iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67553

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Detection of Face Morphing Attacks Using Deep Learning

Mr. Ch. Sunil[1], Y. Gayathri[2], T. Jahnavi[3], Ch. Lavanya[4], K. N. V. Praneeth[5]
Department of Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, Andhra Pradesh, India

Abstract: ***The possibility of various illegal acts increases when face recognition and authentication systems fail. Current face recognition systems can be easily compromised by various biometric techniques. This study focuses on attack detection using morphing. An effective detection system is proposed that accounts for differences in age, lighting, eyewear, and headgear. The system uses a deep learning-based feature extractor in conjunction with a classifier. Additionally, we propose combining features and enhancing images to improve detection accuracy. A multipurpose dataset, including Morph-2 and Morph-3 images generated by advanced techniques with human participation, is also under development. Morph-3 images, due to their photorealistic quality, might be difficult to detect. Notably, no prior study has considered Morph-3 images. Previous studies using free programs and code scripts produced morphs that were less realistic than those generated by professional morphing software in a morph attack scenario. Morphs are created using eight unique face databases: Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET, and FRLL to include all possible variations. After assessing the data across several experimental circumstances, we find that the proposed method yields favorable results.***

Index Terms: Face recognition, Morphing attack detection, biometric security, image enhancement, multipurpose dataset, Morph-2, Morph-3, face databases.

I. INTRODUCTION

The advent of modern technology has converted the world into a global village. Vast distances have been considerably reduced due to the availability of rapid transportation methods, such as airplanes, trains, ships, and buses. The improved accessibility has led to a significant rise in foreign travel, making manual verification of travel documents and facial recognition impractical. To address this challenge, automated border control systems have been implemented in over 180 airports worldwide, streamlining the authentication and approval process for passports. These automated systems utilize face recognition technology to compare a live-captured image of a traveler with the stored image in a travel agency's database, passport, or other machine-readable travel documents (MRTD). If the system confirms a match, the traveler is granted authorization to proceed. This automation enables border control authorities to efficiently manage the growing volume of travelers. However, the widespread availability of image manipulation technologies has also introduced vulnerabilities, allowing criminals to exploit these advancements for fraudulent activities. One such method, face morphing, enables perpetrators to manipulate images to deceive face recognition systems. While image morphing technology has existed since the 1980s, recent advancements in software and hardware have made it more accessible, making fraudulent use easier than ever. Face morphing allows two or more individuals' images to be blended in such a way that the resulting morphed image resembles both contributors. Since facial recognition systems approve these images as legitimate, human inspection also becomes highly challenging. For instance, a wanted criminal banned from traveling can morph their facial image with that of an accomplice, successfully bypassing security checks and obtaining unauthorized travel permission. Numerous morph attack detection techniques have been proposed to mitigate this security vulnerability. These methods are categorized into single-image morph attack detection and differential morph detection. This study presents a complete approach for detecting morph assaults, adept in identifying diverse changed images. The model is trained on a diverse array of photographs including variations in age, facial expressions, posture, lighting, gender, race, hairstyle, facial hair, headgear, and eyewear. Additionally, since different types of ID cards have distinct background colors and specifications, the model is designed to handle these variations effectively, enhancing its robustness in real-world scenarios.

II. LITERATURE SURVEY

Fei Peng and Min Long emphasize the significant threat that face morphing attacks provide to contemporary facial recognition systems. Despite the availability of several detection methods, reconstructing the facial look of the morphing accomplice remains a considerable challenge. To address this problem, they propose a Face De-Morphing Generative Adversarial Network (FD-GAN) designed to restore the accomplice's identity.

