This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

3D Face Morphing Attacks: Generation, Vulnerability and Detection

Jag Mohan Singh, *Member, IEEE* Raghavendra Ramachandra, *Senior Member*

Abstract—Face Recognition systems (FRS) have been found vulnerable to morphing attacks, where the morphed face image is generated by blending the face images from contributory data subjects. This work presents a novel direction toward generating face-morphing attacks in 3D. To this extent, we have introduced a novel approach based on blending the 3D face point clouds corresponding to the contributory data subjects. The proposed method will generate the 3D face morphing by projecting the input 3D face point clouds to depth maps and 2D color images, followed by the image blending and wrapping operations performed independently on the color images and depth maps. We then back-project the 2D morphing color map and the depth map to the point cloud using the canonical (fixed) view. Given that the generated 3D face morphing models will result in holes due to a single canonical view, we have proposed a new algorithm for hole filling that will result in a high-quality 3D face morphing model. Extensive experiments are carried out on the newly generated 3D face dataset comprised of 675 3D scans corresponding to 41 unique data subjects and the publicly available Facescape database with 100 unique identities. Experiments are performed to benchmark the vulnerability of the proposed 3D morph generation scheme against automatic 2D, 3D FRS and human observer analysis. We also present the quantitative assessment of the quality of the generated 3D face morphing models using eight different quality metrics. Finally, we have proposed three different 3D face Morphing Attack Detection (3D-MAD) algorithms to benchmark the performance of the 3D face morphing attack detection techniques.

Index Terms—Biometrics, Face Recognition, Vulnerability, 3D Morphing, Point Clouds, Image Morphing, Morphing Attack Detection

1 INTRODUCTION

FAce Recognition Systems (FRS) are being widely deployed in numerous applications related to security settings such as automated border control (ABC) gates and commercial settings like eCommerce and e-banking scenarios. The rapid evolution of FRS can be attributed to the advances in deep learning FRS [1], [2], which improved accuracy in real-world and uncontrolled scenarios. These factors accelerated the use of 2D face images in electronic machine-readable documents (eMRTD), which are exclusively used to verify the owner of a passport at various ID services, including border control (both automatic and human). Because most countries still use printed passport images for the passport application process, the face morphing attack has indicated the vulnerability of both human and automatic FRS [3], [4]. Face morphing is the process of blending multiple face images based on either facial landmarks [5] or Generative Adversarial Networks [6] to generate a morphing face image. The extensive analysis reported in the literature [7], [8], [9], [10] demonstrated the vulnerability of 2D face morphing images to both deep learning and commercial off-the-shelf FRS.

There exist several techniques to detect the 2D face morphing attacks that can be classified as [11] (a) Single image-based Morph Attack Detection (S-MAD): where the face Morphing Attack Detection (MAD) techniques will use the single face image to arrive at the final decision (b) Differential Morphing Attack Detection (D-MAD): where a pair of 2D face images are used to arrive at the final decision. S-MAD and D-MAD techniques have been extensively studied in the literature, resulting in several MAD techniques. The reader is advised to refer to a recent survey by Venkatesh et al. [11] to obtain a comprehensive overview of existing 2D MAD techniques. Despite the rapid progress in 2D MAD techniques, a recent evaluation report from NIST FRVT MORPH [12] indicates the degraded detection of 2D face morphing attacks. Thus, 2D MAD attacks, especially in the S-MAD scenario, present significant challenges for reliable detection. These factors motivated us to explore 3D face morphing so that depth information may provide a reliable cue that makes morphing detection easier. 3D face recognition has been widely studied over the past several decades, resulting in several real-life security-based applications with 3D face photo-based national ID cards [13], [14], [15], 3D face photo-based driving license cards [15] and 3D face-based automatic border control gates (ABC) [16]. The real case reported in [17] demonstrated using a 2D rendered face image from a 3D face model instead of a real 2D face photo to obtain the ID card bypassing the human observers in the ID card issuing protocol. Although most real-life 3D face applications are based on comparing 3D face models against 2D face images for verification, this is mainly because e-passports use 2D face images.

However, the use of 3D to 3D comparison will be realistic, especially in the border control scenario, as both ICAO 9303 [18] and ISO/IEC 19794-5 [19] standards are well defined to accommodate the 3D face model in the 3rd generation e-passport. The 3D face ID cards are a reality as they are being deployed in countries such as the UAE [13], which can facilitate both human observers and automatic FRS to achieve accurate, secure, and reliable ID verification. Further, the evolving technology has made it possible for 3D

Norwegian University of Science and Technology (NTNU), Norway
e-mail: (jag.m.singh@ntnu.no; raghavendra.ramachandra@ntnu.no).
Both authors have equally contributed to this work.

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

face imaging on handheld devices and smartphones (e.g., Apple Face ID [20] uses 3D face recognition) that can further enable remote ID verification based on 3D face verification. These factors motivated us to investigate the feasibility of generating 3D face morphing and studying their vulnerability and detection. An early attempt in [21] (master's thesis) employed the 3DMM [22] technique to generate a 3D face morphing model. However, the reported results indicate the lowest vulnerability to conventional FRS, indicating the limitation of the 3DMM..

This work presents a novel method for generating 3D face morphing using 3D point clouds. Given the 3D scans from the accomplished and malicious actors, the proposed method will project the 3D point clouds to the depth maps & the 2D color images, which are independently blended, warped, and back-projected to the 3D to obtain 3D face morphing. motivation for projecting to the 2D for morphing is to effectively address the non-rigid registration, especially with the high volume of point clouds (85K) that needs to be registered between two unique data subjects. Further, using canonical view generation to project from 3D to 2D and back project to 3D will assure a high-quality depth even for the morphed face images, thus indicating the high vulnerability of the FRS. Therefore, this is the first framework to address the generation of 3D face morphing of two unique face 3D scans that can result in vulnerability to FRS. More particularly, we aim to answer the following research questions, which will be answered systematically in this study:

- **RQ#1:** Does the proposed 3D face morphing generation technique yield a high-quality 3D morphed model?
- **RQ#2:** Does the generated 3D face morphing model indicate the vulnerability for both automatic 3D FRS and human observers?
- **RQ#3:** Are the generated 3D face morphing models more vulnerable when compared to 2D face morphing images for both automatic 3D FRS and human observers?
- **RQ#4:** Does the 3D point cloud information be used to detect the 3D face morphing attacks reliably?

We systematically address these research questions through the following contributions:

- We present a novel 3D face morphing generation method based on the point clouds obtained by fusing depth maps and 2D color images to generate the 3D face morphing model.
- Extensive analysis of the vulnerability of the generated 3D face morphing is studied by quantifying the attack success rate to 3D FRS. The vulnerability analysis is also performed using 2D FRS (deep learning and COTS).
- Human observer analysis for detecting the 3D face morphing and 2D face morphing is presented to study the significance of depth information in detecting the morphing attack.
- The quantitative analysis of the generated 3D morphed face models is presented using eight different quality features representing color and geometry.
- We present three different 3D MAD techniques based on the deep features from point clouds to benchmark the 3D face MAD.
- A new 3D face dataset with bona fide and morphed models is developed corresponding to 41 unique data subjects resulting in 675 3D scans. We collected a new 3D face dataset as we were interested in capturing high-resolution (suitable for ID enrolment) inner face data [23] Our 3D face dataset consists of raw 3D scans (number of 3D vertices between 31289 & 201065) and processed 3D scans (number of 3D vertices between 35950 & 121088), which is much higher than existing 3D face datasets[1].
- The proposed method is benchmarked on a publicly available dataset from FaceScape and the newly constructed dataset.

In the rest of the paper, we introduce the proposed method in Section 2 and experiments & results in Section 3. This is followed by a discussion about the different aspects of the proposed method in Section 4, followed by limitations & potential future-works in Section 5 and finally conclusions in Section 6.

2 Proposed Method

Figure 1 shows the block diagram of the proposed 3D face morphing generation framework based on the 3D point clouds. We are motivated to employ 3D point clouds over traditional 3D triangle mesh for two main reasons. The first is that connectivity information in a 3D triangle mesh leads to **overhead storage**, processing, managing, and manipulating the triangular meshes. Thus, 3D triangle meshes will significantly increase compute and memory, making them less suitable for low-compute devices. The second reason is that the commodity scanning devices (for example, the Artec Sensor) can reproduce detailed colored point clouds that capture appearance and geometry. Thus, allowing us to generate high-quality 3D face-morphing attacks.

However, the 3D face morphing generation using point clouds introduces numerous challenges (a) Establishing a dense 3D correspondence between two different bona fide 3D point clouds that are to be morphed. Because 3D face point clouds from two different subjects are affected by various factors such as differences in input point density, reliable detection of 3D facial key points, and estimation of affine/perspective warping (b) Locally affine deformation present between two different 3D point clouds to be morphed is difficult to estimate [24], [25], [26]. (c) The misalignment of dense 3D correspondence between the two different 3D point clouds to be morphed increases with non-rigid deformation [27].

