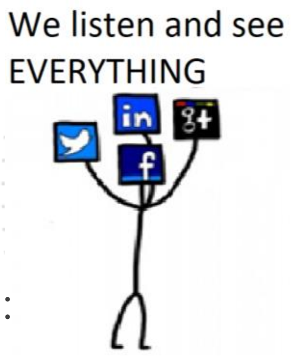
PRIVACY-PRESERVING X-VECTORS SPEAKER VERIFICATION SYSTEM

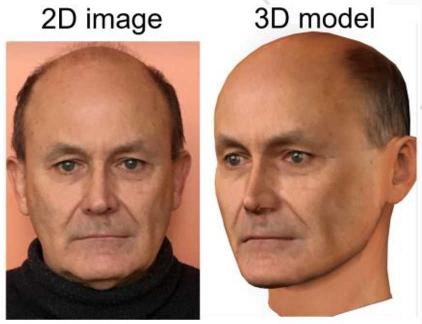
AYMEN MTIBAA,
DIJANA PETROVSKA, JEROME BOUDY,
AHMED BEN HAMIDA

PROBLEMS RELATED TO BIOMETRIC SYSTEMS

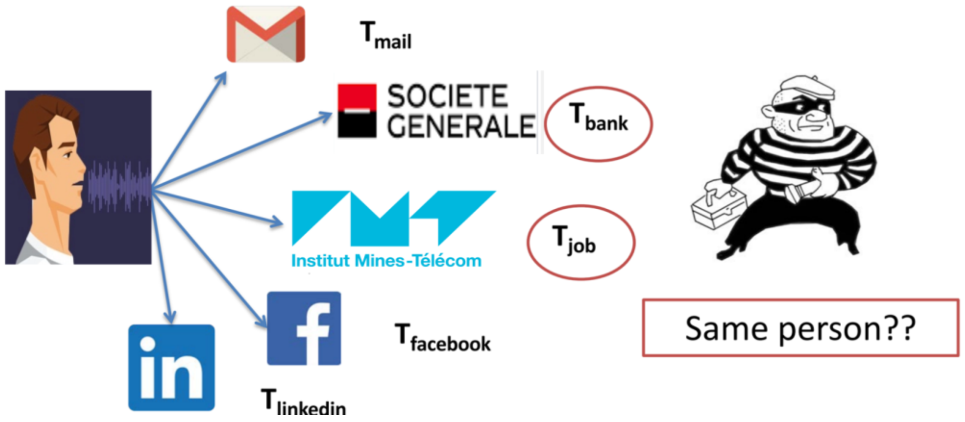


- Biometric data are not private: **PUBLIC**

- Biometric data are permanent, unlike passwords, cannot be changed: **No-Revocability**



- Biometric reference stored in different applications for one user could be cross-linked: **linkability**



OBJECTIVE

- Develop a privacy-preserving speaker verification system that performs the biometric verification while preserving user privacy.

- Achieve the biometric information protection requirements:

