Averaging Dimensionality Reduction and Feature Level Fusion for Post-Processed Morphed Face Image Attack Detection

Mary Ogbuka Kenneth and Bashir Adebayo Sulaimon

Abstract Facial morphing detection is critical when applying for a new passport and using the passport for identity verification due to the limited ability of face recognition algorithms and people to detect morphed photographs. As a result of face recognition systems' vulnerability to morphing attacks, the value of detecting fake passports at the ABC gate is undeniable. Nonetheless, identifying morphed images after they have been altered using image operations like sharpening, compression, blurring, print-scan and resizing is a significant concern in Morphing Attack Detection (MAD). These image operations can be used to conceal the morphing artefacts, which makes MAD difficult. Several researchers have carried out MAD for print-scan images; few researchers have done MAD for compressed images; however, just one paper has considered image sharpening operation. Hence, this paper proposes a MAD technique to perform MAD even after image sharpening operation using averaging dimensionality reduction and feature level fusion of Histogram of Oriented Gradient (HOG) 8 × 8 and 16 × 16 cell size. The 8 × 8 pixels cell size was used to capture small-scale spatial information from the images, while 16 × 16 pixels cell size was used to capture large-scale spatial details from the pictures. The proposed technique achieved a better accuracy of 95.71% compared with the previous work, which reached an accuracy of 85% when used for MAD on sharpened image sources. This result showed that the proposed technique is effective for MAD on sharpened post-processed images.

Keywords Face morphing attack · Bona-fide images · Sharpening · Morphed images · Machine learning

M. O. Kenneth (✉) · B. A. Sulaimon
Department of Computer Science, Federal University of Technology, Minna, Nigeria
e-mail: kenneth.pg918157@st.futminna.edu.ng

B. A. Sulaimon
e-mail: bashirsulaimon@futminna.edu.ng

S. Misra and C. Arumugam (eds.), *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, Lecture Notes on Data Engineering and Communications Technologies 109, https://doi.org/10.1007/978-3-030-93453-8_8

1 Introduction

Face Recognition Systems (FRS) automatically recognize people based on their facial features [1]. FRS is built on data acquired over the last forty years from signals and patterns processing algorithms, resulting in accurate and trustworthy facial recognition algorithms. Biometrics allows people to be identified based on their physiological traits [2]. Face biometrics are now utilized in forensics, criminal identification in airports and train stations, surveillance, credit card authentication, and logical access control to electronic commerce and electronic government services, among other uses. In addition, biometric facial photographs are an essential component of electronic passports [3], which have now been used to create almost 800 million passport instances after ten years of development. As a result, face recognition using these passports has become popular in border checks [4]. Face recognition was chosen for border enforcement because, in the event of a false negative device judgment, the border enforcement officer would conduct a visual comparison, which is a clear benefit over all other multimodal biometric such as fingerprint identification [5]. Face recognition's usefulness in Automatic Border Control (ABC) e-gates is justified by these factors [1]. By matching the live collected face photographs with the face reference picture contained in the electronic Machine Readable Travel Document (eMRTD) passport, a conventional ABC system examines the connection between both the eMRTD and the passport holder (the individual who submits the eMRTD to the border agent). The value of ABC systems, which are based on highly efficient and precise border control operations, has increased as a result [1].

FRS, as a critical component of an ABC system, are vulnerable to a variety of attacks. These attacks can be classified into two kinds. The initial attack targets the ABC system itself is commonly accomplished by introducing a facial artefact into the capture unit. Face spoofing or presentation attacks [6, 7] are examples of this type of attack. On the other hand, these attacks necessitate a significant amount of effort in both creating a face artefact and submitting it to the ABC e-gate. Aside from that, this form of attack will only succeed if the adversary is able to have in possession a lost eMRTD passport and create a facial artefact that matches the eMRTD passport's face photograph [8]. The assault against the eMRTD biometric reference is the second type of attack: The biometric data recorded in the (stolen) passport's logical information structure is changed here to replace the reference image. Because most passport applications allow for a printed face picture as part of the application process, this assault is straightforward to carry out. In addition, for passport renewal and VISA applications, many nations will permit digital photo uploads to a web gateway. This provides intruders with numerous opportunities to submit a false face picture to the passport's issuing body and receive a legitimate eMRTD passport that includes both physical and digital security elements as well as the bogus photo [1]. Simple changes can be made using freely available software to attack the EMRTD biometric reference picture [9].

Among the different face picture adjustments, face morphing is recognized as the most severe attack on the ABC border protection mechanism [10]. Face morphing

is a method of constructing a new face image by combining the precise details from two or more input face photographs belonging to different people. As a result, the morphed face image would eventually reflect the facial appearance elements of many data subjects, contributing to the morphed face [11]. As a result, any invader can morph their face into another data subject and seek an eMRTD passport that both subjects can use. This defective connection of multiple subjects with the document could result in illegal activities such as human trafficking, financial transactions, and illegal immigration [9].

Ferrara [3], Damer [3], Kramer [11] and Scherhag [11] recently proved that humans are unable to discern altered facial photos. Additionally, because eMRTD passports are widely utilized with ABC border control systems, this morphing attack may be carried out without fabricating a passport paper. As a result, to ensure the dependability of border control activities, these types of threats must be prevented.

In the previous years, there have been few authors who have worked on MAD. In 2014 Ferrara [3] introduced a face morphing attack which was called the magic passport. The viability of attacks on Automated Border Control (ABC) systems using morphed face images was examined. It was concluded that when the morphed passport is presented, the officer will recognize the photograph and release the document if the passport is not substantially dissimilar from the candidate's face. And thus, the released document passes all authenticity checks carried out at the gates.

Raghavendra [1] carried out novel research on how this face morphing attack can be detected. The study was conducted using facial micro-textures retrieved via statistically autonomous filters trained on natural photographs. This micro-texture dissimilarity was extracted using Binarised Statistical Image Features (BSIF), and classification had been made via Support Vector Machine (SVM). This was the first research done towards the MAD. Later in 2017, Seibold [12] aimed to perform MAD using a deep neural network. Three Convolutional Neural Network (CNN) architectures were trained from scratch and using already trained networks to initialize the weights. Pretrained networks were noticed to outperform the networks trained from scratch for each of the three architecture. Hence it has been concluded that the attributes acquired for classification tasks are also beneficial for MAD. In 2018 Wandzik [13] suggested a method for MAD based on a general-purpose FRS. This work combined a general-purpose FRS with a simple linear classifier to detect morph images successfully.

