



A Survey of Morphed Face Image Detection Methods

¹Maddi Satya Rohit, ²Er. Rajani Misra

¹Research Scholar Student, ²Assistance Professor,
¹MTech (CSE),

¹Chandigarh University, Punjab, India

Abstract: Technology is developing at a rapid rate, and many security problems are emerging along with it. One of the biggest problems with biometrics recognition technologies is that the system has numerous security flaws, and morph face attacks are becoming more frequent nowadays. Several authors offered different approaches to the problem in different sectors using different procedures. The "detection equal ratio" or comparing the genuine image and morphing image is one of the most important operations. The "CNN" method, which is used for segmentation and feature extraction, is the major algorithm the authors have used. The report also contrasts the numerous research techniques employed by the writers to discover the modified facial image and it's for issue the various author provided various solutions in various fields with various processes .in the most significant processes were the take the "detection equal ratio" or comparing the bonafide image and morphed image. the main algorithm used by the authors was the "CNN" which is used for the segmentation and feature extraction. further, the paper compares the various research methods used by the authors to find out the morphed face image and its detection ratio.

Index Terms – CNN, REST-NET, VG NET

I. INTRODUCTION

Face recognition is a well-established and widely acknowledged technology for biometric-based security solutions in many access control applications [1] [2]. One of the most common biometric applications is automated border crossing enabled by a biometric passport (ePass). ePassports are created in accordance with International Civil Aviation Organization (ICAO) regulations and can store metadata and biometric information. [3] [4]. A major flaw in the passport issuance process is how the applicant's facial image is processed. The face attack is a variant of the attack scenario. Blending two or more separate individual headshots of her affected into one of her yields an artificial face image. The effectiveness of such tampering attacks has been scientifically proven. vulnerability of the industrial FRSto morphing face attacks was originally studied in . Landmarks on either side are recognized [5] and Create morphedface image that represents either faces equally. (fig-1)Skin or the hair color will then need to be corrected, and manual retouching may be required to remove the artifacts. [6]. Approach to detect morphed face attacks described in focuses on patterns of morphed face attacks in digital form. This includes his electronic image-based VISA ap- plication in New Zealand and the one used for e-passport renewals. [7]. However, many countries (including most Schengen countries in Europe) require you to submit a printed headshot to authorities during the application process.For live registration under observation, morphing face attacks are irrelevant [8]of an official. Therefore, we argue that the detection of deformed face attacks is more difficult because information is lost during face photo processing,so the detection of deformed face attacks are not limited to digital domain. It also includes detection of deformed face attacks preorder printing and scanning. Adds noise and graininess. Therefore, the purpose of the study is to evaluate whether a scientific finding on a duplicate of the image and detection of morphed face attacks can be appliedto real-world situations. [9]. The complexity of creating morphed face images stems from a lack of freely available duplicate tools (such as GIMP and GAP, which can create high-ratting morphed face images with minimal effort to



FIGURE 1. Morphed face image

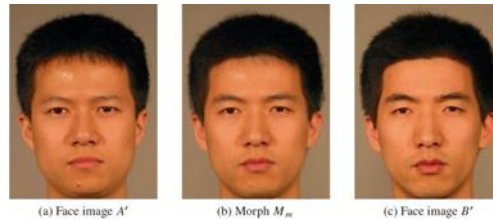


FIGURE 2. MORPHED FACE IMAGE ON LANDMARKS BASED

identify important facial regions, etc.), but the process is relatively simple. These features highlight the importance of recognizing morphed facial images to prevent unauthorized passport holders from passing through automated gatesystems. [10] [11] [12]. Adaptations of such algorithms designed to detect digital forgeries have yielded promising results in detecting altered headshots. In particular, he proposed PRNU-based detection of altered face photos [13] [14]. The extraction of PRNU and examination of distributions across picture cells have been shown to consistently detect morphed face photos, however the method fails when image postprocessing, such as histogram equalisation, is performed to generated morphs. [15] [16]

approach has inspired the work reported in this study presenting the PRNU analysis of variance for identifying morphing face images. Increasing the variance of multiple her PRNU statistics across image cells has been shownto be a valid predictor of image morphing. [17] [18] Moreover, our improved PRNU-based morph detector has proven to be resistant to standard post-processing methods. Finally, the given approach specifically analyzes the interrelationships of image blocks rather than image attributes that may result from a particular morphing technique applied to a particular face database, making it particularly suitable for any post-processing. expected to be more resilient than [19] [20]. Sect describes in detail the proposed morph detection method. Provides technology to detectmorphing facial photo attacks based on digital patterns, such as those used for ePassport renewals in New island onefacial pictures area unit uploaded electronically. However, several countries (including most of the ecu Schengen countries) need you to submit a written headshot to the authorities throughout the appliance method.

