Activity Analysis and Enhancing Security Using Image Processing

ABSTRACT

The rise of technology bring into force loads of types of tools that aspire at more security. Using Face Recognition and Detection system demonstrates the way of unauthorized person movement in a place at that moment. A database of people's face is maintained by the system that handles face detection. When a face needs to be predictable a snap of the one`s look is taken and evaluated to the appearance present in the database to observe if a match is found. There are typically 3 parts related to a face recognition system like Face detector, Eye localize and Face recognizer. Although systems have been developed for face detection and tracking, reliable face recognition still offers a great challenge to computer vision. There are several reasons for recent increased interest in face recognition, including rising public concern for security, the need for identity verification in the digital world, face analysis and modelling techniques. Suppose in a data center there have five person works in different time slot in a specific day and all are authorized in that data center. Person's duty time is fixed and after passing his/her duty time this person will be unauthorized on that data center for security reason. This project aim is to identify the person who is he/she. Is he/she is unauthorized, authorized or unknown in a specific time. Using facial reorganizations system is classify that person and send the notification to the super admin of that data center via SMS and all recognized data will store in a server with persons photo and any time admin can get all records form a web portal.

CHAPTER 01

INTRODUCTION

The rise of technology bring into force loads of types of tools that aspire at more security. Using Face Recognition and detection system demonstrates the way of unauthorized person movement in a place at that moment. There are typically 3 parts related to a face recognition system like Face detector, Eye localize and Face recognizer. Systems have been developed for face detection and face recognition offers a great challenge to computer vision. Several reasons for interest in face recognition, including rising public security, the need for identity verification in the digital world, face analysis and modelling techniques.

1.1 Motivation

Facial recognition is no longer only an application for high-risk locations, such as data center, nuclear power plants and government buildings. A growing number of businesses realize that the ability to identify and recognize specific individuals can help to improve customer service and to serve as a proactive way of protecting their assets. Meanwhile, a broad range of high-resolution network and embedded cameras in combination with the development of commercial AI systems allows for a full replacement of traditional security measures, serving many use cases. The rise of technology bring into force loads of types of tools that aspire at more security.

1.2 Aims & Objective

Facial recognition algorithms can find on the internet and research papers suffer from photo strike. These methods work really well at detecting and recognizing faces on video streams from webcam. However they can’t difference between real-life faces and faces on a photo. This inability to recognize faces is due to the fact that these algorithms work on 2D frames. Aim is to implement an eye-blink detection-based face liveness detection algorithm to anti-

spoofing. The algorithm works in real time through a webcam and displays the person's name only if they blinked. In layman's terms, the program runs as follows:

i. Detect faces in each frame generated by the webcam.
ii. For each detected face, detect eyes.
iii. For each detected eyes, detect if eyes are open or closed.
iv. If at some point it was detected that the eyes were open then closed then open, we conclude the person has blinked and the program displays its name (in the case of a facial recognition door opener, we would authorize the person to enter).

1.3 The Basics of Deep Learning

Deep Learning is nothing but a standard paradigm of Machine learning, or more precisely — one of its algorithms. For the greatest extent, it is based on a concept of a human brain and the interaction of neurons. If start search in Google what Deep learning is, will notice this super-hot word today is far away from being new. Several types of applications and significant place among them is occupied by face recognition. First of all, deep learning gives the power to build recognition biometric software that is capable of uniquely identifying or verifying a person. All this because deep learning methods are able to leverage very large datasets of faces and learn rich and compact representations of faces, allowing modern models to first perform as-well and later to outperform the face recognition capabilities of humans.

1.4 How deep learning work

Deep learning systems are modeled after the neural networks in the neocortex of the human brain, where higher-level cognition occurs. In the brain, a neuron is a cell that transmits electrical or chemical information. When connected with other neurons, it forms a neural network. In machines, the neurons are virtual — basically bits of code running statistical regressions. String enough of these virtual neurons together and you get a virtual neural network. [9]

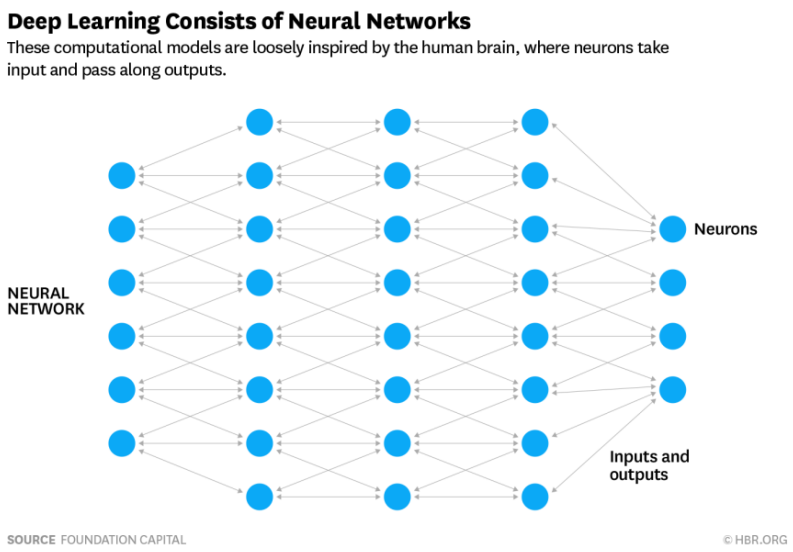

Fig. 1.1: Deep Learning of Neural Network [9]

Computer programs that use deep learning go through much the same process. Each algorithm in the hierarchy applies a nonlinear transformation on its input and uses what it learns to create a statistical model as output. Iterations continue until the output has reached an acceptable level of accuracy. The number of processing layers through which data must pass is what inspired the label deep.

1.5 Face Detection & Reorganization Methods

For the detection and recognition of faces need to install the face recognition library which provides very useful deep learning methods to find and identify faces in an image. Particularly the face locations, face encodings and compare faces functions are three most useful. The face locations method can detect faces using two methods: Histogram of oriented Gradients (HoG) and Convolutional Neural Network (CNN). Because of time constraints the HoG method was chosen. The face encodings function is a pre-trained Convolutional Neural Network able to encode an image into a vector of 128 features. This embedding vector should represent enough information to distinguish between two different persons. Finally, compare face computes the distance between two embedding vectors. The algorithm to recognize face extracted from a webcam frame and compare its embedding vector matrix with all encoded faces in dataset. The closest vectors should correspond to the same person.

1.6 Steps to Detect a Face

Face detection is usually the first step towards computer vision technologies, such as face recognition or identification.