The method employs a symmetric dual-network design and two levels of restoration loss to effectively differentiate identity traits. FD-GAN proficiently reconstructs the accomplice's visage using the obtained facial image, which discloses the criminal's identity, alongside the morphed image preserved in e-passport systems, encompassing both the criminal and the accomplice's identities. Experimental results validate the effectiveness of this technology, highlighting its potential applications in criminal investigations and forensic science. Andrew W. Yip and Pawan Sinha explore how different facial attributes influence identity perception, with a particular focus on color cues. Contrary to previous research that downplayed the role of color in facial recognition, their findings indicate that color significantly enhances recognition, especially when shape information is degraded. In such scenarios, color images yield notably better recognition performance than grayscale images. Their study suggests that color may primarily assist in low-level image analysis processes, such as segmentation, rather than serving as a direct identity cue. Ulrich Scherhag, Johannes Merkle, and Christoph Busch investigate the vulnerability of facial recognition systems to face morphing attacks. Despite the introduction of several Morphing Attack Detection (MAD) methodologies, many exhibit a tendency to overfit certain datasets characterized by unrealistic features, hence limiting their practical applicability. To address this issue, they constructed a more representative dataset including segments of the FERET and FRGCv2 datasets, which included ICAO-compliant authentic photographs, unconstrained probing pictures, and morphing images generated using four different algorithms. Their evaluation, using post-processing methods such as print-scan and JPEG2000 compression, demonstrated that strategies utilizing deep face representation achieved enhanced detection efficacy (with a D-EER around 3%) and robustness across diverse conditions. Additionally, they examined the limitations of existing detection methods. Arash Samani and Xin Yuan discuss the growing field of cross-modality face recognition, driven by the increasing use of diverse imaging sensors in daily applications. They introduce the Tufts Face Database, a collection of over 10,000 images from 113 individuals, featuring multiple modalities such as photographs, thermal images, near-infrared images, videos, computerized facial sketches, and 3D facial scans. Collected under an Institutional Research Board protocol at Tufts University, this database represents individuals from various genders, age groups, and ethnic backgrounds. Their work not only provides an extensive review of face recognition systems and datasets but also makes the Tufts Face Database publicly available for research, supporting advancements in multimodal facial recognition. D. Smythe introduces a novel interpolation technique for medical imaging, specifically designed for both slice and projective interpolation. The proposed method establishes spatial correspondence between adjacent images using a block-matching algorithm and then interpolates image intensities by morphing between them. When tested on 3D tomographic datasets, this morphing-based interpolation demonstrated comparable performance to registration-based interpolation and significantly outperformed traditional linear and block-matching-based methods. One of its key applications is in conformal radiotherapy, where it enables real-time projective interpolation for 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, ocular characteristics, and headgear.

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

To improve detection results, we suggest including features and enhancing images.

A distinctive and varied morphing database is systematically constructed using specific technologies for this study.

This artwork comprises morphing pictures derived from two or three subjects.

An advanced morph identification model is developed and evaluated on a newly created database employing a deep learning feature extractor and a machine learning classifier.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

The research employs multiple analyses to assess the effectiveness of the proposed morph attack detection methodology across various original and modified image types.

A. Advantages

1) Swift and accurate detection of evolving attacks.

2) Identification of individual image morphing attacks and differential morph detection.

