IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An approach For Face Liveness Detection and Face Recognition Using Machine Learning Algorithm

[1]Pranjal Patil,[2]Samruddhi Desale,[3]Vidya Kotkar, [4]Renuka Alkunte, [5]Vitthal S. Gutte

[1,2,3,4]Student,[5]Professor

[1,2,3,4,5], Department of Information Technology,

MIT College of Engineering, Kothrud, Pune, India

Abstract: Today's security purpose, face recognition system approach is used in biometric systems, face recognition is widely used for security purposes as compared to the other systems that are used in security purposes. Face recognition systems are also easily spoofed and unsafe for our security system because face recognition can be done by the images, video frames. Images or videos of a person can be easily available from social media or the internet and can be easily downloaded. Also, pictures of a person can be captured from some distance. As there are more applications, where face recognition is used, this act of sealing and identifying is becoming more serious as people think. To protect from this kind of scams and spoofing, liveness detection technology has been implemented in our system.

Index Terms **- Deep Learning, Face detection, Face liveness detection, Face recognition, Machine learning.**

I. INTRODUCTION

A fundamental task in biometric systems is security, face recognition is used for identifying the person from a digital image or video frame. But like other biometric methods face recognition is also easily spoofed, spoofing done with the images, masks, or a video frame. Images and videos of the person can be easily available from social media as well as easily captured from some distance. Though this system has a strong ability to remember and recognize thousands of human faces, it is still a hard problem for computers.

The face recognition scheme is a technology that is simply the image matching with the database. In the recognition system, a training part database is created for the various persons and some characteristics are pulled out from each face and saved as a reference database. At the time of real application, the image is captured and the same characteristics are pulled out from the face. These features are compared with a database which decides if the person is authorized or not. Such methods are available which depend on different features extracted. But these face recognition schemes can be simply fooled. In technology, many advances are developed to fool such systems applying to spoof. To stop spoofing such systems liveness detection is proposed.

In the face recognition proposed method, liveness is detected using illumination of the characteristics. The work depends on one image and gives an effective liveness detection method to detect traits in face detection. And this liveness detection is based on illumination characteristics of image and texture factor.

The most important superiority of face recognition system technology is that it does not need much attention from the user. Face recognition has some applications in access control, surveillance, ATMs, unlocking software and applications, a criminal investigation, attendance systems, etc.

The Biometric system is the calibration and demographics analysis of the people's substantial and observable characteristics. The main use of this technology is for recognition and access control, or for recognizing particular characteristics that are under observations. The basic thought of biometric verification is that all are different and an individual can be recognized by his or her inherent physical or behavioral features.

There are various forms of biometric recognition strategy such as the face, fingerprint, hand geometry, retina, iris, signature, voice. This scheme exclusively addresses face detection for the real image, namely face recognition. Among all biometric characteristics, face liveness detection has been revealed as only identical biometric system traits to distinguish among different images. The large scale evaluations are determined observable execution in terms of recognition accuracy.

In simple terms, face detection is a Biometric system widely used to recognize the authorized person based on either behavioral characteristics or physical. Spoofing intrusion is nothing but flanking or damaging biometric recognition systems using surety traits to use systems without authorization of permitted users.

II. LITERATURE SURVEY

In face liveness detection, anti-spoof depends on features used like eye shimmering and various facial configuration. Rely upon methods wont to avoid spoofing, face liveness detection methods are classified mainly as motion-based, frequency-based, or quality-based.

Gang Pan et al.[1] presents a spoofing against the image in face recognition using real-time liveness detection using Impulsive eye blinking. This method requires only a standard camera no other hardware to avoid spoofing attacks in a non-intrusive manner. Eye blinking is a physical process that instantaneously opens and closes eyelids persistently in a very minute. The common camera captures 15 frames per second, it gives two frames of faces which used as proof against spoofing attack. Two captured frames in the sequence are acknowledge as an independent. HMM(Hidden Markov Model) produces features from a finite state set. Normal eyeblink activity using HMM features finds a spoofing attack.

Tan et al.[2] presented a real-time and non-intrusive method for face spoofing detection. Their method involved analysis of the Lambertian model. To appreciate this method, an oversized face spoof database was collected with 15 subjects under various conditions of illumination. Over 50,000 photograph images were captured by a customary webcam. Evaluation of the proposed method provided promising performance for spoof detection.