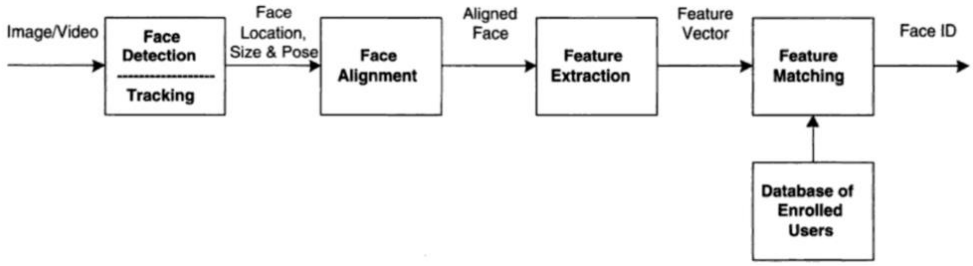

Fig.1.2: Face Reorganization process flow [2]

Face recognition is actually several related steps:

1. First, you need to look at the image and find all the faces on it.
2. Secondly, it is necessary to focus on each face and determine that, despite the unnatural turn of the face or poor lighting, it is the same person.
3. Thirdly, it is necessary to highlight the unique characteristics of the face, which can be used to distinguish it from other people — for example, the size of the eyes, the elongation of the face, etc.
4. In conclusion, it is necessary to compare these unique characteristics of the face with the characteristics of other people you know to determine the name of the person.

1.7 Deep Learning in Facial Recognition

It turns out that the characteristics that seem obvious to us humans (for example, eye color) do not make sense for a computer analyzing individual pixels in an image. The researchers found that the most appropriate approach is to enable the computer to determine the characteristics that need to be collected. Deep learning, in turn, allows much better and faster identification.

Face recognition is the field applying to bring an answer to the question: 'Whose face it is.' For this purpose, people have natural abilities through their human perceptive and cognitive systems, whereas machines need complex systems involving multiple, advanced algorithms and/or large, adequate face databases. Studying, designing and developing such methods and technologies are the domain of automated face recognition (AFR). [8]

AFR could be differentiated further into the computer automated face recognition and the computer automated face verification. Hence, on the one hand, automated face identification consists in a one-to-many search of a face image among a database containing many different face images in order to answer questions such as ‘Is it a known face? On the other hand, automated face verification is a one-to-one search to solve the matter of ‘Is it the face of…’

CHAPTER 02

LITERATURE REVIEW AND REQUIREMENTS

With an increase in the speed of displaying objects, an increase in the number of noises and objects in the image, the recognition rate and its quality of our brain and the brain of primates decrease dramatically. Even the simplest convolutional neural network recognizes objects better. *That is, officially neural networks work better than our brains.*

2.1 Face recognition & Deep Learning arose together

- **DeepFace** is a facial recognition system based on deep convolutional neural networks created by a research group at Facebook in 2014. It identifies human faces in digital images. With an accuracy of 97%, it was a major leap forward using deep learning for face recognition.[2]

- **The DeepID** or "Deep hidden Identity features," is a series of systems (e.g. DeepID, DeepID2, etc.), first described by Yi Sun, et al. in their 2014 paper titled "Deep Learning Face Representation from Predicting 10,000 Classes." Their system was first described much like DeepFace, although was expanded in subsequent publications to support both identification and verification tasks by training via contrastive loss.[2]

- **The VGGFace** (for lack of a better name) was developed by Omkar Parkhi, et al. from the Visual Geometry Group (VGG) at Oxford and was described in their 2015 paper titled "Deep Face Recognition." In addition to a better-tuned model, the focus of their work was on how to collect a very large training dataset and use this to train a very deep CNN model for face recognition that allowed them to achieve then state-of-the-art results on standard datasets.[2]

- **FaceNet** is a face recognition system developed in 2015 by researchers at Google that achieved then state-of-the-art results on a range of face recognition benchmark datasets.

The **FaceNet** system can be used broadly thanks to multiple third-party open source implementations of the model and the availability of pre-trained models.[2]

2.2 Frequency and Texture based analysis

The basic purpose is to differentiate between live face and fake face (2-D paper masks) in terms of shape and detailed ness. A single image-based fake face detection method based on frequency and texture analyses for distinguishing live faces from 2D paper masks. In addition, description method based on Local Binary Pattern (LBP) has been implemented for analyzing the textures on the given facial images. They tried to utilize frequency and texture information in distinguishing the live face image from 2D paper masks. First one is that difference in the existence of 3D shapes, which leads to the difference in the low frequency regions which is related to the illumination component generated by overall shape of a face. Then the variety in the detail information between the live faces and the masks triggers the discrepancy in the high frequency information. The texture information is taken as images taken from the 2D objects, tend to suffer from the loss of texture information compared to the images taken from the 3-D objects. For feature expulsion, frequency-based feature extraction, Texture-based feature expulsion and Fusion-based feature expulsion are being implemented. [7]

2.3 Movement of the eyes based analysis

Method for detecting eyes in sequential input images and variation of each eye region is calculated and whether the input face is real or not is ascertained. The basic assumption is that because of blinking and uncontrolled movements of the pupils in human eyes, there should be big shape variations. [7]

First center point of both eyes is detected in the input human face images. Using detected left eye and right eye, face region are normalized and eye regions are extracted. After that binarizing extracted eye regions in the face, each binarized eye regions are compared and variation is calculated. If the output is bigger than threshold, the input image is recognized as live face, if not, it is discriminated to the photograph. For detection of the eye regions, the fact

that the intensity of the eye region is lower than the rest of face region if the image is considered as a 3D curve. To search the eye region, first, Gaussian filtering to the face image is done, so that the smoothened 3D curve is obtained. In the curve, extract all the local minimums using the method of the gradient descent. To reduce the invalid eye candidates, the eye classifier, which is trained by Viloa's AdaBoost training methods, is applied. Then, face region is being normalized by about a size and rotation by using center point of eyes because the input face can vary in size and orientation. To decrease the effect of illumination, Self-Quotient Image (SQI) is applied. After Normalizing face region, eye regions are extracted based on the center of both left and right eye. Then eye regions are binarized in order to output have the pixel value of 0 and 1 by using a threshold. The threshold is acquired from the mean pixel value of each eye region. Eye regions from real faces have bigger alteration in shape than regions obtained from fake faces. Calculating liveness estimate of each eye region, Hamming distance method is used. If two ordered lists of pixels are compared, the Hamming distance is the number of pixels that do not have same value. If the average liveness score is bigger than threshold, the input image is recognized as live face and in the case of opposite it is discriminated as a photograph. [7]

