iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.34746

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Bare Face Person Recognition System using Deep Learning

Prachi Satpute[1], Mayuri Kulkarni[2], Sayali Tarte[3], Sharwaree Nimbalkar[4], Prof. Jitendra C. Musale[5]
[1, 2, 3, 4, 5] *Computer Department, ABMSP's Anantrao Pawar College of Engineering and Research, Pune -411009*

Abstract: ***Nowadays, maintaining a good hygiene is very important to prevent many diseases like Corona Virus Disease (COVID-19). It has been rapidly affected our day-today life by disrupting the world trade and movements. The World Health Organization (WHO) recommend to the world that all people must wear a mask to prevent COVID-19. The use of masks is part of a comprehensive package of prevention and control measures that can limit the spread of certain respiratory viral diseases. Wearing a protective mask has become a new normal and beneficial for human being to avoid certain diseases. In the near future, many public service providers will ask the customers to wear the masks to provide their services. Therefore, face mask detection has become an important task to help global society. This paper introduce a simplified approach for face mask detection by using Deep learning and python as the programming language. We are also using Open-CV, to search for faces within a picture and then identifies if it has a mask on it or not. By using this system, the surveillance camera system present at some public Space will automatically detect whether the persons are wearing a mask or not.***

Keywords: Input Image/Live Video Input, Face Detection, Image Pre-processing, Mask Detection, Open-CV, Classifier, Image Encryption and Decryption.

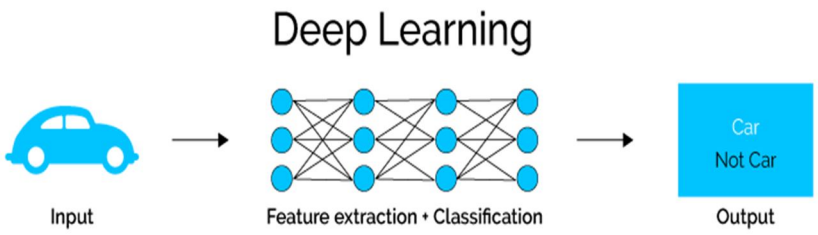
I. INTRODUCTION

Over the recent years, face mask detection system has been considered as the most essential system to avoid certain diseases like COVID-19. Wearing a mask is very essential to prevent certain measures and it is one of the most important step in times when social distancing is very hard to maintain. The face mask detection process can be stated as follows: Given a database consisting of many face pictures of known people, one inputs a face picture of wearing mask or a live video stream, and the process aims to verify or determine the person in the input image or video is wearing a mask or not.

The face mask detection system using image processing and image encryption along with various algorithms has been of interest to many young as well as senior researchers. The development in this area has been quite speedy due to the pandemic situation like COVID-19. For this pandemic situation public should be aware of whether to put on the mask for source control or to avoid COVID-19. To restrain the spread of virus we have to wear a mask, so face mask detection has become a crucial task in present global society.

With the fast growing improvements in deep learning algorithms the attention towards developing the system that would be able to detect whether the person is wearing a mask has been ever increasing. Face mask detection deals with the location of face and determine whether it has mask on it or not. Such kinds of systems have been largely used in multiple educational and institutional organizations for checking whether the students as well as employees and workers are wearing a mask or not. Image processing is an integral part of Facial recognition systems and it deals with filtering, resizing, reshaping and enhancement of images which are further sent for detection to the actual system. This system is very useful in today's environment because it is used to detect the faces not only in static images and videos but also in real time inspection and supervision.

Deep learning - : Deep learning is a part of a Machine learning and it utilizes a hierarchical level of artificial neural networks to carry out the process of machine learning. This artificial neural networks are built like the human brain, to make intelligent decisions on its own. While so for the face mask detection system we are using AES Algorithm.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

In Deep Learning we are basically taking 3 steps

1) *Clutering:* Given a set of a pictures.
2) *Detect:* Find the faces in the pictures.
3) *Classification & Extraction:* Identify and extract the features and then compare both the images (real time image with the database image).

II. LITERATURE WORK

Following are the research papers we studied for the face mask detection system.