Li et.al.[3] proposed a technique using Fourier spectral analysis methods to classify real face images and fake face images.
Wang et.al.[4] proposed a system that uses a single picture or group of pictures by using Fourier spectra to get the face liveness detection. The Feature of the live face and fake face is unique. During this technique, albedo surface ordinances are utilized to separate fake and live faces. Fourier spectra give the distinctive light reflectivity which provides lots of difference in live and fake faces. As an example, a Fourier spectrum of fake faces contains frequency components with higher amplitude than live faces.
There are different deep learning approaches like Convolutional Neural Network (CNN), Stacked Autoencoder [5], and Deep Belief Network (DBN) [6], [7]. CNN usually used algorithms in image and face recognition. CNN may be a quite artificial neural network that employs convolution methodology to extract the features from the computer file to extend the number of features. CNN was firstly proposed by LeCun and was firstly applied in handwriting recognition [8].

P. Huang et al. [9] proposed an Adaptive Linear Discriminant Regression Classification (ALDRC) Algorithm by taking a special examination of various additions of the training samples. ALDRC utilized various weights to differentiate the various additions of the training samples and used this type of weighting information to live the BCRE(Between-Class-Reconstruction-Error) and WCRE(Within-Class-Reconstruction-Error). Then ALDRC tries and finds an optimal projection matrix that may increase the ratio of the BCRE over the WCRE. Broad experimentation was done on the AR, FERET, and ORL face databases showed the efficiency of ALDRC.

More recent attempts include Niinuma et al. 's use of a 3D Morphable Model(3DMM) for multiview 2D face recognition [10]. In their approach, a 3DMM model is fitted to each frontal gallery face image and used to enhance the gallery set by images of various poses. For an input 2D face image, its pose is estimated and a subset of gallery images of parallel pose used for matching.

Tharanga et al. [11] used the PCA method for face recognition for his or her attendance system, achieving an accuracy of 68%.
The proposed method is comparatively well whereby the teacher took a photograph for each student in school using a camera, which they then uploaded onto the computer server system after school [12]. Then the server would detect the face in each photo and cut it. Finally, students would log on and choose their faces which might then record their attendance.

The Haar feature proposed by Viola et al. [13] combined with the AdaBoost cascade classifier can detect face quickly. Since then, many researchers have dedicated themselves to using more advanced features to boost the accuracy of face detection, like Local Binary Patterns (LBP) [14], Histograms of Oriented Gradients (HOG) [15], Scale-invariant Feature Transform (SIFT) [16].

III. FACE RECOGNITION SYSTEM

In this, the system where it can be used to be determined by providing a set of training images of faces. It is used to define a face edge which is a bunch of face-like images. Later this, when a face is encountered it measures a face for it. By connecting this with common faces and using statistical analysis it decided whether the present image is a face or non-face. So, if an image is deciding to be a face the system will determine whether it knows the identity. The block diagram of the face recognition system is as shown in Fig.2.
The present system is classified into two parts such as

A. Face liveness Detection
B. Face Recognition System

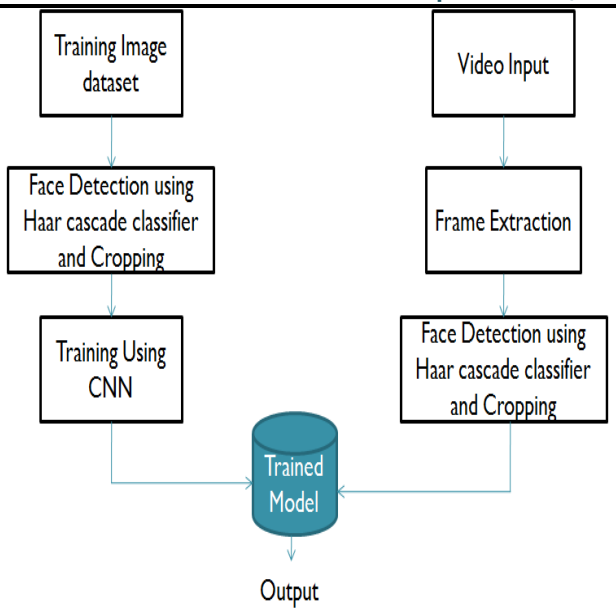


Fig. 1. Block Diagram of Face Recognition System

3.1. Face Liveness Detection

The block diagram of the face liveness detection system is as shown in Fig. 1.