The crucial part of 3D morphing using point clouds is reliable alignment before performing the morphing operation. Given the 3D face point clouds on the source and the target face, the point cloud registration can be defined as aligning a source point cloud to a target point cloud. The point cloud registration can be grouped into three broad categories [28] namely 1) Deformation Field, 2) Extrinsic Methods and 3) Learning-based methods. Deformation Field-based techniques could be defined as the computation of deformation between the two-point clouds, which can be achieved either by assuming pointwise position [29] variables or by pointwise affine transformations [30]. Pointwise position variables methods are simplistic as they don't

1. The reader is referred to Table 1 of 3D face datasets (inner face data only) from the survey by Egger et al. [23])

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

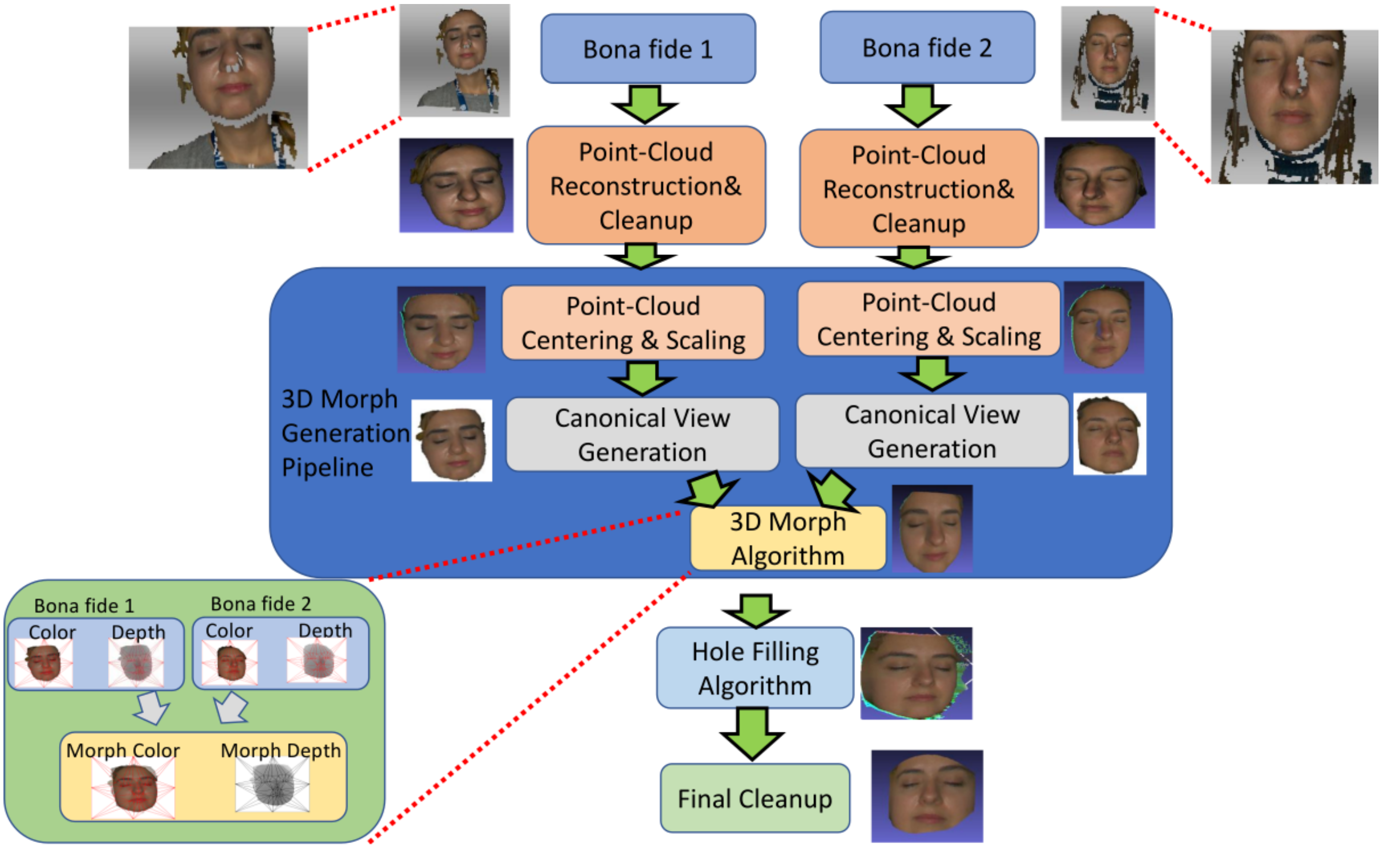

Fig. 1: Block diagram of the proposed 3D face morphing generation technique

model deformations compared with pointwise affine transformations, which model local rotations. However, since the local transformations must be stored and computed at a per-point level, this results in high computational and memory costs. This limitation was overcome by deformation field-based methods using deformation graph embedding over the initial point set, which consists of fewer nodes than the underlying point set [31], [32]. Extrinsic methods are based on optimizing an energy function to compute the point set correspondence which usually includes an alignment term and a regularization term [31]. However, the optimization-based methods compute deterministic modeling of the transformation. Probabilistic modeling of transformation was done by Myronenko et al. [33] in their algorithm Coherent Point Drift (CPD) which assumes the source points to be centroids of equally-weighted Gaussian with isotropic covariance matrix in Gaussian Mixture Model (GMM). CPD consists of alignment and regularization terms for the transformation computation and performs non-rigid registration but has memory and compute costs. However, the main limitation of optimization-based methods is that they produce good results when the input surfaces are close. Further, they require good initialization of the correspondences and the lack of these, leads to convergence to local minima. This was overcome by learning-based data-driven methods, which are of two types (1) Supervised methods and (2) Unsupervised methods. Supervised methods require ground-truth data for training [34] but can work with varying point cloud density and underlying geometry. Unsupervised methods don't require ground-truth data and can be trained using a deformation module based on CNN, followed by an alignment module to compute the deformation [35].

However, the use of existing point cloud registration for this precise application of 3D face morphing point cloud generation will pose challenges such as: **registration using the same individual**: Point cloud registration has mainly focused on the non-rigid registration of two-point clouds from the same individual [28]. This is primarily because high-quality registration aims to produce a globally consistent 3D mesh. Thus, the registration methods have not been tested when two different point clouds are registered compared to those from the same individual. **Vertex accurate correspondence**: 3D Face Morphing requires perfect vertex correspondence between the source and target point clouds, which is challenging and has not been evaluated extensively. **Low vertex count point clouds**: Point cloud registration, especially using learning-based methods, has network architectures based on point clouds with a low number of vertices (1024). Thus, registering point clouds with many vertices (75K) has not been evaluated extensively and is therefore suitable for low-resolution face images. To effectively address these challenges, the proposed method consists of four stages, including (1) point cloud reconstruction and cleanup, (2) 3D morph generation, (3) hole-filling algorithm, and (4) final cleanup. In the following subsections, these steps are discussed in detail.

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

2.1 Point Cloud Reconstruction & Cleanup

We capture a sequence of raw 3D scans using Artec Eva sensor [36] from two data subjects to be morphed (S_1 and S_2). In this work, we consider the case of morphing two data subjects at a time because of its real-life applications, as demonstrated in several 2D face morphing works [3], [11]. We process both S_1 and S_2 by performing a series of pre-processing operations such as noise filtering, texturing, and fusion of input depth maps to generate the corresponding point clouds P_1 and P_2. These operations are carried out using Artec Eva Studio SDK filters together with the Meshlab filter [37]. The cleaned and process point clouds are qualitatively shown in Figure 1.

2.2 3D Morph Generation Pipeline

In the next step, we process the point clouds P_1 and P_2 to generate a 3D face morphing point cloud by the following series of operations which are discussed below:

2.2.1 Point-Cloud Centering & Scaling

We first compute the minimum enclosing spheres using the algorithm from Gärtner et al. [38] to get the two bounding spheres with centers and radii (C_1,r_1), & (C_2,r_2) corresponding to the point cloud P_1, and P_2 respectively. Note $P_1 = (v_1^1, \ldots, v_1^{n1})$ where v_1^i is the i^{th} 3D vertex, and $n1$ is the number of points in the point cloud P_1, and $P_2 = (v_2^1, \ldots, v_2^{n2})$ where v_2^i is the i^{th} 3D vertex, and $n2$ is the number of points in the point cloud P_2. We then subtract the sphere center C_1 from each 3D vertex of P_1 and repeat the same operation on P_2 with C_2. Finally, the centered point clouds are scaled to the common radius, normalizing the 3D point clouds to the common scale. The resulting centered and scaled point clouds corresponding to P_1 and P_2 are denoted as PC_1 and PC_2, respectively. Figure 1 shows this operation's qualitative result, which shows centered and scaled 3D point clouds.

2.2.2 Canonical View Generation

This step performs the fine alignment by projecting the 3D face point clouds PC_1 and PC_2 to the canonical (fixed) view. This step aims to keep the view and projection matrix identical to the 3D face point clouds PC_1 and PC_2. We then project PC_1 and PC_2 to generate 2D color images and depth maps using the canonical view parameters. The generated 2D color images and depth maps are denoted as (I_1,D_1) and (I_2,D_2) that corresponds to the point clouds PC_1, and PC_2 respectively. We particularly choose the canonical view for the fine alignment because the traditional scheme of alignment, such as Iterative Closest Point (ICP) [27] doesn't provide a good alignment result when used on point clouds [25]. This can be attributed to the limitations of the ICP to function when a locally affine/non-rigid deformation exists between the point clouds [39] The qualitative results of the canonical view transformation are shown in Figure 1, which demonstrates the aligned 2D color images and depth maps zoomed in the inset image.

Algorithm 1 3D Face Morphing Algorithm

Input (I_1, I_2, D_1, D_2, CV)
Output (P_M)

1: Detect Facial Keypoints on K_1 on I_1, and K_2 on I_2 using Dlib [43], and generate key-points of the morph using Equation 1.
2: Perform Delaunay Triangulation on K_M which is obtained by blending K_1 and K_2 using Equation 1.
3: Estimate Affine Warping between corresponding triangles of K_1 & K_M denoted as w_1^M, and for K_2 & K_M denoted as w_2^M.
4: Apply affine warping w_1^M on I_1 to obtain I_{1M}, and on D_1 to obtain D_{1M}.
5: Apply affine warping w_2^M on I_2 to obtain I_{2M}, and on D_2 to obtain D_{2M}.
6: Obtain morphed color image I_M using the warped keypoints from the color images I_1, and I_2 using Equation 1, and morphed depth map D_M using Equation 2.
7: Obtain the morphed point cloud by back-projecting I_M, and D_M to obtain the colored 3D point cloud P_M with 3D coordinates $\forall i \in \{1, \cdots, n3\} (x_i, y_i, z_i) = (x_i, y_i, D_M(x_i, y_i))$ and color $\forall i \in \{1, \cdots, n3\} \text{Color}(x_i, y_i, z_i) = C_M(x_i, y_i))$ where $n3 = \min(n1, n2)$.

