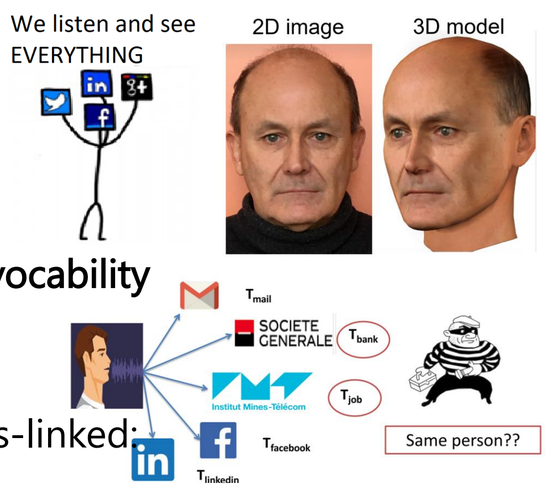
PRIVACY-PRESERVING X-VECTORS SPEAKER VERIFICATION SYSTEM

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

I. PROBLEMS

1. Biometric data are not private: **PUBLIC**
2. Biometric data are permanent, unlike passwords, cannot be changed: **No-Revocability**
3. Biometric reference stored in different applications for one user could be cross-linked: **linkability**

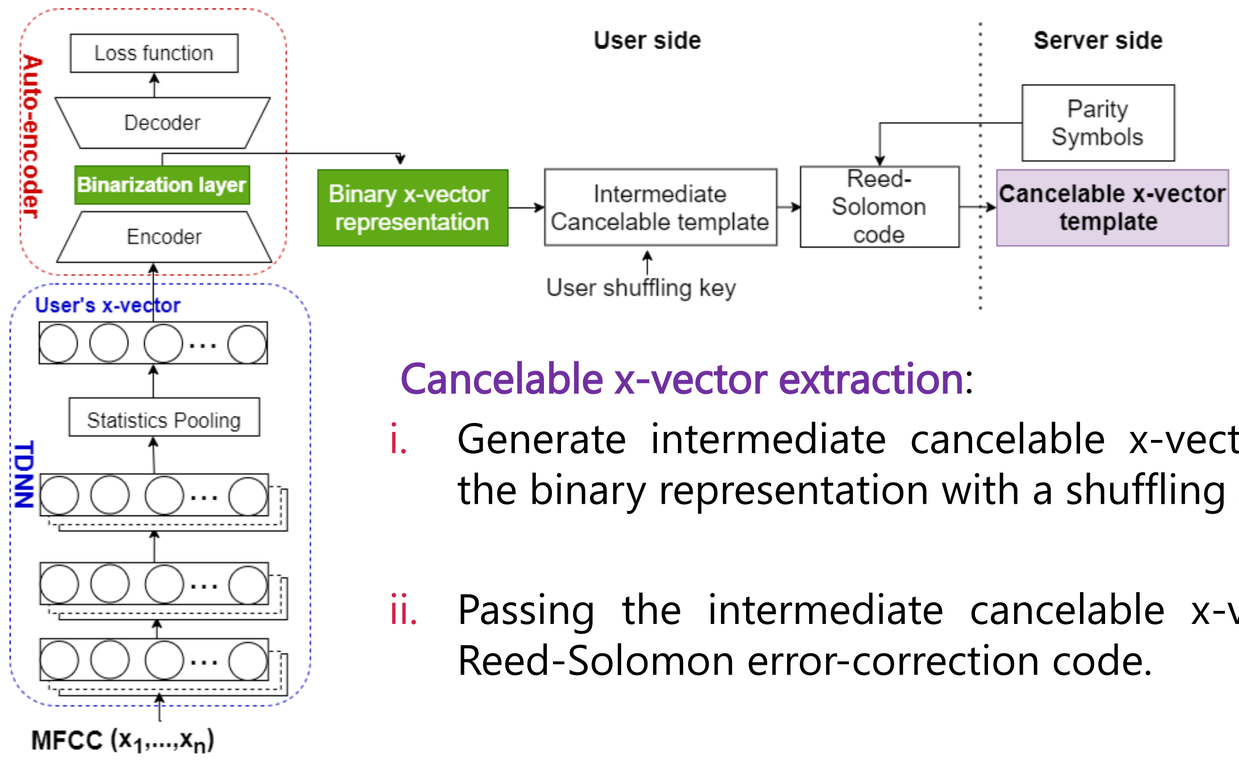


II. OBJECTIVE

1. Develop a privacy-preserving speaker verification system that performs the biometric verification while preserving user privacy.
2. Achieves the biometric information protection requirements:
   - Revocability
   - Unlinkability
   - Irreversibility
   - Maintain the biometric performance

III. PIPELINE OF OUR PRIVACY-PRESERVING X-VECTOR SPEAKER VERIFICATION SYSTEM

x-vectors extraction and **binarization** using an autoencoder on top of a Time Delay Neural Networks (TDNN) [1].



