Face Morphing Attack Detection in the Presence of Post-processed Image Sources Using Neighborhood Component Analysis and Decision Tree Classifier

Ogbuka Mary Kenneth(✉), Sulaimon Adebayo Bashir, Opeyemi Aderiike Abisoye, and Abdulmalik Danlami Mohammed

Department of Computer Science, Federal University of Technology, Minna, Nigeria
kenneth.pg918157@st.futminna.edu.ng, {bashirsulaimon, o.a.abisoye,drmalik}@futminna.edu.ng

Abstract. Recently, Face Morphing Attack Detection (MAD) has gained a great deal of attention as criminals have started to use freely and easily available digital manipulation techniques to combine two or more subject facial images to create a new facial image that can be viewed as an accurate image of any of the individual images that constitute it. Some of these morphing tools create morphed images of high quality which pose a serious threat to existing Face Recognition Systems (FRS). In the literatures, it has been identified that FRS is vulnerable to multiform morphing attacks. Based on this vulnerability, several types of research on the detection of this morph attack was conducted using several techniques. Despite the remarkable levels of MAD reported in various literature, so far no suitable solution has been found to handle post-processed images such as images modified after morphing with sharpening operation that can dramatically reduce visible artifacts of morphed photos. In this work, an approach is proposed for MAD before image post-processing and after image post-processing built on a combination of Local Binary Pattern (LBP) for extraction of feature, Neighborhood Component Analysis (NCA) for selection of features and classification using K-Nearest Neighbor (KNN), Decision Tree Classifier (DTC) and Naïve Bayes (NB) classifier. The outcome gotten by training the different classifiers with feature vectors selected using the NCA algorithm improved the classification accuracy from 90% to 94%, consequently improving the general performance of the MAD.

Keywords: Face morphing · Morphing Attack Detection · Post-processing · Sharpening · Bona fide images · Machine learning

1 Introduction

Biometric features are unique characteristics of an individual that can be used for authentication, identification, and access control across a series of contexts including driving license, smartphone unlocking, border control, forensic identification, national identity card, voter's card, and several other identifications [1]. Authentication and recognition

S. Misra and B. Muhammad-Bello (Eds.): ICTA 2020, CCIS 1350, pp. 340–354, 2021.
https://doi.org/10.1007/978-3-030-69143-1_27

are based on biometric characteristics such as fingerprint, iris, speech, and facial features. Face features are commonly used among these different characteristics because of the uninterrupted idea of the capture procedure and the client comfort involved [2]. Photographs of the face are provided in different types of documentation universally, with driving licenses and passports included. However facial identification systems have recently been identified as defenseless against attacks based on morphed facial images [3]. Studies by Scherhag et al. [4] and Ferrara, Franco and Maltoni [5] showed that electronic passports are particularly sensitive to morphing attacks, especially when the face photograph published on paper and presented by an individual has been manipulated. Face morphing is defined as a technique of image manipulation, where two or more faces of subjects are blended to form a single face in the image [6, 7]. Morphed images may look exactly like all the contributing subjects that make up the image. As a result, a morphed image can be used as an identity credential by multiple, if not all of the individual facial images comprising the morphed image [5, 8]. For a morph attack to be effective, the morphed face image has to be identical to any of the multiple subjects particularly the person requesting the electronic passport, this is important to fool the officials in the issuing process, however, the morphed image must at the same time comprise sufficient characteristics of the concealed subject to allow optimistic authentication at the ABC gate for both/multiple individuals [5].

Morph images may be used to mislead human beings [9], and existing facial recognition systems [10]. This has made the latest identity verification processes insecure, such as those used in automatic border control gates (ABC) [6]. In a typical situation of face morphing attack (MA), if the partner applies for an electronic passport with the transformed face image, a criminal on the run could morph his/her passport with one of the lookalike partners, he/she will get a legal e-passport incorporated with matching security features of the document. With this, the companion as well as the suspect could be checked against the warped picture held in the e-passport with success. This scenario shows that the suspect can use the e-passport to successfully cross the ABC gates [8].

Different researches have been carried out for MAD. Research conducted by Ramachandra [2], Seibold et al. [11], Wandzik, Kaeding and Garcia [12], and Jassim and Asaad [13] have achieved remarkable detection rates, but these results are barely applicable to post-processed images such as image compression [14] and post-morphing image sharpening, which can significantly reduce noticeable artifacts from the morphing process, making the previous algorithms less effective. However some existing research works on MAD considered MAD on post-processed images. The post-processing operations considered in existing research works are print-scan [5], image resizing, and image compression [7], but image sharpening as a post-processing operation have not been considered. Image sharpening is a very common post-processing image operation. It is important to automatically detect this face morphing attack even after the morphed images are post-processed using the image sharpening operation.