Considering this real-world state of affairs of written and scanned facial pictures, this study focuses on the impactof print-scan strategies of digitally morphed facial pictures on FRS and morphing detection. [21] The printing and scanning method introduces noise and coarseness to facial pictures, moving the effectiveness of varied FRS and facialimage recognition algorithms. [22]. Despite this noise, morphed facial pictures are shown to create a big threat to biometric identification systems even when being written and scanned. malformed face image.

II. SUEVEY OF THE PAPERS

The author proposed a model that combined the distance-based and angle-based models. These are the two categoriesproposed by the author in the study [13]. Using distance-based learning, the model can determine the distance between the eyes, nose, and mouth, and using angle-based learning, the model can determine whether the image is original or morphed. a unique approach for altered facial picture identification based on the computation of discrepancies between. Landmarks from the attacker's authentic (i.e., supervised) probing images and landmarks from registered (i.e., allegedly morphed) images. This study will set up a new database for the experiment. [12] two distinct -Both authentic and altered photos were created using morphing techniques. methods. Landmarks in both photos (actual image Ib and passport photo Ip) are identified using face recognition predictors from Idlib(fig-2). This gives the absolute positions of the 68 facial recognition points (10...167). Landmarks in a scaling-resistant system are normalized between 0 and 1. For this purpose, the green and yellow points represent upside left (0.0, 0.0) and lower right (1.0, 1.0) normalization bounds. position of landmarks vary depending on the face area, stance, and emotion. Even if the photos used in this work are normalized in accordance with ICAO guidelines, slight position differences and expressions are unavoidable. [16] To find the optimal outcomes to detect, the author applied machine learning techniques.500 estimators in a Random Forest Without a kernel, SVM SVM with a kernel based on the radial basis function (RBF) Using an SVM model with an RBF kernel may yield the best results. The morph face detection methods weretested on diverse datasets by the authors. Based on the modified face image, there are vulnerable attacks. Attackers can readily access security procedures and gain the information they need to avoid assaults that require an algorithm

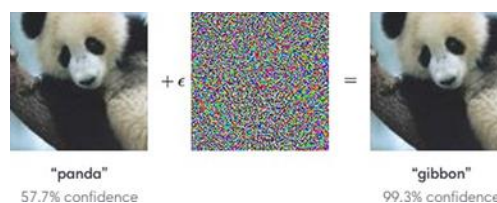


FIGURE 3. PRNU based detection

to recognise the modified face image by carrying out these vulnerable attacks. The detection methods were applied to the various [13] datasets as part of the segmentation and feature extraction procedure by the authors. Bonafide picture calculates the detection ratio of the model based on feature extraction from bona fide and morph images. When the attacks are addressed, the dataset's robustness to detect the original facial image is increased. [12] The four major steps to detect the morph face are discussed in this article.

1. Data Preparation
2. Mistake in detecting
3. Estimate of robustness
4. Validation of robustness The authors calculated the rate of detection of the morph face image based on the four processes. This suggested architecture will also lessen the overfitting risk in the data set. The authors employed the surf detection approach for segmentation. By employing surf detection, [14] the authors determined the important points of the photos to provide correct output. The author adjusted the image's sharpness to improve the texture's performance. The training databases are used to extract feature vectors. Support vector machines (SVMs) are available to help with each algorithm. Using disparate training sets.

