MIPGAN - Generating Robust and High Quality Morph Attacks Using Identity Prior Driven GAN

Haoyu Zhang†, Sushma Venkatesh†, Raghavendra Ramachandra†, Kiran Raja†, Naser Damer‡, Christoph Busch†
† Norwegian University of Science and Technology (NTNU), Norway
‡ Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany.

Abstract—Face morphing attacks target to circumvent Face Recognition Systems (FRS) by employing face images derived from multiple data subjects (e.g., accomplices and malicious actors). Morphed images can verify against contributing data subjects with a reasonable success rate, given they have a high degree of identity resemblance. The success of the morphing attacks is directly dependent on the quality of the generated morph images. We present a new approach for generating robust attacks extending our earlier framework for generating face morphs. We present a new approach using an Identity Prior Driven Generative Adversarial Network, which we refer to as MIPGAN (Morphing through Identity Prior driven GAN). The proposed MIPGAN is derived from the StyleGAN with a newly formulated loss function exploiting perceptual quality and identity factor to generate a high quality morphed face image with minimal artifacts and with higher resolution. We demonstrate the proposed approach’s applicability to generate robust morph attacks by evaluating it against a commercial Face Recognition System (FRS) and demonstrate the success rate of attacks. Extensive experiments are carried out to assess the FRS’s vulnerability against the proposed morphed face generation technique on three types of data such as digital images, re-digitized (printed and scanned) images, and compressed images after re-digitization from newly generated MIPGAN Face Morph Dataset. The obtained results demonstrate that the proposed approach of morph generation profoundly threatens the FRS.

Index Terms—Morph Attacks, GAN, Attack detection, Face Recognition, Vulnerability, Deep Learning

Fig. 1: Results from StyleGAN based face morphing [1] and the proposed MIPGAN (a) Contributing subject 1 (b) StyleGAN [1] (c) Proposed method (d) Contributing subject 2

1 INTRODUCTION

Face Recognition Systems (FRS) have provided ubiquitous way of assessing the identity and verifying the identity in many applications. FRS have been used in everyday applications from low security applications such as smartphone unlocking to high security applications such as identity verification in border crossing. Each of the applications mandate a chosen way of enrolment to FRS where either a supervised enrolment is carried out (for instance in on-boarding at bank premises) or unsupervised enrolment is requested

Haoyu Zhang and Sushma Venkatesh contributed equally.
work on a new kind of attack referred popularly as Morph attacks and mask attacks in the recent years, we focus our work on a new kind of attack referred popularly as Morph Attacks [3].

Face morphing is the process of combining two or more face images to generate a single face image that can resemble visually to all the contributing face images to a greater degree [3]. A good quality morphed face image is also effective in verifying against all contributing subjects by obtaining a comparison score that exceeds the pre-determined threshold (i.e., passes through FRS) [3], [4], [5], [6]. While morphing can be conducted using multiple face images of different persons, the effectiveness of morphed image is reported when the face images of similar ethnicity, gender and age group are considered [7], [8], [9]. This is primarily due to the fact that morphed image should not only defeat the FRS but should also be able to provide high visual similarity if a manual verification is conducted along with the FRS.

Face morphing attacks threaten the FRS due to the current practices in the ID-document application process, where the biometric enrolment is carried out in an unsupervised manner in many countries. Countries like the UK and New Zealand allow citizens to upload a digital face image for various applications such as passport renewal and visa application [10] in an unsupervised manner. In a similar manner, many Asian countries and European countries (e.g. in The Netherlands) request the applicant to upload a scanned face image for passport/visa/identity-card applications. Given that the images are submitted in an unsupervised setting, the applicant has the full access to upload a morphed image with malicious intent underlining the need for robust Morphing Attack Detection (MAD) mechanisms.

1.1 Related Works on Face Morph Generation

While the morphing attacks are studied in the recent years, most of the attacks are conducted using the morphed images created using facial landmarks based approaches needing high degree of supervision to first extract the facial landmarks, there upon align them and then finally blend them to generate morphs. The common set of procedures for warping/blending includes Free Form Deformation (FFD) [13], [14]. Deformation by moving least squares [15], deformation based on mass spring [16]. Bayesian framework based morphing [17] and Delaunay triangulation based morphing [18]. [19], [20], [21], [22], [23]. Due to inadvertent artifacts caused by pixel/region based morphing, the images need additional work in refining them to create highly realistic morph images. A set of post processing steps are usually included as illustrated in number of works [21], [24], [25]. Generally some set of post processing techniques such as image sharpening, edge correction, histogram equalisation, manual retouching, image enhancement to improve the brightness and contrast are used to eliminate the the artefacts generated during morphing process. In a parallel direction, morphed face images can also be generated using landmark based methods available in open-source resources like GIMP/GAP and OpenCV. Morhps generated using GIMP/GAP technique is more efficient in generating good quality morphs (i.e., less noticeable artefacts) as pixels are aligned manually. Despite the minimal amount of effort in creating morphs using such resources, a significant amount of efforts need to be dedicated to correct the artifacts. Additionally, commercial solutions like Face Fusion [26] and FantaMorph [27] can also generate reasonable quality morphed images with manual intervention. Although some steps can be excluded in creating the morphs, it is very critical to meet the face image quality standards laid out by International Civil Aviation Organization (ICAO) [28], [29] for electronic Machine Readable Travel Document (eMRTD) or passport applications.

1.2 GAN Based Face Morph Generation

In an attempt to overcome the cumbersome efforts of manually creating (semi-automated) the morphed images, fully automated approach using the Generative Adversarial Network (GAN) was proposed by Damer et al. [30]. Unlike the supervision required in extracting and aligning the face images in manual morphing, GAN based techniques synthesise morphed images directly by sampling two facial images in the latent space. In the work by Damer et al. [30], the proposed MorGAN architecture for morph generation basically employed a generator constituting encoders, decoders and a discriminator. The generator was trained to generate the images with the dimension 64 × 64 pixels which is a key limiting factor to attack the commercial FRS given they fail to meet the ICAO standards with minimum Inter-Eye Distance (IED) of 90 pixels in most countries. The empirical evaluation of generated morph images using MorGAN against two commercial FRS indicated that they fail to meet both quality standards and the verification performance [1]. Motivated to address the deficiency in MorGAN architecture, in our recent work [1] we proposed an approach based on StyleGAN architecture [31] to increase the spatial dimension to 1024 × 1024 and improved face quality. Unlike the previous approach of MorGAN [30], StyleGAN [1] achieves better spatial resolution by embedding the images in the intermediate latent space. With the increased spatial dimension of resulting morphed images from our recent architecture, we not only demonstrated that the images meet quality standards but also have a reasonable success of attacking the commercial FRS [1].