A. Deep Neural Network for Human Face Recognition.

1) Dr. Priya Guptaa, Nidhi Saxena, Meetika Sharma, Jagriti Tripathia
2) This paper gives information of Face recognition (FR), the process of identifying people through facial images, by using Convolution Neural Networks (CovNets), which is a type of deep networks has been proved to be successful for FR.
3) 2018 (IEEE Journal)

B. A real time DNN-based face mask detection system using single shot multibox detector and MobileNetV2.

1) Preeti Nagrath, Rachna Jain, Agam Madan, Rohan Arora, Piyush Kataria, Jude Hemanth
2) This paper proposes a face mask detection algorithm by using a shot multibox detector and MobileNetV2. The proposed approach in this paper uses deep learning, TensorFlow, Keras, and OpenCV to detect face masks.
3) 2021 (IEEE Journal)

C. Covid-19 Face Mask Detection Using TensorFlow, Keras and OpenCV.

1) Arjya Das, Mohammad Wasif Ansari and Rohini Basak.
2) This paper presents a simplified approach to achieve face mask detection using some basic machine learning packages like TensorFlow, Keras, and OpenCV and Scikit-Learn. The proposed method detects the face from the image correctly and then identifies if it has mask on it or not. A surveillance task performer, it can also detect a face along with a mask in motion.
3) 2019 (IEEE Journal)

D. An Image Encryption and Decryption using AES Algorithm.

1) Priya Deshmukh.
2) In this paper an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output. The AES algorithm for image encryption and decryption which synthesizes and simulated with the help of MATLAB software.
3) 2016 (International Journal of Scientific & Engineering Research Paper)

III. PROPOSED WORK

We are developing the Face mask detection (AI) app using Deep learning and Python as programming language along with image encryption technique to provide the high quality images for facial recognition and increase the security.
The System should strong enough to be able to detect whether the user is wearing a facial mask or not by using traditional image processing system. It should also be able to verify whether the user is wearing a facial mask in live video stream.
We are developing a system which can detect and recognize the face as well as facial mask. Initially we divide the system into four modules:

1) Face Detection
2) Face Recognition
3) Face Mask Detection
4) Image Encryption and Decryption

In Face Detection we are identifying the face of a user by removing all remaining portions in the image or in live video. This face detection includes three methods and they are as follows:

a) Image Processing – Coding
b) Image Enhancement and Restoration
c) Principle Component Analysis (PCA)

In face Recognition we are going to recognize the person's image by comparing it with the detected image of the same person. In this we are going to compare the two images one which is already stored in the database and other one which is real time detected image of a person. This face detection is done by two methods:

i) Segmentation
ii) Open CV

In face mask detection we are going to identify whether the person is wearing the facial mask or not. The main aim of this module to detect the peoples who's not wearing any mask. This can be done by using two processes:

- MobileNetV2
- Building Classifier

By using image encryption we are going to provide data security.
In this we are going to convert image into "unrecognizable" that is encrypted form. And in image decryption we are again convert this encrypted image into the original image. The image encryption have two types and they are as follows:

- Symmetric Encryption
- Asymmetric Encryption

The main motto of our system is to develop face mask detection system which uses Deep Learning as a key ingredient to recognize whether a person is wearing a facial mask or not. It also identify a person's facial mask from a video or Photo and then check whether they are wearing the mask or not.

A. Face Detection

Face detection is detecting a face of a person from its entire image. This is done by using image processing and pattern processing. So for the image processing we have to mainly focus on image coding and image enhancement.

1) *Image Processing – Coding:* It is a basic method to apply an invertible transform to the given image. Image processing is used to reduce the bandwidth of transmitted image. It approximate the image transform and then construct the approximate image by inverting the transform. This transform can be designed so that the errors in this approximation become less noticeable when an image is reconstructed from its transform. Image processing means processing of images using mathematical operations for which input is an image, series of images or a video such as a photograph or video frame and then the output becomes either an image or a set of characteristics or parameters related to that image. Image coding is mainly used for data storage, transmission of images over a network and in encryption. The images are made of very large numbers of bits the goal of image coding is to reduce that bit number.
2) *Image Enhancement and Restoration:* Image enhancement is used to improve appearance of an image. There are mainly 2D digital filters are used for point wise modification of the grayscale image. It is used to remove the effects of degradation on the image. It is a procedure of improving the quality and information content of original data before processing. The aim of image enhancement is to improve the interpretability or perception of information in images for human viewers, or to provide `better' input for other automated image processing techniques. Image restoration is the operation of taking corrupt/noisy/damage image and provide a clean, original image. It mainly used to "undo" the defects which degrade an image.
3) *PCA (Principle Component Analysis):* PCA is unsupervised, non- parametric statistical technique. It is used for dimension reduction and feature extractions of an image. It reduces the dimensionality of large dataset by transforming large set of variables into smaller ones which contain all the information of large dataset. The most important use of PCA is to represent a multivariate data table as a small set of variables in order to observe trends, jumps, clusters and outliers. It is normally used to produce a set of Eigenface. Eigenfaces are nothing but the name given to a set of eigenvectors when they are used in the computer vision problem of human face recognition.

