iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52876

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 11 Issue V May 2023- Available at www.ijraset.com

Generation and Detection of Face Morphing Attacks

G. Sarika Reddy[1], K. Sai Narsimha Reddy[2], Guntha Pooja[3], K. Sreelekha[4]
[1, 2, 3, 4]*Dept. of Electronics and Computer Engineering, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana, India*

Abstract: ***Face morphing attacks are a growing concern in the digital world, with the potential to compromise personal privacy and security. In this project, we investigate the application of deep learning methods for both generating and detecting face morphing attacks. For the generation of morphed, we use a combination of convolutional neural networks and auto encoders to learn the underlying facial features and generate realistic-looking images. On the detection side, we develop a framework based on facial feature consistency analysis to differentiate distorted images from real ones. The proposed framework achieves high accuracy in detecting face morphing attacks, even in cases where the morphed images are visually similar to the genuine ones. This project highlights the potential of deep-learning based approaches for addressing the problem of face morphing attacks and provides insights for further research and development in this area.***
Keywords: ***Morphing Attack Detection, Face Recognition, Deep Learning, Image Morphing, vulnerability***

I. INTRODUCTION

Face morphing assaults use facial image manipulation to combine two distinct people's faces into one image. These assaults can be utilised for political influence, identity theft, and other types of fraud or deception. A variety of techniques, including picture warping, mixing, and texture creation, can be employed to create face morphs. Machine learning models and forensic analysis techniques, which commonly use counters and pixel values, can be used to detect face morphing attacks. Nevertheless, it might be difficult to spot. face morphing attacks because morphs may be made to deceive detection systems and frequently look genuine. These morphing attacks have been documented in the various fields providing threat in real world scenarios such as political campaigns, social media, and identity theft cases. It is expected that continued study and the creation of more advanced detection systems will be necessary for the effective detection and prevention of face morphing attacks.

The number of people that travel has significantly increased as a result of these numerous transportation options. Manual travel document and facial identity verification is impossible with such a huge mobility population. Therefore, the authentication and approval of passports is done by an automated border control system. There are now border control systems installed in more than 180 airports worldwide. [1].

Face biometrics are frequently used in border control applications to secure people identity, where a person's identity is confirmed using either

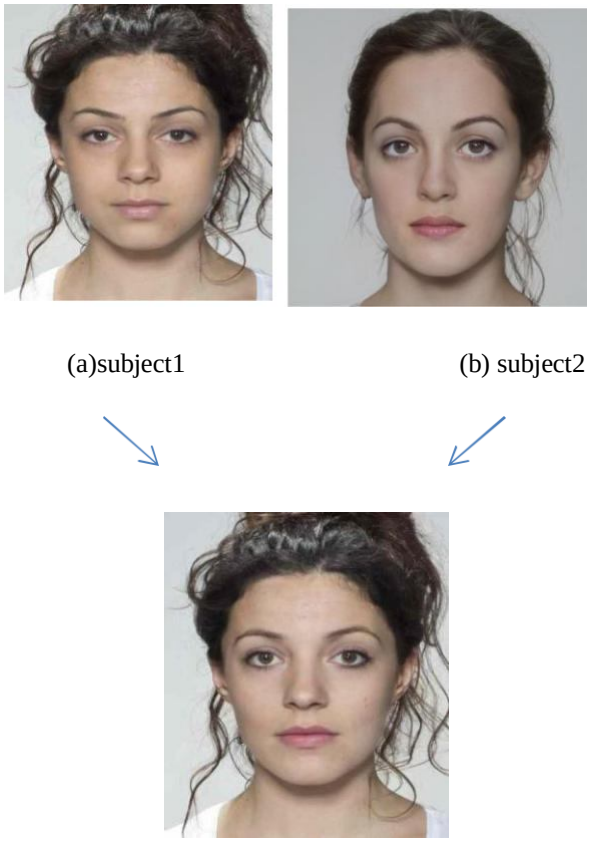
an electronic passport or an identification card given by the government of the concerned nation. While in a few nations the face photograph for the passport is taken under strict supervision within a reputable authority structure. In the vast majority of nations the applicants are required to provide a face photograph. Therefore, the applicants may use morphing techniques to create any facial image that more closely resembles the applicant original face. [2]

