This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

Face Morphing Attack Generation & Detection: A Comprehensive Survey

Sushma Venkatesh Raghavendra Ramachandra Kiran Raja Christoph Busch
Norwegian University of Science and Technology (NTNU), Norway
E-mail: {sushma.venkatesh;raghavendra.ramachandra;kiran.raja;christoph.busch} @ntnu.no

***Abstract*—Face recognition has been successfully deployed in real-time applications, including secure applications such as border control. The vulnerability of face recognition systems (FRSs) to various kinds of attacks (both direct and indirect attacks) and face morphing attacks has received great interest from the biometric community. The goal of a morphing attack is to subvert an FRS at an automatic border control (ABC) gate by presenting an electronic machine-readable travel document (eMRTD) or e-passport that is obtained based on a morphed face image. Since the application process for an e-passport in the majority of countries requires a passport photo to be presented by the applicant, a malicious actor and an accomplice can generate a morphed face image to obtain the e-passport. An e-passport with a morphed face image can be used by both the malicious actor and the accomplice to cross a border, as the morphed face image can be verified against both of them. This can result in a significant threat, as a malicious actor can cross the border without revealing the trace of his/her criminal background, while the details of the accomplice are recorded in the log of the access control system. This survey aims to present a systematic overview of the progress made in the area of face morphing in terms of both morph generation and morph detection. In this paper, we describe and illustrate various aspects of face morphing attacks, including different techniques for generating morphed face images and state-of-the-art morph attack detection (MAD) algorithms based on a stringent taxonomy as well as the availability of public databases, which allow us to benchmark new MAD algorithms in a reproducible manner. The outcomes of competitions and benchmarking, vulnerability assessments and performance evaluation metrics are also provided in a comprehensive manner. Furthermore, we discuss the open challenges and potential future areas that need to be addressed in the evolving field of biometrics.**

I. Introduction

Biometrics is a technique for recognizing an individual based on unique biological (e.g., face, fingerprint, iris) or behavioural (e.g., gait, keystroke style) characteristics [61] [37]. With the drastic improvement in deep learning techniques, biometric-based person identification and verification has emerged as a popular technique that can be widely used for many secure access control applications. The ease of capture and the suitability of face biometric characteristics have further driven face recognition as a popular biometric modality in such applications. Face recognition systems (FRSs) are widely deployed for various applications, especially in secure access control for person identification and verification purposes. Among several other applications, such as healthcare, law enforcement, and e-commerce (banking), one of the most relevant applications is the border control process, where the facial characteristics of a traveller are compared with a reference in a passport or visa database to verify the claimed identity.

Although an FRS effectively distinguishes an individual from other subjects, the FRS's risk of being attacked to mislead or conceal an actual identity is a major concern. As with all applications, the FRS is prone to various attacks, such as presentation attacks, which have the goal of subverting the FRS by presenting an artefact [90], where various types of attacks, such as electronic display attacks, print attacks, replay attacks and 3D face mask attacks, can be used [90] [54] [62] [26] [46] [38] [25] [87] [47] [35]. In addition to these attacks, the morphing attack has emerged in the recent past as a severe threat to the enrolment process that successfully undermines FRS capabilities [48]. Face morphing is defined as "a seamless transition of a facial image transforming a facial image into another" [9] in the context of biometrics; two or more facial images can be combined to resemble the contributing subjects. Morphing attacks raise a major concern, as the morphed image represents the facial characteristics of both individuals contributing to the morphing process (for instance, an accomplice and a malicious actor). Ultimately, the resulting morphed facial image can successfully be verified with probe images from both contributing subjects, making it practically usable for various malicious actions. Therefore, this attack breaks the rule of single ownership; for instance, an identification document such as a passport or electronic machine-readable travel document (eMRTD) [8] has a unique link to the data subject for whom the document was issued. The facial image stored in the eMRTD or passport is compared with the person claiming identity document ownership while crossing the border. If the enrolled facial image is determined as a match with the live image, the data subject can cross the border. Thus, an individual with malicious intent can exploit the face morphing attack and obtain illegal access. Hence, a malicious person can easily cross a border using an eMRTD or passport if he/she has contributed to the morphed image that was used in the passport application process.

Figure 1 illustrates an example scenario in border control where the facial image of a malicious person is morphed with that of a look-like accomplice. As several morphing software programs are freely available, even a non-technical person can perform morphing with ease. The accomplice can submit

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

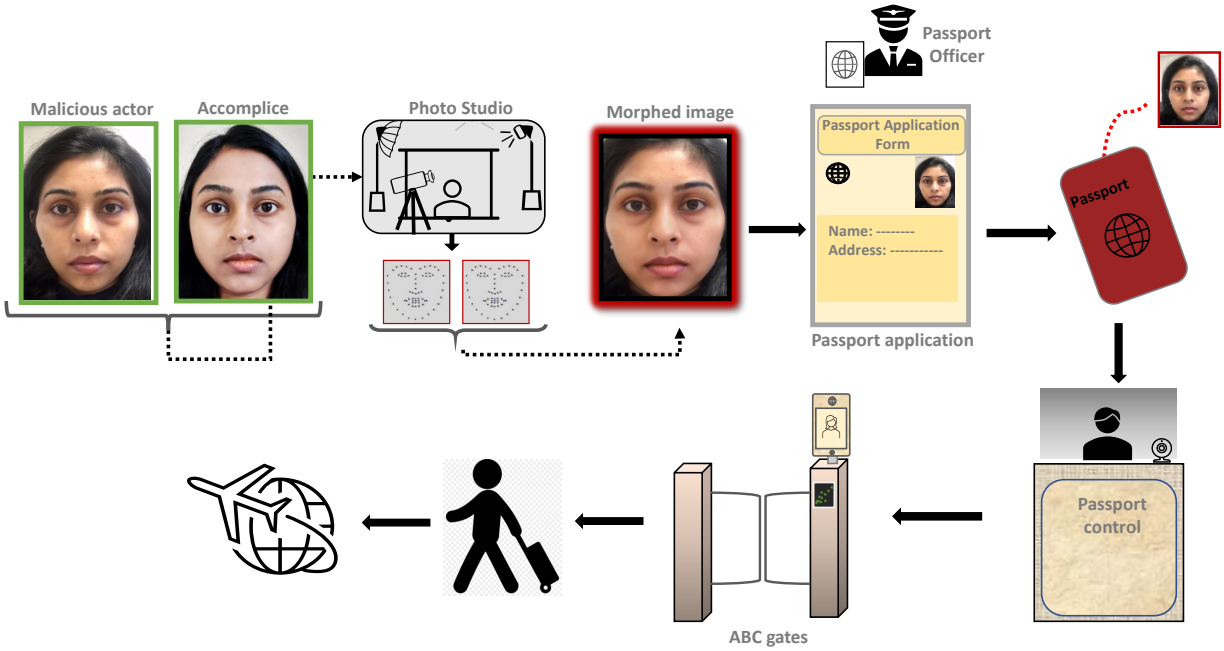

Fig. 1: An example scenario illustrating the vulnerability of FRSs to morphed images in border control.

the generated morphed image for passport enrolment at the passport issuance office. As the morphed image's facial features resemble those of the applicant's face, the passport officer approves the application. Ultimately, a malicious person can successfully use the genuine passport, allowing him/her to achieve all foreseeable purposes (e.g., crossing a border).

In most countries, the applicant submits a printed facial image to the passport office, allowing the possibility of providing a morphed image after printing and scanning. However, some countries, such as New Zealand, Estonia and Ireland, also accept a digital facial image for passport renewal [3]. Hence, an applicant can submit a digital facial image to the web portal. This practice raises a further severe concern, as there is no trusted supervision while uploading the digital facial image, and this opens the possibility of uploading a morphed image. The B1/B2 visa application for the United States also allows the applicant to upload a digital facial image through the web portal [23]. An applicant can use this opportunity to upload a morphed image with the intent to perform illegal activity.

All such vulnerabilities of FRSs have made morphing research crucial in recent years to avoid probable security lapses. Thus, several research projects have been funded by the European Union and national research councils (e.g., SWAN [22], ANANAS [4], SOTAMD [10] and iMARS [18]) to focus extensively on developing morph attack detection (MAD) algorithms. Motivated by the momentum of the problem of morphing and its criticality, a dedicated conference has been initiated by Frontex, the European Border and Coast Guard Agency [6], where a MAD interest group gathered to discuss the challenges and advancements of MAD techniques [53]. Furthermore, the U.S. National Institute of Standards and Technology (NIST) is, in parallel, conducting testing of MAD technology within the framework of the Face Recognition Vendor Test (FRVT) under Part 4: MORPH - Performance of Automated Face Morph Detection [81]. Both industrial and academic institutions are invited to submit their MAD algorithms to benchmark the accuracy [81]. Similarly, the University of Bologna, as part of the SOTAMD project [70], introduced a parallel face morphing evaluation platform to benchmark the performance of the MAD techniques on a sequestered dataset.

The rest of this survey is organised as follows: Section II presents a brief introduction to face morphing attacks, and Section III discusses face morph generation techniques. Section IV describes face morphing datasets, including private and public datasets, Section V discusses human perception capabilities in detecting morphed face images, Section VI presents various automatic morphing attack detection techniques, Section VII presents the performance metrics that are widely used to benchmark the performance of MAD methods as well as the vulnerability of generated morphed images, Section VIII discusses the public evaluation and benchmarking of MAD, Section IX discusses open challenges and potential future work and Section X gives the conclusion.

II. Face Morphing Attack

The morphing process can be defined as a special effect that transforms one image into another image. Figure 2 illustrates the facial morphing process, where two facial images are combined to generate a single morphed image. Morphing can be achieved easily by using one of the numerous and freely available tools, such as MorphThing [20], 3Dthis Face Morph [13], Face Swap Online [17], Abrosoft FantaMorph [14], FaceMorpher [16], and MagicMorph [19]. The morphed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

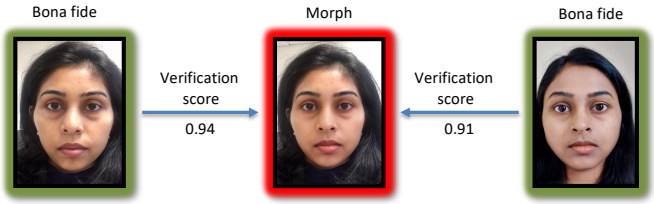

Fig. 2: Impact of face morphing on an FRS. As noted in the figure, the morphed image can be verified equally against both contributing subjects with a high similarity score from the FRS (1 being high similarity).

image possesses near-identical features to those of both subjects contributing to generating the morph when subject pre-selection is applied (e.g., look-alike mode) [91].

Furthermore, when processed with care, the morphed image does not possess many visible artefacts, and thus, a human observer may fail to detect image manipulation based on morphing. In practice, this leads to a situation where a passport officer may not be able to detect the morphing attack despite being an expert in facial comparison [65], [98]. This makes it reasonable for a criminal with malicious intent to be able to use a passport enrolled with a morphed image and cross a border without challenge. Figure 1 illustrates the vulnerability of FRSs when attacked with morphed images in a border control scenario.

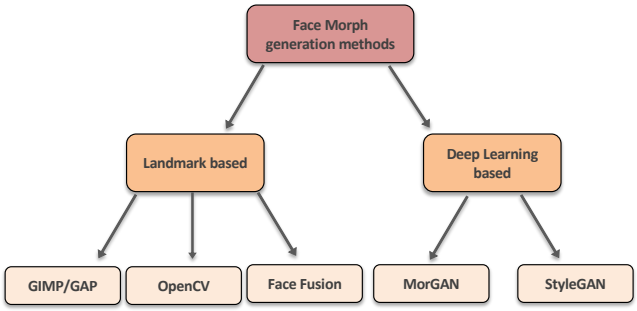

Fig. 3: Taxonomy of face morph generation techniques

III. Face Morph Attack Generation

Face morphing has been widely used for more than a decade, especially in the video animation industry [2], but the attack potential against FRSs has been noted recently [48]. Morphs can be generated using various techniques, from simple image warping to recent generative adversarial networks (GANs) [27], [33], [34], [66], [68], [86], [128], [130], [131]. The most widely used morph generation methods are based on the landmark-based technique [11], [51], [92], [104], where morphing is carried out by combining the images with respect to corresponding landmarks. Recent works eliminate the constraints of landmarks by simply relying on deep network architectures [41], [131]. Figure 3 shows a taxonomy of face morphing generation methods that indicates the broad classification of the available techniques as (a) landmark-based and (b) deep learning-based approaches.