B. Face Recognition

The aim of image recognition is the classification or Structural description of images. Image classification contain feature detection and image measurement. Image description consists of image segmentation and relational structure extraction. Detecting the presence of a specified pattern (such as an edge, a line, a particular shape, etc.) in an image requires matching image with a "template,"

Template matching is implemented as a linear operation in which the degree of match at any point is measured by a linear combination of image in gray levels with a neighborhood point. However, the result of such a linear operation is ambiguous. So such ambiguities can be eliminated by breaking the template into parts and requiring that part with specified match so that the conditions can be satisfied for each part, or for the most of the Parts. This approach has been used to detect curves of images.

1) *Segmentation:* Images are composed of many regions which have Different ranges of grayscale levels, or the values of some local properties so by considering this such image can be segmented. For segmentation there are mainly two methods Parallel method and sequential method. In parallel method region extraction is based on thresholding. Sequential method contains geometrical structures and gray-level properties so they can compare them with any available information about the types of regions or objects that are supposed to be present in the image. Such information can be used to control merging and splitting processes which can be used to create an acceptable partition of the image into regions. By simply we can say that segmentation is the process of partitioning a image into multiple segments like set of pixels (also called as image objects).
2) *Open CV (Computer Vision Library):* OpenCV is a Computer vision library of programming functions which is used at real-time computer vision. It is built to provide a common infrastructure for computer vision applications and it is also used to speed up the use of machine perception in the commercial products. OpenCV is the huge open-source library for the computer vision, machine learning, and image processing. And it plays a major role in real-time operation which is important for face recognition systems. By using it, one can process images and videos to identify objects, faces, or even handwriting of a human being. So we are using Open-CV library for computer vision, which provides bindings for Python. Open-CV uses machine learning algorithms to search for faces within a picture.

C. Face Mask Detection

Face Mask Detection Platform uses Artificial Network to recognize if a user is wearing a mask or not. If the user is not wearing mask then we have to recognize him. For the mask detection we have to build the Neural Network for image data generation and then apply the MoblieNetV2 model.

1) *MobileNetV2:* It is convolutional neural network architecture which is mainly used for mobile based applications. MobileNetV2 are small, low-latency, low-power models made to meet the constraints of a variety of use cases. It contain ability to run deep networks on personal mobile devices to improve uses experience, offering anytime, anywhere access, with the benefits for security, privacy, and energy consumption. In MobileNetV2, there are two types of blocks. One is residual block with stride of 1. And next block with stride of 2 for downsizing. It also contains three layers for both types of blocks. First layer is 1 X 1 convolution with ReLU6. The second layer is the depth wise convolution. The third layer is 1 X 1 convolution but without any non-linearity. It is used to developed detection Model with 97% accuracy, it will automatically detect person is wearing a mask or not in real-time video streams .For that we have to extract the face ROI and facial landmarks and then applied to the face by using the facial to compute. It determined the class label encoding based on probabilities that are associated with color annotation.
2) *Building Classifier:* We are going to make classifier so we can differentiate between faces with masks and without masks. So for building this classifier, we need input data in the form of Images. We have a dataset containing images faces with mask and without a mask, since these images are very less in number, we cannot train a neural network from scratch. Instead, we fine-tune a pre-trained network called MobileNetV2 which is trained on the Image net dataset. This classifier uses training data to understand how given input images are related to the class which contain mask and without mask categories.

D. Image Encryption and Decryption

Encryption is a process which uses finite set of instructions like an algorithm to convert the original image into the encrypted form. Such algorithms are called cryptographic algorithms. With the help of key and algorithm we can encrypt and decrypt the images and also improve the security. In this system the images in the dataset are stored in encrypted format. The authority to open in and view these images is only to the administrator who has the security key. New person can be registered into the system is verified by the admin which makes it highly secure.

