Research Field And Department	Computer Security / Computer Science Department
Supervisor	Carmen Cámara & Pedro Peris-López ({macamara,pperis}@inf.uc3m.es})
Title of the Work	Design, Privacy, and Robustness of AI-Based Biometric Systems Using Contact and Contactless Physiological Signals

Abstract:
This research focuses on the development and analysis of artificial intelligence (AI)-based biometric systems that utilize both contact (e.g., ECG, EEG, GSR) and contactless (e.g., radar, optical, RF) physiological signals for human identification and continuous authentication. In particular, the study emphasizes the design of cancelable and privacy-preserving biometric schemes that can be securely updated or revoked when compromised. The integration of these modalities enables flexible, seamless, and privacy-aware biometric recognition suitable for real-world applications.

The study addresses four main aspects: signal preprocessing, application of AI and deep learning techniques, privacy protection, and adversarial robustness. Advanced signal processing and feature extraction methods will be implemented, followed by the use of AI and deep learning models for multimodal data analysis. Privacy-preserving and adversarially robust mechanisms will be explored to enhance system security and reliability. The final goal is to develop a secure, explainable, and ethically compliant biometric framework.

Main Tasks to Carry Out:

1. Preprocessing of Contact and Contactless Signals
    - Acquisition and filtering of physiological (ECG, EEG, GSR) and contactless (radar, optical, RF) signals.
    - Signal segmentation, normalization, and artifact reduction.
    - Extraction of fiducial and non-fiducial features in time, frequency, and entropy domains.
    - Study of complementarity and fusion between contact and contactless modalities.
2. Use of AI and Deep Learning Techniques for Biometric Systems
    - Application of AI and deep learning models (CNN, LSTM, GCN, etc.) for biometric identification and authentication.
    - Exploration of multimodal fusion strategies to enhance recognition accuracy and robustness.
    - Evaluation using metrics such as accuracy, Equal Error Rate (EER), and inter-session consistency.
    - Interpretation and visualization of model decision processes to ensure explainability.
3. Privacy Analysis of Biometric Systems

- Identification of potential privacy and security risks related to biometric data storage and transmission.
- Development of cancelable templates and privacy-preserving methods (federated learning, homomorphic encryption).
- Assessment of compliance with data protection frameworks such as the General Data Protection Regulation (GDPR).

4. Design of Adversary-Resistant Biometric Systems
   - Modeling of attacks, including spoofing, replay, and adversarial perturbations.
   - Implementation of liveness detection and adversarial training techniques.
   - Evaluation of system robustness under controlled and realistic attack conditions.

References/Bibliography if required

1. Foronda-Pascual, D., Cámara, C., & Peris-López, P. (2025). Non-contact human identification through radar signals using convolutional neural networks across multiple physiological scenarios. Frontiers in Digital Health, 7:1637437. https://doi.org/10.3389/fdgth.2025.1637437
2. Foronda-Pascual, D., Cámara, C., & Peris-López, P. (2025). Untouchable and Cancelable Biometrics: Human Identification in Various Physiological States Using Radar-Based Heart Signals. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1109/JBHI.2025.3566167
3. Cámara, C., Foronda-Pascual, D., & Peris-López, P. (2025). Enhancing biometric identification using 12-lead ECG signals and graph convolutional networks. Frontiers in Digital Health, 7:1547208. https://doi.org/10.3389/fdgth.2025.1547208
4. Cámara, C., & Peris-López, P. (2022). ELEKTRA: Electrocardiomatrix application to biometric identification with convolutional neural networks. Neurocomputing, 506, 37-49. https://www.sciencedirect.com/science/article/abs/pii/S0925231222009171
5. Peris-López, P., & Cámara, C. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 55, 272-289. https://doi.org/10.1016/j.jbi.2015.04.007