2.4 Blinking based analysis

The blinking-based approach for liveness detection using Conditional Random Fields (CRFs) was introduced by Lin Sun et al. [3]. They have used CRFs to model blinking activities, for agreeable long-range dependencies on the observation sequence. Then compared CRF model with a discriminative model like AdaBoost and a generative model like HMM. Conditional random fields (CRFs) are probabilistic models for segmenting and labeling sequence data and mainly used in natural language processing for its accommodating long-range dependencies on the observation sequence. Blinking activity is an action represented by the image sequence which consists of images with close and non-close state. [7]

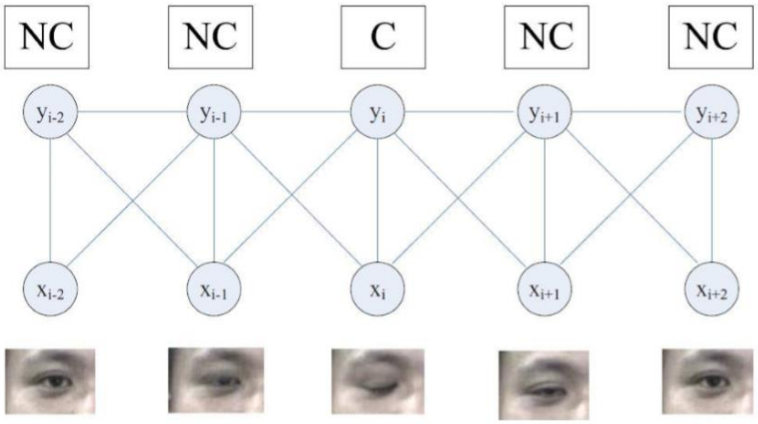

Fig 2.1 Graphic structure of CRF-based blinking model.

Here we show the model based on texts of observation of size 3. Labels C and NC are for close state and non-close state respectively Half-open state is difficult to define commonly over the different individuals, since the eye size of half-open eyes depends on the person eye appearance, like, the open state of a small eye might looks the half-open state of a big eye. As for the blinking model, two state labels, C for close state and NC for non-close (include half-open and open), to label eye states are being employed. [3]

Authors have used video database including blinking video clips and imposter video clips, Used a total of 80 clips which is in blinking video database for 20 individuals, 4 clips for each individual: the first clip includes video without glasses in frontal face view, the second clip is with thin rim glasses in frontal face view, the third clip contains video with black frame glasses in frontal view, and the last clip is having video without glasses in upward view. The blinking number in each clip varies from 1 to 6 times. To test the ability against photo imposters, the authors have used 180 photo imposter video clips of 20 persons with various motions of photo, including rotating, folding and moving. [7]

2.5 Project Requirements

There are many reasons for increased interest in face recognition, including rising public concern for security, the need for identity verification in the world, face analysis and modelling techniques. Project requirement is detect human face and then recognize that using live camera and identifying the person face ID from the data set and classifying the person who is authorize or unauthorized in a specific time. The major concern of this project is security and identify the live person or masking. Using facial reorganizations system is classify that person and send the notification to the super admin of that data center via SMS and all recognized data will store in a server with persons photo and any time admin can get all records form a web portal.

2.6 Tools & Technology Requirement

Programming Language	: Python, Nampy, php, HTML, CSS
Database	: mongoDB
Tools	: Tensorflow, openCV2, Kereas, Frontal face hercasecade face library
IDE use	: pycham, Jupter Note Book, Notepad++
Technology	: GPU devices

CHAPTER 03

ANALYSIS

3.1 Requirement Analysis

Requirement analysis is the third step of System Analysis Development Life Cycle (SDLC) and our project also. The stage is very much important and inseparable of a project. Requirements are a feature of a system or description of something that the system is capable of doing in order to fulfill the system's purpose. It provides the appropriate mechanism for understanding what the customer wants, analyzing the needs assessing feasibility, negotiating a reasonable solution, specifying the solution unambiguously, validating the specification and managing the requirements as they are converted into an operational.

The non-functional requirement describes a restriction on the system that limits our choice for developing a solution to problem. The non-functional requirements in our project are –

Time: Project should be completed within the stipulated time.

Cost: The cost involved in making the project should be feasible. The automated system ought to be less expensive than the manually handled system.

3.2 Feasibility Analysis

Feasibility study defines all the requirements to performance characteristics of software. The software to be feasible, the design needs to undertake various factors or performance requirements by which the software will be operated.

A feasibility analysis is short, focused study which aims at selecting the best system that meets performance requirements. Information is gathered regarding the general requirements of the proposed software.

Evaluating the technical feasibility is the canning part of a feasibility study. Because of this point in time, not too many detailed design of the system, making it difficult to access issues like performance, costs on etc. number of issues have to be deliberated while doing a technical analysis. The main consideration point is to be given to the study of available resources of the organization where the software is to be implemented. Here the system analyst evaluates the

technical advantages of the system giving emphasis on the performance, Reliability, maintainability and productivity.

3.3 Technical Feasibility

Technical feasibility takes of the all issues concerned with the design and development part of the project. It disquiet itself with the software, hardware and the platform related issues

The project would require a lot of space storage of static as well as high configuration computer. Which have GPU and CPU both. Though this project aim is to identify the real face in real time it's needed to powerful computational unit. Which is actuality provides by GPU. Another important thing is camera. Its need to high resolution camera. The numbers 720p HD and 1080p HD refer to the horizontal resolution. Therefore, 720p HD camera resolution provides images that are 1280 x 720 pixels (its adds up to 921,600 pixels, which means a 720p HD camera is not technically a megapixel camera resolutions), and 1080p HD cameras provide 1920 x 1080-pixel resolution, or 2.1 megapixels or more.

Working on face recognition, probably have a large dataset of face images and need to run experiments on multiple machines and GPUs. Setting up these machines, copying data and managing experiments on an ongoing basis will become a burden.

3.4 Process Model Use

All the resources needed for the development of the system as well as the maintenance of the same is available in the organization here we are utilizing the resources which are available already.