2.2.3 3D Morph Generation

Given the 2D face color images (I_1,I_2) and depth-maps (D_1,D_2) corresponding to PC_1, PC_2. We perform the morphing operation as explained in the Algorithm 1. The primary idea is to perform the morphing in 2D and back-project to 3D. The primary motivation for using a 2D morph generation method is to address the challenge of finding correspondence between PC_1 and PC_2. The underlining idea is to perform the steps of morphing (facial landmark detection, Delaunay triangulation, & warping) on 2D color images and re-use the same (facial landmark locations, triangulation, and warping) on the depth maps. In this work, we have used the blending (morphing) factor (α) as 0.5 as it is well demonstrated to be highly vulnerable in the earlier works on 2D face morphing [6]. The morphing is carried out as mentioned in the equation below:

$$
\begin{aligned}
I_M = \alpha \times I_1(K_1') + (1-\alpha) \times I_2(K_2') \\
K_1' = w_1^M(K_1) \\
K_2' = w_2^M(K_2) \\
K_M = \alpha \times K_1 + (1-\alpha) * K_2
\end{aligned}
\tag{1}
$$

where α is the blending factor, K_1 denotes 2D facial landmark locations corresponding to I_1, K_2 denotes 2D facial landmark locations corresponding to I_2, K_M is generated by blending K_1, & K_2, w_1^M denotes the warping function from K_1 to K_M, w_2^M denotes the warping function from K_2 to K_M, and I_M is the morphed 2D color image. Similarly, the same operations are carried out on the depth maps as shown in the equation below:

$$
D_M = \alpha \times D_1(K_1') + (1-\alpha) \times D_2(K_2') \tag{2}
$$

where D_M is the morphed depth map.

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

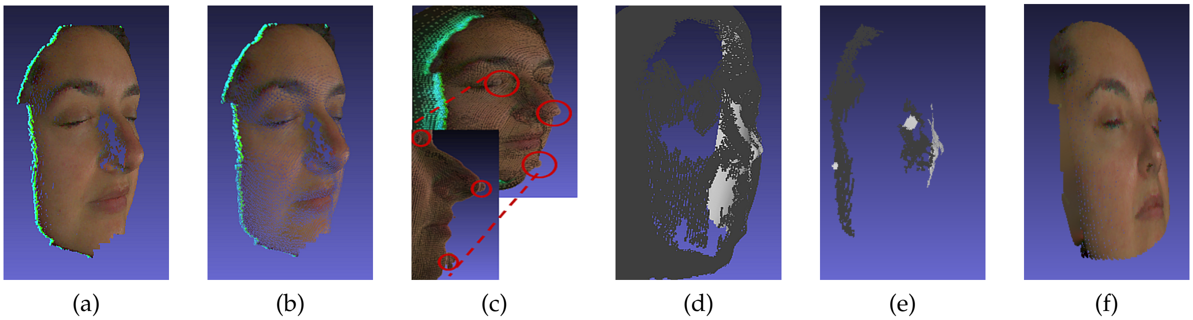

Fig. 2: Qualitative results of the hole filling algorithms (a) Input Point Cloud with holes, (b) Point Cloud with Normals which has noise, (c) Point Cloud with Screened Poisson Reconstruction [40] where artifacts are shown in the inset, (d) Point Cloud Reconstructed with APSS [41], (e) Point Cloud Reconstructed with RIMLS [42], (f) Point Cloud Hole Filled using Proposed Method

In the next step, we back-project I_M, and D_M to get the 3D face morphing point cloud $P_M = (v_M^1, \ldots, v_M^{n3})$ where $n3 = \min(n1, n2)$ is the number of vertices. Note each 3D vertex is obtained using $i = 1^{n3}(x_i, y_i, z_i) = (x, y, D_M(x, y))$ and the qualitative results is shown in Figure 1. However, generating the 3D face morphing will result in multiple holes due to a single canonical view. These holes are visible from other views. Therefore, we present a novel hole-filling algorithm to further improve the perceptual visual quality of the 3D face morphing.

Algorithm 2 Hole Filling Point Cloud

Input ($n4$-views)
Output ($C_{\mathbf{hf}}$,$D_{\mathbf{hf}}$,$P_{\mathbf{hf}}$)

1: Generate n pairs of color-maps, and depth-maps $\{(C_1, D_1), (C_2, D_2), \ldots, (C_j, D_j), \ldots, (C_{n4}, D_{n4})\}$, translated from the canonical view.
2: **for** $j \leftarrow 1$ to $n4$ **do**
3: Perform Image In-painting [44] on C_j, and D_j.
4: Perform Image Registration of C_j with the canonical view-point color-map C_{CV} using the following steps:
5: Feature Computation using Oriented FAST and Rotated BRIEF (ORB) Descriptor [45].
6: Brute-Force Matching of features using Hamming Distance.
7: Homography computation using inlier features.
8: Perspectively warp the color and depth maps using computed homography.
9: **end for**
10: Average all the registered color-maps (C_{hf}) and the depth-maps (D_{hf}).
11: Back-Project the averaged color-map and depth-map from 2D to 3D to generate hole-filled point cloud (P_{hf}) using the canonical view parameters.

2.3 Hole Filling Algorithm

In this step, we propose a new hole-filling algorithm tailored to this specific 3D face morphing generation problem. Since the holes are visible from different views, filling the holes in these views is necessary to improve the perceptual visual quality. Note that the holes are generated when the bona fide subject is looked at from a view different from the canonical camera, especially in high curvature regions such as the nose, as such areas are not completely visible from one canonical view. Therefore, we transform the 3D face morphing point cloud P_M multiple times independently to generate P_M^j where $j = 1 \ldots n4$ and $n4$ is the number of transformations and each transformation is a 3D translation [46]. In this work, we empirically choose the number of 3D translations to 7 to balance computational cost and the visual quality achieved after the hole filling. Using more 3D translations will significantly increase the computational cost and fail to improve the visual quality. We tried the conventional approach of hole filling using 3D triangulation of 3D point cloud proposed in [40], [41], [42]. Figure 2 shows the qualitative results of three different SOTA triangulation algorithms that indicate non-satisfactory results. This is because 3D orientation (3D normal) estimation indicates artifacts in the 3D triangulated mesh. Therefore, filling holes directly in the 3D point cloud is challenging, as the underlying surface (manifold) is not known in advance. The errors in 3D orientation estimation make it difficult to employ the conventional 3D hole-filling approaches.

This has motivated us to devise a new approach to achieve effective hole-filling. To this extent, we project each point cloud P_M^j to the 2D face morphing color image (C_j) and its corresponding depth map (D_j). We fill the holes in C_j & D_j using steps 2 to 9 described in Algorithm 2. Finally, we obtain the hole-filled 3D face morphing point cloud (P_{hf}) as indicated in steps 10 and 11 in Algorithm 2. Figure 2 (e) shows the qualitative results of the proposed hole filling that indicated the superior visual quality compared to the existing methods.

2.4 Final Cleanup Algorithm

The final cleanup uses a clipping region outside a portion of the bounding sphere. The final result corresponding to the proposed 3D face morphing, a point cloud, is shown in Figure 3 for an example data subjects [2]. On the whole, the following are the main advantages of the proposed method:

2. Supporting Video is available at https://folk.ntnu.no/jagms/SupportingVideo.mp4

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

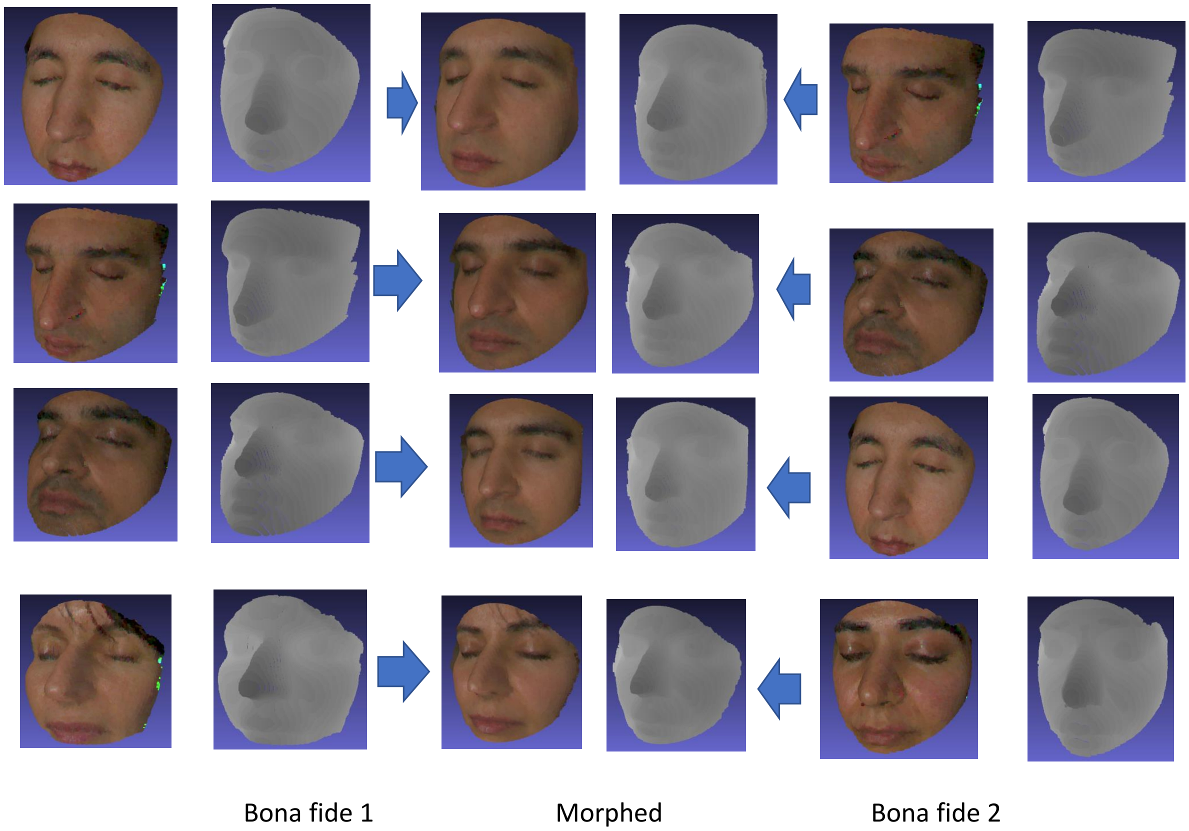

Fig. 3: Illustration of 2D color image and depth maps for bona fide and morphs generated using the proposed method

- The proposed method performs the alignment based on 2D facial key points, which preserves the identity in the generated 3D face morphing attack sample.
- The proposed method results in low computation and memory compared with existing 3D-3D techniques by overcoming the 3D registration.
- The proposed method results in a high vulnerability of FRS as the identity features are preserved for contributed data subjects used to generate the morphing attack. Therefore, the proposed method can cause high-quality 3D face morphing attacks, resulting in the vulnerability of both 2D and 3D face recognition systems.
- The proposed method can handle wide variation in the 3D pose.