Image encryption method makes information unreadable. So no hacker, or eavesdropper, including administrator and other have access to original images or any other data information through network.

1) *Symmetric Encryption:* It is called Private Key Encryption. It uses the same algorithm and key to both encrypt and decrypt the message or image. DES is also uses symmetric encryption format.
2) *Asymmetric Encryption:* It is called Public Key Encryption. It uses two different "one way" keys like a public key to encrypt the message and the private key to decrypt them. This encryption reduces the key distribution problem.

IV. ALGORITHM

There are many Face Recognition algorithms are present. These algorithms are mainly focus on the detection of frontal human faces. By using these algorithms we can perform image detection and recognition in which the image is matched bit by bit.
For face detection and recognition we are using SVM Algorithm because it gives better performance and high accuracy than the remaining algorithms. SVM uses the radial basis function kernels which are used to perform better as they can handle non-linearity in the data. As compare to other algorithms, SVM captures better inherent characteristics of the face.
While developing the system data/ image security is also important.so for this we are using encryption process who securely protect the data that you don't want anyone else to have access to. Many business industries use it to protect corporate secrets and data centers, government's use it to secure information, and many individuals use it to protect personal information to guard against theft. There are many algorithms which provide encryption to the system and they are as follows:

1) AES Algorithm
2) RSA Algorithm
3) DES Algorithm
4) Triple DES Algorithm
5) DSA Algorithm
6) Diffle-Hellman Algorithm
7) RC4 Algorithm
8) SEAL Algorithm

So to provide the data security for our system we are using AES algorithm. It is very strong algorithm and can be designed for maximum 256 bits. This algorithm is faster than the others and it requires less memory space. It is one of the most spread commercial and have open source solutions all over the world. It gives high level of practical security and very effective in software. Many hardware accelerators, including Intel processors uses AES instructions.

A. *Advanced Encryption Standard (AES) :*

AES stands for Advanced Encryption Standard (AES). It is one of the most popular and important techniques in the encryption field. The AES has the advantage over the traditional data security techniques because it can achieve better encryption performance as compared to RSA algorithm whereas; it has better security as compared to other technologies.

The features of AES are as follows –

1) It gives Symmetric key for symmetric block cipher.
2) It works in 128-bit data, 128/192/256-bit keys.
3) It is Stronger and faster than Triple-DES.
4) It Provide full specification and design details.
5) It's Software implementable in C and Java programming languages.

AES is an iterative cipher based on 'substitution–permutation network'. It comprises of a series of linked operations, which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). AES performs the computations on bytes instead of bits. It consider the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in way of four columns and four rows as a matrix for processing. Unlike DES, the number of rounds in AES is variable and it depends on the length of the key. AES algorithm use 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys for the encryption process. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key as we can see in below diagram.

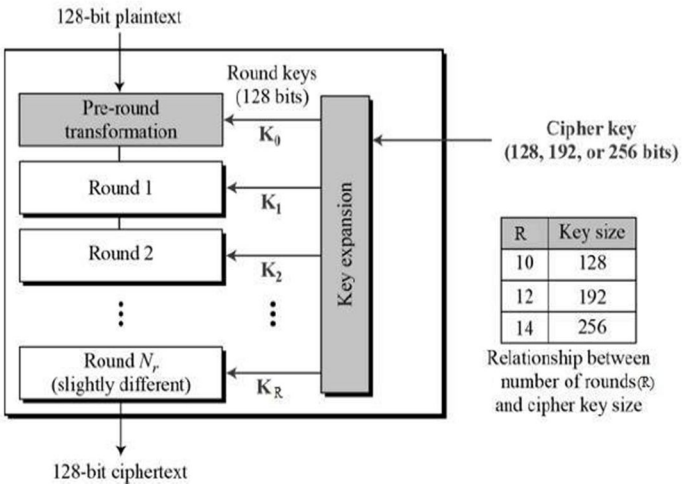


Fig: AES Algorithm Schematic Structure

AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. This classification is done on the basis of the key which is used in the algorithm for encryption and decryption process. The numbers are represent in a size of key in bits. This key size determines the security level as the size of key increases the level of security is also increases.