In 2019 Venkatesh [14] presented a novel approach for MAD focused on quantifying residual noise caused by the morphing phase Venkatesh [14] used an aggregation of several denoising methods estimated using a deep Multi-Scale Context Aggregation Network (MSCAN) to quantify the morphing noise. In 2020 Ortega-Delcampo [14] did not just stop at detecting face morphing attacks but went further to de-morph the morphed face images. Finally, in 2021 Kenneth [15] proposed a method for MAD in the presence of post-processed image sources.

The necessity of detecting false passports at the ABC gate, as a result, is undeniable. Nonetheless, recognizing altered images after they have been processed is a significant challenge in MAD. For example, after creating the morphing facial image,

the image could be further treated with image compression, image sharpening, print-scan, or blurring operations to improve or diminish image quality purposely. This morph picture alteration technique could be used to hide morph artefacts. The automated production of morphed face pictures, in particular, can result in morphing artefacts. Shadow or phantom artefacts may be caused by missing or misplaced landmarks. The facial region can be substituted by an adapted outer space of one of the people to alleviate the issue of the morphed face image.

Weng [16] offers an interpolation of the hair region to hide artefacts in the hair region. On the other hand, interpolating the hair region can disguise morphing objects in the hair region [16]. However, unnatural colour gradients and edges may occur due to insufficient interpolation methods, which can be mitigated by sharpening or blurring. Furthermore, this morphing artefact can be made to obtain realistic histogram forms by adjusting the colour histogram during the sharpening process, which prevents Morphing Attack Detection (MAD) systems from identifying such transformed images.

Hence, in line with these identified challenges, this research proposes a MAD after image sharpening operation using averaging feature dimensionality reduction and summation feature level fusion of 8×8 and 16×16 scale Histogram of Oriented Gradient (HOG) descriptor. As a result, the following are the paper's main contributions:

1. Development of a dimensionality reduction and feature-level fusion technique for MAD even after image sharpening post-processing operation.
2. Evaluation of the technique's performance in (1) using False Acceptance Rate, False Acceptance Rate and Accuracy performance metric.

The following is how the rest of the paper is organized: A survey of relevant studies is included in Sect. 2. Section 3 describes the approach utilized to conduct the research. The findings of the experiment are described in Sect. 4. Section 5 draws conclusions, while Sect. 6 discusses future work.

2 Related Works

MAD's relevance cannot be emphasized, especially after picture post-processing operations such as image sharpening, print-scan, and image compression.

Singh [17] used a deconstructed 3D geometry and diffuse reflectance to accomplish MAD. This approach was recommended because it can detect morphing attacks through print-scan, posture, and illumination abnormalities.In this investigation, actual picture was captured at the ABC gate, and these components are then used to train a MAD linear SVM that compares the real picture taken at the ABC gate to the eMTRD face image. The problem with this paper is that the suggested algorithm ignores image post-processing tasks including print-scan, contrast enhancement, image compression, blurring, and sharpening.

Makrushin [18] performed MAD using Benford features. In this work, a splicing based approach was used to produce blurred facial images which are visually faultless automatically. A spread of Benford highlights extricated from quantised Discrete Cosine Change (DCT) coefficients of JPEG-compacted transformed pictures were utilized as feature vectors, and the Support Vector Machine (SVM) was applied for grouping. The upside of the suggested system is that it could perform well even on JPEG-compacted transformed pictures. Anyway, the strategy could not distinguish morphed images in the wake of performing print and scan operation on the images.

A de-morphing configuration based on a convolutional neural network (CNN) model was proposed by Ortega-Delcampo [19]. This method is characterized by two images: the passport's potentially altered image and the person's photo in the ABC system. The de-morphing procedure aims to reveal the chip picture. Assume the chip image has been altered. The exposing procedure between the in vivo image and the morphing chip image in that case will give the person in the ABC system a different facial identity, disclosing the impostor. If the chip photo is a non-morphing image, the end image will be comparable to a genuine traveler. The significant contribution of this work is the enhancement of picture quality and graphic aspects accomplished following the de-morphing procedure, as well as the discovery of the impostor's concealed identity. The CNN model extracted a large number of features that made training or learning of these features slow. Feature selection could increase learning speed and enhance the result as more relevant features would be used for training.

Kenneth [15] proposed a method for MAD in the presence of post-processed Images sources based on feature selection using Neighborhood Component Analysis (NCA) and classification using decision tree. The Local Binary Pattern (LBP) descriptor was used to extract morphed and bona-fide image features. The image sharpening post-processing operation was considered. In this paper it was identified that image sharpening operation on morph images could alter the morph artefacts making the altered morphed images difficult for a MAD system to detect. Two experiments were conducted in this study. In the first experiment the decision tree classifier was trained with the original LBP without feature selection. In the second experiment the decision tree classifier was trained using just the NCA selected LBP feature sets. The classification using the NCA selected features produced a higher accuracy than classification using all the LBP features. For non-post-processed image sources the proposed system attained and accuracy of 94% while an accuracy of 85% was achieved for the sharpened image sources. A drawback of this study is that the accuracy of the sharpening image sources is low in comparison with the normal images. This result shows that more accurate methods are needed for improved MAD in the presence of image sharpening operation.

Raghavendra [1] used Binarized Statistical Image Features (BSIF) to perform MAD. The suggested technique used BSIF to extract a micro-texture variation from a facial image, and the classification was done with a linear Support Vector Machine (SVM). The image's BSIF characteristics are extracted, and each pixel's response to a filter trained on statistical properties of natural images is computed to represent it as a binary code. With an Attack Presentation Classification Error Rate (APCER) of

1.73%, the system performed well, demonstrating its relevance to real-world circumstances. The work's drawback is its lack of robustness when it comes to the datasets employed. The dataset was generated using a single morphing tool (GNU Image Manipulation Program), limiting its performance. However, in real-world different morphing tools are used to carry out morphing attack.

CNN was used by Raghavendra [20] as a feasible feature extractor and classifier for MAD. To perform MAD for print-scan and digital morphed photos, the proposed method used transferrable features obtained from a pre-trained CNN. VGG19 and AlexNet were two CNN algorithms employed in the feature mining process. The picture features were retrieved independently from the AlexNet and VGG19 models' fully-connected layers. The feature level fusion approach was used to combine these qualities into a single feature vector. In both cases, the proposed method gave better outcomes for digital photos with an Equal Error Rate (EER) of 8.22% than print-scan images with an EER of 12.47%. However, the print-scan post-processing technique was the only one investigated. The effects of compression, resizing, and sharpening were not considered.

