Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ELECTROCARDIOGRAM PLETHYSMOGRAPHIC ELECTROMYOGRAMS BASED BIOMETRIC AUTHENTICATION MODELS

SUNEETHA MADDULURI[1], T. KISHORE KUMAR[2]

[1]Research scholar, Department of Electronics and Communication Engineering, NIT Warangal, Telangana, India

[2]Professor, Department of Electronics and Communication Engineering, NIT Warangal, Telangana, India.

E-mail: [1]sunithasiva06@gmail.com [2]kishoret@nitw.ac.in

ABSTRACT

To verify humans identity, biometric authentication techniques examine observable characteristics. This may be based on a person's fingerprint, iris, retina, Electrocardiogram (ECG), Plethysmographic (PPG), Electromyograms (EMGs) or some other identifying features. There is flexibility in the usage of a single trait or a combination of traits. Because they are both discrete and distinctive, electrocardiograms (ECGs), photoplethysmograms (PPGs), and electromyograms (EMGs) have been investigated as possible biometric features in the last several decades. Research into biometric recognition technologies that are user-unobtrusive has been accelerated by the increased availability of wearable sensors and mobile devices. Due to their distinct characteristics, electrocardiogram (ECG) signals have recently been investigated as a potential biometric identification trait. An electrocardiogram (ECG) can only be used to collect data from individuals who are still alive, as it measures the electrical activity of the heart. The research community is interested in evaluating cardiac signals derived from PPG signals for a number of reasons, one of which is the capacity to perform continuous authentications with affordable devices that can gather signals without user intervention. With the declining quality and resolution of gathered images and security issues such spoofing and copying, this study intends to discuss and analyze biosignals based biometric authentication, which has been dominating former conventional methods. This research provides a brief analysis of ECG, PPG and PCG and their advantages and limitations and proposed an ECG based Biometric Authentication using CNN (ECG-BA-CNN). This analysis helps numerous researchers to design novel biometric innovations overcoming the limitations of traditional models.

Keywords: *Electrocardiogram, Plethysmographic, Electromyograms, Biometric Authentication, User Identity, Security.*

1. INTRODUCTION

These days, recognition systems and authentication systems are employed in many different places to keep ourselves and our data safe. Some of these systems still rely on antiquated technologies like cards, keys, and passwords, despite the fact that these mechanisms frequently provide usability and security challenges. This has led to a renewed focus on biometrics in recent years [1]. Biometrics is a form of automatic identification that makes use of a person's unique physical or behavioral traits. Face, fingerprint, iris, and hand geometry are examples of biometrics, while gait signature and keystroke are examples of behavioral biometrics [2].

ECG signals have been investigated as a biometric recognition trait in recent years because to their distinctive characteristics. Since an electrocardiogram is a recording of the heart's electrical activity, only signals from alive people may be retrieved from an ECG [3]. The analysis of ECG signals can tell us information about a person's identity in addition to their heart conditions as well as emotional and physical status, and they have a high level of security because they are so difficult to forge. Most importantly, ECG signals are highly individual due to variations in ionic potential, plasma electrolyte levels, and physiological variables induced by chest geometry, heart size, and heart position. P waves, QRS complexes, and T waves are the building blocks of an ECG wave, as shown in Figure 1.

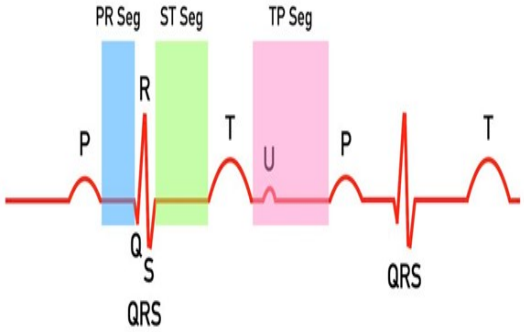

Fig 1: ECG Signal Parts

A biometric system is a piece of equipment that can detect and verify an individual's identity based on their biological characteristics. An acquisition module, a storage module, and a biometric algorithm make up the system's three primary components. Data from the capture and storage modules are processed by the biometric algorithm in two stages: extraction of features and pattern recognition. Several methods exist for acquiring ECG signals for use in biometric systems. Holter ECGs record electrical activity from 5–7 leads for longer lengths of time than the normal 12-lead ECG, which only records for a brief period of time [4]. 12-lead ECGs have the potential to offer more data, however they are impractical for clinical application. Instead, non-invasive techniques have grown more widespread that capture ECG data through skin or finger contact.

With recent developments in sensing technology, ECG is being investigated as a potential non-invasive biometric alternative to other methods such as fingerprinting. This has resulted in ECG's increasing popularity as a biometric. Small wireless ECG sensors for the body are being developed as an adjunct to the more commonplace off-the-body approaches. These monitors use a solitary wire to assess the space between two cardiac electrodes [5]. Because of these sensors, ECG analysis and monitoring can now be applied to fields other than cardiology. However, wearable sensors generate noisier signals than medical devices like Holter devices due to factors including electrode type, number of leads, and placement [6]. Wearable devices typically only employ one to three dry electrodes, with only the first lead used because it is easily implemented in mobile devices, in contrast to the 12 or 6 wet electrodes used by medical ECG recorders. Due to their more involved design and longer recording times, medical ECG recorders tend to produce more trustworthy results than wearable devices [7].

However, ECG signals are difficult to fake because the underlying biometric features are hidden during authentication and can only be obtained through physical measurements of the subject. This is because ECG signals exhibit distinctive physiological features across subjects related to the position and dimensions of the heart. It is crucial to develop a strong approach that accounts for the intra subject variability of the ECG in order to achieve reliable authentication. Continuously collecting and learning ECG data from the user can be one method to achieving a solid identification result with the robustness to the non-stationarity of ECG. After each login attempt, incremental learning is used to update the user identification model rapidly and in real time.

Using a person's unique pattern of behaviour or physical characteristics, biometrics can reliably verify their identity. EMGs, ECGs, PPGs and Electroencephalograms (EEGs) are all types of biosignals. Among these is the EMG signal, which is a voltage reading taken from a micro current that is produced whenever a muscle contracts. Needle electrodes and surface electrodes are used to measure electrical muscle activity. Inserting a needle electrode into a muscle and monitoring the resulting action potential is known as the needle electrode method. Electrodes are placed on the skin's surface to measure an action potential using the surface electrode method. The use of EMG signals in biometrics research has lagged behind those of ECG. PPG and EEG [8]. A problem of EEG signal measurement is that it is distorted as it travels through the skull, while a drawback of ECG signal measurement is that it is a periodic signal, meaning that the waveform of the signal can't be changed if the recorded data is hacked. The EMG signal is simpler to measure than other signals, and its registration data can be altered in a way that is not shared with other gestures with the characteristic indicating a unique waveform of the signal for each action. In previous efforts, EMG signals have been applied to the recognition of gestures or as standalone biometrics [9]. The EMG signals components are shown in Figure 2.

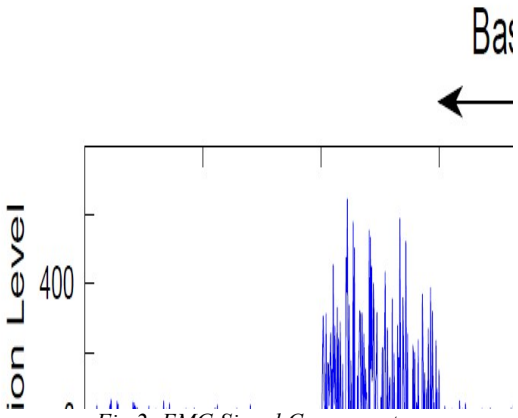

Fig 2: EMG Signal Components

Biometric recognition based on PPG is seen as a promising field of study as of late. Although there have been reports of some success with PPG biometric recognition, difficulties in noise sensitivity and inadequate robustness remain. PPG-based biometric systems are applicable to a wide variety of domains [10], including health monitoring and fitness tracking, where the signals are already received and processed for other purposes. PPG-based biometric systems may collect PPG signals from a wide variety of devices, including those with built-in heterogeneous sensors like medical tools, wearables, cellphones, and digital cameras. Algorithmic methods and Computational Intelligence methods are both viable foundations for biometric recognition [11]. The optical technique of PPG is used to detect and quantify changes in blood flow throughout the human body. PPG signals are routinely used in the clinic to measure blood oxygen levels, heart rates, and other vitals to aid in the diagnosis of cardiovascular diseases [12]. Researchers have begun to investigate the feasibility of using PPG signals in the field of information security because they are relatively simple to acquire and include a plethora of personally identifiable cardiac information [13]. The PPG signal enhances the safety and usability of the identification process with its distinct benefits.

PPG is a non-invasive visual method for detecting the volume of light intercepted or reflected via microvascular in biological tissues, which makes it one of the physiological signals [14]. Because of its distinct benefits, PPG also offers a wide variety of future research opportunities in authentication. Signals from the face, fingertips, and toes can all be collected with just a camera or pulse oximeter to create a full PPG. PPG sensors built into wearable technology also make it more convenient and less expensive to get PPG signals [15]. There are many straightforward ways to compromise conventional biometrics. Copying a user's fingerprints or palmprint from a surface they touched is possible, while distant photographs of the iris or face are possible. PPG signals, on the other hand, are obscured from the attacker's view, making them more difficult to spoof [16]. Since the PPG signal is sensitive to human heartbeat information, the natural liveness detection method guarantees the vitality of all system participants. The PPG signal is shown in Figure 3.

