Iraqi Journal for Computer Science and Mathematics

Volume 6 | Issue 1 Article 12

2025

Hybrid Methods for Detecting Face Morphing Attacks

Essa M. Namis
College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq,
ess22c1002@uoanbar.edu.iq

Khalid Shaker
College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq,
khalidalhity@gmail.com

Sufyan Al-Janabi
College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq,
sufyan.aljanabi@uoanbar.edu.iq

Recommended Citation

Namis, Essa M.; Shaker, Khalid; and Al-Janabi, Sufyan (2025) "Hybrid Methods for Detecting Face Morphing Attacks," *Iraqi Journal for Computer Science and Mathematics*: Vol. 6: Iss. 1, Article 12.
DOI: https://doi.org/10.52866/2788-7421.1242
Available at: https://ijcsm.researchcommons.org/ijcsm/vol6/iss1/12

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:158–168

ORIGINAL STUDY

Hybrid Methods for Detecting Face Morphing Attacks

Essa M. Namis *, **Khalid Shaker**, **Sufyan Al-Janabi**

College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq

ABSTRACT

The face morphing process blends two or more facial images to produce a singular morphed facial image that shows the vulnerabilities of Face Recognition Systems (FRS). The widespread use of facial recognition algorithms, especially in Automatic Border Control (ABC) systems, has elicited concerns about potential attacks, as modified passports pose a significant risk to national security. This research presents a hybrid approach for feature extraction from facial images. The suggested approach involves three stages: The initial phase involves preprocessing the image through resizing and face identification, using the Viola-Jones algorithm to detect and locate the human face in the image, regardless of its size, context, or environment. In the second step, we extract features using three different techniques: Transfer learning using ResNet50, Histogram of Oriented Gradients (HOG), and Local Binary Pattern (LBP); we produce a one-dimensional feature vector that merges the outputs of each technique. The third phase includes the classification process utilizing the Deep Neural Network (DNN) classifier and the Support Vector Machine (SVM) as a secondary classifier. The AMSL dataset that contains real face and morphed face images has been used for training and testing the proposed approach. The DNN classifier achieved an average accuracy of 98.62%, surpassing the SVM, which achieved an accuracy of 97.39%. The results demonstrate a higher accuracy in identifying morphing attacks relative to previous studies.

Keywords: Face recognition systems (FRSs), Morphing attacks, Deep learning, Face detection, ResNet50, Local binary pattern, Histogram of gradient

1. Introduction

Morphing approaches can generate artificial biometric samples that mimic the biometric data of two or more individuals in both image and feature domains. Introducing morphed biometric images into a biometric recognition system will correctly authenticate the individuals represented in the morphed image against the single-enrolled reference data. Therefore, we cannot justify the unique relationship between individuals and their biometric reference data [1]. Specifically, face recognition systems have demonstrated significant susceptibility to attacks utilizing altered facial images [2, 3]. This study aims to demonstrate feature extraction from images utilizing three types of descriptors. We utilize ResNet50 to extract high-level features that effectively capture complex patterns in facial structures, thereby enhancing the performance of facial recognition [4]. We also use HOG to draw attention to important facial features like the eyes, nose, and mouth by capturing gradient orientations [5]. Finally, we use LBP to look at the local texture of facial images, which lets us tell the difference between faces using micro-patterns [6]. Incorporate features to train both SVM and DNN classifiers to achieve optimal accuracy and minimal error without dependence on a comparison with a real-time image of a traveler. Fig. 1 illustrates a scenario of morphing two facial images.

Received 9 November 2024; revised 18 February 2025; accepted 21 February 2025.
Available online 27 March 2025

* Corresponding author.
E-mail address: ess22c1002@uoanbar.edu.iq (E. M. Namis).

https://doi.org/10.52866/2788-7421.1242

Fig. 1. Example for a morphed face image (b) of subject 1 (a) and subject 2 (c). The Morph was manually created using FantaMorph [7].

This research primarily contributes to the following topics:

1. During pre-processing, we have scaled the image size to reduce alterations or distortions, and we have used the Viola-Jones algorithm to find and separate facial areas accurately in real time. This makes preprocessing better for finding face morphing attacks and making sure accurate feature extraction happens.
2. We propose the use of three types of feature extraction methods: the transfer-learning-based ResNet50, the histogram of gradient (HOG), and the local binary pattern (LBP).
3. We have provided detailed results for the transfer-learning-based ResNet50, the histogram of gradients, and local binary patterns related to classifier performance using two different classifiers, SVM and DNNs.

This paper is organized as follows: Section 2 presents relevant literature on face morphing attack detection. Section 3 explains our proposed hybrid approaches for face-morphing attack detection system. Next, Section 4 presents the experimental results and discussion and compares them with the state-of-the-art methods. Finally, Section 5 provides a brief conclusion for the work.

