International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# ECG-Based Biometric Authentication System Using Hybrid Signal Matching

**Prof. Umakant Shirshetti[1] , Astha Tanpure[2], Sakshi Late[3], Shrutika Ghadge[4], Anagha Kamble[5]**

Department of Information Technology
Sou. Venutai Chavan polytechnic, Sinhgad Institutes Pune, Maharashtra, India

**Keywords:** ECG Biometrics, Biomedical Signal Processing, AD8232, Arduino UNO, Dynamic Time Warping

**Abstract**
Biometric authentication systems are increasingly used to improve security in modern digital environments. Traditional authentication mechanisms such as passwords and PIN codes suffer from duplication and credential leakage. Electrocardiogram signals represent the electrical activity of the human heart and provide a unique physiological biometric. This work proposes an ECG-based biometric authentication system using an AD8232 sensor and Arduino UNO. The ECG signal is sampled at 250 Hz and transmitted to a Python backend for signal processing. A hybrid authentication model combining Dynamic Time Warping distance, RR interval comparison, and amplitude difference analysis is implemented. Experimental testing shows that ECG signals can distinguish individuals under controlled conditions.

## 1. INTRODUCTION

Authentication systems protect digital resources from unauthorized access. Traditional authentication techniques such as passwords rely on human memory and are vulnerable to attacks. Biometric authentication uses physiological characteristics of individuals. ECG signals provide an internal biometric difficult to replicate artificially. The ECG waveform contains P wave, QRS complex, and T wave components where the QRS complex contains distinctive identification information.

Biometric authentication methods include fingerprint recognition, facial recognition, iris scanning, and voice recognition. These systems provide improved security because biometric traits are difficult to replicate compared to traditional credentials. Among these techniques, fingerprint and face recognition systems are widely used in smartphones, banking applications, and access control systems. However, they are not completely secure. Fingerprints can be copied using artificial molds, facial recognition can be spoofed using photographs or videos, and voice recognition can be deceived with recorded audio samples. These vulnerabilities highlight the need for more secure biometric systems that are resistant to spoofing attacks.

In recent years, **physiological biometrics derived from internal body signals** have attracted significant research attention. One such signal is the **electrocardiogram (ECG)**, which measures the electrical activity of the human heart. The ECG signal is generated by electrical impulses that trigger the contraction and relaxation of cardiac muscles during each heartbeat. These electrical impulses travel through specialized conduction pathways in the heart, including the **sinoatrial node (SA node), atrioventricular node (AV node), Bundle of His, and Purkinje fibers**. The resulting electrical potential differences can be measured on the surface of the skin using electrodes. A typical ECG waveform consists of several distinct components including the **P wave, QRS complex, and T wave**. The P wave represents atrial depolarization, the QRS complex represents ventricular depolarization, and the T wave represents ventricular repolarization. Among these components, the **QRS complex has the highest amplitude and contains significant morphological features that vary between individuals**. These

variations occur due to differences in heart anatomy, cardiac muscle thickness, electrical conduction speed, and body tissue impedance.

Despite these advantages, implementing ECG-based biometric authentication systems presents several technical challenges. ECG signals are extremely small in amplitude, typically ranging between **0.5 mV and 2 mV**, and are highly susceptible to noise from muscle activity, motion artifacts, and power line interference. Therefore, specialized hardware and signal processing techniques are required to capture and analyze ECG signals accurately. Recent advances in **embedded systems, low-cost biomedical sensors, and signal processing algorithms** have made it possible to develop portable ECG-based biometric systems. Sensors such as the **AD8232 ECG module** allow the amplification and filtering of weak cardiac signals, while microcontrollers like the **Arduino UNO** can perform analog-to-digital conversion and transmit data for further analysis.

## 2. RELATED WORKS

Several studies have investigated ECG signals for biometric identification. Early research focused on morphological analysis of ECG waveforms. Later works introduced statistical feature extraction methods including RR interval variability and amplitude analysis. Machine learning methods such as neural networks and support vector machines have also been explored. Dynamic Time Warping is widely used for time series comparison.

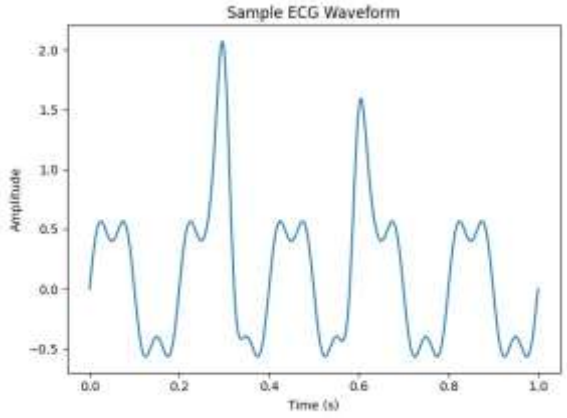
Table 1: Literature Survey of ECG Biometric Systems

| **Author & Year** | **Methodology** | **Technology** | **Limitations** |
|---|---|---|---|
| Israel 2005 | ECG waveform biometrics | Signal processing | Small dataset |
| Odinaka 2012 | Feature extraction | Machine learning | High complexity |
| Zhang 2017 | Deep learning ECG | CNN | Large dataset needed |
| Proposed 2026 | Hybrid DTW model | Arduino + Python | Single lead ECG |

## 3. PROPOSED SYSTEM

The architecture includes signal acquisition, signal processing, and authentication decision layers. ECG signals are collected using electrodes and the AD8232 module. The Arduino UNO converts analog signals to digital samples which are transmitted to a Python backend for authentication.

