DIGIYATHRA

Professor Annamma S Joseph[1], Meera Krishna C[2], Shahala Basheer[3], Shadiya Basheer[4], Vishnu Sabu[5]

[1-5] *Dept. Electronics and Communication, Mar Athanasius College of Engineering, Kerala ,India*

Abstract:- *The aim of the project is to provide a seamless experience for the air travellers at every touch point of the journey. Walk-through the security scanners swiftly owing to advanced biometric security solutions is the main idea behind this project. With this initiative, the airport entry and boarding pass security check-in would be made digital. During online ticket booking, the passenger will be required to provide a passport picture. This would be added under the database of the specific flight. Thereafter, the passenger can access various services like bag-drop, security check-in and boarding using the biometric. Face recognition will make faster airport entry and automated check-in without requiring any paper based interventions. Apart from this, the process will accelerate throughput of passengers at airports, reduce cost as less manpower deployment will be required for verifying paper-ids and tickets at various points. Hence, it ensures flyers complete the airport process quickly*.

Key Words: **Facial recognition, LBPH recognizer, RFID Baggage tracker, airport security systems, microcontroller**

1. INTRODUCTION

Facial recognition is the fastest biometric technology that has one and only purpose – to identify human faces. Forget about fingerprints readers and eye scanners, current face recognition systems analyze the characteristics of a person's face images that were taken with a digital video camera. It's the least intrusive method that provides no delays and leaves the subjects entirely unaware of the process.

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a videosource. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selectedfacial features from given image with faces within adatabase.It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analysing patterns based on the person's facial textures and shape.

Here, we include pictures in a database and the input face is compared with all the images in the database. The confirmed picture is selected from the database and the name is given back. Along with this, an added feature of tracking the bags by using a bag-tag tracker system is also implemented.

1.1 Facial recognition

Face Detection has been one of the hottest topics of computer vision for the past few years. This technology has been available for some years now and is being used all over the place. From cameras that make sure faces are focused before you take a picture, to Facebook when it tags people automatically once you upload a picture. Or some shows like CSI used them to identify "bad guys" from security footage or even unlocking your phone by looking at it! Lets understand the processes working behind this.

As a biometric, facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Regardless of specific method used, facial recognition is accomplished in a five step process. First, an image of the face is acquired. This acquisition can be accomplished by digitally scanning an existing photograph or by using an electro-optical camera to acquire a live picture of a subject. As video is a rapid sequence of individual still images, it can also be used as a source of facial images.

Second, software is employed to detect the location of any faces in the acquired image. This task is difficult, and often generalized patterns of what a face "looks like" (two eyes and a mouth set in an oval shape) are employed to pick out the faces

Once the facial detection software has targeted a face, it can be analyzed. Facial recognition analyzes the spatial geometry of distinguishing features of the face. Different vendors use different methods to extract the identifying features of a face. Thus, specific details on the methods are proprietary. The most popular method is called Principle Components Analysis (PCA), which is commonly referred to as the eigen face method. PCA has also been combined with neural networks and local feature analysis in efforts to enhance its performance. Template generation is the result of the feature extraction process. A template is a reduced set of data that represents the unique features of an enrollee's face. It is

important to note that because the systems use spatial geometry of distinguishing facial features, they do not use hairstyle, facial hair, or other similar factors.

The fourth step is to compare the template generated in step three with those in a database of known faces. In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity.

The final step is determining whether any scores produced in step four are high enough to declare a match. The rules governing the declaration of a match are often configurable by the end user, so that he or she can determine how the facial recognition system should behave based on security and operational considerations

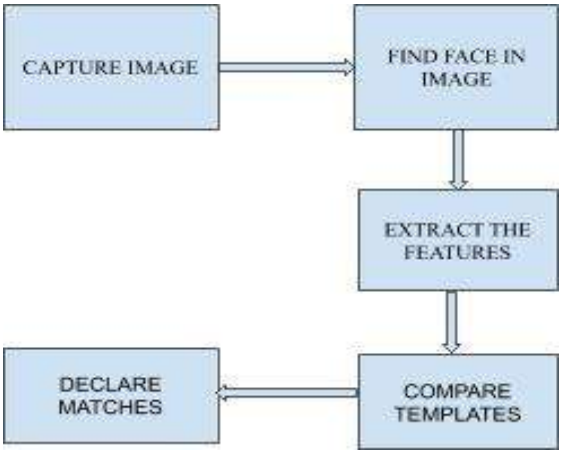

Fig 1:Block diagram of facial recognition

2. FACE RECOGNITION USING LBPH FACE RECOGNIZER

Local binary patterns Histogram is a type of visual descriptor used for classification in computer vision. LBP is the particular case of the Texture Spectrum model proposed i n 1990.LBPH was first described in 1994. It has since been found to be a powerful feature for texture classification; it has further been determined that when LBP is combined with the Histogram of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets.

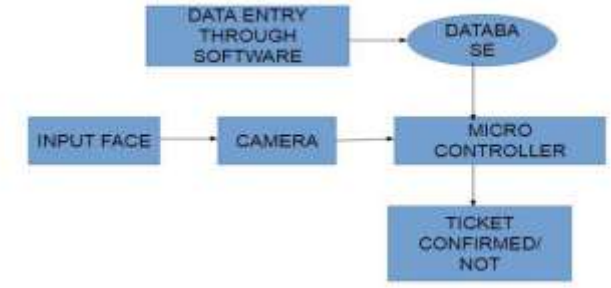

Fig 2:Block diagram of digiyathra

Now that we know a little more about face recognition and the LBPH, let's go further and see the steps of the algorithm:

2.1 Parameters

The LBPH uses 4 parameters:

- Radius: the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.
- Neighbors: the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.

- Grid X: the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

- Grid Y: The number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

2.2 Training the Algorithm

First, we need to train the algorithm. To do so, we need to use a dataset with the facial images of the people we want to recognize. We need to also set an ID (it may be a number or the name of the person) for each image, so the algorithm will use this information to recognize an input image and give you an output. Images of the same person must have the same ID. With the training set already constructed, let's see the LBPH computational steps.

2.3 Applying the LBP operation

The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window, based on the parameters radius and neighbors.

The image below shows this procedure:

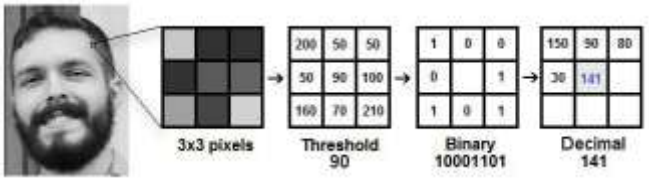

Figure 3: Applying LBP

Based on the image above, let's break it into several small steps :

Suppose we have a facial image in grayscale.

- We can get part of this image as a window of 3x3 pixels.

- It can also be represented as a 3x3 matrix containing the intensity of each pixel (0~255).

- Then, we need to take the central value of the matrix to be used as the threshold.

- This value will be used to define the new values from the 8 neighbors.

- For each neighbor of the central value (threshold), we set a new binary value. We set 1 for values equal or higher than the threshold and 0 for values lower than the threshold.

- Now, the matrix will contain only binary values (ignoring the central value). We need to concatenate each binary value from each position from the matrix line by line into a new binary value (e.g. 10001101). Then, we convert this binary value to a decimal value and set it to the central value of the matrix, which is actually a pixel from the original image. At the end of this procedure (LBP procedure), we have a new image which represents better the characteristics of the original image.

2.4 Extracting the Histograms

Now, using the image generated in the last step, we can use the Grid X and Grid Y parameters to divide the image into multiple grids, as can be seen in the following image:

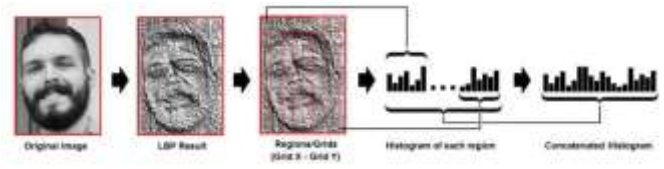

Figure 4: Extracting the histograms

Based on the image above, we can extract the histogram of each region as follows:

- As we have an image in grayscale, each histogram (from each grid) will contain only 256 positions (0~255) representing the occurrences of each pixel intensity.

- Then, we need to concatenate each histogram to create a new and bigger histogram. Supposing we have 8x8 grids, we will have 8x8x256=16.384 positions in the final histogram. The final histogram represents the characteristics of the image original image.

The LBPH algorithm is pretty much it.

2.5. Performing the face recognition

In this step, the algorithm is already trained. Each histogram created is used to represent each image from the training dataset. So, given an input image, we perform the steps again for this new image and creates a histogram which represents the image.

- So to find the image that matches the input image we just need to compare two histograms and return the image with the closest histogram.

- We can use various approaches to compare the histograms (calculate the distance between two histograms), for example: euclidean distance, chi-square, absolute value, etc. In this example, we can use the Euclidean distance (which is quite known) based on the following formula:

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

- So the algorithm output is the ID from the image with the closest histogram. The algorithm should also return the calculated distance, which can be used as a 'confidence' measurement. Note: don't be fooled about the 'confidence' name, as lower confidences are better because it means the distance between the two histograms is closer.

- We can then use a threshold and the 'confidence' to automatically estimate if the algorithm has correctly recognized the image. We can assume that the algorithm has successfully recognized if the confidence is lower than the threshold defined.

