IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REAL TIME MONITERING AND ALERTING SURVEILANCE SYSTEM USING FACE RECOGNITION

[1]Sachuthanandam.P, [2]Krishnamoorthy.K, [3]Dinesh Kumar.G, [4]Ranjith kumar.R,

[1]Assistant Professor, [2]Student, [3]Student, [4]Student
[1] Department of Information Technology,
[1] Anand Institute of Higher Technology, Chennai, India.

Abstract : The ability to automatically recognize human faces based on dynamic facial images is important in security, surveillance and health/independent living domains. Specific applications include access control to secure environments, identification of individuals in a specific location, and intruder detection. This research proposes a real-time system for surveillance using cameras. The process is divided into two steps: (1) face detection and (2) face recognition to identify specific individuals. In the first step, the computer tracks and selects the faces of the detected individuals. An efficient recognition algorithm is used to identify the detected faces with the known database. The proposed approach uses Viola-Jones method for face detection, Kanade-Lucas-Tomasi algorithm as feature tracker and Principal Component Analysis (PCA) for face recognition. The system can be activated in various restricted areas such as a suspect's office or home or the entrance of a sensitive installation. This setting works almost perfectly in reasonable lighting conditions and image depths..

I. INTRODUCTION

A face recognition system could also be a technology which is very capable of matching a personality's face from a digital image or a video frame which it has or use it as a reference to map and identify against info of faces. Researcher's area unit presently developing multiple ways throughout that face recognition systems work. The foremost advanced face recognition methodology that is to boot used to manifest users through ID verification services, works by pinpointing and mensuration countenance from a given image. Face recognition systems, which were initially used as a type of laptop programme, are now more widely used on smartphones and in alternative forms of technology, such as artificial intelligence. Face recognition software is categorised as a bioscience since 14computerized face recognition entails monitoring a human's physiological features. Although face recognition systems' accuracy as a biometric technology is lower than that of iris and fingerprint recognition systems, they are widely used due to their non-intrusive and contactless nature. Advanced human-computer interface, video surveillance, and automated picture compartmentalization all use facial recognition technology. We have developed facial recognition technology that can recognise faces.

II. LITERATURE SURVEY

Ishita Gupta & Varsha Patil et.al.(2016) This paper aims to take facial recognition to a level where computers can replace the use of passwords and RF i-cards for access to high-security systems and buildings. By using the Raspberry Pi kit, we aim to make the system cost-effective and easy to use with high performance[1].

Shilpi Singha & S.V.A.V.Prasadb et.al.(2018) The authors tried to propose the concept of face synthesis to improve the accuracy and recognition rate in different face databases such as. Yale, LFW, 3ORL, and AR. The authors offer a difficult overview of several face recognition methods and difficulties to increase the efficiency and rate of face photos in a large database, as opposed to correctness or recognition rate[2].

Eric-Juwei Cheng & Kuang-Pen Chou et.al.(2019) The authors proposed A sparse representation classifier (SRC) is a popular face classifier that sparsely represents a face image by a subset of training data, which is known to be insensitive to the choice of feature space. The proposed method shows the performance improvement of SRC by accurately selecting the feature. Experimental results show that the proposed method outperforms other methods on the given datasets[3].

This paper proposes three main sub-systems: face recognition, face detection and automatic door access control. The principal component analysis (PCA) technique is adapted to the fast-based principal component analysis (FBPCA) approach to perform a 1-face detection and detection procedure, in which the recorded image is identified using a web camera and compared with the image in the database. . If the image is verified, the door will open immediately; Otherwise, a GSM modem will send an SMS to the user informing them that someone unauthorized has entered the property [4].

Lixiang Li & Xiaohui Mu et.al(2020) The authors introduce the related research of face recognition from different perspectives. The paper describes the development stages and the related technologies of face recognition. We introduce the face recognition study conducted under actual situations, as well as the general assessment criteria and face recognition database. We present a prospective analysis of facial recognition. Face recognition has emerged as a key area for future research and has several potential applications prospects[5].

