Mesopotamian journal of Big Data
Vol. **(2024)**, 2024, **pp**. 82–101
DOI: https://doi.org/10.58496/MJBD/2024/007 ISSN: 2958-6453
https://mesopotamian.press/journals/index.php/BigData

Research Article

Face Morphing Attacks Detection Approaches: A Review

Essa Mokna Namis[1, *], Khalid Shakir Jasim[1], Sufyan Al-Janabi [1]

[1] *College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq*

ARTICLE INFO

Article History
Received 26 Apr 2024
Accepted 28 Jun 2024
Published 20 Jul 2024

Keywords
Face Recognition Systems (FRSs)
Morphing attacks
Deep learning
Face detection
Biometrics

ABSTRACT

Face recognition systems (FRSs) that are applied by real-time applications such as border control are vulnerable to attacks such as face morphing, which blends two or more facial images into a single morphed image. The vulnerability of FRSs to many types of attacks, including both direct and indirect attacks, as well as face-morphing attacks, has garnered significant attention from the biometric field. A morphing attack aims to undermine the security of an FRS at an automated border control (ABC) gate by using an electronic machine-readable travel document (eMRTD) or e-passport that is acquired using a morphed face image. Most countries require applicants for an e-passport to present a passport photograph throughout the application process. A person with malicious intent and a collaborator can create a morphed facial image to illegally get an e-passport. A fraudulent individual, together with their accomplice, can exploit an e-passport with a morphed facial image to successfully travel through a border. Both individuals can authenticate the altered facial image, making it possible. A malicious individual could enter the border undetected, concealing their criminal history, while the access control system's log records information about their accomplice, posing a significant risk. This paper aims to provide a comprehensive overview of face morphing attacks and the developments happening in this field. We will go over the difficulties encountered, the methods for generating morphing images, and the pros and cons of these approaches. Along with the most important performance metrics that measure the efficiency of the algorithms used. The paper also covers the types of techniques used in deep learning and machine learning to detect and determine the attack of mutant faces. Indeed, it provides an overview of the most significant results from studies done in this area of research.

1. INTRODUCTION

Biometrics has been commonly utilized in various areas of security. Biometrics, which refer to the measurement of human features, are a prominent area of research in computer science. They have applications in security of data, access control, and identity systems [1]. Personal identification numbers or passwords were once the primary means of identification for each individual, but this led to numerous problems. As a result of how easy it is for someone to pretend to be someone else simply by knowing their password or phone number, biometric identifiers which are regarded as more reliable are being used more frequently. Since biometrics can provide unique and powerful information that can precisely identify a person, such as skin color, fingerprint, iris, face, hand geometry, retina, DNA, and palm veins, identification is the most widely used application of biometrics [2]. Since every person's face is different and packed with information [3], facial recognition systems are widely used in security and service departments of mobile phones, businesses, international airports, and social media companies on the internet, among other domains [4] .

In an effort to develop systems that can recognize faces accurately even though people are remarkably similar, researchers are currently very interested in facial recognition systems [5]. Face morphing can be a serious security risk when these altered photos are used for passports or identification because it allows multiple people (subjects) to use the information to verify their identities [6, 7] . Multiple subjects' improper connection to the document may lead to a number of illicit activities, including financial transactions, illegal immigration, and human trafficking. The targeted offender would modify his face photo with one of the impersonating partners in a real-world face-morphing attack scenario. If the partner requests an e-passport with an altered face photo, they will receive an authentic e-passport with matching document security features. It is possible to authenticate the accomplice and the partner using the morphed image found in the e-passport. This suggests that by using the e-passport that was given to the accomplice, the criminal can avoid the automated border control gates or perhaps even the human inspections at the gate. For this reason, it is imperative that this face-morphing attack be identified automatically [8].

*Corresponding author. Email: ess22c1002@uoanbar.edu.iq

A border control example scenario is shown in Fig.1, where a malicious person's face is altered to resemble that of an accomplice.

Fig. 1. Example of border control FRS vulnerability to morphed image [23].

When a person applies for a passport, their photo is saved in the electronic passport photo database (eMRTD). Images arrived in two formats: printed and sent online. The ability of changing the image is present in both scenarios. Judgment wanted individuals find this metamorphosis intriguing because it facilitates their cross-border travel [9, 10]. Fig.2 illustrates the scenario involving border control illustrates the use of morphed images. Additionally, Fig.3 illustrates an example of face morphing [11] .

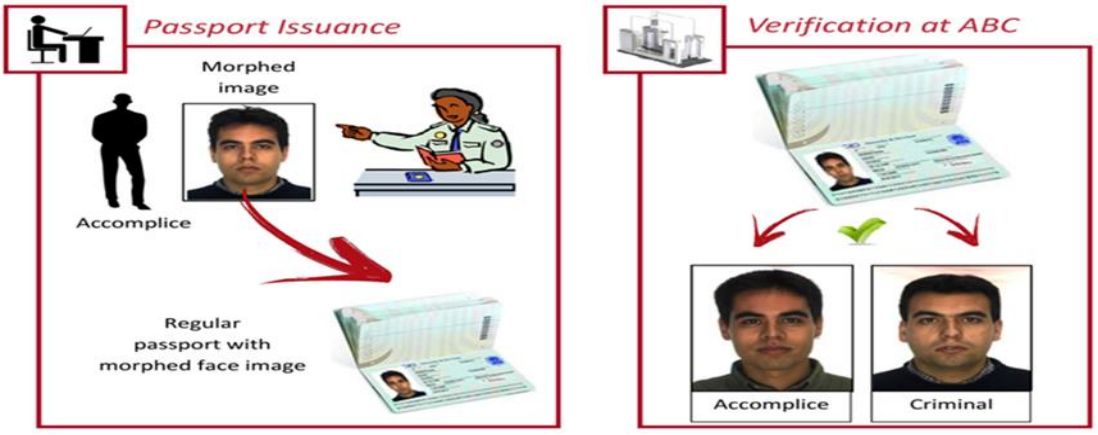

Fig. 2. A scenario involving border control illustrates the use of morphed images [12].

Fig. 3. Example of face morphing [11].

There is a lot of room for optical and electronic illusions with morphing faces. Researchers in this area have thus been hard at work in recent years trying to find solutions to this issue, with a lot of emphasis on either implementing brand-new technology or improving upon older systems [13].

The rest of this paper is structured as follows: Section 2 discusses the limitations of morphing and face recognition systems. Section 3 details the attack and generation of facial morphing. Next, the databases used to identify morphing attacks are reviewed in Section 4. After presenting the face morphing techniques in Section 5, we move on to the parameters and performance metrics used in morphing attack detection (MAD) in Section 6. Finally, the paper is concluded in Section7.The formatter will need to create these components, incorporating the applicable criteria that follow.

2. LIMITATIONS WITH MORPHING AND FACE RECOGNITION SYSTEMS

There are a lot of limitations to overcome when generating a morphing image, including [14, 15]:

1. Generating face morphing from many images of different individuals is difficult according to the increased variety of image textures and features.
2. Image distortion might potentially arise during the process of combining two photos into a single image, hence requiring the need for modifications.
3. The face morphing can only be achieved if the two source images are relatively similar, rather than totally different.
4. To reduce contrast variation, two images must be taken under the same settings.

In addition, there are some problems with face recognition systems that cause them to produce inaccurate results [16, 17]:

1. Because the morphed face is so similar to the traveler's own, there is a high matching ratio, allowing the traveler to cross the border.
2. The passport photo and the traveler's photo might not match, even though thy both belong to the same person, due to alterations made to a person's face features or deformities that can occur as a consequence of an accident.

3. FACE MORPHING ATTACK AND GENERATION

This section describes the most important face-morphing attacks and the methods used for generating them.

3.1 Face Morphing Attacks

One way to describe the morphing process is as an effect that changes the appearance of an image. In order to create a single morphed image, two facial images are combined, as shown in Fig. 4. Using one of the many freely available tools makes morphing a breeze. When subject preselection is used, the morphed image has characteristics that are almost identical to those of the two subjects that contributed to creating the morph. A human observer may not notice morphing-based image manipulation because, when processed carefully, the morphed image does not have many visible artifacts. This means that even a passport official who is very good at comparing faces might miss the morphing attack in practice[18]. A criminal with ill intentions could theoretically use a passport that has had its picture altered to pass through border security unnoticed. In a border control scenario, FRSs can be easily compromised using morphed images, as shown in Fig.1.

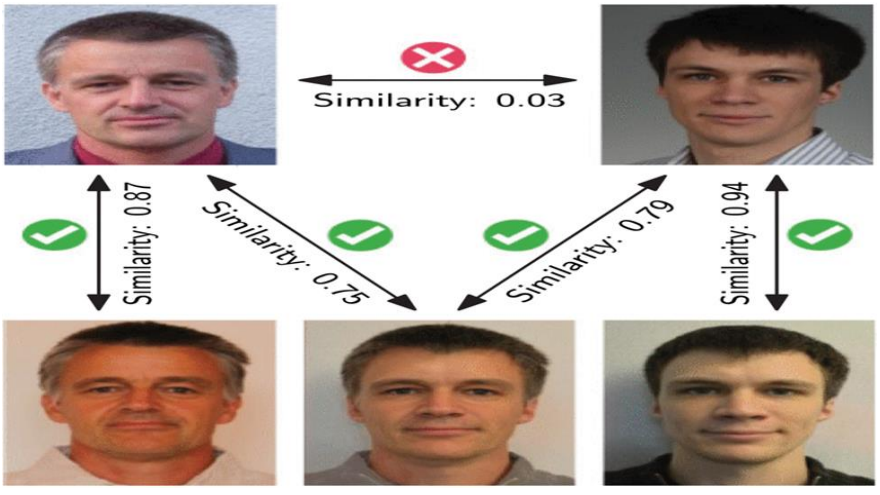

Fig. 4. An example of a face morphing attack would be the successful matching of multiple instances of the subjects' faces in order to create a morph in comparison to it using a COTS available face recognition program that has a default decision threshold of 0.5, leading to a false positive rate at 0.1% [4].

