ScuDo

Scuola di Dottorato ~ Doctoral School

WHAT YOU ARE, TAKES YOU FAR

33rd Cycle

Learning mappings onto regularized space for biometric authentication

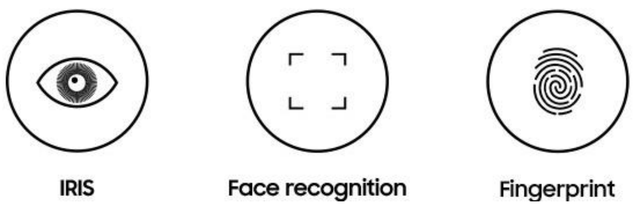
Arslan Ali

Supervisor's: Prof. Enrico Magli, Prof. Tiziano Bianchi

Research context and motivation

- Unauthorized access to sensitive data calls for techniques to protect the security of the devices
- Traditional authentication methods:

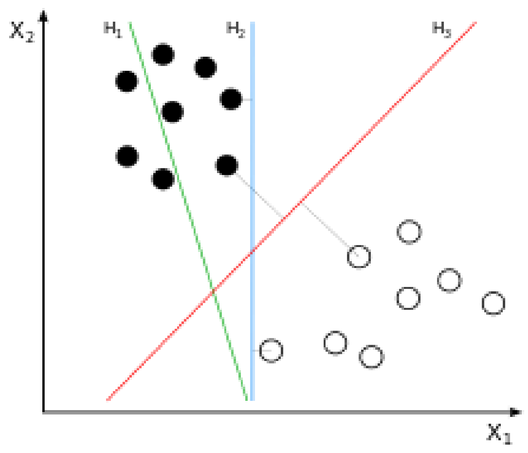
- Biometric authentication methods:

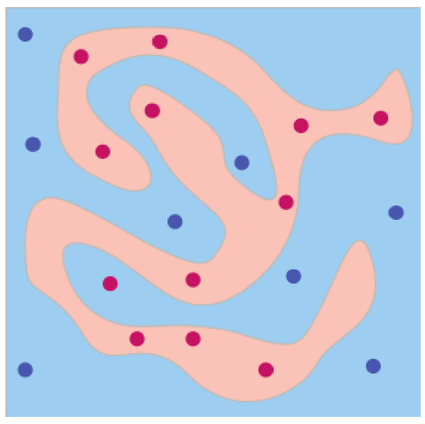


- A generic modular architecture, that can work for different biometries
- A novel framework for biometric authentication based on deep neural networks

Addressed research questions/problems

- In today's connected world the risk of unauthorized access to sensitive data is increasing, leading to an increase in the importance of security
- Deep learning for robust authentication:
  - standard classifiers cannot be utilized since classification regions do not have well-defined boundaries
  - need to find a novel deep learning based approach for biometric authentication

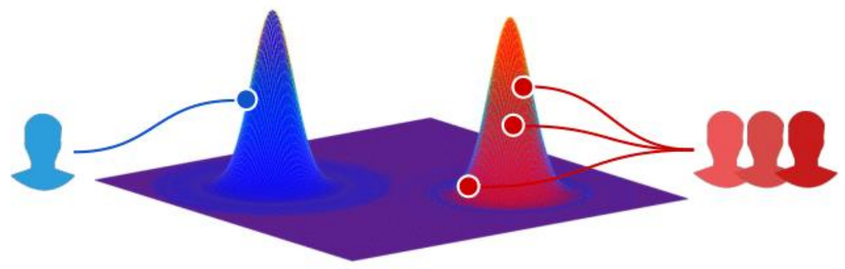




- Computational efficient, generic, robust to adversarial attacks

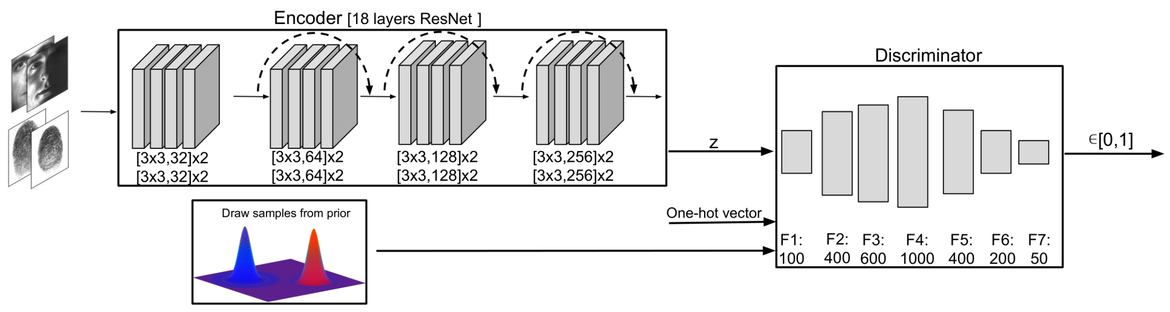
Novel contributions

- A generic novel architecture that:
  - map's enrolled users to a specific distribution in the latent space
  - map's unenrolled users far from it

