International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206383

Design of Intelligent Facial Recognition System using AI for Surveillance Application

Syed Ibrahim*[1], Syed Nahid Suleman[1], Manikanta Suthapalli[1], Abhishek Sharma[1], Shilpa K S[2]

[1]School of Computer Science & Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India

[2]Assistant Professor, School of Computer Science & Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India

ABSTRACT

Organizations presently continue to encounter significant security concerns; consequently, they require much particularly trained staff to achieve the coveted protection. This staff performs blunders that may affect the extent of security. A suggested solution to the matter mentioned above is a Face Recognition Security System, which can monitor and identify trespassers to blocked or high-security areas and assist in overcoming the margin of manual human oversight. This system is comprised of two halves: the hardware part and the software part. The hardware module incorporates a camera, while the software module includes software that uses face-detection and face-recognition algorithms. If a person infiltrates the confine in question, a set of snaps are captured by the camera and dispatched to the software to be examined/identified and equated with an existent database of trusted people. An alert is conveyed to the user if the infiltrator is not recognized.

Keywords : Face Recognition, Surveillance, Haar Cascades

I. INTRODUCTION

Face recognition as a primary modality for biometric authentication, which has received increasing interest in recent years. Personal identification is used to recognize the identity of a person. For this purpose, the Face of a person is used and is stored in a computer database for comparison and identification. The face detection process is an inseparable part of the face recognition process.

An active NIR imaging hardware, algorithms, and system design, to overcome the problem of illumination variation that every face recognition system has to deal with. An illumination invariant face representation is obtained by extracting LBP features NIR images [1]. During the time of capturing the image of the Face, there exist different kinds of variations in face images taken under uncontrolled conditions, such as changes in pose, light, expression, etc. So, instead of going through the "divide and conquer" method, they aimed to directly address face recognition under uncontrolled conditions [2].

A way of differentiating between fake and real face detection to avoid fraudulent access attempts was determined [3]. A novel approach proposed for real-world face recognition under pose and expression variations from only a single frontal image in the gallery, which was very rapid and real-time [4]. To check that if the existing face recognition algorithms work for low- quality CCTV images as well [5].

The application of face recognition technology can be categorized into two main parts: Law Enforcement application and Commercial application.

Face detection using the Viola-Jones method or Haar Cascade is widely used because it produces high accuracy on face detection. The aim of this paper is to create capable software for a hardware model to help the owner/admin of the house/establishment to enhance their security. The intrusion detection model helps in identifying intruders and alerting the admin/owner. This aims to help boost the confidence of the owners and reduce the search time in case of searching for evidence.

II. LITERATURE SURVEY

This segment gives an overview of the human face recognition techniques, advantages and disadvantages of each method are also provided. The methods considered are the NIR-based face recognition system, neutral network, Software-based face recognition system, feature library matrix, face recognition using closed-circuit television images. The aforementioned approaches are analyzed in terms of the facial features they used.

NIR based face recognition system [1]:

In this paper, the proposal for accomplishing illumination invariant face recognition for indoor, cooperative-user applications is using active near-infrared (active NIR) imaging techniques, and for building accurate and fast face recognition systems. The proposed solution consists of the NIR imaging hardware module and the NIR-based face recognition algorithms. Some of the major additions are outlined in the following.

The first addition is the method of an imaging hardware system for yielding face images of a good illumination condition. Active NIR light is used to illuminate the Face from the frontal direction during the image acquisition process. There could be two approaches to illumination invariant face recognition: by a highly nonlinear face matching engine with an illumination variant representation or by an illumination invariant face representation with a less complicated face matching engine. We adopt the latter proposition by taking advantage of active NIR imaging.

The second addition is the method of illumination of an invariant face representation based on active NIR images. It's revealed that the active NIR imaging is mainly subjected to a roughly monotonic transform in the gray tone due to the variation in the distance amid the given Face and the NIR lights and camera lens. Noting that the ordering relationship between pixels is not changed by any monotonic transform, local binary pattern (LBP) features had been used to compensate for the monotonic transform in the NIR images.

