Available online at sjuoz.uoz.edu.krd

Journals of UOZ
journals.uoz.edu.krd

Science Journal of University of Zakho

Vol. 10, No. 4, pp. 258 –267, October-December 2022

SJUOZ

p-ISSN: 2663-628X
e-ISSN: 2663-6298

KURDFACE MORPH DATASET CREATION USING OPENCV

Arezu Rezgar Hussein [a,*], Rasber Dh. Rashid [a]

[a] Dept. Of Computer Science and IT, College of Science, University of Salahaddin, Erbil, Kurdistan Region, Iraq – (**arezu. hussein, rasber.rashid)@su.edu.krd**

Received: *02 Jun., 2022 /* ***Accepted:*** *16 Oct., 2022 /* ***Published:*** *14 Dec., 2022* ***https://doi.org/10.25271/sjuoz.2022.10.4.943***

ABSTRACT:

Automated facial recognition is rapidly being used to reliably identify the identities of individuals for a variety of applications, from automated border control to unlocking mobile phones. The attack of Morphing has presented a significant risk to the face recognition system (FRS) at automated border control. Face morphing is a technique for blending the facial images of two or more people such that the outcome looks like both of them. For example, a morphing attack may be used to get a fake passport by using a morphed image. This passport can be used by both the modified image contributors while crossing the border. Due to the publicly available digital altering tools that criminals may use to carry out face morphing attacks. Morph Attack Detection (MAD) systems have received a lot of attention in recent years. In the absence of automated morphing detection, Face Recognition Systems (FRS) are extremely susceptible to morphing attacks. Due to the limited number of publicly available face morph datasets to investigate, especially to our knowledge, there is no Kurdish morph dataset. In this work, we decided to generate a new face dataset, including morphed images which we named as "KurdFace" dataset. OpenCV was used to generate morphed images. Then we study the susceptibility of biometric systems to such morphed face attacks by designing and creating a Morph Attack Detection model to distinguish morphed images from genuine ones. To evaluate the robustness of our dataset regarding morphing attack detection, we compare it with the AMSL dataset to determine the classification error rate on both datasets to see how our dataset is different from others. Local Binary Pattern and Uniform Local Binary Pattern are used as feature extraction techniques, and as a classifier, SVM is utilized. The experimental result shows that our dataset is suitable for research purposes.

KEYWORDS: Face Recognition System, Biometric System, Morphing Attacks, OpenCV, LBP, Dataset creation.

1. INTRODUCTION

Nowadays, biometric verification systems are present in many fields of daily life. Biometrics is based on a human's biological or behavioural features such as the face, fingerprint, gait, iris, and keystroke style. The benefit of biometric systems over traditional authentication techniques such as token-based authentication or passwords is that biometric attributes cannot be lost, forgotten, or shared (Yang et al., 2021). However, one drawback of this technology is the impossibility of exchanging the corresponding characteristics (and hence the extractable features) if someone obtains unauthorized possession of another individual's biometric features. Although, owing to the uniqueness of face images, their reliability, and availability, face biometrics play a key role in biometric systems. Moreover, the widespread use of facial biometric systems, particularly in secure border control to identify and verify individuals, makes them more vulnerable to different types of attacks. On the one hand, presentation attack also known as direct attacks or spoof attacks, are introduced as one of the attacks on face biometric systems, i.e., the face biometric systems are vulnerable to a variety of attacks, including presentation attacks such as electronic display attacks, print attacks, replay attacks, and 3-D face mask attacks, which aim to corrupt the FRS by presenting an artifact. On the other hand, another attack on these kinds of applications is the face morphing attack, as first announced by Ferrara and his team in 2014 (Ferrara et al., 2014). So, the accuracy of the face biometric recognition system needs to be high, especially in some sensitive applications such as border controls (Ramachandra & Busch, 2018).

The morphing attack's core concept is based on combining facial images of two or more people such that the resulting "morphed" image may be used to verify both the involved participants (a malicious actor and an accomplice) (Pikoulis et al., 2021). I.e., the morphing process is a particular effect that changes one image into another. It is a big problem. This is because morphed faces containing characteristics of both individuals. It can successfully match both identities, posing a security threat (Banerjee & Ross, 2021).

Morphing attacks aim to disrupt face biometric systems at Automated Border Control (ABC) gates by presenting an eMRTD or ePassport based on a morphed facial image. As a result, this attack violates the principle of exclusive possession. As seen in Figure 1, a malicious person's face is merged with that of a look-alike accomplice in border control. As we all know, while crossing the border, the face image stored in the passport or the eMRTD is matched to the individual claiming possession of the identification document. The data subject can pass the border if the enrolled face image matches the live image. As a result, someone with a bad purpose can employ a face-morphing attack to gain unauthorized access. Finally, a malicious individual can use a genuine passport to accomplish all their objectives. Unfortunately, numbers of software and techniques exist to generate morph images, which will be mentioned in the review section. Therefore, the detection of morphed face images has a significant impact on the reliability of face recognition (Venkatesh et al., 2021).

[*] Corresponding author

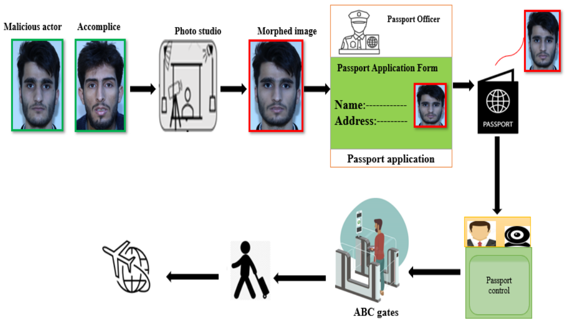


Figure 1. An example scenario that demonstrates FRSs' sensitivity to morphed images in border control.

One of the study's aims is to create a novel face dataset containing five different emotions (Normal, Happy, Sad, Surprised, and Angry) and generate morphed images from normal face images. We decided to create this dataset to serve academic researchers in the Kurdistan region of Iraq as well as other researchers across the world who are passionate in this regard (face processing and face morphing). As mentioned before, morphs are an attack on face biometric systems. Since there is no Morph Attack Detection (MAD) system at most border control and airports (especially in the Kurdistan region of Iraq), most of the fake passports may pass undetected. To prevent morphing attacks, it is imperative to find a solution to preserve the security of face verification systems against such attacks. Especially if the morphed images are generated with high quality, then detection becomes more difficult by human observers (border officers) despite being an expert in facial comparison. So, we intend to design and create a simple Morph Attack Detection model to differentiate morphed images from genuine ones. To the best of the author's knowledge, such a system is not available in the Kurdistan region that helps the airport-related authorities easily control this type of attack. The final aim is to train and test the MAD model with our novel dataset and the AMSL dataset with two different data separations to see how our dataset is different than others regarding resistance to morph attack detection.