Figure 1: Example ECG waveform




## 4. METHODOLOGY

The methodology includes ECG acquisition, filtering, R peak detection, beat segmentation, and feature extraction. A bandpass filter between 0.5 Hz and 40 Hz removes noise. A hybrid score combining DTW distance, RR difference, and amplitude difference determines authentication.

### 4.1 ECG Signal Acquisition

The first stage of the system involves acquiring the electrocardiogram (ECG) signal from the user. ECG signals represent the electrical activity generated by the heart during each cardiac cycle. These signals are extremely small in amplitude, typically ranging between **0.5 mV and 2 mV**, and therefore require amplification before further processing.

The ECG signal is captured using the **AD8232 ECG sensor module**, which acts as an analog front-end designed specifically for ECG measurement. The sensor uses **three electrodes** placed on the user's body in a wrist-based configuration.

Electrode placement includes:

• **RA (Right Arm)** – Right wrist • **LA (Left Arm)** – Left wrist
• **RL (Right Leg / Reference)** – Right forearm or ground reference

### 4.2 Analog to Digital Conversion and Data Transmission

The Arduino UNO is responsible for converting the analog ECG signal into digital samples using its **10bit Analog-to-Digital Converter (ADC)**.

The analog signal from the AD8232 module is connected to the **A0 analog input pin** of the Arduino. The Arduino samples the signal at a **sampling rate of 250 Hz**, which satisfies the Nyquist sampling criterion since the useful ECG frequency range is below **40 Hz**.

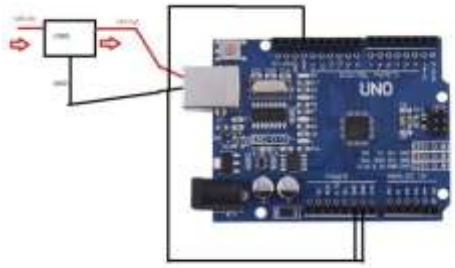
The sampling process ensures that the ECG waveform is accurately reconstructed in digital form. Each sample is transmitted through **serial communication (USB)** to a computer where further signal processing is performed.

### 4.3 Signal Preprocessing

The raw ECG signal obtained from the sensor often contains noise and artifacts caused by various environmental and physiological factors. These may include power line interference, muscle noise (EMG), motion artifacts, and baseline drift. A **bandpass filter with a frequency range of 0.5 Hz to 40 Hz** is applied to the ECG signal. After filtering, the signal is normalized to reduce amplitude variations caused by electrode placement or skin impedance.

### 4.4 Hardware Components


1. AD8232 ECG Sensor Module




2. Arduino UNO Microcontroller

3. Disposable ECG Electrodes

## 4. RESULTS AND DISCUSSION

Testing was performed using ECG recordings from multiple users. Signals from the same user produced lower similarity scores compared to signals from different users. Average scores ranged from 0.7 to 1.2 for the same user and 1.8 to 3.5 for different users. A threshold value of 1.4 determines authentication decisions.

Biometric authentication methods include fingerprint recognition, facial recognition, iris scanning, and voice recognition. These systems provide improved security because biometric traits are difficult to replicate compared to traditional credentials. Among these techniques, fingerprint and face recognition systems are widely used in smartphones, banking applications, and access control systems. However, they are not completely secure. Fingerprints can be copied using artificial molds, facial recognition can be spoofed using photographs or videos, and voice recognition can be deceived with recorded audio samples. These vulnerabilities highlight the need for more secure biometric systems that are resistant to spoofing attacks.

In recent years, **physiological biometrics derived from internal body signals** have attracted significant research attention. One such signal is the **electrocardiogram (ECG)**, which measures the electrical activity of the human heart. The ECG signal is generated by electrical impulses that trigger the contraction and relaxation of cardiac muscles during each heartbeat. These electrical impulses travel through specialized conduction pathways in the heart, including the **sinoatrial node (SA node), atrioventricular node (AV node), Bundle of His, and Purkinje fibers**. The resulting electrical potential differences can be measured on the surface of the skin using electrodes.

A typical ECG waveform consists of several distinct components including the **P wave, QRS complex, and T wave**. The P wave represents atrial depolarization, the QRS complex represents ventricular depolarization, and the T wave represents ventricular repolarization. Among these components, the **QRS complex has the highest amplitude and contains significant morphological features that vary between individuals**. These variations occur due to differences in heart anatomy, cardiac muscle thickness, electrical conduction speed, and body tissue impedance.

Because ECG signals originate from internal physiological processes, they possess several advantages as a biometric modality. First, ECG signals are **extremely difficult to replicate or forge**, making them highly resistant to spoofing attacks. Second, ECG inherently provides **liveness detection**, since the signal can only be generated by a functioning human heart. Third, ECG signals contain both **temporal and morphological information**, which allows the extraction of multiple biometric features such as heartbeat intervals, waveform shape, and amplitude characteristics. Despite these advantages, implementing ECG-based biometric authentication systems presents several technical challenges. ECG signals are extremely small in amplitude, typically ranging between **0.5 mV and 2 mV**, and are highly susceptible to noise from muscle activity, motion artifacts, and power line interference. Therefore, specialized hardware and signal processing techniques are required to capture and analyze ECG signals accurately.

Recent advances in **embedded systems, low-cost biomedical sensors, and signal processing algorithms** have made it possible to develop portable ECG-based biometric systems. Sensors such as the **AD8232 ECG module** allow the amplification and filtering of weak cardiac signals, while microcontrollers like the **Arduino UNO** can perform analog-to-digital conversion and transmit data for further analysis.

## 6. CONCLUSIONS

The ECG biometric authentication system demonstrates the feasibility of physiological signals for identity verification. The hybrid matching method improves authentication reliability using morphological and temporal ECG features. The proposed system integrates low-cost biomedical hardware with signal processing algorithms to capture and analyze ECG signals for user authentication. The AD8232 ECG sensor module was used to acquire cardiac signals from electrodes placed on the user's wrists. The analog signals were digitized using the Arduino UNO microcontroller at a sampling rate of 250 Hz and transmitted to a Python-based backend for signal processing and analysis.

To improve signal reliability, preprocessing techniques such as bandpass filtering were applied to remove noise and baseline drift from the raw ECG signals. R-peak detection and beat segmentation were then performed to extract individual heartbeats and compute important physiological features including RR interval and waveform amplitude. A hybrid biometric matching algorithm was implemented that combines Dynamic Time Warping (DTW) with statistical feature comparison. This approach allows the system to compare the morphological similarity of ECG waveforms while also considering temporal variations in heartbeat intervals.

## 7. FUTURE SCOPE

Future work includes multi-lead ECG sensors, machine learning classifiers, cloud authentication platforms, encrypted template storage, and wearable ECG authentication devices.

The system can be improved by using **multi-lead ECG**, which records the heart's activity from different angles and provides more detailed information. This can help increase the accuracy of authentication.

In future, **machine learning techniques** like SVM, CNN, and LSTM can be used instead of rule-based methods to better identify patterns in ECG signals and improve performance.

Also, by using **cloud and IoT technologies**, ECG data from wearable devices can be sent to cloud servers for secure and real-time authentication. This will make the system more scalable and suitable for wider use.

## ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial support provided by the Sinhagad College of Engineering, Pune, India through the Seed Money Project. We also extend our thanks to our college for providing the necessary facilities to conduct this research.

## REFERENCES

1. Berkaya, S. K., Uysal, A. K., Gunal, E. S., Ergin, S., Gunal, S., & Gulmezoglu, M. B. (2018). A survey on ECG analysis. *Biomedical Signal Processing and Control*, *43*, 216–235. https://doi.org/10.1016/j.bspc.2018.03.003 2. Biel, L., Pettersson, O., Philipson, L., & Wide, P. (2001). ECG analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, *50*(3), 808–812. https://doi.org/10.1109/19.930458

3. deChazal, P., O'Dwyer, M., & Reilly, R. (2004). Automatic classification of heartbeats using ECG morphology and heartbeat interval features. *IEEE Transactions on Biomedical Engineering*, *51*(7), 1196–1206. https://doi.org/10.1109/tbme.2004.827359

4. Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/tit.1983.1056650

5. Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., & Wiederhold, B. K. (2004). ECG to identify individuals. *Pattern Recognition*, *38*(1), 133–142. https://doi.org/10.1016/j.patcog.2004.05.014

6. Li, C., Zheng, C., & Tai, C. (1995). Detection of ECG characteristic points using wavelet transforms. *IEEE Transactions on Biomedical Engineering*, *42*(1), 21–28. https://doi.org/10.1109/10.362922

7. Martinez, J., Almeida, R., Olmos, S., Rocha, A., & Laguna, P. (2004). A Wavelet-Based ECG Delineator: Evaluation on standard databases. *IEEE Transactions on Biomedical Engineering*, *51*(4), 570–581. https://doi.org/10.1109/tbme.2003.821031