Face recognition algorithms based on CNN and hand-crafted characteristics are used by Wandzik [21] to tackle the MAD problem. The face characteristics were mined using four feature extractors: Dlib, FaceNet, High-Dim Local binary pattern and VGG-Face. After completing feature extraction using any of the feature extraction method, the extracted features were used to calculate the Euclidean distance for the face authentication job. Using the reference photo vectors, the SVM was used to conduct classification tasks. The MAD of digital photographs was the focus of this study; however, print-scan photographs were not considered.

Premised on an examination of Photo Response Non Uniformity (PRNU), Debiasi [10] suggested a morphing detection technique. It is based on a spectral study of the morphing-induced fluctuations within the PRNU. The wavelet-based denoising filter was used to extract the PRNU for each image. The frequency distortion removal (FDR) PRNU improvement is next applied to the retrieved PRNU. The Discrete Fourier Transform (DFT) was used to recover the frequency spectrum of the PRNU in each cell as part of the feature extraction process. The magnitude spectrum that results illustrates the morphing-induced changes in the PRNU signal. To quantify these impacts, a histogram of DFT Magnitudes was produced to depict the spectrum's magnitude distribution. Because picture post-processing tasks like sharpening, contrast enhancement, and blurring can have a significant impact on PRNU features, this proposed method investigated the impact of several image post-processing strategies on detection performance. The suggested detection system was resistant to image scaling and sharpening, with the exception of histogram equalization. To combat the failure to recognize altered photos, a deeper analysis and improved detection methodologies are required (histogram equalization). A summary of the related reviews are given in Table 1.

Table 1 Summary of related works

Author	Approaches used	Findings	Limitations
Makrushin [18]	Benford features	The upside of the suggested system is that it had the option to perform well even on JPEG-compacted transformed pictures	The strategy could not distinguish morphed pictures in the wake of performing print and scan operation on the images
Debiasi [10]	PRNU-based technique	The proposed method investigated the effects of various image post-processing techniques on detection efficiency, finding that the proposed detector was resistant to image sharpening and scaling	The system failed for MAD on morphed images processed with histogram equalization
Kenneth [15]	Neighborhood component analysis (NCA) and local binary pattern	In this paper it was identified that image sharpening operation on morph images could alter the morph artefacts making the altered morphed images difficult for a MAD system to detect	A drawback of this study is that the accuracy of the sharpening image sources is low in comparison with the normal images. This result shows that more accurate methods are needed for improved MAD in the presence of image sharpening operation
Raghavendra [20]	VGG19 and AlexNet	When comparing digital photographs with an equal error rate (EER) of 8.223% to print-scan photos with an EER of 12.47%, the proposed method achieves a better outcome for digital photographs	The MAD could not attain an outstanding EER for MAD in the print-scan image compared to the digital images

(continued)

Table 1 (continued)

Author	Approaches used	Findings	Limitations
Ortega-Delcampo [19]	Convolutional neural network (CNN)	The significant contribution of this work is the enhancement of picture quality and visual aspects accomplished following the de-morphing procedure, as well as the discovery of the impostor's concealed identity	The CNN model extracted a large number of features that made training or learning of these features slow
Singh [17]	CNN (pre-trained AlexNet)	The authors provide a novel database of morphing photos and trusted live capture probing images collected in a realistic border crossing scenario with ABC gates Proposed a new method for detecting morphing attacks that uses a combination of scores from a quantized normal-map phase and dispersed reconstructed image features to exploit the intrinsic border crossing situation	The problem with this paper is that the suggested algorithm ignores image post-processing tasks including sharpening, print-scan, compression, and blurring
Wandzik [21]	faceNet, Dlib, VGG-face, high-dim local binary pattern, and SVM	Instead of adding new components, the proposed approach makes use of an established feature extraction pipeline for face recognition systems. It doesn't need any fine-tuning or changes to the current recognition scheme, and it can be trained with a small dataset	This study only looked at the MAD of digital photos, not the print-scanned photos that are utilized for authentication in some nations

(continued)

Table 1 (continued)

Author	Approaches used	Findings	Limitations
Raghavendra [1]	BSIF	The system attained a good performance with APCER of 1.73% that shows its applicability to a real-world scenario	The downside of this work is robustness with respect to the dataset used. The dataset was generated using a single morphing tool (GNU Image Manipulation Program), limiting its performance

3 Methodology

This section presents the description of the methods used to carry out this research [22]. These techniques includes data collection and generation, image post-processing and pre-processing, feature extraction, dimensionality reduction, feature fusion and data classification. The proposed system is illustrated in Fig. 1.

3.1 Data Collection

Using different facial photographs from 100 persons, a new morphed facial data set comprising 200 morphed photos and 150 bona-fide images was developed, totaling 350 image. To assist diversify the database, female and male of diverse complexion were employed in the facial photos. The images for the subjects came from a variety

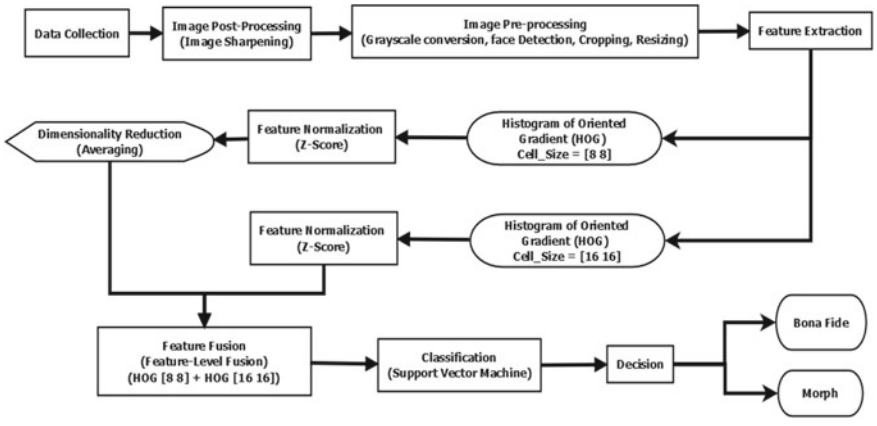

Fig. 1 Proposed system

of electronic sources, including the Yale face database [23] and the 123RF photo website [24]. The altered face images were created with the help of 2 morphing tools:

1. **Magic morph tool**: This is a free Windows-based program that acts as a useful image and graphics utility for users. It is high-speed morphing and warping program. Magic Morph allows users to animate their still images into SWF, GIF, or AVI files with morphing effects. It is easy and straightforward to use. Quick and multithread pyramid methods, expert-quality warping and morphing techniques, and real-time visualization functions are all included in the app. TIFF, BMP, JPEG, J2K, PNG, ICO, GIF, TGA, WBMP, PCX, WMF, and JBG are among the file formats supported by this method. Its compatible output files, on the other hand, are AVI, GIF and SWF Movie, JPEG and BMP Sequence.
2. **FantaMorph tool**: The FantaMorph utility is a transforming software that may be used to create photo transformations and current transform activity effects. It assists users in locating facial features such as the nose, eye, and mouth, and then combines these features from multiple real-life faces to produce a virtual face. FantaMorph comes in three different editions: Standard, Professional, and Deluxe, and it works on both Windows and Mac computers.