Our dataset creation scheme consists of capturing images and generating Morphs. To test the robustness of the created dataset, we designed a simple MAD scheme which includes pre-processing, feature extraction, and classification. The details are described in the methodology section. The rest of this paper is organized as follows: In Section 2, we present a literature review of morph generation techniques, datasets that exist in this field and MAD classification. Our dataset creation and the proposed MAD to evaluate the performance of our dataset are presented in Section 3. Section 4 presents the experimental results, discussion, and datasets used in this work. Finally, in Section 5, we end the paper by giving some conclusions and future direction.

2. RELATED WORKS

In this section, we will present a general review of the morphing generation approaches, face morph datasets, and MAD classification.

2.1 Morph Generation Approaches

Several morphing techniques exist to generate morphed images that mimic the biometric information of two (or more) individuals in the image and feature domain (Scherhag, Rathgeb, et al., 2019). Using one of the freely available software, morphing may be achieved quickly and simply. Even non-technical individuals can perform morphing with simplicity, such as MorphThing[1], Sqirlz Morph 2.1[2], FaceMorpher[3], 3Dthis Face Morph[4], Abrosoft FantaMorph[5], MagicMorph[6], GIMP[7], and Face Swap Online[8]. There are several ways to create morphs, from basic image warping to more advanced generative adversarial networks (GANs) such as OpenCV, StyleGAN, ReGenMorphs,… etc. (H. Zhang et al., 2021). Besides software, there are two basic categories of face morphing generating methods shown in Figure 2. deep learning-based approaches and landmark-based approaches. Additionally, Scherhag et al., in their study, provided a comprehensive list of every publicly available morphing tool, both open source and commercial (Scherhag, Rathgeb, et al., 2019).

The landmark-based strategy is employed in most of morph generation methods (Scherhag, et al., 2019), where the face morphing process is carried out by merging the images concerning corresponding landmarks, and the texture information is blended. Encoding two images into the latent space where the two latent vectors are interpolated and the GAN generator converts the interpolated latent vector into the morphing image and alleviates the restrictions imposed by landmarks (Damer et al., 2018; H. Zhang et al., 2021). Moreover, Damer et al. in 2021 developed the ReGenMorphand, a unique face morphing idea that avoids both artifacts of blending in LMA and artifacts of artificial striping in GAN-based morphs (Damer et al., 2021). With the newly designed loss function that takes use of perceptual quality and identity variables, Zhang et al. 2021 developed MIPGAN, which is based on StyleGAN but has higher resolution and fewer artifacts (H. Zhang et al., 2021).

2.2 Face Morph Dataset

This subsection will cover some of the datasets that exist in the morph attacks field that were proposed by former researchers. It's important to show the number of morphed images in each dataset, their availability and unavailability for research, which is presented in Table 1.

In 2014, Ferrara et al. presented the first face morph database. The authors created morphs of people's faces based on landmarks using the GIMP/GAP tool. In total, there are only 14 digital morphing photos in this dataset, produced from 8 genuine images, including both male and female participants.

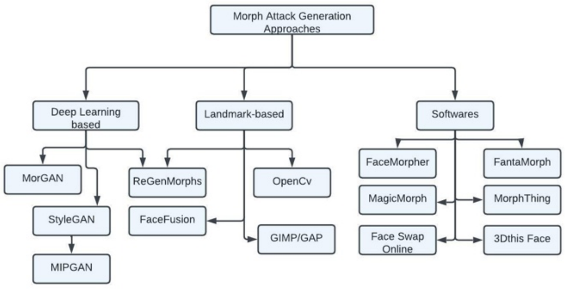


Figure 2. Taxonomy of morph attack generation approaches.

[1] https://www.morphthing.com/

[2] https://download.cnet.com/Sqirlz-Morph/3000-2186_4-10304209.html

[3] http://www.facemorpher.com/

[4] https://3dthis.com/morph.htm

[5] https://www.fantamorph.com/

[6] https://www.effectmatrix.com/morphing/

[7] https://www.gimp.org/

[8] https://icons8.com/swapper

Only digital versions of the morphed images are included in this dataset, which is not publicly available. (Ferrara et al., 2014). In addition, Ferrara et al. used the same tool to generate more morphs and extend this dataset in 2016. Approximately 80 morphing facial images from 10 male and 9 female subjects make up the expanded dataset. This dataset is in digital version but not open to the public. (Ferrara et al. 2016). In 2016, Raghavendra et al. introduced the first huge dataset using face landmarks and the GIMP/GAP morph generation technique, which includes a variety of ethnicities including Asians, Americans, Middle Easterners, Europeans, Latin Americans, and Caucasians. There are a total of 450 morphing face images in this dataset, which were created using 110 people of various racial and ethnic backgrounds. This dataset has not been released to the public and consists only of digital images. (Raghavendra et al., 2016).

In 2017, Raghavendra et al. announced a novel morph dataset that included digital and print-scan images. OpenCV, which is a publicly available automatic tool, was used to create the face morphs. This database produces averaged and morphed face images simultaneously, resulting in a set of 1423 + 1423 morphed face images. (Raghavendra et al., 2017a). Another dataset with morphed faces was introduced in 2017 by Gomez-Barrero et al., which includes 840 morphed images produced from 210 genuine images. This dataset has not been released to the public and consists only of digital images. (Gomez-Barrero et al., 2017). Furthermore, the first face morphing dataset using deep learning-based morph images was introduced in 2018 by Damer and his colleagues. Morph images were made using OpenCV and a GAN architecture by the authors. This dataset is private and limited to digital morphed face images. It contains a total of 1000 morphed images. (Damer et al., 2018). In 2018, Neubert et al. presented another dataset by members of Prof. Jana Dittmann's research team at the AMSL lab of the university of Magdeburg for providing digital and P&S segmented face images. The morphed face images have been created based on landmarks and by a combined approach with 0.5 alpha blending. This dataset consists of 102 genion images and 2175 morph images. This dataset is public and requires some license to obtain it (Neubert et al., 2018).

Another face morph dataset using the both complete and splice method was introduced by Makrushin et al. in 2019. This dataset contains 1326 morphed images in digital forms. The morph images in this database are not available for academic purposes (Makrushin et al., 2019). An additional dataset using the OpenCV morph generation technique to create facial morphs was introduced by Singh et al. in 2019. This dataset is the first to include live probing images taken from ABC gates in varied lighting situations, making it ideal for differential morphing attack detection. There are both digital and print scan images in this dataset. Only 90 morphed facial images exist in this private dataset (Singh et al., 2019). Also, another face morph dataset was introduced in 2019 by Scherhag and his colleagues. It was created with a variety of morphing tools such as OpenCV, FaceFusion, and FaceMorpher. This private dataset includes both digital and print-scan versions of morphed images, with a total of 964 + 964 + 529 morphed face images derived from the source images in the FRGCv2 and FERET datasets (Scherhag, Debiasi, et al., 2019). In 2020, Venkatesh et al. introduced another dataset using deep learning-based morph generation. In order to generate morph images, they utilized StyleGAN network. The 2500 morphed images in this dataset were created using 1270 genuine images. It exclusively contains digitally morphed faces and is not accessible to the general public (Venkatesh, Zhang, et al., 2020).