1.3 Limitations of GAN Based Face Morph Generation and Our Contributions

While our earlier work [1] indicated that better GAN architectures could result in superior quality morphs and 1. The preliminary work results were published at IJWSF-2020 in April, 2020.
could attack the FRS, we also acknowledged the limited threats to Commercial-Off-The-Shelf (COTS) FRS as they do not succeed fully. Approximately 50% of the generated morph images were able to verify against contributing subjects making the attack not very effective as noted from empirical evaluation in our earlier work [1] for a COTS FRS [32] and an open-source FRS based on ArcFace [33] unlike the landmark based morph attacks. With a clear introspection into this aspect, we notice that the resulting morphed images from our earlier work [1] do not retain high degree of facial similarity to both contributing subjects. With lower similarity to contributing subjects in terms of facial structures, the FRS do not provide high comparison score to morphed image as anticipated. In other words, the missing enforcement of identity information of contributing subjects will lead to high visual quality face image but with lower face similarity to contributing face images.

In an effort to make the attacks robust such that both the subjects can be verified with good success rate, in this work, we extend our previous architecture to generate morphs by including the identity priors before generation of morphed faces which we refer as MIPGAN (Morphing through Identity Prior driven GAN). We propose two variants of our proposed approach named as MIPGAN-I and MIPGAN-II based on the employed GAN being StyleGAN or StyleGAN2 [34] respectively. With the inclusion of a new loss function in our proposed architecture, we assert to increase the attack success rate on commercial-off-the-shelf (COTS) FRS. Figure 1 shows the example of morphed face images generated using proposed MIPGAN along with outputs of both the variants. To further achieve superior quality face morphs, we also customize the newly designed loss function to account for ghosting and blurring artifacts in an end-to-end manner with no human or manual intervention eliminating the need for high degree of intervention. As noted in Figure 2, the results from MIPGAN-I and MIPGAN-II is much coherent in retaining the structural similarity data as compared to our earlier architecture [1]. With the updated architecture to generate high quality morphs which preserves both identity information and structural correspondence, we evaluate the applicability in creating stronger attacks by creating a large scale dataset of morphed images by employing the face images derived from FRGC-V2 face database [33]. The created dataset of 1270 bona fide images and 2500 morphed images is first evaluated to measure the attack success rate by verifying the morphed images against the contributing subjects using a commercial FRS from Cognitec (FaceVACS-SDK Version 9.4.2) [32]. Further to measuring the attack success rate from the digital images, we also extend our work by printing and scanning (re-digitizing) to check the consistency of the attack success rate unlike our earlier work which was limited to investigation on digital images alone [1]. We also include the experiments on assessing the impact of compression (to 15kb following ICAO guidelines) of printed and scanned face images that simulate the real-life e-passport scenario. The key motivation to extend our work in this direction is to mimic the passport application process in many European countries and Asian countries who accept the printed-and-scanned face images for issuing the identity document like passports/e-passport.

With the extensive experimental results indicating highly satisfactory attack success rate, we also evaluate a set of MAD algorithms to benchmark the detection challenges. To this extent, we evaluate two state-of-art MAD approaches on digital morphed images, re-digitized and compressed morphed images after re-digitizing. Thus, we comprehensively cover the potential morphing attacks in digital domain and the re-digitized domain. While we note the earlier works [1] arguing that attacks in digital domain can be detected by studying the cues such as residual noise in morphing [35], patterns of noise from morphed images, histogram features of textures or the deep features [4], we also investigate the MAD capabilities for re-digitized images which do not exhibit the similar features (residual noise) as the print-scan process eliminates the digital cues and presents another set of variations. Specifically, given the nature of dataset of having a single morphed image to be determined as morphed or bona fide image, we resort to Single Image based MAD (S-MAD) approaches using two recent but robust approaches using hybrid and ensemble features [36], [37], [38], [39].

We therefore present a summary of contributions of this work as listed below:

- We present a novel approach of generating morphed face images through GAN architecture with enforced identity priors and a customized novel loss function to generate highly realistic images which we refer as MIPGAN (Morphing through Identity Prior driven GAN). We present two variants of the proposed approach for generating attacks with high success rate.
- The proposed approach (both variants) is benchmarked to measure the attack success rate by verifying a COTS FRS through studying the vulnerability using a...
newly generated dataset from our proposed architecture which is referred as MIPGAN Face Morph Dataset.

- Extensive experiments on three different data types such as (a) digital morphed images (b) print-scan morphed image (c) print-scan morphed images with compression are presented to cover the full spectrum of passport application process under morphing attacks.

- The generated images are also benchmarked against the existing MAD approaches both in digital form and the re-digitized form to provide the insights on detection challenges of SOTA approaches.

In the rest of the paper, Section 2 describes the new architecture along with the newly designed loss function to generate high quality morphs. Section 3 provides the details on the quantitative experiments indicating the vulnerability of FRS and the detection challenge. With the set of remarks and future works in this direction, we draw the conclusion in Section 5.