3.2 Generation of Face Morphing Attacks

Despite face morphing's widespread use for over a decade, particularly in the video animation industry, the vulnerability of FRSs has only lately come to light [3]. There are a number of methods that can be used to generate morphs, ranging from traditional image warping to more advanced generative adversarial networks (GANs)[19, 20]. Most popular morph generation strategies are based on the landmark-based approach[21]. In order to face morphing process, one must follow these steps [22]:

1. To achieve the same effect when morphing, preprocess both images.
2. Using the nose, eyes, mouth, and overall facial shape (including the insertion of the ear in some cases) to define facial features (also known as "face landmarking").
3. Both images are distorted and lined up because of the action.
4. Further processing to get rid of artifacts after combining the two images. There are two methods for creating a morphing image: automatically and manually.

A taxonomy of face morphing generation techniques is presented in Fig. 5, which broadly categorizes the available methods into two categories: (a) landmark-based techniques (b) deep learning-based techniques.

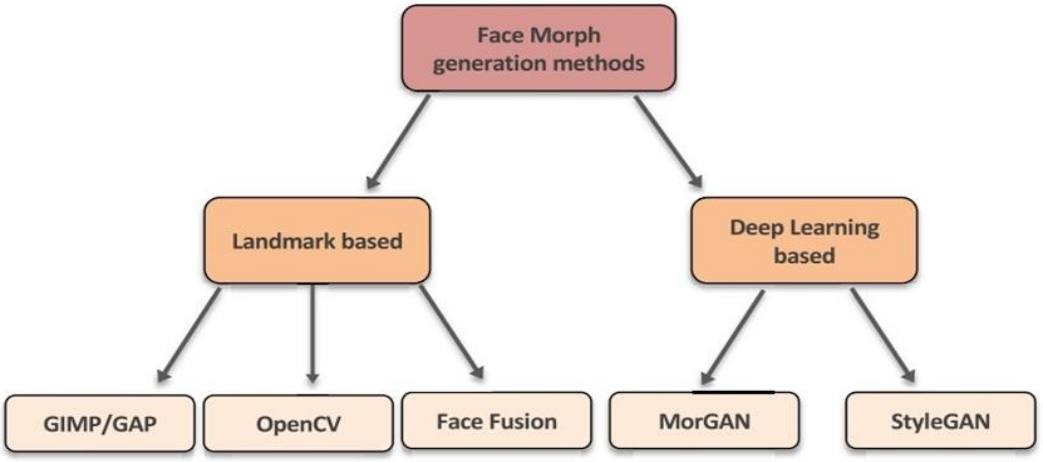

Fig. 5. Taxonomy of face morph generation techniques [23].

A. Landmark-based techniques: A number of programs can be used to accurately and rapidly generate a fake image. Morph Thing, Abrosoft Fanta Morph, Magic Morph, Face Morpher, and 3DAmong the many free apps available, this Face Morph is just one example. Both good and bad images can be produced by these programs due to the time and human intervention needed to remove the artifacts [24]. Use of landmarks The process of morph generation begins with the acquisition of landmark points on various facial regions, such as the nose, eye, and mouth. In order to distort these landmark points that were collected from both sides, the pixels are relocated to new, more averaged locations [25].

B. Deep learning-based techniques: Deep learning's numerous advantages, especially its speed and accuracy, have made it a hot topic recently and led to its expansion into numerous academic domains. One of the deep learning tools that has garnered attention is generative models, which are responsible for the incredible results they produce in this field. The results it produces are influenced by the training methodology, the network's design and structure, and the massive amount of data it utilizes. The enhanced results will be mind-blowing and spot-on in relation to the real content. Media can take many forms, including text, audio, and visuals. In this field, two prominent families have drawn a lot of attention, which are Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) [26].

In the realm of unsupervised learning, a powerful class of neural networks known as generative adversarial networks (GANS) exists. Ian J. Goodfellow initially suggested and advocated for it in 2014. The two main components of a GAN are the generator and discriminator neural network models; these models compete with one another to decompose, capture, and replicate database changes [27, 28]. Two network models make up GANs:

- **Generator:** The initial part of GANs, takes the training data and uses it to generate a vector of arbitrary values; from there, it generates new data that mimics the input data's pattern.
- **Discriminator:** The data generated by the first part must contain a distinction and some remarks. The purpose of this part is to classify the input data as either generated or actual.

On the other hand, Variational autoencoders (VAEs) are generative models designed to generate new samples by capturing the underlying probability distribution of a dataset. Among their many architectural features is an encoder-decoder structure. After the encoder converts the input data into a latent form, the decoder attempts to restore the original data using this latent representation. By reducing the dissimilarities between the original and reconstructed data, the VAE is able to deduce the distribution of the underlying data and generate new samples along those lines. One notable advantage of VAEs is their ability to generate new data samples that closely match the training set. Due to the continuity of the VAE's latent space, the decoder is able to generate new data points that seamlessly interpolate among the training data points. The following components make up a VAE: input, encoder, latent vector (Z) (mean $ standard division), decoder, and output [29, 30]. Table 1 outlines the benefits and drawbacks of the main types of morphing techniques.

TABLE I. GENERATION OF FACE MORPHING METHODS: BENEFITS AND DRAWBACKS

Face morphing generation method	Benefits	Drawbacks
Landmarks Based	1.Conversion is simple and automatic; just choose the photos you want to be transformed.	1. Sometimes removing artifacts requires manual labor.
	1.It takes some time to create a lot of morph images, but the programs are readily available and produce high-quality images.	2. The final image has contrast that needs to be adjusted after processing.
Deep Learning Based	1. No requirement for manual assistance.	1. They have a difficult learning process.
	2. Generation that is smooth and has respectable image quality.	2. Doesn't always produce excellent morphed images.
	3. Many tools that are open-source.	3. Highly prone to geometric distortion.
	4. Doesnot show double edges in the generation images.	4. Requires careful pre-selection of data subjects based on age, gender, ethnicity .

4. DATABASES FOR DETECTING MORPHING ATTACKS

Various attack mechanisms and metrics have led to the generation of public and private datasets with varying attack strengths. This section reviews face morph databases utilized in existing works. Table 2 summarizes established datasets used to evaluate FRS vulnerability and MAD technique performance. The first face morph database was created by Ferrara et al. [31], who utilized landmark-based techniques with GIMP/GAP tools. The dataset contains a limited number of digital images, specifically 14 morphed images created from 8 genuine subjects, comprising both male and female participants. The images in this database have been digitally altered and are not accessible to the public. Using the landmarks and GIMP/GAP tools, Ferrara et al. [32] expanded this dataset. Ten male and nine female participants make up the 80 morphed face images that make up the extended dataset. The database is not accessible to the general public due to its digital format.

Raghavendra et al. [33] presented the first sizable database with a variety of ethnicities (Caucasian, Asian, European, American, Latin American, and Middle Eastern), utilizing facial landmarks and the GIMP/GAP morph generation technique with the GNU image manipulation tool. This database includes 450 facial morphs created from 110 subjects of various ethnicities. This database is private and only includes digital images.Makrushin et al. [34] generated high-quality morph images using automatic tools. Triangulation was used with 68 dlib library facial landmarks [35]. Complete morph (including both facial images) and splicing morph (clipping out face pixels from input faces) were used to generate morphs. Warping two images in complete morphs causes pixel discontinuities. A splicing morph is created. The database contains 1326 complete morphs and 2614 splicing morphs from 52 subjects, including 17 females and 35 males. This digital database of face morph images is private. A print-scan face morph database was first introduced by Scherhag et al. [36]. For morph generation, the authors used landmark-based GIMP/GAP. This database has 231 morphed images from 462 real images. HP Photosmart 5520 and Ricoh MPC 6003 SP printers were used to print and scan images for this private database. Later, Raghavendra et al. [37] developed a face morph dataset with digital and print-scan images. Using OpenCV, a publicly available tool, face morphs were generated automatically. This database generates morphed and averaged face images, totaling 1423 + 1423. In addition to the database, Raghavendra et al. [38] established an evaluation protocol with separate sets for development, training, and testing. Print-scan morphed face images were created using a Ricoh MPC 6003 SP printer. Private database. The dataset now includes 2518 morphed face images and 1273 real images.

Ferrara et al. [39] generated a face morph database using the Sqirlz morphing technique. The dataset contains 100 morphed images in digital and print-scan formats. This database is not accessible to the public for research purposes. Another database by Scherhag et al. [40] uses landmark-based morphing techniques such as OpenCV, FaceMorphed, FaceFusion, and UBO. The database contains around 791+3246 morphed face images from FERET and FRGCv2. This private database contains digital and print-scan morphed face images. Singh et al. [41]produced a facial morph database using OpenCV-based morph

generation. The first dataset for probe images from automatic border control (ABC) gates with varying lighting conditions was introduced for detecting differential morphing attacks. This database contains digital and print-scan enrolment images from an EPSON XP-860 printer and scanner. This dataset contains 90 morphed face images and is not publically available.