For encryption process there are four rounds:

a) Substitute byte
b) Shift row
c) Mix columns
d) Add round key

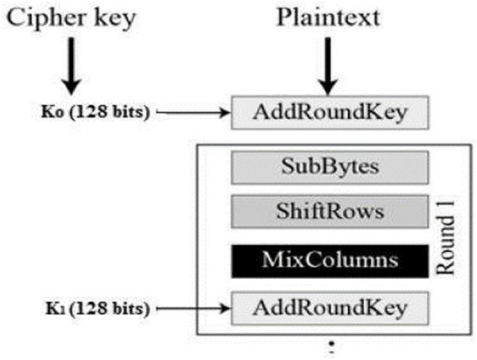


Fig: AES Process

Here, in above diagram we can see description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is given below:

i) *Substitute Byte (SubBytes):* In This 16 input bytes are filled by looking up a fixed table (S-box) given in the design. The result is in a matrix of four rows and four columns.
ii) *Shift Row:* Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows:

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

iii) *Mix Columns:* Each column of four bytes is now transformed using a special mathematical function. This function takes as input for the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix contains 16 new bytes. It should be noted that this step is not performed in the last round.

iv) *Add Round Key:* The 16 bytes of the matrix are now considered as 128 bits and are XOR to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are convert as 16 bytes and we begin another same round of process.

While the decryption process is the reverse process of the encryption which consists of:

- Inverse shift row
- Inverse substitute byte
- Add round key
- Inverse mix columns

Since sub-processes in each round are in reverse manner, the encryption and decryption algorithms are need to be separately implemented, although they are much related.

AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

V. IMPLEMENTATION WORK

The aim of the research was to develop a system that is able to detect the person from image which is uploaded as well as from live stream. Also, it was important to find out whether the person is wearing mask or not.

In order for the system to work, we implement three steps as follows:

A. It must detect a face.
B. It must recognize that face.
C. It must check whether the user is wearing a facial mask or not.

After completing the above implementation we found the system to be running correctly and as expected.

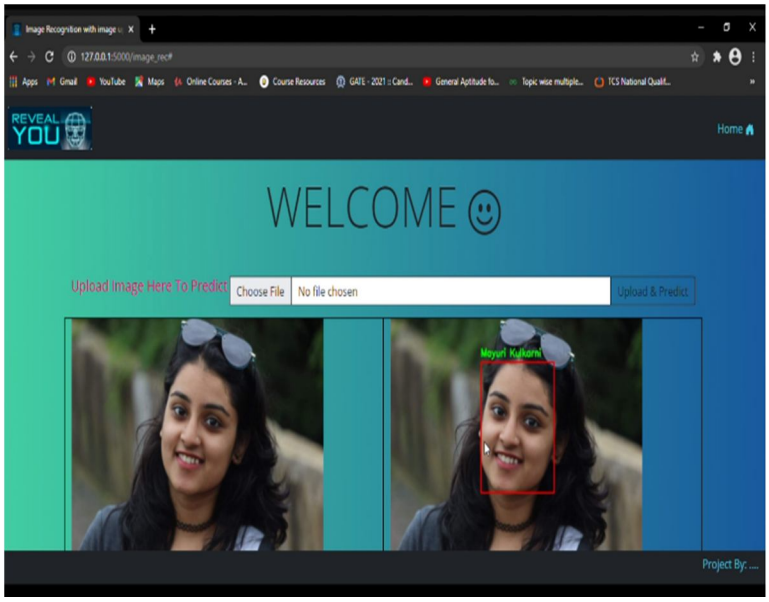


Fig V.I: Image detection from the uploaded image

Here in Fig V.I it is the screenshot of the system where it is able to detect the face of the person from uploaded image, successfully. It also gives the respective name of the person by comparing the uploaded image with the multiple database images.

Our initial aim is to detect the person is wearing a facial mask or not. So by using this system we can easily check out whether the person is wearing a mask or not and if they are wearing then it detect mask with green square box around the persons face.