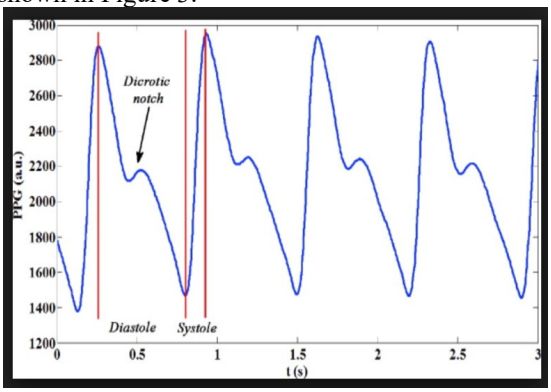

Fig 3: PPG Signal

2. LITERATURE SURVEY

The widespread use of biometric authentication has led many to forego the use of passwords altogether. Biometric recognition technology allows for easier identification verification thanks to its reliability and ease of use. One security problem with biometric authentication is how easily it may be stolen or leaked. Many recent incidents involving cybercrime, data leaks, unauthorized data modification, personal account hacking, etc., have their roots in the widespread usage of insecure password-based security solutions. Therefore, there is a need for a more secure system that can eliminate these security issues. Biometric authentication technology offers a potential alternative that cannot be hacked. This system uses software to identify or validate the user by matching the data with digital images of their unique characteristics.Because this data is impossible to copy or steal, the identification is more trustworthy.

As Augmented Reality (AR) and Virtual Reality (VR) continue to advance, more and more biometric data are being acquired from a variety of sources. The privacy hazards are elevated due to the importance of these data. One common Biometric method is Electrocardiogram-based Identity

Recognition (EIR). The electrocardiogram is a time-continuous biological aspect of the individual. Therefore, EIR may be safer from attacks than more used Biometric techniques like face recognition. Personalized Auto Encoder (PerAE) is an EIR system proposed by Sun et al. [1] based on Autoencoder. Each user in PerAE is represented by a miniature autoencoder model. The Attention-MemAE incorporates a memory module and two attention algorithms to further improve the autoencoder's performance. A person's Attention-MemAE identifies irregularities in other people's heart rates. When the user modifies the way their ECG data is distributed, they can refresh their Attention-MemAE. PerAE's use of personalised autoencoder helps it work faster while requiring less memory. It makes EIR systems more flexible, scalable, and easy to manage.

Recently, interest in biometric systems based on ECGs has increased. The key benefits of an ECG based biometric system are the ease with which signals may be acquired and the system's resistance to forgery. This biometric technology can facilitate the automation of patient authentication and identification for more individualised medical care. In this research, Jyotishi et al. [2] introduced a unique hierarchical long short-term memory (HLSTM) model based on attention for learning a person's biometric representation. To learn the variation in time of the ECG signal at various levels of abstraction, the HLSTM model is proposed in this article. This solves the problem of LSTM network reliance over the long term that users were experiencing. The model's attention mechanism is trained to focus on ECG complexes that include the most relevant biometric data for a given individual. More emphasis is placed on these ECG complexes in order to acquire a more accurate biometric depiction. Since the suggested approach does not rely on the detection of fiducial points, it is simpler and more effective. Using three on-person ECG datasets and two off-person ECG databases, the author tested the suggested approach for solving the person verification and identification difficulties.

Due to the unique, pervasive, and clearly recognisable nature of ECG signals, ECG biometric authentication (EBA) is a viable option for human identification, especially in consumer electronics. Therefore, EBA computing designs require precision, speed, low energy consumption, and safety. Cordeiro et al. [3] used an EBA method to provide a perfect authentication success rate. The author next conducted a detailed analysis of the program to demonstrate the steps' varying execution times and pinpoint the latency bottleneck. The author analyzed the algorithm's execution needs and propose a domain-specific architecture (DSA) to reduce latency and optimized its performance. The author investigated many variants of the DSA, one of which has the additional benefit of assuring constant timing across the various EBA processes, to lessen the possibility of timing-based side-channel assaults.

The ECG is the primary biometric modality employed in this paper for individual authentication purposes. The following are the design steps for the suggested method. The original informational content of the ECG signal is enriched by first segmenting the data and then exploiting its cyclostationarity and spectral correlation. After that, Abdeldayem et al. [4] created spectral correlation photographs. The author skipped the algorithmic phase of detecting fiducial points and removing noise, which is common in other ECG-based machine learning systems but slows down our process significantly. The author then feed the spectral correlation images into two different convolutional neural network (CNN) architectures, fine-tune, test, and assess them, and finally recommend an architecture that shows increased human identification accuracy based on ECG data. The author conducted cross-validation on nine large and small scale ECG databases that include both normal and pathological ECG signals to assess the efficacy of the suggested technique.

The standard password-based systems have been replaced by the biometric authentication approach as a result of the remarkable improvements in the biosensing technology. Applications involving PPGs have gained a lot of interest in recent years due to the fact that they pose no health risks to users. Variations in peripheral blood volume can be measured using PPG. PPG signals are extensively utilized because they can be acquired by low-cost wearable electronic devices and are relatively simple to compare to other biometrics. Instead of performing authentication only once, as is done with traditional methods, Pu et al. [5] developed a revolutionary robust PPG-based authentication system that may authenticate the user on a constant basis. Preprocessing, filtering, motion artefact (MA) removal, template/feature extraction, and training are the components that make up this novel method. As a result, the learning model is able to more accurately categorize users with the related multiwavelet-based feature extraction process, which provides more dependable features than the typical scalar-wavelet approaches. A perfect mapping between the input PPG signal and the latent space is achieved by the corresponding

autoencoder. In conclusion, any distance metric can be utilised for user authentication and classification. Using a person's unique physiological characteristics, or biometrics, to verify their identity is called biometric authentication (BA). Financial transactions, data privacy, and security systems are just some of the many areas where BA has been put to use. Devices like smartphones, smartwatches, and webcams can easily acquire biometric signals through photoplethysmography (PPG). In this research, Ortiz et al. [6] introduced a BA classifier technique for mobile devices that eliminates motion and noise artefacts (MNAs) from raw PPG data before using them to identify people. The BA classifier algorithm uses an EBT classifier with 16 time- and frequency-domain PPG signal characteristics. Measures of sensitivity and specificity, such as the false positive (FP) and false negative (FN) rates, are crucial in the context of BA. Both the FP and FN values were within acceptable ranges.

In this research, Hinatsu et al. [7] proposed protecting a biometric identification system based on PPGs from a presentation attack. By comparing the PPG waveforms recorded at authentic measurement locations to those recorded at non-genuine sites, the countermeasure is able to detect fraudulent PPG signals without the need for additional sensing components. Using PPG signals acquired from several measurement locations on participants and mapped signals to construct fake signals for authentication, the author estimated coefficients of correlation as the similarity indices between PPG waveforms in an experiment. After determining where on the body to take measurements using feature values extracted from PPG signals, the author analyzed the efficacy of the proposed countermeasure.

In this research, Hinatsu et al. [8] looked at PPG based biometric authentication and evaluated an attack based on information leaking. Several methods have been proposed to use PPG to wearable biometric authentication; nevertheless, PPG-based authentication may be vulnerable to a variety of assaults. The information leakage from the numerous PPG measuring points on a body can be exploited in a presentation attack (PA). The PPG of the victim is secretly recorded by the PA on bogus measurement sites and then sent to the PPG sensor in order to circumvent authentication. By comparing the feature values retrieved from the PPG signals, the author was able to examine the information leakage and evaluate the PA. Twelve volunteers' PPG signals were captured from their fingertips and wrists. The author computed differences, correlation coefficients, and mutual information between the feature values retrieved from the recorded PPG signals in order to investigate the loss of information necessary for the PPG-based authentication. The author next computed the permutation relevance of all feature values to evaluate the contribution of each value to authentication and PA, and determined whether or not a PA based on existing PPG-based authentication techniques is feasible.

Human attempts to interact with and manage equipment like robots, prostheses, or virtual worlds are elevating the relevance of EMG acquisition and analysis. In some circumstances, only authorized users should have access to such features. To the best of the authors' knowledge, no prior art exists that can identify persons from a wide range of wrist-hand motions EMG readings within the wearable device, making the security of EMG-based control a major outstanding concern for these applications. Raurale et al. [9] discussed this issue. Methods are discussed that can be utilised to validate users using EMG as a biometric. Users can prove their membership in a trusted network without revealing their identities by wearing an EMG-sensing wristband on their lower arms. Three EMG datasets with comparable EMG sensing across sessions were used in the creation of a comprehensive biometric system. Up to 93% accuracy is reached for verification, and 92% accuracy is reached for identification.

Researchers and manufacturers in the field of Consumer Electronics (CE) have been able to incorporate a wide variety of useful sensors into portable devices with the rapid development of sensor technology made possible by the miniaturization of electronic components. Next-generation consumer electronics are including not only conventional sensors like Inertial Measurement Units (IMUs), cameras, fingerprint readers, and proximity detectors, but also cutting-edge technologies like EEGs and EMGs. Modern consumer electronics frequently make use of touch or air signature authentication methods. The security of such authentication methods, however, can be improved through the combination of mental and physical actions. Consumers can be protected from shoulder surfing attacks in this way. Behera et al. [10] proposed a new technique for verifying air signatures by using sensors in next-generation CE devices to analyse finger movements and cognitive activity. The initial step in identifying a signature is to examine the 3D geometrical aspects of the signer's finger movement. The verification process then involves the analysis of concurrent EEG

signals. The system has been trained with the use of Hidden Markov Model (HMM) and Random Forest (RF) classifiers. Though motion artefacts are present, experimental results show that EEG data are closely associated with finger movements during air signatures.

Surface electromyography (sEMG) is a cutting-edge biometric verification technique that has only recently become available. It is crucial to examine the effects of the EMG system characteristics, such as the feature extraction methods and the amount of channels, on the performance of the sEMG-based biometric system in order to establish optimal system parameters. The number of channels varied from one to eight during this research, and three powerful feature extraction techniques—Time-domain (TD) feature, Frequency Division Technique (FDT), and Autoregressive (AR) feature and their combinations were examined bya Pradhan et al. [11]. The effectiveness of sixteen different static wrist and hand motions was rigorously examined in two different authentication modes: verification and identification, for these system characteristics. Twenty-four participants' results showed that, across the board, TD features outperformed FDT and AR features by a statistically significant margin (p0.05). A four-channel arrangement performed similarly to others with a greater number of channels, the data showed.

