Auto switching car door-lock system based on facial recognition using MATLAB

Arvind Krishnan
arvindkrishnan785@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Rajett Rajeev Nair
rajett@rajeek@yahoo.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Danithraj N
danith97@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Jacqulin Veda Jancy. S
jac76543@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

Door-locks and its corresponding technology form an important aspect in today’s technological sphere and are essential in protecting one’s belongings. The objective of this project is to recognize and annotate the human action in an unconstrained environment, where the images contain a huge range of variability for car door lock system. A high-level security mechanism is provided by the consecutive actions such as initially system captures the human face and check whether the human face is detected properly or not. If the face is not detected properly, it warns the user to adjust his/her face properly to access the system. Still, if the face is not detected properly the system will lock the door of the car for security purpose. As soon as the door is locked, the system will automatically generate a password. After the system recognizes the face it sends a signal to the main door-lock unit which response by granting access to the individual by opening the door of the car. This high security is achieved using this car door lock system.

Keywords: Door-lock, Open CV, Face Detection.

1. INTRODUCTION

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Recently, it has also become popular as a commercial identification and marketing tool.

Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject’s face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. Popular recognition algorithms include principal component analysis using eigenfaces, linear discriminant analysis, elastic bunch graph matching using the Fisherface algorithm, the hidden Markov model, the multilinear subspace learning using tensor representation, and the neuronal motivated dynamic link matching.
A different form of taking input data for face recognition is by using thermal cameras, by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or makeup. A problem with using thermal pictures for face recognition is that the databases for face recognition are limited. Diego Socolinsky, and Andrea Selinger (2004) research the use of thermal face recognition in real life and operation sceneries, and at the same time build a new database of thermal face images. The research uses low-sensitive, low-resolution ferroelectric sensors that are capable of acquiring long wave thermal infrared (LWIR). The results show that a fusion of LWIR and regular visual cameras has the greater results in outdoor probes. Indoor results show that visual has a 97.05% accuracy, while LWIR has 93.93%, and the Fusion has 98.40%, however on the outdoor proves visual has 67.06%, LWIR 83.03%, and fusion has 89.02%. The study used 240 subjects over the period of 10 weeks to create the new database. The data was collected on sunny, rainy, and cloudy days.

In addition to being used for security systems, authorities have found a number of other applications for face recognition systems. While earlier post-9/11 deployments were well-publicized trials, more recent deployments are rarely written about due to their covert nature. At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida used Viisage face recognition software to search for potential criminals and terrorists in attendance at the event. 19 people with minor criminal records were potentially identified.

In the 2000 Mexican presidential election, the Mexican government employed face recognition software to prevent voter fraud. Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new face images to those already in the voter database, authorities were able to reduce duplicate registrations. Similar technologies are being used in the United States to prevent people from obtaining fake identification cards and driver’s licenses.

Face recognition has been leveraged as a form of biometric authentication for various computing platforms and devices; Android 4.0 “Ice Cream Sandwich” added facial recognition using a smartphone’s front camera as a means of unlocking devices, while Microsoft introduced face recognition login to its Xbox 360 video game console through its Kinect accessory, as well as Windows 10 via its “Windows Hello” platform (which requires an infrared-illuminated camera). Apple's iPhone X smartphone introduced facial recognition to the product line with its “Face ID” platform, which uses an infrared illumination system.

Face recognition systems have also been used by photo management software to identify the subjects of photographs, enabling features such as searching images by person, as well as suggesting photos to be shared with a specific contact if their presence were detected in a photo.

Among the different biometric techniques, face recognition may not be the most reliable and efficient. However, one key advantage is that it does not require the cooperation of the test subject to work. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd, without passers-by even being aware of the system. Other biometrics like fingerprints, iris scans, and speech recognition cannot perform this kind of mass identification. However, questions have been raised on the effectiveness of face recognition software in cases of racial bias. Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute in 2008, describes one obstacle related to the viewing angle of the face: “Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there’ve been problems.” Besides the pose variations, low-resolution face images are also very hard to recognize. This is one of the main obstacles to face recognition in surveillance systems.

Face recognition software generally doesn’t do as well in identifying minorities when most of the subjects used in training the technology were from the majority group, which is the case with commercial applications. One study by Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research) found that the error rate for gender recognition for women of color within three commercial facial recognition systems ranged from 23.8% to 36%, whereas for lighter-skinned men it was between 0.0 and 1.6%. Overall accuracy rates for identifying men (91.9%) were higher than for women (79.4%), and none of the systems accommodated a non-binary understanding of gender. Other factors negatively impacting the accuracy of face recognition include poor lighting, sunglasses, hats, scarves, beards, long hair, makeup or other objects partially covering the subject’s face.

Face recognition is less effective if facial expressions vary. A big smile can render the system less effective. For instance: Canada, in 2009, allowed only neutral facial expressions in passport photos.

There is also inconsistency in the datasets used by researchers. Researchers may use anywhere from several subjects to scores of subjects and a few hundred images to thousands of images. It is important for researchers to make available the datasets they used to each other, or have at least a standard dataset.
2. WORKING OF THE PROPOSED SYSTEM

The above illustration is a block diagram of the face recognition system which consists of a number of parts which have specific functions in the entire system:

**Samples:** The samples are of two types: Training samples and testing samples.

**Testing samples:** The training samples are the original samples which are fed during the time of originally configuring the face recognition system. Testing samples contain the facial features of the person under consideration.

**Action instance description:** This part of the system monitors the actions of the test subject under consideration. During this stage, most features of the face are recognized such as the contours, size, and shape of eyebrows, features of the retina and iris etc. In this, the features are analyzed at that particular instance of time. It is attached to the selection block which is powered by the AdaBoost algorithm.

**Action bags description:** This stores the features of one’s face and compares it with the training sample. It basically acts as the storage system.

**Multiple instance learning (SVM):** The multiple instance learning blocks uses the Support Vector Machine model which has a wide range of applications in machine learning. An SVM model represents examples as points of space which are grouped for the process of simplicity.

**Video action recognition and annotation:** This block is responsible for matching the sample and providing access to the system. If the training sample matches the testing sample, then the system is unlocked, otherwise, access is denied.

3. PROCESS FLOW

The above diagram represents the steps involved in recognizing the actual face of the testing samples:

**Input video:** Once the face is placed in front of the camera, the features of an individual’s face is analyzed. It is the initial step in a face recognition system.

**Converting into frames:** The entire picture is broken down into smaller segments which helps during in-depth analysis of the samples and also examines the features of one’s face.

**Background estimation:** Here, the background is examined so that no external element interferes with the operation.

**Keyframe extraction:** Histogram difference between two consecutive frames are found. If the value is greater than the threshold value, then the frames are accepted, else rejected. These frames contain key pose of the particular action.
Silhouette extraction: The part of the system which is actually needed is cropped out from the original picture.

Feature extraction: The main features such as the facial contours, eye shape, characteristics of the iris/retina are analyzed and then scanned.

Testing: The system is tested to check whether there isn’t any virus, discrepancy in the system.

Training action bags: The operations of the action instance and action bags description are performed.

Adaboost Algorithm

AdaBoost, short for Adaptive Boosting, is a machine learning meta-algorithm formulated by Yoav Freund and Robert Schapire, who won the 2003 Gödel Prize for their work. It can be used in conjunction with many other types of learning algorithms to improve performance. The output of the other learning algorithms (‘weak learners’) is combined into a weighted sum that represents the final output of the boosted classifier. AdaBoost is adaptive in the sense that subsequent weak learners are tweaked in favor of those instances misclassified by previous classifiers. AdaBoost is sensitive to noisy data and outliers. In some problems, it can be less susceptible to the overfitting problem than other learning algorithms. The individual learners can be weak, but as long as the performance of each one is slightly better than random guessing, the final model can be proven to converge to a strong learner.

Remote 16-bit I/O expander for Fm+ I2C-bus with interrupt

The PCA9675 provides general purpose remote I/O expansion for most microcontroller families via the two-line bidirectional bus (I2C-bus) and is a part of the Fast-mode Plus family. The PCA9675 is a drop in upgrade for the PCF8575 providing higher Fast-mode Plus (Fm+) I2C-bus speeds (1 MHz versus 400 kHz) so that the output can support PWM dimming of LEDs, higher I2Cbus drive (30 mA versus 3 mA) so that many more devices can be on the bus without the need for bus buffers, higher total package sink capacity (400 mA versus 100 mA) that supports having all 25 mA LEDs on at the same time and more device addresses (64 versus 8) are available to allow many more devices on the bus without address conflicts. The device consists of a 16-bit quasi-bidirectional port and an I2C-bus interface. The PCA9675 has a low current consumption and includes latched outputs with high current drive capability for directly driving LEDs. It also possesses an interrupt line (INT) which can be connected to the interrupt logic of the microcontroller. By sending an interrupt signal on this line, the remote I/O can inform the microcontroller if there is incoming data on its ports without having to communicate via the I2C-bus. The internal Power-On Reset (POR) or software reset sequence initializes the I/Os as inputs.