The third additions are the method for formulating a highly accurate face recognition engine using the LBP features from NIR images. While there are a large number of LBP features, not all are useful or equally useful for face recognition. By using the AdaBoost learning algorithm to learn from acquired training examples to select a small subset of the most discriminative LBP features and thereby constructing a robust classifier.

The fourth additions are a proposed method for reliable eye detection in active NIR images. The frontal active NIR lighting can result in undesired specular reflections on eyeglasses. This makes accurate eye localization very complicated in the active NIR than the typical VL images, which cannot be simply stopped by a simple eye detector. Therefore, the simple-to-complex architecture is used to provide an adequate solution to subdue this critical issue of face recognition using the active NIR images.

This solution is developed for indoor cooperative user applications. It is not yet preferred applications such as face recognition in video surveillance. Nor is it preferable for outdoor use due to the strong NIR component in the sunlight. Later operations can be an enhancement of the solution to overcome such limitations.

Face recognition under uncontrolled conditions [2]:

In this paper, it attempts to directly address face recognition under uncontrolled conditions. The core is the individual stable space (ISS), which exclusively expresses personal characteristics. A neural network named ISNN is proposed to outline a fresh face image into the ISS. After that, three ISS-based algorithms are designed for FR under uncontrolled conditions. There are no restrictions for the images fed into these algorithms. The proposed algorithms are tested on three large face databases with vast variations and achieve superior performance compared with other 12 existing FR techniques.

The development of FR techniques communicates to a journey from strictly controlled conditions to more and more uncontrolled conditions. The methodology utilized by the current work appears to be "divide and conquer," i.e., gradually reduce the restrictions by tackling possible variations one by one. Instead of "divide and conquer," this paper exhibits one of the first attempts directly targeting to FRU.

Since the variations under uncontrolled conditions might be too complex to be well handled, we avoid explicitly modeling them. Instead, we focus on the information useful for recognition and try to filter out all other information. This is achieved by projecting the face images into a subspace called individual stable space (ISS).

Secondly, the four different kinds of information in the face images are analyzed, and the concept of ISS is introduced. To find a solution for FRU, we start by analyzing the components of the face images obtained under uncontrolled conditions.

Third, a neural network named individual stable neural network (ISNN) is proposed to map a face image into the ISS. Here, a technique is intended to outline face images into the ISS based on a pair of neural networks with reverse learning rules, namely, the stochastic gradient ascent (SGA) and the anti-Hebbian version of SGA (ASGA).

Fourth, three ISS-based algorithms for FRU are proposed. Then after the results of the experiment are reported. Finally, conclusions are drawn, and several issues for future work are indicated.

Software-based Face Recognition [3]:

In this paper, the goal of the proposed system is to improve the security of biometric recognition structures, by attaching liveness assessment in a fast, user-friendly, and non-intrusive style, by the use of image quality assessment. The suggested approach exhibits a meagre degree of complexity, which makes it fitting for real-time applications, using 25 general image quality features extracted from one image to discriminate between genuine and phony samples.

Amongst the different threats examined, the direct, or spoofing attacks have triggered the biometric community to study the vulnerabilities against this type of deceitful actions in modalities such as the iris, the fingerprint, the Face, the sign, and multimodal approaches. In these attacks, the invader uses some type of synthetically produced artifact or tries to mimic the behaviour of the genuine user, to fraudulently access the biometric system.

As this type of attack is achieved in the analog domain, and the interaction with the device is done following the regular protocol, the conventional digital protection tools are not practical. So, researchers have concentrated on the design of specific countermeasures that facilitate biometric systems to distinguish bogus samples and discard them, advancing this way the robustness and security level of the arrangements.

Liveness detection techniques are normally classified into two groups:

- Hardware-based techniques.
- Software-based techniques.

These types of methods confer certain benefits and detriments over the other and, overall, a blend of both would be the most sought-after safeguard approach to enhance the security of biometric systems. Hardware-based systems usually present a more crucial counterfeit detection rate, while software-based techniques are in generic cheaper, and less meddlesome since their implementation is transparent to the user.

