MorphDet: Towards the Detection of Morphing Attacks

Jival Kapoor[1], Priyanka Singh[1] and Manoranjan Mohanty[2]
[1]*School of Electrical Engineering and Computer Science, University of Queensland, Australia*
[2]*Information Systems, Carnegie Mellon University in Qatar, Qatar*

Keywords: Face Morphing, Morphing Attack Detection, Biometrics.

Abstract: Biometric authentication systems have become an inevitable part of the society. They are based on the primary traits of an individual that are unique and hard to forge or manipulate by simple means. However, the unprecedented growth of technology has enabled the access of so many advanced tools that could be used for forging these traits. In this paper, we focus on the face morphing attacks. A basic pipeline is used to generate morphed attacks. A face morph detection model based on Resnet-152 is proposed and validated through exhaustive experiments. A dataset of 28,890 images is also contributed to conduct the experiments for varied scenarios, including simple face images, faces with beards, faces with eyeglasses, and a combination of beard and eyeglasses. Comparative performance analysis is done with the other state-of-the-art models i.e. Alexnet and VGG-16 and the proposed framework is found to outperform them.

1 INTRODUCTION

Biometric traits are used for identification and authentication based on unique, verifiable data specific to individuals. Common applications include airport security, law enforcement, mobile authentication, banking, education, and border control (Biometrika,). Some uses are critical—for example, facial recognition at borders compares a person's features with a reference database to verify identity (findbiometrics,), (Bayometric,).

While Facial Recognition Systems (FRS) have proven effective, rapid technological advances have introduced new challenges. Notably, face morphing attacks have emerged, aiming to deceive these systems. For instance, Fox News aired a digitally manipulated image on "Tucker Carlson Tonight" combining Epstein and Reinhart's faces, which went viral on Twitter (Fox news,). In another case, an elderly woman was harassed via WhatsApp using her morphed image, linked to online loan apps (Elo,). Face morphing—blending facial features from two individuals—produces an image resembling both, as illustrated in Fig. 1, which can be used to bypass FRS.

Today, morphing is prevalent across film, animation, social media, and fake news. With accessible tools and tutorials, even unskilled users can easily create convincing morphs.

This paper presents a framework to detect whether an image is authentic or morphed using a CNN-based classifier. The ResNet-152 model is employed for this task. A dataset of 28,890 images was created to evaluate the model across three scenarios: (1) binary classification (original vs. morphed), (2) three-class classification (Individual 1, Individual 2, or morphed), and (3) ten-class classification using four subjects and their six morph combinations. The proposed model's performance is compared with other pre-trained architectures trained from scratch. The key contributions are summarized below:

Image 1 Morph Image 2
Figure 1: Morph result between Image 1 and Image 2.

- **Dataset:** A dataset of 28,460 face images was created using four subjects: Aamir Khan, Amitabh Bachchan, Prabhas, and Salman Khan. Their faces were cropped based on 68 landmark points (see Fig. 3a, Section 3.1) and morphed using a generalized face morphing algorithm (Section 3).
- **Experiment Scenarios:** Proposed framework was evaluated through comprehensive experiments across three scenarios. The first involves binary classification of original vs. morphed im-

Kapoor, J., Singh, P. and Mohanty, M.
MorphDet: Towards the Detection of Morphing Attacks.
DOI: 10.5220/0013623200003979
In *Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT 2025)*, pages 729-734
ISBN: 978-989-758-760-3; ISSN: 2184-7711

ages. The second extends to a three-class setting: Individual 1, Individual 2, and morphed. This scenario also includes sub-cases with plain faces, beards, eyeglasses, and both features. The third scenario uses four subjects and their six morph combinations, resulting in ten classes overall.

- **Comparative Performance Analysis:** The performance of the proposed model is compared with other pre-existing models: Alexnet and VGG16.

2 RELATED WORK

This section reviews the literature on face morphing detection:

Jager et al. conducted early studies on human perception of morphed images, finding that observers struggled to detect morphing based on various parameters (Jäger et al., 2005). Similarly, Kramer et al. noted difficulty in identifying morphing when only a single image was presented (Kramer et al., 2019).

Ulrich et al. proposed a conceptual framework for evaluating face morphing detection methods and highlighted challenges like the quality of morphed images (Scherhag et al., 2019). Seibold et al. introduced a reflection analysis method using 3D models to detect morphing, though it lacked automation (Seibold et al., 2018).