The images were adjusted by hand and blended in an antique shell. The morphing software creates an overview of the transition from one subject to another. The last picture that has been transformed is manually taken by showing its similarity to the participating subjects' faces during transformation. The generated transformations are now high in calibre and have little to no identifiable artefacts.

3.2 Image Sharpening

A morphed image that undergoes a sharpening procedure loses part of its artefacts, causing MAD to be problematic. Since human perception is extremely sensitive to edges and details in a picture, imaging sharpening is typically used as an image post-processing technique. As images are primarily made up of high-frequency portions, high-frequency distortion can degrade graphic quality [15]. Improved quality of the visual image is achieved through improving the high-frequency segments of the picture. Thus, sharpening of the morphed images can emphasize the edges of a picture and modify the subtleties that can also change the morph highlights that make the morphed photo challenging to detect.

3.3 Face Pre-processing

In the face pre-processing stage, four operations were carried out. These operations include Facial landmark detection, cropping, image resizing and Grayscale conversation. Each of these processes is discussed in details in the subsections below.

3.3.1 Facial Features Detection

Facial features, such as the nose, eyes, lips, brows, and jawline, are employed to restrict and signify significant regions of focus [13]. The Viola-Jones approach was used to detect face features in this study. The Viola-Jones computation employs Haar-basis filtering, a scalar object in the middle of the image, and various Haar-like structures [25]. Haar feature selection, integral photo screening, Adaboost training, and a cascading classifier are the four phases of this approach for face recognition [26]. The input image is first converted into an integral image via the Viola-Jones face detection algorithm. The integral image is a method for generating the pixel sum intensities in a square of a picture in an operational manner. A more detailed discussion of the Viola-Jones technique is found in Wang [17], Viola and Jones [18], and Jensen [20].

3.3.2 Image Cropping

Cropping is the removal of a photographic image from unnecessary external areas. The approach typically involves removing some of the peripheral regions of an image to eliminate extra trash from the image, enhance its framing, alter the aspect ratio, or highlight or separate the subject matter from its background. After detecting the facial features using the Voila Jones algorithm, the face images were cropped to magnify the primary subject (face) and further reduce the angle of view to a dimension of 150×150 pixels established on the identified features to make sure that the MAD algorithm is only applied to the face.

3.3.3 Grey-Scale Conversion

A grey-scale image in digital image processing is one in which a single sample representing only a quantity of light is the value of each pixel; that is, it holds only intensity values. The pictures in grey-scale, a kind of grey monochrome, are made entirely of shades of grey. At the lowest intensity, the contrast varies from black to white at the highest [27]. In this phase, the cropped RGB or coloured face images were converted to a grey-scale image to prepare the images for feature extraction.

3.3.4 Image Resizing

The graphic primitives that constitute a vector graphic image can be sized using geometric transformations without losing image quality when resizing it in digital image processing. Image resizing can be interpreted as image resampling or image reconstruction [28, 29]. The image size can be changed in several ways, but the Nearest-Neighbour Interpolation (NNI) algorithm was adopted in this paper. The NNI algorithm is one of the more straightforward ways of increasing image size. This deals with exchanging every pixel in the output with the nearest pixel; this ensures there will be several pixels of the same colour for up-scaling. Pixel art may benefit from this because sharp details can be preserved [30]. In this step, the cropped images were all resized to the same scale to enable the extraction of the same number of feature vectors.

3.4 Feature Extraction

Image features contain essential information such as points and edges that are vital for image analysis. Images are extracted using several techniques. In this paper, the Histogram of Oriented Gradient (HOG) extractor was utilized to extract gradient features from the bona-fide and morphed images.

3.4.1 Histogram of Oriented Gradient (HOG)

The HOG is a function extractor utilized for object discovery in image processing and computer vision. The method counts how many times a gradient orientation occurs in a particular image area [31]. HOG is invariant to photometric and geometric transformations; This makes it very well adapted for human detection [32]. The HOG features are generated as follows: After pre-processing and resizing the image, the variance in the x and y directions for each image pixel is determined. The magnitude and directions are computed using the equations in Eqs. 1 and 2, correspondingly.

$$\text{Total Gradient Magnitude } = \sqrt{(G_x)^2 + \left(G_y\right)^2} \tag{1}$$

where G_y denotes the y-direction gradient and G_x denotes the x-direction gradient.

$$\text{Direction } = \tan(\theta) = {}^{G_y}/_{G_x} \tag{2}$$

The value of the angle (θ) is presented in Eq. 3

$$\theta = a\tan(G_y/G_x) \tag{3}$$

The HOG gradient descriptor was used in this research because the image morphing process reduces the changes in the high frequency of the image and decreases the morphed images' gradient steepness, enhancing MAD.

There are no optimal values or scale in the HOG feature description to extract the best feature for classification. For example, cell size 8 × 8 is HOG with fine cells. But perhaps it is not the best scale (because the cells are too small and noise might just be observed) (On the other hand, too large cells, like cell size 16 × 16, may be too large, and there will have uniform histograms everywhere). The best way to obtain the best features is by extracting HOG at various scales and combining them. Hence the 8 × 8 pixels cell size was used to capture small-scale spatial information from the images, while 16 × 16 pixels cell size was used to capture large-scale spatial details from the pictures. The HOG with 16 × 16 pixels cell sizes consists of 648 feature vectors. The HOG with 8 × 8 pixels cell sizes consists of 4320 feature vectors.

3.5 Feature Normalization

Normalization is the process of converting values measured on multiple scales to a nominally standard scale, which is commonly done before averaging. The approach of feature normalization is used to normalize the range of independent variables or data characteristics. Normalization is the process of converting qualities to a scale that is equivalent. This improves the models' performance and training reliability [33]. The retrieved features were normalised to ensure that the HOG (8 × 8) and (16 × 16) weight feature vectors were all on the same scale and contributed equally to the classification outcome. The Z-Score approach was used to normalize the extracted features.

