www.ijerst.com
Vol. 22, No. 1(1), 2026

Research Paper

Face Morph Detection System

[1]DR K. ASHOK KUMAR, [2]M.HASINI , [3]D.RISHIKA, [4]A.SAMIKSHA

[1]ASSOCIATE PROFESSOR, CSE(AI&ML), Bhoj Reddy Engineering College For Women.

[234]B.TECH, SCHOLAR, CSE(AI&ML), Bhoj Reddy Engineering College For Women.

ABSTRACT

Face morphing attacks are an emerging security threat in biometric authentication systems, particularly in applications such as passport verification, border control, and identity management. A morphed face image is created by blending the facial features of two or more individuals into a single image, enabling multiple people to fraudulently authenticate using the same identity. This creates a serious risk for systems that rely on facial recognition technologies. The Face Morph Detection System is designed to identify and prevent such attacks by analyzing facial images and determining whether an image is genuine or morph-generated. The proposed system employs advanced machine learning and image processing techniques to extract facial features and detect inconsistencies introduced during the morphing process. It is trained on datasets containing both genuine and morphed images to ensure accurate classification. The developed model processes an input image by extracting key facial landmarks and texture features, and then applies a trained classification algorithm to determine its authenticity. By distinguishing between real and morphed images, the system enhances the reliability and security of biometric authentication systems. This project highlights the role of artificial intelligence in strengthening biometric security and offers an effective solution for detecting morphing-based identity manipulation in real-world scenarios.

1.INTRODUCTION

1.1 INTRODUCTION OF THE PROJECT

Face recognition technology has become one of the most widely used biometric authentication methods in modern security systems. It is extensively applied in areas such as border control, passport verification, surveillance systems, and digital identity management. However, with the advancement of image processing and artificial intelligence techniques, biometric systems have become vulnerable to various types of attacks. One of the most critical threats among these is the face morphing attack.

A face morphing attack involves blending two or more facial images to create a single synthetic image that resembles all contributing individuals. This manipulated image can be used to fraudulently obtain identity documents such as passports, enabling multiple individuals to authenticate as the same person. Such attacks exploit the limitations of facial recognition systems, particularly those that rely on visual similarity rather than deep feature analysis. Studies show that morphing attacks can successfully bypass automated border control systems, posing serious risks to national security .

The growing accessibility of advanced image editing tools and generative models has further increased the feasibility of creating high-quality morphed images. These images often appear realistic and are difficult to detect with the human eye or traditional verification systems. As a result, the need for robust face morph detection mechanisms has become essential in strengthening biometric security.

The Face Morph Detection System is designed to address this challenge by distinguishing between genuine and morphed facial images. The system leverages machine learning and deep learning techniques to analyze facial structures, textures, and inconsistencies introduced during the morphing process. By extracting discriminative features such as facial landmarks, pixel-level variations, and blending artifacts, the system can effectively classify images as authentic or manipulated.

Recent advancements in artificial intelligence, particularly convolutional neural networks (CNNs) and generative models, have significantly improved the performance of morph detection systems. These models can learn complex patterns from large datasets and generalize across different types of morphing techniques. Additionally, hybrid approaches combining spatial and frequency domain features have shown promising results in detecting subtle artifacts that are otherwise difficult to identify.

This project focuses on developing an efficient and accurate face morph detection system capable of operating in real-world scenarios. By integrating advanced feature extraction methods and classification algorithms, the system aims to enhance the reliability of biometric authentication systems. Ultimately, it contributes to preventing identity fraud and ensuring the integrity of security infrastructures.

2. LITERATURE SURVEY

Face morphing attack detection has gained significant attention in recent years due to the vulnerabilities it introduces in biometric systems. Several researchers have explored different approaches to generate, analyze, and detect morphed facial images.

According to Venkatesh et al. (2021), face recognition systems are highly susceptible to morphing attacks, especially in applications such as electronic passports and border control systems. The authors provided a comprehensive survey of morph generation and detection techniques, highlighting that morphing attacks can bypass identity verification systems if not properly addressed . They categorized detection methods into single-image based and differential approaches, emphasizing the importance of robust feature extraction.

Scherhag et al. (2019) conducted extensive research on the impact of morphing attacks on face recognition systems. Their study demonstrated that many commercial systems fail to detect morphed images, thus emphasizing the need for dedicated morph detection algorithms. They also explored deep learning-based approaches that utilize convolutional neural networks for improved accuracy.

Ferrara et al. (2018) introduced the concept of face de-morphing and proposed techniques to reconstruct original identities from morphed images. Their work highlighted the complexity of morphing artifacts and the necessity of advanced feature analysis for accurate detection.