Luuk et al. showed that morphing detection can be more robust when trained on diverse datasets (Spreeuwers et al., 2018). They recommended testing on datasets with different sources and morphing methods.

Recent automatic Morphing Attack Detection (MAD) approaches include single-image (S-MAD) and differential-image (D-MAD) methods. S-MAD detects morphing from a single image but is limited by training data, while D-MAD is considered more promising due to its ability to use trusted reference images (Ferrara et al., 2014).

Tom Neubert developed a model for detecting face morphing using image degradation, with accuracies of 91.3% in lab conditions, 85.9% in testing, and 68.4% in real-world scenarios (Neubert, 2017). This paper extends face morph detection using CNN and ResNet-152, focusing on single-image-based MAD across various scenarios.

3 MORPHING PIPELINE

This section discusses the generalized face morphing algorithm step by step. The overview of the basic steps is presented briefly in the flowchart in Fig. 2.

3.1 Locate Landmark Points

The first basic step of face morphing is to locate landmark points for both the images that are intended to morph. Landmark points are the primary features of a face such as eyes, nose, lips, eyebrows, etc. These are used to identify where the human face is located in the whole image and track key-points from a human face. Consider two images shown in Fig. 1 (a) and Fig. 1 (c) as I_1 and I_2.

There are 68 landmark points in the image which covers the region around eyes, eyebrows, nose, mouth, chin and jaw. Also, since this is a one–to–one correspondence, the number of landmark points in I_1 will be equal to the number of landmark points in I_2. So, we have two sets S_{I_1} and S_{I_2} of landmark points for images I_1 and I_2 respectively.

$$S_{I_1} = p_1, p_2, p_3, .., p_k \tag{1}$$

$$S_{I_2} = q_1, q_2, q_3, .., q_k \tag{2}$$

Further, calculate a weighted mean of the points in the two sets, based on the value of α and obtain another set of landmark points for the morph image I_M. Let this set of points be denoted by S_{I_M}.

So, $S_{I_M} = i_1, i_2, i_3, .., i_k$
where

$$i_k = (1-\alpha) \cdot p_k + \alpha \cdot q_k \tag{3}$$

The landmark points for I_1 and I_2 are shown in Fig. 3.

3.2 Delaunay Triangulation

Now, find delaunay triangles using a set of landmark points S_M calculated in the above step which divides the input images and the morph image into many small triangles.

Further, the triangulation is performed for the other two sets of point S_{I_1} and S_{I_2}, giving a one to one correspondence between triangles from image I_M. In Fig. 4, we can see the delaunay triangulation of both the images.

3.3 Affine Transformation

Here, the transformation of the triangles of image I_1 and I_2 to the dimensions of corresponding triangles in morph image I_M is done.

For this, select a triangle T_1 from image I_1, its corresponding triangle T_M in the morph image I_M, and calculate the affine transform that maps the three corners of the triangle T_1 in image I_1 to the three corners

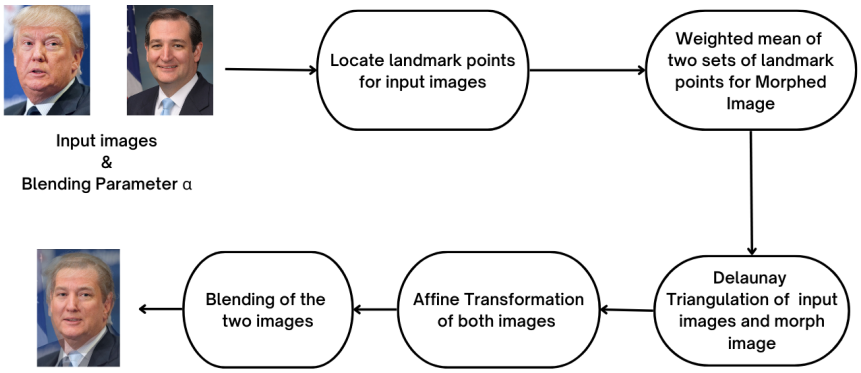
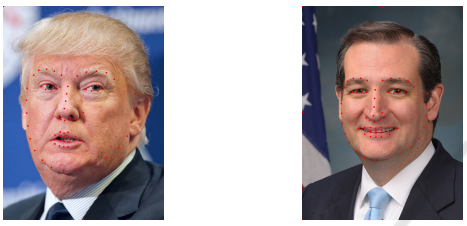


Figure 2: Flowchart of face morphing.