These attacks cause a face recognition system to mistakenly identify two distinct people with a single fake face image. Both subjects can use a piece of formal identification—such as a passport or identity card—that has such a picture encoded in it to prove who is the right owner include a printed photo for the paperwork when applying for a passport. This makes it possible to insert a fake facial image into a real official identification paper. Free morphing software makes it simple to combine two face photos into a single composite image that combines the features of both facial photographs and deceives border control biometric verification systems. To ensure the reliability of such systems, it is crucial to detect this form of fraud. Attacks that contain morph pose a serious concern, particularly to border security [3] Anti-spoofing methods are the focus of numerous recent research studies.

The tremendous difficulty of being recognized makes morphing attacks one of the most hazardous types of attacks. It can be performed by the use of different morphing methods using facial images captured during morphing attacks. In any event, this work primary focus is facial morphing because it is the most harmful and challenging to detect in Automatic Border Control systems [4].

©IJRASET: All Rights are Reserved

It was discovered that an original identity theft scenario can readily fool ABC's FRS. The fundamental idea behind these attacks is that a malicious morphed face image is an amalgam of at least two actual facial photos to look like a large number of different real people, such as an accomplice to a crime. The modified image is then is then registered with the FRS as an identification template. In a successful attack, the perpetrator and any helper can be similar to the images data kept in the system which recognizes faces. It indicates that a desired lawbreaker who is not allowed to travel out of the city can use facial image morphing to combine the faces of two accomplices to have a valid passport. The altered facial picture samples are displayed in Fig1[5].



(a)subject1 (b) subject2

(c) morph

Fig.1. Example of a morphed image created using OpenCV

A. Objective of the Project

The objective of this project is to analyse the photos to find any anomalies or artefacts that might suggest that the image has been altered is necessary to detect face morphing assaults for morph 3 images. Numerous methods, like comparing face landmarks, examining image gradients, and checking for differences in skin texture and lighting, can be used to do this. [1]

This detection method is to accurately differentiate between real facial photos and altered ones. This will improve the security of numerous systems and applications that use face recognition technology while also assisting in the prevention of various forms of fraud and identity theft. [7]

Following the introduction of this concept, some inquiries about the commercial FRS's susceptibility to morphing face attacks have been morphing attacks. Some face morphing detection techniques which are proposed to numerous articles mention impressive detection rates, however these findings hardly ever apply to real-world situations. Firstly, the evaluation's datasets are not realistic. Particularly, most papers do not take into account different image post-processing, such as print-scan transformation or extreme compression, that happens in real situations and may significantly reduce variation that can be seen in morphing distortions. Additionally, the numerous publications from earlier research on differential MAD make extensive use of photographs that don't accurately portray within-subject variation, including lighting, the subject's look, which may include spectacles, a beard, hair, cosmetics, ageing, and clothing, as well as facial expression.[6] [11]

II. RELATED WORK

As morphing techniques have been the subject of numerous experimental investigations over the past few years, there has been a notable advancement and improvement in a number of areas, including visual quality and the development of altered images intended to trick the systems. [4]

The methods which were used in recent investigations has number of limitations. In order to recover the accomplice's facial picture, a face de-morphing generative adversarial network (FD-GAN) is suggested in this paper. It uses two tiers of restoration losses and a dual network design that is symmetric to isolate the morphing accomplice's identifying feature. The analysis and outcomes of the experiments show how effective the suggested plan is. In this paper images with participants who were expressing expression, posture, or some degree of occlusion had a worse time being accurately restored. They only used morph-2 photos fewer morphing resources. [5]

The research paper presents a conceptual categorization, criteria for evaluating such strategies, and a thorough literature review of pertinent works. Along with outstanding problems and difficulties in the field, the methodology surveyed the technical issues and trade-offs are also investigated. The observed assault detection accuracy using facial picture morphing has not yet been generalized to datasets that include a wide range of capture situations encountered in the real world. There are several unresolved problems and obstacles in face morphing and face morphing assault detection research, such as quality and comparability. [9][10]

