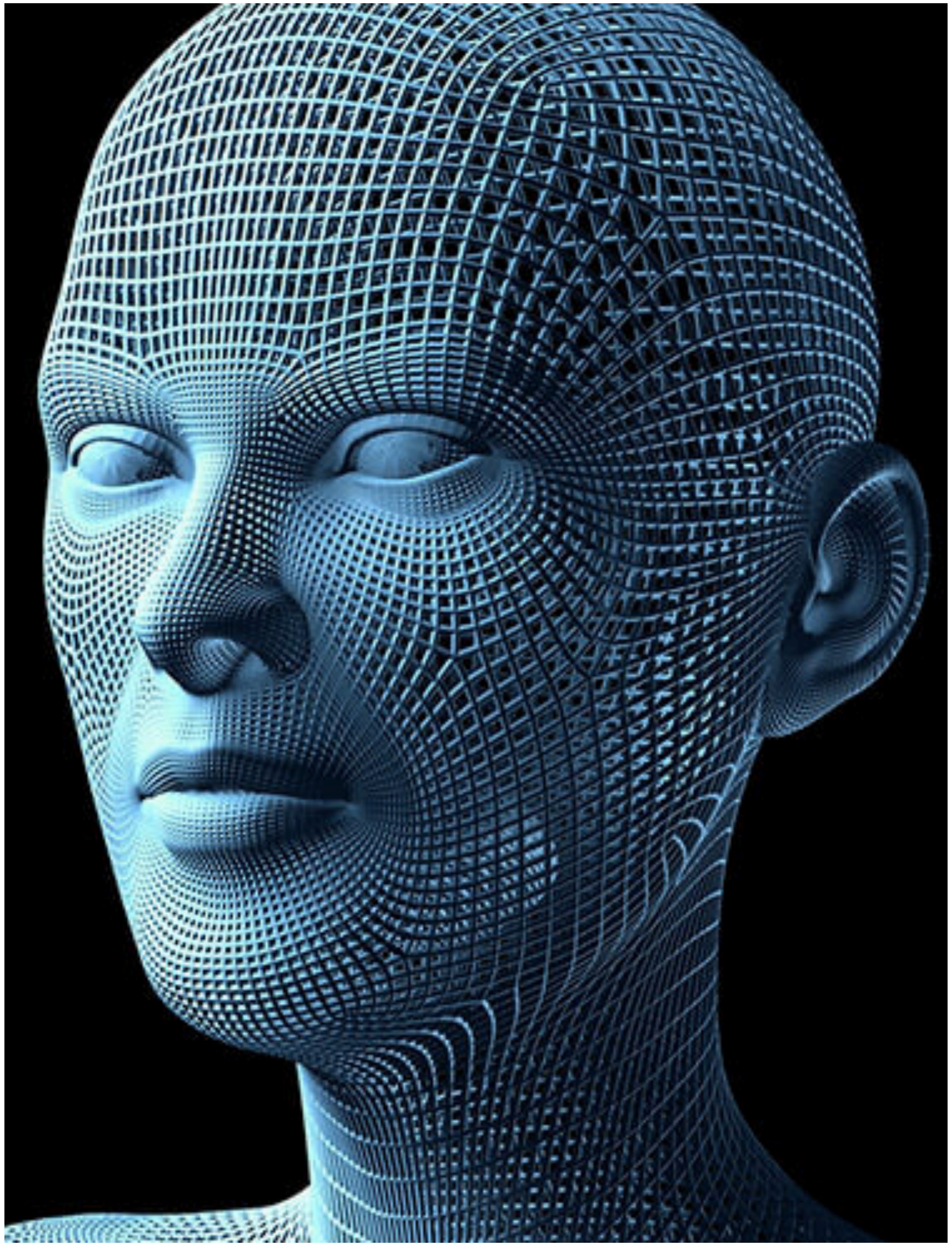
Image Recognition and Image Anonymization



GROUP MEMBERS

1.SANTOSH SAXENA

2018-22,CS,C-4

SYMBIOSIS INSTITUTE OF TECHNOLOGY

Software Requirements

1. Python latest version
2. Numpy , Keras , Sklearn libraries of Python

Hardware Requirements

1. Descent Laptop

Timeline

1.20/3/2020 (4:00 pm) to 21/3/2020 (4:40 AM))
{8 hrs}

Role

1.To make whole project

Facial Recognition with Image Anonymization

Santosh Saxena , 18070122060 , 2018-22 , C4 , CS

Symbiosis Institute of technology.

