a particular image. They are made up of more than one layer that are; the convolutional layer, the pooling layer, then the fully connected layer. VGG16 mimics the human visual system and proved to be able to extract features of different abstraction levels as well to detect spatial relations within the images. Due to its construction, VGG16 puts together unseen layers in a certain sequence to enable the model to learn about hierarchical attributes. The pre-processing in VGG16 is like the human's brain where it only focuses on very crucial features that will help it make a better decision. The VGG model modification aims to enhance the

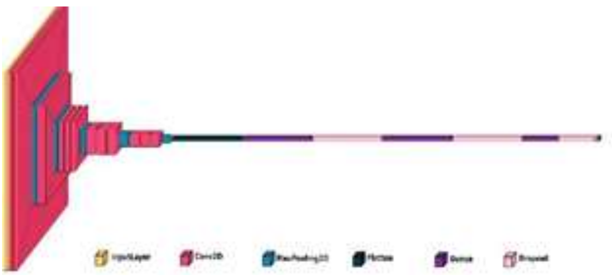

Figure 1: *VGG16 Architecture which we used for both Face and ECG*

speed in training and improve the optimization for certain classification learning tasks for feature learning. To make the understanding of our model easier, Fig. 1 below depicts a graphical representation of our model. Here, the base model is the VGG16, which is first started with out the final layers so that it can contain individual classifier layers. The first and foremost, all layers of the network are frozen with the exception of the layers that are responsible for feature extraction and by doing so computational resources are conserved yet the ability to extract intricate visual features from images are retained. Moreover, the VGG16 model has introduced new classifier layers with an aim of making it more flexible. It is basically a deep learning based model, having three fully connected layers with rectified linear unit activation incorporated in between to avoid problem of overfitting, which are followed by dropout layers. The dense layers consist of neurons amounting to 4096 in each of the layer and the next layer containing 2048 neurons and the final layer; soft max layer contain 30 classes for specific purposes of classification. First, it adheres to the primary development of the deep learning model for identification of hierarchical patterns in the target visual data source; second, it aligns with the standard recommendations used in model refinement for enhancing the intended model accuracy.

3.6 Input Data for evaluation

For capturing input data, we employ the ESP32-CAM module with real time facial images and accurate waveform results from upgraded medical equipment for accurate waveform input. At the moment, the ESP32-CAM is used in the live face capture to offer real-time facial data for the purpose of authentication. Incorporation of the ESP32-CAM also enables the capture of high-quality facial images from the original source improving the reliability of the face authentication model. The future work will involve converting ESP32-CAM to implement real-time ECG biometric data into the architecture of the proposed biometric system making it more stable and versatile.

3.7 Flow Chart

3.8 Authentication

By analysing the fig. 2 we can easily understand that data preprocessing of face and ECG are different from each other. For the case of facial data the images were cropped up to faces and grayscale while for ECG data the noise was removed and the signals segmented. Then feature extraction done with VGG16 architecture, model vgg16.F To combine and access both the ECG and face biometrics models