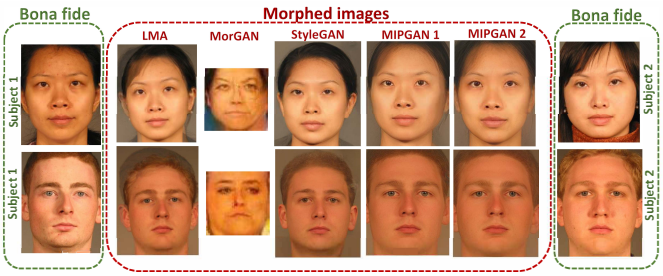

Fig. 4: Illustration of face morph images generated using different methods

A. Landmark-based Morph Generation

Landmark-based morph generation works by obtaining landmark points on facial regions, e.g., the nose, eye, and mouth. These landmark points obtained from both faces are warped by moving the pixels to different, more averaged positions. Different procedures for warping exist, including free-form deformation (FFD) [67], [120], deformation by moving least squares [102], deformation based on mass-spring models [36], and Bayesian framework-based morphing [31]. Ruprecht et al. [100] proposed performing warping by moving the pixel points of both contributing subjects to the nearest landmark point. Delaunay triangulation was later proposed, where the pixels of both contributing facial images are distorted and moved to different directions to generate triangles [56], [73], [106], [108], [113], [129]. Images that are to be morphed are blended by considering the blending factors or the morphing factor. Face morphing applications employ a morphing factor of 0.5 to generate high-quality and useful morphs that can resemble both contributing subjects equally, to which the COTS FRS is vulnerable [91]–[93]. As the morphing process translates landmarks and the associated texture, there may be some misaligned pixels that contribute to noise generating artifacts and ghost-like images and making the images unrealistic in appearance (i.e., easy for a human observer to detect). Hence, certain post-processing steps, such as image smoothing, image sharpening, edge correction, histogram equalisation, manual retouching, and image enhancement improve the brightness and contrast and can reduce or minimise the artefacts generated during the morphing process [32], [113], [126].

Face morph generation using open-source resources such as GIMP/GAP and OpenCV also relies upon landmarks. While open-source software based on GIMP/GAP and OpenCV can generate morphs, significant effort must be made to post-process the generated images to eliminate artefacts. Several commercial solutions, such as Face Fusion [109] and FantaMorph [14], can also be used to generate large-scale morphed images with reasonable post-processing effort. The reader is further referred to Scherhag et al. [109], where all the publicly available morphing tools (both open-source and commercial) are listed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

TABLE I: Face Morphing Generation Methods: Advantages and Limitations

Face Morph Generation Method	Advantages	Limitations
Facial Landmark-based	- Availability of open-source tools. - Generates high quality morphing images. - Successfully deceives the COTS FRS. - Easy and seamless generation of morphed images by an automatic process.	- Requires manual intervention to ensure high-quality face morphing generation. - Needs post-processing to reduce ghosting effects and double edges. - Data subject selection is crucial to deceive the COTS FRS.
Deep Learning-based	- No need for manual intervention. - Seamless generation with acceptable image quality. - Does not show double edges in the generated images. - Reasonably successful in deceiving the COTS FRS. - Several open-source tools.	- Requires a complex learning procedure. - Does not always generate high-quality morphed images. - Highly prone to geometric distortions. - Requires careful pre-selection of data subjects based on age, gender and ethnicity.

B. Deep Learning-based Morph Generation

Recent improvements in deep learning-based techniques have given rise to morph generation approaches based on generative adversarial networks (GANs) [41] [125]. In general, GAN-based methods synthesise morphed images that are generated by sampling two facial images in the latent space of the deep learning network. The MorGAN architecture for morph generation basically employs a generator that consists of encoders, decoders and a discriminator. The generator is trained to generate images with dimensions of 64×64 pixels. Another recent approach based on StyleGAN architecture [24], [125] has improved the morph generation process both by increasing the spatial size to 1024×1024 and by increasing face quality. The pre-trained StyleGAN achieves this by embedding the images in the intermediate latent space. The use of identity priors to enable high-quality morphed face generation was also proposed in [131] and illustrates the increased threat to FRSs by GAN-based morphs. Figure 4 provides sample facial morphs generated using the landmark-based technique and MorGAN- and StyleGAN-based methods. It can be noted from Figure 4 that deep learning-based approaches, especially with MIPGAN-I and MIPGAN-II, indicate a superior quality of the morphed face image compared to that of landmark-based morphed face generation.

IV. Databases for Morphing Attack Detection

Given various kinds of attack generation mechanisms and the relevant attack potential determination metrics, many datasets have been generated, ranging from public to sequestered datasets with various attack strengths. This section summarises the different face morph databases that are used in existing works. A summary of the different datasets is provided in Table II from existing works that are typically used to benchmark both the vulnerability of FRSs and the performance of MAD techniques.

The first face morph database was introduced by Ferrara et al. [48], in which the authors employed landmark-based face morph generation using GIMP/GAP tools. This dataset has a small set of digital images consisting of only 14 morphed images generated from 8 bona fide subjects, including both male and female participants. The morphed images in this database are only in digital format and the database is not available publicly. This dataset was extended by Ferrara et al. [49] using the landmarks and GIMP/GAP tools. The extended dataset consists of approximately 80 morphed face images, with 10 male and 9 female participants. The database is in digital form and is not publicly available.

The first large database with different ethnicities (Caucasian, Asian, European, American, Latin American, and Middle Eastern) was introduced by Raghavendra et al. [92] and employs facial landmarks and the GIMP/GAP morph generation technique using the GNU image manipulation tool. This database consists of 450 morphed face images generated using 110 subjects of different ethnic backgrounds. This database contains only digital images and has not been made public.

Makrushin et al. [73] employed automatic morph generation tools to generate high-quality morph images. They employed a triangulation method based on 68 facial landmarks extracted using the dlib library [15]. Two different morph generation techniques, namely, complete morph (consisting of the facial geometry of both facial images) and splicing morph (the pixels representing the face are clipped out from the input faces), were used. A splicing morph is generated to address the pixel discontinuity caused by warping two images in complete morphs. This database consists of approximately 1326 complete morphs and 2614 splicing morphs generated from 52 data subjects consisting of 17 females and 35 males. This database consists of face morph images in digital format only and has not been made public.

The first print-scan face morph database was presented by Scherhag et al. [106]. The authors employed the landmark-based GIMP/GAP technique for morph generation. This database consists of 231 morphed images generated from 462 bona fide images. This database is private and contains

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

TABLE II: Public and Private Face Morph Image Databases

Reference	Morph Generation Type	Morph Generation Method	Digital/Print-scan	Bona fide & Morph	Public/Private
Ferrara et al [48]	Landmark-based	GIMP/GAP	Digital	Morph: 14	Private
Ferrara et al [49]	Landmark-based	GIMP/GAP	Digital	Morph: 80	Private
Raghavendra et al [92]	Landmark-based	GIMP/GAP	Digital	Morph: 450	Private
Makrushin et al [73]	Landmark-based	Automatic generation (dlib landmark)	Digital	Complete morph: 1326, Splicing morph: 2614	Private
Scherhag et al [106]	Landmark-based	GIMP/GAP	Digital and Print-scan	Bona fide: 462 Morph: 231	Private
Raghavendra et al [91]	Landmark-based	GIMP/GAP	Digital and Print-scan	Bona fide: 1000 Morph: 1423+1423	Private
Raghavendra et al [93]	Landmark-based	GIMP/GAP	Digital and Print-scan	Morph: 362	Private
Gomez-Barrero et al [55]	-	-	Digital	Morph: 840	Private
Dunstone [12]	-	-	Digital	Morph: 1082	Public
Ferrara et al [50]	Landmark-based	Sqirlz morph	Digital and Print-scan	Morph: 100	Private
Damer et al [41]	GAN-based	GAN	Digital	Morph: 1000	Private
Raghavendra et al [94]	Landmark-based	GIMP/GAP	Digital and Print-scan	Bona fide: 1272 Morph: 2518	Private
Scherhag et al [104]	Landmark-based	OpenCV, FaceFusion, Face Morpher	Digital and Print-scan	Bona fide: 984+984+529 Morph: 964+964+529	Private
Ferrara et al [51]	Landmark-based	Triangulation	Digital	Morph: 560	Private
Scherhag et al [110]	Landmark-based	OpenCV, FaceFusion, Face Morpher, UBO morpher	Digital and Print-scan	Bona fide: 791+3298 Morph: 791+3246	Private
Singh et al [116]	Landmark-based	OpenCV	Digital and Print-scan	Morph: 588	Private
Venkatesh et al [124]	Landmark-based	UBO morpher	Digital	Morph: 10538+3767	Private
Venkatesh et al [125]	GAN-based	StyleGAN	Digital	Bona fide: 1270 Morph: 2500	Private
Raja et al [96]	Landmark-based	UBO morpher	Digital and Print-scan	Bona fide: 300+1096 Morph: 2045+3073	Sequestered
NIST-FRVT-MORPH et al [76]	Landmark-based	Automatic generation	Digital and Print-scan	Low-quality morph: 1183 Automated morph: 39113 High-quality morph: 492	Sequestered

digital and print-scan (or re-digitised) images, for which HP Photosmart 5520 and Ricoh MPC 6003 SP printers were employed.

Raghavendra et al. [91] later introduced a new face morph dataset consisting of both digital and print-scan images. The face morphs were generated using an automatic tool, OpenCV, that is publicly available. This database generates morphed face images along with averaged face images and hence has a set of $1423 + 1423$ morphed face images. Along with the database, Raghavendra et al. [91] provided an evaluation protocol by defining independent sets for development, training and testing partitioning. The print-scan morphed face images were obtained by employing a Ricoh MPC 6003 SP printer. This database is private. This dataset was extended to 2518 morphed face images and 1273 bona fide images [94].

Gomez et al. [55] introduced a new face morph dataset that consists of 840 morphed face images generated from 210 subjects. This database is private and has only digital morphed face images.

Ferrara et al. [50], [52] introduced a face morph database based on the Sqirlz morphing technique. This dataset has 100 morphed images in both digital and print-scan forms. This database has not been made public for research purposes. Scherhag et al. [104] introduced a face morphing dataset that was generated using different morphing tools, such as OpenCV, FaceFusion and FaceMorpher. This is a private database that consists of both digital and print-scan samples of morphed images and is composed of $964 + 964 + 529$ morphed face images generated from subjects contained in the FRGCv2 and FERET databases. Another database by Scherhag et al. [110] employs landmark-based morph generation techniques that include OpenCV, FaceMorphed, FaceFusion and the UBO morphing method. This database consists of approximately 791+3246 morphed face images from the FERET and FRGCv2 databases. This private database consists of morphed face images in both digital and print-scan formats. Another database by Ferrara et al. [51] employs triangulation with the dlib landmark method of morph generation. This is a private database that consists of 560 digital morphed face images. The only publicly available morphed face dataset was introduced by Biometix [12], which consists of 1082 morphed face images in digital form. However, information on the morphed image

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

generation method involved is not available.

Singh et al [116] provided another database that employs the OpenCV-based morph generation technique to generate facial morphs. This was the first dataset introduced for probe images captured live from ABC gates with different lighting conditions, which is relevant for differential morphing attack detection. This database consists of both digital and print-scan enrolment images generated using an EPSON XP-860 printer and scanner. This dataset consists of 90 morphed face images and is not available to the public.

