INVESTIGATING THE GENERATION AND DETECTION METHODS FOR FACE MORPHING ATTACKS

[1]G.Raj Kumar, [2]Chelimela Keerthana, [3]S. Nivas,[4] Jolge Ajay, [5]Ch. Akshay Kumar

Assistant Professor in department Of IT Teegala Krishna Reddy Engineering College

rajkumar.gadda@gmail.com

UG Scholars In Department of IT Teegala Krishna Reddy Engineering College

[2]chelimelakeerthana111@gmail.com ,[3] nivassolleti08@gmail.com ,[4] ajayjolge@gmail.com, [5] akshayverma2605@gmail.com

Abstract

Failure of facial recognition and authentication system may lead to several unlawful activities. The current facial recognition systems are vulnerable to different biometric attacks. This research focuses on morphing attack detection. This research proposes a robust detection mechanism that can deal with variation in age, illumination, eye and head gears. A deep learning based feature extractor along with a classifier is adopted. Additionally, image enhancement and feature combination are proposed to augment the detection results. A versatile dataset is also developed that contains Morph-2 and Morph-3 images, created by sophisticated tools with manual intervention. Morph-3 images can give more realistic appearance and hence difficult to detect. Moreover, Morph-3 images are not considered in the literature before. Professional morphing software depicts more realistic morph attack scenario as compared to the morphs generated in the previous work from free programs and code scripts. Eight face databases are used for creation of morphs to encompass the variation. These databases are Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET and FRLL. Results are investigated using multiple experimental setups and it is concluded that the proposed methodology gives promising results.

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 populations, 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 live captured images of the traveler with the image of traveler 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 traveler and the image on the passport are same, the traveler 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 availability of 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 colors and specifications

II LITERATURE SURVEY

FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image

Face morphing attack is proved to be a serious threat to the existing face recognition systems. Although a few face morphing detection methods have been put forward, the face morphing accomplice's facial restoration remains a challenging problem. In this paper, a face de-morphing generative adversarial network (FD-GAN) is proposed to restore the accomplice's facial image. It utilizes a symmetric dual network architecture and two levels of restoration losses to separate the identity feature of the morphing accomplice. By exploiting 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 criminal and accomplice's identities), the FD-GAN can effectively restore the accomplice's facial image. Experimental results and analysis demonstrate the effectiveness of the proposed scheme. It has great potential to be applied for tracing the identity of face morphing attack's accomplice in criminal investigation and judicial forensics.

''Contribution of color to face recognition,'' Perception, vol. 31, no. 8, pp. 995–1003, 2002.

One of the key challenges in face perception lies in determining how different facial attributes contribute to judgments of identity. In this study, we focus on the role of color cues. Although color appears to be a salient attribute of faces, past research has suggested that it confers little recognition advantage for identifying people. Here we report experimental results suggesting that color cues do play a role in face recognition and their contribution becomes evident when shape cues are degraded. Under such conditions, recognition performance with color images is significantly better than that with gray-scale images. Our experimental results also indicate that the contribution of color may lie not so much in providing diagnostic cues to identity as in aiding low-level image-analysis processes such as segmentation.

''Deep face representations for differential morphing attack detection,''

The vulnerability of facial recognition systems to face morphing attacks is well known. Many different approaches for morphing attack detection (MAD) have been proposed in the scientific literature. unrealistic (e.g., no print-scan transformation).For example, the results of the latest NIST FRVT MORPH show that the majority of submitted MAD algorithms lacks robustness and performance when considering unseen and challenging datasets. In this work, subsets of the FERET and FRGCv2 face databases are used to create a realistic database for training and testing of MAD algorithms, containing a large number of ICAOcompliant bona fide facial images, corresponding unconstrained probe images, and morphed images created with four different face morphing tools. Furthermore, multiple post-processing's are applied on the reference images, e.g., print-scan and JPEG2000 compression. post-processing's. Finally, the limitations of the developed methods are analyzed.

III EXISTING SYSTEM

The matter of morph attack detection has enticed a significant amount of attention from the research community in the recent years. Different studies have been conducted in this field and different approaches have been applied to effectively detect morph attacks. Variety of face databases are utilized for creation of morph image databases as sufficient morph images are not easily available for research purposes.