The factors for deciding the process model includes:

- Nature of software
- Application
- Tools and Methods used
- Deliverables

Our project follows the waterfall model/ Linear Sequential Model. The linear sequential model also called as classic life cycle or the waterfall model is a sequential software development model

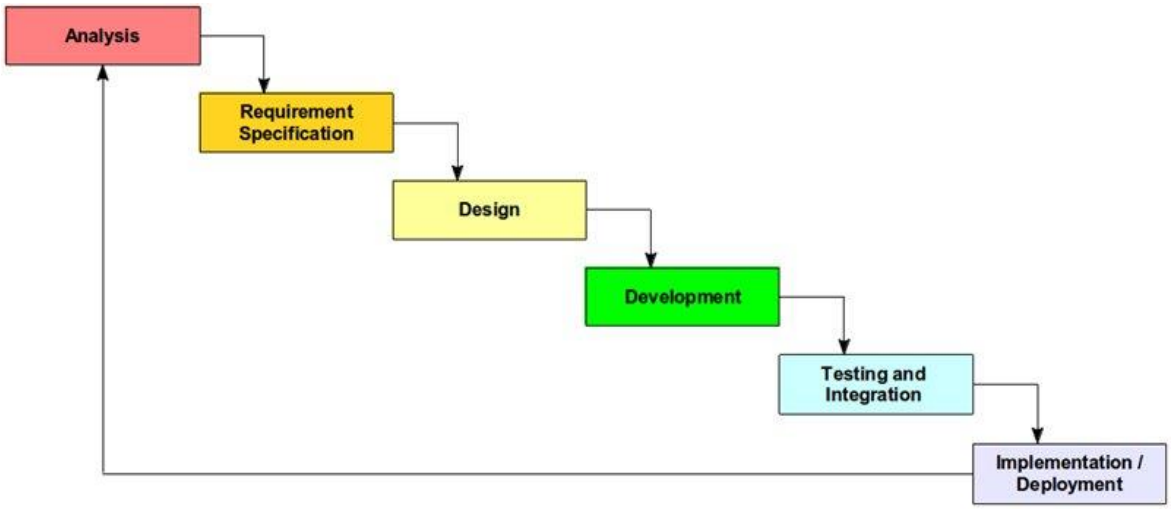

Fig. 2.2: Waterfall model.

(Process for the creation of software) in which development is seen as flowing steadily downwards (like a waterfall) through the phases of requirements analysis, design, implementation, testing, integration, and maintenance.

The steps of waterfall model are:

- Requirement Definition
- System and Software Design
- Implementation
- Integration and System Testing
- Operation and Maintenance.

Reasons for use

1. It is simple to implement and also the amount of resources required for it are minimal.
2. It is significantly better than the haphazard approach to develop software.
3. It provides a template into which methods of analysis, design, coding, testing and maintenance can be placed.
4. It is preferred in projects where quality is more important as compared to schedule or cost.
5. A small change in any previous stage can cause big problem for subsequent phases as all phases are dependent on each-other.

3.5 Proposed Methodology

There are several reasons for recent increased interest in face recognition, including rising security concerns, the need for identity verification in the digital eras, face analysis and modelling techniques. Suppose in a data center there have five person works in different time slot in a specific day and all are authorized in that data center. Person's duty time is fixed and after passing his/her duty time this person will be unauthorized on that data center for security reason. This project aim is to identify the person who is he/she. Is he/she is unauthorized, authorized or unknown in a specific time. Using facial reorganizations system is classify that person and send the notification to the super admin of that data center via SMS and all recognized data will store in a server with persons photo and any time admin can get all records form a web portal.

Application is filled with the following process:

- Detect person face.
- Recognize face and generate Face-ID
- Identify the person who are actually authorized or unauthorized.
- Send notification via SMS.
- Send data into server

Manage web admin:

- Set Employee Duty roster
- Add new Employee
- Get roster list.
- Get daily activity data list.
- Export data sheet.

CHAPTER 04

DESIGN

The design phase of software development deals with transforming requirements as described in the SRS documents into a form implementable using a programming language. Design is the specification of the interaction between a system and its environment. this phase proceeds at a high level of abstraction with respect to the inner workings of the system, during interface design, the internal of the systems are completely ignored and the system is treated as a black box.

4.1 Liveness Detection System Module

Flow chart shows the overall structure of the proposed liveness detection system. For live face detection we use five sequential face images.

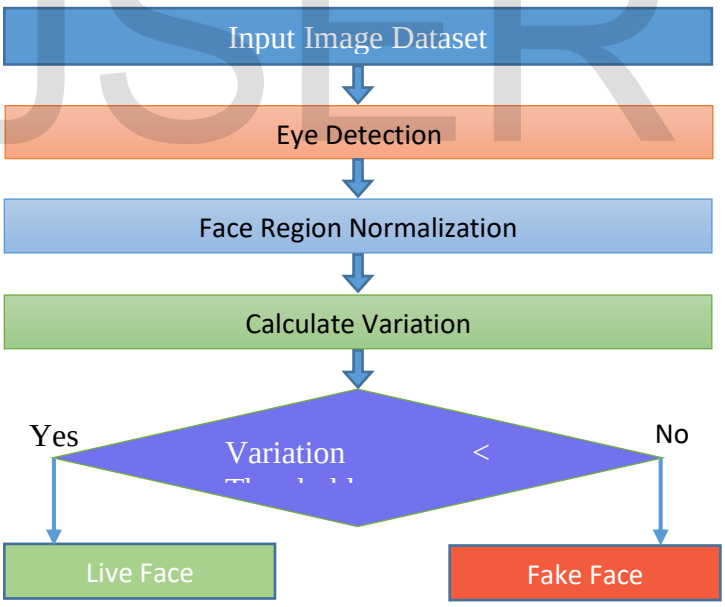

Fig. 4.1 The flowchart of live face detection

First detect center point of both eyes in the input face image. Using detected both eyes, normalize face region and extract eye regions. After binarizing extracted eye regions, compare

each binarized eye regions and calculate variation. If the result is bigger than threshold, the input image is recognized as live face, if not, it is discriminated to the photograph or video.

4.2 Prepare Dataset Module

This system a web admin portal by this admin panel admin add an employee with their respective information including photo. All information will store in database and photos are store in a different storage folder by naming person name. This is the overall dataset of face recognition. Using tensorFlow deep learning tool train the frontal face harcasecade model and recognizing the face of any person with identification.

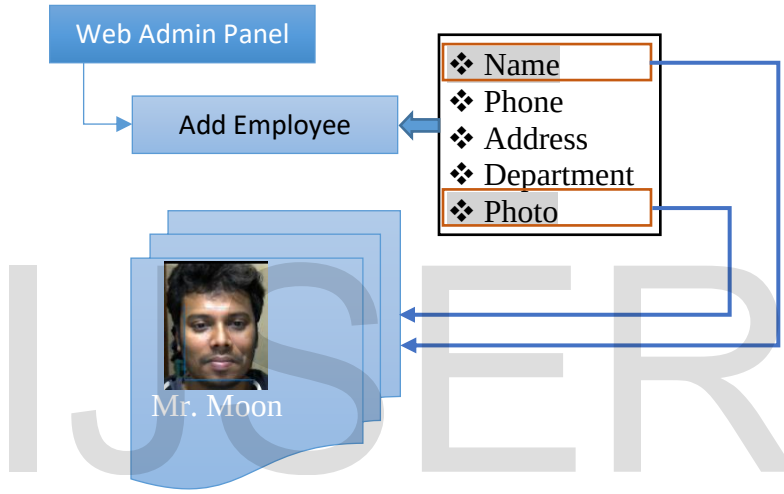

Fig. 4.2 Dataset preparing using photo with labeled name.

