IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 February 2023, accepted 16 March 2023, date of publication 23 March 2023, date of current version 27 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3261247

RESEARCH ARTICLE

Deep Composite Face Image Attacks: Generation, Vulnerability and Detection

JAG MOHAN SINGH, (Member, IEEE), AND RAGHAVENDRA RAMACHANDRA, (Senior Member, IEEE)

Norwegian Biometrics Laboratory, Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), 2815 Gjøvik, Norway

Corresponding author: Jag Mohan Singh (jag.m.singh@ntnu.no)

This work was supported by the Norwegian Biometrics Laboratory, Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway.

ABSTRACT Face manipulation attacks have drawn the attention of biometric researchers because of their vulnerability to Face Recognition Systems (FRS). This paper proposes a novel scheme to generate Composite Face Image Attacks (CFIA) based on facial attributes using Generative Adversarial Networks (GANs). Given the face images corresponding to two unique data subjects, the proposed CFIA method will independently generate the segmented facial attributes, then blend them using transparent masks to generate the CFIA samples. We generate 526 unique CFIA combinations of facial attributes for each pair of contributory data subjects. Extensive experiments are carried out on our newly generated CFIA dataset consisting of 1000 unique identities with 2000 bona fide samples and 526000 CFIA samples, thus resulting in an overall 528000 face image samples. We present a sequence of experiments to benchmark the attack potential of CFIA samples using four different automatic FRS. We introduced a new metric named Generalized Morphing Attack Potential (G-MAP) to benchmark the vulnerability of generated attacks on FRS effectively. Additional experiments are performed on the representative subset of the CFIA dataset to benchmark both perceptual quality and human observer response. Finally, the CFIA detection performance is benchmarked using three different single image based face Morphing Attack Detection (MAD) algorithms. The source code of the proposed method together with CFIA dataset will be made publicly available: https://github.com/jagmohaniiit/LatentCompositionCode

INDEX TERMS Biometrics, face recognition, morphing attacks, image compositing, vulnerability, generalized morphing attack potential, composite attack detection.

I. INTRODUCTION

FRS demonstrates highly accurate verification rates, which has led to their widespread usage in eCommerce, online banking, surveillance and security applications. The recent advances in deep learning techniques have further increased the accuracy of the FRS [1], [2] that enabled them to be deployed in the border control applications. However, the FRS is vulnerable to various attacks, among which the face morphing attacks have gained attention due to their impact on the border control applications. Recent benchmarking results reported in NIST FRVT MOPRH [3] indicate that the higher the accuracy of the FRS, the higher the vulnerability for the morphing attacks.

One of the most widely used attacks toward FRS is the Presentation Attacks (PA), a.k.a spoofing attacks, which can be achieved by presenting a biometric artefact to the biometric capture device. PA can be performed by generating a Presentation Attack Instrument (PAI) that includes either a printed photo (print-photo), displaying an image (display-photo), displaying a video (replay-video), or the use of a rigid/non-rigid 3D face mask (mask-attack). Biometric researchers had thus devised Presentation Attack Detection (PAD) as a countermeasure to PA that is extensively discussed in [4], and [5].

The second type of widely studied attack on the FRS is the adversarial attack, which can be performed by applying a small perturbation (noise), a.k.a adversarial perturbation,

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Liu.

to a facial image. Even though the introduced perturbation is indistinguishable to the human eye but can lead to mis-classification with high-confidence [6] and can be used to expose vulnerabilities of the FRS. Adversarial attacks have shown high vulnerability in FRS, especially on the deep learning-based FRS [7]. The white box adversarial attack requires complete knowledge of the underlying deep learning model. Adversarial attacks could also be black-box attack performed during testing, and the attacker does not know the underlying deep-learning model. Several countermeasures to address the adversarial attacks are extensively discussed in [8] and [9]. It needs to be pointed out that adversarial attacks are digital when performed on images, but they can also be performed in the physical world by using a unique eyeglass for impersonation [8].

Face morphing attacks are gaining high momentum in the biometric community. The face morphing process seamlessly combines face images from two or more subjects (also called contributory subjects) to generate a morphing image. The generated morphing image shows substantial visual similarity to both contributory subjects therefore challenging to detect by the experts (border guards and police) [10], [11], [12], [13]. Notably, the morphed images will get verified to both the contributory subjects when used with automatic FRS [10]. Therefore, the morphing attacks can be instrumented to acquire the ID documents like passports, driving licenses, bank accounts, etc. For example, a subject with criminal background can obtain a passport by collaborating with an accomplice to generate a morphing image. Then, the accomplice can apply for an ID document using the morphed image. The subject with a criminal background can use the obtained ID document to cross the border [10], [11].

Face morphing can be generated using algorithms based on facial landmarks such as Face Morpher [14] and UBO-Morph [15]. More recently, algorithms based on Generative Adversarial Networks (GANs) such as MorGAN [16], MIPGAN [17] and ReGenMorph [18] have also been used to generate face morphing images. These generated face morphing images have demonstrated the high vulnerability of FRS, especially in the passport application scenario, including automatic border control. Further, morphing attacks can deceive both human observers (border control officers) and automatic FRS in Automatic Border Control (ABC) [10], [12], [19]. Following the initial paper [11], there have been several papers on morphing detection, and the reader is advised to refer to the survey by Venkatesh et al. [10] to get a detailed overview on face morphing.

Most face morphing generation works are devised by performing the blending operation on the complete (or total) face images [10]. However, the success rate of the full-face morphing attack is high when contributory subjects are lookalikes to deceive the super-recognizer and highly trained border guards [12]. Therefore, partial face morphing was introduced in [20] where the blending operation is carried out using Poisson image editing [21]. The generated composite morphs have shown vulnerabilities of FRS based on deep-learning features such as VGGFace [22], Arcface [2] and commercial-off-the-shelf (COTS) that includes Neurotech [23] and Cognitec [24]. Further, the human observer analysis is also discussed. However, the work presented in [20] has several limitations, including (1) it is based on landmarks, and this would lead to pixel-based artifacts due to alignment issues, and correction of these would require manual intervention [10] (2) Only a few arbitrary regions are used to generate the composite images (3) Limited only to the base regions like nose, mouth, eye and forehead. (4) Limited only to the single facial attribute composite generation (5) failure to achieve a high vulnerability of FRS.

Thus, motivated by the limitations of the existing method [20], we aim to generate the composite images in a fully automatic fashion using GANs. Even though the GANs are extensively used for full face morphing attack generation [17], [28], [29], the composite (or facial attribute) based attack generation is presented for the first time in this work. The recent work by Chai et al. [26] presented a highly realistic facial image synthesis with missing regions using GAN-inversion. In this work, we modified the approach from Chai et al. [26] to generate the CFIA samples with the primary motivation to demonstrate the vulnerabilities of FRS to CFIA. Further, we exhaustively varied the regions based on facial attributes to evaluate their attack potential. The proposed method for CFIA generation is designed to consider the optimal pairing of the input images used during the compositing process to ensure high-quality CFIA generation. The CFIA samples are generated based on multiple facial attributes. Both single and multiple facial attributes are blended using the transparent (or real) value that can further improve the attack potential and challenge the detection of CFIA samples. Use of facial attributes or partial morphing will not alter the entire face and thus results in less distortion because the proposed CFIA approach will only choose the facial attributes from the contributory subjects and then synthesize the rest of the facial image using GAN. Hence, the generated CFIA images are challenging to be detected by expert border guards. The key contributions of our proposed method are as follows:

- We propose a novel framework for Composite Face Image Attack (CFIA) generation using regression and GAN-based image synthesis. The primary motivation of the proposed CFIA approach is to generate high-quality facial attack images using facial attributes with high attack potential. Further, it should be challenging to detect by both human and automatic morph detection techniques. Therefore, we generate CFIA based on single and multiple face attributes for given contributory data subjects. Further, we propose a transparent blending to improve the attack potential of the generated CFIA. Thus, we introduce 526 different types of CFIA based on various combinations of facial attributes from contributory data subjects.

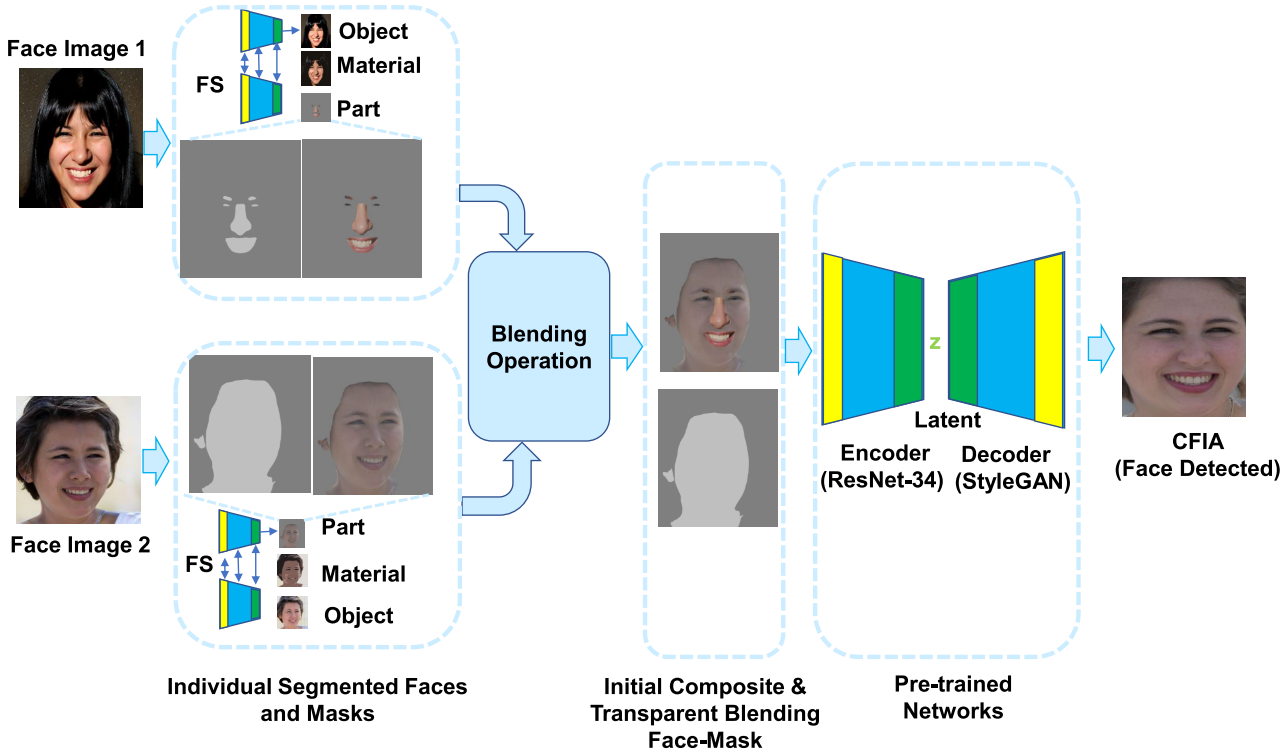


FIGURE 1. Block diagram of the proposed approach where FS is based on UPerNet Face Segmenter from Zhou et al. [25], the Encoder is based on Resnet-34 [26], and Decoder is based on StyleGAN [27] and the encoder-decoder synthesizes the final composite.

- We present a new CFIA dataset generated using 1000 unique data subjects (synthetic identities). The dataset consists of 526000 CFIA samples and 2000 bona fide samples.
- We present extensive vulnerability analysis on the newly generated CFIA dataset using deep learning-based FRS.. We also introduce an vulnerability metric called Generalized Morphing Attack Potential (G-MAP) to benchmark the attack potential effectively by considering real-life scenarios.
- We present the perceptual image quality analysis of the CFIA dataset using the Peak-Signal-to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) to benchmark the quality of the generated CFIA samples on a sub-set of the CFIA dataset with 14 unique combinations selected from the 526 combinations.
- We present the human observer study on the newly generated CFIA dataset (subset of 14 combinations) with 43 observers with and without face image manipulation detection background.
- We present extensive experiments benchmarking the performance to automatically detect the CFIA (subset of 14 combinations) using three different existing single image based face MAD techniques.
- The CFIA dataset, together with the source code of the proposed method, will be made publicly available to enable the reproducibility of the results presented in this paper https://github.com/jagmohaniiit/LatentCompositionCode.