Abstract : As Technology is updating everyday. We also need security system to get updated. Todays World is generating a data of 1.7 mb in each second per person. Hence it is important that the data should be given in rightful hands. Todays World is heading towards Artificial Intelligence. At the same time it is also important that data present in machine in the form of dataset is also protected. For that some Anonymization Algorithm can be used. Hence forth we have came up with a solution of face recognition with Image Anonymization.

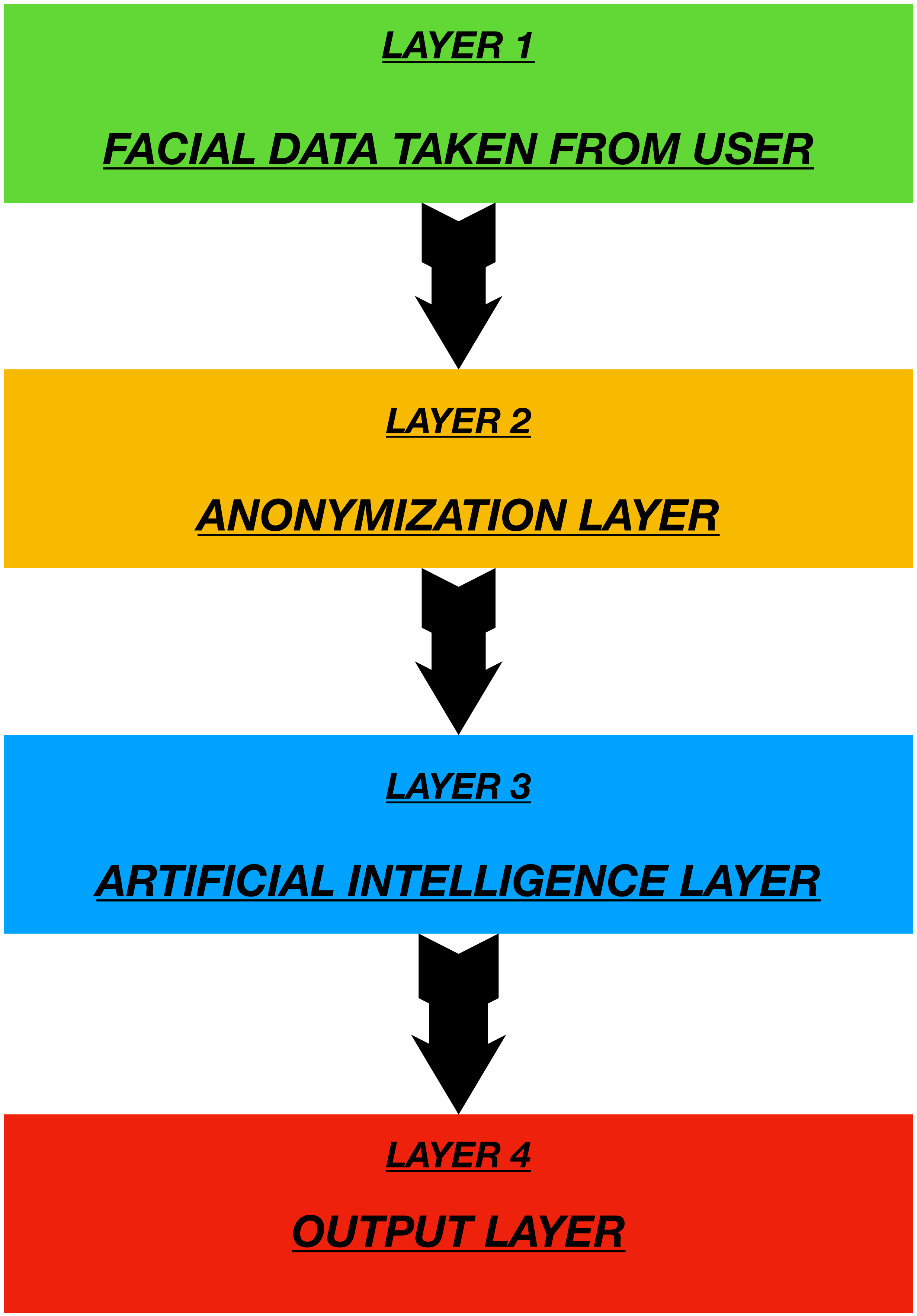
INTRODUCTION and LITERATURE SURVEY

The security system previously consists of username and password. The drawback of this security system is that it can be easily trackable. The next security system came is fingerprint unlock . Fingerprint gives you the proper security but due to hardware components it costs a bomb to the user which is a drawback of fingerprint security system. After this face unlock came into existence. Which is a very good security system as well as cause less expense. Hence if we apply Artificial Intelligence to face unlock security system. Then we can easily rely on our system in terms of data privacy.

The system which we will create is a facial recognition system, Which will classify a face into two categories i.e user and random person. In our Whole model data will be our main priority because our model will going to keep some confidential data. Hence It will a barrier for hacker to extract an important information through our data base. Our model will use CNN Algorithm for this classification. We will try to annonymize the data so that only an individual machine can understand the data and not by humans and any other machine.

Our security system will work same as face unlock security system. The main difference will be that the Artificial Intelligence will decide that data authentication should be provided or not to the person using that particular device. At the same time if an unknown person is trying use the confidential data immediately his facials details should be transfer to some authorised community which can take an action against that person.

