Cancelable Biometrics Based on Deep Learning

Using Electrocardiogram Data.

Arturo Calvera Tonin.

What’s Cancelable Biometrics?

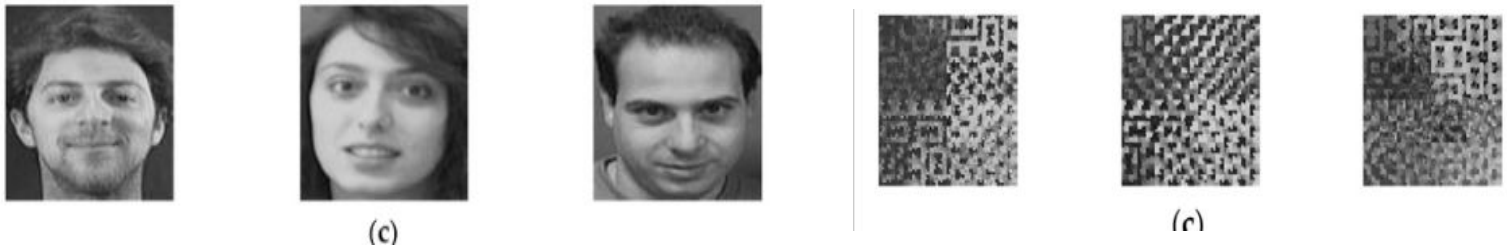
The transformation of Biometric signals in a useful, covert and irreversible template.

→ **Non-invertibility:** the recovery of original biometric data should be impossible.

→ **Efficiency**: satisfying the requirements imposed by cancelable biometrics should not deteriorate recognition performance.

→ **Diversity**: Many protected templates from the same biometric feature need to be generated.

→ **Revocability**: there should be straightforward revocation and reissue procedures in the event of compromise.



Motivation & Use Case

The infamous *WorldCoin* and the widespread *FaceID*

- *“Sam Altman & Alex Blania’s CryptoProject banned in several countries”.*

- Why should I comply with Apple keeping “*pictures*” of my face?

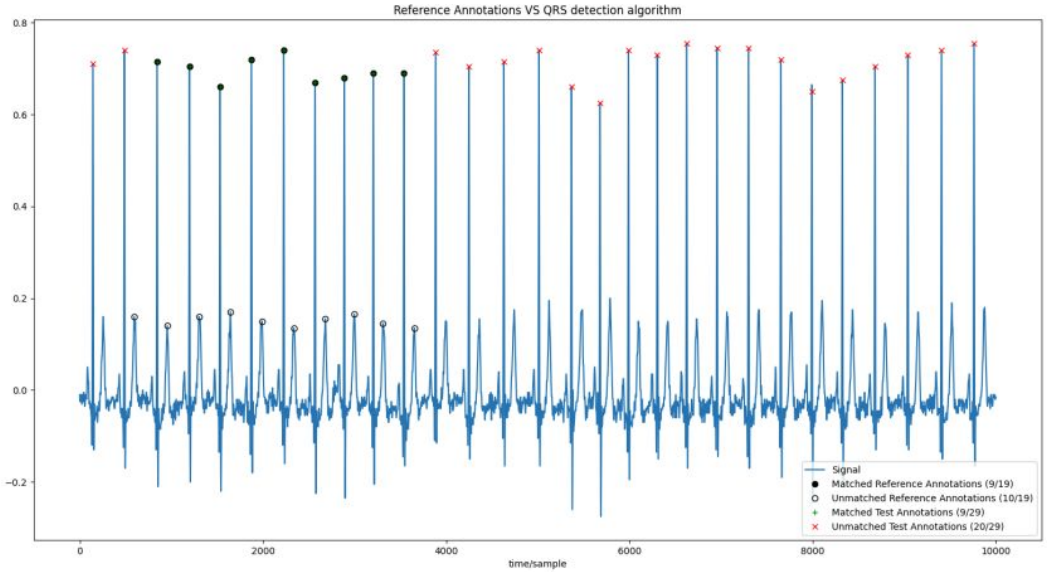
- Is there an alternative to today’s landscape? YES! Use cancelable biometric templates!

