Karbala International Journal of Modern Science

Volume 9 | Issue 2 Article 15

Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network

Iman S. Razaq
Department of Computer Science, College of Computer Science and Mathematics, University of Kufa, Najaf, Iraq,
imans.alrihbawy@student.uokufa.edu.iq

Baheja k. Shukur
College of Computer Science & Information Technology, University of Kerbala, Kerbala, Iraq

Recommended Citation

Razaq, Iman S. and Shukur, Baheja k. (2023) "Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network," *Karbala International Journal of Modern Science*: Vol. 9 : Iss. 2 , Article 15.
Available at: https://doi.org/10.33640/2405-609X.3298

Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network

Abstract

Face recognition is the most extensively utilized security and public safety verification method. In many nations, the Automatic Border Control system uses face recognition to confirm the identification of travelers The ABC system is vulnerable to face morphing attacks; the face recognition systems give acceptance for the traveller, even though the passport photo does not represent the actual image of the person but is a result of the merger of two images. Therefore, it is vital to determine whether the passport image is altering (morph) or actual. This research proposes an improved method to extract features from facial images. The proposed method consists of four phases: In the first stage, morph images were generated using a set of databases of images of real people, used every two images that were similar in general shape or landmarks in producing the morphed image using three types of techniques used in this field (Automatic selection landmark, StyleGAN, and Manual selection landmark). StyleGAN has been relied upon to achieve the best results in producing artefact-free images. In the second phase, a Faster Region Convolution neural network is utilizing for determining and cutting important landmarks area (eyes, nose, mouth, and skin) in the face, where we leave the hair, ears, and image background for every image in the database. In the third phase, the features are extracted using three techniques Principal component analysis, eigenvalue, and eigenvector; a matrix of two-dimensional features is generated with one layer for each technique. Then merge the extracted features (with out s) from each image into one image with three layers. The first layer represents the principal component analysis features, the second the eigenvalue features, and the third the eigenvector features. Finally, the features are introduced into the convolutional neural networks to obtain optimal features. The fourth phase represents the classification process using the Deep Neural Network (DNN) classifier and Support Vector Machine (SVM) second classifier. The DNN classifier achieved an average accuracy of 99.02% compared with SVM, with an accuracy of 98.64%. The power of the proposed work is evident through the FRA and RFF evaluation. Which achieved values as low as possible for DNN FAR 0.018, indicating the error rate in calculating morphed images is actual, and FRR 0.003, meaning the error rate in calculating the actual images is morphed, FAR 0.023, FRR 0.06 for SVM whenever these ratios are less than one, the higher system's accuracy in detection. The AMSL dataset (Accuracy 95.8%, FAR 0.039, FRR 0%) (Accuracy 95.2%, FAR 0.047, FRR 0.98) for DNN and SVM, respectively. It turned out that the training of the proposed network optimized for the features extracted for the landmarks area significantly affects finding the difference and discovering the modified images, even in the case of minor modifications as in the AMSL dataset.

Keywords

Deep learning, Face morphing attacks, Convolution Neural Network, Principle Component Analysis, Support Vector Machine, And Faster Region Convolution Neural Network

Creative Commons License

Cover Page Footnote

The cooperation of the Prof. and students at the College of Education at the University of Kufa is appreciated. We also express our thanks and gratitude to the managing editor of the journal and all reviewers of the research for giving their valuable comments.

RESEARCH PAPER

Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network

Iman S. Razaq [a,*], Baheja K. Shukur [b]

[a] Department of Computer Science, College of Computer Science and Mathematics, University of Kufa, Najaf, Iraq
[b] College of Computer Science & Information Technology, University of Kerbala, Kerbala, Iraq

Abstract

Face recognition is the most extensively utilized security and public safety verification method. In many nations, the Automatic Border Control system uses face recognition to confirm the identification of travelers The ABC system is vulnerable to face morphing attacks; the face recognition systems give acceptance for the traveller, even though the passport photo does not represent the actual image of the person but is a result of the merger of two images. Therefore, it is vital to determine whether the passport image is altering (morph) or actual. This research proposes an improved method to extract features from facial images. The proposed method consists of four phases: In the first stage, morph images were generated using a set of databases of images of real people, used every two images that were similar in general shape or landmarks in producing the morphed image using three types of techniques used in this field (Automatic selection landmark, StyleGAN, and Manual selection landmark). StyleGAN has been relied upon to achieve the best results in producing artefact-free images. In the second phase, a Faster Region Convolution neural network is utilizing for determining and cutting important landmarks area (eyes, nose, mouth, and skin) in the face, where we leave the hair, ears, and image background for every image in the database. In the third phase, the features are extracted using three techniques Principal component analysis, eigenvalue, and eigenvector; a matrix of two-dimensional features is generated with one layer for each technique. Then merge the extracted features (with out s) from each image into one image with three layers. The first layer represents the principal component analysis features, the second the eigenvalue features, and the third the eigenvector features. Finally, the features are introduced into the convolutional neural networks to obtain optimal features. The fourth phase represents the classification process using the Deep Neural Network (DNN) classifier and Support Vector Machine (SVM) second classifier. The DNN classifier achieved an average accuracy of 99.02% compared with SVM, with an accuracy of 98.64%. The power of the proposed work is evident through the FRA and RFF evaluation. Which achieved values as low as possible for DNN FAR 0.018, indicating the error rate in calculating morphed images is actual, and FRR 0.003, meaning the error rate in calculating the actual images is morphed, FAR 0.023, FRR 0.06 for SVM whenever these ratios are less than one, the higher system's accuracy in detection. The AMSL dataset (Accuracy 95.8%, FAR 0.039, FRR 0%) (Accuracy 95.2%, FAR 0.047, FRR 0.98) for DNN and SVM, respectively. It turned out that the training of the proposed network optimized for the features extracted for the landmarks area significantly affects finding the difference and discovering the modified images, even in the case of minor modifications as in the AMSL dataset.

Keywords: Deep learning, Face morphing attacks, Convolution neural network, Principle component analysis, Support vector machine, Faster region convolution neural network

1. Introduction

Face recognition systems are a successful application that has occupied significant space in the verification field. The human face holds a multitude of information that can be studied, therefore, used for verification, particularly in security, due to this information and its uniqueness [1,2]. The Automatic Border Control system (ABC) primarily uses face

Received 18 December 2022; revised 18 March 2023; accepted 21 March 2023.
Available online 10 May 2023

* Corresponding author.
E-mail addresses: imans.alrihbawy@student.uokufa.edu.iq (I.S. Razaq), baheeja.k@uokerbala.edu.iq (B.K. Shukur).
Peer review under responsibility of Institute of Seismology, China Earthquake Administration.

https://doi.org/10.33640/2405-609X.3298

recognition techniques to verify the identity of travellers. ABC is an electronic control system that compares the stored passport image with a live image captured at the electronic gates upon the traveller's arrival [3]. The image on the passport might not be authentic, but somewhat modified (Face morphed). Face morphing is creating an image by combining two images, one for an average person and the other required by law. Fig. 1 shows the morphing process between two authentic images and produces an image similar to both.

