Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **S-6 Year 2023** Page **593:601***

Real-Time Anti Spoofing Face Detection with Mask Using CNN

Amoolya M[1*], Amrutha B P[2], Ambika Y N[3], Alok R Patil[4], Thirumagal E[5]

[1,2,3,4,5]*Department of Computer Science Engineering, REVA University, Bangalore, Karnataka, India*
Email: [1]amoolyam1999@gmail.com, [2]amruthapradeep738@gmail.com, [3]ambikanagaraj32@gmail.com, [4]alokpatil676@gmail.com, [5]thirumagal.e@reva.edu.in

**Corresponding author's E-mail: amoolyam1999@gmail.com*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 29 Nov 2023

Abstract

As COVID-19 spread the whole way across the world, a significant number of us got mindful of how significant face covers are. Medical services authorities and nearby foundations from one side of the planet to the other are encouraging individuals to wear masks ,as it is the best way to forestall the transmission of the infection. Masks have without a doubt frustrated the facial-acknowledgment industry; the innovation has likewise adjusted. It might sound odd yet wearing a cover does not really prevent a PC from recognizing somebody. We are intending to prepare our model to recognize whether the pictures are genuine or fake one even though individuals are wearing face cover. In this paper, we intend to make a liveness detector equipped for spotting counterfeit faces. To make a liveness detector, we will prepare a deep learning neural network fit for recognizing genuine versus counterfeit appearances. It deals with two correlative spaces: RGB space and multi-scale Retinex (MSR) space. The RGB space contains the point-by-point facial surfaces, yet it is sensitive to illumination whereas the MSR pictures can adequately catch the high recurrence data, which is discriminative for face recognition.

Keywords: *Face anti-spoofing, convolutional neural networks, liveness detection, open cv*

1. Introduction

Face recognition applications are becoming more popular than ever before, with applications ranging from face recognition on our smartphones to face recognition for mass surveillance. Face recognition systems are easily fooled by spoofing attacks these days. It is critical to create a face verification structure to effectively protect an individual's privacy. Over the most recent couple of years, Face recognition frameworks have gained popularity in recent years as a result of face-rich features that provide a solid biometric sign to see individuals for a variety of purposes. Face biometrics are gradually being used as a replacement to passwords on mobile phones. Regardless of the remarkable advancements in facial recognition systems, the multifaceted nature of spoofing attacks continues to evolve as more complex counter methodologies are developed, which are efficient, productive, and decreased. Face Spoofing: Face spoofing is an attempt to gain someone else's perks or access rights by imitating someone else's face with a snapshot.

Anti-spoofing: The task of preventing false facial verification by using a snapshot, video, mask, or other alternative replacement for an authorized individual's face is known as facial anti-spoofing. A few instances of assaults:

Print assault: The attacker uses someone's picture in a print assault. The picture is printed or displayed on a high-tech computer. This is the most often seen type of attack, since most peoples have facial pictures available on the internet, and photos could be obtained easily without authorization.

Replay/video assault: A more refined approach to deceiving the framework, which usually includes a circled video of a casualty's face. This strategy ensures immediate and facial changes to appear more 'characteristic' as compared to keeping someone's picture.

3D mask attack: In this type of attack, a mask is used as the parodying apparatus of choice. It is a lot more complicated than just seeing a face frame. Notwithstanding regular facial developments, it

empowers approaches to misdirect some additional layers of insurance like profundity sensors. Photograph assault and video answer trap are the most by and large saw assaults.

Face recognition using OpenCV:

OpenCV is a multi-stage library that can be used to develop ongoing PC vision applications. It primarily focuses on image processing, video capture, and analysis, with features such as face recognition and item location. OpenCV plays a major role in actual event. The OpenCV library has over 2500 updated libraries that can be used to identify and perceive faces, recognize objects, organize human activities in recordings, and monitor camera movements, among other things. To create a face recognition system, we first perform face exploration, then use profound learning to extract face embeddings from each face, then train a face recognition model on the embeddings from each face using deep learning, and then recognize faces in the two pictures and video transfers using OpenCV.