2. Related work

This section presents pertinent studies related to this topic. Several studies employed texturing approaches, including binarized statistical image features, scale-invariant feature transforms (SIFT), and steerable pyramids, etc. In most studies employ pre-existing CNN models, such as VGGNet, AlexNet, and ResNet, for feature extraction. We explore some of them:

Tian Ma et al. [8] proposed and implemented two methods: neural networks and occlusion detection. Use them together, and the results are exceptional. They analyzed the proposed training methods that they trained with a pretrained network for better results regarding accuracy, generality, robustness, and their decision-making process. Even though his combined methods do not yield the highest general accuracy of the network, they make it more robust against different types of attacks. Using the proposed methods, they increased the robustness of the system against any form of attack with accuracy values up to 94%. **Venktatesh et al. [9]** propose a multi-level fusion of deep information to identify face morphing attacks in a single image. Deep convolutional neural networks like AlexNet and ResNet50 retrieve features. They use feature and score integration to determine if the facial image is a morph. To test the Single Image Morph Attack Detection (S-MAD) method, use a face-morphing dataset with three types of data and five production methods. Digital, re-digitized, and compressed print-scan are data media. They run detailed studies with intra- and inter-evaluation scenarios (the same and distinct data types for training and testing) and also compare the proposed method to state-of-the-art (SOTA) reference-based/single image morph attack detection (S-MAD) methods. The statistical research reveals the suggested strategy works better in all three mediums. The work of **Ramachandra et al. [10]** investigated feature extraction and classification of the eyes, mouth, and nose separately. This study collects rough and fine texture data from multimodal areas using BSIF and LBP. After separating the features using P-CRC and SRKDA, the study adds their scores at different levels to determine its final decisions. Their extensive studies on three datasets compare the proposed method's detection

performance to existing approaches. The recommended solution outperforms existing methods on all three datasets using distinct performance evaluation protocols. The findings demonstrate the framework's reliability for single image-based morph attack detection. **Singh et al. [11]** presented a novel approach to face-morphing attack generation and detection, particularly in three-dimensional situations. Their point cloud-based 3D face-morphing model construction method is new. The vulnerability research uses 2D and 3D facial recognition systems to evaluate the new 3D face-morphing attacks. They study human observers to determine the value of 3D information in morphological detection. The results show that the 3D face morphing models are susceptible. They also automatically assess the quality of 3D morphing models, which match actual 3D scans. To identify 3D morphing attacks using pretrained point-based CNN models, this paper offers three 3D MAD approaches. Comprehensive research shows that 3D MAD algorithms can detect 3D face morphing attacks. **Tapia et al. [12]** present and examine a single Morphing attack detection (SMAD) approach for morphed facial images, which are generated from varying numbers of participants. We selected facial photos from K subjects and their associates to generate morphing face images for K = 2, 4, 8, and 16 individuals. Images that undergo morphing with additional contributors manifest as obscured faces. They used MobileNetV3 to build a multiclass Convolutional Neural Network (CNN) called AlphaNet. They then added three levels of alpha filters to the RGB channels and tested AlphaNet both within and between datasets. They also tested the technique on fake pictures and got a BPCER10 of 4.41% and a BPCER20 of 4.56% in cross-dataset testing. **Jia et al. [13]** proposed a novel detection framework that utilizes high-frequency characteristics and an advanced two-branch network architecture. The method utilized both the RGB stream and the high-frequency information stream to detect morphing faces simultaneously, and enhanced the interaction between the two streams through the use of SEM and IEM. We validated the method's efficacy and generalizability on the HNU and FEI datasets. In the FEI dataset, the TSCNN achieved an ACER of 0.67%, an EER of 0.32%, and an ACC of 98.93%. In the HNU (MDB1) dataset, the ACER was 1.95%, the EER was 0.88%, and the ACC was 98.26%. In both datasets, the two-branch network outperformed the single-branch network. **Iman et al. [14]** presents an improved facial feature extraction method. The suggested method comprises four phases: generating morph images from real-life images using automatic selection landmarks, StyleGAN, and manual selection landmarks. They trust StyleGAN for optimum, artifact-free photos. A Faster Region The second phase employs a convolutional neural network to cut face landmarks (eyes, nose, mouth, and skin) while preserving hair, ears, and the image background for each database image. The third phase extracts features using PCA, eigenvalue, and eigenvector methods to create a two-dimensional matrix with one layer per method. Create a three-layer image from each image's extracted characteristics (without S). Layers describe principal component analysis, eigenvalue, and eigenvector features. Finally, optimize convolutional neural networks by inserting features. DNN and SVM second classifiers classify in the fourth phase. The DNN classifier averaged 99.02% accuracy versus SVM's 98.64%. The FRA and RFF evaluations demonstrate the proposed work's strength. This reduced DNN (FAR 0.018, FRR 0.003) and SVM (FAR 0.023, FRR 0.06) error rates. These ratios, below one, improve detection accuracy. DNN had 95.8% accuracy, FAR 0.039, FRR 0%, and SVM 95.2% accuracy, FAR 0.047, FRR 0.98 on the AMSL dataset.

Singh et al. [15] proposed an S-MAD architecture that can spot face-morphing attacks by using a number of attributes, classifiers, and comparison scores at different levels. Human post-processing creates artifact-free face-morphing photographs in our new dataset. The collection includes digital, print-scan (PS-1 re-digitized by DNP and PS-2 by CANON), and compression photos. They extensively tested the suggested strategy using two evaluation methods to compare it to existing methods. In two evaluation protocols, the new strategy outperforms existing methods.

