A Key to Your Heart:
Biometric Authentication Based on ECG Signals

Who Are You?! Adventures in Authentication Workshop (WAY) 2019

Nikita Samarin, Donald Sannella

Berkeley
UNIVERSITY OF CALIFORNIA

THE UNIVERSITY of EDINBURGH
informatics

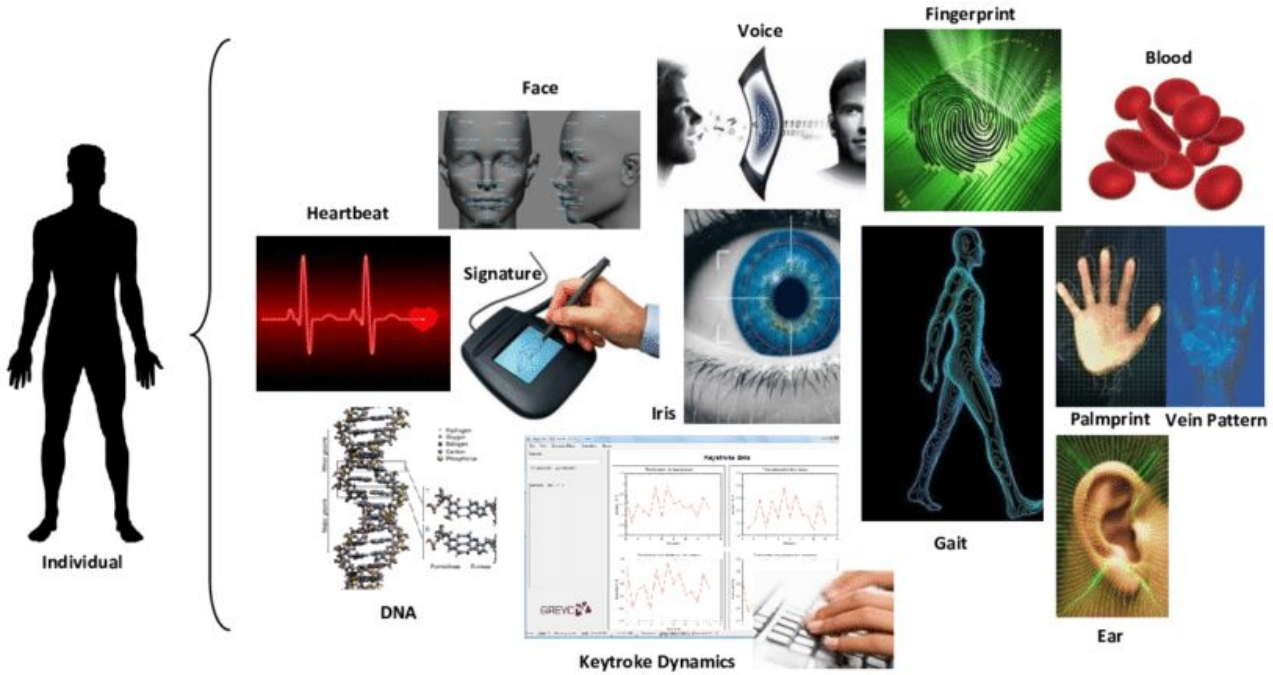
Traditional Passwords

- Most common mechanism of authenticating users online…
- … despite having numerous usability issues…
- … leading to serious security problems.
  - For instance, 81% of data breaches occur due to poor password hygiene [1]

[1] Verizon. Verizon Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/#report, 2017.

