

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

Arc2Morph: Identity-Preserving Facial Morphing with Arc2Face

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

Domenico, N.D., Franco, A., Ferrara, M., Maltoni, D. (2026). Arc2Morph: Identity-Preserving Facial Morphing with Arc2Face. Institute of Electrical and Electronics Engineers Inc. [10.1109/fg67764.2026.11557008].

Availability:

This version is available at: <https://hdl.handle.net/11585/1070910> since: 2026-07-07

Published:

DOI: <http://doi.org/10.1109/fg67764.2026.11557008>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

Arc2Morph: Identity-Preserving Facial Morphing with Arc2Face

Nicolò Di Domenico, Annalisa Franco, Matteo Ferrara, Davide Maltoni

Department of Computer Science and Engineering, University of Bologna, Italy

Abstract—Face morphing attacks are widely recognized as one of the most challenging threats to face recognition systems used in electronic identity documents. These attacks exploit a critical vulnerability in passport enrollment procedures adopted by many countries, where the facial image is often acquired without a supervised live capture process. In this paper, we propose a novel face morphing technique based on Arc2Face, an identity-conditioned face foundation model capable of synthesizing photorealistic facial images from compact identity representations. We demonstrate the effectiveness of the proposed approach by comparing the morphing attack potential metric on two large-scale sequestered face morphing attack detection datasets against several state-of-the-art morphing methods, as well as on two novel morphed face datasets derived from FEI and ONOT. Experimental results show that the proposed deep learning-based approach achieves a morphing attack potential comparable to that of landmark-based techniques, which have traditionally been regarded as the most challenging. These findings confirm the ability of the proposed method to effectively preserve and manage identity information during the morph generation process.

I. INTRODUCTION

Face morphing attacks [15] are widely recognized as one of the most challenging threats to Face Recognition Systems (FRSs) used in electronic identity documents. These attacks exploit a critical weakness in the enrollment procedures adopted by many countries, where the facial image is often acquired without a supervised live capture process. Under these conditions, two individuals may collaborate to create a single morphed facial image that combines identity features from both subjects. This image can be presented during the document issuance phase to deceive the human officer responsible for identity verification, resulting in the storage of a double-identity image within the document's chip. The severity of this attack lies in the intrinsic vulnerability of face verification systems [42]: due to the blended nature of the morphed image, it can successfully match against both contributing subjects. Consequently, if the morphing attack is not detected during enrollment, two different individuals may later authenticate as the same identity holder, effectively sharing a single regular identity document. Two conditions must be met for an attack to be successful: (i) the morphed image must convincingly deceive a human examiner by showing high similarity to the document applicant and maintaining strong visual realism, with no noticeable artifacts or defects; (ii) at the same time, the image must also deceive



Fig. 1: Samples of morphed images (center column) generated with our proposed method. On the first row, Accomplice (left column) and criminal (right column) are sourced from the ONOT [11] dataset; on the second row, accomplice and criminal are sourced from the FEI [45] dataset.

the FRS used for automatic identity verification, allowing it to be successfully matched to both individuals.

Since the introduction of face morphing attacks in 2014 [15], significant research efforts have focused on developing effective detection methods. These approaches operate either on a single image, suitable for the enrollment stage, or on an image pair, which is more feasible during identity verification at the borders. In parallel with advancements in detection techniques, face morphing generation methods have also evolved continuously, becoming increasingly sophisticated and harder to detect. Existing morphing techniques can be broadly classified into two main categories [14]. The first category comprises landmark-based approaches, where the morphing process relies on extracting corresponding facial landmarks that are used to geometrically warp the two contributing faces, followed by a texture blending step. The second category includes deep learning-based techniques, which exploit the generative capabilities of neural networks to synthesize a morphed facial image directly from the face images of two different subjects. For a long time, landmark-based approaches were considered the most effective solution, as they can generate high-quality morphed images while reliably preserving the identity information from both contributing subjects. More recently, however, the rapid advancement of deep generative models has significantly increased interest in deep learning-based morphing techniques, which are now capable of producing highly realistic and identity-preserving morphs.

This project received funding from the European Union's Horizon Europe research and innovation program under Grant Agreement No.101121280. This text reflects only the author's views, and the commission is not liable for any use that may be made of the information contained therein. Code available at <https://github.com/MI-BioLab/arc2morph>.

Since identity preservation represents a critical challenge for deep learning-based morphing approaches, this paper investigates the feasibility of leveraging a model specifically designed to capture representative identity features, namely Arc2Face, for face morphing generation (see Figure 1 for some examples). Particular attention is given to the generation of ISO/ICAO compliant images, feasible for a realistic enrollment process, by explicitly controlling some characteristics of the generated image such as the pose and the background. In particular, the main contributions of this work are as follows:

- a novel deep learning-based morphing approach that achieves attack potential comparable to, and in some cases exceeding, that of landmark-based techniques, while clearly outperforming existing State-Of-The-Art (SOTA) deep learning-based morphing methods;
- an extensive evaluation and comparison of several SOTA morphing approaches on both real and synthetic face images, providing an up-to-date overview of the current landscape of morphing attacks;
- the public release of the implementation to ensure full reproducibility and to foster further research on this topic;
- two newly generated datasets of morphed facial images, created using the proposed method and made publicly available to the research community for benchmarking and research purposes.

The following sections provide a brief review of the SOTA in face morphing, followed by a description of the proposed approach and the experimental evaluation carried out to evaluate its effectiveness.

II. RELATED WORKS

The literature includes a wide range of face morphing approaches which can be classified into two main categories: landmark-based or deep learning-based [14], [44], [46] methods.