3.5.1 Z-Score

A prevalent technique to normalise features to zero mean and unit variance is the Z-score normalisation technique [34]. The Z-Score is an arithmetic statistic for comparing a score to the average of a collection of scores [35]. Z-Score is calculated based on the formula in Eq. 4.

$$Z_{\text{score}}(i) = \frac{x_i - \mu}{s} \tag{4}$$

where μ is the mean of the distribution, s is the standard deviation and x_i = number of object in the distribution. Equation 5 provides the formula for calculating the standard deviation:

$$s = \sqrt{\frac{1}{n-1}} \sum_{i=1}^{n} (x_i - \mu)^2 \tag{5}$$

3.6 Averaging Dimensionality Reduction and Feature Fusion

Dimensionality reduction is the translation of data from a high-dimensional space into a low-dimensional space such that some significant features of the source data are preserved by the low-dimensional representation, preferably similar to its fundamental dimension [36, 37].

3.6.1 Averaging Dimensionality Reduction

In this study, dimensionality reduction was performed as an intermediate step to facilitate the feature fusion process. Dimensionality reduction was performed only on HOG 8 × 8 pixels cell size. The HOG 8 × 8 pixels cell size consisting of 4320 features was reduced to 648 features. Dimensionality was performed using averaging. Averaging was used to ensure that every initial HOG 8 × 8 features contributed to the new reduced features. The averaging dimensionality reduction was performed on HOG 8 × 8 features because the summation feature-level technique can only be applied to different features of the same dimension. Hence, the HOG 8 × 8 features' dimensionality must be equal to the HOG 16 × 16 features' dimensionality.

To average the HOG 8 × 8 features, the features were divided by the number of HOG 16 × 16 features. The result of this division was used to group the features for averaging. For example, the 4320 (the number of HOG (8 × 8) features) was divided by 648 (number of GLCM features), which results in approximately 7. This means that the first seven (7) features will be averaged first, followed by the next seven features. Averaging of each seven feature continues till the 4320th feature. The algorithm for dimensionality reduction and feature-level fusion technique is presented in algorithm 1.

ALGORITHM 1: Averaging Dimensionality Reduction and Feature Fusion

Inputs:
H8[] ={$X_1, X_2, X_3, \ldots, X_n$} //HOG (8 x 8 cell size) feature vectors
H16[] ={$Y_1, Y_2, Y_3, \ldots, Y_n$} //HOG (16 x 16 cell size) feature vectors

Output:
F[] //Fused feature of H8[] and H16[]

1: get number of rows for H8[],n_rows
2: get number of columns for H8[], C1
3: get number of columns for H16[], C2
4: M1 = floor ($^{C_2}/_{C_1}$) // get floor value for C2 divided by C1
5: N1= (C2 – M1) * C1 + M1 //to get first set of columns to average
6: for i = 1 to n_rows //Looping through rows
7: Q1 = mean(H8(1 to N1) // to average the selected first set of columns for H8[] features
8: for t=N1 + 1 to C2 //Loop through the group columns and /increment by M1
9: Q1 =Concatenate (Q1, mean(H8(t to t + M1 – 1)) //merge the average of the first, second, third, fourth, …C1 selected set of columns for H[] features
10: end
11: end
12: $\sum H_{16}[]\, Q_1$ //average Feature fusion for H16[] and reduced dimension H8[]
13: F[] = Concatenate ($H_{16}[], Q_1$)
14: return F[]

3.6.2 Feature Fusion

Feature Fusion is a technique for combining similar data extracted from a collection of training and testing images without losing any detail [38–40]. Summation feature-level technique was used for fusion. The summation feature-level method is expressed in Eqs. 6 and 7. The summation feature-level fusion formula to fuse H8 and H16 is presented in Eq. 6.

$$\sum \mathrm{H_{16}Q_1} \tag{6}$$

The fused H_8 and H_{16} were then concatenated to produce the final feature vectors using the formula in Eq. 7.

$$\mathrm{F} = \text{Concatenate } (\mathrm{H_6}, \mathrm{Q_1}) \tag{7}$$

The new set of concatenated feature vectors (648 features) generated using the summation feature level fusion technique were used to train the SVM classifier.

The main advantage of feature-level fusion is that it detects correlated feature values produced by different feature extraction methods, resulting in a compact collection of salient features that can boost detection accuracy [41].

3.7 Image Classification

Classifications algorithms simply categorize the input to correspond to the desired output [42]. Image classification is the technique of categorizing and marking sets of pixels inside an image according to a set of laws [43]. In this paper, the SVM classifier was utilized to classify the face photos into morph or bona-fide photos.

3.7.1 Support Vector Machine (SVM)

SVM is a supervised learning framework with related learning algorithms for regression and classification analysis [44]. The SVM technique seeks to locate a hyper-plane in a D-dimensional domain (where D denotes the number of features) that distinguishes between data sets [45]. Hyperplanes are decision lines that help categorize data. Data points on either side of the plane can be allocated to various groups. The number of functions determines the hyperplane's dimension as well. The decision function of a binary SVM is described in the input space by Eq. 8:

$$\gamma = h(x) = \text{sign}\left(\sum_{j=1}^{n} u_j y_j K\left(x, x_j\right) + v\right) \tag{8}$$

where x is the to-be-categorised feature vector, j indexes the training instances, n is the number of training instances, y_j is the label (1/−1) of training example j, $K(,)$ is the kernel function, and u_j and v are fit to the data to maximise the margin. Training vectors for which $u_j \neq 0$ are called support vectors [46]. A significant advantage of SVM is that it is versatile (that is, different Kernel functions can be specified for the decision function) [47].

3.8 Performance Metrics

The following evaluation metrics were used to assess the performance of the suggested technique.

1. **Attack Presentation Classification Error Rate (APCER)**: This is the same as the false acceptance rate. It is defined as a percentage of morphing attack that is classified as bona-fide images [48]. Equation 9 contains the formula for APCER:

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

2. **Bona fide Presentation Classification Error Rate (BPCER)**: This is the same as the false rejection rate. In a particular context, the BPCER is described as the

fraction of genuine presentations wrongly categorized as presentation attacks, or the fraction of genuine photos incorrectly labelled as morphing attacks [21]. In Eq. 9, the BPCER formula is presented

$$\text{BPCER} = \text{False Negative}/(\text{True Positive} + \text{False Negative}) \quad (10)$$

3. **Accuracy (ACC)**: This is a statistic for evaluating the consistency of categorization models. The percentage of correctly classified instances for an independent testing data set can be precisely described as accuracy [49]. Equation 11 shows the accuracy:

$$\text{ACC} = \frac{\text{True Positive} + \text{True negative}}{\text{True Positive} + \text{True negative} + \text{False Positive} + \text{False negative}} \quad (11)$$

4 Results and Discussion

In this paper, experimentation were carried out based on three techniques: HOG (8 × 8) + SVM, HOG (16 × 16) + SVM and HOG (16 × 16) + HOG (8 × 8) + SVM (proposed system) algorithms with respect to the sharpened images and non-sharpened images. The following six categories of investigations have been carried out:

1. Classification images that have not been post-processed using HOG (8 × 8) + SVM technique.
2. Non-post-processed images classification using HOG (16 × 16) + SVM technique.
3. Non-post-processed images classification using a fusion of HOG (8 × 8) and HOG (16 × 16) features algorithm.
4. Post-processed images classification using HOG (8 × 8) + SVM algorithm.
5. Post-processed images classification using HOG (16 × 16) + SVM algorithm.
6. Post-processed images classification using a fusion of HOG (8 × 8) and HOG (16 × 16) features algorithm.