ARCHITECTURE



LAYER 1

FACIAL DATA TAKEN FROM USER

LAYER 2

ANONYMIZATION LAYER

LAYER 3

ARTIFICIAL INTELLIGENCE LAYER

LAYER 4

OUTPUT LAYER

IMPLEMENTATION

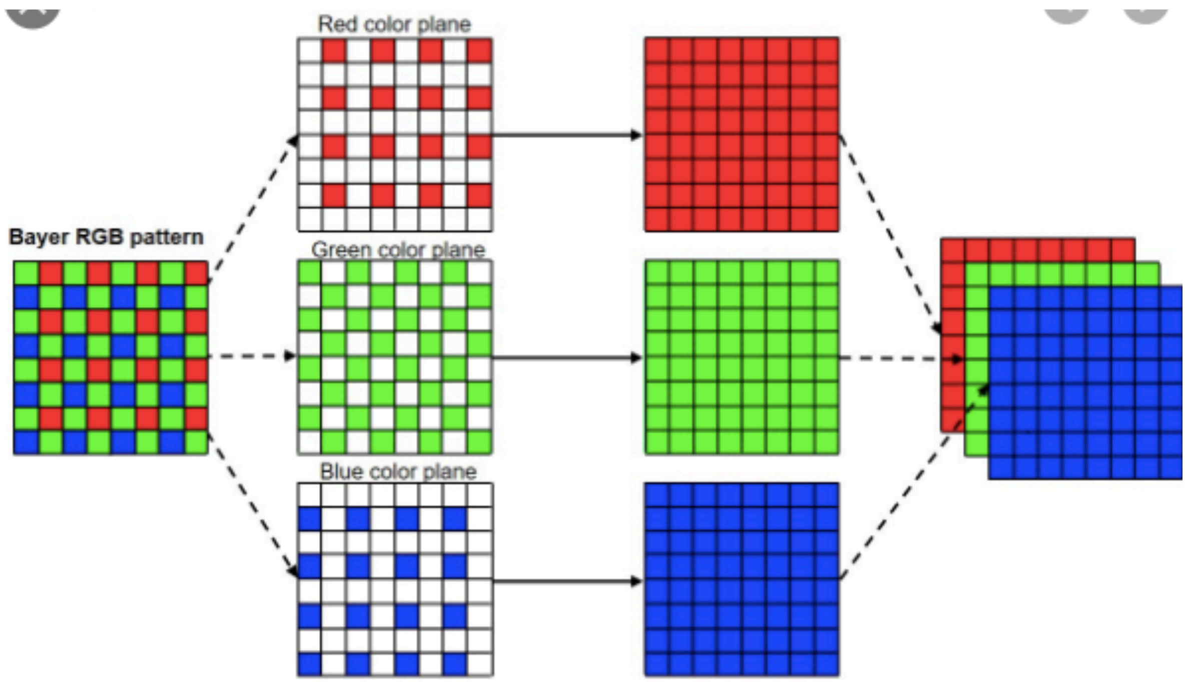
Layer 1 : Facial data taken from user

The first layer consists of taking a new data and feed to the machine to predict whether it is a user or not. The image received by the machine will be in this format. Machine will convert this image into 3 dimensional matrix and will be stored in the data base. Each value of matrix consists of intensity of light of that particular pixel present in the image.

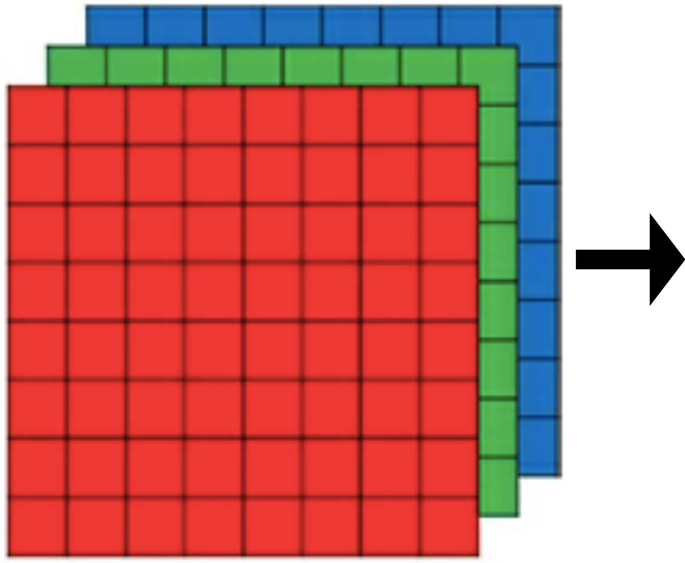
Layer 2: Anonymization Layer

Each image consists of 3 layers red , blue and green. Image can be convert into any other layer format. Standard represent of any image is done is RGB i.e red , green and blue.

In Image Anonymization. Every image layers is broken into their layer and 2 dimensional matrix is processed 3 times. After we processed the images. We can combine those layers to form a raw image. Suppose if the dimensions of the matrix is (100,100,3) then the image will be covered into the layers. The dimensions of that layers will be (100,100,0) , (100,100,1) , (100,100,2). The diagrammatic representation of the layers is as follows.