2.5 Qualitative and Quantitative Comparison of Proposed Method with SOTA

To illustrate the effectiveness of the proposed method, we selected a few SOTA methods based on non-rigid point cloud registration and methods generating a 3D face model from a 2D face image. Our current evaluation of SOTA for non-rigid point cloud registration (NRPCR) methods includes CPD by Myronenko et al. [33] and Cornnet3D by Zeng et al. [47]. CPD is based on optimization and was the SOTA method for NRPCR earlier, whereas Corrnet3D is a more recent unsupervised deep learning-based method for NRPCR. Further, for evaluating methods generating a 3D face model from a 2D face image, we selected 3DMM by Blanz et al. [22] and a more recent deep-learning-based method FLAME by Li et al. [48]. 3DMM introduced the concept of the morphable model, where the parameters such as shape and texture can be controlled during 3D face synthesis. Further, 3DMM provided earlier SOTA results on 3D face generation from a 2D face image. FLAME enhanced the quality of the generated 3D face model from a 2D face image by using more controllable parameters such as pose, expression, shape and texture during the 3D face synthesis process.

2.5.1 Qualitative Comparison and Analysis

The results of qualitative comparison with SOTA are shown in Figure 4 and the quantitative vulnerability computed using MMPMR [49] and FMMPMR [50] (refer Section 3.3 for the definition of these metrics) is indicated in the Table 1. It can be noticed from Figure 4 that SOTA methods don't contain identity features of the 3D face morphing model to a large extent. However, CPD does contain the identity features of the 3D face morphing model but fails on the alignment of the two input point clouds, which results in double features such as eyebrows. Orrnet3D produces lower-quality results, which can be attributed to the fact that the authors have yet to focus on face registration exclusively. Further, 3DMM and FLAME generate a 3D face model from a 2D face image. Thus, we passed the rendering (2D face image) of the 3D face morphing model as an input. However, these methods fail to preserve the identity features during the 3D face model generation, as seen from Figure 4. The

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

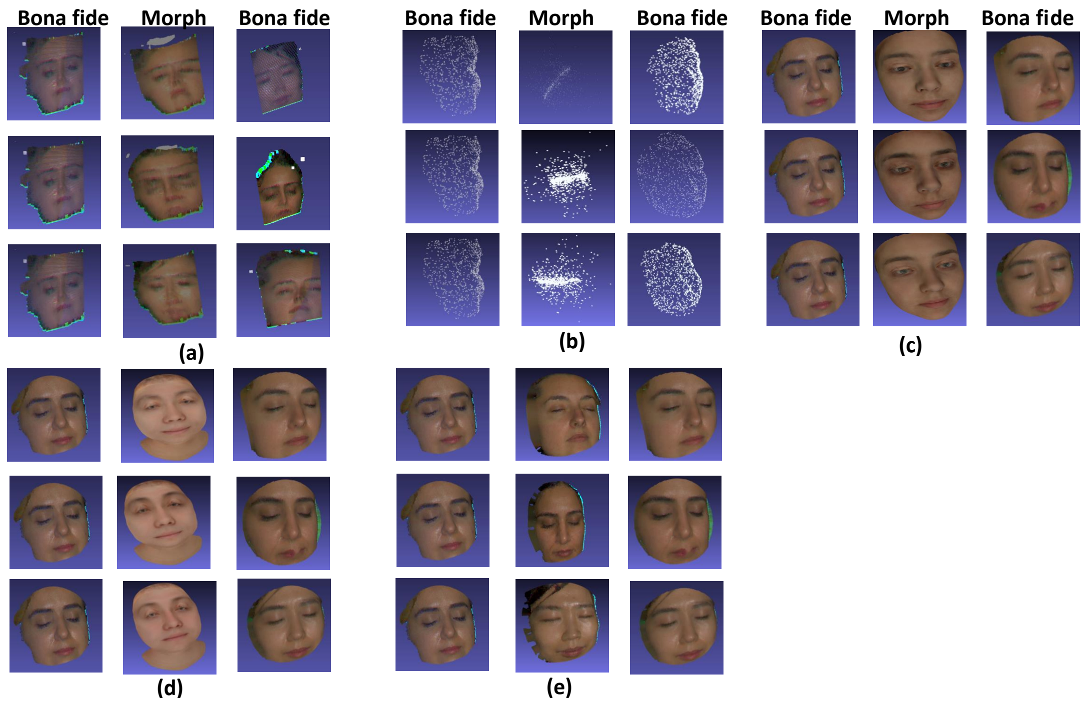

Fig. 4: Illustration of the SOTA Comparison showing Bona fide and Morphs generated using (a) CPD [33], (b) Corrnet3D [47], (c) 3DMM [22] (d) FLAME [48], (e) Proposed Method. Note that both 3DMM and FLAME need a single image as input, and in the current evaluation, we pass a 2D rendering generated using the proposed method. Note that the proposed method shows high-quality rendering and identity features of the 2D face morphing image.

generated 3D model has a low resemblance to the identity features of the face morphing image.

TABLE 1: Vulnerability of SOTA on Comparison Dataset

Feature	3DMM [22]	FLAME [48]	CPD [33]	Proposed
PointNet++ [51]	0	0	0	100%
LED3D [52]	66.67%	0	0	100%

2.5.2 Quantitative Comparison and Analysis

The results of the quantitative comparison are shown in Figure 5, where we have evaluated two 3D point feature extraction methods, namely LED3D [52] and Pointnet++ [51]. However, it can be seen that 3D comparison results in low values for SOTA compared to the proposed method. This can be attributed to the low-resolution of the identity-specific depth generation by the SOTA, which is also shown in Figure 6.

3 Experiments and Results

In this section, we present the discussion on extensive experiments carried out on the newly acquired 3D face dataset. We discuss the quantitative results of the various experiments, including vulnerability study on automatic FRS and human observer study, quantitative quality estimation based on color and geometry of the generated 3D face morphing models and automatic detection of 3D MAD attacks.

TABLE 2: Statistics of newly collected 3D Morphing Dataset (3DMD)

3D face Bona fide		
Total Data Subjects	Males	Females
41	28	13
Total 3D samples	Males	Females
330	224	106
3D face Morphs		
Total 3D Morphs	Males	Females
345	278	67

3.1 3D Face Data Collection

In this work, we have constructed a new 3D face dataset using the Artec Eva 3D scanner [36]. The data collection is carried out in an indoor lighting environment. The data subjects are asked to sit on the chair by closing their eyes to avoid the light's strong reflection from the 3D scanner. The 3D scanner is moved in the vertical direction to capture the 3D sequence.

We have used the Artec Studio Professional 14 for the 3D data collection and processing. We have collected the 3D face data from 41 subjects, including 28 males and 13 females. We have captured nine to ten samples for each data subject in three different sessions in three days. The statistics of the whole 3D face dataset are summarized in Table 2. We name our newly collected dataset as 3D Morphing Dataset (3DMD).

We may have used the existing 3D face datasets such as

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

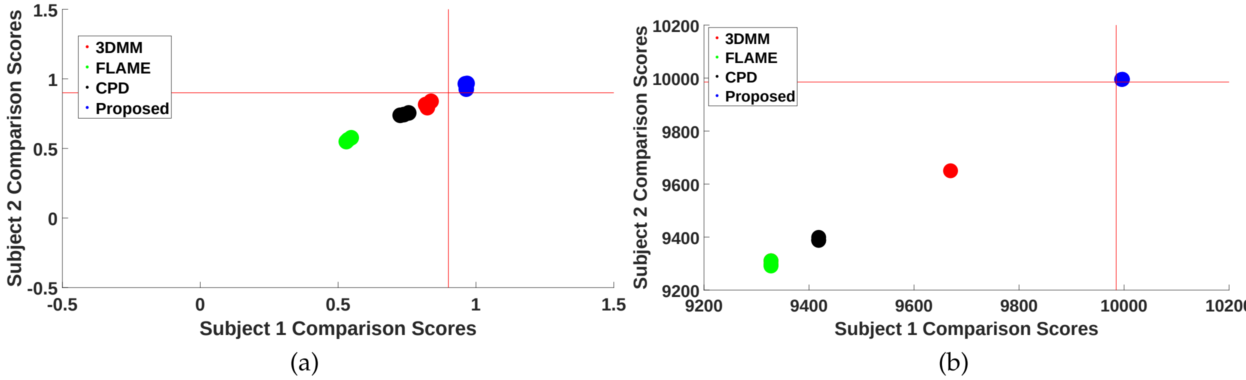

Fig. 5: Illustration showing scatter plot of Comparison scores using Bona fide and Morphs generated using Proposed Method (a) LED3D [52] and (b) Pointnet++ [51] based where SOTA algorithms are 3DMM [22], FLAME [48], CPD [33]

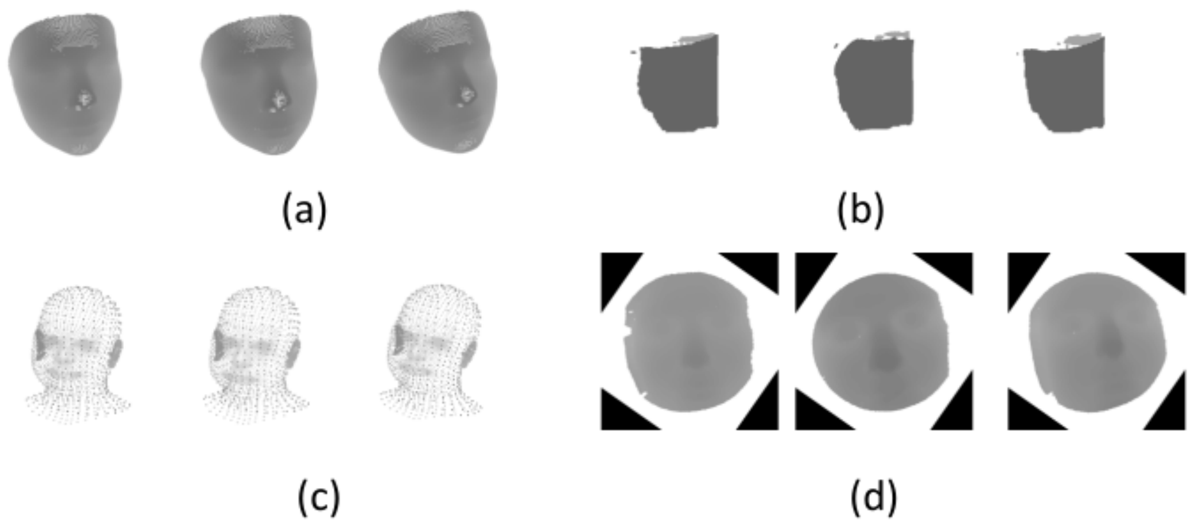

Fig. 6: Illustration showing depth maps using SOTA and proposed method (a) 3DMM [22], (b) CPD [33], (c) FLAME [48] and (d) Proposed Method.