V. SYSTEM MODEL

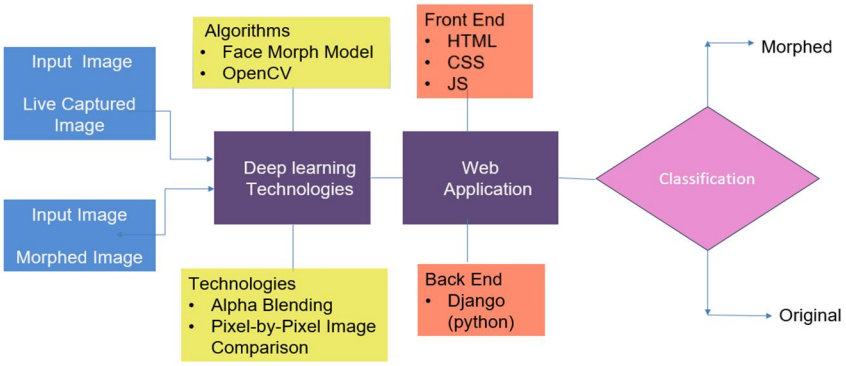


Figure .1 System Model

VI. IMPLEMENTATION MODULES:

A. Image Morphing

Face image morphing was first introduced in the late 1980s and 1990s as a technique for creating visual effects in movies and animations. The process involves comparing facial features from two images and determining their spatial relationships to generate a combined image. After aligning both images through warping, color interpolation is applied, resulting in a blended image that contains features of both original inputs. The degree of warping and color interpolation is known as transition control.

Several techniques have been developed for image morphing, including:

Mesh Warping: Uses a mesh structure to link control points between two face images. Certain regions of the image are held static while others are warped based on these control points to create a seamless transition.

Field Morphing: Employs a pair of reference lines to map corresponding facial features between two images. The warping process is determined by the distance of feature points from these reference lines.

Radial Basis Morphing: Represents image features as a set of points. A mapping process is performed between the surfaces of the two images, allowing for smooth blending and transformation.

B. Methods Of Morph Attack Detection (MAD)

Morph attack detection methods can be broadly categorized into two types:

1) Single-Image MAD

These methods analyze a single image to detect signs of morphing. Morphed images often contain artifacts that serve as indicators of manipulation. Some key techniques used in this approach include:

Texture descriptors, such as Binary Statistical Image Features (BSIF), which help classify textures in an image.

Detection of ghosting or shading artifacts, which are common byproducts of image morphing.

Deep neural networks (DNNs), which can be trained to recognize morphing artifacts when provided with a diverse dataset of genuine and morphed images.

2) Differential MAD

These methods compare a potentially morphed image with a live-captured image of the same individual. This approach involves:

Extracting and comparing feature vectors from both images to detect inconsistencies.

Demorphing techniques, which attempt to reverse the morphing process to reveal the identity of the accomplice by subtracting the live image from the morphed image.

C. Innovative Research

Extensive research has been conducted on morph attack detection, using various tools, preprocessing techniques, and datasets to generate morphed images. An summary of relevant studies is presented in the survey.

Although several studies demonstrate exceptional detection accuracy, many have been assessed on datasets with limited variability that do not fully represent real-world conditions. Essential factors like as age, race, facial hair, headgear, eyeglasses, lighting, facial expressions, and posture are often undervalued or overlooked in several research. Furthermore, most research studies rely on a restricted array of datasets, so limiting their generalizability. A notable drawback is the reliance on fixed contribution weights in the integration of attacker and accomplice images, rather than using variable contribution weights that more properly reflect genuine morphing attempts. Moreover, pictures using headgear and spectacles might lead to inaccurate classification, since original images are often misidentified as altered versions. Finally, previous studies have often relied on high-quality live-captured images for comparison, which does not align with real-world security checkpoints, where image quality may vary significantly depending on available resources. Addressing these gaps is essential for improving the robustness and practical applicability of morph attack detection systems.