Avinash Kumar Singh & Piyush Joshi et.al.(2014) In this paper, the author proposes a robust liveness detection scheme based on the challenge and response method. A Liveness module is added as an extra layer of security before the face recognition module. The Liveness module creates arbitrary challenges and tracks the user's response using face macro characteristics, mainly eyes and mouth movement. The 2liveness module is put to the test by using various spoofing attacks on various mediums, such as images, videos, etc. Our technology has been able to identify and thwart five different sorts of assaults[6].

Urvashi Bakshi1 & Rohit Singhal et.al.(2014) The author proposed system is a whole process of face recognition that involves face detection, feature extraction, and recognition will be in three steps. Each of the three phases calls for a different approach. These methods vary depending on the environment, including the backdrop, lighting, facial position, and exposure. This article offers a comprehensive examination and analysis of the major face detection methods[7].

Farah Deeba1 & Aftab Ahmed et.al.(2019) In this paper, authors developed a face recognition method LBPH-based technology is used to deal with real-time recognition of human faces in both low- and high-resolution photos. To encode edges more affordably, we wish to boost the proper contrast for facial emotions and open edges. Local Binary Pattern Histogram (LBPH) is the name of these effective characteristics[8].

Maliha Khan & Sudeshna Chakraborty. et.al.(2019) The authors proposed system is PCA (Principal Component Analysis) face recognition method. Principal component analysis (PCA) is a statistical method under the broad heading of factor analysis. PCA is used to shrink enormous data storage volumes to the size of the feature space needed to cost-effectively represent the data. Using a large 1-D pixel vector created from a 2-D face picture intended for face identification by PCA, a compact key component 4 of the space function is used. The self-space projection is what is meant by this[9].

Sefik Ilkin Serengil & Alper Ozpinar .et.al.(2020) In this paper, first an iterative face recognition is performed and then the developed lightweight hybrid high-performance face recognition framework is described. Its hybrid feature helps replace face recognition models in sophisticated models[10].

III. PROPOSED SYSTEM

The proposed solution is a real-time face recognition system reads video from a camera connected to a computer running software, detects the face in front of the camera, and uses the face to check whether this face exists in a set of face images in a database. Authentication technique. Face detection and face recognition are the two sections of the program. In the past ten years, a lot of face recognition software has been put into use. Every program differs from other software in its processes and algorithms. To identify the face, some facial recognition software pulls facial elements from the input image. Some face recognition algorithms normalize a collection of face photographs, then compress the face data and save it in an image. Face data is compared to the supplied picture. Three-dimensional face recognition is a novel technique used for face identification. 1 InIn this technique, the face's shape is captured using a 3-D sensor so that only its distinctive traits, such its

IV. MODULES AND DESCRIPTION

4.1 System Modules

The system comprises of 4 simple modules namely-

- **Sensor module**
- **Camera module**
- **Face Access Control Lock**
- **Notification service**

4.1.1 Sensor Module

Distributed around home devices and entry points, the sensor module can record signals whenever the sensors are triggered. The main door is fitted with a door magnet sensor. In the absence of the owner, when the door is opened/broken, the home alarms will start sounding and the owner will be alerted with specific notifications. If an intruder tries to force open the door, vibration sensors mounted on the door will detect it. A vibration sensor is integrated into window panes, a common entry point for burglars. The window grill is covered with wire that runs through all parts of the grill. If the thief tries to cut/weld the grill, the wire will cut and in turn, a signal will be generated. A PIR sensor mounted inside or outside a home can detect human presence where it normally wouldn't. There is an emergency panic switch, which can be used in emergency situations, about possible theft while the owner is inside. Another important aspect of using a panic switch is for senior citizens who are alone indoors and require medical attention.

4.1.2 Camera Module

The camera module consists of a primary camera and a secondary camera. The primary camera is a web cam, which is mounted on the tracking device. This camera is used for face detection and recognition. D. The secondary camera, on the other hand, has its own recording and tracking system. It is a DVR equipped Hikvision network camera with 1TB HDD capacity. This network camera captures and transmits images/videos.

4.1.3 Face Access Control

It is a door lock that is simulated by a servo motor attached to a miniature door model. The face recognition program runs in a loop and once a known face is detected, a servo is activated for access. If the detected face is not visible, no permission will be granted. A person can be distinguished from a thief by finding out if he has any weapons. For demonstration purpose, simple tools such as hammer, scissors, knife etc. are readily available in the public dataset. This reduces development time because pre-trained models trained on those datasets are readily available.

