IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 4, Ser. II (Jul. –Aug. 2022), PP 27-38
www.iosrjournals.org

A Robust Face Recognition Model against Morphing Attacks using CNN

Kholoud Albalawi[1], Anas Bushnag[2], Ali Alessa[3], Slim Ben Chaabane[4]
[1](Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia)
[2](Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia)
[3](Institute of Public Administration, Saudi Arabia)
[4](Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia)

Abstract:*Recently, face recognition systems (FRSs) have received significant attention from researchers due to their valuable benefits, such as monitoring and tracking banned individuals, observing borders, and controlling authenticated access to sensitive places. However, when using traditional techniques, FRS suffers from low accuracy. This struggle is because advanced attacks, such as morphing attacks and changes in luminance of the environment, are not considered. This work aims to build an FRS that can detect and recognize faces under an unconstrained environment using a CNN. The experimental results showed that the proposed FRS achieved high performance with an accuracy value of 99.7%. Thus, the proposed system was applied to morphed images to test its robustness against advanced attacks such as morphing. The face recognition results under morphing attacks showed a high accuracy of 95%.*

Key Word*:Face Recognition; Face Detection; Morphing Attack; CNN; Deep Learning; AI, Security*.

Date of Submission: 07-08-2022 Date of Acceptance: 22-08-2022

I. Introduction

1.1 Background

Automatic face image manipulation is increasingly used due to the evolution of artificial intelligence (AI) and computer vision applications. AI-based digital face manipulation technologies include face detection and face recognition. For example, face detection (FD) technology identifies an area of a face from a given image that captures a person's whole body. In other words, FD isolates the face from the rest of the body [1]. Face recognition (FR) is a technology that refers to the process of identifying a given person among other people [2].

Face recognition is an area of science combining three research fields: image processing, artificial intelligence, and cybersecurity. Image processing is a branch of computer science concerned with performing operations on images to improve them according to specific standards or extract some information from them [3]. Artificial intelligence is concerned with algorithms that simulate the human brain. Such algorithms can collect, analyze and interpret data and make decisions [4]. Cybersecurity can be defined as the techniques that protect computers, servers, networks, and information systems to defend against malicious attacks and unauthorized intrusion [5].

Face recognition systems in real life are applied in many fields, such as the following:

- Forensics: To prevent retail crime, these systems are employed to instantly identify recorded retail criminals or fraudsters while robbing retail malls [6].
- Mobile Security: Face recognition is now being used for unlocking mobile phones. This technology is a powerful method for protecting the privacy and security of users and ensuring that if a phone is stolen, sensitive data remain inaccessible [7].
- Marketing: For more innovative advertising, FR can target advertising by making knowledgeable guesses at people's age and gender [8].
- Social: To assist people with visual impairments, some companies have developed ground-breaking facial recognition apps, which can launch vibrations to alert users to smiles or other expressions. This usage contributes to a better understanding of social situations by individuals with disabilities [9].
- Medical: For diagnosing diseases, the key idea is to detect facial changes due to abnormal medical situations [10].

Face recognition systems have developed significantly over the last few years due to the evolution of AI techniques. Thus, face recognition approaches can be classified into two classes: deep learning and traditional, as shown in Fig. 1.

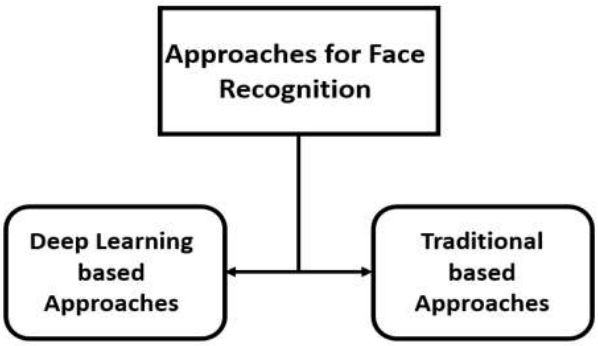

Fig. 1 Categories of face recognition approaches.

Traditional face recognition methods are based on handcrafted facial features, which depend on edge analysis, texture scanning, or manipulating facial images pixel by pixel using a standard technique called eigenfaces [11]. Traditional approaches suffer from poor performance (very long processing time), low resistance against changes, and high complexity at computation and time levels [12]. The traditional methods go through several steps, as described below and shown in Fig. 2.

- The first step is face detection, in which the primary objects of the body are determined, such as the shoulders, chest, and hands. This process is achieved using specialized filters, such as erosion close and open filters [13].
- The second step is face localization, which involves a cropping operation to isolate the face from other parts of the body.
- The third stage is matching the handcrafted features, which means that the cropped face is tested with some faces stored in a dataset prepared previously for matching and equipped with advanced SQL queries.