2 PROPOSED MORPHED FACE GENERATION

Figure 3 presents the block diagram of the proposed morphed face image generation using MIPGAN. The proposed method is based on the end-to-end optimisation using a new loss function that can preserve the identity of the generated morphed face image through enforced identity priors. The proposed MIPGAN framework is designed independently on two different GAN models based on StyleGAN [31] and StyleGAN2 [34] model. We refer the proposed scheme with StyleGAN as MIPGAN-I and with StyleGAN2 as MIPGAN-II respectively. Given the face images from the accomplice \( I_1 \) (contributing subject 1) and the malicious \( I_2 \) (contributing subject 2) data subjects, we predict the corresponding latent vectors \( L_1' \) and \( L_2' \) in the first step. In this work, we have employed a latent prediction network based on the pretrained model using ResNet50 and several tree connected layers [10]. The latent prediction network takes an image as an input and predicts the corresponding latent vector in specific StyleGAN [31] and StyleGAN2 [34] model. The predicted latent vectors thus provide the initialization for the morphed face generation that is obtained using a weighted linear average of \( L_1' \) and \( L_2' \) as follows:

\[
L_M' = \frac{w_1 * L_1' + w_2 * L_2'}{2}
\]  

(1)

Where \( w_1 \) and \( w_2 \) indicate the weights, which we have chosen to be \( w_1 = w_2 = 1 \). Equal weights are selected as shown in earlier work [41] that the morphing images generated with equal weights can indicate higher vulnerability to COTS FRS. Finally, \( L_M' \) is passed through the synthesis network (independently for StyleGAN [31] and StyleGAN2 [34] model) to generate the corresponding morphed image \( I_M \) that has a resolution of \( 1024 \times 1024 \) pixels. The generated morphed face image \( I_M' \) is then optimised using the proposed loss function to generate the high quality morphed face image. In the following section, we discuss the loss function to optimise the latent vector obtained using Equation 1.

2.1 Proposed Loss Function

The proposed loss function is based on both perceptual fidelity, quality and identity factor that can facilitate the high quality face morph generation. The common issue with the GAN based morph generation is the presence of the ghost artifacts and the blurring issues. We employ the perceptual loss with multiple layers to eliminate such effects as given by Eqn 2:

\[
\text{Loss}_{\text{perceptual}} = \frac{1}{2} \sum_i \frac{1}{N_i} || F_i(I_1) - F_i(I_M') ||_2^2
\]  

(2)

\[+ \frac{1}{2} \sum_i \frac{1}{N_i} || F_i(I_2) - F_i(I_M') ||_2^2\]

where \( N_i \) denotes the number of features in layer \( i \) and \( F \) denotes features in layer \( i \) of the perceptual network (VGG-16 in our case). We choose \( \text{conv}1_1, \text{conv}1_2, \text{conv}2_2, \text{conv}3_3 \) inspired by [12] for the combination of perceptual layers. Compared with the original combination of layers \( \text{conv}1_2, \text{conv}2_2, \text{conv}3_3, \text{conv}4_3 \) [45], our design measures low-level features instead of high-level features like style of an image and is closer to our goal of morphing faces with high quality.
The main goal of this paper is to generate the morphed face images that can significantly attack FRS. In order to achieve this, we have introduced the identity loss function based on the feedback from FRS. We employ Arcface [33] - a deep learning based FRS because of its robust and accurate performance to obtain the feedback on generated morphed face. Specifically, we employ a pretrained embedding extractor with ResNet50 as the backbone to extract the unit embedding vectors and define the identity loss by their cosine distance to improve the morph generation process as given by Eqn(3)

\[
\text{Loss}_{\text{Identity}} = \frac{1}{2} \left( 1 - \frac{\|\hat{v}_1 - \hat{v}_M\|}{\|\hat{v}_1\|\|\hat{v}_M\|} \right) + \frac{1}{2} \left( 1 - \frac{\|\hat{v}_2 - \hat{v}_M\|}{\|\hat{v}_2\|\|\hat{v}_M\|} \right)
\]

(3)

where \(\hat{v}_1, \hat{v}_2, \hat{v}_M\) respectively denotes the embedding vectors which are extracted from image \(I_1, I_2, I_M\) respectively.

To further prove the loss function is differentiable for the morphed embedding vector \(\hat{v}_M\), we define \(x_d, y_d, z_d\) to be the value of vector \(\hat{v}_1, \hat{v}_2, \hat{v}_M\) in dimension \(d\) respectively and \(d' \neq d\) to be other dimensions except \(d\). The expanded identity loss function and its partial derivative are:

\[
\text{Loss}_{\text{Identity}} = \frac{1}{2} \left( \sum_{i=1}^{l} (x_{d_i}^2 + (y_{d_i}^2) \right) + \frac{1}{2} \left( \sum_{i=1}^{l} (y_{d_i}^2) \right)
\]

(4)

\[
\frac{\partial \text{Loss}_{\text{Identity}}}{\partial z_d} = 1 - \frac{x_d}{2 \|\hat{v}_1\|} \frac{\partial}{\partial z_d} \left( \frac{z_d}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} \right)
\]

(5)

\[
\frac{\partial}{\partial z_d} \left( \frac{z_d}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} \right) = \frac{1}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} \left( \frac{2z_d^2}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} \right)
\]

\[
= \frac{2z_d^2}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} - \frac{2z_d^2}{\sqrt{\frac{z_d}{2} + \sum_{d' \neq d} z_d^2}} \sum_{d' \neq d} z_d^2
\]

\[
= \frac{(z_d^2 + \sum_{d' \neq d} z_d^2)^2}{(z_d^2 + \sum_{d' \neq d} z_d^2)}
\]

(6)

For any value \(z_d = z_d'\), it is obvious that:

\[
\lim_{\Delta z_d \to 0} \frac{\partial \text{Loss}_{\text{Identity}}(z_d' + \Delta z_d)}{\partial z_d} = 1 - \frac{(z_d'^2 + \sum_{d' \neq d} z_d'^2)^2}{(z_d'^2 + \sum_{d' \neq d} z_d'^2)}
\]

\[
= \frac{\partial \text{Loss}_{\text{Identity}}(z_d')}{\partial z_d}
\]

Hence, for any dimension of \(d\), the partial derivative of the identity loss function is continuous. Because the partial derivative with respect to each dimension is continuous, the identity loss function is differentiable for the morphed embedding vector. As we have preprocessed the embedding vectors to be unit vectors, it is even simple to make the proof for our model.

It is interesting to note that the identity loss based on the Arcface feature extractor model is trained to maximize the face class separability and thus is more sensitive to face attributes. Hence, only optimizing the identity loss cannot achieve the same reconstruction performance as the perceptual loss but applying it on the face region can effectively control the generated attributes to be recognized as both subjects.