Along these lines, we propose an approach to detect face morphing attacks even after image post-processing using a combination of Local Binary Pattern (LBP) technique for extraction of features, NCA for feature selection, and DTC, KNN, and NB for classification. Hence, the fundamental contributions of this paper include:

1. Presentation of a method for detecting post-processed morphed images which are more hardened to detection compared to ordinary morphed images.
2. Introduction of a post-processed morphed image dataset that is created from our generated ordinary morphed images. The dataset is composed in a way to eliminate bias.
3. Comparative experimentation of different classifiers on the features obtained from the proposed approach.

The rest of this paper is organized as follows: Sect. 2 offers a summary of recent MAD works. The methodology used for conducting the study is outlined in Sect. 3. Section 4 describes the findings obtained during the experiment and addresses the results presented. Conclusions were drawn in Sect. 5, and Sect. 6 presents future works.

2 Related Work

A variety of methods suggested in recent years for detecting MAD is loosely categorized into two major classes [15]: the single image-based (given a single image identity, it is either categorized as bona-fide or morph) and the differential image-based (manages the correlation between a live picture and that stored on the e-archive). The vast majority of the literature belong to the single category of images.

Ramachandra et al. [2] proposed another methodology of recognizing face morphing attack dependent on removing scale-space highlights utilizing the Steerable pyramid, which is generally a set of oriented filters that are produced as a linear grouping of an elementary function. These separated features were sorted utilizing a collaborative representation classifier. The proposed algorithm achieved a Bona fide Presentation Classification Error (BPCER) of 13:12% at an Attack Presentation Classification Error Rate (APCER) of 10%. Furthermore, the suggested strategy was utilized to detect MA even after the print-scan procedure has been performed. However, this proposed algorithm did not consider other image post-processing tasks such as image sharpening, compression, contrast enhancement, and blurring.

Scherhag et al. [3] developed a MAD method founded on the Non-Uniformity Photo Response (PRNU) analysis. The spectral and spatial features mined from the PRNU designs across picture cells were inspected. In the threshold selection point, the dissimilarities between the features of morphed images and bona fide were measured via the Dresden image database, which is precisely constructed for the PRNU examination in digital image forensics. The algorithm proposed was robust as MAD was performed on morphed images created using various morphing tools that represent a typical real-life scenario. However picture post-processing tasks, for example, contrast enhancement, sharpening, or blurring, can seriously influence the PRNU features which can thoroughly lessen the proficiency of a PRNU-based MAD system [16].

The profound neural system as viable feature extraction and classification procedure in machine learning was embraced by Raghavendra et al. [17] for MAD. The proposed method exploited transferrable features acquired from a pre-trained Convolutional Neural Network (CNN) to execute MAD for both print-scan and digital morphed pictures. Two CNN strategies which are VGG19 and AlexNet were utilized to carry out the feature

mining task. The image features were extracted separately from the first fully connected layers of both the AlexNet and VGG19 model and these features were joined to produce a single feature vector using the feature level fusion method. Anyway, the proposed method accomplish a superior exhibition result for digital images with an equal error rate of 8.223% when contrasted with the print-scan pictures with an equal error rate of 12.47%.

Topology data analysis (TDA) as an advancing structure for investigation of big data was adopted by Jassim and Asaad [13] for MAD. For each image, a series of simplex complexes were fabricated, whose vertices are the assigned set of landmarks, for a series of distance thresholds. The assorted variety of topological invariants was utilized to separate the regular face pictures from the morphed ones. The proposed method achieved high accuracy for MAD on digital images but performed poorly on print and scan images. After performing feature concatenation the single feature vector was feed to a collaborative representation classifier for final classification.

Singh et al. [18] performed MAD using the decomposed 3d shape and diffuse reflectance. This method was proposed as it can detect MA in the incidence of posture, print-scan, and lighting artifacts. In this technique, the genuine image taken at the ABC gate and the face image mined from the electronic Machine Readable Travel Document (eMTRD) are disintegrated into a quantized ordinary guide and diffuse remake image. These extracted structures are then used for training linear SVM for MAD founded on the evaluation of the dissimilarities between the bona fide image taken at the ABC gate and the face image mined from the eMTRD. The impediment of this paper is that the proposed algorithm did not consider picture post-processing tasks, for example, the print-scan operation, image compression, contrast enhancement, sharpening, and blurring.

Wandzik, Kaeding and Garcia [12] addresses the issue of MAD utilizing facial recognition techniques dependent on Convolutional Neural Networks (CNN) and hand-crafted features. Four feature extraction algorithms were used to mine the facial features and these algorithms include faceNet, Dlib, and VGG-Face and one shallow learning approach dependent on High- Dim Local binary pattern. After performing feature extraction using any of the feature extraction algorithms, the output feature vectors were used to calculate the Euclidean distance for the face verification task. The reference image vectors were supplied to the support vector machine (SVM) to perform binary classification for MAD. This work can be utilized to perform both face verification and MAD. However, this work only considered MAD of digital images without considering the print and scanned images which are used for verification in some countries.

