ISSN: 0067-2904

Techniques and Challenges for Generation and Detection Face Morphing Attacks: A Survey

Iman Saleem*[1], Bahja Khudair Shukr[2]
[1]*Department of Medical lab. Technology, Al-Zahrawi University College, Karbala, Iraq*
[2]*Department of Software, College of Information Technology, University of Karbala, Karbala, Iraq*

Received: 8/1/2021 Accepted: 17/4/2022 Published: 30/1/2023

Abstract:

Face recognition system is the most widely used application in the field of security and especially in border control. This system may be exposed to direct or indirect attacks through the use of face morphing attacks (FMAs). Face morphing attacks is the process of producing a passport photo resulting from a mixture of two images, one of which is for an ordinary person and the other is a judicially required. In this case, a face recognition system may allow travel of persons not permitted to travel through face morphing image in a Machine-Readable Electronic Travel Document (eMRTD) or electronic passport at Automatic Border Control (ABC) gates. In creating an electronic passport, most countries rely on applicant to submit images in a form of a document or via the Internet, and this allows applicants to manipulate the images to produce morphing images. These photos allow both beneficial and harmful partners to cross borders using the same passport. This is considered a major threat to the security systems that allow them to travel without revealing their true identity. This paper aims to provide a comprehensive overview of face morphing attacks and the development taking place in this specialty. This paper describes the techniques for generating metamorphic images and challenges they face, in addition to the advantages and disadvantages of these techniques. It also dealt with types of techniques used in detecting and determining the attack of mutant faces in the field of deep learning or machine learning, in addition to the laws and criteria for measuring the efficiency of the algorithms used. It provides a general summary of the work that has been produced in this field.

Keywords: E-passport, Morphing detection, Face recognition, Biometric, Face landmark.

تقنيات وتحديات لتوليد واكتشاف هجمات تحويل الوجه: دراسة استقصائية

ايمان سليم سامي*[1] ، بهجة خضير[2]
[1]قسم المختبر الطبي. التكنولوجيا ، كلية الزهراوي الجامعية ، كربلاء ، العراق
[2]قسم البرمجيات ، كلية تكنولوجيا المعلومات ، جامعة كربلاء ، كربلاء ، العراق

الخلاصه

نظام التعرف على الوجوه هو التطبيق الأكثر استخدامًا في مجال الأمن وخاصة في مراقبة الحدود. قد يتعرض هذا النظام لهجمات مباشرة أو غير مباشرة من خلال استخدام هجمات تحويل الوجه .(FMAs) هجمات تحويل الوجه هي عملية إنتاج صورة جواز سفر ناتجة عن مزيج من صورتين ، إحداهما لشخص

*Email: imans.alrihbawy@student.uokufa.edu.iq

عادي والأخرى مطلوبة قضائيًا. في هذه الحالة ، قد يسمح نظام التعرف على الوجوه بسفر الأشخاص غير المسموح لهم بالسفر من خلال صورة تحويل الوجه في مستند السفر الإلكتروني المقروء آليًا (eMRTD) أو جواز السفر الإلكتروني عند بوابات التحكم التلقائي في الحدود (ABC) عند إنشاء جواز سفر إلكتروني ، تعتمد معظم الدول على مقدم الطلب لإرسال الصور في شكل مستند أو عبر الإنترنت ، وهذا يسمح للمتقدمين بالتلاعب بالصور لإنتاج صور متحولة. تسمح هذه الصور للشركاء المستفيدين والضارين بعبور الحدود باستخدام نفس جواز السفر. هذا يعتبر تهديدا كبيرا للأنظمة الأمنية التي تسمح لهم بالسفر دون الكشف عن هويتهم الحقيقية. تهدف هذه الورقة إلى تقديم نظرة عامة شاملة عن هجمات تحويل الوجه والتطور الذي يحدث في هذا التخصص. يصف هذا البحث تقنيات توليد الصور المتحولة والتحديات التي يواجهونها ، بالإضافة إلى مزايا وعيوب هذه التقنيات. كما تناول أنواع التقنيات المستخدمة في كشف وتحديد هجوم الوجوه المتحولة في مجال التعلم العميق أو التعلم الآلي ، بالإضافة إلى قوانين ومعايير قياس كفاءة الخوارزميات المستخدمة. يقدم ملخصًا عامًا للعمل الذي تم إنتاجه في هذا المجال.

1. Introduction

Biometrics has been used very heavily in the field of security. Biometrics are measurements related to human characteristics that have played a major role in the field of computer science and have been used in the field of identification, data security and access control technologies [1, 2, 3]. Previously, identification systems depended on symbols such as a password or a personal identification number for each individual, but it led to many problems. It is very easy for anyone to impersonate another person by simply knowing their number or password, so the trend towards biometric identifiers has increased, which is considered more reliable. Identification is the most common area in the use of Biometrics because it contains unique and powerful information capable of identifying people well, which represents the fingerprint, iris, face, hand geometry, retina, DNA, and palm veins, as well as skin color [4, 5].

Recognizing faces from biometrics, which has taken a large space in the field of identification locally and globally, because faces are rich in information and differ greatly from one person to another. Facial recognition systems are widely used in security and service departments, such as international airports, the field of businesses, social media companies on the web, mobile phones, and other fields [6, 7]. The face recognition system has become of great interest to researchers to reach a system that has a great ability to identify, despite the similarity between people [8]. International airports are among the domains that are most interested in facial recognition system for travelers. The faces in the passport are compared with the real face of the traveler. Used facial digital identity information from an electronic Machine-Readable Travel Document (eMRTD). How does that happen? Airports have surveillance cameras that take pictures of people traveling and this live image is compared with a picture of the same people previously stored in the eMRTD when a passport application was submitted. The comparison process is done through face-based identity verification systems. The system will either issue an accept if the two images are identical according to a certain threshold limit or give a rejection if the result is less than the threshold limit [10, 11]. In addition, there is a manual verification step between a person himself and a copy of the passport by the person checking the passport and responsible for the transit of travelers(passport officer). The image taken for the traveler must not contain any problems to be distinguished correctly. The traveler must take a straight position and exclude hair from the face, in addition to opening the eyes and not wearing glasses, also not wearing masks [10, 11, 12].

But years ago, a problem arose in one of the European countries. A person required to justice could travel using a faked passport (impersonating an individual is not required for

justice), despite using the same manual and electronic verification. This revealed that the facial recognition systems used are unable to identify precisely and need to be updated by adding new algorithms and new techniques. The reason for this is that the stored image eMRTD contains modifications, which means when creating a passport, two photos of the traveler and another person are combined, resulting in an image that contains part of the first person and part of the other person. This condition is called a morphing face [13, 14]. Figure 1 represent morph image.