To summarize, not all of the datasets we have mentioned in the Table 1 are available for research purposes except the dataset created by Neubert et al. in 2018, which is publicly available called the AMSL dataset. Even when using publicly available face datasets, the license terms prohibit the redistribution of the resultant morphed face datasets. Although there is no Kurdish morph dataset in the Kurdistan region of Iraq, and the maximum number of morphs in the mentioned dataset is 2500 morphs, here, we decided to create a Kurdish morph dataset with more morphs than the morphs in the earlier mentioned datasets.

2.3 MAD Classification

The seriousness of morphing attacks motivates researchers to think about a way to design and create a morph detection or prevention scheme. Researchers broadly consider two scenarios for morph attack detection: single morph attack detection (S-MAD) also called (no reference), and differential morph detection (DMA). Single morph detection is when the algorithm bases its classification result only on the potential morphed image and there is no additional source to compare with it. However, differential morph detection uses an additional trusted image, typically a live capture at border control, to compare to the potential morphed image to make its decision. Differential morph detection is not within the scope of our investigation , but readers interested in learning more can refer to the work done by (Ferrara et al., 2018).

In 2016, Raghavendra et al. were the first researchers that presented a morph attack detector model. They extracted features by using binarized statistical image features (BSIF) from gray-scale images. In order to make classification, the SVM classifier was used (Raghavendra et al., 2016). Moreover, in 2017, Kraetzer et al. proposed a method for the purpose of detecting morphed facial images using keypoint descriptors and edge operators.

They used Speed Up Robust Feature (SURF), Features from Accelerated Segment Test (FAST), Generic Accelerated Segment Test AGAST, Scale Invariant Feature Transform (SIFT), and Adaptive and Oriented BRIEF (ORB) to get face keypoints. The classification was conducted with a decision tree classifier (Kraetzer et al., 2017). In 2017, Raghavendra et al. trained a Probabilistic Collaborative Representation Classifier (Pro-CRC) using LBP-feature derived from the color channels (HSV, YCbCr) (Raghavendra et al., 2017b). Due to the fact that our focus is on morph dataset creation, we are not going into detail about former MAD methods here. Readers interested in can return to (Venkatesh et al., 2021).

Table 1. Summary of Face Morph datasets

References	Morph Generation Type	Morph Generation Method	Digital _ Print & Scan	Genuine & Morph	Limitations
(Ferrara et al., 2014)	Landmark	GIMP/GAP	digital	14 morphs	Limited in number of samples and it is private dataset
(Ferrara et al., 2016)	Landmark	GIMP/GAP	digital	80 morphs	Limited in number of samples and it is private dataset
(Raghavendra et al., 2016)	Landmark	GIMP/GAP	digital and Print & Scan	1423+1423 morph	It is private dataset and researchers could not access it.
(Raghavendra et al., 2017b)	Landmark	GIMP/GAP	digital	450 morphs	This dataset is private, and limited in number of samples
(Gomez-Barrero et al., 2017)	---	---	digital	840 morphs	The dataset is private and limited in number of samples
(Damer et al., 2018)	Generative Adversarial Network	GAN	digital	1000 morphs	The dataset is private.
(Neubert et al., 2018)	Landmark	combined_alpha0.5	digital	102 genuine 2175 morphs	The dataset is public but limited in number of morph and genuine samples.
(Makrushin et al., 2019)	Landmark	Complete and splice	digital	1326 morphs	The dataset is private.
(Singh et al., 2019)	Landmark	OpenCV	digital and print scan	90 morphs	The dataset is private and limited in number of samples.
(Scherhag, Debiasi, et al., 2019).	Landmark	OpenCV, FaceFusion, Face Morpher	digital and print & scan	964+964+529 morphs	The dataset is private.
(Venkatesh, Zhang, et al., 2020)	Landmark, Generative Adversarial Network	MorGAN and StyleGAN	digital	2500 morphs	It is unavailable dataset for research purposes.

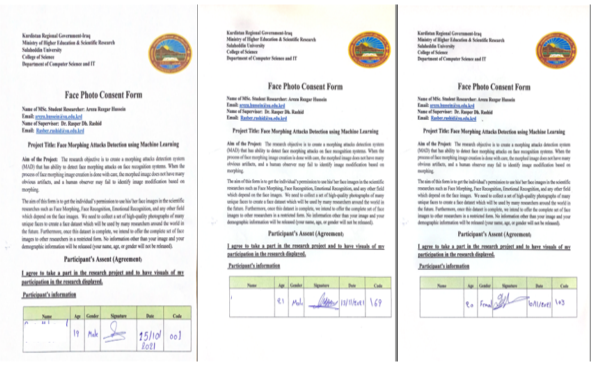
3. METHODOLOGY

Regarding the limitation mentioned above in the previous section. This section discusses the dataset generation in detail. Our dataset creation scheme consists of capturing images and generating Morphs. To test the robustness of the created dataset, we designed a simple MAD scheme which includes pre-processing, feature extraction, and classification.

3.1 Dataset Creation

Data was introduced as the oil of the 21st century, i.e., data is an important part of the research area. To investigate and solve real-world problems, there is a serious need to access robust and reliable data. However, there is a limit to the datasets available, especially in the field of "Morphing Attacks Detection," because most datasets are private. The decision to create a morph dataset was based on this limitation. The main goal of our dataset creation is to serve academic research in the Kurdistan region of Iraq as well as other scholars across the world who are passionate in this regard. The face image dataset generation needs some procedures, such as getting permission from our university to collect data.

In addition, we prepared permission forms for individuals who wanted to participate in the experiments (see Figure 3). On October 15, 2021, we began the collection of (capturing) face images at the Computer Science and IT Department of Salahaddin University in the Kurdistan region of Iraq, as well as several subjects from various cities and universities.



Kurdistan Regional Government-Iraq
Ministry of Higher Education & Scientific Research
Salahaddin University
College of Science
Department of Computer Science and IT

Face Photo Consent Form

Name of MSc. Student Researcher: Arezu Rezgar Hussein
Email: arezu.hussein@su.edu.krd
Name of Supervisor: Dr. Rasper Dh. Rashid
Email: Rasber.rashid@su.edu.krd

Project Title: Face Morphing Attacks Detection using Machine Learning

Aim of the Project: The research objective is to create a morphing attacks detection system (MAD) that has ability to detect face morphing attacks on face recognition systems. When the process of face morphing image creation is done with care, the morphed image does not have many obvious artifacts, and a human observer may fail to identify image modification based on morphing.