3 Methodology

This section includes an overview of the techniques used in performing this study. The proposed solution is shown in Fig. 1, and this solution is discussed in detail in this section. These methods include data collection, post-processing, pre-processing, extraction of features, selection of features, classification, and finally the decision (bona fide or morphed).

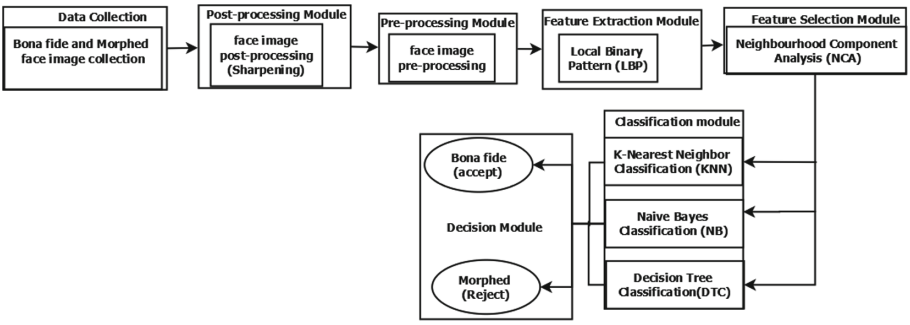

Fig. 1. Proposed approach

3.1 Data Collection

In this study, a new morphed face database comprising of 300 morphed images was produced using different facial images from 100 subjects. To diversify the database, the face pictures utilized contains male and female of both white and dark skin people. The subject pictures were gathered from different online databases, for example, the Yale face database, surveillance cameras face database, and also some arbitrarily looked through online face pictures were utilized.

The morphed face pictures were produced utilizing two morphing apparatuses which are:

1. **Magic morph tool:** This is an elite transforming and wrapping software. It is anything but difficult to utilize, and it delivers top-notch transformed pictures. It utilizes a multithread pyramid calculation.
2. **FantaMorph tool:** This is a transforming software utilized for making a photograph transform and modern transform activity impacts. It helps users to consequently find facial highlights, for example, the nose, eye, and mouth. And consolidates these highlights of various genuine countenances to create a virtual face.

The face pictures were manually adjusted and merged to shroud the transformed antique. The morphing software creates a progression of picture outlines showing the transition of one subject to another. The last transformed image is picked manually by underwriting its similarity to the faces of the contributing subjects to the transforming procedure. Henceforth the made transforms are of high caliber and are low to no recognizable artifacts.

3.2 Post-processing (Image Sharpening)

The images used in identity credentials can go through several processing operations before been embedded into e-visa. A post-processed morphed image loses some of its artifacts which makes MAD of such images troublesome. A typical image post-processing technique is picture sharpening and compression. Image sharpening activity is usually utilized as an image post-processing activity since human perception is

incredibly touchy to edges and fine subtleties of a picture and since pictures are made up predominantly of high-frequency segments, the graphic quality can be decreased if the high frequencies are distorted. Improvement of the high-frequency segments of a picture leads to an upgrade in the image graphic quality. Hence sharpening of morphed images can highlight edges and adjust subtleties in the picture which can likewise modify the morph highlights making such a picture hard to detect. Image sharpening operation was identified by Scherhag [8] as one challenge faced in MAD. Hence image sharpening was performed on the morphed images to hardened their detection and elicit the effectiveness of the proposed MAD method even after performing post-processing operation for enhancement of the morphed images.

3.3 Face Pre-processing

In the image pre-processing phase facial landmarks detection was carried out. Facial landmarks are used to confine and signify noticeable areas of the face, for example, nose, eyes, mouth, eyebrows, and jawline [19]. Identification of facial landmarks involves the following steps:

- **Step 1:** Localize the object of interest (face in the image).
- **Step 2:** Recognize the principle facial characteristics on the face region of interest.

In this work, the Viola-Jones algorithm was embraced for face feature discovery. Viola-Jones algorithm was applied because of its exceptionally high discovery rate, and its functional application. The Viola-Jones calculation utilizes the Haar-basis filters, which is a scalar item amid the picture and some Haar-like layouts [20]. This algorithm has four phases for face recognition which are: Haar feature selection, an indispensable image selection, Adaboost training, and cascading classifier. The indispensable image is a method for the operational generation of the sum of pixel concentrations in a stated rectangle in an image.

