MorCode: Face Morphing Attack Generation using Generative Codebooks

Aravinda Reddy PN[1]

Raghavendra Ramachandra[2]

Krothapalli Sreenivasa Rao[1]

Pabitra Mitra[1]

[1] Indian Institute
of Technology Kharagapur, India

[2] Norwegian University of
Science and Technology,
Gjøvik Norway

Abstract

Face recognition systems (FRS) can be compromised by face morphing attacks, which blend textural and geometric information from multiple facial images. The rapid evolution of generative AI, especially Generative Adversarial Networks (GAN) or Diffusion models, where encoded images are interpolated to generate high-quality face morphing images. In this work, we present a novel method for the automatic face morphing generation method *MorCode*, which leverages a contemporary encoder-decoder architecture conditioned on codebook learning to generate high-quality morphing images. Extensive experiments were performed on the newly constructed morphing dataset using five state-of-the-art morphing generation techniques using both digital and print-scan data. The attack potential of the proposed morphing generation technique, *MorCode*, was benchmarked using three different face recognition systems. The obtained results indicate the highest attack potential of the proposed *MorCode* when compared with five state-of-the-art morphing generation methods on both digital and print scan data.

1 Introduction

Face Recognition Systems (FRS) are extensively deployed in various access control applications, including border control, because of their high accuracy and user convenience. Nevertheless, these systems are susceptible to various forms of attacks such as presentation and adversarial attacks, which can compromise their security. Of particular concern are morphing attacks, which have gained prominence for their ability to undermine the security of automatic border-control scenarios. Morphing is the process of blending two or more facial images to result in a single composite facial image that reflects both texture and geometric information corresponding to facial images used for morphing. Therefore, the generated morphing images indicate a vulnerability to human observers, including border guards [9] and automatic FRS [24]. NIST Face Analysis Technology Evaluation (FATE) Morph [15] illustrates the vulnerability of several FRS to morphing attacks. Therefore, that indicates that, higher the accuracy of FRS implies higher vulnerability.

Face morphing attacks have garnered significant attention, with the objective of maintaining identity-related features from facial images that represent multiple identities. The primary focus is on preserving the individual's identity within the morphed image, as this can enhance the attacker's potential to launch successful morphing attacks on the FRS. To this extent, researchers have proposed several 2D [24] and 3D face morphing generation [20] algorithms that have indicated a higher attack potential when presented to automatic FRS. The available face morphing generation algorithms can be broadly classified as [24] (a) facial landmark-based and (b) deep learning-based. Facial landmark-based methods use pixel information from facial images of multiple identities to obtain the morphing image, whereas deep learning-based methods generate or synthesize the morphing face image based on the compact representation (also called latent) corresponding to multiple identities. Because morphing attacks are applicable to border control scenarios, the goal of morphing generation techniques must be to generate facial images fulfilling the quality constraints laid down by the International Civil Aviation Organization (ICAO), which requires a high-quality facial image.

Early work on generating face morphing images was based on facial landmark-based face morphing techniques. Given two facial images, facial landmark-based methods first extract the facial landmarks (approximately 64 points) after alignment. Triangulation is then performed, followed by wrapping and blending to generate the morphing image. Landmark-based methods include open-source software from open CV [12] and FaceMorpher [1] which are employed in the literature to generate morphing attacks. One of the major limitations of facial landmark-based methods is ghost artifacts that are prominent in the eye, mouth, and nose regions, hindering image quality issues. Therefore, post-processing using facial landmark-based methods [12] further improves the quality of the morphed images.

The evolution of generative AI techniques has enabled the generation of face-morphing images that overcome ghost artifacts. Early works used the vanilla GAN [3], in which the latent from the facial images to be morphed is averaged to obtain a single latent, which is then used to construct the morphed image. However, the quality of the image rendered in [3] was low because of the output dimensions of 64 × 64 pixels. The first work on generating an ICAO-quality morphing image using StyleGAN was presented in [22], which also used latent averaging. However, the use of GAN degrades the identity information, which degrades the attack potential of the generated face-morphing image. To overcome this, MIPGAN [25] was introduced, in which the fusion of the latent from StyleGAN was optimized to achieve the highest attack potential using the FRS as a loss function. MIPGAN has higher attack potential than other GAN-based approaches [25]. The pixel2style2pixel (pSp) encoder-based latent extraction and fusion using spherical interpolation was proposed in [18]. Finally, the fused latent was used to generate the face morphing image by employing StyleGAN2. The use of the pSp encoder, spherical interpolation, and StyleGAN2 combination indicated a higher attack potential for the morphed image, and it is worth noting that there is no need for identity-based optimization.