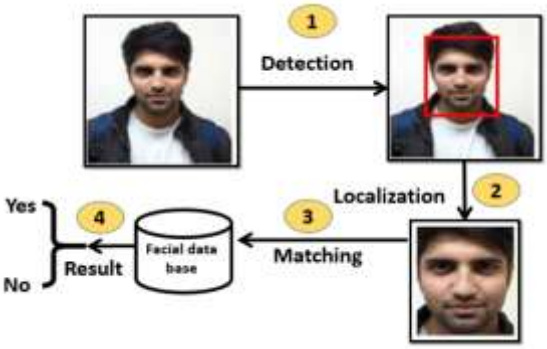

Fig. 2 Steps of traditional systems designed for face recognition.

Recent FR systems are based on deep learning techniques that learn the best and most robust features by training the models on large datasets. For example, deep learning-based face recognition systems include two stages: detecting a person's face using advanced neural network algorithms and extracting features to draw a face map. Fig. 3 illustrates the general scenario using deep learning methods for face recognition.

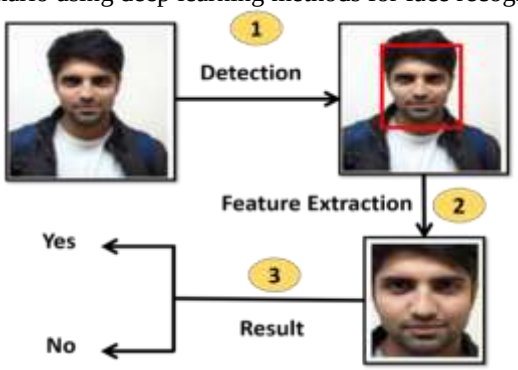

Fig. 3 Steps in DL-Based methods for face recognition.

The downside of traditional face recognition systems is that they are time-consuming processes, which lead to high computational cost and complexity. Therefore, deep learning face recognition systems are preferred. Table no 1 compares the traditional and advanced face recognition systems regarding processing time, complexity, computational cost, response time, and accuracy.

Table no 1: Comparison between traditional and DL-based face recognition systems.

Criteria	**Traditional systems**	**DL-based systems**
Processing time	Very long	Considerable
Complexity	Very high	Considerable (based on the used method)
Computational cost	Very high	Less
Response time	Very long	Shorter
Accuracy	Acceptable	High

1.2 Problem Definition

The traditional FR process scenario should be explored first to understand the problem. Fig. 4 illustrates how users access an information system remotely.

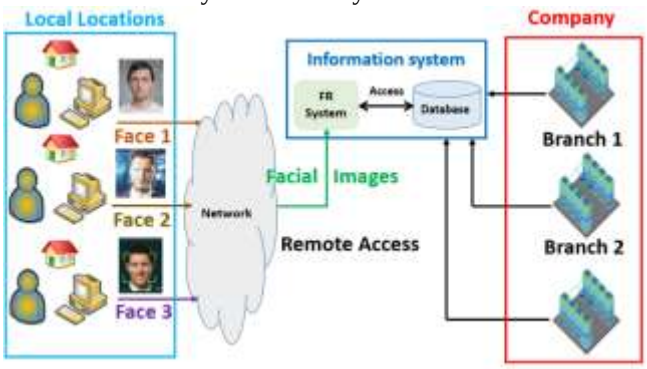

Fig. 4 Remote access to information systems in traditional FR processes.

As shown in Fig. 4, several employees use the FR system to access the information system from their locations (homes). Each employee sends a face image via the network to the FR system linked to a database to allow remote access to the company's various branches. Currently, this scenario is common, especially after the widespread COVID-19 epidemic. However, this classical scenario has no resistance against adversarial attacks. An existing adversary between the employees and the information system leads to severe problems, as shown in Fig. 5.

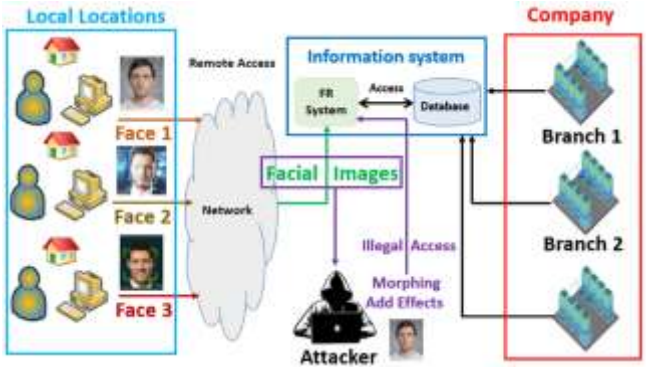

Fig. 5 Problems of illegal access.

