PRIVACY AND DATA PROTECTION IN BIOMETRICS

Author: Daniel Pérez Cabo

Universidad de Vigo

Advisors: Ferando Pérez González
Daniel González Jiménez

Gradiant
GALICIAN RESEARCH AND DEVELOPMENT CENTER IN ADVANCED TELECOMMUNICATIONS

Motivation of the work

Biometrics have emerged as a more secure alternative to passwords and their use is exponentially increasing.

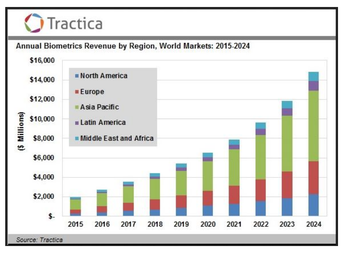


Figure 1: Mobile market estimated revenue for next years

However it is necessary to keep in mind that biometrics may have weaknesses related to users' privacy and security:

- Is it possible for users to cancel and renew their biometric templates?
- Could an attacker be able to infer the biometric sample from the biometric template?
- Could an attacker be able to link a given user through different services?

Biometric systems must handle these issues in order to preserve users' privacy.

Thesis objectives

The main objectives of this thesis are as follows:

1. Understand the fundamentals of biometrics and data protection schemes.
2. Develop a face-based biometric system which achieves state of the art performance and, at the same time, preserves users' privacy. Therefore this objective will be divided in two:
   (a) A **biometric recognition module** with state of the art performance in realistic, large databases.
   (b) A **privacy module** which preserves biometrics performance and meets the privacy characteristics specified at **ISO/IEC 24745**:
   - Unlinkability
   - Revokability
   - Irreversibility

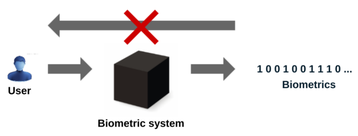


Figure 2: Irreversibility

Research Plan

This thesis will focus on facial biometrics, being the initial research plan as follow:

1. Review the state of the art.
2. Analyze well known approaches for face recognition: hand-crafted features versus deep learning approaches. The goal is to select the approach with the best characteristics to preserve the users' privacy and, at the same time, is able to offer a good biometric security.
3. Design the benchmarks for evaluation of the biometric module.
4. Design and develop the biometric module given the two main objectives: biometric security and privacy.
5. Design benchmarks for evaluation of the privacy module.
6. Design and develop the privacy module scheme.
7. Evaluate the final system and assess fulfilment of thesis objectives.

Figure 3: Popular protection schemes: Fuzzy Extractor (left) and Secure Sketch (right)

Results and discussions

Related to **biometric module**, there are two main conclusions at this point:

- Hand-crafted features have more redundancy than deep learning approaches.

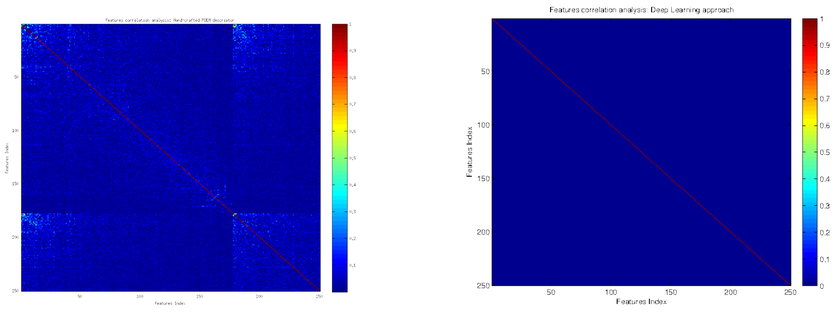


Figure 4: Features correlation analysis: Hand-crafted (left) and deep learning (right)

- Deep learning approaches offer a better output in terms of stability.

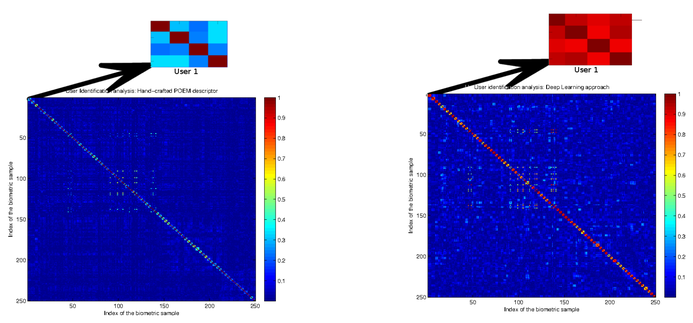


Figure 5: User identification analysis: Hand-crafted (left) and deep learning (right)

Therefore, the next steps will focus on deep learning approaches.