Figure 1: Morphing face in the center from right and left images.

What are the most exposed places to morph process? and why? International airports are most used of facial recognition systems, which are subject to a morph attack, and they are the most dangerous places because through them the passport image is falsified and people who are not authorized to travel are allowed to travel without detection through a monitor or facial recognition system [3]. The problem occur during the passport application process. The rate of forgery may be decreased in two cases: When a specific person wants to have a passport, either a direct photo of the traveler is taken and added to the passport, or the identification systems are modified and developed to be able to detect the face morphing [15].

Photographs of travelers are stored in the eMRTD while applying for a passport. Photos came by two forms, either in printed form or sent via web platforms. Both cases enable the person to manipulate the image. This morphing process is interesting to judicially wanted persons so it allows them to travel easily across international borders [16,17]. Figure 2 represent morph process.

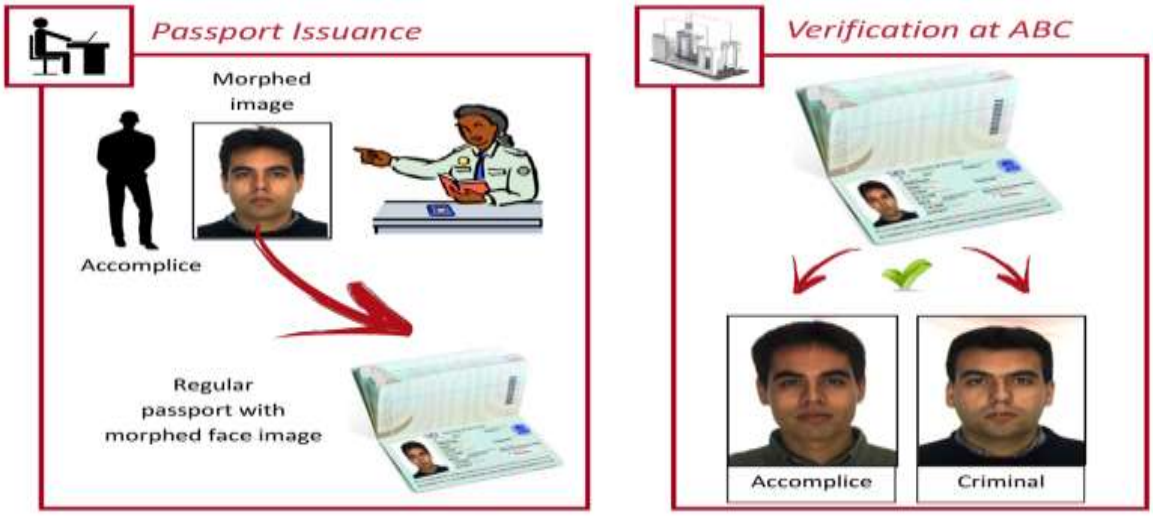

Figure 2 : An example explains morphed images in border control scenario.

Morphing face has a great potential for optical as well as electronic illusion. Therefore, work has been done in this field in recent years to reduce this problem, as many researches

have focused on the use of new devices and technologies or modification of previous systems [18]. The rest of the paper is organized as follows: The second section includes challenges facing face morphing and faces recognition systems. Discusses face morphing and generation presented in the third section. While the fourth section introduces discusses face morphing techniques, and finally the conclusions.

2. Challenges Facing Face Morphing and Face Recognition System

A. The process of creating a morphing image faces many challenges, including [13, 19]:

1. Using more than one image for several people and producing face morphing is difficult because the differences in the image textures and features will increase.
2. When two images are used to produce one image, distortion may occur in the image and needs to be modified.
3. The two images used to produce the face morphing must be close together and not completely different. When they are different, the difference will be visible in the image and easy to detect.
4. Two images must be taken under the same conditions to reduce the contrast between them.

B. Face recognition systems face some challenges that make them give incorrect results:

1. The great similarity between face morphing and the traveler's face gives a large matching ratio and thus the traveler can pass across the border.
2. The modifications that someone makes to the facial features or the deformations that may affect a person as a result of an accident may give a mismatch between the traveler's photo and the passport photo, even though it belongs to the same person.

3. Face Morphing Attack and Generation

This section includes an explanation of face morphing and methods of generating it:

3.1 Face Morphing Attack

The morphing process can be expressed as the process of merging two images to produce a new image, and this resulting image gives a large proportion of matches for the first image and the second image as a result of manual or automatic changes. Both images were taken for the face region to produce another face image similar to both images [20]. The figure below shows the ratio of images morphing and truth in the faces recognition system [6].

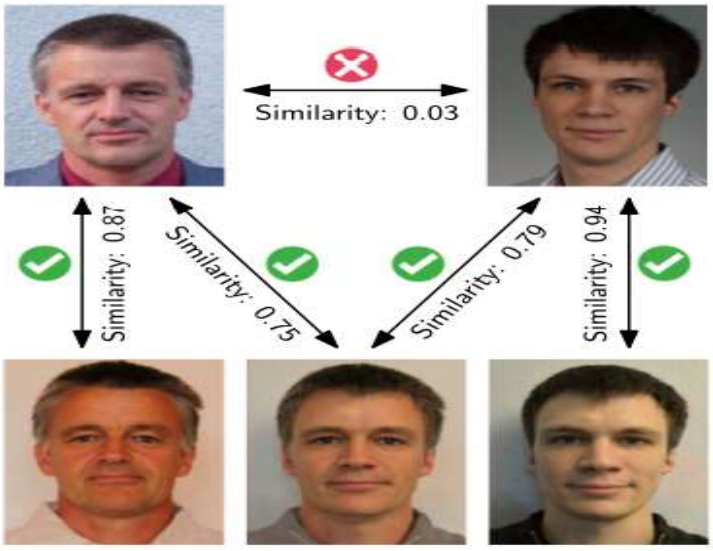

Figure 3: Effect of face morphing on face recognition system. As known in the figure, the morphed image can be equally verified against both contributing subjects with a high similarity score from FRS.

3.2 Generation Face Morphing

The process of creating face morphing consists of those steps [21]:

1. Preprocess both images before morphing to have the same effect.
2. Defining the features of the face (face landmarking) from the nose, eyes, mouth, roundness of the face, and some inserting the ear within it.
3. Action align and warp for the two images.
4. Combine two images with one image (image blending).
5. Subsequent processing after merging the two images to remove artifacts.

A morphing image is generated in two ways, either manually or automatically. Figure 4 explain techniques morphing [3].