(a) Image 1 (b) Image 2

Figure 3: Landmark Points of two Images.

(a) Image 1 (b) Image 2

Figure 4: Delaunay triangulation of two images.

of the corresponding triangle T_M in the morphed image I_M. Then, apply affine transform to all the triangles which applies the transformation matrix pixel by pixel in image I_1 to get the warped image I_1'. Similarly, get the warped image I_2' using image I_2.

3.4 Blending

After the alignment of the two contributing images, blend the two images to get the morph image and the most frequent way of blending for face morph creation is alpha blending.

The equation for alpha blending is given as:

$$M(x,y) = (1-\alpha)\cdot I_1'(x,y) + \alpha \cdot I_2'(x,y) \qquad (4)$$

where I_1' is warp image of image I_1 and I_2' is warp image of image I_2.

The morphed image of the two contributing images is shown in Fig. 1.

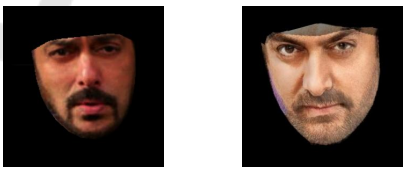
4 DETECTION OF FACE MORPHING ATTACKS

In this section, details of the various experiment scenarios, description of the dataset collected, and the findings pertaining to the experiment scenarios are discussed. In order to identify face morphing attacks, the CNN-based RESNET-152 model is exploited and trained using batch size of 64, number of epochs as 30, and learning rate as 0.001.

4.1 Experiment Scenarios

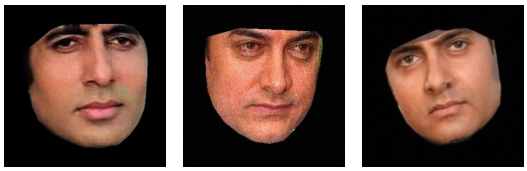
This sub-section describes the experiment scenarios:

1. **First Scenario:** The first scenario detects whether a given image is original or morphed. It is a binary classification and considers two classes: original image and morph image.



(a) Original Image (b) Morphed Image

Figure 5: First scenario.



(a) Amitabh (b) Aamir (c) Morphed

Figure 6: Second scenario sub-dataset 1.

2. **Second Scenario:** The second scenario extends classification by detecting whether the image is original or morphed and identifying its class. It

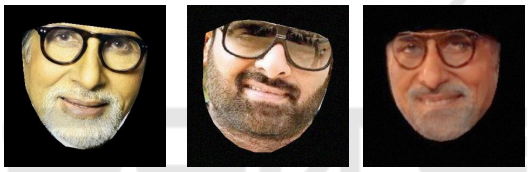
(a) Aamir (b) Salman' (c) Morphed

Figure 7: Second scenario sub-dataset 2.

(a) Salman (b) Amitabh (c) Morphed

Figure 8: Second scenario sub-dataset 3.

includes three classes: Individual 1, Individual 2, and morphed. Four sub-scenarios were tested: plain faces, bearded faces, faces with eyeglasses, and faces with both features.



(a) Amitabh's Image (b) Prabhas' Image (c) Morphed Image

Figure 9: Second scenario sub-dataset 4.

3. **Third Scenario:** The third scenario extends second scenario to four subjects and six different morphed image combinations by combining any two individuals at a time. In total, ten classes are considered here.

4.2 Database

Dataset was collected for carrying out the experiment for the three aforementioned scenarios. In the dataset, every image has a frontal view of a person's face, as necessary for passport photos. The captured individual has open eyes, a closed or open mouth, eyeglasses, a beard face, varied perspectives, and different brightness and contrast settings.

1. **First Scenario:** For this scenario, we used a total of 18488 images for training, 4623 images for validation, and 5779 photos for testing. This scenario involves identifying if the image is a morph or the original.
2. **Second Scenario:** The dataset contains a total of $28,890$ images, divided across four sub-scenarios: simple faces, faces with beards, faces with eyeglasses, and faces with both beards and eyeglasses. For each sub-dataset, the training/validation/testing split was as follows: simple faces—$3834/959/1198$; beards only—$5558/1389/1736$; eyeglasses only—$1682/336/421$; and beards with eyeglasses—$7268/1817/2271$.
3. **Third Scenario:** In this scenario, total of 18488 training Images, 4623 validation images and 5779 testing Images were used. In total, ten classifications are taken into account here.

