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

ABSTRACT

In recent years, morphing of facial images has arisen as an important attack vector on biometric systems. Detection of morphed images has proven challenging for automated systems and human experts alike. Likewise, in recent years, the importance of efficient (fast) biometric identification has been emphasised by the rapid rise and growth of large-scale biometric systems around the world.

In this paper, the aforementioned, hitherto unrelated, topics within the biometrics domain are combined: the properties of morphed images are exploited for the purpose of improving the transaction times of a biometric identification system. Specifically, morphs of two or more samples are used in the pre-selection step of a two-stage biometric identification system. In a proof-of-concept experimental evaluation using two state-of-the-art open-source facial recognition frameworks it is shown, that the proposed system achieves hit rates comparable to that of an exhaustive search-based baseline, while significantly reducing the penetration rate (and thus the computational workload) associated with the biometric identification transactions.

***Index Terms*—** Biometric identification, Face morphing, Computational workload reduction, Indexing, Pre-selection

1. INTRODUCTION

In recent years, the interest around biometric technologies has been growing steadily. This is evidenced by various market value studies (see *e.g.* [1, 2]), as well as flourishing deployments of national and international systems for purposes of, among others, personal identification, law enforcement, and facilitating elections (see *e.g.* [3, 4, 5, 6]).

In this paper, two hitherto unrelated areas of biometric research are combined:

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

Specifically, facial image morphing, a crucial vulnerability of operational biometric systems is turned into an advantage through which the penetration rate (computational workload) of biometric identification transactions can be significantly reduced. This is achieved by employing a two-stage retrieval approach, which exploits certain properties of morphed facial images.

The remainder of this paper is organised as follows: section 2 introduces the relevant background concepts and the related work. In section 3, the proposed system is described and visualised conceptually. Section 4 presents the experimental setup and the achieved results, while a summary and concluding remarks are given in section 5.

2. BACKGROUND AND RELATED WORK

In this section, the research fields relevant to this paper are briefly introduced: the operation modes of a biometric system and challenges associated with biometric identification (subsection 2.1), and facial images morphing (subsection 2.2).

2.1. Operation Modes of a Biometric System

Biometric systems generally operate in one of two modes:

Verification Resolved in a 1:1 comparison between a biometric probe and the biometric reference of a claimed identity.

Identification No identity claim is made. Thus, in the worst case, an exhaustive linear search is required in order to find a candidate list or to reach a decision with the rank one on the list.

The second case is obviously more challenging from the practical point of view. However, the naïve approach of the exhaustive search suffers from two key issues:

Computational cost The growing number of enrolled subjects, gradually slows down the response times, which in turn requires investment into optimisations and/or hardware architecture.

False positives costs The probability of at least one false positive (P_N) occurring in a identification scenario is: $P_N = 1 - (1 - P_1)^N$, where N is the number of enrolled subjects and P_1 the false positive probability of a one-to-one template comparison (see Daugman [7]). This relationship is very demanding – even for systems

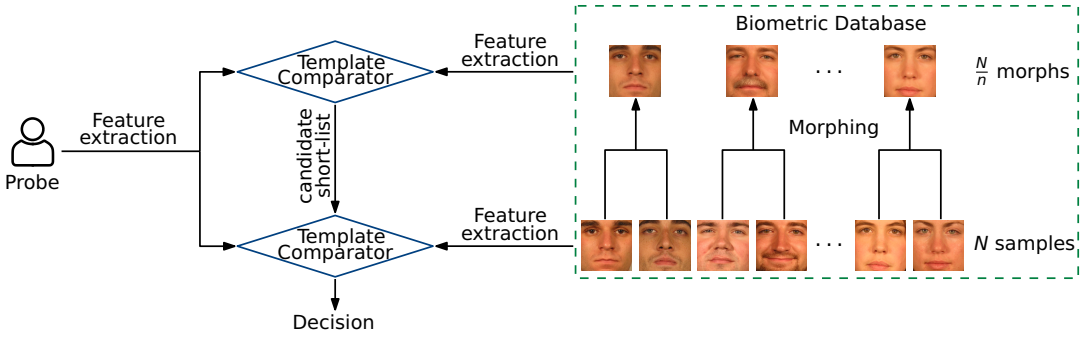

Fig. 1: Proposed system overview (here, $n = 2$)

which perform extremely well in verification mode (*i.e.* have low P_1), the value of P_N very quickly becomes unacceptably high, as the number of enrolled subjects N increases.