In the rest of the paper we introduce the proposed method in Section II, discussion on database generation methodology in presented in Section III, vulnerability analysis and G-MAP is discussed in Section IV, Section V discuss the quantitative results of the perceptual quality evaluation, human observer study is discussed in Section VI, and discussion on CFIA detection (CAD) is presented in the Section VII. Lastly, the Section VIII draws the conclusions and future-work.

II. PROPOSED CFIA GENERATION TECHNIQUE

Figure 1 shows the block diagram of the proposed CFIA method. The proposed CFIA method aims to automatically select single and multiple facial attribute regions from the given face images and blend them to generate a composite face image. The proposed CFIA method consists of three main functional blocks (1) generation of individual segmented faces and masks from given face images, (2) computation of the initial composite image and transparent blending face mask and (3) final CFIA generation based on pre-trained GANs.

A. INDIVIDUAL SEGMENTED FACES AND MASKS

The proposed CFIA composite image generation is based on the different facial parts from the two contributory data subjects (e.g., skin from the first data subject and eyes from the second data subject). Therefore, we employed a high precision and accurate method to segment different facial parts. In this work, we choose the unified parsing network (UPerNet) [30] for automatic facial region segmentation,

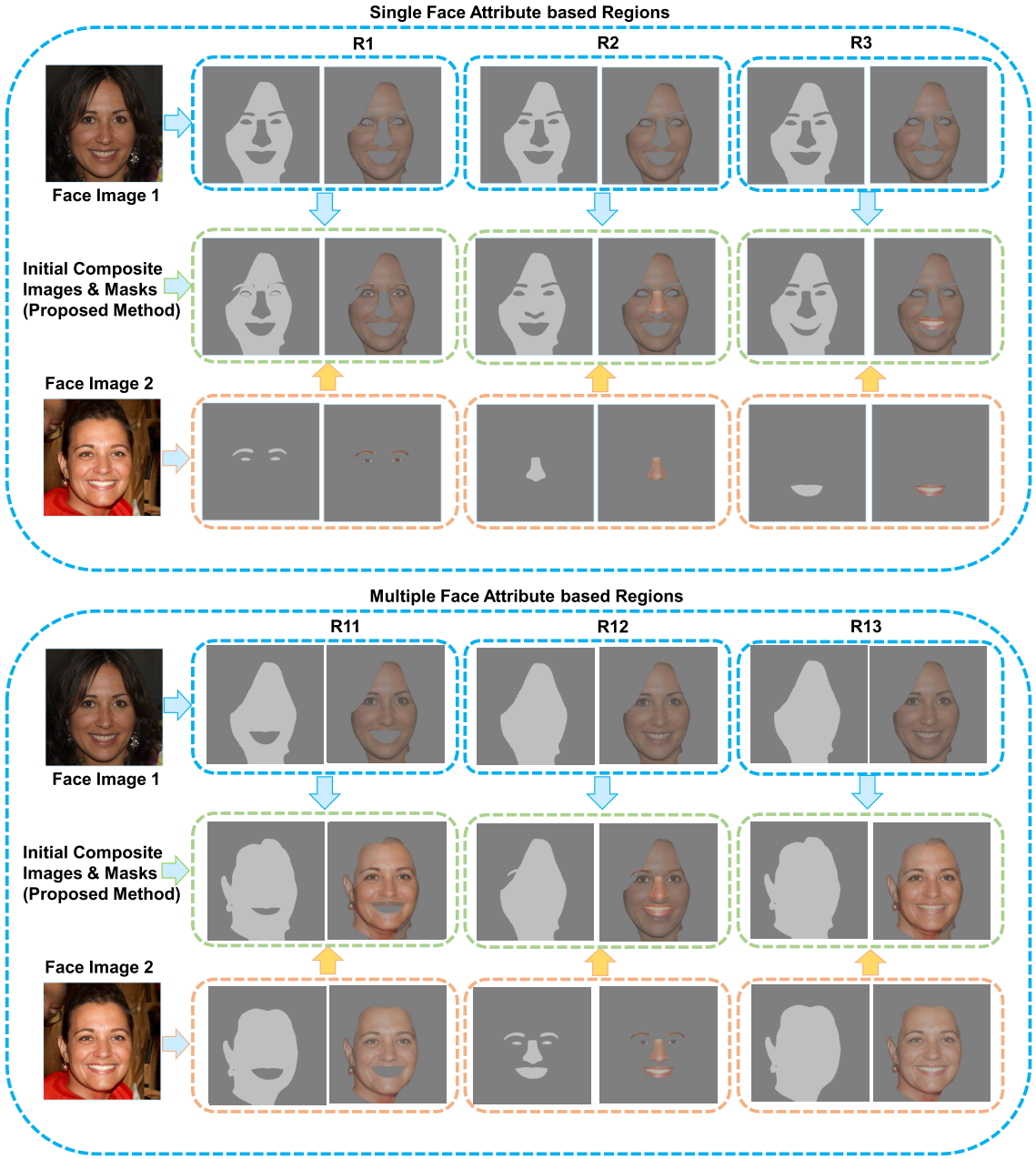


FIGURE 2. Illustration showing the comparison between the single face attribute based regions and multiple face attribute based regions for the generation of the initial composite using the proposed method.

which is denoted as $\mathbb{FS}$. UPerNet [30] is based on multi-task learning and semantic segmentation to achieve high-quality results on facial segmentation and classification tasks. Thus, given the face image, UPerNet [30] provides six facial regions (or attribute) masks, including Skin (S), Eye (E), Nose (N), Mouth (M), Hair (H), and Background (B).

In this work, we have considered only two contributory face images based on real-time use-case applicability (for e.g. attacks on eMRTD or ID cards) [10], [20]. We denote the first contributory face image by F_1 and the corresponding part-based segmented masks obtained using UPerNet [30] be $SM1_i$, where $i = \{1, 2, \ldots, 6\}$ and its corresponding segmented image be $IS1_i$. Similarly, the second contributory face image be F_2 and the corresponding part-based segmented masks be $SM2_j$, where $j = \{1, 2, \ldots, 6\}$ and its corresponding segmented image be $IS2_j$. The face region segmentation process to obtain individual segments can be expressed as follows:

$$\begin{aligned} \{SM1_i, IS1_i\} &= \mathbb{FS}(F_1), \forall i = \{1, 2, \ldots, 6\} \\ \{SM2_j, IS2_j\} &= \mathbb{FS}(F_2), \forall j = \{1, 2, \ldots, 6\} \end{aligned} \tag{1}$$

Based on these six part-based segmentation masks (or region or facial attributes), we generate an exhaustive list of combinations from $SM1_i$ and $SM2_j$ that resulted in

526 unique CFIA samples as listed in Table 2. It needs to be pointed out that the selected areas are exhaustive as listed in Table 1. Table 1 mentions the CFIA Region Index, through which we give a numerical index to the output segments so that overall, it increases with the number of combinations. E.g., if we consider two combinations case, we select two regions from $SM1$ and choose a maximum of two regions out of six (in a step-wise manner) from $SM2$. Therefore, in two combinations case (see Table 1), we have CFIA region index 2, in which, we select 2 regions from $SM1$ and one region from $SM2$. Similarly, for CFIA region index 3 we select 2 regions from $SM1$ and 2 regions from $SM2$. We repeat this process for the various combinations of regions (or facial attributes), such that CFIA region index 2 results in 50 combinations corresponding to 3 output segments. Similarly, CFIA region index 3 results in 100 combinations corresponding to 4 output segments. These steps are repeated for different CFIA region indexes from 1 to 16, resulting in a total of 607 combinations. However, out of 607 combinations some of the combinations are redundant. For example, selecting face attributes from $SM1$ and $SM2$ such as SE-NM (SkinEyes-NoseMouth) can occur in two ways, firstly Skin, Eyes from $SM1$ and Nose, Mouth from $SM2$ and secondly SEN-M (SkinEyesNose-Mouth), Skin, Eyes and Nose from $SM1$ and Mouth from $SM2$ resulting in a redundant combination. Therefore, we removed all such redundant combinations and considered unique combinations. Hence, we generate 526 unique CFIA samples corresponding to two unique facial identities.

B. INITIAL COMPOSITE IMAGE AND TRANSPARENT BLENDING FACE-MASK

In the next step, we generate the initial composite image and transparent blending of face segments by applying the blending operation on the individual segmented faces ($IS1_i$ & $IS2_j$) and their corresponding masks ($SM1_i$ & $SM2_j$) from contributory data subjects (F_1 & F_2). The blending operation is carried out independently for the mask and the individual segmented faces. The blended mask m_c is generated by a simple union operation that can represent the combined facial region from $SM1_i$ and $SM2_j$ as described in Equation 2. The generation of the initial composite image (IC) is done in three consecutive steps shown in Equation 3, where first IC is initialized 0, then in the next step, IC is updated using the compositing equation with the segmented region ($IS1_i$) from the data subject F_1 as input. Finally, IC is updated using the compositing equation with the segmented region ($IS2_j$) from data subject F_2, and its segmentation masks $SM2_j$ as an input. These steps are mathematically presented in Equation 3.

$$m_c = SM1_i \bigcup SM2_j \tag{2}$$

$$\begin{aligned} IC &= 0 \\ IC &= IS1_i \\ IC &= IS2_j + (1 - SM2_j) \times IC \end{aligned} \tag{3}$$

TABLE 1. Table showing the generation process of 526 unique CFIA combinations which are listed in detail Table 2.

CFIA Region Index	Output Segments	Possible Pairs (Unique)
One Combinations		
1	2	$\binom{5}{1} \times \binom{5}{1} = 25(13)$
Two Combinations		
2	3	$\binom{5}{2} \times \binom{5}{1} = 50(26)$
3	4	$\binom{5}{2} \times \binom{5}{2} = 100(100)$
Three Combinations		
4	4	$\binom{5}{3} \times \binom{5}{1} = 50(50)$
5	5	$\binom{5}{3} \times \binom{5}{2} = 100(78)$
6	6	$\binom{5}{3} \times \binom{5}{3} = 100(86)$
Four Combinations		
7	5	$\binom{5}{4} \times \binom{5}{1} = 25(25)$
8	6	$\binom{5}{4} \times \binom{5}{2} = 50(50)$
9	7	$\binom{5}{4} \times \binom{5}{3} = 50(47)$
10	8	$\binom{5}{4} \times \binom{5}{4} = 25(25)$
Five Combinations		
11	6	$\binom{5}{5} \times \binom{5}{1} = 5(5)$
12	7	$\binom{5}{5} \times \binom{5}{2} = 10(10)$
13	8	$\binom{5}{5} \times \binom{5}{3} = 10(10)$
14	9	$\binom{5}{5} \times \binom{5}{4} = 5(5)$
15	10	$\binom{5}{5} \times \binom{5}{5} = 1(1)$
Six Combinations		
16	12	$\binom{6}{6} \times \binom{6}{6} = 1(1)$
Total Output Segments Possible		
607		
Total Unique Segments Possible		
526		

Figure 2 shows the qualitative results of the initial composite image and the corresponding mask for both single-face attribute-based composite regions & multiple-face attribute-based composite regions.

C. FINAL CFIA SAMPLES GENERATION

Once the initial composite image and the transparent blending face mask are generated, we generate the final CFIA samples using the image inpainting based on pre-trained regressor and GAN [26]. The input composite image and its mask are passed through a pre-trained encoder ($\mathbb{E}$) and then to the decoder ($\mathbb{G}$) to generate the final composite image (FCI). The process of generating the CFIA sample is as indicated in Equation 4.

$$CFIA = \mathbb{D}(\mathbb{E}(IC, m_c)) \tag{4}$$

The encoder network ($\mathbb{E}$) selected in our work is pre-trained Resnet-34 [26], and the decoder network ($\mathbb{G}$) is a pre-trained StyleGAN-I decoder which was trained on FFHQ dataset [27]. The primary motivation for the choice of the encoder and decoder networks was that image to latent conversion is posed as a regression problem [26]. Further, it is found that Resnet-34 is suitable for regressing the latent from a face image with missing information and renders the high-quality face image. Lastly, we use the decoder ($\mathbb{D}$) based on StyleGAN-I as it provides a linear latent subspace [31]. Hence, reconstruction from the generated latent is of good perceptual quality even with missing information in the input image. Figure 3 shows example results corresponding to five combinations generated using the proposed method. For the simplicity, we have included the illustration for five

TABLE 2. Exhaustive List of Regions used for Composition where the compositions S1 are used for Subject 1 and S2 are used for Subject 2 where the facial attributes are B=Background, S=Skin, E=Eye, N=Nose and M=Mouth. The compositions listed in left to right order are in increasing order of Composition Region Index (for Composition Region Index, please refer Table 1).