4.3 Experiment Results

This sub-section presents the results of the experiments conducted to validate the proposed detection model. The accuracy of the classification scenarios are summarized in Table 3.

1. **First Scenario:** Here, total number of testing samples considered were 5779, out of which 5221 testing samples were classified correctly. Hence, the accuracy obtained here is 90.37%.

Table 1: Confusion matrix for binary classification.

Classes	0	1
0	108	36
1	1	143

2. **Second Scenario:** Here, we examined four sub-scenarios: the first with only plain face images, the second with bearded face images, the third with face images wearing eyeglasses, and the fourth with beards and eyeglasses. The result of those 4 sub-scenarios is as follows.
   (a) In sub-scenario 1, simple face images without eyeglasses or beards were used. Images of 4 individuals and their morph combinations were tested in 6 pairwise experiments (e.g., Aamir–Amitabh, Aamir–Prabhas), as shown in Table 2. The average classification accuracy across these experiments was 80.55%.
   (b) For sub-scenario 2, we used beard face images without eyeglasses. For this also, we followed the same approach as for the sub-scenario 1 and averaged the accuracy over all the iterations and got an accuracy of 86.01%.
   (c) For sub-scenario 3, we used eyeglasses face images without beard. Similar iterative process done here also as for earlier sub-scenarios and calculated the average accuracy to be 74.22%.
   (d) For sub-scenario 4, we used face images having both beard and eyeglasses. Similar

(a) Aamir's Image (b) Amitabh's Image (c) Prabhas' Image (d) Salman's Image (e) Morphed Image.

(f) Morphed Image (g) Morphed Image (h) Morphed Image (i) Morphed Image (j) Morphed Image

Figure 10: Third scenario.

Table 2: Second scenario accuracy table.

Sub-scenarios	Individual 1	Individual 2	Morphed	Resnet-152	VGG16 (Pre-trained)	Alexnet (Scratch)
Simple Face Images	Aamir	Amitabh	Morph	83.68%	93.33%	61.05%
	Aamir	Prabhas	Morph	88.73%	77.46%	53.52%
	Aamir	Salman	Morph	76.49%	73.67%	76.61%
	Amitabh	Salman	Morph	84.40%	84.62%	73.18%
	Amitabh	Prabhas	Morph	93.47%	86.96%	77.53%
	Prabhas	Salman	Morph	96.86%	92.95%	89.03%
Beard Face Images	Aamir	Amitabh	Morph	85.01%	76.57%	52.58%
	Aamir	Prabhas	Morph	87.87%	87.65%	46.49%
	Aamir	Salman	Morph	83.23%	92.95%	65.52%
	Amitabh	Salman	Morph	85.65%	81.17%	58.30%
	Amitabh	Prabhas	Morph	94.12%	88.08%	67.88%
	Prabhas	Salman	Morph	88.96%	80.16%	61.60%
Eyeglasses Face Images	Aamir	Amitabh	Morph	97.29%	76.38%	83.78%
	Aamir	Prabhas	Morph	94.36%	84.51%	53.52%
	Aamir	Salman	Morph	97.77%	93.21%	66.66%
	Amitabh	Salman	Morph	95.36%	69.54%	53.64%
	Amitabh	Prabhas	Morph	97.61%	79.69%	59.52%
	Prabhas	Salman	Morph	98.36%	81.97%	66.39%
Beard and Eyeglasses Face Images	Aamir	Amitabh	Morph	95.52%	89.31%	56.21%
	Aamir	Prabhas	Morph	88.02%	91.55%	53.52%
	Aamir	Salman	Morph	90.18%	96.93%	56.44%
	Amitabh	Salman	Morph	96.31%	92.03%	55.41%
	Amitabh	Prabhas	Morph	93.66%	94.07%	56.58%
	Prabhas	Salman	Morph	95.63%	86.27%	68.17%

Table 3: Comparative analysis of the proposed model with other state-of-the-art approaches.

	Resnet-152	VGG16	Alexnet
First Scenario	90.37%	84.38 %	93.21%
Second Scenario sub-dataset 1	87.27%	84.83%	71.83%
Second Scenario sub-dataset 2	87.47%	84.43%	58.72%
Second Scenario sub-dataset 3	96.79%	80.88%	63.91%
Second Scenario sub-dataset 4	93.22%	91.69%	57.72%
Third Scenario	45.53%	45.12%	50.72 %

iterative process done here also as for earlier sub-scenarios and calculated the average accuracy to be 86.78%.