Damer et al. [42] created the first face morphing database using deep learning-based images.The landmark-based morphs and deep learning database are compared. Landmark-based morph generation used 68 dlib landmark points and deep learning-based morph generation used GAN architecture. The database contains 1000 morphed face images, but the current 64x64 GAN-based morphs do not meet ICAO standards. This private database contains only digitally morphed faces. The first database of morphed face images under ageing was introduced by Venkatesh et al. [43]. The authors used the University of Bologna's UBO morphing method, which uses dlib and 68 landmark points for morph generation [44]. The database includes 14305 (10538+3767) morphed face images aged 2-5 years. This database contains digital morphed face images that are not accessible to the public.

Raja et al. [45] introduced the sequestered BolognaSOTAMD face morphing dataset during a recent public competition and benchmarking on the Bologna Online Evaluation Platform (BOEP), in line with the FVC-onGoing series. The dataset contains images from 150 individuals gathered from three distinct geographic locations, representing different ethnicities, genders, and ages. Face morphing is performed using six techniques, with automatic and manual postprocessing to correct any artifacts resulting from the process. The dataset contains printed and scanned versions produced by various printers, and the enrollment images adhere to the ICAO standards for passport images. The probe images are captured from different ABC gates and gate emulations. The database contains 5748 morphed face images and 1396 bonafide face images.Iman S. Razaq [46] built database with the help of the StyleGAN method. Since it is devoid of artifacts, it is unable to discriminate and produces an image that is most like the real and more complex ones. A total of 3,515 morph images, derived from 1451 source images, make up the dataset. Furthermore, the AMSL dataset contains 2000 morphed images in addition to the 201 original images from the Face Research Lab London set. Qiaoyun et al. [47] proposed a new morphing attack method for FRSs. Morphed landmarks were generated adaptively to better maintain facial geometry of contributing subjects. Using GCNs, morphing features are extracted from landmarks and combined with appearance features to generate high-quality morphed images with high attack success rates. They quantitatively and qualitatively compare the method to leading methods. The results show that the method improves both identity preservation and visual quality. Moreover, Singh et al. [48] introduced a technique for creating 3D facial transformations using two authentic point cloud data sets. This approach initially identifies authentic point clouds exhibiting neutral facial emotions. The two input point clouds were registered using a Bayesian Coherent Point Drift (BCPD) algorithm, without any optimization. The shape and color of the registered point clouds were then averaged to create a point cloud representing a morphed face. The suggested technique produces 388 points clouds for face-morphing using data from 200 genuine individuals. Table 2 below displays some details of the previous work that has been done using various databases.

TABLE II. MORPH FACE IMAGE DATABASES.

Reference	Type OF Generation	Method of Generation	Bonafide & Morph
Ferrara et al.[31]	Landmark method	GIMP GAP	No. of Morph images: 14
Ferrara et al. [32]	Landmark method	GIMP GAP	No. of Morph images: 80
Raghavendra et al[33].	Landmark method	GIMP GAP	No. of Morph images : 450
Markrushine et al. [34]	Landmark method	Automatic generation (dlib landmark)	No. of Morph images: 1326
Scherhag et al. [36]	Landmark method	GIMP GAP	No. of Morph images: 231
Raghavendra et al. [37]	Landmark method	GIMP GAP	No. of Morph images: 1423 + 1423
Raghavendra et al. [38]	Landmark method	GIMP GAP	No. of Morph images:2518
Ferrara et al. [39]	Landmark method	Sqirlz Morph	No. of Morph images:100
Scherhag et al.[40]	Landmark method	OpenCV Face Fusion Face Morpher	No. of Morph images: 791+3246
Singh et al.[41]	Landmark method	OpenCV	No. of Morph images:90
Damer et al.[42]	GAN-based	GAN	No. of Morph images: 1000
Venkatesh et al.[43]	Landmark method	UBO Morpher	No. of Morph images: (10538+3767)
Raja et al.[45]	Landmark method	UBO Morpher	No. of Morph:1396
Iman S. Razaq et al.[46]	Style-GAN	Style-GAN	No. of Morph images: 3515
Qiaoyun et al.[47]	GCNs	Graph Convolutional Networks (GCNs)	----------
Singh et al.[48]	Landmark method	Bayesian Coherent Point Drift (BCPD) without optimization, and the geometry and color of the registered point clouds.	No. of Morph images: 388

5. DETECTION OF FACE MORPHING ATTACKS

Various automated MAD methods have been proposed as a solution to the problems caused by human observers. Since the previous section introduced face morphing attacks on FRSs, we provide an overview of MAD strategies here [49]. The current MAD methods can be broadly classified into two groups: S-MAD, which uses a single image, and D-MAD, which uses a differential image. Both of them are shown in Fig.6 below [50, 51]. Moreover, approaches in both MAD categories that have been reported to date are depicted in Fig. 7.

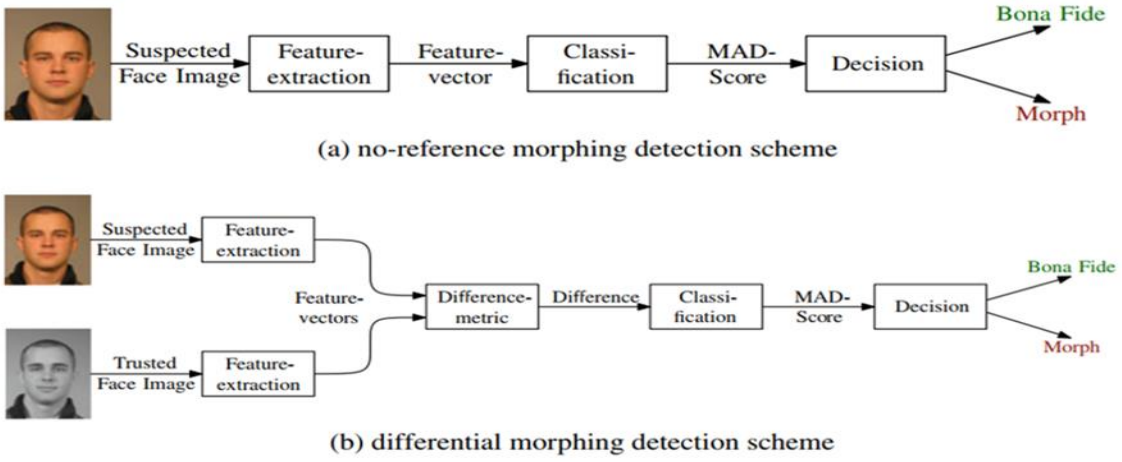

Fig. 6. Types of Morphing Attacks Detection [52].

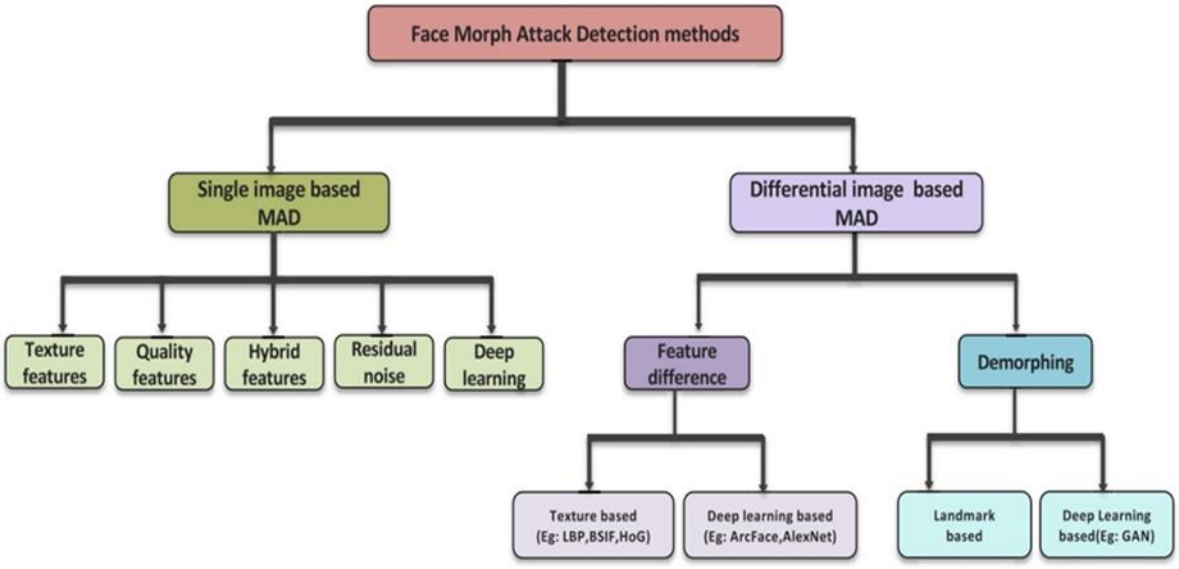

Fig. 7. Taxonomy of MAD techniques [23].

5.1 Single Image MAD Method (No-Reference MAD)

In order to determine if an input image is bone-fide or morphed, single image MAD methods analyze only the morphed version of the image. Because image morphing always results in artifacts and traces, it takes advantage of that. The algorithm for detecting face morphing attacks is fed a single image. Here, a photo of the applicant's face is submitted with the passport application in order to assess its potential for suspicion. The reason S-MAD is the most difficult type is that it relies on a single image and does not have the actual image available [22, 53]. Not only do digital images pose a problem, but scanned images do as well. given that certain nations make use of scanned images. There are often traces in digital images from the morphing process. Because noise is often associated with images, scanning them will be a huge challenge.

Table 3 provides a brief summary of the pros and cons of various S-MAD approaches for reference., Table 4 and Table 5 summarize some research in this field.