Using anything that truly describes the individual would allow for more trustworthy verification or identification. Biometrics provide automated ways of identification or verification based on the idea of observable behavioral or physiological traits, like a voice sample or a fingerprint. Both the traits and their uniqueness can be measured. Unfortunately, it is frequently feasible to produce a duplicate that is recognized by the biometric system as a genuine sample, even though these traits should not be replicable.

3. PROPOSED MODEL

Just as fingerprints are absolutely unique for each individual, so too are ECGs in terms of their rhythm and form. Cloning and hacking ECG biometric systems are quite challenging. Therefore, electrocardiogram signals have been implemented in several secure biometric recognition systems. Problems with (i) signal noise, (ii) automatic feature extraction, and (iii) system performance are highlighted throughout the existing research. This work proposes a novel method based on matching templates to ECG in order to address issues that have so far defied conventional approaches. In the pre-processing stage of the proposed method, beat denoising, R-peak detection, and segmentation of the ECG are performed [14]. The suggested method is applied to grayscale images of these noise-free ECG beats. In addition, this work creates a tailored activation function to speed up the convergence of the learning network [15]. The suggested network can automatically discern features within the input data. The proposed method is evaluated in comparison to the current literature, and the network's performance is tested using the open-source ECGID biometric database.

Authentication refers to the steps used to verify the claimed origin of a given item. Due to the critical nature of healthcare data, authentication provides a means of controlling who has access to this information by verifying that their credentials match those already stored on the server. Adaptive authentication relies on the use of deep learning. Security barriers can be lowered and problems with security addressed by putting in place deep learning model [16]. The degree of similarity between a dataset and every possible data classification procedure is computed by deep learning classifiers. Then, using their own made-up measure of likelihood, they pick the most comparable category as the winner. Classifier-based authentication models, on the other hand, only use legitimate class samples during training [17].

Feature engineering is the procedure of extracting useful characteristics from unprocessed data for the purpose of training a deep learning model. In the context of ECG signals for authentication, feature engineering comprises identifying the most relevant and informative aspects of the ECG signals. Some physiological states and characteristics can be identified by looking for specific waveform patterns, amplitudes, or frequency components. During the registration and verification processes, this is a vital step. To do this, features may need to be extracted, selected, and then used in a training classification. To build the authentication method, they need a very complex basis. This means that several features can be extracted from signals. Real-time implementation will be hampered if there are too many features, due to the curse of dimensionality. The same problem with large test datasets may be experienced with deep learning methods. Overfitting is another problem that might reduce performance. So, conventional deep learning methods are laborious and time consuming because they rely on static and hand-crafted features. In their place, a more straightforward structure for an authentication system can be provided by deep

learning algorithms that can self-learn valuable features from input ECG signals.

There are two phases to biometric identification: registration and recognition. During registration, the user collects biometric data that is then stored in a central database. In the recognition phase, collected biometric data is compared to previously recorded data about a previously unknown individual. A successful identification is determined if the features supplied from an unknown individual match the features from the database according to a set of criteria. The success of a biometric identification system depends on a number of factors, and this is a multi-stage process.

Atrial depolarization (P wave), ventricular repolarization (T wave), and ventricular depolarization (QRS complex) are the three principal segments of the ECG that correlate to different cardiac operations. Hybrid ECG features, non-fiducial ECG features, and fiducial ECG features are all available. Discrete-time properties, such as timestamps, pulse widths, angles, and dynamical intervals, are extracted from the ECG using fiducial features, which are based on landmarks within the ECG waveform. Hybrid characteristics combine fiducial and non-fiducial methods, while non-fiducial characteristics modify the feature points through transformation functions. Fiducial approaches are being considered by researchers since they solely use Electrocardiogram data from fiducial markers as characteristics in the temporal domain. Monitoring heart rate and activity with an Electrocardiogram is a common diagnostic tool used for assessing cardiac muscle and electrical function.

The CNN is given a dataset consisting of ECG signals and their respective labels. The input layer is the first stage in the CNN's processing of the ECG signals, while the output layer is the last. There are several units in each layer, which are weightedly coupled to one another and to the units in the layers above and below. As CNN analyses the ECG data, it picks up on the traits that distinguish legitimate from fake readings. Convolution is used to learn these features by slicing the input data using a kernel and then computing the dot products at each place. Following this, the dot products are fed into an activation function, which decides whether or not the unit should be activated. The weights of the units are updated as the CNN analyses the ECG data in an effort to reduce the discrepancy between the predicted and actual labels. Backpropagation is used to train a CNN to appropriately categorize ECG readings. After the CNN is trained, it can be used to determine the authenticity of new ECG signals by classifying them. To do this, we feed the fresh ECG data into a CNN and use its output to create a forecast.

In this study, the suggested CNN architecture depicted in Figure 4 was used to develop the feature patterns for the ECG. There are five convolutional layers in total, each of which is followed by a max pooling layer, fully connected layer, and soft-max layer. The FC layer architecture is standard across all networks. All FC layers are equipped with ReLU activation since local response standardisation does not improve the efficacy of our Electrocardiogram collection and instead increases computation time and memory use.

Fig 4: Proposed CNN Model

Signal registration, preprocessing of signals, feature extraction, feature assessment, feature selection based on informativeness, and feature classification are the main phases of biometric identification. When it comes to biometric identification, there is some debate over which ECG features are most effective. The amplitude and timing properties of the P, Q, S, and T peaks of cardiac cycles are important in authentication model. There is no universally applicable set of characteristics for accurately classifying all ECG signals. It's possible that some traits are useful for discrimination in some settings but not others. Classification efficiency can be improved by using many features in different ways, although careful feature selection is still necessary to keep errors low. This research provides a brief analysis of ECG, PPG and PCG and their advantages and limitations and proposed a ECG based Biometric Authentication using CNN (ECG-BA-CNN).

Algorithm ECG-BA-CNN

{

Input: ECG Signal Set {Eset}

Output: Authentication Process Status

Initially perform normalization of the ECG signals by loading them from the Eset. The values in the ECG dataset are analyzed and the mean and standard deviation operations are performed and then normalized to a balanced range for signal processing. The normalization is performed as

$$Nset[M] = \sum_{r=1}^{M} getattr(r) + mean\big(attr(r, r+1)\big) + \frac{std((r, r+1))}{len(Eset(r))} + \mu(attr(r)) \begin{cases} return\ mean(r, r+1) & if\ \mu(r) < Th \\ continue & Otherwise \end{cases}$$

Here getattr() is used to retrieve each and every ECG record from the dataset, mean() calculates the mean between the adjacent attributes and std() is applied to update the standard deviation value.μ considers the missing and unwanted and unfilled

Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

values in the dataset. Th is the threshold range for updating the dataset.

The features of the ECG are used to process and select the best features from the list to perform training of the model. The feature extraction and selection is performed as

$$Fextr[M] = \sum_{r=1}^{M} \frac{\max(attr(Nset(r))}{len(Nset)} + \lambda(Nset(r, r+1)) - \mu(r)$$

Here λ is the model for attribute feature extraction for all records. Unfilled and unwanted noisy values are removed from the dataset.

For feature extraction in a CNN, the kernel is only a filter. Input data is moved by a matrix called the kernel, which then executes a dot product with a sub-region of that data and obtains the result as another matrix. The process of CNN kernel based feature selection is performed as

$$K[M] = \prod_{r=1}^{M} \frac{\max(corr(r, r+1))}{len(Fextr)} + \frac{\omega(Fextr(r, r+1))}{\max(Fextr)} + \tau(r)$$

Here corr() model is used to calculates the correlation factor among the features and ω is used to detect the features of the threshold range and τ is the threshold limit of correlation factor.

Convolutional layers, pooling layers, fully-connected layers, and normalization layers are the typical components of a CNN's hidden layers. It simply implies that convolution and pooling functions are utilized as activation functions rather than the conventional activation functions. The hidden layer processing of ECG features are performed as

$$HL[M] = \sum_{i,j,r=1}^{M} \frac{We(r)}{len(K)} + \eta_i * \eta_j + \sum_{i,j} We_i * We_j + bias(r)$$

Here We is the weight allocated to a feature vector. η_i and η_j are vectorized features considered from the feature set.

The decision of whether or not to activate a neuron is made by an Activation Function. This implies that the network will use less complex mathematical procedures to determine the relevance of each neuron's input to the prediction process. The activation function is applied as

$$ActFunc[M] = \sum_{r=1}^{M} 1/(1 + e^{K(r)}) \begin{cases} 0 \text{ if } K(r) < Th \\ 1 \quad Otherwise \end{cases}$$

The biometric authentication model verifies the ECG signals that are trained with the testing ECG signal and the authentication process is performed to validate the user that is performed as

$$Tattr[M] = \sum_{r=1}^{N} getECG(r) \begin{cases} Fextr(r) \\ K(r) \\ ActFunc(r) \end{cases}$$

$$Auth[Eset] = \sum_{r=1}^{M} \frac{Tattr(r) + getMax(K(r)) + HL(r, r+1)}{len(HL)} + \max(We(r, r+1)) + attr(ActFunc(r)) \begin{cases} 1 \text{ if } simm(Tattr(r), Eset(r)) > Th \\ 0 \quad Otherwise \end{cases}$$

}

4. DISCUSSIONS

This article analyzes ECG, PPG, and EMG based biometrics for individual identification. To accomplish identification using biomedical waveform features, it is common practice to estimate how closely those features match a set of reference features. Examples of transformation domain identification solutions include the Fourier transform for ECG and EMG, the wavelet transform for PPG, and the Karhunen-Loève transform for PPG. This work provides a high-level overview of biometric systems based on cyclostationary signals, in which signal characteristics vary over time but follow a predictable pattern. The benefits, drawbacks, and difficulties of health-based biometrics are also investigated in this paper. This research provides a brief analysis of ECG, PPG and PCG and their advantages and limitations.