Region List						
S1-S2	S1-S2	S1-S2	S1-S2	S1-S2	S1-S2	S1-S2
E-H	H-E	H-H	H-M	H-N	H-S	M-H
N-H	S-H	S-E	S-N	S-M	S-S	EM-H
EN-H	HE-E	HE-H	HE-M	HE-N	HE-S	HM-E
HM-H	HM-M	HM-N	HM-S	HN-E	HN-H	HN-M
HN-N	HN-S	HS-E	HS-H	HS-M	HS-N	HS-S
NM-H	SE-H	SM-H	SN-H	EM-EM	EM-EN	EM-HE
EM-HM	EM-HN	EM-HS	EM-NM	EM-SE	EM-SM	EM-SN
EN-EM	EN-EN	EN-HE	EN-HM	EN-HN	EN-HS	EN-NM
EN-SE	EN-SM	EN-SN	HE-EM	HE-EN	HE-HE	HE-HM
HE-HN	HE-HS	HE-NM	HE-SE	HE-SM	HE-SN	HM-EM
HM-EN	HM-HE	HM-HM	HM-HN	HM-HS	HM-NM	HM-SE
HM-SM	HM-SN	HN-EM	HN-EN	HN-HE	HN-HM	HN-HN
HN-HS	HN-NM	HN-SE	HN-SM	HN-SN	HS-EM	HS-EN
HS-HE	HS-HM	HS-HN	HS-HS	HS-NM	HS-SE	HS-SM
HS-SN	NM-EM	NM-EN	NM-HE	NM-HM	NM-HN	NM-HS
NM-NM	NMS-E	NMS-M	NMS-N	SEE-M	SEE-N	SEH-E
SEH-M	SEH-N	SEH-S	SEN-M	SES-E	SES-M	SES-N
SME-M	SME-N	SMH-E	SMH-M	SMH-N	SMH-S	SMN-M
SMS-E	SMS-M	SMS-N	SNE-M	SNE-N	SNH-E	SNH-M
SNH-N	SNH-S	SNN-M	SNS-E	SNS-M	SNS-N	ENM-E
ENM-H	ENM-M	ENM-N	ENM-S	HEM-E	HEM-H	HEM-M
HEM-N	HEM-S	HEN-E	HEN-H	HEN-N	HEN-S	HNME
HNM-H	HNM-M	HNM-N	HNM-S	HSE-E	HSE-H	HSE-S
HSM-E	HSM-H	HSM-M	HSM-N	HSM-S	HSN-E	HSN-H
HSN-N	HSN-S	SEM-E	SEM-H	SEM-M	SEM-N	SEM-S
SEN-E	SEN-H	SEN-N	SEN-S	SNM-E	SNM-H	SNM-M
SNM-N	SNM-S	ENM-HE	ENM-HM	SEN-EM	SEN-EN	ENM-HN
ENM-HS	HEM-EM	HEM-EN	HEM-HE	HEM-HM	HEM-HN	HEM-HS
HEM-NM	HEM-SE	HEM-SM	HEM-SN	HEN-EM	HEN-EN	HEN-HE
HEN-HM	HEN-HN	HEN-HS	HEN-NM	HEN-SE	HEN-SM	HEN-SN
HNM-EM	HNM-EN	HNM-HE	HNM-HM	HNM-HN	HNM-HS	HNM-NM
HNM-SE	HNM-SM	HNM-SN	HSE-EM	HSE-EN	HSE-HE	HSE-HM
HSE-HN	HSE-HS	HSE-NM	HSE-SE	HSE-SM	HSE-SN	HSM-EM
HSM-EN	HSM-HE	HSM-HM	HSM-HN	HSM-HS	HSM-NM	HSM-SE
HSM-SM	HSM-SN	HSN-EM	HSN-EN	HSN-HE	HSN-HM	HSN-HN
HSN-HS	HSN-NM	HSN-SE	HSN-SM	HSN-SN	SEM-HE	SEM-HM
SEM-HN	SEM-HS	SEN-HE	SEN-HM	SEN-HN	SEN-HS	SNM-HE
SNM-HM	SNM-HN	SNM-HS	ENM-HEM	ENM-HEN	ENM-HNM	ENM-HSE
ENM-HSM	ENM-HSN	HEM-ENM	HEM-HEM	HEM-HEN	HEM-HNM	HEM-HSE
HEM-HSM	HEM-HSN	HEM-SEM	HEM-SEN	HEM-SNM	HEN-ENM	HEN-HEM
HEN-HEN	HEN-HNM	HEN-HSE	HEN-HSM	HEN-HSN	HEN-SEM	HEN-SEN
HEN-SNM	HNM-ENM	HNM-HEM	HNM-HEN	HNM-HNM	HNM-HSE	HNM-HSM
HNM-HSN	HNM-SEM	HNM-SEN	HNM-SNM	HSE-ENM	HSE-HEM	HSE-HEN
HSE-HNM	HSE-HSE	HSE-HSM	HSE-HSN	HSE-SEM	HSE-SEN	HSE-SNM
HSM-ENM	HSM-HEM	HSM-HEN	HSM-HNM	HSM-HSE	HSM-HSM	HSM-HSN
HSM-SEM	HSM-SEN	HSM-SNM	HSN-ENM	HSN-HEM	HSN-HEN	HSN-HNM
HSN-HSE	HSN-HSM	HSN-HSN	HSN-SEM	HSN-SEN	HSN-SNM	SEM-HEM
SEM-HEN	SEM-HNM	SEM-HSE	SEM-HSM	SEM-HSN	SEN-HEM	SEN-HEN
SEN-HNM	SEN-HSE	SEN-HSM	SEN-HSN	SNMHEM	SNM-HEN	SNM-HNM
SNM-HSE	SNM-HSM	SNM-HSN	SEN-SEM	SEN-SEN	HENM-E	HENM-H
HENM-M	HENM-N	HENM-S	HSEM-E	HSEM-H	HSEMM	HSEM-N
HSEM-S	HSEN-E	HSEN-H	HSEN-N	HSEN-S	HSNME	HSNM-H
HSNM-M	HSNM-N	HSNM-S	SENM-E	SENM-H	SENM-M	SENM-N
SENM-S	HENM-EM	HENM-EN	HENM-HE	HENM-HM	HENM-HN	HENM-HS
HENM-NM	HENM-SE	HENM-SM	HENM-SN	HSEM-EM	HSEM-EN	HSEM-HE
HSEM-HM	HSEM-HN	HSEM-HS	HSEM-NM	HSEM-SE	HSEM-SM	HSEM-SN
HSEN-EM	HSEN-EN	HSEN-HE	HSEN-HM	HSEN-HN	HSEN-HS	HSEN-NM
HSEN-SE	HSEN-SM	HSEN-SN	HSNM-EM	HSNM-EN	HSNM-HE	HSNM-HM
HSNM-HN	HSNM-HS	HSNM-NM	HSNM-SE	HSNM-SM	HSNM-SN	SENM-EM
SENM-EN	SENM-HE	SENM-HM	SENM-HN	SENM-HS	SENM-NM	SENM-SE
SENM-SM	SENM-SN	SENM-ENM	HENM-ENM	HENM-HEM	HENM-HEN	HENM-HNM
HENM-HSE	HENM-HSM	HENM-HSN	HENM-SEM	HENM-SEN	HENM-SNM	HSEM-ENM
HSEM-HEM	HSEM-HEN	HSEMH-NM	HSEMH-SE	HSEMH-SM	HSEM-HSN	HSEM-SEM
HSEM-SEN	HSEM-SNM	HSEN-ENM	HSEN-HEM	HSEN-HEN	HSEN-HNM	HSEN-HSE
HSEN-HSM	HSEN-HSN	HSEN-SEM	HSEN-SEN	HSEN-SNM	HSNM-ENM	HSNM-HEM
HSNM-HEN	HSNM-HNM	HSNM-HSE	HSNM-HSM	HSNM-HSN	HSNM-SEM	HSNM-SEN
HSNM-SNM	SENM-HEM	SENM-HEN	SENM-HNM	SENM-HSE	SENM-HSM	SENM-HSN
HENMH-ENM	HENMH-SEM	SENM-SENM	HENM-HSEN	HENM-HSNM	HENM-SENM	HSEM-HENM
HSEM-HSEM	HSEM-HSEN	HSEM-HSNM	HSEM-SENM	HSEN-HENM	HSEN-HSEM	HSENH-SEN
HSENH-SNM	HSEN-SENM	HSNM-HENM	HSNM-HSEM	HSNM-HSEN	HSNM-HSNM	HSNM-SENM
SENM-HENM	SENM-HSEM	SENM-HSEN	SENM-HSNM	HSENM-E	HSENM-H	HSENM-M
HSENM-N	HSENM-S	HSENME-M	HSENME-N	HSENMH-E	HSENMH-M	HSENMH-N
HSENMH-S	HSENMN-M	HSENMS-E	HSENMS-M	HSENMS-N	HSENMEN-M	HSENMH-EM
HSENMH-EN	HSENMH-NM	HSENMH-SE	HSENMH-SM	HSENMH-SN	HSENMS-EM	HSENMS-EN
HSENMS-NM	HSENMH-ENM	HSENMH-SEM	HSENMH-SEN	HSENMH-SNM	HSENM-SENM	HSENM-HSENM
HBSENM-HBSENM						

combination and full 526 CFIA samples are included in the supplement material.

III. CFIA DATABASE GENERATION

This section presents the dataset generation process used to evaluate the proposed composite image generation. Owing to the ethical and legal challenges with face biometric datasets that will eventually limit the distribution, in this work, we generate the synthetic face images corresponding to the unique identities using StyleGAN inversion [26]. Earlier works [17], [32], [33] indicated that generating the synthetic face images have demonstrated both realness in terms of

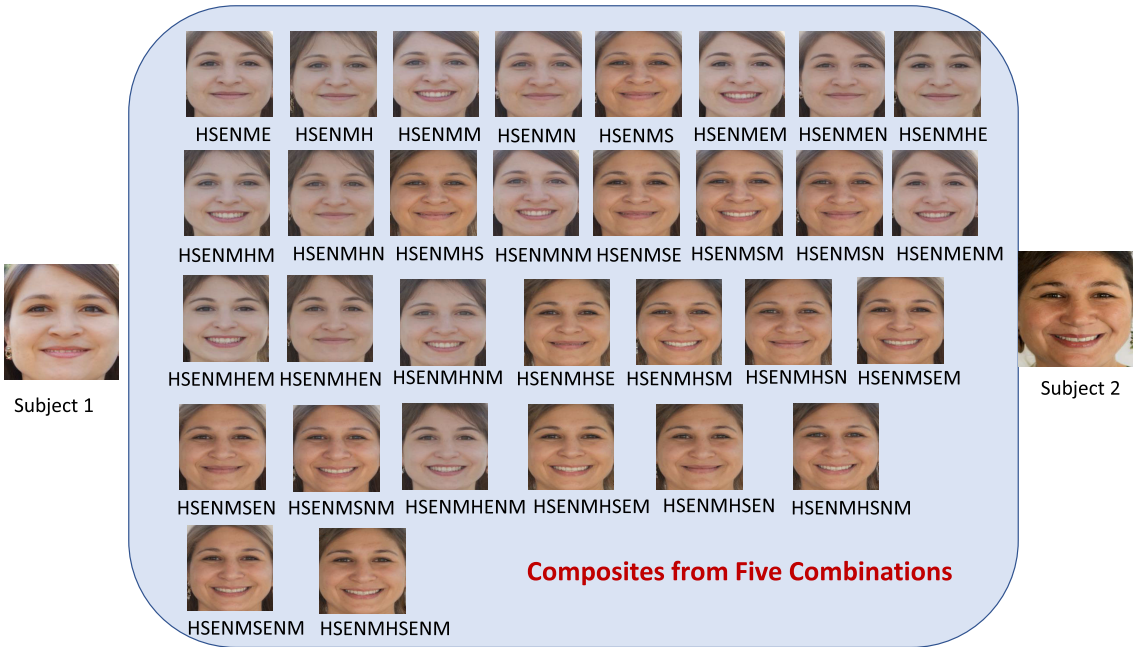


FIGURE 3. Illustration showing five combinations based composites.

quality, uniqueness and verification accuracy. Further, synthetic face images will overcome the need for privacy and legal limitations to make the database public, which is vital for reproducible research. Figure 4 illustrates the CFIA dataset generation process.