A. Texture Features Based S-MAD: The image's texture is the primary focus of these algorithms. It is possible to identify and differentiate between images based on their texture since every image has its own distinct texture. There is a plethora of algorithms that examine the texture of an image. Some examples are Binary Gabor pattern, GLCM, LBP, Hybrid color local binary patterns, and BSIF. Among scanned mutant faces, color textures (LBP), deep learning, and BSIF are the most popular algorithms for identifying them [54, 55].

B. Deep Learning-Based S-MAD: This area of expertise has put a lot of resources into uncovering the morphing faces because deep learning has been so successful. The use of image data for network training is widespread. The input data for these networks is derived from images. When fed into this network, morphed images can actually work to your advantage. among other networks, such as DenseNet, ResNet101, ResNet50, VGG-19, and VGG-16 [39, 56, 57].

C. Quality-Based S-MAD: Image quality is the primary concern of this approach, which means that it uses quality-related metrics to determine if a picture has been damaged or has artifacts introduced by manipulation. This technique can detect morphed images even when they have degradation or distortions. Metadata, reflection analysis, edge and corner distortions, and picture Response Non-Uniformity (PRNU) are just some of the features that can be studied using this approach. Even with this method, it does well in detection; however, this is due to the image's specifics. Finding or studying it will be difficult if the morphing process works [58, 59].

D. Residual Noise Based S-MAD: It is well-known that the morph process is concerned with the movement of parts between two images, particularly two images of faces. Since there has to be a change in the size of the features or the skin tone, the pixel values will differ between the two pictures. The result is visual artifacts known as noise. Using the transformed face's noise output as an identifier is the foundation of this technology. To isolate the noise-containing areas, the basic idea of this method is to subtract the modified image from the original, noise-free image. This method had remarkable detection power, but it requires the original, noise-free image to function. Skillful application of this method was made for the first time to remove noise from images generated by the CNN algorithm [60, 61].

E. Hybrid Based S-MAD: The principal idea behind this approach is to combine different methods for extracting facial features. This method has been used extensively and has produced good results because there are so many different techniques to extract the features. This technology's strength lies in its combination, as opposed to alternatives that rely on a single feature extraction technique. On the other hand, there is a significant financial and time commitment involved [38, 62].

TABLE III : THE PROS AND CONS FOR S-MAD TECHNIQUES.

Features Type	Pros	Cons
Hybrid Features	1. Adept at identifying various morph image types - digital or scanned. 2.It has generalizability. 3.Every time, extract a different feature.	1. Finding appropriate parameters that fit the detection process and integrating the methods together is a challenging implementation process that takes work. 2.Expensive.
Image Quality Features	1.Easy to execution. 2.Less cost. 3.Utilize a scanner and different digital data types.	1.When it comes to the same data type,whether digital or scanner, its performance varies. 2.Impacted by data that has been compressed.
Deep CNN features	1.It works effectively with both kinds of digital scans and images.	1.It functions well with various types of digital scans and images. 2. A sizable database is needed for the various face and movement types.
Residual Noise Features	1.Easy to execution. 2.Less computing power is needed. 3.High performance for digital data. 4.Despite the images varying resolutions ,it can still generalize.	1.It exclusively works with digital images and is sensitive to image compression. 2.If there is no audible noise during the conversion process, it cannot detect well.
Texture Features	1.Easy to execution. 2.Reduced costs. 3.Improved digital data efficiency and accurate detection.	1.Not optimal for scanning data. 2.This has an impact on the images' accuracy, particularly if the resolution is low.

TABLE IV: SOME RELATED WORKS FOR S-MAD TECHNIQUES HIGHLIGHTING APPROACH, ALGORITHM AND DATABASE.

Reference	Approach	Algorithm	Database
Raghavendra et al. [33]	Texture Method	Many techniques: LBP with SVM, BSIF with SVM, Image Gradient with SVM	Digital Images
Makrushin et al. [34]	Quantized DCT coefficients	Benford features	Digital Images
N. Tom et al. [63]	Image degradation Method	Corner feature detector	Digital Images
Makrushin et al. [64]	Quantized DCT coefficients	Features extracted for Benford from quantized DCT coefficients	Digital Images
N. Tom et al. [65]	Morph pipeline footprint detector	Features extracted for Benford from quantized DCT coefficients	Digital Images
Luuk et al. [66]	Texture based approach	LBP-SVM, Down-up sampling	Digital Images
H. Mario et al. [59]	Stirtrace Method	Multi-compression anomaly detection	Digital Images
Debiasi.L et al. [58]	Image degradation	Photo Response Non-Uniformity (PRNU)	Digital Images
Remachandra et al. [62]	Steerable features	Luminance component extraction	Print-Scan
D. Naser et al. [67]	MAD Multidetector fusion	LBPH, Transferable deep-CNN Digital	Digital Images
F. Matteo et al. [68]	Deep learning	Many Deep Neural Network: AlexNet, VGG19, VGG-Face16, VGG-Face2	Print-Scan
S. Uirich et al. [56]	multi-algorithm fusion	feature extraction through four techniques: 1. Texture descriptor using (LBP, BSIF), 2. Key point extractors using (SIFT, SURF) 3. gradient estimators (HoG) 4.Deep neural network	Digital Images
A. Aras et al. [69]	Texture Method	Topological data analysis method	Digital Images
S. Ulrich et al. [36]	Texture and frequency Method	LBP, LPQ, BSIF, 2DFFT with SVM classifier	Digital Print/Scan
K. Christian et al. [70]	Texture Method	Media forensics	Digital Images
S. Clemens et al. [71]	Deep learning Method	Many Deep Neural Network: VGG19 Net, Google Net, Alex Net	Digital Images
Remachandra et al. [37]	Texture Method	color textures, BSIF , LBP, LPQ.	Print/Scan
Min Long et al. [72]	Light weight convolution network	Bag Net	Digital Images
Tian Ma et al. [73]	Feature Pyramid Network	FSG-FD	Digital Images
Ramachandra et al. [74]	Different approaches: Deep feature s, Hand crafted, morph noise	Scale space features and SRKDA	Digital Images
Singh et al. [75]	Deep CNN	AlexNet with SVM ,ResNET with SVM	Digital Images
Venktatesh et al. [76]	Deep learning Method	AlexNet,ResNET50 WITH SRKDA	Digital, Print-Scan ,print-Scan compression images
Ramachandra et al. [77]	Texture Method	BSIF, LBP WITH P-CRC and SRKDA	Digital,print-scan,print-scan compression images.
Singh et al. [78]	Point based deep learning Method	Linear-SVM	Digital Images
Darguad et al. [55]	Texture Method	PCA with SVM	Digital Images
Juan Tapia et al. [79]	Deep learning Method	Deep Neural Network (AlphaNet)	Digital Images
AGHDAIE et al. [80]	Deep CNN Method	Convolutional Block Attention Module (CBAM)	Digital Images
SINGH et al. [81]	Deep learning Method	ResNET 34, StyleGAN	Digital Images
Tapia et al. [82]	Texture Method	(SRM, ELA, DFT, SVD, LBP and BSIF) With Random forest	Digital Images
Cheng-kun Jia et al. [83]	multi-algorithm fusion	Texture descriptors, image quality, deep learning	Digital Images
Iman S. Razaq et al. [46]	multi-algorithm fusion	PCA,Deep Neural Network	Digital Images
Singh et al. [84]	multi-algorithm fusion	LBP,HoG and BSIF with three types of classifiers (SVM , SRKDA and P-CRC)	Digital &Print-Scan&Print-Scan compression
Ibsen et al. [85]	Deep learning Method	Neural network architecture optimized by a Tetra-Loss function	Digital images
Ramesh et al. [86]	Deep learning Method	Deep Neural Network, VGG19	Digital images

TABLE V: SOME RELATED WORKS FOR S-MAD TECHNIQUES HIGHLIGHTING LIMITATIONS AND MAIN RESULTS.