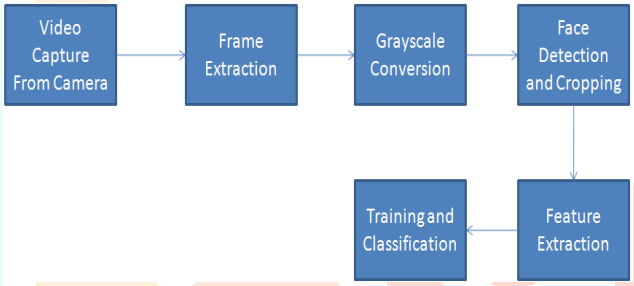


Fig. 2. Block Diagram of Face Liveness detection System

Face recognition is widely used for security purposes as compared to other systems that are used for security purposes. Face recognition done with digital images or videos. But as we know like other biometric methods, face recognition is also easily spoofed or unsafe for our security system, because face recognition can easily be spoofed. Spoofing a security system is done with images, video frames. To protect from this kind of scams and spoofing, liveness detection technology has been implemented in our system.

The face liveness detection approach identified based on the variant types of the approach used for liveness detection. This categorization helps to understand different spoof attacks scenarios. The main objective is to offer a simple path and a more secure face liveness detection way.

Liveness detection technology assures that the input biometric element is from a living user and it is not created artificially. The aliveness detection technique is used in different ways are bring out

- **Using hardware:** An extra hardware that can be used to identify the liveness in the input biometric sample of the user. It is an extensive method because of the expected cost for adding the extra device to identify liveness so quicker than the remaining methods.

- **Using different software:** Procedure software is used to identify the liveness sample. This will be done at the conversion stage. The use of this method is that it is less expensive than hardware-based methods but is equivalently slow than the other early methods.

- **Combination of hardware and software:** They may use the combination of both hardware and software techniques for liveness detection. Various intrinsic properties to the human body such as consumption, reflectance, etc and impulsive signals of the human anatomy such as blood pressure are also used for detection of life symptoms.

3.1.1 Database

The images of three different persons are collected in the database. The real images of a person were collected directly by capturing the image of printed photos. Each database contains image samples in different environments. The database distribution of the data used for training and testing is as shown in Table 3.1.

Table 3.1: Database distribution of the face liveness detection system

Database	Real	Fake
Total Images	2110	2326
Training	1583	1745
Testing	527	581

3.1.2. Preprocessing of face liveness detection

The approach of preprocessing contains grayscale conversion. The video stream is an input of the system. The frame is extracted to the video stream for the next processing. The extracted frames are in the RGB colorspace. And for the face detection using the Haar cascade classifier, the frames need to convert into the grayscale. Therefore in the preprocessing step, the RGB frame is converted into grayscale. The red color has more intuition than all of three colors and the green color that has not only less intuition than red color but also green color gives a smooth impact to the eyes. so the equation for this (Eq. 1.),

$$Grayscale = (0.3 \times R + 0.59 \times G + 0.11 \times B) \quad (1)$$

With this equation, Red contributed 30%, Green contributed 59% so it is most significant in all three colors and added to that blue contributed 11%.

3.1.3. Face detection

The object detection using a Haar feature-based cascade classifier is the effective object detection method. This is the machine learning-based approach where a cascade function is instructed from a set of positive and negative images. This is used to determine things in corresponding images. We work here with face detection. First, the algorithm needs lots of positive images and negative images to instruct the classifier. Then we were required to extract characteristics from it. Each feature is obtained only one value by deducting the sum pixel below the white rectangle from the sum of the pixels below the black rectangle.