A. Landmark-based approaches

Landmark-based face morphing approaches synthesize smooth and gradual transformations between two facial images by relying on facial landmarks extracted from the input images. These landmarks are typically detected using publicly available models, such as DLib [31], and correspond to salient facial features (e.g., eyes, nose, mouth, and eyebrows) and are used to approximate the shape and structure of the face. The morphing process is generally realized through a combination of geometric warping and texture blending. Specifically, image warping is applied to align the facial geometry of the two subjects according to the extracted landmarks, while texture blending merges their visual appearance to produce a coherent morphed image [17], [16]. One of the main advantages of these methods is the high degree of control they offer over the resulting identity, as the transformation can be explicitly guided by the precise positioning of facial features. However, the quality of landmark-based morphed images strongly depends on the

accuracy of landmark detection. In case where landmarks are imprecise or absent, visual artifacts often appear, particularly around critical facial areas such as the eyes, nose, and mouth. To address these limitations, recent research efforts have increasingly focused on the development of post-processing methods aimed at automatically removing visible artifacts [5], [10], [54], [49], [48], as well as on improved morphing approaches able to produce higher-quality and artifact-free images [32], [2].

B. Deep learning-based approaches

Deep-learning-based face morphing approaches aim to generate morphed images while avoiding the artifacts typically associated with landmark-based methods. These techniques exploit the generative capabilities of models such as Generative Adversarial Networks (GANs) and, more recently, diffusion models, to synthesize morphed faces by jointly sampling from the latent representations of the two contributing facial images. Generally, these methods achieve high visual quality; however, they often provide less explicit control over the resulting identity and may still introduce artifacts, typical for instance of GAN-based generation.

MorGAN [6] represents one of the earliest GAN-based face morphing methods and is inspired by the Bidirectional Generative Adversarial Network (BiGAN) architecture [12], which introduces an encoder to map images into a latent space. By jointly discriminating image-latent pairs, the BiGAN framework encourages the encoder to invert the generator, MorGAN adapts this idea to enable face morph generation. Despite its conceptual relevance, MorGAN is constrained by the low resolution of the generated images (64×64 pixels), which is insufficient to satisfy ISO/ICAO quality standards [26], [27], [29], [28]. To overcome this limitation, subsequent work focused on the generation of high-resolution morphed images (up to 1024×1024 pixels) using StyleGAN [47]. In this approach, facial images are first embedded into StyleGAN's latent space via a mapping network, after which morphing is performed by computing a weighted combination of the latent codes corresponding to the two subjects. The resulting latent representation is then passed through the synthesis network to generate high-quality morphed images. This methodology was further refined by MIPGAN (Morphing through Identity Prior driven GAN) [52], which incorporates an identity-preserving loss to better retain the biometric characteristics of the contributing subjects. More recent deep learning-based morphing approaches generally follow a common pipeline consisting of three main stages: (i) encoding the input images into a latent representation, (ii) interpolating the corresponding latent codes, and (iii) decoding the interpolated representation to generate the finale morphed image. The MorCode approach [39] exploits a Vector Quantized GAN (VQGAN) architecture for the encoding/decoding stage. The recent LADIMO algorithm [21] exploits the generative power of diffusion models, relying on a Latent Diffusion Model (LDM)-based framework [43] designed to invert biometric MagFace [33] templates and generate morphed images through spherical

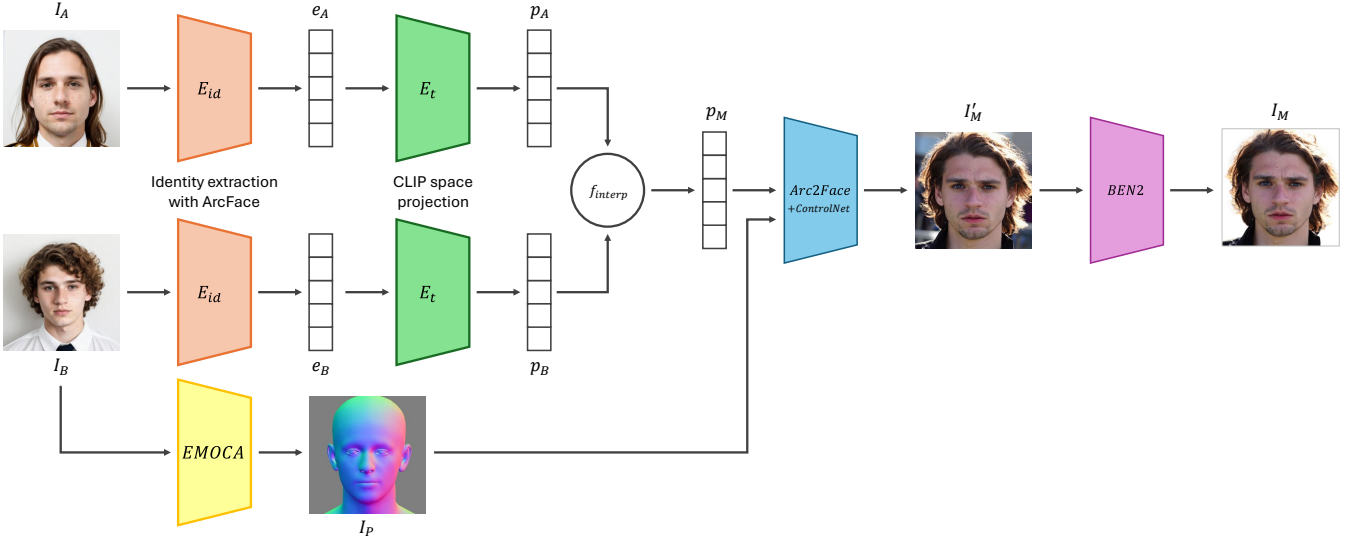


Fig. 2: Overview of the proposed method. The input images I_A and I_B are encoded by the identity encoder $E_{id}(\cdot)$ to produce identity embeddings e_A and e_B . In parallel, we use EMOCaV2 [7], [19] to extract the pose conditioning image I_P for Arc2Face. e_A and e_B are then mapped to the CLIP latent space and interpolated to obtain p_M , which is decoded together with I_P to generate the morphed image I'_M . Finally, BEN2 is used to remove the background from I'_M , yielding the final morphed image I_M .

linear interpolation.

III. PROPOSED METHOD

Inspired by recent advances in conditional synthetic face generation, we propose a novel face morphing framework based on Arc2Face [37], an identity-conditioned face foundation model capable of synthesizing photorealistic facial images from compact identity representations.