Ibsen et al. [16] proposed a new framework and loss function to enhance the resilience of deep learning-based facial recognition systems against morphing attacks. They improved a neural network structure that uses a special TetraLoss function to tell the difference between topic embeddings and morphing attack embeddings in morphed data. Results indicate that the suggested strategy can improve the performance of state-of-the-art face recognition systems against morphing attacks while maintaining excellent performance. At FMR = 0.1%, two distinct backbone architectures enhance RIAPAR by at least 45%, ensuring operational relevance for ArcFace, MagFace, and AdaFace. **Ramesh et al. [17]** proposed a deep convolutional neural network-based morphing attack detection approach. Training and testing components of their image-morphing process were interchangeable. Due to compression and anti-forensic measures, the networks used semantic artifact-focused data. They scaled, rotated, and cropped the images before feeding them into

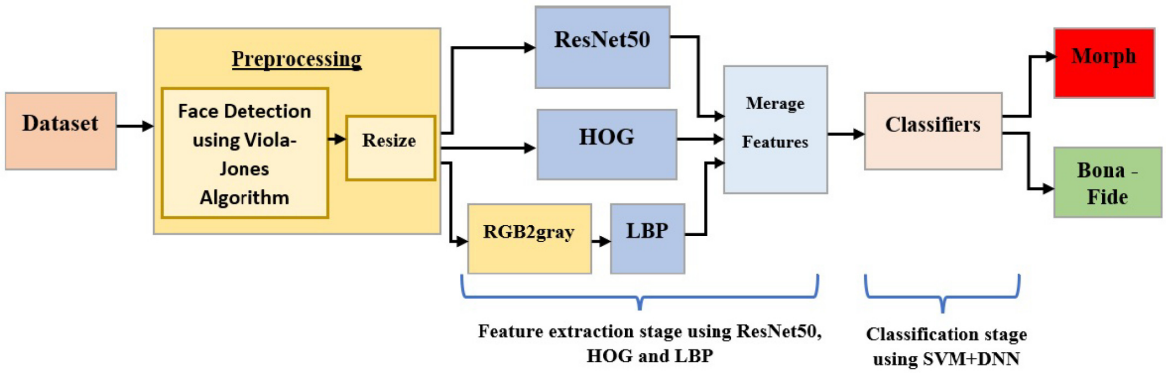

Fig. 2. The design of the proposed face morphing attack detection system.

traditional manipulation traces. They also added noise and blur to the training and test data sets and trained three convolutional neural network architectures from pretrained networks. The trained networks' FRR ranges from 3.5% to 16.2% and FAR from 0.8% to 2.2%. The VGG19 The trained model has the best FRR and FAR, 3.5% and 0.8%, respectively. **Senthil et al. [**18**]** suggested approach, utilizing CNN (Convolutional Neural Network), safeguards individual privacy and data. It distinguishes between an artificially generated character and a real human in the image. This ensures that only authorized individuals can access their information. Industries like security, law enforcement, financial services, education, government services, and retail utilize facial recognition technologies. If unauthorized individuals access the aforementioned sections, the outcome will be perilous. The efficacy of the suggested system is evaluated by accuracy, precision, and sensitivity. Experimental results demonstrate that the CNN-based facial recognition system excels.

To reduce the computational cost, we have used three types of feature extracts in our proposed approach: a deep learning technique based on transfer learning, HOG, and LBP. We fuse the extracted features to train SVM and DNN classifiers for the detection of real and morphed face images.

3. The proposed approach

This section discusses the details of the presented model, which has three steps. The first step is the preprocessing stage. The second stage utilizes ResNet50, HOG, and LBP for feature extraction, while the final stage involves classification utilizing DNN and SVM classifiers. Fig. 2 illustrates the architecture of the proposed method. The primary objectives of our technique are to enhance accuracy while minimizing the model's training duration. The subsequent subsections contain an explanation of each stage.

3.1. The preprocessing stage

Most feature extractors require prior preprocessing of the facial image. The efficacy of feature extractors depends upon the resolution of the analyzed image [19]. Image preprocessing involves converting unprocessed image data into a usable and meaningful format. It facilitates the elimination of unwanted distortions and the enhancement of essential characteristics for computer vision applications [20]. Fig. 3 shows the preprocessing stage. Our approach involves performing the following actions:

1. **Resizing:** Standardizing image dimensions is essential for the optimal performance of machine learning algorithms. We chose the size 224*224*3 so that all images are identical and to fit the size required by the pre-trained networks (ResNet50).
2. **Face detection using Viola Jones algorithm:** Face detection is a fundamental and significant task within the domain of computer vision. Face identification and detection in images and video streams provide the basis of numerous applications, including facial recognition systems and digital image processing [21]. Among the other algorithms created to address this challenge, the viola jones algorithm face detection has emerged as a revolutionary method known for its rapidity and precision [22]. Fig. 4 show an example of face detection using Viola-Jones algorithm.

In the following sections, we will examine the four primary steps of the Viola-Jones algorithm [23].

1. **Selecting Haar-like features:** Haar-like features are utilized in digital image processing

Fig. 3. Preprocessing stage.