The attacker obtains the sent facial images. Then, the attacker can modify those images using morphing operations or add effects that blur the images, such as noise. Morphing operations are a term that refers to creating a modified copy of the face using filters and advanced image processing manipulations [14][15]. In this way, the attacker can illegally modify the obtained face image to be kept for future access to the information system. In other words, the attacker steals the identity of the authenticated users, which is a significant issue in the cybersecurity domain. For adding effects (noise), the attacker might add drops of rain or dust to the obtained facial images to harm the authenticated users. Therefore, the FR system cannot access the information system due to unclear face images [16].As a result, the attacker prevents authenticated users from accessing the information system or gains illegal access. Thus, FR systems must be robust against morphing attacks and handle images under environmental factors, such as sharp lightning and rain. From the deep learning point of

view, the problem can be transformed into a low accuracy (noisy image) problem. Fig. 6 illustrates the problem from the deep learning perspective.

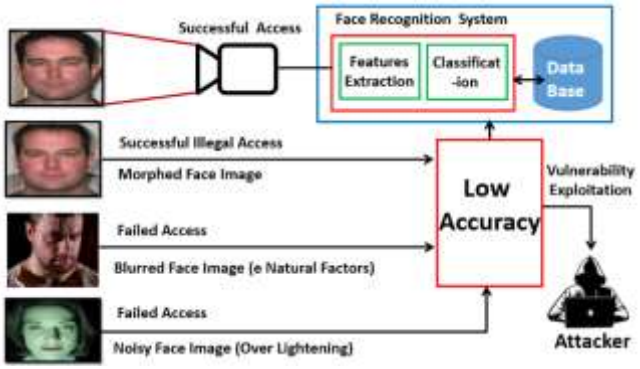

Fig. 6 Visual problem from the deep learning point of view.

Fig. 6 reflects the problem in terms of low accuracy. This low accuracy means that the FR system does not recognize users with a high level of trust. The FR system requires extracting features and then classifying the face images based on the feature map. Since the images are modified initially or are noisy due to some factors, the generated feature map is incorrect, which means that there is a vulnerability that attackers can easily exploit.

II. Related Work

This section discusses related works that proposed various FR systems with different methods and scenarios of image sets, including blurry and morphed images. These can enhance security systems against advanced attacks.

Ulrich et al. [14] investigated morphed images and their linked attacks. Morphed images are produced artificially, where the morphed image has some features from a given image and other features from another image. Fig. 7 illustrates the concept of morphed images.

Fig. 7 Morphed images [14].

In Fig. 7, the middle face image is morphed from the image located on the right side and the image located on the left side. The critical problem of morphed images is that those detection algorithms designed for recognizing the face are included in such images' success if the morphed images are manipulated in their digital format. However, the algorithms fail if the morphed images are printed (i.e., used physically). In other words, if we have a face recognition system, it will have the ability to detect morphed facial images in the digital world. However, it cannot do this if the morphed facial images are printed and placed in front of the capturing device. This failure means that the face recognition systems suffer from low resistance against morphed image attacks. To respond to this concern, the authors propose an evaluation system to test the face recognition algorithms against morphing attacks. The system consists of three parts: two databases and the algorithms involved in the testing process. The first database includes facial images scanned after the morphing generation process, while the second database is created based on flatbed scanned images. The results showed that most face detection algorithms suffer from morphing attacks. The advantage of this work is that it highlights the danger of morphing attacks when dealing with sensitive systems. In contrast, this work's disadvantage is related to paying little attention to the performance aspect of the tested algorithms under the threat of a morphing attack.

[17] addressed the low performance and high complexity of facial recognition systems that use deep learning in their construction. The main reason for the low performance and high complexity is the density of the features extracted from the images. This density is represented by the dense branches in the decision tree

(referred to as the overfitting problem), which increases the training time, especially when implementing the training stage on machines equipped only with a central processing unit (CPU). The researchers propose a face recognition system depending on CNN in this work. To solve the low performance, the authors used a machine equipped with graphical processing units (GPUs). The proposed intelligent grid network comprises nine convolution layers, pooling, and classification. In the process of classification, the softmax activation function is used. The softmax function is linked with two fully connected layers to stack features (i.e., reducing the number of features). Caffe, a deep learning framework, is employed in the training and testing phases. The ORL dataset, a public dataset of 400 images, is used to train the CNN, while the AR dataset, a public face database, is used for the testing stage. The presented face recognition system achieves a 99.82% level of accuracy. The advantage of this research is the high performance due to less time consumption during the training stage. However, the system was not tested against noisy and morphed facial images caused by environmental conditions.

[18] handled some issues in the face recognition field that form obstacles against actual application. The issues are related to the limitations of the face recognition-based systems for noisy faces, the size of the face images, and the different luminance levels. Such issues lead to a low level of recognition accuracy. Therefore, the authors proposed an intelligent system that uses CNN to classify facial images in response to these issues. In depth, the CNN-based system has four main steps. The first step is data specification. Then, the people located in a given scene are determined. In addition, the images of people are taken from different directions.

