Turning a Vulnerability into an Asset: Accelerating Facial Identification with Morphing

P. Drozdowski*†
C. Rathgeb*
C. Busch*

* da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
† Norwegian Biometrics Laboratory, NTNU, Gjøvik, Norway
(pawel.drozdowski, christian.rathgeb, christoph.busch)@h-da.de

Introduction & Motivation

Background
For large-scale biometric systems, the high computational workload and chance of false positives caused by a naïve, brute-force identification (i.e. 1 to N search) algorithm quickly becomes unacceptable as the size of the enrolment database increases.

Contribution
In this work, two hitherto unrelated areas of biometric research are combined in a proof-of-concept manner to facilitate a more efficient search:

1. Computational workload reduction in biometric identification.
2. Facial image morphing.

Experimental Setup

- FERET image database, ICAO compliant images only.
- Face recognition with FaceNet and ArcFace using pre-trained models.
- Cross-validation over 10 folds.
- \( n \in \{2, 4, 8\} \) samples morphed together for the pre-selection using open-source tools.
- \( N = 400 \) enrolled subjects, and varying number \( k \in \{1, \ldots, N\} \) of the pre-selected candidate short-list.
- Evaluation in terms of hit rate (HR), penetration rate (PR), and rank-1 identification rate (RR-1).

Future Work

This proof-of-concept work could be extended, e.g. by considering:

- Other feature extractors and recognition frameworks, particularly commercial off-the-shelf systems.
- Additional morphing techniques and tools.
- Larger datasets.
- Intelligent morphing process (instead of random sample selection).
- Utilising morphing for the purposes of privacy protection.

Acknowledgements

Supported by the German Federal Ministry of Education and Research (BMBF), by the Hessische State Ministry for Higher Education, Research and the Arts (HMWK) within Center for Research in Security and Privacy (CRISP), and the LOEWE-3 BioBiDa Project (594/18-17).