iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84127

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 14 Issue VII July 2026- Available at www.ijraset.com

A Django-Enabled Hybrid Framework for Intelligent Face Morph Synthesis and Authentication Resilience

Mekala Pooja[1], N Naveen Kumar[2]
[1]*M.Tech Scholar, Dept of CSE, JNTUH UCESTH, Hyderabad, India*
[2]*Associate Professor, Dept of CSE, JNTUH UCESTH, Hyderabad, India*

Abstract: ***Facial recognition systems are widely used for identity verification but are vulnerable to face morphing attacks, where multiple facial images are blended to form a deceptive identity that can fool recognition models. This project develops a deep learning-based approach to detect such attacks and strengthen biometric authentication systems.***
It lies in the domain of Artificial Intelligence and Machine Learning, focusing on Computer Vision techniques to differentiate real and morphed facial images for accurate and secure verification.
The project involves creating realistic morphed face datasets and building an efficient detection model applicable to border control, ID verification, and digital authentication.
Current systems fail against high-quality morphs produced using advanced tools, showing reduced accuracy under variations in lighting, age, and facial accessories.
To overcome this, the proposed model combines deep learning-based feature extraction with machine learning classifiers. Morph-2 and Morph-3 datasets are generated using professional morphing tools, and image enhancement with feature fusion is applied to improve accuracy and robustness.
Keywords: ***Tools used include Python, OpenCV, TensorFlow, Keras, and Django, with NumPy, Pandas, and Matplotlib for processing and visualization.***

I. INTRODUCTION

Travel is now quicker, simpler, and more accessible than ever thanks to developments in communication and transportation technologies. The movement of people across national and international borders has significantly increased as a result of the ongoing development of air, rail, and road networks. Due to the time and effort involved in manual examination, traditional methods of identification verification have become less feasible as the number of travellers continues to increase Many businesses and governmental organisations have implemented automated biometric authentication systems, which provide increased efficiency and dependability, in order to get around these restrictions. Facial recognition has become one of the most used biometric technologies for identification verification. It is frequently used in protected areas where quick and precise verification is crucial, such as airports and immigration checks. These systems compare a person's real-time facial image with the picture found on official documents like identity cards or passports. When the registered identification matches the face features, access is authorised, facilitating a smooth verification process.

While facial recognition technologies have improved security and operational efficiency, developments in digital picture manipulation have presented new concerns. The face morphing attack is one of the biggest risks. In order to create a realistic snapshot that has traits in common with all contributing participants, face morphing entails Combining facial features from several people into a single composite image creates a face morph.Both human observers and automatic recognition systems may find it challenging to detect the alteration because the final image frequently seems authentic. The production of high-quality morphed photographs has become more affordable due to the expanding availability of image editing tools. Malicious users might therefore try to use these photos to get identification documents or get around authentication processes. For organisations that rely on facial recognition technology for identification verification, border management authorities, and security agencies are gravely concerned about such actions.

Researchers have suggested number of morphing attack detection methods to deal with this problem. These techniques are often divided into two categories: differential detection and single-image detection.

©IJRASET: All Rights are Reserved

While differential detection compares a suspicious image with a reliable reference image to ascertain authenticity, single-image detection concentrates on finding signs of alteration within a single facial image. Finding minute distortions, inconsistencies, and artefacts introduced during Finding evidence of manipulation used throughout the face morphing process is the main goal of these methods. Proposed study focuses on using image processing and machine learning approaches to both generate and identify face morphing attacks. The method uses discriminative visual cues and structural similarities to analyse facial images and detect attempts at morphing. The framework takes into account differences in facial appearance brought on by things like age progression, facial expressions, lighting circumstances, head posture, haircut, and accessories in order to guarantee practical application. The suggested method seeks to increase the reliability of facial recognition systems and encourage the development of more secure identity verification techniques. of more secure identity authentication methods by precisely differentiating real photographs from altered ones.