The second step is face detection. The area of the face is isolated from the person's body. The third step is face augmentation. The facial image is manipulated to generate five instances. The generation process depends on adding different levels of noise. The last step is face recognition, which enables the classification of the input images. The softmax function is used in the classification process since there are more than two classes. The dataset used for training and testing includes 300 images captured from various angles. The proposed system achieves 98% accuracy. The advantage of this work is that the proposed system can effectively deal with noisy facial images, which fits reality. However, the system suffers from an extended processing time and the inability to recognize faces that hold masks.

[19] stated that the primary reason behind the limitation in using face recognition systems is the following: (1) low accuracy of the classification process in real-time applications, (2) changes in people's faces due to different feelings, (3) various levels in the lighting environment, and (4) long processing time. A strategy of three steps is utilized to enhance accuracy. The first step is preprocessing, which creates a hybrid dataset called the T-dataset. This new dataset contains different images of the same person under different lighting and expression effects. Then, the correlation images are trained to generate the T-dataset. In other words, for a given face image for a specific person, the correlation (or similarity) between this image and other images in the training dataset is calculated. Then, based on the correlation, the most similar images are processed to produce a series of images for the person. The local binary pattern histogram (LBPH) method is used in the second step. This method is responsible for feature extraction and reduction in dimensionality (reduction in the number of extracted features). This method divides the face image into a net of cells for feature extraction. Then, the patterns are defined, such as an eyebrow. After defining the patterns, the histogram is generated for each pattern and the features are extracted. For reduced features, the patterns located in the cells that do not contribute to face recognition are filtered, such as hair and neck. The third step is classification, and here, the K-nearest neighbor technique is used. The dataset is called YALE and AT&T. In terms of accuracy, the system achieves 95.71%. The advantage of this system is the low processing time due to the dimensionality reduction included in the second step. However, the disadvantage of this work is related to not testing the system using different feature extraction methods, such as CNN and SIFT.

III. Proposed Model

The proposed model presented in this work consists of six steps, starting with selecting the suitable database for training the CNN model and evaluating the constructed model's accuracy during the testing phase. Fig. 8 shows the six steps in detail.

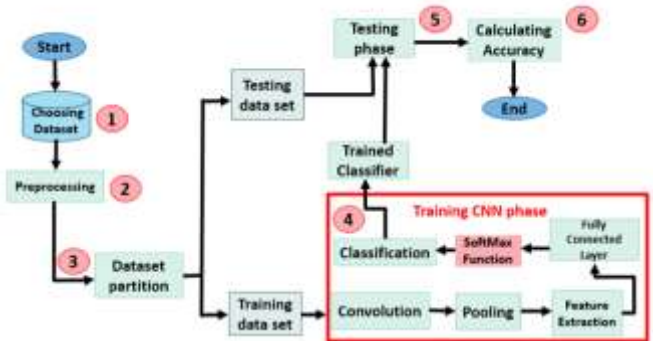

Fig. 8 Proposed model.

3.1 Dataset used

The Georgia Tech Face dataset is used[20]. It is described in terms of the number of images, size of image, colors, and other features in Table no 2.

Table no 2:Description of the dataset used.

Number of images	Mechanism of collecting images	Location of collation	Size of images	Type of images	Number of owners	Size of dataset
750	Using Center for Signal and Image Processing	Web	150 × 150 pixels	JPEG	50	15.9MB

It is worth mentioning that there are no conditions under which the facial images are captured in the Georgia Tech Face. Fig. 9 shows a 6-image sample from the Georgia Tech Face dataset.
As shown in Fig. 9, the facial images are captured from different angles. In addition, there are some artificial effects related to the background, such as the first image in the second row. Moreover, some images are unclear, such as the second image in the first row and the last image in the second row. All of these issues require a preprocessing step.

Fig. 9A sample from the Georgia Tech Face dataset.

3.2 Preprocessing

The objective of this step is to obtain high-quality facial images. From the input and output points of view, the preprocessing step takes a facial image as an input and generates only the region of interest with high quality. Fig. 10 shows the input and output of the preprocessing step.

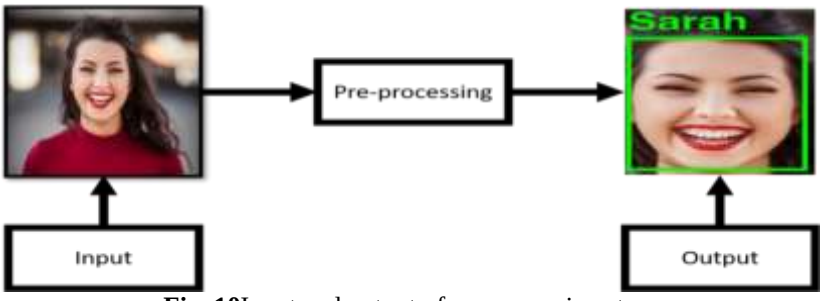

Fig. 10 Input and output of preprocessing step.