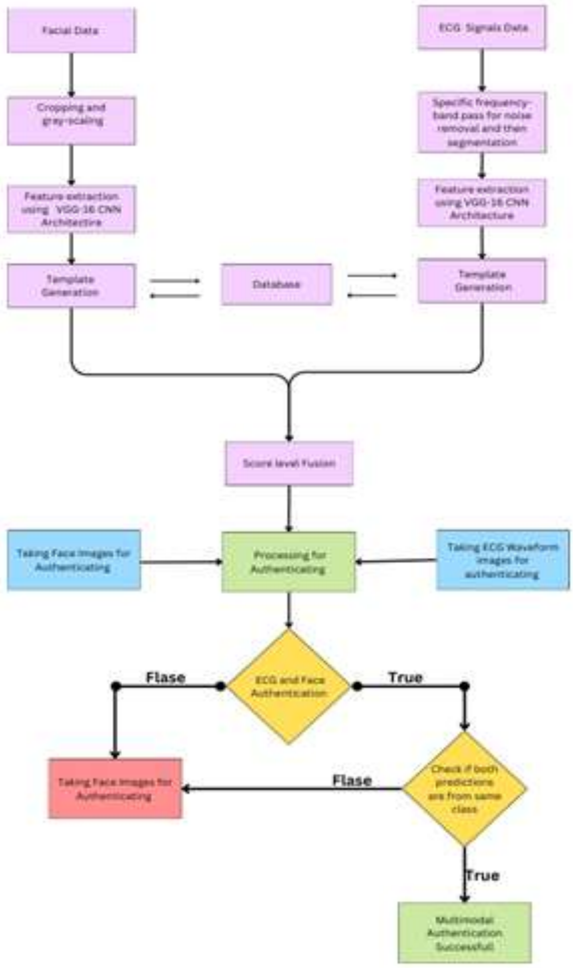

Figure 2. *Complete Flowchart*

we used logical 'and' operator. Users are asked for their ECG data which they can upload in the application and their face data through a camera interface. The system then processes these inputs by loading the respective pre-trained models: One of the door locks will be for ECG authentication on the other for face recognition. The ECG and the face model compare an uploaded ECG signal and the facial for identification by using a threshold score. Then after that if one model confirms the other model result that the ECG and face data belong to the same person then the system announces "Authentication for Weapon successful. 'Person (no.) Unlocked. " and the system records the result. Otherwise it will display "Authentication Failed". Such an integration guarantees a fast and efficient biometric authentication since it combines the best features of ECG signals and facial recognition.

4. Results and Discussions

4.1 Performance Evaluation

In order to analyse performance of the models trained, key performance indicators were used for the ECG authentication, the face authentication as well as their fused model (table 2). In particular, Accuracy, Recall, Precision and F1 score was used for the evaluation as these measurements give the complete overall view about the performance of each model in terms of true positive and false results. Recall: It measures the proportion of true positives correctly identified.

$$\text{Recall} = \frac{True\_Positive(TP)}{True_{Positive(TP)} + False\_Negative(FN)}$$

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

$$\text{Precision} = \frac{True\_Positive(TP)}{True_{Positive(TP)} + False\_Positive(FP)}$$

F1: This score offers a measure of repertoire of precision and the amount of recall all rolled into a single performance metric.

$$\text{F1 score} = \frac{Precision * Recall}{Precision + Recall}$$

Accuracy: It stands for the ratio between the number of correct predictions to the total number of predictions that was made.

$$\text{Accuracy} = \frac{True\_Positive\ +\ True\ Negative\ (TN)}{All\ Samples}$$

Table 2: *Comparative Metrics Evaluations*

	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 gives the user an understanding of the classifier whereby the y-axis represents the improved class and the x-axis represents the reduced class over the total classes implemented for the classifier. (fig. 3, fig. 7).
A model loss graph shows the error function based on training wherein the convergence of the model and the ability to minimize the mistakes are presented. (fig. 4, fig. 8)
The ROC curves are used to portray the diagnostic capacity of the binary classifier frameworks crosswise over discrimination points, it is basically a