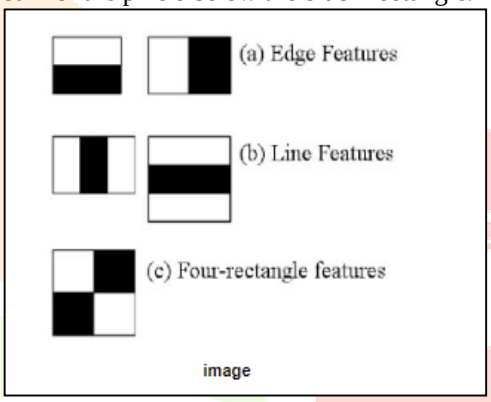


Fig. 3. Haar feature-based cascade classifier

All the feasible measurements and locations of every kernel were used to calculate more and more features. This requires a lot of computation. The 24*The 24 window result is over 160000 features for whole feature calculation, there we are required to find the sum of the pixels below the white and black rectangle. To resolve this, introduce the integral image so large your image, it reduces the calculation for a given pixel to a function requiring just four pixels. It produces objects quickly. So, between all these characteristics we are calculated, the maximum is inappropriate. For example, examine the below image. The uppermost row displays two quality characteristics. The initial feature selected implies targeting the object that the surface of the eyes is frequently dimmed than the surface of the nose and cheeks. The next feature selected depends on the object that the eyes are dimmed more than the span of the nose. So, the same window put into cheeks or some other place is irrelevant. So it is difficult to select out of the 160000+ feature. It is achieved by Adaboost.

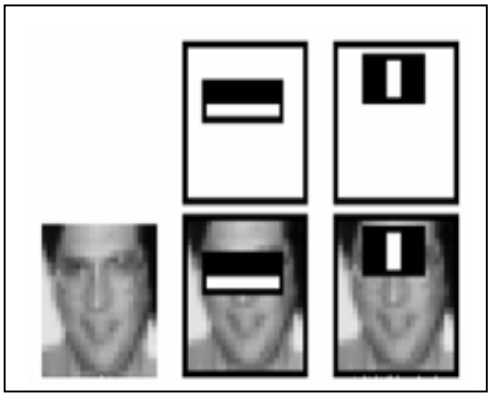


Fig. 4. Example of Haar cascade classifier

3.1.3. Feature Extraction

There are so many techniques that have been utilized to pull out the features from images. But, some commonly used methods are as follows:

- Color Features
- Spatial Features

3.1.3.1. Color Feature

The colors are commonly defined in the three-dimensional color spaces. The color span representation can be transformed as hardware-oriented and user-oriented. The hardware situated color spans, involving an RGB, CMY, and YIQ, depend on the three color stimuli theory. The RGB color span used by computers, graphics cardboard, and monitors or LCDs. It is made up of three components: Red, Green, and Blue, it is called base or primary colors. The color is derived by blending the three base colors. Determined by how much you remove from every single base color, you can produce all the colors which a monitor later displays. If you can mix red and green, you will get yellow and if you blend red and blue, you will get magenta. By blending all three roots colors with enough strength, you will get white color. So by blending the root color in various strengths, you can produce any essential color.

To explain that, how color can be produced within the cubes color space, Let consider the base color green which is placed on the vertical which is Y-Axis with an arbitrary range of 0-100% is at the Black end and 100% is at the full intensity. The model cube displays you what appears when you fixed green color to a sequence of stable values and then at every stable value differ the red and the blue components. You can effectively create a variety of horizontal pieces and scenes every piece from the top.

3.1.3.2. Spatial Features

The input of the feature extraction block is only a cropped face of the user; it may be live or fake. Features are accustomed to discover the liveness of the users are illumination characteristics that are luminance factor this is for photo attack and the mask texture factor being used. To make the system more efficient and accurate other basic image properties are used in the liveness detection like energy, entropy, mean RGB values, Skewness, standard deviation and mean YCbCr values. These values vary for the fake and live faces, which gives much more space to set a threshold to differentiate live and fake faces.

- **Luminance**

Luminance is a density of the light which is leaving a plane area in a specific direction. It gives the density of reflected light from a particular surface. This illumination characteristic changes for each surface, as the surface becomes more contrast its value increases, and value depends on the type of surface. If luminance is calculated for a live face then its value is different from the image of a fake face. Due to the 3D effect of eyes, nose, etc. the luminance value for the live face from each part is random while for fake the face value is approximately the same because of the no changes in structure or shape of image photo or mobile photo its plane surface.