Hamza et al. (2022) presented a detailed review of morphing attack detection (MAD) methods and analyzed their performance across various datasets. The study discussed different morph generation techniques and their corresponding detection challenges, providing insights into the strengths and limitations of existing approaches .

Nightingale et al. (2021) investigated both human and computational abilities to detect morphed images. Their findings revealed that humans are generally poor at identifying morphs, reinforcing the need for automated detection systems. The study also highlighted the importance of perceptual and computational analysis in improving detection accuracy .

Saleem and Shukr (2018) proposed a texture-based approach for morph detection using techniques such as Local Binary Patterns (LBP) and Gray-Level Co-occurrence Matrix (GLCM). Their system extracted texture features and applied classification algorithms to distinguish between real and morphed images .

Raghavendra et al. (2017) introduced differential morph detection techniques that compare the input image with a trusted live capture. This method improves detection accuracy but requires additional data, making it less practical in some real-world scenarios.

Recent research has focused on deep learning-based solutions. A study published in 2024 proposed a method combining error-level analysis with an efficient selective kernel network to improve detection accuracy while maintaining computational efficiency . This approach demonstrated that analyzing color channel inconsistencies can significantly enhance classification performance.

Ivanovska and Štruc (2023) introduced a diffusion-based morph detection method that identifies morphed images as out-of-distribution samples. Their approach addresses the generalization problem in traditional models and achieves competitive performance across multiple datasets.

Sarkar et al. (2020) analyzed the vulnerability of face recognition systems to morphing attacks using generative adversarial networks (GANs). Their work highlighted the importance of robust datasets and evaluation techniques in developing reliable detection systems.

3. METHODOLOGY

The proposed Face Morph Detection System follows a structured approach consisting of data collection, preprocessing, feature extraction, and classification. Initially, a dataset containing both genuine and morphed facial images is collected. These datasets may include publicly available biometric databases and synthetically generated morph images.

In the preprocessing stage, images are normalized to ensure consistency in size, resolution, and illumination. Face detection algorithms are applied to isolate the facial region from the background. Landmark detection techniques are then used to identify key facial points such as eyes, nose, and mouth.

Feature extraction plays a crucial role in detecting morphing artifacts. The system extracts both geometric and texture-based features. Geometric features include distances and angles between facial landmarks, while texture features are derived using methods such as Local Binary Patterns and frequency domain analysis.

After feature extraction, the data is fed into a machine learning or deep learning model. Convolutional Neural Networks (CNNs) are commonly used due to their ability to capture spatial hierarchies in images. The model is trained using labeled data to distinguish between genuine and morphed images.

Finally, the trained model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score. The system outputs a classification result indicating whether the input image is authentic or morphed.

4.EXISTING METHODS

Existing face morph detection methods can be broadly categorized into texture-based, feature-based, and deep learning-based approaches.

Texture-based methods analyze pixel-level inconsistencies introduced during the morphing process. Techniques such as Local Binary Patterns and Gray-Level Co-occurrence Matrix are widely used to capture texture variations. While these methods are computationally efficient, they may struggle with high-quality morphs.

Feature-based methods rely on geometric relationships between facial landmarks. These approaches detect irregularities in facial structure caused by blending multiple faces. Although effective in some cases, they may not capture subtle texture differences.

Differential methods compare a suspected image with a trusted live image of the same individual. This approach provides higher accuracy but requires additional data, making it less practical for standalone systems.

Deep learning-based methods have gained popularity due to their superior performance. CNNs and GAN-based models can automatically learn discriminative features from large datasets. However, these methods require significant computational resources and large amounts of training data.

Despite these advancements, existing methods face challenges such as poor generalization to unseen morphing techniques and sensitivity to image quality variations.

5. PROPOSED SYSTEM

The proposed system aims to overcome the limitations of existing methods by integrating multiple feature extraction techniques with a robust classification model. It combines both spatial and frequency domain analysis to capture a wide range of morphing artifacts.

The system utilizes advanced preprocessing techniques to enhance image quality and improve feature extraction. Facial landmarks are accurately detected to analyze geometric inconsistencies, while texture features are extracted using multi-scale analysis.

A hybrid deep learning model is employed to improve detection accuracy. The model combines convolutional layers for spatial feature extraction with attention mechanisms to focus on critical regions of the face. This enhances the model's ability to detect subtle morphing artifacts.

Additionally, the system incorporates error-level analysis to identify compression inconsistencies in morphed images. This approach improves robustness against high-quality morphs.