Being software-based, this confers the typical benefits of this type of approach: fast, as it only necessitates one image to identify whether it is genuine or bogus, non-intrusive, user-friendly, inexpensive, and effortless to install in previously working systems.

The failure valuations obtained by this suggested protection scheme were, in many instances, less than those proclaimed by different trait-specific high-end anti-hackable systems at that time. This proposed technique was able to hypothesize well to diverse databases, retrieval conditions, and offensive situations.

Face Recognition via Feature Library Matrix [4]:

In this paper, the focus was to obtain an innovative approach for face recognition under the act, and appearance changes are intended to just a unique picture in the exhibit. A Feature Library Matrix (FLM) is created for every subject in the album from complete Face poses by pivoting the 3D reconstructed figures, including deriving features in the pivoted face pose. Hence, every feature library matrix is consequently executed for each subject in the album based on triplet ends of face poses. Accordingly, a 3D figure is initially reconstructed from frontal face pictures in actual situations. To restore a 3D model from each human frontal Face in real-world circumstances, the PFER-GEM was proposed. Then, the feature library matrices were formed based on the suggested method, and finally, face recognition is implemented by iterative scoring classification.

This suggested method was experimented on various databases to perform pose-invariant face recognition. It was exhibited that the performance of the recommended method for pose-invariant face recognition was enhanced in judgment to high-end techniques. Further, the suggested face recognition system would be extended to unconstrained face recognition that will be robust to a broad spectrum of face variations, including makeup, cosmetic surgery, facial appearance, face occlusion, and many other characteristics.

Different Face Recognition Algorithms Using Closed Circuit Television Images [5]:

In this paper, the focus was to determine the performance of various face recognition algorithms on the Closed-Circuit Television Images of low quality. The different algorithms of face recognition work well on high-definition digital pictures. To fulfill the purpose of the paper, three algorithms were selected. These algorithms are Principal Component Analysis, Artificial Neural Network, and Single Value Decomposition and phrased as algorithm A, algorithm B, and algorithm C, respectively.

For the verification of the identity of a person, their identification is required. The Face of a person is used and is collected in a computer database for matching and identification. The different types of methods are the ones named in the above paragraph.

These three algorithms were evaluated with an observation that the algorithm B's performance is better than algorithm A and algorithm C. And it was also noted that the computing time of algorithm B was more than the other two algorithms evaluated. The hurdles in this study were posing and the low-quality images of CCTV cameras. To overcome these hurdles, the quality of the CCTV images was enhanced before the preparation for face recognition.

The result of this study was that of the CCTV pictures, the precision rate of algorithm A, algorithm B, and algorithm Care 75%, 85%, and 65%, respectively. It was also found that the efficiency of all three algorithms diminished when the number of faces inputted rises.

S. No	**Paper name/year**	**Methodology used**	**Result**	**Advantages**	**Disadvantages**
[1]	"Illumination Invariant Face Recognition Using Near-Infrared Images/ 2007	Near-Infrared (NIR) imaging hardware. NIR based face recognition algorithms.	The solution is only developed for cooperative user applications indoor.	Fast face recognition and high accurate systems are built.	The result obtained here can only be used for an indoor purpose, and due to the strong NIR component in the sunlight , this system cannot be used outdoors.
[2]	Individual Stable Space: An Approach to Face Recognition Under Uncontrolled Conditions/2008	A neural network named ISNN algorithms.	The three large face databases which have a lot of variations among them are taken into consideration and tested with the algorithms to achieve a better performance of the system under uncontrolled conditions	View angle is not required for achieving excellent performance for face recognition.	ISS is used for recognizing the intricate patterns in the Database, and those patterns that are identified are used in the future for pattern recognition.
[3]	Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face	Novel software-based fake detection method.	The proposed technique was able to hypothesize well to diverse databases, retrieval conditions,	The first approach to increase security in biometric systems is the combination of both hardware and softwar	Lacks Generality.