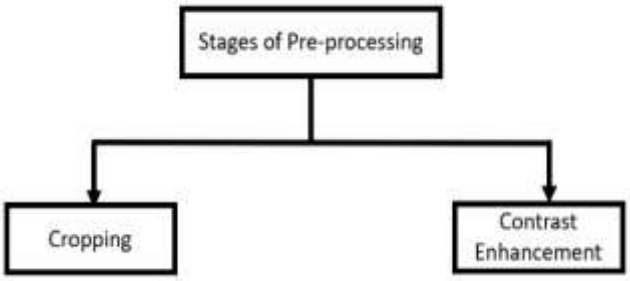

Fig. 11 The two stages of preprocessing step.

There are two main stages in the preprocessing step, as shown in Fig. 11. The cropping stage is required because the facial images have undesirable objects in addition to the region of interest. For instance, the image illustrated in Fig. 12 highlights the unwanted objects. A green rectangle surrounds the region of interest. This image has four unwanted objects: shoulders, body, books, packs, and a cupboard. These unwanted objects should be removed because they are not used for determining the person's identity.

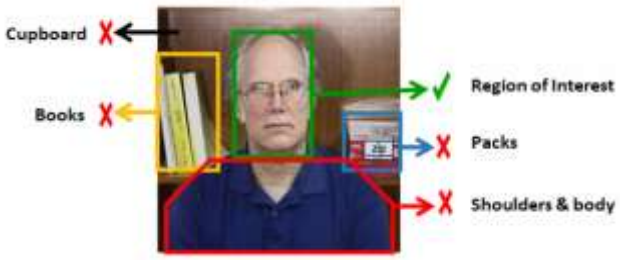

Fig. 12 Unwanted objects and the region of interest for a given facial image.

After isolating the region of interest, it is better to ensure its quality. The reason behind this is related to enhancing face recognition accuracy. Therefore, contrast enhancement is used in this work to improve accuracy. The work analyzes and discusses many contrast enhancement methods from [21]. All of the methods are based on histogram equalization. Three of the methods are the most appropriate for the proposed model, as shown in Fig. 13.

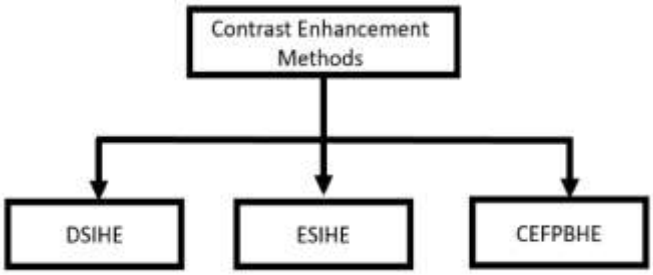

Fig. 13 Contrast enhancement methods depending on histogram equalization.

Dualistic subimage histogram equalization (DSIHE): This uses the probability distribution function for histogram separation (HS). This function is the replacement of the mean value of the image. In other words, it operates on the pixel level for enhancement [22].

Exposure-based subimage histogram equalization (ESIHE): In this method, image equalization is achieved by using the histogram as two parts by assuming an exposure value as a threshold [23]. Then, histogram clipping is executed on bins of the histogram with the assistance of the mean value of the intensity occurrences to control the enhancement. This clipping means that other neighboring pixels contribute to the enhancement; therefore, the enhancement quality is not insensitively focused.

Contrast enhancement using feature preservation bihistogram equalization (CEFPBHE): This method operates in two main phases. To increase the contrast and preserve the image features, the histogram was modified to have a uniform distribution. Then, gamma transformation is utilized to control the histogram spikes, which causes overenhancement[24]. In other words, an external function (or effects) is used, leading to enhanced contrast in a limited range due to involving an external function from outside the manipulated images.

From a visual point of view, Fig. 14 shows the effect of the three methods in terms of quality and clarity.

Fig. 14 Impact comparison of the three contrast enhancement methods [21].

3.3 Dataset Division

In this step, the facial image dataset is divided into two subgroups. One is used for training, and the second is used for testing. Decomposing relies on allocating 80% of the original dataset for training and 20% for testing. Since the total number of facial images is 780, 624 are used for training, and 156 are used for testing.

3.4 Training phase

The training dataset is used for training the CNN. The name of the CNN that is used in this work is Alexie. The training process includes two main stages: convolutional procedure and pooling. The convolution scans the given facial image using filters. The convolutional output is partial features related to the faces (region of interest). The pooling collects the partial features in one container to form all features representing the region of interest. The pooling output procedure is a vector of extracted features. At the end of this step, a trained classifier is generated and entered the second phase.