The aim of this form is to get the individual's permission to use his/ her face images in the scientific researches such as Face Morphing, Face Recognition, Emotional Recognition, and any other field which depend on the face images. We need to collect a set of high-quality photographs of many unique faces to create a face dataset which will be used by many researchers around the world in the future. Furthermore, once this dataset is complete, we intend to offer the complete set of face images to other researchers in a restricted form. No information other than your image and your demographic information will be released (your name, age, or gender will not be released).

Participant's Assent (Agreement)

I agree to take a part in the research project and to have visuals of my participation in the research displayed.

Participant's information

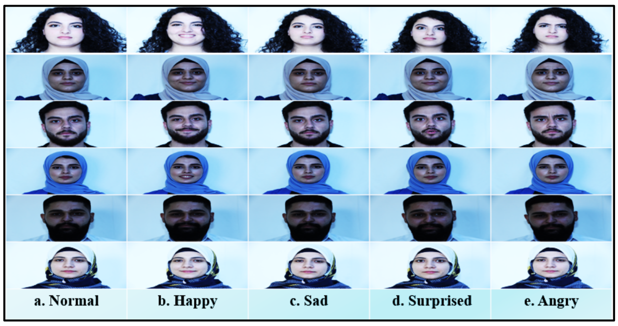
Name	Age	Gender	Signature	Date	Code
	19	Male		15/10/2021	001

Name	Age	Gender	Signature	Date	Code
	٢١	Male		13/11/٢٠٢١	١٦٩

Name	Age	Gender	Signature	Date	Code
	٢٠	Femal		6/11/٢٠٢١	١٠٣

Figure 3. Samples of our dataset permission form

We named our dataset KurdFace, which consists of 845 facial images from 169 individuals, and for each individual, five different emotions (Normal, Happy, Sad, Surprised, and Angry) are taken. The individuals are distributed among various age groups between 18 to 45, and both genders (male and female). Some samples are shown in Figure 4.



a. Normal b. Happy c. Sad d. Surprised e. Angry

Figure 4. Samples of our dataset.

The frontal faces are captured as the first step in our data collection. To capture frontal face images, we used a Canon camera model EOS Kiss X5 with a Canon zoom LENS EF_S 18_135MM 1:3.5_5.6 IS. We used normal face images to generate morphed face images (the generation process is explained in the next subsection). Figure 5 provides instances of morphing facial images acquired from two separate individuals.

To the best of the author's knowledge, this is the first dataset in the Kurdistan region of Iraq with 169 genuine images of individuals. The genuine images were merged to produce 3951 distinct morphing face images, and our dataset could be used in several applications related to face recognition, emotion recognition, and morph attack detection.

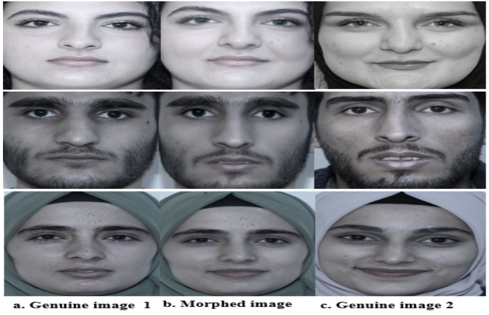


Figure 5. Samples of morphed face images in our dataset.

3.2 The KurdFace dataset's limitation

In this subsection, the limitations of our dataset are described as follows:

- The dataset does not contain a diversity of images.
- Images were taken under uncontrolled illumination conditions due to the unavailability of a studio to capture images.
- Images were taken from various distances to represent the attacker's scenario, which is the unavailability of passport images in some scenarios.
- The dataset consists of more young individuals than older ones.

3.3 Morph Generation

To study morphing attack detection, a large number of morphed face images are required. The reader who's interested in morphing generation steps in detail can refer to (Scherhag, Rathgeb, et al., 2019) and (Neubert et al., 2018). In this work, an open-source automated generating morphed images called OpenCV (Mallick, 2021) based on landmarks has been used. We utilized OpenCv for several reasons. First, it is publicly available. Second, it quickly generates a large number of morph images automatically. Third, it proved from previous research that obtained images are secure.

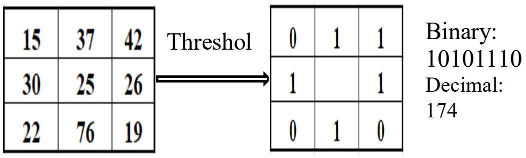
OpenCV is a self-implementation morphing method, that is easy to be use. An interested researcher can follow this tutorial "Face Morph Using OpenCV" for more details. It employs the Dlib library's 68-point annotator for face morphing (King, 2009). Facial landmarks are extracted from both genuine source images, and Delaunay triangles are created from these landmarks, which are then warped and alpha-blended.

We consider the gender of participants during the generation of morph images since morphing people of various genders usually results in morphs that look unnatural. In the real scenario, the generation of morphs with subjects of a different gender is not predictable; thus, they are excluded from the dataset. Morph images were formed in a way to keep the ratio between two genuine images in balance with a 0.5 alpha blending factor. To ensure a clear separation of datasets during training and testing, the morph images are created within a single folder. While open-source software OpenCV can generate a large number of morphs, it has the drawback of requiring a significant effort to post-processing the generated images.

3.4 Morphed Face Detection Framework

To test the robustness of our dataset, we aimed to implement a simple Morph Attack Detection (MAD) algorithm based on the extraction of texture features from the faces. Texture is one of the most important characteristics of images in general and especially in face images. Different texture descriptors were used in many different applications, such as Local Binary Patterns (LBP) (Asma & Brahim, 2022), Local Phase Quantization (LPQ) features (Raghavendra et al., 2018), and the Binarized Statistical Image Feature (BSIF) (Adjabi et al., 2021). These texture descriptors are important for more applications, especially face recognition (Rashid et al., 2013), and face morph detection (Damer et al., 2018). The design of our morphing detector is based on the idea that the morphing process changes the variation in the micro_texture of images. If the morphed images are generated accurately, and with high quality, the differences between these textures will not be visible to the human eye. Due to this, it is important to generate MAD systems at border controls. The proposed scheme uses LBP and uniform LBP as texture descriptors to adequately distinguish between genuine and morphed face images.