For a given facial image, the SVMs of every single algorithm generate a normalized attack. The detection score. The authors proposed an image detection mode using the PRNU variance analysis. The PRNU variance analysis analyses photo response non-uniformity and is based on the image's cell (fig-3). It is feasible to tell difference between genuine image and morphed image by capping cells in the image. The author took the 961 bona fide photos and the 2,414 automatically morphed images [4] and obtained the 10.5 detection ratio or detection error for that dataset. Both the original and triangulation maps are twisted by the resulting triangulation. After acquiring the resulting triangulation, I conducted the alpha blending to achieve the final output. The PRNU offers significant advantages for detection of altered face photos. [5] First and foremost, as previously stated All virtual image sensors, according to (Fredrich et al.) display PRNU. As a result, sensor noise may be found in practically every image captured. It is also reported to be resistant to high-quality printing and scanning, as well as being independent of scene content and resistant to standard processing methods like as lossy compression or gamma correction. Furthermore, while the PRNU is in principle independent of the visual content, its high-frequency components may interfere with the PRNU. However, different PRNU improvement approaches can reduce this influence. This work extends the technique by investigating the PRNU variance for morphing faces. Image recognition. Because of the nature of the morphing process, which produces inhomogeneous adjustments across distinct image regions, there is an increased variation. The PRNU signal is expected to go across picture cells. Response comprehensive The author employed deep CNN to extract image attributes from digital and printed scanned facial images to determine the morph image. [3] The authors demonstrate the security issue of morphing face photos, which they highlight as occurring throughout the passport or visa application procedure. Generally, for the passport process, printed scans of photographs are taken or some are digital images, but extracting the features from the digital images is a very tough procedure, thus the author devised a solution to extract the features by using the deep caching network. CNN is commonly used for segmentation and feature extraction. Electronic commerce is defined as the sale of electronic items. [6] The author employed two deep CNN layers, VGG19 and ALEXNET; both layers are specified for fine adjustment. The proposed method was utilised on the live problem or screencast. Run the model to apply the deep CNN layers' transfer learning approach to the first layers of the fusion. after the model is finished tweaking the photos present in the dataset. e Conv3 is the fine-tuned AlexNet function with convolution filter size 33 and length 384. It is important to note that each convolution filter exhibits both face and texture aspects. In addition, the highlighted regions (different colors) show facial features in highly trained AlexNet.. [10] Equivalent observations can be obtained using Conv3 layers and fine-tuned VGG19 of length 256. The first fully connected layer (FC-6) features were obtained from both AlexNet and VGG19, and the pre-trained D-CNN network was applied to the training set corresponding to both real and manipulated headshots. is fine-tuned using the facial image of Allow the FC-6 function obtained from AlexNet as FA and the VGG19 function as FV. The collected features were then concatenated into a single feature vector $T_{rF} = [FA || FV]$ and used to train P-CRC. The test face images F_{Te} are separately projected onto the FC-6 layers of AlexNet and VGG19 D-CNN to recover the associated features F_{TeA} and F_{TeV} . APCER is the percentage of attack presentations (morphed face samples) that are incorrectly classified as genuine under certain circumstances. BPCER: Percentage of actual presentation. [8] The recommended method yielded the lowest detection equivalent error rate (D-EER) of 8.23 for the digital image database, 17.64 DEER for printed scans (HP), and 12.47 D-EER for printed scans (HP). Yes (Ricoh). The BSIFSVM approach offers the second best detection performance for presentation assaults in a given context (i.e. altered image). The author investigated the vulnerable assault on the morphing facial image and how it leads to security vulnerabilities. The morphing facial image is made unnaturally and automatically. and then blended with the original image to create the new image (fig-4). The author estimated the image detection error for the new image. There is a wide spectrum of attacks on the printed and digital picture these days. [9] The "BPCER10" and "BPCER20" are used to mitigate that assault. In general, the ePass application procedure involves taking a photo, printing the photo on the ePass, and then converting the photo into digital format when the visa process goes under the scanner to scan [3] the photo, the snapshot is translated into digital format and the attack will happen. A new library of altered facial photographs was created by first printing the digitally transformed photographs and then scanning them using a variety of techniques. We started with an existing digitally morphed face database (including cropped grayscale photos) and added a slightly larger test set of 231 morphed images and 462 similar unmorphed faces. . As part of this project, several FRS vulnerabilities are reported.: [5]

1. Presentation Match Rate for Impostor Attacks (IAPMR)
2. Error Rate in Attack Presentation Classification (APCER)
3. Error Rate in Presentation Classification (BPCER)
4. .BPCER10
5. BPCER 20
6. FAR AND FRR

The analysed methods increased the BPCER10 by more than 20percentage absolute, with line scans having a greater influence than flat bed scans. The flat-bed scanner's absolute BPCER20 grew by 28.57 percent, while the linescanner's climbed by 31.6 percent.. [1] [16]