4.1 Electrocardiogram (ECG)

Many consumer electronics, from smartphones to wearables, are incorporating biometrics into their high-performance user identification systems. Fingerprint readers, iris scanners, and facial recognition software are replacing passwords as the primary means of biometric authentication. This information is vulnerable to outside interference, though, due to the transparent character of most biometric features. Nevertheless, electrocardiogram (ECG) signals are hard to forge as the subject's physical measurements are the only way to uncover the secret biometric characteristics used for authentication. Reason being, depending on the size and location of the heart, ECG signals display unique physiological characteristics in different individuals. Numerous efforts have been made to enhance the authentication performance of ECG-based biometric authentication using various methodologies in the decades since the initial research on ECG signal processing for biometric recognition. However, a person's ECG signals may change depending on his or her physical state or health condition, which might potentially lead to authentication failure.

Authentication systems that use a user name and password are vulnerable, but security biometrics provide a safe alternative. ECG signals, which consist of five waves, P, Q, R, S, and T, have recently been discovered to be completely individual. In fact, it outperforms other measures of biometrics by providing evidence of the subject's continued viability in addition to the standard biometric data. Human identification systems that rely on bioelectrical signals are a burgeoning field of study due to their many desirable characteristics. The aetrial contractions that occur as a result of electrical impulses originating from the Sino-atrial (SA) node of the heart and travelling to the Atrioventricular (AV) node. These impulses cause contractions in the ventricles, which are sent from the AV node located above the ventricles. These signals travel throughout the body. Electric potentials are the driving force behind surface electrode ECG recording. The components and characteristics of ECG signal is represented in Table 1.

Table 1: ECG Components and Characteristics

Component	Characteristics
Heart Rate	60 to 100 bpm
PR Interval	0.12 to 0.20 sec
QRS Interval	0.06 to 0.10 sec
QT Interval	Less than half of RR Interval
ST Interval	0.08 sec

The repolarization and depolarization of heart muscle fibers over the course of one ECG cycle is represented by the P-wave, QRS-complex, and T-wave. Since each person's ECG depends on their specific myocardium, it has been successfully used for human identification. It also has the four other characteristics universality, liveness detection, permanence, and difficulty to spoof that are required for biometric authentication. Fig. 4 is a schematic depiction of an electrocardiogram with all waves represented. The accuracy of biometrics can be improved by training the system on a large variety of data sets, as different health conditions have a noticeable effect on ECG signals. Furthermore, in times of peril and threat, the heart's natural defence mechanism is activated in response to the dynamic shift in the signal. These factors need to be taken into account and worked on in order to improve performance. Additionally, the system's accuracy is negatively impacted by the 12 lead ECG signal's vulnerability to interference.

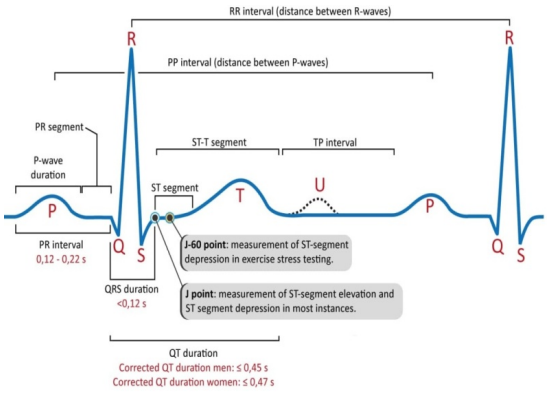

Fig 4: Analysis of ECG Signals

4.2 Photoplethysmography (PPG)

PPGs are common physiological signals utilized as biometric features. Since PPG signals may be obtained using just a light source and a light sensor, they find more widespread application than other physiological signals. Well-known wearable devices that track health, such as those made by Samsung and Apple, use PPG sensors. Consequently, compared to other physiological indications, PPG signals are better and more practical for usage in the real world. For the recognized concerns against PPG-based biometric authentication to exist, it is necessary to capture the victim's PPG signal. Because being physically close to the victim is required, the possibility of an attack is reduced. Since the signals are already being received and processed for other reasons, PPG-based biometric systems can be used in many different domains, such as health monitoring and fitness tracking. For PPG-based biometric systems, PPG signals can be collected from a wide variety of heterogeneous sensors, including medical equipment, wearables, telephones, digital cameras, and more.

Normally, PPG signals are received via sensors that come into touch with the skin's surface. These sensors measure the blood's infrared absorption and reflectance rates. Variations in blood vessel volume are reflected in the recorded signals throughout the cardiac cycle. Two main categories of PPG sensors exist based on the technology they use: those that detect light transmission and those that detect light reflection. To determine how much light has passed through an absorbent material like skin, bone, arterial blood, or venous blood, the first category of sensors use a detector in conjunction with filters and converters. The second kind of sensor counts

the amount of light that a detector picks up after it reflects off the skin. A sensor that relies on light reflection may thus detect a wide variety of body components. An analysis of the results using computational intelligence approaches indicates that recent biometrics based on PPG have demonstrated good performance in various contexts. However, PPG-based biometric systems are still nascent technologies, and many issues must be resolved before such systems can be considered reliable and accurate. The relative amount of blood in the skin can be measured with PPG, a noninvasive method. The PPG signal analysis is shown in Figure 5.

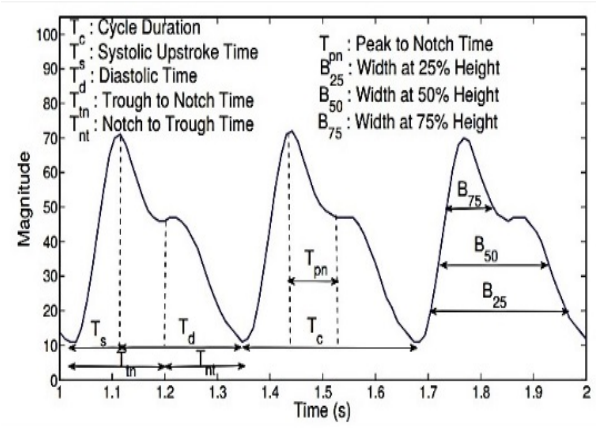

Fig 5: PPG Signal Analysis

PPG signals work on the basis of the skin's reflectance. Hemoglobin's light-absorbing properties mean that the skin's apparent brightness shifts in response to changes in blood volume induced by each heartbeat. The PPG signal is a luminance-based indicator of blood flow. PPG may monitor heart rate in any area of the body that can transmit light, including the earlobes, fingertips, and wrists, but an ECG requires two or three sensors to be put around the heart. The pulse can be determined without the need for an ECG by merely observing the variations in light intensity reflected back from the body. There are essentially two halves to a PPG waveform. The anacrotic phase refers to the initial crest that arises during the systolic rise, while the catacrotic phase describes the initial crest that appears during the diastolic decline.

3.3 Electromyogram (EMG)

The use of EMG signals in biometrics research has lagged behind those of ECG and EEG. A problem of EEG signal measurement is that it is distorted as it travels through the skull, while a drawback of ECG signal measurement is that it is a periodic signal, meaning that the waveform of the signal cannot be altered if the registered data is hacked. The EMG signal is simpler to measure than the EEG signal, and its registration data can be altered in a way that is not shared with other gestures with a characteristic indicating a unique waveform of the signal for each action. In previous efforts, EMG signals have been applied to the recognition of gestures or as standalone biometrics.

Depending on its intended application, the recorded EMG signal must be preprocessed to remove noise and remove information about things like muscle movement and muscle exhaustion. Muscle contraction data is located in the sub-500-hertz range. A band-pass filter or a low-pass filter is required for usage with this data, and a notch filter set at 50Hz is employed to eliminate interference from the power supply. Figure 6 displays the waveform of the raw and filtered EMG signals.

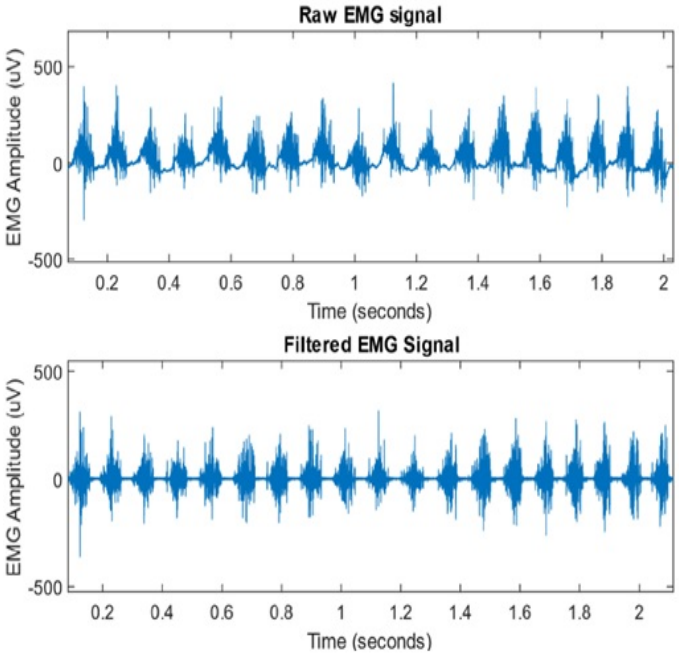

Fig 6: EMG Signal Analysis

A good way to do biometric identification and prevent the spoofing attacks is to use a biometric containing living body properties, like an EMG signal. A personal recognition system can function as an identifying system or a verification system,

depending on the needs of the application. When set to personal identification, the system will attempt to match the user's template against all of the others in the database. In the personal verification mode, the system checks the collected characteristics against the user's own templates in the database to ensure the user's identification. Muscle contraction produces an electrical signal called EMG. In scoliosis patients, for instance, muscle activity can be evaluated using EMG using surface electrodes positioned at various levels of the back. Having more electrodes located farther from the heart increases the likelihood of ECG interference from EMG. Since both the ECG and EMG signals are obtained at the same time, isolating them is crucial. Muscle action potentials are recorded using EMG.