Table 2 consists of the MAD experimentation result for post-processed images.

Table 2 shows that the suggested system had the highest accuracy for the sharpened images, with a value of 95.71%, as opposed to HOG (8 × 8) + SVM and HOG (16 × 16) + SVM, which had accuracy of 94.29 and 90.00%, correspondingly. According on the BPCER figures shown in Table 2, the suggested system has the best result, with BPCER of 3.36% at APCER = 5% and BPCER of 1.68% at APCER = 10%. Also, the suggested system performed better when compared with a previous work by Kenneth [15] on MAD after performing an image sharpening operation.

Figure 2 shows a chart comparing the performance of four different MAD techniques, namely HOG (8 × 8), HOG (16 × 16), proposed technique (HOG (8 × 8)

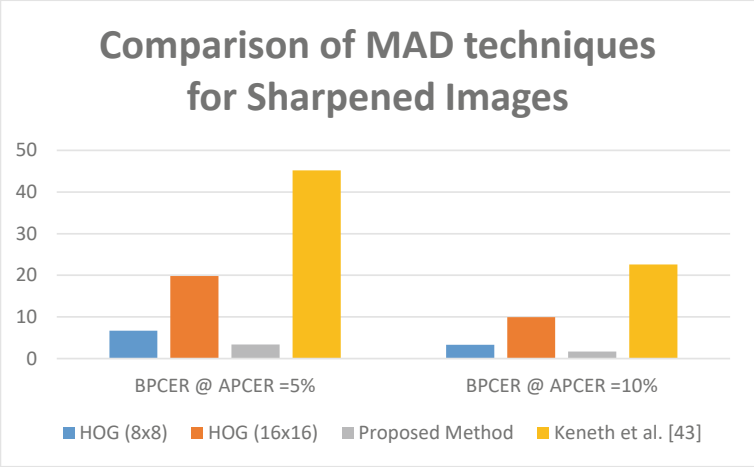

Fig. 2 Comparison of MAD techniques for Sharpened Images

+ HOG (16 × 16)) and Kenneth [15]. Figure 2 is a visualization of the performance measures in Table 2.

The proposed system's improved performance can be attributed to the concatenation of gradient features HOG (8 × 8) and HOG (16 × 16) extracted from the post-processed morphed and bona-fide images.

Table 3 shows that the suggested system had the best performance for non-sharpened images, with a rating of 97.14%, contrasted to HOG (8 × 8) + SVM and HOG (16 × 16) + SVM, both of which had a value of 94.29%. The proposed solution also has the best result, with BPCER of 1.63% at APCER = 5% and BPCER of 0.82% at APCER = 10%, according to the BPCER estimates shown in Table 3. Whereas the methods offered by Ramachandra [48] and Ramachandra [50] have BPCER of 45.76% and BPCER = 7.59% at APCER = 5% and BPCER of 13.12% and BPCER = 0.86% at APCER = 10%.

Figure 3 shows a chart comparing the performance of seven different MAD techniques, namely HOG (8 × 8), HOG (16 × 16), proposed technique (HOG (8 × 8) +

Table 2 MAD Classification Result for Sharpened Images

Sharpened images			
Algorithm	Accuracy (%)	BPCER (%) @	
		APCER = 5%	APCER = 10%
HOG (8 × 8) + SVM	94.29	6.67	3.33
HOG (16 × 16) + SVM	90.00	19.85	9.93
Kenneth [15]	85	45.19	22.59
Proposed method (HOG (8 × 8) + HOG (16 × 16) + SVM)	95.71	3.36	1.68

Table 3 MAD classification results for non-sharpened images

Non-sharpened images			
Techniques	Accuracy (%)	BPCER (%) @	
		APCER = 5%	APCER = 10%
HOG (8 × 8) + SVM	94.29	4.93	2.47
HOG (16 × 16) + SVM	94.29	4.93	2.47
Proposed method (HOG (8 × 8) + HOG (16 × 16) + SVM)	**97.14**	**1.63**	**0.82**
Steerable textures [48]	–	45.76	13.12
Laplacian pyramid + LBP [50]	–	7.59	0.86
Deep color residual noise [51]	–	3.00	1.50
Transferable deep-CNN [20]	–	14.38	7.53

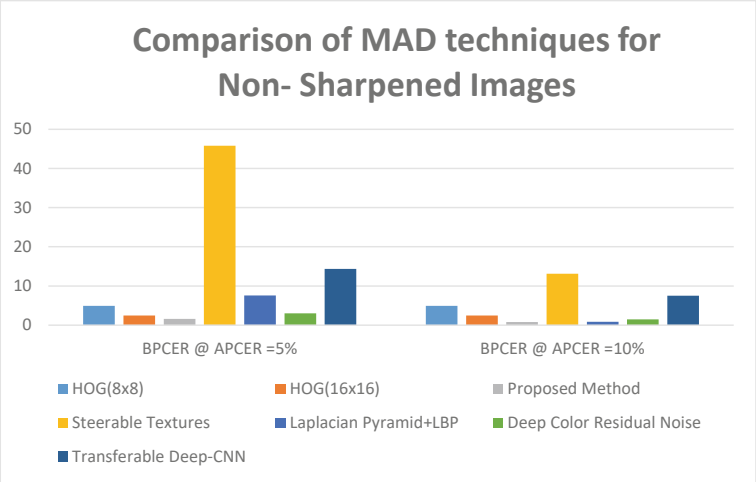

Fig. 3 Comparison of MAD techniques for non-sharpened images

HOG (16 × 16)), steerable texture, Laplacian Pyramid + LBP, Deep colour residual noise and Transferable deep-CNN techniques. Figure 3 is also a visualization of the performance measures in Table 3.

This paper was competent to accomplish MAD more reliably than earlier MAD research. This is due to the system's capacity to recognize altered images utilizing a fusion of powerful and resilient feature descriptors, after image sharpening functionality has been performed on those images.