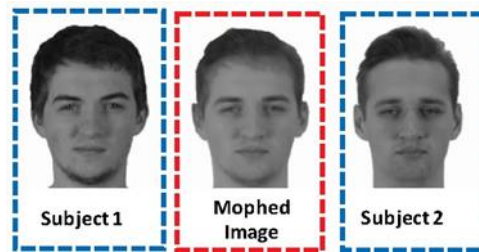


FIGURE 4. Morphed face image using CNN

III. METHOD OF THE PROCESS

The segmentation technique is critical for the image detection part. To perform a better process, the image is divided into segments. Taking the image directly to process consumes a lot of space and time. The image can be divided into pixels using segmentation. Finding the accurate pixel [8] by going through that process is a pretty simple undertaking. There are several sorts of segmentation processes in deep learning models, but surf segmentation is one of the best [11].

3.1 Surf Segmentation

The technique of dividing an image into layers and delivering each pixel in that image is known as segmentation. Surf segmentation is one of the primary operations in the segmentation phase of the surf algorithm. The photograph will depict breach breaks, point breaks, and reef breaks (fig-5). The image was represented as a three-layer surface plot during the process.

The surf segmentation boosts the image's "robust feature" speed. By enhancing the robust feature, it is easier to discern the image's flaw rejection ratio and flaw detection ratio. [10]

One type of categorization procedure is sand segmentation.

It categorizes and names the image. When you apply the surf approach to an image, it will extract the feature based on the distance and angle between the features, making feature extraction pretty simple.

The surf method is faster than the smooth method. Although more computationally intensive than the surf method, the sift method extracts image features. On larger scales, however, techniques show that sift outperforms surf. [12]

The CNN and YOLO algorithms are frequently used in segmentation. When the image is large, the quick techniques work together to speed things up and increase the contrast.

The most common use of robustness analysis is to identify image noise. During the image classification process, it also reflects image noise.

the tenacity During the classification process, when the classifier is deleted or added to the model, it calculates the coefficient of the pictures. In image processing techniques, contrast is frequently used for hypothesis testing. It investigates the defined performance of the model during the running state. Robustness is a four-step procedure for categorizing images. [9] [13]

1. preparation of data
2. estimate of detection error
3. estimate of robustness
4. Validation of robustness

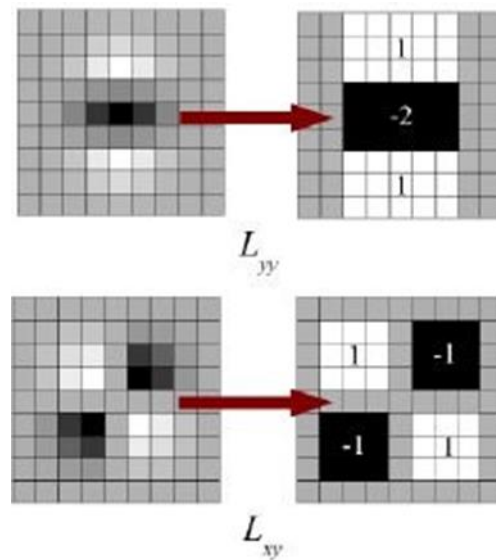


FIGURE 5. Surf detection graph

3.2 Preparation Of Data

The info is employed to make prime quality facial morphs. first time The info is split into 2 areas: The coaching set went to train every feature extractor and classifier for the check set. His 2 latter datasets area unit referred to as the analysis set and therefore the validation set.

3.3 Estimate Of Detection Error

Evaluate the primary recognition error victimization the coaching set and also the best guess. the edge is mounted. Detection errors within the check and analysis sets square measure then evaluated supported the chosen call threshold.

3.4 Estimate Of Robustness

The toughness (or brittleness) of a fabric is calculated as a operate of t and e . additionally, acceptable exclusion criteriaar outlined to get rid of morph detectors that ar unfeasible with reference to the algorithmic program and parametersused.

3.5 Validation Of Robustness

Finally, the lustiness of chosen morph recognition approach verified on validation set.