	Recognition/2014		and offensive situations.	e-based techniques. This combination leads to detect whether the Face is real or fake.	
[4]	Real-World and Rapid Face Recognition Toward Pose and Expression Variations via Feature Library Matrix/ 2015	3D facial expression recognition model. Constrained Local Model (CLM) method. FLM+PFER-GEM method.	The solution is developed for obtaining the actual facial recognition by capturing the pose and expressions with different variations from a single frontal image through a gallery within a short time rapidly.	The constrained local model is used for automatically detecting the landmarks on the images captured through the surveillance system.	The result obtained is not suitable for face recognition under different face variations like a face with makeup, different facial expressions, and also if the Face is blocked while a person is passing through the surveillance system.
[5]	An Experimental Evaluation of Different Face Recognition Algorithms Using Closed Circuit Television Images /2017	Algorithms used are: - • ANN. • PCA. • SVD.	The proposed method shows that the efficiency of all three algorithms diminished when the number of faces inputted rises.	While comparing which algorithm performs well, with the accuracy obtained, it is clear that the ANN algorithm performs better than the SVD and PCA algorithm.	The quality of the closed-circuit camera has to be checked before assigning it for face recognition. If the CC camera quality is not right, then the results obtained may vary while calculating.

III.IMPLEMENTATION

Implementation is a combination of methods that facilitate the conception, development, implementation, and maintenance of the real-world application. To achieve the purpose or our paper, we implemented the various technologies with the required hardware to create a Face Recognition System, which would be able to detect and recognize the face and issue alert for the unknown Face. For the purpose of doing these various hardware and software technologies are used.

Technologies Used

a. Haar Cascade Algorithm:

The classifier is trained on a dataset that consists of positive and negative images. Positive images are those class of images which have Face or object in them. Negative images do not have an object in them. The cascades algorithm needs to be trained on a massive dataset of these images. This algorithm extracts necessary features from the training images using Haar features. The sum of pixels under the white rectangle region of the Haar feature is subtracted from the amount of pixels under the black rectangle region of the Haar feature to obtain the feature, which is a single value. This is similar to convolution kernels used in CNN.

Different types of Haar features or kernels of varying sizes and positions are implemented to extract features in an image. The same calculation, as mention above, is followed for every kernel. The algorithm applies every feature to the training dataset images and classifies based on a certain threshold and the features which produce the smallest error.

Applying all the Haar features produces a large number of features, almost 160000 plus features for a 24*24 image. Most of the features are irrelevant, and we need to choose the best ones. This is accomplished by used Adaboost, which trains weak classifiers, and their combination results are a robust classifier. The developer can train the custom Haar classifier. OpenCV provides a pre-trained cascades classifier, which is an XML file.

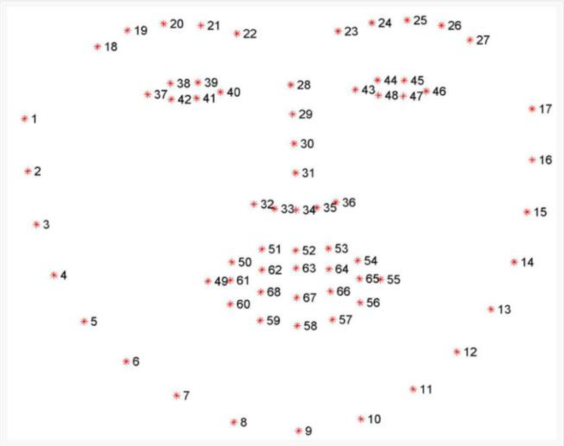
b. dlib's "68 point face landmark detection."

The dlib library in Python provides pre-trained facial landmark detector which is used to estimate the location of 68 (x, y)-coordinates (landmarks) that map to facial structures on the Face.