Fig. 4. Fece detection utilizing Viola-Jones algorithm.

for object recognition. All human faces exhibit certain common features, such as the eye region being darker than adjacent pixels and the nose region being brighter than the eye region. There are three types of Haar-like features that Viola and Jones identified in their research: edge features, line features, and four-sided features.

2. **Creating an integral image:** An integral image refers to both a data structure and the algorithm employed to generate it. It serves as a rapid and effective method for computing the aggregate of pixel values in an image.
3. **Running AdaBoost training:** By providing training data, a machine learning algorithm trains AdaBoost to identify significant features, enabling it to learn and make predictions based on that knowledge. The method establishes a minimum threshold for evaluating the classification of a feature as beneficial or not.
4. **Creating classifier cascades:** Maybe the AdaBoost will finally select the best features around say 2500, but it is still a time-consuming process to calculate these features for each region. We have a 24 × 24 window in which we slide over the input image, and we need to find if any of those regions contain the face. The job of the cascade is to quickly discard non-faces and avoid wasting precious time and computations. This process ensures the speed required for instantaneous face identification.

3.2. Feature extraction and features fusion

In this work, we utilize three types of descriptors and integrate them, which we will discuss in details.

3.2.1. Feature extraction

The feature extraction step uses three types of descriptors: ResNet50, which has 2048 features per image; Histogram of Gradient (HOG), which has 1296 features per image;and Local BinaryPattern (LBP), which has 882 features per image. Fig. 5 illustrates the feature extraction stage.

A. **ResNET50:** Transfer learning is a technique when a model developed for one task is employed as the basis for a model addressing a different difficulty. The objective is to transfer the weights acquired by a network from the first task to a new second task. The learning process begins with patterns identified during the execution of a task related to the subject being

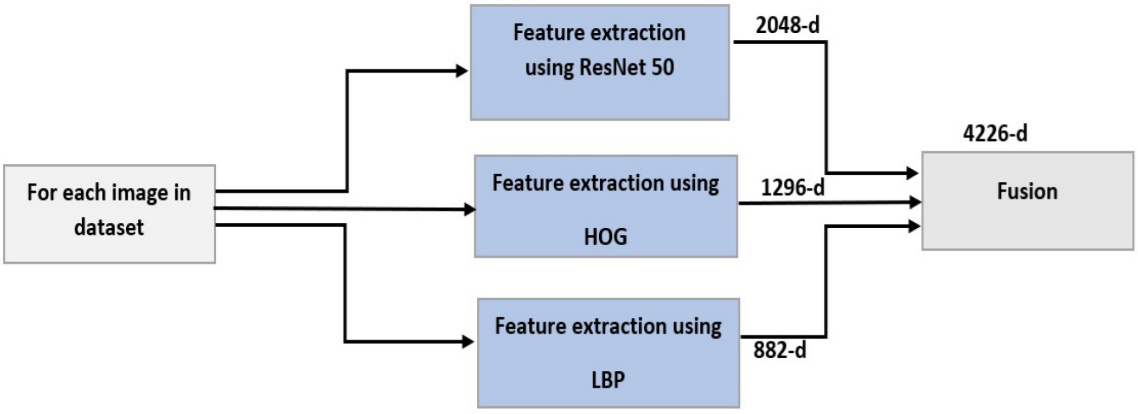

Fig. 5. Feature extraction using multi-techniques.

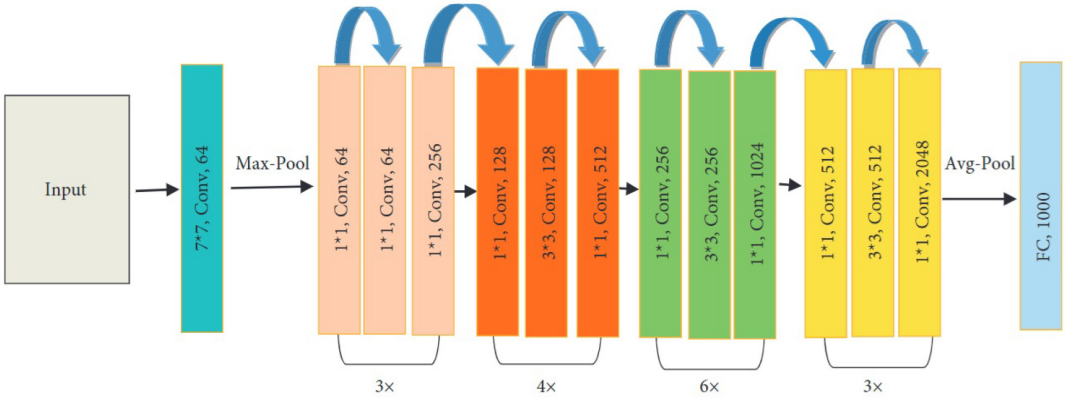

Fig. 6. ResNet-50 architecture [25].

studied rather than starting anew. Applications that require substantial computational resources, like computer vision, natural language processing, and image classification, predominantly employ transfer learning.