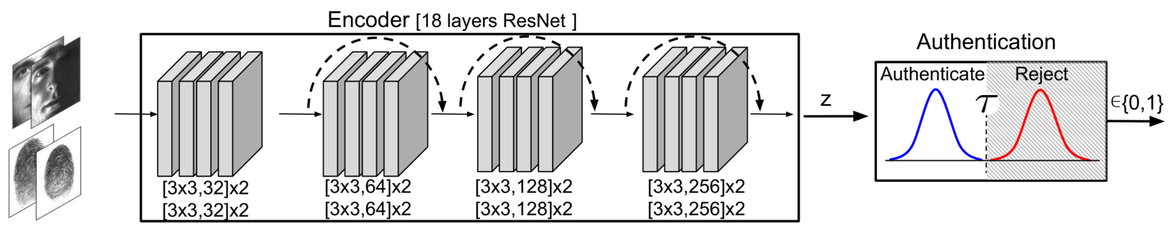


Adopted methodologies

- Using adversarial model (GAN) to enforce desired distributions: AuthNet

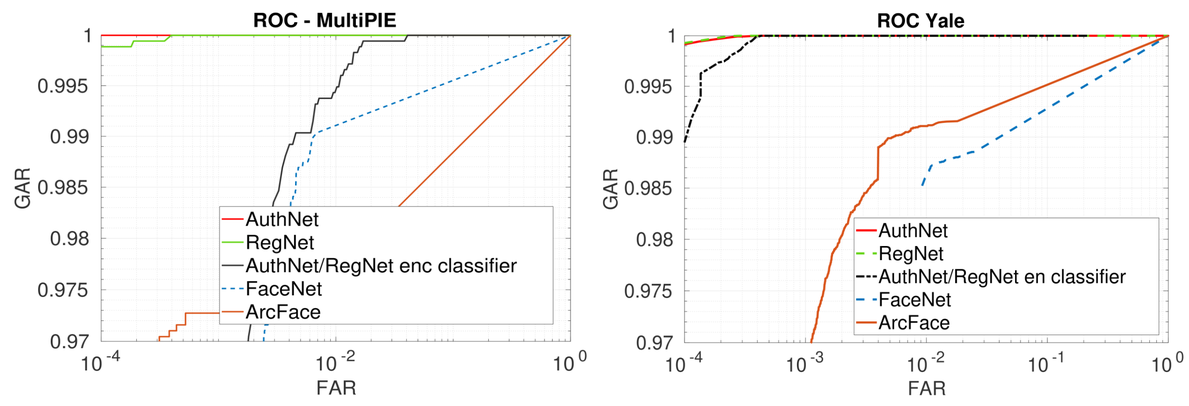


- Using statistical distance model (KL divergence) to enforce desired distributions: RegNet



- Using Siamese networks to compute the distance between faces: BioMetricNet

Results



Future work

- Explore BioMetricNet → novel architectures, fair comparisons
- Robust multi class classification analysis
- Modifying proposed architectures for adversarial attacks robustness

Submitted and published works

- Arslan Ali, Matteo Testa, Tiziano Bianchi, Enrico Magli, *"AuthNet: Biometric Authentication through Adversarial Learning"* in *IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), IEEE, 2019*
- Matteo Testa, Arslan Ali, Tiziano Bianchi, Enrico Magli, *"Learning Mappings onto Regularized Spaces for Biometric Authenticatoin"* in *IEEE 21st International Workshop on Multimedia Signal Processing (MMSP), IEEE, 2019*
- Arslan Ali, Matteo Testa, Tiziano Bianchi, Enrico Magli, *"Adversarial learning of mappings onto regularized spaces for biometric authentication*" submitted to *IEEE Transactions on Information Forensics and Security*
- Arslan Ali, Matteo Testa, Tiziano Bianchi, Enrico Magli, *"BioMetricNet: Deep unconstrained Face Recognition through regularized learning of mapping onto latent space*" targeted submission *IEEE Conference on Computer Vision and Pattern Recognition (CVPR), IEEE 2020*

List of attended classes

- 01SHCRV – Unsupervised neural networks (9/4/2018, 30)
- 01QTEIU – Data mining concepts and algorithms (6/3/2018, 20)
- 01QSAIU – Heuristics and metaheuristics for problem solving (13/7/2018, 20)
- 02LWHRV – Communication (15/2/2018, 5)
- 01PJMRV– Etica informatica(14/3/2018, 20)
- 08IXTRV – Project management (15/2/2018, 5)
- 01RISRV – Public speaking (15/2/2018, 5)
- 02RHORV – The new Internet Society (13/3/2018, 6)
- 01RELKG - Probability applications and machine learning (3/9/2018, 3)
- 01QRQRV - Compressed sensing: theory and applications (30/5/2019, 3)
- 01TEVRV - Deep learning (4/6/2019, 3)

POLITECNICO DI TORINO

PhD program in

Electrical, Electronics and Communications Engineering