To solve the imbalance between different subjects, we introduce an identity difference loss as given by Eqn(7)

\[
\text{Loss}_{1D-Diff} = \left( 1 - \frac{\|\hat{v}_1 \cdot \hat{v}_M\|}{\|\hat{v}_1\|\|\hat{v}_M\|} \right) - \left( 1 - \frac{\|\hat{v}_2 \cdot \hat{v}_M\|}{\|\hat{v}_2\|\|\hat{v}_M\|} \right)
\]

(7)

With the idea of Lagrange multiplier, it adds a constraint to the optimisation process to force the cosine distance between morph embedding and each of the two reference embeddings to be the same. Since \(\text{Loss}_{1D-Diff}\) is usually small with value less than 1, we apply L1 loss on the difference of two cosine distance terms to avoid vanishing gradient problem.

Finally, in order to improve the structural visibility of the generated morphed face image, we also apply the Multi-Scale Structural Similarity (MS-SSIM) loss \(L_{MS-SSIM}\) to measure the structure similarity [44]. Given two discrete non-negative signals (images in our case) \(x\) and \(y\), luminance, contrast and structure comparison measures were given by \(l, c, s\) as computed using Eqn(8)

\[
l(x, y) = (2\mu_x \mu_y + (K_1 L)^2) \mu_x^2 + \mu_y^2 + (K_1 L)^2,
\]

\[
c(x, y) = ((2\sigma_x \sigma_y + (K_2 L)^2) \sigma_x^2 + \mu_y^2 + (K_2 L)^2),
\]

\[
s(x, y) = \frac{(\sigma_x + (K_2 L)^2)}{\sigma_x \sigma_y + (K_2 L)^2},
\]

(8)

where \(\mu_x, \sigma_x\) and \(\sigma_x y\) denote the mean of \(x\), the variance of \(x\) and the covariance of \(x\) and \(y\) respectively. \(L\) is the dynamic range of the signal and \(K_1 \ll 1, K_2 \ll 1\) are two constant scalars. The MS-SSIM loss \(L_{MS-SSIM}\) is further defined by Eqn(9)

\[
L_{MS-SSIM} = l[j(x, y)]^{\alpha_j} \cdot \prod_{j=1}^{J} c[j(x, y)]^{\beta_j} [s[j(x, y)]^{\gamma_j}
\]

(9)

where \(j = 1, 2, \ldots, J\) represents the \(j\)-th scale and \(\alpha_j, \beta_j\) and \(\gamma_j\) are the factors of relative importance. As suggested in [44], we also set \(\alpha_j = \beta_j = \gamma_j, \sum_{j=1}^{J}\gamma_j = 1\) and use the resulting parameters \(\beta_1 = \gamma_1 = 0.0448, \beta_2 = \gamma_2 = 0.2856, \beta_3 = \gamma_3 = 0.3001, \beta_4 = \gamma_4 = 0.2363, \alpha_5 = \beta_5 = \gamma_5 = 0.1333\).

Thus, the proposed loss function can be formulated as:

\[
\text{Loss} = \alpha_1 \text{Loss}_{Perceptual} + \alpha_2 \text{Loss}_{1D-Diff} + \alpha_3 \text{Loss}_{MS-SSIM} + \alpha_4 \text{Loss}_{ID},
\]

(10)

where \(\alpha_1, \alpha_2, \alpha_3\) and \(\alpha_4\) are the hyper-parameters that are set to achieve both stable and generalised convergence. In this work, we empirically set \(\lambda_1 = 0.0002, \lambda_2 = 10, \lambda_3 = 1\) and \(\lambda_4 = 1\).
2.2 Training and Optimisation

The training and optimisation of the proposed method are carried out on Tensorflow version 1.13 and version 1.14 for StyleGAN and StyleGAN2, respectively. The optimisation is carried out using NVIDIA GTX 1070 8 GB GPU with CUDA version 10.0 and CUDNN version 7.5 and NVIDIA Tesla P100 PCIE 16 GB GPU. The Adam optimiser with hyper-parameters $\beta_1 = 0.9$, $\beta_2 = 0.999$ and $\epsilon = 1 \times 10^{-8}$ as recommended in the original paper \cite{97} is employed on this work. The list of morphing pairs is generated in advance with careful considerations to gender. During each optimisation process of 150 iterations, the learning rate is initially set to $\eta = 0.03$ with an exponential decay per 6 iterations of $\eta_{new} = \eta \times 0.95$.

Figure 4 illustrates the qualitative results of the proposed MIPGAN framework based on StyleGAN and StyleGAN2. Further, the qualitative results of the existing methods based on StyleGAN \cite{1} and MorGAN \cite{30} is provided alongside for the convenience of the reader in the same figure. It is interesting to note that the proposed MIPGAN generated face morph images indicates both perceptual and geometric features correspondence to both contributing subjects (for instance, malicious actor and accomplice).

3 EXPERIMENTS AND RESULTS

This section presents and discusses the experimental protocols, datasets, and quantitative results of the proposed face morphing technique. The images generated from proposed MIPGAN-I and MIPGAN-II architectures are compared with the state-of-the-art techniques based on both facial landmarks \cite{8} and StyleGAN based morph generation \cite{1}. The effectiveness of the face morphing generation techniques is quantitatively evaluated by bench-marking the vulnerability of the COTS FRS for generated morphed face images. Further, we also evaluate the morph attack detection potential by evaluating the generated morphed face images using the most recent and robust MAD techniques.

3.1 MIPGAN Face Morph Dataset

We employ the face images from FRGC-V2 face database \cite{29} to generate the MIPGAN Face Morph Dataset consisting of morphed face images using both state-of-the-art and the proposed MIPGAN technique. We have selected 140 unique data subjects from the FRGC dataset by considering the high-quality face images captured in constrained conditions that resemble the passport image quality. Among 140 data subjects, the 47 data subjects are female and 93 data subjects are male. Each data subject has a variable size of 7-21 additional captures making the whole dataset to have 1270 samples corresponding to 140 data subjects. We employ two different face morph generation techniques based on Facial landmarks constrained by Delaunay triangles with blending \cite{8} and StyleGAN \cite{1}. We do not consider MorGAN \cite{30} \cite{46} based face morph generation as it was earlier demonstrated that MorGAN does not generate ICAO compliant images and thus makes COTS FRS not vulnerable \cite{1}. All the samples are pre-processed to meet the ICAO standards \cite{29} and morphing is carried out by following the guidelines outlined earlier \cite{8} \cite{9}, i.e, careful selection of subjects based on age, gender and comparison score using FRS to make attacks realistic.

To effectively evaluate the proposed method’s quantitative performance and the existing techniques, we create three different types of attacks from morphed images, such as Digital morphed images: Morphed face images that are obtained from morph generation process in the digital domain. Print-scanned morphed images: The digital morphed images are printed and then scanned (or re-digitized) to simulate the passport application process. We have employed DNP-DS820 \cite{47} dye-sublimation photo printer to generate the print of the digital morphed and bona fide face images in this work. The use of a dye-sublimation photo printer guarantees high-quality photo printing (generally used for a passport application) and makes sure that printed photos are free from dotted patterns (or individual droplets of ink) that are resulting from the printing process of conventional printers. Each of these printed photos is then scanned (or re-digitized) using the Canon office scanner to have 300 dpi as suggested in ICAO standards \cite{29}. Print-scanned compressed morphed images: The printed and scanned images (both morphed and bona fide) are compressed to have a size of 15kb that makes it suitable to store in the e-passport. This
Fig. 5: Illustration of morphing in digital, print-scan and print-scan compression data (a) Contributing subject 1 (b) Facial landmarks [8] (c) StyleGAN [1] (d) MIPGAN-I (e) MIPGAN-II (f) Contributing subject 2

process reflects the real-life scenario of face image storage in passport systems. Thus, the overall dataset has $2500 \times 3$ (types of morph data) $\times 4$ types of morph generation technique = 30,000 morph samples and $1270 \times 3$ (types of morph data) $\times 4$ types of morph generation technique = 15,240 bona fide samples. Figure 5 illustrates the three data types of attacks that are used to evaluate the effectiveness of the proposed method and the existing methods of face morph generation. It is evident that the visual quality of the images vary largely for different attack types (for instance, the digital data attack indicates the best quality and print-scan with compression indicates the lowest quality).

3.2 Vulnerability Analysis

In order to evaluate the applicability of proposed approach in devising efficient attacks on FRS, we measure the attack success on a COTS-FRS provided by Cognitec. The Cognitec FRS (Version 9.4.2) has an operational threshold of 0.5 to successfully verify a given data subject under the consideration at False Accept Rate (FAR) of 0.1% following the guidelines of Frontex [48]. In this work, we have considered only the COTS to evaluate the vulnerability motivated from our earlier work [1] where COTS was shown to be highly vulnerable when compared with deep learning FRS. Further, we have also used the open-source deep learning based FRS using Arcface [33] to achieve the identity prior in association with the proposed method and to avoid any bias introduced by deep learning model already used for morph generation process, we employ COTS alone to report the vulnerability.

The vulnerability is assessed using two metrics of Mated Morphed Presentation Match Rate (MMPMR) [9] and Fully Mated Morphed Presentation Match Rate (FMMPMR) [1] based on the threshold provided by Cognitec FRS. For a given morph image $M_{I_1, I_2}$ obtained using two subjects, we compute the vulnerability by enrolling $M_{I_1, I_2}$ and verifying it against the corresponding contributing subjects $I_1$ and $I_2$. The obtained comparison scores $S_1$ and $S_2$ for both images $I_1$ and $I_2$ against the morphed image $M_{I_1, I_2}$ indicates the threat to FRS, if and only if both $S_1$ and $S_2$ cross the preset verification threshold at FAR = 0.1%. The corresponding metric FMMPMR [1] [41] is therefore computed as:

$$FMMPMR = \frac{1}{P} \sum_{M,P} (S_{1M}^P \geq \tau) \& (S_{2M}^P \geq \tau) \ldots \& (S_{kM}^P \geq \tau)$$

(11)

2. COTS evaluation also reflects the operational evaluation where open-source systems are typically employed, for instance in NIST FRVT tests.
Fig. 6: Vulnerability analysis using COTS-FRS on digital dataset (a) Face landmarks [8] (b) StyleGAN [1] (c) Proposed Method

Fig. 7: Vulnerability analysis using COTS-FRS on print-scan dataset (a) Face landmarks [8] (b) StyleGAN [1] (c) Proposed Method

Fig. 8: Vulnerability analysis using COTS-FRS on print-scan compression dataset (a) Face landmarks [8] (b) StyleGAN [1] (c) Proposed Method

Where \( P = 1, 2, \ldots, p \) represent the number of attempts made by presenting all probe images of the contributing subjects against \( M^i \) morphed image, \( K = 1, 2, \ldots, k \) represents the number of composite image constitute to generate the morphing image (in our case \( K = 2 \)), \( S_k^i \) represents the comparison score of the \( K^i \)th contributing subject obtained with \( P^i \) attempt corresponding to \( M^i \) morphing image and \( r \) represents the threshold value corresponding to FAR = 0.1%. The images not meeting such a requirement laid by FMMPMR is discarded to make the new dataset robust and applicable to realistic operational research. In order to also establish the relevance with respect to earlier metric, we also provide the vulnerability using MMPPM [9]. The obtained success rate, or alternatively the vulnerability of FRS is provided in Table [1].

Figure 6, Figure 7, and Figure 8 shows the scatter plots of the comparison scores obtained using COTS FRS. The horizontal and the vertical red lines in the figures indicate the threshold set at FAR = 0.1%. The Figure 6, Figure 7 and Figure 8 can be interpreted using four different quadrants. The first quadrant (bottom left quadrant) indicates the morphed image being not verified for both contributing data subjects. Thus, the large number the comparison scores in the first quadrant indicates that the morph generation method is not strong enough to deceive the COTS FRS. The second quadrant (top left quadrant) indicates the morphed image being verified to data subject-2 (one of the contributing subjects) only. The third quadrant (top right
TABLE 1: Quantitative evaluation of vulnerability of FRS from various morph generation approaches