II. Related works

[1] Kunj Bihari Meena proposed a way to distinguish CG photographs from PG pics using a two-flow convolutional neural community (CNN). there are numerous fields inclusive of the movie enterprise, virtual reality, video games where pc-generated (CG) pics are used broadly. CG pictures also can be misused in many approaches. consequently, there may be a want of distinguishing CG pics from real photographic (PG) pics. in the proposed technique, the primary move takes the advantage of the know-how found out by the pre-trained VGG-19 network, and then this know-how is transferred to analyse the distinct capabilities of CG and PG pictures. we advise a 2d stream, that pre-processes the photos the use of 3 excessive-skip filters which intention to help the community to cognizance on noise-based awesome functions of CG and PG photographs. sooner or later, we recommend an ensemble version to merge the outcomes of the proposed two streams.

[2] Surya teja karri proposed 3-D-CNN strategies: MicroExpSTCNN and MicroExpFuseNet, for unconstrained facial miniature demeanour notoriety with the guide of abusing the spatiotemporal records in CNN structure. The MicroExpSTCNN thinks about the entire spatial records, while the MicroExpFuseNet is based absolutely at the 3-d-CNN highlight combination of the eyes and mouth zones. The investigations are executed over CAS(ME) 2 and SMIC microb articulation data sets. The proposed MicroExpSTCNN form outflanks the cutting-edge techniques.

[3] Daqiang Mu proposed a way which utilizes CNN (convolutional neural local area) works as opposed to hand made highlights for face hostile to satirizing. with an end goal to intertwine more prominent discriminative chrominance information, this paper proposes a solitary face hostile to parodying strategy principally dependent on a twofold stream CNN and large demonstrating of highlights from overall face photo and nearby fixes, as well as coordinating the elements of uncommon shade territories, we investigate the discriminative portrayal for face against mocking.

[4] Yongjae Gwak proposed a method for face anti-spoofing based on stereo facial photographs. because the 3-dimensional shape of a live face genuinely yields a structural distinction within the photograph pair taken via a stereo camera, whereas sizable variations do now not occur in faux faces of -dimensional planes, this paper proposes to learn the differences of left-proper image pairs in the latent space of a deep neural network. One critical gain of the proposed method is that the structural distinction is encoded implicitly in a nonlinear way thru the deep architecture without explicitly computing the disparity. The experimental outcomes on a constructed dataset revealed the proposed technique to be effective for numerous spoofing assaults.

[5] Dongjun Yu, proposed a remarkable face against satirizing recognition set of rules utilizing least rectangular weight combination of channel-based element classifiers. To this surrender, we first circuit the tone and surface highlights through data entropy, the spatial and recurrence highlights are then sifted and melded by utilizing SVM-RFE trademark determination approach. likewise, the combination abilities of two convolutional neural organizations are worked through autoencoder. second, for the produced 3 sorts of combination abilities, we receive AdaBoost, SVM and Randomforest to achieve the solid classification, individually. The last objective of the proposed strategies to utilize the most un-rectangular method to change the most reasonable loads of the got 3 assortments of class impacts, through this implies the strong and green face hostile to caricaturing discovery result can be accomplished.

III. COMPARISON AND EXISTING WORKS.

SL NO	YEAR OF PUBLICATION , AUTHORS and NAME OF THE PAPER	METHODOLOGY	PERFORMANCE	FUTURE WORK/CHALLENGE
1	2012 J Yang , Stan Z Li Face Liveness Detection Using 3D Structure Recovered From a Single Camera	For a given video or image captured from more than two viewpoints, the facial landmarks are detected and key frames are selected	Support vector machine classifier is trained to distinguish real or fake face	It is difficult to estimate in-depth information and this method is sensitive to noise
2	2012 Andre Anjos LBP-TOP Based Counter Measure Against Face Spoofing Attack	A method to verify faces by Counter measures based on texture and motion. Texture is analyzed using lower binary patterns and motion is analyzed using correlation method	The input video frames are divided into N frames window. Each frame is then analysed based on the motion and micro-texture	User authentication is an important step to protect information

dimensional shape of a live face genuinely yields a structural distinction within the photograph pair taken via a stereo camera, whereas sizable variations do now not occur in faux faces of -dimensional planes, this paper proposes to learn the differences of left-proper image pairs in the latent space of a deep neural network. One critical gain of the proposed method is that the structural distinction is encoded implicitly in a nonlinear way thru the deep architecture without explicitly computing the disparity. The experimental outcomes on a constructed dataset revealed the proposed technique to be effective for numerous spoofing assaults.