These annotations are part of the 68 points recognized features from the training dataset (iBUG 300-W). Their other face landmark detectors as well, such as the 194-point model, which is trained on a different dataset (HELEN dataset). Irrespective of the dataset used, the dlib the framework can be advantageous to train a face keypoint detector.

The stream from WebCam is used to capture a frame using OpenCV and convert each frame into a NumPy array. Frames at the rate of 320x240 are recorded. We can also record full HD frames, but performing face detection will take a lot of time on Raspberry Pi. Then after using the "haarcascade_frontalface_alt2.xml" model, we detect faces in the given frame. Once all the Face in a frame is identified, the result has stored a list, so that each Face can be compared with saved faces.

An example image of 68 coordinates on the Face can be visualized on the image below:



As shown in the above fig, 68 points are recognized as landmarks on the Face that we want to recognize. We will load the annotation of known Face that is stored in NumPy array to compare with the newly recognized landmarks. The distance between these landmarks of the known/saved Face and recently detected Face is calculated. We are using 0.6 as the threshold. If the distance value of landmark is below the threshold, then it is the known person entering into the room, else it is an unknown person (intruder).

IV. Methodology

PIR sensor is applied to find out when to start the inference engine and perform face recognition. The moment the PIR sensor identifies any kind of movement, the camera will start capturing frames for 10 seconds. At the same time, OpenCV's "Haar Cascades" will start recognizing faces, and dlib's "68-point face landmark detection" will match identified Face's landmarks with saved ones to check whether it's an intruder or not.

Using OpenCV, we can take frames from the Webcam and convert each frame into a NumPy array. Here, we are recording frames at the pace of 320x240. Then later, using the "haarcascade_frontalface_alt2.xml" model, we identify faces in the given frame. Once we recognize all the faces, we will collect them in one list to compare each of them with saved faces.

We will use dlib for face comparison. dlib 68-point face landmark detection will give you landmarks for a given face. We do have some known face landmarks stored in NumPy data, which we will load before comparison.

Once we have all the landmarks, we will find a distance between those landmarks. We are managing 0.6 as the threshold. The face landmark, which gives you the meagerest distance below the threshold, is the known person. If the value is not lesser, the threshold then, it's an intruder!!

Flowchart

In figure 1, the flowchart of the proposed system and its working is shown. Here the process begins with image acquisition after motion detected is more significant than predefined threshold motion.

Face Detection is done to verify if a face image is present in the acquired image. If the Face detected, it is further processed to identify Face using ML algorithm from the pre-trained DatabaseDatabase. If the Face is not matched with pre-trained data in the DatabaseDatabase, then it will send an alert notification to the admin.

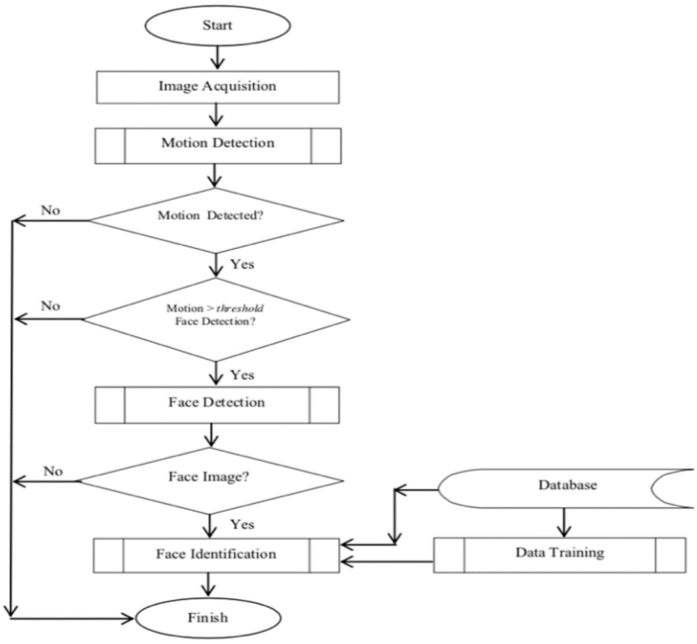


Figure 1 The Design of Motion Detection and Face Identification

System Architecture

The External System of the Architecture consists of the hardware module. It consists of a Raspberry Pi microprocessor which contains a 4gb RAM and a Wi-Fi module in-built. For motion detection, a PIR Sensor is used. Raspberry Pi Camera is used for image acquisition. These are the major components used in the External system of the System Architecture proposed for this project.