3. **Third Scenario:** In this scenario, there are 10 classes for classification. Four classes for individuals and six classes for the morphed images. Here, as shown in Fig. 10, class 0 is Aamir khan (Fig. 10a), class 1 is Amitabh bachchan

(Fig. 10b), class 2 is Prabhas (Fig. 10c), class 3 is Salman khan (Fig. 10d), class 4 is morph image of Aamir khan and Amitabh bachchan (Fig. 10e), class 5 is morph image of Aamir khan and Prabhas (Fig. 10f), class 6 is morph image of Aamir khan and Salman khan (Fig. 10g), class 7 is morph image of Amitabh bachchan and Prabhas (Fig. 10h), class 8 is morph image of Amitabh bachchan and Salman khan (Fig. 10i), and class 9 is morph image of Prabhas and Salman khan (Fig. 10j).

The total number of testing samples used were 5779, out of which, the number of correctly classified were 2631. Hence, the accuracy came out to be 45.53%.

4.4 Comparative Performance Analysis

To validate the performance of the proposed Resnet-152 model, we compare it with pre-trained VGG16 and Alexnet models. VGG16 and Alexnet were trained and tested on our dataset, with input sizes of 224×224 and 227×227, respectively, while Resnet-152 used 256×256 images. All models were trained for 30 epochs, with batch size 64 and a learning rate of 0.001. VGG16 is a 16-layer model using transfer learning, and Alexnet is an 8-layer CNN. While using pre-trained models yielded better results, Alexnet was implemented from scratch to reduce overfitting. We found that Alexnet performed well for binary classification but struggled as the number of classes increased. Overall, Resnet-152 proved to be the most efficient model.

5 CONCLUSION

In this paper, a model is proposed to detect face morphing attacks. Various experiment scenarios, i.e. simple face morphs, face morphs with beards, face morphs with eyeglasses, and face morphs with a combination of beards and eyeglasses are considered to validate the proposed model. A dataset covering these scenarios is also contributed to carry out the experiments. Further, a comparative performance analysis using the dataset is done with the popular pre-existing CNN models: Alexnet and VGG16. As a whole, the proposed Resnet-152 has shown better performance in terms of accuracy. In future, we plan to extend this model for more possible attack scenarios and test the scalability with other available benchmark datasets.

REFERENCES

E-loan app: Woman sent morphed pic. https://timesofindia.indiatimes.com/city/mumbai/e-loan-app-woman-sent-morphed-pic/articleshow/91930043.cms. [Online; accessed 01-Jun-2022].

Bayometric. How biometric identification for airport and border security can deter illegal border crossings? https://www.bayometric.com/biometric-identification-for-airport-and-border-security/. [Online; accessed 02-August-2022].

Biometrika. Introduction to biometric systems. http://www.biometrika.it/eng/wp_biointro.html. [Online; accessed 02-August-2022].

Ferrara, M., Franco, A., and Maltoni, D. (2014). The magic passport. *IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics*.

findbiometrics. Border control and airport biometrics. https://findbiometrics.com/applications/border-control-airports/. [Online; accessed 02-August-2022].

Fox news, y. Fox news aired a bizarre fake photo replacing jeffrey epstein with the judge who signed off on trump's search warrant. https://www.yahoo.com/news/fox-news-aired-bizarre-fake-153544605.html. [Online; accessed 02-August-2022].

Jäger, T., Seiler, K., and Mecklinger, A. (2005). Picture database of morphed faces (mofa): technical report. http://psydok.sulb.uni-saarland.de/volltexte/2005/505/.

Kramer, R. S., Mireku, M. O., Flack, T. R., and Ritchie, K. L. (2019). Face morphing attacks: Investigating detection with humans and computers. *Cognitive research: principles and implications*, 4(1):1–15.

Neubert, T. (2017). Face morphing detection: An approach based on image degradation analysis. In Kraetzer, C., Shi, Y.-Q., Dittmann, J., and Kim, H. J., editors, *Digital Forensics and Watermarking*, pages 93–106, Cham. Springer International Publishing.

Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., and Busch, C. (2019). Face recognition systems under morphing attacks: A survey. *IEEE Access*, 7:23012–23026.

Seibold, C., Hilsmann, A., and Eisert, P. (2018). Reflection analysis for face morphing attack detection. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pages 1022–1026. IEEE.

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