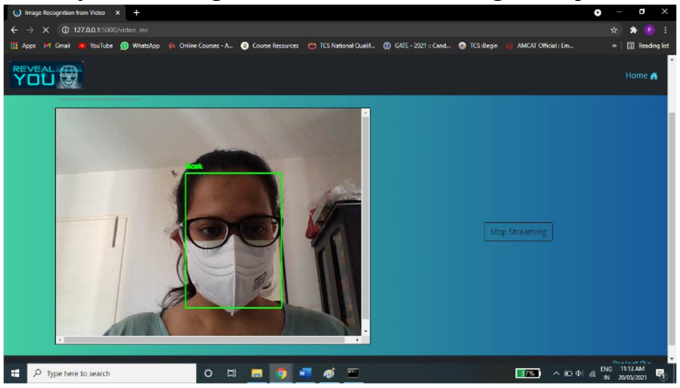


Fig V.II: Mask detection from live stream

The Fig V.II is the screenshot of the system where it is able to detect from a live video stream that a person is wearing mask.

We can also detect or recognize the person via live video stream. And along with recognition it will also check the presence of the facial mask.

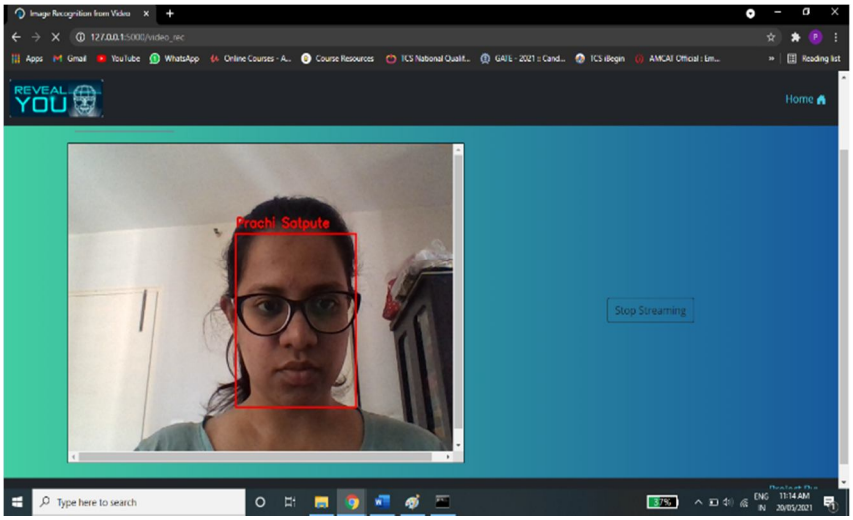


Fig V.III: Person detection from live stream

In this Fig V.III we can see that if the person is not wearing the mask, then the system draws a red color box around the detected face and the displays the name of the person.

