ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

DETECTING AND GENERATING FACE MORPHING ATTACKS

R.Ashok kumar[1], R.Vamshi Krishna[2], Bachu Adithya[3], P.Sai Sharan Reddy[4], I.Vijendhar Reddy[5]

Assistant professor, Department of Computer Science and Engineering[1]

Student, Department of Computer Science and Engineering[2,3,4,5]

Sree Dattha Group of Institutions, Sheriguda, Telangana. [1,2,3,4,5]

ABSTRACT

Face recognition and authentication systems are vulnerable to various illegal activities when they fail to detect morphing attacks effectively. Current systems can be compromised by sophisticated biometric manipulation techniques. This study focuses on detecting morphing attacks with an innovative approach that considers factors like age, lighting, eyewear, and headgear variations. The proposed system integrates a deep learning-based feature extractor with a classifier to enhance detection accuracy. Additionally, techniques for combining features and image enhancement are explored to further improve detection capabilities.A versatile dataset is being developed, encompassing Morph-2 and Morph-3 images generated through advanced techniques involving human participation. Morph-3 images, known for their high photorealism, pose a significant challenge in detection due to their realistic appearance, a factor not addressed in previous studies. Unlike free programs and scripts, professional morphing software produces more realistic morphs, highlighting the need for comprehensive testing across diverse face databases including Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET, and FRLL.Experimental results across various settings demonstrate promising outcomes for the proposed technique, marking a significant step forward in mitigating morphing attacks in face recognition systems.

Index Terms: Face recognition, morphing attack detection, deep learning, biometric security, image enhancement, versatile dataset, Morph-2, Morph-3, face databases.

I.INTRODUCTION

The world has become a global village with the introduction of modern technologies. Vast distances have now shrunk due to the availability of fast means of conveyance like airplanes, trains, ships and buses. These abundant conveyance options have given rise to a significant increase in the travelling population. With such a large number of mobile population, manual verification of travelling documents and facial authentication is not possible. Therefore, an automatic border control system is used for authentication and approval of passports. Border control systems are now deployed in more than 180 airports around the world . This automatic system uses face recognition system to compare the livecaptured images of the traveller with the image of traveller that is stored in the travel agency's database system or in the form of passport or any

other type of machine readable travel documents (MRTD).

After face recognition system approves that both the live captured image of the traveller and the image on the passport are same, the traveller is granted travelling authorization. In this way an automatic border control system is implemented to deal with enormous travelling population. Availability of image manipulation technology has also enabled the culprits to use this technology for fraudulent activities. In order to gain legal entry permission into foreign countries for unlawful activities many criminals are utilizing a technology called face morphing to trick the face recognition system. Image morphing has been around since 1980s but now with the ease and abundance in availabilityof software and hardware technology to the general public, creating morphed images for fraudulent activities is easier than ever. In face morphing technology the image of two or more persons can be combined or merged together in such a way that it resembles the participants of the morphed image and the facial recognition system approves the morphed image as the original image of the applicant. Furthermore, the ratio of merger of different persons in the morphed image is controlled in such a way that human inspection is also extremely difficult. Example of morphed images is shown in which two separate morphed images are created from two subjects that are resembling both subjects. By using image morphing a wanted criminal who is barred from travelling can easily morph his facial image with the facial image of an accomplice and successfully acquire travel permission in an unauthorized country.

In order to alleviate this vulnerability of the face recognition systems several methods have been proposed in the past. These methods are categorized based on their methodology of morph detection. Single image morph attack detection and differential morph detection. This study introduces a general morph attack detection model that would be able to classify a wide variety of images. Images of different types and varying features (age, expression, posture, illumination, gender, race, hair style, facial hair, head gear, eye wear) are used as different type of ID cards have different back ground colours and specifications.

II.LITERATURE SURVEY

- Fei Peng, Le-bing Zhang, and Min Long proposed that face morphing attacks pose a significant threat to existing face recognition systems. While a few face morphing detection methods have been introduced, restoring the facial image of the morphing accomplice remains challenging. In their paper, they present a face de-morphing generative adversarial network (FD-GAN) to restore the accomplice's facial image. This method uses a symmetric dual network architecture and two levels of restoration losses to separate the identity features of the morphing accomplice. By utilizing the captured facial image (containing the criminal's identity) from the face recognition system and the morphed image stored in the e-passport system (containing both the criminal and accomplice's identities), the FD-GAN effectively restores the accomplice's facial image. Experimental results and analysis demonstrate the effectiveness of the proposed scheme, showing its potential application in tracing the identity of face morphing attack accomplices in criminal investigations and judicial forensics.