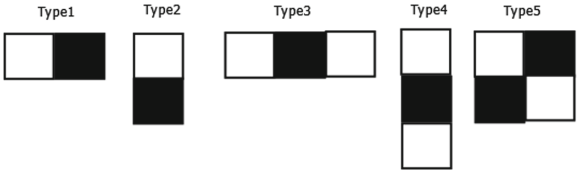

Fig. 2. Haar features in Viola Jones

The Haar features in Fig. 2 have various width and height. In Fig. 2 it can be seen that the image is represented with either black or white pixels and the summation of white pixel and summation of the black pixel are gotten and then deducted to get a lone value. If this calculated value is more in that region, then it signifies a part of the face and is recognized as nose, eyes, mouth, etc. Ada boost diminishes redundant features by determining the significant features and insignificant features. Subsequently, after the identification of the significant features and the insignificant features the Ada boost

allocates weight to all of them. And hence generate robust classifiers as a linear grouping of feeble classifiers. Nearly 2500 features are calculated [21]. Hence cascading is used to reduce the number of computations. The features are retained in an additional set of classifiers in a cascading format, to aid it to discover if it is a face or not in a faster time.

After the facial landmarks were detected the face images were cropped to a size of 130 by 130 pixels based on the detected landmarks to ensure that the MAD algorithm is only used on the facial region. Lastly, the cropped face image is transformed into a gray-scale image.

3.4 Feature Extraction

Image features, like edges and points of interest, contain rich data about the content of an image. In an image, features correspond to local regions and are vital in several image analysis application domains such as identification, matching, and reconstruction. These image features can be extracted using several feature extraction techniques. Feature extraction defines the specific shape details found in an image such that a structured procedure makes the task of classifying the image simple.

In this study, feature extraction was performed on the pre-processed images (bona fide and morphed) using the Local Binary Pattern (LBP) technique. The LBP was used as a feature extractor as it has proved to extract very high-quality features that improve the accuracy of classification [22]. Texture features are responsible for the measure of properties such as regularity, coarseness, and smoothness [23]. LBP is an active texture feature descriptor for images that threshold the surrounding pixels based on the current pixel value. The histogram of LBP labels summed over an image is used as a descriptor of that image's texture [27]. Given a neighborhood of Q sample points on a circle of radius of R. And given a pixel at (x_c, y_c). LBP is expressed in Eq. 1 below:

$$\mathrm{LBP}_{Q,\mathrm{R}(x_c,y_c)} = \sum_{\mathrm{Q}=0}^{\mathrm{Q}-1} \mathrm{u}\left(i_Q - i_c\right)2^Q \tag{1}$$

where i_c and i_Q are, correspondingly, gray-level values of the dominant pixel and Q neighboring pixels in the circle region with a radius R, and function u(x) is defined in Eq. 2 as:

$$\mathrm{u}(x) = \begin{cases} 1 \text{ if } x \geq 0 \\ 0 \text{ if } x < 0 \end{cases} \tag{2}$$

The LBP was used as the feature descriptor because it is anticipated that the image morphing process will lead to a change in the textual properties of morphed images which will make it a useful function for differentiating between morph and bona fide images.

3.5 Feature Selection

Feature selection was performed on the extracted LBP image features. The NCA was utilized to perform the feature selection operation. The NCA is a non-parametric algorithm for choosing features with the point of augmenting forecast accuracy of classification

systems. NCA learns a component weighting vector by augmenting the likely leave one out classification accuracy with a regularization term. A key advantage of NCA as distinguished by Yang, Wang and Zuo [25], is that it is commonly unaffected by the rise in the number of insignificant features and it does superior to most feature selection approaches in most cases. Hence feature selection was performed to improve the classification accuracy. The working of NCA is described below.

Given that A = {(x1,y1),…,(xi,yi),…,(xN,yN)} is a collection of training examples, where xi is a feature vector, yi is the matching label and N is a number of examples. The weighting vector w that chooses the feature subset is given in Eq. 3:

$$V_w(x_i, x_j) = \sum_{l=1}^{d} w_l^2 |x_{il} - x_{jl}| \tag{3}$$

Where $V_w(x_i, x_j)$ is the weighted distance between two examples x_j and x_i. To succeed in nearest neighbor classification, an inherent and active approach is to make the most of its leave-one-out CA on the training examples A. hence the likelihood of x_i selecting x_j as its reference point is given in Eq. 4.

$$p_{ij} = \begin{cases} \dfrac{B(V(x_i, x_j))}{\sum_{B \neq 1} B(V_w(x_i, x_B))}, & \text{if } i \neq j \\ 0, & \text{if } i = j \end{cases} \tag{4}$$

Where $B(z) = \exp(-z/\sigma)$ is a kernel function and the kernel width σ is an input parameter that impacts the likelihood of the respective points being chosen as the reference point. From the formula above the likelihood of the query point xi being properly grouped is presented in Eq. 5:

$$p_i = \sum_j y_{ij} p_{ij} \tag{5}$$

Where $y_{ij} = 1$ if and only if $y_i = y_j$ and $y_{ij} = 0$ otherwise. Hence, the estimated leave-one-out accuracy is presented in Eq. 6:

$$\xi(v) = \frac{1}{N} \sum_i p_i = \frac{1}{N} \sum_i \sum_j y_{ij} p_{ij} \tag{6}$$