3.4.1 Local Binary Pattern (LBP): LBP is a texture descriptor whose aim is to efficiently summarize the local structures of images. In terms of representing local structures, LBP is one of the strongest descriptors, it has the ability against illumination changes, and it is easy to compute. Ojala and Pietikainen were the first researchers who introduced LBP to characterize texture in images (Ojala and Pietikainen, 1996). Subtracting the central pixel from its eight neighbours is the first step in the LBP process. From the upper-left corner, the subtraction result will determine whether each place gets 0 or 1. Concatenation and encoding of binary strings are performed clockwise on the resulting bits for all neighbouring pixels. LBP codes, or Local Binary Patterns, are the derived binary strings. Figure 6 displays the decimal LBP code for the central pixel.



15	37	42
30	25	26
22	76	19

0	1	1
1		1
0	1	0

Figure 6. Basic LBP operator

Uniform LBP codes have 0 or 2 bitwise transitions from 0 to 1 or vice versa. It has been demonstrated that uniform LBP (ULBP) codes represent 90% of the LBP codes in face images (Ojala et al., 2002). 00000000 (0 transitions) and 10000001 (2 transitions) are examples of uniform values, but 10100101 (6 transitions) and 01100110 (4 transitions) are not. It is simple to demonstrate that only 58 uniform patterns can be found in the 8-1 neighbourhood, and the standard LBP histogram contains 59 bins for the 58 uniform patterns and one bin for the summation of non-uniform patterns. Our proposed approach for robust morphing facial image detection is shown in a block diagram in Figure 7. Pre-processing, feature extraction, and classification are the three main steps of our proposed technique.

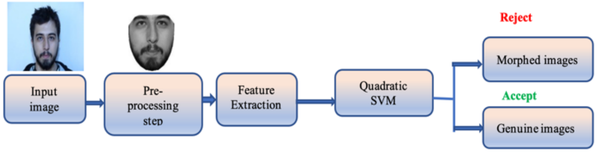


Figure 7. The block diagram of our proposed approach

The idea behind the pre-processing is to extract the standardized face size. In this work, face detection is carried out using the Dlib landmark detector (King, 2009). Subsequently, we automatically select the maximum size of face images from both genuine and morph images, and then all face images are rescaled with the selected maximum size, which is cropped to 315×302 pixels to ensure that the detection algorithm is only applied to the facial region. Finally, the cropped face part is converted to a grayscale image.

The strategy of extracting discriminant features of a face image that are robust to varying conditions is crucial to the reliability of face morph attack detection. In the feature extraction step, 256 bins of Local Binary Pattern (LBP) and 59 bins of the Uniform LBP are extracted separately. Then the histogram of the obtained LBP code is calculated. These histograms are the final feature vectors describing the images. After labelling the features (Genuine = 0 and Morph = 1), we separate them into training and testing sets, which will be mentioned in the next section. We use 5-fold cross-validation for our experiments. Finally, the classification is conducted by an SVM classifier. We train the model with the training set features and test the model with the testing set features.

4. EXPERIMENTAL DATA, RESULTS, AND DISCUSSION

4.1 MAD performance measurements

The following measurements were widely used to evaluate the performance of face-morphing attack detection methods. For more details, go back to study (Misra & Arumugam, 2022).

1. False Rejection Rate (FRR) or Bona Fide Presentation Classification Error Rate (BPCER)
2. False Acceptance Rate (FAR) or Attack Presentation Classification Error Rate (APCER)
3. Detection-Equal Error Rate (D-EER)
4. Average Classification Error Rate (ACER)
5. Accuracy (ACC)
6. True Positive Rate (TPR) TPR.

Most of the researchers used the mentioned metrics for MAD performance evaluation in their investigations (Kraetzer et al., 2017) (Wandzik et al., 2017) (Jassim & Asaad, 2018) (L.-B. Zhang et al., 2018) (Makrushin et al., 2018) (Debiasi et al., 2018) (Damer et al., 2019) (Ramachandra et al., 2019) (Venkatesh et al., 2019) (Scherhag, Rathgeb, et al., 2020) (Ferrara et al., 2021). Due to this, we used the BPCER, APCER, and ACER metrics to evaluate the performance of our proposed method, as explained in Table 2.

When the values of BPCER are high, it indicates many false rejects (false negatives), while when the values of APCER are high, it represents a huge number of false positives resulting from successful attacks. Thus, low values of both metrics and lower ACER indicate robust MAD performance.

Table 2. Metrics definitions and equations

Metrics	Definition	Equation
False Acceptance Rate (FAR) or Attack Presentation Classification Error Rate (APCER)	It is defined as the proportion of attack images misclassified as genuine images (Scherhag et al., 2017)i.e., the ratio at which morph attacks are misclassified as genuine	APCER = {False Positive / (False Positive + True Negative)} (1)
False Rejection Rate (FRR) or Bona Fide Presentation Classification Error Rate (BPCER)	It is defined as the proportion of bona fide (genuine) images misclassified as presentation (morph) attacks (Scherhag et al., 2017). i.e., the ratio at which genuine images are misclassified as morph images.	BPCER = {False Negative / (False Negative + True Positive) } (2)
Average Classification Error Rate (ACER)	The average between APCER and BPCER can be represented in an Average Classification Error Rate (ACER). i.e., the rate of error classification of the model generally	ACER = (APCER + BPCER) / 2 (3)

4.2 Datasets used

Due to the limited number of publicly available face morphing datasets and the lack of a Kurdish morph dataset, we constructed a face morph dataset which we named as KurdFace Dataset, described in section 3.1. Thus, to compare the robustness of our morph dataset regarding how morph images were generated in our dataset, whether they were as robust as morph images in other datasets or not, and the classification error rate, we used the AMSL dataset in our experiments to compare with it. AMSL stands for Advanced Multimedia and Security Lab. The morph images in the AMSL dataset were generated by the Combined Morphs tool, which is presented in (Neubert et al., 2018). This dataset was created at the University of Magdeburg, in Germany. The AMSL dataset consists of 102 genuine neutral, 102 smiling passport images, and 2175 morph images. The morph images from the AMSL dataset are generated from bona fide images of the FRLL dataset (DeBruine & Jones, 2021) and the Utrecht ECVP Dataset[9].

4.3 Performance evaluation protocol, results, and discussion

In order to effectively evaluate the performance of algorithms, we divide both the mentioned datasets separately into training and testing sets without overlapping subjects. We keep an equal number of genuine and morphed images during the training and testing of the model to avoid unbalancing issues (different numbers of genuine and morphed images). The SVM classifier is trained entirely on images from the training set, which consists of 75% (50%) genion images and 75% (50%) morphed images. The testing set consists of 25% (50%) of genion and 25% (50%) of morphed images to share the findings of the morph face detection method. We used these two percentages of data separation because most of the papers in the field of morph attack detection utilized the percentages of between 50 to 80 of the datasets to train and test the models(Venkatesh, Ramachandra, et al., 2020), (Hamza et al., 2022).