Damer et al. [41] introduced the first face morphing database consisting of deep learning-based morph images. The generated deep learning-based database is compared with landmark-based morphs. The authors employed 68 landmark points extracted from dlib for landmark-based morph generation and GAN architecture for deep learning-based morph generation. This database consists of 1000 morphed face images; however, the GAN-based morphs are of size 64×64, which does not meet ICAO standards. This database is private and has only digital morphed face data. Another database by Venkatesh et al. [125] employs deep learning-based morph generation. The authors employed the StyleGAN network to generate synthetic morph images by mapping the input images into the latent space. This database consists of 2500 morphed images generated using 1270 bona fide images. It has only digital morphed face images and is not publicly available.

Venkatesh et al. [124] introduced another database that consists of morphed face images under ageing as the first database of its kind. The authors employed the UBO morphing method from the University of Bologna that employs dlib and 68 landmark points for morph generation [51]. This database consists of 14305 (10538+3767) morphed face images aged by 2 to 5 years. This database has morphed face images in digital form and is not open to the public.

Raja et al. [96] presented the sequestered Bologna-SOTAMD face morphing dataset used in a recent public competition and benchmarking on the Bologna Online Evaluation Platform (BOEP), following the FVC-onGoing series [1]. The dataset comprises images from 150 data subjects collected in three different geographic locations with varying ethnicity, gender and age. Face morphing is carried out using six different techniques followed by automatic and manual post-processing to override the artefact results from face morphing. The dataset also includes printed and scanned versions with different printers, and the enrolment images follow the ICAO standards for passport images. The probe images are taken from various ABC gates and gate emulations. The database consists of 5,748 morphed face images and 1,396 bona fide face images.

A. Discussion

Although there exist several morphing datasets, the majority of them are private due to data protection regulations and licensing conditions. Even for publicly available face databases that are used to create face morphing datasets, the licensing conditions limit the redistribution of the generated morphed face datasets; therefore, most of the above datasets are not openly available. For the time being, the best way to compare new morphing detection methods with already published approaches is to submit the methods to the two ongoing benchmarks, either the SOTAMD benchmark at the university of Bologna, which was reported by Raja et al. [96], or the U.S. NIST-FRVT-MORPH benchmark, which was reported by Ngan et al. [76]. Note that in both cases, a sequestered dataset is used.

V. Human Perception and Morphed Face Detection

The threat of morphing attacks is known for border crossing and ID management scenarios. Therefore, the success of a morphing attack depends on deceiving human observers, particularly ID experts and border guards. A practical scenario for a border crossing includes border guards, who compare the passport of a traveller containing a photograph (printed from a data page or digitally extracted from a chip) with the physical appearance of the traveller. Thus, the border guard considers the facial similarity of the traveller to the reference data in the passport to make his/her final decision. Several studies in the literature have indicated the effectiveness of morphed images in deceiving expert human observers [49], [60], [65], [73]–[75], [98], [99], [127]. Early investigations on human perception analysis of morphed images were reported by Jäger et al. [60], where different experiments were performed to benchmark the ability of human observers to detect face morphing and its dependency on various parameters (i.e., different alpha/morphing factors). While this was an interesting study, the human observers in the experiments were students who were not trained to compare human faces. Furthermore, this work was based on only a single image and did not provide any reference images for the human observers. A similar analysis was provided by Kramer et al. [65], where a single image was provided before requesting a decision on morphing. Despite being different in terms of the underlying benchmarking mechanism, both works reported difficulty in detecting morphed face images for human observers.

Investigating the impact of morphing on FRSs and human observers simultaneously, Ferrara et al. [48] studied the detection ability of human observers and correlated it with automatic FRSs. Unlike the previous work, the human observers in the work of Ferrara et al. [48] included both trained border guards and non-specialists who were asked to compare a morphed face image with a bona fide face image to make the decision. The analysis reported a challenge in detecting morphs even when the examiner, for instance, a border guard, was trained. Robertson et al. [98] further studied the morph detection ability of humans by comparing live face images to morphed face images with and without rudimentary training. The study reported improved performance in morph detection by human observers when provided with rudimentary training in detecting artefacts [99]. Similarly, Kramer et al. [65] investigated the role of face image quality (of the morphed image produced) on human perception and concluded that high-quality morphed images are more difficult for humans to detect.

A similar web-based experiment simulating border control was presented by Makrushin et al. [74], who studied human

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

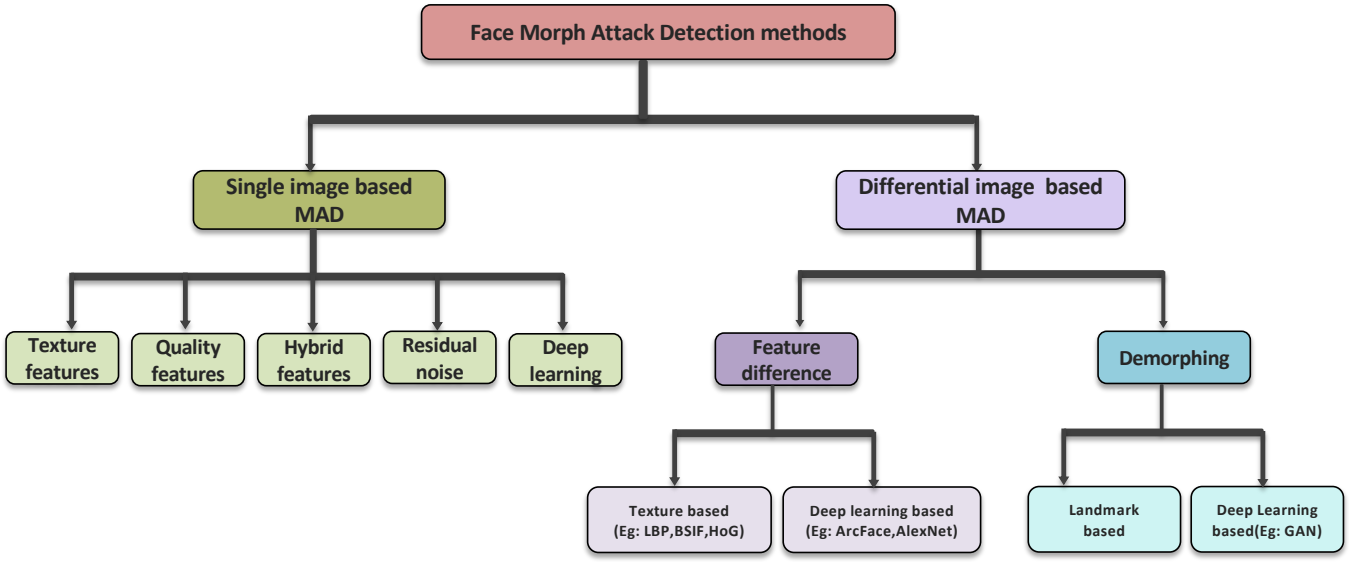

Fig. 5: Taxonomy of morph attack detection techniques

perception analysis by both skilled and unskilled humans and further extended [75] to obtain more unbiased and realistic images. In both cases, skilled humans (who have knowledge of morphed face images) show the best performance in detecting a morphed face image. Summarising the works on human perception analysis, it is noted that both skilled and unskilled human observers often fail to detect morphed face images. However, it is also noted that considerable training of human observers can improve morphed face detection [75], [99].

VI. Face Morph Attack Detection Techniques

Noting the limitations of human observers, a number of automatic MAD approaches have been proposed in the recent past. In this section, we summarise the MAD techniques since the introduction of face morphing attacks on FRSs [48]. The available MAD techniques can be classified into two major types: (a) single image-based MAD (S-MAD) and (b) differential image-based MAD (D-MAD). Figure 5 shows the taxonomy of approaches in both MAD categories reported to date.

A. Single Image-based MAD (S-MAD)

The goal of S-MAD is to effectively detect a face morphing attack based on a single image presented to the algorithm. Figure 6 illustrates a real-life example for S-MAD in a passport application scenario, where a facial image is submitted by the applicant for biometric enrolment in the passport application process. This submitted image is checked to potentially detect a morph of a suspect image. The passport application can be initiated by the applicant either physically or when submitting his/her facial image through a web service [3], [5], [7], [21]. Thus, depending on the use case, the morphed image can be one of two types: (a) digital or (b) re-digitised (also commonly referred to as print-scan). S-MAD is challenging, as it is expected to be robust to image quality variations, different types of sensors (cameras), different types of morph generation tools and different types of print-scan processes (e.g., the equipment and parameter set chosen for the printing and scanning process).

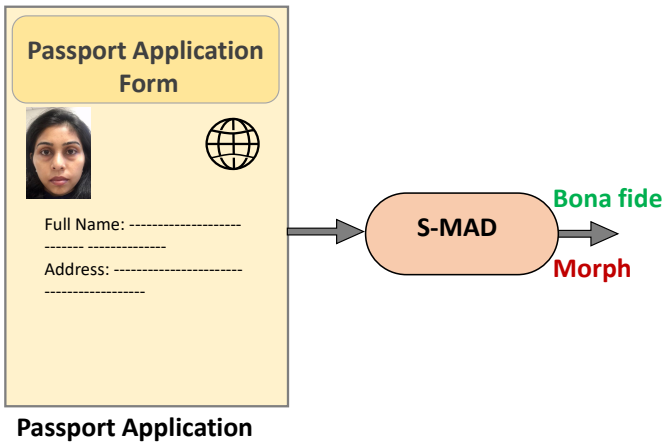

Fig. 6: An example illustrating single image-based morph attack detection in a passport application scenario.

As shown in Figure 5, the existing S-MAD techniques can be further classified into five subtypes based on the features employed: (a) texture feature-based S-MAD, (b) quality-based S-MAD, (c) residual noise-based S-MAD, (d) deep learning-based S-MAD, and (e) hybrid approaches for S-MAD. Table III summarises the existing S-MAD techniques. In the next section, we briefly discuss the existing S-MAD techniques for the convenience of the reader.

a) Texture Feature-based S-MAD: The first work on using texture features was presented by Raghavendra et al.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