Reference	Limitations	Main Results
Raghavendra et al. [33]	The available morphing tools for creating morphed photos are highly restricted. Only morph-2 images were used	ACER = 1.73%.
Makrushin et al. [34]	The available morphing tools for creating morphed photos are highly restricted	Accuracy = 98.44%
N. Tom et al. [63]	Data do not include images with varying feature space by more degradation sensitive features, only three corner detectors which describe the degradation	Accuracy = 90.1% under laboratory conditions and 84.3% under real world conditions.
Makrushin et al. [64]	The available morphing tools for creating morphed photos are highly restricted	TPR values are higher than 98.6%
N. Tom et al. [65]	The available morphing tools for creating morphed photos are highly restricted	Reduced the False Alarms by 83.67%.
Luuk et al. [66]	The available morphing tools for creating morphed photos are highly restricted.	In the case of within-database detection, the EER jumped from less than 5% to more than 20% when noise was added, and from more than 12% when down-up scaling was applied. Almost no one could tell that either case involved manipulation.
H. Mario et al. [59]	Additional post-processing operations, should be applied order to expand StirTrace.	Improved StirTrace to address the use case of face morphing forgeries, when the results demonstrate that the current state of the anomaly detection approach is sufficient for passport-scaling, line/column removal, cropping, and rescaling up to 75% and 90%, respectively.
Debiasi.L et al. [58]	The available morphing tools for creating morphed images are extremely limited.	When it came to image sharpening and scaling, the suggested detection system held its own. The only time it failed was with the applied histogram equalization.
Remachandra et al. [62]	The dataset does not contain images with different lighting conditions. In addition, differences in headgear, eyewear, and facial hair are also excluded from consideration.	Bonafide Presentation Classification Error of 13.12% at Attack Presentation Classification Error Rate of 10%.
D. Naser et al. [67]	The available morphing tools for creating morphed photos are highly restricted. Only morph-2 images were used	The best-performing single detector's BPCER was 15.7% and 3.0%, respectively, and the suggested solution reduced it to 2.7% and 0.0% at a 1.0% APCER.
F. Matteo et al. [68]	Only morph-2images are employed.	BPCER=2.3% at APCER=10%.
S. Uirich et al. [56]	The dataset does not contain images with different lighting conditions. In addition, differences in headgear, eyewear, and facial hair are also excluded from consideration.	D-EER= 2.8%.
A. Aras et al. [69]	The dataset does not contain images with different lighting conditions. In addition, differences in headgear, eyewear, and facial hair are also excluded from consideration.	Most misclassified images are actually morph images, and the complete morphing scheme achieved an accuracy of around 60%.
S. Ulrich et al. [36]	The dataset does not contain images with different scanning resolutions.	A rise of more than 20% absolute in BPCER10 was observed in the algorithms under study, with line-scans outperforming flatbed scans. The absolute increase in BPCER20 for the flat-bed scanner was 28.57%, while for the line scanner it was 31.6%.
K. Christian et al. [70]	differences in headgear, eyewear, and facial hair are also excluded from consideration.	The accuracy of a decision tree classifier ranges from 81.3% to 98% depending on the specific training and test scenarios.
S. Clemens et al. [71]	The dataset does not contain images with different lighting conditions. In addition, differences in headgear, eyewear, and facial hair are also excluded from consideration.	The FAR ranges from 0.8% to 2.2% and the FRR from 3.5% to 16.2% among our trained networks. With a FRR of 3.5% and a FAR of 0.8%, the VGG19 (pretrained) achieved the best result for both rates.
Remachandra et al. [37]	The present face databases are limited in size and raise privacy concerns.	EER=02.93%. APCER10 = 0.86%. APCER5= 1.72%.
Min Long et al. [72]	The dataset in this article lacks comprehensiveness and does not include the postprocessing of morphing attacks utilizing digital images. Therefore, the performance of the method requires further investigation and confirmation. The evaluation criteria do not take into account the threshold relationship in the specified indicators.	Results from experiments on 3 datasets and comparison with current methods indicate that the proposed method improves detection performance with fewer network model parameters and operations. Additionally, cross-dataset testing demonstrates the robustness of the proposed method.
Tian Ma et al. [73]	The collective techniques do not produce the highest overall accuracy of the network.	Accuracy values = 94%.

Ramachandra et al. [74]	The algorithms are unfair on training and testing on different ethnic groups.	When trained and tested on different ethnic groups, the results show that all six S-MAD methods are unfair. This suggests that there needs to be a reliable MAD approach to reduce algorithmic bias.
Singh et al. [75]	The alignment technique being utilized is not capable of handling non-rigid deformations. In addition, the alignment procedure does not produce any gaps or openings in the face morphing image.	EER=2.1%
Venktatesh et al. [76]	The dataset does not contain images with different lighting conditions.	1.The data medium and morph generation methods impact the detection performance of the MAD approaches. 2. The S-MAD algorithms' MAD performance is negatively impacted by the inter dataset evaluation protocol. 3. Out of all three mediums, the inter-evaluation protocol has shown that the proposed method outperforms the existing methods. 4.The proposed multi-level fusion method outperforms the state-of-the-art approaches in the majority instances.
Ramachandra et al. [77]	The dataset does not contain images with different lighting conditions.	●D-ERR=23.92% on SMAD-MORPHDB-D-1.0. ● D-EER = 40.45% on SMAD-BIOLAB1.0.
Singh et al. [78]	●Removing unwanted noise from 3D images can be a difficult process that sometimes requires direct intervention. ●The proposed method has not been implemented on datasets of significant size that have varying 3D resolutions.	D-EER = 1.59%.
Darguad et al. [55]	Synthetic data has not been utilized to enhance performance in a cross-morphed evaluation setting.	Specifically in cross-domain scenarios with a realistic diversity of morphing algorithms, such as StyleGAN-based approaches, the results demonstrate how challenging it is to detect single image morphing attacks. It is possible for the suggested method to outperform the MobileNetV2 strategy that was tested.
Juan Tapia et al. [79]	The present face databases are limited in size and raise privacy concerns.	PCER10=4.41% and BPCER 20 of=4.56%.
AGHDAIE et al. [80]	The limitation of the present research arises from the various combinations of attention modules in the deep neural network (DNN) and the specific levels at which these attention modules are integrated.	Theis method reduces detection error rates compared to existing techniques.
SINGH et al. [81]	The level of quality in the generation of composites is not higher. This method has not been evaluated on real face photos from public datasets	Although the proposed CFIA is challenging to detect using both human and automated methods, the results showed that it could reveal the FRS's vulnerability.
Tapia et al. [82]	The fusion-specific features should be expanded to incorporate Deep Learning methods in order to accurately detect certain morphing tools. This is because synthetic images generated using GANs may be easily identified using the DCT feature, as opposed to landmark-based approaches like FaceMorpher.	Face-Morpher reached an EER=11.90%, ,OpenCV= 8.38%, StyleGAN2= 3,30%, and Web Morph obtained a 3,23%. The BPCER10/20 obtained is 13.5% and 16.3%.
Cheng-kun Jia et al. [83]	This method does not utilize high-frequency characteristics and a progressively upgraded two-stream network for detection.	EER was 0.88% on HNU (FaceMDB2), the EER was 1.06% on HNU (FaceMDB3), and the EER was 0.77% on HNU (FaceMDB3). Compared with nine MAD technologies, the proposed approach achieved excellent detection results on datasets with various pixel fusion factors. Under various pixel fusion and position fusion factors, the proposed approach was still robust.
Iman S. Razaq et al. [46]	This approach does not quantify the changes between the original image and the modified image in order to determine the percentage of change in both the quantity and quality of the original and morphed images, specifically focusing on the comparison of facial features.	In comparison to SVM's 98.64% accuracy, the DNN classifier attained an average accuracy of 99.02%. The FRA and RFF evaluation clearly shows how powerful the proposed work. Which obtained the lowest feasible values for DNN FAR 0.018, FRR 0.003, FAR 0.023, and FRR 0.06 for SVM, indicating that the error rate in calculating the actual images is morphed. When these ratios are smaller than one, the detection accuracy of the system is higher.

Singh et al. [84]	This method doesn't evaluate advanced fusion techniques, conduct benchmarking, or compare current state-of-the-art (SOTA) procedures.	The results showed that the proposed method outperformed the existing methods in two separate evaluation protocols.
Ibsen et al. [85]	This method does not delve into the development of synthetic data to enhance the generalization power of the proposed system across different attackers and environmental situations.	At FMR=0.1%, ArcFace, MagFace, and AdaFace achieve a minimum 45% improvement in Relative Impostor Attack Presentation Accept Rate (RIAPAR).
Ramesh et al. [86]	This method does not investigate the areas that influence the decision-making process of a network, nor does it assess the disparities between various topologies and pretrained networks.	The false rejection rate (FRR) of the trained networks varies from 3.5% to 16.2%, while the false acceptance rate (FAR) ranges from 0.8% to 2.2%. The VGG19 model, which was pretrained, achieved the best result for both rates, with a False Rejection Rate (FRR) of 3.5% and a False Acceptance Rate (FAR) of 0.8%.

5.2 Differential Morphing Attack Detection (D-MAD) Method

By comparing the passport image with the live image of the traveler, this technique can detect the morphing image. Compared to the previous method, this one is simpler, requires less effort, and offers a higher probability of getting a clear shot of the tourist's face [87]. Both images are typically used to extract the same features. The classifier determines whether the observed change is a morph or not by comparing them to a predetermined metric and then using the difference as its basis. One benefit of this approach is that it incorporates the supplementary data from the TLC into the decision-making process. Keep in mind that TLCs in the real world are typically obtained in semi-supervised settings, like a border gate, and might have worse quality and more variation than the suspected images because of this [88] [89]. An example of D-MAD is presented in Fig. 8.

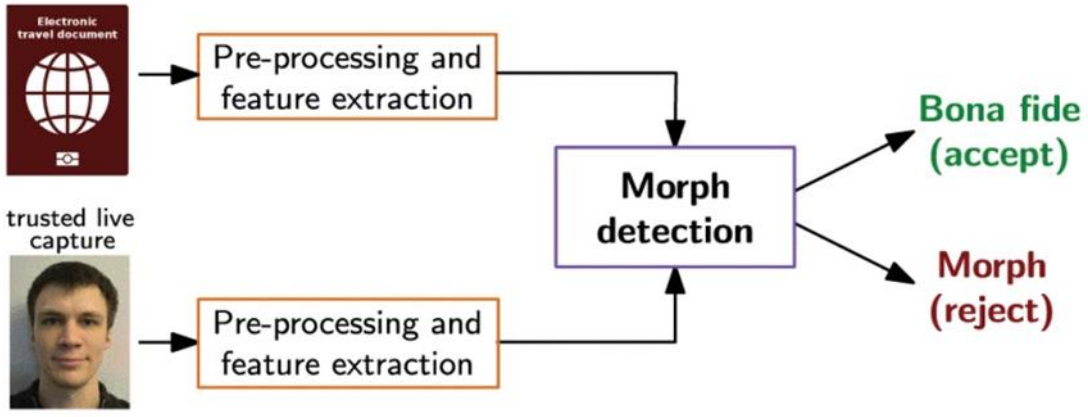

Fig. 8. An example for D-MAD [4].

Figure 7 shows a taxonomy of D-MAD approaches, which can be categorized into two main types: Feature Difference Based D-MAD, and Demorphing. Table 6 Outlines the benefits and constraints of current D-MAD approaches, Table 7 and Table 8 summarize some research in this field.

1. **Feature Difference Based D-MAD:** This type is based on the idea of identifying the features that differ between two images. To identify a morph attack, the features of the suspect's passport photo and their live photo are computed, and the difference between the two is then found. Stated differently, utilizing the distinction between the attributes and determining that ratio If it is big, it indicates that the two individuals are not the same; if it is small, it indicates that they are. In this field, there are numerous methods for obtaining feature extraction from gradients, textures, deep features, and landmark points [18, 41].
2. **Demorphing Based D-MAD:** This method depends entirely on face detection, unless multiple images are combined to create a transformed image. This technology is strong, cutting edge, and performs effectively through CNN's deep learning. When the intended person's live image is taken at ABC Gates, the quality of the photos that are captured affects the method's performance, which deteriorates when the image is affected by noise and lighting [89, 90].

TABLE VI: THE BENEFITS AND CONSTRAINTS OF D -MAD APPROACHES.

Algorithm Type	Benefits	Constraints
Feature difference	1.Easy to execution. 2. For images, the likelihood of detection is acceptable despite the accuracy of the images varying.	1.High computational cost 2.The kind of data used and the features extracted have an impact on image detection
Demorphing	1.Easy to execution. 2.Restricted and highly accurate detection data are needed. In the event that the suspected image is converted, it can see the face.	1. Facial positions and shooting conditions, including variations in lighting and facial movement,have an impact on detection.

TABLE VII: SOME RELATED WORKS FOR D-MAD TECHNIQUES HIGHLIGHTING DETECTION TYPE, APPROACH ALGORITHM AND DATABASE.

Reference	Detection Type	Approach Algorithm	Database
P. Fei et al. [90]	GAN using for Face restoration	Symmetric dual network architecture	Digital Images
S. Ulrich et al. [40]	Deep Face Representation	ArcFace Network, FaceNet algorithm	Digital, Scan Images
Scherhag et al. [91]	difference-based method	The first step Pre-processing and second step feature extraction through four techniques: 1. Texture descriptors. 2. Deep learning. 3. Key point extractors. 4. Gradient estimators.	Digital Images
D.Naser et al. [67]	Multi detector fusion	Transferable deep-CNN, LBPH	Digital Images
Singh et al. [41]	Deep learning	SfS Net and Alexnet	Digital, Scan Images
Clemens et al. [92]	Deep Learning	Layer Wise Relevance Propagation (LRP)	Digital Images
Delcampo et al. [89]	Deep CNN, Demorphing method.	Auto-generation (encoders).	Digital, Scan Images
S. Ulrich et al. [93]	Landmark method	Many techniques 1. Distance-method. 2. Random Forest for feature extraction. 3. SVM without using kernel. 4. Function classifier for SVM with radial basis	Digital Images
HAMZA et al. [8]	Deep Learning	SVM	Digital Images
Singh et al. [94]	Deep Learning	AlexNET,ResNet50,Resnet101,xception,VGG 16,VGG19 with L-SVM	Digital Images
Long et al. [95]	Demorphing method	Face de-morphing is performed on landmarks-based and learning-based morphed facial images, respectively	Digital Images

TABLE VII: SOME RELATED WORKS FOR D-MAD TECHNIQUES HIGHLIGHTING LIMITATIONS AND MAIN RESULTS.

Reference	Limitation	Main Results
P. Fei et al.[90]	This technique does not prioritize enhancing the restoration accuracy for datasets with varying fusion factors or reducing the inference time.	Evaluate the efficacy of the suggested plan, we also contrast the suggested FD-GAN in two cases with the most recent face de-morphing technique: ●Scenario1= 85.97%. ●Scenario2=64.90%.
S. Ulrich et al. [40]	This solution is not feasible for implementation in a real-world environment. It is important to conduct testing using realistic data. Nevertheless, the issue remains that the transfer of databases is challenging as a result of privacy rules.	(D-EER less than 3%)
Scherhag et al. [91]	This solution is not feasible for implementation in a real-world environment. It is important to conduct testing using realistic data. Nevertheless, the issue remains that the transfer of databases is challenging as a result of privacy rules.	● D-EER=3.9% for LBP. ● D-EER for BSIF is as low as 2.4%. ● D-EER for Texture descriptors =2.9%.
D.Naser et al. [67]	The available morphing tools for creating morphed photos are highly restricted.Only morph-2 images were used	By implementing this approach, the Attack Presentation Classification Error Rate dropped from 3.0% to 2.7% and the Bona Fide Presentation Classification Error Rate from 15.7% to 0.0%, respectively, compared to the best performing single detector.
Singh et al. [41]	This approach has not been tested on a large-scale database.	This method yields an EER of 8.6±0.1, compared to the best EER of 28.5±0.4 for SOTA. The detection error

		trade-off curves show that fusing scores improve the proposed algorithm more than SOTA. While the approach outperforms SOTA, it still has moderate deficiencies for single cameras.
Clemens et al. [92]	This approach lacks the integration of complicated multiclass pretraining with defense mechanisms against adversarial attacks, which would enhance the robustness of the neural network models.	A reliable and precise network was obtained by the proposed method. Unlike the other training methods, this network's decision-making process revealed that it compared different regions among each other to detect morphing attacks.
Delcampo et al. [89]	This approach has not been tested on a large-scale database.	The presented approach has a lower EER and better performance. The accuracy rate rises to 98% across all corpora. The first corpus, FRAV-ABC-Test, had 0.78 EER and 98.7% accuracy with a similar threshold.
	This method does not integrate landmark-based information with complimentary information obtained from the image texture.	The proposed algorithm achieves 32.7% Equal Error Rates.
S. Ulrich et al. [93]	The proposed solution is not feasible for implementation in a real-world environment in order to enhance performance, it is imperative to train and evaluate the model using actual images.	This model yields promising results for age, illumination, posture, and expression variations. Morphed images were tested using various machine learning classifiers, with SVM yielding the best results.
HAMZA et al. [8]	The suggested approach does not enhance the generalizability across various morphing image qualities, particularly with varying print quality.	This method combines six pre-trained deep CNNs using hierarchical fusion. The novel method uses spherical interpolation computed by SLERP for residual feature fusion. All three protocols showed improved performance with the proposed method.
Singh et al. [94]	This model has a limited inference time speed.	This method achieves 90.88% restoration accuracy in Scenario1 and 88.18% in Scenario2 The restoration accuracy is comparable when identity features are separated in semantic latent space, eliminating pixel-level loss constraints and preserving identity features.

6. MAD PARAMETERS AND PERFORMANCE METRICS

In this section, both of the parameters and performance metrics of MAD systems are discussed. The most important parameters used in MAD are [96]:

1. **Training dataset:** The MAD algorithm is trained using these morphed and real images. The MAD algorithm performs better with a better training dataset. It makes up roughly 70% of the whole dataset.
2. **Testing dataset:** Once a MAD algorithm has been trained using the training dataset, these morphed and real images are used to evaluate the algorithm's effectiveness. One can test the accuracy of an algorithm using the testing dataset. It makes up about 30% of the total dataset.
3. **Landmark-detection:** Landmark detection is one of the key MAD parameters. In this preprocessing step, morphed and authentic images are identified and normalized based on key facial features like the mouth, eyes, and nose. For improved MAD, the facial image can be cropped using landmark detection to concentrate only on the facial features.
4. **Feature extraction:** For interesting portions of the images, it functions as a kind of dimension reduction that effectively represents a compact characteristic vector. To tell if an image is morphed and authentic, features extraction is utilized. Steerable pyramids and local binary patterns are a couple of examples of feature extractors.
5. **Classification:** This is about using the training dataset whose membership in the category is identified to determine which of a set of groups the individual testing data set belongs to. There are two classification categories in MAD: morphed images and bonefide images.
6. **Scenario:** Discusses the methods employed in MAD. Additionally, there are just two scenarios: the no-reference (single-image) based scenario and the reference (differential) based scenario.
7. **Post-processing:** Focuses on settings that can change a morphed image's inherent properties in order to thwart attack detection. Print-scan operations, image compression, and image sharpening are a few examples of these parameters.

In addition, the most important papers utilized five performance metrics to evaluate face morphing attacks, these five-performance measure are as follows:

1. The Bona Fide Presentation Classification Error Rate (BPCER) OR False Rejection Rate (FRR): measures the proportion of real presentations that are incorrectly identified as presentation attacks in a given scenario, or the relative number of real images that are incorrectly identified as morphing attacks. The expected

percentage of transactions that are mistakenly rejected with genuine identity claims (in a positive identity system) is another way to define BPCER [97].

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_{BF}} \qquad (1)$$

Where N_{BF} represents the overall count of the legal presentations. The variable "Res_i" is assigned a value of 1 if the presentation is categorized as an attack presentation, and a value of 0 if it is categorized as a bona fide presentation.

2. **Attack Presentation Classification Error Rate (APCER) OR False Acceptance Rate (FAR):** This can be expressed as a relative number of morphing attacks classified as true images, or as the percentage of attacks that use the same presentation attack device species but are mistakenly classified as true (bone fide) presentations in a given scenario [31].

$$APCER = \frac{1}{NpAI} \sum_{1=1}^{NpAI} (1 - Res_i) \quad (2)$$

The N_{PAI} represents the total count of attack presentations for the specified PAI. The variable "Res_i" is assigned a value of 1 when the presentation is categorized as an attack presentation, and a value of 0 when it is categorized as a bona fide presentation.

3. **Detection-Equal Error Rate (D-EER):** An algorithm called D-EER is used to explain the BPCER Threshold values and its APCER. The equal error is the common value that results when the rates are same or equal. The APCER percentage and the BPCER percentage are equal, according to the common value. This is where BPCER = APCER is found. It serves as the training's ideal starting point. The precision of the biometric system increases with decreasing D-EER. The detection error equation based on the evaluated decision threshold (δ)[98].

$$D - EER = (APCER(\theta) + BPCER(\theta))/2) \quad (3)$$

4. **Accuracy (ACC):** This can be defined as the proportion of accurately classified images to all images that have been categorized [99].

$$ACC = Accurate\ Classification/Total\ Classified\ Image \qquad (4)$$

5. **True Positive Rate (TPR**): Also referred to as Sensitivity or Recall, TPR calculates the proportion of real positives classified as such (for instance, the number of altered images identified as an attack) [99].

$$TPR = \frac{TruePostive}{TruePositive + FalseNegative} \qquad (5)$$

7. CONCLUSION

FRSs have established significant trust for applications related to security. However, morphing attacks against FRSs may hinder the development of a secure society. Furthermore, various morphing attack detection techniques have been proposed by several researchers to effectively detect morphed images. In order to enable current face systems to identify morphed faces, numerous algorithms have been developed along new methods. The researchers have done extensive study in this area. There has been a recent uptick in efforts to revolutionize deep learning, a technique that is crucial in image recognition. Due to the numerous unfilled gaps and ongoing system updates, work is still ongoing in this area. In this paper, we have described the progress of various morph generation methods, providing a short summary of the various morphing attack detection methods, and reporting the most important performance metrics for each method. This area is still undergoing research. Those interested in this field may find this paper useful as a reference since it summarizes the most recent technologies used.

Authors contribution

As a testament to the cooperative environment, every author made equally significant contributions. The researchers carefully designed and implemented the study framework, followed by a thorough analysis of the data and integration of their findings into a cohesive report. Their smooth cooperation and combined expertise propelled every phase of our undertaking, solidifying this effort as a genuine tribute to our shared dedication.

Funding

There was no outside funding for the research that led to the writing or publishing of this article.

Conflict of intrestrst

None.

References

[1] Ambikapathy, T. D. Beeta, R. K. Kanna, A. Danquah-Amoah, V. S. Ramya, and U. Mutheeswaran, "Biometric Application on Facial Image Recognition Techniques," in 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), 2024, pp. 848-851.
[2] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," International Journal on Interactive Design and Manufacturing (IJIDeM), vol. 15, pp. 365-380, 2021.
[3] M. Keshavarz and S. Khosravi, "The magic of borders," e-flux Architecture, vol. 14, pp. 1-7, 2020.
[4] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," IEEE Access, vol. 7, pp. 23012-23026, 2019.
[5] M. I. Ghareb, D. J. Hamid, S. D. Sabr, and Z. F. Tofiq, "New approach for Attendance System using Face Detection and Recognition," Passer Journal of Basic and Applied Sciences, vol. 4, pp. 124-141, 2022.
[6] D. J. Robertson, R. S. Kramer, and A. M. Burton, "Fraudulent ID using face morphs: Experiments on human and automatic recognition," PLoS One, vol. 12, p. e0173319, 2017.
[7] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Accurate and Robust Neural Networks for Security Related Applications Exampled by Face Morphing Attacks, June 2018. arXiv180604265," ed, 2020.
[8] M. Hamza, S. Tehsin, H. Karamti, and N. S. Alghamdi, "Generation and detection of face morphing attacks," IEEE Access, vol. 10, pp. 72557-72576, 2022.
[9] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl, "Detection of face morphing attacks based on PRNU analysis," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 1, pp. 302-317, 2019.
[10] N. Davison, "Whole-of-government reforms in New Zealand," London: UK Institute for Government, 2016.
[11] K. Raja, S. Venkatesh, and R. Christoph Busch, "Transferable deep-cnn features for detecting digital and print-scanned morphed face images," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017, pp. 10-18.
[12] C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, Handbook of digital face manipulation and detection: from DeepFakes to morphing attacks: Springer Nature, 2022.
[13] 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, vol. 3, pp. 1-11, 2018.
[14] L. Wandzik, R. V. Garcia, G. Kaeding, and X. Chen, "CNNs under attack: on the vulnerability of deep neural networks based face recognition to image morphing," in International Workshop on Digital Watermarking, 2017, pp. 121-135.
[15] E.-V. Pikoulis, Z.-M. Ioannou, M. Paschou, and E. Sakkopoulos, "Face morphing, a modern threat to border security: Recent advances and open challenges," Applied Sciences, vol. 11, p. 3207, 2021.
[16] M. K. Rusia and D. K. Singh, "A comprehensive survey on techniques to handle face identity threats: challenges and opportunities," Multimedia Tools and Applications, vol. 82, pp. 1669-1748, 2023.
[17] S. Mishra, "Challenges in Face Recognition-A Critical Review," International Journal of Early Childhood Special Education, vol. 14, 2022.
[18] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhörst, A. Braun, et al., "Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts," in Pattern Recognition: 40th German Conference, GCPR 2018, Stuttgart, Germany, October 9-12, 2018, Proceedings 40, 2019, pp. 518-534.
[19] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye, "A review on generative adversarial networks: Algorithms, theory, and applications," IEEE transactions on knowledge and data engineering, vol. 35, pp. 3313-3332, 2021.

[20] T. Chakraborty, U. R. KS, S. M. Naik, M. Panja, and B. Manvitha, "Ten years of generative adversarial nets (GANs): a survey of the state-of-the-art," Machine Learning: Science and Technology, vol. 5, p. 011001, 2024.
[21] Q. He, Z. Deng, Z. He, and Q. Zhao, "Optimal-Landmark-Guided Image Blending for Face Morphing Attacks," in 2023 IEEE International Joint Conference on Biometrics (IJCB), 2023, pp. 1-9.
[22] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Single image face morphing attack detection using ensemble of features," in 2020 IEEE 23rd International Conference on Information Fusion (FUSION), 2020, pp. 1-6.
[23] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face morphing attack generation and detection: A comprehensive survey," IEEE transactions on technology and society, vol. 2, pp. 128-145, 2021.
[24] U. Scherhag, J. Kunze, C. Rathgeb, and C. Busch, "Face morph detection for unknown morphing algorithms and image sources: a multi-scale block local binary pattern fusion approach," IET Biometrics, vol. 9, pp. 278-289, 2020.
[25] I. Batskos, L. Spreeuwers, and R. Veldhuis, "Visualizing landmark-based face morphing traces on digital images," Frontiers in Computer Science, vol. 5, p. 981933, 2023.
[26] A. A. Ali and M. I. Ghareb, "Knowledge Discovery in Health Domain using Deep Neural Network Algorithms," Passer Journal of Basic and Applied Sciences, vol. 4, pp. 107-123, 2022.
[27] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," IEEE signal processing magazine, vol. 35, pp. 53-65, 2018.
[28] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, et al., "Generative adversarial networks," Communications of the ACM, vol. 63, pp. 139-144, 2020.
[29] C. Doersch, "Tutorial on variational autoencoders," arXiv preprint arXiv:1606.05908, 2016.
[30] A. Vahdat and J. Kautz, "NVAE: A deep hierarchical variational autoencoder," Advances in neural information processing systems, vol. 33, pp. 19667-19679, 2020.
[31] F. Matteo, F. Annalisa, and M. Davide, "The magic passport," in IEEE International Joint Conference on Biometrics (IJCB'14), 2014, pp. 1-7.
[32] M. Ferrara, A. Franco, and D. Maltoni, "On the effects of image alterations on face recognition accuracy," Face recognition across the imaging spectrum, pp. 195-222, 2016.
[33] R. Ramachandra, K. Raja, and C. Busch, "Detecting morphed face images," in 8th IEEE International Conference on Biometrics Theory, Applications and Systems, BTAS, 2016, pp. 1-7.
[34] A. Makrushin, T. Neubert, and J. Dittmann, "Automatic generation and detection of visually faultless facial morphs," in international conference on computer vision theory and applications, 2017, pp. 39-50.
[35] D. E. King, "Dlib-ml: A machine learning toolkit," The Journal of Machine Learning Research, vol. 10, pp. 1755-1758, 2009.
[36] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "On the vulnerability of face recognition systems towards morphed face attacks," in 2017 5th international workshop on biometrics and forensics (IWBF), 2017, pp. 1-6.
[37] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 555-563.
[38] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Towards making morphing attack detection robust using hybrid scale-space colour texture features," in 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA), 2019, pp. 1-8.
[39] M. Ferrara, A. Franco, and D. Maltoni, "Face morphing detection in the presence of printing/scanning and heterogeneous image sources," IET Biometrics, vol. 10, pp. 290-303, 2021.
[40] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep face representations for differential morphing attack detection," IEEE transactions on information forensics and security, vol. 15, pp. 3625-3639, 2020.
[41] J. M. Singh, R. Ramachandra, 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), 2019, pp. 106-112.
[42] N. Damer, A. M. Saladie, S. Zienert, Y. Wainakh, P. Terhörst, F. Kirchbuchner, et al., "To detect or not to detect: The right faces to morph," in 2019 international conference on biometrics (ICB), 2019, pp. 1-8.
[43] S. Venkatesh, K. Raja, R. Ramachandra, and C. Busch, "On the influence of ageing on face morph attacks: Vulnerability and detection," in 2020 IEEE International Joint Conference on Biometrics (IJCB), 2020, pp. 1-10.
[44] 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), 2019, pp. 1-5.
[45] K. Raja, M. Ferrara, A. Franco, L. Spreeuwers, I. Batskos, F. de Wit, et al., "Morphing attack detection-database, evaluation platform, and benchmarking," IEEE transactions on information forensics and security, vol. 16, pp. 4336-4351, 2020.

