ECG biometric authentication: A comparative analysis

K. Haripriya[1], M. Akshitha[2], B. Sangeetha[3], N. Rajeswari[4]

[1,2,3]Research Scholar, Vignan Institute of Management and Technology for Women, Kondapur, Ghatkesar, Medchal -50130.

[4]Assistant Professor, Vignan Institute of Management and Technology for Women, Kondapur, Ghatkesar, Medchal -50130.

ABSTRACT

The primary goal of this research is to use ECG signals to authenticate the user. An electric indication of heart activity known as An electrocardiogram (ECG) has very strong human recognition capabilities. Despite the recent success of ECG-based authentication, successful pattern classification and discriminant feature extraction still confront a number of challenges. There is an urgent need to secure the equipment's integrity and the sensitive data, making authentication methods necessary. Passwords allowed for controlling crucial data, but they also exposed their weaknesses. We provide a method of authentication called "ECG Biometric Authentication" that can successfully grant access to the user The main elements of this authentication are filtering type, segmentation, feature extraction, and ECG health condition.

Keywords: ECG Biometric, Authentication.

I. INTRODUCTION

The biometric community has taken a keen interest in this alleged facial vulnerability, and numerous papers on countermeasure investigations have been published. The aforementioned picture print and video replay assaults are the main focus of research activity in this field, primarily due to their ease of use and inexpensive cost. The three main categories of existing anti-spoofing defenses against these types of attacks are liveness detection, motion analysis, and texture analysis.

Many anti-spoofing solutions look at the texture of the acquired facial image, presuming the presence of indications such as printing artifacts [and/or blurring]. Similar to this, a new study suggests leveraging multi-scale local binary patterns for micro-texture analysis. One may argue that the effectiveness of these methods greatly depends on the methods heavily rely on how well the video or printed image is displayed. The second set of techniques examines the scene's motion to spot spoofing attempts since planar items such as a piece of paper or a smartphone screen move quite differently from actual people. To check if a facial picture is authentic or fake, for instance, the trajectories of specific tiny regions are studied.

Similar to this, Marsico et al. take advantage of the same occurrence by computing the geometric invariants of a collection of facial points that were located automatically The liveness of the face is judged using the last set of approaches based on distinctive live-face characteristics like lip or eye blinking.

Due to the unique characteristics of electrocardiogram (ECG) signal patterns, continuous biometric authentication is a viable next-generation technology and trait mechanism. ECG-based technology is often used for continuous authentication to identify a specific person since ECG signals are ubiquitous, easy to utilize, and difficult to counterfeit [8].Additionally, numerous applications can be combined with a continuous ECG monitor allowing users to derive a quantitative measurement of their present stress level, exhaustion, and illness.

This allows users to comprehend their bodies' genuine states and take the necessary steps. In other words, ECG signals may be utilized for biometric identification as they are already being recorded for medical purposes. Additionally, real-time ECG signal recording has become a routine activity in our everyday lives for user health monitoring thanks to the development of sophisticated wearable gadgets like Apple watches.

Despite the substantial work invested into making the ECG a biometric modality, it still hasn't reached a level of acceptability and technical maturity that is necessary. The immaturity of ECG development is a result of the scarcity of reliable ECG data. The research community also relies on a small ECG gallery, which has decent performance but significant error rates. The bulk of the current methodologies typically fail to give standard metrics for assessing the outcomes of ECG data assessment in order to balance various important evaluation metrics, such as the erroneous acceptance rate, false reject rate, and equal error rate.

Additionally, the effectiveness of filtering, segmentation, feature extraction, and matching hasn't yet been fully evaluated for the majority of approaches.
The largest off-the-person ECG datasets will be included in this study for the first time, and we'll also learn about and assess the efficacy of various methodologies at various stages of ECG biometric systems.

Using a range of ECG data sets, including our sizable new data set, we provide a detailed analysis of current well-known techniques. This research suggests a novel filtering method for developing a bio template for biometric identification.
Through thorough tests and considerable literature research in the area of ECG biometric systems, we share our knowledge with the ECG-based research community.

II. EXSITING METHOD

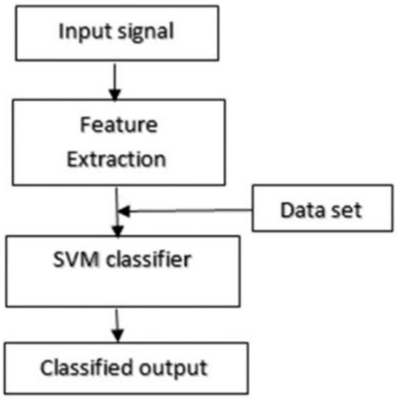
We use the support vector machine (SVM) to further enhance the verification process since the verification based on the Euclidian distance is straightforward but insufficient for applying the authentication using the intra-body propagation signal in actual applications.