4.1.4 Notification Service

Notifications to the owner can be on his phone or any remote device. The smartphone/feature phone is the primary device for receiving alerts in the form of notifications, SMS, calls, etc. using the IFTTT app on Android and iOS. Alerts can be created to inform the police in case of theft. This module reports activity through sensors and sends messages when an intruder with a weapon is captured by a camera.

4.2 Image Processing Algorithms

An algorithm was developed to manage the tasks of facial access control and weapons detection. A survey of state-of-the-art methods was carried out, providing clues to the performance of these algorithms. Image processing involves acquiring image/video data and performing a series of numerical calculations to produce the desired output. The entire processing pipeline includes multiple stages to achieve outputs in different ways such as bounding box detection, ROI landmark detection, bounding box labelling, pose estimation, optical flow, gathering information about activity, tracking a specific object in real-time. The image should be pre-processed before sending it to the algorithm so that inferences are faster. Pre-processing stages include cropping, resizing, blurring, scaling, colour changes, etc. After obtaining the projections, post-processing is required to display the frame in its original form. The objective of the Face Access Control Lock module is to recognize faces as input in real-time footage from video captured by the Raspberry Pi Camera and grant access to that person if authorized.

4.3 Face Recognition

The task of face recognition is to detect faces in each frame of a video object created for live feed. Detection can be done using a deep learning-based CNN model, pre-trained on faces and available as open-source software. The results of the detection give the location of the detected faces in each frame. For each detected face, a 128-D feature vector is generated by calculating the distances between eyes, nose, mouth, chin, jaw, forehead, etc., and their measurements using facial landmarks. These vectors are matched to known faces with its predicted feature vectors. If they match, the corresponding name stored by the vector is returned as labels. The end result is a bounding box with a name label on top of the face. It should be noted that the above model used to implement the above method does not work for face front detection and other orientations of faces.

4.3.1 Face Recognition

Various detection algorithms have been developed to detect faces. The first method was developed by Paul Viola and Michael Jones in the early 2000s and has been widely adopted. It returns the detected eyes and faces as output. Advanced methods are now being used. Some methods are as follows-

4.3.2 Haar-cascades: These methods extract features such as Haar from a given image to convert feature points into feature vectors. One of the popular methods is histogram of oriented gradients (HOG). This method indicates arrows at each pixel by comparing the brightness levels of neighbouring pixels in the grayscale image. A collection of such arrows gives the direction of pixel intensity as it varies from dark to bright areas. However, the dimensions are large for processing. Dimensionality can be reduced by considering larger areas of the image instead of going pixel-by-pixel.

4.3.3 Eigen Faces: This method reduces the dimensionality of images by extracting only relevant information from the image. This method uses principal component analysis (PCA) of the image, which are the features with maximum variance, for feature extraction. This reduces the image representation complexity and saves time and space during computation.

4.3.4 Fisher Faces: This approach promises to overcome the disadvantages of the Eigen Faces method. Extrinsic factors such as illumination affect PCA, where components containing biased information can also be removed. The solution lies in minimizing the variance between classes rather than maximizing the overall variance through LDA (Linear Discriminant Analysis). It basically separates same classes from different classes. So it is used to recognize faces.

4.3.5 Linear Binary Pattern Histograms: The methods described above work well with low-dimensional data. However, they fail if the data size is reduced and the factors introduce noise at non-ideal levels. According to this algorithm, each pixel is assigned a value of 1 or 0 based on whether its intensity increases or decreases compared to the previous pixel's intensity value. Neighboring pixels form a 3x3 neighbourhood. The pattern of numbers generated in this manner gives a better representation of the image known as LBP codes. These symbols help to recognize faces. More recently, new statistical and probabilistic models have been developed using the above approaches. These approaches are deep learning-based CNNs adapted for the purpose of face detection.