The introduction of diffusion models for image generation has attracted researchers to adapt the model for face morphing generation. In [5] [2], denoising diffusion probabilistic models (DDPM) is adapted to generate face morphing images by manipulating the latent code. However, identity information is not sufficient to generate high attack potential. Therefore, in [27], identity-prior-based optimization was introduced to DDPMS to generate morphed images with a higher attack potential. However, the results indicate a marginal increase in attack potential. In [26], a transformer-based GAN model with identity loss functions was used to generate face morphing images. However, the attack potential of morphing images generated using [26] did not indicate a higher attack potential compared to conventional MorDiff [5] [2]. As per existing research, it is crucial to demonstrate the vulnerability of the Face Recognition System (FRS) by exhibiting a higher attack potential with the generated face-morphing image. In this regard, it is essential to utilize latent representations in generative networks. Consequently, we were inspired to incorporate a Vector-Quantized Generative Adversarial Network (VQ-GAN) [7] into our work, which conditions the latent facial image with codebook to achieve high-quality morphing generation.

In this work, we introduce a novel method for 2D face morphing generation using a codebook learned using VQ-GAN [7] which we refer to as *MorCode*. The novelty of the proposed method lies in the introduction of latent conditioning, which results in a discrete and compact representation of the latent. Thus, it is our assertion that the representation of latent using codebooks will enable a high-quality face morphing generation algorithm. Furthermore, the proposed method employs spherical interpolation to blend the latent corresponding to multiple face images, which contributes to high-quality morphing generation. The main contributions of this work are as follows:

- Proposed a novel 2D face morphing generation using codebook and spherical interpolation to achieve high quality face morphing generation.
- Introduced a new dataset MorCode Morphing Dataset (MMD) with the proposed face morphing generation technique using publicly available face dataset FRGC V2. Newly generated dataset is comprised of 160 data subjects resulting in a total of 1277 bona fide and 2526 morphing images.
- Extensive experiments are carried on the newly generated dataset and comparison of the proposed morphing technique is quantitatively benchmarked with four different existing face morphing techniques using Generalized Morphing Attack Potential (G-MAP) vulnerability metric. The attack potential of the proposed an existing morphing techniques are evaluated against three different deep learning based FRS such as ArcFace [6], MagFace [13] and AdaFace [11].
- The proposed method is open sourced to support the reproducibility : https://github.com/Aravinda27/MorCode

The rest of the paper is organised as follows: Section2 discuss the proposed *MorCode* method for 2D face morphing generation method, Section 3 presents the new dataset generated using the proposed morphing techniques, Section 4 presents the vulnerability evaluation results of the proposed and existing morphing generation methods against three FRS system and Section 5 draws the conclusion.

2 *MorCode*: Proposed 2D Face morphing generation

In this work, we present a new method for generating a high quality 2D face morphing attack using Vector Quantized Generative Adverserial Network (VQGAN). VQGAN [7] utilizes a noise-conditioned score network (NCSN++)-based encoder-decoder architecture, which is a score-based generative model. The application of NCSN++ differs from facial morphing; however, its U-Net structure and discrete codebook of acquired representations for each image possess the capability to capture the rich features that are essential for the face morphing generation task. Figure 1 shows the block diagram of the proposed morphing generation technique. The proposed method can be structured in three steps (a) Encoder (b) Spherical Interpolation and (c) Decoder. The underlining idea of the proposed method includes the step from image to latent space manipulation and final image image decoding to ensure the generated morphed image that can preserve the identity information resulting in the higher attack potential. More particularly, the use of perceptually rich codebook in VQGAN allows the representation of the given face image as the spatial collection allows the high quality representation of the latent that enable the high quality image generation [7].