A. SYNTHETIC FACE IMAGE GENERATION

Given a random latent vector, we use the approach from Chai et al. [26] to generate a synthetic face corresponding to unique data subjects using StyleGAN inversion. We further perturb the random latent by an ϵ amount to generate the mated face image corresponding to the given identity. The choice of ϵ is made empirically, which is small enough not to alter the identity of the generated face. However, the generation of synthetic face images with corresponding mated face images with unique identities will result in non-ICAO compliant photos with glasses, non-frontal pose, and a non-neutral face expression, as shown in Figure 5. Therefore, it is necessary to detect the ICAO-compliant faces for which we select faces with frontal pose automatically and remove photos with glasses and non-neutral face expressions manually.

B. HYPERPARAMETERS SELECTION

This section discusses the choices of the parameters associated with SOTA and the proposed method as tabulated in Table 3. In total, we have four different hyperparameters that are discussed as follows:

- **Epsilon(ϵ)**: The value of ϵ is empirically chosen as 10^{-7}. Since values higher than 10^{-1} lead to artifacts and a sample of different identities as shown in Figure 6. Thus, we choose an ϵ conservatively.
- **Alpha**: We choose α=0.5 as it is known to create the highest vulnerability towards FRS for Face Morphing Image Attack (FMIA) [10]. of segments possible is shown in Table 2

TABLE 3. Different Hyper-parameters used for the proposed method. Note the proposed method modifies a large number of hyper-parameters compared with SOTA [26].

Hyper-parameters	SOTA [26]	Proposed Method
Frontal Pose Selection	No	**Yes**
Optimal Pairing	No	**Yes**
Epsilon(ϵ)	No	10^{-7}
Alpha(α)	1	0.5

C. FRONTAL FACE POSE SELECTION

We have developed the algorithm to automatically select the ICAO compliant face images corresponding to each unique identity as indicated in the Algorithm 1. The primary motivation behind this algorithm is that the face in a frontal pose would have similar angles between Left-Eye, Nose, and Mouth (Left Part) and Right-Eye, Nose, and Mouth (Right Part). A slight change in the face pose from a frontal face to a profile face would result in a skew, which would cause these two angles to be different. The qualitative results of the proposed frontal face selection algorithm are as shown in Figure 5. Since we are currently not interested in the computation of exact face pose, the heuristic works sufficiently well for our dataset, which does not consist of extreme face poses.

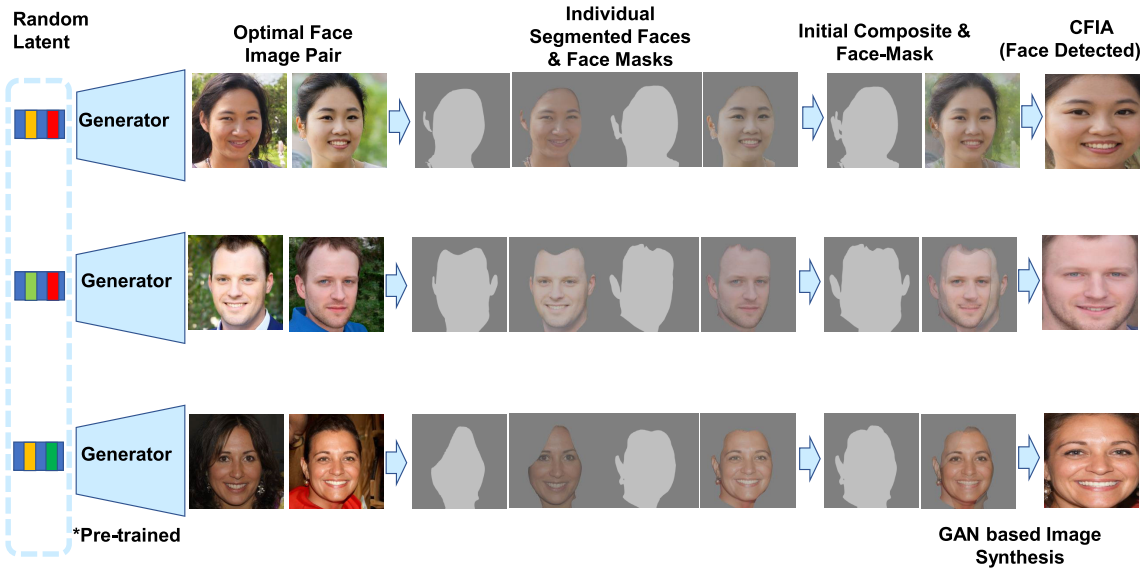


FIGURE 4. Illustration showing the CFIA dataset generation process.

FIGURE 5. Illustration showing faces selected and rejected by our proposed frontal-pose detection Algorithm 1. Note face images with glasses and GAN-based artifacts are rejected manually.

D. OPTIMAL FACE PAIR GENERATION FOR COMPOSITE IMAGE GENERATION

It is essential to select the look-alike data subjects to achieve the optimal attack potential with the proposed composite face image generation. We choose the optimal pairs to generate the composite face images to this extent. Given n synthetic samples, the total number of pairs possible is $((n)\times(n-1))/2$, and thus finding optimal pairs using this approach is quadratic ($O(n^2)$) as we have to compute the pair-wise distance for all pairs. The quadratic time for pair-finding is within the computing limits as our dataset now consists of 1000 unique data subjects. We have put an additional constraint in the pair-finding algorithm not to return swapped pairs, i.e., if (i,j) is the list, then (j,i) is not added to the optimal pair list. The approach for optimal pair finding is summarized in an algorithmic format in Algorithm 2 and a few optimal pairs are shown in Figure 4. The distance metric used in our approach is cosine-distance from Arcface [2] features.

Algorithm 1 Non-Frontal Pose Identification

Input: Face Image with 5 Landmarks (Left-Eye (LE), Right-Eye (RE), Nose (N), Left-Mouth (LM), and Right-Mouth (RM)

Output: True if Face Image is Frontal

1: Compute the angle between the vectors of Left-Eye, Nose, and Left-Mouth, Nose
$\theta_1 \leftarrow \arccos((\overrightarrow{LEN} \cdot \overrightarrow{LMN}))$.
2: Compute the angle between the vectors of Nose, Right-Eye, and Nose, Right-Mouth
$\theta_2 \leftarrow \arccos((\overrightarrow{NRE} \cdot \overrightarrow{NRM}))$.
3: Compute absolute difference between the angles, as $angleDiff \leftarrow \theta_1 - \theta_2$
4: **if** $angleDiff \leq \tau$ **then**
5: Face is Frontal
6: **return** True
7: **end if**
8: **return** False

Thus, the CFIA dataset has 1000 unique identities with 2000 bona fide samples and 526000 CFIA samples. The whole dataset will made publicly available for research purposes along with code at the following link https://github.com/jagmohaniiit/LatentCompositionCode.

IV. VULNERABILITY ANALYSIS

This section presents the vulnerability analysis of the proposed CFIA samples on the automatic FRS. We have benchmarked four different FRS based on deep learning. The deep learning FRS employed in this work are Arcface [37] (Model R100 V1), VGGFace [38] (Version 2), Facenet [39] and Magface [40]. The proposed CFIA samples are generated based on the face images corresponding to two contributory

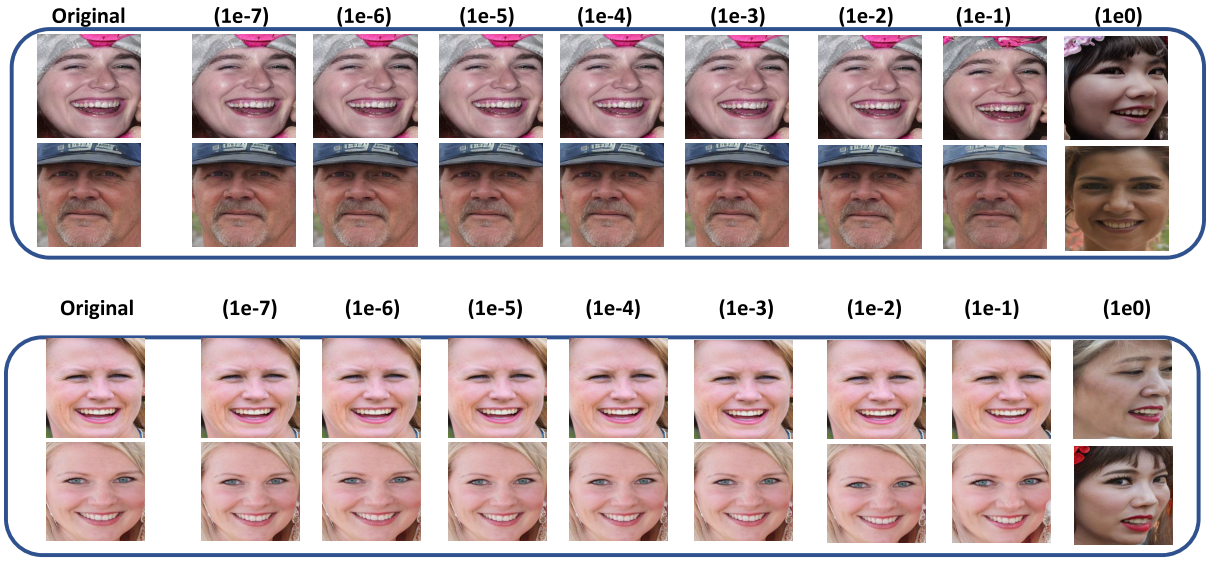


FIGURE 6. Illustration of the effect of perturbation based on epsilon (ϵ) for synthetic face generation, note artifacts start appearing when ($\epsilon = 0.1$) and results in change in identity when ($\epsilon = 1$).

Algorithm 2 Optimal Pair Finding Algorithm

Input: Random Image Pairs $(I_1^1, I_2^1), \cdots, (I_1^N, I_2^N)$
Output: Optimal Image Pairs $(O_1^1, O_2^1), \cdots, (O_1^N, O_2^N)$

```
Compute Arcface features on the input face images.
Optimal-Pair ← []
for i ← 1 to N do
    Compute Index of nearest arcface feature j to i
    if (j, i) ∉ Optimal-Pair then
        Append (i, j) to Optimal-Pair
    else
        Compute Index of second-nearest arcface feature k to i
        Append (i, k) to Optimal-Pair
    end if
end for
return Optimal-Pair
```

subjects. Therefore, we benchmark the attack potential of CFIA by comparing the FRS scores computed from both contributory subjects against the pre-set threshold of FAR = 0.1%. The comparison scores from FRS are computed by enrolling the attack samples to FRS and then probing the face images from the contributory subjects.

In the literature, the vulnerability of FRS can be calculated using three different types of metrics namely: Mated Morphed Presentation Match Rate (MMPMR) [34], Fully Mated Morphed Presentation Match Rate (FMMPMR) [35] and Morphing Attack Potential (MAP) [36]. The MMPMR metric is based on the independent attempts, while FMMPMR employs pair-wise probe attempts of the contributory subjects. The MAP metric improves existing metrics by accommodating multiple FRS together with pair-wise probe attempts. However, the MAP metric will represent the vulnerability results in the matrix form as attempts versus multiple FRS. Hence, MAP does not quantify the vulnerability as a single number. Further, the constant number of attempts will also limit the evaluation as it enforces all enrolled attack samples to have the same number of attempts which is not true in a real-life scenario. Additionally, while computing the vulnerability, the existing metrics do not consider accommodating Failure-to-Acquire Rate (FTAR) and multiple morphing generation techniques. Even though the enroled face image (attack/CFIA/morphing or bona fide) is captured in the constrained conditions, the probe images are not essentially captured in the constrained conditions due to the nature of ID verification scenarios (for example, in border control gates, smartphone authentication, etc.). Further, the availability of different types of morphing (or attack) generation techniques (full face/partial face/facial attribute) allows an attacker to generate various attack samples. Hence, the vulnerability computation needs to accommodate different types of morphing generation. These factors motivated us to enhance the existing vulnerability metrics (MAP) to include more utility features such as (a) Dynamic attempts per morph image, (b) Accountability for FTAR, (3) Accountability for multiple morphing techniques, and (4) Single numeric value indicating the vulnerability. The enhanced vulnerability metric is termed as Generalised Morphing Attack Potential (G-MAP). Table 4 presents utility features of the proposed G-MAP compared to existing metrics such as MMPMR [34], FMMPMR [35] and MAP [36].