Where $\xi(v)$ is the true leave-one-out CA. To implement feature selection and ease over-fitting, regularization is introduced which is given in Eq. 7:

$$\xi(v) = \sum_i p_i - \lambda \sum_{i=1}^{d} w_l^2 \tag{7}$$

Where $\lambda > 0$ is a regularization parameter that is tuned through cross-validation. Since $\xi(v)$ is differentiable the resultant derivative is given in Eq. 8:

$$\frac{\partial \xi(v)}{\partial v_l} = 2\left(\frac{1}{\sigma} \sum_i \left(p_i \sum_{j \neq i} p_{ij} |x_{il} - x_{jl}| - \sum_j y_{ij} p_{ij} |x_{il} - x_{jl}|\right) - \lambda\right) v_l \tag{8}$$

Hence the formula in Eq. 8 represents the NCA for feature selection.

3.6 Image Classification

The last phase of the proposed system is the classification stage. The selected features generated from the feature selection stage were feed to three classifiers namely DTC, KNN, and NB. These classifiers were used for the classification of the Images into either bona fide or morphed images.

1. **Decision Tree Classifier (DTC):** A decision tree is a simple and commonly used predictive modeling technique. This is a type of supervised learning where the data is continuously divided according to a certain parameter. The decision tree is represented in a tree-like structure, in this tree structure leaves denote labels and branches signify combinations of features that produce the class labels. DTC is easy to understand and interpret, does not require normalization or scaling of data and it involves less work for data preparation.
2. **K-Nearest Neighbor (KNN):** KNN is a non-parametric algorithm applied to solve regression and classification problems. In KNN an object is grouped by the majority vote of its neighbors, with an object being distributed to a class most common among its k-nearest neighbor. KNN requires no training step, it is easy to understand and implement and can be used for both regression and classification problems. However KNN suffers from the curse of dimensionality, it requires homogeneous features and KNN is sensitive to outliers.
3. **Naïve Bayes (NB):** NB classifier is a probabilistic machine learning model centered on using Bayes theorem with high independence assumptions between the features and it is used for the classification task. NB is also easy to implement and the training period is less as it requires a small amount of data to estimate the test data. However, the main limitation of NB is the assumption of independent predictors.

3.7 Performance Metrics

The proposed technique performance was estimated utilizing the following assessment measurements.

1. **False Acceptance Rate (FAR):** is identical to the APCER. It is described as a relative amount of MA classified as genuine images [2]. The formula is given in Eq. 9:

$$\text{FAR} = \text{False positive}/(\text{True Positive} + \text{False Positive}) \tag{9}$$

2. **False Rejection Rate (FRR):** this is identical to the BPCER. FRR is described as the ratio of bona fide presentations inaccurately categorized as presentation attacks in a particular situation or as the comparative quantity of genuine images categorized as MA [13]. The FRR formula is given in Eq. 10 as:

$$\text{FRR} = \text{False Negative}/(\text{True Positive} + \text{False Negative}) \tag{10}$$

3. **Accuracy (ACC):** is a metric used for the evaluation of classification models. Accuracy can simply be defined as the degree of accurate classifications either for an independent test set or using some deviation of the cross-validation idea. The formula is given in Eq. 11 as:

$$\text{ACC} = \frac{\text{True Positive} + \text{True negative}}{\text{True Positive} + \text{True negative} + \text{False Positive} + \text{False negative}} \tag{11}$$

4 Results and Discussion

In this work, experiments were conducted on three algorithms which are DTC, KNN, and NB classifiers for post-processed images (image sharpening) and NCA feature selection algorithm. Four types of experiments were carried out which are:

1. Classification of non-post-processed images (bona fide and morphed) using feature vectors selected based on the NCA algorithm.
2. Classification of non-post-processed images (bona fide and morphed) without application of the NCA feature selection algorithm.
3. Classification of post-processed images (bona fide and morphed) without application of the NCA feature selection algorithm.
4. Classification of post-processed images (bona fide and morphed) using feature vectors selected based on the NCA algorithm.

The results of the four experiments conducted using the three aforementioned classification techniques are shown in Table 1.