[46] I. S. Razaq, "Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network," Karbala International Journal of Modern Science, vol. 9, p. 15, 2023.
[47] Q. He, Z. Deng, Z. He, and Q. Zhao, "Optimal-Landmark-Guided Image Blending for Face Morphing Attacks," arXiv preprint arXiv:2401.16722, 2024.
[48] J. M. Singh and R. Ramachandra, "3D Face Morphing Attack Generation using Non-Rigid Registration," arXiv preprint arXiv:2404.15765, 2024.
[49] A. Makrushin and A. Wolf, "An overview of recent advances in assessing and mitigating the face morphing attack," in 2018 26th European Signal Processing Conference (EUSIPCO), 2018, pp. 1017-1021.
[50] R. Christian, T. Ruben, V.-R. Ruben, and B. Christoph, "Handbook of digital face manipulation and detection," ed: Springer Open Access, 2022.
[51] C. R. Elidona Shiqerukaj, "Fusion of Face Demorphing and Deep Face Representations for Differential Morphing Attack Detection," BIOSIG 2022, 2022.
[52] U. Scherhag, C. Rathgeb, and C. Busch, "Face morphing attack detection methods," in Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, ed: Springer International Publishing Cham, 2022, pp. 331-349.
[53] J. E. Tapia and C. Busch, "Single morphing attack detection using feature selection and visualization based on mutual information," IEEE Access, vol. 9, pp. 167628-167641, 2021.
[54] I. S. Razzaq and B. K. Shukr, "Generating and Detecting Face Morphing Using Texture Techniques," Journal of Kufa for Mathematics and Computer Vol, vol. 10, pp. 102-107, 2023.
[55] L. Dargaud, M. Ibsen, J. Tapia, and C. Busch, "A principal component analysis-based approach for single morphing attack detection," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2023, pp. 683-692.
[56] U. Scherhag, C. Rathgeb, and C. Busch, "Morph deterction from single face image: A multi-algorithm fusion approach," in Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications, 2018, pp. 6-12.
[57] C. Seibold, A. Hilsmann, and P. Eisert, "Style your face morph and improve your face morphing attack detector," in 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), 2019, pp. 1-6.
[58] 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), 2018, pp. 1-7.
[59] 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), 2017, pp. 1-6.
[60] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2020, pp. 280-289.
[61] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, "Morphed face detection based on deep color residual noise," in 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), 2019, pp. 1-6.
[62] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Detecting face morphing attacks with collaborative representation of steerable features," in Proceedings of 3rd International Conference on Computer Vision and Image Processing: CVIP 2018, Volume 1, 2019, pp. 255-265.
[63] T. Neubert, "Face morphing detection: An approach based on image degradation analysis," in Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16, 2017, pp. 93-106.
[64] 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, 2018, pp. 49-54.
[65] T. Neubert, C. Kraetzer, and J. Dittmann, "Reducing the false alarm rate for face morph detection by a morph pipeline footprint detector," in 2018 26th European Signal Processing Conference (EUSIPCO), 2018, pp. 1002-1006.
[66] L. Spreeuwers, M. Schils, and R. Veldhuis, "Towards robust evaluation of face morphing detection," in 2018 26th European Signal Processing Conference (EUSIPCO), 2018, pp. 1027-1031.
[67] N. Damer, S. Zienert, Y. Wainakh, A. M. Saladie, F. Kirchbuchner, and A. Kuijper, "A multi-detector solution towards an accurate and generalized detection of face morphing attacks," in 2019 22th International Conference on Information Fusion (FUSION), 2019, pp. 1-8.
[68] F. Matteo, F. Annalisa, and M. Davide, "Face morphing detection in the presence of printing/scanning and heterogeneous image sources," ArXiv.

[69] A. Asaad and S. Jassim, "Topological data analysis for image tampering detection," in Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16, 2017, pp. 136-146.
[70] 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, 2017, pp. 21-32.
[71] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16, 2017, pp. 107-120.
[72] M. Long, X. Zhao, L.-B. Zhang, and F. Peng, "Detection of face morphing attacks based on patch-level features and lightweight networks," Security and Communication Networks, vol. 2022, 2022.
[73] T. Ma, A. Bamweyana, M. Guo, and K. Benon, "A Face Morph Detection Method Based on Convolutional Neural Networks and Occlusion Test," in 2022 7th International Conference on Image, Vision and Computing (ICIVC), 2022, pp. 158-165.
[74] R. Ramachandra, K. Raja, and C. Busch, "Algorithmic fairness in face morphing attack detection," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2022, pp. 410-418.
[75] J. M. Singh and R. Ramachandra, "Fusion of deep features for differential face morphing attack detection at automatic border control gates," in 2022 10th European Workshop on Visual Information Processing (EUVIP), 2022, pp. 1-5.
[76] S. Venktatesh, "Multilevel fusion of deep features for face morphing attack detection," in 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2022, pp. 1-7.
[77] R. Raghavendra and G. Li, "Multimodality for reliable single image based face morphing attack detection," IEEE Access, vol. 10, pp. 82418-82433, 2022.
[78] J. M. Singh and R. Ramachandra, "3D Face Morphing Attacks: Generation, Vulnerability and Detection," IEEE Transactions on Biometrics, Behavior, and Identity Science, 2023.
[79] J. Tapia and C. Busch, "AlphaNet: Single Morphing Attack Detection Using Multiple Contributors," in 2023 IEEE International Workshop on Information Forensics and Security (WIFS), 2023, pp. 1-6.
[80] P. Aghdaie, S. Soleymani, N. M. Nasrabadi, and J. Dawson, "Attention Augmented Face Morph Detection," IEEE Access, vol. 11, pp. 24281-24298, 2023.
[81] J. M. Singh and R. Ramachandra, "Deep composite face image attacks: Generation, vulnerability and detection," IEEE Access, 2023.
[82] J. E. Tapia and C. Busch, "Face Feature Visualisation of Single Morphing Attack Detection," in 2023 11th International Workshop on Biometrics and Forensics (IWBF), 2023, pp. 1-6.
[83] C.-k. Jia, Y.-c. Liu, and Y.-l. Chen, "Face morphing attack detection based on high-frequency features and progressive enhancement learning," Frontiers in Neurorobotics, vol. 17, p. 1182375, 2023.
[84] J. M. S. S. V. Ramachandra, "Robust Face Morphing Attack Detection Using Fusion of Multiple Features and Classification Techniques," arXiv preprint arXiv:2305.03264, 2023.
[85] M. Ibsen, L. J. González-Soler, C. Rathgeb, and C. Busch, "TetraLoss: Improving the Robustness of Face Recognition against Morphing Attacks," arXiv preprint arXiv:2401.11598, 2024.
[86] M. A. Ramesh, B. S. Lakshmi, D. Narendar, M. M. Najeeb, and V. Sai, "DETECTION OF FACE MORPHING USING DEEP LEARNING."
[87] R. Ramachandra, S. Venkatesh, N. Damer, N. Vetrekar, and R. S. Gad, "Multispectral Imaging for Differential Face Morphing Attack Detection: A Preliminary Study," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2024, pp. 6185-6193.
[88] Y. Han and H. J. Kim, "Face morphing using generative adversarial networks," Journal of Digital Contents Society, vol. 19, pp. 435-443, 2018.
[89] 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, vol. 8, pp. 92301-92313, 2020.
[90] F. Peng, L.-B. Zhang, and M. Long, "FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image," IEEE Access, vol. 7, pp. 75122-75131, 2019.
[91] U. Scherhag, C. Rathgeb, and C. Busch, "Towards detection of morphed face images in electronic travel documents," in 2018 13th IAPR International Workshop on Document Analysis Systems (DAS), 2018, pp. 187-192.
[92] 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.
[93] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch, "Detecting morphed face images using facial landmarks," in Image and Signal Processing: 8th International Conference, ICISP 2018, Cherbourg, France, July 2-4, 2018, Proceedings 8, 2018, pp. 444-452.

[94] J. M. Singh and R. Ramachandra, "Reliable face morphing attack detection in on-the-fly border control scenario with variation in image resolution and capture distance," in 2022 IEEE International Joint Conference on Biometrics (IJCB), 2022, pp. 1-10.
[95] M. Long, Q. Yao, L.-B. Zhang, and F. Peng, "Face De-morphing Based on Diffusion Autoencoders," IEEE Transactions on Information Forensics and Security, 2024.
[96] M. O. Kenneth, B. A. Sulaimon, S. M. Abdulhamid, and L. C. Ochei, "A systematic literature review on face morphing attack detection (mad)," Illumination of Artificial Intelligence in Cybersecurity and Forensics, pp. 139-172, 2022.
[97] U. Scherhag, C. Rathgeb, and C. Busch, "Performance variation of morphed face image detection algorithms across different datasets," in 2018 International Workshop on Biometrics and Forensics (IWBF), 2018, pp. 1-6.
[98] R. Tolosana, M. Gomez-Barrero, C. Busch, and J. Ortega-Garcia, "Biometric presentation attack detection: Beyond the visible spectrum," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1261-1275, 2019.
[99] S. Gupta, K. Saluja, A. Goyal, A. Vajpayee, and V. Tiwari, "Comparing the performance of machine learning algorithms using estimated accuracy," Measurement: Sensors, vol. 24, p. 100432, 2022.
[100] R. S. Kramer, M. O. Mireku, T. R. Flack, and K. L. Ritchie, "Face morphing attacks: Investigating detection with humans and computers," Cognitive research: principles and implications, vol. 4, pp. 1-15, 2019.