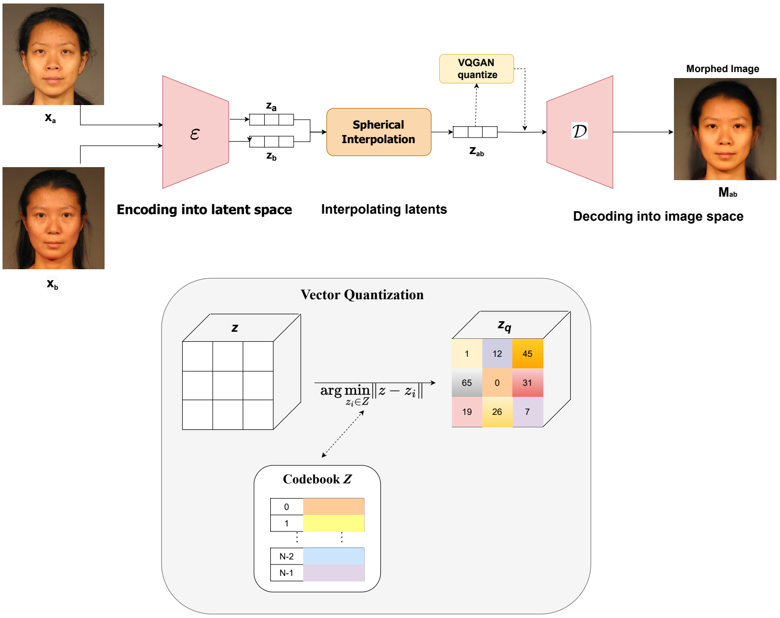

Figure 1: Block Diagram of the proposed method *MorCode* to construct high quality morphed images.

In the following, we present in detail different building blocks of the proposed face morphing generation method.

2.1 Encoder

The encoder architecture consists of serial connection of convolution layer followed by ResNet block and the downsample layer. The use of ResNet blocks will learn the feature representation while preserving spatial dimensions. Subsequently, a downsampling layer reduces the spatial dimensions of the feature maps, conserving only the most salient features. The downsampling is performed twice, each time followed by two residual blocks to further refine the features. After another single residual block, an attention block (Attn Block) is applied to capture long-range dependencies within the data. The output of the attention block passes through the final residual block before a convolutional layer with three filters (Conv(3)), producing a pre-quantization convolutional representation preQuantConv.

Given the two facial images x_a and x_b, the encoder will map into the latent space resulting in the latent representation z_a and z_b respectively with dimensions compressed by the downsampling factor f. The encoder facilitates this dimensionality reduction, mapping the high-resolution input images from their original space $\mathbb{R}^{H\times W\times 3}$ to a more manageable latent space $\mathbb{R}^{h\times w\times c}$, where $h = H/f$, $w = W/f$, and c represents the depth of the latent space. We use $f = 4$ and downsample the image dimensions by a factor of 4 while representing latent space dimensions. Given by $z_a = E(x_a), \quad z_b = E(x_b)$

2.2 Spherical Interpolation

In the next step, we perform spherical interpolation on the latent representations z_a and z_b. This is a critical step where we generate a single, morphed latent representation z_{ab} that encapsulates the characteristics of both z_a and z_b while ensuring a smooth transition within the latent space. Given by $z_{ab} = slerp(z_a, z_b; \gamma)$.

The spherical interpolation utilizes the geodesic path on the unit hypersphere and is mathematically represented as:

$$z_{ab} = \frac{\sin((1-\gamma)\Omega)}{\sin(\Omega)} z_a + \frac{\sin(\gamma\Omega)}{\sin(\Omega)} z_b \tag{1}$$

where Ω is the angle between z_a and z_b, and γ is the interpolation factor that dictates the blend between the two latent representations. The resultant z_{ab} possesses dimensions analogous to z_a and z_b, enabling us to handle it within the latent space as we would with any individual latent vector.

2.3 Vector Quantization

The spherically interpolated output z_{ab} is then quantized using a codebook Z_k. The quantization process maps the continuous latent features to a discrete set of codes within the codebook to obtain the quantized latent representation $\hat{z}_{ab}$. This quantization allows for the generation of a compact, discrete representation of the interpolated or blended data, which is beneficial for high perceptual image quality reconstruction. Given by $\hat{z}_{ab} = VQ(z_{ab})$

2.4 Decoder

The decoder mirrors the encoder's structure but operates in reverse, aiming to reconstruct the input from its quantized representation $\hat{z}_{ab}$. Starting with the quantized tensor $\hat{z}_{ab}$, the decoder applies a convolutional layer with 512 filters (Conv(512)) and proceeds through a series of upsampling and residual blocks (ResBlock x3, UpSample, ResBlock x3, UpSample, ResBlock x3). Each upsampling step increases the spatial dimensions, enabling the reconstruction of the original image size. An attention block is then used similarly to the encoder, followed by a single residual block and a final convolutional layer with three filters (Conv(3)). The reconstructed morphed image M_{ab} can be defined as $M_{ab} = D(\hat{z}_{ab})$.