Table 1. MAD classification result

	Non-post-processed images			Post-processed images (Sharpening)		
Algorithm	Accuracy (%)	FAR (%)	FRR (%)	Accuracy (%)	FAR (%)	FRR (%)
LBP + NCA + DTC	94	4.8	7.7	85	15.8	14.3
LBP + DTC	90	11.8	7.7	82	10.5	25.0
LBP + NCA + NB	82	23.8	7.7	80	36.8	4.8
LBP + NB	80	29.4	7.7	72	47.4	10.0
LBP + NCA + KNN	77	41.2	0.0	83	21.1	14.3
LBP + KNN	74	28.6	23.1	79	31.6	10.0

From Table 1 above it can be deduced that for the non-post-processed images the decision tree classifier (DTC) trained with NCA selected feature vectors produced the

highest accuracy with a value of 94% as compared to KNN and NB that were also trained with the NCA selected feature vector which produced an accuracy of 77% and 80% respectively. Also for the post-processed images using the NCA selected feature vectors DTC performed better with an accuracy of 85% as compared to NB and KNN with an accuracy of 80% and 83%. Based on the FAR (4.8%) and FRR (7.7%) metric it can be seen that DTC trained with NCA selected feature vector has a very low percentage which is below 10%. This shows that DTC performed better with NCA selected feature vectors as compared to KNN and NB. The accuracy rate is high in LBP + NCA + DTC and low in LBP + NCA + KNN for non-post processed images because the features used in this experimentation were not normalized and KNN is sensitive to the scale of the data while DTC is insensitive to the scale of data [26]. The number of neighbors used can also affect KNN classification accuracy.

From Table 1 is can be seen that DTC gave a higher accuracy when trained with all the extracted feature vectors (i.e. is without performing feature selection with NCA) for both non-post-processed images (bona fide and morphed) and the post-processed images. As compared with the post-processed images it can be deduced that the proposed system was able to perform MAD better on images that were not post-processed as it got an accuracy of 94% while the experiment on post-processed images gave an accuracy of 85%. It can also be seen that LBP + KNN got the least accuracy for non-post-processed images and LBP + NB got the least accuracy rate for post-processed images (sharpening), this is because post-processing reduces the morphing artifact. That is, after applying post-processing operation on the image, the features of the image is been altered to a different set of features, which makes NB and KNN react differently to the non-post processed and the post-processed image features.

From the conducted experiment it can be inferred that training a classifier for MAD using NCA selected feature vectors improves the performance accuracy of the system. With low FAR and FRR and high prediction accuracy, it can be seen that the LBP + NCA + DTC algorithm is suitable for a reliable MAD.

Table 2. MAD classification results for non-post-processed images

Non post-processed images			
Algorithm	Accuracy (%)	FRR (%) @	
		FAR = 5%	FAR = 10%
Proposed method (LBP + NCA + DTC)	**94**	**7.39**	**3.69**
Steerable textures [2]	-	45.76	13.12

Based on the values of FRR and FAR presented in Table 2 it can be seen that LBP + NCA + DTC has indicated the best performance with FRR of 7.39% at FAR = 5% and FRR of 3.69% at FAR = 10%. While the method proposed by Ramachandra et al. [2] has FRR of 45.76% at APCER = 5% and FRR of 13.12% at APCER = 10%.

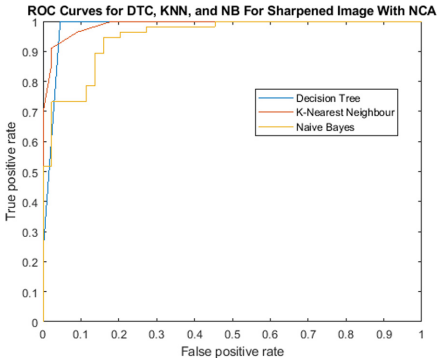

Fig. 3. ROC Curves for DTC, KNN, and NB classifiers trained with NCA selected features of post-processed images.

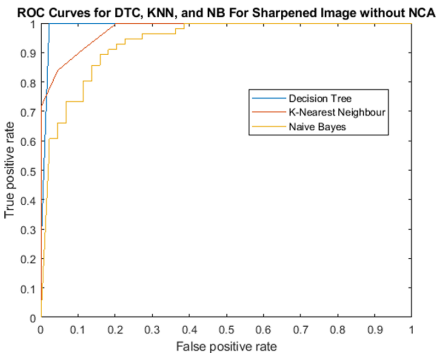

Fig. 4. ROC Curves for DTC, KNN, and NB classifiers trained without NCA selected features of post-processed images.

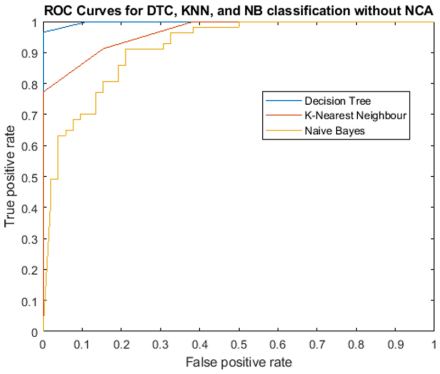

Fig. 5. ROC Curves for DTC, KNN, and NB classifiers trained without NCA selected features of non-post-processed images.

