International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

GENERATION AND DETECTION OF FACE MORPHING ATTACKS

G. Prabhakar[1],D. Nithisha[2], Y. Sai Manisha[3],B.Manvitha[4]

[1]Assistant professor, School of CSE ,Malla Reddy Engineering College For Women(Autonomous Institution), Maisammaguda, Dhulapally,Secunderabad,Telangana-500100

[234]UG Scholar, Department of CS,Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100
Email : prabhakarm.tech@gmail.com

ABSTRACT

Face recognition systems have become an essential component in secure real-time applications such as automated border control (ABC) systems. However, face morphing attacks are becoming a challenge to these systems because a morphed image, generated by morphing the facial features of two or more individuals, can bypass biometric authentication. Such attacks pose a serious security threat because they enable unauthorized people to obtain electronic machine-readable travel documents (eMRTDs) or e-passports, which allow them to pass through borders without detection. This paper provides an in-depth review of face morphing attacks, considering both the generation and detection of morphed images. Several morph generation techniques, including image warping, deep learning models, and hybrid approaches, are discussed against state-of-the-art methods for morph attack detection, that include forensic analysis, deep learning-based detection, and cross-domain techniques. Benchmarking efforts and public databases are also reviewed against evaluation metrics for MAD systems. The paper discusses the current challenge of realism in the generated morphs, robust detection over diverse conditions, and considerations of privacy. Finally, potential future directions such as real-time detection, adversarial training, and multimodal biometric approaches are explored in order to address these emerging threats for biometric security systems**.**

Keywords - Face recognition systems, face morphing attacks, biometric security,automated border control, e-passports, morph generation, morph attack detection (MAD), deep learning, forensic feature analysis, benchmarking

I. INTRODUCTION

Biometric recognition has become the foundation of modern identity verification and secure access control systems. By utilizing unique biological traits, such as face, fingerprint, and iris, or behavioral characteristics, such as gait and keystroke dynamics, biometric systems offer reliable methods for person identification and verification. Among these, face recognition systems (FRSs) have become very popular as facial images can be captured easily and for a wide variety of applications including healthcare, law enforcement, e-commerce, and border control. In fact, the Automated Border Control (ABC) systems heavily rely on FRSs for verifying traveler's identity against facial images captured in their passport or eMRTD. Despite their advantages, FRSs are susceptible to a variety of attacks targeting their security.

Presentation attacks involving digital displays, printed images, or 3D masks are well-known. However, face morphing attacks have recently emerged as one of the most severe risks. A morphing attack combines the facial features of two or more people to form a composite image that can be authenticated as being both individuals. This poses a tremendous security threat because an e-passport or eMRTD created with a morphed image can allow a malevolent actor to bypass identity checks and gain unauthorized access with the accomplice's identity left on record. Face morphing

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

attacks challenge the core principle of single ownership in biometric systems, which undermines the integrity of secure documents.

Advanced detection mechanisms must be deployed to identify morphed images during enrollment and verification stages of biometric systems. This project focuses on the generation and detection of face morphing attacks using up-to-date morphing techniques and countermeasures. This project aims to propose robust solutions for mitigating the risk of morphing attacks in FRSs, especially in critical applications such as border control, by reviewing existing MAD methods, benchmarking databases, and evaluation metrics.

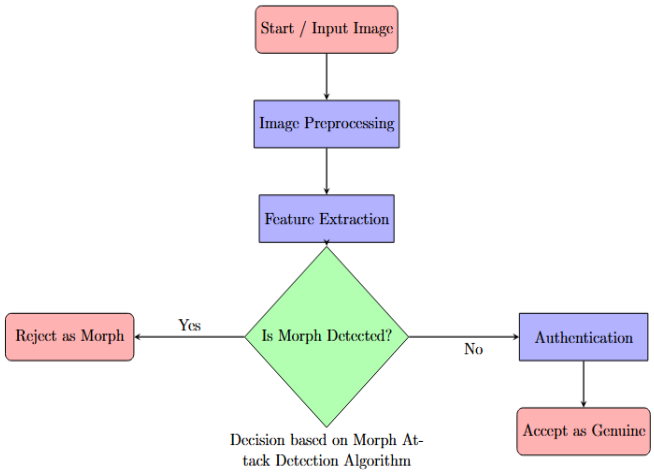

Fig 1: System Architecture

II. RELATED WORK

1. Title: Face Demorphing .

Authors: M. Ferrara, A. Franco, and D. Maltoni .