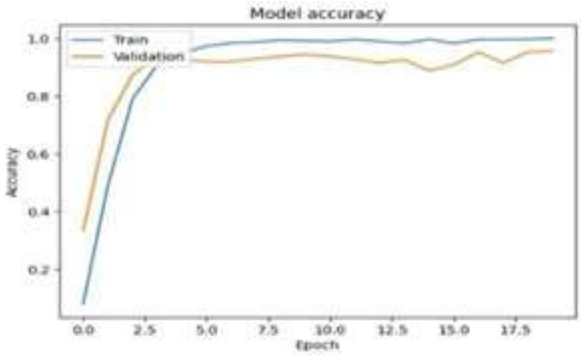

Figure 3*. Model's accuracy curve for face recognition*

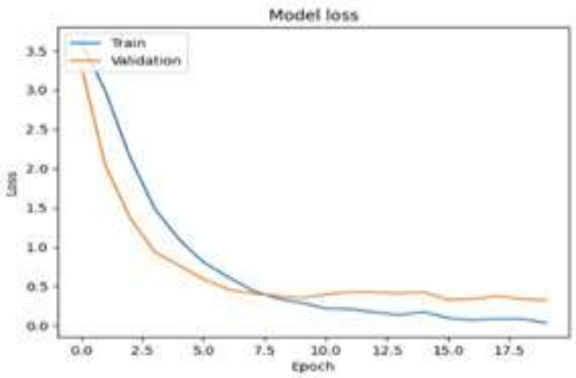

Figure 4*. Model's loss curve for face recognition*

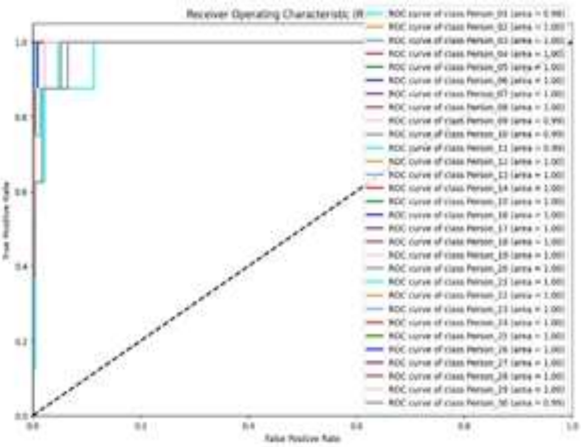

Figure 5. *ROC for face recognition*

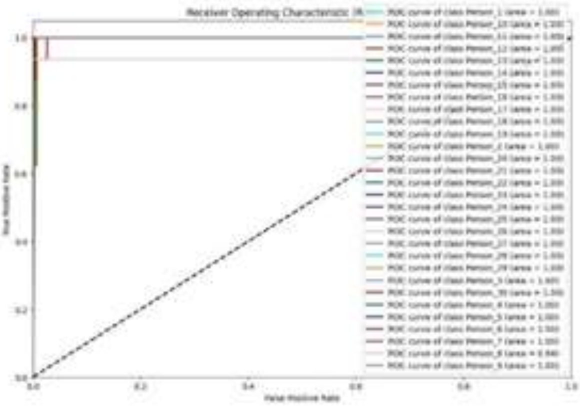

Figure 6*. Confusion Matrix for face recognition*

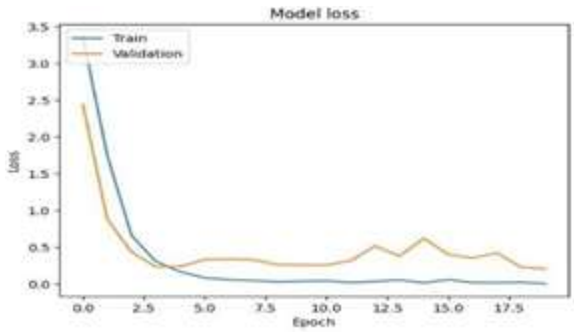

Figure 7. *Model's accuracy curve for ECG recognition*

graph of the true positive rate versus false positive rate measurement. (fig. 5, fig. 9, fig. 11)

Lastly, the confusion matrix also provides a detailed view of the classification results in that it shows the number of examples which have been correctly classified and misclassified by the model, thereby providing a deeper insight of the efficiency of the model. (fig. 6, fig. 10, fig. 12)