Another study looks at techniques that can detect differential morphing attacks. It is demonstrated that deep face representation-based approaches offer incredibly high detection sensitivity and robustness are shown to have extremely high detection processings. The methodologies and flaws are then examined in detail**.** However, excellent morphs and morphs that are quite comparable to live-captured images weren't given the proper classification. The misclassification of photographs was also aided by differences in facial expression, headgear, eyewear, illumination, and focus. There was also lack of a database that accurately represents a real-world circumstance. [6]

The de-morphing architecture put forth in this research is to build on a machine learning based convolutional neural network (CNN) architecture. This method depends on the usage of two images: the passport photo that may have been altered and the person's current live picture in the system for Automatic Border Control. The de-morphing process aims to decode the picture. [4]

III. PROPOSED METHODOLOGY AND ARCHITECHTURE

A. Architechture

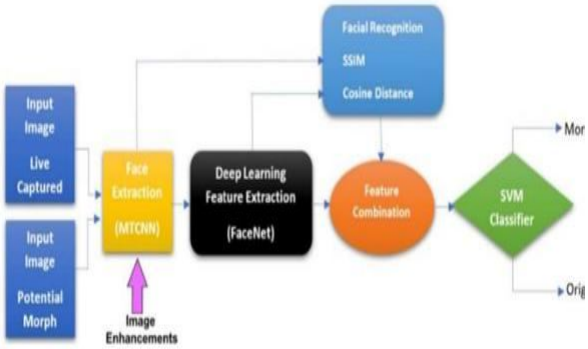


Fig2: Architecture to detect the morphed images

In this method, a reliable detection method is proposed that can account for age, lighting, eye, and headgear variations. A classifier and a feature extractor based on deep learning are used. To improve the detection outcomes, image enhancement and feature combination are also suggested. In this work, a distinctive and varied morphing database is manually constructed utilising expert software. This work includes morphed photos made from two and three topics. On the newly created database, the use of extraction of features with deep learning model like FaceNet and an artificial intelligence-based classifier like SVM forms the basis of a contemporary morph detection algorithm.

This study's goal is to evaluate the suggested morph attack detection model's performance on various morphed and unmorphed image types.

1) *Face image acquisition:* Collect a dataset of facial images, including genuine images and morphed images, with various types of morphing techniques applied.

2) *Feature Extraction:* Extract features from the facial images, such as geometric features, texture features, or frequency domain features.
3) *Morphing Image Generation:* Generate morphing images using various techniques, such as image warping, averaging, or deep learning-based methods.
4) *Training of Morphing Detection Model:* Training a machine learning model to discriminate between real photos and altered images, such as a Support Vector Machine (SVM).
5) *Detection of Morphing Attacks:* Apply the trained model to detect morphed images in test datasets.

B. Dataset

Attack samples developed for research databases may not be the same as attack samples from the actual world. The creation of a large number of attack samples, which can be done automatically, is required to provide meaningful evaluation findings. A method must be utilized to enhance the deep learning model's performance such that the model's architecture has been appropriately improved and modified to attain the best outcomes. As a result, the primary aim of this research is to create a database that would aid the model in learning and enhancing its performance. The FERET, FRGC, and FRLL datasets which are available were used to create morphs for the photos using the OpenCV and FaceMorpher programming tools, which were obtained from prior studies [1].There are also another methods where the criminals use different tools to create a realistic image

In this study, two different kinds of altered images are produced:

1) Morph-3, images made by combining the faces of three separate people.
2) Morph-2, which simply combines the facial images of two people to produce images.

As various features like variation in lighting effects known as illumination cause artefacts in morphs and lower the quality of morphs, no attempt has been made to produce morphs by combining photos
from various databases. Comparable facial photos are modified to produce better results because they have comparable facial structure and features.