| Morph generation type | MMPMR(%) | FMMPMR(%) | MMPMR(%) | FMMPMR(%) | MMPMR(%) | FMMPMR(%) |
|-----------------------|----------|-----------|----------|-----------|----------|-----------|
|                       | Digital  | Print-Scan| Print-Scan with compression |
| Facial Landmark       |          |           |          |           |          |           |
| StyleGAN              | 100      | 98.77     | 97.23    | 97.34     | 97.38    | 96.95     |
| MIPGAN-I              | 63.51    | 41.27     | 60.59    | 39.51     | 57.12    | 35.05     |
| MIPGAN-II             | 93.35    | 83.08     | 91.72    | 80.55     | 91.07    | 77.89     |
|                       | Male     | Female    | Male     | Female    | Male     | Female    |
| FaceLandmark          | 100      | 99.26     | 99.37    | 99.02     | 99.78    | 99.24     |
| StyleGAN              | 68.75    | 42.62     | 66.45    | 42.01     | 66.45    | 40.49     |
| MIPGAN-I              | 98.57    | 93.11     | 98.16    | 91.22     | 96.12    | 90.52     |
| MIPGAN-II             | 95.91    | 87.66     | 95.30    | 86.26     | 94.69    | 84.47     |
|                       | Combined |           |          |           |          |           |
| FaceLandmark          | 100      | 98.84     | 97.64    | 97.60     | 97.84    | 97.30     |
| StyleGAN              | 64.68    | 41.49     | 61.72    | 39.90     | 58.92    | 35.89     |
| MIPGAN-I              | 94.36    | 84.65     | 92.97    | 82.23     | 92.29    | 79.88     |
| MIPGAN-II             | 92.93    | 81.59     | 80.56    | 79.02     | 90.24    | 75.20     |

quadrant) indicates that the morphed image being verified to both the contributing data subjects (subject-1 and subject-2). Thus, the larger the number of comparison scores in this quadrant indicates higher vulnerability of COTS FRS. The fourth quadrant (bottom right quadrant) indicates the morphed image being verified as subject-1 only.

As noted from the Figure 6, Figure 7 and Figure 8, the dataset generated from the proposed approach (MIPGAN-I and MIPGAN-II) has high attack success as compared to competing method obtained using StyleGAN alone. However, it has to be noted that the dataset generated from proposed approach is highly similar to attacks from landmark based morph attacks. Further, it is interesting to note that the images obtained from the proposed approach is equally threatening the FRS in digital domain, re-digitized domain and compressed images after re-digitizing exemplifying no deterioration of attack threat due to print-scan or compression process.

As it can be noted from the Table 1, the FRS system is vulnerable to proposed attack generation mechanism to a higher degree as compared to its counterpart StyleGAN approach while having similar performance to facial landmark based approach [8]. While it can also be noted that the FMMPMR is lower than MMPMR consistently as FMMPMR imposes strict selection of attack images unlike MMPMR. MIPGAN-I based morphed images shows the marginally better performance in attacking the FRS as compared to images generated by MIPGAN-II.

3.3 Morph Attack Detection Potential

Considering the success rate of the newly generated dataset, we naturally choose to evaluate the morphing attack detection performance to also validate the robustness of existing MAD mechanism. Morph Attack Detection has been widely addressed in the literature by developing the MAD techniques based on both deep learning [49], [50], [23], [51], [52], [53] and non-deep learning [54], [20], [55], [56] approaches. Owing to the recent works detailing the applicability of Hybrid features [37] and Ensemble features [38] in detecting the morph attacks, we choose to bench-mark both Hybrid features [37] and Ensemble features [38]. While the Hybrid features [37] resort to extracting features using both scale space and color space combined with multiple classifiers, Ensemble features [38] employ a variety of textural features in conjunction with set of classifiers. In commonality, both the approaches evaluate a wide variety of MAD mechanism reported so far in a holistic manner supported by empirical results [37], [38]. In addition, the Hybrid features [37] is also validated against the ongoing NIST FRVT morph challenge dataset [39] with best performance in detecting printed and scanned morph images justifying our selection of algorithm to benchmark the newly composed database.

The performance of the MAD is presented using the ISO-IEC metrics [57] using Attack Presentation Classification Error Rate (APCER (%)) which defines the proportion of attack images (morph images) incorrectly classified as bona fide images and Bona fide Presentation Classification Error Rate (BPCER (%)) in which bona fide images incorrectly classified as attack images [57] along with the Detection Equal Error Rate (D-EER (%)). To evaluate the generated morphed face image’s attack potential, we have sub-divided the newly generated database into two sets for training and testing that consists of independent data subjects with no overlap between the splits. The training set includes 690 bona fide images and 1190 morphed images. The testing set consists of 580 bona fide and 1310 morphed images. Table 2 presents the set of results obtained on all three different
subsets (or types) of data obtained using the proposed morph generation methods.

Noting the results from Table 2 we make some concrete observations as listed below:

- The morph attack images stemming from landmark based morphs can be detected with a good success rate (with less than 2% error for re-digitized and compressed images).
- The attack images created using Style-GAN and proposed MIPGAN can be efficiently detected using both the employed approaches with high accuracy.
- Despite the approaches performing with very high accuracy, we cautiously also note the missing study targeting multiple printers and scanners. Such as variation of different printers and scanners may challenge the employed MAD mechanism needing future works to investigate this further.

4 LIMITATIONS OF CURRENT WORK AND POTENTIAL FUTURE WORKS

Despite the work presenting a new and robust approach to generate the morph attacks which is empirically evaluated using COTS FRS, this work has few noted limitations. In the current scope of work, we evaluate the impact of print and scan (re-digitizing) using one printer reflecting realistic scenario. The MAD mechanism employed in this work has not investigated wide range of printers and scanners that may impact the MAD performance. While we assert that the MAD performance may not vary extremely due to wider combination of printers and scanners, the empirical evaluation is yet to be conducted in future works.

As a second aspect, the proposed approach needs pre-selection of ethnicity for generating stronger attacks. Figure 9 shows the example morph face images generated using the proposed method using MIPGAN-I and MIPGAN-II that fail to get verified to contributing subjects when ethnicity pre-selection is not performed [8]. We notice that the selection of contributing subject plays an important role with the proposed method to generate stronger attacks with MIPGAN. It is our assertion that the selection of contributing subjects with similar geometric structure (particularly ethnicity) can improve the performance of the proposed system, but needs further investigation.