VI. CONCLUSION

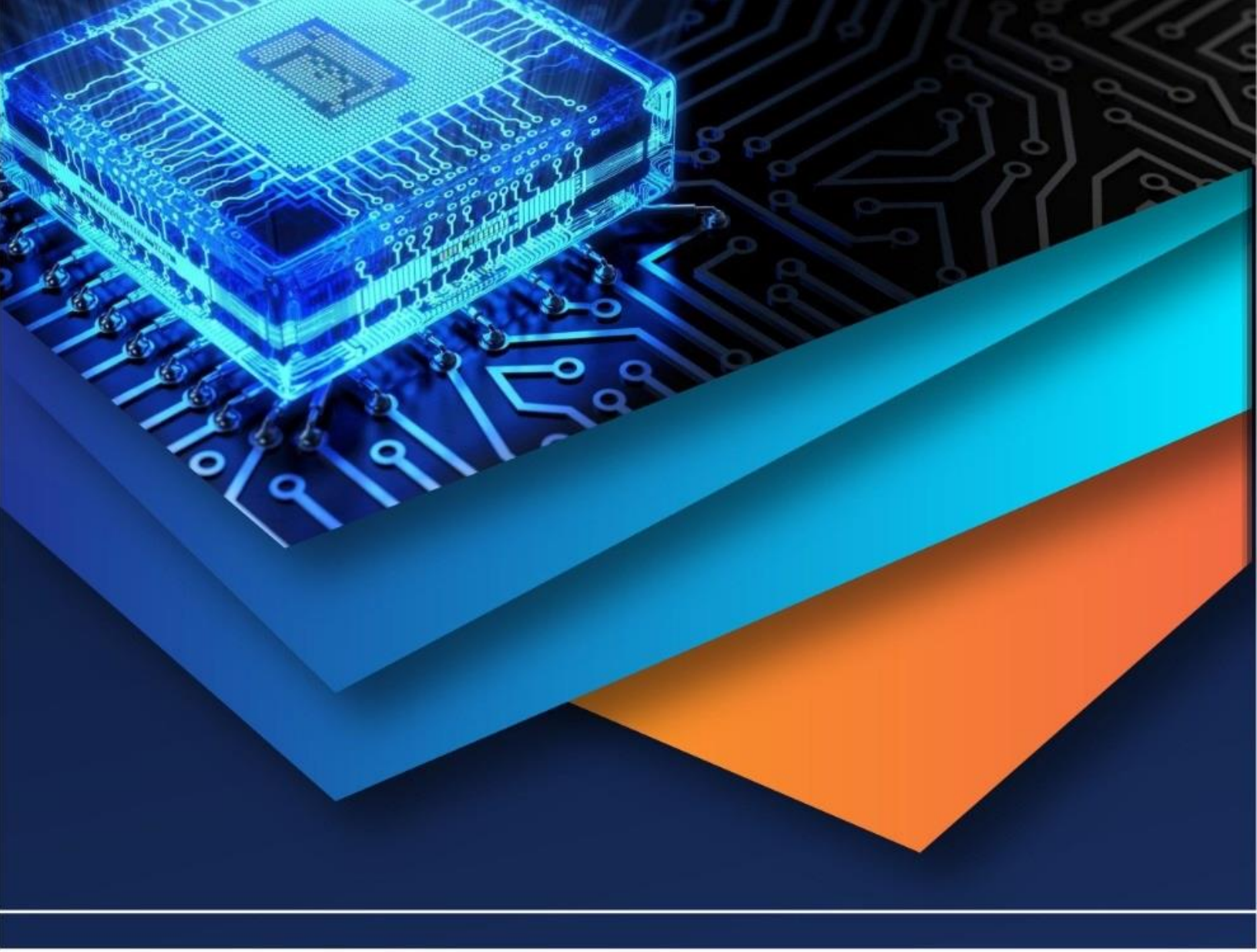
This paper mainly aims at developing a significant system of face mask detection in which Deep learning is a key ingredient as well as image encryption and AES algorithm. This article mainly reviews on a new face mask detection system where we can easily verify if the user or person is wearing a facial mask or not and if the person is not wearing a mask then identify that person by comparing the images that is real time image with the image that is stored in the database. But apart from that the Face expression, occlusion, pose variation, and illumination problems are still a big challenge in this system.

The image enhancement-coding, segmentation, PCA, Open-CV and MobileNetV2 techniques are most important for face mask detection. And for the image encryption and decryption AES algorithm is important.

Hence for the implementation where the biometric system must verify users who wears facial mask and identify the users who wears not. This facial mask scanning (Recognition and Verification) system is very effective and efficient in today's era.

REFFERENCES

[1] Dr. Priya Guptaa, Nidhi Saxena, Meetika Sharma, Jagriti Tripathia: "Deep Neural Network for Human Face Recognition." [2018 IEEE Journal].
[2] Priya Deshmukh: "An Image Encryption and Decryption using AES Algorithm." [2016 IJSER Journal].
[3] R.Gopinath, M.Sowjanya, (2012, October)."Image Encryption for Color Images Using Bit Plane and Edge Map Cryptography Algorithm", International Journal of Engineering Research and Technology (IJERT) volume-1, issue-8, pp.1-4
[4] William Stallings, "Advance Encryption Standard," in Cryptography and Network Security, 4th Ed., India: PEARSON, pp. 134–165.
[5] Vedkiran Saini, Parvinder Bangar, Harjeet Singh Chauhan, (2014, April)."Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application", International Journal of Emerging Science and Engineering (IJESE) volume-2, issue-6, pp.33-37.
[6] Manoj .B, Manjula N Harihar (2012, June). "Image Encryption and Decryption using AES", International Journal of Engineering and Advance Technology (IJEAT) volume-1, issue-5, pp.290-294.
[7] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, (2010, March), "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of computing,volume2-,issue-3,pp.152-157
[8] Kundankumar R. Saraf,Sunita P. Ugale, "Implementation of text encryption and decryption in Advance Encryption Standard", ASM'S International E-journal of ongoing Research in Management and IT



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY