HEARTBEAT RECOGNITION

Biometric System Based on Electrocardiogram Patterns

ECG

Marco Sodano Ballestero

Table of contents

System analysis: Introduction

Heartbeat recognition is an innovative biometric system that identifies individuals based on their unique electrocardiogram (ECG) patterns.

Unlike traditional biometrics, which rely on physical or behavioral traits, heartbeat recognition uses the electrical activity of the heart to establish a person's identity.

This method offers a secure and non invasive way of authentication, leveraging the inherent uniqueness of each individual's heartbeat.

System analysis: Attributes

Universality

Every person has a unique ECG pattern, making it a universal biometric trait.

Uniqueness

The intricate details in ECG patterns ensure high distinctiveness among individuals.

Permanence

Heartbeat patterns remain consistent over time, barring medical conditions.

Collectability

Modern technology allows easy collection of ECG data through wearable devices.

Performance

Exhibits high accuracy, particularly in controlled environments.

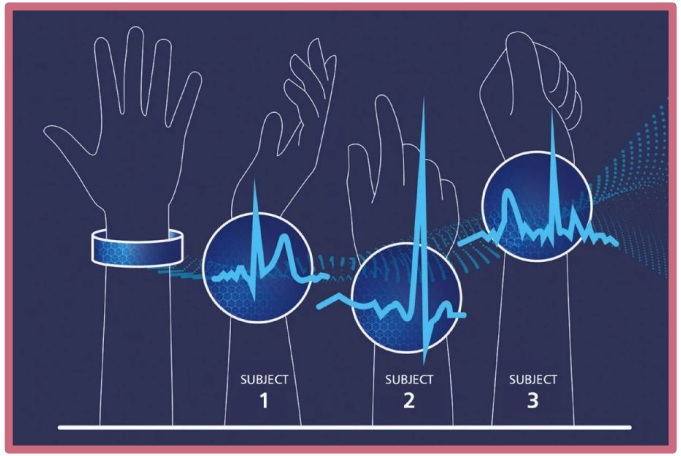
Acceptability

Generally well accepted by users due to its non intrusive nature.

System analysis: Applications

- Healthcare for patient tracking and emergency identification.
- Security systems for access control in sensitive areas.
- Financial services for secure transactions and banking.
- Law enforcement for suspect identification and tracking.

Approaches: Detection

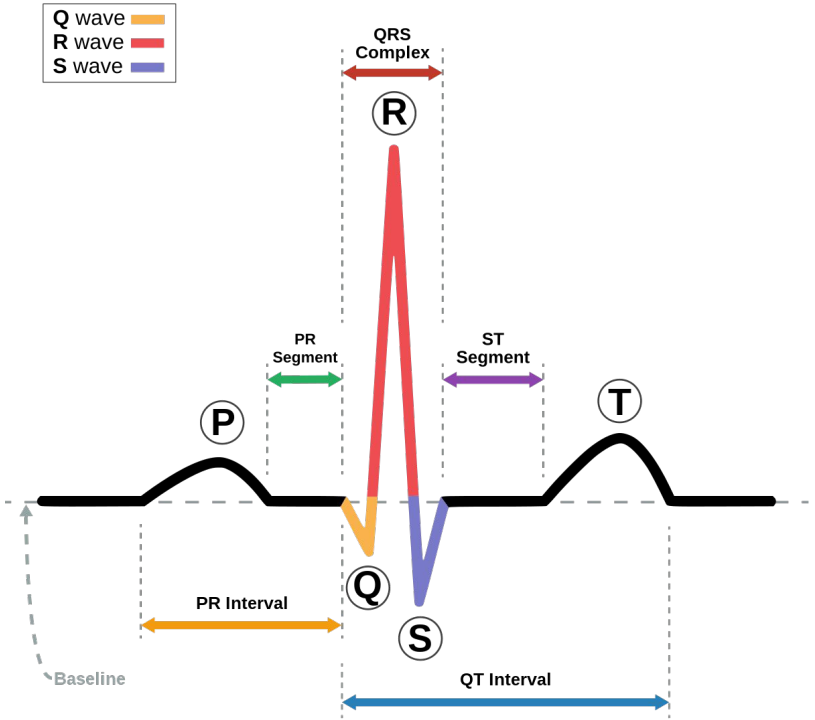


ECG signal acquisition is achieved through sensors placed on the skin or in wearable devices.
These sensors detect the electrical signals generated by the heart's activity, which are then converted into a digital format for analysis.

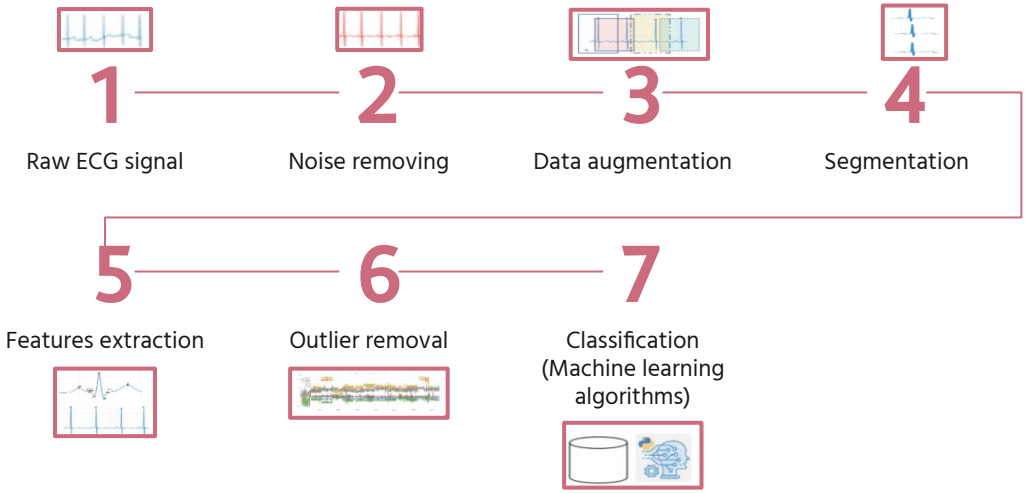
Approaches: Feature extraction

The ECG waveform is analyzed to extract key features such as the QRS complex, which represents the depolarization of the right and left ventricles of the human heart.

Other features like heart rate variability also play a significant role in individual identification.



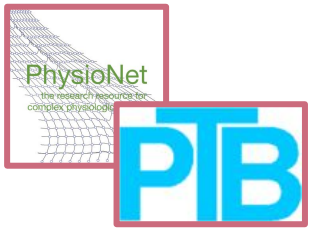
Approaches: Recognition



Pattern recognition in heartbeat biometrics involves using algorithms to match ECG patterns.

Machine learning techniques, including deep learning, are increasingly employed to enhance the accuracy and efficiency of recognition processes.

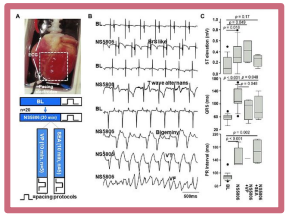
Testing conditions



Databases

Utilizes public and private ECG databases. These databases are essential for training and testing the algorithms that power heartbeat recognition systems. Here some examples:

- PhysioNet
- PTB Diagnostic ECG database
- Private databases



Protocols

Adheres to standard protocols for biometric system evaluation to ensure reliability and reproducibility of results.

Results

Accuracy in controlled settings	Heartbeat recognition systems show high accuracy in controlled environments, often outperforming traditional biometrics like fingerprints or facial recognition. The complex nature of ECG patterns contributes to this high accuracy.
Comparison with other biometrics	Heartbeat recognition is more stable under various conditions compared to other biometrics, offering a reliable alternative for identity verification.
Variability in performance	Performance can fluctuate with physical activity, stress, or emotional states, as these factors might alter ECG patterns, affecting identification accuracy.
Real world challenges	In less controlled environments, factors like movement, sweat, and sensor issues can introduce noise, impacting the system's effectiveness. Ongoing improvements in sensor and algorithm design are addressing these challenges.
Future directions	Research is focused on enhancing system adaptability and reliability, particularly in diverse and real world conditions, through advances in technology and machine learning.

Commercial systems

Banking/financial services:

Financial institutions are adopting heartbeat recognition for secure customer authentication in ATM and online banking, enhancing security against identity theft and fraud.

Automotive industry

Car manufacturers are exploring heartbeat recognition for driver identification and vehicle security, personalizing settings and enhancing anti theft measures.

Consumer Electronics

Incorporation of heartbeat recognition in smartphones and tablets offers a secure and convenient alternative to traditional passwords and PIN

High security access control

Used in government and military facilities, heartbeat recognition provides high level security by granting access based on unique ECG patterns.

Bibliography

- *Advances in ECG technology in 2022: Retaining a key role for patient care*. (s. f.). GE HealthCare (United States). https://www.gehealthcare.com/insights/article/advances-in-ecg-technology-in-2022-retaining-a-key-role-for-patient-care
- Aziz, S., Ahmed, S., & Alouini, M. (2021). ECG-based machine-learning Algorithms for heartbeat classification. *Scientific Reports*, *11*(1). https://doi.org/10.1038/s41598-021-97118-5
- Barros, A., Resque, P., De Almeida, J. A. T., Mota, R., Oliveira, H., Rosário, D., & Cerqueira, E. (2020). Data improvement model based on ECG Biometric for user authentication and identification. *Sensors*, *20*(10), 2920. https://doi.org/10.3390/s20102920
- *EEG and ECG Biometrics Market Report 2023, Growth, Trends 2028*. (s. f.). https://www.syndicatedanalytics.com/eeg-and-ecg-biometrics-market
- *FIGURE 1. ECG Signal. Schematic representation of the QRS complex and. . .* (s. f.). ResearchGate. https://www.researchgate.net/figure/ECG-signal-Schematic-representation-of-the-QRS-complex-and-P-T-U-waves-U-wave-may-not_fig1_347268837
- Mitchell, A. R., Ahlert, D., Brown, C., Birge, M., & Gibbs, A. (2023). Electrocardiogram-based biometrics for user identification – using your heartbeat as a digital key. *Journal of Electrocardiology*, *80*, 1-6. https://doi.org/10.1016/j.jelectrocard.2023.04.001
- Platsis, G. (2020, 21 agosto). *When your Heartbeat Becomes Data: benefits and risk of biometrics*. Security Intelligence. https://securityintelligence.com/posts/biometrics-for-enterprise-security/