An image is calculated using RGB parameters of that image. Luminance will be calculated using the following formula (Eq.2).

$$Luminance = (0.299 \times R + 0.587 \times G + 0.114 \times B) \quad (2)$$

In this equation Red, Green and Blue are three basic color component mean values of an image.

- **Variance**

It provides several gray size values fluctuations to the denote gray size values.

- **Standard Deviation-**

The second color moment which is the standard deviation, it will be deliberated by removing a square root of the variance of the color in distribution

3.1.4. Classifier

It is a problem of identifying in a firm of classification a new perception into, on the foundation of a training set of data including perceptions whose grouping association is known.

3.1.4.1. KNN

K-nearest neighbor method is a supervised learning classifier. It finds the K-nearest Sample from the training data and assigns the label of the highest votes of the nearest neighbor to the trial case.

The algorithm for KNN classification :

1. A positive integer value k is defined, along with the new sample.
2. We choose the k data entries in our dataset collection which is to the new testing sample.
3. We find out the most similar classification of these entries.
4. We give some samples to the new sample by using the value of K and this is the classification.
5. The value of K change until not getting satisfactory results

KNN is an algorithm which is the simplest of classification algorithms which is applicable for supervised learning applications. It is to find the closest match to the test data in feature space. Classification of the KNN algorithm is shown in the following figure

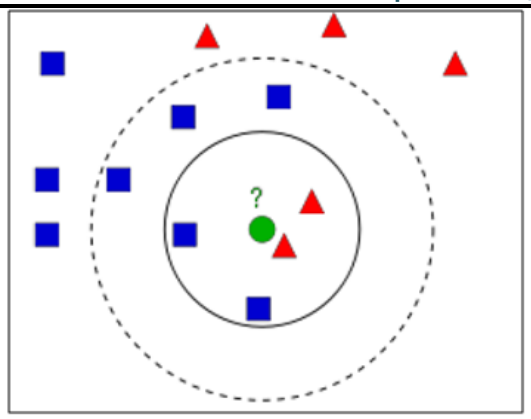


Fig. 5. Classification of KNN algorithm

In the above Fig. 5. , there are two families, one is Blue Squares and another one is Red Triangles. We can call each family as Class. In the above diagram, the houses are shown also called feature space. when new members come in the town he can create the new home as shown in Fig. 5. as we can see in the green circle.

3.1. Face Recognition system

The block diagram of the face recognition system is as shown in Fig.6.

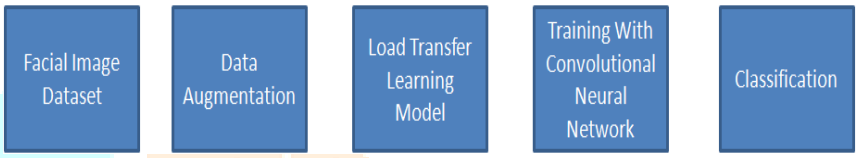


Fig. 6. Classification of KNN algorithm

The main steps include Image Acquisition, Database development, Face detection, Pre-processing, Feature extraction, and Classification stages. There two main phases: Training (enrolment) phase and testing (Recognition) phase

3.1.1. Training

Each block of the training phase is explained below.

3.1.1.1. Image Capture

The database is created by collecting the number of faces of different students. In this approach, the database of three students is recorded for the development of the system. The database distribution of the training and testing data is as shown in Table 3.2.

Table 3.2. Database distribution for the face recognition system

Database	Total Image	1	2	3	4
Training	1913	361	631	591	330
Testing	825	120	211	196	298

3.1.1.2. Preprocessing

Sometimes the captured facial images may need some preprocessing like cropping the face, resizing to a reasonable size, histogram equalization for eliminating illumination variance, reduction of noise, thresholding, converting to the binary, or grayscale image, etc. The given input image is in RGB color format. For further processing, the RGB is converted into grayscale images. conversion of RGB to gray color given by Eq. (1).