Year: 2018**.**

This paper introduces techniques for demorphing to counter vulnerabilities in biometric systems caused by facial morphing. It focuses on restoring original facial features from morphed images, thereby improving the reliability of face recognition systems in forensic and security applications.

2. Title: FD-GAN: Face De-Morphing Generative Adversarial Network for Restoring Accomplice's Facial Image

Authors: F. Peng, L.-B. Zhang, and M. Long

Year: 2019

The authors propose a generative adversarial network-based framework, named FD-GAN to reconstruct the original facial images from the morphed ones. This is an approach that effectively tackles the morphing threats and, therefore, makes the face recognition systems more robust against the detection of accomplice identities.

3. Title: Face Recognition Systems Under Morphing Attacks: A Survey

Authors: U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch

Year: 2019

This survey provides an exhaustive review of morphing attacks on face recognition systems and existing detection techniques. It has brought out the challenges these attacks pose and called for robust methods to address the issue effectively.

4. Title: Contribution of Color to Face Recognition

Authors: A. W. Yip and P. Sinha

Year: 2002

This paper explores the role of color in facial recognition systems. Although it is not particularly focused on morphing attacks, it offers some foundational information regarding factors affecting face recognition, which plays an important role in understanding and enhancing recognition capabilities.

5. Title: Deep Face Representations for Differential Morphing Attack Detection

Authors: U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch

Year: 2020

This work focuses on using deep learning techniques to detect morphing attacks by analyzing the differences in deep face representations. It introduces advanced methods to enhance the robustness of biometric systems against these sophisticated threats.

III IMPLEMENTATION

Several key stages involved in the implementation of a face morphing attack detection system would identify morphing attempts. These begin with preprocessing, which standardizes the input images, captured either live or obtained from electronic machine-readable travel documents (eMRTDs), through face alignment, normalization, and resizing for uniformity in analysis. Next, the system applies feature extraction with advanced deep learning models, like CNNs, to identify biometric patterns. These models are trained on large datasets that contain genuine and morphed images so that they can detect the subtle artifacts introduced during the morphing process. The Morph Attack Detection (MAD) is the core stage in the system, where extracted features are analyzed to classify images as either genuine or morphed.

Ensemble learning, forensic feature analysis, and/or frequency domain analysis are incorporated in the system to improve the accuracy of detection. Decision thresholds are set based on valid outcomes achieved while trying to balance sensitivity with specificity. After classifying, the system flags the image as a morph for rejection, raising a security alert or goes on to authentication where the actual image is matched with stored templates to verify the identity. It is utilized with publicly available datasets for its validation and optimizes performances using metrics such as FAR and FRR. The system ensures that the approach is real-time and enables it to be suitable for such applications as automated border control and other secured biometric applications.

IV ALGORITHM

Input Acquisition:

- Acquire a facial image from a live camera or extract it from an electronic machine-readable travel document (eMRTD).

Preprocessing:

- Face alignment by key landmarks such as eyes, nose, and mouth.
- Resize the image and apply color correction.

Feature Extraction:

- Pass the preprocessed image through a deep learning model, like convolutional neural network (CNN), to extract appropriate biometric features.
- Spatial and frequency domain analysis for further forensic features

Morph Detection:

- Take the extracted features and run them through a classification model which was trained on both authentic and morphed face databases
- Use ensemble learning or support vector machines for classification.