[5] Dongjun Yu, proposed a remarkable face against satirizing recognition set of rules utilizing least rectangular weight combination of channel-based element classifiers. To this surrender, we first circuit the tone and surface highlights through data entropy, the spatial and recurrence highlights are then sifted and melded by utilizing SVM-RFE trademark determination approach. likewise, the combination abilities of two convolutional neural organizations are worked through autoencoder. second, for the produced 3 sorts of combination abilities, we receive AdaBoost, SVM and Randomforest to achieve the solid classification, individually. The last objective of the proposed strategies to utilize the most un-rectangular method to change the most reasonable loads of the got 3 assortments of class impacts, through this implies the strong and green face hostile to caricaturing discovery result can be accomplished

SL NO	YEAR OF PUBLICATION , AUTHORS AND NAME OF THE PAPER	METHODOLOGY	PERFORMANCE	FUTURE WORK/CHALLENGE
3	2014 Javier Galbally Face Anti-Spoofing Based On General Image Quality Assessment	The input image is first converted to grayscale image. The grayscale image is then filtered using a low-pass Gaussian filter for generating the distorted version of the image.	Comparing the quality between the grayscale and distorted version of the input image by using Image Quality Assessment	Very low degree of complexity
4	2015 D Wen Face Spoof Detection With Image Distortion Algorithm	The features Considered are color diversity, reflection, blurriness and Chromatic moment.	features are trained and Classified using Support Vector Machine (SVM) to identify the face to be either real or spoof face.	It works when the images are captured by web cameras . There is no public-domain face spoof database using mobile phone

SL NO	YEAR OF PUBLICATION , AUTHORS AND NAME OF THE PAPER	METHODOLOGY	PERFORMANCE	FUTURE WORK/CHALLENGE
5	2015 K Patel Live Face Video vs Spoof Face Video : Use Of Moire Patterns To Detect Replay Video Attack	In this we analyze the moire pattern aliasing that commonly appears during the recapture of video or photo replays on a screen in different channels (R , G , B and Grayscale) and regions	The moire patterns can be detected using MLBP and DSIFT features	They capture replay video attacks using either low quality cameras or expensive
6	2016 J Komulainen Face Spoofing Detection Using Colour Texture Analysis	Proposed a methodology to detect the close-up non-real faces by using Histogram of Oriented Gradient (HOG) descriptors.	The alignment of the face is analysed using the upper body detector.	Possibility of printed attacks is more

SL NO	YEAR OF PUBLICATION ,AUTHORS AND NAME OF THE PAPER	METHODOLOGY	PERFORMANCE	FUTURE WORK/CHALLENGE
7	2019 L Ashok Kumar Face Anti Spoofing Using Neural Networks	The convolutional network architecture is constructed to arrest the spoofed faces from accessing in the name of genuine users. Own datasets of real and fake images are created to train the neural network.	The two datasets are trained separately to resolve the absolute outcome.	There's no stable set of features that the convolutional network would see and understand

IV. PROPOSED WORK AND MODULES IDENTIFIED

Spoofing discovery is a classification issue. In profound learning time, a characteristic arrangement of this assignment is to take care of the information RGB pictures to a deliberately planned CNN. In our venture we mean to make a liveness identifier equipped for spotting counterfeit faces and perform against satirizing in face acknowledgment frameworks. To make a liveness indicator, we will prepare a profound neural organization fit for recognizing genuine versus counterfeit appearances. We will attempt to clarify the progression of the arrangement in the following steps:

Step:1: Building the image dataset.

Step:2: Implement LivenessNet.

Step:3: Training the model.

Step:4: Implement it into the real-time.

1) Building the image dataset

In our project we will be training our model using two types of datasets namely: real dataset and fake dataset. For building the real dataset we will record the video using the web camera of the system wherein for the fake dataset we will record the video of a person in our smartphones and then replay it Infront of the web camera. As an input, we'll give our programme the path to these images, and as an output, we'll give it the path to a directory where each of the cropped faces will be saved. We will filter the weak faces and skip the similar adjacent frames. We create blob from an image, define the frame dimensions and extract face ROI coordinates.