3.1.1.3. Data Augmentation

Data augmentation which is a technique to artificially create new training data from old training data. This can be done using specific techniques to examples from the training data which create new and different training datasets. Image data augmentation creates the transformed version of the dataset which belongs to the same class of the original image and it is a type of data augmentation. Image data augmentation is only used for the training dataset, and which can not be applied to the validation or test the dataset.

3.1.1.4. Training and testing Using CNN

CNN's are Neural Networks that have proven very effective in areas that are image recognition and classification. CNN's are a type of feed-forward neural network made up of many layers.

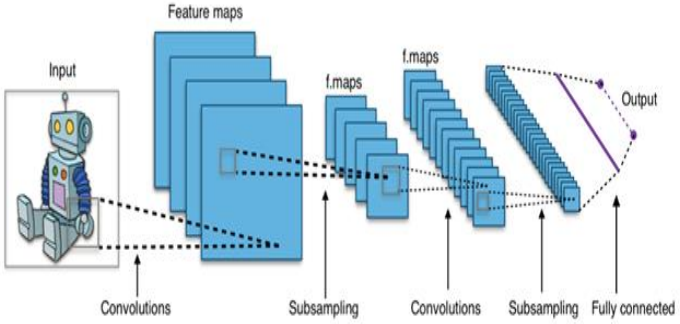


Fig. 7. Classification of KNN algorithm

- **Convolutional Layer**

This layer operates on a convolution layer to perform the core building block. The secondary purpose of the Convolution layer is to extract features to input data which is an image. This layer maintains the spatial relationship between the pixels by learning image features using a small square of input images.

- **Pooling Layer**

This layer reduces the dimension of each activating map but it continues to have very much important information. The input images are separate into the non-overlapping rectangles sets. Each region is downsampled by the nonlinear operation which is as average or maximum. This layer is usually placed in between the convolutional layers.

- **ReLU Layer**

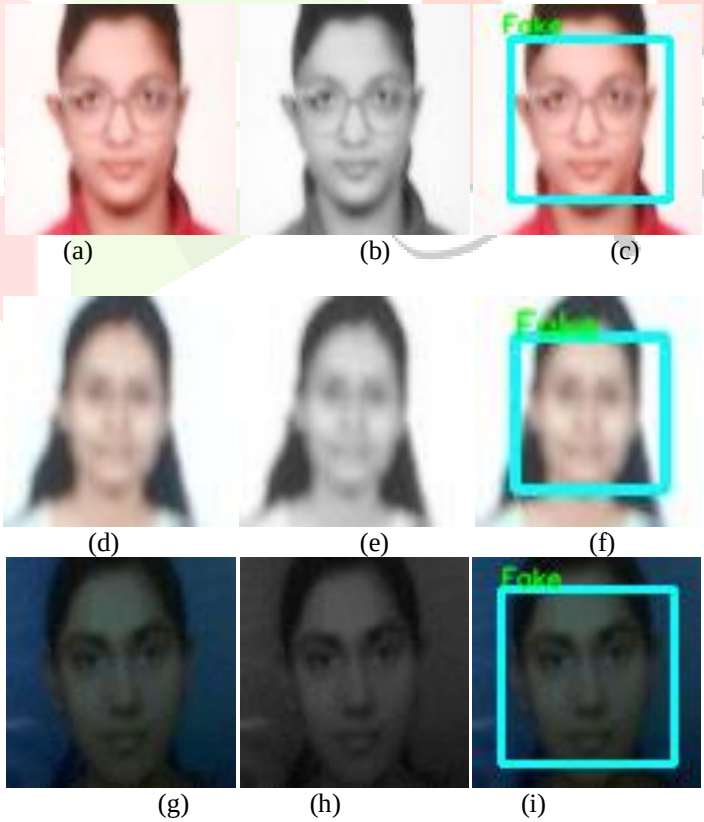
It is a nonlinear operation and it includes units employing the rectifier. This is the element-wise operation that means it is applied per pixel of all negative values map by zero in the feature.

IV. RESULTS

The results of this system are presented using Qualitative and Quantitative analysis for face liveness detection and face recognition system.

4.1. Qualitative Analysis

The qualitative analysis of the face liveness detection system is as shown in Fig. 8 and Fig. 9.