Table 3–10 illustrates the quantitative results of Normal LBP and Uniform LBP on both kurdFace and AMSL datasets with two different data separation scenarios. In the first scenario, 75% of the datasets were used for training the model, and 25% of the datasets were used for testing the model. In the second scenario, 50%, which is half of the datasets, goes to train the model, and the other half is used to test the model.

We pick morph features at random five times (no. of the trail). In each trial, we select the morph feature sets along with the genuine feature sets to train the model. This means that a model is trained five times, and we. repeated the same procedure for testing the model. As mentioned before, the classification was performed using an SVM classifier. In the next step, the performances are calculated for each run separately. Then, the final classification error was calculated by averaging the results from all five runs. In each case, we measure the APCER,

[9] http://pics.stir.ac.uk/

BPCER, and ACER of the model, as you can see from Tables (3–10).

4.3.1 Results of Normal LBP on KurdFace and AMSL Dataset: Table 3-6 indicates the quantitative performance of the normal LBP method on both KurdFace and AMSL datasets with 75%–25% and 50%–50% data separation protocols. As mentioned in the earlier section, low values of BPCER and APCER as well as lower ACER indicate the robust performance of a MAD technique.

In the 75%-25% scenario, when training and testing the model conducted with AMSL dataset, the average BPCER is 12.8% after five trails. That indicates genuine images are incorrectly classified as morph attacks, but the result is 8 in some tests, such as trail four and five. In contrast, the average of APCER is 16.8% after five trails, which indicates morph attacks are incorrectly classified as genuine images. We also have a case where APCER is 8 in trail five. As you can see in Table 3, there are some cases where most of the genuine and morph images are correctly classified into their original classes. When we train and test the model with the KurdFace dataset, which is presented in Table 4, the average of the (A. ACER) after five trials is 12.85%. However, this on the AMSL dataset is 14.8%. It is interesting to note that the classification error of the proposed method is nearly equal to each other in both datasets. This can be attributed to the suitable texture features extracted from the frontal face images in both datasets. This also indicates that our dataset is as robust as the AMSL dataset.

In 50%-50% scenario, when training and testing of the model were conducted with the AMSL dataset, the average ACER increased to 19.21%. As you can see in Table 5, this indicates that more images are misclassified into their original classes when compared with the 75%–25% scenario. In addition, Table 6 presents the least average classification error rate, which is11.07%, when the model is trained and tested with the KurdFace dataset in a 50%–50% scenario.

Table 3. The quantitative results of Normal LBP on the AMSL dataset (75%_25%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	20	5	6	19	20	24	22	12.8	16.8	14.8
2	22	3	4	21	12	16	14			
3	21	4	6	19	16	24	20			
4	23	2	3	22	8	12	10			
5	23	2	2	23	8	8	8			

Table 4. The quantitative results of Normal LBP on KurdFace dataset (75%_25%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	37	5	5	37	11.90	11.90	11.90	11.42	14.28	12.85
2	37	5	7	35	11.90	16.66	14.28			
3	38	4	9	33	9.52	21.42	15.47			
4	37	5	5	37	11.90	11.90	11.90			
5	37	5	4	38	11.90	9.52	10.71			

Table 5. The quantitative results of Normal LBP on the AMSL dataset (50%_50%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	43	8	5	46	15.68	9.80	12.74	16.47	21.96	19.21
2	41	10	13	38	19.60	25.49	22.54			
3	45	6	15	36	11.76	29.41	20.58			
4	41	10	14	37	19.60	27.45	23.52			
5	43	8	9	42	15.68	17.64	16.66			

Table 6. The quantitative results of Normal LBP on KurdFace dataset (50%_50%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	77	7	8	76	8.33	9.52	8.92	10.23	11.90	11.07
2	75	9	9	75	10.71	10.71	10.71			
3	74	10	12	72	11.90	14.28	13.09			
4	76	8	7	77	9.52	8.33	8.92			
5	75	9	14	70	10.71	16.66	13.69			

4.3.2 Results of Uniform LBP on KurdFace and AMSL datasets: The quantitative result of Uniform LBP method on both KurdFace and AMSL datasets with both data separation protocol shows in Tables (7-10).

In the 75%-25% scenario, when the training procedure is conducted with the training set features of the AMSL dataset, and the testing procedure is conducted with the testing set features of the same dataset, the average of BPCER, APCER, and ACER is 15.2%, 16%, and 15.6%, respectively, which is reported in Table 7. This indicates that the classification error is approximately balanced between morph and genuine images. As Table 8 illustrates, the average of BPCER, APCER, and ACER is 14.28%, 18.09%, and 16.19% achieved on the KurdFace dataset, respectively. This means that the rate of error classifications on the AMSL dataset is very close to the rate of error classifications on the KurdFace dataset.

In the 50%-50% scenario, when training and testing of the model were conducted with the AMSL dataset, the average of BPCER, APCER, and ACER increased to 20.39%, 25.88%, and 23.13%, respectively. Table 9 presents this evidence. This indicates that more images are misclassified into their original classes when compared with the 75%–25% scenario. In addition, Table 10 presents the least average classification error rate, which is 11.66%, when the model is trained and tested with the KurdFace dataset in the 50%–50% scenario.

Furthermore, we discovered in Tables 3-10 that the correct classification of genuine and morph images (TP and TN) is roughly balanced on both datasets and in both scenarios.

Table 7. The quantitative results of Uniform LBP on the AMSL dataset (75%_25%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	20	5	3	22	20	12	16	15.2	16	15.6
2	21	4	4	21	16	16	16			
3	22	3	3	22	12	12	12			
4	21	4	4	21	16	16	16			
5	22	3	6	19	12	24	18			

Table 8. The quantitative results of Uniform LBP on KurdFace dataset (75%_25%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	38	4	10	32	9.52	23.80	16.66	14.28	18.09	16.19
2	37	5	4	38	11.90	9.52	10.71			
3	36	6	9	33	14.28	21.42	17.85			
4	35	7	8	34	16.66	19.04	17.85			
5	34	8	7	35	19.04	16.66	17.85			

Table 9. The quantitative results of Uniform LBP on the AMSL dataset (50%_50%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	43	8	16	35	15.68	31.37	23.52	20.39	25.88	23.13
2	42	9	16	35	17.64	31.37	24.50			
3	41	10	11	40	19.60	21.56	20.58			
4	37	14	11	40	27.45	21.56	24.50			
5	40	11	12	39	21.56	23.52	22.54			

Table 10. The quantitative results of Uniform LBP on KurdFace dataset (50%_50%)

No. of Trail	TP	FN	FP	TN	BPCER	APCER	ACER	A. BPCER	A. APCER	A. ACER
1	76	8	12	72	9.52	14.28	11.90	9.52	13.80	11.66
2	79	5	13	71	5.95	15.47	10.71			
3	75	9	8	76	10.71	9.52	10.11			
4	72	12	14	70	14.28	16.66	15.47			
5	78	6	11	73	7.14	13.09	10.11			

Table 11. Summary of our experiments

Datasets		**Data Separation**		**Normal LBP**	**Uniform LBP**
		Training set	**Testing set**	**256 bins (ACER)**	**59 bins (ACER)**
AMSL	First Scenario	75%	25%	14.8	15.6
	Second Scenario	50%	50%	19.21	23.13
KurdFace	First Scenario	75%	25%	12.85	16.19
	Second Scenario	50%	50%	11.07	11.66

In summary, the experimental results shown in the above table show that the strategy of data separation has a direct effect on the recognition rate. In both scenarios, the average classification error rate (ACER) after 5 trials using normal LBP on both datasets achieved a lower error rate than using uniform LBP on the same datasets. This demonstrates that the number of features is affecting the classification rate. However, the ACER on the AMSL dataset is more than when it's applied to the KurdFace dataset, but it is still close to each other. We can say our dataset is robust like the AMSL dataset for such kinds of texture features, and researchers can use it in their investigations.

In addition, the results of the experiments show clear support for the normal LBP. This analysis found evidence that normal LBP outperformed uniform LBP in terms of the least average classification error rate. The result shows that LBP is better than uniform LBP because normal LBP takes 256 features of face images as one package, which represents the whole face image, while in uniform LBP only 59 features remain, and these features don't seem to be the exact features that are represented in the whole face image, i.e., these uniform LBP features are not enough to effectively distinguish morphed images from genuine ones.

5. CONCLUSION AND FUTURE WORK

Due to the importance of data and the unavailability of morph datasets in the Kurdistan region of Iraq, we constructed a KurdFace dataset which consists of 845 images of 169 individuals with five different emotions to serve academic research, especially in the fields of Face Recognition, Emotion Recognition, and Face Morph Attack Detection. In addition, we generated 3951 morphed images from normal frontal faces using the OpenCV morph generator technique.

We designed the MAD method, which is based on normal LBP and uniform LBP as feature extractors and SVM as classifiers with two different data separations, to test the robustness of our dataset and see how it compares to other datasets in terms of resistance to morph attack detection.

The experimental results show that the rate of wrong classifications (ACER) on the AMSL dataset is very close to the rate of wrong classifications (ACER) on the KurdFace dataset. Moreover, the correct classification of genuine and morph images (TP and TN) is approximately balanced across both datasets and in both scenarios. This indicates that the KurdFace dataset is as robust as the AMSL dataset and it can be used for research purposes. We aim to conduct more investigations into our new dataset by conducting different feature extraction methods and classification algorithms in the future.

REFERENCES

Adjabi, I., Ouahabi, A., Benzaoui, A., & Jacques, S. (2021). Multi-Block Color-Binarized Statistical Images for Single-

Sample Face Recognition. *Sensors, 21(3),* 728. https://doi.org/10.3390/s21030728

Asma, Z., & Brahim, N. (2022). Local Binary Pattern Regrouping for Rotation Invariant Texture Classification: *Journal of Information Technology Research, 15(1),* 1–15. https://doi.org/10.4018/JITR.299945

Banerjee, S., & Ross, A. (2021). Conditional Identity Disentanglement for Differential Face Morph Detection. *International Joint Conference on Biometrics (IJCB),* 1–8. IEEE http://arxiv.org/abs/2107.02162

Damer, N., Boller, V., Wainakh, Y., Boutros, F., Terhörst, P., Braun, A., & Kuijper, A. (2019). Detecting Face Morphing Attacks by Analyzing the Directed Distances of Facial Landmarks Shifts. In T. Brox, A. Bruhn, & M. Fritz (Eds.), *Pattern Recognition,*11269, 518–534. Springer International Publishing. https://doi.org/10.1007/978-3-030-12939-2_36

Damer, N., Raja, K., Süßmilch, M., Venkatesh, S., Boutros, F., Fang, M., Kirchbuchner, F., Ramachandra, R., & Kuijper, A. (2021). *ReGenMorph: Visibly Realistic GAN Generated Face Morphing Attacks by Attack Re-generation* (arXiv:2108.09130). arXi*v.*1–23. Springer. http://arxiv.org/abs/2108.09130

Damer, N., Saladie, A. M., Braun, A., & Kuijper, A. (2018). MorGAN: Recognition Vulnerability and Attack Detectability of Face Morphing Attacks Created by Generative Adversarial Network. *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS),* 1–10. https://doi.org/10.1109/BTAS.2018.8698563

Debiasi, L., Scherhag, U., Rathgeb, C., Uhl, A., & Busch, C. (2018). PRNU-based detection of morphed face images. *2018 International Workshop on Biometrics and Forensics (IWBF),* 1–7. https://doi.org/10.1109/IWBF.2018.8401555

DeBruine, L., & Jones, B. (2021, April 1). *Face research lab London set*. figshare. Retrieved October 15, 2022, from https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666

Ferrara, M., Franco, A., & Maltoni, D. (2014). The magic passport. *IEEE International Joint Conference on Biometrics*, 1–7. https://doi.org/10.1109/BTAS.2014.6996240

Ferrara, M., Franco, A., & Maltoni, D. (2016). On the Effects of Image Alterations on Face Recognition Accuracy. In T. Bourlai (Ed.), *Face Recognition Across the Imaging Spectrum*,195–222. Springer International Publishing. https://doi.org/10.1007/978-3-319-28501-6_9

Ferrara, M., Franco, A., & Maltoni, D. (2018). Face Demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4), 1008–1017.https://doi.org/10.1109/TIFS.2017.2777340

Ferrara, M., Franco, A., & Maltoni, D. (2021). Face morphing detection in the presence of printing/scanning and heterogeneous image sources. *IET Biometrics*, *10*(3), 290–303. https://doi.org/10.1049/bme2.12021

Gomez-Barrero, M., Rathgeb, C., Scherhag, U., & Busch, C. (2017). Is your biometric system robust to morphing attacks? *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 1–6. https://doi.org/10.1109/IWBF.2017.7935079

Jassim, S., & Asaad, A. (2018). Automatic Detection of Image Morphing by Topology-based Analysis. *2018 26th European Signal Processing Conference (EUSIPCO)*, 1007–1011. https://doi.org/10.23919/EUSIPCO.2018.8553317

King, D. E. (2009). Dlib-ml: A Machine Learning Toolkit. *The Journal of Machine Learning Research,* 10, 1755-1758.https://doi.org/10.1145/3082031.3083244

Kraetzer, C., Makrushin, A., Neubert, T., Hildebrandt, M., & Dittmann, J. (2017). Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 21–32. https://doi.org/10.1145/3082031.3083244