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

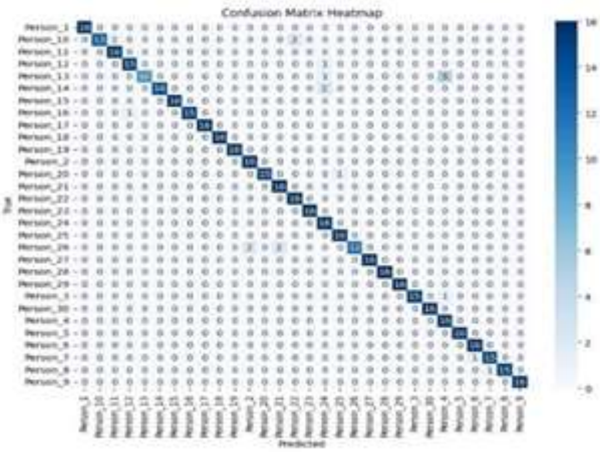

Figure 8*. Model's loss curve for ECG recognition*

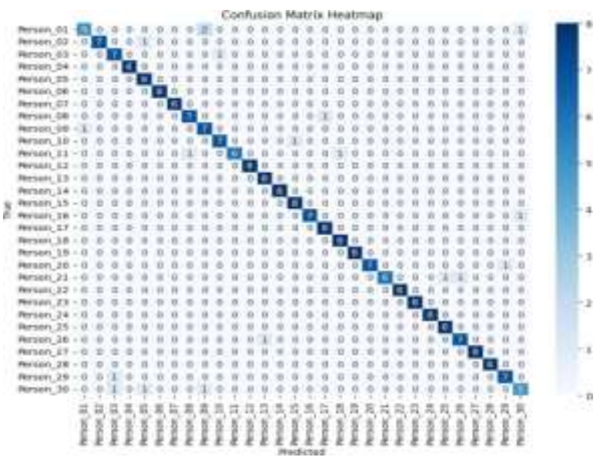

Figure 9*. ROC for ECG recognition*

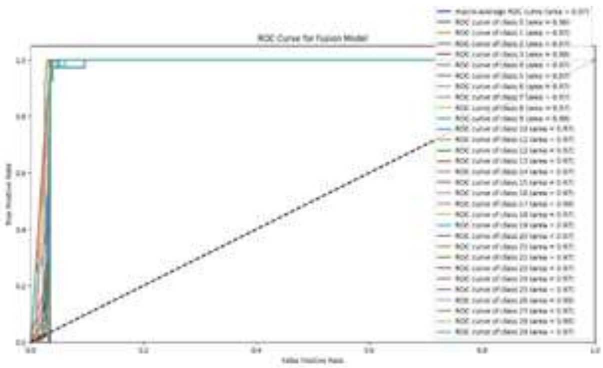

Figure 10. *Plot of Confusion Matrix for ECG recognition*

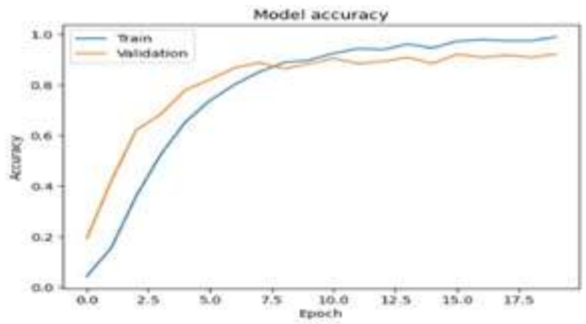

Figure 11. *ROC for Fusion*

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.

Figure 12. *Confusion Matrix for fusion*

Figure 13. *Authentication Success*

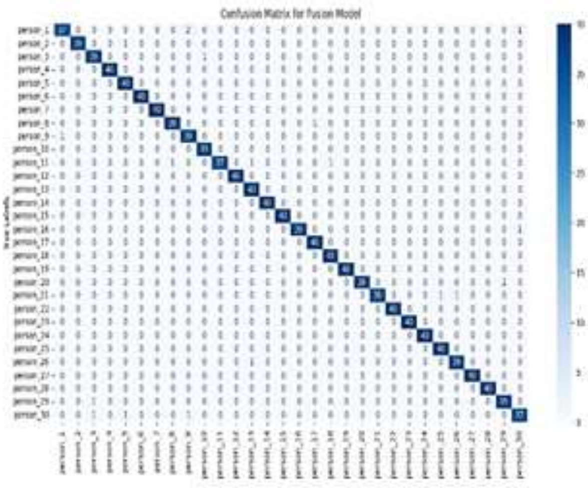

Figure 14. *Authentication Failure*

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).