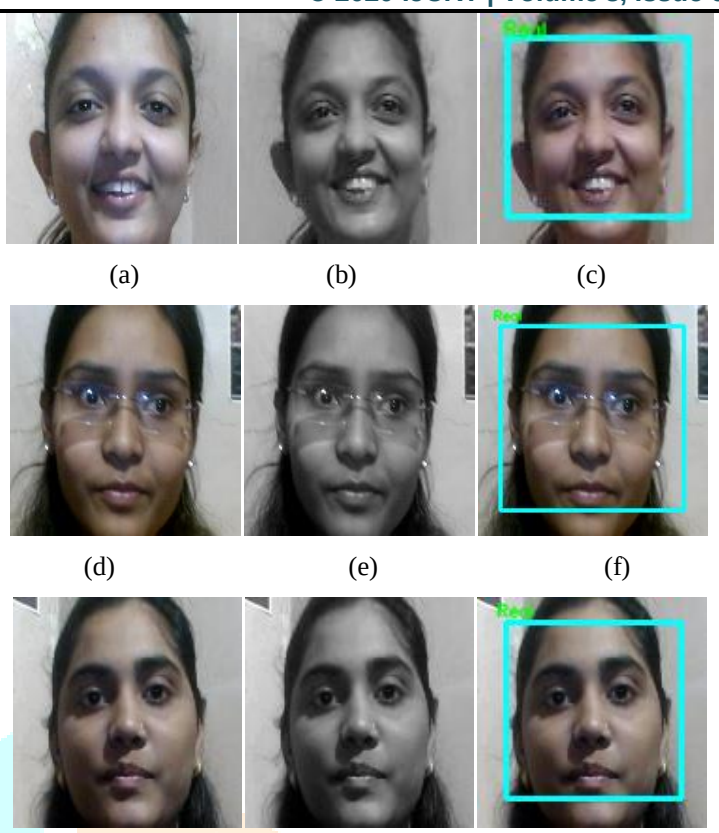


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig.8 Result on Fake images (a,d,g) Input Image (b, e, h) Grayscale Image (c,f,i)



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig.9. Result on Real images (a,d,g) Input Image (b,e.h) Grayscale Image (c,f,i)

The qualitative analysis of the face recognition system is as shown in Fig. 10.

Fig.10. Output of the face recognition system

4.2. Quantitative Analysis

The quantitative analysis of the proposed system is calculated using an accuracy parameter. The accuracy of the face recognition system is given as (Eq.3.).

$$Accuracy = \frac{No\ of\ faces\ correctly\ detected}{Total\ no\ of\ samples} \quad (3)$$

Table 4.1. Quantitative analysis of face liveness detection

Algorithm	Parameters	Accuracy (%)
SVM	RBF	79.92
KNN	K=1	99.61
	K=3	99.04
	K=5	98.59
	K=7	98.27

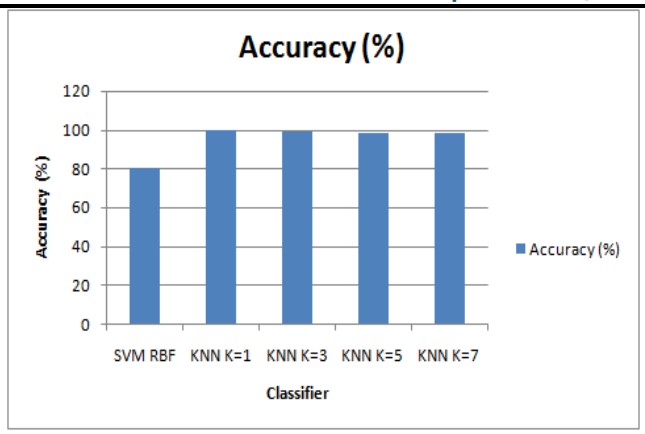
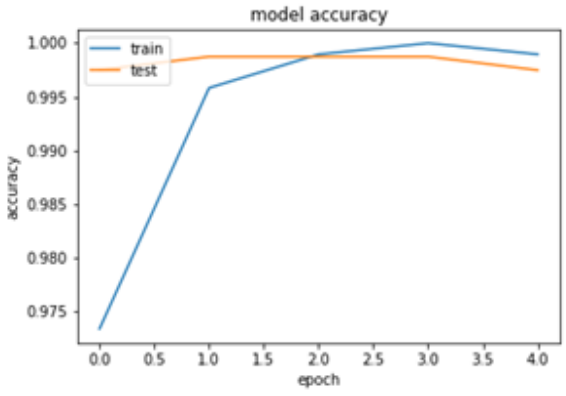
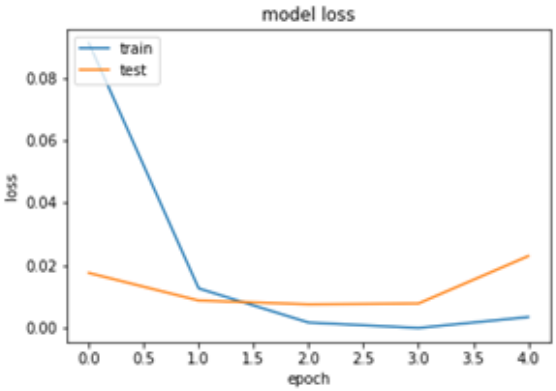