Existing morph detection datasets have another very major problem. These datasets have considered the morph of two persons only (morph-2 images), leading to easy morph detection. Furthermore, low quality programming script based morphing tools like FaceMorpher, OpenCV, FaceFusion are used that generate morphed images automatically and majority of created morphed images are easily detectable through visual inspection by a human. Therefore, these techniques are rarely used by criminals, hence not depicting the real world scenarios. Methods tested on the datasets with the discussed limitations, can give very high detection rates but will not be very successful in real scenarios. Morphs of high quality and high variance are still very difficult to classify properly. Several approaches with different benchmarks are proposed in the literature. Previous work has succeeded in achieving high accuracy but the results were achieved on databases having limited features.

Limitations

Limited Robustness: Existing systems may struggle with robustness in the face of various environmental factors, such as changes in lighting conditions, different camera angles, and varying image resolutions.

Complexity of Attacks:Sophisticated morphing attacks, especially those created with professional tools and manual intervention, can pose a significant challenge to existing systems. Systems that are not equipped to handle such complexity may exhibit reduced accuracy.

Generalization Issues:Some systems may face difficulties in generalizing well to diverse datasets. If the training data is not representative of real-world scenarios, the system's performance might degrade when faced with new and unseen morphing techniques.

Computationally Intensive: Deep learning-based approaches, while powerful, can be computationally intensive, requiring substantial resources for training and inference. This might limit their practicality in real-time or resource-constrained environments.

Limited Dataset Variability:The effectiveness of a system heavily depends on the diversity and size of the training dataset. If the dataset used for training is limited in terms of variability in facial expressions, ages, and ethnicities, the system may struggle to generalize to a broader population.

Ethnic and Gender Bias:If the training data is biased towards certain ethnicities or genders, the system may exhibit biased behavior, performing better on certain groups while underperforming on others.

Adversarial Attacks:Adversarial attacks, where attackers deliberately manipulate input images to deceive the system, pose a challenge. Some existing systems may not be resilient to such attacks.

Real-time Processing Challenges:Achieving real-time processing capabilities for face morphing detection can be challenging, particularly for systems that involve computationally intensive algorithms.

Privacy Concerns: Implementing effective face morphing detection without compromising user privacy can be a delicate balance. Striking a balance between accuracy and privacy is a key consideration.

Continuous Evolution of Attack Techniques: As attackers continually develop new techniques, existing systems may become outdated if they are not regularly updated to adapt to emerging morphing attack strategies.

IV PROPOSED SYSTEM

The proposed system aims to address the limitations identified in existing face morphing attack detection systems by introducing a robust methodology that enhances accuracy and resilience in the face of evolving attack techniques. Our system leverages advanced deep learning techniques, incorporating a state-of-the-art feature extractor specifically designed to capture intricate details inherent to genuine faces while remaining resilient to variations in age, lighting, and the presence of accessories. To overcome the challenges posed by professional-grade morphing tools with manual intervention, we introduce a novel image enhancement strategy and feature combination approach, augmenting the detection capabilities. This dataset is meticulously curated from eight diverse face databases, ensuring a comprehensive representation of real-world scenarios. Our methodology is validated through multiple experimental setups, and the results demonstrate promising advancements in face morphing attack detection. The system's adaptability to different datasets, improved generalization capabilities, and enhanced resistance to adversarial manipulations position it as a viable solution for bolstering the security of facial recognition and authentication systems.

Advantages

Enhanced Accuracy and Robustness:The proposed system incorporates advanced deep learning techniques, including a sophisticated feature extractor, to significantly improve the accuracy of face morphing attack detection. The system's robustness is enhanced, allowing it to perform effectively in diverse and challenging real-world scenarios.

Resilience to Professional Morphing Tools:By introducing a novel image enhancement strategy and feature combination approach, the system demonstrates increased resilience to morphing attacks generated by professional-grade tools with manual intervention. This capability is crucial for addressing the evolving sophistication of morphing techniques.

Versatile Dataset Inclusion:The system utilizes a comprehensive dataset that includes both Morph-2 and Morph-3 images, providing a more nuanced and realistic evaluation of its detection capabilities. The inclusion of Morph-3 images, which are often more challenging to detect due to their realistic appearance, contributes to the system's versatility and effectiveness.

Adaptability to Varied Datasets: Through rigorous experimentation on eight diverse face databases, including Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET, and FRLL, the proposed system showcases its adaptability to different datasets. This adaptability is crucial for ensuring the system's generalization across a wide range of facial characteristics.