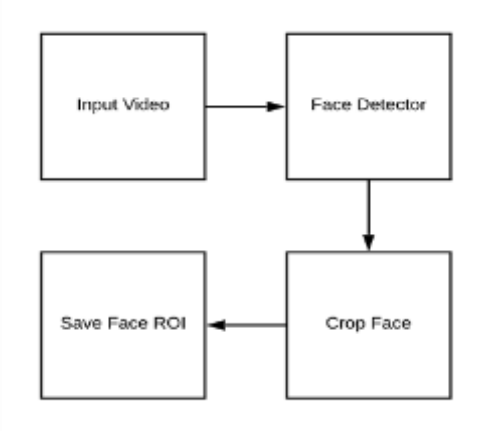


Figure. 1 Diagrammatic flow of dataset collection

2)Implement LivenessNet

Livenessnet is a simple CNN network. In this step we add other layers to our CNN network like :

RELU LAYER- It is an initiation layer.

POOLING LAYER - The pooling layer lessens portion by integrating the yield of neuron packs from one layer into a neuron in the next layer.

FULLY CONNECTED LAYER -completely associated layer interface of each neuron in one layer to each neuron in another layer.

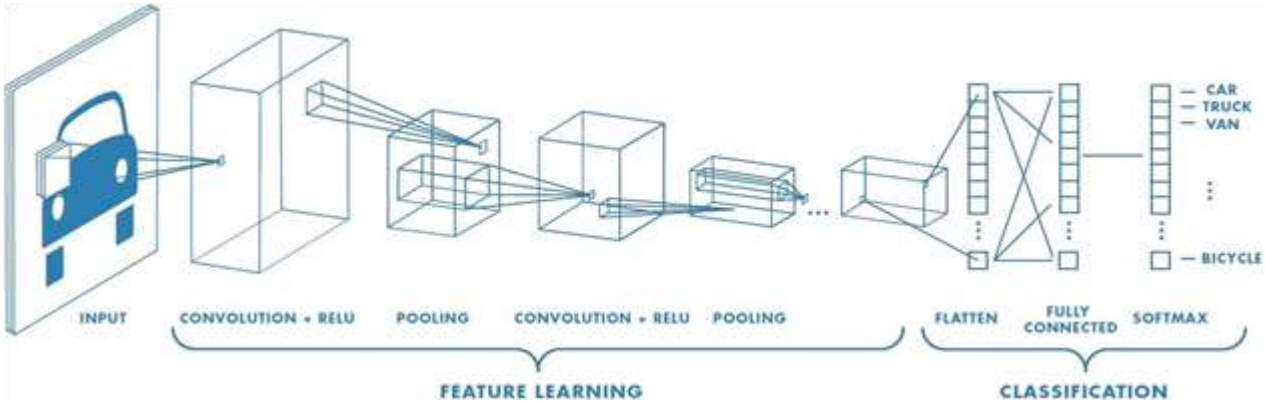


Figure. 2 The various layers of CNN

3) Training the model

We use the datasets of real and fake images and also the liveness Net to train our model. Initially we load the data then resize them to desired pixel values. Each picture will have a label associated with it, which will be stored in the label list. The data must then be partitioned for training and research.

In the end we compile and train our face liveness model.

4) Implementing it into real-time

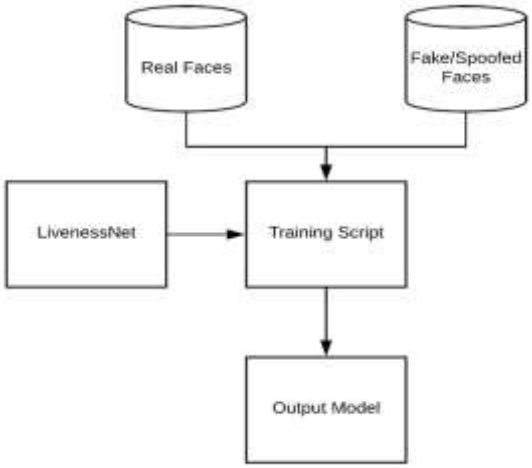


Figure.3 Block diagram

A) Modules Split-up:

The modules identified in the proposed system are as follows:

1. KERAS: Keras is an open-source library for neural networks that provide a Python framework.

2. TENSORFLOW: TensorFlow is a free and open-source software library for dataflow and distinct programming that can be used to solve a variety of problems.