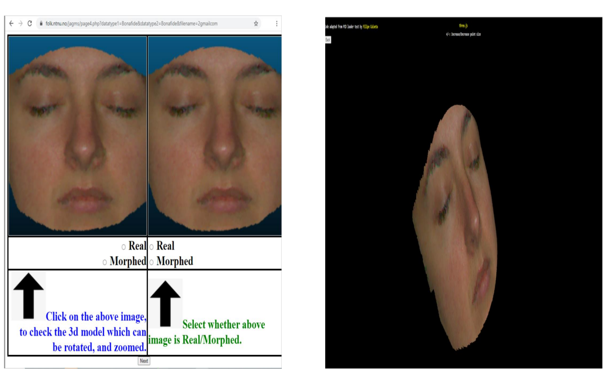

Fig. 7: Screenshots from the GUI of human observer web page (a) Full Page Screenshot, and (b) Screenshot of 3D model page.

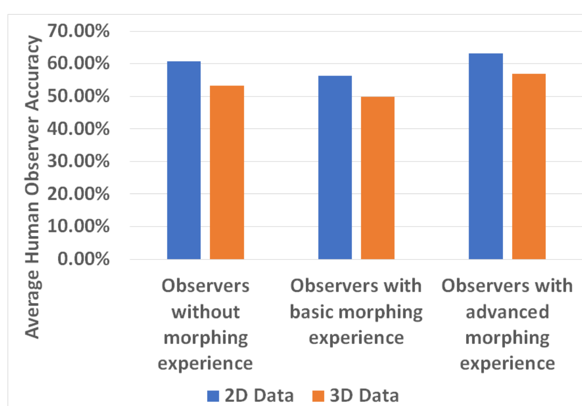

Fig. 8: Illustration of average accuracy of human observer study, note that 2D accuracy is always higher than 3D.

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

FRGC [53] and BU-3DFE [54]. However, the FRGC dataset provides a single depth map and a color image. Thus, a high-quality point cloud cannot be generated. Further, the dataset has a few misaligned color images and depth maps [55] that will result in a low-quality 3D morphing generation. The BU-3DFE [54] dataset does provide 3D models, but these are perfectly registered, and the capture conditions are identical for all the subjects. This does not model the real-world scenario of capturing 3D point clouds with changes in capture conditions that could happen during data collection. The quality of our 3D face dataset has a much higher number of 3D vertices between 35950 & 121088 for the inner face compared to previous methods [23]. These factors motivated us to generate a new 3D face dataset to enable a high-quality 3D face morphing generation suitable for the ID control scenario.

3.2 Human Observer Analysis

We perform the human observer analysis to evaluate the human detection performance of the generated 3D morphs. The survey is set up online[3] and is created using PHP, & HTML-CSS tools. GDPR norms are followed during the survey creation, and participants' email (used only for registration to avoid duplication), gender, & experience with the morphing problem are only recorded. All measures are implemented with full consideration of the anonymity of participants. We have designed the GUI for the human observer study to benchmark the single image morphing detection in this work.

Figure 7 shows the screenshot of the web portal used for the human observer's study. The GUI is designed to display two face images simultaneously, such that one corresponds to the 2D face and another to the 3D face. Then, the human observer is prompted to independently decide these face images as either morph or bona fide. The human observers are provided with an option to rotate the 3D face in different directions to make their decision effectively. Further, the opportunities to zoom in and out of the 3D face model are also provided. We have mainly selected to present both 2D/3D face images for human evaluation simultaneously to check whether the 3D information might help detect the morphing attacks. Due to the time factor, we have used 19 bona fide and 19 morph samples independently from 2D and 3D for the human observer study. Thus, each human observer spent around 20 minutes on average to complete this study. The detailed step-wise instructions on using the web portal are available for every participant beforehand.

The human observer study uses 36 observers with and without face morphing experience. The quantitative results of the human observer study are shown in Figure 8. We summarize the human observer's results from the survey as follows:

- The average detection accuracy of human observers for 2D face bona fide samples is 55.83% and 42.5% in a 3D face, respectively. The average detection accuracy of human observers for morphs in 2D is 58.33% and 51.85% in a 3D face. Thus, detection accuracy is similar for bona fide and morph in 2D. However, the detection accuracy in 3D is lower for bona fide when compared with morph.
- The average detection accuracy is similar for observers without morphing experience and basic morphing experience. Human observers with advanced morphing experience have the highest average detection accuracy. The observers without morphing experience perform similarly to observers with basic morphing experience, which can be attributed to the innate human capacity to distinguish between bona fide v/s morphed.
- The survey further validates that generated 3D morphs are challenging to detect from human observations. The average detection accuracy of human observers does not exceed 63.15%, which shows that 2D and 3D morphs developed in this work are high quality and difficult to detect.

The average detection accuracy in a 2D face is higher than that in a 3D face, which can be attributed to the following reasons:

- The fact that 2D morph is more prevalent, and thus observers generally look for specific artifacts in different regions of the face, makes the task relatively easy with a 2D face.
- The aspect of what artifacts to look at in 3D is unclear to the human observers, as they are not trained for this task.
- The quality of generated 3D morphs is high, so human observers find it difficult to distinguish the 3D morphs from the 3D bona fide.

3.3 Vulnerability Study

In this work, we benchmark the performance of the automatic FRS on both 2D and 3D face models. The 2D face vulnerability is computed using the color image and the 3D face vulnerability is calculated based on depth-map/point cloud. We have used two different metrics to benchmark the vulnerability assessment that, includes Mated Morphed Presentation Match Rate (MMPMR) [49] and Fully Mated Morphed Presentation Match Rate (FMMPMR) [50]. MMPMR can be defined as the percentage of morph samples which can be verified with all the contributing data subjects [50]. However, MMPMR does not consider the number of attempts made during score computation. This is rectified in FMMPMR [50], where the morphing image sample should be verified across all the attempts. The higher value of MMPMR and FMMPMR indicates the higher vulnerability of the FRS. The vulnerability analysis is performed by enrolling the morphing image (2D/3D) and then obtaining the comparison score by probing both contributory data subjects' face images (2D/3D). To compute the vulnerability of 2D face morphing images, we have used two different FRS such as Arcface [2] and a Commercial-off-the-Shelf (COTS) FRS [4]. The 3D face vulnerability analysis uses Deep Learning-based FRS such as Led3D [52] and PointNet++ [51]. The thresholds for all FRS used in this work are set at FAR=0.1% following the guidelines of Frontex for border control [57].

3. https://folk.ntnu.no/jagms

4. The name of the COTS is not indicated to respect confidentiality

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

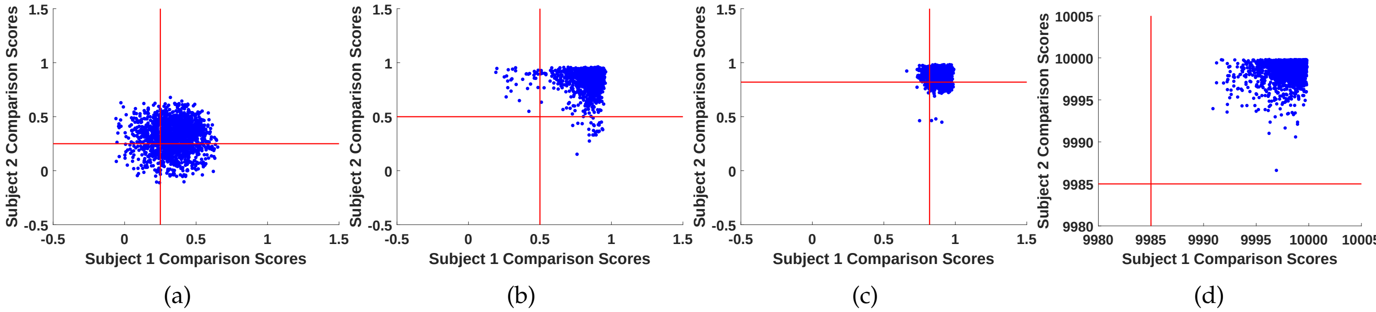

Fig. 9: Vulnerability Plots using 2D & 3D FRS on 3D Morphing dataset (3FMD) (a) 2D face FRS using Arcface [2], (b) 2D face FRS using COTS, and (c) 3D face FRS using Led3D [52], and (d) 3D face FRS using Pointnet++ [51]

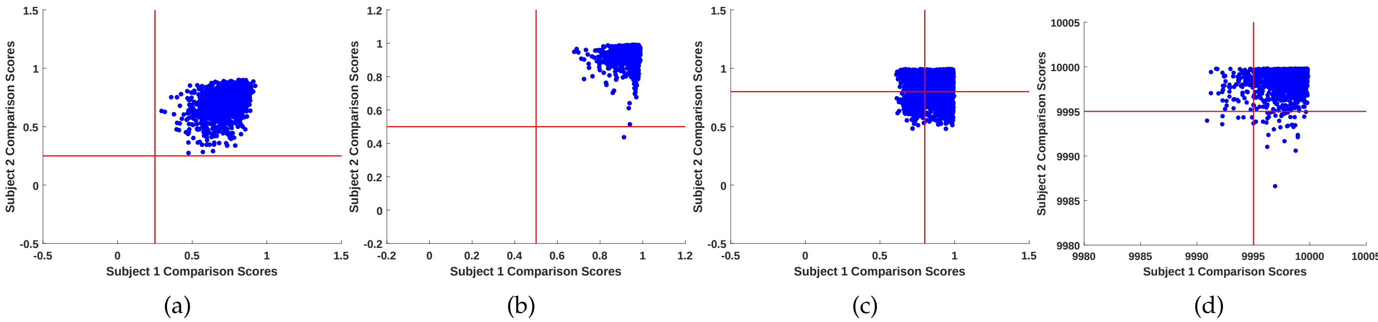

Fig. 10: Vulnerability Plots using 2D & 3D FRS on Facescape Dataset (a) 2D face FRS using Arcface [2], (b) 2D face FRS using COTS, and (c) 3D face FRS using Led3D [52], and (d) 3D face FRS using Pointnet++ [51]