TABLE III: State-of-the-art S-MAD

Reference	Detection Type	Approach	Algorithm	Database
Raghavendra et al. [92]	S-MAD	Texture-based approach	Local Binary Pattern (LBP)-SVM, Binary Statistical Image Features (BSIF)-SVM, Image Gradient (IG)-SVM	Digital
Makrushin et al. [73]	S-MAD	Quantised DCT co-efficients	Benford features	Digital
Neubert et al. [77]	S-MAD	Image degradation approach	Corner feature detector	Digital
Seibold et al. [113]	S-MAD	Deep learning-based approach	VGG19, Google Net, Alex Net	Digital
Raghavendra et al. [91]	S-MAD	Texture-based approach	LBP, LPQ, BSIF, colour textures	Print-scan
Asaad et al. [28]	S-MAD	Texture-based approach	Topological data analysis approach	Digital
Scherhag et al. [106]	S-MAD	Texture- and frequency-based approach	LBP, LPQ, BSIF, 2DFFT with SVM classifier	Digital Print-scan
Kraetzer et al. [**?**]	S-MAD	Texture-based approach	Media forensics	Digital
Raghavendra et al. [93]	S-MAD	Deep CNN-based approach	Feature fusion of fully connected layers of VGG19 and Alex Net	Digital Print-scan
Kraetzer et al. [64]	S-MAD	Image life cycle model	Keypoints (SIFT, SURF, ORB, FAST, AGAST) and loss of edge operators (Canny and Sobel)	Digital
Hildebrandt et al. [57] [80]	S-MAD	StirTrace-based approach	Multi-compression anomaly detection	Digital
Debiasi et al. [45]	S-MAD	Image degradation	Photo Response Non-uniformity (PRNU)	Digital
Raghavendra et al. [94]	S-MAD	Steerable features	Luminance component extraction	Print-scan
Hildebrandt et al. [56]	S-MAD	StirTrace	StirTrace face morph forgery detection	Print-scan
Seibold et al. [111]	S-MAD	Image degradation	Specular reflection	Digital
Makrushin et al. [72]	S-MAD	Quantised DCT co-efficients	Benford features extracted from quantised DCT co-efficients	Digital
Neubert et al. [79]	S-MAD	Morph pipeline footprint detector	Benford features extracted from quantised DCT co-efficients	Digital
Spreeuwers et al. [119]	S-MAD	Texture-based approach	LBP-SVM, Down-up sampling	Digital
Scherhag et al. [108]	S-MAD D-MAD	Feature difference-based approach	Pre-processing and feature extraction using texture descriptors , keypoint extractors, gradient estimators and deep learning-based method	Digital
N Damer et al. [43]	S-MAD	Multi-detector fusion	LBPH, Transferable deep-CNN	Digital
Ferrara et al. [52]	S-MAD	Deep learning	AlexNet, VGG19, VGG-Face16, VGG-Face2	Print-scan
Scherhag et al. [107]	S-MAD	Multi-algorithm fusion	Texture descriptors (LBP, BSIF), Keypoint extractors (SIFT, SURF), gradient estimators (HoG), Deep neural network	Digital
Debiasi et al [44]	S-MAD	PRNU	PRNU DFT magnitude histogram and PRNU DFT energy	Digital
Seibold et al. [114]	S-MAD	Complex multi-class pre-training	VGG-19 network	Digital
Damer et al. [40]	S-MAD	Texture and deep learning based	Anomaly detection using LPQ and VGG features	Digital
Venkatesh et al. [123]	S-MAD	Colour denoising-based approach	Denoising Deep Convolutional Neural Network	Digital
Scherhag et al. [104]	S-MAD	PRNU	Spectral features and spatial features	Print-scan
Makrushin et al. [71]	S-MAD	Dempster-Shafer Theory	KeyPoints (SIFT, SUFT, FAST, ORB, AGAST, High Dim LBP, GoogleNet, VGG19	Digital
Raghavendra et al. [95]	S-MAD	Scale space approach	Colour scale space features	Print-scan
Neubert et al. [78]	S-MAD	Frequency and spatial domain feature space approach	Discrete Feature Transformation (DFT) , SURF, SIFT, ORB, FAST, AGAST, Canny edge, SobelX, SobelY)	Digital
Seibold et al. [112]	S-MAD	Style Transfer-based approach	LBP, BSIF, Image degradation, Deep neural network (VGG19)	Digital
Venkatesh et al. [122]	S-MAD	Colour denoising-based approach	Context Aggregation Network	Digital
Venkatesh et al. [121]	S-MAD	Ensemble-of-features-based approach	LBP, HoG, BSIF	Print-scan

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

[92]. Following the initial work, several approaches were proposed, as indicated in Table III. The popular texture-based methods include local binary patterns (LBPs) [83], local phase quantisation (LPQ) features [84] and binarised statistical image features (BSIFs) [63]. Furthermore, these texture features were extracted for different colour channels [91] to obtain a robust detection performance. Variants of LBPs and BSIFs as well as histogram of oriented gradients (HOG) features, scale-invariant features (SIFT) [69] and speed-up robust features (SURF) [**?**], [30], [71], [106], [107] have also been widely explored in the reported works. The use of micro-texture-based methods has shown reasonable performance on both digital and print-scan types of S-MAD. While superior accuracy has been reported for digital S-MAD with texture-based features, the main limitation of these techniques is in their generalisability across different image qualities, imaging sensors and print-scan processes [96].

b) Quality-based S-MAD: The quality-based techniques largely analyse image quality features by quantifying the image degradation to identify a given image as morphed or bona fide [45], [56], [57], [104], [111]. Several features, such as double-compression artifacts, photo response non-uniformity (PRNU), corner and edge distortions, reflection analysis and meta information in the images, are commonly used to detect distortion in a morphed image. Although these techniques have shown good performance on digital data, they have limited performance on print-scan data. However, the generalisation ability of these techniques has yet to be studied for different print and scan versions in the current literature [96], [104].

c) Residual Noise-based S-MAD: Residual noise-based methods are designed to analyse pixel discontinuities that may be greatly impacted by the morphing process. The basic idea of this approach is to extract noise patterns by subtracting the given image from the denoised version of the same image. The noise patterns obtained are further analysed to detect morphing. The first work in this area was introduced in [123] based on CNN-based denoising on colour channels. Furthermore, the residual noise is effectively captured using the deep CNN approach [122]. The use of residual noise has shown considerably good performance in terms of generalisation capabilities across different digital datasets. However, these techniques have not been evaluated on print-scan face morphed datasets.

d) Deep Learning-based S-MAD: The success of deep learning approaches for image classification tasks has motivated researchers to embrace deep convolutional neural networks (CNNs) for face MAD. All existing works are based on pre-trained networks and transfer learning. The first work in this direction was based on using pre-trained networks such as AlexNet and VGG18, in which the features are fused and classified to detect a morphing attack [93]. Following this, several deep CNN pre-trained networks, such as AlexNet, VGG19, VGG-Face16, GoogleNet, ResNet18, ResNet150, ResNet50, VGG-Face2 and OpenFace [52], [43], [122], [112], [107], [108], [113], [71], [112], have been explored. Although deep CNNs have shown better performance than hand-crafted texture descriptor-based MAD methods on both digital and print-scan data, the generalisation capability of these approaches is limited across different print and scan datasets [110].

e) Hybrid S-MAD: Hybrid approaches are based on multiple feature extractors or classifiers that are combined to detect face morphing attacks. Several approaches have been proposed that combine features, morphing detection scores or decision scores [121], [43], [71], [107], [94], [95]. As these approaches combine more than one feature extractor and classifier, the MAD performance is generally superior to that of single-mode MAD techniques. Despite the superior performance, the computational cost is high, and generalisation of the approach is not well established with respect to different types of print-scan processes.

A summary of advantages and limitations is given in Table IV for all types of S-MAD techniques for reference.

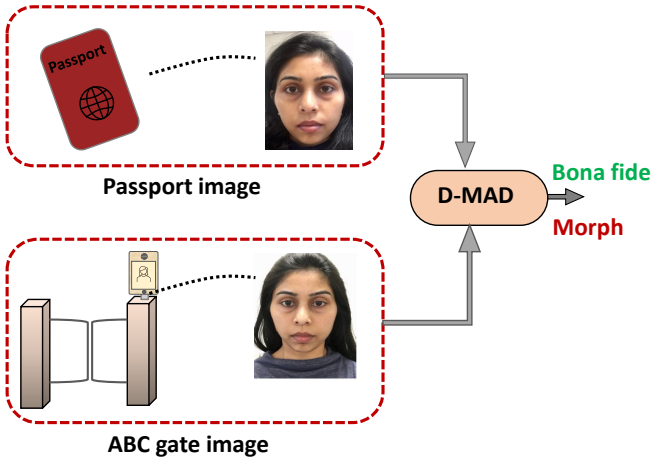

Fig. 7: Example illustrating differential image-based morphing attack detection (D-MAD) in a passport control scenario

B. Differential Image-based MAD (D-MAD)

The objective of D-MAD approaches is to make a decision regarding whether a suspect image is morphed or bona fide when a corresponding image captured in a trusted environment is available. The D-MAD technique is well suited to the border crossing scenario, where the suspected morph image can be obtained from the passport and can then be compared against the live captured face image (or trusted image) from the ABC gates [85]. Figure 7 illustrates the application of D-MAD, specifically in a border control scenario. A taxonomy of D-MAD techniques is presented in Figure 5, and they can be divided into two broad types: (a) feature difference-based D-MAD and (b) demorphing. Table V summarises the existing D-MAD techniques, which are briefly discussed below.

a) Feature Difference-based D-MAD: The basic idea of this approach is to subtract the features computed on both the suspected morph image and a live image captured in a trusted environment. The features are further classified by computing the difference in the feature vectors to detect a morphing attack. To this end, several feature extraction techniques are studied,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

TABLE IV: S-MAD Techniques: Advantages and Limitations

Feature Type	Advantages	Limitations
Texture Features	- Easy to implement. - Low computational cost. - Good performance when trained and tested with the same morph data types (digital/print-scan). - Effective on digital morph face data	- Lacks generalisation capabilities across both image resolution and morph data type (digital/print-scan). - Sensitive to image resolution. - Degraded performance with print-scan data.
Image Quality Features	- Easy to implement. - Low computational cost. - Less sensitive to accurate segmentation of the face region. - Can be used with different morph data types (digital/print-scan).	- Lacks generalisation across both image resolution and morph data types (digital/print-scan). - Sensitive to compressed data. - Not a reasonable performance across different face morph data types (digital/print-scan).
Hybrid Features	- Good detection performance across different morph data types (digital/print-scan). - Good detection performance when trained and tested with the same morph data type (digital/print-scan). - Reasonable generalisability performance for different morph data types (digital/print-scan).	- Difficult to implement, as it requires hyper-parameter tuning. - High computational cost. - Requires optimisation of several hyper-parameters.
Residual Noise Features	- Easy to implement. - Low computational cost. - Highly accurate detection performance on digital morph data type. - Less sensitive to face region. - Generalisation ability across different image resolutions.	- Applicable only to the digital morph data type. - Promising results for high-resolution images. - Sensitive to image compression.
Deep CNN features	- Good performance when trained and tested with the same morph data type (digital/print-scan). - No need to train CNN from scratch, as deep CNN shows good detection performance.	- High computational cost. - Lacks generalisation across different face morph data types (digital/print-scan). - Training CNN from scratch requires large database.

which involve texture information, 3D information, gradient information, landmark points and deep feature information [110], [116], [43], [103], [39]. Based on the reported results, the deep CNN features have shown the best performance [110]. The majority of the existing works are reported for use cases with digital images, except for a recent work in which a print and scan dataset was explored with improved results [81], [110].

b) Demorphing: Face demorphing techniques invert the morphing procedure and reveal the component images that are used to generate the morphed image. The first proposal in this area was that of Ferrara et al. [50], which was designed to work with landmark-based morph generation. Recent work along these lines is based on using deep CNNs [85] [88]. These techniques are robust when the image quality is good; however, the detection performance degrades when a face image is captured in real-life conditions with pose and lighting variations that are commonly encountered in ABC gates. Table VI presents the advantages and limitations of existing D-MAD techniques.

VII. Performance Metrics

In this section, we discuss the performance evaluation metrics that are widely used in the literature and publicly available competitions to benchmark the performance of MAD techniques.

