Use of biometrics for regeneration of cancelable post-quantum crypto-biometric keys

Organization:

Institut Mines-Télécom

TELECOM SudParis

samovar UMR 5157

Supervisors

Dijana Petrovska Delacrétaz

Bernadette Dorizzi

PhD student

Mohamed Amine HMANI

Funding

H2020

SPEECHXRays

Project Empathic

Contact :
mohamed.hmani@telecom-sudparis.eu

1. Motivation

The goal of this work is to create cryptographic keys from biometric data that are resistant to quantum computing. The work is motivated by the advances in Quantum computing. For example, Groover algorithm reduces the security of symmetric keys by half.

2. Goal

Our goal is to create symmetric keys with at least 400-bit entropy.

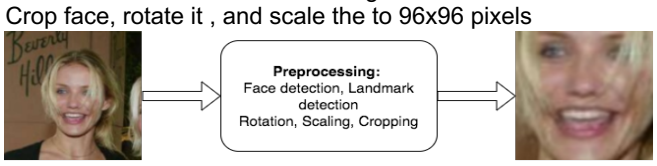
3. Plan

5. Face verification system

Based on openFace project

Preprocessing

- Face and landmark detection using DLIB
- Crop face, rotate it , and scale the to 96x96 pixels



DNN architecture

- Based on the FaceNet architecture
- # Layers : 24
- # parameters : 3 733 968

Learning goal

The goal of the training phase is to obtain the best representation that separates the positives identities from negatives using triplet embedding

Triplet selection constraint

$$\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha > 0$$

x^a_i: anchor sample, x^p_i: positive sample, x^n_i: negative sample, α: margin

Triplet Loss Function

$$L(\theta) = \sum_i^N \left[\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha\right]$$

L: loss function, x^a_i: anchor sample, x^p_i: positive sample, x^n_i: negative sample, α: margin

6. Binarization

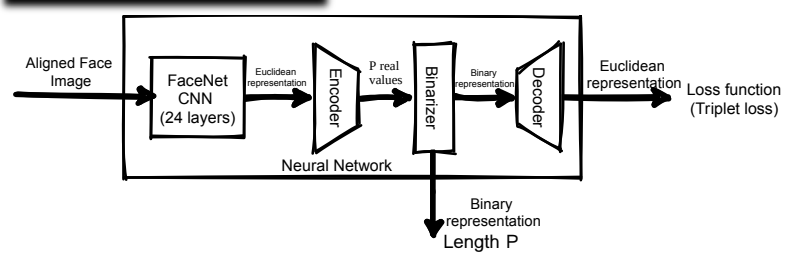


Table2 : Biometirc recognition Performance of the binary representations

Length	Accuracy on LFW	Mobio Eval Female (HTER)	Mobio Eval Male (HTER)
Pretrained CNN (OpenFace)	99.22 %	3.94 %	1.15 %
128	97.3	6.00	2.48
256	97.5	5.00	1.35
512	98.8	4.34	1.51
1024	**99.12**	**5.26**	**1.27**
2048	99.00	4.32	1.33
4096	99.00	4.29	1.38

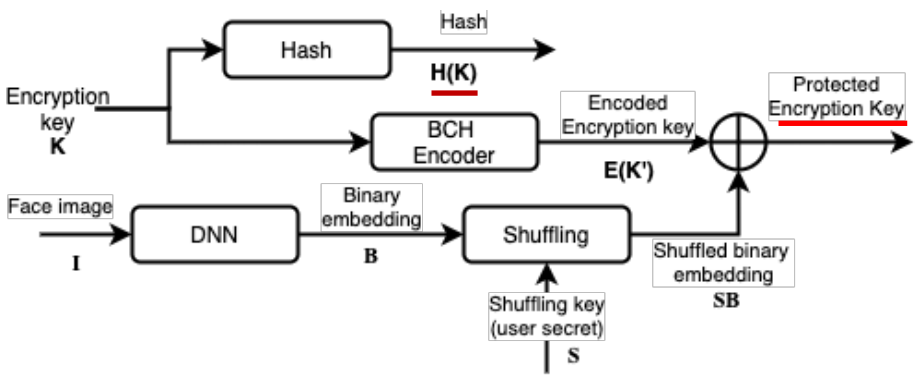
4. Datasets

Table1 : Datasets used for the training and evaluation of the DNN model

Database	Number of subjects	Number of images	Usage
MS-celeb-1M	99 892	8 million	Training DNN models
LFW	5 750	13 320	Performance evaluation
MOBIO	150	18 000	Performance evaluation