We suggested a pre-trained deep residual network, ResNet-50, for the extraction of image features.ResNet-50, a deep residual network that emerged victorious in the ImageNet competition 2015. The "50" indicates the number of layers it possesses. The primary innovation of ResNet, and the principal justification for proposing this model over other pre-trained models, is the skip connection. The skip connection allows input shortcuts to bypass the other weight layers inside the block. By transmitting the shortcut input without multiplying it by a layer's weight matrix, this attribute reduces the computational expense [24]. Fig. 6 illustrates the ResNet-50 architecture.

The present work used the ResNet 50 model for feature extraction, as shown in Fig. 2. Using these steps:

1. To obtain outputs for 1000 distinct classes, remove the fully connected layers from the pre-trained ResNet-50 model, trained on the AMSL dataset.
2. Restrict the remaining layers of ResNet-50 to function solely as a feature extractor for the new dataset.

B. **Histogram of Gradient:** Numerous techniques in computer vision are developed to extract spatial features for object identification by utilizing information regarding image gradients [26]. HOG, or Histogram of Oriented Gradients, is one such algorithm. A histogram is an approximate representation of the distribution of numerical data resembling a bar graph. Each bar signifies a collection of data that resides inside a specific range of values, referred to as bins. Orientation refers to the direction of an image gradient. HOG will generate a histogram of gradient orientations in an image. To classify the output into two categories in this feature extraction descriptor, we retrieve a 1296-dimensional vector from the new

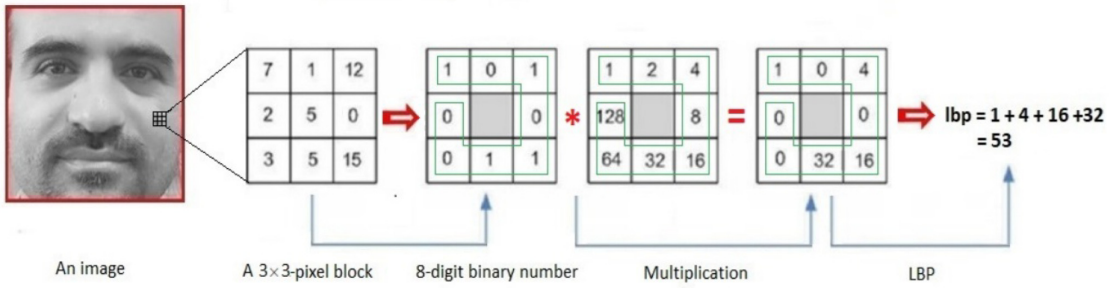

Fig. 7. Computing techniques for LBP values. Each 3 × 3 pixel block in the image is represented by an LBP value [29].

dataset, which includes both real and morphed samples.

We implement the HOG technique using the following steps [27]:

i. Compute the magnitude and direction of the gradients for each pixel in the input image.
ii. Segment the image into uniformly sized cells. The size of the cells is an optional feature. You must select the dimensions to ensure that the features align with the cell's scale.
iii. Categorize the gradient orientations of all pixels within each cell into a predetermined number of orientation bins. Total slope magnitudes in each bin represent bin heights.
iv. Organize the cells into uniformly sized blocks. Stride refers to the extent of the block window's displacement across the image.
v. Normalize the cell histogram with relation to the other cells inside the block. All normalized histograms from the blocks will be aggregated into a single feature vector. The feature vector is referred to as the HOG descriptor.

C. **Local Binary Patterns (LBP)**: Local Binary Pattern (LBP) is a widely utilized texture descriptor in the field of computer vision. It functions on images by assigning a binary code to each pixel through comparisons with adjacent pixels. To implement LBP, we segment a picture into multiple local regions and successively retrieve LBP features from these regions. We subsequently concatenate the LBP features to generate a comprehensive description of the image. As illustrated in Fig. 7, LBP generally functions on 3 × 3 pixel blocks, wherein the disparity between the central pixel and its eight neighboring pixels is utilized as the local texture feature representation [28].

We convert the images in the AMSL dataset from RGB to gray and retrieve an 882-dimensional vector from the dataset, which includes both real and morphed images.

3.2.2. Features fusion

We have extracted 2048-d features from the Deep Residual Features, 1296-d features from the Histogram of Gradient (HOG) descriptor, and 882-d features from the Local Binary Pattern (LBP) descriptor from the AMSL dataset, which contains real and morph images, respectively. We fuse all these features, resulting in a total of 4226-d features, that we utilize for training SVM and DNN classifiers for the classification of real and morph images.

3.3. Classification

The ending step of the suggested model is classification, utilizing two classifiers: SVM and DNN. The machine learning algorithm Support Vector Machine (SVM) categorizes both linear and nonlinear data with great efficiency, particularly in binary classifications [30]. DNN denotes deep neural networks, which are components of CNN [31]. Both of them classify effectively by training the network using weights to minimize the error between the output and the desired class.

4. Experimental results and discussion

This section explains the accuracy, robustness, and variety achieved by our multiple training tables, in addition to the insights derived from both types of machine learning and deep learning. We also examined the biometric quality of the modified images of faces. The following metrics evaluated the efficacy of the proposed model in identifying morphing faces: Accuracy (ACC), False Acceptance Rate (FAR), and False Rejection Rate (FRR) [32, 33]. Eqs. (1) to (3)

Fig. 8. Sample from AMSL dataset.