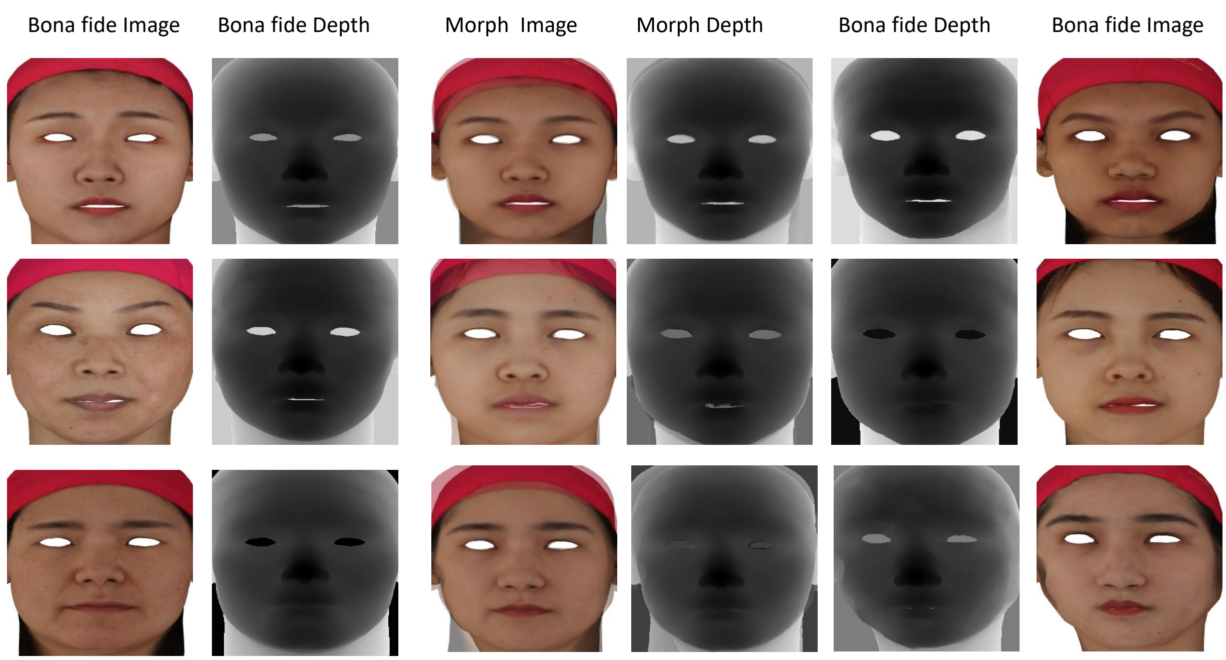

Fig. 11: Illustration of the Color Images and Depth Maps of Bona fide Samples and Face Morphs generated using the proposed method on Facescape Dataset [56]

TABLE 3: Vulnerability analysis of 2D and 3D FRS on 3D morphing dataset

Combined			Male		Female	
Algorithm	MMPMR%	FMMPR%	MMPMR%	FMMPR%	MMPMR%	FMMPR%
2D Vulnerability Analysis						
COTS	97.45%	89.78%	97.98%	90.65%	94.03%	86.36%
Arcface	63.81%	28.66%	64.92%	27.13%	59.70%	33.33%
3D Vulnerability Analysis						
LED3D [52]	81.69%	54.00%	82.67%	51.84%	77.61%	63.64%
PointNet++ [51]	95.65%	80.52%	95.32%	79.42%	95.52%	84.85%

TABLE 4: Vulnerability analysis of 2D and 3D FRS on FaceScape Dataset

Combined			Male		Female	
Algorithm	MMPMR%	FMMPR%	MMPMR%	FMMPR%	MMPMR%	FMMPR%
2D Vulnerability Analysis						
COTS	100%	99.9%	100%	99.9%	100%	100%
Arcface	100%	100%	100%	100%	100%	100%
3D Vulnerability Analysis						
LED3D [52]	88.8%	88.8%	90.5%	90.5%	84.9%	84.9%
PointNet++ [51]	95.4%	95.4%	94.1%	94.1%	97.5%	97.5%

3.3.1 Quantitative vulnerability results on 3D morphing dataset

The results are summarized in Table 3, and the vulnerability plots are shown in Figure 9. Based on the obtained results, it can be noted that (1) Both 2D and 3D FRS are vulnerable to the generated face morphing attacks (2) Among the 2D FRS, the COTS indicates the highest vulnerability compared to the Arcface FRS. (3) Among the 3D FRS the PointNet++ [51] indicates the highest vulnerability. Thus, the quantitative results of the vulnerability analysis indicate the effectiveness of the generated 3D face morphing attacks.

3.3.2 Quantitative vulnerability results on Facescape dataset

We have employed 100 unique databases with 56 male and 44 female data subjects. For each data subject, we have selected two 3D face scans. One is used to generate the 3D face morphing, and another is used as the probe image to obtain the comparison score to compute the vulnerability metrics. We then used the proposed method to get the 3D morphing models, resulting in 2486 morphing models. Figure 11 shows the example of the proposed 3D morphing generation samples together with the bona fide 3D scans from Facescape Dataset [56]. The quantitative vulnerability results on the Facescape dataset are indicated in Table 4, and the vulnerability plots are shown in Figure 10. Here also, it can be noticed that the proposed 3D face morphing generation samples exhibit a high vulnerability with both 2D and 3D FRS. Among 2D FRS, both COTS and Arcface indicate a similar vulnerability with MMPMR = 100%. However, among 3D FRS, PointNet++ [51] shows the highest vulnerability.

Thus, based on the vulnerability analysis reported on 3DMD and Facescape datasets with 2D and 3D FRS, the proposed 3D face morphing technique indicates a consistently high vulnerability. The vulnerability is noted high with the Facescape dataset compared to the 3D morphing dataset. The variation in the vulnerability performance across different FRS can be attributed to the type of feature extraction and classification techniques employed in individual FRS. For example, 2D face recognition systems are based on identity features, whereas 3D-based systems are based on high-resolution depth and shape.

3.4 Automatic 3D Face Point Cloud Quality Estimation

In this work, we estimate the visual quality based on the effectiveness of different types of features, including both color and geometry, as proposed in [58]. This study aims to quantitatively estimate the quality of the generated 3D face morphing point clouds and the bona fide 3D face point clouds to quantify the quality of the proposed morphing generation. To this extent, five different point cloud features based on geometry, namely curvature, anisotropy, linearity, planarity, sphericity, and three color information features, namely L color component, A color component, B color component, are computed to benchmark the quality based on the geometry of the generated 3D morphing models.

TABLE 5: Quantitative values of quality features for 3D face point clouds corresponding to 3D bona fide and morph based on color and geometry

3D Face Quality Features (mean ± std. deviation)	Data type	
	Bona fide	Morphed
L Color	6.5614±0.2191	6.6076±0.2340
A Color	5.9368±0.3547	5.8546±0.3260
B Color	5.7998±0.5074	5.5326±0.4198
Linearity	2.4708±0.2196	2.4911±0.1776
Sphericity	0.3318±0.0807	0.2936±0.0592
Anisotropy	0.3318±0.0807	0.2936±0.0592
Curvature	0.3330±0.0821	0.2965±0.0606
Planarity	2.4430±0.2176	2.4711±0.1733

Figure 12 shows the box plot of the eight different quality metrics for both 3D bona fide and 3D morphing point clouds. The quantitative values (mean and standard deviation) of different quality features are also shown in Table 5. As noted from Figure 9, the quality estimations, mainly

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

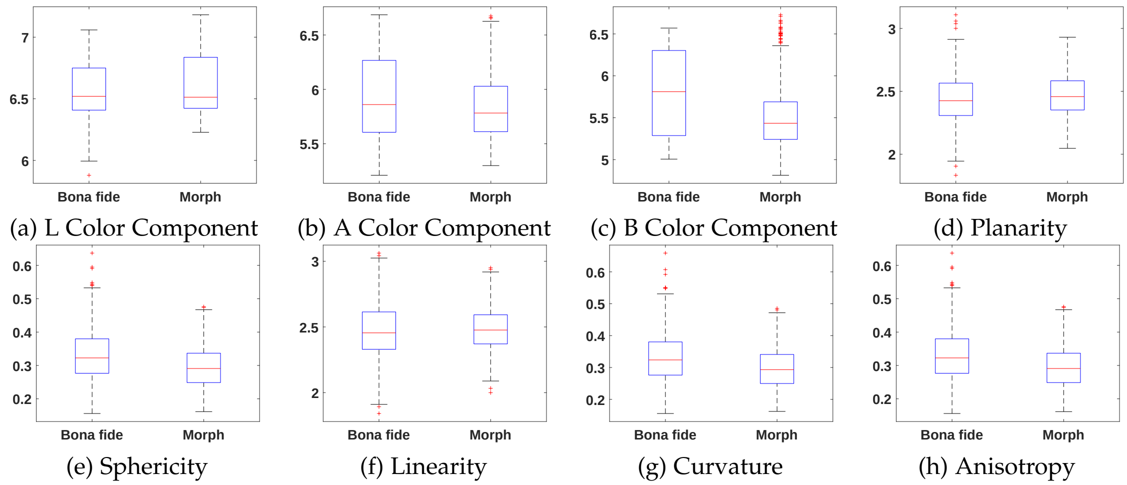

Fig. 12: Box plots showing the eight different 3D model quality estimation from 3D bona fide and 3D morph based on color and geometry

based on geometry, indicate the near-complete overlapping for 3D bona fide and 3D morph. Thus, the proposed 3D face morphing generation did not degrade the depth quality. Instead, it has achieved comparable quality based on geometry from bona fide 3D models used for the morphing operation. A similar observation can also be noted with the color image quality estimation.