VII. RESLUTS

Figure.2 Home page

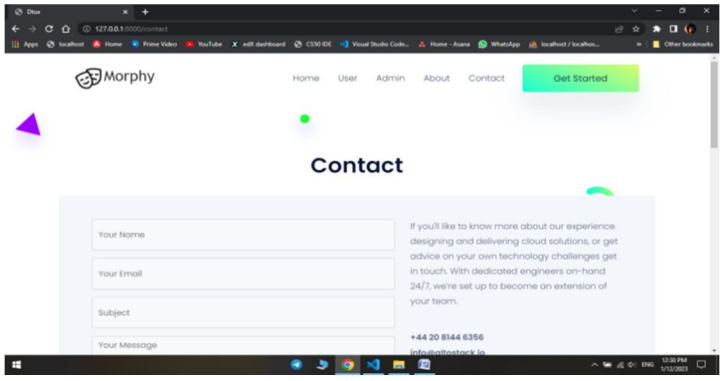


Figure.3 Contact Page

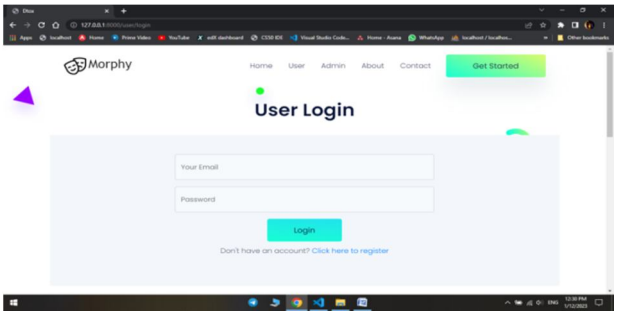


Figure .4 Login page

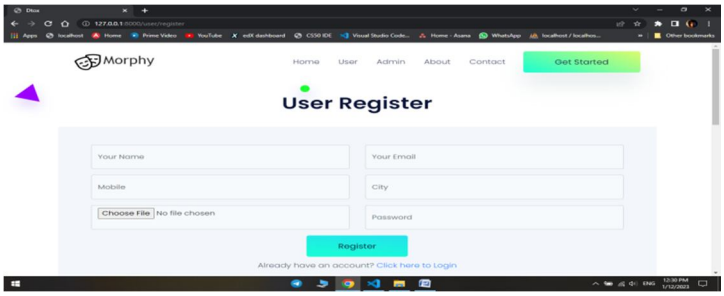


Figure.5 User Register page

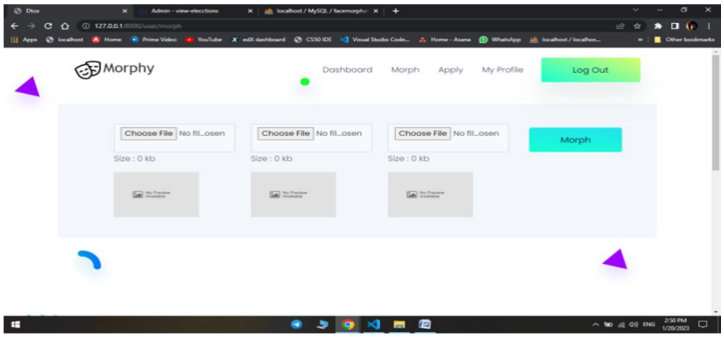


Figure.6 User Morph Uploading page

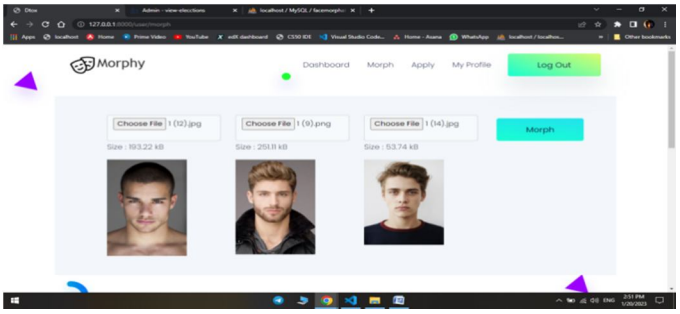


Figure.7 Uploaded

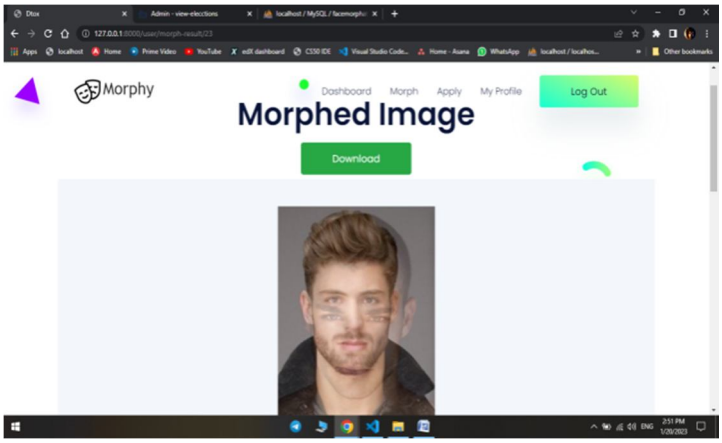


Figure.8 Image Morph

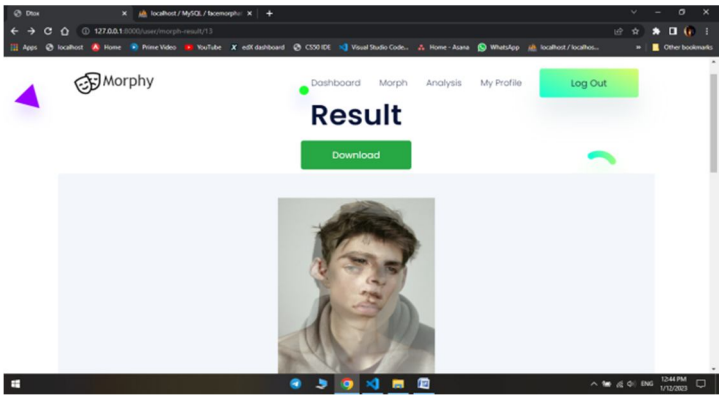


Figure.9 Result

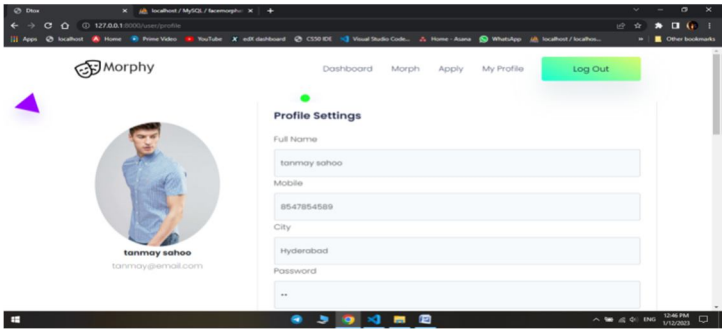


Figure.10 User Profile

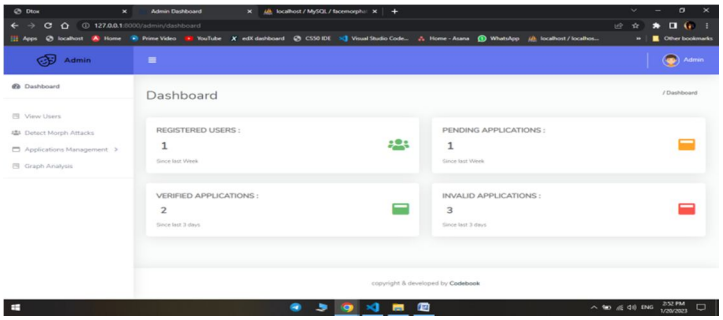


Figure.11 Admin Dashboard

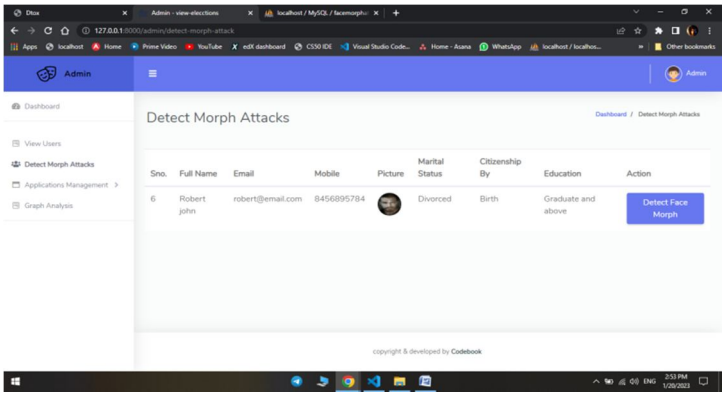


Figure .12 Detect Morph

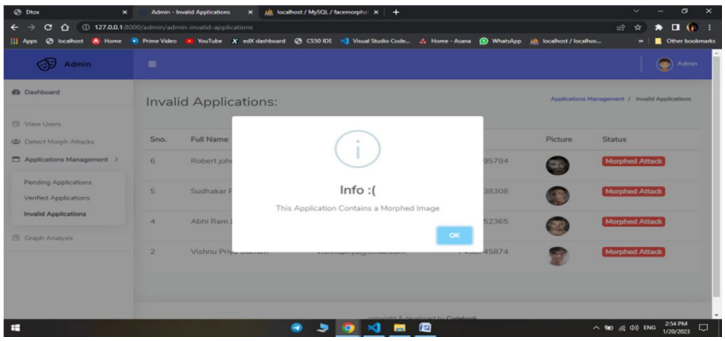


Figure.13 checking for morphed image

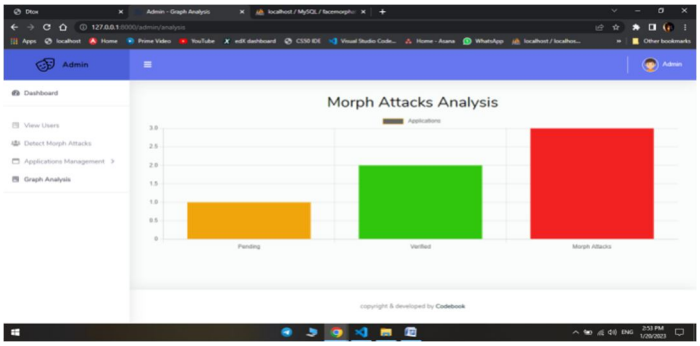


Figure.14 Morph Attack Analysis Graph

VIII. CONCLUSION