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

- Andrew W. Yip and Pawan Sinha addressed a key challenge in face perception: determining how different facial attributes contribute to judgments of identity, focusing specifically on color cues. Although past research suggested that color confers little recognition advantage for identifying people, their experimental results suggest otherwise. They found that color cues play a significant role in face recognition, particularly when shape cues are degraded. Under such conditions, recognition performance with color images is significantly better than with gray-scale images. Their findings indicate that the contribution of color may lie more in aiding low-level image-analysis processes, such as segmentation, rather than providing diagnostic cues to identity.

- Ulrich Scherhag, Johannes Merkle, and Christoph Busch examined the vulnerability of facial recognition systems to face morphing attacks. Numerous approaches for morphing attack detection (MAD) have been proposed, but these algorithms often overfit to specific datasets with limited or unrealistic image characteristics. Consequently, the results may not apply to real-world scenarios. They used subsets of the FERET and FRGCv2 face databases to create a realistic database for training and testing MAD algorithms, incorporating ICAO-compliant bona fide facial images, unconstrained probe images, and morphed images created with four different tools. They applied multiple post-processings, such as print-scan and JPEG2000 compression. Their evaluation showed that algorithms based on deep face representations could achieve very high detection performance (less than 3% D-EER) and robustness to various post-processings. They also analyzed the limitations of these methods.

- Arash Samani and Xin Yuan highlighted the emerging topic of cross-modality face recognition due to the widespread use of different sensors in daily applications. They introduced the Tufts Face Database, which includes images in various modalities: photographs, thermal images, near-infrared images, videos, computerized facial sketches, and 3D images of each volunteer's face. Collected under an Institutional Research Board protocol from a diverse group of individuals at Tufts University, the database contains over 10,000 images from 113 individuals of various genders, ages, and ethnic backgrounds. This work contributes by providing a detailed description of the Tufts Face Database, making it publicly available to researchers worldwide, and offering a comprehensive review of face recognition systems and face datasets.

- D. Smythe proposed a method for fast interpolation between medical images, intended for both slice and projective interpolation. The method establishes spatial correspondence between adjacent images using a block matching algorithm, then interpolates image intensities by morphing between the images. Compared to standard linear interpolation, block-matching-based interpolation, and registration-based interpolation in 3D tomographic data sets, the morphing-based method

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 2, 2024

showed similar performance to registration-based interpolation and significantly outperformed both linear and block-matching-based methods. This method is applied in conformal radiotherapy for online projective interpolation between Digitally Reconstructed Radiographs (DRRs).

III.EXISTING SYSTEM

Researchers have recently shown a great deal of interest in the topic of morph attack detection. In order to successfully identify morph assaults, several researchers have explored this topic and used various methods. Since there aren't enough morph photos readily accessible for study, a variety of face databases are used to create morph image databases.
Another serious issue exists with the current morph detection datasets. Because these datasets have just taken two people's morphs into account (morph-2 photos), morph identification has been made easier. In addition, automated morphing pictures are generated using low-quality script-based morphing tools like FaceMorpher, OpenCV, and FaceFusion; the bulk of these altered photos may be detected by human eyes. Thus, these methods do not reflect actual criminal behaviour since they are seldom used. Despite producing relatively high detection rates on datasets with the aforementioned restrictions, methods evaluated on these datasets will not do well in real-world situations. Proper classification of morphs with significant variation and quality is still challenging. The literature presents a number of methods that use various standards. While prior work has achieved great accuracy, it was on datasets with restricted characteristics.

IV.PROPOSED SYSTEM

• This research presents a reliable detection method that accounts for differences in age, lighting, eye, and headgear.

• A classifier and a feature extractor based on deep learning are used.

• To further improve the detection results, we also suggest combining features and enhancing images.

A one-of-a-kind and varied morphing database is hand-crafted utilising expert software for this investigation.

• Included in this piece are morphed photos made from two or three subjects.

• A state-of-the-art morph detection model is trained and evaluated on the newly-created database using a feature extractor based on deep learning and a classifier based on machine learning.

• The research employs a variety of studies to examine how well the suggested morph attack detection model performs on various original and transformed picture types.