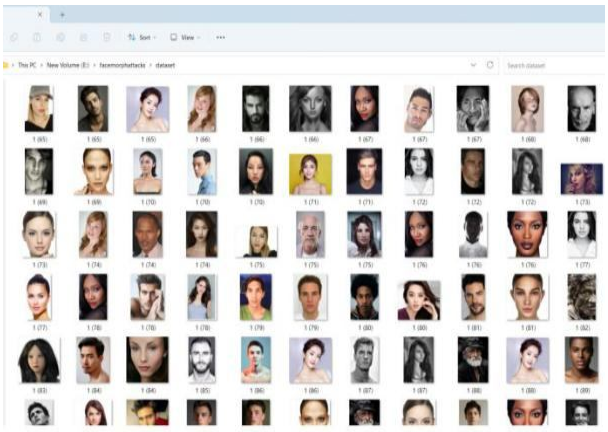


Fig3: Dataset

C. Methodology

The project comes to an end involving various stages. The project can be performed in two main stages which include lot of different processings. The stages can be divided as:

1) Generation of Morphed Image
2) Detection of Morphed Image

a) Generation

Generating a good morph with the best algorithm for morph3 involves a number of steps, including selecting appropriate images, detecting and aligning facial landmarks, morphing the images, and blending the resulting morphed image.

Select two or three images that have similar facial features, such as the same person in different poses or with different expressions.

Detect facial landmarks using a suitable facial landmark detection algorithm, such as the dlib library in Python.

Use the detected landmarks to align the two images so that the facial features are in the same location and orientation in both images.

Generate an intermediate image by morphing the two aligned images. There are several algorithms available for morphing images, such as linear blending, weighted averaging, and thin-plate splines.

Blend the intermediate image with the two original images to produce a final morphed image. There are various methods for blending images, such as cross-dissolve, alpha blending, and Poisson blending.

Fig4: Detecting landmarks for subject1

Fig5: Detecting landmarks for subject2

b) Detection

In this project, the deep learning techniques are used to detect the morphed image.

Face detection using MTCNN: MTCNN is a deep learning algorithm that detects faces in an image. In this stage, the images are given as the input one which is the live captured image and other the potential morph.

The facial region of the input image is extracted using this approach. MTCNN is capable of detecting faces at different scales, orientations, and positions in an image, which makes it a useful tool for various face-related applications.

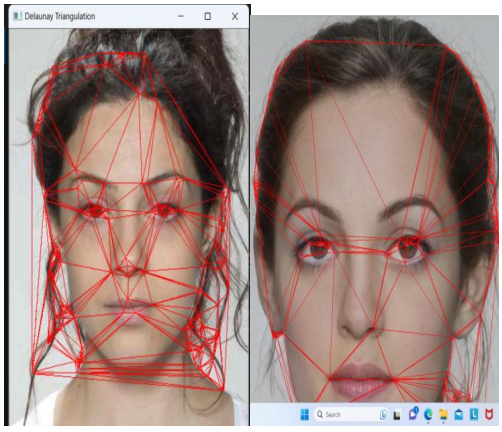


Fig 6: Formation of Delaunay triangles using detected features

Face representation using FaceNet: FaceNet is a deep learning algorithm that generates a high-dimensional feature vector that represents the face. In this stage, the algorithm is used to extract a feature vector from the face region detected in the previous stage. The facial recognition component is also incorporated to identify the individual in the face image. This can help in identifying any anomalies in the feature vector that may be caused by morphing.

Morphing detection using feature combination: In this stage, the feature vectors generated by FaceNet are combined with additional parameters such as SSIM, PSNR and cosine distance to improve the accuracy of morphing detection. The cosine distance measures the separation between two feature vectors, whereas the SSIM measures the similarity between two images. By incorporating these parameters, the algorithm can better distinguish between morphed and non-morphed faces.