A. MATHEMATICAL FORMULATION OF G-MAP

Let $\mathbb{P}$ denote the set of paired probe images (which can also be denoted as number of attempts), $\mathbb{F}$ denote the set of FRS, $\mathbb{D}$ denote the set of Morphing Attack Generation Type,

TABLE 4. Utility features of existing and proposed vulnerability metrics.

Utility Features	MMPMR [34]	FMMPMR [35]	MAP [36]	G-MAP
Multiple Attempts for individual morphing Image	✓	✓	✗	✓
Pairwise comparison of probe samples	✗	✓	✓	✓
Multiple FRS	✗	✗	✓	✓
Multiple Morphing Types	✗	✗	✗	✓
Accountability for FTAR	✗	✗	✗	✓
Vulnerability as a single number	✓	✓	✗	✓

$\mathbb{M}_d$ denote the face morphing image set corresponding to Morphing Attack Generation Type d, τ_l indicate the similarity score threshold for FRS (l), and $||$ represents the count of elements in a set during metric evaluation. The G-MAP metric is presented as below:

$$\text{G-MAP} = \frac{1}{|\mathbb{D}|}\sum_{d}^{|\mathbb{D}|}\frac{1}{|\mathbb{P}|}\frac{1}{|\mathbb{M}_d|}\min_{l} \sum_{i,j}^{|\mathbb{P}|,|\mathbb{M}_d|}\left\{\left[(S1_i^j > \tau_l) \wedge \cdots (Sk_i^j > \tau_l)\right] \times [(1 - FTAR(i,l))]\right\} \quad (5)$$

where, $FTAR(i,l)$ is the failure to acquire probe image in attempt i using FRS (l). The algorithm for G-MAP is presented in 3 and the code is made available in the link [41].

Algorithm 3 Generalized Morph Attack Potential (G-MAP)

Input: Set of Probe Images $\mathbb{P}$, Set of FRS $\mathbb{F}$, Set of Morphing Attack Generation Type $\mathbb{D}$, Set of Morphing Attack Images in d^{th} attack $\mathbb{M}_d$, τ_l indicate the similarity score threshold for FRS.
Output: G-MAP

Compute G-MAP Metric as follows.
for $j \leftarrow 1$ to $|\mathbb{M}_d|$ **do**
  for $d \leftarrow 1$ to $|\mathbb{D}|$ **do**
    for $l \leftarrow 1$ to $|\mathbb{F}|$ **do**
      for $i \leftarrow 1$ to $|\mathbb{P}|$ **do**
        Compute QF(i,l)=(1-FTAR(i,l))
        Compute G-MAP(d)=$\frac{1}{|\mathbb{P}|}\frac{1}{|\mathbb{M}_d|}\min_l \sum_{i,j}^{|\mathbb{P}|,|\mathbb{M}_d|}(S1_i^j > \tau_l) \wedge \cdots (Sk_i^j > \tau_l) \times QF(i,l)$
      end for
    end for
  end for
end for
Compute G-MAP= $\frac{1}{|\mathbb{D}|}G - MAP(d)$
return G-MAP

B. COMPUTING G-MAP

Given the fact that G-MAP can be computed with different parameters, which include multiple probe attempts, multiple FRS and the morph attack generation types. **G-MAP with multiple probe attempts** is calculated from Equation 5 by setting D = 1 and F = 1 where the similarity scores ($S1_i^j$) should be greater than threshold (τ_l) and FTAR(i,l) is calculated for each probe attempt and FRS. Thus, making **G-MAP with multiple probe attempts** identical to FMMPMR when FTAR = 0. Further, **G-MAP with Multiple FRS and multiple probe attempts** is computed by taking minimum across FRS and using D=1. Finally, the full **G-MAP metric** would provide a single value indicating the vulnerability which is by taking the average as shown in Equation 5.

C. QUANTITATIVE EVALUATION OF VULNERABILITY

In this section, we present the qualitative and quantitative evaluation of the vulnerability corresponding to FRS for all 526 CFIA samples generated using a different combination of facial attributes. Since G-MAP is a function of attempts, FRS, and morphing types, this will allow one to analyse the quantitative results corresponding to (a) probe attempts independently to FRS and attack image generation type (b) Multiple FRS with multiple attempts independent of attack image generation type (c) Final G-MAP value as a function of attempts, multiple FRS and different types of attack image generation together with FTAR.

In this work, we first present the vulnerability of the full CFIA dataset using four different FRS such as Arcface [37] (Model R100 V1), VGGFace [38] (Version 2), Facenet [39] and Magface [40]. The vulnerability reported in this work is computed by setting the threshold of FRS at FAR = 0.1%. Figure 7 shows the plot of G-MAP values that are computed for multiple probe attempts independent of FRS and CFIA generation type. The composite region index started from the output segment with two regions (left extreme of x-axis in Figure 7) and continued till six combinations (right extreme of x-axis in Figure 7). Table 5 shows the quantitative values of G-MAP with probe attempts corresponding to four different FRS. For simplicity, we have only indicated the quantitative results to 14 combinations sampled from 526 regions. *It needs to be pointed out that these 14 regions are indicative of least, moderate and most vulnerable regions from 526 unique CFIA combinations.*

Based on the obtained results following are the main observations:

- The number of composite regions used to generate the CFIA samples plays a vital role in the vulnerability of FRS. Using a smaller number of regions (for example, 2, 3 and 4) to generate the CFIA will result in a lower vulnerability of FRS. This it can be attributed to the fact that in these regions, the blending for the generation of

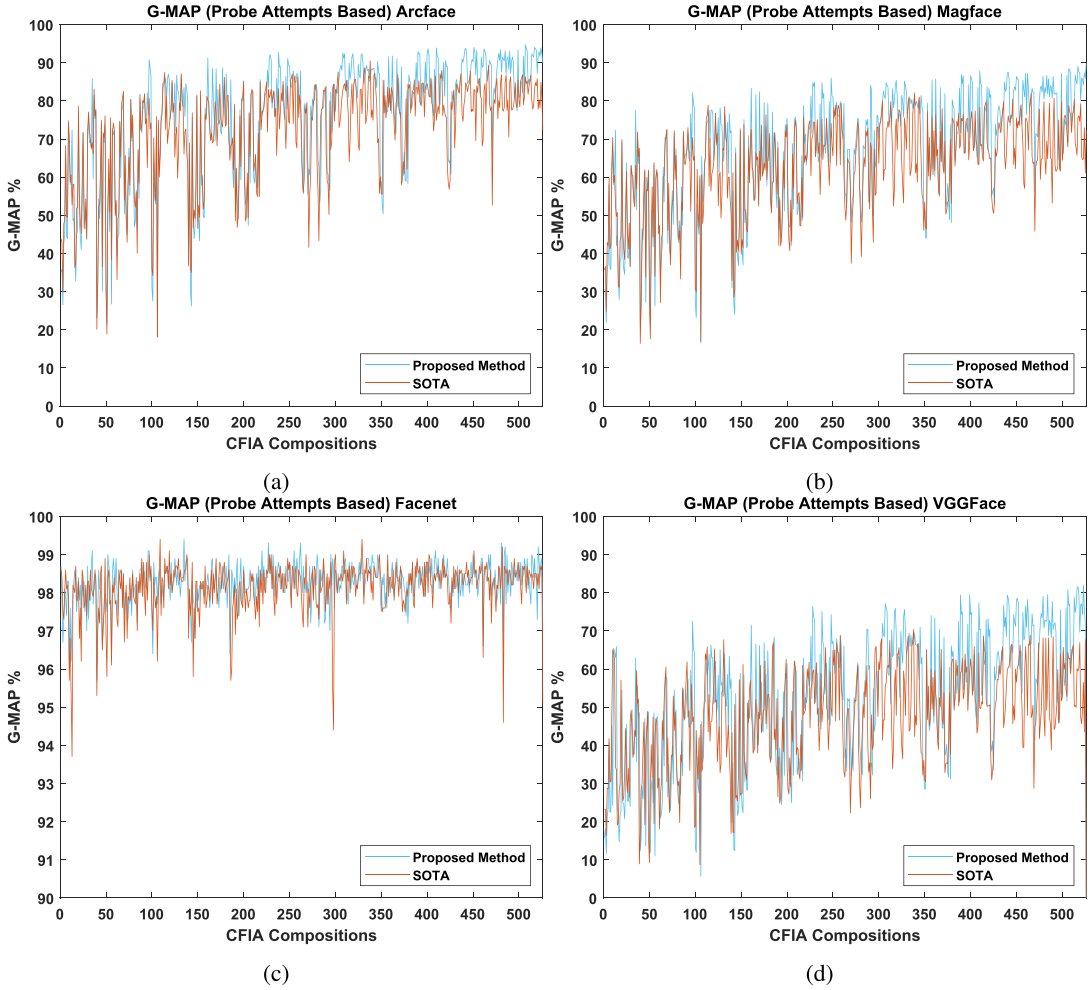


FIGURE 7. Vulnerability Plots G-MAP (Probe Attempts). X-axis indicates the number of unique CFIA generated where the index 0 corresponds to E-H, the index 1 corresponds to H-E, and the following indices in the left to right order corresponding to Table 1. Thus, finally, index 525 to HBSENM-HBSENM.

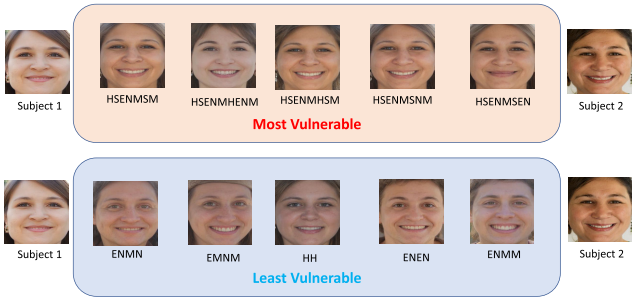


FIGURE 8. Most and Least Vulnerable CFIA Samples from the dataset.

composite happens in a small region and the remainder of the face is generated by GAN-based image inpainting. For example, if we consider the two regions (or facial attribute) CFIA generation, then one region is taken from the contributory subject 1 and another region is taken from the contributory subject 2, from these selected regions, the whole face is generated using the GAN. This process results in the loss of identity information in the generated CFIA due to the availability of a few regions.

Figure 8 illustrates the example of low vulnerable CFIA samples generated using two and three region combinations. The lower vulnerability is noted with both SOTA and the proposed CFIA generation.

- The CFIA samples generated using 4, 5 and 6 regions have indicated higher vulnerability of FRS. This can be attributed to the fact that the larger the number of facial attributes used from both the contributory data subjects, the higher the vulnerability of the FRS. This trend is noticed equally with both SOTA and the proposed CFIA generation. Figure 8 shows the CFIA samples for the top 5 highest vulnerable combinations indicating the rich identity features corresponding to both contributory subjects.
- Among the four different FRS employed in this work, the Facenet [39] indicates the higher vulnerability across different region combinations. The lowest vulnerability is noted with the VGG FRS [38].
- The proposed CFIA generation technique indicates the higher vulnerability of FRS when compared with the SOTA [26]. The higher vulnerability of FRS to the

TABLE 5. Vulnerability analysis using the G-MAP metric (probe attempts-based) for the proposed method and the SOTA [26], where the description of regions is provided in Table 1. Where R1 is (S-E), R2 is (S-N), R3 is (S-M), R4 is (S-S), R5 is (SEN-M), R6 is (SEM-N), R7 is (SNM-E), R8 is (SEN-EM), R9 is (SEN-EN), R10 is (SEN-SEM), R11 is (SEN-SEN), R12 is (SENM-ENM), R13 is (SENM-SENM), and R14 is (HBSENM-HBSENM)).

