**ECG BIOMETRIC AUTHENTICATION: A COMPARATIVE ANALYSIS**

**Abstract:**

The main theme of this project is to authenticate the user by using ECG signals. Electrocardiogram (ECG) is an electric signal of cardiac activity posing highly discriminative properties related to human recognition. ECG based authentication has gained much success in recent times however discriminant feature extraction and efficient pattern classification still encounter numerous challenges. In these present situations authentication methods became an indispensable urgent task to protect the integrity of the devices and the sensitive data. Passwords have provided to control the important data, but have shown their inherent vulnerabilities. We propose an authentication method, which can effectively provide the access to the user, which is known as ‘ECG Biometric Authentication’. This authentication mainly involves filtering type, segmentation, feature extraction, and health status on ECG biometric by using the evaluation metrics.

**Keywords:** ECG Biometric, Authentication.

**Existing Method:**

This method proposed a novel methodology for ECG based biometric authentication system. This method first de-noise single lead raw ECG signal through Empirical Mode Decomposition (EMD). The EMD method can extract global structure and deal with fractal-like signals. The EMD method was developed so that the data can be examined in an adaptive time–frequency–amplitude space for nonlinear and non-stationary signals. Region of interest from ECG signals having maximum characteristic information related to subject's recognition is also extracted through EMD. Next, feature extraction is performed by combination of five features from statistical, time and frequency domains. Finally, selected features were categorized with classifier of Support Vector Machines (SVM). The block diagram of existing method is shown below:

Input signal

Feature Extraction

Data set

SVM classifier

Classified output

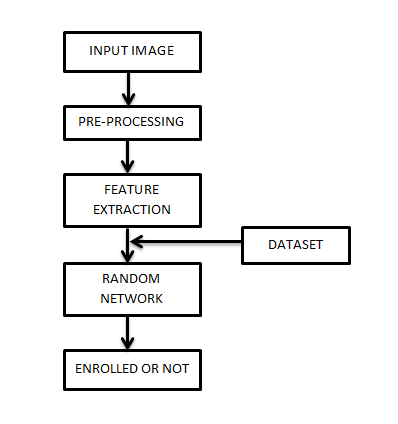
**Fig: Block Diagram of Existing Method**

**Disadvantages:**

* Choosing a “good” kernel function is not easy.
* Long training time for large datasets.
* Difficult to understand and interpret the final model, variable weights and individual impact.

**Proposed System:**

This proposed method is implemented to protect the data and devices securely. We use ECG based dataset for authentication which is collected from the given paper. The signal is plotted form this given database. Then we apply the IIR butterworth filter for filtering operation. Non fiducial is used for feature extraction. Daubechies wavelet is applied in two phases. After that network random algorithm is performed for biometric authentication. Two signals with equivalent features arranged in the same order can appear very different due to differences in the durations of their sections.



**Fig: Proposed Methodology**

**Advantages:**

* Gives the better authentication results of biometric.
* Accuracy is more.

**Applications:**

There are numerous applications for the use of Biometric Technology, but the most common ones are as follows:

* Logical Access Control.
* Physical Access Control.
* Time and Attendance.
* Law Enforcement.
* Surveillance.

**Software & Hardware Requirements:**

**Software Requirements:**

MATLAB R2018a or above

**Hardware Requirements:**

**Operating Systems:**

• Windows 10

• Windows 7 Service Pack 1

• Windows Server 2019

• Windows Server 2016

**Processors:**

Minimum: Any Intel or AMD x86-64 processor

Recommended: Any Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support.

**Disk:**

Minimum: 2.9 GB of HDD space for MATLAB only, 5-8 GB for a typical installation

Recommended: An SSD is recommended a full installation of all MathWorks products may take up to 29 GB of disk space

**RAM:**

Minimum: 4 GB

Recommended: 8 GB