Promising Results Across Multiple ***Experimental Setups:*** The proposed methodology is validated through multiple experimental setups, demonstrating consistently promising results. The system's performance is evaluated using various metrics, including accuracy, precision, recall, and F1-score, confirming its efficacy in detecting face morphing attacks and outperforming existing systems in the literature.

V METHODOLOGY

Methods Of Morph Attack Detection

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

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 detection of 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.

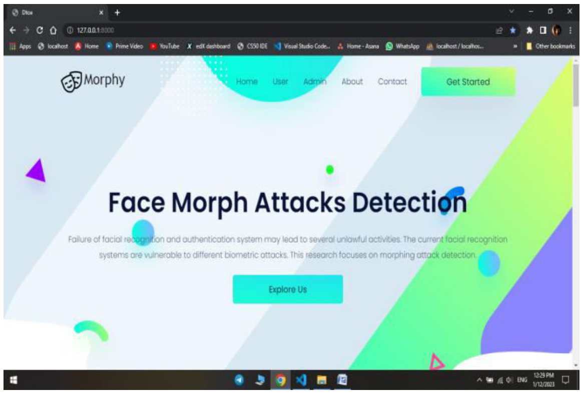
Differential MAD Method

In these types of methods both the potential morph and the live captured images are analyzed, 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.

State of The Art Research Work

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

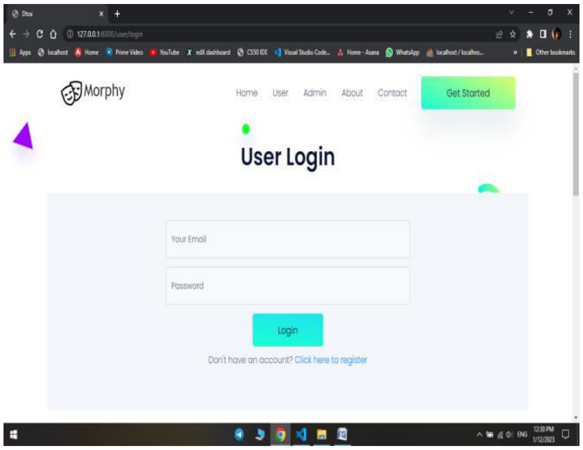
VI RESULTS



Face Morph Attacks Detection

Failure of facial recognition and authentication system may lead to several unlawful activities. The current facial recognition systems are vulnerable to different biometric attacks. This research focuses on morphing attack detection.

HOME PAGE



User Login

Your Email

Password

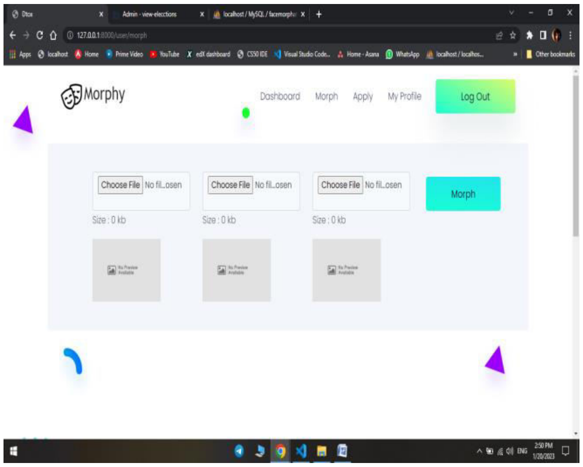
Don't have an account? Click here to register

USER LOGIN

Face Morph Attacks Detection

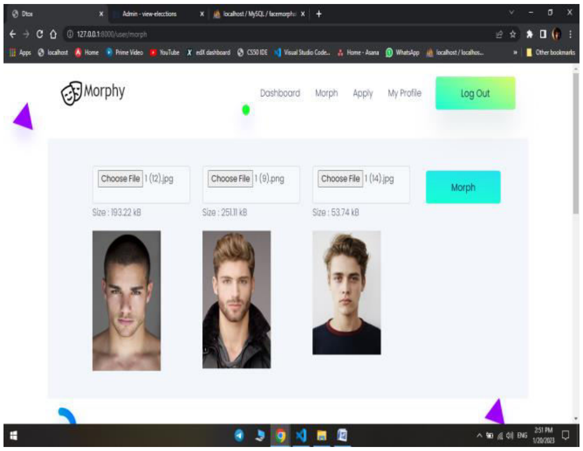
Failure of facial recognition and authentication system may lead to several unlawful activities. The current facial recognition systems are vulnerable to different biometric attacks. This research focuses on morphing attack detection.