The Internal System of the Architecture consists of the software module. First, the training dataset, which contains the input images of authorized users, is trained, so that features from different angles of the Face are trained, and encodings are stored. The steps involved in the live testing process (as shown in fig 2) is to firstly detect motion to trigger the camera to capture the image from the live CCTV feed. The image acquired is then processed for Face detection using

Haar Cascades ML algorithm. If the Face is detected then it is sent for face recognition which uses a 68-point feature recognition. The Face is compared and used to send alert notification to the admin if an unknown face is recognized. This is the working of the Internal System of the Architecture.

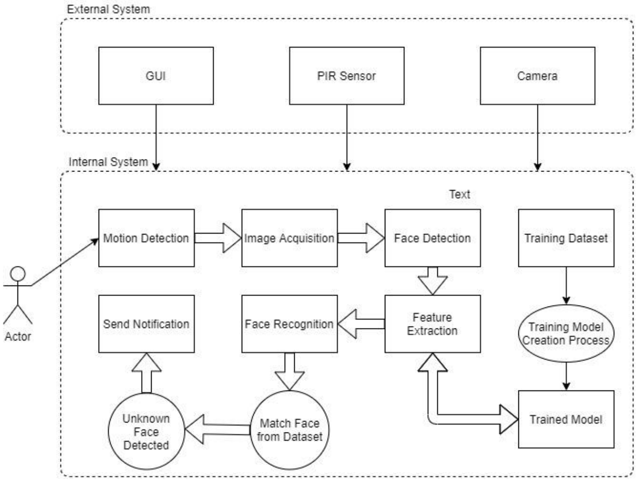
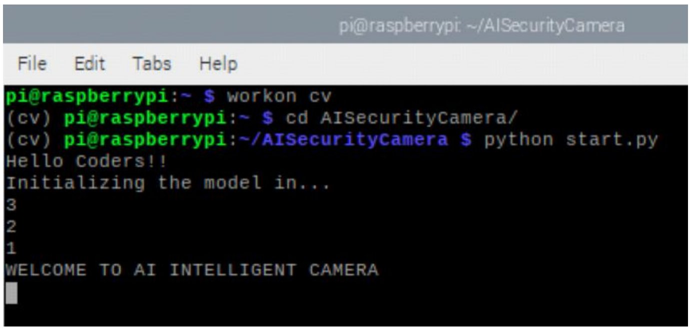


Fig 2: System Architecture

V. RESULTS AND DISCUSSION

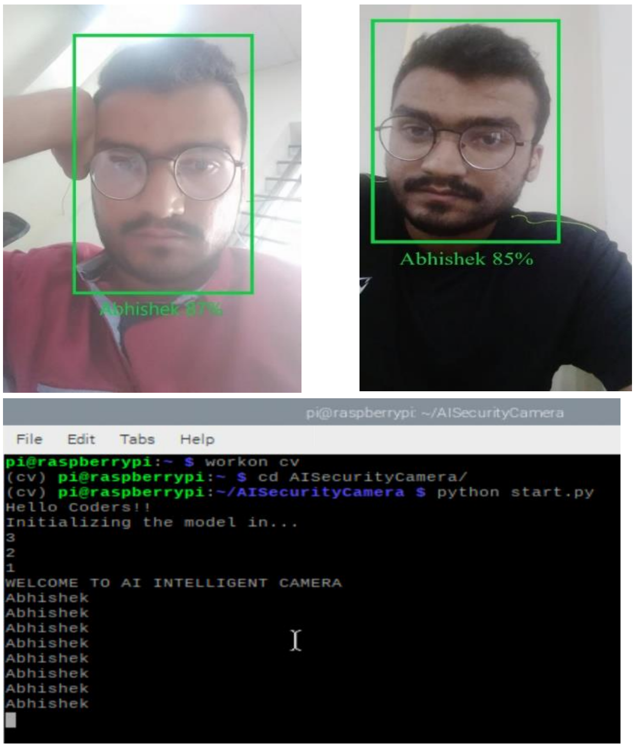
We had connected raspberry pi to screen using HDMI or SSH after this execution of the program is done, and camera feed is started using "*Python start.py*"



```
pi@raspberrypi:~ $ workon cv
(cv) pi@raspberrypi:~ $ cd AISecurityCamera/
(cv) pi@raspberrypi:~/AISecurityCamera $ python start.py
Hello Coders!!
Initializing the model in...
3
2
1
WELCOME TO AI INTELLIGENT CAMERA
```