Despite our extensive experiments on MAD, another limitation is the missing study on pure generalization aspect by investigating the pre-trained MAD mechanism on the newly generated dataset. Such a study will also reveal the

| Morph Generation Type | MAD Algorithms | D-EER(%) | BPCER @ APCER = D-EER(%) | BPCER @ APCER = D-EER(%) | BPCER @ APCER = D-EER(%) |
|------------------------|---------------|---------|--------------------------|--------------------------|--------------------------|
|                        |               | Digital | Print-Scan               | Print-Scan               | Print-Scan               |
| Facial LandMarks [8]   | Hybrid Features [37] | 0.16    | 0.00                     | 1.85                     | 2.25                     |
|                        | Ensemble Features [38] | 0.00    | 0.00                     | 1.45                     | 1.71                     |
| StyleGAN [1]           | Hybrid Features [37] | 0.00    | 0.00                     | 0.00                     | 0.00                     |
|                        | Ensemble Features [38] | 0.00    | 0.00                     | 0.34                     | 0.51                     |
| MIPGAN-I               | Hybrid Features [37] | 0.00    | 0.00                     | 0.00                     | 0.00                     |
|                        | Ensemble Features [38] | 0.00    | 0.00                     | 0.00                     | 0.00                     |
| MIPGAN-II              | Hybrid Features [37] | 0.00    | 0.00                     | 0.00                     | 0.00                     |
|                        | Ensemble Features [38] | 0.00    | 0.00                     | 0.00                     | 0.00                     |

TABLE 2: Quantitative performance of different MAD algorithms on MIPGAN Morph Face dataset
scaling capability of existing MAD mechanism for newer attacks from GAN in addition to training the MAD from the GAN attack data and this has to be considered in future works in this direction.

5 Conclusion
Addressing the limitations of generating the robust morph attacks using GAN, we have proposed a new architecture for generating morph attacks in this work. The proposed approach (MIPGAN with two variants) for devising robust morphing attacks uses identity prior driven GAN with a customized loss exploiting perceptual quality and identity factors to generate realistic images that can threaten FRS greatly. To validate the new attack generation approach's attack potential, we have created a new dataset consisting of 30,000 morphed images and 15,240 bona fide images. A COTS FRS was evaluated empirically to measure the success rate of the new approach and vulnerability was reported indicating the applicability of the new approach and newly generated database. In a similar direction, the dataset is also validated for detection performance by studying two state-of-art MAD mechanisms. Despite the high attack detection success rate by employed MAD, we note that the morphed images generated by MIPGAN can severely threaten FRS in a present state without MAD in FRS.

References
[1] 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 International Workshop on Biometrics and Forensics (IWBF). IEEE, 2020, pp. 1–6.
[2] R. Raghavendra and C. Busch, “Presentation attack detection methods for face recognition systems: A comprehensive survey,” ACM Computing Surveys (CSUR), vol. 50, no. 1, pp. 1–37, 2017.
[3] M. Ferrara, A. Franco, and D. Maltoni, “The magic passport,” in IEEE International Joint Conference on Biometrics. IEEE, 2014, pp. 1–7.
[4] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, “Transferable deep-cnn features for detecting digital and print-scanned morphed face images,” in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, 2017, pp. 1822–1830.
[5] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, “Is your biometric system robust to morphing attacks?” in 2017 5th International Workshop on Biometrics and Forensics (IWBF). IEEE, 2017, pp. 1–6.
[6] R. Raghavendra, K. B. Raja, and C. Busch, “Detecting morphed face images,” in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2016, pp. 1–7.
[7] K. Raja, M. Ferrara, A. Franco, L. Spreuwers, I. Batskos, F. De Wit Marta Gomez-Barrero, U. Scherhag, D. Fischer, S. Venkatesh, J. M. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Ramachandra, C. Rathgeb, D. Frings, U. Seidel, F. Knoopjes, R. Veldhuis, D. Maltoni, and C. Busch, “Morphing attack detection – database, evaluation platform and benchmarking,” 2020.
[8] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, “Face morphing versus face averaging: Vulnerability and detection,” in IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 555–563.
[9] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. Veldhuis, L. Spreuwers, M. Schiba, D. Maltoni, P. Grother, S. Marcel, B. Ralph, R. Raghavendra, and C. Busch, “Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting,” in 2017 International Conference of the Biometrics Special Interest Group (BISIG). IEEE, 2017, pp. 1–7.
[10] Gov.uk. [Online]. Available: https://www.gov.uk/photos-for-passports/photo-requirements
[11] Department of Internal Affairs (DIA), NZ. [Online]. Available: https://www.passports.govt.nz/passport-photos/passport-photo-requirements
[12] Photo for a passport or identity-card, Netherlands. [Online]. Available: https://www.netherlandsworldwide.nl/countries/iran/living-and-working/photo-for-a-passport-or-identity-card
[13] S.-Y. Lee, K.-Y. Chwa, S. Y. Shin, and G. Wolberg, “Image metamorphosis using snakes and free-form deformations,” in SIGGRAPH, vol. 95. Citeseer, 1995.
[14] T. Ucic, “Feature-based image metamorphosis,” Computer graphics, vol. 26, p. 2, 1992.
[15] S. Schaefer, T. McPhail, and J. Warren, “Image deformation using moving least squares,” in ACM transactions on graphics (TOG). ACM, 2006, pp. 533–540.
[16] D. W. Choi and C. J. Hwang, “Image morphing using mass-spring system,” 2011.
[17] M. Bichsel, “Automatic interpolation and recognition of face images by morphing,” in Proc. of the Second Intl. Conf. on Automatic Face and Gesture Recognition. IEEE Comput. Soc. Press, 1996.
[18] A. Makrushin, T. Neubert, and J. Dittmann, “Automatic generation and detection of visually faultless facial morphs,” in Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 6: VISAPP (VISIGRAPP), 2017, pp. 39–50.
[19] J. Wu, “Face recognitionjammer using image morphing,” Dept. Elect. Comput. Eng., Boston Univ., Boston, MA, USA, Tech. Rep. ECE-2011, 2011.
[20] 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 International Workshop on Biometrics and Forensics (IWBF 2017), 2017, pp. 1–6.
[21] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, “Detection of face morphing attacks by deep learning,” in International Workshop on Digital Watermarking, 2017, pp. 107–120.
[22] U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, “On the vulnerability of face recognition systems towards morphed face attack,” in International Workshop on Biometrics and Forensics (IWBF 2017), 2017, pp. 1–6.
[23] U. Scherhag, C. Rathgeb, and C. Busch, “Towards detection of morphed face images in electronic travel documents,” in 2018 13th IAPR International Workshop on Document Analysis Systems (DAS), 2018, pp. 187–192.
[24] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, “Face swapping: Automatically replacing faces in photographs,” ACM Trans. Graph., vol. 27, no. 3, pp. 39:1–39:8, 2008. [Online]. Available: http://doi.acm.org/10.1145/1360612.1360638
[25] Y. Weng, L. Wang, X. Li, M. Chai, and K. Zhou, “Hair interpolation for portrait morphing,” Computer Graphics Forum, vol. 32, no. 7, pp. 79–84, October 2013.
[26] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, “Face recognition systems under morphing attacks: A survey,” IEEE Access, vol. 7, pp. 23,012–23,026, 2019.
[27] “Abrosoft fantamorph,” Fantamorph,Abrosoft.http://www.fantamorph.com/2020, accessed: May 2020.
[28] International Civil Aviation Organization, “Machine readable passports – part 1 – introduction,” http://www.icao.int/publications/Documents/9303_p1_cons_en.pdf International Civil Aviation Organization (ICAO), 2015.
[29] ———, “Machine readable passports – part 9 – deployment of biometric identification and electronic storage of data in eMRTDs,” http://www.icao.int/publications/Documents/WBS_pr_p9_cons_en.pdf International Civil Aviation Organization (ICAO), 2015.
[30] N. Damer, A. M. Saladi, 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), Oct 2018, pp. 1–10.
[31] T. Karras, S. Laine, and T. Aila, “A style-based generator architecture for generative adversarial networks,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 4401–4410.
[32] C. S. GmbH. (2020) Facevacs technology - version 9.4.2. [Online]. Available:https://www.cognitec.com/facevacs-technology.html
[33] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “Arcface: Additive angular margin loss for deep face recognition,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 4690–4699.
[34] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, and T. Aila, “Analyzing and improving the image quality of stylegan,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 8110–8119.

