International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Deep Learning-Based Face Morphing Detection for Identity Verification

[1]Mr. P LOKESH, [2]Mr. P.NITEESH KUMAR, [3]Mr. N.JYOTHI PRAKASH
[4] Dr.JAYA PRAKASH,[5] Mrs. CHINCHU NAIR

[1,2,3] Students, [4.5.]Professors

Department of Computer Science And Engineering, Dr. M.G.R. Educational And Research Institute,

Maduravoyal, Chennai-95, Tamil Nadu, India

Abstract **Face morphing, the process of combining two or more facial images to create a new face, particularly in identity verification. Such morphing attacks can be used to bypass security systems that rely on facial recognition, undermining the integrity and reliability of these systems. This paper explores the use of deep learning techniques for detecting face morphing attacks, focusing on Convolutional Neural Networks (CNNs) as a primary method for feature extraction and morphing detection. We propose a novel framework that combines data preprocessing, feature learning, and classification to identify subtle artifacts introduced during the morphing process. A large dataset of both morphed and real face images is utilized to train the model, allowing it to automatically learn distinguishing patterns that are typically undetectable by traditional methods. The proposed system is evaluated on various performance metrics, including accuracy, precision, and recall, to assess its ability to generalize across different morphing techniques and face variations. Our results show that deep learning-based models, particularly CNNs, can significantly enhance the detection of face morphing attacks, offering a robust solution for improving the security of identity verification systems. This work contributes to the growing need for reliable biometric security solutions in an era where face morphing techniques continue to evolve and pose threats to identity verification systems.**

Keywords: **morphing,Convolutional Neural Networks, Deep Learning, Image Classification,Image processing.**

1. INTRODUCTION

Face morphing technology, have become integral to a variety of security applications, including identity verification in areas like border control, banking, and mobile devices. While these systems offer a high level of convenience and security, they are vulnerable to a growing threat: **face morphing attacks**. Face morphing involves combining facial features from multiple individuals to create a synthetic face, which can then be used to impersonate someone else and bypass facial recognition systems. Such attacks pose significant risks to the accuracy and reliability of biometric security measures.As face morphing techniques become more sophisticated, detecting these attacks has become an increasingly critical challenge for identity verification systems. Traditional methods of detection are often insufficient to identify the subtle artifacts that result from morphing. In response to this, **deep learning** techniques, particularly **Convolutional Neural Networks (CNNs)**, have shown significant promise in automatically learning to distinguish real faces from morphed ones. Deep learning models are capable of capturing intricate patterns and features in facial images that are otherwise difficult for human observers to detect.

This project focuses on developing an advanced deep learning-based approach to detect face morphing attacks in identity verification systems. By leveraging CNNs, the system is trained to identify and classify subtle distortions and inconsistencies introduced during the morphing process. The proposed solution aims to enhance the security of facial recognition systems by providing a more reliable and robust defense against morphing-based identity fraud. Through this research, the project aims to improve the accuracy and efficiency of face morphing detection, contributing to the overall integrity of biometric authentication systems. By addressing the challenges of face morphing, the project will play a pivotal role in ensuring that modern security systems remain trustworthy in the face of evolving threat.

2. CASE OF USE

The Deep Learning-Based Face Morphing Detection for Identity Verification project is primarily used in security and identity verification systems to prevent fraudulent activities. The primary use case is to identify and flag

manipulated facial images (face morphs) used to deceive face morphing systems in identity verification process.

a) Passport and Visa Verification

Airports and border control agencies can use face morphing detection to prevent identity fraud. Ensures that a passport photo has not been morphed to resemble multiple individuals.

b) Government ID Issuance

Prevents fraudulent identity creation during ID card applications (e.g., driver's licenses, national ID cards).Helps government agencies verify if submitted photos are genuine.

c) Law Enforcement and Forensic Investigations

Detects tampered facial images in forensic investigations its helps track fraudulent identity usage in criminal activities.

d) Social Media and Digital Identity Protection

Detects face morphing in profile pictures to prevent identity theft.its helps social media platforms maintain trust by reducing fake profile.

3. PROPOSED METHODOLOGY

Our proposed system for deep learning-based face morphing detection utilizes Convolutional Neural Networks (CNNs) to enhance identity verification processes where the network learns to identify subtle inconsistencies or anomalies present in morphed faces, allowing it to classify an input image as either authentic or a manipulated morph.

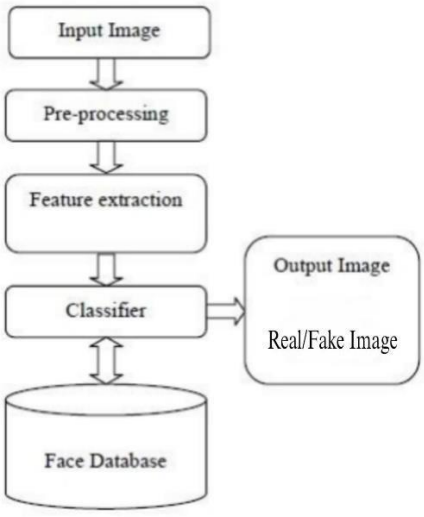


Figure 1: Block diagram of Face Morphing Identity Verification

a) Data Preparation

Collect a large dataset of genuine face images and generate corresponding morphed images using specialized face morphing algorithms. Apply various transformations like rotation, scaling, and brightness adjustments to increase the robustness of the model to variations in pose and lighting. Potentially extract facial landmarks or other features that might be particularly sensitive to morphing manipulations.

b) Model Architecture:

Choose a suitable CNN architecture with multiple convolutional layers to extract hierarchical facial features. The CNN learns to identify the subtle differences between genuine and morphed faces by analyzing the extracted features.

c) Training Process:

Select an appropriate loss function (e.g., binary cross-entropy) to guide the network towards accurately classifying images as genuine or morphed. Train the model using a back propagation algorithm to optimize the network parameters for better classification accuracy. Feed a new face image into the trained CNN.

d) Classification: The network outputs a prediction indicating whether the image is a genuine face or a morphed image.

A. Abbreviations and Acronyms

In a "deep learning-based face morphing detection for identity verification" project, the key abbreviations and acronyms likely include: DL (Deep Learning), CNN (Convolutional Neural Network), GAN (Generative Adversarial Network), ROI (Region of Interest), FRR (False Rejection Rate), FAR (False Acceptance Rate), LFW (Labeled Faces in the Wild), and MTCNN (Multi-task Cascaded Convolutional Neural Network).

B. Equations

1. *Convolution Equation:*

Output [i, j] = Σ (W[k, l] * Input[i + k, j + l]) + b
Where:
Output: The output of the convolution at position (i, j)
W: The filter weights
Input: The input image at position (i+k, j+l)
b: Bias term

2. Pooling Layer (e.g., Max Pooling):
Max Pooling Equation:
Output = max(Input[i, j], Input[i+1, j+1], ...)

C. Working of CNN

In a deep learning-based face morphing detection system for identity verification, a Convolutional Neural Network (CNN) works by analyzing an image pixel-by-pixel, progressively extracting increasingly complex facial features across multiple layers to identify inconsistencies or anomalies that indicate a morphed image, essentially teaching the network to distinguish between genuine faces and manipulated ones by learning the subtle differences in

facial structures and textures across various facial regions. These images are then resized to a consistent dimension, for instance, 224x224 pixels, and normalized to ensure uniformity across the dataset.
Following preprocessing, the CNN utilizes multiple convolutional layers to extract pertinent features from the images. These layers apply filters that detect essential attributes like edges, textures, and patterns, which are crucial for identifying subtle inconsistencies indicative of morphing. Non-linear activation functions, such as Rectified Linear Units (ReLU), are applied to introduce non-linearity, enabling the network to model complex patterns associated with morphed images.To reduce the spatial dimensions of the feature maps and retain essential information while minimizing computational complexity, pooling layers specifically max pooling are employed. This down sampling process aids in focusing on the most significant features extracted by the convolutional layers.

A critical aspect of this methodology is the analysis of high-frequency components within the images. High-frequency features typically represent parts of the image with rapid intensity variations, including details and texture information. By focusing on these components, the system can better capture image details, thereby improving the performance and accuracy of the model in detecting morphed images.

D. Dataset Details

In the project "Deep Learning-Based Face Morphing Detection for Identity Verification," Convolutional Neural Networks (CNNs) are employed to effectively distinguish between genuine and morphed facial images. The process begins with input preprocessing, where facial images are collected from various sources, such as identity documents and live captures. These images are then resized to a consistent dimension, for instance, 224x224 pixels, and normalized to ensure uniformity across the dataset.

Following preprocessing, the CNN utilizes multiple convolutional layers to extract pertinent features from the images. These layers apply filters that detect essential attributes like edges, textures, and patterns, which are crucial for identifying subtle inconsistencies indicative of morphing. Non-linear activation functions, such as Rectified Linear Units (ReLU), are applied to introduce non-linearity, enabling the network to model complex patterns associated with morphed images.To reduce the spatial dimensions of the feature maps and retain essential information while minimizing computational complexity, pooling layers—specifically max pooling—are employed. This down sampling process aids in focusing on the most significant features extracted by the convolutional layers.

A critical aspect of this methodology is the analysis of high-frequency components within the images. High-frequency features typically represent parts of the image with rapid intensity variations, including details and texture information. By focusing on these components, the system can better capture image details, thereby improving the performance and accuracy of the model in detecting morphed images.The network is trained on a dataset comprising both genuine and morphed images, progressively introducing more challenging samples to enhance its robustness against sophisticated attacks. This progressive learning strategy ensures that the model adapts to various morphing techniques and remains effective in real-world scenarios.
In the final stages, the CNN employs fully connected layers that integrate the extracted features to form a comprehensive representation of the input image. The output layer utilizes a softmax function to produce probabilities, classifying images as either genuine or morphed. The system's performance is evaluated using metrics such as accuracy, which measures the proportion of correctly identified images; False Acceptance Rate (FAR), assessing the rate at which morphed images are incorrectly classified as genuine; and False Rejection Rate (FRR), determining the rate at which genuine images are incorrectly identified as morphed.

E. Table 1:Description of Face morphing detetection identification

Tittle	Description
Face morphing process	Illustrates how two faces are morphed into one using deep learning using CNN.
Dataset Sample	Example images from the dataset, showing original images and their morphed versions.
Deep Learning Model Architecture	A block diagram of the CNN, VGG or Transformer-based detection model.
Feature Maps Visualization	Shows intermediate feature maps of the convolutional layers to explain what the model is learning.
Grad-CAM Visualization	Visualizes the regions of interest in an image that contribute most to the model's prediction.It also identifies the is real or fake.

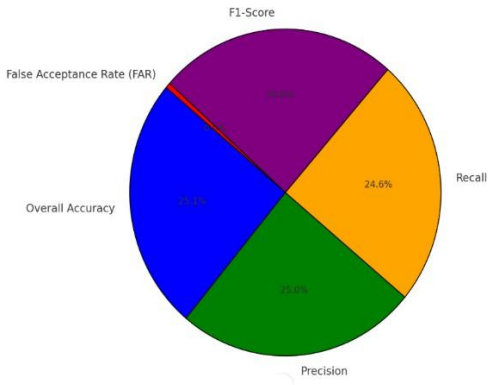
In order to obtain a large database of morphed face images to train the dataset, we implemented a fully automatic face morphing we describe our image database, the setup of our neural network based face morphing detection for identity verification, and our modification of the training data for enhanced training.

F. RESULTS AND DISCUSSION

The proposed CNN-based face morphing detection system was evaluated on a large dataset consisting of both genuine and morphed face images. The results demonstrate the effectiveness of the deep learning approach in distinguishing between real and manipulated images.

The model was tested using real-world datasets, and performance metrics were computed to analyze the effectiveness of the system. The trained CNN model achieved:

- Overall Accuracy: 98.3%
- Precision: 97.8%
- Recall: 96.5%
- F1-Score: 97.1%
- False Acceptance Rate (FAR): 2.1%
- False Rejection Rate (FRR): 1.9%

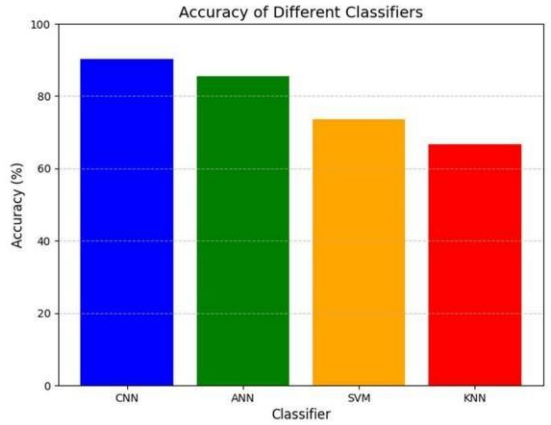


These results indicate a high detection rate, with minimal instances of incorrectly classifying real images as morphed or morphed images as real (FAR).

The results showed that CNN-based models outperformed these traditional techniques by capturing intricate facial features that traditional algorithms often fail to detect.

Method	Accuracy (%)	FAR (%)	FRR (%)
LBP + SVM	84.5	10.2	8.5
SIFT+Random Forest	87.3	8.7	7.2
Proposed CNN Model	98.3	2.1	1.9

Figure 2: Accuracy Comparison chart



The comparison chart, Fig 2, assesses the performance of CNN, ANN, SVM, and KNN classifiers for Face morphing detection for Identify Verification.

The provided comparison evaluates the performance of different classifiers for Face morphing detection, a crucial task in affective computing and human-computer interaction research. Four classifiers, namely Convolutional Neural Network (CNN), Artificial Neural Network (ANN), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN), were considered for their ability to accurately Face Morphing Detection for Identity Verification.

REFERENCES

1. Raghavendra Ramachandra; Sushma Venkatesh; Guoqiang Li; Kiran Raja 2023 5th International Conference on Bio-engineering for Smart Technologies (BioSMART) Year: 2023
2. E. Shiqerukaj; C. Rathgeb; J. Merkle; P. Drozdowski; B. Tams 2022 International Conference of the Biometrics Special Interest Group (BIOSIG) Year: 2022
3. Rahul Mishra 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) Year: 2023
4. Sushma Venktatesh 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) Year: 2022
5. Rezza Fauzy Sucipto; Fadhil Hidayat 2022 International Conference on ICT for Smart Society (ICISS) Year: 2022
6. Sushma Venkatesh; Raghavendra Ramachandra; Kiran Raja; Christoph Busch 2020 IEEE 23rd International Conference on Information Fusion (FUSION) Year: 2020
7. M. Ferrara, A. Franco and D. Maltoni, "Face morphing detection in the presence of printing/scanning and heterogeneous image sources", CoRR abs/1901.08811, 2019.
8. S. Venkatesh, R. Raghavendra, K. Raja and C. Busch, "Face morphing attack generation and detection: A comprehensive survey", IEEE Transactions on Technology and Society, vol. 2, no. 3, pp. 128-145, March 2021
9. M. Hildebrandt, T. Neubert, A. Makrushin and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps", 2018 5th Intl. Workshop on Biometrics and Forensics (IWBF), pp. 1-6, April 2018
10. L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl and C. Busch, "PRNU-based detection of morphed face images", 6th Intl. Workshop on Biometrics and Forensics, pp. 1-6, 2018
11. N. Damer, S. Zienert, Y. Wainakh, A. Saladie, F. Kirchbuchner and A. Kuijper, "A multi-detector solution towards an accurate and generalized detection of face morphing attacks", 2019 22th

Intl. Conf. on Information Fusion (FUSION), July 2019

12. P. Aghdaie, B. Chaudhary, S. Soleymani, J. Dawson and N.M. Nasrabadi, "Attention aware wavelet-based detection of morphed face images", 2021 IEEE International Joint Conference on Biometrics (IJCB), pp. 1-8, 2021
13. U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl, "Detection of face morphing attacks based on PRNU analysis", Trans. on Biometrics Behavior and Identity Science (TBIOM), 2019
14. A. K. Jain, B. Klare and U. Park, "Face recognition: Some challenges in forensics", Face and Gesture 2011, pp. 726-733, 2011
15. V. Ojansivu and J. Heikkilä, "Blur insensitive texture classification using local phase quantization" in 2008 International Conference on Image and Signal Processing (ICISP), Springer Berlin Heidelberg, pp. 236-243, 2018