A. Vulnerability Assessment of FRSs

For a morphed image to be deemed a significant threat to an FRS, it is necessary to establish the threat potential. Most works determine the threat potential by measuring the vulnerability of FRSs. We therefore provide a brief overview of suitable metrics for establishing the relevance of morph attacks through vulnerability metrics. The goal of face vulnerability analysis is to measure whether the generated morphed face image can be verified against all contributory data subjects. Thus, when a morphed face image is enrolled into an FRS and probed with another image from a contributing subject, the FRS must successfully verify all contributory subjects corresponding to the pre-set verification threshold. In most works, the threshold

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

TABLE V: State-of-the-art D-MAD

Reference	Detection Type	Approach	Algorithm	Database
M Ferrara et al. [50]	D-MAD	Demorphing	Demorphing by image subtraction	Print-scan
M Ferrara et al. [50]	D-MAD	Demorphing approach	Face verification	Digital
U Scherhag et al. [103]	D-MAD	Landmark-based approach	Distance-based and angle-based feature extraction with Random Forest, SVM without kernel and SVM with radial basis function classifier	Digital
U Scherhag et al. [108]	S-MAD + D-MAD	Feature difference-based approach	Pre-processing and feature extraction using texture descriptors, keypoint extractors, gradient estimators and deep learning-based method	Digital
N Damer et al. [43]	D-MAD	Multi-detector fusion	LBPH, Transferable deep-CNN	Digital
J M Singh [116]	D-MAD	Deep learning	SfS Net, AlexNet	Digital + Print-scan
N Damer et al. [39]	D-MAD	Landmark shift	Landmark detection, shift representation	Digital
F Peng et al. [88]	D-MAD	Face restoration by demorphing GAN	Symmetric dual-network architecture	Digital
U Scherhag et al. [110]	D-MAD	Deep Face Representation	ArcFace Network, FaceNet algorithm	Digital + Print-scan
C Seibold et al. [115]	D-MAD	Deep Learning	Layer-wise Relevance Propagation (LRP)	Digital
D Ortego et al. [85]	D-MAD	Demorphing, Deep CNN-based	Auto-encoders	Digital + Print-scan
S Soleymani et al. [117]	D-MAD	Deep learning	Siamese network	Digital
S Soleymani et al. [118]	D-MAD	Deep learning	Appearance and landmark disentanglement	Digital
S Autherith et al. [29]	D-MAD	Analysis of geometric facial features	Facial anthropometry-based facial feature comparison	Digital

TABLE VI: D-MAD Techniques: Advantages and Limitations

Algorithm Type	Advantages	Limitations
Feature difference	- Easy to implement. - Reasonable detection performance across varying image quality and resolution.	- High computational cost. - Detection performance is sensitive to the type of image data and features. - Detection performance is sensitive to the segmentation of the face region.
Demorphing	- Easy to implement. - Moderate computational time. - High detection accuracy with constrained conditions. - Can visualise the demorphed face if the suspect image is morphed	- Performance is sensitive to the facial pose and imaging conditions. - Requires constrained image data. - Fails with facial pose and lighting variations. - Prior knowledge of the blending factor (or alpha factor) is required.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

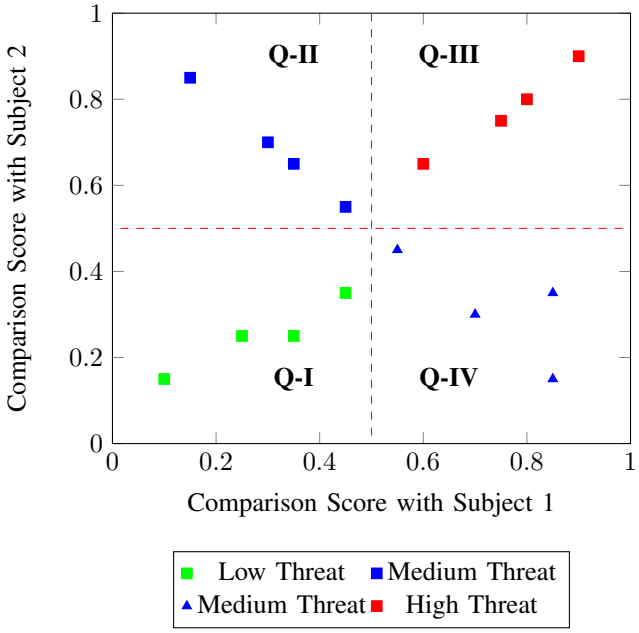

Fig. 8: Threats of morphed images with respect to comparison scores against both contributing subjects. The figure illustrates that morphed images crossing the threshold of 0.5 (i.e., those lying in quadrant Q-III) are effective attacks with a more severe threat to the FRS than those in Q-II and Q-IV.

of the FRS is adjusted to correspond to a false match rate (FMR) of 0.1% following the guidelines of FRONTEX [53].

Figure 8 illustrates an example of the vulnerability plots that represent the scattered data of comparison scores from FRSs. The sample vulnerability plot is simplified for visualisation purposes to provide an illustration of the vulnerability analysis. Figure 8 can be interpreted using four different quadrants. The first quadrant (bottom left quadrant) $Q-I$ indicates that the morphed image is not verified as belonging to either of the two contributing data subjects. Thus, a large number of comparison scores in the first quadrant indicates that the morph generation method is not strong enough to deceive the COTS FRS (in other words, the morphed image is not a severe threat). The second quadrant (top left quadrant) $Q-II$ indicates that the morphed image can be verified as data subject-2 (one of the contributing subjects) only. Therefore the morphed images pose an intermediate-strength threat. The third quadrant (top right quadrant) $Q-III$ indicates that the morphed image is verified as both contributing data subjects (subject-1 and subject-2). Thus, the larger the number of comparison scores in this quadrant, the greater the threat and vulnerability of the analysed FRS with respect to morphed images. The fourth quadrant (bottom right quadrant) $Q-IV$ indicates that the morphed image can be verified as data subject-1 only. Therefore, the morphed images again pose an intermediate-strength threat to the FRS.

To mathematically quantify the vulnerability of an FRS to morphed face images, the metrics below have been developed and adapted in the literature.

*a) **Mated Morph Presentation Match Rate (MMPMR)**:* This metric was initially proposed by Scherhag et al. in [105]. It defines the proportion of morphed images verified with its contributing images.

$$MMPMR = \frac{1}{M}\sum_{m=1}^{M}[min_{n=1\ldots N_m} S_m^n] > \tau \qquad (1)$$

where M is the number of morphed images and N_m is the total number of subjects contributing to morph m. S_m^n is the comparison score for mated morph for morph m of the n^{th} subject, and τ is the threshold of the FRS at a chosen False Match Rate (FMR).

The rationale of MMPMR is that a morphing attack succeeds if all contributing subjects are verified successfully against the morphed image. MMPMR considers multiple comparisons, which are related to multiple authentication attempts. This may not always be the case. A successor of the MMPMR metric named the fully matched morph presentation match rate (FMMPMR) was introduced by Venkatesh et al. [124] to address the quadrants employed for vulnerability assessment, as shown in Figure 8. The details of the FMMPMR are provided below.

*b) **Fully Mated Morph Presentation Match Rate (FMMPMR)**:* This metric defines the proportion of morphed images verified with their contributing subjects again under the condition that the morphed image is verified successfully against both contributing subjects [124]. This metric further takes into account both pairwise comparisons of contributing subjects and the number of attempts compared to MMPMR and is described as follows:

$$FMMPMR = \frac{1}{P}\sum_{M,P}(S1_M^P > \tau) AND (S2_M^P > \tau) \ldots AND (Sk_M^P > \tau) \qquad (2)$$

where $P = 1, 2, \ldots, p$ represents the number of attempts made by comparing all probe images from the contributing subject against the M^{th} morphed image, $K = 1, 2, \ldots, k$ represents the number of data subjects contributing to the constitution of the generated morphed image (in our case, $K = 2$), Sk_M^P represents the comparison score of the K^{th} contributing subject obtained in the P^{th} attempt (in this case, the P^{th} probe image from the dataset) corresponding to the M^{th} morph image and τ represents the threshold value corresponding to FMR = 0.1%. The FMMPMR metric verifies the morphed image with its contributing subjects and takes into account the number of attempts. It is therefore a relevant and realistic metric to quantify the vulnerability and establish the true attack strength of a morph generation method.

*c) **Joint Evaluation of an FRS and Vulnerability to Morph Attacks**:* In addition to Figure 8, we note that the FRS can have a high recognition accuracy (i.e., biometric performance) but can also have a high vulnerability to morphing attacks. It is therefore essential to first evaluate the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

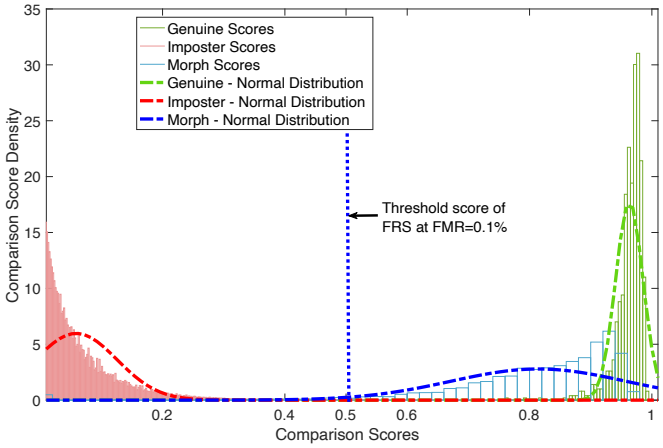

Fig. 9: Illustration of morph attacks in conjunction with the strength of the FRS. As noted from the figure, the genuine and impostor distributions of the comparison scores are clearly separated, indicating the strength of the FRS while indicating the vulnerability to morph attacks, as most of them cross the pre-defined threshold of 0.5 at a chosen $FMR = 0.1\%$.

biometric performance of the FRS according to international standard ISO/IEC 19795-1 [58] and subsequently evaluate its vulnerability by using the pre-set threshold (e.g., FMR = 0.1%). We illustrate a chosen COTS FRS in Figure 9, where one can see the success of the morphing attack for a selected threshold (τ) of 0.5, corresponding to $FMR = 0.1\%$. We conclude that the real strength of an FRS cannot be established unless good recognition performance and robustness with respect to morphing attacks are analysed and reported. For this reason, Scherhag et al. [105] established a relative measure that combines the recognition accuracy with vulnerability measures, and this metric is referred to as the relative morph match rate ($RMMR(\%)$). Specifically, when τ is employed to obtain either the MMPMR or FMMPMR, as discussed earlier, the RMMR can be defined as follows [105]:

$$RMMR(\tau)_{MMPMR} = 1 + (MMPMR(\tau)) - [1 - FNMR(\tau)] \quad (3)$$

$$RMMR(\tau)_{FMMPMR} = 1 + (FMMPMR(\tau)) - [1 - FNMR(\tau)] \quad (4)$$

where $FNMR$ indicates the false rejection rate ($FNMR$) of the FRS under consideration obtained at the threshold τ.

B. MAD Performance Metrics

The robustness of MAD algorithms is measured using the performance metrics defined in the International Standard ISO/IEC 30107-3 [59] and is applicable to reporting the morphing attack detection performance. Since the MAD performance can be visualised as a binary classification problem, the following metrics are widely used to benchmark MAD algorithms:

- **Attack presentation classification error rate (APCER):** Defines the proportion of attack samples incorrectly classified as bona fide face images.
- **Bona fide presentation classification error rate (BPCER):** Defines the proportion of bona fide images incorrectly classified as attack samples.

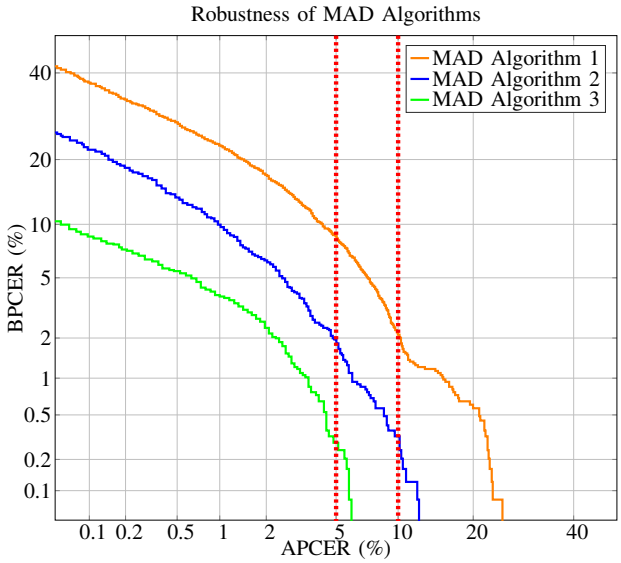

Fig. 10: Sample illustration of the detection accuracy of MAD algorithms at different operating points with a detection error trade-off curve (DET). As noted from the figure, MAD Algorithm 3 performs best at a chosen APCER of 5% or 10%.

However, it is not possible to optimise both the APCER and BPCER jointly; it is thus natural to set (or fix) either the BPCER or APCER and report the result with a dependency of the other metric (either the APCER or BPCER). Most works have reported results by setting a pre-defined security level (e.g., indicating the maximum proportion of morph accepts they can tolerate) and then fixing the APCER accordingly at values of @1%, 5% or 10% [81], [93], [96]. As shown in Figure 10, MAD Algorithm 3 would be preferred at a given APCER of 5% or 10% in the benchmark compared with the other two algorithms.