4.3 Overall Process Module

Process model shows that live camera capture the real time picture first detect eyes the face detection. After detecting the face then using deep learning tools tensorflow train the pre-train model from the dataset. After recognize the face system will check the face liveliness and classify known and unknown. The checking in known and unknown will classify the face authorize and unauthorized. If getting any unauthorized person then send notification via on SMS and data will send into a server.

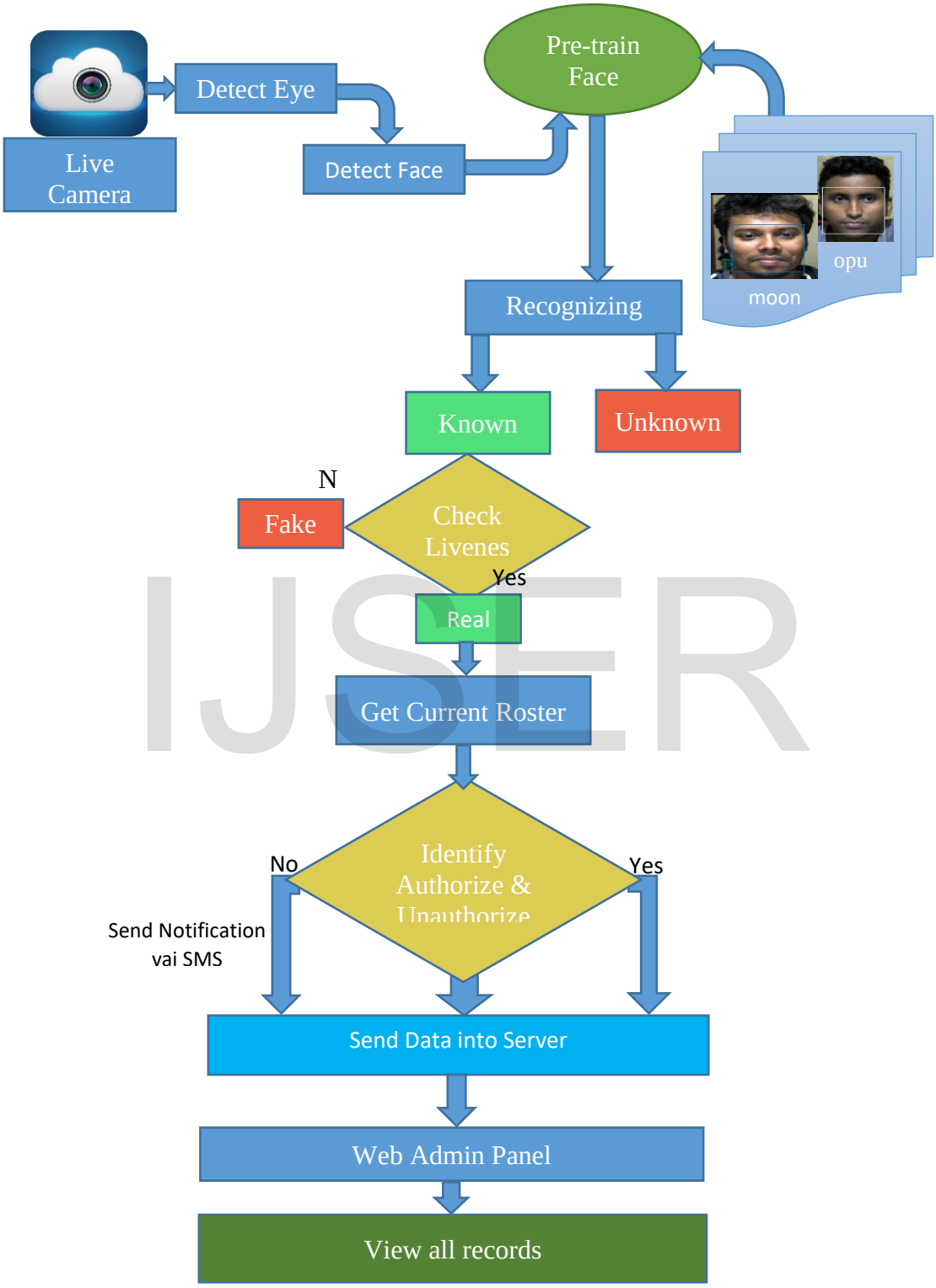

Fig. 4.3 The flowchart of live face detection

4.4 ER Diagram

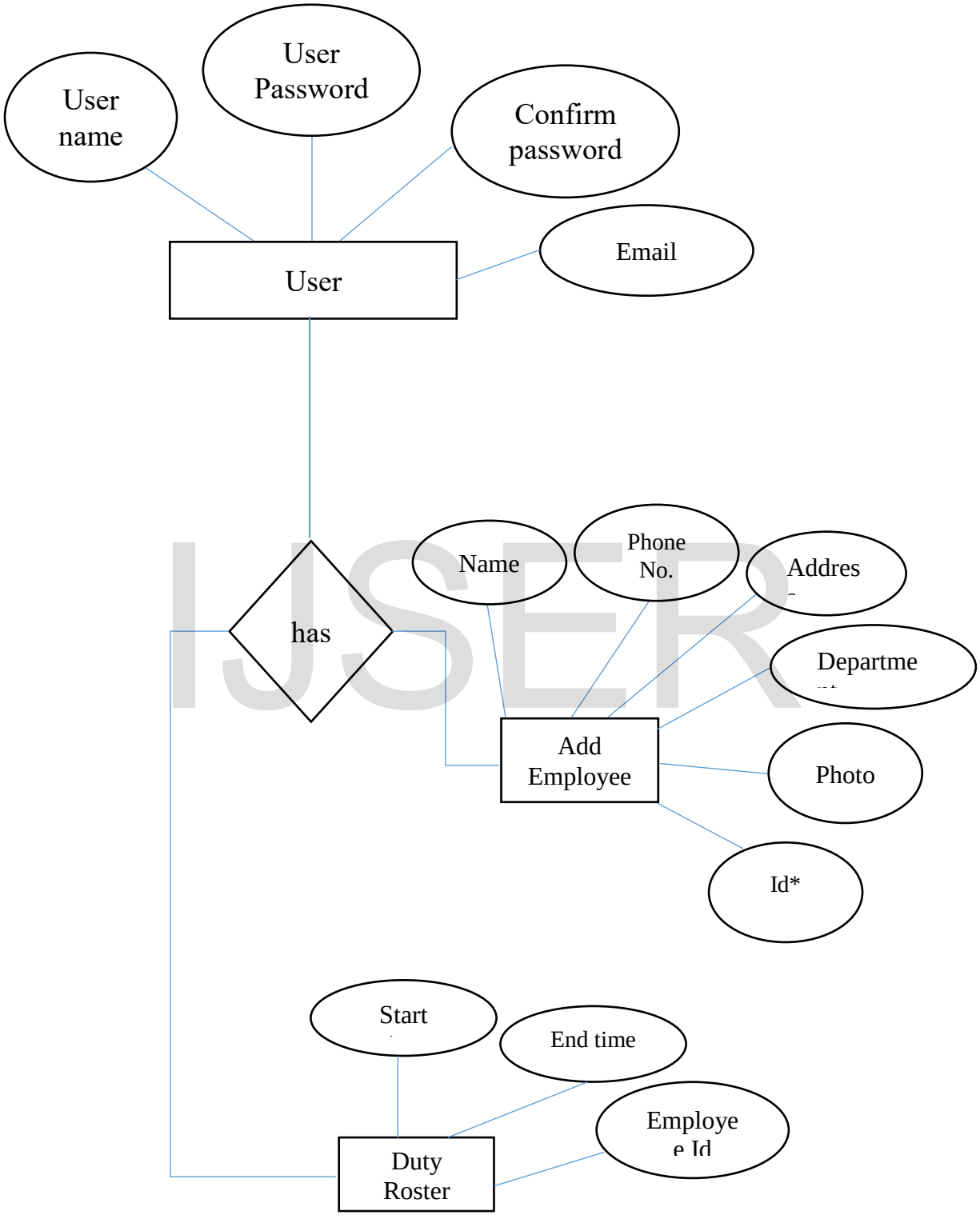

Fig-4.4: E-R diagram of Activity Analysis

CHAPTER 05

IMPLEMENTATION

This project has three implementing part one is face detection, recognition & classify the person with measuring high performance, second one is Send alert notification SMS and third one is recording daily activity data for security analysis.

5.1 Real time Face Detection & Recognition

At the beginning the system will detect face and recognize create a rectangle over the eye and face. If the person's face is not having in the data set it's treated as unknown. If use any fishy image like from mobile phone image in front of the camera then this system don't identify as a live person.

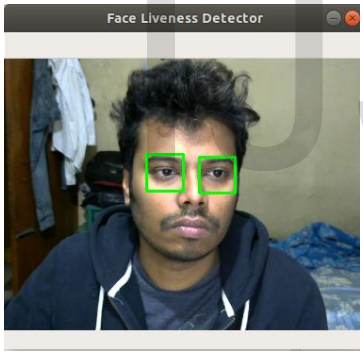

Fig-5.1: Detecting Eye and Face

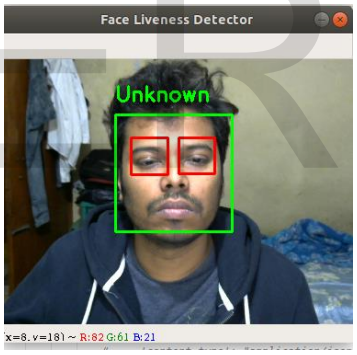

Fig-5.2: Recognition Face

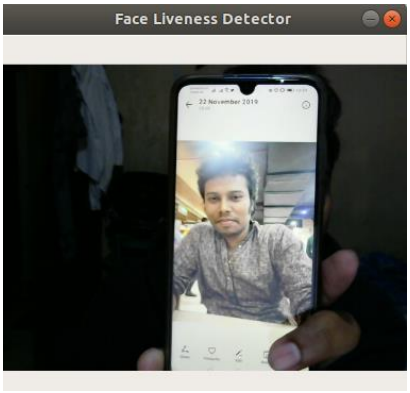

Fig-5.3: Fake image not identify