IV. FEATURES EXTRACTION

To preserve local information, preprocessed face images are optionally split into 44 cells during feature extraction. That is, the feature extractor is applied to each texture cell individually to build the final feature. The vector formation is the result of concatenating the features. [19] retrieved vectors from each cell

Texture descriptors like native binary pattern (LBP) and binarized applied mathematics image options ar extracted from the cropped face image (BSIF). Readers ar inspired to be told additional concerning these texture descriptors. LBP merely analyzes neighboring element values for every element, whereas BSIF uses a special filter learned from a series of pictures. The ensuing feature values ar saved in an

exceedingly bar chart. [20] Using a keypoint extractor, accelerated strong options (SURF) extracts a group of native keypoints. Readers square measure inspired to scan any material on keypoint detection, keypoint descriptor extraction, and keypoint matching. A key purpose extractor is employed as a result of morphed pictures square measure expected to possess fewer key purpose locations outlined as maxima and minima as a results of mathematician operate variations. [21] A gradient estimator is constructed by extracting the histogram of gradients (HOG) and sharpness properties from the normalized grayscale image. See HOG for more information. The 2D gradient average is computed as the sharpness feature. A gradient-based approach is used because morphing process minimizes high-rate changes and consequently, gradient steepness. [22]

V. RESULTS AND DISCUSSION

5.1 A Overview of Morph face Image Detections

AUTHOR	TECHNIQUES USED	ALGORITHMS	AUCCRACY	DETECTION ERROR
Ulrich Scherhag(et.al)	Distance based and Angle based model	Random Forest SVM(without kernel) SVM(Radial Basis Function)	the highest accuracy achieved using SVM on angle based model 87.0% using SVM(RBF) on distance-based model 84.9%	on angle-based model achieved 43.9% on distance-based model achieved 44.1%
Christian Rathgeb(et.al.)	Segmentation feature extraction robustness anaysis	Open CV robustness validation Surf algorithm	20.8% detection error on DFF 100% on COTS 48% on dff	29.3% on dff validation and 39.0% on the DFF evaluation
Luca Debiasi(et.al.)	PRNU Variance analysis	variance analysis feature extraction	attack classification error ratio = bonafide classification ratio	10.5% is detection ratio
R. Raghavendra(et.al.)	Transferable Deep-CNN	VGG18 Alexnet	94.52 achieved accuracy on svm on hp print scan	41.78 is the detection ratio
. B. Raja(et.al)	deep neural network	SVM BPCER10 BPCER20	95.9% on hp scanned images	Flase acceptance ratio(FAR) 0.1% Flase rejection ratio(FRR) 10.81%

The result and analysis consideration compared the results of paper and different techniques and algorithm in the used paper and accuracy achieved on the performance of the model. When the results of the following paper are compared, notice that the morphed image can be recognized with 100% accuracy using the robustness and CNN approaches after using the surf model. However, finding it in papers is challenging because the algorithms are difficult to utilize if the facial photographs contain any expression. After all, the authors did not use proper wording. As a result, the surf model only matches a subset of images, and finding the SCLAR image dataset is incredibly difficult. The author used the sift algorithm over the dataset to recognize SCLAR images, however, the model will need time to become sophisticated.

VI. CONCLUSION AND FUTURE WORK

The work is compared to other publications, and it is found that the morph image retrieval is 100% by using the surf and sift model on the CNN approaches, however in the case of images with facial expressions, retrieving the morphed image from the original image may be almost impossible. Moreover, the model's attack detection is also low in comparison to other papers. Author B. Raghavendra (et al.) proposed the model to improve model speed. The Alexnet uses the original image data set to extract image features, while VGG18 is used on morphing images to extract feature extraction; the authors combined both to detect the image, but the model has a 95 percent accuracy rate. In comparison to other models, however, the model is less sophisticated and has a lower detection ratio (45%). The issue is that noise detection in images is not achievable. So, the next work recommended for the morph image detection is a model with 5 layers and combined with robustness, where the YOLO algorithm is complicated and avoids expression in the image like any fault acceptance features, and robustness will avoid the noise existing in the image. false. The documents, however, have some limits.

1. Avoiding expressions is a difficult issue in distance and angle calculations.
2. to eliminate image noise
3. The model's attack precision is low.