C. Joint Evaluation of MAD Algorithms and Vulnerability

In a real-life scenario, an FRS may operate with a MAD sub-system in integrated processing. For a successful attack, it is therefore important that the morphed face image can invade the enrolment process and can match to probe images from the contributing subjects. To quantify the vulnerability in the presence of a MAD, a metric called the Actual mated Morph Presentation Match Rate (AMPMR) was recently proposed in [89] and can be written as follows:

$$AMPMR(th_{fa}, th_{mad}) = \frac{1}{N}\sum_{i=1}^{N}(((\min_{j=1,..Mi} SC_{ij}) > th_{fa}) AND (SC_{mad-i} > th_{mad})) \quad (5)$$

where the total number of morphed images is denoted by N. SC_{ij} is the face recognition score of the i^{th} morphed image when compared to a probe sample of the j^{th} contributor.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

Mi is the number of contributors to the morphed image. SC_{mad-i} is the MAD score of the i^{th} sample. Based on these metrics, higher values of the AMPMR indicate more severe vulnerability.

VIII. Public Evaluation and Benchmarking

In this section, we summarise evaluations that publicly benchmark morphing attack detection performance. At the time of this writing, there are two such benchmarks: The Face Recognition Vendor Test (FRVT) Part 4: MORPH - Performance of Automated Face Morph Detection [76] and Bologna-SOTAMD: Evaluation of Differential Morph Attack Detection and Single Image Morph Attack Detection [96]. These benchmarks have provided a common platform that includes datasets, evaluation protocols and the computational environment. The platforms provide a trustworthy assessment of submitted algorithms. Below, we briefly describe the databases used in each platform and the performance achieved by various algorithms that are presented.

A. NIST-FRVT Part 4: MORPH - Performance of Automated Face Morph Detection

The FRVT MORPH test was introduced in June 2018 to provide a common platform for independent testing of MAD face technologies and to ensure a common assessment methodology. The dataset used in the evaluation was created using different morphing methods with the objective of identifying low-quality morphing (generated using freely available tools), automated morph generation (generated using an automatic tool without human intervention) and high-quality morph generation (generated with commercial morphing software and additional post-processing that is carried out to mask potential artifacts). The evaluation is carried out for both S-MAD and D-MAD techniques. However, the probe data used in the D-MAD evaluation are not effectively obtained from ABC gates. Several algorithms are evaluated, and the majority of the participants in the competition to date are from academic institutions. Most of the submissions for S-MAD are based on texture features, while for D-MAD, both face demorphing and differential feature-based techniques are evaluated. Based on the recent evaluation report, it can be noted that

1) None of the algorithms has indicated a reliable detection performance meeting the FRONTEX operational requirement [53], and thus, face morphing attack detection remains a challenging task.
2) The quality of morph generation has a direct impact on the performance of both S-MAD and D-MAD techniques.

In the S-MAD category, the use of hybrid features [95] has shown better performance than other MAD methods, while among the methods in the D-MAD category, the approach of latent feature differences based on ArcFace features [110] has attained the best detection performance.

B. Bologna-SOTAMD: Differential Morph Attack Detection

The Bologna-SOTAMD benchmark was opened for evaluation in 2019 and provided a common evaluation platform to benchmark D-MAD techniques. The Bologna-SOTAMD D-MAD benchmark consists of a database collected in the European SOTAMD project [10] using real ABC gates. The morphing was carried out using automated approaches with both open-source and commercial software. Several MAD techniques have been benchmarked, which include both face demorphing and feature difference methods, and the details of the evaluation protocol and the performance of various submitted algorithms can be found in [96]. Among the multiple algorithms evaluated, it can be noted that the existing D-MAD techniques are not robust enough to detect face morphing attacks in accordance with the FRONTEX operational requirement [53], highlighting the challenge of MAD again. The use of the feature difference-based D-MAD technique shows better performance than face demorphing techniques. The best result, a detection equal error rate (D-EER) of 3.36 $\%$, has been reported on digital data, and D-EER = 3.36 $\%$ has been reported on print-scan data.

C. Bologna-SOTAMD: Single Morph Attack Detection

The Bologna server has also hosted a public benchmark for S-MAD since 2020. The S-MAD dataset was constructed using high-quality passport images similar to those used in real passports. The morphed images were generated using both commercial (FantaMorph, FaceFusion) and open-source (triangulation with facial landmarks) face morphing software. Post-processing was carried out using automatic and manual processes to reduce the artefacts generated using the face morphing software. For more information on the database and evaluation protocol, see [96]. As evaluation started only recently, few algorithms have been benchmarked on the Bologna S-MAD platform. The baseline performance reported a D-EER of 37.10% and 38.99% on print-scan and digital morphed images. These preference measures indicate the challenges in detecting face morphing images using S-MAD techniques.

D. Discussion of Public Evaluation

Based on the above discussion of publicly available benchmarks and competitions, it can be noted that the reliable detection of face morphing attacks remains challenging. The performance of S-MAD is severely degraded compared to that of D-MAD. This can be attributed to the availability of additional information (another image) that can be used to make the final decision. The interesting outcomes of these competitions indicate that the use of the hybrid feature-based S-MAD technique has shown improved generalisability across various morph generation methods. At the same time, the feature difference method used in the context of D-MAD has shown a more robust performance on both benchmarks.

IX. Open Challenges

The research topic of face morphing and detection has received great interest from both research and governmental stakeholders. This has resulted in intensive research activities around studying the vulnerability of COTS FRSs and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3066254, IEEE Transactions on Technology and Society

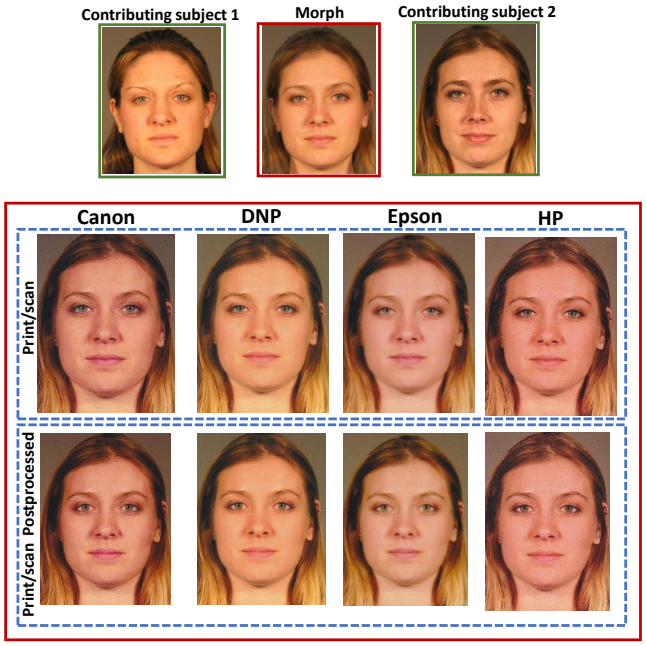

Fig. 11: Example of print-scan images and post-processed images. The variation in the data quality across different printers and scanners is notable, which challenges the MAD algorithms.

development of several MAD techniques to reliably detect such attacks. However, there are still several challenges and open issues that need to be addressed. In the next section, we present these challenges and open issues in the field of face morphing attack detection.

a) ***Unavailability of large-scale public datasets with variation****:* The unavailability of large-scale face morphing datasets reflecting real-life scenarios hinders the development of robust MAD. Furthermore, considering the different modes of morph attacks (digital and print-scan), it is necessary to generate and evaluate MAD algorithms on digital and print-scan datasets. However, the generation of large print-scan databases is quite expensive and tedious. Additionally, these databases cannot be shared publicly due to licensing restrictions or to privacy and General Data Protection Regulation (GDPR) [82] concerns. Hence, there is a limitation in accessing the existing morphing databases. Although the publicly available benchmarks now host large-scale databases, those datasets can only test submitted MAD algorithms. They cannot aid the further development of MAD algorithms. However, the systematic generation of morphed face images with various types of morphing software combined with different types of print-scan processes must result in large-scale databases that will become available for researchers in order to achieve significant progress in MAD.

b) ***Generalisability of MAD techniques****:* The generalisation of MAD techniques is crucial in achieving reliable performance in real-life border control scenarios. However, the existing MAD techniques are evaluated only on known types of face morph generation techniques and known sources of re-digitisation (printer and scanner types), except in NIST-FRVT Part 4: MORPH - Performance of Automated Face Morph Detection and Bologna-SOTAMD. Figure 11 illustrates the variation in morphed image quality due to different types of printers and scanners. The performance reported in the benchmarking study [76], [1], [96] also indicated the degraded performance of MAD techniques on both D-MAD and S-MAD when tested on unknown sources of generation. More significant degradation is noted with S-MAD methods, which is attributed to learning-based systems that can learn a decision policy based on known data. These factors limit the applicability of learning-based MAD techniques if they are not trained on a large-scale dataset with all real-life variants. Thus, it is essential to devise a MAD approach that is robust in detecting face morphing attacks.

c) ***Selection of data subjects for morphing****:* In earlier studies, morphed images were generated by randomly selecting the contributing data subjects. It is a well-established assumption that a morphing attack will be more successful with both human observers and machines (FRSs) if the candidate data subjects are selected based on a look-like measure. Some recent works [101], [91], [42], [124] describe the selection of data subjects in the morphing process. However, in the systematic study of these existing methods regarding the impact on FRS vulnerability, the detection performance of both human observers and automatic MAD detection methods still needs to be investigated.

d) ***Variation with face co-variates****:* The critical aspect that is not systematically studied with MAD is the role of face co-variates, which include age, gender, ethnicity, identification factors, image post-processing and image quality. A preliminary study on the effect of ageing on morphing vulnerability and detection was presented in [124] and has revealed the influence of ageing on face morphing vulnerability. The variation of face co-variates has a greater influence on S-MAD techniques, while for D-MAD techniques, the imaging quality plays a vital role. As the images are captured using an ABC gate in D-MAD, the influence of varying illumination due to day and night light settings needs to be investigated. Additionally, images captured live at an ABC gate may be acquired with eyeglasses or hair occlusions, and this has not yet been investigated. Thus, it is essential to benchmark both D-MAD and S-MAD techniques in a real-life scenario with all those co-variates. Another aspect that has not yet been investigated with regard to its impact on MAD is potential face beautification. It is expected that face images are beautified prior to applying for a passport in many countries [97]. As the beautification process changes the image properties, it is essential to understand both vulnerability and MAD for this particular problem.

e) ***Performance metrics****:* Considering that face morphing attack detection is emerging as a new operational problem, there has been only a slow convergence towards harmonised testing and reporting. Publicly available benchmarking and competitions have employed ISO/IEC metrics [59] to benchmark the detection performance of MAD techniques. However, there are no standardised metrics yet to evaluate the vulnerability of FRSs

with respect to morphing attacks. Furthermore, the available vulnerability metrics, such as FMMPMR and MMPMR, are not feasible for use in operational scenarios, including ABC gates and passport application scenarios. Therefore, there is a strong need for a standardised vulnerability evaluation metric incorporating experience from both practitioners and researchers working on face MAD. The availability of an international standard using ISO/IEC, together with commonly used vulnerability metrics, is discussed in Section VII, and this needs further effort.

f) ***Component-based morphing****:* Almost all literature has studied face morphing as a holistic problem with full-face image morphing. Le el al. [89] introduced partial face morphing, including a preliminary study on morphing only specific regions of the face. Extensive experiments indicate that partial morphing of the eye and nose poses a severe threat to commercial face recognition systems [89]. However, the systematic evaluation of high-quality face images has yet to be studied together with the impact on human expert observers (for example, border guards and super-recognisers).

g) ***Identical twins and look-alikes****:* The influence of morphing on identical twins and look-alikes is an interesting problem that needs systematic study within the scope of morphing. The vulnerability of FRSs to face morphing images generated from identical twins and similar subjects needs to be studied on large-scale databases.

h) ***User convenience****:* The design of user-convenient (or user-friendly) MAD systems plays a crucial role in making detection subsystems deployable in real-time applications. Thus, there is a need to design face MAD systems that allow minimal user intervention (from both operators and applicants). This fact needs to be considered when designing D-MAD techniques that are tailored for ABC systems.