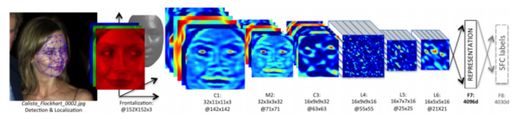


Figure 6: Outline of the DeepFace architecture

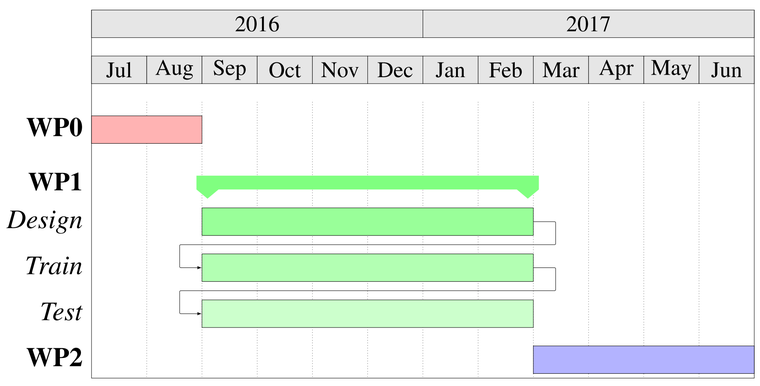
Related to **privacy module**, one problem arises when one tries to analyze the system using cryptography. For instance, are conventional database tests and analysis valid when one wants to estimate the collision probability?

Next Year Planning

WP0: Design the benchmarks and select the databases to test the biometric module.
WP1: In an iterative process. Design, train and test the biometric module, such that it fulfills:

- Intra-class distance as low as possible (**high reliability**)
- Inter-class distance as high as possible (**high discrimination**)

WP2: Approach the problem of collisions from a cryptographic point of view. Try to find and model the worst-case scenarios. This task is motivated by the question raised on "Results and Discussions" paragraph.



References

[1] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, March 2008.

[2] Marc Fischlin and Jean-Sébastien Coron, editors. *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*. Springer, 2016.

[3] Gene Itkis, Venkat Chandar, Benjamin W. Fuller, Joseph P. Campbell, and Robert K. Cunningham. Iris biometric security challenges and possible solutions: For your eyes only?using the iris as a key. *IEEE Signal Process. Mag.*, 32(5):42–53, 2015.

[4] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, pages 28–36, New York, NY, USA, 1999. ACM.

[5] Meng-Hui Lim, Andrew Beng Jin Teoh, and Jaihie Kim. Biometric feature-type transformation: Making templates compatible for secret protection. *IEEE Signal Process. Mag.*, 32(5):77–87, 2015.

[6] Preda Mihailescu. The fuzzy vault for fingerprints is vulnerable to brute force attack. *CoRR*, abs/0708.2974, 2007.

[7] Andreas Nautsch, Hong Hao, Themos Stafylakis, Christian Rathgeb, and Christoph Busch. Towards PLDA-RBM based speaker recognition in mobile environment: Designing stacked/deep PLDA-RBM systems. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2016, Shanghai, China, March 20-25, 2016*, pages 5055–5059, 2016.

[8] O. M. Parkhi, A. Vedaldi, and A. Zisserman. Deep face recognition. In *Proceedings of the British Machine Vision Conference (BMVC)*, 2015.

[9] Enrique Argones Rúa, Josef Kittler, Jose Luis Alba Castro, and Daniel González Jiménez. *Advances in Biometrics: International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006. Proceedings*, chapter Information Fusion for Local Gabor Features Based Frontal Face Verification, pages 173–181. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[10] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. *CoRR*, abs/1503.03832, 2015.

[11] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. Deepface: Closing the gap to human-level performance in face verification. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2014.

[12] Ngoc-Son Vu and Alice Caplier. *Computer Vision – ECCV 2010: 11th European Conference on Computer Vision, Heraklion, Crete, Greece, September 5-11, 2010, Proceedings, Part I*, chapter Face Recognition with Patterns of Oriented Edge Magnitudes, pages 313–326. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.