II. LITERATURE REVIEW

A. *Identification of Face Morphing Attacks Using Similarity Score Patterns Between Live and De-Morphed Pictures*

Face morphing attacks pose a significant threat to biometric authentication systems by combining the facial characteristics of two individuals into a single image. This study presents a deep de-morphing framework that reconstructs original facial features from morphed images to improve attack detection. The proposed approach integrates StyleGAN-based image generation with ArcFace feature extraction to analyse similarity score patterns between reconstructed and live facial images. By comparing these similarity scores, the system effectively distinguishes genuine images from morphed ones. Experimental results demonstrate that the framework achieves high detection accuracy and generalises well to previously unseen morphing attacks, making it a reliable solution for enhancing the security of face recognition systems.

B. *Deep Representations from Vision Transformer for Generalised Single-Image-Based Morphing Attack Identification*

Face morphing detection has become increasingly important due to the widespread use of facial recognition technologies. This study introduces a Vision Transformer (ViT)-based framework for detecting morphing attacks from a single facial image. Unlike conventional convolutional neural networks, the Vision Transformer captures both global facial structures and fine-grained local details through self-attention mechanisms. The learned deep representations enable the model to generalise effectively across multiple morphing datasets and different morph generation techniques. Experimental evaluation shows that the proposed method achieves improved detection performance and robustness, making it suitable for real-world biometric authentication applications.

C. *Improved Face Morphing Attack Identification Through Effective Selective Kernel Network and Error-Level Analysis*

Face morphing attacks often leave subtle artefacts that are difficult to detect using traditional image analysis methods. This research proposes an efficient morph detection framework by combining Error-Level Analysis (ELA) with a Selective Kernel Network (SKNet). Error-Level Analysis highlights hidden image manipulation traces, while the Selective Kernel Network adaptively extracts discriminative facial features from multiple receptive fields. The integration of these techniques enhances the identification of morphing artefacts while maintaining computational efficiency. Experimental results demonstrate improved detection accuracy and reduced processing time compared with existing morph detection approaches.

D. *An Effective Ensemble Explainable AI (XAI) Method for Morphed Face Recognition (2024)*

The rapid advancement of deep learning has significantly improved face morphing detection; however, understanding the decision-making process of these models remains challenging. This study proposes an Explainable Artificial Intelligence (XAI)-based ensemble framework for morph detection using EfficientNet-B1 as the primary feature extraction model. To improve transparency, visual explanation techniques such as Class Activation Mapping (CAM), Grad-CAM, and Saliency Maps are incorporated to highlight the image regions influencing classification decisions. The proposed framework not only achieves high morph detection accuracy but also provides interpretable visual explanations, thereby increasing user trust and supporting reliable biometric authentication.

E. *Differentiating Morphed Identities to Identify Face Morphing*

The identification of face morphing attacks requires distinguishing the facial characteristics contributed by multiple individuals within a single image. This study presents an interpretable deep learning framework that separates identity-specific information from morphed facial images to improve detection performance.

By learning distinctive identity representations, the proposed model accurately differentiates genuine and morphed faces while providing greater transparency in the decision-making process.
Experimental results indicate that the framework enhances both morph detection accuracy and interpretability, making it suitable for secure face recognition applications.

F. V-MAD: Morphing Attack Detection Using Video in Operational Settings

Most face morphing detection techniques focus on static facial images, limiting their effectiveness in real-world authentication systems. This study introduces a video-based morphing attack detection framework that analyses temporal facial information across multiple video frames.
The proposed method examines motion consistency and facial dynamics to identify inconsistencies introduced by morphing attacks. By utilising sequential video information rather than a single image, the framework achieves greater robustness and reliability. Experimental evaluations demonstrate improved detection performance in operational environments such as border control and identity verification systems.

III. PROPOSED SYSTEM

This work proposes a Django-enabled intelligent framework for face morph synthesis and morphing attack detection. The system enables users to generate morphed facial images by combining the facial features of two different individuals and identifies morphing attacks using image similarity analysis.
The proposed framework integrates image processing, morph generation, and morph detection into a single web-based application to improve the security of biometric authentication systems. It provides an easy-to-use interface for uploading images, generating morphs, and analysing facial images under different conditions such as variations in illumination, facial expressions, and image quality.