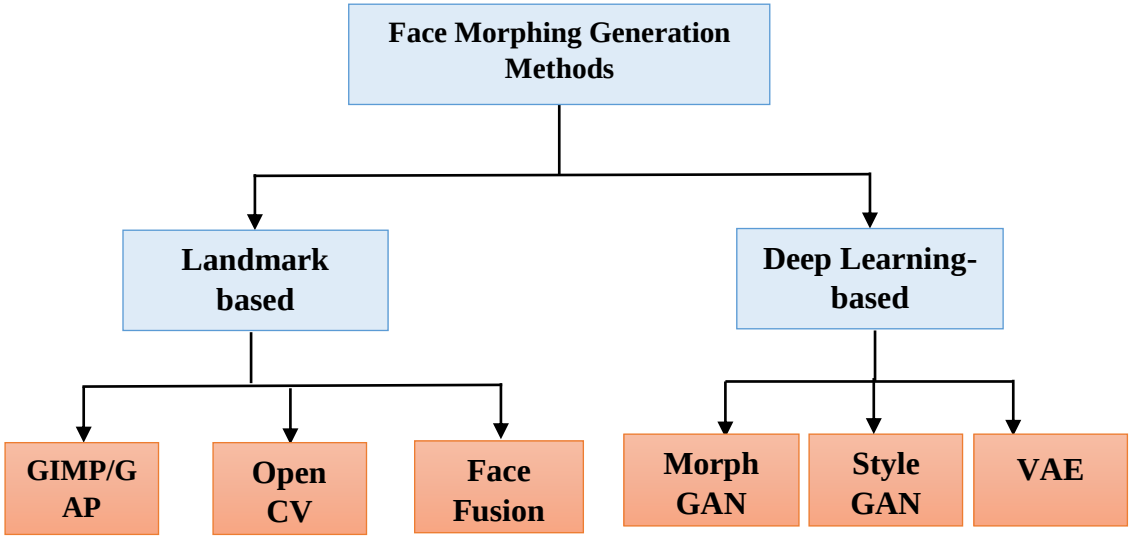

Figure 4: Techniques use in generation face morphing.

(a) Landmark-based: Many programs can be used to create a fake image quickly and accurately. Most of these programs are free, such as Morph Thing, 3Dthis Face Morph, Face Swap Online, Abrosoft Fanta Morph, Face Morpher, and Magic Morph. These programs create good or bad images because they need time and manual intervention to remove the artifacts [22].

(b) Deep Learning-based: Deep learning has gained a great and increasing interest in recent years and has become a very wide field of application in various disciplines because of its different advantages and great benefits represented by speed and accuracy. Generative models are one of the deep learning tools that have gained interest due to the amazing results they give in this field. The results it provides depends on the huge amount of data it use, the structure and design of the network and the training technique. Better results will be amazing and very close to reality in terms of content. Content can be images, sounds, or text. There are two notable families in this field that have received a lot of attention [23, 24, 25]:

- Generative Adversarial Networks (GANs).
- Variational Autoencoders (VAEs).

Generative Adversarial Networks (GANs): It is the first family belonging to deep learning that has the ability to produce fake data that is very similar to the real data on which it has been trained [26].

A GAN consists of two networks models:

- Generator: It represents the first part of the GAN that takes the training data and turns it into a vector of random values and generates new data from it with the same pattern as the input data.
- Discriminator: The data generated from the first part must contain a difference and contain some observations. This section tries to classify the data that is entered as real or generated.

Variational Autoencoders (VAEs): VAE is the second family that relies heavily on deep learning that also produces outputs similar to the input data and has the same characteristics. It is mainly based on the Probability Density Function (PDF). Both the first and second families are unsupervised learning, which increases their importance in data generation. This network has two parts, encoding and decoding, and both parts are a neural network. The cipher part takes the entered data and turns it into a vector with its properties in the form of mean and stander division. This vector is as an input to the decoding part, and it generates data from it similar to reality. The training relies on the reconstruction loss and the Kullback-Leibler (KL) divergence between the distributions of the latent variables and independent standard normal distributions. [27]. Component of VAE: (Input, Encoder, Latent Vector (Z) (mean $ standard division), Decoder, Output). Table 1 explain advantages and disadvantages for morphing techniques.

Table. 1: Presents the advantages, disadvantages, and challenges of each techniques generate face morphing.

Face Morph Generation Method	Advantages	Disadvantages	Challenges
Landmarks Based	1. The conversion process takes place easily and automatically, just select the images to be morphed 2. The programs used are freely available and generate high-quality images, in addition to the fact that it takes a little time to create many morph images	1. Sometimes it needs manual interventions to remove artifacts 2. The resulting image contains contrast that require post-processing.	1. Variability Usually individuals are different in terms of facial features, these differences are considered challenges in addition to the external differences of the image in terms of camera accuracy, location, as well as lighting. 2. Acquisition conditions: The generation of faces is affected by the background and illumination of the image as well as its resolution. It is not limited to these only and is affected by the expressions, the type of database chosen, the model used in the generation, as well as occlusion. 3. It depends on the landmarks taken from the faces, the more the better, in addition to its accuracy.
	1. Images are generated	1. Requires careful	1. Number of Images in

Deep Learning-based	automatically without human intervention and in high quality. 2. Images do not have double edges	selection of data. 2. The process of preparing the network parameters to obtain good results is difficult and requires experiments to reach the optimal parameters.	Database. 2. Type of Images (size of image, resolution, illumination, the convergence of pictures that include the ages of people's gender).

The following, Table 2, shows some of the work that used different databases [3]:

Table 2: Morph face image database.