5. Conclusion

In conclusion, our study strongly highlights the problems of employing the unimodal biometric systems that are based on the single modes such as fingerprints or face. These systems are prone to exhibit higher errors and security threats because they rely on one factor of identity. To overcome these challenges, the paper supports the use of multiple biometric systems. By combining different biometric attributes, including ECG waveforms as well as the facial structure. The development of our proposed multimodal system means that there are improvements in terms of accuracy and reliability. Particularly, the proposed approach based on the VGG16 model provided results with a 92. 09% of accuracy for ECG data, 95. 6% for the facial data, and overall accuracy of 98%. 28% when combining both the vocal and visual modalities. This shows that the combination of multimodal biometric increases the reliability of the authentication process, increases integrity levels, and protects users from privacy invasions in different applications.

Author Statements:

- **Conflict of interest:**The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:**The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:**The authors declare that they have equal right on this paper.

- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] L. Sun, Z. Zhong, Z. Qu and N. Xiong, (2022). PerAE: An Effective Personalized AutoEncoder for ECG-Based Biometric in Augmented Reality System, *IEEE Journal of Biomedical and Health Informatics*, 26(6);2435-2446, doi: 10.1109/JBHI.2022.3145999.

[2] D. Jyotishi and S. Dandapat, (2022). An ECG Biometric System Using Hierarchical LSTM With Attention Mechanism, *IEEE Sensors Journal*, 22(6);6052-6061 doi: 10.1109/JSEN.2021.3139135.

[3] R. Cordeiro, D. Gajaria, A. Limaye, T. Adegbija, N. Karimian and F. Tehranipoor, (2020). ECG-Based Authentication Using Timing-Aware Domain-Specific Architecture, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(11);3373-3384, doi: 10.1109/TCAD.2020.3012169.

[4] S. S. Abdeldayem and T. Bourlai, (2020). A Novel Approach for ECG-Based Human Identification Using Spectral Correlation and Deep Learning, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2(1);1-14, doi: 10.1109/TBIOM.2019.2947434.

[5] L. Pu, P. J. Chacon, H. -C. Wu and J. -W. Choi, (2022). Novel Robust Photoplethysmogram-Based Authentication, *IEEE Sensors Journal*, 22(5);4675-4686, doi: 10.1109/JSEN.2022.3146291.

[6] B. L. Ortiz, J. W. Chong, V. Gupta, M. Shoushan, K. Jung and T. Dallas, (2022). A Biometric Authentication Technique Using Smartphone Fingertip Photoplethysmography Signals, *IEEE Sensors Journal*, 22(14);14237-14249, doi: 10.1109/JSEN.2022.3176248.

[7] S. Hinatsu, N. Matsuda, H. Ishizuka, S. Ikeda and O. Oshiro, (2022). Identification of PPG Measurement Sites Toward Countermeasures Against Biometric Presentation Attacks, *IEEE Access*, 10;118736-118746, doi: 10.1109/ACCESS.2022.3221456.

[8] S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda and O. Oshiro, (2022). Evaluation of PPG Feature Values Toward Biometric Authentication Against Presentation Attacks, *IEEE Access*, 10;41352-41361, doi: 10.1109/ACCESS.2022.3167667.

[9] S. A. Raurale, J. McAllister and J. M. D. Rincón, (2021). EMG Biometric Systems Based on Different Wrist-Hand Movements, *IEEE Access*, 9;12256-12266, doi: 10.1109/ACCESS.2021.3050704.