X. Conclusion

Face recognition systems have gained a large amount of trust for security-related applications. However, morphing attacks on face recognition systems can be a hindrance to establishing a secure society. Furthermore, various morphing attack detection techniques have been proposed by several researchers to effectively detect morphed images. However, improvements in deep learning and machine learning techniques have resulted in the generation of high-quality morphs using various new techniques. Hence, generalising morph attack detection methods is still predicted to be far in the future considering the basic challenge of obtaining large public databases with variations and different morph generation techniques. In this paper, we detail the advancement of different types of morph generation techniques. Along with a brief overview of the different types of morphing attack detection techniques, the corresponding performance metrics are reported. We also provide a brief discussion of the challenges faced in this field in developing a robust technique to detect morphs, which serves as a reference for future work.

XI. Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356. This text reflects only the author's views and the Commission is not liable for any use that may be made of the information contained therein.

References

[1] Bologna online evaluation platform (boep): Differential morph attack detection. https://biolab.csr.unibo.it/fvcongoing/UI/Form/BenchmarkAreas/BenchmarkAreaDMAD.aspx. Accessed: May 2020.
[2] Cartoon brew. https://www.cartoonbrew.com/vfx/10-unforgettable-morphs-film-tv-music-videos-144036.html. Accessed: May 2020.
[3] Department of Internal Affairs (DIA), NZ. https://www.passports.govt.nz/passport-photos/passport-photo-requirements/.
[4] Federal Ministry of Education and Research . https://www.bmbf.de/en/index.html. Accessed: May 2020.
[5] GOV.UK. https://www.gov.uk/photos-for-passports/photo-requirements. Accessed: May 2020.
[6] International conference on biometrics for borders: Morphing and morphing attack detection methods. https://frontex.europa.eu/research/invitations/international-conference-on-biometrics-for-borders-morphing-and-morphing-attack-detection-methods-dER8qa. Accessed: May 2020.
[7] OCI services, india. https://ociservices.gov.in/Photo-Spec-FINAL.pdf. Accessed: May 2020.
[8] Passport,Wikipedia. https://en.wikipedia.org/wiki/Passport#National_conditions. Accessed: May 2020.
[9] Science Daily, Morphing. https://www.sciencedaily.com/terms/morphing.htm. Accessed: May 2020.
[10] State of the art morphing detection SOTAMD. https://www.ntnu.edu/iik/sotamd. Accessed: May 2020.
[11] Gnu image manipulation program (gimp). https://www.gimp.org, 2016. Accessed: 2014-08-19.
[12] New face morphing database for vulnerability research. https://www.linkedin.com/pulse/new-face-morphing-dataset-vulnerability-research-ted-dunstone, 2017. Accessed: May 2020.
[13] 3dthis face morph. https://3dthis.com/morph.htm, 2020. Accessed: October 2020.
[14] Abrosoft fantamorph. FantaMorph,Abrasoft:http://www.fantamorph.com/, 2020. Accessed: May 2020.
[15] Dlib programming library. http://dlib.net/, 2020. Accessed: October 2020.
[16] Face morpher. http://www.facemorpher.com/, 2020. Accessed: October 2020.
[17] Face swap online. https://faceswaponline.com/, 2020. Accessed: October 2020.
[18] imars. https://cordis.europa.eu/project/id/883356, 2020. Accessed: October 2020.
[19] Magic morph 1.95. https://downloads.tomsguide.com/magic-morph,0301-6817.html, 2020. Accessed: October 2020.
[20] Morph thing. https://www.morphthing.com/, 2020. Accessed: October 2020.
[21] Photo for a Passport or Identity-card, Netherlands. https://www.netherlandsworldwide.nl/countries/iran/living-and-working/photo-for-a-passport-or-identity-card, 2020. Accessed: October 2020.
[22] Secure access control over wide area network. https://www.ntnu.edu/iik/swan, 2020. Accessed: May 2020.
[23] United states visa. https://www.ustraveldocs.com/no/no-niv-photoinfo.asp, 2020. Accessed: October 2020.
[24] R. Abdal, Y. Qin, and P. Wonka. Image2stylegan: How to embed images into the stylegan latent space? *CoRR*, abs/1904.03189, 2019.
[25] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, and A. Noore. Face presentation attack with latex masks in multispectral videos. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, July 2017.
[26] A. Anjos and S. Marcel. Counter-measures to photo attacks in face recognition: A public database and a baseline. In *2011 International Joint Conference on Biometrics (IJCB)*, pages 1–7, 2011.
[27] N. Arad, N. Dyn, D. Reisfeld, and Y. Yeshurun. Image warping by radial basis functions: Application to facial expressions. *CVGIP: Graphical models and image processing*, 56(2):161–172, 1994.

[28] A. Asaad and S. Jassim. Topological data analysis for image tampering detection. In *International Workshop on Digital Watermarking*, pages 136–146, 2017.

[29] S. Autherith and C. Pasquini. Detecting morphing attacks through face geometry features. *Journal of Imaging*, 6:115, 2020.

[30] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool. Speeded-up robust features (SURF). *Computer Vision and Image Understanding*, 10(3):346–359, 2008.

[31] M. Bichsel. Automatic interpolation and recognition of face images by morphing. In *Proc. of the Second Intl. Conf. on Automatic Face and Gesture Recognition*. IEEE Comput. Soc. Press, 1996.

[32] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar. Face swapping: Automatically replacing faces in photographs. *ACM Trans. Graph.*, 27(3):39:1–39:8, 2008.

[33] V. Blanz, T. Vetter, et al. A morphable model for the synthesis of 3d faces. In *Siggraph*, volume 99, pages 187–194, 1999.

[34] O. Celiktutan, S. Ulukaya, and B. Sankur. A comparative study of face landmarking techniques. *EURASIP Journal on Image and Video Processing*, 2013.

[35] I. Chingovska, A. R. Dos Anjos, and S. Marcel. Biometrics evaluation under spoofing attacks. *IEEE transactions on Information Forensics and Security*, 9(12):2264–2276, 2014.

[36] D. W. Choi and C. J. Hwang. Image morphing using mass-spring system. 2011.

[37] R. S. Choras. Multimodal biometrics for person authentication. In *Digital Identity*. IntechOpen, 2019.

[38] A. Costa-Pazo, S. Bhattacharjee, E. Vazquez-Fernandez, and S. Marcel. The replay-mobile face presentation-attack database. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–7, 2016.

[39] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhörst, A. Braun, and A. Kuijper. Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In T. Brox, A. Bruhn, and M. Fritz, editors, *Pattern Recognition*, pages 518–534, Cham, 2019. Springer International Publishing.

[40] N. Damer, J. H. Grebe, S. Zienert, F. Kirchbuchner, and A. Kuijper. On the generalization of detecting face morphing attacks as anomalies: Novelty vs. outlier detection. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–5, 2019.

[41] N. Damer, A. M. Saladié, A. Braun, and A. Kuijper. Morgan: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10, Oct 2018.

[42] N. Damer, A. M. Saladié, S. Zienert, Y. Wainakh, P. Terhörst, F. Kirchbuchner, and A. Kuijper. To detect or not to detect: The right faces to morph. In *2019 International Conference on Biometrics (ICB)*, pages 1–8, 2019.

[43] N. Damer, S. Zienert, Y. Wainakh, A. M. Saladié, F. Kirchbuchner, and A. Kuijper. A multi-detector solution towards an accurate and generalized detection of face morphing attacks. In *22th International Conference on Information Fusion (FUSION)*, pages 1–8, 2019.

[44] L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, and C. Busch. PRNU variance analysis for morphed face image detection. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–9, 2018.

[45] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, and C. Busch. PRNU-based detection of morphed face images. In *2018 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–7, 2018.

[46] N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. *IEEE Transactions on Information Forensics and Security*, 9(7):1084–1097, 2014.

[47] N. Evans, S. Z. Li, S. Marcel, and A. Ross. Guest editorial: Special issue on biometric spoofing and countermeasures. *IEEE Transactions on Information Forensics and Security*, 10(4):699–702, 2015.

[48] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *IEEE International Joint Conference on Biometrics*, pages 1–7, sep 2014.

[49] M. Ferrara, A. Franco, and D. Maltoni. *Face Recognition Across the Imaging Spectrum*, chapter On the Effects of Image Alterations on Face Recognition Accuracy, pages 195–222. Springer International Publishing, 2016.

[50] M. Ferrara, A. Franco, and D. Maltoni. Face demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4):1008–1017, 2018.

[51] M. Ferrara, A. Franco, and D. Maltoni. Decoupling texture blending and shape warping in face morphing. In *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5, 2019.

[52] M. Ferrara, A. Franco, and D. Maltoni. Face morphing detection in the presence of printing/scanning and heterogeneous image sources. *CoRR*, abs/1901.08811, 2019.

[53] FRONTEX. Best practice technical guidelines for automated border control ABC systems, 2015.

[54] J. Galbally, S. Marcel, and J. Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, 23(2):710–724, 2014.

[55] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch. Is your biometric system robust to morphing attacks? In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2017.

[56] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann. Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.

[57] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann. Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2017.

[58] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization and International Electrotechnical Committee, March 2006.

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

[60] T. Jäger, K. H. Seiler, and A. Mecklinger. Picture database of morphed faces (mofa) : technical report. 2005.

[61] A. K. Jain, P. Flynn, and A. A. Ross. *Handbook of biometrics*. Springer Science & Business Media, 2007.

[62] S. Jia, G. Guo, and Z. Xu. A survey on 3d mask presentation attack detection and countermeasures. *Pattern Recognition*, 98:107032, 2020.

[63] J. Kannala and E. Rahtu. BSIF: Binarized statistical image features. In *2012 21st Intl. Conf. on Pattern Recognition (ICPR)*, pages 1363–1366, 2012.

[64] C. Kraetzer, A. Makrushin, T. Neubert, M. Hildebrandt, and J. Dittmann. Modeling attacks on photo-id documents and applying media forensics for the detection of facial morphing. In *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec '17, pages 21–32, 2017.

[65] R. S. S. Kramer, M. O. Mireku, T. Flack, and K. L. Ritchie. Face morphing attacks: Investigating detection with humans and computers. *Cognitive Research: Principles and Implications*, 4, 2019.

[66] S. Lee, G. Woberg, K.-Y. Chwa, and S. Y. Shin. Image metamorphosis with scattered feature constraints. *IEEE Transactions on Visualization and Computer Graphics*, 2(4):337–354, Dec. 1996.

[67] S.-Y. Lee, K.-Y. Chwa, S. Y. Shin, and G. Wolberg. Image metamorphosis using snakes and free-form deformations. In *SIGGRAPH*, volume 95. Citeseer, 1995.

[68] J. Liao, R. S. Lima, D. Nehab, H. Hoppe, P. V. Sander, and J. Yu. Automating image morphing using structural similarity on a halfway domain. *ACM Trans. Graph.*, 33(5):168:1–168:12, Sept. 2014.

[69] G. D. Lowe. Object recognition from local scale-invariant features. In *IEEE Intl. Conf. on Computer Vision (ICCV 1999)*, volume 2, pages 1150–1157. IEEE Computer Society, 1999.

[70] D. Maio, D. Maltoni, R. Cappelli, A. Franco, and M. Ferrara. Fvc-ongoing–benchmark area: face morphing challenge. 2018.

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

[72] A. Makrushin, C. Kraetzer, T. Neubert, and J. Dittmann. Generalized benford's law for blind detection of morphed face images. In *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec '18, pages 49–54, 2018.

[73] A. Makrushin, T. Neubert, and J. Dittmann. Automatic generation and detection of visually faultless facial morphs. In *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 6: VISAPP, (VISIGRAPP 2017)*, pages 39–50, 2017.