Fig 3: Software initialization

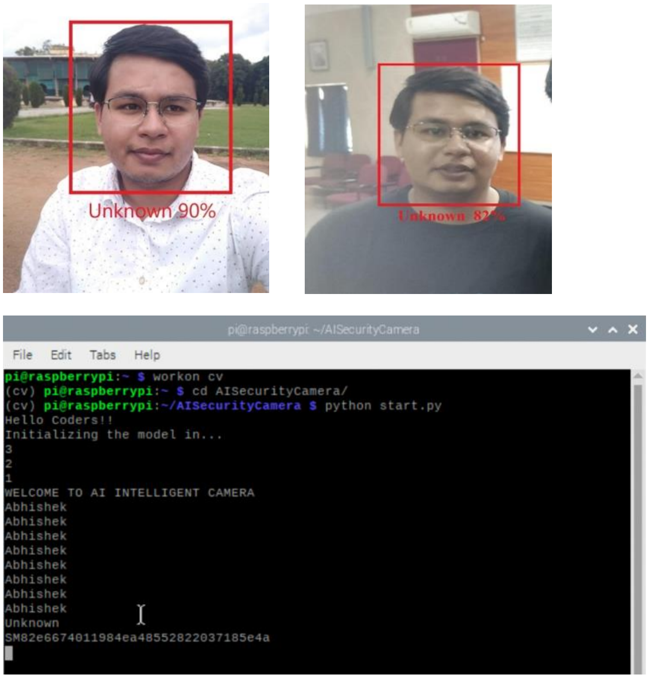
After the initialization is complete, a person goes in front of the camera, which will trigger the PIR sensor detecting motion and turn on the camera. If the Face detected is known Face, then the program will simply print out the name; otherwise, it will be revoked and sends the alert message to the admin.



```
pi@raspberrypi:~ $ workon cv
(cv) pi@raspberrypi:~ $ cd AISecurityCamera/
(cv) pi@raspberrypi:~/AISecurityCamera $ python start.py
Hello Coders!!
Initializing the model in...
3
2
1
WELCOME TO AI INTELLIGENT CAMERA
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
```

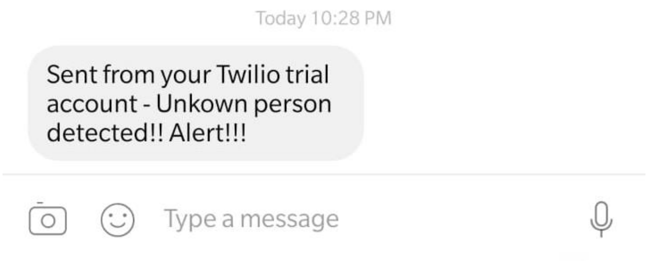
Fig 4: Known Person Detected

If an unknown face is detected, then the camera sends an alert message to the user/admin and raises the alarm to alert.



```
pi@raspberrypi:~ $ workon cv
(cv) pi@raspberrypi:~ $ cd AISecurityCamera/
(cv) pi@raspberrypi:~/AISecurityCamera $ python start.py
Hello Coders!!
Initializing the model in...
3
2
1
WELCOME TO AI INTELLIGENT CAMERA
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Abhishek
Unknown
SM82e6674011984ea48552822037185e4a
```

Fig 5: Intruder Detected



Today 10:28 PM

Sent from your Twilio trial account - Unkown person detected!! Alert!!!

Fig 6: Message sent to alert admin

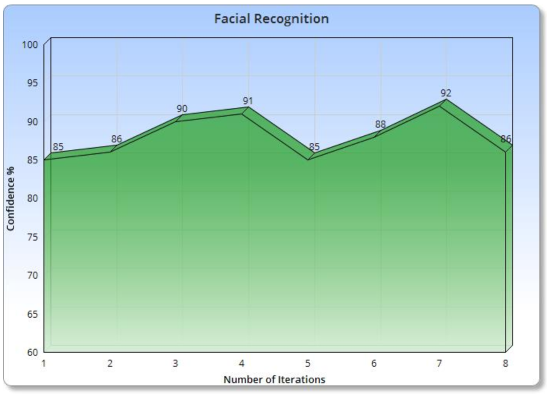


Fig 7: Face Recognition confidence

The model was successfully implemented for real-world applications. The accuracy depends on the data/images used for training. Large and functional datasets give desirable and precise results. In the case of low photos, the model started to underfit. The model can be used at homes or institutes. As soon as the motion is detected, it starts to collect frames and detect faces. The detected faces are recognized, and a further decision is taken to alert the owner upon an intruder or unknown face detection. The model is compact, lightweight, and easy to implement. Results are satisfactory for a microprocessor running OpenCV.

VI.CONCLUSION

We have created a facial recognition system to detect unknown faces with an alerting system. Detailed information gathering has to be done without that the purpose of manufacturing the software won't be adequately satisfied. Implementing the software requires changing the existing CCTVs. Efficient detection of intruder, alert, and notification can be enhanced if AWS or GCP services are used. In this project, we can also include emotional recognizer and weapon detection to advance the model into a more secure one. It secures business that is having a potential threat from thefts and vandalism. There is also a scope to expand by implementing newer technologies like cloud, etc. The accuracy of the Facial Recognition System can be increased by using cutting edge hardware to increase efficiency and reduce time consumption.

VII. REFERENCES

[1]. Illumination Invariant Face Recognition Using Near-Infrared Images. Stan Z. Li, Senior Member, IEEE, Ru Feng Chu, Sheng Cai Liao, and Lun Zhang. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, APRIL 2007 pp. 0162-8828/07/$25.00 2007 IEEE

[2]. Individual Stable Space: An Approach to Face Recognition Under Uncontrolled Conditions. Xin Geng, Zhi-Hua Zhou, Senior Member, IEEE, and Kate Smith-Miles, Senior Member, IEEE. IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 19, NO. 8, AUGUST 2008. pp. 1045-9227/$25.00 © 2008 IEEE

[3]. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez. IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 2, FEBRUARY 2014 pp. 1057-7149 © 2013 IEEE

[4]. Real-World and Rapid Face Recognition Toward Pose and Expression Variations via Feature Library Matrix. Ali Moeini and Hossein Moeini, Student Member, IEEE. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 5, MAY 2015 pp. 1556-6013 © 2015 IEEE

[5]. An Experimental Evaluation of Different Face Recognition Algorithms Using Closed Circuit Television Images. Shahzada Fahad, Sami ur Rahman, Imran Khan, Sanaul Haq. 2017 IEEE 2nd International Conference on Signal and Image Processing. pp. 978-1-5386-0969-9/17/$31.00 ©2017 IEEE

Cite this article as :

Syed Ibrahim, Syed Nahid Suleman, Manikanta Suthapalli, Abhishek Sharma, Shilpa K S, "Design of Intelligent Facial Recognition System using AI for Surveillance Application", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.346-356, May-June-2020. Available at
doi : https://doi.org/10.32628/CSEIT206383
Journal URL : http://ijsrcseit.com/CSEIT206383