A. Arc2Face generation pipeline

Arc2Face leverages ArcFace [8] embeddings as semantic identity priors to enable controllable, identity-preserving image generation. Given a reference facial image I , Arc2Face extracts a normalized 512-dimensional identity embedding with a pretrained ArcFace encoder $E_{id}(\cdot)$, i.e., $e = E_{id}(I)$. This embedding is then projected into CLIP’s [41] multimodal latent space via a modified text encoder $E_t(\cdot)$.

The identity embedding is injected into a fixed prompt, “photo of a $\langle id \rangle$ person”, where $\langle id \rangle$ denotes a padded version of the ArcFace embedding. The encoder outputs token embeddings $(e_1, e_2, e_3, e_{id}, e_5)$, explicitly encoding identity in the textual conditioning. The resulting CLIP representation $p = E_t(e)$ serves as the semantic conditioning signal for image synthesis.

Arc2Face can also be combined with ControlNet [53] to further condition generation on pose and facial expression using a target 3D facial normal map.

B. Proposed morphing algorithm

We extend the Arc2Face model from single-identity generation to a generative face morphing algorithm. Given two facial images I_A and I_B , we aim to synthesize a morphed

image I_M with a hybrid identity, both perceptually and according to SOTA FRSs.

We first extract ArcFace identity embeddings:

$$e_A = E_{id}(I_A), \quad e_B = E_{id}(I_B), \quad (1)$$

and map them into the Arc2Face conditioning space:

$$p_A = E_t(e_A), \quad p_B = E_t(e_B). \quad (2)$$

These CLIP-space vectors act as semantic identity priors of the two subjects..

To construct the hybrid identity prior, we interpolate between p_A and p_B in the CLIP latent space. Thanks to its multimodal, continuous structure and L2-normalized embeddings optimized with cosine similarity, identity can be smoothly blended by interpolation in this space.

We define the morphed identity representation as

$$p_M = f_{\text{interp}}(p_A, p_B, \alpha), \quad (3)$$

where α controls the relative contribution of the two identities. By default, $\alpha = 0.5$ produces an equal blend, which we use in all experiments.

We consider two choices for f_{interp} : linear interpolation (lerp) [50] and spherical linear interpolation (slerp) [51]. CLIP embeddings are L2-normalized and optimized using cosine similarity, therefore semantics are largely captured by angles, making slerp a reasonable heuristic for identity blending. Lerp, however, remains a valid option that does not impose additional geometric assumptions about the embedding space.

For completeness, spherical linear interpolation between vectors a and b is:

$$\text{slerp}(a, b, t) = \frac{\sin((1-t)\theta)}{\sin\theta}a + \frac{\sin(t\theta)}{\sin\theta}b, \quad (4)$$

where θ is the angle between a and b .

The interpolated CLIP representation p_M is finally used as the conditioning input to Arc2Face, producing the morphed image I'_M .

To generate morphed images that adhere as much as possible to ISO/ICAO standards [26], [27], [29], [28] for pose, facial expression, and background, we use a two-stage control strategy. First, we control pose and facial expression following [37], using a ControlNet [53] conditioned on a target 3D facial normal map. In our setup, the condition map (I_P) is extracted from the input image I_B with the EMOCaV2 model [7], [19] used in Arc2Face, ensuring realistic, identity-consistent facial geometry in the generated output. Second, since the background appearance cannot be directly controlled in the original generative model, we apply the BEN2 background removal network [34], which estimates an alpha channel isolating the facial region. This allows the original background to be replaced with a uniform white background, enhancing compliance with ISO/ICAO document photo requirements.

IV. EXPERIMENTAL EVALUATION

An extensive experimental evaluation has been conducted to validate the effectiveness of the proposed morphing approach. In particular, the experiments compare the proposed method with several SOTA techniques, both landmark- and deep learning-based, in terms of attack potential.

A. Datasets

To provide a comprehensive evaluation of our morphing algorithm, we selected four face datasets, two publicly available and two private, as sources for morph generation. For each dataset, morphed images produced using different existing tools are also available. These datasets therefore serve as benchmarks for comparison, enabling a rigorous assessment of the effectiveness of the proposed algorithm. All employed document images are compliant with ISO/IEC 19794-5 and 39794-5 standards [27], [28].

- FEI [45] and FEI Morph v2 datasets [9] [35]: The FEI dataset comprises images of 200 subjects, equally distributed between male and female, with ages ranging mainly from 19 to 40 years. The images exhibit a good variability in terms of appearance, hairstyle, and presence of accessories. For each subject at least one document-quality image is present, with uniform background and lighting, as well as frontal pose and neutral expression. The FEI Morph v2 dataset was derived from the FEI images using seven SOTA landmark-based morphing algorithms (see Table I) and two morphing factors (0.3 and 0.5), resulting in a total of 14000 morphed images.
- ONOT [11] and MONOT [4] datasets: The ONOT dataset consists of a synthetic collection of high-quality face images, and include 254 distinct synthetic subjects.

The MONOT dataset was generated from ONOT images using six SOTA landmark-based morphing algorithms (see Table I) and two morphing factors (0.3 and 0.5), yielding a total of 15240 morphed images. In addition, for each subject, the MONOT dataset provides ten “in the wild images” (generated using the Arc2Face model [37]), to simulate live acquisitions at airport gates. Two evaluation protocols are considered for these datasets: (i) a single probe image per subject from the ONOT dataset, and (ii) ten “in the wild images” probe images from MONOT, used as gate attempts.