Decision Making:

- If the classification model identifies the image as morphed, tag it as an attack and reject it.
- If the classification model identifies the image as authentic, proceed with authentication.

Authentication:

- Compare the features of the genuine image with the stored template for verifying the claimed identity
- If the match is good, then grant access else reject the authentication attempt

Performance Evaluation:

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

- Use metrics like FAR and FRR for the validation dataset to benchmark the system.
- Tune the model and decision thresholds according to the benchmarking results

Output

- Give a clear decision: Accept as Genuine or Reject as Morph.
- This algorithm strives for a systematic approach to face morphing attack detection while maintaining high precision and reliability.

V.RESULTS

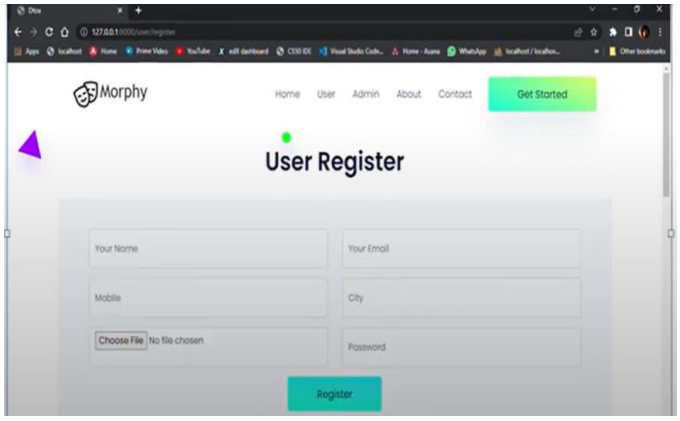

Fig 1: User Register

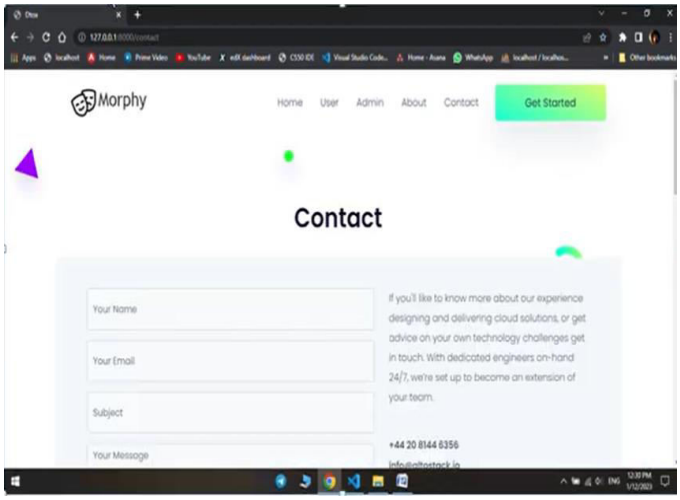

Fig 2: Contact

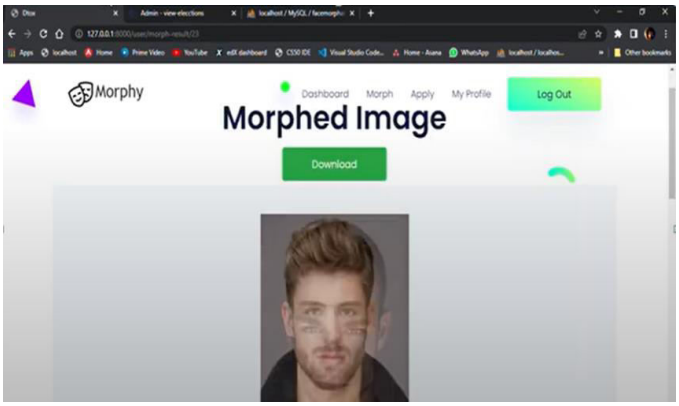

Fig 3: Morphed Image

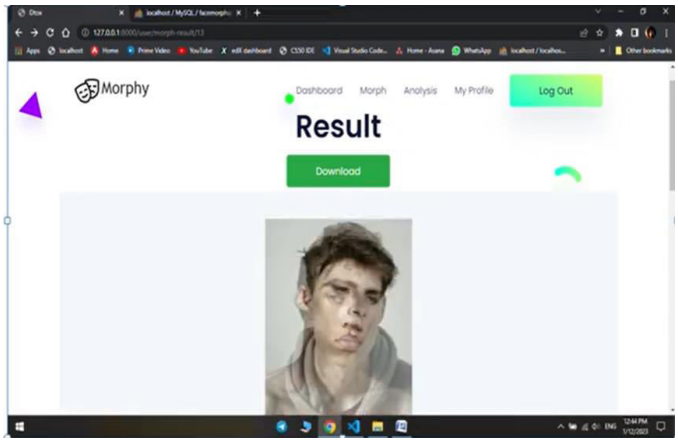

Fig 4:Result Image

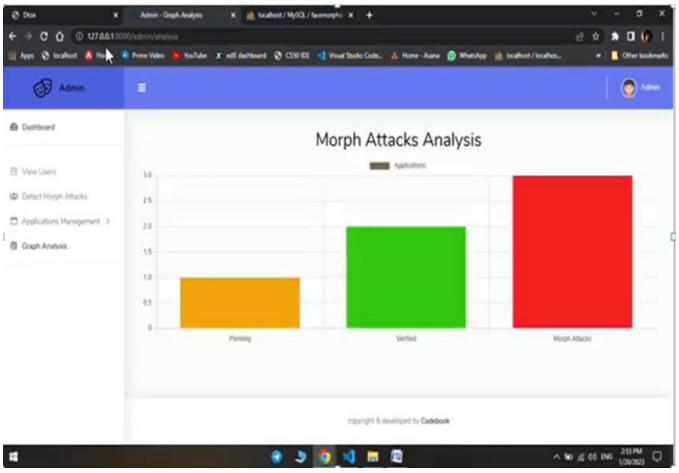

Fig 5: Accuracy Bar Graph

VI.CONCLUSION

Facial recognition systems play a very significant role in security and authentication processes, but vulnerability to biometric attacks, like morphing, poses challenges. The proposed work addresses such challenges by providing a robust mechanism for the detection of morphing attacks with variation in age, illumination, and accessories, like eye and headgear. The proposed system therefore improves detection accuracy by a deep learning-based feature extractor and classifier together with advanced image enhancement and feature combination techniques. The key contribution of this work is the development of a versatile dataset that includes Morph-2 and Morph-3 images, with Morph-3 offering more realistic