5 Conclusion

This study conducted MAD after the sharpening operation was applied on both the morphed and bona-fide images based averaging dimensionality reduction and summation feature-level fusion of the HOG (8×8) and HOG (16×16) gradient features using the SVM classifier. These extracted features were normalized to adjust the features measured on different scales to a notionally standard scale. These normalized features were fused using the feature-level fusion method. The SVM classifier learned these fused features, which classified the features into two categories: morphed or bona-fide. The proposed method was compared to existing MAD techniques and single feature descriptor methods. From the results obtained, it can be concluded that the proposed system has a high-performance accuracy of 97.14 and 95.71% for non-sharpened images and sharpened images, respectively as compared to the existing MAD methods.

6 Future Works

This study used only two morphing applications to create the altered photos. To improve MAD's robustness, several morphing algorithms should be utilized to build a more resilient morphed datasets. The morphed datasets utilized in this study was created in-house using morphing software that was readily available. There was no currently accessible extensive database for MAD. As a result, it is suggested that in the future, a extensive publicly accessible morph database containing both real and morphed photographs be created as a baseline for MAD algorithms.

References

1. Raghavendra R, Raja KB, Busch C (2016) Detecting morphed face images. In: 2016 IEEE 8th international conference on biometrics theory, applications and systems (BTAS), Niagara Falls, NY, USA, pp 1–7. https://doi.org/10.1109/BTAS.2016.7791169
2. Olanrewaju L, Oyebiyi O, Misra S, Maskeliunas R, Damasevicius R (2020) Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose—Chaudhuri—Hocquenghem error-correcting codes. Signal Image Video Process 14(5):847–855. https://doi.org/10.1007/s11760-019-01609-y
3. Damer N, Saladie AM, Braun A, Kuijper A (2018) MorGAN: recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In: 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS), Redondo Beach, CA, USA, pp 1–10. https://doi.org/10.1109/BTAS.2018.8698563
4. Ferrara M, Franco A, Maltoni D (2014) The magic passport. In: IEEE international joint conference on biometrics, Clearwater, FL, USA, pp 1–7. https://doi.org/10.1109/BTAS.2014.6996240
5. Mislav G, Kresimir D, Sonja G, Bozidar K (2021) Surveillance cameras face database. In: SCface—Surveillance cameras face database. https://www.scface.org/. Accessed 02 Feb 2021

6. Bharadwaj S, Dhamecha TI, Vatsa M, Singh R (2013) Computationally efficient face spoofing detection with motion magnification. In: 2013 IEEE conference on computer vision and pattern recognition workshops, OR, USA, pp 105–110. https://doi.org/10.1109/CVPRW.2013.23
7. Tolosana R, Gomez-Barrero M, Busch C, Ortega-Garcia J (2020) Biometric presentation attack detection: beyond the visible spectrum. IEEE Trans Inf Forensics Secur 15:1261–1275. https://doi.org/10.1109/TIFS.2019.2934867
8. Chingovska I, Mohammadi A, Anjos A, Marcel S (2019) Evaluation methodologies for biometric presentation attack detection. In: Marcel S, Nixon MS, Fierrez J, Evans N (eds) Handbook of biometric anti-spoofing. Springer International Publishing, Cham, pp 457–480. https://doi.org/10.1007/978-3-319-92627-8_20
9. Damer N et al (2019) Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In: Brox T, Bruhn A, Fritz M (eds) Pattern recognition, vol 11269. Springer International Publishing, Cham, pp 518–534. https://doi.org/10.1007/978-3-030-12939-2_36
10. Debiasi L, Scherhag U, Rathgeb C, Uhl A, Busch C (2018) PRNU-based detection of morphed face images. In: 2018 international workshop on biometrics and forensics (IWBF), Sassari, pp 1–7. https://doi.org/10.1109/IWBF.2018.8401555
11. Kramer RSS, Mireku MO, Flack TR, Ritchie KL (2019) Face morphing attacks: investigating detection with humans and computers. Cogn Res Princ Implic 4(1):28. https://doi.org/10.1186/s41235-019-0181-4
12. Scherhag U, Rathgeb C, Merkle J, Breithaupt R, Busch C (2019) Face recognition systems under morphing attacks: a survey. IEEE Access 7:23012–23026. https://doi.org/10.1109/ACCESS.2019.2899367
13. Seibold C, Samek W, Hilsmann A, Eisert P (2017) Detection of face morphing attacks by deep learning. In: Kraetzer C, Shi Y-Q, Dittmann J, Kim HJ (eds) Digital forensics and watermarking, vol 10431. Springer International Publishing, Cham, pp 107–120. https://doi.org/10.1007/978-3-319-64185-0_9
14. Venkatesh S, Ramachandra R, Raja K, Spreeuwers L, Veldhuis R, Busch C (2019) Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network, p 10
15. Kenneth OM, Sulaimon AB, Opeyemi AA, Mohammed AD (2021) Face morphing attack detection in the presence of post-processed image sources using neighborhood component analysis and decision tree classifier. In: Misra S, Muhammad-Bello B (eds) Information and communication technology and applications. ICTA 2020, vol 1350, pp 340–354. https://doi.org/10.1007/978-3-030-69143-1_27
16. Weng Y, Wang L, Li X, Chai M, Zhou K (2013) Hair interpolation for portrait morphing. Comput Graph Forum 32(7):79–84. https://doi.org/10.1111/cgf.12214
17. Singh JM, Ramachandra R, Raja KB, Busch C (2019) Robust morph-detection at automated border control gate using deep decomposed 3D shape and diffuse reflectance. http://arxiv.org/abs/1912.01372. Accessed 01 Sep 2020
18. Makrushin A, Neubert T, Dittmann J (2017) Automatic generation and detection of visually faultless facial morphs. In: Proceedings of the 12th international joint conference on computer vision, imaging and computer graphics theory and applications, Porto, Portugal, pp 39–50. https://doi.org/10.5220/0006131100390050
19. Ortega-Delcampo D, Conde C, Palacios-Alonso D, Cabello E (2020) Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access 1–1. https://doi.org/10.1109/ACCESS.2020.2994112
20. Raghavendra R, Raja KB, Venkatesh S, Busch C (2017) 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. https://doi.org/10.1109/CVPRW.2017.228
21. Wandzik L, Kaeding G, Garcia RV (2018) Morphing detection using a general- purpose face recognition system. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1012–1016. https://doi.org/10.23919/EUSIPCO.2018.8553375