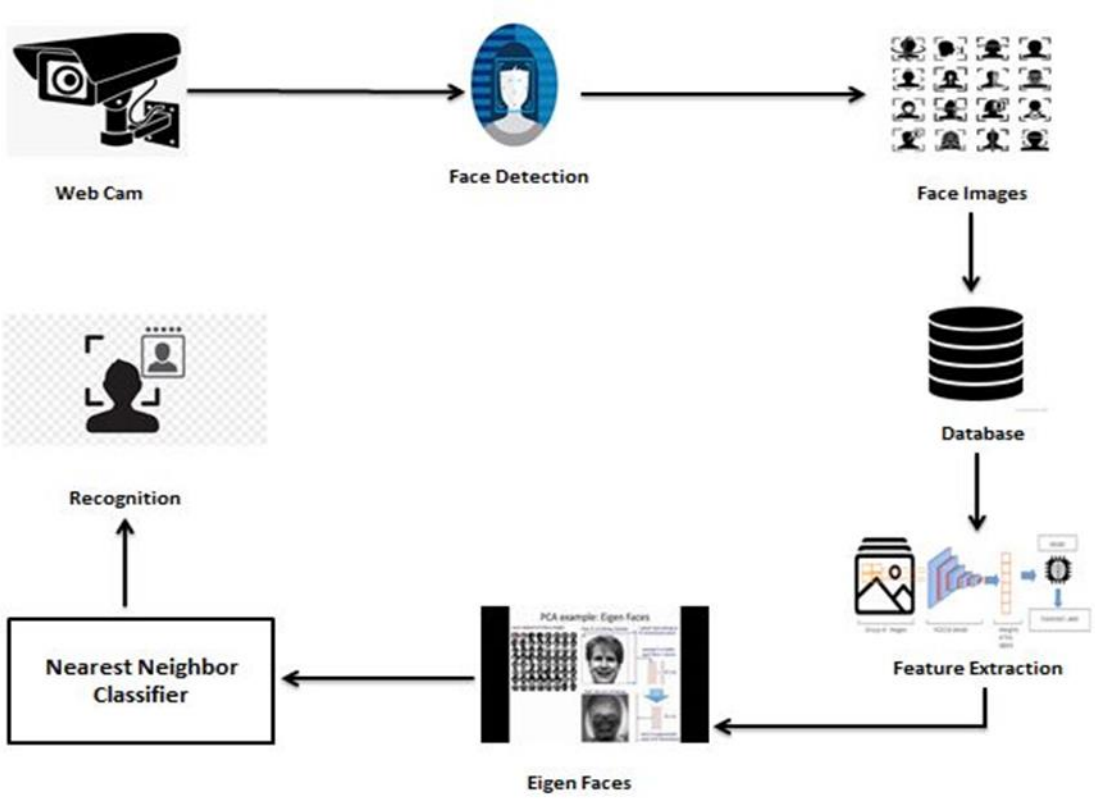

FIG.1: System Architecture

V. EVALUATION RESULTS AND EXECUTION

5.1 HOME PAGE: This project has a home page that will open the user interface to run the program

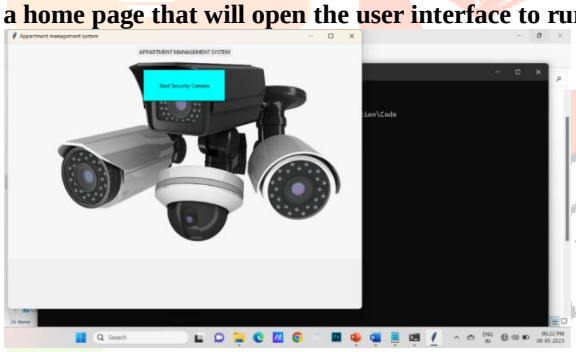

Fig.2

5.2 The next page is called user verification for the new and existing users will get to verify their identity.

Fig.3

5.3 If the identified person is a new user the application will automatically will starts to scan the person

Fig.4

5.4 This screenshot will explain the collection of the new user data

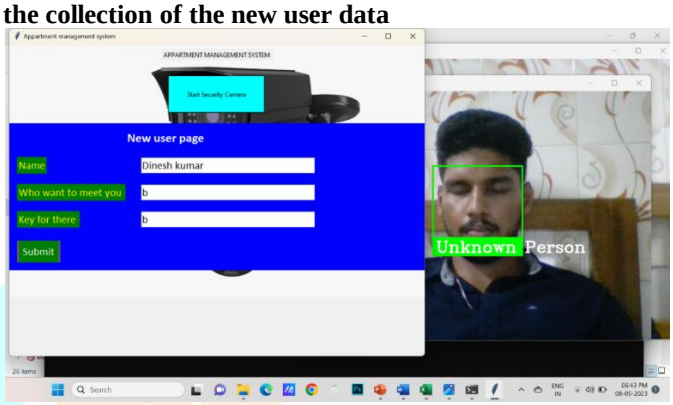

Fig.5

5.5 This screenshot will explain the collection of the new user data

Fig.6

5.6 And this will show their entry and exit time in the Excel file

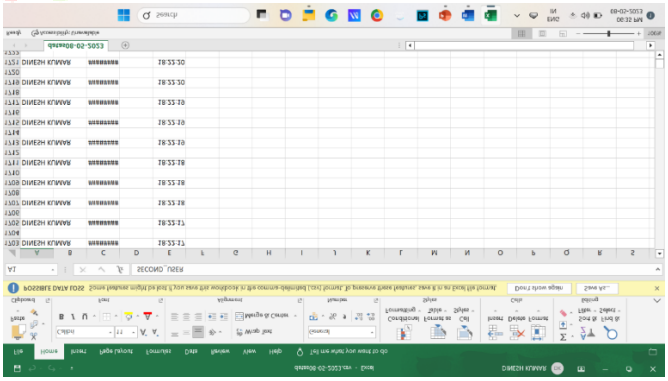

Fig.7

VI. CONCLUSION

As they perform better than other security systems in the future, face recognition technologies will be employed for security purposes more and more. A facial recognition system under experimental research that can be used to access control and identity systems is given. It was discovered that the suggested facial similarity meter operated adequately. Based on face detection and identification, the system's software was written in Python. Even though this system's accuracy is greater than 90%, it might be made better by adding more features. The threshold value might be improved with some light normalization and precise facial

segmentation. The execution time can be sped up by, for instance, leveraging relative face rotation and gesture geometry modeling to go across warp space more effectively.

FUTURE ENHANCEMENT

In future system there will multiple ways to calculate the In and Out time of the users using PIR-based motion detector (PID) and infrared (IR).And with the help PIR-based motion detector (PID) and infrared (IR) of and the servo motor will automatically operates the door.

The another system which will detect the iris in the human eye with help of iris scanner The iris cameraWill detect the iris in the human eye and will entry the In and Out time of the user.

If the stranger tries to brute force to bypass the door the Door Collision Detection will alarm the Surroundings and will send notification to the corresponding maintenance or admin team.

REFERENCES

[1]. Gupta, Ishita, et al. "Face detection and recognition using Raspberry Pi." 2016 IEEE international WIE conference on electrical and computer engineering (WIECON-ECE). IEEE, 2016.
[2]. Singh, Shilpi, and S. V. A. V. Prasad. "Techniques and challenges of face recognition: A critical review." Procedia computer science 143 (2018): 536-543.
[3]. Cheng, Eric-Juwei, et al. "Deep sparse representation classifier for facial recognition and detection system." Pattern Recognition Letters 125 (2019): 71-77.
[4]. Yugashini, I., S. Vidhyasri, and K. Gayathri Devi. "Design and implementation of automated door accessing system with face recognition." International Journal of Science and Modern Engineering (IJISME) 1.12 (2013).
[5]. Li, Lixiang, et al. "A review of face recognition technology." IEEE access 8 (2020): 139110-139120.
[6]. Singh, Avinash Kumar, Piyush Joshi, and Gora Chand Nandi. "Face recognition with liveness detection using eye and mouth movement." 2014 international conference on signal propagation and computer technology (ICSPCT 2014). IEEE, 2014.
[7]. Bakshi, Urvashi, and Rohit Singhal. "A survey on face detection methods and feature extraction techniques of face recognition." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3.3 (2014): 233-237.
[8]. Deeba, Farah, et al. "LBPH-based enhanced real-time face recognition." International Journal of Advanced Computer Science and Applications 10.5 (2019).
[9]. Khan, Maliha, et al. "Face detection and recognition using OpenCV." 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE, 2019.
[10]. Serengil, Sefik Ilkin, and Alper Ozpinar. "Lightface: A hybrid deep face recognition framework." 2020 Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE, 2020.