3. SKLEARN: It features support vector machines, random forests, gradient boosting, k-means, and DBSCAN, amongst many other classification, regression, and clustering algorithms, and is designed to work with the Python numerical and science libraries NumPy and SciPy.

4. MATAPLOTLIB: Matplotlib is a Python library that allows users to create static, animated, and interactive visualizations.

B) Algorithm:

1) Surface analysis, which involves registering Local Binary Patterns (LBPs) over face districts and categorizing the appearances as genuine or satirical using an SVM.

2) Recurrence investigation, like as looking at the face's Fourier space.

3) Variable centring analysis, such as investigating the range of pixel values between two sequential edges.

4) Calculations based on generalizations, such as eye growth, lip development, and flicker position These calculations help to monitor the client's eye development and squints to ensure that the customer

is not keeping an image of anybody else (since a photograph does not really flicker or move its lips) [17-21].

SYSTEM REQUIREMENTS

Hardware Requirements: Windows 10(i3 processor),

8 GB RAM

Software Requirements: Python

PyCharm

Anaconda 3

Modules: Open CV (cv2) and NumPy

3. Results and Discussion

Figure.4 Loss graph

The above graph shows the accuracy of training in four ways. Screen shots of data sets: We have two datasets namely real images and fake images.

Real: Real video is given as input and the program is written to prepare the data set like this where the images are cropped and stored in the same size.

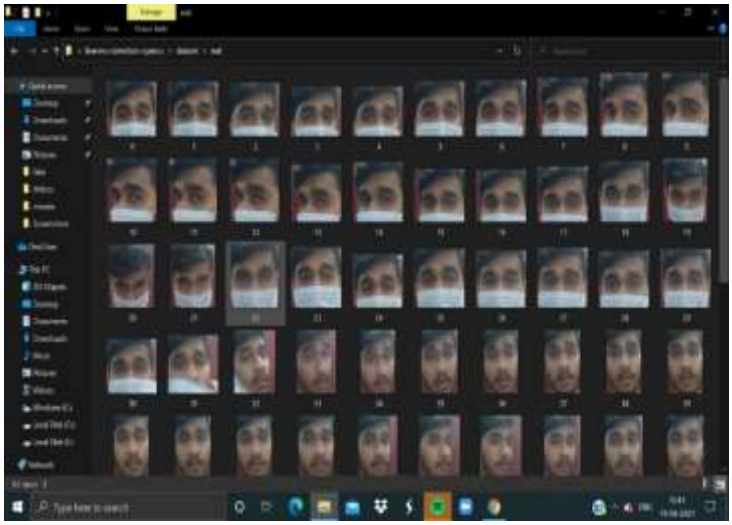


Figure.5 Real images dataset

Fake: Fake video is given as input and the program is written to prepare the data set like this where the images are cropped and stored in the same size.

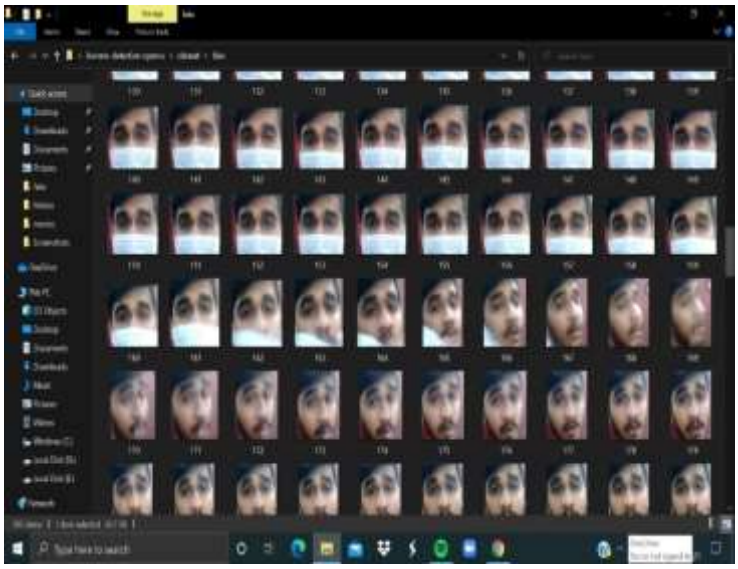


Figure.6 Fake images dataset

Analysis:

(To analyse whether the images are real or spoof)

For real image:

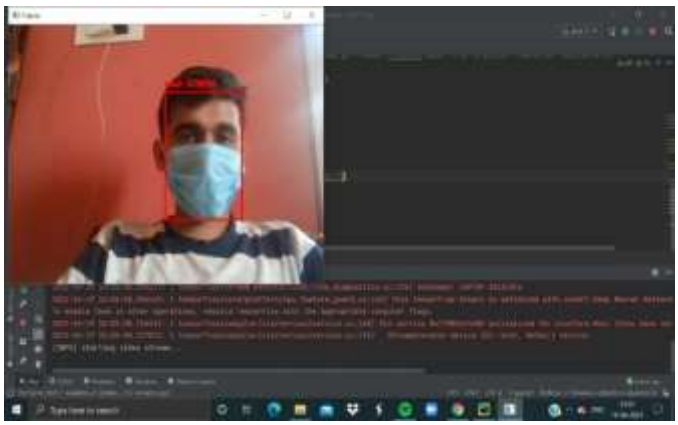
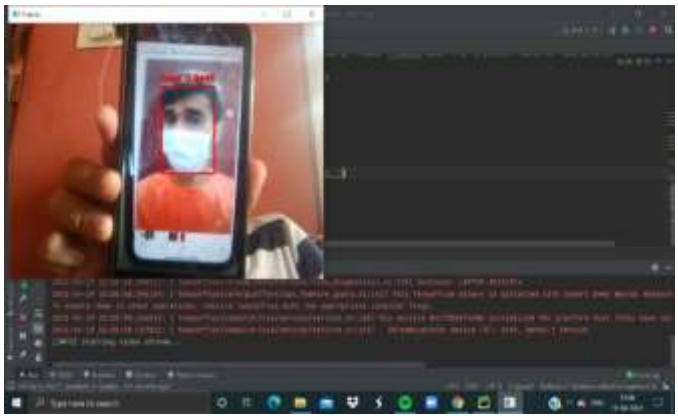


Figure.7 Detection of real image

As you can see in the figure a real face is detected.

For spoof image:



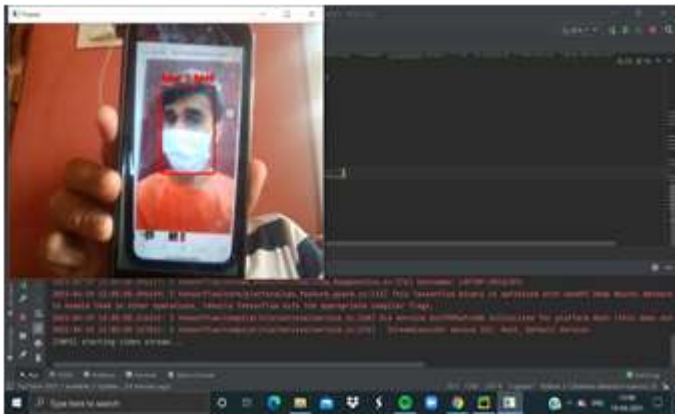


Figure.8 Detection of fake image

If the person tries to spoof using photo masking or video masking techniques then the result will be shown as fake, as you see in the figure 6.

4. Conclusion

To adequately defend an individual's privacy, face recognition systems must always be made more accessible, and we must be able to identify fake faces. We used OpenCV to detect liveness in order to accomplish this. We developed a liveness detector for face recognition systems that can detect fake faces and perform anti-face spoofing. We used OpenCV, TensorFlow, and Keras libraries. We have repeatedly prepared the model with data collection to framework using Keras and sklearn modules.

Acknowledgment

This paper and the examination behind it would not have been conceivable without the remarkable help of our institution teachers. Their eagerness and encouragement have been a constant motivation that kept our work on target. We would like to take this opportunity to express our gratitude to our major project Guide, Prof. Thirumangal E, School of C&IT for continuously supporting and guiding us in every endeavour as well as taking a keen and active interest in the progress of every phase of our Major project. Thank you for providing us with the necessary inputs and suggestions for advancing with our mini project work. We deeply appreciate the wise guidance and express our sincere gratitude to our professor for her ingenuity.

References:

[1]AP Song, Q Hu, XH Ding, XY Di, ZH Song , "Similar face recognition using the IE-CNN model". IEEE Access, 2020.

[2]YX Yang, C Wen, K Xie, FQ Wen, GQ Sheng, XG Tang ,"Face recognition using the SR-CNN model". Sensors, 2018.

[3]SZ Li, J Lu ,"Face recognition using the closest feature line method". IEEE transactions on neural networks, 1999.

[4]J Li, K Xie, FQ Wen, "Face recognition using the deep CNN model based on decision-level fusion", Sensors, 2018

[5]M Khan, S Chakraborty, R Astya,"Face Detection and recognition using OpenCV", 2019 International Conference Computing Communication, and Intelligent Systems.

[6]Bienvenido B. Abad, Jr,"Proposed Image Pre-Processing Techniques For Face Recognition Using Opencv",Proceedings of the 3rd SPUP International Research 2017.

[7]K Goyal, K Agarwal and R Kumar, "Face detection and tracking: Using OpenCV",2017 International conference of Electronics, Communication and Aerospace Technology.

[8]Z Balogh, M Magdin, G Molnár,"Motion Detection and Face Recognition using Raspberry Pi, as a Part of, the Internet of Things", Acta Polytechnica Hungarica, 2019 .

[9]U Scherhag,C Rathgeb, J Merkle,"Face Recognition Systems Under Morphing Attacks: A Survey, IEEE Access 2019.

[10]Z Deng, X Peng, Z Li,"Mutual Component Convolutional Neural Networks for Heterogeneous Face Recognition", IEEE Transactions on Image Processing (Volume: 28, Issue: 6, June 2019).

[11]S Venkatesh, H Zhang, R Ramachandra,"Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs?",2020 8th IWBF.

[12]G Singh, A K Goel,"Face Detection System by Digital Image Processing",2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA).

[13]R Singh, A Agarwal, M Singh," On the Robustness of Face Recognition Algorithms Against Attacks and Bias",Proceedings of the AAAI Conference on Artificial Intelligence 2020.

[14]K. S. Krishnapriya, V Albiero, K Vangara,"Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone", IEEE Transactions on Technology and Society (Volume : 1, Issue: 1, March 2020).

[15]M Abdelmaksoud, E Nabil,"A Novel Neural Network Method for Face Recognition With a Single Sample Per Person",IEEE Access (Volume: 8) 2020. [16] Sudhan Murugan Bhagavathi, Anitha Thavasimuthu, Aruna Murugesan, Charlyn Pushpa Latha George Rajendran, A Vijay, Raja Laxmi, Rajendran Thavasimuthu, Weather forecasting and prediction using hybrid C5.0 machine learning algorithm International Journal of Communication Systems, Vol. 34, Issue. 10, Pp. e4805, 2021.
[17] PM Surendra, S Manimurugan, A New Modified Recurrent Extreme Learning with PSO Machine Based on Feature Fusion with CNN Deep Features for Breast Cancer Detection, Journal of Computational Science and Intelligent Technologies, Vol. 1, Issue. 3, Pp. 15-21, 2020.
[18] PK Sadineni, Comparative Study on Query Processing and Indexing Techniques in Big Data, 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 933-939, 2020.
[19] AH Omar Baabood, Prajoona Valsalan, Tariq Ahmed Barham Baomar, IoT Based Health Monitoring System, Journal of Critical Reviews , Vol. 7, Issue. 4, pp. 739-743, 2020.
[20] Sajay KR, Suvanam Sasidhar Babu, Vijayalakshmi Yellepeddi, Enhancing The Security Of Cloud Data Using Hybrid Encryption Algorithm, Journal of Ambient Intelligence and Humanized Computing, 2019. https://doi.org/10.1007/s12652-019-01403-1
[21] Bindhia K Francis, Suvanam Sasidhar Babu, Predicting academic performance of students using a hybrid data mining approach, Journal of Medical Systems, 43:162, 2019. https://doi.org/10.1007/s10916-019-1295-4