Protecting Biometric Data Privacy in Facial Recognition and Authentication: The Polyprotect Algorithm Solution

José Silva[1]
recpad2023@silvajose.net
Nuno Gonçalves[23]
nunogon@deec.uc.pt

[1] Institute of Systems and Robotics
University of Coimbra
Coimbra, Portugal

[2] Institute of Systems and Robotics
University of Coimbra
Coimbra, Portugal

[3] INCM Lab
Portuguese Mint and Official Printed Office
Lisbon, Portugal

Abstract

Facial recognition and authentication are techniques that are increasingly being used to guarantee the reliability and privacy of personal data. Their use is aimed at practical application in the most varied areas of everyday life, namely in the use of data in official documents such as passports and ID cards; in the authentication of computer equipment (smartphones, laptops, desktops); and the recognition of official documents with national institutions (social security, finance).

With this goal in mind, we used the face recognition model of Medvedev *et al.* [1] to extract a numerical representation of the face (face embedding), protecting this representation with the Polyprotect algorithm of Hahn and Marcel [2].

Our theoretical and practical contribution to the field of facial recognition and authentication, using Hahn and Marcel's Polyprotect algorithm, associated with Medvedev *et al.*'s facial authentication model, is to ensure enhanced privacy of biometric data.

1 Introduction

Face Recognition technology uses algorithms to recognize a face through facial features, such as the shape of the face, the distance between the eyes, or the position of the nose and mouth. The set of biometric features detected and extracted makes it possible to uniquely recognize a subject, and so a conventional Face Recognition system comprises the tasks of detecting, aligning, representing, and classifying the face [3].

The pipeline produces a numerical representation in a space of biometric features, which corresponds to the mapping of a high-dimensional vector, the face embedding. The distance between the face embeddings indicates whether the faces are similar or different. Identity recognition is provided by distance functions. Thus, if the distance between two face embeddings is above a certain threshold, there is a high similarity between the two samples, and the system concludes that they are the same subject.

Face embeddings can be generated using different algorithms, in particular convolutional neural networks (CNNs). Composed of CNNs, Face Recognition models are trained on large datasets to learn how to extract face embeddings. In this training process, the network parameters are adjusted so that the embeddings represent the biometric characteristics of the face [4].

In light of biometric data protection regulations and policies, face embeddings are considered sensitive data, as they uniquely identify a citizen's face by containing the biometric traits that represent a subject's unique physical characteristics. The use of face embeddings in computer systems can inadvertently make it possible to track users' actions in different applications and digital media.

To solve this privacy problem, algorithms are used to protect biometric characteristics. Our contribution, to protect biometric characteristics, consists of the combined use of the Polyprotect algorithm by Hahn and Marcel [2] and the facial authentication model by Medvedev *et al.* [1]. This new method will use obfuscation techniques, preventing third-party access to biometric characteristics.

2 Background Theory

There are several approaches proposed in the literature to protect biometric characteristics.

Pandey *et al.* [5] proposes a framework that uses features from localized regions of the face to achieve an exact match, then uses conventional hash functions (such as *SHA-256*) to protect the biometric data.

Maiorana *et al.* [6] and Abdellatef *et al.* [7] use bio-convolution, which maintains the privacy of biometric templates without affecting recognition accuracy. In bio-convolving, the sequence of n original biometric features, $r(n)$, is transformed by the function $f(n) = r(n) * d(n)$, where $d(n)$ is the transformation key.

Mohan *et al.* [8] create a representation, which is formed by a maximum entropy binary code (MEB), which provides decoupling with the original biometric data (cancelability). This proposed method does not significantly affect recognition, and guarantees the reproducibility and security of the biometric data.

Rathgeb *et al.* [9] make use of Fuzzy Vaults, where sensitive data is protected using a unique combination of specific biometric characteristics, these characteristics being used as a private key.

Phillips *et al.* [10] propose an authentication algorithm that applies a fusion process to the private keys, which have been generated using the biometric characteristics extracted from users.

Boddeti *et al.* [11] uses a framework based on homomorphic encryption to protect biometric data. The framework preserves user privacy and allows recognition to take place directly in the encrypted domain.

Although these approaches are valid, the Polyprotect method combined with CNN networks shows better results for protecting biometric characteristics, namely because this new method guarantees irreversibility and does not allow the extraction of biometric characteristics by computational means; it allows the revocation of the secure version by replacing the secret key; it has high accuracy in facial recognition on secure data; and finally, it does not degrade the performance of the facial recognition system.

3 Method

The experimental method uses the *MOBIO* dataset and the *VGGFace2* dataset, which constitute a large volume of biometric data of the human face. *MOBIO* is a dataset created by the Idiap Research Institute that was generated using mobile devices, so it provides real samples taken from mobile phone cameras and laptops [12]. The VGGFace2 dataset is a wild dataset made up of ∼3M images, ∼9k classes, ∼360 samples per class (License - CC BY-SA 4.0), and therefore provides a high number of identities.

The experimental process is as follows (see Fig. 1): 1) Face detection and alignment: The initial phase involves the application of an algorithm specialized in face detection, which identifies the facial components and is then used to cut out and align the face region; 2) Generation of embeddings: After the face detection and alignment process, the images are processed by the model of Medvedev *et al.* thus generating an embedding that describes the face denoted by V. This embedding is needed to encode a secure template using Polyprotect; 3) Data obfuscation: The original, unaltered data, V, is split into smaller sets and encrypted by a private key. After transforming the data, we obtain and store its protected

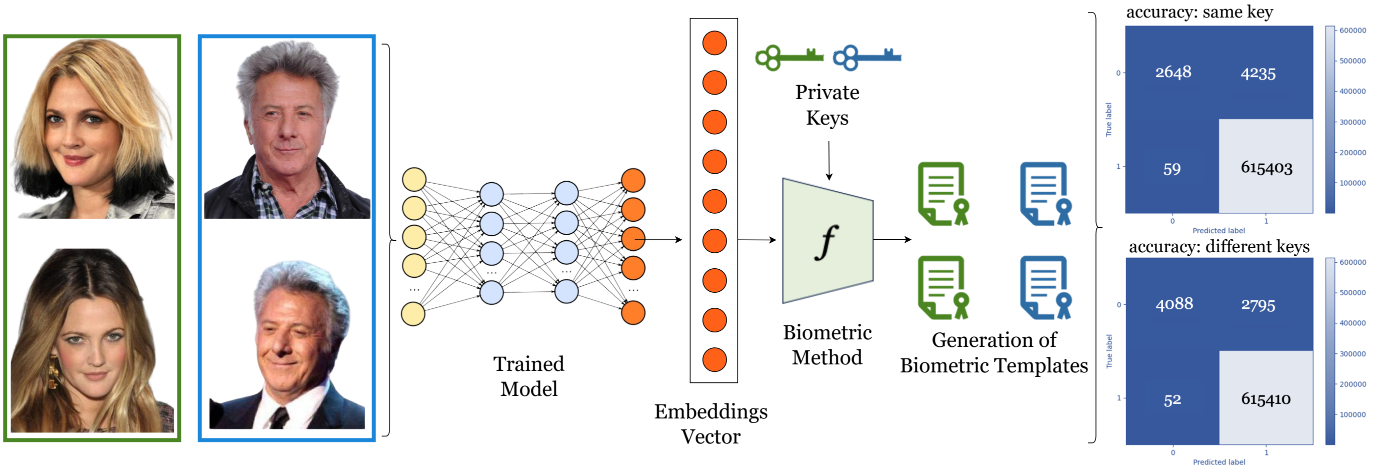

Figure 1: Schematic of the process of generating secure biometric templates from human face images. The pre-trained model extracts the embedding vectors from the face images (the images shown are from the VGGFace2 dataset). Protected templates are built by the protection algorithm, which uses the embedding vectors and the user's key. Results shown when the key is the same and different between the classes in the dataset.

version, which we call P; 4) Comparative analysis: In the final phase, the P protected templates are compared and evaluated in light of the properties of accuracy, irreversibility, and renewability. This evaluation reveals insights into the impact of the transformation and the choice of private key.