Visualization of Image Processing



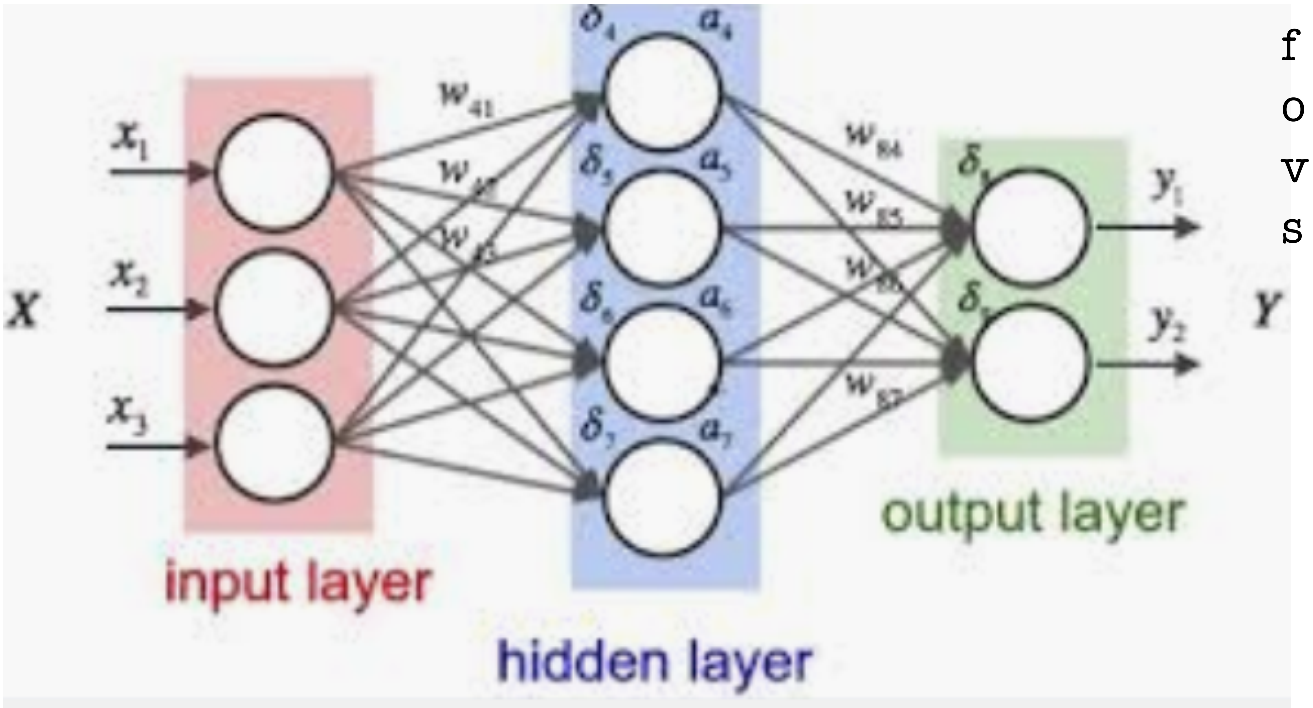
Layers of an Images

Raw images

If we process the layers of image individually. It is totally not understood by the humans. The advantage is that we can't even plot any layer of an image if we don't have at least one Layer of an image. If we try to encrypt the data of image then we to decrypt the images. The reason behind this will be get confused and once affect the accuracy. In layer system actual data is feed to the machine cause less confusion and better accuracy.

Layer 3 : Artificial Intelligence Layer

After machine accessible data is ready Data is feed to the machine. In Deep Learning The CNN algorithm is used in that because the layer is a type of two dimensional matrix we need to apply conv-1d algorithm. The basic diagram of neural network is