The ECG and EMG amplitude and bandwidth levels are represented in Table 2.

Table 2: ECG and EMG Amplitude and Bandwidth Levels

Signal	Amplitude (mV)	Bandwidth(Hz)
ECG	1 to 5	0.05 to 100
EMG	1 to 10	20 to 2000

The useful parameters and individual model drawbacks are represented in Table 3.

Table 3: Biometric Model Overview

Signal	**Advantages**	**Drawbacks**
ECG	The three primary parameters of clinical importance that ECG may measure are heart rhythm and rate, cardiac axis, and myocardial muscle health. Topographic data representation is used in ECG, which results in more useful diagnostic information. ECG's early analysis of cardiac parameters aids in the prevention of heart attacks. After a patient has had anaesthesia for surgery or another procedure, an ECG can be used to diagnose their heart's health. The ECG test takes little time, causes no discomfort, and is completely risk-free. The cost of an ECG test is minimal. It is Non-invasive	Only during the brief time an ECG is recorded and the heart rate and rhythm can be determined. Ambulatory monitoring may be necessary if the abnormal heartbeat is too brief for an electrocardiogram to detect. In patients with no outward signs of cardiac trouble, it does not reveal any underlying issues. It does not always aid in accurate diagnosis. Serious heart abnormalities may be undetected by a normal ECG curve and require additional testing to pinpoint. The heart issues will be considered as main issue in ECG based biometric failures.
EMG	EMG is a diagnostic tool used to evaluate the condition of muscles and the motor neurons that govern them. In addition to revealing nerve and muscle dysfunction, EMG data can also identify difficulties with nerve-to-muscle transmission of	Only the most superficial muscles are targeted. No standardized method of electrode insertion; may alter subject's motor habits. It is possible that the area of detection does not accurately reflect the complete muscle. Challenges in

	signals. Surface electrodes for EMG sensors can be applied in a flash. There is no requirement for certification or medical supervision. It causes very little discomfort. The EMG sensor's fine wire electrodes capture the activity of individual muscles. It allows to reach deep muscle tissue. It's a very delicate situation. EMG readings are quantitative and continuous. Muscle bottlenecks can be found with multi-channel EMG. Muscle weariness can be detected in its earliest stages with the help of EMG data.	monitoring active muscular tissue.
PPG	Direct current and alternating current are used to depict the PPG waveform. Tissue-based signals are picked up by	It is not capable of measuring BP. The heart rate need to be determined from an external ECG signal.
	DC, while blood volume changes are detected by AC. It's cheap, straightforward, and trustworthy. The usage of PPG based wearable devices does not necessitate any particular training or instruction, and it may be simply integrated with healthcare equipment for various health related metrics like pulse rate, blood flow, Heart Rate Variability, etc.	It takes the PPG sensor a lot longer to settle down than the ECG sensor does. It uses more energy while running 30 mW than an electrocardiogram 2.5 mW. For precise timing regulation, an external crystal oscillator is needed. Due to the high power consumption of LEDs, the maximum feasible sampling rate places a cap on peak interval precision. HRV (Heart Rate Variability) calls for more extensive monitoring (often > 5 minutes). It can only be used to get an average heart rate. An ECG sensor provides precise readings of heart rate.

5. RESULTS AND DISCUSSIONS

The proposed analysis considers three models that are using ECG, EMG and PPG signals for biometric authentication. The considered models are PlexNet: A fast and robust ECG biometric system for human recognition [12], EMG Biometric Systems Based on Different Wrist-Hand Movements [13] and Evaluation of the Time Stability and Uniqueness in PPG based Biometric System [14].

ECG Model Analysis [12]

For almost 20 years, scientists have investigated the feasibility of using ECGs as biometrics. When it comes to protecting biometric systems against fraudulent attacks, ECG's inherent attribute of liveliness is invaluable. For ECG biometric detection, this model proposes a novel ensemble of the state-of-the-art pre-trained deep neural networks, namely ResNet and DenseNet. Models are fine-tuned using the transfer learning principle. 'PlexNet' is a stacking model that combines the information from four different models that have been fine-tuned to work together [12]. PlexNet is a novel model for ECG biometrics that is more secure and robust than previous methods based on deep networks by leveraging transfer learning and ensemble learning. The suggested ensemble is evaluated using the public datasets PTB and CYBHI for human identification.

Using the most recent advancements in deep neural networks for ECG biometrics, this research presents an ensemble of fine-tuned architectures called PlexNet. In contrast to other ECG biometrics methods, the notion of transfer learning is utilised by the suggested ensemble of deep networks, i.e., PlexNet. By combining transfer learning with ensemble learning, the PlexNet creates a unique framework that is more reliable than previous CNN-based ECG biometrics approaches. As can be seen in Fig. 7, PlexNet's architecture consists of four distinct phases: preprocessing the ECG data, converting the 1D signal to 2D pictures, training the ensemble, and finally testing the model. The first step involves preprocessing the raw ECG data by removing noise and segmenting heartbeats. The next step is to create 2D images from the ECG signals. In ensemble learning, each fine-tuned mode receives an input image.

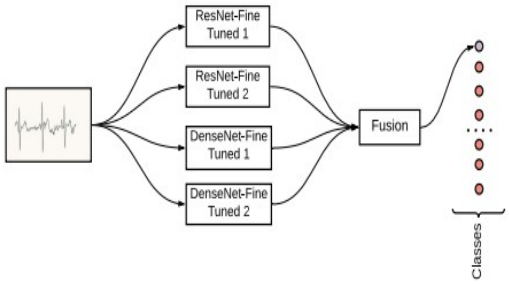

Fig 7: Structure Of Plexnet With Fine-Tuned Models [12]

In many computer vision tasks, utilising an ensemble of learning methods has been shown to significantly increase classification accuracy. Avoiding underfitting of learned data is what gives it such great performance. By combining the search space, an ensemble of algorithms can more closely approximative the ideal result. An ensemble of pretrained networks is offered as a means to boost the performance of the ECG biometric system without resorting to underfitting. The system combines the excellent characteristics from two cutting-edge CNN architectures trained with different starting values. After trying out different pre-trained architectures on ImageNet, we settle on the residual network (ResNet) and the dense convolutional network (DenseNet). Two pre-trained ImageNet architectures are used in the proposed ensemble model. In addition, there is a complementary relationship between the two structures. PlexNet is a four-network-path design that incorporates the training and tuning weights of several networks. Since the ImageNet dataset is built on millions of images, the pre-trained architectures pick up a wide variety of visual cues. The ECG dataset is utilised to train these designs' weights, taking advantage of prior knowledge.

The majority of ECG biometric research use one of three common approaches to collecting ECG data: on-the-person, in-the-person, or remotely. In-person ECG data gathering is an invasive procedure infrequently utilized in medical diagnostics. The next step is to record an ECG directly from the patient by attaching electrodes to their skin using conductive gel, as in a regular 12-lead ECG. Finally, the off-the-body way of acquiring ECG data employs noninvasive means, such as tapping electrodes on fingers or palm with minimum skin contact or employing wireless means, such as a laser vibrometory that collects ECG from a distance of 200 metres. The current trend in research is away-from-person ECG datasets, which can be more convenient for users but have significant quality issues. Another important issue is the lack of publicly available benchmark datasets for ECG biometrics. Most ECG biometric algorithms are validated using Physionet's ECG datasets, which were collected for scientific purposes.

Although a public dataset has been produced for biometric research employing off-the-person setup a few of years ago, Check Your Biosignals Here Initiative (CYBHI). The ECG signals in this dataset have lower signal-to-noise ratios (SNRs), meaning that there is significantly more noise influence, thus diminishing the performance of ECG biometric detection. Therefore, it is necessary to create a reliable strategy for enhancing recognition performance for multi-session ECG data collected remotely. Using the CYBHI dataset and the ECG dataset from Physionet, we were able to verify the

efficacy of our PlexNet model, an ensemble proposed for ECG biometric identification.

Based on their recognition ability as reported using the CYBHI dataset, ResNet and DenseNet architecture are chosen as the basis for PlexNet's base models. Table 4 displays the results of deep learning architectures on PTB and CYBHI datasets with varying training/test splits. At a training and testing ratio of 80:20, DenseNet and ResNet are said to have the highest accuracies, with 97.63% and 97.3%, respectively. These two architectures are chosen for PlexNet because they compliment each other and produce superior accuracy results. Furthermore, the accuracy of these designs is verified on two alternative 80:20 and 90:10 ratios of training and test datasets. This partitioning of the dataset is used for the biometric experiment.

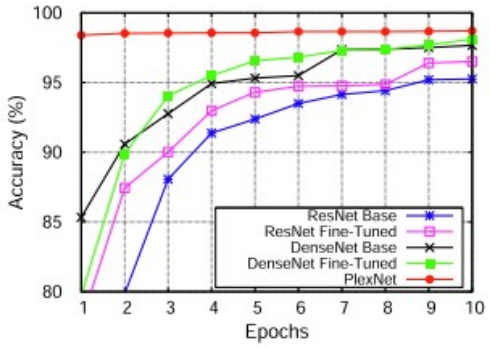

Fig 8: Testing Accuracies For Different Architectures Of Plexnet On Mixed Dataset.

At 1, 2, 5, 8, and 10 epochs, the reported testing accuracies for ResNet's base architecture are 78.73%, 79.87%, 92.38%, 94.42%, and 95.26%, respectively. With ResNet's fine-tuned architecture, these accuracies are further enhanced; for 1, 2, 5, 8, and 10 epochs, they are, respectively, 85.33 percent, 90.59 percent, 95.32 percent, 97.39 percent, and 97.67 percent. DenseNet compatible architectures are similarly fine-tuned using the basic architecture's learning. The testing accuracies for DenseNet base are 77%, 79%, 87%, 44%, 94%, and 96%, respectively, throughout epochs 1, 2, 5, 8, and 10. Utilising this knowledge in a DenseNet-tuned model yields testing accuracies of 79.73 percent, 89.9 percent, 96.5 percent, 97.3 percent, and 98.11 percent after 1, 2, 5, 8, and 10 iterations, respectively.

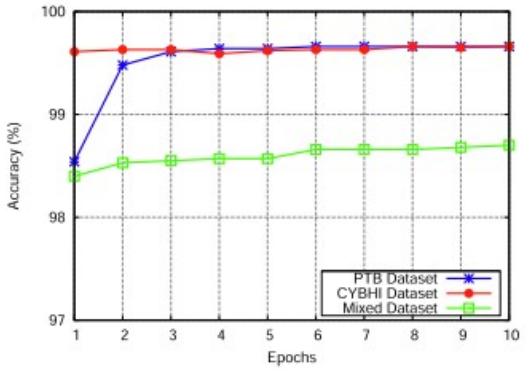

Fig 9: Testing Accuracies Of Plexnet On Different Datasets

The Precision, recall and F1-score reported by PlexNet on different datasets is represented in Table 1.

Table 4: Evaluation Metrics

Dataset	Precision	Recall	F1-Score
PTB	99.6	99.5	99.6
CYBHI	99.7	99.7	99.7
Mixed	99.5	99.4	99.5

The testing results validate the efficacy of the model, with the best reported identification accuracy of 99.66% on both healthy and ill people. When considering signal collecting techniques, dataset sizes, and subjects' health conditions, the suggested ECG biometric method is shown to be highly resilient.

EMG Model Analysis [13]

Human attempts to interact with and manage equipment like robots, prostheses, or virtual worlds are elevating the relevance of EMG acquisition and analysis [13]. In some circumstances, only authorized users should have access to such features. To the best of the authors' knowledge, no prior art exists that can identify persons from a wide range of wrist-hand motions EMG readings within the wearable device, making the security of EMG-based control a major outstanding concern for these applications. This model seeks to solve such issue. Methods are discussed that can be utilised to validate users using EMG as a biometric. Users can prove their membership in a trusted network without revealing their identities by wearing an EMG-sensing wristband on their lower arms.

By using a mapping function, feature projection lowers the dimensionality of the feature vectors to a lower-dimensional space. Since every user is

separated into two groups authenticated and non authenticated linear mapping is the best option for our system. As a result of their superior accuracy at separating classes into two groups based on little data, linear models are widely favoured for use in binary data. A feature categorization method is then used to the predicted features. Area under the operating characteristic curve (AUC) measures for various classifiers are used to evaluate how well they can distinguish between classes.

The EMG amplitudes for various wrist-hand movements show that everyone has variable muscular strength. Since the amplitude of an EMG signal varies from muscle to muscle and from movement to movement, amplitude normalisation uses this variation to determine an individual's "typical" amplitude. The power involved at that time is represented by the average amplitude.

Each 256-sample window is amplitude adjusted and converted into an RSS feature vector for training. Twenty sessions from the first week (1280 windows per session from eight motions) are used for training, along with ten sessions from the Raurale datset (240 windows per session) and three sessions from the Angeles datset (112 windows per session). The multi-session dataset yields a total of 25600 feature vectors per subject, the Raurale dataset yields 2400 feature vectors per subject, and the Angeles dataset yields 336 feature vectors per subject.

The effectiveness of continuous identification is evaluated for re-identification intervals of 1024, 2048, and 3072 samples. Table 5 details the continuous re-identification accuracy for all 10 users over all nine wrist-hand movements based on this setup. Re-identification accuracy ranges from 90% for a 1024 sample interval to over 91% for a gap of 2048 or 3072 samples. With a majority voting configuration of 5 samples, the best re-identification accuracy is attained at a 3072-sample interval, or 92.08%.

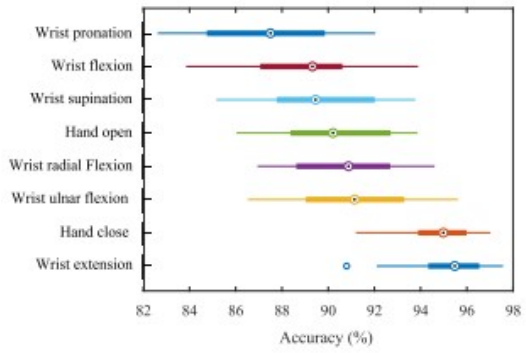

Fig 10: Identification accuracy across different movements

The One-time identification performance for different system configurations are represented in Table 5.

Table 5: Evaluation Metrics

Configuration	Accuracy	Precision	Recal	F1-
Single Window	91	63	90	74
Majority Voting	91	65	91	76

The On-going identification accuracy for different system configurations are indicated in Table 6.

Table 6: On-going identification accuracy for different system configurations.

System Configuration	Time Frame (k)		
	1024	2048	3072
Single Window	91	92	92
Majority Voting	91	92	92

The Biometric verification performance in different system modes are depicted in Figure 11.

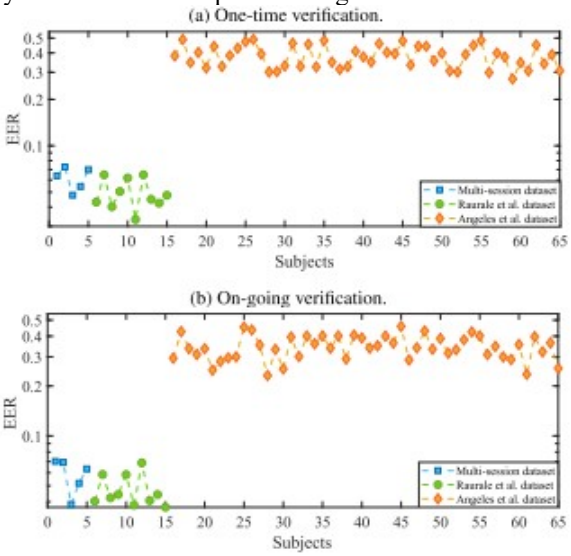

Fig 11: Biometric verification performance in different system modes.

Up to 93% accuracy is reached for verification, and 92% accuracy is reached for identification. It is also demonstrated that the system runs in real-time on an ARM Cortex A-53 embedded CPU compact enough to be housed in an EMG wearable device, with verification and identification latencies of 1.06 ms and 1.61 ms, respectively. These parameters are more than adequate for usage in portable, battery-operated EMG authentication devices in real-time.

PPG Model Analysis [14]

In the study [14], the author showed that the biometric PPG signal may be successfully implemented in human authentication scenarios. For many purposes, including user access control, the PPG signal is preferable due to its accessibility and portability. To improve the verification system's durability and performance with the PPG signal, the author build a robust time-stable characteristics by signal analysis and deep learning models. In order to make advantage of several deep learning models, the suggested system combines at the data level many stretching algorithms, including Dynamic Time Warping, zero padding, and interpolation with the Fourier transform. In order to construct a user-specific model for the verification task, the designers of the deep models used here primarily focus on Convolutional Neural Networks (CNNs) and Long-Short Term Memories (LSTMs). Using the Plux pulse sensor, we gathered data from a sample of 100 people across two separate recording sessions. This dataset, together with two more public databases, is used to gauge the accuracy and consistency of the proposed verification method.

Signals from a Plux pulse sensor were used to compile the first dataset, titled BioSec. PPG Dataset 1 (Biosec1). During signal collection, a constant sample rate of 100 Hz was used. This dataset includes 31 people, all of whom had their PPG signals collected over the course of at least two sessions separated by at least 14 days. The signals were recorded while the sensor was resting on the participant's fingertip throughout a three-minute period. The second dataset, Biosec. PPG Dataset 2 (Biosec2), was also collected from the Biosec. Lab at the University of Toronto. This work's database is an expanded and improved version of an earlier database that was gathered using a different method of data collecting. The sensor, sample rate, and health and safety parameters in the environment were all held constant. Finally, this work examines the PRRB database, which contains information gathered during elective surgery and normal anaesthesia. There is only one session of data included, which records the PPG signal for 8 minutes while the subject breathes naturally or under control. This work's primary purpose is user authentication, so an 8-minute recording would be unreasonable. As a result, the author only analyzed the first three minutes of each subject's PPG signal. The sample rate was maintained at 300 Hz among 42 individuals (29 children and 13 adults).

In this study, the author used two distinct forms of data augmentation. In the first form, the author thought about normalising the single pulse before incorporating the noise. Since the DTW input was already normalised, there is no effect from the normalisation. The input data takes on distinctive forms depending on whether it is ZT or IN normalised. The simulated data is meant to verify this suggested verification mechanism using many data sources. In each segment of the experimental outcomes, six unique scenarios were tested. No CNN augmentation, No CNN and LSTM augmentation, Three versions of CNN augmentation, four of CNN and LSTM augmentation, five of CNN augmentation, and six of CNN and LSTM augmentation for version 2. TensorFlow 1.14.0 was used on Nvidia Tesla T4 for entire training. The author examined the average of accuracy (ACC), the error rate (EER), the time to execute, and the receiver operating characteristic (ROC) curve as performance metrics. Accurate predictions as a percentage of total inputs makes up the ACC. The ACC does not accurately reflect the efficiency of the verification system.

The results of the subjects' accuracy using the various input data are depicted in Fig. 12. Using the CNN model, we calculate the results using the data from both sessions of Biosec2. It's obvious that various people have varying preferences for input data, thus it makes sense to use the selection approach to boost the system's performance as a whole.

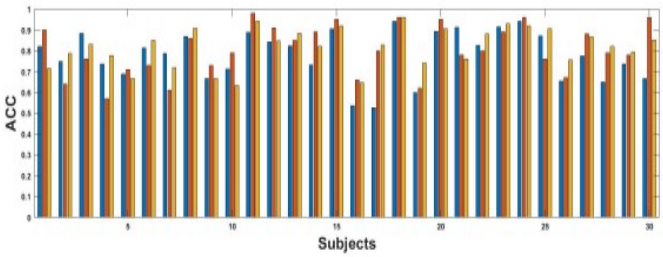

Fig. 12: Performance Of Input Data For Different Subjects

ROC curves for combination, 2 channel, and 1 channel inputs to Biosec1 are shown on Fig. 13. Biosec1's PPG signals from two sessions show that the combined input provides the best overall

performance, as measured by the least area under the curve (AUC), regardless of the model used. Therefore, it is safe to say that the selection procedure has universal applicability in Biosec1.

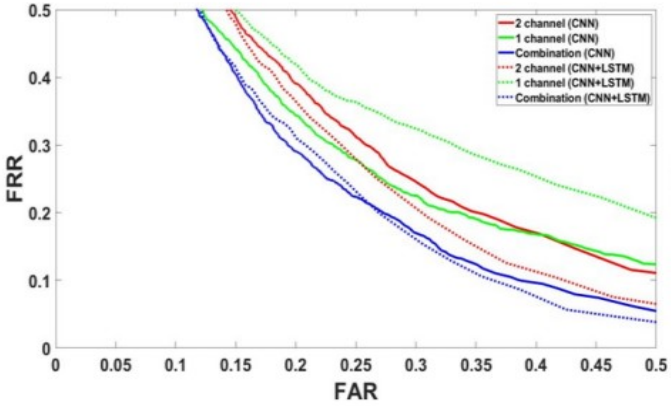

Fig 13: Average ROC curves with selection method in Biosec1.

The average ROC curve for combination, 2 channel, and 1 channel input in Biosec2 is shown in Fig. 14. Combination input data performs better than (2 or 3 times as well as) 2 channel and 1 channel input in both the CNN and CNN with LSTM models for two-sessions of PPG data in Biosec2. Since Biosec2's training data is more diversified thanks to detecting the signal three times during sensor relocation, it is able to achieve greater performance in 2 channel and 1 channel input compared to Biosec1's selection technique. Therefore, the scope for further development is narrower, but the selection approach is still useful for completing the refinement in Biosec2.

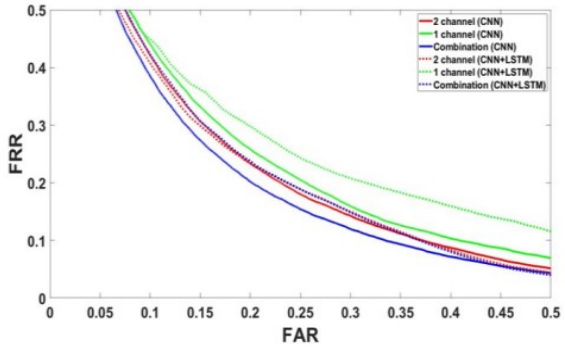

Fig 14: Average ROC curves with selection method in Biosec2.

Table 7: Evaluation Metrics

Model	Biosec1	Biosec2
CNN	97	95
CNN+LSTM	99	97
Aug V1,CNN	97	95
Aug V1,CNN+ LSTM	98	97

The end result shows that our suggested solution is superior to two other public databases when evaluated on our custom-built dataset. Our greatest single-session performance (98%) and best two-session performance (87.1%) both come from our gathered two-sessions database.

The final comparison results of the ECG, EMG and PPG models in terms of Time complexity and computational complexity levels and user authentication accuracy levels are shown in Figure 15, Figure 16, Figure 17 and Figure 18.

The models considered in the analysis and based on the working of the models, the time complexity levels of the ECG, EMG and PPG are shown in Table 8 and Figure 15.

Table 8: Time Complexity Levels

Subjects Considered	Signals Considered			
	ECG-[illegible]	ECG	EMG	PPG
100	10	12.1	14.2	19.2
200	10.2	12.3	14.5	19.5
300	10.4	12.5	15	19.7
400	10.7	12.7	17	20
500	10.8	12.8	18	21
600	11	13	19	22

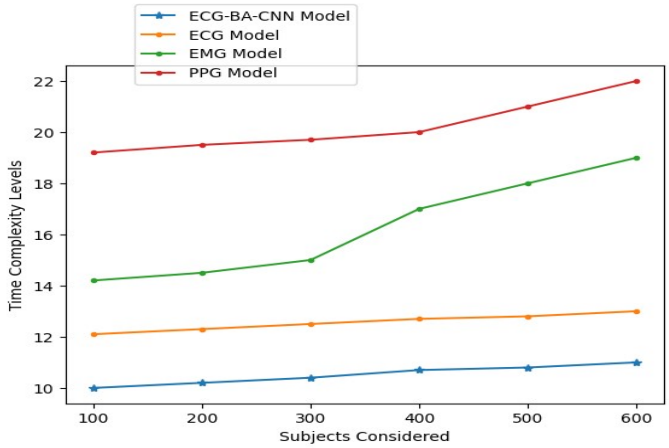

Fig 15: Time Complexity Levels

Computational complexity levels represent the latency of the model in user identification. The computational complexity levels of any model must be minimum for better performance. The computational complexity levels of the 3 models are represented in Table 9 and Figure 16.

Table 9: Computational Complexity Levels

Subjects Considered	Signals Considered			
	ECG-[illegible]	ECG	EMG	PPG
100	14.8	15.7	25	21.5
200	14.9	16	25.3	21.7
300	15	16.5	25.4	22
400	15.2	17	25.6	22.3
500	15.5	17.5	25.7	22.6
600	16	18	26	23

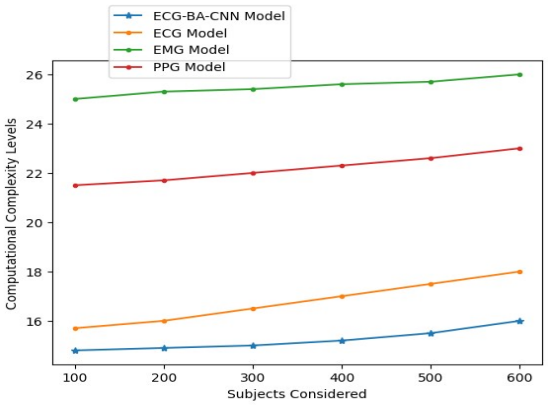

Fig 16: Computational Complexity Levels

Based on the signals considered, the users authentication will be performed. Attackers play different techniques to fake the model. The User Authentication Time Levels and the accuracy levels of the 3 models considered are depicted in Table 10, Table 11 and Figure 17 and Figure 18.

Table 10: User Authentication Time Levels

Subjects Considered	Signals Considered			
	ECG-[illegible]	ECG	EMG	PPG
100	8	8.8	12.3	15
200	8.3	8.9	12.6	15.3
300	8.5	9	13	15.8
400	8.7	9.2	13.2	16.4
500	8.9	9.4	13.5	17
600	9	9.5	14	18

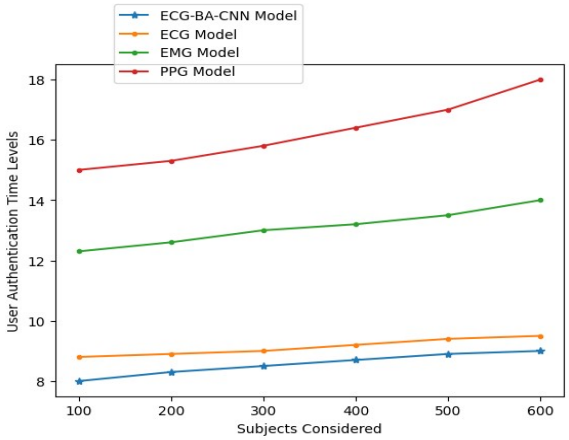

Fig 17: User Authentication Time Levels

Table 11: User Authentication Accuracy Levels

Subjects Considered	Signals Considered			
	ECG-[illegible]	ECG	EMG	PPG
100	99.2	98.9	94.2	92
200	99.4	99	94.3	92.1
300	99.4	99.1	94.5	92.3
400	99.5	99.2	94.7	92.5
500	99.6	99.4	94.8	92.6
600	99.7	99.5	95	93

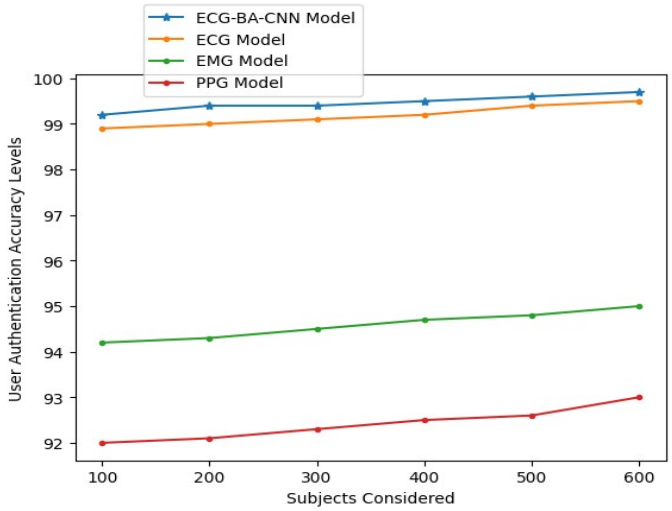

Fig 18: User Authentication Accuracy Levels

6. CONCLUSION

The purpose of this research was to evaluate biosignal-based biometric systems including EMG,

PPG and ECG. Subject age, gender, database size, and the impact of diseases on biometric performance are all factors that can reduce the accuracy of any biometric system. There are studies being done to incorporate a more potent characteristic that is less vulnerable to these elements. The recognition rate can be boosted with the help of deep learning techniques, alternative classifiers, and multimodal biometrics that combine two or more biosignals. According to studies, the existing ECG database is undersized, loud, and might include anomalies. Additionally, when comparing the data sets of healthy participants with those with abnormalities, the recognition rate is lower in the former. This is because a distorted QRS complex is a hallmark of heart disease. When it comes to safety concerns, this is an issue with ECG. The use of surrounding noises and sounds generated by internal organs is likely to be incorporated into the analysis, as PPG biometrics depends on heart sounds. The inability to muffle these sounds makes data collection a pain and has a major impact on the recognition rate. As a result, PCG is less useful as a biometric instrument. In comparison to these signals, PPG offers a few benefits and can be easily measured using inexpensive sensors. Since electrodes and gel are not required for skin placement of the sensors, this technique is considered non-invasive. Not to mention that even a low degree of accuracy is required for the authentication of PPG data due to its many distinct characteristics. The device's portability and low power consumption make it a convenient and cost-effective acquisition sensor. EMG sensor is used to describe the device that records electromyograms. Muscle contraction and resting electrical activity are both measured by EMG. Muscle electrical activity is filtered and rectified by this sensor. An EMG sensor is typically one that has a tunable gain, a compact design, and full integrability. There is a correlation between the total number of motor units within a muscle and the force with which it contracts. EMG captured during a muscle contraction appears as a series of brief, spike-like signs. The duration of the burst is programmed to match that of the muscle contraction exactly. There is a direct correlation between the amount of electrical activity in the muscle and the intensity of the resulting contraction in striated muscles. This research proposed an ECG based Biometric Authentication using CNN. Based on the advantages and limitations of the models analyzed in this research proposed ECG model is preferable for the biometric in consideration of acquisition, processing, analysis, cost and security. This research helps numerous researchers to design innovative biometric authentication models using ECG signals for enhancing the security levels of organizations.

REFERENCES

[1] L. Sun, Z. Zhong, Z. Qu and N. Xiong, "PerAE: An Effective Personalized AutoEncoder for ECG-Based Biometric in Augmented Reality System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 6, pp. 2435-2446, June 2022, doi: 10.1109/JBHI.2022.3145999.

[2] D. Jyotishi and S. Dandapat, "An ECG Biometric System Using Hierarchical LSTM With Attention Mechanism," in IEEE Sensors Journal, vol. 22, no. 6, pp. 6052-6061, 15 March15, 2022, doi: 10.1109/JSEN.2021.3139135.

[3] R. Cordeiro, D. Gajaria, A. Limaye, T. Adegbija, N. Karimian and F. Tehranipoor, "ECG-Based Authentication Using Timing-Aware Domain-Specific Architecture," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3373-3384, Nov. 2020, doi: 10.1109/TCAD.2020.3012169.

[4] S. S. Abdeldayem and T. Bourlai, "A Novel Approach for ECG-Based Human Identification Using Spectral Correlation and Deep Learning," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 1, pp. 1-14, Jan. 2020, doi: 10.1109/TBIOM.2019.2947434.

[5] L. Pu, P. J. Chacon, H. -C. Wu and J. -W. Choi, "Novel Robust Photoplethysmogram-Based Authentication," in IEEE Sensors Journal, vol. 22, no. 5, pp. 4675-4686, 1 March1, 2022, doi: 10.1109/JSEN.2022.3146291.

[6] B. L. Ortiz, J. W. Chong, V. Gupta, M. Shoushan, K. Jung and T. Dallas, "A Biometric Authentication Technique Using Smartphone Fingertip Photoplethysmography Signals," in IEEE Sensors Journal, vol. 22, no. 14, pp. 14237-14249, 15 July15, 2022, doi: 10.1109/JSEN.2022.3176248.

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

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

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

[10] S. K. Behera, P. Kumar, D. P. Dogra and P. P. Roy, "A Robust Biometric Authentication System for Handheld Electronic Devices by Intelligently Combining 3D Finger Motions and Cerebral Responses," in IEEE Transactions on Consumer Electronics, vol. 67, no. 1, pp. 58-67, Feb. 2021, doi: 10.1109/TCE.2021.3055419.

[11] Pradhan, J. He and N. Jiang, "Performance Optimization of Surface Electromyography Based Biometric Sensing System for Both Verification and Identification," in IEEE Sensors Journal, vol. 21, no. 19, pp. 21718-21729, 1 Oct.1, 2021, doi: 10.1109/JSEN.2021.3079428.

[12] Ranjeet Srivastva, Ashutosh Singh, Yogendra Narain Singh, PlexNet: A fast and robust ECG biometric system for human recognition, Information Sciences, Volume 558, 2021, Pages 208-228, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2021.01.001..

[13] V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[14] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[15] L Narayana, V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2023). Optimized Nature-Inspired Computing Algorithms for Lung Disorder Detection. In: Raza, K. (eds) Nature-Inspired Intelligent Computing Techniques in Bioinformatics. Studies in Computational Intelligence, vol 1066. Springer, Singapore. https://doi.org/10.1007/978-981-19-6379-7_6.

[16] Khan, M.U.; Choudry, Z.A.; Aziz, S.; Naqvi, S.Z.H.; Aymin, A.; Imtiaz, M.A. 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. Cooperative sensing and wearable computing for sequential hand gesture recognition. *IEEE Sens. J.* **2019**, *19*, 5575–5583.

[18] Oh, D.C.; Jo, Y.U. 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. Surface EMG hand gesture recognition system based on PCA and GRNN. *Neural Comput. Appl.* **2020**, *32*, 6343–6351.

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

[21] H. Wang et al., "Joint Biological ID : A Secure and Efficient Lightweight Biometric Authentication Scheme," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2578-2592, 1 May-June 2023, doi: 10.1109/TDSC.2022.3186999.

[22] W. Yan, J. Tang and S. Stucki, "Design and Implementation of a Lightweight Deep CNN-Based Plant Biometric Authentication System," in IEEE Access, vol. 11, pp. 79984-79993, 2023, doi: 10.1109/ACCESS.2023.3296801.

[23] Y. Wu et al., "Attacks and Countermeasures on Privacy-Preserving Biometric Authentication Schemes," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1744-1755, 1 March-April 2023, doi: 10.1109/TDSC.2022.3162623.

[24] S. Zhang, Z. Yan, W. Liang, K. -C. Li and C. Dobre, "BAKA: Biometric Authentication and Key Agreement Scheme Based on Fuzzy Extractor for Wireless Body Area Networks," in IEEE Internet of Things Journal, vol. 11,

no. 3, pp. 5118-5128, 1 Feb.1, 2024, doi: 10.1109/JIOT.2023.3302620.
[25] Y. Zhang, Y. Huang, L. Wang, and S. Yu, "A comprehensive study on gait biometrics using a joint CNN-based method," Pattern Recognition, vol. 93, pp. 228-236, 2019.
[26] F. Caldwell, "Voice biometrics systems and methods," ed: Google Patents, 2019.
[27] S. Ismail, I. Siddiqi, and U. Akram, "Localization and classification of heart beats in phonocardiography signals—a comprehensive review," EURASIP Journal on Advances in Signal Processing, vol. 2018, no. 1, pp. 1-27, 2018.
[28] H. Aghili, "Bioelectrical Signals: A Novel Approach Towards Human Authentication," in Fundamental Research in Electrical Engineering: Springer, pp. 3-13, 2019.
[29] S. A. El_Rahman, "Biometric human recognition system based on ECG," Multimedia Tools and Applications, vol. 78, no. 13, pp. 17555-17572, 2019.
[30] L. Ivanciu, I.-A. Ivanciu, P. Farago, and S. Hintea, "An ECGBased Authentication Scheme for Body Area Networks," in 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME): IEEE, pp. 114-117, 2019.
[31] X. Cheng, P. Wang, and C. She, "Biometric Identification Method for Heart Sound Based on Multimodal Multiscale Dispersion Entropy," Entropy, vol. 22, no. 2, p. 238, 2020.
[32] M. U. Khan, S. Aziz, A. Zainab, H. Tanveer, K. Iqtidar, and A. Waseem, "Biometric system using PCG signal analysis: a new method of person identification," in 2020 international conference on electrical, communication, and computer engineering (icecce): IEEE, pp. 1-6, 2020.
[33] J. Sancho, Á. Alesanco, and J. García, "Biometric authentication using the PPG: a long-term feasibility study," Sensors, vol. 18, no. 5, p. 1525, 2018.
[34] S.-W. Lee, D.-K. Woo, Y.-K. Son, and P.-S. Mah, "Wearable Bio-Signal (PPG)-Based Personal Authentication Method Using Random Forest and Period Setting Considering the Feature of PPG Signals," JCP, vol. 14, no. 4, pp. 283-294, 2019.
[35] D. Biswas et al., "CorNET: Deep learning framework for PPGbased heart rate estimation and biometric identification in ambulant environment," IEEE transactions on biomedical circuits and systems, vol. 13, no. 2, pp. 282-291, 2019.
[36] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics," 2020.
[37] A.I. Siam, A. Abou Elazm, N. A. El-Bahnasawy, G. M. El Banby, and F. E. Abd El-Samie, "PPG-based human identification using Mel-frequency cepstral coefficients and neural networks," Multimedia Tools and Applications, pp. 1-19, 2021.
[38] J. Yang, Y. Huang, R. Zhang, F. Huang, Q.Meng, and S. Feng, "Study on PPG Biometric Recognition Based on Multifeature Extraction and Naive Bayes Classifier," Scientific Programming, vol. 2021, 2021.