- SOTAMD Digital [42] and EINMorph-HQ v2 datasets: The SOTAMD Digital dataset contains high-resolution face images with frontal pose, neutral expression, and controlled illumination, including 300 bona fide images and 1500 gate images collected within the SOTAMD European project [42] from 150 subjects of various ethnicities. The EINMorph-HQ v2 dataset was derived from the bona fide images of the 150 SOTAMD subjects using six SOTA morphing algorithms (see Table I) and multiple morphing factors, resulting in 9600 morphed images. For morph generation, subject pairs were selected through similarity assessments performed with three commercial SDKs, in order to replicate a realistic and challenging evaluation scenario.
- iMARS-MQ and EINMorph-MQ v2 datasets: The iMARS-MQ dataset was collected within the iMARS European project [25] at six different sites, including two international airports (Lisbon and Athens) and four research laboratories. Image acquisition was performed under real border-control conditions using operational Automatic Border Control (ABC) gates. A total of 60 subjects participated in the acquisition, with some individuals captured at multiple locations. Overall, the data set comprises 205 bona fide images acquired in a controlled setup, and 612 live gate images captured using real ABC gates. The EINMorph-MQ v2 dataset was generated from the bona fide images of the iMARS-MQ subjects using six SOTA morphing algorithms (see Table I) and multiple morphing factors, yielding 4720 morphed images. As in the HQ case, subject pairs were selected based on similarity assessments performed with three commercial SDKs to ensure a realistic and challenging evaluation setting.

For all datasets, the same subject pairs defined in the original benchmarks were used to generate morphed images with Arc2Morph, ensuring a direct and fair comparison across all methods.

B. Evaluation metric

The effectiveness of the proposed morphing algorithm was evaluated by measuring the attack potential of the generated images and comparing it with that obtained from morphed images produced by other SOTA methods. For this purpose, we adopted the Morphing Attack Potential (MAP) metric, introduced in [18] and recently incorporated into the ISO/IEC 20059:2025 standard [1] as the recommended methodology

Algorithm	Type	FEI Morph v2	MONOT	EINMorph-HQ v2	EINMorph-MQ v2
C01 [40]	L	×	×		
C02 [13]	L	×	×		
C03 [42]	L	×	×		
C05 [16]	L	×	×		
C05-PA97 [16] [49] †	L			×	×
C05-PA98 [16] [48] †	L			×	×
C05-PA99 [16] [54] †	L			×	×
C08 ‡	L	×			
C15 [22] [23]	L	×	×		
C16 [3]	L	×	×		
C20 [21]	D			×	×
C21 ‡	D			×	×
C22 ‡	D			×	×

TABLE I: List of the morphing algorithms used to generate the morphed images for the datasets considered in this work. The column *Type* indicates whether the corresponding method is based on facial landmarks (L) or on deep learning techniques (D). † indicates that morphed images have been automatically retouched with a face restoration technique; ‡ indicates that details about this algorithm cannot be disclosed due to privacy constraints.

to evaluate the resistance of biometric recognition systems to morphing attacks. MAP quantifies the attack potential (i.e., the probability of successful attacks) of a dataset of morphed images M by jointly considering multiple probe images and multiple FRSs. MAP is represented as a matrix in which rows correspond to the number of probe images per morph and columns correspond to the number of FRSs involved in the evaluation. Each matrix element $MAP[r, c]$ represents the percentage of morphed images in the dataset M that can be successfully verified with at least r probe images of both contributing subjects by at least c FRSs.

The two dimensions of the MAP matrix capture key factors for assessing morphing attack potential. The vertical axis represents *robustness*: moving from top to bottom, it reflects the ability of morphed samples to be successfully verified against an increasing number of probe samples. Morphed samples appearing in the lower rows therefore exhibit a robust similarity to both contributing subjects, rather than incidental matches with a single probe. The horizontal axis represents *generality*: moving from left to right, it evaluates the ability of morphed samples to deceive an increasing number of FRSs. Morphed images in the rightmost columns therefore exhibit a broader and more system-independent attack capability. The most critical morphed samples are those located in the bottom-right corner of the MAP matrix, as they exhibit both high robustness and high generality. Nevertheless, this region contains only a small number of samples, since relatively few morphs satisfy both conditions simultaneously.

In addition, to facilitate the comparison across different algorithms, the robustness and generality curves are plotted as suggested in the ISO/IEC 20059:2025 standard [1]. These two curves are computed as the normalized weighted sums of the columns and rows of the MAP matrix, respectively. Specifically, the weight assigned to each row r is $\frac{r}{r_{max}}$ and, analogously, the weight assigned to each column c is $\frac{c}{c_{max}}$ (where r_{max} and c_{max} are the total number of rows and columns in the MAP matrix, respectively).

C. Face Recognition Systems

For the MAP computation on the FEI Morph v2 and MONOT datasets, and to ensure a fair comparison with the MAP values reported in [4], the same three Commercial Off-The-Shelf (COTS) FRSs adopted in [4] were employed. These systems were identified as top performers in the Face Recognition Technology Evaluation (FRTE) 1:1 verification benchmark [36].

Conversely, for the MAP computation on the EINMorph-HQ v2 and EINMorph-MQ v2 datasets, a more comprehensive evaluation protocol was adopted. In this case, six FRSs were considered: the three COTS systems used for FEI Morph v2 and MONOT, together with three SOTA deep learning-based face recognition models (MagFace [33], AdaFace [30], and CurricularFace [24]).

The verification thresholds of all FRSs were set to operate at a False Acceptance Rate (FAR) of 0.1%, which represents the reference operating point for FRSs in electronic Machine Readable Travel Document (eMRTD) applications [20]. For the three COTS systems, the thresholds were selected according to vendor recommendations, whereas for the three deep learning models they were calibrated to achieve a FAR of 0.1% on a subset of the FRGC database [38].

D. Qualitative comparison

To better understand the quality of the generation, we perform a visual evaluation of the generated images by generating morphed images from the same pair of subjects using all the selected competitors reported in Table I. Results are shown in Figure 3. While the proposed method produces visually consistent results with the selected competitors, it is important to note that the current implementation leverages ControlNet guidance limited to pose and facial expression. Therefore, other attributes, e.g., presence of accessories, illumination uniformity, are not explicitly controlled, which may affect the overall visual realism of the generated images. Future work will focus on extending controllability to these additional attributes in order to further enhance image quality.