morphs created using professional morphing software. This dataset fills a critical gap in the literature, as Morph-3 images have not been explored before, and they better simulate real-world morphing scenarios. The use of eight diverse facial databases ensures the system's robustness across a wide range of variations.

Extensive experimental evaluations clearly show that the proposed method outperforms current methods and yields promising results in detecting even sophisticated morphing attacks. This work hence forms a strong foundation for further developments of secure facial recognition systems and underlines the need for continuous innovation against evolving biometric threats..

REFERENCES

[1] M. Ferrara, A. Franco and D. Maltoni, "Face demorphing", IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 1008-1017, Apr. 2018.
[2] .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.
[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, et al., "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, pp. 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", Proc. 21st Int. Conf. pattern Recognit. (ICPR2012), pp. 1363-1366, 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.
[13] R. Raghavendra, K. B. Raja, S. Venkatesh and C. Busch, "Transferable deep-CNN features for detecting digital and print-scanned morphed face images", Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), pp. 10-18, Jul. 2017
[14] .S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis and C. Busch, "De
R. Raghavendra, K. B. Raja and C. Busch, "Detecting morphed face images", Proc. IEEE 8th

Int. Conf. Biometrics Theory Appl. Syst. (BTAS), pp. 1-7, Sep. 2016.tecting morphed face attacks using residual noise from deep multi-scale context aggregation network", Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), pp. 280-289, Mar. 2020.

[15]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.