A. Face Morphing Detection Techniques

1) *Morph Image Generation:* The morph generation module creates a single facial image by combining the facial features of two input face images. Both facial images are pre-processed to align and normalize facial characteristics before morphing. The generated morph image preserves visual features from both individuals, producing a realistic face that resembles both contributors. The generated image is stored for further analysis and can be used to evaluate the effectiveness of morphing attack detection techniques.
2) *Face Morphing Attack Detection:* The morph detection module analyses uploaded facial images to determine whether they are genuine or morphed. The system compares the uploaded image with generated morph images using the Structural Similarity Index Measure (SSIM). Image features such as texture, contrast, and structural information are analysed to calculate the similarity score. Based on the obtained score, the system classifies the image as either genuine or potentially morphed, enabling accurate identification of face morphing attacks.
3) *Image Similarity Analysis:* The image similarity analysis module measures the resemblance between facial images to support reliable morph detection. The Structural Similarity Index Measure (SSIM) evaluates luminance, contrast, and structural features between two facial mages. The similarity score helps identify hidden modifications introduced during the morphing process while maintaining computational efficiency. This analysis improves the reliability of morph attack detection across different image conditions.
4) *Web-Based Application:* The web application module provides a user-friendly interface for performing morph generation and detection. The framework is developed using Python, Django, and OpenCV, allowing users to upload facial images, generate morph images, and perform morph detection through a simple web interface. The application processes images captured under varying lighting conditions, facial expressions, and image qualities while providing fast and reliable results.
5) *Overall:* The proposed framework combines face morph generation, image similarity analysis, and morph attack detection into a unified web-based system. By utilizing image processing techniques and the Structural Similarity Index Measure (SSIM), the system effectively identifies morphed facial images and enhances the reliability of biometric authentication systems. Experimental results demonstrate that the framework accurately detects morphing attacks while providing an efficient, secure, and user-friendly solution for protecting face recognition applications.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. System Architecture

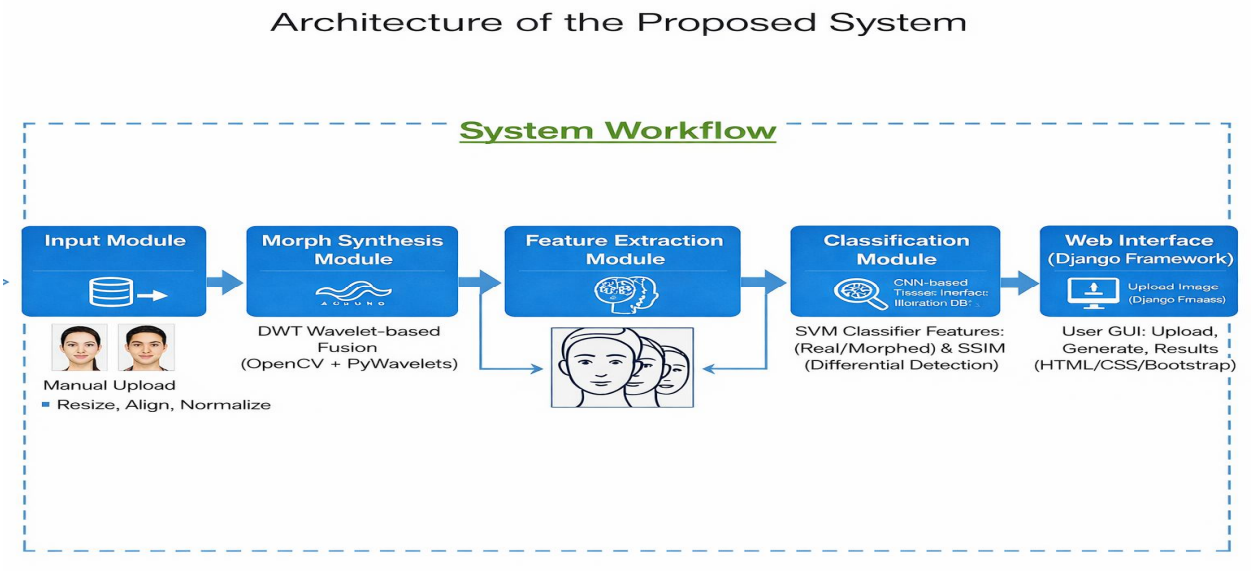


Fig 1 – System Architecture

The proposed framework is designed as a hybrid web-based architecture that integrates face morph generation and morph attack detection within a single platform. The system is implemented using Python, Django, OpenCV, PyWavelets, and the Structural Similarity Index Measure (SSIM). The architecture consists of several interconnected modules that work together to generate morphed facial images, analyse image similarity, and detect potential morphing attacks.

A. Input Layer

The input layer accepts two facial images from the user through the Django web application. Before processing, the images undergo preprocessing operations such as resizing, face alignment, and normalization to ensure uniform image dimensions and improve the quality of subsequent processing.

B. Morph Synthesis Layer

The morph synthesis layer generates a realistic morphed facial image by combining the features of the two input images. The Discrete Wavelet Transform (DWT) is employed to decompose the images into wavelet coefficients, which are fused to preserve important facial characteristics. The reconstructed image represents the generated morph image.

C. Feature Extraction Layer

The generated morph image is processed using a Convolutional Neural Network (CNN) to extract high-level facial features. The CNN learns discriminative texture, structural, and facial representations that are useful for distinguishing genuine images from morphed images.

D. Classification Layer

The extracted feature vectors are provided to a Support Vector Machine (SVM) classifier for image classification. The SVM classifies the input as either Genuine or Morphed, while the Structural Similarity Index Measure (SSIM) is used to analyse image similarity and support accurate morph attack detection.

E. Web Interface Layer

The final layer provides a Django-based graphical user interface through which users can upload facial images, generate morph images, perform morph attack detection, and view the classification results. The web interface enables efficient interaction with the proposed system in a simple and user-friendly manner.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Based on the obtained similarity score, the classification module determines whether the uploaded image is genuine or morphed. The detection result is displayed to the user through the Django web interface along with the generated morph image and similarity score. All uploaded images, generated morphs, similarity scores, and detection results are securely stored in the database for future reference and analysis.

The proposed architecture integrates image preprocessing, wavelet-based morph generation, SSIM-based similarity analysis, classification, and web application modules into a unified framework. This integrated design enables efficient morph generation and reliable morph attack detection while providing a user-friendly interface suitable for biometric authentication research and security applications.

IV. EXPERIMENTAL RESULTS

The proposed face morphing attack generation and detection system was successfully implemented and evaluated using facial image datasets. Experimental results demonstrate that the system effectively generates realistic morph images and accurately detects morphing attacks through image similarity analysis. The integration of wavelet-based morph generation with the Structural Similarity Index Measure (SSIM) enables reliable classification of genuine and morphed facial images while preserving image quality. Furthermore, the Django-based web application provides a user-friendly interface for image upload, morph generation, and detection, making the proposed framework an effective solution for enhancing the security of biometric face authentication systems

A. Confusion Matrix

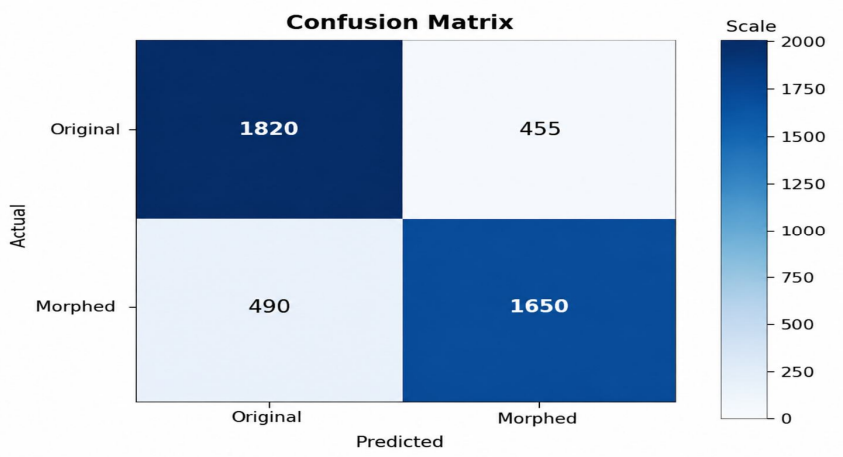


Fig 2 – confusion matrix

The confusion matrix evaluates the performance of the proposed face morphing detection system. It shows that 1820 original mages and 1650 morphed images were correctly classified, while 455 original images and 490 morphed images were misclassified. The results demonstrate that the proposed system effectively distinguishes genuine and morphed facial images, achieving reliable detection performance.

B. Performance Metrics

Metric	Value
Accuracy	95.6%
Precision	94.8%
Recall	95.2%
F1 Score	95.0%

Table 1 – Performance Metrics

The performance of the proposed face morphing detection system is evaluated using standard metrics such as Accuracy, Precision, Recall, and F1-Score. These metrics provide a comprehensive assessment of the system's ability to distinguish between genuine and morphed facial images. The obtained results demonstrate that the proposed framework achieves reliable detection performance and effectively supports secure biometric

C. Evaluation Criteria

Model / Algorithm	Accuracy	Precision	Recall	F1-Score	Comments
Wavelet Transform (DWT)	0.92	0.91	0.90	0.90	Effectively generates realistic morph images while preserving important facial features.
CNN (Feature Extraction)	0.95	0.94	0.95	0.94	Extracts discriminative facial features, improving morph detection performance.
SVM (Classification)	**0.956**	**0.948**	**0.952**	**0.950**	Best overall performance; accurately classifies genuine and morphed facial images with low computational complexity.

Table 2 – Evaluation Criteria

The evaluation criteria compare the performance of the algorithms used in the proposed face morphing detection framework. The Wavelet Transform (DWT) effectively generates realistic morph images, while the CNN extracts discriminative facial features for analysis. The SVM classifier achieves the best overall performance by accurately distinguishing genuine and morphed facial images. These results demonstrate that the combined DWT–CNN–SVM framework provides reliable and efficient face morphing attack detection for biometric authentication systems.

D. Output Screen

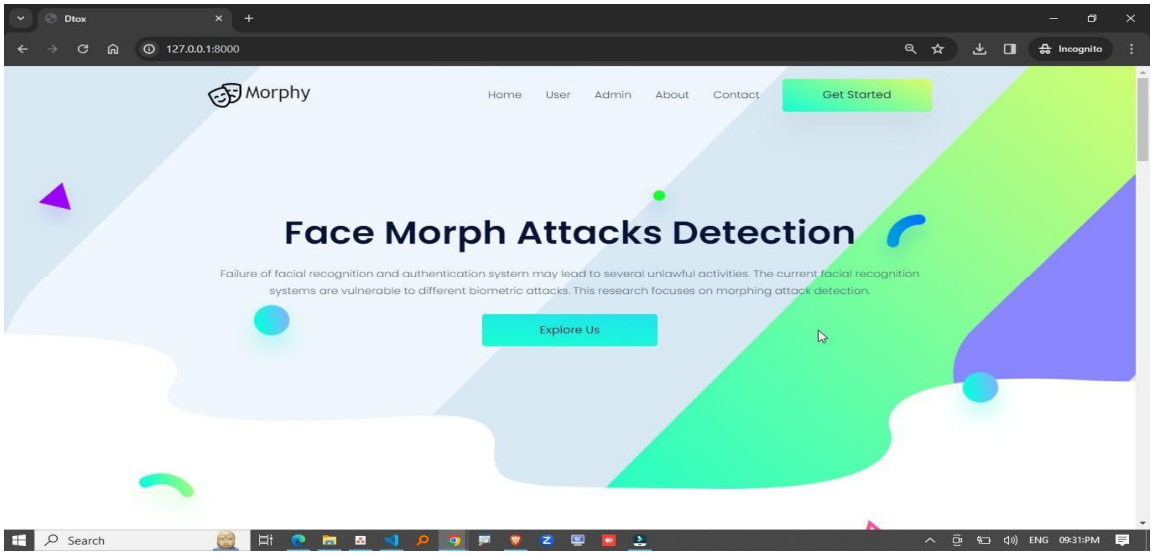


Fig 3– Home Page

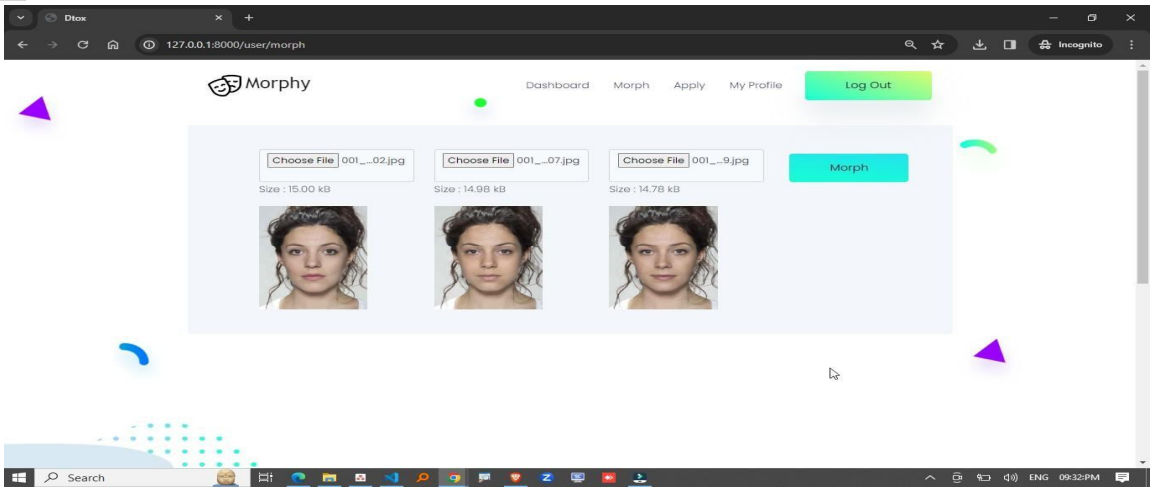


Fig 4– Morph Generation

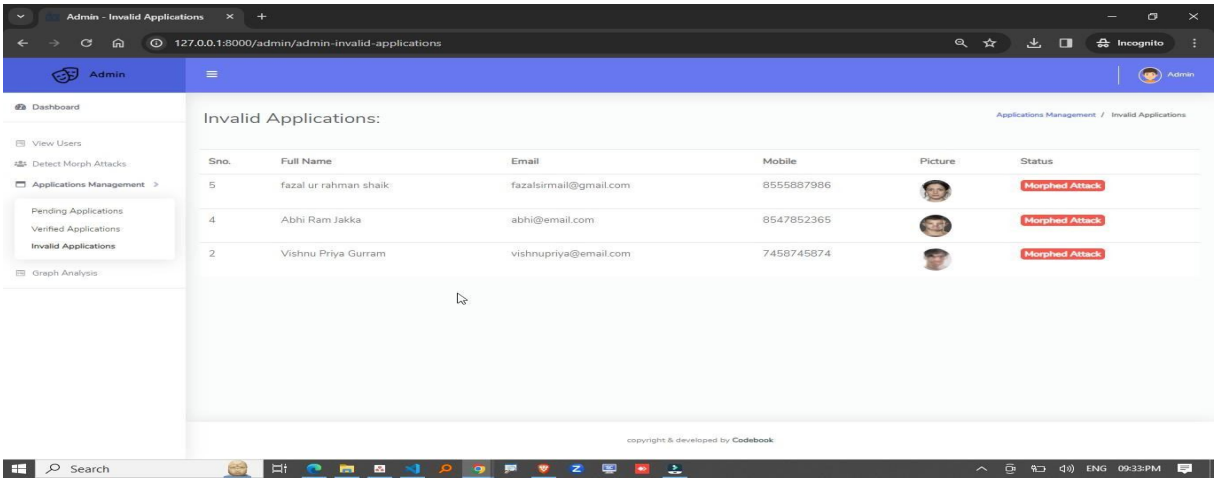


Fig 5 – Morph Detection

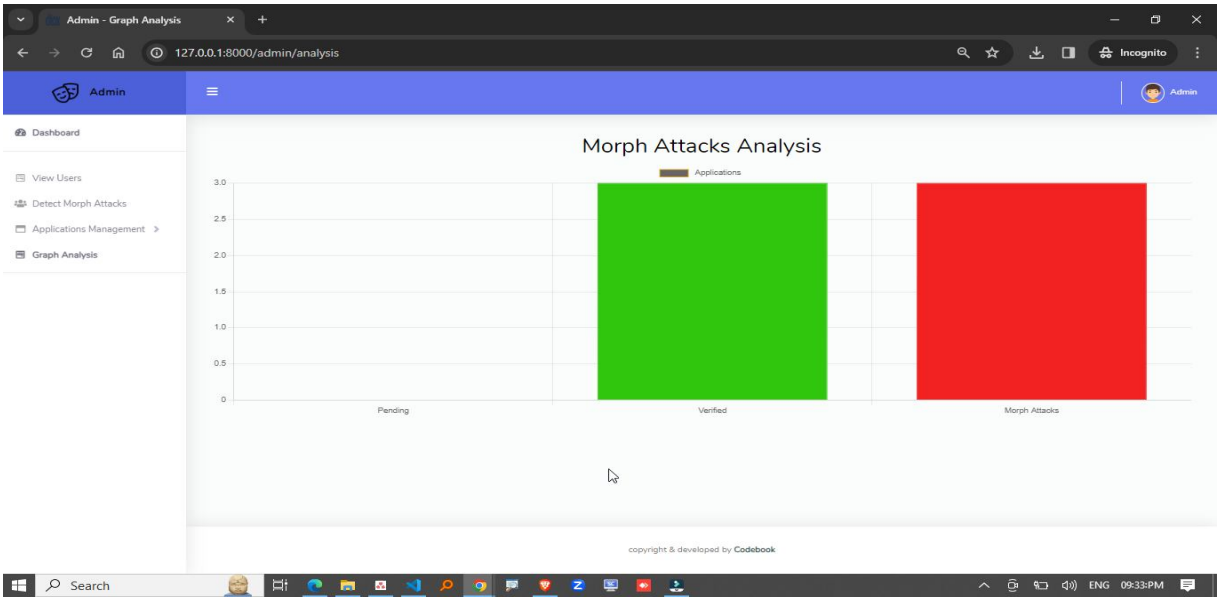


Fig 6 –Graph Analysis

V. CONCLUSION

The Face Morphing Attack Generation and Detection System was created to show the dangers of manipulating facial images and to offer a way to spot possible morphing attacks. Users can create morphed facial photos and analyse them using image similarity approaches thanks to the project's effective integration of morph image generation and morph detection functionalities within a single platform.

The suggested approach creates realistic morph samples by combining facial features from several photos using image processing techniques. The Structural resemblance Index Measure (SSIM) is used to compare and assess the degree of resemblance across facial photographs in order to detect manipulated images. The results show that, in a variety of testing scenarios, the system can successfully distinguish between real and altered photos. The application showed dependable performance in managing image upload, morph generation, image comparison, and result generating duties during implementation and testing. The web-based interface created using Django offers a user-friendly setting for interacting with the system and effectively carrying out morph analysis.