REFERENCES

- [1] Poorya Aghdaie, Baaria Chaudhary, Sobhan Soleymani, Jeremy Dawson, and Nasser M Nasrabadi. Attention aware wavelet-based detection of morphed face images. In *2021 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–8. IEEE, 2021.
- [2] Baaria Chaudhary, Poorya Aghdaie, Sobhan Soleymani, Jeremy Dawson, and Nasser M Nasrabadi. Differential morph face detection using discriminative wavelet sub-bands. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 1425–1434, 2021.
- [3] Naser Damer, Alexandra Mosegui Saladie, Steffen Zienert, Yaza Wainakh, Philipp Terhörst, Florian Kirchbuchner, and Arjan Kuijper. To detect or not to detect: The right faces to morph. In *2019 International Conference on Biometrics (ICB)*, pages 1–8. IEEE, 2019.
- [4] Luca Debiasi, Christian Rathgeb, Ulrich Scherhag, Andreas Uhl, and Christoph 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. IEEE, 2018.
- [5] Luca Debiasi, Naser Damer, Alexandra Moseguí Saladié, Christian Rathgeb, Ulrich Scherhag, Christoph Busch, Florian Kirchbuchner, and Andreas Uhl. On the detection of gan-based face morphs using established morph detectors. In *International Conference on Image Analysis and Processing*, pages 345–356. Springer, 2019.
- [6] Muhammad Hamza, Samabia Tehsin, Mamoona Humayun, Maram Fahaad Almufareh, and Majed Alfayad. A comprehensive review of face morph generation and detection of fraudulent identities. *Applied Sciences*, 12(24):12545, 2022.
- [7] Andrey Makrushin, Christian Kraetzer, Tom Neubert, and Jana 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*, pages 49–54, 2018.
- [8] Alakananda Mitra, Saraju P Mohanty, Peter Corcoran, and Elias Kougiianos. Detection of deep-morphed deepfake images to make robust automatic facial recognition systems. In *2021 19th OITS International Conference on Information Technology (OCIT)*, pages 149–154. IEEE, 2021.
- [9] Kelsey O’Haire, Sobhan Soleymani, Baaria Chaudhary, Poorya Aghdaie, Jeremy Dawson, and Nasser M Nasrabadi. Adversarially perturbed wavelet-based morphed face generation. In *2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021)*, pages 01–05. IEEE, 2021.
- [10] Kiran Raja, Sushma Venkatesh, RB Christoph Busch, et al. Transferable deep-cnn features for detecting digital and print-scanned morphed face images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 10–18, 2017.
- [11] David J Robertson, Andrew Mungall, Derrick G Watson, Kimberley A Wade, Sophie J Nightingale, and Stephen Butler. Detecting morphed passport photos: a training and individual differences approach. *Cognitive research: principles and implications*, 3(1):1–11, 2018.
- [12] Ulrich Scherhag, Ramachandra Raghavendra, Kiran B Raja, Marta Gomez-Barrero, Christian Rathgeb, and Christoph Busch. On the vulnerability of face recognition systems towards morphed face attacks. In *2017 5th international workshop on biometrics and forensics (IWBF)*, pages 1–6. IEEE, 2017.
- [13] Ulrich Scherhag, Dhanesh Budhrani, Marta Gomez-Barrero, and Christoph Busch. Detecting morphed face images using facial landmarks. In *International conference on image and signal processing*, pages 444–452. Springer, 2018.
- [14] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Performance variation of morphed face image detection algorithms across different datasets. pages 1–6, 2018.
- [15] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Towards detection of morphed face images in electronic travel documents. pages 187–192, 2018.
- [16] Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, and Christoph Busch. Deep face representations for differential morphing attack detection. *IEEE transactions on information forensics and security*, 15:3625–3639, 2020.
- [17] Sobhan Soleymani, Baaria Chaudhary, Ali Dabouei, Jeremy Dawson, and Nasser M Nasrabadi. Differential morphed face detection using deep siamese networks. In *International Conference on Pattern Recognition*, pages 560–572. Springer, 2021.
- [18] Sobhan Soleymani, Ali Dabouei, Fariborz Taherkhani, Jeremy Dawson, and Nasser M Nasrabadi. Mutual information maximization on disentangled representations for differential morph detection. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pages 1731–1741, 2021.
- [19] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Luuk Spreeuwers, Raymond Veldhuis, and Christoph Busch. Morphed face detection based on deep color residual noise. In *2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pages 1–6. IEEE, 2019.
- [20] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Luuk Spreeuwers, Raymond Veldhuis, and Christoph Busch. Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pages 280–289, 2020.
- [21] Sushma Venkatesh, Kiran Raja, Raghavendra Ramachandra, and Christoph Busch. On the influence of ageing on face morph attacks: Vulnerability and detection. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–10. IEEE, 2020.
- [22] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, and Christoph Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE transactions on technology and society*, 2(3):128–145, 2021.