Reference	Generation Type	Generation Method	Bonafide & Morph
F. Matteo et al. [28]	Landmark method	GIMP GAP	No. of Morph image : 80
Remacgandra et al. [29]	Landmark method	GIMP GAP	No. of Morph image: 450
M. Andrey et al. [24]	Landmark method	Automatic generation (dlib landmark)	Complete No. of Morph image: 1326, Splicing No. of Morph image: 2614
Scherhag et al. [11]	Landmark method	GIMP GAP	No. of Bonafide image: 462 No. of Morph image: 231
Remacgandra et al. [30]	Landmark method	GIMP GAP	No. of Bonafide image: 1000 No. of Morph image: 1423+1423
G. B. Marta et al. [31]	Landmark method	GIMP GAP	No. of Morph image: 840
Dunstone [32]	Landmark method	GIMP GAP	No. of Morph image: 1082
Damer et al [33]	Deep learning-method	GAN	No. of Morph image: 1000
Remacgandra et al [34]	Landmark method	GIMP GAP	Bonafide: 1272 & Morph: 2518
Scherhag et al. [35]	Landmark method	OpenCV, FaceFusion, Face Morpher	No. of Bonafide image: 791+3298 Morph: 791+3246
V. Sushma et al. [23]	Deep learning-method	Style GAN	No. of Bonafide image: 1270 Morph: 2500
Raja et al. [36]	Landmark method	UBO Morpher	No. of Bonafide: 300+1096 Morph: 2045+3073
N. Mei et al. [37]	Landmark method	Automatic method of generation	morph image with Low-quality: 1183 Automated morph: 39113 morph image with High-quality: 492
Clemens et al. [38]	Deep learning-method	GAN	All image:1250
Rien Heuver. [25]	Deep learning and Landmark methods	PCA & VAE	N0. of Morph image: 249

4. Face Morphing Detection Techniques

Due to the limited ability of humans to detect morphed images as well as the facial recognition systems used today, morphing detection has become important to work on using new technologies or fixing bugs of previous systems. The detection techniques used vary depending on whether the travel passport image is a document image or a live image.

Algorithms and methods of detection work to search for the differences between the two images and focus on the key points that represent the basic changes between faces.

It is necessary to conduct experiments for fake images on face recognition systems to measure their efficiency in identifying the correct person. Samples were taken and studied, whereby the efficiency was measured by the matching performance is measured Morph Acceptance Rate (FAR) and False Rejection Rate (FRR). The word acceptable means to us that the two pictures are similar, the observer sees both the traveler and the passport picture are identical, and be rejected when they do not match. As for the AFR system, it shows us the word "accepted" in the event that the image of the passport and the photo of the traveler is equal to or exceeds the threshold, and if it is less, it will be rejected [39, 40].

$$FAR = \frac{|Accepted\ morphs|}{|All\ morphed\ images|} \quad (1)$$

$$FRR = \frac{|Rejected\ genuine\ individuals|}{|All\ genuine\ individuals|} \quad (2)$$

$$ACC = \frac{|Correctly\ classified\ images|}{|All\ classified\ images|} \quad (3)$$

The process of detecting the transformed face previously was based on a personal comparison by the security officer, so the traveling person and his photo in the passport are looked to see if they are similar or not. In addition, they used facial recognition systems through programs based on machine learning algorithms, and then developed and became based on deep learning [3]. A threshold is usually set for measuring outcomes. The methods for detecting face morphing are divided into three sections, according to the diagram below (Figure 5) [3]:

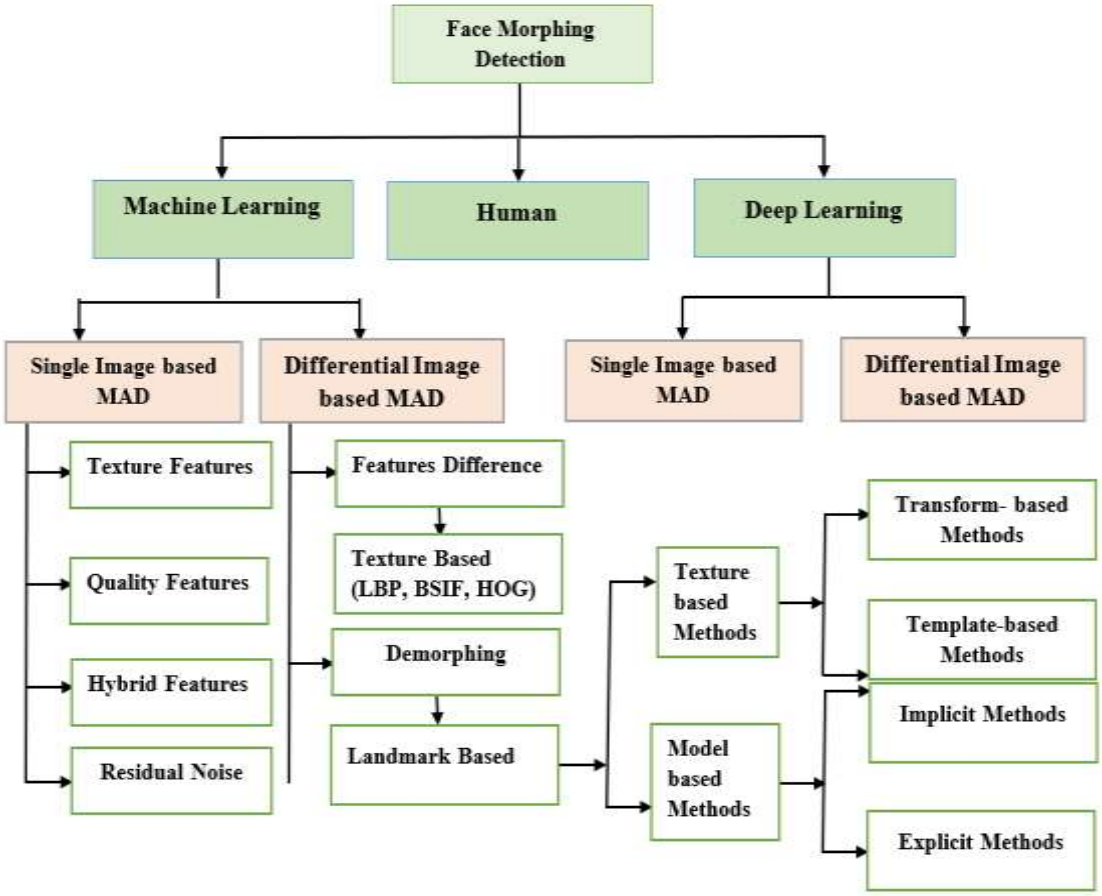

Figure 5 illustrate techniques using in FMD.

Both deep learning and machine learning techniques rely on the detection process in two ways: single image S-MAD (Single Morphing Attack Detection) or difference image D-MAD (Differential Morphing Attack Detection).

4.1 Single Image Based MAD (S-MAD or No-Reference)

Most countries are not subject to direct supervision in creation of the official travel document, where applicant is asked to send an image of his/her face and based on which the passport is formed. Therefore, this matter allows the applicant to manipulate the photo with great accuracy and without errors through the use of morphing techniques. The input to the face morphing attack detection algorithm is a single image. In this case, the applicant of the passport submits a photo of his/her face, and this photo will be examined whether is it suspicious or not? S-MAD is the most difficult type because it is based on a single image without the availability of the actual image [21, 41].