3.5 Testing phase

In this step, the trained classifier and the testing dataset are involved in a testing process phase. The testing process measures the classification quality, in other words, how accurately it regards correct predictions.

3.6 System Evaluation

The performance of the proposed system is evaluated using different metrics: accuracy (Equation 1), sensitivity (Equation 2), and error rate (Equation 3). These metrics are inspired by the confusion matrix shown in Fig. 15. The confusion matrix refers to the various cases that may occur with a given classifier, considering the output of the classifier and the actual value. In this context, it can be seen as a practical framework that can recognize records (facial images) of different classes [25]. The confusion matrix has four terms:

- True positives (TP): TP reflects the positive records correctly labeled by the proposed face recognition system (classifier). The true positive face image (TPFI) symbol represents this term in this work.
- True negatives (TN): TN reflects the negative records correctly labeled by the proposed face recognition system (classifier). The true negative face image (TNFI) symbol represents this term in this work.
- False positives (FP): TP reflects the negative records that are incorrectly labeled positive. The false positive face image (FPFI) symbol represents this term in this work.
- False negatives (FN): FN reflects the positive records that are mislabeled negative. The false negative face image (FNFI) symbol represents this term in this work.

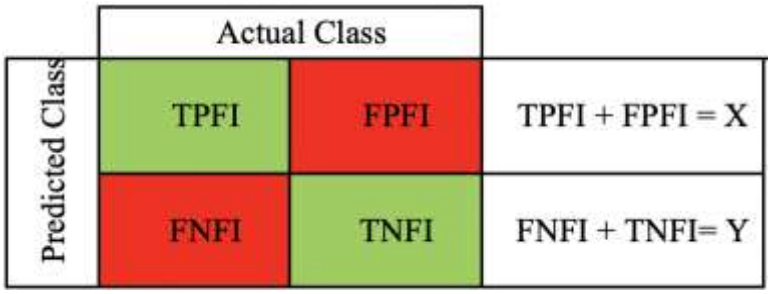

Fig. 15 Confusion matrix structure.

The accuracy can be calculated by:

$$Accuracy = \frac{TPFI + TNFI}{Number\ \ of\ \ all\ \ facial\ \ images\ \ in\ the\ testing\ \ set} \quad (1)$$

The proposed model can be asserted based on the fact that a higher accuracy corresponds to a better classifier output.

$$Sensitivity = \frac{TPFI}{X} \quad (2)$$

The proposed model can also be asserted based on the fact that a higher sensitivity corresponds to a better classifier output.

The error rate is the accuracy opposition and is defined as:

$$Error\ Rate = 1 - accuracy \quad (3)$$

IV. Discussion and Experimental Results

This section presents the experimental results of the proposed deep learning-based recognition model. The experiments were executed on a standard computer (2.00 GHz Intel Core i3 processor and 4 GB RAM). The evaluation strategy used in this work depends on the metrics defined previously to guide the evaluation and the corresponding discussions. For the first metric, accuracy, the proposed face recognition system is evaluated from two aspects: the accuracy of detecting and recognizing faces. Then, for the resistance level against morphing attacks, an artificial dataset is created to test (i.e., calculate the accuracy) the proposed model. Fig. 16 shows the strategy of the proposed system evaluation.

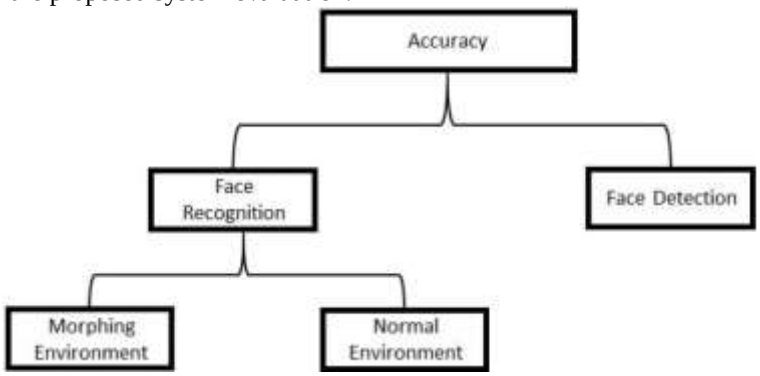

Fig. 16 Strategy of the proposed system evaluation.