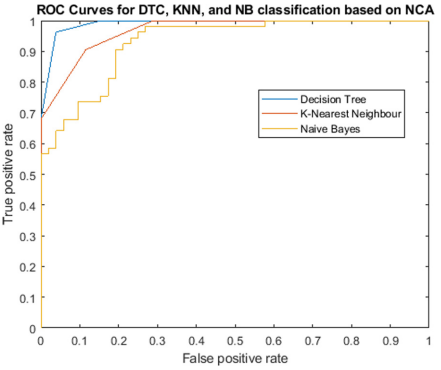

Fig. 6. ROC Curves for DTC, KNN, and NB classifiers trained with NCA selected features of non-post-processed images.

In Fig. 3 the ROC curves of the three classifiers for the post-processed images based on NCA selected feature vectors are shown. Figure 4 shows the ROC curve for the KNN, NB, and DTC classifiers for the post-processed images trained with extracted features without application of the NCA algorithm. Figure 5 presents the ROC curves for the NB, KNN, and DTC classifiers for the images which were not post-processed and trained with the normal features without application NCA algorithm. Figure 6 presents the ROC curve for the three classifiers for the images which were not post-processed based on NCA selected feature vectors. From the ROC curves, it can be seen that the DTC classifier has a higher area under a curve (AUC) value as compared to the other two classifiers KNN and NB which shows that DTC generally has a high performance as compared to KNN and NB.

5 Conclusion

This study was able to perform MAD more robustly as compared to existing research works on MAD. This is due to the ability of the system to detect morphed images even after post-processing operation has been applied to those images. From this study, it can be concluded that the application of the NCA algorithm for feature selection can also improve the classification accuracy. In conclusion, a system was developed which can perform MAD even after the application of sharpening post-processed operations based on the LBP + NCA + DTC algorithm.

6 Future Works

The morphed dataset used for this work was generated using available morphing software as there was no publicly available large-scale database for MAD and most researches have been conducted using different in-house databases. Hence it is recommended that a large-scale publicly available Morph database should be created to make MAD algorithms more reliable and robust. The experiment was conducted on morphed images generated by only two morphing software hence to improve the robustness of MAD several morphing tools should be used to generate morphed datasets. And lastly more common image post-processing tasks such as image compression should be considered. This study was not able to compare the result of the post-processed images with other related works, as current works of literature are focused on print-scan, image compression and image resize post-processing operations and none focused on image sharpening as a post-processing operation. Hence it is recommended that more work should be done on MAD on images post-processed with image sharpening using different algorithms.

References

1. Kramer, R.S.S., Mireku, M.O., Flack, T.R., Ritchie, K.L.: Face morphing attacks: investigating detection with humans and computers. Cogn. Res. Principles Implications **4**(1), 1–15 (2019). https://doi.org/10.1186/s41235-019-0181-4
2. Ramachandra, R., Venkatesh, S., Raja, K., Busch, C.: Detecting face morphing attacks with collaborative representation of steerable features. In: Chaudhuri, B.B., Nakagawa, M., Khanna, P., Kumar, S. (eds.) Proceedings of 3rd International Conference on Computer Vision and Image Processing. AISC, vol. 1022, pp. 255–265. Springer, Singapore (2020). https://doi.org/10.1007/978-981-32-9088-4_22
3. Scherhag, U., Debiasi, L., Rathgeb, C., Busch, C., Uhl, A.: Detection of face morphing attacks based on PRNU analysis. IEEE Trans. Biom. Behav. Identity Sci. **1**(4), 302–317 (2019). https://doi.org/10.1109/TBIOM.2019.2942395
4. Scherhag, U., Budhrani, D., Gomez-Barrero, M., Busch, C.: Detecting morphed face images using facial landmarks. In: Mansouri, A., El Moataz, A., Nouboud, F., Mammass, D. (eds.) ICISP 2018. LNCS, vol. 10884, pp. 444–452. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94211-7_48
5. Ferrara, M., Franco, A., Maltoni, D.: Face morphing detection in the presence of printing/scanning and heterogeneous image sources, p. 23 (2019)