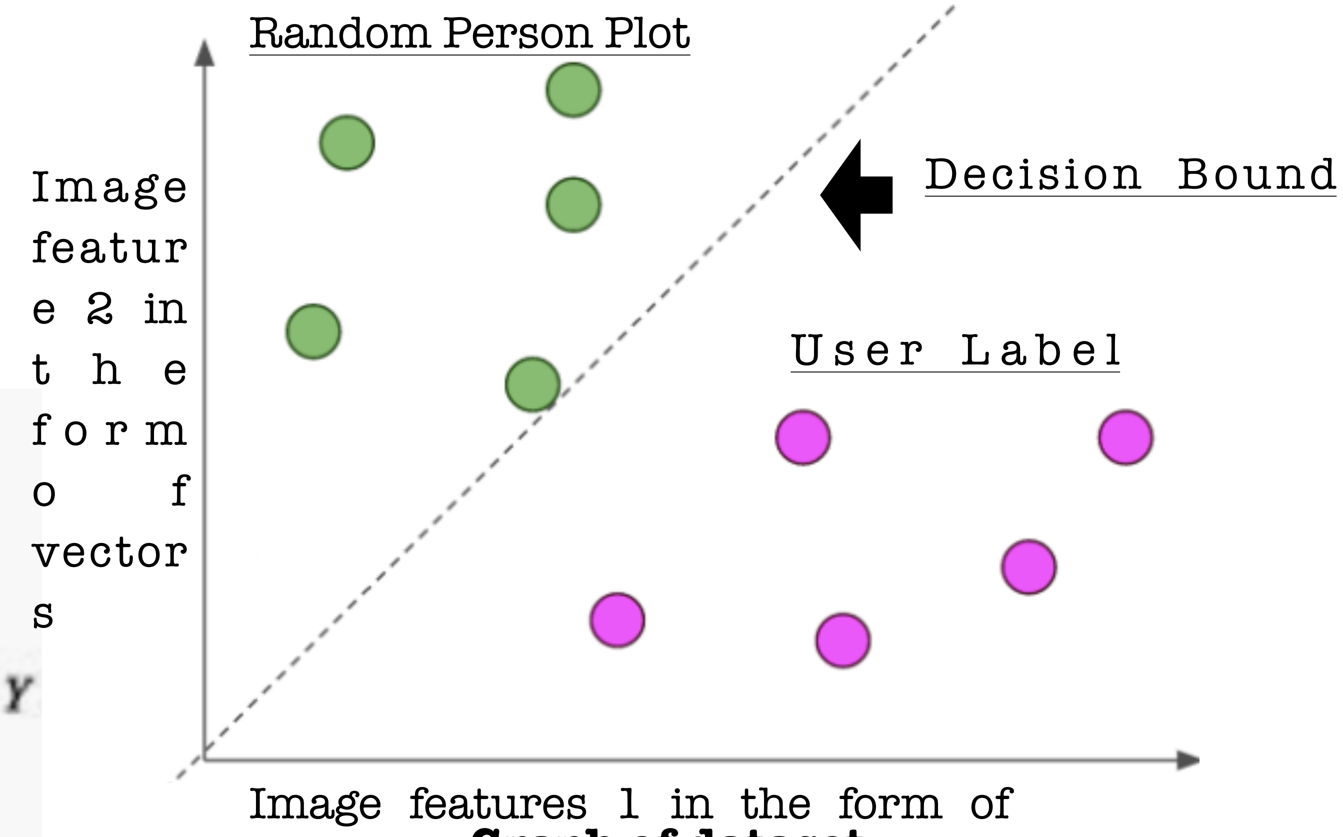


Basic representation of Neural Network

In this figure. The notations are as follows.

1. x = Input = Layer of an image
2. Y = Output = Label which machine will predict (user or random person)
3. Others are technical terms of Artificial intelligence I.e cost function , Decision Bound etc

Our machine will predict the output in this fashion.