Figure 2 shows an example of a face-morphing image generated using the proposed *MorCode* method. The qualitative results of the proposed method were also compared with five state-of-the-art face morphing generation methods. The qualitative results indicate the superior perceptual quality of the proposed *MorCode*, particularly in preserving the shape and texture features.

3 MorCode Morphing Dataset (MMD)

In this section, we present the MorCode Morphing Dataset (MMD), which is a newly constructed face morphing dataset that utilizes the proposed *MorCode* face morphing generation technique. MMD dataset was constructed using the publicly available dataset FRGC V2 [16]. We selected 143 subjects with neutral expressions and postures, which were captured under optimal lighting conditions to reflect the conditions of passport enrolment. We followed the recommended procedures for creating face morphs, as outlined in [17]. To simulate a real-life scenario, we utilized a commercial off-the-shelf product from Neurotek [14] to pair

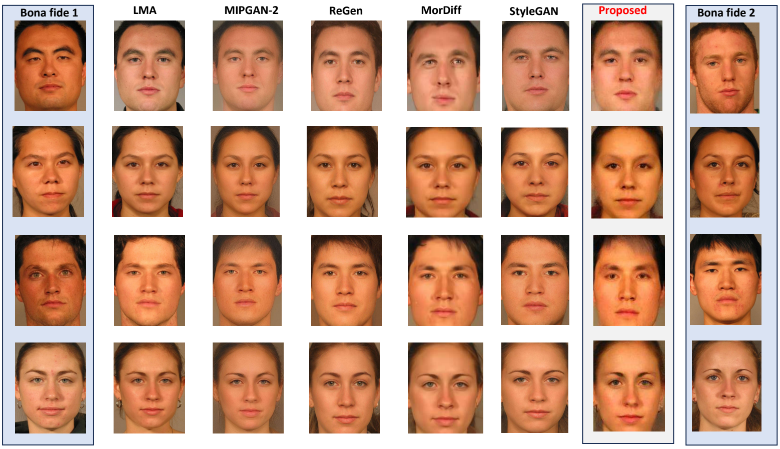

Figure 2: Example images from MMD dataset representing Digital samples. The proposed MorCode face morphing technique is qualitatively compared with the five different existing techniques.

face identities based on their closest match. We performed face morphing generation using five existing morphing techniques: landmark-based [8], MIPGAN-2 [25], ReGen Morph [4], StyleGAN2 [22] and MorDiff [5].

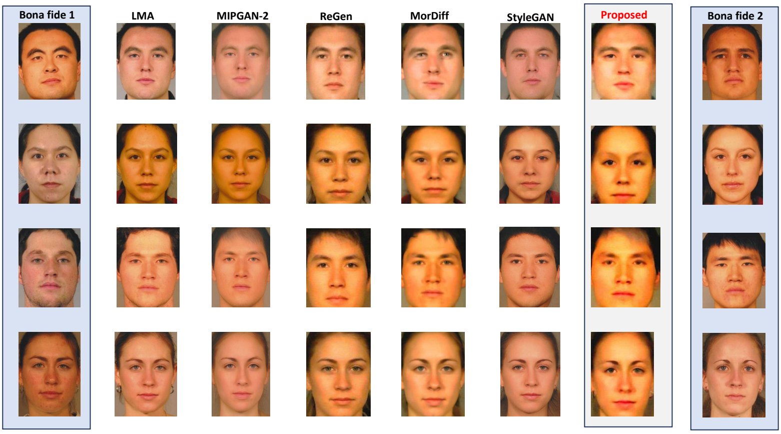

Figure 3: Example images from MMD dataset representing print scan using DNP printer samples. The proposed MorCode face morphing technique is qualitatively compared with the five different existing techniques.