By identifying the relevant factors of greatest significance in the protection of biometric data, strategies are developed to improve protection models and algorithms in the field of facial authentication.

4 Results

By identifying the relevant factors of greatest significance in the protection of biometric data, strategies are developed to improve protection models and algorithms in the field of facial authentication.

The generation of keys and the grouping of biometric characteristics affect the various properties of a biometric template, namely accuracy, irreversibility, and revocability. If biometrics are always protected with the same key, the similarity between templates increases, which produces more false positives. On the other hand, if biometrics are protected with different keys, then distinguishability increases, which generates false negatives (see Fig. 1).

To reduce the number of false positives and negatives, and to optimize the degree of irreversibility and revocability of the biometric templates, it will be necessary to run tests and evaluate the choice of initial parameters for the Polyprotect method.

5 Conclusion

In conclusion, the use of Medvedev *et al*. [1] facial recognition model, together with Hahn and Marcel's Polyprotect algorithm [2] guarantees greater privacy of biometric data. This is especially important considering the increasing use of these techniques in different areas of everyday life, such as official documents and authentication on computer equipment and mobile devices. Ultimately, this theoretical and practical approach can significantly contribute to improving the reliability and privacy of personal data.

6 ACKNOWLEDGEMENTS

This work has been supported by Fundação para a Ciência e a Tecnologia (FCT) under the project UIDB/00048/2020. The authors would like to thank the Portuguese Mint and Official Printing Office (INCM) and the Institute of Systems and Robotics - the University of Coimbra for the support of the project Facing2. The research in this paper used the MOBIO Corpus made available by the Idiap Research Institute, Martigny, Switzerland.

References

[1] Iurii Medvedev, Farhad Shadmand, and Nuno Gonçalves. Mordeephy: Face morphing detection via fused classification. *ICPRAM. Lisbon, Portugal*, 2023.

[2] Vedrana Krivokuća Hahn and Sébastien Marcel. Towards protecting face embeddings in mobile face verification scenarios. *arXiv e-prints*, pages arXiv–2110, 2021.

[3] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1701–1708, 2014.

[4] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 815–823, 2015.

[5] Rohit K Pandey and Venu Govindaraju. Secure face template generation via local region hashing. In *2015 international conference on biometrics (ICB)*, pages 299–304. IEEE, 2015.

[6] Emanuele Maiorana, Patrizio Campisi, Julian Fierrez, Javier Ortega-Garcia, and Alessandro Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):525–538, 2010.

[7] Essam Abdellatef, Nabil A Ismail, Salah Eldin SE Abd Elrahman, Khalid N Ismail, Mohamed Rihan, and Fathi E Abd El-Samie. Cancelable multi-biometric recognition system based on deep learning. *The Visual Computer*, 36:1097–1109, 2020.

[8] Deen Dayal Mohan, Nishant Sankaran, Sergey Tulyakov, Srirangaraj Setlur, and Venu Govindaraju. Significant feature based representation for template protection. In *CVPR Workshops*, pages 2389–2396, 2019.

[9] Christian Rathgeb, Johannes Merkle, Johanna Scholz, Benjamin Tams, and Vanessa Nesterowicz. Deep face fuzzy vault: Implementation and performance. *Computers & Security*, 113:102539, 2022.

[10] Tyler Phillips, Xukai Zou, Feng Li, and Ninghui Li. Enhancing biometric-capsule-based authentication and facial recognition via deep learning. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, pages 141–146, 2019.

[11] Vishnu Naresh Boddeti. Secure face matching using fully homomorphic encryption. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10. IEEE, 2018.

[12] Elie Khoury, Laurent El Shafey, Christopher McCool, Manuel Günther, and Sébastien Marcel. Bi-modal biometric authentication on mobile phones in challenging conditions. *Image and Vision Computing*, 32(12):1147–1160, 2014.