Faces in the passport are compared with the traveler's live face image using facial information [3]. The procedure of comparison is carried out with the use of face-based identification verification techniques. Following a predetermined threshold limit, the system will either approve if the two images match or grant rejection if the result is lower than the threshold limit [3–5]. The problem is that the courts may want the traveler (by a criminal case), or he is not entitled to travel for other reasons, for example (child smuggling), so he can impersonate another person who can travel without restriction, a result of merging two images. This generates a state security problem, leading to more secondary difficulties. Fig. 2 explains the morphed attack that occurs in the traveller's passport.

Numerous challenges exist in the generation of morphing images [6], including:

1. Using many images for multiple people and making face morphing is challenging because of the increasing variances in image textures and features.
2. When two images are combined to create a single image, distortion may occur, necessitating image modification.
3. The two images that were used to create the face morphing have to be reasonably similar to one another. If there is a difference, it will be clear in the image and simple to detect.

The morphing face has excellent potential for optical as well as electronic illusion. Therefore, work has been done in this field in recent years to reduce this problem. Much research has focused on using new devices and technologies or modifying previous systems. This paper presented an approach that combines machine learning and deep learning to lessen this issue.

Some countries dealt with the problem by taking a live image directly of the person and putting it in the passport without adopting paper images. However, some others do not rely on this technology. In addition, the forgery will likely occur in circles to create a passport. The other solution is to develop different ways to identify the passport photo if it is forged by comparing it with a live image you take of the traveller at the airport. Here, too, electronic deception can occur, and the system does not recognize it [4,5].

Efforts and research have been strengthened so far within this field, trying to produce systems with high accuracy in detection. Every system has weaknesses and strengths, as development continues today on systems. The system's effectiveness can be determined by testing a set of high-resolution morph images and determining the accuracy and error rate.

The main contributions of this paper are outlined as follows.

- During pre-processing, the image size was scaled using deep learning technology to reduce alterations or distortions caused by resizing the images with conventional methods.
- Creating high-resolution images by generating morphed images in various ways, both manually and automatically.
- Creating a developed feature extraction model. Using principal component analysis, eigenvalue, eigenvector, and convolutional neural network, followed by DNN and SVM classification.

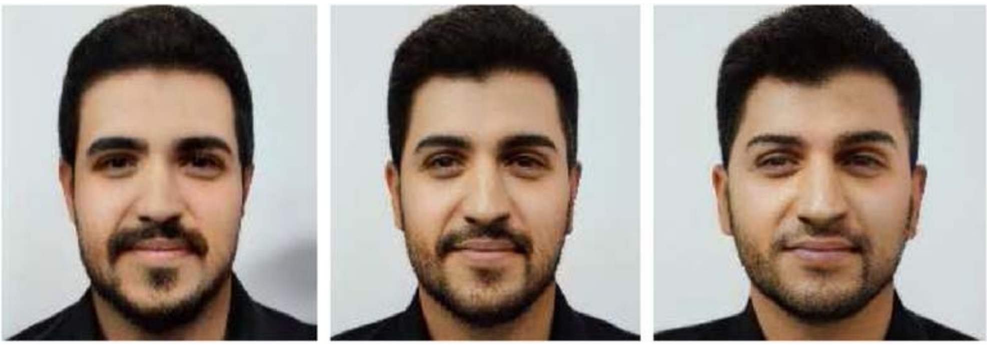

Fig. 1. Generate morph attack (right and left images authentic images, center: morphed image similar to left and right images).

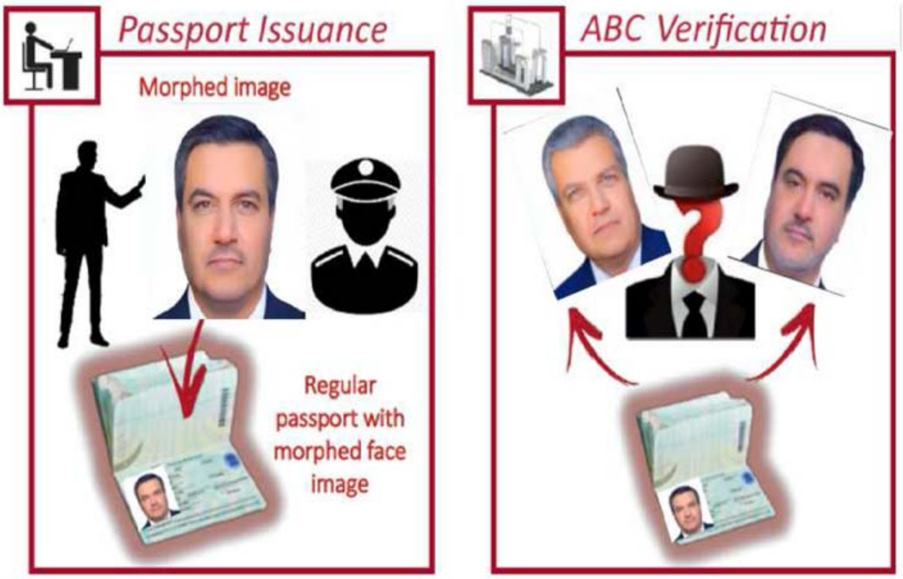

Fig. 2. It shows two authentic images, with the assumption that the first photo is of a person who can travel and the second photo is of a person who cannot travel; therefore, he blended the two images and produced an image that resembled the first and second person and was placed in the passport.

- Built a model that uses Faster Region CNN to determine faces in images.

This paper has two objectives, and the first is to create a database of morphed images and upload them to the Kaggle website to be a place for studying many types of research since most of the morphing rules are private. The second objective is to present this paper by using the extraction of the improved features and training them within a proposed convolutional neural network to obtain the best characteristics that distinguish the real faces from the modified ones and to reach the highest accuracy and the least error without relying on a comparison with a live image of a traveler and being satisfied with the passport image.

The paper is organized as follows: section two includes related work. Generation faces morphing in section three. At the same time, the fourth section, methodology, and the final section introduce the results and the conclusion.

2. Related works

This section provides relevant research on this topic. Some studies also utilized texturing techniques such as Local Binary Patterns, Binarized Statistical Image Features, Histograms of Oriented Gradients, etc. In most studies, ready-made CNN models, such as VGGNet, AlexNet, ResNet, etc., are used for feature extraction. We discuss some of them:

The study in [7] depend on a dataset of 52 pairs of real people's images (17 women, 35 men). Only images containing standard facial expressions without movements were selected when 1326 morph images were produced from these pairs. The method of detecting the morphed images was based on analyzing JPEG compression artifacts.It is considered that the original image taken from the camera has been subjected to JPEG compression, so after morphing the image, part of it is uncompressed. When this process is completed, the resulting image will be compressed. The Landmark of the original image will be compressed twice, and the resulting morphing parts will be compressed once, analyzed for those blocks, extracted the features using Benford features, and then classified. The performance evaluation results were FAR 44.60% and FRR 43.46%. The error rate is significant compared with our method.