The MMD dataset comprises two types of media: digital and Print-Scan (PS). The digital version encompasses conventional morphing images, whereas the PS morphing images are re-digitized versions of digital morphing images. The inclusion of the PS version was motivated to reflect the passport issuance scenario in which printed passport images were accepted. In this work, we utilized DNP printers, which are specifically designed to produce high-quality passport images featuring facial biometrics. Figure 2 and 3 show examples from the MMD dataset corresponding to both the Digital and PS datasets. It is worth noting that the quality of the images was slightly degraded by PS. The MMD dataset contains 1276 bona fide samples (separately for digital and morphing) and 2526 morphing images (separately for six different morphing techniques, including the proposed method, and separately for digital and PS). Therefore, the MMD dataset has $1276 \times 2 = 2552$ bona fide samples and $2526 \times 6 \times 2 = 30312$ morphing images.

4 Experiments and Results

In this section, we present a quantitative analysis of the vulnerability of face recognition systems to the proposed *MorCode* morphing generation. The quantitative analysis of the vulnerability was benchmarked using three different deep learning-based FRS that are openly available: ArcFace [6], MagFace [13] and AdaFace [11]. These FRS were selected based on their outstanding verification performance reported in the literature [1]. We also compared the performance of the proposed MorCode method with five different state-of-the-art morphing generations: landmark-based [8], MIPGAN-2 [25], ReGen Morph [4], StyleGAN2 [22] and MorDiff [5].

FRS Systems	Morphing Generation Techniques	G-MAP with MA	
		Operating Threshold: FAR =	
		1%	0.1%
AdaFace [11]	landmark-based [8]	84.67	17.29
	MIPGAN-2 [25]	91.45	15.23
	ReGen Morph [4]	29.92	0
	MorDiff [5]	90.81	17.47
	StyleGAN2 [22]	67.99	1.89
	Proposed method (MorCode)	**93.22**	**19.62**
ArcFace [6]	landmark-based [8]	85.63	26.20
	MIPGAN-2 [25]	90.12	24.59
	ReGen Morph [4]	33.44	0.04
	MorDiff [5]	84.09	15.74
	StyleGAN2 [22]	73.30	3.78
	Proposed method (MorCode)	**92.25**	**27.52**
MagFace [13]	landmark-based [8]	92.21	38.49
	MIPGAN-2 [25]	93.56	36.44
	ReGen Morph [4]	64.19	0.17
	MorDiff [5]	93.18	33.57
	StyleGAN2 [22]	83.79	8.58
	Proposed method (MorCode)	**96.27**	**39.48**

Table 1: Quantitative performance with G-MAP MA on MMD dataset (Digital).

Morphing Generation Techniques	G-MAP with MA and MFRS	
	Operating Threshold: FAR =	
	1%	0.1%
Landmark-based [8]	84.67	17.29
MIPGAN-2 [25]	90.12	15.23
ReGen Morph [4]	29.92	0
MorDiff [5]	84.09	15.74
StyleGAN2 [22]	67.99	1.89
Proposed method (MorCode)	**92.25**	**19.52**

Table 2: Quantitative performance with G-MAP with MA and multiple FRS on MMD dataset (digital).

There are four different metrics that are employed to benchmark the vulnerability (a) Mated Morph Presentation Match Rate (MMPMR)[19] (b) Fully Mated Morph Presentation Match Rate (FMMPMR)[23] (c) Morphing Attack Potential (MAP) [10] and (d) Generalized Morphing Attack Potential (G-MAP)[21]. In this work, we quantify the attack potential of morphing generation methods using the Generalized Morphing Attack Potential (G-MAP) vulnerability metric, as it is designed to address the limitations of other evaluation metrics, as discussed in [21] .[2] The G-MAP can be computed as follows[21] [3]:

$$\text{G-MAP} = \frac{1}{|\mathbb{D}|}\sum_{d}^{|\mathbb{D}|}\frac{1}{|\mathbb{P}|}\frac{1}{|\mathbb{M}_d|}\min_{\mathbb{F}_l}\sum_{i,j}^{|\mathbb{P}|,|\mathbb{M}_d|}\Bigg\{\Big[(S1_i^j > \tau_l)\wedge\cdots(Sk_i^j > \tau_l)\Big] \\ \times\left[(1 - FTAR(i,l))\right]\Bigg\} \qquad (2)$$

[1] We employed Commercial Off-the-Shelf technology (Neurotek [14]) to select face image pairs for morphing. To prevent bias in our vulnerability study, we have decided not to use the same COTS. Due to licensing issues involving costs, we are unable to access other Commercial Off-The-Shelf (COTS) FRS. Consequently, we were unable to include the study of COTS within the scope of this research.