3.5 3D Face Morphing Attack Detection

In this section, we present our proposed method for a single 3D model-based MAD. Because the 3D face morphing is extensively presented in this paper for the first time, there exists no state-of-the-art to detect these attacks. Therefore, we are motivated to develop 3D MAD techniques to detect these attacks reliably. The proposed 3D MAD techniques are based on the pre-trained 3D point-based networks used to extract the features, as shown in Figure 13. Thus, given the 3D face point clouds, we first compute the features from the pre-trained network and in the next step, we feed the same to the linear support vector machine to make the final decision on either bona fide or morph. In this work, we have used three different pre-trained point could networks such as Pointnet [59], [60], Pointnet++ [51], [60] and SimpleView [60] independently to benchmark the 3D MAD performance. All three pre-trained CNNs are trained on ModelNet40 dataset [61].

The Pointnet [59], [60] is one of the earliest point-based classifications of deep learning networks invariant to the permutation of 3D vertices. Given the 3D face point clouds, we extract the feature from the classification task layer corresponding to the feature dimension of 4096. The Pointnet++ [51], [60] is the improved version of Pointnet [59], [60] achieved by introducing a hierarchical neural network that was applied recursively. In this work, given the 3D face point clouds, we extract the features from the classification task layer of Pointnet++ to obtain a 40-dimensional feature vector. The SimpleView [60] network is based on projecting the point clouds to multiple view depth maps. In this work, given the 3D face point clouds, we extract the features from the classification task layer of the SimpleView network to obtain a 40-dimensional feature vector.

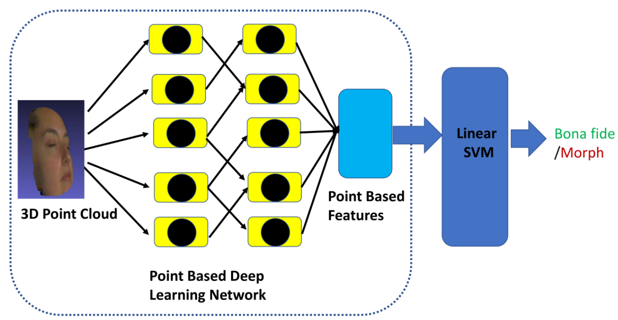

Fig. 13: Illustration of the proposed 3D face MAD

To effectively benchmark the performance of the proposed 3D MAD, we divide the newly collected dataset into two independent sets, namely training and testing. The training set consists of 3D bona fide and morphing samples from 21 unique data subjects and the testing set consists of 3D samples from 20 unique data subjects. Thus, the training set consists of 168 bona fide and 194 morphed features and the testing set consists of 160 bona fide and 151 morphed features summarized in Table 6. Table 7 shows the quantitative performance of the proposed 3D MAD techniques. Figure 14 shows the performance of individual algorithms in DET. The performance is benchmarked using ISO/IEC metrics [62] defined as Attack Presentation Classification Error Rate (APCER), which is the mis-classification rate of attack presentations and Bona fide Presentation Classification Error Rate (BPCER) is the mis-classification of bona fide presentation as attacks. Based on the results, the best performance is obtained with the SimpleView [60] network with a D-EER of 1.59%.

4 Discussion

Based on the extensive experiments and obtained results made above, the research questions formulated in Section 1 are answered below.

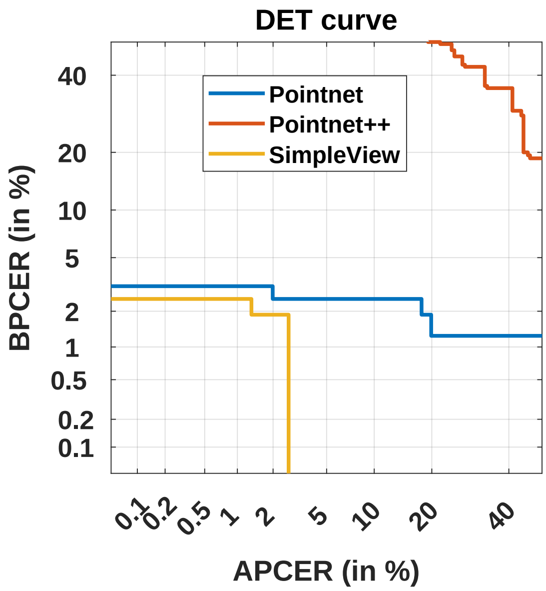

Fig. 14: DET Curve for the Proposed 3D Morphing Detection methods.

TABLE 6: Morphing Attack Detection (S-MAD) Method Protocol

Train Dataset (21 Subjects)	
Bona fide Samples	Morphing Samples
168	194
Test Dataset (20 Subjects)	
Bona fide Samples	Morphing Samples
160	151

TABLE 7: Quantitative performance of the proposed 3D MAD techniques

Algorithm Proposed Method	D-EER (%)	BPCER @ APCER =	
		5%	10%
Pointnet [59]	2.57	3.12	2.5
Pointnet++ [51]	37.33	81.87	68.12
SimpleView [60]	**1.59**	**2.5**	**0**

- **RQ#1**. Does the proposed 3D face morphing generation technique yield a high-quality 3D morphed model?
  - Yes, the proposed method of generating the 3D face morphing has resulted in a high-quality morphed model almost similar to that of the original 3D bona fide. The quality analysis reported in Figure 12 and Table 5 also justifies the quality of the generated 3D morphs quantitatively as the quality values from 3D morphing show larger overlapping with the 3D bona fide. In addition, the human observer analysis reported in Section 3.2 also justifies the quality of the proposed 3D face morphing generation method as it is found reasonably difficult to detect based on the artefacts.
- **RQ#2**. Does the generated 3D face morphing model indicate the vulnerability for both automatic 3D FRS and human observers?
  - Yes, based on the analysis reported in Section 3.3, the generated 3D face morphing model indicates a high degree of vulnerability for both automatic 3D FRS and human observers.
- **RQ#3**. Are the generated 3D face morphing models more vulnerable when compared to 2D face images for both automatic 3D FRS and human observers?
  - Equally vulnerable, the 3D face morphing models are more vulnerable than their 2D counterparts, as shown in Figure 9 when using automatic FRS.
  - However, the vulnerability is almost comparable when evaluated by a human observer study (see Section 3.2), where one of the main reasons could be more prevalence of 2D morphs, which makes human observers sensitive about which artifacts to look for.
- **RQ#4**.Can the 3D point cloud information be used to detect the 3D face morphing attacks reliably?
  - Yes, on using the proposed 3D face morphing attack Detection approaches (see Section 3.5) the point cloud information can be used for reliable 3D morphing detection.

5 Limitations of Current Work and Potential Future Works

Although the work presents a new dimension for face morphing attack generation and detection, especially in 3D, this work has a few limitations. In the current scope of work, the 3D morph generation and detection are carried out on the high-quality 3D scans collected using the Artec Eva sensor. We have employed high-quality 3D face scans to achieve good enrolment quality scans that may reflect the real-life ID enrolment scenario. Thus, future works could investigate the proposed 3D morphing generation and detection techniques using low-quality (depth) 3D scans. Further, extending the study towards in-the-wild capture can also be considered in future work. As a second aspect, the analysis is carried out using 41 data subjects due to the present pandemic outbreak. However, we have also presented the results on the publicly available 3D face dataset, Facescape, with 100 unique IDs. Future work can benchmark the proposed method on large-scale datasets with different 3D resolutions. As a third aspect, cleaning noise from 3D scans is tedious and sometimes requires manual intervention. Thus, future work can develop a fully automated noise removal in 3D point clouds to easily the 3D morph generation.

6 Conclusion

This work presented a new dimension for face morphing attack generation and detection, especially in 3D. We have introduced a novel algorithm to generate high-quality 3D face morphing models using point clouds. To validate the attack potential of the newly generated 3D face morphing attacks, the vulnerability analysis uses 2D and 3D FRS. Further, the human observer analysis is also presented to investigate the usefulness of 3D information in morph detection. Obtained results justify the high vulnerability of the proposed 3D face morphing models. We also presented an automatic quality analysis of the generated 3D morphing models that indicate a similar quality as the bona fide 3D scans. Finally, we have proposed three different 3D MAD algorithms to detect the 3D morphing attacks using pre-trained point-based CNN models. Extensive experiments

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3324684

indicate the efficacy of the proposed 3D MAD algorithms in detecting 3D face morphing attacks.

REFERENCES

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

[2] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4685–4694.

[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, and C. Busch, "Detecting morphed face images," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–7.

[5] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008–1017, 2017.

[6] 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*, vol. 3, no. 3, pp. 365–383, 2021.

[7] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel *et al.*, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 2017, pp. 1–7.

[8] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2017, pp. 555–563.

[9] N. Damer, A. M. Saladie, 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)*. IEEE, 2018, pp. 1–10.

[10] 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)*. IEEE, 2020, pp. 1–6.

[11] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face morphing attack generation & detection: A comprehensive survey," *IEEE Transactions on Technology and Society*, 2021.

[12] M. Ngan, P. Grother, K. Hanaoka, and J. Kuo, "Part 4: Morph - performance of automated face morph detection," https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf, 2021, [Online; accessed 16-October-2021].

[13] A. A. Deeb, "Uae reviews features of new id card, 3d photo included," https://www.gulftoday.ae/news/2021/08/05/uae-reviews-features-of-new-id-card-3d-photo-included, 2020, [Online; accessed 16-October-2021].

[14] IDEMIA, "Stereo laser image," https://www.idemia.com/wp-content/uploads/2021/02/stereo-laser-image-idemia-brochure-202007.pdf, 2020, [Online; accessed 18-October-2021].

[15] J. W. J. ter Hennepe, "3d photo id," https://www.icao.int/Meetings/AMC/MRTD-SEMINAR-2010-AFRICA/Documentation/11_Morpho-3DPhotoID.pdf, 2010, [Online; accessed 16-October-2021].

[16] D. Face Based ABC Systems, "3d face enrolment for id cards," http://cubox.aero/cubox/php/en_product01-2.php?product=1/, 2021, [Online; accessed 18-October-2021].

[17] S. Dent, "Using a 3d render as a french id card 'photo'," https://engt.co/3EiPnQv, 2017, [Online; accessed 16-October-2021].

[18] ICAO, "Machine readable travel documents. part 11: Security mechanisms for mrtds. technical report doc 9303," 2021.

[19] ISO/IEC JTC1 SC37 Biometrics, "ISO/IEC 39794-5:2019 information technology — extensible biometric data interchange formats — part 5: Face image data," 2019.

[20] "Apple Face ID," https://en.wikipedia.org/wiki/Face_ID, 2017.