[74] A. Makrushin., T. Neubert., and J. Dittmann. Humans vs. algorithms: Assessment of security risks posed by facial morphing to identity verification at border control. In *Proceedings of the 14th International Joint Conference on Computer Vision, Imaging and Computer Graphics*

Theory and Applications - Volume 4: VISAPP,, pages 513–520. INSTICC, SciTePress, 2019.

[75] A. Makrushin, D. Siegel, and J. Dittmann. Simulation of border control in an ongoing web-based experiment for estimating morphing detection performance of humans. pages 91–96, 2020.

[76] N. Mei, P. Grother, K. Hanaoka, and J. Kuo. Face Recognition Vendor Test (FRVT) Part 4: Performance of Automated Face Morph Detection. Technical report, National Institute of Standards and Technology, July 2021.

[77] T. Neubert. Face morphing detection: An approach based on image degradation analysis. In *International Workshop on Digital Watermarking*, pages 93–106.

[78] T. Neubert, C. Kraetzer, and J. Dittmann. A face morphing detection concept with a frequency and a spatial domain feature space for images on emrtd. In *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec'19, page 95–100, New York, NY, USA, 2019. Association for Computing Machinery.

[79] T. Neubert, C. Krätzer, and J. Dittmann. Reducing the false alarm rate for face morph detection by a morph pipeline footprint detector. *2018 26th European Signal Processing Conference (EUSIPCO)*, pages 1002–1006, 2018.

[80] T. Neubert, A. Makrushin, M. Hildebrandt, C. Kraetzer, and J. Dittmann. Extended stirtrace benchmarking of biometric and forensic qualities of morphed face images. *IET Biometrics*, 7:325–332, 2018.

[81] M. Ngan, P. Grother, K. Hanaoka, and J. Kuo. Face recognition vendor test (frvt) part 4: Morph-performance of automated face morph detection. *National Institute of Technology (NIST), Tech. Rep. NISTIR*, 8292, 2020.

[82] Official Journal of the European Union. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679from=ENd1e2513-1-1, 2016.

[83] T. Ojala, M. Pietikäinen, and D. Harwood. A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, 29(1):51–59, 1996.

[84] V. Ojansivu and J. Heikkilä. Blur insensitive texture classification using local phase quantization. In *2008 International Conference on Image and Signal Processing (ICISP)*, pages 236–243. Springer Berlin Heidelberg, 2008.

[85] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello. Border control morphing attack detection with a convolutional neural network de-morphing approach. *IEEE Access*, 2020.

[86] A. Patel. Image morphing algorithm: A survey. 2015.

[87] K. Patel, H. Han, A. K. Jain, and G. Ott. Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *2015 International Conference on Biometrics (ICB)*, pages 98–105, 2015.

[88] F. Peng, L.-B. Zhang, and M. Long. FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image. *IEEE Access*, 7:75122–75131, 2019.

[89] 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 Transactions on Biometrics, Behavior, and Identity Science*, pages 1–16, 2020.

[90] R. Raghavendra and C. Busch. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv.*, 50(1), Mar. 2017.

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

[92] R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In *8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2016.

[93] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch. Transferable deep-cnn features for detecting digital and print-scanned morphed face images. In *Proc. IEEE Conf. Computer Vision Pattern Recognition Workshops (CVPRW)*, pages 1822–1830, 2017.

[94] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch. Detecting face morphing attacks with collaborative representation of steerable features. In *IAPR International Conference on Computer Vision & Image Processing (CVIP-2018)*, pages 1–7, 2018.

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

[96] K. Raja, M. Ferrara, A. Franco, L. J. Spreeuwers, I. Batskos, F. de Wit, M. Gomez-Barrero, U. Scherhag, D. Fischer, S. Venkatesh, J. M. Singh, G. Li, L. Bergeron, S. Isadskiy, R. Raghavendra, C. Rathgeb, D. Frings, U. Seidel, F. Knopjes, R. N. J. Veldhuis, D. Maltoni, and C. Busch. Morphing attack detection - database, evaluation platform and benchmarking. *ArXiv*, abs/2006.06458, 2020.

[97] C. Rathgeb, C.-I. Satnoianu, N. Haryanto, K. Bernardo, and C. Busch. Differential detection of facial retouching: A multi-biometric approach. *IEEE Access*, 2020.

[98] D. Robertson, R. S. Kramer, and A. M. Burton. Fraudulent id using face morphs: Experiments on human and automatic recognition. *PloS ONE*, 12(3):1–12, 2017.

[99] D. J. Robertson, A. Mungall, D. G. Watson, K. A. Wade, S. J. Nightingale, and S. Butler. Detecting morphed passport photos: a training and individual differences approach. *Cognitive Research: Principles and Implications*, 3(27):1–12, 2018.

[100] D. Ruprecht and H. Muller. Image warping with scattered data interpolation. *IEEE Computer Graphics and Applications*, 15, 1995.

[101] A. Röttcher, U. Scherhag, and C. Busch. Finding the suitable doppelgänger for a face morphing attack. In *International Joint Conference on Biometrics (IJCB)*, pages 1–8, September 2020.

[102] S. Schaefer, T. McPhail, and J. Warren. Image deformation using moving least squares. In *ACM transactions on graphics (TOG)*, pages 533–540. ACM, 2006.

[103] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch. Detecting morphed face images using facial landmarks. In *Image and Signal Processing*, pages 444–452. Springer International Publishing, 2018.

[104] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl. Detection of face morphing attacks based on PRNU analysis. *Trans. on Biometrics, Behavior, and Identity Science (TBIOM)*, 2019.

[105] 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 *Intl. Conf. of the Biometrics Special Interest Group BIOSIG 2017*, pages 1–7, 2017.

[106] U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch. On the vulnerability of face recognition systems towards morphed face attack. In *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.

[107] U. Scherhag, C. Rathgeb, and C. Busch. Morph detection from single face image: A multi-algorithm fusion approach. In *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, ICBEA '18, page 6–12, New York, NY, USA, 2018. Association for Computing Machinery.

[108] U. Scherhag, C. Rathgeb, and C. Busch. Towards detection of morphed face images in electronic travel documents. In *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*, pages 187–192, 2018.

[109] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch. Face recognition systems under morphing attacks: A survey. *IEEEAccess*, 2019.

[110] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch. Deep face representations for differential morphing attack detection. *IEEE Transactions on Information Forensics and Security*, 15:3625–3639, 2020.

[111] C. Seibold, A. Hilsmann, and P. Eisert. Reflection analysis for face morphing attack detection. *arXiv preprint arXiv:1807.02030*, 2018.

[112] C. Seibold, A. Hilsmann, and P. Eisert. Style your face morph and improve your face morphing attack detector. In *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–6, 2019.

[113] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert. Detection of face morphing attacks by deep learning. In *International Workshop on Digital Watermarking*, pages 107–120, 2017.

[114] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert. Accurate and robust neural networks for security related applications exampled by face morphing attacks. *arXiv preprint arXiv:1806.04265*, 2018.

[115] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert. Accurate and robust neural networks for face morphing attack detection. *Journal of Information Security and Applications*, 53:102526, 2020.

[116] J. M. Singh, R. Raghavendra, K. B. Raja, and C. Busch. Robust morph-detection at automated border control gate using deep decomposed 3d shape diffuse reflectance. In *2019 15th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, pages 106–112, 2019.

[117] S. Soleymani, B. Chaudhary, A. Dabouei, J. Dawson, and N. M. Nasrabadi. Differential morphed face detection using deep siamese

networks. *arXiv preprint arXiv:2012.01541*, 2020.

[118] S. Soleymani, A. Dabouei, F. Taherkhani, J. Dawson, and N. M. Nasrabadi. Mutual information maximization on disentangled representations for differential morph detection. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pages 1731–1741, 2021.

[119] L. Spreeuwers, M. Schils, and R. Veldhuis. Towards robust evaluation of face morphing detection. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pages 1027–1031, Sep. 2018.

[120] T. Ucicr. Feature-based image metamorphosis. *Computer graphics*, 26:2, 1992.

[121] S. Venkatesh, R. Raghavendra, K. Raja, and C. Busch. Single image face morphing attack detection using ensemble of features. In *23rd International Conference on Information Fusion*, pages 1–5, 2020.

[122] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch. Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network. In *The IEEE Winter Conference on Applications of Computer Vision (WACV)*, pages 1–8, March 2020.

[123] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch. Morphed face detection based on deep color residual noise. In *International Conference on Image Processing, Theory, Tools and Applications (IPTA)*, pages 1–8, November 2019.

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

[125] S. Venkatesh, H. Zhang, R. Raghavendra, K. Raja, N. Damer, and C. Busch. Can GAN generated morphs threaten face recognition systems equally as landmark based morphs? - vulnerability and detection. In *International Workshop on Biometrics and Forensics(IWBF)*, pages 1–5, 2020.

[126] Y. Weng, L. Wang, X. Li, M. Chai, and K. Zhou. Hair interpolation for portrait morphing. *Computer Graphics Forum*, 32(7):79–84, October 2013.

[127] D. White, R. I. Kemp, R. Jenkins, M. Matheson, and A. M. Burton. Passport officers' errors in face matching. *PloS one*, 9(8):e103510, 2014.

[128] G. Wolberg. Image morphing: a survey. *The visual computer*, pages 360–372, 1998.

[129] J. Wu. Face recognition jammer using image morphing. *Dept. Elect. Comput. Eng., Boston Univ., Boston, MA, USA, Tech. Rep. ECE-2011*, 2011.

[130] V. Zanella, G. Ramirez, H. Vargas, and L. V. Rosas. Automatic morphing of face images. In M. Kolehmainen, P. Toivanen, and B. Beliczynski, editors, *Adaptive and Natural Computing Algorithms*, pages 600–608, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[131] H. Zhang, S. Venkatesh, R. Ramachandra, K. Raja, N. Damer, and C. Busch. MIPGAN–generating robust and high quality morph attacks using identity prior driven GAN. *arXiv e-prints*, abs/2009.01729, 2020.

Sushma Venkatesh has been a Ph.D. candidate at the Norwegian University of Science and Technology (NTNU), Norway, since 2019. She obtained a bachelor's degree in computer science in 2008 and a master's degree in computer science and technology in 2011. Her recent research interests include deep learning, image processing, and applied machine learning with applications to biometrics, deception detection, privacy and security. She has authored a number of technical papers in various journals and conferences and serves as a reviewer for various scientific publication venues.

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 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. He is a member of the editorial board of the IET journal on biometrics, SN Computer Science, Springer and Journal of Imaging, MDPI.

Kiran Raja obtained a Ph.D. in computer science from the Norwegian University of Science and Technology (NTNU), Norway, in 2016. He is a faculty member at the dept. of computer science at NTNU, Norway. His main research interests include statistical pattern recognition, image processing, and machine learning with applications to biometrics, security and privacy protection. He has participated in the EU projects SOTAMD and iMARS and other national projects. He has authored several papers in his fields of interest and serves as a reviewer for a number of journals and conferences. He is a member of the EAB and chairs the Academic Special Interest Group at the EAB.

Christoph Busch is a member of the Norwegian University of Science and Technology (NTNU), Norway. He holds a joint appointment with Hochschule Darmstadt (HDA), Germany. Furthermore, he has lectured on biometric systems at Denmark's DTU since 2007. On behalf of the German BSI, he has been a coordinator of the project series BioIS, BioFace, BioFinger, BioKeyS Pilot-DB, KBEinweg and NFIQ2.0. He has been a partner of the EU projects 3D-Face, FIDELITY, TURBINE, SOTAMD, RESPECT, TReSPsS, iMARS and others. He is also a principal investigator at the German National Research Center for Applied Cybersecurity (ATHENE) and is a co-founder of the European Association for Biometrics (EAB). Christoph has co-authored more than 500 technical papers and has been a speaker at international conferences. He is a member of the editorial board of the IET journal on Biometrics and of the IEEE TIFS journal. Furthermore, he chairs the TeleTrusT biometrics working group as well as the German standardisation body on Biometrics and is a convenor of WG3 in ISO/IEC JTC1 SC37.