6. Ngan, M., Grother, P., Hanaoka, K., Kuo, J.: Face Recognition Vendor Test (FRVT) part 4:: MORPH - performance of automated face morph detection, National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8292, March 2020. https://doi.org/10.6028/NIST.IR.8292
7. Scherhag, U., Rathgeb, C., Merkle, J., Busch, C.: Deep Face Representations for Differential Morphing Attack Detection, April 2020. arXiv200101202. https://arxiv.org/abs/2001.01202. Accessed 01 Sept 2020
8. Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., Busch, C.: Face recognition systems under morphing attacks: a survey. IEEE Access **7**, 23012–23026 (2019). https://doi.org/10.1109/ACCESS.2019.2899367
9. Robertson, D.J., Mungall, A., Watson, D.G., Wade, K.A., Nightingale, S.J., Butler, S.: Detecting morphed passport photos: a training and individual differences approach. Cogn. Res. Principles Implications **3**(1), 1–11 (2018). https://doi.org/10.1186/s41235-018-0113-8
10. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, pp. 1–7, September 2014. https://doi.org/10.1109/BTAS.2014.6996240
11. Seibold, C., Samek, W., Hilsmann, A., Eisert, P.: Accurate and Robust Neural Networks for Security Related Applications Exampled by Face Morphing Attacks, June 2018. arXiv180604265. https://arxiv.org/abs/1806.04265. Accessed 01 Sept 2020
12. Wandzik, L., Kaeding, G., Garcia, R.V.: Morphing detection using a general-purpose face recognition system. In: 2018 26th European Signal Processing Conference (EUSIPCO), Rome, pp. 1012–1016, September 2018. https://doi.org/10.23919/EUSIPCO.2018.8553375
13. Jassim, S., Asaad, A.: Automatic detection of image morphing by topology-based analysis. In: 2018 26th European Signal Processing Conference (EUSIPCO), Rome, pp. 1007–1011, September 2018. https://doi.org/10.23919/EUSIPCO.2018.8553317
14. Alfa, A.A., Ahmed, K.B., Misra, S., Adewumi, A., Ahuja, R., Ayeni, F., Damasevicius, R.: A comparative study of methods for hiding large size audio file in smaller image carriers. In: Somani, A.K., Ramakrishna, S., Chaudhary, A., Choudhary, C., Agarwal, B. (eds.) ICETCE 2019. CCIS, vol. 985, pp. 179–191. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-8300-7_15
15. Makrushin, A., Wolf, A.: An overview of recent advances in assessing and mitigating the face morphing attack. In: 2018 26th European Signal Processing Conference (EUSIPCO), Rome, pp. 1017–1021, September 2018. https://doi.org/10.23919/EUSIPCO.2018.8553599
16. Debiasi, L., Scherhag, U., Rathgeb, C., Uhl, A., Busch, C.: PRNU-based detection of morphed face images. In: 2018 International Workshop on Biometrics and Forensics (IWBF), Sassari, pp. 1–7, June 2018. https://doi.org/10.1109/IWBF.2018.8401555
17. Raghavendra, R., Raja, K.B., Venkatesh, S., Busch, C.: Transferable Deep-CNN features for detecting digital and print-scanned morphed face images. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, pp. 1822–1830, July 2017. https://doi.org/10.1109/CVPRW.2017.228
18. Singh, J.M., Ramachandra, R., Raja, K.B., Busch, C.: Robust Morph-Detection at Automated Border Control Gate using Deep Decomposed 3D Shape and Diffuse Reflectance, December 2019. arXiv191201372. https://arxiv.org/abs/1912.01372. Accessed 01 Sept 2020
19. Seibold, C., Samek, W., Hilsmann, A., Eisert, P.: Detection of face morphing attacks by deep learning. In: Kraetzer, C., Shi, Y.-Q., Dittmann, J., Kim, H.J. (eds.) IWDW 2017. LNCS, vol. 10431, pp. 107–120. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64185-0_9
20. Wang, Y.-Q.: An analysis of the Viola-Jones face detection algorithm. Image Process. Line **4**, 128–148 (2014). https://doi.org/10.5201/ipol.2014.104
21. Deshpande, N.T., Ravishankar, S.: Face detection and recognition using Viola-Jones algorithm and Fusion of PCA and ANN. Adv. Comput. Sci. Technol. **10**(5), 18 (2017). ISSN 0973-6107

22. Huang, D., Shan, C., Ardabilian, M., Wang, Y., Chen, L.: Local binary patterns and its application to facial image analysis: a survey. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **41**(6), 765–781, November 2011. https://doi.org/10.1109/TSMCC.2011.2118750
23. Patil, M.Y., Dhawale, C.A., Misra, S.: Analytical study of combined approaches to content based image retrieval systems. Int. J. Pharm. Technol. **8**(4), 14 (2016)
24. Oloyede, M.O., Hancke, G.P., Myburgh, H.C.: A review on face recognition systems: recent approaches and challenges. Multimedia Tools Appl. **79**(37–38), 27891–27922 (2020). https://doi.org/10.1007/s11042-020-09261-2
25. Yang, W., Wang, K., Zuo, W.: Neighborhood component feature selection for high-dimensional data. J. Comput. **7**(1), 161–168 (2012). https://doi.org/10.4304/jcp.7.1.161-168
26. Comparative study of K-NN, Naive Bayes and decision tree classification techniques. Int. J. Sci. Res. IJSR **5**(1), 1842–1845, January 2016. https://doi.org/10.21275/v5i1.NOV153131