Features and benefits-
- 1 MHz I2C-bus interface
- Compliant with the I2C-bus Fast and Standard modes
- SDA with 30 mA sink capability for 4000 pF buses
- 2.3 V to 5.5 V operation with 5.5 V tolerant I/Os
- 16-bit remote I/O pins that default to inputs at power-up
- Latched outputs with 25 mA sink capability for directly driving LEDs
- Total package sink capability of 400 mA
- The active LOW open-drain interrupt output
- 64 programmable slave addresses using 3 address pins
- Readable device ID (manufacturer, device type, and revision)
- Low standby current

Applications-
- LED signs and displays
- Servers
- Industrial control
- PLCs
- Cellular telephones
- Gaming machines
- Instrumentation and test measurement

Infrared (IR) Sensor

An infrared sensor is an electronic device that emits in order to sense some aspects of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. These types of sensors measure only infrared radiation, rather than emitting it that is called as a passive IR sensor. Usually, in the infrared spectrum, all the objects radiate some form of thermal radiations. These types of radiations are invisible to our eyes that can be detected by an infrared sensor. The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR photodiode which is sensitive to IR light of the same wavelength as that emitted by the IR LED. When IR light falls on the photodiode, the resistances and these output voltages, change in proportion to the magnitude of the IR light received.
An infrared sensor circuit is one of the basic and popular sensor modules in an electronic device. This sensor is analogous to human’s visionary senses, which can be used to detect obstacles and it is one of the common applications in real time. This circuit comprises of the following components:

- LM358 IC
- 2 IR transmitter and receiver pair
- Resistors of the range of kilo ohms.
- Variable resistors.
- LED (Light Emitting Diode).

**Principle of Working**

The principle of an IR sensor working as an Object Detection Sensor can be explained using the following figure. An IR sensor consists of an IR LED and an IR Photodiode; together they are called as Photo – Coupler or Opto – Coupler.

When the IR transmitter emits radiation, it reaches the object and some of the radiation reflects back to the IR receiver. Based on the intensity of the reception by the IR receiver, the output of the sensor is defined.

### 4. OUTPUT

<table>
<thead>
<tr>
<th>Heuristic</th>
<th>x</th>
<th>y</th>
<th>width</th>
</tr>
</thead>
<tbody>
<tr>
<td>978</td>
<td>74</td>
<td>31</td>
<td>60</td>
</tr>
<tr>
<td>1872</td>
<td>74</td>
<td>33</td>
<td>60</td>
</tr>
<tr>
<td>1994</td>
<td>75</td>
<td>32</td>
<td>58</td>
</tr>
<tr>
<td>2125</td>
<td>76</td>
<td>32</td>
<td>56</td>
</tr>
<tr>
<td>2418</td>
<td>76</td>
<td>34</td>
<td>56</td>
</tr>
<tr>
<td>2389</td>
<td>79</td>
<td>32</td>
<td>50</td>
</tr>
<tr>
<td>2388</td>
<td>80</td>
<td>33</td>
<td>48</td>
</tr>
<tr>
<td>2622</td>
<td>81</td>
<td>33</td>
<td>46</td>
</tr>
<tr>
<td>2732</td>
<td>82</td>
<td>32</td>
<td>44</td>
</tr>
<tr>
<td>2936</td>
<td>84</td>
<td>33</td>
<td>40</td>
</tr>
</tbody>
</table>
5. APPLICATIONS

- Used in current mobile phones such as iPhone 10, Samsung galaxy s8. Used in many banks and other high-level security systems.
- Facial recognition was used during the elections in Mexico in order to prevent voter fraud i.e. preventing others from voting multiple times.
- Facial recognition is used on many social media platforms like Snapchat, Instagram.

6. CONCLUSION

Thus, we achieve high security using car door lock system using facial recognition. Finally, the project is evaluated and presented using the above parameters.

7. FUTURE SCOPE

Cars today still use the normal doorlock systems which are susceptible to theft and other fraudulent activities. Hence automobile companies could develop facial recognition based doorlock systems beyond which would result in advanced security, thus making it really hard for an intruder to break into the system and steal the car.

8. REFERENCE