ADVANTAGES OF PROPOSED SYSTEM

- Fast and Accurate detection of morphing attacks
- Single image morph attack detectionand differential morph detection

V.SYSTEM ARCHITECTURE

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

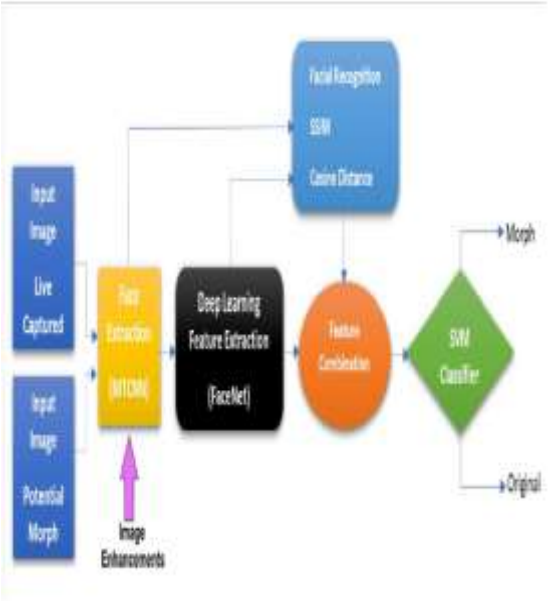


Figure .1 System Architecture

VI. IMPLEMENTATION MODULES:

A. IMAGE MORPHING

In the late 1980s and 1990s, face image morphing was used for introducing visual effects in movies and animations . In image morphing, features of two face images were compared and spatial relationship between the features was determined for combination. After the alignment of both images through warping, colour interpolation is applied to generate a new image. The new image is a mix of both input images . The varying of warping and colour interpolation was referred to as transition control. Different techniques of morphing like mesh warping [8], field morphing [9] and radial basis morphing have been used for creation of morphed faces. In mesh warping, meshes are used to link different landmarks or control points on the images of two subjects. The source image is morphed into the target image by freezing some parts of the image while warping others through control points. In field morphing, a pair of lines were used to map corresponding features between two images. Different points on the images were mapped based on their distance from the respective line. In radial basis functions, the features on the image were considered to be represented by a set of points. Different lines and curves that formulated a mesh on an image were considered as a set of points. Mapping was done from the two surfaces that were considered on both images.

B. METHODS OF MORPH ATTACK DETECTION

There are two basic types of morph attack detection (MAD) methods that are prevalent in the literature.

i).SINGLE IMAGE MAD METHOD

In these types of methods only the morphed image is analysed for presence of morphing attempt. Morphing an image leaves some artifacts in the image that are traced for detectionof morph. Texture descriptors like binary statistical image features (BSIF) are utilized for texture classification. Furthermore, ghosting or shading artifacts are also detected in such images. Similarly, deep neural network can also be trained to detect such artifacts as long as the training data contain variety of images.

ii).DIFFERENTIAL MAD METHOD

In these types of methods both the potential morph and the live captured images are analysed, compared and processed to detect morphing attempt ,Feature vectors from both images are extracted for comparison .Demorphing process is also done in some of these techniques to extract the identity of the accomplice by subtracting the live captured image from the morphed image.

C. STATE OF THE ART RESEARCH WORK

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Significant amount of work has been done in the field of morph attack detection. Different tools, preprocessing methods and databases are used for morph image creation. Overview of related literature work is shown in Table 1. Several research studies in the area of morph attack detection have reported good detection results but these studies are tested on the datasets with limited variations and lack real world scenarios. Features like variation in age, race, facial hair, head gear, eye wear, illumination, expression and posture are underutilized or not utilized at all in many studies. Similarly limited number of databases are utilized for morph attack detection. Furthermore, fixed contribution weights (attacker and accomplice) are used in creation of morphed images instead of random contribution weights from attacker's and accomplice's images. Images in which head gear and eye wear are present, resulted in incorrect classification of original images as morph images. The quality of live captured images is very high in previous studies that is not applicable for all checkpoints due to variation of available resources.