[35] 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), June 2005, pp. 947–954 vol. 1.

[36] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, “Morphed face detection based on deep color residual noise,” in ninth International Conference on Image Processing Theory, Tools and Applications (IPTA 2019). IEEE, 2019, pp. 1–5.

[37] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch, “Towards making morphing attack detection robust using hybrid scale-space colour texture features,” in IEEE International Conference on Identity, Security and Behaviour Analysis (ISBA 2019), 2019, pp. 1–7.

[38] S. Venkatesh, R. Raghavendra, K. Raja, and C. Busch, “Single image face morphing attack detection using ensemble of features,” in 23rd International Conference on Information Fusion, 2020, pp. 1–5.

[39] NIST. (2020) Frvt morph web site. [Online]. Available: https://pages.nist.gov/frvt/html/frvt_morph.html

[40] O. Richter and R. Wattenhofer, “Treeconnect: A sparse alternative to fully connected layers,” in 2018 IEEE 30th International Conference on Tools with Artificial Intelligence (ICTAI). IEEE, 2018, pp. 924–931.

[41] S. Venkatesh, K. Raja, R. Raghavendra, and C. Busch, “On the influence of ageing on face morph attacks: Vulnerability and detection,” in International Joint Conference on Biometrics (IJCB), September 2020, pp. 1–8.

[42] R. Abdal, Y. Qin, and P. Wonka, “Image2stylegan++: How to edit the embedded images?” arXiv preprint arXiv:1911.11544, 2019.

[43] J. Johnson, A. Alahi, and L. Fei-Fei, “Perceptual losses for realtime style transfer and super-resolution,” in European conference on computer vision. Springer, 2016, pp. 694–711.

[44] Z. Wang, E. P. Simoncelli, and A. C. Bovik, “Multiscale structural similarity for image quality assessment,” in The Thirty-Seventh Asilomar Conference on Signals, Systems & Computers, 2003, vol. 2. Ieee, 2003, pp. 1398–1402.

[45] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” arXiv preprint arXiv:1412.6980, 2014.

[46] N. Damer, F. Boudros, A. Mosegui Saladi, F. Kirchbuchner, and A. Kuijper, “Realistic dreams: Cascaded enhancement of generated images with an example in face morphing attacks,” 10 2019.

[47] Dnp printer. [Online]. Available: http://dnpphoto.com/en-us/Products/Printers/DS820A

[48] Frontex, “Best Practice Technical Guidelines for Automated Border Control ( ABC ) Systems,” Tech. Rep., 2012.

[49] M. Ferrara, A. Franco, and D. Maltoni, “Face morphing detection in the presence of printing/scanning and heterogeneous image sources,” CoRR, vol. abs/1901.08811, 2019. [Online]. Available: http://arxiv.org/abs/1901.08811

[50] C. Seibold, A. Hilsmann, and P. Eisert, “Style your face morph and improve your face morphing attack detector,” in 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), 2019, pp. 1–6.

[51] A. Makrushin, C. Kraetzer, J. Dittmann, C. Seibold, A. Hilsmann, and P. Eisert, “Dempster-shafer theory for fusing face morphing detectors,” in 2019 27th European Signal Processing Conference (EUSIPCO), 2019, pp. 1–5.

[52] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello, “Border control morphing attack detection with a convolutional neural network de-morphing approach,” IEEE Access, pp. 1–1, 2020.

[53] F. Peng, L.-B. Zhang, and M. Long, “FD-GAN: Face de-morphing generative adversarial network for restoring accomplice’s facial image,” IEEE Access, vol. 7, pp. 75122–75131, 2019. [Online]. Available: https://doi.org/10.1109%2FAccess.2019.2920713

[54] 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 2017 5th International Workshop on Biometrics and Forensics (WBF), 2017, pp. 1–6.

[55] C. Seibold, A. Hilsmann, and P. Eisert, “Reflection analysis for face morphing forgery detection: Application of media forensics for the detection of facial morphing,” in the presence of printing/scanning and heterogeneous image sources,” in the presence of printing/scanning and heterogeneous image sources,” in Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, ser. IH&MMSec ’17, 2017, pp. 21–32.

[56] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3. Information Technology - Biometric presentation attack detection - Part 3: Testing and Reporting, International Organization for Standardization, 2017.