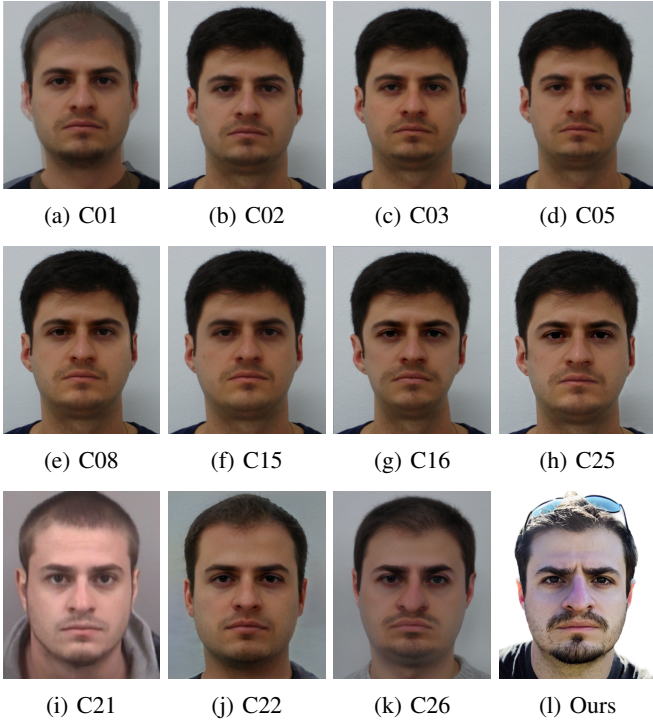


Fig. 3: Qualitative evaluation of the same morphed image produced by each of the selected competitors and by the morphing algorithm proposed in this work. The first two rows are all landmark-based algorithms, while the last one depicts only diffusion-based algorithms. Contributing subjects of the morphed images are depicted in Figure 4a and 4f.

and fidelity.

E. Morphing Attack Potential results

This section analyzes the results in terms of MAP, evaluated across the different testing datasets. The results obtained on the FEI Morph v2 dataset are reported in Table II where the MAP of the proposed approach is compared with that of other seven SOTA morphing algorithms (see Table I). The proposed approach demonstrates outstanding performance in this evaluation, achieving MAP values higher than all other evaluated methods. The results show that 98.7% of the morphed images generated by the proposed approach deceive all three COTS systems, thereby confirming the effectiveness of the algorithm in preserving identity features.

Table III reports the results obtained on the MONOT dataset when a single probe image for each subject (taken from the ONOT dataset) is considered. Overall, the observed MAP is lower than that measured on the FEI Morph v2 dataset. This difference is likely due to the characteristics of the datasets: FEI contains real images, whereas ONOT consists of synthetic samples, which tend to exhibit larger intra-subject variations than those typically observed in real-world data, thereby making successful morphing attacks more challenging. In this scenario, the proposed approach achieves the highest attack capability when targeting a single FRS, with a success rate exceeding 97%. Although the MAP

	1	2	3
C01	97.9%	91.7%	74.0%
C02	99.7%	98.9%	95.9%
C03	97.3%	89.9%	70.2%
C05	98.4%	93.5%	78.0%
C08	98.6%	94.4%	82.5%
C15	97.7%	91.5%	70.9%
C16	99.3%	97.4%	88.7%
Arc2Morph (ours)	99.9%	99.7%	98.7%

TABLE II: MAP computed on the FEI Morph v2 dataset for the proposed approach and seven competitors. Best results for each column are highlighted in bold. In this case, a single probe image is available, so the MAP of each algorithm is represented by a single row.

	1	2	3
C01	94.2%	86.7%	73.5%
C02	94.1%	86.7%	74.0%
C03	90.9%	80.8%	63.4%
C05	91.8%	83.0%	67.4%
C15	89.3%	78.3%	55.8%
C16	91.8%	82.3%	61.6%
Arc2Morph (ours)	97.6%	86.5%	63.6%

TABLE III: MAP computed on the MONOT dataset for the proposed approach and the six competitors reported in [4], considering a single ONOT image for each subject as probe (the MAP of each algorithm is represented by a single row). Best results for each column are highlighted in bold.

decreases as the number of targeted FRSs increases, the proposed method remains comparable to (or outperforms) most competing approaches. Only C01, C02, and C05 show higher generality when all three FRSs are considered.

The MAP results in Table IV, computed using ten "in the wild" probe images for each subject, show an overall very high MAP for the proposed algorithm across all evaluation settings. Even as the number of probe images increases, the attack success rate remains close to saturation for one and two FRSs, and extremely high even when three FRSs are considered, confirming the very high quality of the generated morphed images. Only under the most restrictive conditions (when a large number of probe images is combined with three FRSs) a performance drop is observed. Nevertheless, even in these cases, the MAP values remain high, indicating that the morphed images preserve a stable similarity with both contributing identities. This consistently high MAP can be partially attributed to the experimental setup: in this scenario, all probe images have been generated using Arc2Face [4]. As a result, the proposed method produces morphed images that are particularly challenging for the FRSs, as they are well aligned with the characteristics of the probe-generation process.

For this testing case, the comparison with the other competitors is provided in concise form in Figure 5, through the robustness (Figure 5a) and generality (Figure 5b) curves. The graphs clearly highlight the higher attack potential of the proposed approach with respect to both metrics. As in the previous analysis, the effectiveness is particularly high due to the use of Arc2Face to generate the MONOT "in the

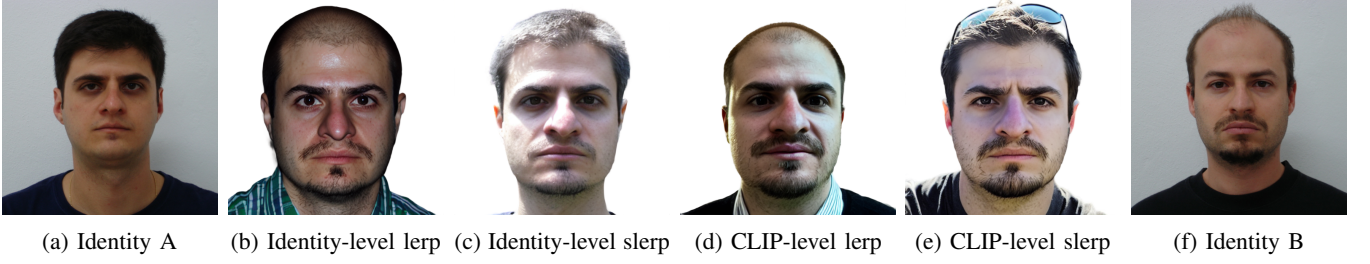


Fig. 4: A visual example of the morphed images obtained using the different interpolation approaches.