[2] Readers can refer [21] and Table 4 (in [21]) to embrace the more information on G-MAP.

[3] Taken from [21]

FRS Systems	Morphing Generation Techniques	G-MAP with MA	
		Operating Threshold: FAR =	
		1%	0.1%
AdaFace [[illegible]]	landmark-based [[illegible]]	88.41	**17.34**
	MIPGAN-2 [[illegible]]	92.16	13.85
	ReGen Morph [[illegible]]	35.32	0.24
	MorDiff [[illegible]]	92.40	21.57
	StyleGAN2 [[illegible]]	73.61	3.22
	Proposed method (MorCode)	**93.26**	6.61
ArcFace [[illegible]]	landmark-based [[illegible]]	90.14	**25.34**
	MIPGAN-2 [[illegible]]	92.57	22.67
	ReGen Morph [[illegible]]	42.93	0.55
	MorDiff [[illegible]]	88.15	23.15
	StyleGAN2 [[illegible]]	75.99	5.54
	Proposed method (MorCode)	**94.15**	5.49
MagFace [[illegible]]	landmark-based [[illegible]]	91.14	**39.16**
	MIPGAN-2 [[illegible]]	92.58	34.71
	ReGen Morph [[illegible]]	58.98	1.21
	MorDiff [[illegible]]	94.17	33.34
	StyleGAN2 [[illegible]]	86.69	13.13
	Proposed method (MorCode)	**93.22**	21.13

Table 3: Quantitative performance with G-MAP MA on PS version of MMD dataset.

Morphing Generation Techniques	G-MAP with MA and MFRS	
	Operating Threshold: FAR =	
	1%	**0.1%**
Landmark-based [[illegible]]	88.41	17.34
MIPGAN-2 [[illegible]]	92.16	13.85
ReGen Morph [[illegible]]	35.32	0.24
MorDiff [[illegible]]	88.15	**21.57**
StyleGAN2 [[illegible]]	73.61	3.22
Proposed method (MorCode)	**93.22**	5.49

Table 4: Quantitative performance with G-MAP with MA and multiple FRS on MMD dataset (PS).

Where, $\mathbb{P}$ denote the set of paired probe images, $\mathbb{F}$ denote the set of FRS, $\mathbb{D}$ denote the set of Morphing Attack Generation Type, $\mathbb{M}_d$ denote the face morphing image set corresponding to Morphing Attack Generation Type d, τ_l indicate the similarity score threshold for FRS (l),$||$ represents the count of elements in a set during metric evaluation and $FTAR(i,l)$ is the failure to acquire probe image in attempt i using FRS (l). In this work, we present two results by varying the parameters of G-MAP, as mentioned in [21] (a) G-MAP with Multiple probe Attempts (MA) by setting $\mathbb{D}$ and $\mathbb{F}_{<}$ to 1 (b) G-MAP with MA and multiple FRS (G-MAP MA and MFRS) by setting $\mathbb{D} = 1$. In both experiments, we set $FTAR = 0$.

To compute the vulnerability of the FRS (or attack potential of morphing generation techniques), we enrol the morphing image and probe the identities that are used to generate the morphing image. The probe facial images correspond to different independent attempts made by the individual identity. A morphing image is considered vulnerable if the probe attempts made by all identities exceed the preset threshold at the given FAR. In this study, we used the preset thresholds of the FRS with FAR = 1% and 0.1%. Therefore, the higher the value of G-MAP, the higher is the vulnerability of the FRS for the given morphing attack generation technique.

Tables 1 and 3 show the quantitative benchmarks of the vulnerability of three different FRS using G-MAP MA for digital and print-scan morphing data. Based on the obtained results, the following can be observed.

- The vulnerability performance of the FRS varies across digital and PS-morphing images. MagFace [13] FRS indicates the highest vulnerability in a digital database with a G-MAP MA of 96.27% at FAR = 1%. With the PS database, all three FRS indicated a similar performance in which ArcFace [6] indicated a marginally higher vulnerability at FAR = 1%. However, with the lower FAR values (0.1%), all FRS indicate lower vulnerability, and among different FRS, MagFace [13] indicates a higher vulnerability.