The proposed system is designed to generalize well across different datasets and morphing techniques. It provides a reliable and efficient solution for real-world biometric applications.

6. SCREENSHOTS

OUTPUT SCREENS:

Fig 6.1: Home Page

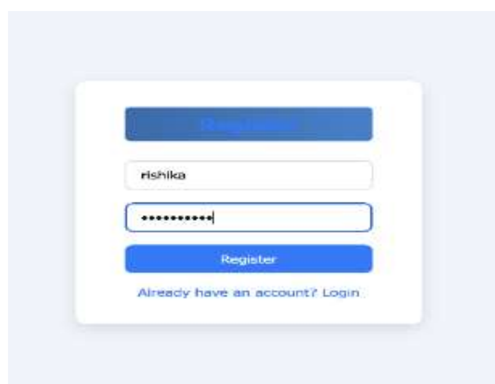


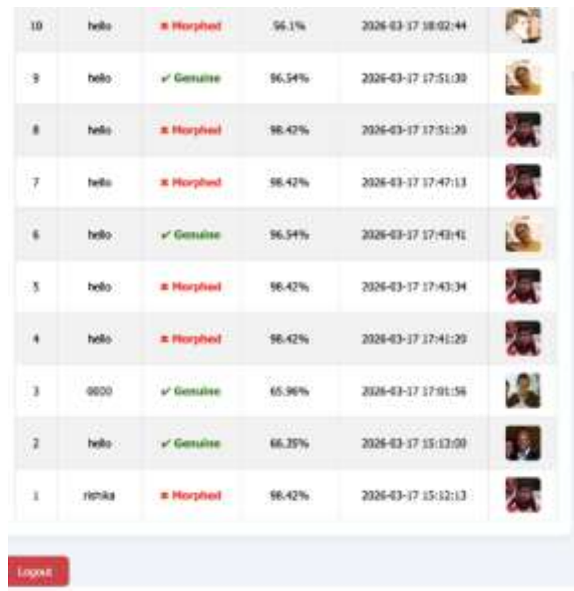
Fig 6.2 : Registration Page

Fig 6.3: Login Page

Fig 6.4: User Page

Fig 6.5: Morphed Image in user page

Fig 6.6: Admin Login



6.7: Admin DashBoard

6.8: Redirects to home page after logout

7. CONCLUSION

Face morphing attacks pose a significant threat to biometric authentication systems, particularly in high-security applications. The development of effective morph detection systems is essential to prevent identity fraud and enhance system reliability.

This project demonstrates the application of machine learning and image processing techniques in detecting morphed facial images. By combining multiple feature extraction methods and advanced classification models, the proposed system achieves improved accuracy and robustness.

The study highlights the importance of continuous research and innovation in biometric security to address emerging threats.

8. FUTURE SCOPE

Future research in face morph detection can focus on improving model generalization to handle unseen morphing techniques. Developing lightweight models for real-time applications is another important direction.

The integration of multimodal biometric systems, such as combining face recognition with fingerprint or iris recognition, can further enhance security. Additionally, the use of explainable AI can help understand model decisions and improve trust in detection systems.

Advancements in generative models also require continuous updates in detection techniques to stay ahead of evolving threats.

9. REFERENCE

1. Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2021). Face morphing attack generation and detection: A comprehensive survey. IEEE Transactions on Technology and Society.

2. Hamza, M., Tehsin, S., Humayun, M., Almufareh, M. F., & Alfayad, M. (2022). A comprehensive review of face morph generation and detection of fraudulent identities. Applied Sciences.

3. Nightingale, S. J., Agarwal, S., & Farid, H. (2021). Perceptual and computational detection of face morphing. Journal of Vision.

4. Saleem, I., & Shukr, B. K. (2018). Generating and detecting face morphing using texture techniques. Journal of Kufa for Mathematics and Computer.

5. Saleem, I., & Shukr, B. K. (2023). Techniques and challenges for

generation and detection face morphing attacks: A survey. Iraqi Journal of Science.

6. Zhang, Y., et al. (2024). Enhanced face morphing attack detection using error-level analysis and selective kernel networks. Computers & Security.

7. Scherhag, U., Rathgeb, C., Merkle, J., & Busch, C. (2019). Face recognition systems under morphing attacks: A survey. IEEE Access.

8. Ferrara, M., Franco, A., & Maltoni, D. (2018). Face demorphing. IEEE Transactions on Information Forensics and Security.

9. Sarkar, E., Korshunov, P., Colbois, L., & Marcel, S. (2020). Vulnerability analysis of face morphing attacks.

10. Ivanovska, M., & Štruc, V. (2023). Face morphing attack detection using diffusion models.