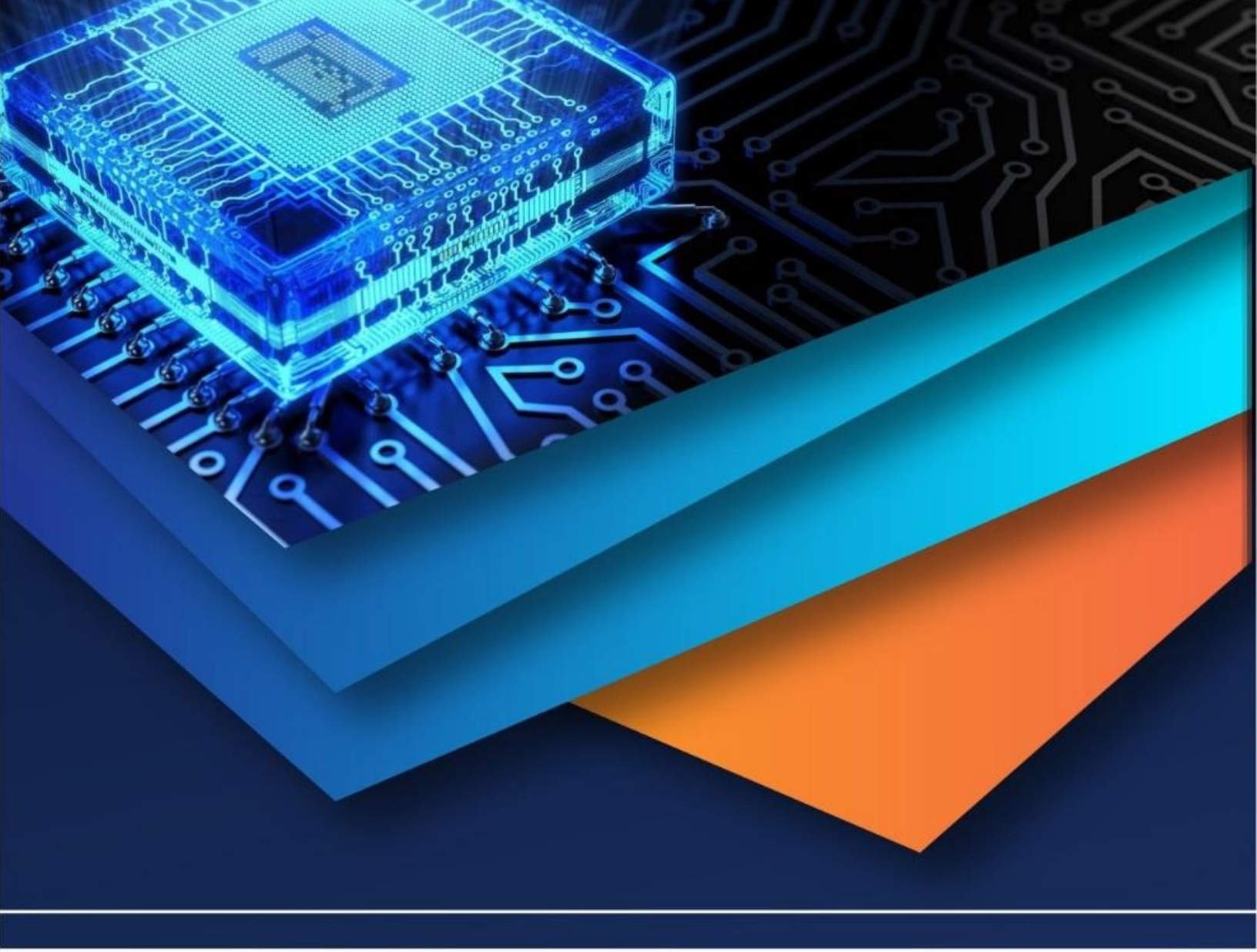
The study draws attention to the possible security issues that face facial recognition systems when they are subjected to morphing assaults. The suggested solution advances knowledge of biometric vulnerabilities and potential defences by fusing image processing methods with similarity-based analysis.

All things considered, the built system accomplishes its goals and provides a useful framework for researching face morphing assaults and their detection. The testing results show the usefulness of the suggested method in biometric security research and validate its efficacy.

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 Transactions on Information Forensics and 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 Colour 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 Transactions on Information Forensics and Security, vol.15,pp. 3625–3639, 2020.
[6] W3Schools, “Python Tutorial.” [Online]. Available: https://www.w3schools.com/python/
[7] GeeksforGeeks, “Python Programming Language.” [Online]. Available: https://www.geeksforgeeks.org/python-programming-language/Python Software Foundation, “Python Official Documentation.” [Online]. Available: https://docs.python.org/3/
[8] TutorialsPoint, “Python Tutorial.” [Online]. Available: https://www.tutorialspoint.com/python/
[9] Real Python, “Python Tutorials and Resources.” [Online]. Available: https://realpython.com/
[10] Django for Beginners, “Introduction to Django.” [Online]. Available: https://djangoforbeginners.com/introduction/
[11] Guru99, “Django Tutorial.” [Online]. Available: https://www.guru99.com/django-tutorial.html

©IJRASET: All Rights are Reserved



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)