Table 1. AMSL Dataset without augmentation.

Class of AMSL dataset	Number of images
Real	201
Morph	2000

Table 2. AMSL Dataset with augmentation.

Class of AMSL dataset	Number of images
Real	1030
Morph	2000

describe the evaluation metrics:

$$ACC = (TP + TN) / (TP + TN + FP + FN) * 100 \quad (1)$$

$$FPR = FP/ (FP + TN) \quad (2)$$

$$FNR = FN/ (FN + TP) \quad (3)$$

We trained the proposed model using the AMSL dataset. The AMSL dataset contains real images of 201 persons from the Face Research Lab London collection and 2000 morph images, as detailed in Tables 1 and 2. AMSL was chosen because it has a higher quality morphing process, a wider range of subjects, and a controlled environment. This makes it a reliable standard for testing morphing attack detection methods. This dataset makes sure that the simulations of real attacks are accurate and provides a solid foundation for testing and training detection methods. Fig. 8 illustrates a sample from the AMSL dataset.

The results illustrate the use of various feature extraction methods, including Resnet50, HOG, and LBP, utilized both separately and in conjunction. Finally, we merged these techniques in order to train support vector machine (SVM) and deep neural network (DNN) classifiers for the classification of real and morph images Table 3. We evaluate the accuracy utilizing ResNet50 (with 2048 features). The DNN classifier obtains an accuracy of 95.55%, a FPR of 0.060, and a FNR of 0.020. The SVM classifier achieves an accuracy of 93.51, a FPR of 0.104, and an FNR of 0.018. Table 4 shows the accuracy of the LBP, which contains 1296 features. The DNN classifier achieves an accuracy of 95.71%, a FPR of 0.070, and a FNR of 0.005. The SVM classifier achieves an accuracy of 95.45%, an FPR of 0.070, and an FNR of 0.009. Table 5 illustrates the accuracy of the HOG classifier, which utilizes 882 features. The DNN classifier achieves an accuracy of 82.65, a FPR of 0.223, and a FNR of 0.100. The SVM classifier achieves an accuracy of 89.199, a FPR of 0.143, and a FNR of 0.064.

Table 6 shows the accuracy using ResNet50 and HOG(total features 2930). With the DNN classifier, the accuracy is 96.26, the FPR is 0.030, and the FNR is 0.015. With the SVM classifier, the accuracy is 96, the FPR is 0.040, and the FNR is 0.022. Table 7 shows the accuracy using ResNet50 and LBP(total features

Table 3. Performance metrics with ResNet50.

Model	Accuracy	FPR	FNR
DNN	95.55	0.060	0.025
SVM	93.51	0.104	0.018

Table 4. Performance metrics with LBP.

Model	Accuracy	FPR	FNR
DNN	95.71	0.070	0.005
SVM	95.45	0.070	0.009

Table 5. Performance metrics with HOG.

Model	Accuracy	FPR	FNR
DNN	82.65	0.223	0.100
SVM	89.199	0.143	0.009

Table 6. Performance metrics with ResNet50 and HOG.

Model	Accuracy	FPR	FNR
DNN	96.26	0.030	0.015
SVM	96	0.040	0.022

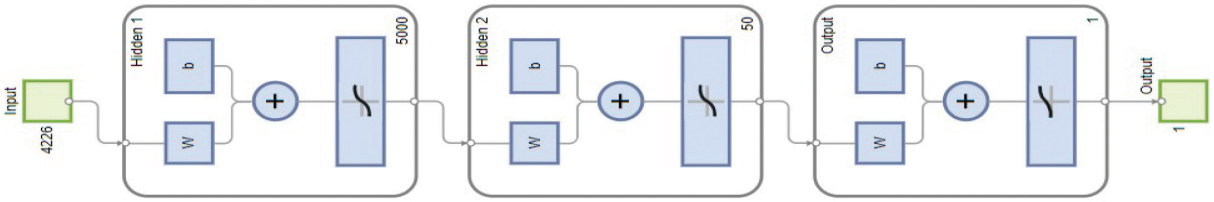

Fig. 9. Architecture of deep neural network classifier.

Table 7. Performance metrics with ResNet50 and LBP.

Model	Accuracy	FPR	FNR
DNN	96.33	0.031	0.019
SVM	96.15	0.042	0.022

Table 8. Performance metrics with HOG and LBP.

Model	Accuracy	FPR	FNR
DNN	93.83	0.101	0.011
SVM	92.96	0.030	0.020

Table 9. Performance metrics with ResNet50, HOG and LBP.

Model	Accuracy	FPR	FNR
DNN	98.62	0.030	0.001
SVM	97.39	0.045	0.003

3344). With the DNN classifier, the accuracy is 96.33, the FPR is 0.031, and the FNR is 0.019. With the SVM classifier, the accuracy is 96.15, the FPR is 0.042, and the FNR is 0.022. Table 8 shows the accuracy obtained using LBP and HOG(total features 2178). With the DNN classifier, the accuracy is 93.83, the FPR is 0.101, and the FNR is 0.011. With the SVM classifier, the accuracy is 92.96, the FPR is 0.030, and the FNR is 0.020.