G-MAP % (Multiple probe attempts)															
FRS	**Method**	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**	**R12**	**R13**	**R14**
Arcface (FAR=0.1%)	**SOTA [26]**	70.5	58.7	60.6	52.7	70.8	69.2	72.9	71.6	69.1	69.1	67.6	74.1	69.6	72.3
	Proposed	67.3	58.1	60.2	72.4	70.4	68.4	72.5	71.9	71.4	84.2	82.8	76.4	86.8	**89.9**
MagFace (FAR=0.1%)	**SOTA [26]**	57.6	45.0	48.7	42.7	58.0	57.3	61.0	60.7	61.1	59.0	52.6	65.1	57.7	54.0
	Proposed	67.3	58.2	60.1	72.4	70.4	68.6	72.5	72.0	71.4	84.2	82.8	76.4	86.7	**89.8**
VGGFace (FAR=0.1%)	**SOTA [26]**	65.2	64.2	62.7	63.6	64.9	63.9	66.1	65.7	67.0	67.2	65.4	65.9	68.1	67.7
	Proposed	65.4	64.4	63.0	65.9	66.4	68.1	69.1	66.0	68.5	70.5	70.5	68.6	71.0	**71.9**
Facenet (FAR=0.1%)	**SOTA [26]**	95.8	96.9	95.4	93.8	95.3	96.5	95.9	95.8	96.1	95.6	94.5	96.4	94.7	95.2
	Proposed	96.1	97.7	96.3	97.4	95.5	97.3	95.4	96.4	97.4	97.2	97.3	96.6	96.6	**97.0**

TABLE 6. Vulnerability analysis using the G-MAP metric (Multiple FRS and multiple probe attempts-based) for the proposed method and the SOTA [26].

G-MAP % (Multiple FRS and multiple probe attempts)														
Method	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**	**R12**	**R13**	**R14**
SOTA [26]	57.6	45.0	48.7	42.7	58.0	57.3	61.0	60.7	61.1	59.0	52.6	65.1	57.7	54.0
Proposed	65.4	58.1	60.1	65.9	66.4	68.1	69.1	66.0	68.5	70.5	70.5	68.6	71.0	71.9

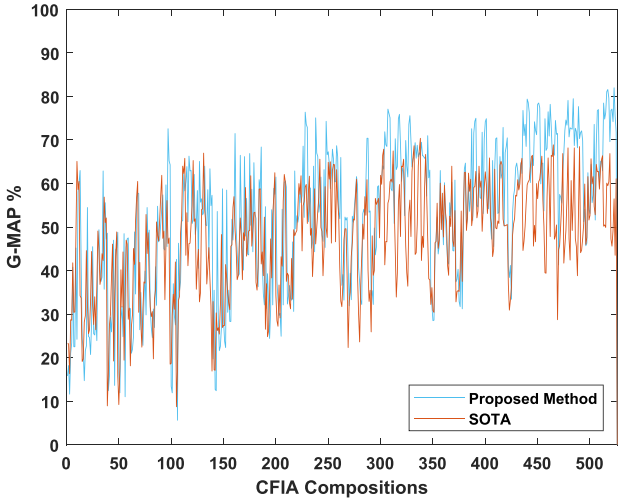


FIGURE 9. Vulnerability Plots G-MAP (Multiple FRS and multiple probe attempts-based). X-axis indicates the number of unique CFIA generated where the index 0 corresponds to E-H, the index 1 corresponds to H-E, and the following indices in the left to right order corresponding to Table 1. Thus, finally, index 525 to HBSENM-HBSENM.

proposed technique is noted with the CFIA samples that are generated using five and six-region combinations.

- Additional experiments on Commercial-Off-The-Shelf (COTS) to indicate the importance of FTAR is included in the Appendix.

Figure 9 shows the vulnerability of FRS with G-MAP computed across multiple FRS and multiple attempts for both SOTA and proposed CFIA with 526 combinations. Given CFIA sample is said to be vulnerable if the multiple probe attempts must successfully deceive the multiple FRS. Thus, the G-MAP will provide a single value indicating the vulnerability by taking the average probe attempts while accounting for FTAR. Table 6 indicates the G-MAP (multiple FRS and multiple probes) for 14 different regions (that are the same as

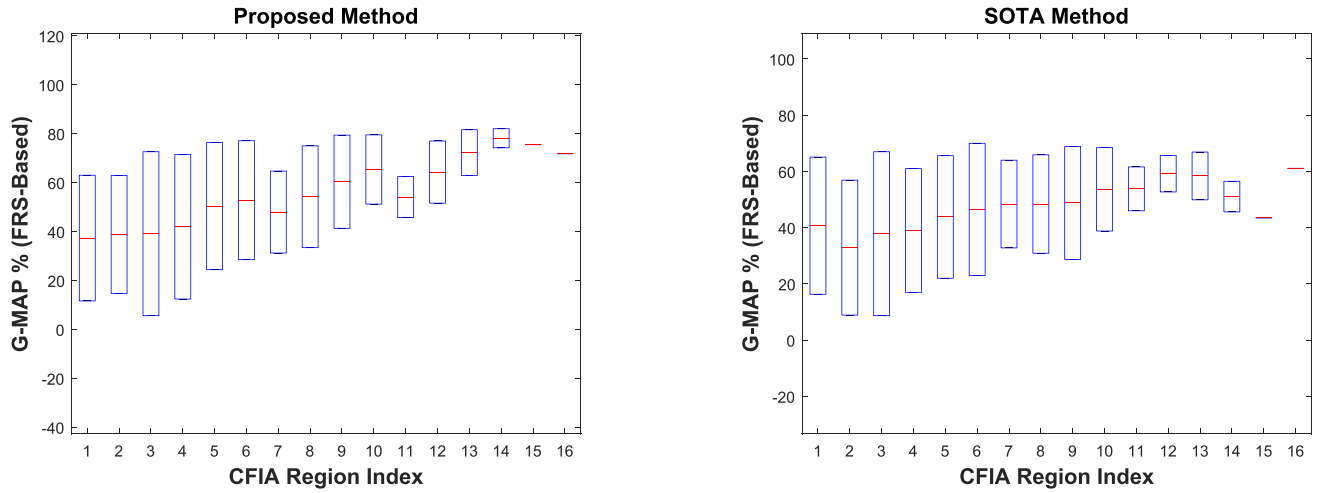
TABLE 7. G-MAP for SOTA Method and the Proposed Method computed using 526 CFIA compositions.

G-MAP %	
SOTA Method [26]	**Proposed Method**
46.9%	52.4%

Table 5) for simplicity. Based on the obtained results following are the main observations:

- The CFIA samples generated with five and six regions combinations indicate higher vulnerability of multiple FRS. This is noted with both SOTA and the proposed CFIA technique.
- The proposed CFIA samples indicate the higher vulnerability of FRS compared to SOTA.
- Figure 10 shows the box plots of proposed method and SOTA computed across CFIA region index as mentioned in Table 1 indicates the mean and variance computed by taking the average of G-MAP values computed over all region combinations within the CFIA region index. As noticed from Figure 10 and Table 8, the combinations with less number of regions do not significantly increase the vulnerability. The combination of five regions with CFIA region index of 13, 14 and 15 indicates the higher vulnerability of FRS with the proposed CFIA technique.

Table 7 indicates the vulnerability computed with full capacity of G-MAP in which multiple attempts, multiple FRS, multiple attack types and FTAR. The G-MAP values indicated in the 7 quantify the vulnerability of the proposed and SOTA for the complete CFIA dataset with 526 attack types and four different FRS. The obtained results indicate that the proposed method gives higher bounds of vulnerability for all 526 attack types.



(a) (b)

FIGURE 10. G-MAP Combinations (FRS-Based) where the number denotes the CFIA Region Index of (a) Proposed and (b) SOTA Method [26] (Table 1).

TABLE 8. Table showing mean and standard deviation for each CFIA region index based on SOTA [26] and the Proposed Method. (for CFIA region index please refer Table 1).

CFIA Region Index	Proposed Method	SOTA Method [26]
1	37.3±36.3	40.7±34.5
2	38.8±34.0	32.9±33.9
3	39.1±47.3	37.8±41.2
4	41.9±41.7	39±31.1
5	50.4±36.7	43.8±30.8
6	52.8±34.3	46.5±33.2
7	47.9±23.6	48.4±22.0
8	54.2±29.4	48.4±24.7
9	60.3±26.9	48.8±28.4
10	65.3±20.0	53.6±21.0
11	54.1±11.8	53.8±11.0
12	64.3±17.9	59.2±9.1
13	72.2±13.2	58.4±12.0
14	78.1±5.5	51.0±7.7
15	75.5±0	43.5±0
16	71.8±0	61.1±0

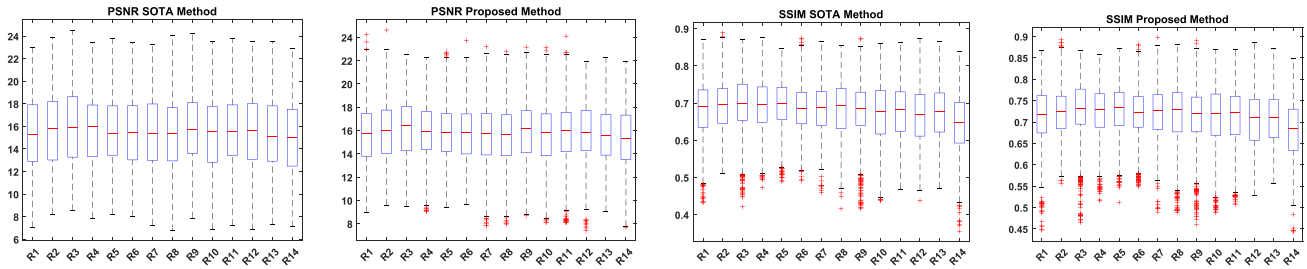
V. PERCEPTUAL QUALITY EVALUATION OF THE COMPOSITE IMAGES

This section presents the quantitative analysis of the proposed CFIA samples using two perceptual image quality metrics, namely, PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index). We present the results pertaining to 14 regions out of 526 unique regions for the simplicity and these regions are same as mention in Section IV and in Table 5. It is worth noting that, these 14 regions will represent the lower, moderate and high vulnerability of FRS. Both PSNR and SSIM are reference image-based quality metrics and thus require a pair of images for evaluation (face image from the contributory data subject and the generated face composite image). Table 9 indicates the quantitative analysis of the perceptual quality analysis on both SOTA [26] and the proposed CFIA method. Figure 11 illustrates the box plots corresponding to both SSIM and PSNR computed on all 14 regions. Following are the main observations from the obtained results:

TABLE 9. Perceptual Image quality metrics PSNR and SSIM comparison for SOTA [26] and proposed method on 14 different regions mentioned in the Table 5.

Region	PSNR		SSIM	
R1	SOTA [26]	Proposed	SOTA [26]	Proposed
R1	15.4±10.2	15.6±7.0	0.68±0.01	0.71±0.00
R2	15.5±9.5	15.7±6.6	0.68±0.01	0.71±0.00
R3	15.5±10.2	15.6±7.0	0.68±0.01	0.71±0.00
R4	15.6±8.6	15.9±4.6	0.69±0.01	0.71±0.00
R5	15.4±10.6	15.6±7.4	0.68±0.01	0.71±0.00
R6	15.5±10.0	15.7±6.9	0.68±0.01	0.71±0.00
R7	15.5±10.6	15.7±7.4	0.68±0.01	0.71±0.00
R8	15.4±9.6	15.6±6.8	0.68±0.01	0.71±0.00
R9	15.4±8.6	15.7±6.7	0.68±0.01	0.73±0.00
R10	15.7±8.7	16.0±4.7	0.69±0.01	0.72±0.00
R11	15.6±9.9	16.0±5.0	0.69±0.01	0.72±0.00
R12	15.3±7.8	15.7±6.4	0.67±0.00	0.71±0.00
R13	15.7±10.3	16.0±5.2	0.69±0.01	0.72±0.00
R14	15.8±14.4	16.0±6.4	0.68±0.01	0.71±0.00

- The PSNR metric has a higher mean-value and less variance for the proposed CFIA method compared with SOTA [26] indicating lesser noise in the face composites generated using the proposed CFIA method. This is expected as transparent blending would produce a lower contrast image, as the choice of blending-factor ($\alpha = 0.5$) would generate a pixel value lower than those from contributory data subjects as the blending equation is applied twice refer Equation 3. Thus, the proposed CFIA method generates a more consistent image quality irrespective of the region compared with SOTA [26].
- The SSIM metric produces a more stable value for both the proposed CFIA method and SOTA [26]. The proposed CFIA method gives a higher value for SSIM than the SOTA [26]. Since SSIM is a metric more tuned to the Human Visual System (HVS), [42] as it measures



(a) PSNR SOTA (b) PSNR Proposed (c) SSIM SOTA (d) SSIM Proposed

FIGURE 11. Box plots showing PSNR of SOTA [26] and the proposed Method for 14 regions. These 14 regions are same as indicated in Table 5.