Biometric Authentication

Proves the identity of the user with “something they are”, improving the usability of systems

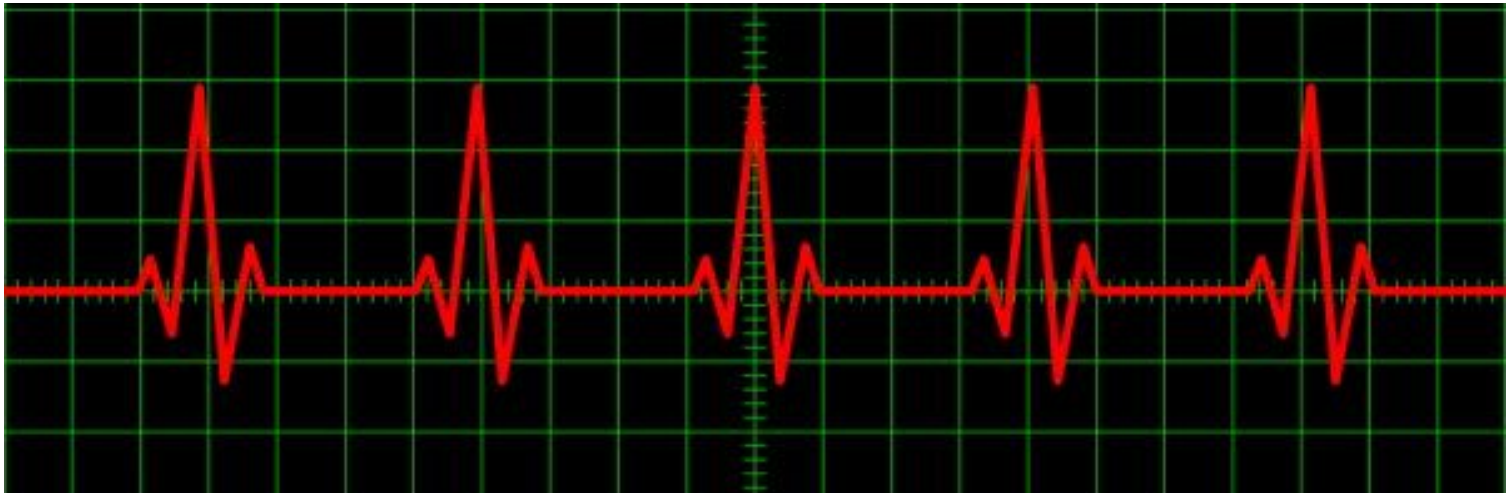


Motivation

- Insufficient research has been done to explore novel biometrics
- We investigate a biometric based on electrocardiogram (ECG) signals
- We want to validate the uniqueness and stability properties of an ECG that is recorded using a consumer-grade ECG monitor

Electrocardiogram as a Biometric

- Recording of the electrical activity of the heart
- Electrical impulse can be detected on the surface of the body using an ECG monitor



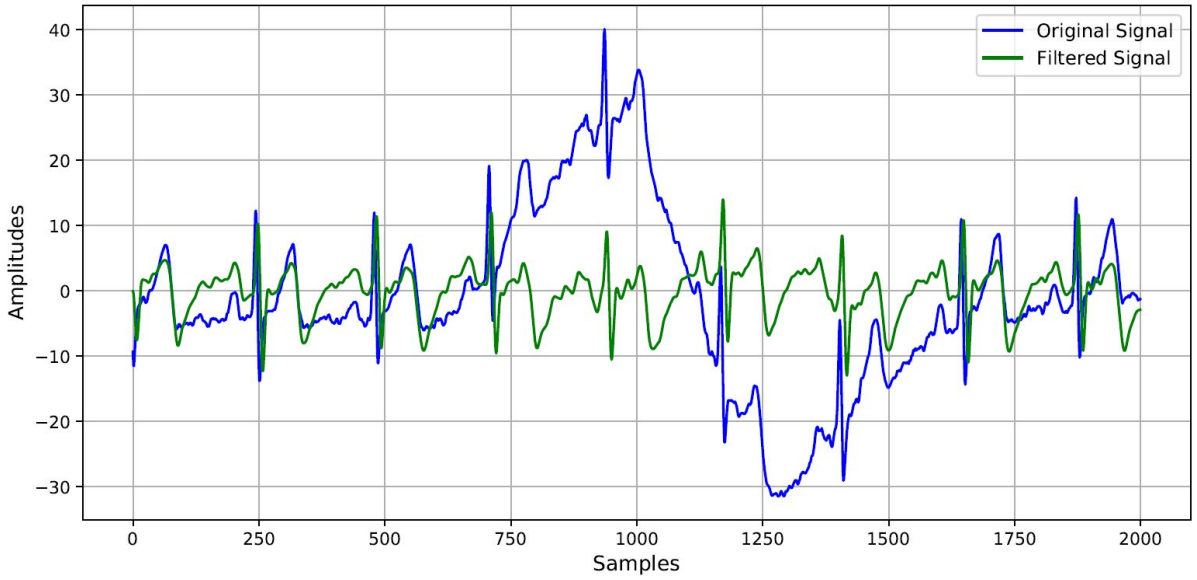
How did we collect ECG data?