A hybrid technique has been presented by Lukasz et al. [8], combining facial recognition and morphing detection. They used deep learning techniques, which are ready-made models of convolutional neural networks such as (Dlib, FaceNet, and VGG-Face) and machine learning in feature extraction (High-Dimension Local Binary Pattern). The High-Dim LBP method divides facial features into the eye area, nose area, and mouth corners. Each pixel is divided into 4*4 blocks, and applying LBP to this block will produce a vector of 99,120-dimensional features. Firstly, the original image to be queried is entered. Secondly, the features are calculated using the above methods. Thirdly, the Euclidean distance is calculated using a specific threshold limit for face verification. On the other hand, the features are classified using SVM, and finally, the results of verification and classification are combined for decision-making. They used two datasets: Multi-PIE dataset (morph and verification) and the LFW dataset (verification). The accuracy of this method was within 98–99%. However, there are several gaps in this paper, the first of which is that we notice through the results tables that those that lead to good results in verification are bad in detecting transformation, and vice versa. They are secondly relying on the reference image to discover the morph. Thirdly, the size of the Multi-PIE dataset is minimal. In addition, only pictures with snapshots suitable for the work were taken, representing the front images. Fourth, the threshold limit is variable to obtain the best results—a very restricted application. The error rate of the two scales, FAR and FRR, is significant compared to this paper.

Rien [9] presented a method for creating morph images with three techniques (Landmark available in python, Principal Component Analysis, and Variational Autoencoder (VAE)) and testing them on a facial recognition system to visualize how deceiving these systems are. To produce morph images using the last two techniques that go through the process of normalization, including identifying the eyes in the image, then finding the angle between the eyes and the horizontal length of the face to reduce the size of the image with a dimension of m * m to obtain the face area only, leaving the background. These images go through the training of both PCA and VAE techniques and produce morphed images. PCA gave poor results in generation morph, while VAE made good images. Use the FRGC database that contains a group of pictures of real people. The amount of test data is 126, and the training data is 24,332. Then use CNN and detect Local Binary Patterns as templates for face recognition. The images generated using Landmark were marked for artifacts in the morph images. The images generated using VAE are not distinguished because the resulting images are entirely different on the faces in the database. No method was used to check whether the morphological addition to the amount of test data was low. Images were generated far from the morphe used in the Border Control system, which causes visual and electronic deception, but fundamentally different images that the system cannot distinguish because they do not belong to anyone in the database.

Clemens et al. [10] 1900 morphed images generated from 1900 authentic images using different datasets using pipeline landmarks. This dataset was used to create four individual datasets using various proportions of both types: i. Naive: authentic 50%, morphed 50%. ii. Only region: authentic 50%, morphed 10%, and 40% another morphed. ii. Complex: authentic 50%, morphed 10%, 40% multi-morphed. V. Multiclass: Multi-morphed 20% for each morphed image. They used the trained neural network VGG19 in training the datasets and relying on the previous weights by changing the last layer by adding only two nodes. The method achieved effective results, with an accuracy of 98%–99% for some individual databases and 60%–80% for others. Gaps in this method of post-morph images require manual intervention, as mentioned, and others require another algorithm to deal with distortions and artifacts, which requires time and effort. The error rate is significant compared to our results. He also mentioned that the accuracy of recognizing morphed faces is higher than real faces. The reason for this is the use of morphed images in producing morphed images and for multiple people, which causes discrepancies in the image and apparent differences that are easy to detect. Finally, the generated images represent the manipulation of the image more than the imaginary morphology of two persons.

We add other knowledge to reach high accuracy and the lowest error percentage. We also decided based on a single image entered into the system and tested without comparison with the original to reduce time and cost. We are generating morph images similar to two people, so it isn't easy to distinguish between them using multiple datasets from the internet and the researcher community with different shapes, lightness, and many other factors. This increases the system's detection power.

3. Dataset

To compile the actual dataset, we obtained a variety of accessible face datasets and captured several face images for students. We picked only those images that match the guidelines and requirements for passport images. Our dataset comprises two stages: 1) Preparing a collection of real image pairs with comparable landmarks and 2) Generating morph faces from these pairs. Real pairs were taken from the various dataset (AMSL, Players Football, Young Adult White, American Multiracial Face Dataset (AMFD), Basel Face Database, Bogazici Face Database, Chicago Face Database, MR2 face dataset)

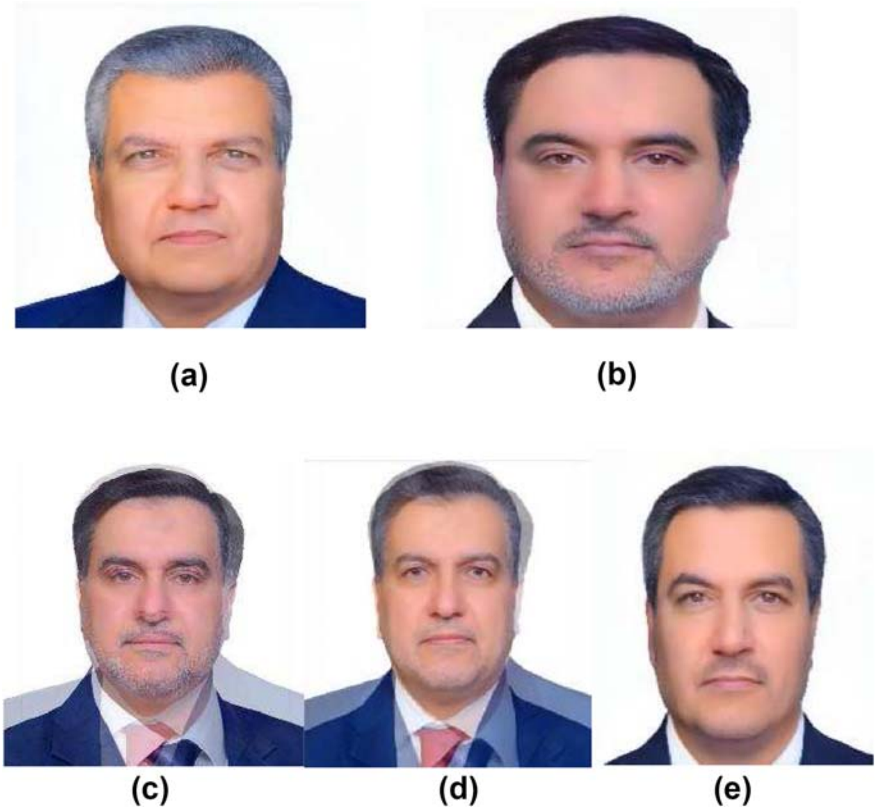

Fig. 3. (a) real image1 (b) real image2 (c) apply manual Landmark (d) apply automatic Landmark (e) apply StyleGAN.

[11–18]. Generated the morphing face using many techniques (Automatic selection landmark, StyleGAN, Manual selection landmark). Fig. 3 shows the results of applying the techniques above on samples images.

Automatic Landmark: selection of two real images and pass them through four steps: 1) Extraction Landmark automatic, 2) Triangulate, 3) Warp, and 4) Alpha Blend. In contrast, a manual selection landmark is a detection Landmark manual mixing between two real images with a ratio of 0.5.

StyleGAN: Images are generated automatically without human intervention and of high quality based on deep learning [19].

Fig. 2 demonstrates that StyleGAN yields the best results. Our database was constructed using the technique StyleGAN. Produces an image most similar to the real and more complex images since it cannot be discriminated because it lacks artifacts, as in images (c) and (d). The dataset consists of 3515 morph images generated from 1451 real images. In addition, using the AMSL dataset of face morph images [20] includes the authentic images of 201 people from the face research lab London set and 2000 morphed images. We split the original images into a training set (70%), a testing set (30%), and a validation set (10%).

4. Methodology

This section explains the details of the proposed model, which consists of four stages: (i) Pre-processing, (ii) Face detection using faster region CNN, (iii) feature extraction with PCA, eigenvalue, and eigenvector, (iv) Selection of the optimal features using CNN (v) classification. Fig. 4 explains how to feature extraction and passed to CNN. Fig. 5 shows the steps of a proposed model.

4.1. Pre-processing

Due to its enormous impact on study outcomes, almost no image-processing research is conducted without pre-processing. Several operations include pre-processing, cropping, resizing, enhancing brightness, deblurring, eliminating opacity, filtering, denoising, edge detection, and image registration. As part of the feature extraction and training requirements, all image sizes in the dataset must be identical. Deep learning is used to resize images without altering their data. The following steps illustrate the process of resizing.

- Extract the size of the input image.
- Determine desired output size.
- Determine output grid size and scale transformation based on input provided.

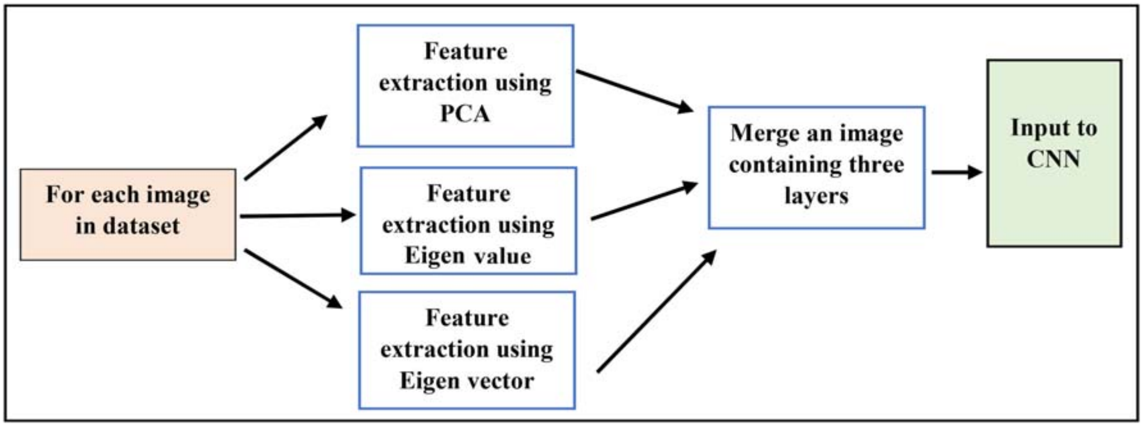
For each image in dataset
Feature extraction using PCA
Feature extraction using Eigen value
Feature extraction using Eigen vector
Merge an image containing three layers
Input to CNN

Fig. 4. Represent features extraction using multi-techniques.

- Determine the start location and stride along each spatial dimension.
- Perform actual interpolation.

4.2. Principle component analysis (PCA)

In machine learning, PCA is regarded as one of the main techniques for analyzing extensive data with multiple dimensions. PCA permits data interpretation and dimension reduction while maintaining as much information as possible after transforming the data from the linear system to the coordinate system. This method focuses on the Gaussian distribution with standard deviation and identifies the eigenvectors of the covariance matrix [21,22]. The algorithm below shows PCA in steps.

Algorithm 1: Principle Component Analysis.

```
Input: Color Image (three dimensions).
Output: Features with one dimension.
Begin:
1. Compute the mean of the image.
$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i$ (1)
Where n number of pixels, $x_i$ Represent a pixel in the location $i$, $\mu$ mean of an image.
2. Find the summation $K$ of the squared difference between each pixel and the mean.
$K = \sum_{i=1}^{n} (x_i - \mu)^2$ (2)
3. Compute the standard deviation $Sd$ based on step 2.
$Sd = \sqrt{\frac{K}{n-1}}$ (3)
5. Calculate the covariance matrix to determine the correlations between the data. If have three-dimensional like (x, y, z), find covariance between dimensions (x, y), dimensions (x, z), and dimensions (y, z). $con(x,y) = \frac{\sum_{i=1}^{n} (x_i - \mu)(y_i - \mu)}{(n-1)}$ (4)
6. Compute eigenvectors and eigenvalues from the covariance matrix to identify the principal components.
7. Choose the eigenvectors to depend on quantity variance.
$Featur = (eigenv_1, eigenv_2, \ldots, Eigenv_n)$ (5)
End
```

4.3. Eigenvalue and eigenvector

Eigen is an eigenvector with non-zero linear resolves [22,23]. It can be summarized in the following steps.

- Read matrix A with size $n \times m$ to find eigenvalue, compute AA^T.
- The eigenvalues of AA^T are calculated using the following equation: $Ax = \gamma x,$ to find γ by setting the determinant of the coefficient matrix to zero. From γ will get on eigenvectors.

The first column of the matrix is the sort eigenvector of the largest eigenvalue, followed by the second largest eigenvalue, and so on, until the last column is the smallest eigenvalue.

4.4. Convolutional neural networks

Deep learning is one of the prevalent techniques that uses deep neural networks that train large amounts of data to classify, detect an object, generate an object, colorize, improve image resolution, remove blur, etc. In the field of digital image processing, deep learning has many algorithms [24].

Artificial neural networks have layers of neurons connected by weight values inspired by biological neural networks. Each neuron calculates the weighted sum of input values from the preceding layer, adds a bias term, evaluates a nonlinear function (activation function), and outputs the function value to the next layer. Training an artificial neural network involves modifying weights and bias factors to produce output values from the training set. Convolutional layers are the significant difference between standard and convolutional neural networks. Unlike fully linked levels, convolutional layers receive small, spatially continuous inputs from the previous layer [24,25]. The most well-known Deep Learning (DL) model is the

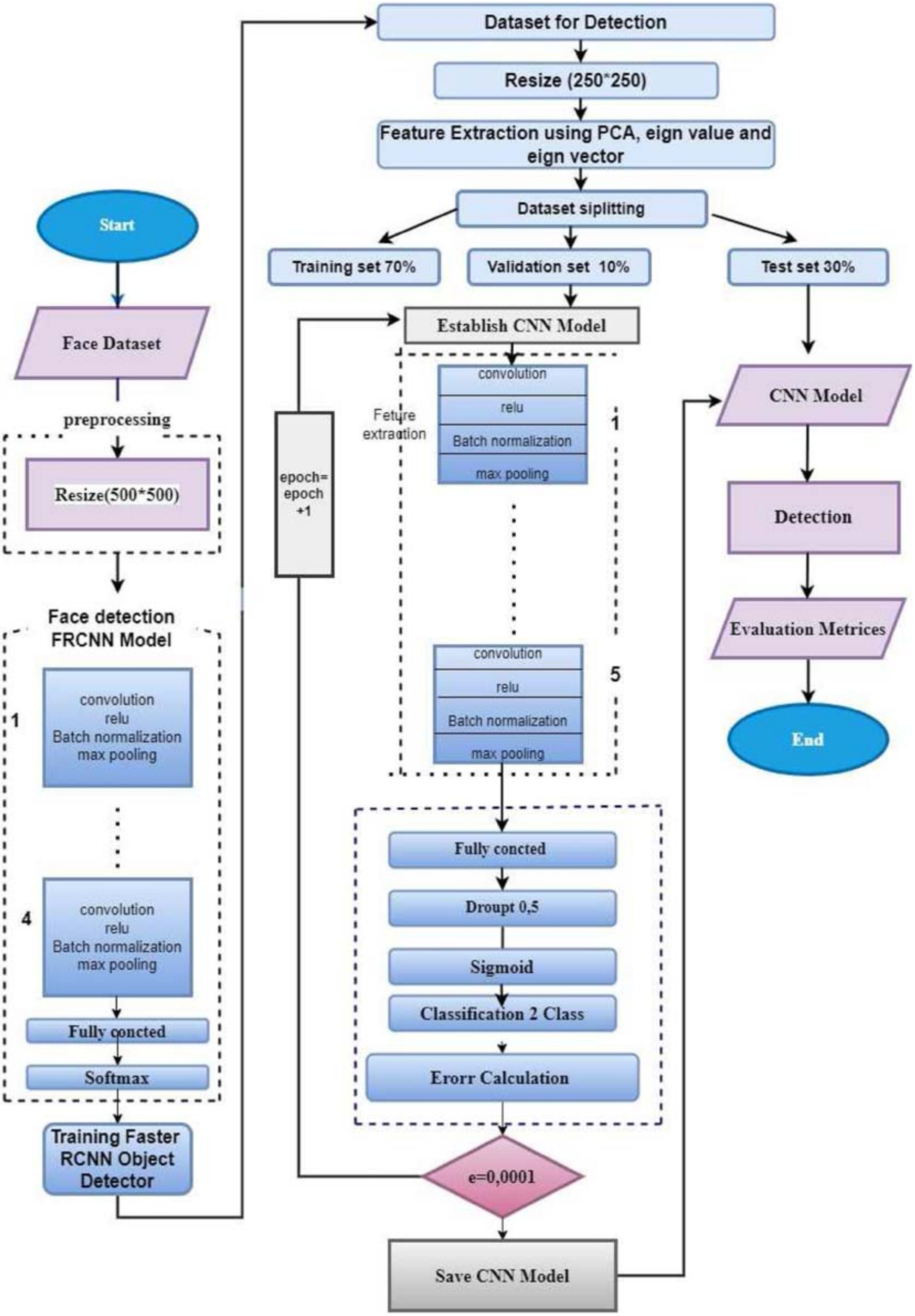

Fig. 5. Explain the proposed model.

Convolutional Neural Network (CNN). DL appears more complicated by having more layers than conventional artificial neural network models [26].

Table 1 shows the CNN of the proposed model includes the following layers.

- Input layer: This layer contains defining the dimensions of the inputs (images), such as rows, columns, and the number of layers (250, 250, 3), respectively.
- Convolution layers: In this layer, generated set of filters are applied to the input images to obtain the so-called features map. The parameters of this layer are the number of filters, the size of each filter, and padding. The weights of these filters update automatically with each epoch.
- ReLU activation function: After applying a convolution to the input data, the negative value is overridden because it does not represent features by using this function.

$$f(\mathcal{S}) = \max(0, \mathcal{S}) = \begin{cases} \mathcal{S}_i, if\ \mathcal{S}_i \geq 0 \\ 0, if\ \mathcal{S}_i < 0 \end{cases} \quad (6)$$

$\mathcal{S}$ is the input value and $f(\mathcal{S})$ The output.

- Batch-normalization layer (BN): It aims to make training neural networks more stable and faster. BN is used after each layer of convolution.

Table 1. The architecture of the CNN model for the proposed system.

Name	Type	Activation
Image input	Image input	250 × 250 × 3
Conv_1	2-D Conv.	250 × 250 × 30
Relu_1	Activation Fun.	250 × 250 × 30
BatchNo_1	Batch Norm.	250 × 250 × 30
Maxpool_1	2-D max Po.	125 × 125 × 30
Conv_2	2-D Conv.	125 × 125 × 60
Relu_2	Activation Fun.	125 × 125 × 60
BatchNo_2	Batch Norm.	125 × 125 × 60
Maxpool_2	2-D max Po.	62 × 62 × 60
Conv_3	2-D Conv.	62 × 62 × 90
Relu_3	Activation Fun.	62 × 62 × 90
BatchNo_3	Batch Norm.	62 × 62 × 90
Maxpool_3	2-D max Po.	31 × 31 × 90
Conv_4	2-D Conv.	31 × 31 × 30
Relu_4	Activation Fun.	31 × 31 × 30
BatchNo_4	Batch Norm.	31 × 31 × 30
Maxpool_4	2-D max Po.	15 × 15 × 30
Conv_5	2-D Conv.	15 × 15 × 60
Relu_5	Activation Fun.	15 × 15 × 60
BatchNo_5	Batch Norm.	15 × 15 × 60
Maxpool_5	2-D max Po.	7 × 7 × 30
FC	Fully Conn.	1 × 1 × 1500
Drop.	–	0.5
Sigmoid_1	Activation Fun.	_
Class output	Classification	Two

Option	Training Opt.	Optimizer = Adam
		Epoch = 100 learn rate = 0.0001

Max-Pooling layer: The feature map from the convolution layer is reduced by using this layer. Aim to reach the lowest and best features. The feature maps are divided into blocks of size 2 * 2 and take the maximum value for each block.

- Dropout layer: Dropout is a simple and effective technique to reduce overfitting during training and improve the model's generalization. Using this technique, parts of hidden neurons are usually randomly ignored during training based on the probability of the neurons in the specified hidden layers [27].
- Flatten layer: The final features are converted to a one-dimensional vector.
- Sigmoid activation function: This function is used as an activation function in the classification phase. It is used to classify binary classes and may return zero or one [28].

4.5. Faster regions with convolutional neural networks object detection (FR-CNN)

Deep learning has become widely involved in various directions and is not limited to classification, as it is known in CNN. Therefore, it enters the field of identifying the objects in the images, which significantly helps reduce the time and effort used by the mechanical methods that sometimes require manual intervention in identifying the object [29–31]. This technique is based on CNN. Table 2 shows layers of FRCNN.

4.6. Classification

The final stage of the proposed model is classification, as two classifiers (SVM and DNN) were used [32–34]. Support Vector Machine (SVM) is a machine-learning algorithm used to classify linear and nonlinear data with a high ability to classify data with binary categories. DNN represents deep neural networks that are part of CNN. They classify optimally by training the network with weights to achieve the smallest possible error between the output and target class.

5. Results and discussion

Following is a discussion of the accuracy, robustness, and generality produced by our various training tables and the insights gained through a combination of machine and deep learning. In addition, the biometric quality of the resulting altered facial images was investigated.

Table 2. The architecture of the FR-CNN model.

Name	Type	Activation
Image input	Image input	500 × 500 × 3
Conv_1	2-D Conv.	500 × 500 × 30
Relu_1	ReLU	500 × 500 × 30
BatchNo_1	Batch Norm.	500 × 500 × 30
Maxpool_1	2-D max Po.	250 × 250 × 30
Conv_2	2-D Conv.	250 × 250 × 60
Relu_2	ReLU	250 × 250 × 60
BatchNo_2	Batch Norm.	250 × 250 × 60
Maxpool_2	2-D max Po.	250 × 250 × 60
Conv_3	2-D Conv.	125 × 125 × 90
Relu_3	ReLU	125 × 125 × 90
BatchNo_3	Batch Norm.	125 × 125 × 90
Maxpool_3	2-D max Po.	62 × 62 × 90
Conv_4	2-D Conv.	62 × 62 × 30
Relu_4	ReLU	62 × 62 × 30
BatchNo_4	Batch Norm.	62 × 62 × 30
Maxpool_4	2-D max Po.	31 × 31 × 30
FC_1	Fully Conn.	1 × 1 × 4000
Relu_5	ReLU	–
Drop.	–	0.5
FC_2	Fully Conn.	1 × 1 × 2100
Softmax_1	SoftMax	_
Class output	Classification	–

Option	Training Opt.	Optimizer = Sgdm
		Epoch = 50 learn rate = 0.0001

Training	Training object detect	*NegativeOverlapRange* = [0 0.3] *PositiveOverlapRange* = [0.5 1] *SmallestImageDimension* = 500

Figures in the introduction section: the first figure includes images taken of students at the College of Education at the University of Kufa. Their permission was obtained to create the morphed image and have it alongside their original images in the research.

Figs. 2 and 3 include an image of Prof. Dr. Nidhal al-Abadi, a professor at the University of Kufa's College of Education and a staff engineer within the college's scope. Their permission was obtained to create the morphed image and use it alongside the original image in the research.

All the individuals mentioned above are well-versed in the research subject and method of publication.

The following measures evaluated the performance of the proposed model in detecting morphing faces: Accuracy (ACC), False Acceptance Rate (FAR), and False Rejection Rate (FRR) [30]. Equations (7)–(9) represent the evaluation metrics:

$$FAR = \frac{|Accepted\ morphs|}{|All\ morphed\ images|} \tag{7}$$

$$FRR = \frac{|Rejected\ genuine\ individuals|}{|All\ genuine\ individuals|} \tag{8}$$

$$ACC = \frac{|Correctly\ classified\ images|}{|All\ classified\ images|} \tag{9}$$

The proposed model was trained on two datasets (1) our dataset and (2) the AMSL dataset.

After features are extracted using machine learning methods as a two-dimensional matrix, they are input into the proposed CNN deep learning. These features are separated into training at 70%, validation at 10%, and testing at 30%.

It was trained first on a database whose images were produced using landmark technique and again using ready-made and manual software techniques. The detection rate was 100%, and the error accuracy was zero. In such a case, the results are incorrect because the images resulting from this method contain artifacts that make it easier for the trained network to discover and identify them easily and distinguish them from the original images that do not have distortions. Therefore, we used StyleGAN technology to produce high-resolution morph images free from distortion and artifacts that cause an optical illusion.

We indicate in the tables below the system's accuracy in distinguishing between real images and morphed images when it reaches 100%, meaning a system capable of detecting morphs correctly and without error, where the error rate is 0%. We also point out the error in classifying morphed images as real and vice versa. When the percentage reaches 0% or slightly higher, this gives an advantage to the system that relies on detecting correctly and accurately. Table 4 presents the results after 100 epochs of feature training. The overall accuracy rate reached 99.02% for the DNN classifier, representing the highest accuracy obtained compared to the rest of the classifiers mentioned. The SVM classifier followed it with an accuracy of 98.64%, followed by KNN with a minimal difference from the SVM classifier. It also achieved the lowest error rate of 0.0186 for the morphed images classified as real and an error rate of 0.003 for the real images classified as morphed. The system can generally classify real images better than morph images, even with a minimal error difference.

The training began on the number of epochs 30, as shown in Table 4. The DNN classifier was also better than the SVM regarding (should be deleted) accuracy, which amounted to 97.64%, and the error rate achieved a lower value. When compared with 100 epochs, the difference is minimal.

The results of increasing the number of epochs from 30 to 70 are presented in Table 5. It is observed that the accuracy improved as the number of training cycles increased. The accuracy and error

Table 3. Performance results for our dataset with the parameters of proposed CNN with multi-classifiers, epoch 100, and time 20 h.

Classifiers	Acc. %	FAR %	RFF %
DNN	99.02	0.0186	0.003
SVM	98.64	0.023	0.066
Naïve Bayes	85.5	5.2	3.7
Decision Tree	95.32	0.065	0.033
K-Nearest Number	98.44	0.032	0.003

Table 4. Performance results for our dataset with the parameters of proposed CNN, epoch 30, and time 6 h.

Classifiers	Acc. %	FAR %	RFF %
DNN	97.64	0.047	0.005
SVM	95.98	0.085	0.016

Table 5. Performance results for our dataset with the parameters of proposed CNN, epoch 70, and time 14 h.

Classifiers	Acc. %	FAR %	RFF %
DNN	98.22	0.020	0.002
SVM	98	0.100	0.100

rate improved when the number of training iterations was increased for the DNN classifier. However, with the SVM classifier, the accuracy increased, and the error rate was from 0.085 to 0.100 for the morph images diagnosed as real and from 0.016 to 0.100 for the real images interpreted as a morph.

After the KNN classifier attained a high accuracy and small error, we analyzed the various K instances indicated in Table 6.

Table 7 provides the findings (accuracy) of the proposed system for each diagnosis, true or false, for each of the two image types for which the accuracy rate was provided in Table 3.

The proposed work was compared with a set of ready-made CNN models, as shown in Table 8.

Also implemented on the AMSL database was the proposed approach. This rule is seen as belonging to the field of morph in which we are engaged. Instead, it is a change in the eyes, nose, or mouth of one person based on another image, as if it were a modification of specific facial landmarks, and it is not a total alteration coming from merging two photographs into one image to create an image that resembles the two individuals. Although there was a high degree of similarity between the morph and actual images of the same individual, the proposed method could identify the morph accurately.

Table 6. Performance results for our dataset using difference K for K-Nearest Number.

Value of K	Acc. %	FAR %	RFF %
5	98.44	0.032	0.003
10	98.25	0.028	0.01
30	95	0.056	0.075
50	90	0.60	0.87

Table 7. Total correct detection of real and morph images.

Images	True Detection	False Detection
Morph	99.5	0.5
Real	98.7	1.3
Average	99.0	1.0

Table 8. Compression between our models and other models of CNN.

Model	Acc.%	FAR %	FRR %
Alexnet [35]	94.65	0.095	0.033
VGG16 [36]	95.12	0.088	0.072
VGG19 [36]	94.20	0.230	0.041
GoogleNet [37]	93.11	0.114	0.243
ResNet50 [37]	95.5	0.075	0.099

According to Table 10 with 100 epochs and Table 9 with 30 epochs, the DNN and SVM classifiers achieved the maximum accuracy of 95.8 and 95.2%, respectively. Compared to the amount of the resulting error, the classifier DNN successfully classified all the actual images. Thus, the error rate was 0, while a portion of the morph images was mistakenly classified, with an error rate of 0.039. In contrast to the SVM classifier, which properly categorized every morph image with a 0% error rate, the classification of actual images had an error rate of 0.098.

6. Conclusions and recommendations

This paper presented a model combining the features extracted from machine learning and deep learning to get the best features for detection. In comparison to other previous publications, the proposed technique yielded promising findings. This paper's benefit is obtaining a system with high accuracy in diagnosing morphed images with minimal error. Morph images were created using the StyleGAN method from multiple datasets, and we were not limited to one database, as in most research. StyleGAN, unlike other ways, gave more realistic

Table 9. Performance metrics AMSL dataset with 30 epochs.

Model	Acc.	FAR	RFF
AMSL dataset	91.57	0.082	0
AMSL dataset	91.60	0	0.96

Table 10. Performance metrics AMSL dataset with 100 epochs.

Model	Acc.	FAR	FRR
AMSL dataset + DNN	95.8	0.039	0
AMSL dataset + SVM	95.2	0	0.098

results, free of distortions and artifacts. One of the challenges in producing these images is the difficulty of selecting two similar images in terms of facial features to create a morphed image that is difficult to distinguish by face recognition systems, in addition to the many differences in terms of luminance, head movement, background, hair, clothes, and others. After extracting the features PCA, eigenvalues, and eigenvectors separately for each image, the stage of its introduction to the CNN is to extract optimal features that increase the accuracy of morph detection. The optimal features from CNN are classified based on DNN and SVM with an accuracy of 99% and 98%, respectively, the lowest percentage of the metric FAR and FRR 0.018, 0.003 for DNN, 0.023, and 0.06 for SVM. It also achieved higher accuracy of the proposed model than previously published models (VGG, AlexNet, etc.). The proposed model was applied to the AMSL data set. Despite the minimal difference between the real and the morph images, which leads to a very high electronic illusion, it achieved an accuracy of 95.8%, FAR 0.039 FRR 0 for DNN, and 95.2%, FAR 0%, FRR 0.098. Classification using DNN achieved more positive results for all metrics compared to SVM and other models. We are working on another paper to combine deep learning features, features from one of the texture algorithms, and features based on image frequencies to improve accuracy. Future work on the original image and the morph, in which the facial features are compared, is possible using wavy duplication techniques that allow calculating the changes between the original image and the improved or modified image and determining the percentage of change in quantity and quality.

Ethics approval

The research involved working on and manipulating images of real people. All individuals whose images were utilized in this work gave their written, informed consent for publishing.

Acknowledgment

The cooperation of the Prof. and students at the College of Education at the University of Kufa is appreciated. We also express our thanks and gratitude to the managing editor of the journal and all reviewers of the research for giving their valuable comments.

References

[1] Y. Kortli, M. Jridi, A. al Falou, M. Atri, Face recognition systems: a survey, Sensors 20 (2020) 342, https://doi.org/10.3390/s20020342.

[2] R.V. Petrescu, Face recognition as a biometric application, J. Mech. Robot. 3 (2019) 237–257, https://doi.org/https://doi.org/ 10.3844/jmrsp.2019.237.257.

[3] J.S. del Rio, D. Moctezuma, C. Conde, I.M. de Diego, E. Cabello, Automated border control e-gates and facial recognition systems, Comput. Secur. 62 (2016) 49–72, https://doi.org/10.1016/j.cose.2016.07.001.

[4] O.O. Petrova, K.B. Bulatov, Methods of machine-readable zone recognition results post-processing, ICMV 11041 (2019) 387–393, https://doi.org/10.1117/12.2522792.

[5] S. Noori, Suspicious infrastructures: automating border control and the multiplication of mistrust through biometric e-gates, Geopolitics 27 (2022) 1117–1139, https://doi.org/10.1080/14650045.2021.1952183.

[6] D. Ortega, A. Fernández-Isabel, I. Martín de Diego, C. Conde, E. Cabello, Dynamic facial presentation attack detection for automated border control systems, Comput. Secur. 92 (2020) 101744, https://doi.org/10.1016/J.COSE.2020.101744.

[7] A. Makrushin, T. Neubert, J. Dittmann, Automatic generation and detection of visually faultless facial morphs, VISIGRAPP 7 (2017) 39–50, https://doi.org/10.5220/0006131100390050.

[8] L. Wandzik, G. Kaeding, R.V. Garcia, Morphing detection using a general-purpose face recognition system, EUSIPCO 2076–1465 (2018) 1012–1016, https://doi.org/10.23919/EUSIPCO.2018.8553375.

[9] R. Heuver, Generating Facial Morphs through PCA and VAE[1], Uni. Twen.. (2020), pp. 1–11. http://essay.utwente.nl/81372/.

[10] C. Seibold, W. Samek, A. Hilsmann, P. Eisert, Accurate and robust neural networks for face morphing attack detection, J. Inf. Secur. Appl. 53 (2020) 102526, https://doi.org/10.1016/j.jisa.2020.102526.