22. Misra S (2021) A step by step guide for choosing project topics and writing research papers in ICT related disciplines. In: Misra S, Muhammad-Bello B (eds) Information and communication technology and applications, vol 1350. Springer International Publishing, Cham, pp 727–744. https://doi.org/10.1007/978-3-030-69143-1_55
23. Yale face database. In: Yale face database. http://vision.ucsd.edu/content/yale-face-database. Accessed 11 Nov 2020
24. 23RF (2020) Black man face stock photos and images. In: Black man face stock photos and images. https://www.123rf.com/stock-photo/black_man_face.html?sti=lo3vts77wcrg1jyzpbl. Accessed 07 Dec 2020
25. Wang Y-Q (2014) An analysis of the viola-jones face detection algorithm. Image Process Line 4:128–148. https://doi.org/10.5201/ipol.2014.104
26. Viola P, Jones M (2001) Rapid object detection using a boosted cascade of simple features. In: Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001, Kauai, HI, USA, vol 1, p I-511–I-518. https://doi.org/10.1109/CVPR.2001.990517
27. Saravanan C (2010) Color image to grayscale image conversion. In: 2010 second international conference on computer engineering and applications, Bali Island, Indonesia, pp 196–199. https://doi.org/10.1109/ICCEA.2010.192
28. Dong W-M, Bao G-B, Zhang X-P, Paul J-C (2012) Fast multi-operator image resizing and evaluation. J Comput Sci Technol 27(1):121–134. https://doi.org/10.1007/s11390-012-1211-6
29. Malini MS, Patil M (2018) Interpolation techniques in image resampling. Int J Eng Technol 7(34):567. https://doi.org/10.14419/ijet.v7i3.34.19383
30. Parsania Mr PS, Virparia Dr PV (2016) A comparative analysis of image interpolation algorithms. IJARCCE 5(1):29–34. https://doi.org/10.17148/IJARCCE.2016.5107
31. Suard F, Rakotomamonjy A, Bensrhair A, Broggi A (2006) Pedestrian detection using infrared images and histograms of oriented gradients. In: 2006 IEEE intelligent vehicles symposium, Meguro-Ku, Japan, pp 206–212. https://doi.org/10.1109/IVS.2006.1689629
32. Dalal N, Triggs B (2005) Histograms of oriented gradients for human detection. In: 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05), San Diego, CA, USA, vol 1, pp 886–893. https://doi.org/10.1109/CVPR.2005.177
33. Kumar BS, Verma K, Thoke AS (2015) Investigations on impact of feature normalization techniques on classifier's performance in breast tumor classification. Int J Comput Appl 116(19):11–15. https://doi.org/10.5120/20443-2793
34. Shalabi LA, Shaaban Z, Kasasbeh B (2006) Data mining: a preprocessing engine. J Comput Sci 2(9):735–739. https://doi.org/10.3844/jcssp.2006.735.739
35. Kolbaşi A, Ünsal PA (2015) A comparison of the outlier detecting methods: an application on turkish foreign trade data. J Math Stat Sci 5:213–234
36. Sembiring RW, Zain JM, Embong A (2011) Dimension reduction of health data clustering, p 10
37. Yang W, Wang K, Zuo W (2012) Neighborhood component feature selection for high-dimensional data. J Comput 7(1):161–168. https://doi.org/10.4304/jcp.7.1.161-168
38. Gawande U, Zaveri M, Kapur A (2013) A novel algorithm for feature level fusion using SVM classifier for multibiometrics-based person identification. Appl Comput Intell Soft Comput 2013:1–11. https://doi.org/10.1155/2013/515918
39. Sudha D, Ramakrishna M (2017) Comparative study of features fusion techniques. In: 2017 international conference on recent advances in electronics and communication technology (ICRAECT), Bangalore, India, pp 235–239. https://doi.org/10.1109/ICRAECT.2017.39
40. Vaidya AG, Dhawale AC, Misra S (2016) Comparative analysis of multimodal biometrics. Int J Pharm Technol 8(4):22969–22981
41. Bhardwaj SK (2014) An algorithm for feature level fusion in multimodal biometric system. Int J Adv Res Comput Eng Technol 3(10):5
42. Olaleye T, Arogundade O, Adenusi C, Misra S, Bello A (2021) Evaluation of image filtering parameters for plant biometrics improvement using machine learning. In: Patel KK, Garg D, Patel A, Lingras P (eds) Soft computing and its engineering applications, vol 1374. Springer, Singapore, pp 301–315. https://doi.org/10.1007/978-981-16-0708-0_25

43. Shinozuka M, Mansouri B (2009) Synthetic aperture radar and remote sensing technologies for structural health monitoring of civil infrastructure systems. In: Structural health monitoring of civil infrastructure systems, Elsevier, pp 113–151. https://doi.org/10.1533/9781845696825.1.114
44. Meyer D, Leisch F, Hornik K (2003) The support vector machine under test. Neurocomputing 55(1–2):169–186. https://doi.org/10.1016/S0925-2312(03)00431-4
45. Chih-Wei H, Chih-Jen L (2002) A comparison of methods for multiclass support vector machines. IEEE Trans Neural Netw 13(2):415–425. https://doi.org/10.1109/72.991427
46. Sopharak A et al (2010) Machine learning approach to automatic exudate detection in retinal images from diabetic patients. J Mod Opt 57(2):124–135. https://doi.org/10.1080/09500340903118517
47. Crammer K, Singer Y (2001) On the algorithmic implementation of multiclass Kernel-based vector machines, p 28
48. Ramachandra R, Venkatesh S, Raja K, Busch C (2020) Detecting face morphing attacks with collaborative representation of steerable features. In: Chaudhuri BB, Nakagawa M, Khanna P, Kumar S (eds) Proceedings of 3rd international conference on computer vision and image processing, vol 1022. Springer, Singapore, pp 255–265. https://doi.org/10.1007/978-981-32-9088-4_22
49. Ferrara M, Franco A, Maltoni D (2016) On the effects of image alterations on face recognition accuracy. In: Bourlai T (ed) Face recognition across the imaging spectrum. Springer International Publishing, Cham, pp 195–222. https://doi.org/10.1007/978-3-319-28501-6_9
50. Ramachandra R, Venkatesh S, Raja K, Busch C (2019) Towards making Morphing attack detection robust using hybrid scale-space colour texture features. In: 2019 IEEE 5th international conference on identity, security, and behavior analysis (ISBA), Hyderabad, India, pp 1–8. https://doi.org/10.1109/ISBA.2019.8778488
51. Venkatesh S, Ramachandra R, Raja K, Spreeuwers L, Veldhuis R, Busch C (2019) Morphed face detection based on deep color residual noise. In: 2019 ninth international conference on image processing theory, tools and applications (IPTA), Istanbul, Turkey, pp 1–6. https://doi.org/10.1109/IPTA.2019.8936088