[21] S. P. Vardam, "Vulnerability of 3d face recognition systems of morphing attacks," August 2021. [Online]. Available: http://essay.utwente.nl/88470/

[22] V. Blanz and T. Vetter, "A morphable model for the synthesis of 3d faces," in *Proceedings of the 26th annual conference on Computer graphics and interactive techniques*, 1999, pp. 187–194.

[23] B. Egger, W. A. Smith, A. Tewari, S. Wuhrer, M. Zollhoefer, T. Beeler, F. Bernard, T. Bolkart, A. Kortylewski, S. Romdhani *et al.*, "3d morphable face models—past, present, and future," *ACM Transactions on Graphics (TOG)*, vol. 39, no. 5, pp. 1–38, 2020.

[24] Y. Yao, B. Deng, W. Xu, and J. Zhang, "Quasi-newton solver for robust non-rigid registration," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.

[25] H. Li, R. W. Sumner, and M. Pauly, "Global Correspondence Optimization for Non-Rigid Registration of Depth Scans," *Computer Graphics Forum*, 2008.

[26] N. Gelfand, N. J. Mitra, L. J. Guibas, and H. Pottmann, "Robust global registration," in *Symposium on Geometry Processing*, 2005, pp. 197–206.

[27] P. J. Besl and N. D. McKay, "Method for registration of 3-d shapes," in *Sensor fusion IV: control paradigms and data structures*, vol. 1611. International Society for Optics and Photonics, 1992, pp. 586–606.

[28] B. Deng, Y. Yao, R. M. Dyke, and J. Zhang, "A survey of non-rigid 3d registration," *arXiv preprint arXiv:2203.07858*, 2022.

[29] M. Liao, Q. Zhang, H. Wang, R. Yang, and M. Gong, "Modeling deformable objects from a single depth camera," in *2009 IEEE 12th International Conference on Computer Vision*, 2009, pp. 167–174.

[30] J. Yang, D. Guo, K. Li, Z. Wu, and Y.-K. Lai, "Global 3d non-rigid registration of deformable objects using a single rgb-d camera," *IEEE Transactions on Image Processing*, vol. 28, no. 10, pp. 4746–4761, 2019.

[31] H. Li, R. W. Sumner, and M. Pauly, "Global correspondence optimization for non-rigid registration of depth scans," in *Computer graphics forum*, vol. 27, no. 5. Wiley Online Library, 2008, pp. 1421–1430.

[32] K. Zampogiannis, C. Fermüller, and Y. Aloimonos, "Topology-aware non-rigid point cloud registration," *CoRR*, vol. abs/1811.07014, 2018. [Online]. Available: http://arxiv.org/abs/1811.07014

[33] A. Myronenko and X. Song, "Point set registration: Coherent point drift," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 12, pp. 2262–2275, 2010.

[34] G. Trappolini, L. Cosmo, L. Moschella, R. Marin, S. Melzi, and E. Rodolà, "Shape registration in the time of transformers," *Advances in Neural Information Processing Systems*, vol. 34, 2021.

[35] Y. Zeng, Y. Qian, Z. Zhu, J. Hou, H. Yuan, and Y. He, "Corrnet3d: unsupervised end-to-end learning of dense correspondence for 3d point clouds," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 6052–6061.

[36] "Artec eva sensor," https://bit.ly/3BiGnJ1, 2021, [Online; accessed 16-October-2021].

[37] P. Cignoni, M. Callieri, M. Corsini, M. Dellepiane, F. Ganovelli, and G. Ranzuglia, "MeshLab: an Open-Source Mesh Processing Tool," in *Eurographics Italian Chapter Conference*, V. Scarano, R. D. Chiara, and U. Erra, Eds. The Eurographics Association, 2008.

[38] B. Gärtner, "Fast and robust smallest enclosing balls," in *European symposium on algorithms*. Springer, 1999, pp. 325–338.

[39] D. Haehnel, S. Thrun, and W. Burgard, "An extension of the icp algorithm for modeling nonrigid objects with mobile robots," in *IJCAI*, vol. 3, 2003, pp. 915–920.

[40] M. Kazhdan and H. Hoppe, "Screened poisson surface reconstruction," *ACM Trans. Graph.*, vol. 32, no. 3, jul 2013. [Online]. Available: https://doi.org/10.1145/2487228.2487237

[41] G. Guennebaud and M. Gross, "Algebraic point set surfaces," *ACM Trans. Graph.*, vol. 26, no. 3, p. 23–es, Jul. 2007. [Online]. Available: https://doi.org/10.1145/1276377.1276406

[42] A. C. Öztireli, G. Guennebaud, and M. Gross, "Feature preserving point set surfaces based on non-linear kernel regression," in *Computer graphics forum*, vol. 28, no. 2. Wiley Online Library, 2009, pp. 493–501.

[43] D. E. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, pp. 1755–1758, 2009.

[44] A. Telea, "An image inpainting technique based on the fast marching method," *Journal of graphics tools*, vol. 9, no. 1, pp. 23–34, 2004.

[45] E. Rublee, V. Rabaud, K. Konolige, and G. Bradski, "Orb: An efficient alternative to sift or surf," in *2011 International Conference on Computer Vision*, 2011, pp. 2564–2571.

[46] J. D. Foley, A. Van Dam, S. K. Feiner, J. F. Hughes, and R. L. Phillips, *Introduction to computer graphics*. Addison-Wesley Reading, 1994, vol. 55.

[47] Y. Zeng, Y. Qian, Z. Zhu, J. Hou, H. Yuan, and Y. He, "Corrnet3d: Unsupervised end-to-end learning of dense correspondence for 3d point clouds," in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021, pp. 6048–6057.

[48] T. Li, T. Bolkart, M. J. Black, H. Li, and J. Romero, "Learning a model of facial shape and expression from 4D scans," *ACM Transactions on Graphics, (Proc. SIGGRAPH Asia)*, vol. 36, no. 6, pp. 194:1–194:17, 2017. [Online]. Available: https://doi.org/10.1145/3130800.3130813

[49] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Ramachandra, 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 (BIOSIG)*, 2017, pp. 1–7.

[50] 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)*, 2020, pp. 1–6.

[51] C. R. Qi, L. Yi, H. Su, and L. J. Guibas, "Pointnet++: Deep hierarchical feature learning on point sets in a metric space," *arXiv preprint arXiv:1706.02413*, 2017.

[52] G. Mu, D. Huang, G. Hu, J. Sun, and Y. Wang, "Led3d: A lightweight and efficient deep approach to recognizing low-quality 3d faces," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019.

[53] 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)*, vol. 1, 2005, pp. 947–954 vol. 1.

[54] L. Yin, X. Wei, Y. Sun, J. Wang, and M. J. Rosato, "A 3d facial expression database for facial behavior research," in *7th international conference on automatic face and gesture recognition (FGR06)*. IEEE, 2006, pp. 211–216.

[55] T. Maurer, D. Guigonis, I. Maslov, B. Pesenti, A. Tsaregorodtsev, D. West, and G. Medioni, "Performance of geometrix activeidˆ tm 3d face recognition engine on the frgc data," in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)-Workshops*. IEEE, 2005, pp. 154–154.

[56] H. Yang, H. Zhu, Y. Wang, M. Huang, Q. Shen, R. Yang, and X. Cao, "Facescape: A large-scale high quality 3d face dataset and detailed riggable 3d face prediction," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.

[57] FRONTEX, "Best practice technical guidelines for automated border control abc systems," 2015.

[58] Z. Zhang, "No-reference quality assessment for 3d colored point cloud and mesh models," *arXiv preprint arXiv:2107.02041*, 2021.

[59] C. R. Qi, L. Yi, H. Su, and L. J. Guibas, "Pointnet++: Deep hierarchical feature learning on point sets in a metric space," 2017. [Online]. Available: https://arxiv.org/abs/1706.02413

[60] A. Goyal, H. Law, B. Liu, A. Newell, and J. Deng, "Revisiting point cloud shape classification with a simple and effective baseline," *International Conference on Machine Learning*, 2021.

[61] Z. Wu, S. Song, A. Khosla, X. Tang, and J. Xiao, "3d shapenets for 2.5d object recognition and next-best-view prediction," *CoRR*, vol. abs/1406.5670, 2014. [Online]. Available: http://arxiv.org/abs/1406.5670

[62] ISO/IEC JTC1 SC37 Biometrics, "ISO/IEC IS 30107-3. information technology - biometric presentation attack detection - part 3: Testing and reporting," 2017.

Jag Mohan Singh (Member, IEEE) received the B.Tech. (Hons.) and M.S. by research in computer science degrees from the International Institute of Information Technology (IIIT), Hyderabad, in 2005 and 2008, respectively. He is currently in the final year of his Ph.D. with the Norwegian Biometrics Laboratory (NBL), Norwegian University of Science and Technology (NTNU), Gjøvik. He worked with the industrial research and development departments of Intel, Samsung, Qualcomm, and Applied Materials, India, from 2010 to 2018. He has published several papers at international conferences focusing on presentation attack detection, morphing attack detection and ray-tracing. His current research interests include generalizing classifiers in the cross-dataset scenario and neural rendering.

Raghavendra Ramachandra obtained a Ph.D. in computer science and technology from the University of Mysore, Mysore India and Institute Telecom, and Telecom Sudparis, Evry, France (carried out as collaborative work) in 2010. He is currently a full professor at the Institute of Information Security and Communication Technology (IIK), Norwegian University of Science and Technology (NTNU), Gjøvik, Norway. He is also working as R&D chief at MOBAI AS. He was a researcher with the Istituto Italiano di Tecnologia, Genoa, Italy, where he worked with video surveillance and social signal processing. His main research interests include deep learning, machine learning, data fusion schemes, and image/video processing, with applications to biometrics, multi-modal biometric fusion, human behaviour analysis, and crowd behaviour analysis. He has authored several papers and is a reviewer for several international conferences and journals. He also holds several patents in biometric presentation attack detection and morphing attack detection. He has also been involved in various conference organising and program committees and has served as an associate editor for various journals. He has participated (as a PI, co-PI or contributor) in several EU projects, IARPA USA and other national projects. He is serving as an editor of the ISO/IEC 24722 standards on multi-modal biometrics and an active contributor to the ISO/IEC SC 37 standards on biometrics. He has received several best paper awards, and he is also a senior member of IEEE.