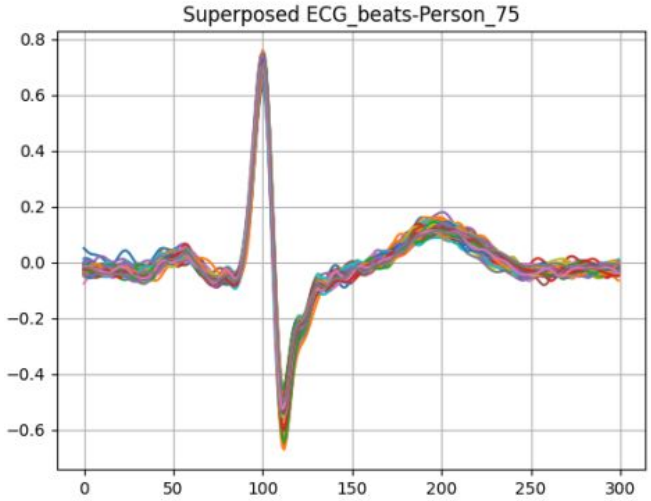
Why ECG? Prior work?

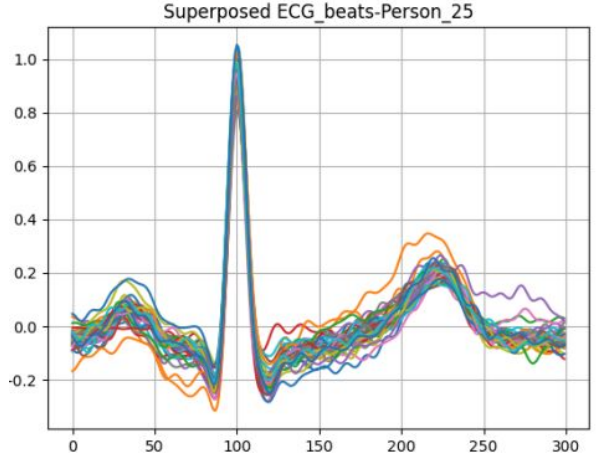
- **Electrocardiogram (ECG)** has been widely studied as a promising biometrics for authentication, identification and liveness validation.
  It has presented great possibilities for its strength against counterfeit. However, the ECG feature templates are completely irreplaceable.

- **Sakr et al., 2022:** in this article, the authors propose a novel cancelable ECG method using DNA and Amino Acid data combined with deep learning. They are the first to propose a cancelable ECG system that employs deep learning for human authentication yet their approach is too complex for widespread implementation.

The ECG-ID Database







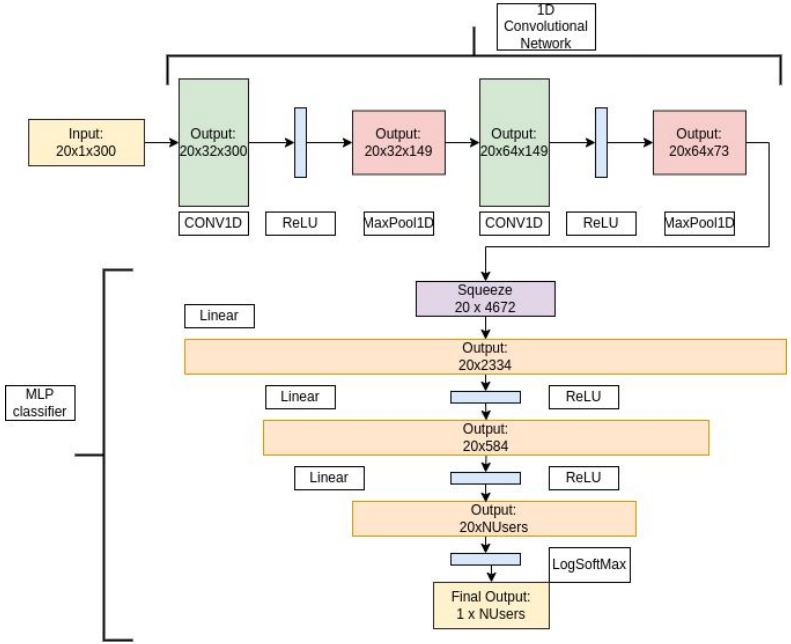
PyTorch

NVIDIA

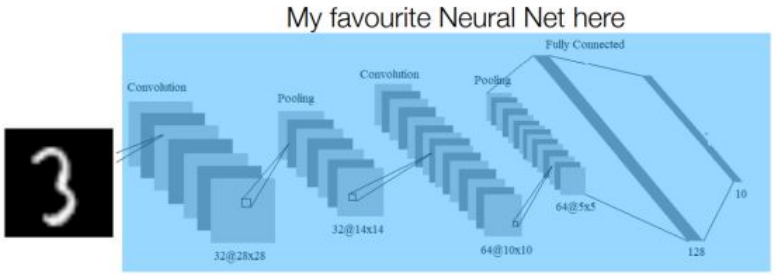
Harnessing the Neural Network’s inner knowledge