Fig-5.4: Fake image not identify

5.2 Face Image Identification and Classify

When in a specific time period a person who is unauthorized. Then the system recognize the face and identify as an unauthorized person.

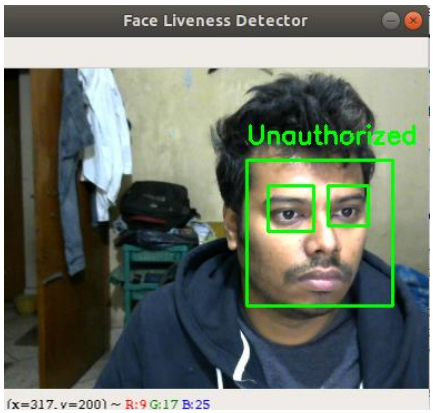

Fig-5.5: Identify and classify the person

5.3 Sending SMS for alert

After getting any unauthorized face then our system will send a notification SMS to the owner of that data center or admin's phone number.

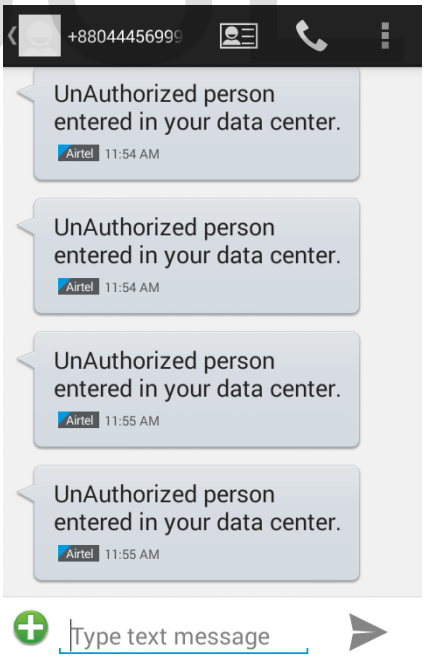

Fig-5.6: SMS notification

5.4 Daily Activity Data

In a specific day's data list shows in the table.

Serial ID	Identity	Person Name	Date & Time
1	Unauthorized	Moon	2019-11-25 23:42:55
2	Unauthorized	Moon	2019-11-25 23:42:58
3	Unauthorized	Moon	2019-11-25 23:42:59
4	Unauthorized	Moon	2019-11-25 23:43:00
5	Unauthorized	Moon	2019-11-25 23:43:01
6	Unauthorized	Moon	2019-11-25 23:45:29
7	Unauthorized	Moon	2019-11-25 23:46:05

Fig-5.7: Daily activity Data list.

CHAPTER 06

CONCLUSION AND FUTURE WORKS

An approach for the recognition of "**Activity analysis and enhancing security using image processing.**" presented in this paper. The objective of this project is to identify the person who is he/she. Is he/she is unauthorized, authorized or unknown in a specific time. Using facial reorganizations system is classify that person and send the notification to the super admin of that data center via SMS and all recognized data will store in a server with persons photo and any time admin can get all records form a web portal.