	1	2	3
1	100.0%	100.0%	99.9%
2	100.0%	100.0%	99.8%
3	100.0%	100.0%	99.8%
4	100.0%	100.0%	99.6%
5	100.0%	100.0%	99.6%
6	100.0%	99.9%	99.1%
7	100.0%	99.9%	99.1%
8	100.0%	99.8%	98.1%
9	100.0%	99.4%	95.1%
10	99.8%	96.5%	84.3%

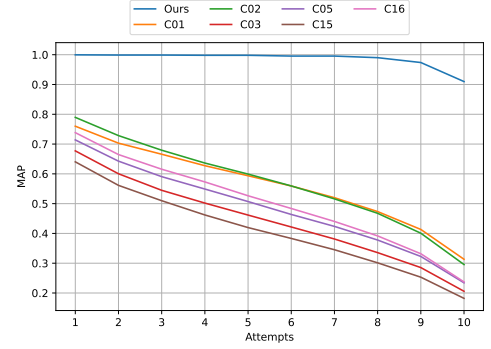
TABLE IV: MAP computed on the MONOT dataset for the proposed approach, considering ten "in the wild" images for each subject as probe.

wild" probe images.

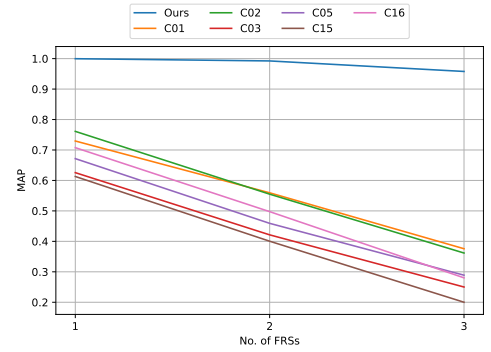
A noticeable superiority over the other morphing algorithms, in terms of both robustness and generality, is also confirmed for the EINMorph-HQ v2 (see Figure 6) and EINMorph-MQ v2 (see Figure 7) datasets. The curves show that the proposed approach not only surpasses the other deep learning-based algorithms, but also outperforms landmark-based techniques, traditionally considered significantly more challenging for FRs.

V. ABLATION STUDY: IDENTITY INTERPOLATION

As discussed in Section III, several choices can be considered for interpolating the two source identities. In particular, interpolation can also be applied at the level of identity features, obtaining $e_M = f_{interp}(e_A, e_B, \alpha)$ where e_A and e_B denote the ArcFace identity embeddings of the input images. The resulting interpolated identity embeddings e_M can then be encoded into the CLIP latent representation $p_M = E_t(e_M)$, which is subsequently decoded by Arc2Face to generate the morphed image I'_M . Then interpolation function f_{interp} can be implemented either as linear interpolation (lerp) or spherical linear interpolation (slerp). Moreover, the interpolation can be performed either in the ArcFace identity space (prior to projection into the CLIP latent space) or directly in the CLIP embedding space. Four combinations are therefore possible, and we compared these alternatives in order to determine the most effective strategy in terms of attack potential. This analysis is carried out on the FEI and ONOT datasets by varying the interpolation method and the embedding space in which it is applied. For each configuration, the MAP is computed. To facilitate comparison across configurations, MAP values are reported as a single scalar



(a) Robustness curve



(b) Generality curve

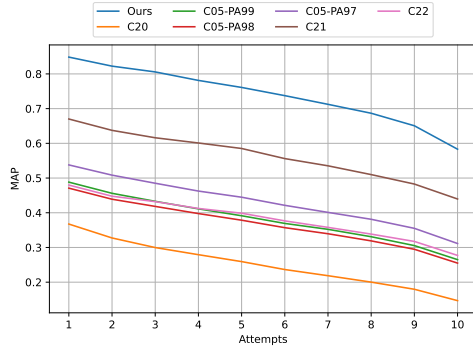
Fig. 5: Visualization of the MAPs computed on the MONOT dataset for the proposed approach and the competitors, considering ten "in the wild" images as probe.

value MAP_{Avg} , obtained using the scalarization procedure defined in the ISO/IEC 20059:2025 standard [1].

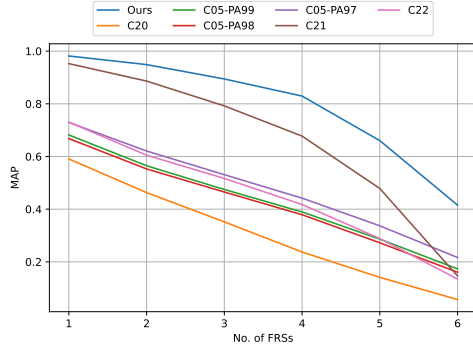
As shown in Table V, spherical linear interpolation applied in the CLIP latent space yields the highest overall MAP_{Avg} . We hypothesize that this apparently counterintuitive behavior is due to the higher dimensionality and richer semantic structure of CLIP's latent space, which allow it to capture finer details than the ArcFace embedding space alone. A visual comparison of images generated using the different interpolation strategies is provided in Figure 4.

VI. CONCLUSIONS AND FUTURE WORKS

This work introduces a new deep learning-based face morphing approach that proved to have an attack potential noticeably higher than that of existing methods, including the

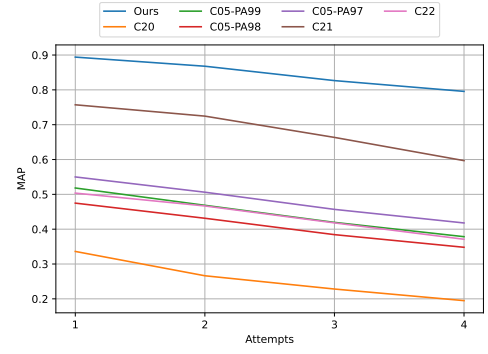


(a) Robustness curve

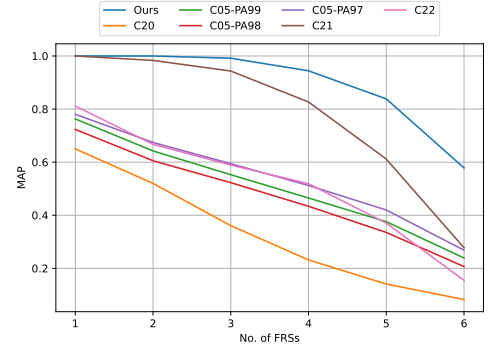


(b) Generality curve

Fig. 6: Visualization of the MAPs computed on the EINMorph-HQ v2 dataset for the proposed approach and the competitors.