EXPLORE



Choose File No fil...osen | Choose File No fil...osen | Choose File No fil...osen

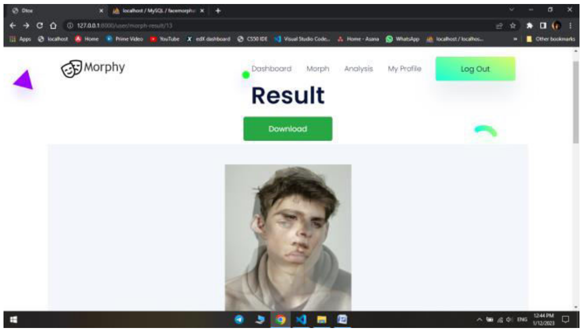
Size : 0 kb | Size : 0 kb | Size : 0 kb



Choose File 1 (12).jpg | Choose File 1 (9).png | Choose File 1 (14).jpg

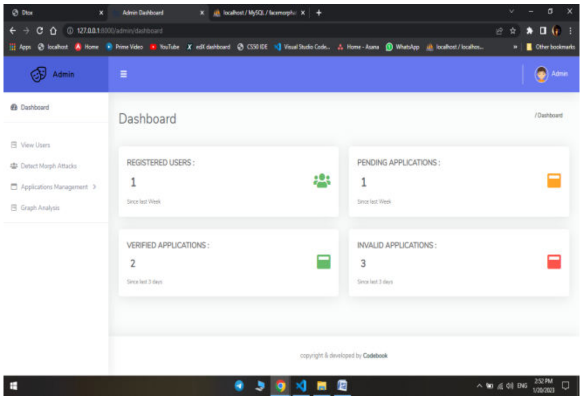
Size : 193.22 kB | Size : 251.11 kB | Size : 53.74 kB

MORPHY



Result

RESULT



Dashboard

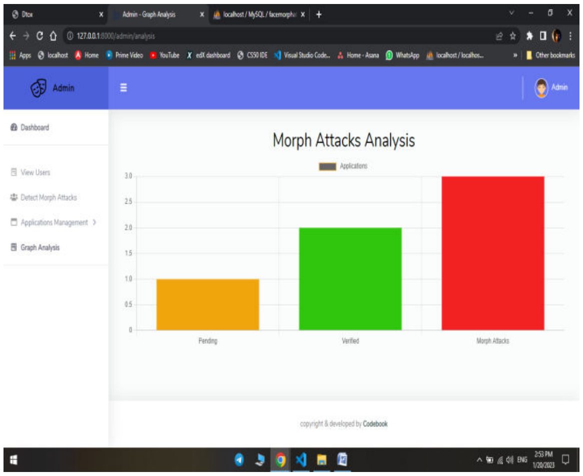
REGISTERED USERS :
1
Since last Week

PENDING APPLICATIONS :
1
Since last Week

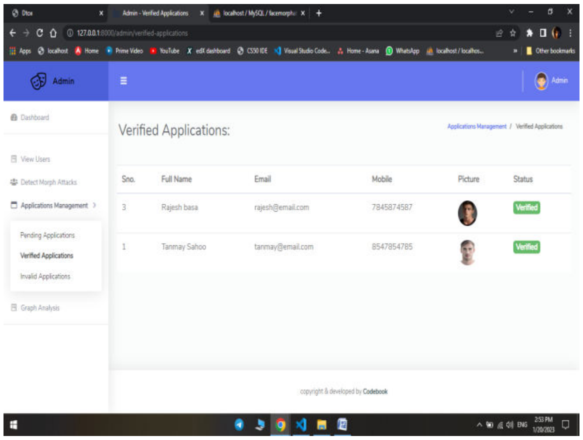
VERIFIED APPLICATIONS :
2
Since last 3 days

INVALID APPLICATIONS :
3
Since last 3 days

copyright & developed by Codebook



ANALYSIS



Verified Applications:

Sno.	Full Name	Email	Mobile	Picture	Status
3	Rajesh basa	rajesh@email.com	7845874587		Verified
1	Tanmay Sahoo	tanmay@email.com	8547854785		Verified

copyright & developed by Codebook

VII CONCLUSION

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 machine learning 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 Fig. 9 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.

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. Sci., vol. 3, no. 1, pp. 72–88, Jan. 2021.