6.1 Conclusion

Some features of this project very helpful like owner can see live face detection, reorganization, classify authorize & unauthorized can take proper decision based on application.

The project program was a great opportunity for us to exercise the working in the relevant sectors and bring our academies to practice. This project was very much helpful in learning and working in a remarkable research area. The project was all about the Data center security and we are very much confident that this experience will be a great boost and help for our career ahead. The project period was an excellent experience of working under helpful project supervisor. Overall, it was a great exercise of learning brain and will greatly benefit us in our future.

6.2 Drawback Analysis

Every software has drawback and limitation. In this software also have some drawback which is much more negligible form the others software solutions. Face recognition is the most resource hungry solutions it need more RAM and processing capacity of a computer. Currently if any person wants to work extra hour in that place our solution does not identify as a valid person, after duty time over the person will be unauthorized person of that area.

6.2 Future Work

This project will helpful for our targeted user that they can benefited very much from this project. A number of inputs of this project is not satisfactory and more time need to analyze them to make them correct. Future works is:

- Face reorganization and liveliness performance make higher
- Security case increasing
- Employee roster update

APPENDIX

Web admin panel:

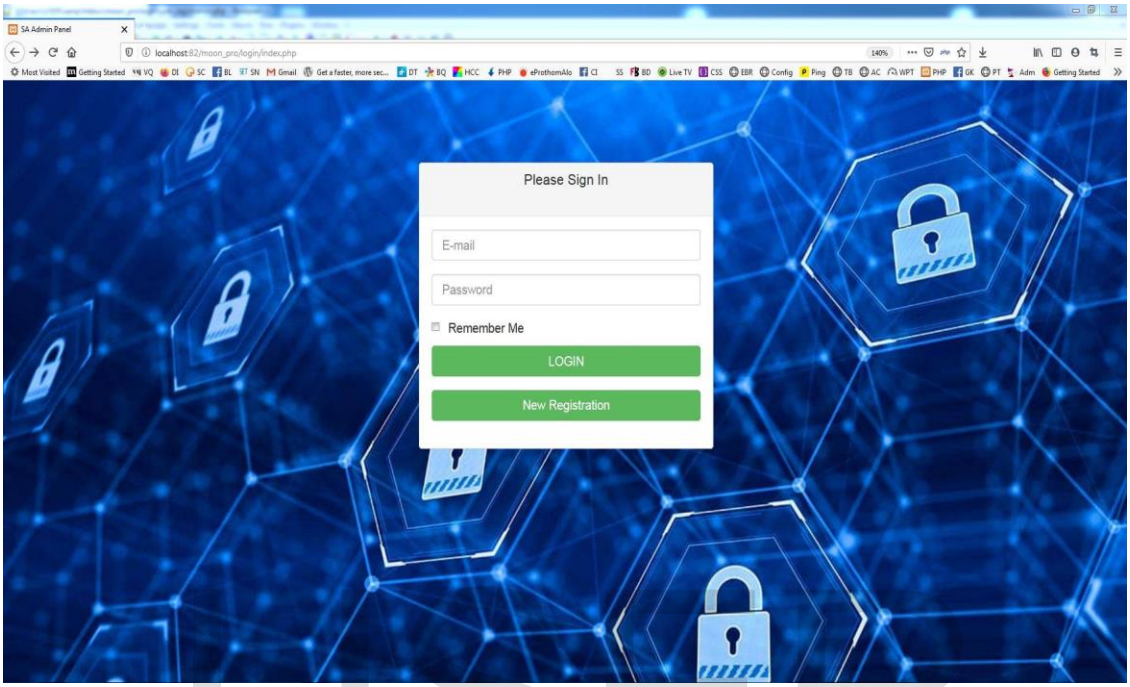

Fig.: Login interface

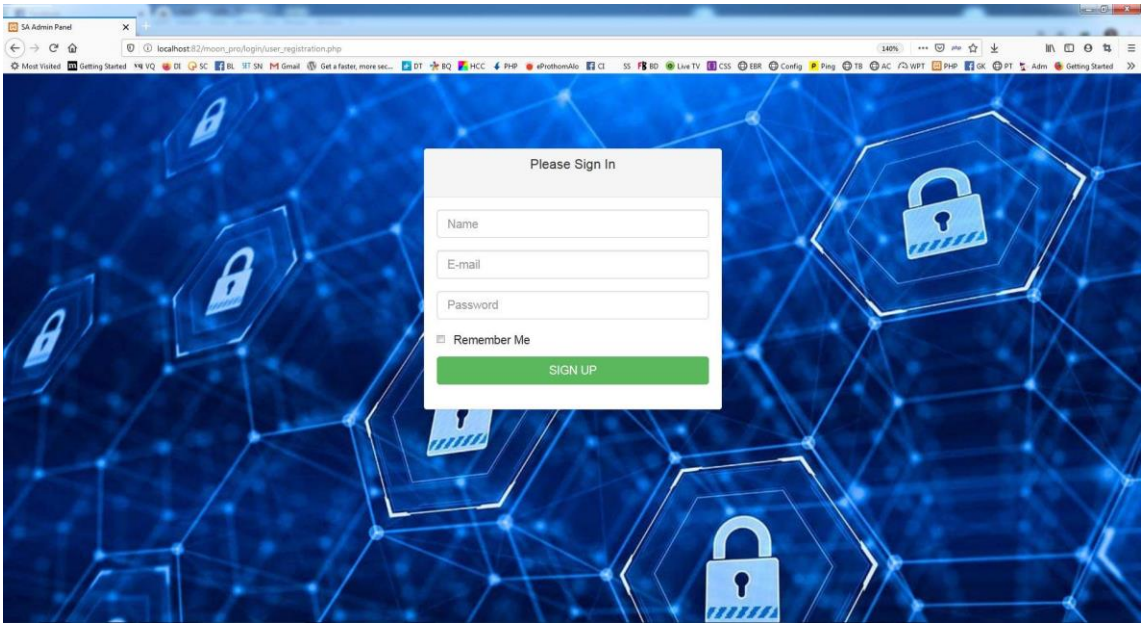

Fig.: Registration interface

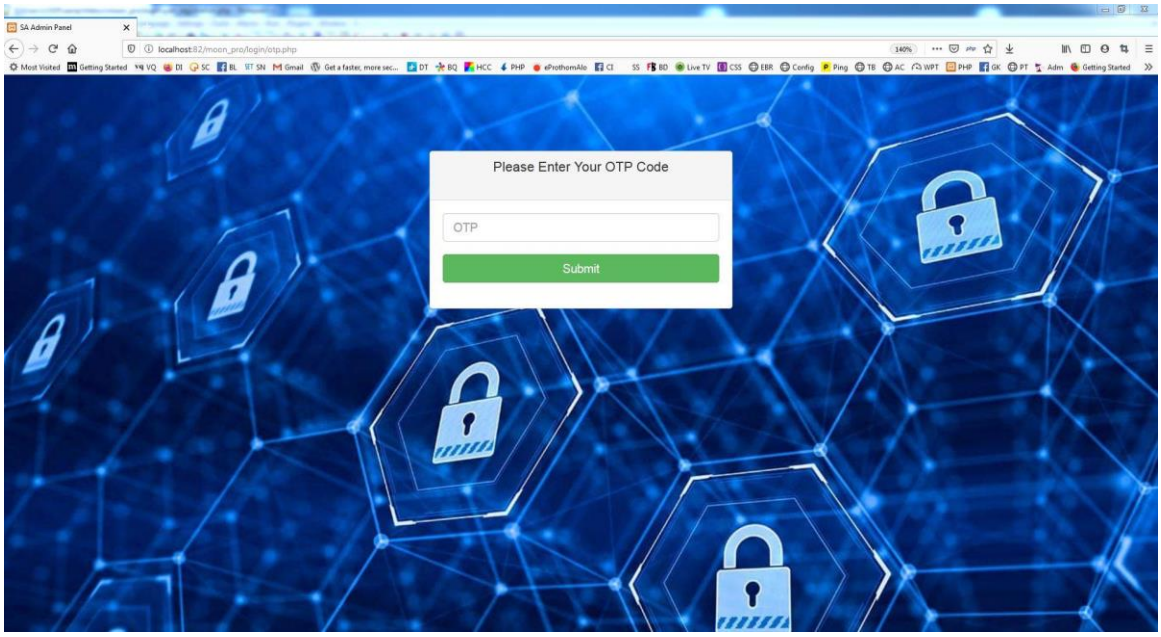

Fig.: OPT Authentication

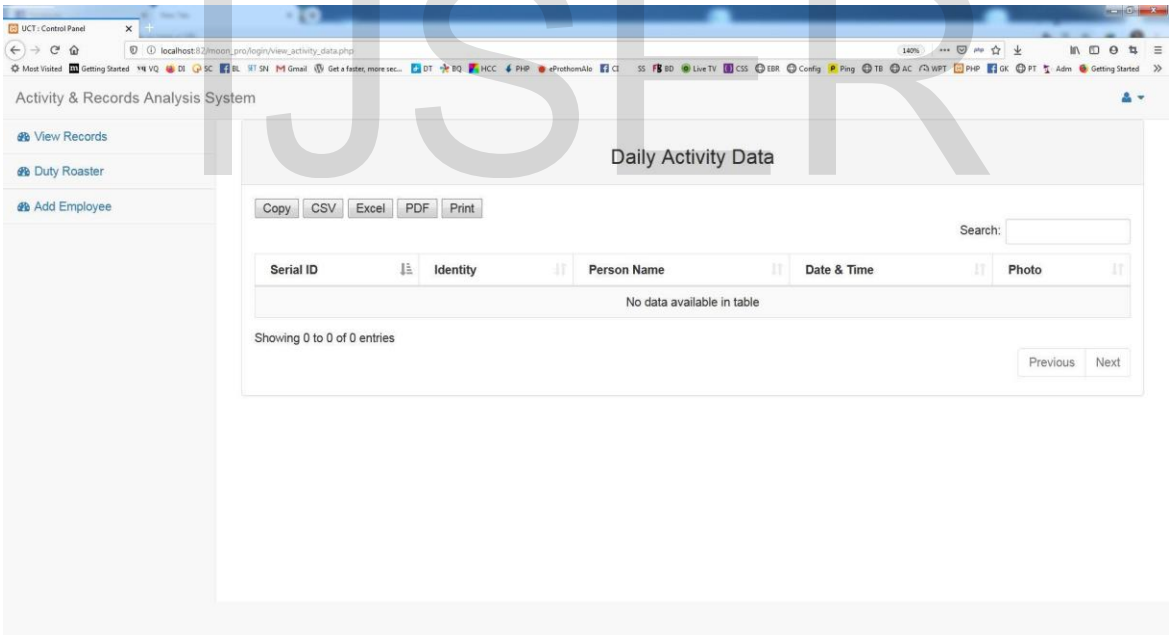

Fig.: Admin Panel Dashboard

REFERENCES

[1] Saptarshi Chakraborty1 and Dhrubajyoti Das2 “AN OVERVIEW OF FACE LIVENESS DETECTION”, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014, Page: 16-19