Performing accurate and efficient biometric identification (*i.e.* not by an exhaustive search) has been stated to be one of the important, unsolved issues in the biometrics field in general by Daugman, the inventor of iris recognition in a recent interview [8]. Over time, many approaches have been developed in this field; for more insights, the reader is referred to surveys by *e.g.* Proença *et al.* [9], Schuch *et al.* [10], and Kavati *et al.* [11].

2.2. Morphing of Facial Images

By using image morphing methods, it is possible to create biometric samples which *contain biometric information from two or more distinct data subjects*. The resulting artificial sample resembles the two (or more) original samples in the image and feature domain; thus, breaking the unique link between data subjects and their biometric reference data (*i.e.* the enrolment record). In other words, the subjects whose biometric samples were used to create the morphed image can both be matched (accepted) during subsequent biometric recognition transactions with the morphed reference image. This vulnerability was first introduced by Ferrara *et al.* [12] (the so-called "magic passport") and shown to be a feasible attack vector against automated systems and human experts alike [13]. A typical morphing process includes:

1. Facial landmark detection and triangulation in two or more images.
2. Landmark averaging to a single set of landmarks.
3. Image warping and alpha blending.

The process is quite simple, and even non-experts can generate realistic looking morphed face images with a variety of inexpensive or even free software tools. Figure 2 shows an example of facial image morphing.

In recent years, significant research effort has been devoted to development of methods capable of automatically

(a) Subject 1 (b) Morph (c) Subject 2

Fig. 2: Morphing example (from Scherhag *et al.* [14])

detecting morphed images. Among others, methods based on general purpose texture descriptors (*e.g.* Scherhag *et al.* [14]), deep learning (*e.g.* Seibold *et al.* [15]), media forensics (*e.g.* Hildebrandt *et al.* [16]), and camera noise (*e.g.* Debiasi *et al.* [17]) have been proposed. For more detailed treatment of morph creation and detection methods, the reader is referred to a recent survey by Makrushin *et al.* [18]. It is not the intention of this paper to develop morphing detection algorithms; instead, the goal is to take advantage of morphing in the context of a biometric identification system.

3. PROPOSED SYSTEM

Figure 1 shows a conceptual view of the proposed system. Following symbols are used:

N the number of enrolled subjects.
n the number of samples contributing to a morph.
k the number of morphs in the selected candidate short-list.

The key idea is to perform a fusion of the enrolled samples on image level through morphing. Each thus created image contains biometric information from multiple subjects (recall subsection 2.2). The morphed images are expected to retain enough discriminative power, so that upon retrieval the comparison score of a biometric against the correct (mated) morphed image will tend to be better than scores against other (non-mated) morphs. It would then possible to select a candidate short-list based on the comparison scores between the

biometric probe and the morphs. Hence, a biometric identification transaction proceeds in a two-stage process (conceptually similar to *e.g.* Gentile *et al.* [19]):

1. Perform template comparisons between the biometric probe and the enrolled morphed samples exhaustively. Based on the comparison scores, pre-select a short-list of the most likely candidates.
2. Within the candidate short-list, perform template comparisons between the biometric probe and the normal enrolled samples.

In order for the system to reduce the computational workload associated with an identification transaction, the following relation must be satisfied: $\frac{N}{n} + k * n < N$. Figure 3 visualises this relation between the parameters n and k, and the number of necessary comparisons for a biometric identification transaction for $N = 400$ subjects. The baseline (exhaustive search), which is not dependent on those parameters is plotted as a horizontal line for reference.