Graph of dataset

In this figure. The notations are as follows

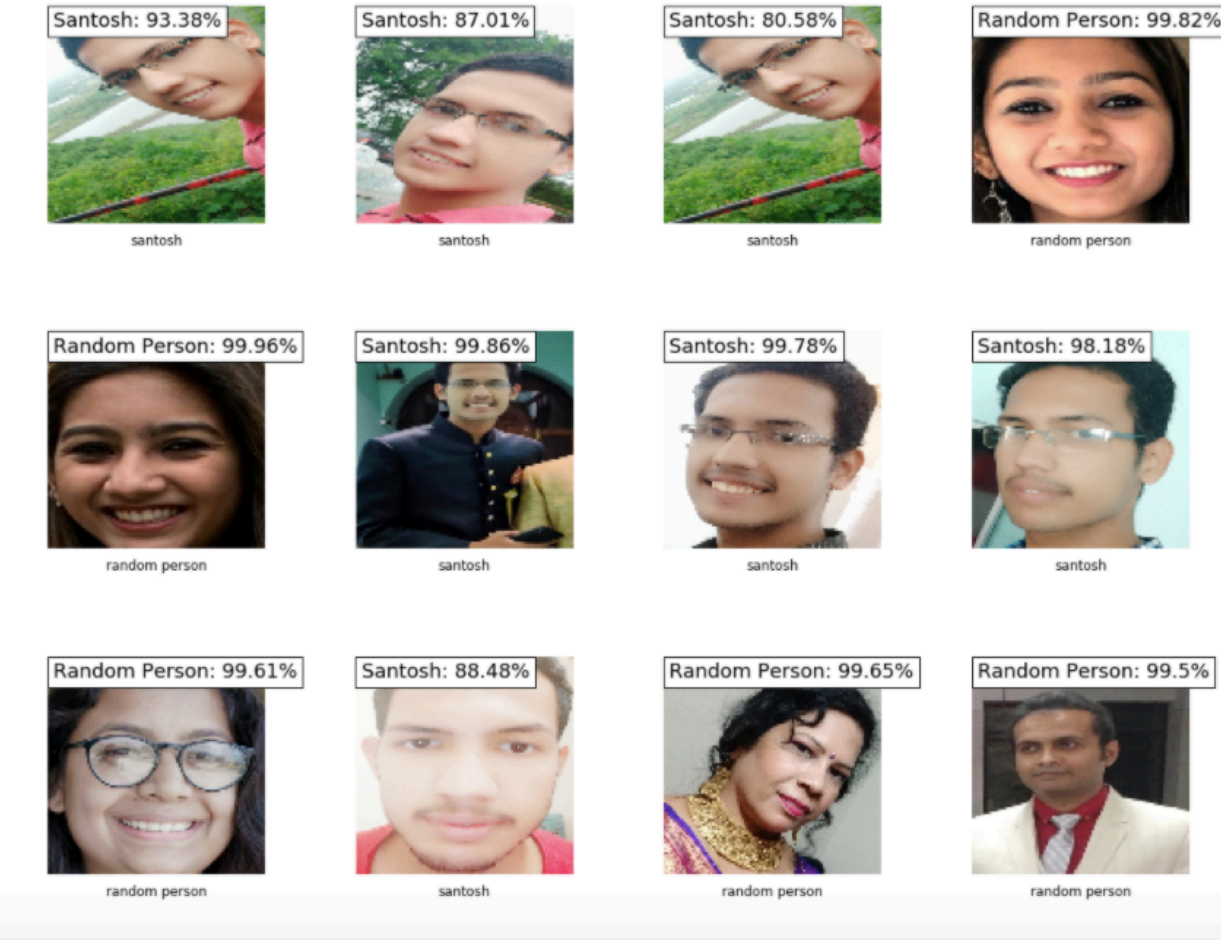
1. X- axis = Image layer vector 1
2. Y- axis = Image layer vector 2
3. Decision bound
4. Pink plot = That plots are marked as a user in output
5. Green plot = That plots are marked as a Random person plot

Decision Bound

This is the line which classify both the label. If the plot lies in left in this case is a random person and vice versa.

Layer 4: The Output Layer

After machine get ready to give output you can access the data with higher security and without any fear. The output of the code looks like this



Output of my code

You can refer the whole code in my GitHub account . The link is given at the end of the presentation.

ADVANTAGE

1. Much advancement in data privacy.
2. Data can be transferable through server hence hackers cannot stay in particular page at longer time .
3. The machine will learn with your previous input on continuous basis.
4. No need to remember Password.
5. Long thread of forgot password can be totally resolved.

Reference

1. Andrew Ng notes
2. Keras.io Website

you can find the whole code in this link

https://github.com/S-SANTOSH/Face-recognition-part-2/blob/master/Final%20DS%20Project.ipynb

Written by:

SANTOSH SAXENA.
18070122060 , C4 , CS,
Symbiosis institute of technology.