Using a diverse set of morphed photos as a foundation, this research presents an expanded and thorough technique for identifying morph assaults, with the goal of improving the practical detection effectiveness. The most effective strategy for morph recognition was found to be feature concatenation, out of those that were evaluated. Although this approach improved detection accuracy, it also increased computational complexity.

A key observation was that high-quality, manually created morphed images were significantly more challenging to detect when models were trained on databases generated using low-quality, automated morphing tools such as OpenCV and FaceMorpher. In contrast, training on high-quality, manually created morphs substantially improved detection accuracy. The proposed model effectively handled variations in age, illumination, posture, and facial expressions.

The detection of morph assaults was assessed using several machine learning classifiers, with Support Vector Machine (SVM) producing the most advantageous outcomes. Furthermore, the use of image enhancement techniques improved detection efficacy, particularly for datasets with little lighting and color variation. Notably, manually created morph-3 pictures were difficult to recognize when the model was only trained on morph-2 images produced by inferior equipment. Detection performance significantly improved when trained on high-quality morph-3 images. These findings highlight the need of include a diverse range of morphs into the training database to enhance model resilience.

Among the datasets we examined, FGNET presented the most challenge because to the large range of ages, picture quality, color diversity, and facial expressions included. The detection system has a very hard time accurately classifying the complicated morphing pictures produced by the severe variants.