[11] L. DeBruine, B. Jones, Face Research Lab London Set, 2017. https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666/. (accessed May 30 2017). accessed.

[12] J. Bird, Football Players and Staff Faces, Dataset for Project Generating a Football Team with Progressive GAN (PGAN) and Char-RNN, 2020. https://www.kaggle.com/datasets/birdy654/football-players-and-staff-faces/. (accessed November 27 2022). accessed.

[13] L. DeBruine, B. Jones, Young Adult White Faces with Manipulated Versions, 2022. https://figshare.com/articles/dataset/Young_Adult_White_Faces_with_Manipulated_Versions/4220517/. (accessed November 27 2022). accessed.

[14] J.M. Chen, J.B. Norman, Y. Nam, Broadening the stimulus set: introducing the American multiracial faces database, Behav Res 53 (2021) 371–389.

[15] M. Walker, S. Schönborn, R. Greifeneder, T. Vetter, The basel face database: a validated set of photographs reflecting systematic differences in big two and big five personality dimensions, PLoS One 13 (2018) e0193190, https://doi.org/10.1371/journal.pone.0193190.

[16] S. Adil Saribay, A.F. Biten, E.O. Meral, P. Aldan, V. Trebicky, K. Kleisner, The Bogazici face database: standardized photographs of Turkish faces with supporting materials, PLoS One 13 (2018) e0192018, https://doi.org/10.1371/journal.pone.0192018.

[17] D.S. Ma, J. Kantner, B. Wittenbrink, Chicago face database: multiracial expansion, Behav. Res. 53 (2021) 1289–1300, https://doi.org/10.3758/s13428-020-01482-5.

[18] N. Strohminger, K. Gray, V. Chituc, J. Heffner, C. Schein, C.T.B. Heagins, MR2 face database, Behav. Res. 48 (2016) 1197–1204, https://doi.org/10.3758/T45216-060-00322-5.

[19] S. Price, S. Soleymani, N.M. Nasrabadi, Landmark enforcement and style manipulation for generative morphing, Indian J. Clin. Biochem. 2474–9699 (2022) 1–10, https://doi.org/10.1109/IJCB54206.2022.10008001.

[20] T. Neubert, A. Makrushin, M. Hildebrandt, C. Kraetzer, J. Dittmann, Extended StirTrace benchmarking of biometric and forensic qualities of morphed face images, IET Biom. 7 (2018) 325–332, https://doi.org/10.1049/IET-BMT.2017.0147.

[21] S. Karamizadeh, S.M. Abdullah, A.A. Manaf, M. Zamani, A. Hooman, An overview of principal component analysis, JSIP 4 (2013) 173−175, https://doi.org/10.4236/JSIP.2013.43B031.

[22] P.B. Denton, S.J. Parke, T. Tao, X. Zha, Eigenvectors from eigenvalues: a survey of a basic identity in linear algebra, Bull. Am. Math. Soc. 59 (2022) 31−58, https://doi.org/10.1090/bull/1722.

[23] N.A. Abdullaha, M.J. Saidi, N.H.A. Rahmanb, C.C. Wenc, I.R.A. Hamidd, Face recognition for criminal identification: an implementation of principal component analysis for face recognition, AIP Conf. Proc. 1891 (1−6) (2017) 020002, https://doi.org/10.1063/1.5005335.

[24] H. Sigaki, E. Lenzi, R. Zola1, M. Perc, H. Ribeiro, Learning physical properties of liquid crystals with deep convolutional neural networks, Sci. Rep. 10 (2020) 7664−7710, https://doi.org/10.1038/s41598-020-63662-9.

[25] A. Esteva, K. Chou, S. Yeung, N. Naik, A. Madani, A. Mottaghi, Y. Liu, E. Topol, J. Dean, R. Socher, Deep learning-enabled medical computer vision, Npj Digit. Med. 4 (2021) 1−9, https://doi.org/10.1038/s41 746-020-00376-2.

[26] M. Surucu, Y. Isler, M. Perc, R. Kara, Convolutional neural networks predict the onset of paroxysmal atrial fibrillation: theory and applications, J. Nonlinear Sci. 31 (11) (2021) 113119−113210, https://doi.org/10.1063/5.0069272.

[27] A.M. Alhassan, W.M.N.W. Zainon, Brain tumor classification in magnetic resonance image using hard swish-based RELU activation function-convolutional neural network, Neural Comput. Appl. 33 (2021) 9075−9087.

[28] H. Faris, I. Aljarah, S. Mirjalili, Training feedforward neural networks using multi-verse optimizer for binary classification problems, Appl. Intell. 45 (2016) 322−332, https://doi.org/10.1007/S10489-016-0767-1.

[29] C. Cao, B. Wang, W. Zhang, X. Zeng, X. Yan, Z. Feng, Y. Liu, Z. Wu, An improved faster R-CNN for small object detection, IEEE Access 7 (2019) 106838−106846, https://doi.org/10.1109/ACCESS.2019.2932731.

[30] S. Ren, K. He, R. Girshick, J. Sun, R.-C.N.N. Faster, Towards real-time object detection with region proposal networks, IEEE Trans. Pattern Anal. 39 (2017) 1137−1149, https://doi.org/10.1109/tpami.2016.2577031.

[31] M. Karthikeyan, T. Subashini, Automated object detection of mechanical fasteners using faster region based convolutional neural networks, Int. J. Electr. Comput. Eng. 11 (2021) 5430−5437, https://doi.org/10.11591/ijece.v11i6.pp5430-5437.

[32] S. Oztürk, U. Ozkaya, M. Barstugan, Classification of Coronavirus (COVID-19) from X-ray and CT images using shrunken features, Int. J. Imag. Syst. Technol. 31 (2021) 5−15.

[33] M.A. Chandra, S.S. Bedi, Survey on SVM and their application in image classification, Int. J. Inf. Technol. 13 (2018) 1−11, https://doi.org/10.1007/S41870-017-0080-1.

[34] H. Zhao, H. Liu, Multiple classifiers fusion and CNN feature extraction for handwritten digits recognition, J. Granular Computing. 5 (2020) 411−418, https://doi.org/10.1007/s41066-019-00158-6.

[35] K.M. Hosny, M.A. Kassem, M.M. Fouad, Classification of skin lesions into seven classes using transfer learning with AlexNet, J. Digit. Imag. 33 (2020) 1325−1334.

[36] A. Krishnaswamy Rangarajan, R. Purushothaman, Disease classification in eggplant using pre-trained VGG16 and MSVM, J. Sci. Reports. 10 (2020) 1−11, https://doi.org/10.1038/s4 159 8-020-59108-x.

[37] B. Li, D. Lima, Facial expression recognition via ResNet-50, Int. J. Cognit. Comput. Eng. 2 (2021) 57−64, https://doi.org/10.1016/J.IJCCE.2021.02.002.