4.1 Results of Face Detection and Recognition

Face detection and recognition processes are essential to building facial-based applications. The evaluation of face detection and recognition using the previously discussed measures shows that the proposed model achieved a high detection accuracy of 100%, high recognition accuracy of 99.7%, and sensitivity of 95%. The reviewed studies, presented in the section of the related work, attempted to enhance the processes of face detection and recognition for better facial image classification. One system builds a system based on face detection and recognition to classify face expressions and feelings [17]. The face detection accuracy of the FoF(feeling of face) system is 100%, and its recognition accuracy is 95.7%. Another study proposed a system that addresses noisy faces [18]. Therefore, we refer to it as NoF (noise of face). The face detection accuracy of the NoF System is 100%, and the accuracy of its recognition of nonnoisy images is 98%. A summary of the performance results of the reviewed works is shown in Table no 3.

Table no 3: Face recognition performance of the reviewed studies.

Reference	Accuracy	Error Rate	Sensitivity

FoF [17]	95.7%	4.3%	90%
NoF [18]	98%	2%	93%
Proposed System	99.7%	0.3%	95%

4.1.1 Face Detection

Face detection locates the view within which the face appears in a given image, where other undesirable objects are filtered. The detection accuracy of the proposed system and the reviewed methods (FoF and NoF) is 100%. This is because each system succeeds in locating the faces without any errors. Therefore, the performance is evaluated better in terms of recognition performance.

4.1.2 Face Recognition

As shown in Table no 3, the proposed model is top-ranked with 99.7% accuracy. This performance can be justified by the effective methods used in the preprocessing step, where the quality of the facial images is high, which leads to extracting more accurate features and consequently translates into better training efforts and a higher degree of accuracy.

4.2 Results of face recognition under morphing attacks

For verification purposes and to incorporate measuring the level of resistance against morphing attacks, an artificial dataset is created to test the performance of the proposed system.

We combined the images from several classes to apply the morphology process. For example, we took an image from a class called S36 and another from a different class (S01) and then used the morphing and named the morphed image (s36s01). This process was repeated 29 times. In this way, the attack folder was created, consisting of 30 morphed images, and this folder was added to the gt-DB dataset, which consisted of 50 classes, for a total of 51. Finally, we used the FaceApp application to perform morphing on the photos. This application is commonly used to edit photos and videos with an artificial intelligence mechanism. The following steps explain how to generate morphing facial images using the FaceApp application:

1. Open the application
2. Select a library of images
3. Select a specific image
4. There will be a list of options, where the face swap is the option that is selected
5. There will also be several other options, where the morphing option is selected
6. this step, a new area within the same interface will appear asking to identify the second facial image.
7. Select the second facial image from the library
8. This step triggers the processing step to start the morphing manipulation
9. The final step is to save the resultant facial images in a folder named "attack."

Fig. 17 and Fig. 18 show the steps of generating the morphing faces process using FaceApp. Some outputs of morphed facial images with corresponding original images are shown in Fig. 19.

Fig. 17 The original and the second images were selected using the FaceApp application.

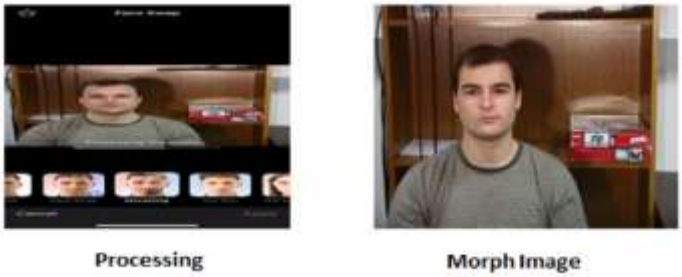

Fig. 18 Processing via the FaceApp application and resulting morphed image.

Fig. 19 Sample of morphed facial images.

The proposed system was evaluated using the generated morphed facial images to test the robustness of the proposed model against morphing attacks. The experiments show that the proposed model achieved an accuracy of 95% for morphing attack detection, an error rate of 5%, and sensitivity of 93%. These results reflect the system's ability to resist morphing attacks. The main reason is related to the proactive layer of enhancing the quality of the facial images before extracting the training features. This process means that the negative effects of the morphing attack are mitigated due to using histogram equalization and contrast enhancement to reveal new effects that refer to them as the morphing attacks.

V. Conclusion

In advanced facial-based attacks, face recognition systems may not recognize individuals. This disadvantage leads to the importance of developing accurate face recognition systems for higher resistance against advanced attacks such as morphing. This work presented a proposed model to build a CNN-based face recognition system. The proposed model employs two techniques to deal with morphing attacks and mitigate their negative impact: histogram equalizations and contrast enhancement. The proposed system was trained on the Georgia Tech Face dataset. The experimental results show high face recognition accuracy and sensitivity compared to FoF and NoF. To test the robustness of the proposed system against morphing attacks, morphed faces were created using a unique tool supported by a mobile application. Then, the proposed system was evaluated using the generated morphed facial images. The results show that the proposed system achieved an accuracy of 95% against morphed images.