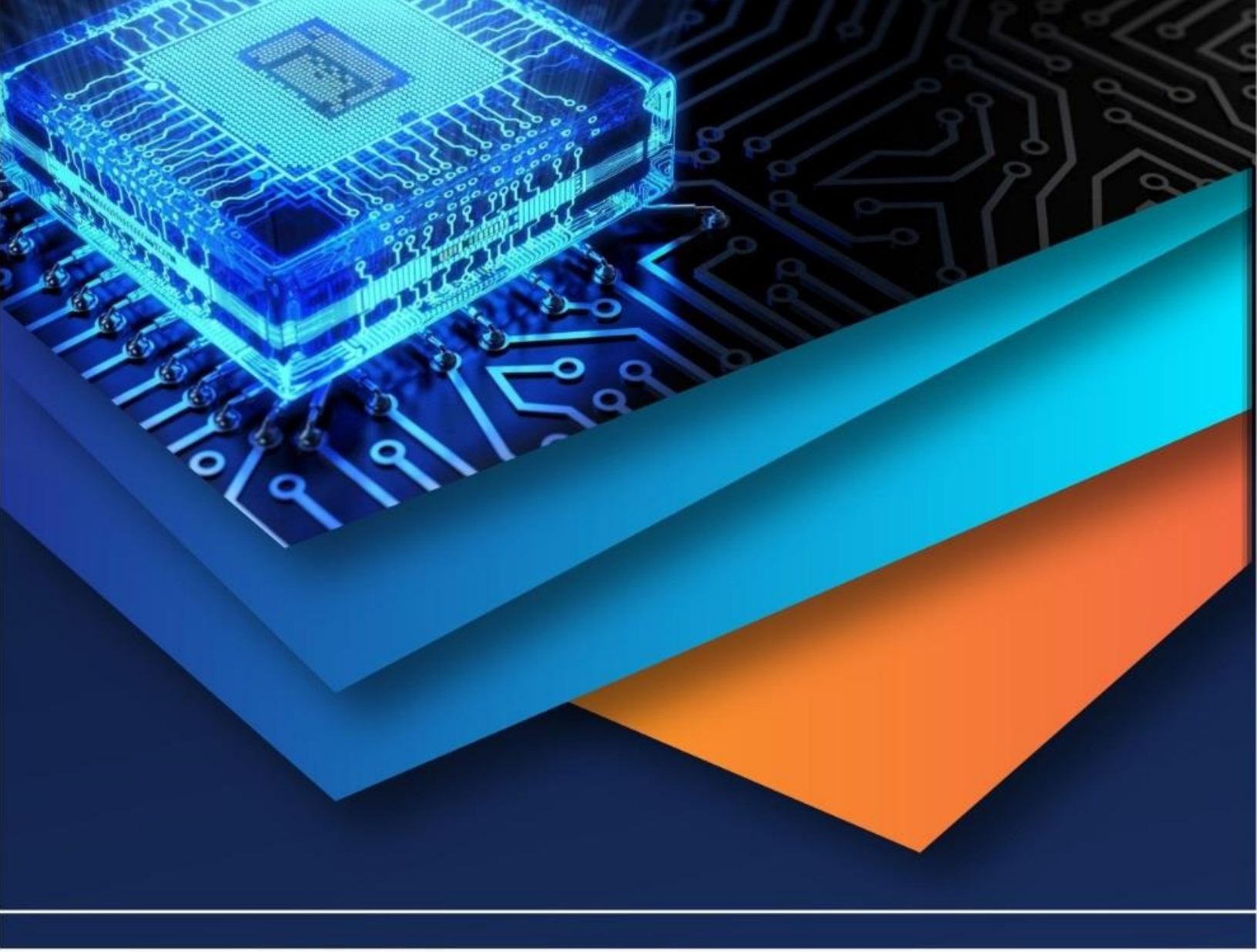
IX. FUTURE ENHANCEMENT

Future research should prioritize the collection of genuine morphing photographs submitted to various organizations, including airports, identity card authorities, travel companies, universities, and security institutions, to enhance the model and facilitate its practical use. Assessing the model using these authentic pictures will improve its precision and robustness in practical applications.

Additionally, developing an adaptive morph attack detection model could significantly enhance performance. Such a model should dynamically adjust to the characteristics of input images by applying appropriate image enhancement techniques as needed. Furthermore, incorporating more than three images in the morphing process could refine detection capabilities and improve the model's ability to identify complex morph attacks more effectively.

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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY