Access Control in Offices Using Face Recognition

R.Arthi[1], Dr.Jasmin Sabeena[2], Dr.K.Shanthi[3]
[1, 2, 3] Dept of Computer Science
[1, 2, 3] SRI VENKATESWARA Engineering College,Tirupati

Abstract- *Human face is the most significant characteristic to identify a person. From unlocking smartphones to speeding-up the identification process at airport border controls, Face Recognition is used. Face recognition is one of the rapid growing biometric security technologies. With the recent advancement of computer vision and AI/ML techniques, Face Recognition is no longer a challenging task. Hence, we are proposing a method which will be able to recognize either a person is having the access to enter the office or not, using the Local Binary Patterns Histograms (LBPH) algorithm.First, we need to train the algorithm with the facial images of the people we want to recognize and apply the LBP operation and create a histogram to represent each image from the training dataset. Similarly, for given input image, we create a histogram which represents it and find the image that matches the input image, by comparing the histograms. LBPH is provided by the OpenCV library. OpenCV supports a wide variety of languages like Python, C++, Java, etc., In our Project, we are implementing the LBPH algorithm in Python Programming Language. We can evaluate the model using either image or video based data in our project. After Face recognition, the access status is displayed*

Keywords- Face Recognition, Face detection, Camera calibration, unconstrained environment, access control, Principal Component Analysis, Neural Network, Door Access.

I. INTRODUCTION

Human beings can perform face recognition automatically and practically with no effort. Though it looks like a very simple task for us, it has been proven to be a complex task for a computer, because it has many variables that can impair the accuracy of the methods like illumination variation, low resolution, occlusion, etc. Face recognition is the task of recognizing a person based on its facial image. Before Face Recognition, Face Detection needs to be done.

Object detection is a broad area in the field of Image processing and computer vision. Face detection is one of the major research fields under object detection. The motivation behind face detection algorithms is to locate whether there are any faces in an image or not. In an image to recognize the face in it, first, have to detect whether there is a face in the image or not. An image has to be generated which can be manipulated and used for various identification is important in face area determination. Once the face is detected, using the location of the detected face, the face recognition algorithm can be used to find the person in it.

Face Detection has the objective of finding the faces (location and size) in an image and extract them to be used by the face recognition. Face Recognition is done with the facial images already extracted, cropped, resized and usually converted to grayscale. The face recognition algorithm finds characteristics which best describe the image. There are different types of face recognition algorithms like Eigen faces, Local Binary Patterns Histograms (LBPH), Fisher faces, Scale Invariant Feature Transform, etc. Each method has a different approach to extract the image information and perform the matching with the input image. In our project, we are using one of the popular face recognition algorithms: Local Binary Patterns Histograms (LBPH).

II. EXISTING SYSTEM

In existing system, the traditional security system needs an individual to use a key, identification (ID) card or password to access an area such as home and workplace. However, it has many weaknesses as they can be easily lost or stolen. Most doors are controlled by persons with the employment of keys, security cards, or pattern to open the door.

III. PROPOSED SYSTEM

The aim of this system is to assist users for improvement of office security by using face detection and recognition. In our proposed work, we are implementing a method, which will able to recognize the faces and displays whether the person is having the access, or not by using Local Binary Patterns Histograms (LBPH) algorithm. We are also integrating the model into Web Application using Flask Framework for better User Interface.

3.1 PROPOSED ALGORITHM

Local Binary Pattern (LBP) is a simple and yet very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of every pixel and

considers the result as a binary number. As LBP is a visual descriptor it can used for face recognition tasks. The LBPH uses 4 parameters:

Radius: The radius, which represents the radius around the centre pixel, is utilised to construct the circular local binary pattern. Usually, it is set to one.

Neighbors:the quantity of sample points needed to create a circular local binary pattern. Remember that the computational cost increases as you include more sample points. Typically, it is set to eight.

Grid X:the amount of horizontally oriented cells. The resulting feature vector has a higher dimensionality the more cells there are and the finer the grid is. The default setting is eight. The purpose of this technology is to aid users in enhancing office security through face detection and identification. In our suggested work, we are putting into practise a system that can identify faces and shows whether or not the person has access by using the Local Binary Patterns Histograms (LBPH) algorithm. For a better user interface, we are also integrating the model into a web application using the Flask Framework.

Grid Y: the quantity of cells arranged vertically. The resulting feature vector has a higher dimensionality the more cells there are and the finer the grid is. The default setting is eight.
The first computational step of LBPH is to create an intermediate image that describes the original image in a good and better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window method, based on the parameter's radius and Neighbors. Each histogram graph created is used to represent each image from the training dataset. So, given an input image, we need to perform the steps again for this new image and creates a histogram which represents the image. So as to find the image that matches the input image we just need to compare two histograms and return the image with the closest histogram.

1) Data Flow Diagram

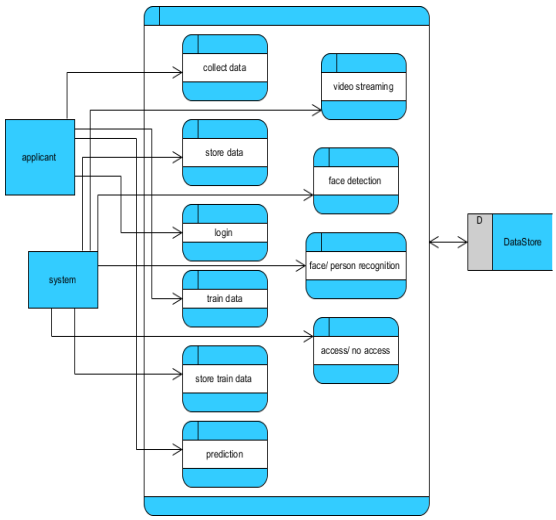


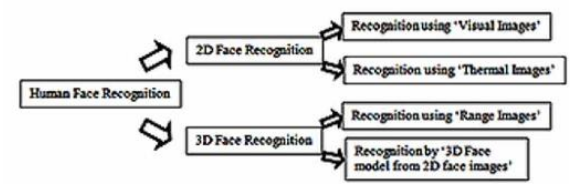
Fig.[1] Data Flow diagram for Access control using Face Recognition

IV. SYSTEM MODULE

1. *Face Acquisition*
2. *Pre-processing*
3. *Feature Extraction*
4. *Face Recognition*
5. *Face Detection*

1)Face Acquisition

Three-dimensional (3D) face data acquisition is the first phase in face acquisition study, and the quality of the data gathered directly influences the subsequent research. There are new tools and ways for data collecting as a result of the advancement of computer vision technology. Almost any static camera or video system that produces images of appropriate quality and resolution may capture faces using facial-scan technology. The definition of the facial characteristics to be utilized in all upcoming authentication activities may be found in identity enrollment photographs, which are crucial for final verification. It is necessary to use specialized reader hardware for face recognition access. If a picture of the person's face is being used to access doors, a camera-based terminal is necessary. That's frequently not enough. Special camera sensors built into the hardware allow it to measure the depth and three-dimensional structure of the view in front of it. This enables face recognition technology to distinguish between a real person and a snapshot of that person in front of the device. Face recognition technology requires this crucial security element. For face recognition, you shouldn't just use a standard camera or CCTV camera.



2)Preprocessing

In this study, a modified version of the adaptive thresholding (ADT) approach developed by Bradley and Roth [15] is suggested. We briefly describe the proposed ADT approach before applying it to the face identification application's input image preprocessing.

The proposed face representation method

Most thresholding techniques select a predetermined threshold value and compare each pixel's value to it. A fixed thresholding method fails in such a setting because it is not resilient to variations in light. ADT is a method for dealing with changes in light. By utilising the integral image, Bradley & Roth [16] improved the ADT approach first presented by Wellner [17]. To obtain a representation of the photos with faces, we enhanced this method.

$$C = 0.95 + \frac{|\mu - \sigma|}{1000}$$

where, **μ** and **σ**represent the input image's average and standard deviation of intensity. If a pixel's value is less than the sum of its mean values plus one, it is set to 0 (dark), otherwise it is set to 1. (white). Wellner [17] and Bradley et al [16] select the value of the image length's and its number. Additionally, Bradley & Roth argued that one can employ a different for various applications, Due to the fact that facial features like the eyes, nose, and mouth have no relationship to backdrop pixels, the number of surrounding pixels must be chosen. So, as a minor constant, we select the quantity of surrounding pixels. If the image has high intensity values, ADT might not succeed because the pixel value often increases faster than the surrounding pixels and might be set incorrectly to. When setting pixels with a value of, the same scenario repeated in images with low intensity values (dark). To solve this issue, the suggested solution interferes the mean and standard deviation in the coefficient.With respect to earlier efforts, we contrasted our suggested depiction of facial images. It should be noted that a fair comparison cannot be made because these methods suggested to handle augmented reality or photos with character information. We merely provide an illustration to demonstrate the effectiveness of the coefficient given in equation 1. Four techniques are contrasted in Fig. 4. The suggested method scales binary images produced from the input image to look for faces in images of various scales. Wellner techniques had the drawback of not fully highlighting facial features. As a result, missing facial characteristics might occasionally occur when photos are scaled. Fig. 4 illustrates qualitatively how our suggested strategy highlights the face features more effectively.

Preprocessing phase

Using the suggested representation strategy, we preprocess arbitrary input images into binary images. Guidelines derived from the threshold learning process are as follows:

Rule 1: $(Region1 + Region2) > (Region3 + Region4)$.
Rule 2: $W > T1$ and $W < T2$, where W denotes the summation of pixels in whole window.
Rule 3: $(Region1 + Region2) > T3$.
Rule 4: $Regions(1 + 2 + 6 + 7) > k \times W$, where $0 < k < 0.5$.

a **b** **c**

Where (a) Normalized reference model obtained from ADT, where (b) RM and (c)regional maxima.

3)Feature Extraction

A Face extraction is the manual or mechanical procedure of opening a clogged or compacted pore. It's common practice to include extractions in a facial. Most people require at least a few extractions during each facial, though if this is your first facial, you might need more.

Geometric Feature Based Methods

The geometrical features of the eyes, mouth, and nose are computed using the feature-based or analytical approach. The feature vector in this illustration is made up of the face's outline and the locations of the various facial characteristics. The feature points are typically picked 5659 for a decent extraction process based on their accuracy for automatic extraction and importance for face depiction. The positions of those points are employed in the computation of the geometrical relationships. Such a system is insensitive to changes in image position. However, Geometric features display the dimensions and placements of facial elements, which are then removed to create a feature vector that symbolizes the face (Mahto & Yadav, 2014). This comprises the lips, eyes, brows, and nose (Lajevardi & Hussain, 2012).

Holistic Based Methods

The overall characteristics of the human face pattern are taken into account in holistic or appearance-based techniques. Contrary to feature-based recognition, the entire face region is recognized without the use of a few points from various facial regions. Holistic techniques frequently encode the depiction of faces as pixel intensity arrays without detecting any facial features. Since the identification of geometric facial features is not necessary, this class of face extraction is more practical and simpler to construct than geometric feature-based approaches. Such methods that reduce the image to a low-dimensional feature space with increased discrimination power are essential to holistic methods. This is due to the possibility that, in a high-dimensional feature space, the distances between a given probe's nearest and farthest neighbors may become indistinguishable. Face photos include high statistical regularities or redundancies, like the majority of natural signals. Therefore, by relying on their statistical regularities, numerous dimensionality reduction frameworks have been created to find low-dimensional representations of human face images. Look-based approaches extract the changes in the face's appearance by applying image filters, like Gabor wavelets, to either the entire face or selected facial areas (Mahto & Yadav, 2014). Principal Component Analysis (PCA), Independent Component Analysis (ICA), Locality Preserving Projections (LPP), Linear Discriminate Analysis (LDA), Gabor wavelets, Local Binary Pattern (LBP), and Discrete Cosine Transform are examples of appearance-based methods (DCT). Additionally, two or more algorithms are typically integrated to create a hybrid approach in order to create a full face recognition system.

4)Face Recognition

Face recognition is a technique used to identify people whose faces have been saved in a data set. Face recognition has always been an important area of research, despite the fact that other identification methods may be more accurate. This is because face recognition is a non-intrusive means of identifying and because it is a common way for people to identify themselves. For facial recognition, there are numerous methods. For facial recognition in this case, we utilize OpenCV. In order to recognize faces, a face recognizer must first be trained using an image that has been preprocessed. We put the recognizer to the test after training it to see how it performs. The recognition rate (RR) is calculated as follows

$$RR\,(\%) = \frac{Number\ of\ correct\ match}{Number\ of\ training\ set} * 100$$

	Recognition Rate (%)					
Method	50% 50%		70% 30%		90% 10%	
LBP +KNN Using:	Yale	ORL	Yale	ORL	Yale	ORL
Euclidean Distance	91.1	93	95.6	93.3	100	94
Correlation Distance	90	94	97.8	94.5	100	95
Canberra Distance	91.1	95	100	96	93.3	98
Manhattan Distance	94.4	96.5	95.6	97.3	100	99
Mahalanobis Distance	94.4	97	100	97.5	100	98

Eigen Face Recognizer- The Eigenfaces face recognizer analyses each training image of each character as a complex system and attempts to identify its constituent parts. By excluding the less important portions of the images, it not only recovers the crucial components from the training data but also conserves memory. These components are important and beneficial (the areas that capture the most variance/change).

Fisher Faces Recognizer-The Fisher faces method removes important traits that distinguish one person from the others instead of generating beneficial features that represent all the faces of all the people. The characteristics that make one individual stand out from the rest do not predominate over those of the other people.

Local Binary Patterns Histograms- Since light has an impact on Eigenfaces and fisher faces in real life, it is impossible to guarantee ideal lighting. The LBPH face recognizer is a development that addresses this flaw. Finding an image's local features is not the goal. The LBPH algorithm compares each pixel with its surrounding pixels in an effort to identify the local structure of an image.

5)Face Detection

Face detection is also known as facial detection and from computer technology that uses artificial intelligence to find and recognize human faces in digital photographs. Face detection technology can be utilized in a multitude of fields, including security, biometrics, law enforcement, entertainment, and personal safety, to enable real-time surveillance and tracking of people. From basic computer vision methods to developments in machine learning (ML) to increasingly complex artificial neural networks (ANN) and related technologies, face detection has advanced, leading to ongoing performance increases. It now serves as the foundation for a number of crucial applications, such as face tracking, face analysis, and facial recognition. The application's ability to perform sequential tasks has a substantial impact on face detection.

Despite the fact that face detection is a component of all facial recognition systems, not all face detection techniques are emp loyed for facial recognition.Face detection can also be used for facial motion capture, which involves employing cameras or l aser scanners to electronically translate a person's face motion s into a digital database. Using this database, realistic compute r animation for movies, video games, or avatars can be created .A software implementation of emotional inference, which can be used, for instance, to help people with autism comprehend the emotions of those around them, is another usage for face detection. The software uses cutting-edge image processing to "read" the emotions displayed on a person's face. Lip reading, or inferring language from visual signals, is another application. This may be useful in security applications as it enables computers to identify the speaker. In order to ensure privacy, face detection can also be used to determine which portions of an image should be blurred.

V. LIMITATION OF EXISTING SYSTEM

The LBP algorithm is highly sensitive to image quality and it is highly affected by the blurred images. LBP is a texture based descriptor which extracts the local grayscale features by performing feature extraction on a small region throughout the entire image. Hence, test images and train images have to be of same quality and need to be captured by the same device to obtain high accuracy.

In our project, the laptop built-in webcam is the default device to capture image. The webcam and lighting source of the laptop can be of low performance which cause the captured images appear to be darker and blurred. This cause the system to work the best only if the test image and train image are captured at the same place under approximately same illumination.

If an individual wears make up in the image for face recognition, the important features will be covered. Similarly, the face region should not be covered by hair or any accessories to ensure better performance because anything covering the face region will be assumed as a face feature. This can cause a relatively large difference between train image and test image.

VI. APPLICATIONS

- Security companies use face recognition to secure their premises.
- Ride-sharing companies can use face recognition to ensure that right passengers are picked up by the right drivers.
- Immigration checkpoints use face recognition for enforcing smarter border control.
- Face recognition can be used for automatic attendance system in Schools and College

VII. CONCLUSION

The goal of our project was to build a Face Recognition system for Access Control in Offices using LBPH algorithm and to integrate the model with Web Application using Flask. Once implemented, it can be used to recognize people who are having access to enter into office. The Proposed model was tested for detecting faces and to recognize faces, using Haarcascade classifier for face detection and LBPH algorithm for face recognition. Our system is capable of detecting and recognizing faces and the performance of system have acceptable good results.

VIII. FUTURE ENHANCEMENTS

Important topics for future work with access control on voice recognition and biometrics to enhance the features of fraudulent detection and integration of all this modules in cloud for avoiding the data loss by strengthening the encryption schemes to create secure cloud storage mechanisms. With reasonable engineering effort, the framework can be integrated into production environments to strengthen the data security.

REFERENCES

[1] A. M. Jagtap, V. Kangale, K. Unune and P. Gosavi, "A Study of LBPH, Eigenface, Fisherface and Haar-like features for Face recognition using OpenCV," 2019 International Conference on Intelligent Sustainable Systems (ICISS), 2019, pp. 219-224, doi: 10.1109/ISS1.2019.8907965.

[2] K. Kadir, M. K. Kamaruddin, H. Nasir, S. I. Safie and Z. A. K. Bakti, "A comparative study between LBP and Haar-like features for Face Detection using OpenCV," 2014, pp. 335-339, doi: 10.1109/ICE2T.2014.7006273.

[3] J. -J. Lin and S. -C. Huang, "The implementation of the visitor access control system for the senior citizen based on the LBP face recognition," 2017 International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2017, pp. 1-6, doi: 10.1109/iFUZZY.2017.8311817.

[4] H. K. Ekenel, and R. Stiefelhagen, “Local appearance based face recognition using discrete cosine transform,” in Proceedings of International Conference on Signal Processing, Antalya, Turkey,4-8 Sept. 2005, pp. 1-5.

[5] A. Hadid, M.Pietikainen and T.Ahonen. A discriminative feature space for detecting and recognizing aces. In Proceedings of the 2004 IEEE computer society conference on Computer vision and pattern recognition, Washington, DC, USA, 2004, CVPR '04, pp. 797-804, IEEE Computer Society.

[6] M. A. Abuzneid and A. Mahmood, "Enhanced Human Face Recognition Using LBPH Descriptor, Multi-KNN, and Back-Propagation Neural Network," in IEEE Access, vol. 6, pp. 20641-20651, 2018, doi: 10.1109/ACCESS.2018.2825310.