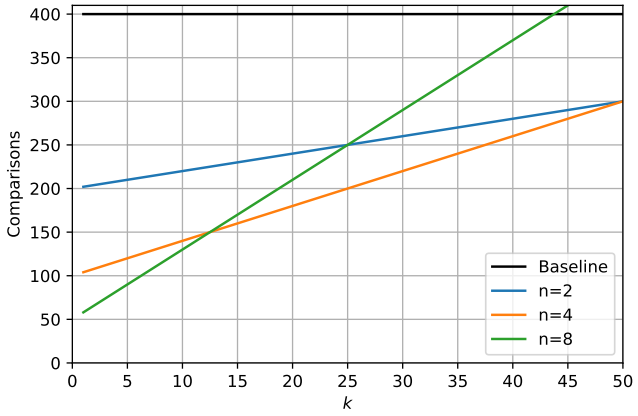

Fig. 3: Template comparisons per identification transaction

4. EXPERIMENTS

In this section, the experimental setup and the used dataset are described (subsection 4.1), along with the results of the experiments (subsection 4.2).

4.1. Experimental Setup

The experiments are conducted using the FERET facial image database [20], which contains 14126 images from 1199 data subjects (with varying number of images per subject). Specifically, frontal images compliant with the ISO/IEC requirements [21] for high quality facial images have been selected, resulting in a subset consisting of 6963 images from 573 subjects. The morphed images were automatically generated from pairs of images using landmark detection by dlib [22], Delaunay triangulation [23], and image warping and alpha blending as described in [24]. The alpha value is always set to $\frac{1}{n}$, *i.e.* the samples contribute equally to the morph.

Two state-of-the-art open-source facial recognition frameworks based on deep neural networks were used: FaceNet [25] and ArcFace [26], both with the pre-trained models provided by their authors. The frameworks extract feature vectors (embeddings) from the non-morphed and morphed facial images consisting of 512 float values, which can be subsequently compared using metrics such as the cosine distance.

The experiments were conducted in the biometric identification mode, utilising cross-validation over 10 folds. The variables mentioned in section 3 are as follows: $N = 400$ (200 men and 200 women; morphs were created within the same gender only, but no other heuristics were used when deciding which samples to morph, *i.e.* they were selected at random), $n \in \{2, 4, 8\}$, and $k \in \{1 \dots \frac{N}{n}\}$. Thus, for each experiment, several thousand identification transactions are performed (depending on the enrolled subjects, since the number of samples per subject in the dataset varies). The biometric performance is evaluated in terms of metrics defined by ISO/IEC [27]: hit rate (HR)[1], penetration rate (PR), and rank-1 identification rate (RR-1).

4.2. Results

The accuracies achieved by various configurations of the proposed system in the pre-selection step are shown in table 1 and figure 4, where the trade-off between hit rate and penetration rate is plotted. Best results for the high hit rates ($\geq$99%) are achieved using the ArcFace feature extractor, whereby the penetration rate is approximately halved. The FaceNet feature extractor achieves significantly poorer results, albeit it still manages to reduce the penetration rate somewhat. It can also be observed, that enough biometric information for high hit rates and penetration rate reduction is retained even when morphing $n = 8$ subjects together, although the best results occur when $n = 2$ or $n = 4$.

Table 1: Pre-selection results

Feature Extractor	n	PR at		
		95% HR	**99% HR**	**99.5% HR**
ArcFace	2	50.5%	52.0%	55.0%
	4	32.0%	48.0%	57.0%
	8	42.5%	70.5%	80.5%
FaceNet	2	57.0%	86.0%	95.0%
	4	42.5%	70.5%	80.5%
	8	60.5%	86.5%	94.5%

The results achieved by the baseline and the two-stage system (with optimal k values) are shown in tables 2 and 3, respectively. All the results are reported with a 95% confidence interval. It is observed, that particularly for the ArcFace feature extractor virtually no biometric performance loss occurs at $n = 2$, while the penetration rate is significantly reduced.

[1] *i.e.* 100% minus the pre-selection error rate.