VII.RESLUTS:

Figure.2 Home page

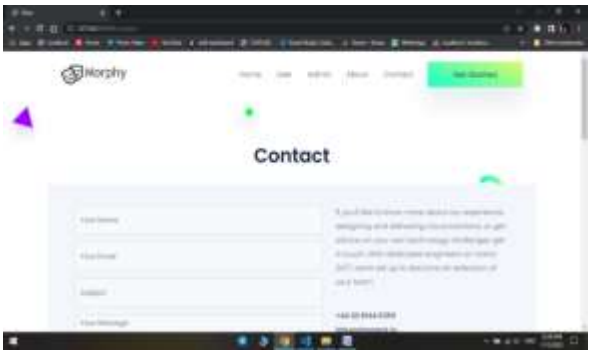


Figure.3 Contact Page

Figure .4 Login page

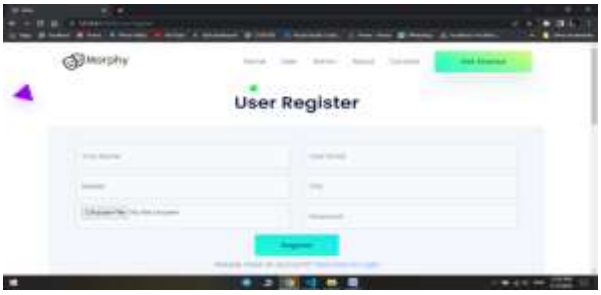


Figure.5 User Register page

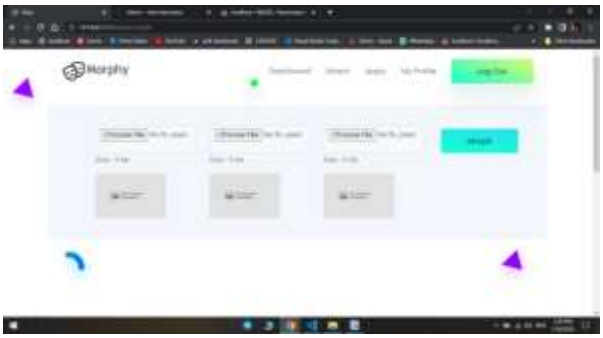


Figure.6 User Morph Uploading page

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

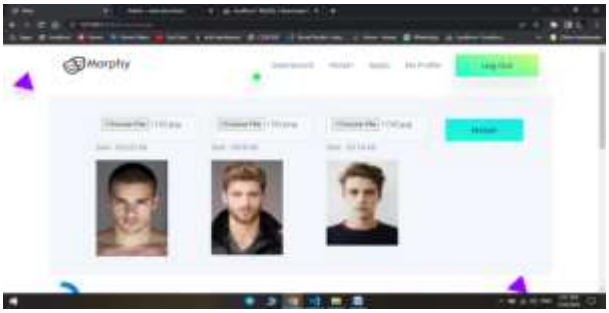


Figure.7 Uploaded

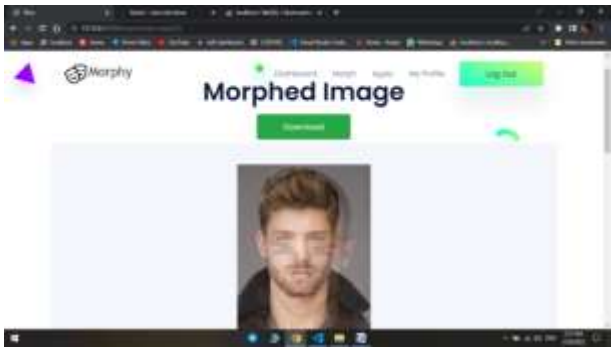


Figure.8 Image Morph

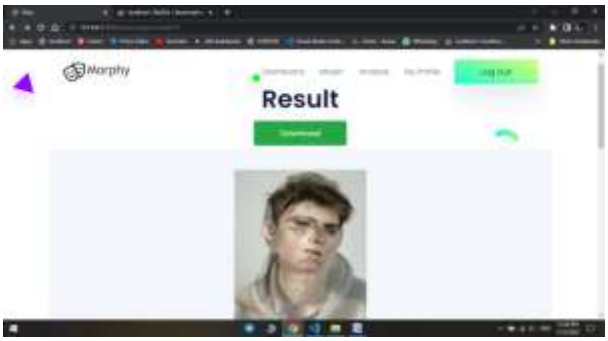


Figure.9 Result

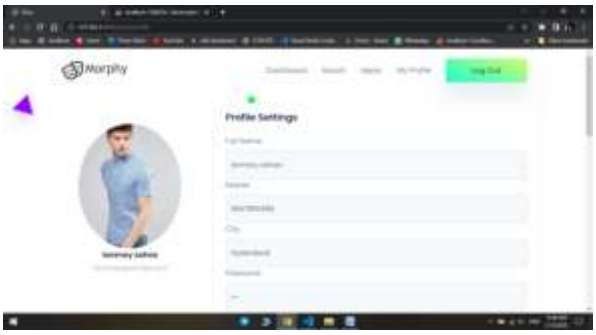


Figure.10 User Profile

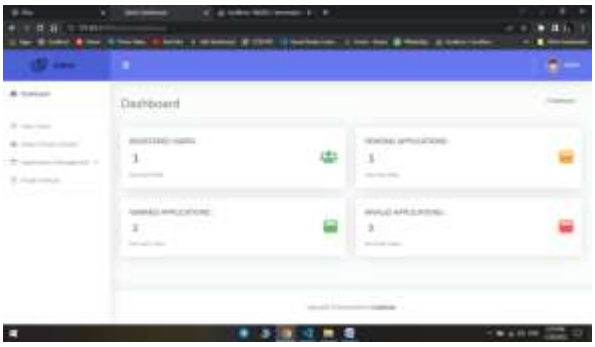


Figure.11 Admin Dashboard

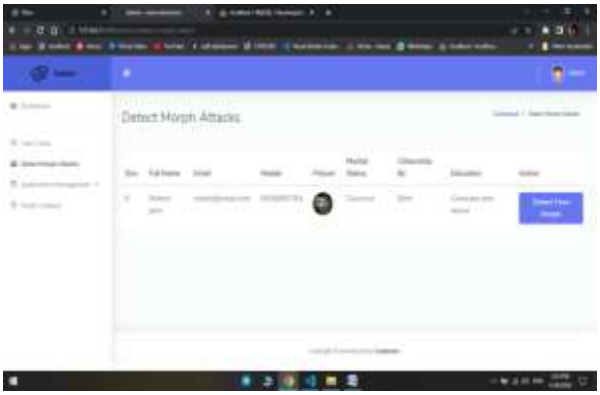


Figure .12 Detect Morph

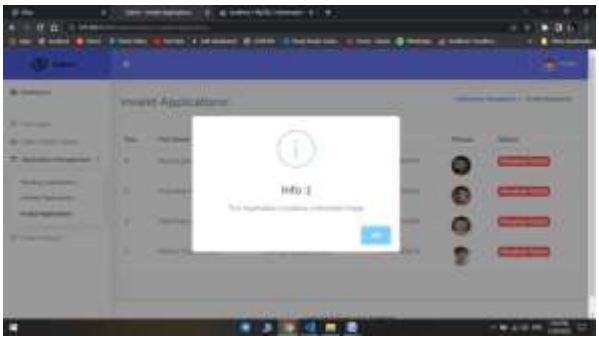
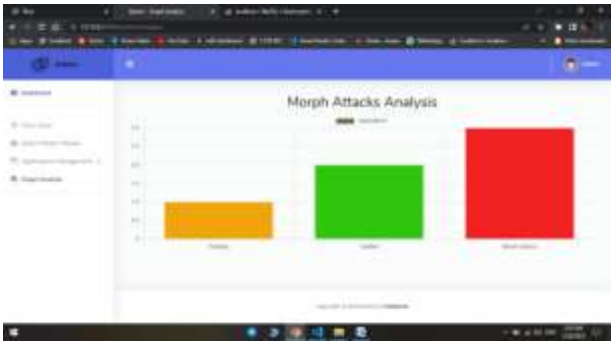


Figure.13 checking for morphed image



ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Figure.14 Morph Attack Analysis Graph

VIII.CONCLUSION

In this study, a robust and generalized morph attack detection model and a very diverse morphed database is introduced to better deal with morph attacks in a practical scenario. Different feature combination techniques are analysed and feature concatenation proved to be the best technique for morph detection. Some of the methods like feature concatenation provided better morph attack detection performance but with the increase of computational cost. Similarly, it was observed that manually created morphed images with high quality morphing tools were difficult to detect by the models that were trained on morphed databases that had low variation and were made automatically from low quality morphing tools like OpenCV and FaceMorpher using programming scripts.

The training of model on manually created morphed databases with high quality tools proved to be helpful in achieving good results and the results achieved by the model on testing data improved significantly. Proposed model gives very encouraging and improved results in case of age, illumination, posture and expression variations. Testing of morphed images was also done using different machinelearning based classifiers and SVM produced the best results. Different image enhancement techniques were also applied on image databases and it was observed that databases with low variation in illumination and colour benefited from image enhancement. Manually created morph-3 images were very difficult to detect when the model was only trained on morph-2 images created from low quality tools. After training the model on morph-3 images created from high quality tools, the performance of morph-3 detection increased significantly.