An additional challenge besides digital images, the scanned images. Because in some countries they rely on scanned images. Digital images often contain remnants of the morphing process. As for images, scanning often contains noise attached to the image, so it will add a huge challenge. Table 3 explain these techniques from where advantage and disadvantage and Table 4 deals some work within this field.

(a) Texture Features Based S-MAD: These algorithms involve focusing on the texture of the image. It is known that each image has a different texture from the other, so it can be distinguished and detected by texture. There are many algorithms that work on analyzing the texture of the image such as Binarized Statistical Image Features (BSIF), Local Binary Patterns (LBP), Gray Level Co-occurrence Matrix (GLCM).), Hybrid color local binary patterns, Binary Gabor pattern. The most widely used algorithms in detecting mutant face, especially scanned ones, are color textures (LBP), deep learning, (BSIF) [29, 42, 43,44].

(b) Deep Learning-Based S-MAD: Because of the great success achieved by deep learning, it has been invested in this specialty to reveal the faces of morphing. Many networks are designed to train a set of images data. These networks deal with the input data that are images. It is possible to take advantage of morphed images as an input to this network. Such as networks (AlexNet, VGG-19, VGG-16, ResNet101, ResNet50, GoolgleLeNet, DenseNet) [45, 46, 47].

(c) Quality-Based S-MAD: This technique focuses on the quality of images, meaning that it analyzes the features related to image quality by determining whether an image contains artifacts or may be degraded and this is the result of manipulating the image and changing it. This technique can reveal that it is a morphed image simply if it contains distortions or deterioration. Among the features that can be analyzed using this technique are image Response NonUniformity (PRNU), reflection analysis, meta information, corner and edge distortions. Despite this technique, it performs well in detection, but this is due to the situation of the image. If the morph process is good, it will be difficult to detect or analyze it [48, 49].

(d) Residual Noise Based S-MAD: It is also known that the morph process focuses on transport the parts between two images (two face images). There must be changes between the two images in terms of skin color or in terms of the dimensions of the features, so there will be a difference in the pixel values, as this generates noise in the image. This technology is based on the detection of the transformed face through the noise output from the transformation. The general principle of this technique is to extract the parts that contain noise by subtracting the transformed image from the image itself without noise. But this technique

requires the presence of the original image without noise, and it had a great ability to detect. This technique was used for the first time with deep knowledge in removing the noise generated in the images generated by the CNN algorithm [50, 51].

(e) Hybrid Based S-MAD: This technique is based on extracting facial features from multiple techniques and merging them to make it a single technique. This method has been used a lot and it has given good results due to the features that have been extracted with many method. This combination makes it a powerful technology compared to other techniques that rely on a single method of feature extraction. But it requires a high cost in addition to the time spent [52, 53].

Table. 3 Explain advantages and disadvantages for S-MAD techniques [3].

Features Type	Advantages	Limitations
Texture Features	- Simple to execution. - Less cost. - More effective digital data and good detection.	- Not working well for data scanning. -The accuracy of the images is affected, especially if the resolution is low.
Image Quality Features	- Simple to execution. - Less cost. - Use with various digital data and scanner.	- Its performance is variable for the same data type in the case of digital or scanner. -Affected by compressed data.
Hybrid Features	-Good at detecting different types of morph images, whether digital or scanner. -It has generalizability. -Extract different features each time.	-The implementation process is difficult and requires effort to integrate the methods and find good parameters that fit the detection. -High cost.
Residual Noise Features	- Simple to execution. - It requires less computing cost. -It has high performance for digital data -It has the ability to generalize despite the different resolutions of the images	- It is sensitive to image compression and deals with digital images only -It cannot detect well if the conversion process has no noticeable noise
Deep CNN features	- It performs well for both types of digital images and scans.	-The training part requires a high cost. -It requires a large database for different types of face and different movements.

Table 4: Some Related works for S-MAD techniques.

Reference	Approach	Algorithm	Database
Raghavendra et al. [29]	Texture Method	Many techniques: LBP with SVM, BSIF with SVM, Image Gradient with SVM	Digital Images
Makrushin et al.[54]	Quantized DCT coefficients	Benford features	Digital Images
N. Tom et al. [55]	Image degradation Method	Corner feature detector	Digital Images
S. Clemens et al. [56]	Deep learning Method	Many Deep Neural Network: VGG19 Net, Google Net, Alex Net	Digital Images
Remachandra et al. [57]	Texture Method	color textures , BSIF , LBP, LPQ,	Print/Scan
A. Aras et al. [58]	Texture Method	Topological data analysis method	Digital Images
S. Ulrich et al. [59]	Texture and frequency Method	LBP, LPQ, BSIF, 2DFFT with SVM classifier	Digital Print/Scan
K. Christian et al. [60]	Texture Method	Media forensics	Digital Images
Remachandra et al. [61]	Deep CNN	Feature fusion of fully connected layers of VGG19 and Alex Net	Digital Print/Scan

K. Christian et al. [62]	Image life cycle model	Key points (SIFT, SURF, ORB, FAST, AGAST) and loss of edge operators (canny and Sobel)	Digital Images
H. Mario et al. [63]	Stirtrace Method	Multi-compression anomaly detection	Digital Images
D. Luca et al. [48]	Image degradation	Photo Response Non-Uniformity (PRNU)	Digital Images
Remachandra et al. [64]	Steerable features	Luminance component extraction	Print/Scan
H. Mario et al. [65]	StirTrace	StirTrace face morph forgery detection	Print/Scan images
S. Clemens et al. [66]	Image degradation	Specular reflection	Digital Images
Makrushin et al. [67]	Quantized DCT coefficients	Features extracted for Benford from quantized DCT coefficients	Digital Images
N. Tom et al. [68]	Morph pipeline footprint detector	Features extracted for Benford from quantized DCT coefficients	Digital Images
S. Luuk et al. [69]	Texture based approach	LBP-SVM, Down-up sampling	Digital Images
S. Ucicrtlunldcus et al. [70]	D-MAD Feature difference- 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. [71]	MAD Multidetector fusion	LBPH, Transferable deep-CNN Digital	Digital Images
F. Matteo et al. [72]	Deep learning	Many Deep Neural Network: AlexNet, VGG19, VGG-Face16, VGG-Face2	Print/Scan
S. Uirich et al. [73]	multi-algorithm fusion	feature extraction through four techniques: 1. Texture descriptor using (LBP, BSIF), 2. Keypoint extractors using (SIFT, SURF) 3. gradient estimators (HoG) 4. Deep neural network	Digital Images
D. Luca et al.[74]	PRNU	Merge two method DFT magnitude histogram with PRNU DFT's energy.	Digital Images
S. Clemens et al. [75]	Complex multi-class pre-training	VGG-19 network.	Digital Images

4.2 Differential Image-Based MAD (D-MAD)

In this approach, the morphing image is detected by comparing the passport image and the traveler's image (live image). This is an easier approach than the previous approach, less challenging, and more reliable to ensure a direct image of the traveler's face. Table 5 explain techniques D-MAD and Table 6 explain some works within this field [6].