Cancelable x-vector extraction:

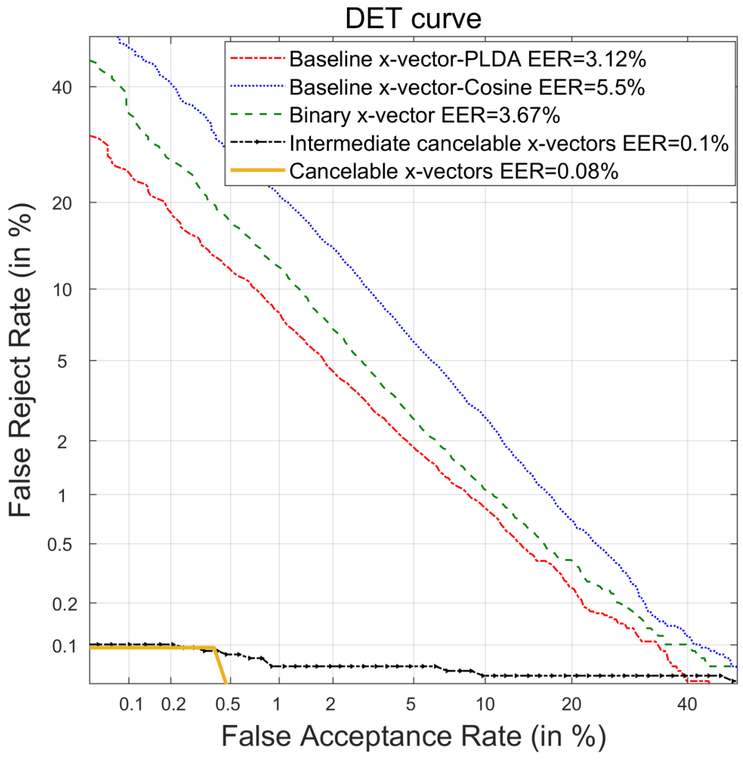
i. Generate intermediate cancelable x-vector by protecting the binary representation with a shuffling scheme [2].

ii. Passing the intermediate cancelable x-vector through a Reed-Solomon error-correction code.

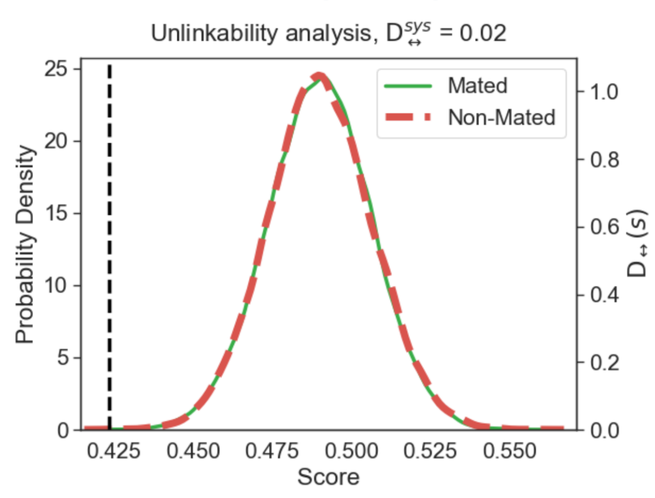
IV. EVALUATION AND RESULTS

The evaluation was performed on the test set of VoxCeleb1 text-independent database [3]

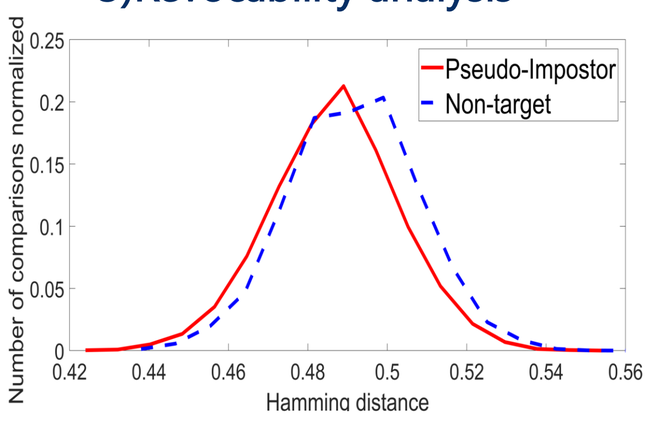
1) Biometric performance evaluation



2)Unlinkability analysis



3)Revocability analysis



4) Security analysis

FAR stolen biometric =0
FAR brute force = 0
FAR stolen shuffling key =1.94%

V. CONCLUSIONS

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.

REFERENCES:

[1] D. Snyder, D. Garcia-Romero, D. Povey, and S. Khudanpur, "Deep neural net-work embeddings for text-independent speaker verification." inInterspeech,2017, pp. 999–1003
[2] Mtibaa, Aymen, et al. "Privacy-preserving speaker verification system based on binary I-vectors." IET Biometrics 10.3 (2021): 233-245.
[3] A. Nagrani, J. S. Chung, and A. Zisserman, "Voxceleb: a large-scale speakeridentification dataset," inINTERSPEECH, 2017
[4] ISO/IEC JTC1 SC27 Security Techniques,ISO/IEC 24745:2011. Informa-tion Technology - Security Techniques - Biometric Information Protection,International Organization for Standardization, 2011.

Contact aymen.mtibaa@telecom-sudparis.eu

Partners:
This work is partially supported by the Empathic project that received funding from the European Union's Horizon 2020 research and innovation program, under Grant Agreements N: 769872