The SVM has been suggested as a supervised learning-based pattern classification technique. The SVM performs better separation for unlearned data because it learns a separating hyperplane that optimizes the distance (margin) between two classes. For each user, the intraday propagation signals are measured, and their spectra are then extracted, smoothed, and normalized. The smoothing is done using the same approach as before.

For intraday communication, three transmission types—the simple circuit type, the electrostatic coupling type, and the waveguide type—have been suggested. contains a signal generator, a detector-acting digital oscilloscope, and gelpadped body surface electrodes.

It is anticipated that the intrabody propagation signal's spectrum would have distinct features, hence it is crucial to consider which frequency ranges will result in the best verification performance.

During the verification process, each user identifies themselves by giving the system their name or ID number, which it then uses to select the template. And the intra body propagation signal for confirmation.



Block Diagram of Existing Method

DRAWBACKS:

1. It is difficult to select a "good" kernel function.
2. Large datasets require lengthy training times.
3. The final model's varying weights and individual impacts make it challenging to comprehend and analyze.

III. PROPOSED METHOD:

Implementing the suggested approach will secure data and device protection. For authentication, we make use of an ECG-based dataset that was taken from the referenced research. There are phases for enrollment and verification. This database is used to plot the signal. The IIR Butterworth Filter is then used to perform the filtering process.

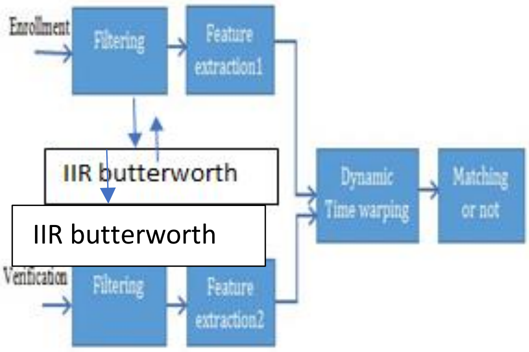
This particular signal processing filter is made to have a pass band frequency response that is as flat as feasible. The term "maximally flat magnitude filter" is also used to describe it.
Butterworth demonstrated that increasing the number of filter elements with the appropriate values led to ever closer approximations.

The discrete wavelet transform is defined by wavelets, which are orthogonal wavelets. Wavelets are identified by having a maximum number of vanishing moments for a given support.

DTW is then utilized for biometric authentication. Due to variations in the lengths of their portions, When two comparable signals are arranged in the same sequence, they might seem quite different from one another.

Dynamic time warping is used to distort these durations, highlighting the similarities between the signals by making related aspects appear at the same location on a common time axis.

The dialogue box indicates that the biometric has been matched if the difference between the features of the two phases is zero; else, the dialogue box displays that biometric is not matched.



Block diagram of proposed method.

IV. METHODOLOGY

This technique offered a novel approach for an ECG-based biometric authentication system. This technique first uses Empirical Mode Decomposition to de-noise a single lead raw ECG signal (EMD). The EMD approach can handle fractal-like signals and extract global structures. The EMD method was created in order to analyze the data for nonlinear and non-stationary signals in a space of adjustable time, frequency, and amplitude.

The area of interest in the ECG data that includes the most recognized, unique information about the person is also extracted using EMD. Then, characteristics are extracted by combining five features from the statistical, temporal, and frequency domains.

ADVANTAGES

Improves biometric authentication results;
•Greater accuracy.

APPLICATIONS:

Although there are many uses for biometric technology, the following are the most widespread ones:

- logical access management.
- Control of physical access.
- Attendance and time.
- Legal Action.
- Surveillance.

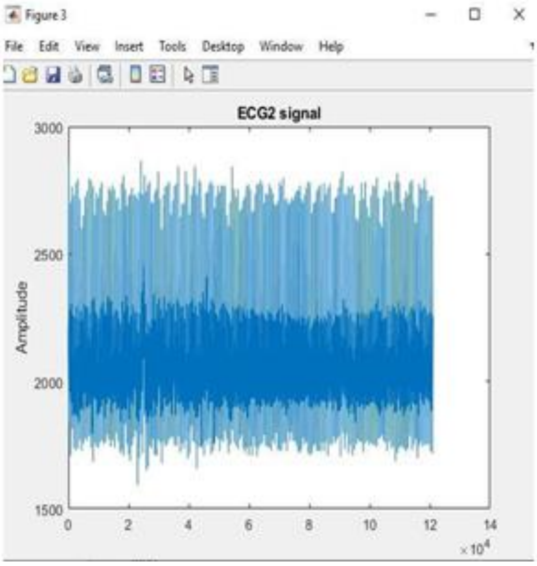
SOFTWARE REQUIRED:

MATLAB R2018a or above

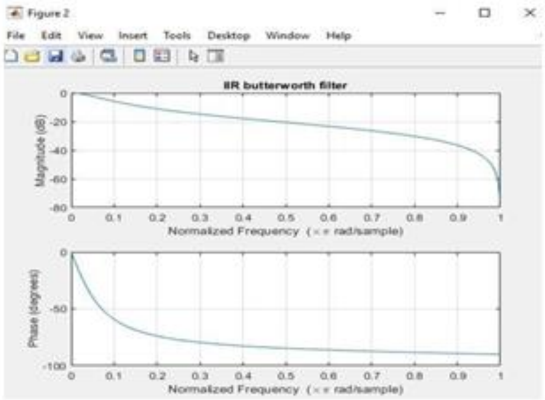
IV. RESULTS

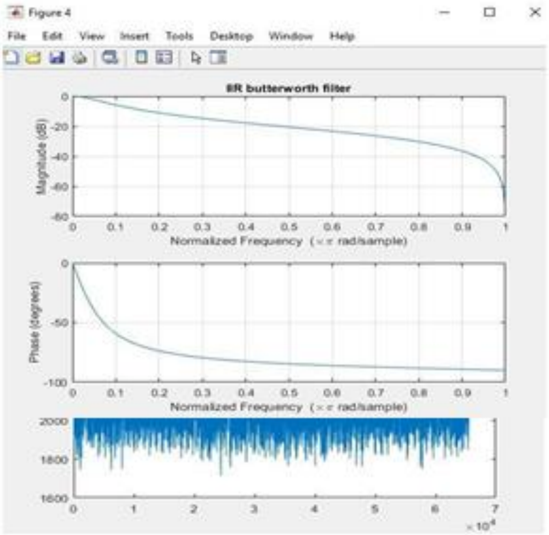
The electromyogram (EMG), which is created by the electrical activity of the muscles, appears as quick variations that are substantially quicker than the ECG waves.The produced ECG signal is depicted in the diagram below.

This particular signal processing filter is made to have a pass band frequency response that is as flat as feasible. The term "maximally flat magnitude filter" is also used to describe it. The IIR Butterworth filter is depicted in the below figure. The produced ECG signal is shown in the figure below during the phase of verification.



The IIR Butterworth filter for the verification step is shown in the next image.





V. CONCLUSION

In this work, we extensively evaluate the effect of filtering type, segmentation, feature extraction, and health condition on ECG biometrics using evaluation measures such as accuracy, FAR, FRR, and ERR. ECG dataset is utilized for authentication in order to safeguard the devices and data. In other words, a number of experimental findings were made to assess the effects of such crucial methods on ECG biometric systems. This research demonstrates that, when compared to the current strategy, our new proposal performs better. Since the proposed approach has a 95 percent accuracy rate.

REFERENCES

[1] Nesli Erdogmus and Sebastien Marcel. Spoofing face recognition with 3d masks. IEEE transactions on information forensics and security, 9(7):1084–1097, 2014.

[2] Abdenour Hadid, Nicholas Evans, Sébastien Marcel, and Julian Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5):20–30, 2015.

[3] Neslihan Kose and Jean-Luc Dugelay. On the vulnerability of face recognition systems to spoofing mask attacks. In 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pages 2357– 2361. IEEE, 2013.

[4] Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de Rivera, Davide Maltoni, Julian Fierrez, Javier Ortega-Garcia, and Dario Maio. An evaluation of direct attacks using fake fingers generated from iso templates. Pattern Recognition Letters, 31(8):725–732, 2010.

[5] Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti. Biometric liveness detection: Challenges and research opportunities. IEEE Security & Privacy, 13(5):63–72, 2015.

[6] Majid Komeili, Narges Armanfard, and Dimitrios Hatzinakos. Liveness detection and automatic template updating using fusion of ecg and fingerprint. IEEE Transactions on Information Forensics and Security, 13(7):1810–1822, 2018.

[7] Patrick PK Chan, Weiwen Liu,

Danni Chen, Daniel S Yeung, Fei Zhang, Xizhao Wang, and Chien-Chang Hsu. Face liveness detection using a flash against 2d spoofing attack. IEEE Transactions on Information Forensics and Security, 13(2):521–534, 2017