References

[1]. X. Sun, P. Wu, and S. C. Hoi, "Face detection using deep learning: Animproved faster rcnn approach," Neurocomputing, vol. 299, pp. 42–50, 2018.
[2]. G. Guo and N. Zhang, "A survey on deep learning based face recognition,"Computer vision and image understanding, vol. 189, p. 102805, 2019.
[3]. N. Dey, J. Chaki, L. Moraru, S. Fong, and X.-S. Yang, "Firefly algorithm and its variants in digital image processing: A comprehensive review,"Applications of firefly algorithm and its variants, pp. 1–28, 2020.
[4]. L. Rice, E. Wong, and Z. Kolter, "Overfitting in adversarially robust deep learning," in International Conference on Machine Learning. PMLR, 2020, pp. 8093–8104.
[5]. A. Rot and B. Olszewski, "Advanced persistent threats attacks in cyberspace. threats, vulnerabilities, methods of protection." in FedCSIS (Position Papers), 2017, pp. 113–117.
[6]. P. Tome, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Facial soft biometric features for forensic face recognition," Forensic science international, vol. 257, pp. 271–284, 2015.
[7]. E. Kremic, A. Subasi, and K. Hajdarevic, "Face recognition implementation for client server mobile application using pca," in Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces. IEEE, 2012, pp. 435–440.
[8]. Spivak, S. Krepych, V. Faifura, and S. Spivak, "Methods and tools of face recognition for the marketing decision making," in 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Scienceand Technology (PIC S&T). IEEE, 2019, pp. 212–216.
[9]. Y. Zhao, S. Wu, L. Reynolds, and S. Azenkot, "A face recognition application for people with visual impairments: Understanding use beyond the lab," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–14.

[10]. M. I. Razzak, S. Naz, and A. Zaib, "Deep learning for medical image processing: Overview, challenges and the future," Classification in BioApps, pp. 323–350, 2018.
[11]. G. M. Zafaruddin and H. Fadewar, "Face recognition using eigenfaces,"in Computing, communication and signal processing. Springer, 2019, pp.855–864.
[12]. S. Zhou and S. Xiao, "3d face recognition: a survey," Human-centric Computing and Information Sciences, vol. 8, no. 1, pp. 1–27, 2018.
[13]. F. G. De Natale and G. Boato, "Detecting morphological filtering of binary images," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1207–1217, 2017.
[14]. U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb,and C. Busch, "On the vulnerability of face recognition systems towardsmorphed face attacks," in 2017 5th International Workshop on Biometricsand Forensics (IWBF). IEEE, 2017, pp. 1–6.
[15]. C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in International Workshop on Digital Watermarking. Springer, 2017, pp. 107–120.
[16]. H. Ben Fredj, S. Bouguezzi, and C. Souani, "Face recognition in unconstrained environment with cnn," The Visual Computer, vol. 37, no. 2, pp.217–226, 2021.
[17]. K. Yan, S. Huang, Y. Song, W. Liu, and N. Fan, "Face recognition based on convolution neural network," in 2017 36th Chinese Control Conference (CCC). IEEE, 2017, pp. 4077–4081.
[18]. M. Zulfiqar, F. Syed, M. J. Khan, and K. Khurshid, "Deep face recognition for biometric authentication," in 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE, 2019, pp. 1–6.
[19]. M. A. Abuzneid and A. Mahmood, "Enhanced human face recognition using lbph descriptor, multi-knn, and back-propagation neural network," IEEE access, vol. 6, pp. 20 641–20 651, 2018.
[20]. "Georgia tech face database." [Online]. Available: https://computervisiononline.com/dataset/1105138700
[21]. D. Vijayalakshmi, M. K. Nath, and O. P. Acharya, "A comprehensive survey on image contrast enhancement techniques in spatial domain," Sensing and Imaging, vol. 21, no. 1, pp. 1–40, 2020.
[22]. Y. Wang, Q. Chen, and B. Zhang, "Image enhancement based on equal area dualistic sub-image histogram equalization method," IEEE transactions on Consumer Electronics, vol. 45, no. 1, pp. 68–75, 1999.
[23]. K. Singh and R. Kapoor, "Image enhancement using exposure based subimage histogram equalization," Pattern Recognition Letters, vol. 36, pp.10–14, 2014.
[24]. X. Wang and L. Chen, "Contrast enhancement using feature-preserving bi-histogram equalization," Signal, Image and Video Processing, vol. 12, no. 4, pp. 685–692, 2018.
[25]. A. Luque, A. Carrasco, A. Martín, and A. de Las Heras, "The impact of class imbalance in classification performance metrics based on the binary confusion matrix," Pattern Recognition, vol. 91, pp. 216–231, 2019.

Kholoud Albalawi, et. al. "A Robust Face Recognition Model against Morphing Attacks using CNN." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 24(4), 2022, pp. 27-38.