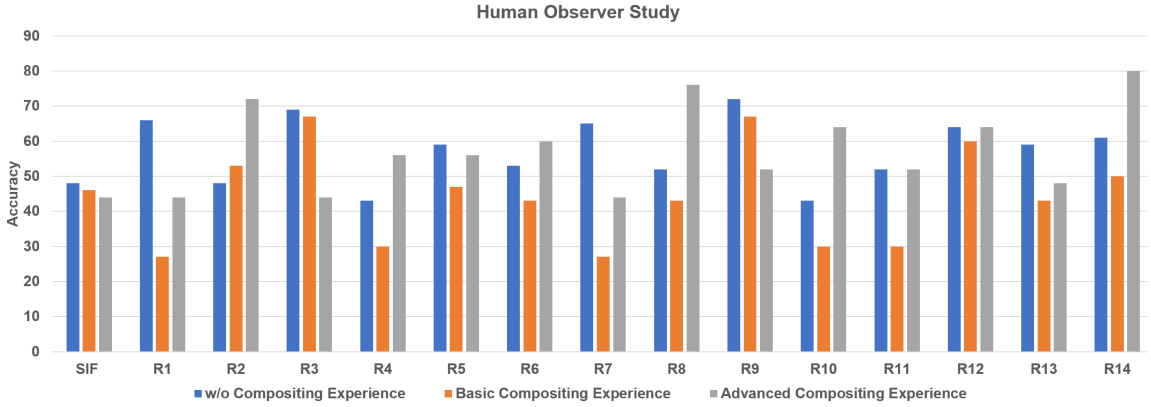


FIGURE 12. Illustration showing average accuracy quantitatively for the human observer study where bona fide or Synthetic Face Image (without any modification) is denoted as SIF.

FIGURE 13. Screenshot from the GUI (Full Page) of human observer web page.

luminance distortion, contrast distortion, and loss of correlation. Thus, our proposed CFIA method generates higher-quality composites for HVS.

VI. HUMAN OBSERVER STUDY

We perform a Human Observer Study (HOS) of the generated composites to evaluate the detection performance by human experts. We present the results pertaining to 14 regions out of 526 unique regions for the simplicity and these regions are same as mention in Section IV and in Table 5. It is worth noting that, these 14 regions will represent the lower, moderate and high vulnerability of FRS. The HOS is conducted using a web-based application[1] where a dedicated web page is set up with the use of PHP and HTML-CSS. In this study, GDPR norms are respected, and we only store the individual's email, gender, experience with the composite problem, and age group. We have made sure that the user remains anonymous during the study. Figure 13 shows the screenshot of the GUI of our website where the HOS is carried out. In this study, a human observer is shown a webpage with two images at a time where the observer has to decide independently on whether each of them is real/composite (or manipulated). The current study shows 43 image pairs, and it takes around 20 minutes to complete the study. The study includes synthetic face images and 14 different types of composites as mentioned in Table 5. Further, the human observer is explained in detail the step-wise instructions to perform the study. This enables people without awareness of the image manipulation problem and those with basic and advanced awareness of the composition problem to participate in the study. In the current evaluation, 51 human observers have participated and completed the study, including 40 participants without awareness, 6 with basic awareness, and 5 with an advanced awareness of the composition problem.

The quantitative results of HOS are as shown in Figure 12 and the following are the important observations:

- The average detection accuracy is similar for human observers without awareness of the composition problem and those with basic awareness. This can be attributed to the innate human ability to detect composites. However, the average detection accuracy for human observers with advanced awareness of the composition

[1] https://folk.ntnu.no/jagms/indexCompositeUpdated.html

problem is much higher than both without awareness and basic awareness.

- The average accuracy is not very high for faces based on the composition, which utilizes a single facial attribute except for **R2** with advanced awareness. This can be attributed to the fact that a large part of the facial region needs to be inpainted in the case of single facial attribute composition.
- The average detection accuracy is high for the regions **R8**, **R10**, **R12**, and **R14**. **R8** has moderate parts of faces being used for compositing from the two contributory data subjects. The reason for high detection accuracy can be attributed to the fact that **R8** has only eyes from both the contributory data subjects but his nose and mouth from different contributory data subjects. The same reasoning with more significant facial parts used for compositing can be extended to **R10** where the nose and mouth are from different contributory data subjects but have skin and eyes from both contributory data subjects. Now for the compositing region **R12**, the skin region is only from one contributory data subject. Thus, in all three cases, the asymmetry in the regions from the contributory data subjects aids the human observer in performing the detection at high accuracy.
- However, the average performance of the human observers for detecting a normal face image (or non-composite) is 46%. Further, it is also interesting to observe that degraded performance is noted in the advanced experience group. Thus, our analysis indicates that human observers are limited in detecting the normal face images compared to the composite face images.
- Now, for the compositing region **R14** all facial parts from the contributory data subjects are being used. Thus, the composited image can be distinguished from a synthetic face image using global image-based cues.
- In summary, we could say that either asymmetric regions or global level cues can help the human observer perform detection at high accuracy rates. However, our analysis indicates that it is very challenging for humans to detect composite attacks.

VII. COMPOSITE FACE IMAGE ATTACK DETECTION

In this section, we benchmark CFIA detection based on a single image. Since the generation of CFIA is procedurally similar to morphing generation with transparent blending. Therefore, we have employed three different Face Morphing Attack Detection (MAD) techniques to benchmark the CFIA detection. MAD methods are selected by considering their detection performance on various morphing data sources, including NIST FRVT MORPH benchmarking. To this extent, we have chosen three different S-MAD approaches, namely: Color denoising based S-MAD (DetAlgo1) [43], Hybrid features (DetAlgo2) [44] and Residual noise-based S-MAD Network (DetAlgo3) [45]. We also report the performance of CAD algorithms on 14 different regions for the same reasons that were descried in previous section IV. These algorithms are briefly explained as follows:

Color denoising based S-MAD (DetAlgo1) [43]: DetAlgo1 is based on using the color information by converting the RGB image HSV color space. Then, each color channel is denoised using a Deep Convolutional Neural Network to compute the corresponding residual noise. In the next step, Pyramid LBP (P-LBP) and an SRKDA classifier for final detection.

Hybrid features (DetAlgo2) [44]: DetAlgo2 is based on two different colors spaces. Given the RGB image, firstly, it is converted to HSV and YCbCr color space. In the next step, micro-texture features are computed using pyramid-LBP and passed through the SRKDA classifier. The final classification is performed using SUM rule fusion to make the final decision on detection.

Residual noise-based S-MAD Network (DetAlgo3) [45]: DetAlgo3 is based on the computing the residual noise using the Multi-Scale Context Aggregation Network (MS-CAN). The residual noise is further processed through Alexnet to obtain the classified features using the Collaborative Representative Classifier (CRC) to make the final decision to detect the attack.

To benchmark CFIA detection performance we resort to the off-the-shelf S-MAD. Three different S-MAD methods employed in this work are trained using different morph generation types (landmark-based and deep learning) and three different mediums (Digital, print-scanned, and print-scanned compression) generated using the publicly available FRGC face database. The quantitative results are presented using the ISO/IEC metrics [46] which are as follows: 1) Attack Presentation Classification Error Rate (APCER (%)) defining the percentage of attack images (morph images) incorrectly classified as bona fide images [46], 2) Bonafide Presentation Classification Error Rate (BPCER (%)) defining the percentage of bona fide images incorrectly classified as attack images [46] and 3) Detection Equal Error Rate (D-EER (%)) [17]. The detection performance is benchmarked with both SOTA and proposed CFIA images and quantitative results are presented in Table 10 and bar chart with D-EER (%) on all 14 different regions. Based on the obtained results following are the main observations:

- The CFIA detection performance is degraded with all three detection algorithms.
- Among three different detection algorithms. DetAlgo3 indicates the better detection accuracy attributed to the quantification of residual noise.
- Among the 14 different regions, the degraded detection performance is noted with the R14 on all three detection algorithms.

Thus, based on the obtained results, we can conclude that the detection of CFIA attacks is very challenging and this needs more sophisticated detection algorithms to be devised for reliable detection.

TABLE 10. CFIA attack detection using DetAlgo1 [43], DetAlgo2 [44], and DetAlgo3 [45].

Detection Method (Region)	D-EER (%)		BPCER @ APCER =			
			5%		10%	
R1	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	42.9	96.0	92.1	92.5	86.3
DetAlgo2 [44]	50.0	50.0	95.9	94.3	92.4	89.2
DetAlgo3 [45]	38.2	28.7	85.4	74.0	78.5	57.2
R2	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	44.6	96.0	93.0	92.3	86.0
DetAlgo2 [44]	50.0	50.0	96.2	94.4	92.3	91.2
DetAlgo3 [45]	39.5	29.3	87.1	78.5	78.9	64.8
R3	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	47.0	95.5	93.9	92.1	88.7
DetAlgo2 [44]	50.0	50.0	96.3	94.7	92.8	91.5
DetAlgo3 [45]	40.6	32.2	88.3	79.1	80.3	65.8
R4	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	49.0	39.6	94.3	90.5	89.0	81.7
DetAlgo2 [44]	50.0	50.0	96.1	92.6	92.8	88.9
DetAlgo3 [45]	42.8	32.4	89.8	77.7	82.2	64.6
R5	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	45.0	95.0	93.3	91.0	86.6
DetAlgo2 [44]	50.0	50.0	96.6	93.9	92.7	90.8
DetAlgo3 [45]	42.0	31.6	87.9	76.5	80.7	64.8
R6	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	44.1	95.5	92.5	91.8	84.6
DetAlgo2 [44]	50.0	50.0	95.3	92.7	91.0	88.9
DetAlgo3 [45]	38.0	29.3	85.3	73.2	78.5	60.2
R7	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	43.5	95.0	92.5	90.8	85.8
DetAlgo2 [44]	50.0	49.7	95.8	92.8	92.1	87.5
DetAlgo3 [45]	39.5	29.8	87.9	73.7	78.9	60.0
R8	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	44.6	96.2	94.0	92.2	85.9
DetAlgo2 [44]	50.0	49.8	96.0	92.5	92.0	87.4
DetAlgo3 [45]	41.7	30.6	87.4	75.4	81.3	61.5
R9	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	43.4	95.7	91.8	90.6	84.5
DetAlgo2 [44]	50.0	50.0	95.8	91.6	91.5	86.3
DetAlgo3 [45]	40.5	28.4	87.5	78.5	81.7	63.2
R10	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	48.2	38.5	94.2	86.6	87.9	77.9
DetAlgo2 [44]	50.0	48.0	94.7	91.8	90.7	87.4
DetAlgo3 [45]	41.6	30.2	87.0	76.2	80.9	61.9
R11	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	49.0	37.3	95.2	88.0	89.6	76.3
DetAlgo2 [44]	50.0	50.0	93.7	92.7	92.2	88.6
DetAlgo3 [45]	41.9	31.7	87.1	80.0	80.7	67.8
R12	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	43.7	95.4	90.6	91.4	83.0
DetAlgo2 [44]	50.0	48.8	94.8	91.4	91.4	86.0
DetAlgo3 [45]	41.8	30.8	87.6	76.4	80.5	64.1
R13	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	48.7	37.4	94.2	86.8	89.0	76.6
DetAlgo2 [44]	50.0	49.1	93.6	91.6	91.4	86.7
DetAlgo3 [45]	41.4	32.2	86.9	78.5	80.2	64.8
R14	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**	**SOTA [26]**	**Proposed**
DetAlgo1 [43]	50.0	42.6	97.6	90.2	94.8	83.7
DetAlgo2 [44]	50.0	49.5	97.2	95.7	93.4	88.0
DetAlgo3 [45]	46.4	34.0	92.2	83.8	83.2	72.1

VIII. CONCLUSION

In this work, we presented a new type of digital attack based on the facial attributes and we termed it as Composite Face Image Attack (CFIA). Given the facial images from the two contributory data subjects, the proposed CFIA will first segment the face images into six different attributes independently. Then, these segments are blended using a transparent mask based on both single face-attribute and multiple face attributes. These attributes are processed using the image inpainting based on pre-trained GAN to generate the final

TABLE 11. Vulnerability analysis using the proposed GMAP metric (probe attempts-based with FTAR) for the proposed method and the SOTA [26].