(a) Robustness curve



(b) Generality curve

Fig. 7: Visualization of the MAPs computed on the EINMorph-MQ v2 dataset for the proposed approach and the competitors.

Dataset	Interp. location	f_{interp}	MAP_{Avg}
FEI	Identity	lerp	0.9778
		slerp	0.9679
	CLIP	lerp	0.9747
		slerp	0.9835
MONOT	Identity	lerp	0.8539
		slerp	0.8486
	CLIP	lerp	0.8163
		slerp	0.8858

TABLE V: MAP_{Avg} reported on FEI and MONOT datasets for each choice of interpolation location (*i.e.*, identity-level or CLIP latent-level) and interpolation function f_{interp} (*i.e.*, linear interpolation or spherical linear interpolation).

landmark-based techniques, which have traditionally been considered as the most challenging for FRSs.

Future research will focus on further improving the morph generation process, with particular attention on the explicit control of additional image characteristics beyond pose, such as illumination, gaze direction, and exposure. Addressing these factors is expected to yield morphed images that are more closely aligned with ISO/ICAO requirements for identity document photographs.

ETHICAL IMPACT STATEMENT

This work studies face morphing attacks as a security vulnerability in FRSs for electronic identity documents. The research was conducted without collecting new biometric data and without direct interaction with human participants; therefore, ethical review board oversight was not required under applicable regulations. All experiments are based exclusively on publicly available and internal-use-only datasets, used in compliance with their intended research purposes and associated consent and privacy constraints. As no new personal data were collected and no individuals were contacted, risks to human subjects are minimal. The proposed morphing method is developed solely for research and evaluation purposes, with the aim of improving the robustness of morphing attack detection systems. While advanced morphing techniques may pose risks if misused and may reflect limitations in pretrained models, this work does not promote operational deployment of such attacks. Instead, it contributes to strengthening biometric system security by supporting the development of more effective countermeasures.

REFERENCES

- [1] Iso/iec 20059: Information technology – biometrics – concepts and definitions, 2021. International Standard.