4. CIRCUIT DIAGRAM

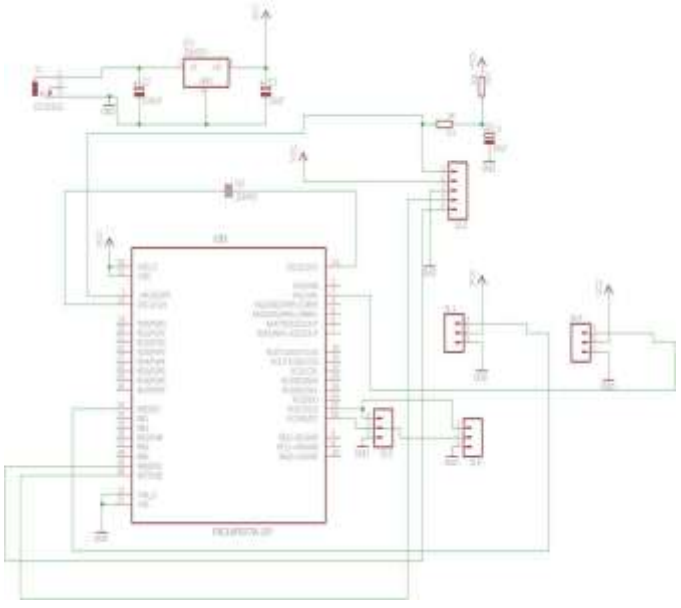

Fig 4: Circuit diagram

4.1 PIC CONTROLLER (PIC16F877A)

PIC is a family of microcontrollers made by Microchip Technology, derived from the PIC1650 originally developed by General Instrument's Microelectronics Division. The name PIC initially referred to Peripheral Interface Controller, then it was corrected as Programmable Intelligent Computer. The first parts of the family were available in 19576; by 2013 the company had shipped more than twelve billion individual parts, used in a wide variety of embedded systems.

This powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) CMOS FLASH-based 8-bit microcontroller packs Microchip's powerful PIC® architecture into an 40- or 44-pin package and is upwards compatible with the PIC16C5X, PIC12CXXX and PIC16C7X devices. The PIC16F877A features 256 bytes of EEPROM data memory, self programming, an ICD, 2 Comparators, 8 channels of 10-bit Analog-to-Digital (A/D) converter, 2 capture/compare/PWM functions, the synchronous serial port can be configured as either 3-wire Serial Peripheral Interface (SPI™) or the 2-wire Inter-Integrated Circuit (I^2C™) bus and a Universal Asynchronous Receiver Transmitter (USART). All of these features make it ideal for more advanced level A/D applications in automotive, industrial, appliances and consumer applications.

4.2 MERITS

Face recognition technology has always been a concept that lived in fictional worlds, whether it was a tool to solve a crime or open doors.Below are the major advantages.

1. **Greater Accuracy**:With today's technology, face ID technology is becoming more and more reliable. The success rate is currently at a high due to the developments of 3D facial recognition technologies and infrared cameras. The combination of these technologies make it very hard to trick the system. With such accuracy, you can have confidence that the premise is more secure and safe for you and your peers.3D mapping, deep learning and other advances make FRT more reliable and harder to trick

2. Better Security: Research shows a 1-in-50,000 chance of a phone with touch ID being unlocked with the wrong fingerprint. With 3D facial modeling, the probability drops to nearly 1-in-1,000,000.A facial biometric security system can drastically improve your security because every individual who enters your premise will be accounted for. Any trespassers will be quickly captured by the recognition system and you would be alerted promptly. With a facial recognition security system, you can potentially reduce costs of hiring a security staff.

3. **Convenient and Frictionless**: FRT is easy. It can be used passively without a user's knowledge; or actively, such as having a person "smile for the camera."

4. **Smarter Integration**: Face recognition tools are generally easy to integrate with existing security infrastructures, saving time and cost on software redevelopment.

5. **Automation**: Automated and accurate 24/7 security eliminates the need for security guards to visually monitor entry points, perform security checks and view security cameras.

5. CONCLUSIONS

Face recognition technology has come a long way in the last twenty years. Today, machines are able to automatically verify identity information for secure transactions, for surveillance and security tasks, and for access control to buildings etc. These applications usually work in controlled environments and recognition algorithms can take advantage of the environmental constraints to obtain high recognition accuracy. However, next generation face recognition systems are going to have widespread application in smart environments -- wherecomputers and machines are more like helpful assistants.

To achieve this goal computers must be able to reliably identify nearby people in a manner that fits naturally within the pattern of normal human interactions. They must not require special interactions and must conform to human intuitions about when recognition is likely. This implies that future smart environments should use the same modalities as humans, and have approximately the same limitations. These goals now appear in reach -- however, substantial research remains to be done in making person recognition technology work reliably, in widely varying conditions using information from single or multiple modalities.

This system was tested under very robust conditions in this experimental study and it is envisaged that real-world performance will be far more accurate

REFERENCES

[1] Face recognition : a literature review by Ahmed Tolba

[2] Facial recognition system: wikipedia

[3] https://www.upwork.com/hiring/for-clients/pro s-cons-facial-recognition-technology-business/

[4] https://www.google.co.in/url?sa=t&rct=j&q=&esr

c=s&source=web&cd=18&cad=rja&uact=8&ved=2

ahUKEwiH3vqb8K7iAhVCeysKHZxqCUEQFjAReg

QICBAB&url=https%3A%2F%2Fwww.techopedia

.com%2Fdefinition%2F32071%2Ffacial-recogniti on&usg=AOvVaw0LXnygcdTvC1uzGq5PvDWi