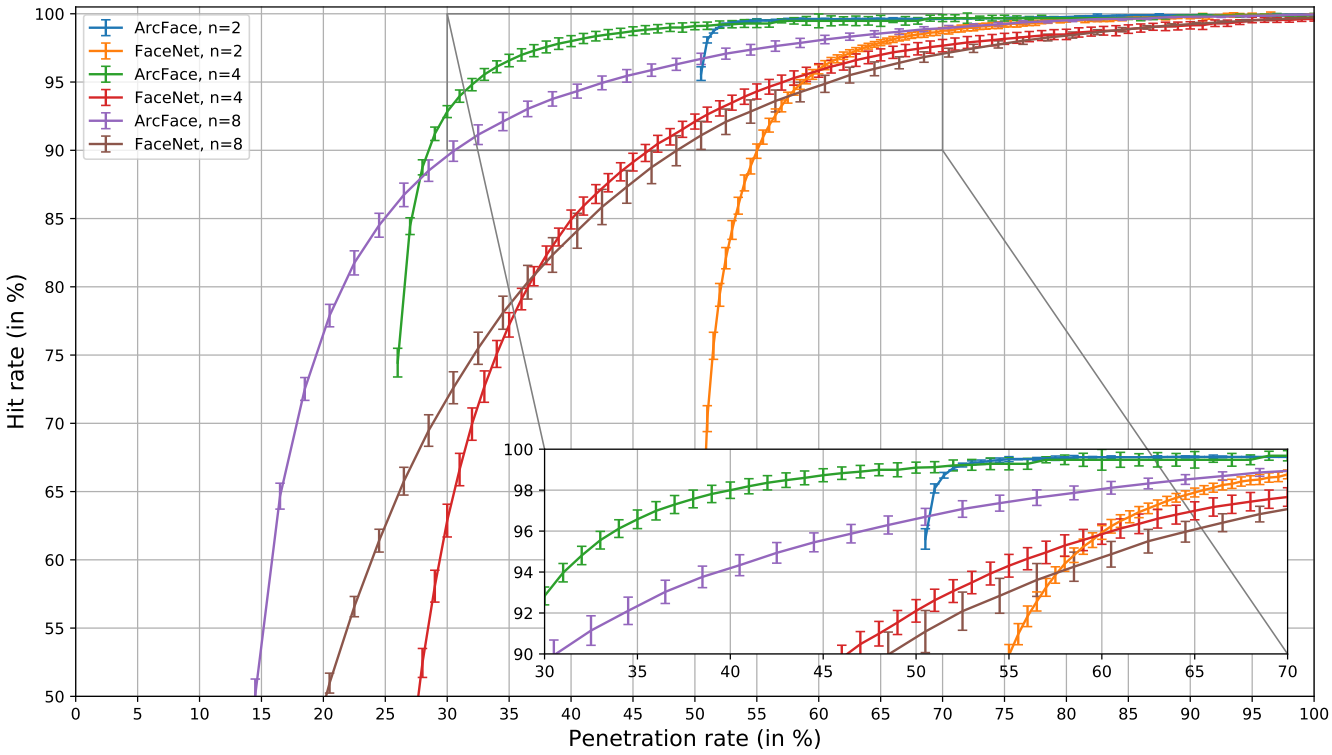

Fig. 4: Results (with errorbars denoting the 95% confidence interval)

Table 2: Baseline results

Feature Extractor	RR-1	PR
ArcFace	99.18% ± 0.11%	1.0
FaceNet	98.84% ± 0.16%	

Table 3: Two-stage system results

Feature Extractor	n	k	RR-1	PR
ArcFace	2	5	98.82% ± 0.12%	52.5%
	4	20	97.57% ± 0.26%	45.0%
	8	25	96.09% ± 0.19%	50.0%
FaceNet	2	30	96.97% ± 0.31%	65.0%
	4	30	93.61% ± 0.56%	55.0%
	8	30	96.51% ± 0.26%	72.5%

5. SUMMARY

In this paper, two heretofore unrelated fields within the domain of biometrics have been combined. Specifically, the properties of morphed facial images have been used at the pre-selection step of a two-stage biometric identification system. It has been shown, that through the morphing process of two or even more data subjects, enough biometric information is retained to facilitate an accurate pre-selection of a candidate short-list. The experiments with two state-of-the-art open-source deep facial recognition frameworks show high (≥99%) hit rates, while reducing the associated penetration rates (and thus the computational workload) down to around 50% of the baseline system. Future work could consist of a more comprehensive evaluation extending this proof-of-concept study, for example utilising:

- Other feature extractors and recognition frameworks, particularly commercial off-the-shelf systems.
- Additional morphing techniques and tools.
- Larger datasets.