- The proposed *MorCode* indicates the highest attack potential compared to five different morphing generation techniques on the digital morphing images. All three FRS indicate the highest vulnerability for the proposed *MorCode* with G-MAP MA = 93.22% (for AdaFace), 92.25% (for ArcFace), and 96.27% (for MagFace), with FAR = 1%. Similar observations can also be made with a lower FAR value of 0.1%. Among the three different FRS, MagFace [13] indicates a higher vulnerability for the proposed *MorCode*, irrespective of the operating threshold. The improved attack potential of the proposed *MorCode* can be attributed to the shape and texture information captured from the identities that contribute to morphing generation.

- The proposed *MorCode* indicates the higher vulnerability on all three FRS especially at higher FAR values. The attack potential of the proposed method at FAR = 1% indicates similar performance across all three FRS. However, at FAR = 0.1%, the proposed method indicates degraded performance, which can be attributed to the granular noise in the morphing image being further enhanced during the print-scan operation. The effect of the print-scan process on the proposed methods can also be visualized in Figure 3, where the degradation in the image quality is noted more compared to other existing morphing techniques.

Tables 2 and 4 illustrate the attack potential of morphing generation techniques, which are quantified using G-MAP with MA and multiple FRS. In this work, the given morphing image is considered to have attack potential if it can successfully deceive all three FRS that were used in this work when probed (with various attempts) with the identities that were used to generate the morphing images. Based on the obtained results following can be noted:

- The proposed *MorCode* has indicated a highest attack potential on digital MMD dataset compared to the five different state-of-the art morphing generation techniques. The proposed method indicates an attack potential of G-MAP (MA and MFRS) = 92.25% and 19.52% at FAR = 1% and FAR = 0.1% respectively. The second-best performance was noted with the MIPGAN-2 [25] morphing technique.

- With PS version of MMD dataset, the proposed *MorCode* indicates the highest attack potential at higher FAR = 1% with G-MAP (MA and MFRS) = 93.22% . However, at lower FAR values, the performance of the proposed method indicated degraded results. MorDiff [2, 5] demonstrated the best performance with G-MAP (MA and MFRS) = 27.57% at FAR = 0.1%.

- It is interesting to note that, the proposed method has indicated the similar attack potential across both digital and PS medium at lower FAR = 1%.

- When compared to the landmarks based morphing generation, the generative deep learning based techniques have indicates higher vulnerability as indicated in the Table 2 and 4.

5 Conclusion

This paper introduces MorCode, a novel face morphing attack generation method. Leveraging a VQGAN-conditioned encoder-decoder architecture, MorCode generates morphing images by spherically interpolating latent representations of two target faces. Through extensive experiments on a newly constructed dataset encompassing both digital and print-scan data, MorCode demonstrated superior attack efficacy against three state-of-the-art face recognition systems compared to five other morphing generation methods. These findings underscore the potency of MorCode for generating highly effective face morphing attacks.

References

[1] Face morpher. http://www.facemorpher.com/, 2020. Accessed: October 2020.

[2] Zander Blasingame and Chen Liu. Leveraging diffusion for strong and high quality face morphing attacks. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, pages 1–1, 2024. doi: 10.1109/TBIOM.2024.3349857.

[3] N. Damer, Y. Wainakh, V. Boller, S. von den Berken, P. Terhörst, A. Braun, and A. Kuijper. MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In *Proc. of the 9th IEEE Intl. Conf. on Biometrics: Theory, Applications, and Systems (BTAS)*. IEEE, 2018.

[4] N. Damer, K. Raja, M. Sussmilch, S. Venkatesh, F. Boutros, M. Fang, F. Kirchbuchner, R. Raghavendra, and A. Kuijper. ReGenMorph: Visibly realistic GAN generated face morphing attacks by attack re-generation. *Inernational Symposium on Visual Computing ISVC*, 2021.

[5] Naser Damer, Meiling Fang, Patrick Siebke, Jan Niklas Kolf, Marco Huber, and Fadi Boutros. Mordiff: Recognition vulnerability and attack detectability of face morphing attacks created by diffusion autoencoders. In *2023 11th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2023. doi: 10.1109/IWBF57495.2023.10157869.