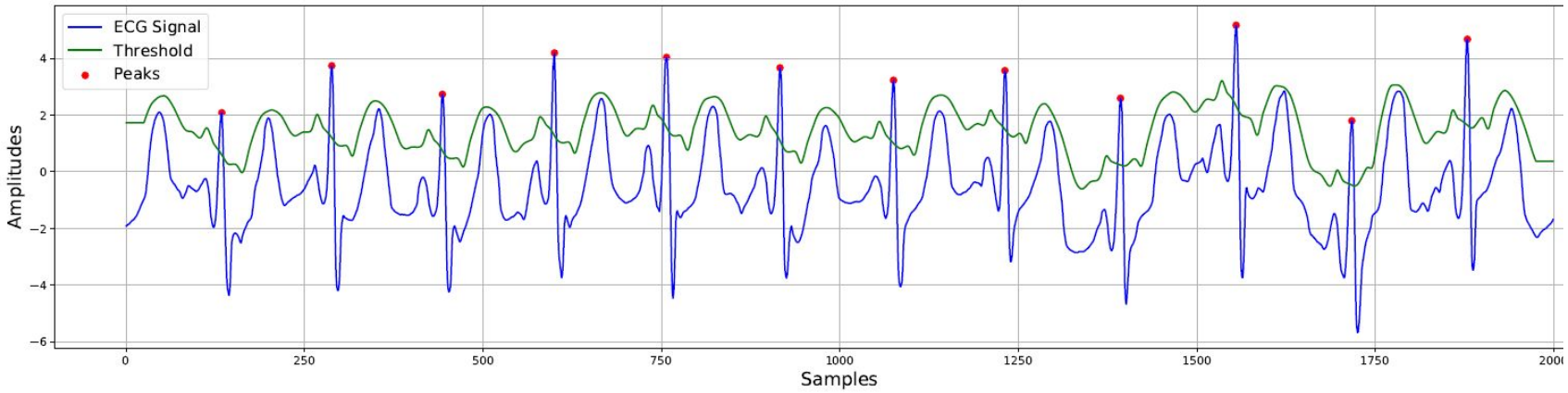
ECG Data Collection

- Using a consumer-based ECG monitor, we have collected ECG readings from 55 participants during two sessions
    - Performed in October 2017 and March 2018
    - Each session lasted 8 minutes

What is the proposed design of our system?