7. Cryptographic key regeneration

Enrolment



Key regeneration

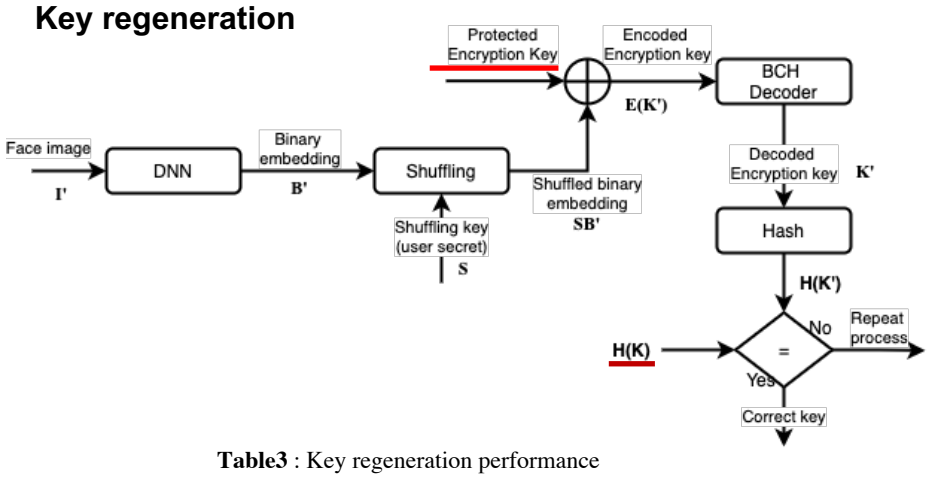


Table3 : Key regeneration performance

Key length (bits)	Encoded Key	T (number of corrections)	FRR MOBIO	FAR MOBIO
516 (86 blocs x 6)	2635 (86 blocs X 31)	602 (86 X 7)	0 %	0.3%
512 (32 X 16)	1008 (16 X 63)	176 (16 X 11)	4 %	0%
510 (51 X 10)	3213 (51 X 63)	663 (51 X 13)	0 %	0.56 %
528 (24 X 22)	3084 (24 X 127)	552 (24 X 23)	0.8 %	0.3 %
420 (28 X 15)	3556 (28 X 127)	756 (28 X 27)	0%	1%
430	2047	214	1.3%	0.3%
430	4095	495	1 %	0.4%

8. Conclusion

- We created and optimized a state-of-the-art face recognition system based on publicly available datasets and open-source tools.
- Innovation in the binarization method.
- Improvement in the length of the symmetric crypto-biometric keys.

9. ACKNOWLEDGMENT

This work is partially supported by the SpeechXRays project that has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 653586 and the EMPATHIC under grant agreement No 769872.

References

[1] M. A. Hmani and D. Petrovska-Delacrétaz, "State-of-the-art face recognition performance using publicly available software and datasets," 2018 4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, Tunisia, 2018, pp. 1-6.

[2] Hmani, M. A., Mtibaa, A., Petrovska-Delacrétaz, D., Bauzou, C., Crucianu, I. (2020). Evaluation of the H2020 SpeechXRays project Cancelable Face System Under the Framework of ISO/IEC 24745:2011. 2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), IEEE

[3] Hmani, M. A., Mtibaa, A., Petrovska-Delacrétaz, D.,. Joining Forces of Voice and Facial Biometrics: a Case Study in the Scope of NIST SRE'19. In Voice Biometrics: Technology, trust and security (chapter 9). IET.