It further solidifies the approach to include diverse range of morphs in the training database to improve the robustness of morph detection model. FGNET database proved to be the most difficult database of images in terms of morph detection as it can be seen in Figure that this database has a vast range of diversity in terms of age, image quality, colour variation and expression. These extreme levels of variations led to the creation of highly complex morphed images that were very difficult to classify by the morph attack detection model.

IX.FUTURE ENHANCEMENT

Future work that can be done to improve this model and train it for all possible morph attacks in a real world deployment scenarios will require the acquisition of real morphed images that were submitted to different organizations like airports, identity card issuing authorities, travel agencies, universities and security institutions. The model should then be trained and tested on the real images to ensure better performance. Furthermore, an adaptive morph attack detection model should be designed that automatically adapts to the input images by applying the image enhancements as per requirement. More than three images may also be used for morphing.

X.REFERENCES

[1] F. Peng, L.-B. Zhang, and M. Long, ‘‘FD-GAN: Face de-morphing generative adversarial network for restoring accomplice’s facial image,’’ IEEE Access, vol. 7, pp. 75122–75131, 2019.

[2] M. Ferrara, A. Franco, and D. Maltoni, ‘‘Face demorphing,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 1008–1017, Apr. 2018.

[3] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, ‘‘Face recognition systems under morphing attacks: A survey,’’ IEEE Access, vol. 7, pp. 23012–23026, 2019.

[4] A. W. Yip and P. Sinha, ‘‘Contribution of color to face recognition,’’ Perception, vol. 31, no. 8, pp. 995–1003, 2002.

[5] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, ‘‘Deep face representations for differential morphing attack detection,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3625–3639, 2020.

[6] K. Panetta, Q. Wan, S. Agaian, S. Rajeev, S. Kamath, R. Rajendran, S. P. Rao, A. Kaszowska, H. A. Taylor, A. Samani, and X. Yuan, ‘‘A comprehensive database for benchmarking imaging systems,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 42, no. 3, pp. 509–520, Mar. 2020.

[7] G. Wolberg, ‘‘Image morphing: A survey,’’ Vis. Comput., vol. 14, no. 8, pp. 360–372, 1998.

[8] D. B. Smythe, ‘‘A two-pass mesh warping algorithm for object transformation and image interpolation,’’ Rapport Technique, vol. 1030, p. 31, Mar. 1990.

[9] T. Beier and S. Neely, ‘‘Feature-based image metamorphosis,’’ ACM SIGGRAPH Comput. Graph., vol. 26, no. 2, pp. 35–42, Jul. 1992.

[10] J. Kannala and E. Rahtu, ‘‘Bsif: Binarized statistical image features,’’ in Proc. 21st Int. Conf. pattern Recognit. (ICPR2012), pp. 1363–1366, IEEE, 2012.

[11] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello, ‘‘Border control morphing attack detection with a convolutional neural network de-morphing approach,’’ IEEE Access, vol. 8, pp. 92301–92313, 2020.

[12] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, ‘‘Accurate and robust neural networks for face morphing attack detection,’’ J. Inf. Secur. Appl., vol. 53, Aug. 2020, Art. no. 102526.

[13] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, ‘‘Transferable deep-CNN features for detecting digital and print-scanned morphed face images,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jul. 2017, pp. 10–18.

[14] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, ‘‘Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network,’’ in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Mar. 2020, pp. 280–289.

[15] R. Raghavendra, K. B. Raja, and C. Busch, ‘‘Detecting morphed face images,’’ in Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Sep. 2016, pp. 1–7.

[16] L. Qin, F. Peng, S. Venkatesh, R. Ramachandra, M. Long, and C. Busch, ‘‘Low visual distortion and robust morphing attacks based on partial face image manipulation,’’ IEEE Trans. Biometrics, Behav., Identity Sci., vol. 3, no. 1, pp. 72–88, Jan. 2021.

[17] D. ICAO, 9303-Machine Readable Travel Documents—Part 9: Deployment of Biometric Identification and Electronic Storage of Data in EMRTDS, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2015.

[18] B.-C. Chen, C.-S. Chen, and W. H. Hsu, ‘‘Face recognition and retrieval using cross-age reference coding with cross-age celebrity dataset,’’ IEEE Trans. Multimedia, vol. 17, no. 6, pp. 804–815, Jun. 2015.