- [2] I. Batskos and L. Spreeuwens. Improving fully automated landmark-based face morphing. In *2024 12th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2024.
- [3] I. Batskos, L. Spreeuwens, and R. Veldhuis. Visualizing landmark-based face morphing traces on digital images. *Frontiers in Computer Science*, 5, 2023.
- [4] G. Borghi, N. D. Domenico, M. Ferrara, A. Franco, U. Latif, and D. Maltoni. Monot: High-quality privacy-compliant morphed synthetic images for everyone. In *2024 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–8, 2024.
- [5] G. Borghi, A. Franco, G. Graffieti, and D. Maltoni. Automated artifact retouching in morphed images with attention maps. *IEEE Access*, 9:136561–136579, 2021.
- [6] N. Damer, A. M. Saladié, A. Braun, and A. Kuijper. Morgan: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10, 2018.
- [7] R. Daněček, M. J. Black, and T. Bolkart. Emoca: Emotion driven monocular face capture and animation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 20311–20322, 2022.
- [8] J. Deng, J. Guo, N. Xue, and S. Zafeiriou. Arcface: Additive angular margin loss for deep face recognition. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 4690–4699, 2019.
- [9] N. Di Domenico, G. Borghi, A. Franco, and D. Maltoni. Combining identity features and artifact analysis for differential morphing attack detection. In *International Conference on Image Analysis and Processing*, pages 100–111. Springer, 2023.
- [10] N. Di Domenico, G. Borghi, A. Franco, and D. Maltoni. Face restoration for morphed images retouching. In *2024 12th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2024.
- [11] N. Di Domenico, G. Borghi, A. Franco, D. Maltoni, et al. Onot: a high-quality ica-compliant synthetic mugshot dataset. In *The 18th IEEE International Conference on Automatic Face and Gesture Recognition (FG)*, pages 1–6, 2024.
- [12] J. Donahue, P. Krähenbühl, and T. Darrell. Adversarial feature learning, 2017.
- [13] FaceFusion. FaceFusion. <http://www.wearemoment.com/FaceFusion/>. [Accessed: 2024-12-01].
- [14] M. Ferrara and A. Franco. *Morph Creation and Vulnerability of Face Recognition Systems to Morphing*, pages 117–137. Springer International Publishing, Cham, 2022.
- [15] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *IEEE International Joint Conference on Biometrics*, pages 1–7, 2014.
- [16] M. Ferrara, A. Franco, and D. Maltoni. Face demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4):1008–1017, 2018.
- [17] M. Ferrara, A. Franco, and D. Maltoni. Decoupling texture blending and shape warping in face morphing. In *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5, 2019.
- [18] M. Ferrara, A. Franco, D. Maltoni, and C. Busch. Morphing attack potential. In *2022 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2022.
- [19] P. P. Filntsis, G. Retsinas, F. Paraperas-Papantoniou, A. Katsamanis, A. Roussos, and P. Maragos. Visual speech-aware perceptual 3d facial expression reconstruction from videos. *arXiv preprint arXiv:2207.11094*, 2022.
- [20] Frontex. *Best practice technical guidelines for Automated Border Control (ABC) systems – Research and development unit*. Publications Office of the European Union, 2012.
- [21] M. Grimmer and C. Busch. Ladimo: Face morph generation through biometric template inversion with latent diffusion. In *2024 IEEE International Joint Conference on Biometrics (IJCB)*, 2024.
- [22] I. Group. INGROUPE web site. <https://ingroupe.com/>. [Accessed: 2026-01-13].
- [23] S. Group. SURYS web site. <https://surys.com/>. [Accessed: 2026-01-13].
- [24] Y. Huang, Y. Wang, Y. Tai, X. Liu, P. Shen, S. Li, J. Li, and F. Huang. Curricularface: Adaptive curriculum learning loss for deep face recognition. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020.
- [25] iMARS. iMARS european project. <https://imars-project.eu/>. [Accessed: 2026-01-13].
- [26] International Civil Aviation Organization (ICAO). Portrait Quality: Reference Facial Images for MRTD. Standard, International Civil Aviation Organization, 2018.
- [27] International Standards Organization. ISO/IEC 19794-5 — Information technology — Biometric data interchange formats — Part 5: Face image data. Standard, International Organization for Standardization, 2011.
- [28] International Standards Organization. ISO/IEC 39794-5 — Information technology — Extensible biometric data interchange formats — Part 5: Face image data. Standard, International Organization for Standardization, 2019.
- [29] International Standards Organization. ISO/IEC 29794-5 — Information technology — Biometric sample quality — Part 5: Face image data. Standard, International Organization for Standardization, under development.
- [30] M. Kim, A. K. Jain, and X. Liu. Adaface: Quality adaptive margin for face recognition. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022.
- [31] D. E. King. Dlib-ml: A machine learning toolkit. *Journal of Machine Learning Research*, 10:1755–1758, 2009.
- [32] A. Makrushin, T. Neubert, and J. Dittmann. Automatic generation and detection of visually faultless facial morphs. In *International conference on computer vision theory and applications*, volume 7, pages 39–50. SciTePress, 2017.
- [33] Q. Meng, S. Zhao, Z. Huang, and F. Zhou. Magface: A universal representation for face recognition and quality assessment. In *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021.
- [34] M. Meyer and J. Spruyt. Ben: Using confidence-guided matting for dichotomous image segmentation. *arXiv preprint arXiv:2501.06230*, 2025.
- [35] MI@BioLab. FEI Morph Dataset. <https://miatbiolab.csr.unibo.it/fei-morph-dataset/>. [Accessed: 2026-01-13].
- [36] NIST. Face Recognition Technology Evaluation (FRTE) 1:1 verification. <https://pages.nist.gov/frvt/html/frvt11.html>. [Accessed: 2026-01-13].
- [37] F. P. Papantoniou, A. Lattas, S. Moschoglou, J. Deng, B. Kainz, and S. Zafeiriou. Arc2face: A foundation model for id-consistent human faces. In *European Conference on Computer Vision*, pages 241–261. Springer, 2024.
- [38] P. Phillips, P. Flynn, T. Scruggs, K. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. In *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, volume 1, pages 947–954 vol. 1, 2005.
- [39] A. R. PN, R. Ramachandra, S. Venkatesh, K. S. Rao, P. Mitra, and R. Krishna. Morcode: Face morphing attack generation using generative codebooks. *arXiv preprint arXiv:2410.07625*, 2024.
- [40] A. Quek. FaceMorpher. https://github.com/alyssaq/face_morpher. [Accessed: 2026-01-13].
- [41] A. Radford, J. W. Kim, C. Hallacy, A. Ramesh, G. Goh, S. Agarwal, G. Sastry, A. Askell, P. Mishkin, J. Clark, et al. Learning transferable visual models from natural language supervision. In *International conference on machine learning*, pages 8748–8763. PmLR, 2021.
- [42] K. Raja, M. Ferrara, A. Franco, L. Spreeuwens, I. Batskos, F. de Wit, M. Gomez-Barrero, U. Scherhag, D. Fischer, S. K. Venkatesh, J. M. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Ramachandra, C. Rathgeb, D. Frings, U. Seidel, F. Knopjes, R. Veldhuis, D. Maltoni, and C. Busch. Morphing attack detection-database, evaluation platform, and benchmarking. *IEEE Transactions on Information Forensics and Security*, 16:4336–4351, 2021.
- [43] R. Rombach, A. Blattmann, D. Lorenz, P. Esser, and B. Ommer. High-resolution image synthesis with latent diffusion models. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 10684–10695, 2022.
- [44] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch. Face recognition systems under morphing attacks: A survey. *IEEE Access*, 7:23012–23026, 2019.
- [45] C. E. Thomaz and G. A. Giralaldi. A new ranking method for principal components analysis and its application to face image analysis. *Image and Vision Computing*, 28(6):902–913, 2010.
- [46] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE transactions on technology and society*, 2(3):128–145, 2021.
- [47] S. Venkatesh, H. Zhang, R. Ramachandra, K. Raja, N. Damer, and C. Busch. Can gan generated morphs threaten face recognition systems equally as landmark based morphs? - vulnerability and detection. In *2020 8th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2020.
- [48] X. Wang, Y. Li, H. Zhang, and Y. Shan. Towards real-world blind face restoration with generative facial prior. In *Proceedings of the*

IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), June 2021.

- [49] Z. Wang, J. Zhang, T. Chen, W. Wang, and P. Luo. Restoreformer++: Towards real-world blind face restoration from undegraded key-value pairs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(12), 2023.
- [50] Wikipedia. Linear interpolation. https://en.wikipedia.org/wiki/Linear_interpolation. [Accessed: 2026-01-13].
- [51] Wikipedia. Spherical linear interpolation. <https://en.wikipedia.org/wiki/Slerp>. [Accessed: 2026-01-13].
- [52] H. Zhang, S. Venkatesh, R. Ramachandra, K. Raja, N. Damer, and C. Busch. Mipgan—generating strong and high quality morphing attacks using identity prior driven gan. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(3):365–383, 2021.
- [53] L. Zhang, A. Rao, and M. Agrawala. Adding conditional control to text-to-image diffusion models. In *Proceedings of the IEEE/CVF international conference on computer vision*, pages 3836–3847, 2023.
- [54] S. Zhou, K. C. Chan, C. Li, and C. C. Loy. Towards robust blind face restoration with codebook lookup transformer. In *Proceedings of the 36th International Conference on Neural Information Processing Systems (NIPS)*, 2022.