Through the use of various parameters, such as concatenation, addition, or subtraction, the live-captured input image's attributes are combined with the potential morph image. SSIM and cosine distance verification from the facial acknowledgement system afterwards, the features of the prospective morph and the corresponding live acquired image are integrated. Between the conceivable morph photos and the collected corresponding live-captured images, the cosine distance and SSIM score are computed. Cosine distance uses the generated feature vectors derived from the source photos, as opposed to SSIM, which uses the retrieved uploading face images for measurement of similarity. PSNR scores are also calculated to understand the changes in accuracy metrics of detection. An average is used to integrate the cosine distance and SSIM scores. Using the lowest SSIM similarity score and cosine combination, the live image is merged with the characteristics of a potential altered image. [1]

Classification using SVM: Finally, the SVM is trained on the combined feature vector to classify the given inputs. After classifying the input images, it produces the output as either morphed or a valid image which the passport of the user valid.

IV. RESULTS

Fig7: Web user Interface for Detection

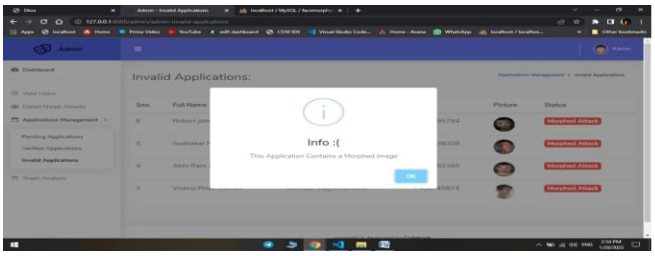


Fig8: Morphed Attack Detection

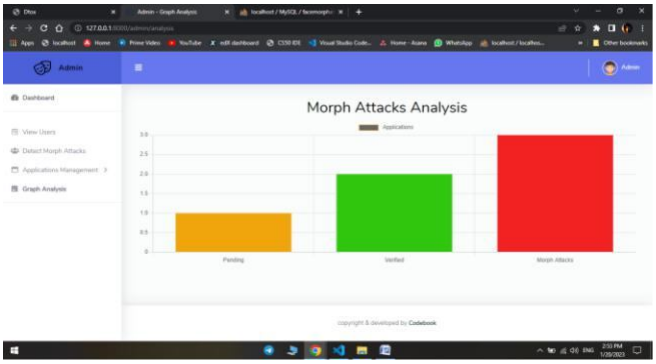


Fig9: Morph Attack Analysis

V. CONCLUSION

It can be concluded that, we explored different techniques for generating and detecting face morphing attacks. The generation process involved the use of deep learning models to morph two or more faces to create a single image, while the detection process focused on identifying the inconsistencies in the facial features of a morphed image compared to genuine images.