G-MAP % (Probe Attempts) with FTAR															
FRS	Method	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14
Neurotech (FAR=0.1%)	SOTA [26]	18.2	10.4	10.9	8.1	16.2	14.6	19.0	18.8	19.3	14.2	14.0	21.6	15.0	11.3
	Proposed	13.8	10.2	9.7	17.6	13.5	14.4	16.0	17.1	19.3	22.2	22.9	21.0	23.7	**23.3**
Cognitec (FAR=0.1%)	SOTA [26]	31.6	22.2	23.3	19.8	27.7	28.8	33.1	34.0	37.9	30.0	24.8	41.1	25.1	21.3
	Proposed	30.5	22.9	22.3	43.9	28.1	26.9	31.9	34.7	35.3	54.6	55.1	43.0	57.6	**60.7**

TABLE 12. Vulnerability analysis using the G-MAP metric (Probe Attempts- without FTAR) for the proposed method and the SOTA [26].

G-MAP % (Probe Attempts) without FTAR															
FRS	Method	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14
Neurotech (FAR=0.1%)	SOTA [26]	54.4	33.1	35.1	32.4	50.0	44.3	59.1	58.1	59.5	51.3	50.3	65.4	55.0	45.3
	Proposed	43.1	31.6	33.1	57.8	41.8	43.5	49.7	51.9	56.9	72.2	75.2	63.9	79.5	79.2
Cognitec (FAR=0.1%)	SOTA [26]	31.9	22.5	23.5	20.0	28.0	29.2	33.5	34.4	38.3	30.3	25.2	41.6	25.5	21.6
	Proposed	30.8	23.2	22.6	44.4	28.4	27.2	32.2	35.1	35.7	55.2	55.8	43.4	58.3	61.4

CFIA samples. In this work, given the face images from two contributory data subjects, we generate 526 different composite face images based on single and multiple face attributes. We contributed a new dataset with 1000 unique identities that will result in 526000 CFIA samples. Extensive experiments are performed to evaluate the attack potential of the newly generated CFIA using four different FRS. To effectively benchmark the vulnerability of the generated CFIA, we have introduced a generalized vulnerability metric. Further, we benchmark the detection accuracy using both human and automatic detection techniques. Our results demonstrated that the proposed CFIA could indicate the vulnerability of the FRS while it is difficult to detect using both human and automatic detection techniques. In the future work, we would like to extend the present work in several directions: 1) Generation of composites of higher quality, 2) Evaluation of the proposed method on real face images on public datasets, 3) Development of novel detection techniques.

APPENDIX. ROLE OF FTAR IN COMPUTING VULNERABILITY

In this appendix, we present additional results on the vulnerability of COTS to illustrate the importance of FTAR in computing the G-MAP. The use of academic FRS does not include quality estimation to optimize the verification performance; thus, FTAR can be assumed to be zero. However, with COTS FRS (which is more practical), the captured face quality is imposed because of which the FRS seeks good-quality face images to optimize the verification performance. The requirement of good quality will result in the rejection of probe attempts deemed low-quality face capture and, thus, the failure of verification with reasonable attempts. Hence the proposed FTAR will penalise the failure to verify with a reasonable attempt.

Table 11 and 12 indicates the quantitative results of two different Commercial-Off-The-Shelf (COTS) such as Neurotechnology Version 10.0 [23] and Cognitec FaceVACS-SDK Version 9.4.2 [24][2] in which G-MAP is computed with the multiple attempts on 14 different combinations. These 14 regions are the same as those used in the earlier sections of the papers that are representative of low, moderate and high vulnerability combinations. As noticed from the Tables 11 and 12 the G-MAP with FTAR will indicate the less vulnerability meaning that, the COTS FRS fail to perform the verification. Therefore accountability to FTAR is important to be consider for vulnerability calculation.

[2]Disclaimer: These results were produced in experiments conducted by us and should; therefore, the outcome does not necessarily constitute the best the algorithm can do.

REFERENCES

[1] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2015, pp. 815–823.
[2] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4685–4694.
[3] (2020). *NIST FRVT Morph*. Accessed: 19, 2022. [Online]. Available: https://pages.nist.gov/frvt/html/frvt_morph.html
[4] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–37, Jan. 2018.
[5] F. Abdullakutty, E. Elyan, and P. Johnston, "A review of state-of-the-art in face presentation attack detection: From early development to advanced deep learning and multi-modal fusion methods," *Inf. Fusion*, vol. 75, pp. 55–69, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253521000919
[6] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *Proc. 3rd Int. Conf. Learn. Represent.*, Y. Bengio and Y. LeCun, Eds. San Diego, CA, USA, 2015, pp. 1–11.
[7] Y. Xu, K. Raja, R. Ramachandra, and C. Busch, "Adversarial attacks on face recognition systems," in *Handbook of Digital Face Manipulation and Detection*. Cham, Switzerland: Springer, 2022, pp. 139–161.
[8] F. Vakhshiteh, A. Nickabadi, and R. Ramachandra, "Adversarial attacks against face recognition: A comprehensive study," *IEEE Access*, vol. 9, pp. 92735–92756, 2021.
[9] N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey," *IEEE Access*, vol. 6, pp. 14410–14430, 2018.
[10] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face morphing attack generation and detection: A comprehensive survey," *IEEE Trans. Technol. Soc.*, vol. 2, no. 3, pp. 128–145, Sep. 2021.
[11] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep. 2014, pp. 1–7.
[12] S. R. Godage, F. Løvasdal, S. Venkatesh, K. Raja, R. Ramachandra, and C. Busch, "Analyzing human observer ability in morphing attack detection—Where do we stand?" *IEEE Trans. Technol. Soc.*, vol. 4, no. 2, pp. 125–145, Jul. 2023.
[13] C. Burt. (2022). *Morphing Attack Detection for Face Biometric Spoofs Needs More Generalization, Datasets*. [Online]. Available: https://bit.ly/3lsJ1K8
[14] Quek, Alyssa. (2018). *Face Morpher*. Accessed: Jan. 19, 2022. [Online]. Available: https://github.com/alyssaq/face_morpher
[15] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 1008–1017, Apr. 2018.
[16] N. Damer, A. M. Saladié, A. Braun, and A. Kuijper, "MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network," in *Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Oct. 2018, pp. 1–10.
[17] 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 Trans. Biometrics, Behav., Identity Sci.*, vol. 3, no. 3, pp. 365–383, Jul. 2021.
[18] N. Damer, K. Raja, M. Sußmilch, S. Venkatesh, F. Boutros, M. Fang, F. Kirchbuchner, R. Ramachandra, and A. Kuijper, "ReGenMorph: Visibly realistic GAN generated face morphing attacks by attack re-generation," in *Proc. Int. Symp. Vis. Comput.* Cham, Switzerland: Springer, 2021, pp. 251–264.
[19] S. R. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Ramachandra, and C. Busch, "Analyzing human observer ability in morphing attack detection—Where do we stand?" *IEEE Trans. Technol. Soc.*, 2022.

[20] L. Qin, F. Peng, S. Venkatesh, R. Ramachandra, M. Long, and C. Busch, "Low visual distortion and robust morphing attacks based on partial face image manipulation," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 3, no. 1, pp. 72–88, Jan. 2021.

[21] P. Pérez, M. Gangnet, and A. Blake, "Poisson image editing," in *Proc. ACM SIGGRAPH*. New York, NY, USA: Association for Computing Machinery, 2003, pp. 313–318, doi: 10.1145/1201775.882269.

[22] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *Proc. Brit. Mach. Vis. Conf. (BMVC)*, M. W. X. Xie and G. K. L. Tam, Eds. Sep. 2015, pp. 1–12, doi: 10.5244/C.29.41.

[23] Neurotechnology. (2019). *Neurotech Verilook SDK (11.1)*. Accessed: Jan. 19, 2022. [Online]. Available: https://www.neurotechnology.com/verilook.html

[24] Cognitec. (2019). *Cognitec Face VACS (9.6)*. Accessed: Jan. 19, 2022. [Online]. Available: https://www.cognitec.com/facevacs-technology.html

[25] B. Zhou, H. Zhao, X. Puig, S. Fidler, A. Barriuso, and A. Torralba, "Scene parsing through ADE20K dataset," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 5122–5130.

[26] L. Chai, J. Wulff, and P. Isola, "Using latent space regression to analyze and leverage compositionality in GANs," in *Proc. Int. Conf. Learn. Represent.*, 2021, pp. 1–30.

[27] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4396–4405.

[28] 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 *Proc. 8th Int. Workshop Biometrics Forensics (IWBF)*, Apr. 2020, pp. 1–6.

[29] N. Damer, K. Raja, M. Sußmilch, S. Venkatesh, F. Boutros, M. Fang, F. Kirchbuchner, R. Ramachandra, and A. Kuijper, "ReGenMorph: Visibly realistic GAN generated face morphing attacks by attack re-generation," in *Advances in Visual Computing*, G. Bebis, V. Athitsos, T. Yan, M. Lau, F. Li, C. Shi, X. Yuan, C. Mousas, and G. Bruder, Eds. Cham, Switzerland: Springer, 2021, pp. 251–264.

[30] T. Xiao, Y. Liu, B. Zhou, Y. Jiang, and J. Sun, "Unified perceptual parsing for scene understanding," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018, pp. 418–434.

[31] Y. Shen, C. Yang, X. Tang, and B. Zhou, "InterFaceGAN: Interpreting the disentangled face representation learned by GANs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 4, pp. 2004–2018, Apr. 2022.

[32] E. Sarkar, P. Korshunov, L. Colbois, and S. Marcel, "Vulnerability analysis of face morphing attacks from landmarks and generative adversarial networks," 2020, *arXiv:2012.05344*.

[33] N. Damer, C. A. F. López, M. Fang, N. Spiller, M. V. Pham, and F. Boutros, "Privacy-friendly synthetic data for the development of face morphing attack detectors," 2022, *arXiv:2203.06691*.

[34] 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 *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2017, pp. 1–7.

[35] S. Venkatesh, K. Raja, R. Ramachandra, and C. Busch, "On the influence of ageing on face morph attacks: Vulnerability and detection," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Sep. 2020, pp. 1–10.

[36] M. Ferrara, A. Franco, D. Maltoni, and C. Busch, "Morphing attack potential," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Apr. 2022, pp. 1–6.

[37] InsightFace. (2022). *Insightface: 2D and 3D Face Analysis Project*. [Online]. Available: https://github.com/deepinsight/insightface.git

[38] R. Malli. (2022). *Keras-VGGFace*. [Online]. Available: https://github.com/rcmalli/keras-vggface.git

[39] D. Sandberg. (2022). *FaceNet TensorFlow*. [Online]. Available: https://github.com/davidsandberg/facenet.git

[40] I. Meng. (2023). *Magface*. [Online]. Available: https://github.com/IrvingMeng/MagFace.git

[41] N. J. M. Singh. (2022). *Generalized Morphing Attack Potential*. [Online]. Available: https://github.com/

[42] A. Horé and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 2366–2369.

[43] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Morphed face detection based on deep color residual noise," in *Proc. 9th Int. Conf. Image Process. Theory, Tools Appl. (IPTA)*, Nov. 2019, pp. 1–6.

[44] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Towards making morphing attack detection robust using hybrid scale-space colour texture features," in *Proc. IEEE 5th Int. Conf. Identity, Secur., Behav. Anal. (ISBA)*, Jan. 2019, pp. 1–8.

[45] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2020, pp. 269–278.

[46] *Information Technology—Biometric Presentation Attack Detection—Part 3: Testing and Reporting*, International Organization for Standardization, Standard ISO/IEC 30107-3, 2017.

JAG MOHAN SINGH (Member, IEEE) received the B.Tech. (Hons.) and M.S. (Research) degrees in computer science from the International Institute of Information Technology (IIIT), Hyderabad, in 2005 and 2008, respectively. He is currently pursuing the Ph.D. degree 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 (Senior Member, IEEE) received the joint Ph.D. degree 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 with the Institute of Information Security and Communication Technology (IIK), Norwegian University of Science and Technology (NTNU), Gjøvik, Norway. He is also a Research and Development Chief with MOBAI AS. He was a Researcher with Istituto Italiano di Tecnologia, Genoa, Italy, where he worked with video surveillance and social signal processing. His research interests include deep learning, machine learning, data fusion schemes, and image/video processing, with applications to biometrics, multi-modal biometric fusion, human behavior analysis, and crowd behavior 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 organizing and program committees and has served as an associate editor for various journals. He has participated (as a PI, a Co-PI or a contributor) in several EU projects, IARPA USA, and other national projects. He has received several best paper awards. He is serving as an Editor for the ISO/IEC 24722 standards on multi-modal biometrics and an Active Contributor for ISO/IEC SC 37 standards on biometrics.