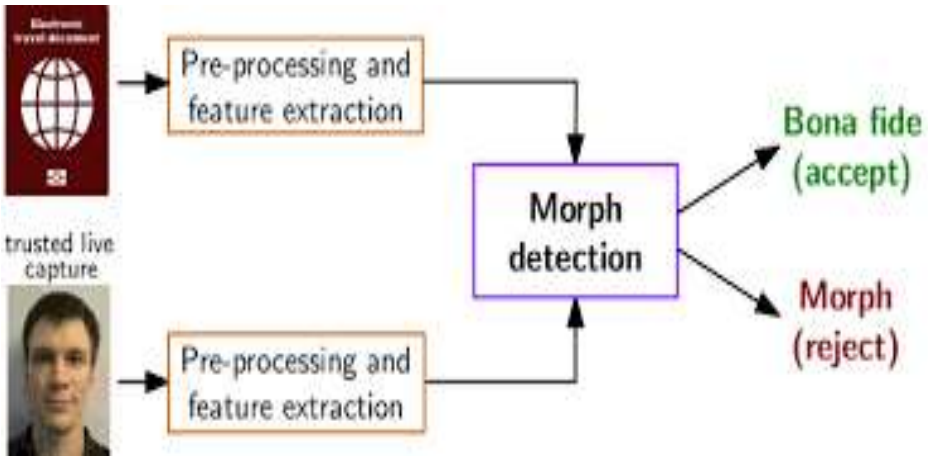

Figure 6: example for D-MAD.

(a)Feature Difference Based D-MAD: The principle on which this type is based is to find the difference features between two images. The features are calculated for the passport photo of the suspect and the live photo features of the same person and then find the difference between the features to detect the morph attack. In other words, relying on the difference between the features and finding that ratio if it is large, meaning the two people are different, and if it is small, it is considered the same person. Many techniques are used in this field where you extract the features from texture, gradient, deep feature and landmark points [76, 77].

(b) Demorphing Based D-MAD: This technique relies on detection faces completely automatic, until in case the merging of more than one image to form the transformed image. This technology is powerful, modern and has good results based on deep learning that is CNN. The results of this method are affected by the quality of the captured images as its performance is poor and deteriorated when the image is affected by lighting and noise factors when the live image of the intended person is captured at ABC gates. The table below illustrates the advantages and limitations of D-MAD-based techniques [78, 79].

Table 5: Explain advantages and Limitations for M-MAD techniques.

Algorithm type	Advantages	Limitations
Feature difference	- Simple to execution. - The possibility of detection is acceptable for images, although they vary in accuracy.	- Big computational cost -Image detection is affected by the type of data used and the characteristics extracted
Demorphing	- Simple to execution. - The required data is restricted and high detection accuracy. Where it has the ability to visualize the face if the suspected image was converted.	-Detection is affected by facial positions and shooting conditions in terms of facial movement and lighting differences.

Table 6: Some Related works for D-MAD techniques.

Reference	Detection Type	Approach Algorithm	Database
F. Matteo et al. [80]	Demorphing method	image subtraction using (Demorphing)	Scan Images
F. Matteo et al. [80]	Demorphing method	Verification of Face image	Digital Images
S. Ulrich et al. [81]	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
U Scherhag et al. [82]	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. [71]	Multi detector fusion	Transferable deep-CNN, LBPH	Digital Images
J M Singh. [83]	Deep learning	SfS Net and Alexnet	Digital, Scan Images
D. Naser et al. [77]	Landmark shift	shift representation and Landmark of face detection	Digital Images
P. Fei et al. [79]	GAN using for Face restoration	Symmetric dual network architecture	Digital Images
S. Ulrich et al. [35]	Deep Face Representation	ArcFace Network, FaceNet algorithm	Digital, Scan Images
S. Clemens et al. [75]	Deep Learning	Layer Wise Relevance Propagation (LRP)	Digital Images
O. Delcampo et al. [78]	Deep CNN, Demorphing method.	Auto-generation (encoders).	Digital, Scan Images

Landmark based: Facial features are the most important part of the human body to distinguish one person from another. Common facial features in Table 7. These features are considered essential points and have complete significance for the face that can be considered as a reference for identification. Figure 7 represent landmark dependent tasks.

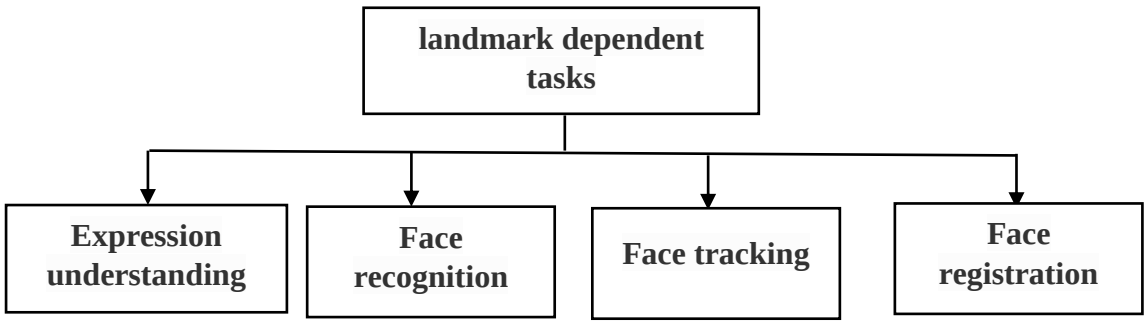

Figure 7: landmark dependent tasks.

Table 7: Explain primary and secondary landmarks.

Primary the Features (landmarks)			Secondary the Features (landmarks)		
No.	**landmarks**	**Direction**	**No.**	**landmarks**	**Direction**
16	Eyebrow	Left (outer corner)	1	Temple	Left
19	Eyebrow	Left (inner corner)	8	Chin tip	-
22	Eyebrow	Right (inner corner)	2-7, 9-14	Cheek contours	-
25	Eyebrow	Right (inner corner)	15	Temple	Right
28	Eye	Left (outer corner)	16-19	Eyebrow contours	Left
30	Eye	Left (inner corner)	22-25	Eyebrow corners	Right
32	Eye	Right (inner corner)	29, 33	Eyelid corners	Upper
34	Eye	Right (outer corner)	31,35	Eyelid corners	Lower
41	Nose tip	-	36, 37	Nose saddles	-
46	Mouth corner	Left	40, 42	Nose peaks	-
52	Mouth corner	Right	38-40, 42-45	Nose contours	-
63, 64	Eye centers	-	47-51, 53-62	Mouth contours	-

1) Expression understanding: Facial expressions are another way to express a person's feelings, but in a non-verbal way, and this has a great role in dealing with people who are unable to speak. These expressions, such as the movement of the head, mouth, and eyes, can be analyzed in classifying the reaction of people. For each movement, there is a specific indication [85].

2) Face recognition: This part is used a lot in the field of security. It usually deals with the face as a set of comprehensive features for the face. Features are extracted without specifying the eye, nose or mouth area, but rather depend on the features of the face in general, where the face is seen as one area [86].

3) Face tracking: In this type, the contours of the face are tracked with movement. Through it, it is possible to track the presence of a human face in the video and to sense the movements and gestures of the head and face, and extract from them indications that can be interpreted and benefited from, especially in the field of security. This technique is important and can be used in cases related to the Internet or not. Through it, it is possible to analyze the face and identify it, calculate the number of people in the video, or know the facial expressions and feelings that it shows [87].

4) Face recording: Face recognition systems are becoming more important and more capable of diagnosing when using face recording. It represents a video that contains many frames that take different situations for a person. A person can be accurately distinguished because a system has several snapshots of a person and different movements [88].

Landmark approach

a) Texture-based methods: This model consists of two parts, which are transform-based, the image is divided into blocks and the features are extracted from each block, so all the features are grouped into a vector called the features vector. of the algorithms used in this part (PCA, Gabor transform, Discrete cosine transform, Independent component analysis, Landmark initialization heuristics). The feature vector compares with the patterns it has learned. The other part is template-based. Here, the feature template selects the target parameter by

examining the image according to the strength of the model matching response. of the algorithms used in this part (Fixed templates, Deformable templates) [89].

b) Model-based methods: This model consists of two parts:

- Implicit model-based: The methods used in this section are based on models without case information. The goal of this type is to deal with the spatial value of the pixel, meaning the dependence on the color intensity of the image. Where it takes the pixels that represent the gray level of the image as an input to the neural network in order to discover and identify the features of the face in the image, so it tries to find the spatial relationships in the face between landmarks points. Genetic algorithm may be one of the algorithms used in this field.

- Explicit model-based: This part is represented by the methods that take a field in the graph. Most of the algorithms used in this part depend mainly on the active appearance of the graph. The algorithms used in this part (Graph methods, Two-tier graph methods, Active shape and appearance models).

5. Conclusions

As it is known, faces have become one of the most widely used vital characteristics at the present time, as they contain many unique information that help in determining identity. Despite the power of the systems used to recognize faces, it is possible to be exposed to attacks that are face-shifting attacks. Many algorithms have been designed, in addition to new techniques to modify existing face systems, to make them able to detect mutated faces. It has conducted a lot of research in this field. Currently, the trend has increased to transform deep learning, which plays a very important role in the field of image recognition. Work is still underway in this field because there are many gaps that need to be filled and constantly updated for the systems. This paper provides a summary of the techniques and challenges faced by mutant face recognition systems, as well as how to generate such data in the two methods of machine learning and deep learning, and indicated the advantages and disadvantages of each. Research is still ongoing in this regard. It is possible that this paper will be a suitable reference for those who want to work in this field to give them a summary of the latest technologies used.

References

[1] B. Jain and I. Bansal, "E-Handbook," 2019. [Online]. Available: www.a2ztaxcorp.com

[2] V. Arulalan, V. Premanand, and G. Balamurugan, "An overview on multimodal biometrics," International Journal of Applied Engineering Research, vol. 10, no. 17, pp. 37534–37538, Sep. 2015.

[3] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face Morphing Attack Generation & Detection: A Comprehensive Survey BioMobile View project RESPECT-reliable, secure and privacy preserving multi-biometric person authentication View project Face Morphing Attack Generation & Detection: A Comprehensive Survey", doi: 10.13140/RG.2.2.11773.79849.

[4] O. A. Aghzout, J. Ruiz-Alzola, R. de Luis-Garcã, C. Alberola-Lã Opez, and O. Aghzout, "Biometric identification systems Biometric identiÿcation systems," Signal Processing, vol. 83, pp. 2539–2557, 2003.

[5] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," Journal of Pattern Recognition Research, vol. 7, no. 1, pp. 116–139, 2012.

[6] 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.

[7] D. N. Parmar and B. B. Mehta, "Face Recognition Methods & Applications." [Online]. Available: www.ijcta.com

[8] M. Keshavarz and S. Khosravi, "At The Border The Magic of Borders." [Online]. Available: https://www.e-flux.com/architecture/at-the-border/325755/the-magic-of-borders/

[9] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of Image Alterations on Face Recognition Accuracy," In Bourlai, T. (ed.) Face Recognition Across the Electromagnetic Spectrum, pp. 195–222, 2016.

[10] U. Scherhag et al., "On the vulnerability of face recognition systems towards morphed face attacks Biometrics View project BATL: Biometric Authentication with Timeless Learner (IARPA-BAA-16-04) View project On the Vulnerability of Face Recognition Systems Towards Morphed Face Attacks," 2017.

[11] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," ACM Comput Surv, vol. 50, no. 1, Mar. 2017.

[12] Wandzik, L., Kaeding, G., & Garcia, R. V. (2018, September). Morphing detection using a general-purpose face recognition system. In 2018 26th European Signal Processing Conference (EUSIPCO) (pp. 1012-1016). IEEE.

[13] 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 (Switzerland), vol. 11, no. 7, Apr. 2021.

[14] U. M. Kelly, L. Spreeuwers, and R. Veldhuis, "Improving Deep-Learning-based Face Recognition to Increase Robustness against Morphing Attacks,", In 9th International Conference on Signal, Image Processing and Pattern Recognition, Dec. pp. 1–12, 2020.

[15] R. S. S. Kramer, M. O. Mireku, T. R. Flack, and K. L. Ritchie, "Face morphing attacks: Investigating detection with humans and computers," Cogn Res Princ Implic, vol. 4, no. 1, pp. 1–15, Dec. 2019.

[16] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl, "Detection of Face Morphing Attacks Based on PRNU Analysis," IEEE Trans Biom Behav Identity Sci, vol. 1, no. 4, pp. 302–317, Oct. 2019.

[17] Department of Internal Affairs (DIA), NZ. https:// www.passports.govt.nz/passport-photos/passport-photo-requirements/.

[18] 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," Cogn. Res. Princ. Implicat., vol. 3, no. 1, p. 27, Jun. 2018.

[19] M. O. Oloyede, G. P. Hancke, and H. C. Myburgh, "A review on face recognition systems: recent approaches and challenges," Multimed Tools Appl, vol. 79, no. 37–38, pp. 27891–27922, Oct. 2020.

[20] C. Seibold, A. Hilsmann, and P. Eisert, "Reflection Analysis for Face Morphing Attack Detection," In 26th European Signal Processing Conference (EUSIPCO), (pp. 1022-1026). Jul. 2018, [Online]. Available: http://arxiv.org/abs/1807.02030

[21] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Single image face morphing attack detection using ensemble of features," in Proceedings of 2020 23rd International Conference on Information Fusion, FUSION 2020, Jul. 2020.

[22] 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 Biom, vol. 9, no. 6, pp. 278–289, Nov. 2020.

[23] S. Venkatesh, H. Zhang, R. Ramachandra, K. Raja, N. Damer, and C. Busch, "Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs? - Vulnerability and Detection," in 2020 8th International Workshop on Biometrics and Forensics, IWBF 2020 - Proceedings, Apr. 2020.

[24] A. Makrushin, T. Neubert, and J. Dittmann, "Automatic generation and detection of visually faultless facial morphs," in VISIGRAPP 2017 - Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, vol. 6, pp. 39–50, 2017.

[25] R. Heuver, "Generating facial morphs through PCA and VAE 1." [Online]. Available: https://github.com/rienheuver/VAE-morpher

[26] O. Mogren, "C-RNN-GAN: Continuous recurrent neural networks with adversarial training," Nov. 2016, [Online]. Available: http://arxiv.org/abs/1611.09904

[27] X. Hou, L. Shen, K. Sun, and G. Qiu, "Deep Feature Consistent Variational Autoencoder," Oct. 2016, [Online]. Available: http://arxiv.org/abs/1610.00291

[28] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch, "Detecting morphed face images using facial landmarks," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10884 LNCS, pp. 444–452, 2018.

[29] P. Aghdaie, B. Chaudhary, S. Soleymani, J. Dawson, and N. M. Nasrabadi, "Detection of Morphed Face Images Using Discriminative Wavelet Sub-bands," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.08565

[30] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in IEEE International Joint Conference on Biometrics, IJCB 2017, pp. 555–563 2018-January.

[31] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, "Is Your Biometric System Robust to Morphing Attacks?" [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-

[32] Università degli studi Roma tre, European Association for Signal Processing, IEEE Signal Processing Society, and Institute of Electrical and Electronics Engineers, EUSIPCO 2018 : 26th European Signal Processing Conference : Rome, Italy, September 3 - 7, 2018.

[33] N. Damer, A. M. Saladie, A. Braun, and A. Kuijper, "MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network," in 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems, BTAS 2018, Jul. 2018. doi: 10.1109/BTAS.2018.8698563.

[34] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch, "Detecting Face Morphing Attacks with Collaborative Representation of Steerable Features."

[35] 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, doi: 10.1109/TIFS.2020.2994750.

[36] 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.

[37] 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, March 2020.

[38] C. Seibold, W. Samek, A. Hilsmann, P. and Eisert, "Detection of face morphing attacks by deep learning," In International Workshop on Digital Watermarking (pp. 107-120). Springer, Cham, (2017, August).

[39] ISO/IEC 30107-3:2017, Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting, 2017.

[40] 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) (pp. 1017-1021). 2018.

[41] 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, doi: 10.1109/ACCESS.2021.3136485.

[42] D. G. Lowe, "Object Recognition from Local Scale-Invariant Features," 1999.

[43] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," Pattern Recognit, vol. 29, no. 1, pp. 51–59, Jan. 1996, doi: 10.1016/0031-3203(95)00067-4.

[44] V. Ojansivu and J. Heikkilä, "Blur Insensitive Texture Classification Using Local Phase Quantization."

[45] M. Ferrara, A. Franco, and D. Maltoni, "Face morphing detection in the presence of printing/scanning and heterogeneous image sources," IET Biom, vol. 10, no. 3, pp. 290–303, May 2021, doi: 10.1049/bme2.12021.

[46] 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.

[47] 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.

[48] 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.

[49] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," Proceedings - 2017 5th International Workshop on Biometrics and Forensics, IWBF 2017, May 2017.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] T. Neubert, "Face morphing detection: An approach based on image degradation analysis," In International Workshop on Digital Watermarking, pages 93–106, 2019.

[56] 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.

[57] 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.

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

[59] 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.

[60] 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, IHMMSec '17, pages 21–32, 2017.

[61] 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.

[62] 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, IHMMSec '17, page 21–32, New York, NY, USA, 2017. Association for Computing Machinery.

[63] 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.

[64] 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.

[65] 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.

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

[67] 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, IHMMSec '18, pages 49–54, 2018.

[68] T. Neubert, C. Kratzer, 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.

[69] 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.

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

[71] 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 22th International Conference on Information Fusion (FUSION), pages 1–8, 2019.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] M. Singh, R. Raghavendra, K. B. Raja, and C. Busch, "Robust morphdetection 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

[77] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhorst, 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.

[78] 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.

[79] 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.

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

[81] 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.

[82] 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.

[83] J. M. Singh, R. Raghavendra, K. B. Raja, and C. Busch, "Robust morphdetection 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.

[84] B. Parkinson, "Do Facial Movements Express Emotions or Communicate Motives?," 2005.

[85] A. Pentland, B. Moghaddam, and T. Starner, "View-Based and Modular Eigenspaces for Face Recognition."

[86] J. F. Cohn, J. J. Lien, A. J. Zlochower, and T. Kanade, "Feature-Point Tracking by Optical Flow Discriminates Subtle Differences in Facial Expression."

[87] L. Teijeiro-Mosquera and J. L. Alba-Castro, "Performance of active appearance model-based pose-robust face recognition," IET Computer Vision, vol. 5, no. 6, pp. 348–357, Nov. 2011, doi: 10.1049/iet-cvi.2010.0184.

[88] D. Xi and S. W. Lee, "Face detection and facial feature extraction using support vector machines," Proceedings - International Conference on Pattern Recognition, vol. 16, no. 4, pp. 209–212, 2002.

[89] R. Brunelli and T. Poggio, "Template Matching: Matched Spatial Filters and beyond."