Furthermore, improvements to the morphing process of the enrolled samples could be attempted – for instance, morphing most similar subjects together, rather than doing so randomly. Lastly, the morphed images could possibly be organised into a tree-like hierarchical search structure with the aim of further reducing the search space. One technical limitation of the proposed method is that it requires frontal images of good quality, albeit in practice such images are already being captured in data acquisition with controlled environment and cooperative data subjects (*e.g.* passport issuance).

6. ACKNOWLEDGMENTS

This work was partially supported by the German Federal Ministry of Education and Research (BMBF), by the Hessen 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).

7. REFERENCES

[1] Global Market Insights, "Biometrics market size by application," Tech. Rep. GMI493, August 2017.

[2] Markets and Markets, "Biometric system market by authentication type - global forecast to 2023," Tech. Rep. SE 3449, July 2018.

[3] UIDAI, "Role of biometric technology in Aadhaar enrollment," Tech. Rep., January 2012.

[4] eu-LISA, *Biometrics in Large-Scale IT*, 2015.

[5] FBI, "CODIS statistics," `https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics`.

[6] Consortium for Elections and Political Process Strengthening, "Assessment of electoral preparations in the Democratic Republic of the Congo," May 2018.

[7] J. Daugman, "Biometric decision landscapes," Tech. Rep. UCAM-CL-TR-482, University of Cambridge - Computer Laboratory, January 2000.

[8] Institute of Electrical and Electronics Engineers, "Biometric council newsletter," November 2015.

[9] H. Proença and J. C. Neves, *Iris biometric indexing*, pp. 101–124, Security. Institution of Engineering and Technology, 2017.

[10] P. Schuch, "Survey on features for fingerprint indexing," *IET Biometrics*, 2018.

[11] I. Kavati, M. Prasad, and C. Bhagvati, "Search space reduction in biometric databases: a review," in *Computer Vision: Concepts, Methodologies, Tools, and Applications*, pp. 1600–1626. IGI Global, 2018.

[12] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Intl. Joint Conf. on Biometrics (IJCB)*. September 2014, IEEE.

[13] M. Ferrara, A. Franco, and D. Maltoni, "On the effects of image alterations on face recognition accuracy," in *Face Recognition Across the Imaging Spectrum*, pp. 195–222. Springer, 2016.

[14] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "On the vulnerability of face recognition systems towards morphed face attacks," in *Intl. Workshop on Biometrics and Forensics (IWBF)*. April 2017, IEEE.

[15] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in *Digital Forensics and Watermarking*, pp. 107–120. Springer International Publishing, 2017.

[16] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," in *Intl. Workshop on Biometrics and Forensics (IWBF)*. April 2017, IEEE.

[17] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, and C. Busch, "PRNU-based detection of morphed face images," in *Intl. Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2018.

[18] A. Makrushin and A. Wolf, "An overview of recent advances in assessing and mitigating the face morphing attack," in *European Signal Processing Conference (EUSIPCO)*. 2018, IEEE.

[19] J. E. Gentile, N. Ratha, and J. Connell, "An efficient, two-stage iris recognition system," in *Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*. 2009, pp. 211–215, IEEE.

[20] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Trans. on pattern analysis and machine intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.

[21] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 19794-5:2011. Information technology – Biometric data interchange formats – Part 5: Face image data*.

[22] D. E. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, 2009.

[23] D.-T. Lee and B. J. Schachter, "Two algorithms for constructing a Delaunay triangulation," *International Journal of Computer & Information Sciences*, vol. 9, no. 3, pp. 219–242, 1980.

[24] S. Mallick, "Face morph using OpenCV – C++ / Python," https://www.learnopencv.com/face-morph-using-opencv-cpp-python/, March 2016.

[25] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Conf. on Computer Vision and Pattern Recognition (CVPR)*. 2015, pp. 815–823, IEEE.

[26] J. Deng, J. Guo, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," *arXiv:1801.07698*, 2018.

[27] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, International Organization for Standardization and International Electrotechnical Committee, April 2006.