Makrushin, A., Kraetzer, C., Neubert, T., & Dittmann, J. (2018). Generalized Benford's Law for Blind Detection of Morphed Face Images. *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 49–54. https://doi.org/10.1145/3206004.3206018

Makrushin, A., Neubert, T., & Dittmann, J. (2019). Humans Vs. Algorithms: Assessment of Security Risks Posed by Facial Morphing to Identity Verification at Border Control: *Proceedings of the 14th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications,* 513–520. https://doi.org/10.5220/0007378905130520

Misra, S., & Arumugam, C. (Eds.). (2022). *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (Vol. 109). Springer International Publishing. https://doi.org/10.1007/978-3-030-93453-8

Neubert, T., Makrushin, A., Hildebrandt, M., Kraetzer, C., & Dittmann, J. (2018). Extended *StirTrace* benchmarking of biometric and forensic qualities of morphed face images. *IET Biometrics,* 7(4), 325–332. https://doi.org/10.1049/iet-bmt.2017.0147

Ojala, T., & Pietikainen, M. (1996). A comparative study of texture measures with classification based on featured distributions. *Pattern recognition,* 29(1), 51-59. https://doi.org/10.1016/0031-3203(95)00067-4

Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 24*(7), 971–987. https://doi.org/10.1109/TPAMI.2002.1017623

Pikoulis, E.-V., Ioannou, Z.-M., Paschou, M., & Sakkopoulos, E. (2021). Face Morphing, a Modern Threat to Border Security: Recent Advances and Open Challenges. *Applied Sciences, 11*(7), 3207, 1–15. https://doi.org/10.3390/app11073207

Raghavendra, R., Raja, K. B., & Busch, C. (2016). Detecting morphed face images. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS),* 1–7. https://doi.org/10.1109/BTAS.2016.7791169

Raghavendra, R., Raja, K. B., Venkatesh, S., & Busch, C. (2017a). Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images. *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 1822–1830. https://doi.org/10.1109/CVPRW.2017.228

Raghavendra, R., Raja, KiranB., Venkatesh, S., & Busch, C. (2017b). Face morphing versus face averaging: Vulnerability and detection. *2017 IEEE International Joint Conference on Biometrics (IJCB),* 555–563. https://doi.org/10.1109/BTAS.2017.8272742

Raghavendra, R., Venkatesh, S., Raja, K. B., Wasnik, P., Stokkenes, M., & Busch, C. (2018). Fusion of Multi-Scale Local Phase Quantization Features for Face Presentation Attack Detection. *2018 21st International Conference on Information Fusion (FUSION)*, 2107–2112. https://doi.org/10.23919/ICIF.2018.8455781

Ramachandra, R., & Busch, C. (2018). Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *ACM Computing Surveys, 50*(1), 1–37. https://doi.org/10.1145/3038924

Ramachandra, R., Venkatesh, S., Raja, K., & Busch, C. (2019). Towards making Morphing Attack Detection robust using hybrid Scale-Space Colour Texture Features. *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, 1–8. https://doi.org/10.1109/ISBA.2019.8778488

Rashid, R. D., Jassim, S. A., & Sellahewa, H. (2013). LBP based on multi wavelet sub-bands feature extraction used for face recognition. *2013 IEEE International Workshop on Machine Learning for Signal Processing (MLSP)*, 1–6. https://doi.org/10.1109/MLSP.2013.6661911

Scherhag, U., Debiasi, L., Rathgeb, C., Busch, C., & Uhl, A. (2019). Detection of Face Morphing Attacks Based on PRNU Analysis. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 1*(4), 302–317. https://doi.org/10.1109/TBIOM.2019.2942395

Scherhag, U., Raghavendra, R., Raja, K. B., Gomez-Barrero, M., Rathgeb, C., & Busch, C. (2017). On the vulnerability of face recognition systems towards morphed face attacks. *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 1–6. https://doi.org/10.1109/IWBF.2017.7935088

Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., & Busch, C. (2019). Face Recognition Systems Under Morphing Attacks: A Survey. *IEEE Access, 7, 23012–23026.* https://doi.org/10.1109/ACCESS.2019.2899367

Scherhag, U., Rathgeb, C., Merkle, J., & Busch, C. (2020). Deep Face Representations for Differential Morphing Attack Detection. *IEEE Transactions on Information Forensics* *and Security*, 15, 3625–3639. https://doi.org/10.1109/TIFS.2020.2994750

Singh, J. M., Ramachandra, R., Raja, K. B., & Busch, C. (2019). Robust Morph-Detection at Automated Border Control Gate using Deep Decomposed 3D Shape and Diffuse Reflectance. 2019 15th *International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 106-112. IEEE*. http://arxiv.org/abs/1912.01372

Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2020). Single Image Face Morphing Attack Detection Using Ensemble of Features. *2020 IEEE 23rd International Conference on Information Fusion (FUSION),* 1–6. https://doi.org/10.23919/FUSION45008.2020.9190629

Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2021). Face Morphing Attack Generation and Detection: A Comprehensive Survey. IEEE Transactions on Technology and Society, 2(3), 128–145. https://doi.org/10.1109/TTS.2021.3066254

Venkatesh, S., Ramachandra, R., Raja, K., Spreeuwers, L., Veldhuis, R., & Busch, C. (2019). Morphed Face Detection Based on Deep Color Residual Noise. 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), 1–6. https://doi.org/10.1109/IPTA.2019.8936088

Venkatesh, S., Zhang, H., Ramachandra, R., Raja, K., Damer, N., & Busch, C. (2020). Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs? -- Vulnerability and Detection. 2020 8th International Workshop on Biometrics and Forensics (IWBF) 1-6. IEEE. http://arxiv.org/abs/2007.03621

Wandzik, L., Garcia, R. V., Kaeding, G., & Chen, X. (2017). CNNs Under Attack: On the Vulnerability of Deep Neural Networks Based Face Recognition to Image Morphing. In C. Kraetzer, Y.-Q. Shi, J. Dittmann, & H. J. Kim (Eds.), *Digital Forensics and Watermarking*10431, 121–135. Springer International Publishing. https://doi.org/10.1007/978-3-319-64185-0_10

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things Security: A Review. *Sensors, 21*(18), 6163. https://doi.org/10.3390/s21186163

Zhang, H., Venkatesh, S., Ramachandra, R., Raja, K., Damer, N., & Busch, C. (2021). MIPGAN—Generating Strong and High Quality Morphing Attacks Using Identity Prior Driven GAN. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 3*(3), 365–383. https://doi.org/10.1109/TBIOM.2021.3072349

Zhang, L.-B., Peng, F., & Long, M. (2018). Face Morphing Detection Using Fourier Spectrum of Sensor Pattern Noise. *2018 IEEE International Conference on Multimedia and Expo (ICME)*, 1–6. https://doi.org/10.1109/ICME.2018.8486607