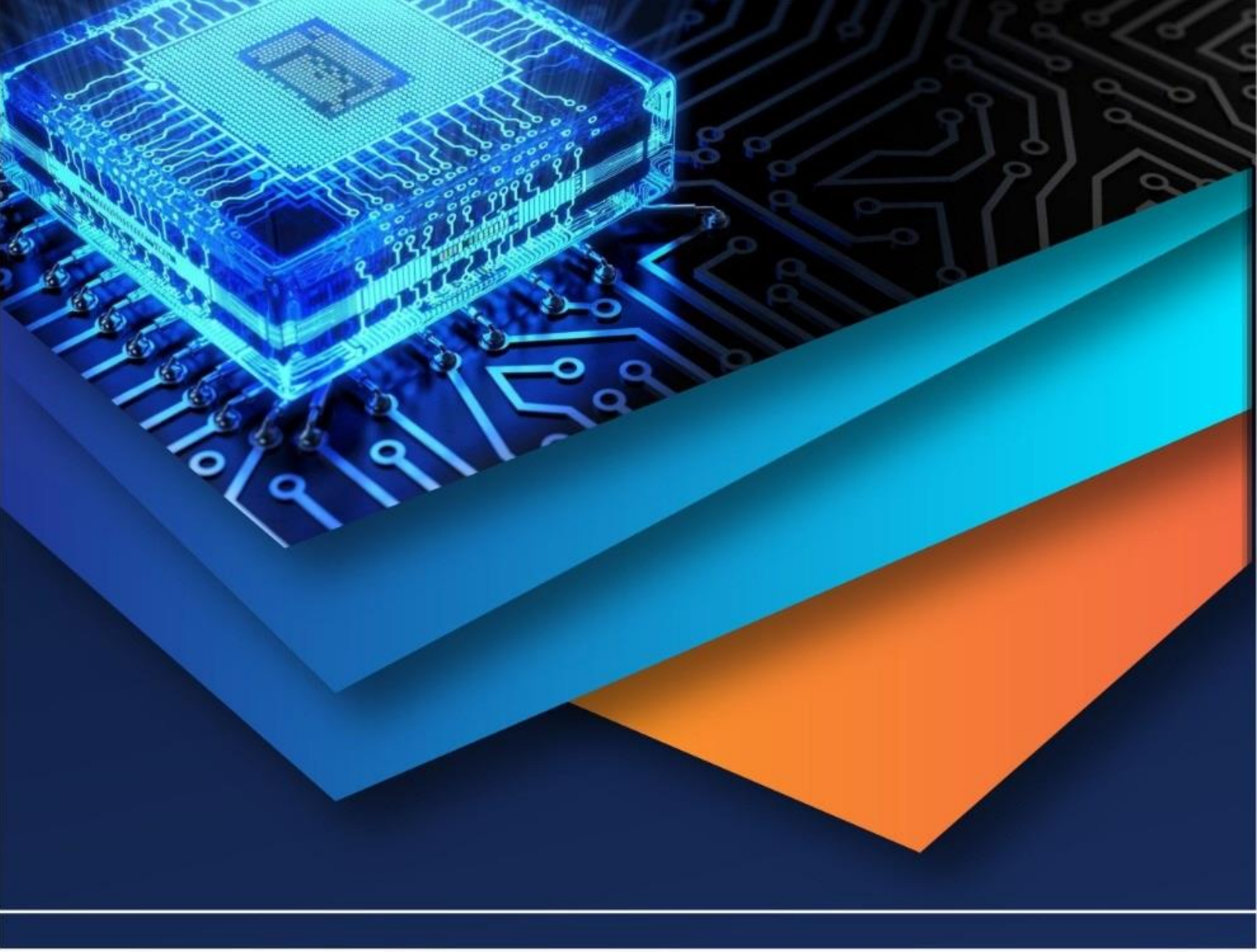
The project demonstrated the potential of deep learning-based approaches for both generating and detecting face morphing attacks. The performance of morph-3 identification dramatically improved once the morph 3 photos produced using superior tools are used for training. Additionally, we investigated the effectiveness of other machine learning based classifiers, and the best outcomes are produced by SVM. Following an analysis of various feature combining strategies, feature concatenation emerged as the most effective method for morph identification. In terms of age and lighting, the proposed model provides better results. [1]

VI. FUTURE SCOPE

Face morphing attacks are becoming increasingly common with the proliferation of social media and online identity verification systems. As such, there is a need for effective methods to detect and prevent such attacks. This project can be extended to explore more advanced techniques for generating and detecting face morphing attacks, such as the use of generative adversarial networks (GANs) or the integration of facial recognition technologies. The project can also be extended to develop practical solutions and tools to protect against face morphing attacks in real-world scenarios.

REFERENCES

[1] Muhammad Hamza , Samabia Tehsin, Hanen Karamti,“Generation and Detection Face Morphing Attacks” IEEE Access Volume 10,2022
[2] Christoph Busch, “Single Image Face Morphing Attack Detection Using Ensemble of Features” ,IEEE Xplore,2020
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[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] M. Ferrara, A. Franco, and D. Maltoni, ‘‘Face demorphing,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 1008–1017, Apr. 2018.
[10] 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.
[11] A. W. Yip and P. Sinha, ‘‘Contribution of color to face recognition,’’ Perception, vol. 31, no. 8, pp. 995–1003, 2002.
[12] 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.
[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] “Detection of Face Morphing Attacks by Deep Learning”, Conference: Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Lecture Notes in Computer ScienceVolume: 10431,DOI: 10.1007/978-3-319-64185-0_9



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)