Signal Processing

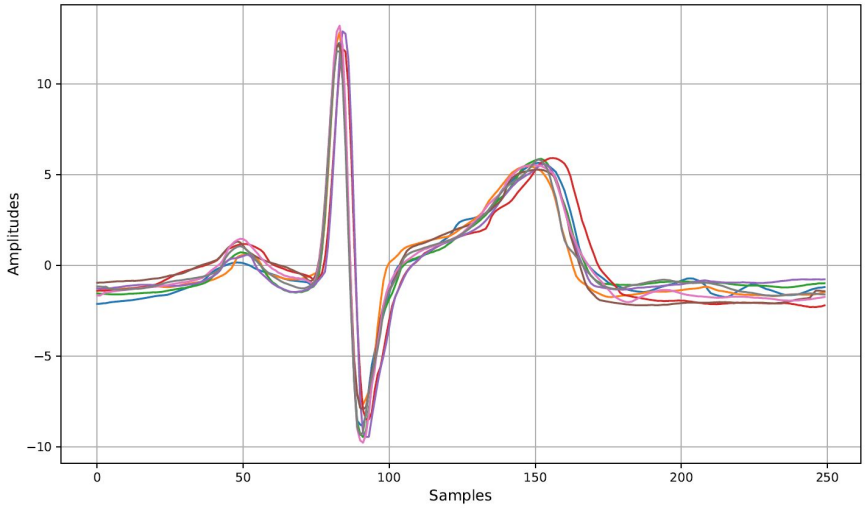




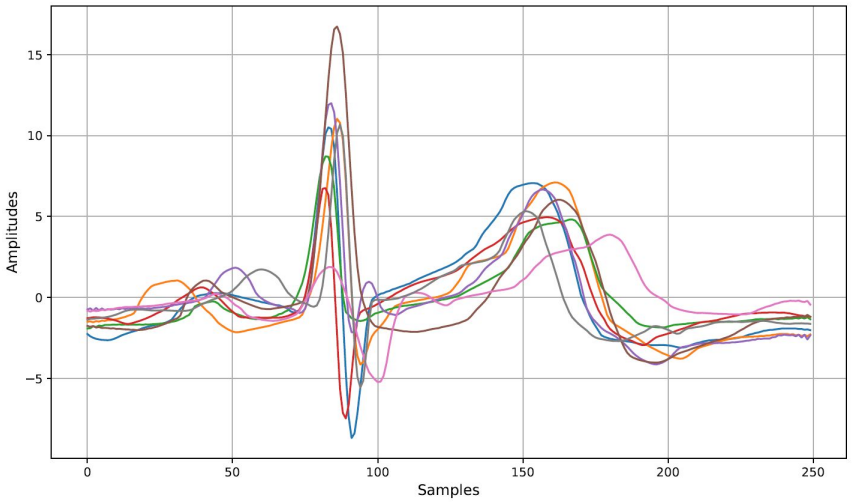
Classification

We use support vector machines to classify preprocessed segmented heartbeat waveforms

Variability within same individual



Variability within different individuals



How well does this system perform?

Evaluation

Training	Testing	Average EER	Standard Deviation
S1	S1	3.22%	2.99%
S2	S2	**2.44%**	2.40%
S1	S2	9.65%	11.35%

Table 1: Results obtained using the first evaluation approach. The first two columns reflect from which session (S1 or S2) the corresponding dataset originates. Lower scores indicate better performance.

Comparison to Existing Studies

Study	Subjects	Duration	EER
Present Work	49	Short	**2.4%**
Present Work	49	Long	**9.7%**
Carreiras et al. [6]	63	Short	**13.3%**
Coutinho et al [7]	19	Short	**0.4%**
Falconi et al.[2] [3]	10	Short	**9.8%**
Silva et al. [8]	63	Short	**1.0%**
Silva et al. [8]	63	Long	**9.1%**
Singh et al. [28]	126	Short	**3.4%**
Komeili et al. [20]	70	Short	**11.0%**

Table 3: Results from studies on ECG-based biometric authentication. All studies follow the "off-the-person" approach and use a single-lead ECG monitor. 'Duration' indicates whether the result is obtained using short- or long-term data.

Summary & Takeaways

- We have investigated the performance of an ECG as a biometric, when it is collected from a consumer-grade monitor
- Results obtained using data from single session recordings support the uniqueness property of ECG biometrics
- We have also demonstrated that ECG biometrics degrade over time
- Future work could focus on better signal preprocessing and classification, as well as improving the performance of ECG biometrics over longer periods of time

Evaluation

Equal Error Rate (EER) is achieved when the decision threshold of the classifier is tuned such that the number of false accepts and false rejects that the system makes is equal

Training	Testing	Average EER	St. Deviation
S1	S1	3.22%	2.99%
S2	S2	2.44%	2.40%
S1	S2	9.65%	11.35%