Table 9 shows the accuracy using combined features Resnet50, HOG, and LBP (total features 4226). With the DNN classifier, the accuracy is 98.62, the FPR is 0.030, and the FNR is 0.001. With the SVM classifier, the accuracy is 97.39, the FPR is 0.045, and the FNR is 0.003.

As shown in Fig. 9, the DNN classifier sends each image's 4226 features to a three-layer feed-forward network. This network has two sigmoid hidden layers with 5000 and 50 neurons each, as well as softmax output neurons that guess between two outputs: real or morph. The network undergoes training using scaled conjugate gradient back propagation. We calculated the network's performance using cross-entropy and found that minimizing cross-entropy leads to excellent classification. Table 9 shows a comparison of the performance of SVM against the DNN classifier; results show that DNN outperforms SVM in accuracy. Table 9 demonstrates that the combined feature techniques (Resnet50, HOG, and LPB) achieved the highest accuracy when compared to other techniques, as shown through Tables 3 to 8.

Table 10. Our model's accuracy compared to other CNN models.

Model	Accuracy	FPR	FNR
Hosny et al. [34]	94.65	0.095	0.033
Rangarajan et al. [35]	95.12	0.088	0.072
Rangarajan et al. [35]	94.20	0.230	0.041
Li et al. [36]	93.11	0.114	0.243
Li et al. [36]	95.5	0.075	0.099
Iman et al. [14]	95.8 0	0.039	0
Our Proposed Approach	98.62	0.030	0.001

We compared the proposed work with a set of ready-made CNN models, as shown in Table 10. These results clearly demonstrate that our proposed approach outperformed the state-of-the-art methods in accuracy.

5. Conclusion

This study aims to distinguish morphing attack images from real images by employing a structured preprocessing, feature extraction, and classification approach. First, face detection is performed using the Viola-Jones algorithm, followed by image resizing to ensure uniformity. Feature extraction is conducted through three distinct methods: (i) deep learning-based transfer learning using ResNet50, (ii) Histogram of Oriented Gradients (HOG) for capturing shape-based features, and (iii) Local Binary Patterns (LBP) for extracting texture-based features. These methods are combined to enhance feature representation while reducing computational cost. For classification, Deep Neural Networks (DNN) and Support Vector Machines (SVM) are utilized. The proposed model is evaluated on the AMSL dataset, which presents a challenging scenario due to the minimal differences between real and morphed images, creating a strong electronic illusion. Despite these challenges, the fusion of ResNet50, HOG, and LBP features achieves high detection accuracy. The DNN classifier achieves an accuracy of 98.62%, a False Positive Rate (FPR) of 0.030, and a False Negative Rate (FNR) of 0.001, while the SVM classifier achieves an accuracy of 97.39%, an FPR of 0.045, and an FNR of 0.003. Experimental results demonstrate

that the fused feature extraction approach significantly improves classification performance compared to individual methods. Moreover, the proposed model outperforms previously published approaches, including VGG and AlexNet, in terms of accuracy. For future work, we plan to incorporate a feature selection method to identify and retain the most significant features while removing redundant and less informative ones.

Authors contribution

As a testament to the cooperative environment, every author made equally significant contributions. The researchers carefully designed and implemented the study framework, followed by a thorough analysis of the data and integration of their findings into a cohesive report. Their smooth cooperation and combined expertise propelled every phase of our undertaking, solidifying this effort as a genuine tribute to our shared dedication.

Funding

There was no outside funding for the research that led to the writing or publishing of this article.

Conflict of interest

None.