1 Dimensional CNNs

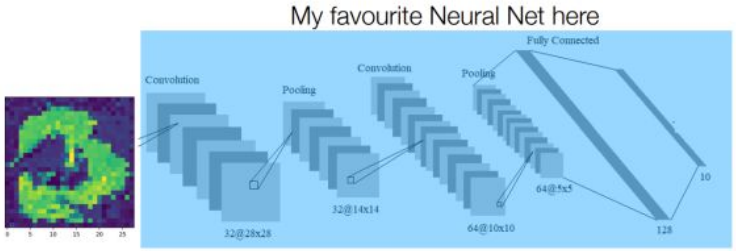
- Used with signals. Very common in the BioSignal Industry.
- **IDEA:** Build a good ECG classifier and harness the inner knowledge.



Overview Activation Maximization (AM)

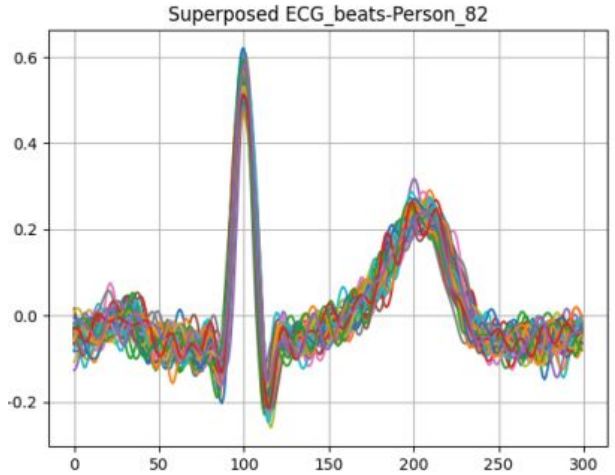


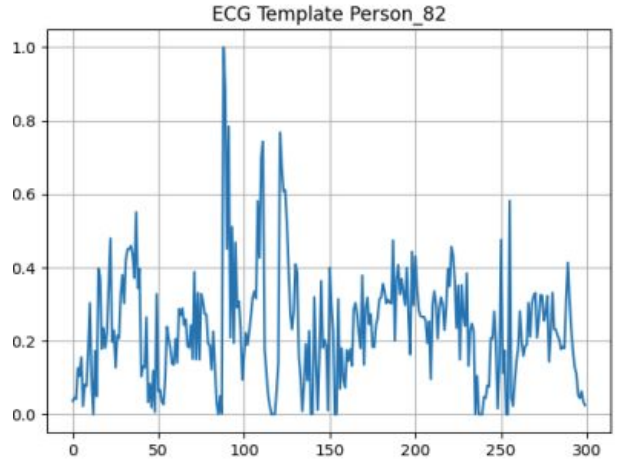
$$y = \begin{bmatrix} 0.001 \\ 0.001 \\ 0.001 \\ 0.91 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \end{bmatrix}$$



$$y = \begin{bmatrix} 0.001 \\ 0.001 \\ 0.001 \\ 0.91 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \\ 0.001 \end{bmatrix}$$

Applied in the current environment:





- Invertible?
- Diverse?
- Efficient?

Model	Recognition Rate	Weighted F1-Score
Original DL	95.062%	94.99%
Random Forest Classifier	96.296%	95.02%
Peng-Tzu et al., 2017	97.58%	-
Kim & Chun, 2019	93%	-
Sakr et al., 2022	98.60%	-

What about revocability?

- Something to work on in the future...
- ***“low-cost” solution:***
  - Revocation Authority + Watermarks embedded within the templates.
  - Did this template come from the original system?
  - Is this template still valid?
  - (Adi et al., 2018), (Uchida et al., 2017) and (Pagnotta et al., 2022).
  - Resilient against tampering.

Use Case?

Collaborative Neural Network Training

- A star topology of smartwatches training a 1D-CNN.
- “Train the model with a mini-batch of my data and forward to the next random node”.
- Distribute the final “Template Generator”. Use my templates as I wish.

Closing Statement

- Simple yet effective.

- Room for improvement:
  - Revocability.
  - Robustness and efficiency.
  - Better Deep Learning models.

- A stepping stone for future work on cancelable biometrics, user privacy and liberty.