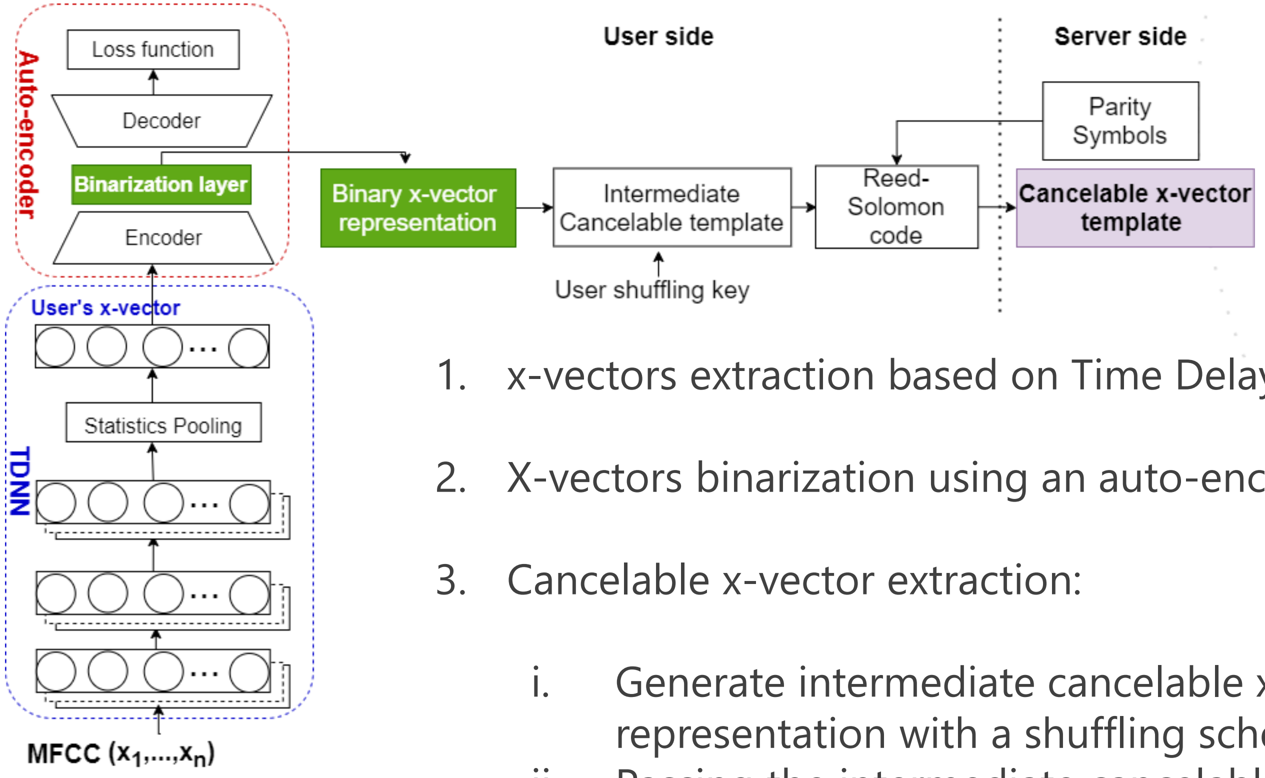
  Revocability

  Unlinkability

  Irreversibility

  Maintain the biometric performance

DESCRIPTION OF THE PROPOSED PRIVACY-PRESERVING X-VECTORS SYSETM



1. x-vectors extraction based on Time Delay Neural Networks (TDNN)

2. X-vectors binarization using an auto-encoder

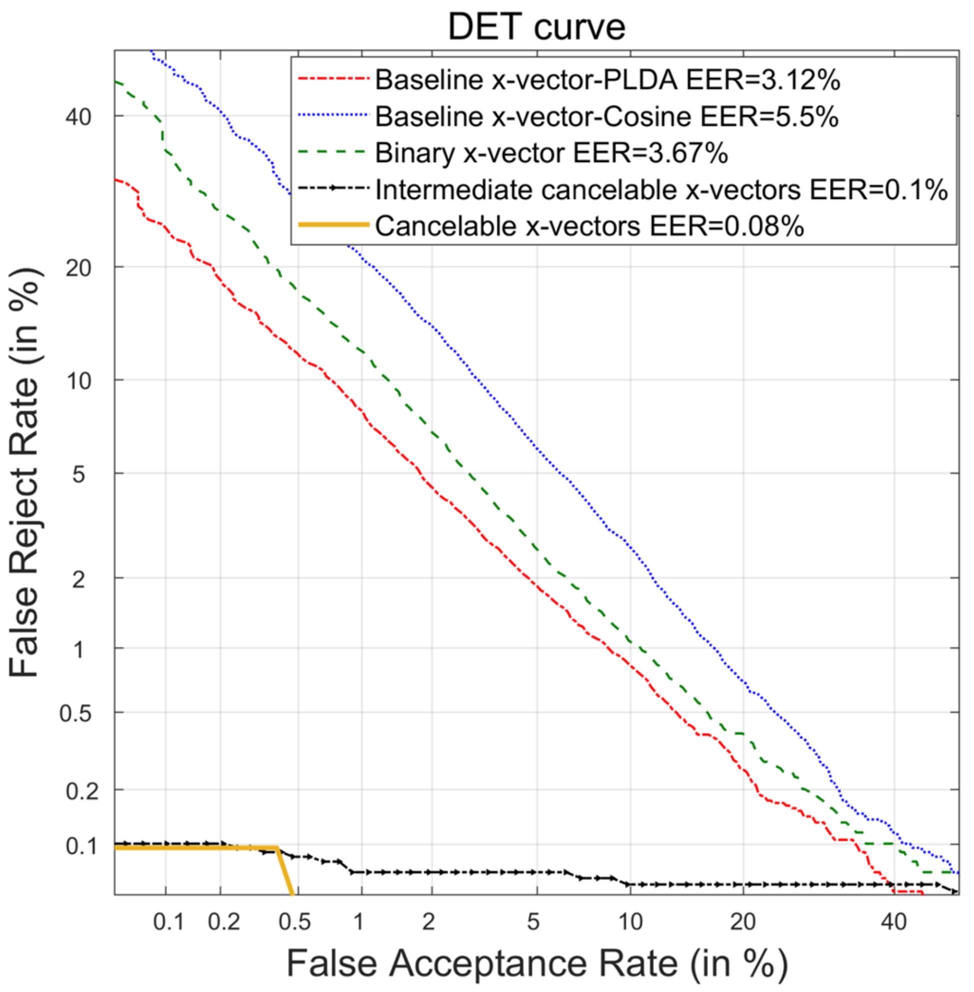
3. Cancelable x-vector extraction:

   i. Generate intermediate cancelable x-vector by protecting the binary representation with a shuffling scheme.
   ii. Passing the intermediate cancelable x-vector through a Reed-Solomon error-correction code.

EVALUATION AND RESULTS

The evaluation was performed on the test set of VoxCeleb1 text-independent database

- ✓ Improves the biometric performance
- ✓ Unlinkability
- ✓ Revocability
- ✓ Irreversibility
- ✓ Robust to different attack scenarios



CONCLUSION

The proposed privacy-preserving speaker verification system:

- ✓ Achieves the privacy requirements (revocability, Unlinkability, irreversibility) according to the standard ISO/IEC 24745 [4] for biometric information protection.
- ✓ Performs speaker verification without revealing the user’s biometric information.
- ✓ Improves the biometric performance compared to the baseline x-vector system.
- ✓ Shows a good level of security against different attack scenarios.