References

1. R. A. Aljanabi, Z. Al-Qaysi, M. Ahmed, and M. M. Salih, "Hybrid model for motor imagery biometric identification," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, pp. 1–12, 2024.
2. E. M. Namis, K. S. Jasim, and S. Al-Janabi, "Face morphing attacks detection approaches: A review," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 82–101, 2024.
3. Y. L. Khaleel, M. A. Habeeb, and H. Alnabulsi, "Adversarial attacks in machine learning: Key insights and defense approaches," *Applied Data Science and Analysis*, vol. 2024, pp. 121–147, 2024.
4. S. Borade, N. Jain, B. Patel, V. Kumar, M. Godhrawala, S. Kolaskar, et al., "ResNet50 DeepFake detector: Unmasking reality," *Indian Journal of Science and Technology*, vol. 17, pp. 1263–1271, 2024.
5. U. Scherhag, C. Rathgeb, and C. Busch, "Face morphing attack detection methods," In *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*, ed: Springer International Publishing Cham, pp. 331–349, 2022.
6. A. Makandar and S. B. Javeriya, "Enhancing aadhar card image security with machine learning-based face morphing detection," In *2024 1st International Conference on Communications and Computer Science (InCCCS)*, pp. 1–6, 2024.
7. 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.
8. T. Ma, A. Bamweyana, M. Guo, and K. Benon, "A face morph detection method based on convolutional neural networks and occlusion test," In *2022 7th International Conference on Image, Vision and Computing (ICIVC)*, pp. 158–165, 2022.
9. S. Venktatesh, "Multilevel fusion of deep features for face morphing attack detection," In *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1–7, 2022.
10. R. Raghavendra and G. Li, "Multimodality for reliable single image based face morphing attack detection," *IEEE Access*, vol. 10, pp. 82418–82433, 2022.
11. J. M. Singh and R. Ramachandra, "3d face morphing attacks: Generation, vulnerability and detection," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2023.
12. J. Tapia and C. Busch, "AlphaNet: Single morphing attack detection using multiple contributors," In *2023 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, 2023.
13. C.-k. Jia, Y.-c. Liu, and Y.-l. Chen, "Face morphing attack detection based on high-frequency features and progressive enhancement learning," *Frontiers in Neurorobotics*, vol. 17, p. 1182375, 2023.
14. I. S. Razaq, "Improved face morphing attack detection method using PCA and convolutional neural network," *Karbala International Journal of Modern Science*, vol. 9, p. 15, 2023.
15. J. M. Singh, S. Venkatesh, and R. Ramachandra, "Robust face morphing attack detection using fusion of multiple features and classification techniques," In *2023 26th International Conference on Information Fusion (FUSION)*, pp. 1–8, 2023.
16. M. Ibsen, L. J. González-Soler, C. Rathgeb, and C. Busch, "TetraLoss: Improving the robustness of face recognition against morphing attacks," *arXiv preprint arXiv:2401.11598*, 2024.
17. M. A. Ramesh, B. S. Lakshmi, D. Narendar, M. M. Najeeb, and V. Sai, "Detection of face morphing using deep learning," *International Journal of Progressive Research in Engineering Management and Science (IJPREMS)*, vol. 4, pp. 930–942, 2024.
18. S. S. Pandi, M. Monesh, and B. Lingesh, "A novel approach to detect face fraud detection using artificial intelligence," In *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, pp. 1–6, 2024.
19. A. Alsajri, A. Steiti, and H. A. Salman, "Enhancing IoT security to leveraging ML for DDoS attack prevention in distributed network routing," *Babylonian Journal of Internet of Things*, vol. 2023, pp. 74–84, 2023.
20. M. Ivanovska, A. Kronovšek, P. Peer, V. Štruc, and B. Batagelj, "Face morphing attack detection using privacy-aware training data," *arXiv preprint arXiv:2207.00899*, 2022.
21. P. William, A. Shrivastava, N. Shunmuga Karpagam, T. Mohanaprakash, K. Tongkachok, and K. Kumar, "Crime analysis using computer vision approach with machine learning," In *Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022*, ed: Springer, pp. 297–315, 2023.
22. A. S. Lateef and M. Y. Kamil, "Facial recognition technology-based attendance management system application in smart classroom," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, pp. 136–158, 2023.
23. G. S. Prasanna, K. Pavani, and M. K. Singh, "Spliced images detection by using viola-jones algorithms method," *Materials Today: Proceedings*, vol. 51, pp. 924–927, 2022.

24. Z. Zhu, K. Lin, A. K. Jain, and J. Zhou, "Transfer learning in deep reinforcement learning: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023.
25. R. Jha, V. Bhattacharjee, and A. Mustafi, "Transfer learning with feature extraction modules for improved classifier performance on medical image data," *Scientific Programming*, vol. 2022, p. 4983174, 2022.
26. M. Chandrakala and P. D. Devi, "Two-stage classifier for face recognition using HOG features," *Materials Today: Proceedings*, vol. 47, pp. 5771–5775, 2021.
27. N. Ipe, "A comparison of PCA and HOG for feature extraction and classification of human faces," *Authorea Preprints*, 2023.
28. S. Karanwal, "Robust local binary pattern for face recognition in different challenges," *Multimedia Tools and Applications*, vol. 81, pp. 29405–29421, 2022.
29. Z. Sedaghatjoo, H. Hosseinzadeh, and B. S. Bigham, "Local binary pattern (LBP) optimization for feature extraction," *arXiv preprint arXiv:2407.18665*, 2024.
30. S. Devi, P. Maury, and U. N. Tripathi, "A novel method of using machine learning techniques to protect clouds against distributed denial of service (DDoS) attacks," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 133–141, 2024.
31. J. Ayad, "Survey on neural networks in networking: Applications and advancements," *Babylonian Journal of Networking*, vol. 2024, pp. 135–147, 2024.
32. X. Liang, Z. Zhang, and R. Xu, "Multi-task deep cross-attention networks for far-field speaker verification and keyword spotting," *Eurasip Journal on Audio, Speech, and Music Processing*, vol. 2023, p. 28, 2023.
33. R. A. M. San Ahmed, "Hard voting approach using SVM, naïve bays and decision tree for kurdish fake news detection," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, pp. 25–33, 2023.
34. K. M. Hosny, M. A. Kassem, and M. M. Fouad, "Classification of skin lesions into seven classes using transfer learning with AlexNet," *Journal of Digital Imaging*, vol. 33, pp. 1325–1334, 2020.
35. A. Krishnaswamy Rangarajan and R. Purushothaman, "Disease classification in eggplant using pre-trained VGG16 and MSVM," *Scientific Reports*, vol. 10, p. 2322, 2020.
36. B. Li and D. Lima, "Facial expression recognition via ResNet-50," *International Journal of Cognitive Computing in Engineering*, vol. 2, pp. 57–64, 2021.