[6] J. Deng, J. Guo, and S. Zafeiriou. ArcFace: Additive angular margin loss for deep face recognition. In *Conf. on Computer Vision and Pattern Recognition (CVPR)*, June 2019.

[7] Patrick Esser, Robin Rombach, and Bjorn Ommer. Taming transformers for high-resolution image synthesis. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 12873–12883, 2021.

[8] M. Ferrara, A. Franco, and D. Maltoni. Decoupling texture blending and shape warping in face morphing. In *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. IEEE, September 2019.

[9] Sankini Rancha Godage, Frøy Løvåsdal, Sushma Venkatesh, Kiran Raja, Raghavendra Ramachandra, and Christoph Busch. Analyzing human observer ability in morphing attack detection—where do we stand? *IEEE Transactions on Technology and Society*, 4(2):125–145, 2023. doi: 10.1109/TTS.2022.3231450.

[10] ISO/IEC JTC1 SC37 Biometrics. ISO/IEC CD 20059 - methodologies to evaluate the resistance of biometric recognition systems to morphing attacks. 2023.

[11] Minchul Kim, Anil K Jain, and Xiaoming Liu. Adaface: Quality adaptive margin for face recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022.

[12] Facial landmark based face morphing. Open CV. https://www.learnopencv.com/face-morph-using-opencv-cpp-python/.

[13] Qiang Meng, Shichao Zhao, Zhida Huang, and Feng Zhou. MagFace: A universal representation for face recognition and quality assessment. 2021.

[14] Neurotechnology. VeriLook SDK. http://www.neurotechnology.com/verilook.html.

[15] NIST. FRVT morph web site. https://pages.nist.gov/frvt/html/frvt_morph.html.

[16] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, Jin Chang, K. Hoffman, J. Marques, Jaesik 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)*, pages 947–954 vol. 1, June 2005. doi: 10.1109/CVPR.2005.268.

[17] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch. Face morphing versus face averaging: Vulnerability and detection. In *Proc. Intl. Joint Conf. on Biometrics (IJCB)*, 2017.

[18] Aravinda Reddy, Sreenivasa Rao, Raghavendra Ramachandra, and Pabitra mitra. Extswap: Leveraging extended latent mapper for generating high quality face swapping. In *International Conference on Computer Vision and Machine Intelligence (CVMI)*, pages 1–8, 2023.

[19] U. Scherhag and et al. Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In *Intl. Conf. of the Biometrics Special Interest Group BIOSIG 2017*, pages 1–7, 2017.

[20] Jag Mohan Singh and Raghavendra Ramachandra. 3d face morphing attacks: Generation, vulnerability and detection. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, pages 1–1, 2023. doi: 10.1109/TBIOM.2023.3324684.

[21] Jag Mohan Singh and Raghavendra Ramachandra. Deep composite face image attacks: Generation, vulnerability and detection. *IEEE Access*, 11:76468–76485, 2023. doi: 10.1109/ACCESS.2023.3261247.

[22] S. Venkatesh, H. Zhang, R. Raghavendra, 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. doi: 10.1109/IWBF49977.2020.9107970.

[23] S. Venkatesh, R. Raghavendra, and K. Raja. Face morphing of newborns can be threatening too : Preliminary study on vulnerability and detection. In *2021 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–8, 2021. doi: 10.1109/IJCB52358.2021.9484367.

[24] S. Venkatesh, R. Raghavendra, K. Raja, and C. Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE Transactions on Technology and Society*, 2(3):128–145, March 2021. doi: 10.1109/TTS.2021.3066254.

[25] H. Zhang, S. Venkatesh, R. Raghavendra, K. Raja, N. Damer, and C. Busch. MIP-GAN—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. doi: 10.1109/TBIOM.2021.3072349.

[26] Na Zhang, Xudong Liu, Xin Li, and Guo-Jun Qi. Morphganformer: Transformer-based face morphing and de-morphing, 2023.

[27] Raghavendra; Raja Kiran; Busch Christoph Zhang, Haoyu; Ramachandra. Morph-pipe: Plugging in identity prior to enhance face morphing attack based on diffusion model. In *Norsk IKT-konferanse for forskning og utdanning (NISK)*, volume 3, pages 1–6, 2023.