[10] S. K. Behera, P. Kumar, D. P. Dogra and P. P. Roy, (2021). A Robust Biometric Authentication System for Handheld Electronic Devices by Intelligently Combining 3D Finger Motions and Cerebral Responses. *IEEE Transactions on Consumer Electronics*, 67(1);58-67, doi: 10.1109/TCE.2021.3055419.

[11] Pradhan, J. He and N. Jiang, (2021). Performance Optimization of Surface Electromyography Based Biometric Sensing System for Both Verification and Identification, *IEEE Sensors Journal*, 21(19);21718-21729, doi: 10.1109/JSEN.2021.3079428.

[12] Ranjeet Srivastva, Ashutosh Singh, Yogendra Narain Singh, (2021). PlexNet: A fast and robust ECG biometric system for human recognition, *Information Sciences*, 558;208-228, https://doi.org/10.1016/j.ins.2021.01.001..

[13] S. A. Raurale, J. McAllister and J. M. D. Rincón, (2021). EMG Biometric Systems Based on Different Wrist-Hand Movements, *IEEE Access*, 9;12256-12266, doi: 10.1109/ACCESS.2021.3050704.

[14] D. Y. Hwang, B. Taha, D. S. Lee and D. Hatzinakos, (2021) Evaluation of the Time Stability and Uniqueness in PPG-Based Biometric System, *IEEE Transactions on Information Forensics and Security*, 16;116-130, doi: 10.1109/TIFS.2020.3006313.

[15] Li, Q.; Dong, P.; Zheng, J. (2020). Enhancing the security of pattern unlock with surface EMG-based biometrics. *Appl. Sci.*, 10, 541.

[16] Khan, M.U.; Choudry, Z.A.; Aziz, S.; Naqvi, S.Z.H.; Aymin, A.; Imtiaz, M.A. (2020). Biometric authentication based on EMG signals of speech. In *Proceedings of the International Conference on Electrical, Communication, and Computer Engineering, Istanbul, Turkey*, 12–13 June 2020.

[17] Zhang, X.; Yang, Z.; Chen, T.; Chen, D.; Huang, M.C. (2019). Cooperative sensing and wearable computing for sequential hand gesture recognition. *IEEE Sens. J.*, 19, 5575–5583.

[18] Oh, D.C.; Jo, Y.U. (2019). EMG-based hand gesture classification by scale average wavelet transform and CNN. *In Proceedings of the International Conference on Control, Automation and Systems, Jeju, Korea*, 15–18 October 2019.

[19] Qi, J.; Jiang, G.; Li, G. (2020) Surface EMG hand gesture recognition system based on PCA and GRNN. *Neural Comput. Appl. 32;*6343–6351.

[20] Chen, L.; Fu, J.; Wu, Y.; Li, H.; Zheng, B. (2020). Hand gesture recognition using compact CNN via surface electromyography signals. *Sensors* 20;672.

[21] Asif, A.R.; Waris, A.; Gilani, S.O.; Jamil, M.; Ashraf, H.; Shafique, M.; Niazi, K. (2020). Performance evaluation of convolutional neural network for hand gesture recognition using EMG. *Sensors* 20;1642.

[22] K. Prlhodova and M. Hub, (2019). Biometric Privacy through Hand Geometry-A Survey, *International Conference on Information and Digital Technologies (IDT): IEEE*, pp. 395-401.

[23] J. J. Winston and D. J. Hemanth, (2020). Moments-Based Feature Vector Extraction for Iris Recognition," in *International Conference on Innovative Computing and Communications:* Springer, pp. 255-263.

[24] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, and C. Valli, (2019). Integration of biometrics and

steganography: A comprehensive review, *Technologies*, 7(2);34.

[25] Sekhar, J. N. Chandra, Bullarao Domathoti, and Ernesto D. R. Santibanez Gonzalez. (2023). Prediction of Battery Remaining Useful Life Using Machine Learning Algorithms *Sustainability* 15(21);15283 https://doi.org/10.3390/su152115283.

[26] F. Caldwell, (2019). Voice biometrics systems and methods, *ed: Google Patents.*