[2] Yi Xu, True Price, Jan-Michael Frahm, Fabian Monrose “Virtual: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos”, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014, Page: 6

[3] Jie Wang and Zihao Li “AN OVERVIEW OF FACE LIVENESS DETECTION”, IOP Conf. Series: Earth and Environmental Science 170 (2018) 032110 doi:10.1088/1755-1315/170/3/032110, Page: 10-19

[4] Shuhua Liu , Yu Song, Mengyu Zhang, Jianwei Zhao, Shihao Yang and Kun Hou “An Identity Authentication Method Combining Liveness Detection and Face Recognition”, *Sensors* (ISSN 1424-8220; CODEN: SENSC9) Page: 3-5

[5] Meenakshi Saini1, Dr. Chander Kant2 “Liveness Detection for Face Recognition in Biometrics: A Review”, IOSR Journal of Computer Engineering (IOSR-JCE), Vol.3, No.2, April 2014, Page: 32, 33, 34

[6] Meenakshi Saini1, Dr. Chander Kant2 “Face Recognition based Surveillance System Using FaceNet and MTCNN on Jetson TX2”, IOSR Journal of Computer Engineering (IOSR-JCE), Vol.3, No.2, April 2014, Page: 4

[7] Hyung-Keun Jee, Sung-Uk Jung, and Jang-Hee Yoo “Liveness Detection for Embedded Face Recognition System”, International Journal of Biological and Medical Sciences 1:4 2006, Page: 3-4

[8] Avinash Kumar Singh, Piyush Joshi, G.C. Nandi “Face liveness detection through face structure analysis”, Int. J. Applied Pattern Recognition, Vol. 1, No. 4, pp.338–360

[9] Missinglink.ai
Convolutional Neural Networks for Image Classification
Link:https://missinglink.ai/guides/convolutional-neural-networks/convolutional-neural-networks-image-classification/

[10] Towards data science
An Intro to Deep Learning for Face Recognition
link: https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb

[11] Towards data science
Face Recognition: Understanding LBPH Algorithm
Link: https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b

[12] Towards data science
How Do You Train a Face Detection Model?
Link: https://towardsdatascience.com/how-do-you-train-a-face-detection-model-a60330f15fd5