Fig.10 Performance Of The Different Machine Learning Classifier

The performance of the Convolutional Neural Network for the face recognition system is as shown in Fig.11. in terms of accuracy and Loss.



(a)



(b)

Fig.11 Quantitative Analysis (a) Accuracy (b) Loss

V. CONCLUSION

The face recognition and liveness detection system is an interesting research approach. In this approach, the camera will capture the image as an input. To create the database faces are detected using the Haar cascade classifier model. Once the face is detected, the images are fed to the deep learning algorithm. Also, the automated system has more advantages over traditional methods, as it saves time, and accuracy is better. The proposed approach gives an accuracy of 99.40% on the training dataset.

REFERENCES

[1] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink -based anti-spoofing in face recognition from a generic web camera," in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[2] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Computer Vision–ECCV 2010, 2010, pp. 504–517

[3] J.W. Li, Y.H. Wang, T.N. Tan and A.K. Jain, "Live face detection based on the analysis of Fourier spectra", In Biometric Technology for Human Identification. 2004, pp. 296-303.

[4] Wang, T. Tan, and A. K. Jain, "Live face location dependent on the investigation of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identification., pp. 296–303, Aug. 2004.

[5]R. Xia, J. Deng, B. Schuller, and Y. Liu, "Modeling gender information for emotion recognition using Denoising autoencoder," in ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing – Proceedings, pp. 990–994, 2014.

[6] G. E. Hinton, S. Osindero, and Y. W. Teh, "A fast learning algorithm for deep belief nets," Neural Comput., vol. 18, no. 7, pp. 1527–1554, 2006.

[7] Y. Bengio, "Learning Deep Architectures for AI," vol. 2, no. 1, 2009.

[8] Y. LeCun, "Backpropagation Applied to Handwritten Zip Code Recognition," Neural Comput., vol. 1, no. 4, pp. 541–551, Dec. 1989.

[9] P.Huang, Z.Lai, G.Gao, G.Yang, and Z. Yang, "Adaptive linear discriminative regression classification for face recognition" Digital Signal Processing, 55, pp.78-84,2016.

[10] K. Niinuma, H. Han, "Automatic multi-view face recognition via3d model based pose regularization," in BTAS, 2013.

[11] Tharanga, J. G. Roshan, "SMART ATTENDANCE USING REAL TIME FACE RECOGNITION (SMART-FR)." Department of Electronic and Computer Engineering, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka.

[12] Xiao-Yong Wei, Zhen-Qun Yang, "Mining In-Class Social Networks for Large-Scale Pedagogical Analysis", ACM Multimedia 20.

[13] Viola P, Jones M J. Robust real-time face detection[J]. International Journal of Computer Vision, 2004 .57(2):137- 154.

[14] Ojala T, Pietikainen M, Maenpaa T., "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002,24(7):971-987.

[15] Dalal N, Triggs B., "Histograms of oriented gradients for human detection", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2005. IEEE, 2005, pp. 886- 893.

[16] Ng P C, Henikoff S. SIFT: Predicting amino acid changes that affect protein function [J]. Nucleic acids research, 2003, 31(13).