IMPACT: International Journal of Research in
Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 8, Aug 2014, 53-60
© Impact Journals

DEVELOPING AUTOMATED GATE CONTROLLED SECURITY SYSTEM USING BIOMETRICS AUTHENTICATION TECHNIQUE BY CREATING REAL TIME DATABASE IN MATLAB

DESHANT[1] & RAHUL JOHARI[2]

Department of Electrical Communication Engineering, Guru Gobind Singh Indraprastha University, Dwarka, Delhi, India

ABSTRACT

In today's world of technology, security for systems/restricted places has become a challenging task. Authentication plays a major role for any security system where access can be given to only authorized persons. Authentication is the process of giving someone the identity so that he or she can access that particular application or data. It is like confirming something what it claims to be something like we are showing our ID proof to get access in the particular area restricted to particular persons only. In today's world of data/password hacking, biometric systems are emerging fastly to fulfill or to meet the requirements of securing the data or to avoid the unauthorized identities to hack/access the data/control. Objective of the authentication technique using Face detection is to provide and to ensure the full proof security of the information or the data we are sharing by the mean of processing & comparing the unique structure of the face of the person to authenticate him.

KEYWORDS: Authentication, Matrix, Biometric, MATLAB, Security System

INTRODUCTION

Authentication can be defined as of three types:

- Authentication using something we can remember like Password, PIN or any code.
- Authentication using something physical thing we can have like Swipe card, Token or any Key.
- Authentication using something we possess within us that is our Biological characteristics which is called Biometrics.

Biometric Authentication

Biometric authentication requires to compare a registered biometric sample against a newly captured biometric sample (captured during a login). This is a three-step process followed by a process. During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. Next step is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed mathematical representation. In next phase, the processed sample (mathematical representation of the biometric) is stored / registered in a storage medium for future comparison during an authentication.

A biometric system works by capturing and storing the information and then comparing the recorder/stored information with what is stored in the memory of the device.

LITERATURE REVIEW

Facial recognition software used to have to rely on a 2D image with the person almost directly facing the camera. Now, with Face It, a 3D image can be compared to a 2D image by choosing 3 specific points off of the 3D image and converting it into a 2D image using a special algorithm that can be scanned through almost all databases. Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.

Since 1993, the error rate of automatic face-recognition systems has decreased by a factor of 272. The reduction applies to systems that match people with face images captured in studio or mugshot environments. In Moore's law terms, the error rate decreased by one-half every two years.

FACE RECOGNITION

Face recognition uses camera technology to acquire images of the detailed structures of the face. Digital templates encoded from these patterns, by mathematical algorithms. These algorithms allow the identification of an individual. Databases of existing templates are searched & matched by the matcher engines at speeds measured in the millions of templates per second per CPU.

Face Detection Process

The process of capturing a face into a biometric template consists of below steps:

- Image Capture
- Image optimization
- Storing the image & than comparing.

Image Capture

The image of the face can be captured using a standard camera using both visible and infrared light and may be either a manual or automated procedure. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the face in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face and face automatically thus making this process much more user friendly.

Image Optimization

The face detection system identifies the image that has the best focus and clarity of the face. The image is then analyzed to identify the outer boundary of the face.

The face detection system then identifies the areas of the face image that are suitable for feature extraction and analysis. This involves removing areas that are covered, any deep shadows and reflective areas.

Storing the Image & than Comparing

Once the image has been captured, an algorithm is used to map segments of the face into hundreds of vectors. These algorithms also take into account the changes that can occur with a face, for example the pupil's expansion and contraction in response to light will stretch and skew the face. This information is used to produce a code which is called as the Face Code, which is a 512-byte record. This record is then stored in a database for future comparison.

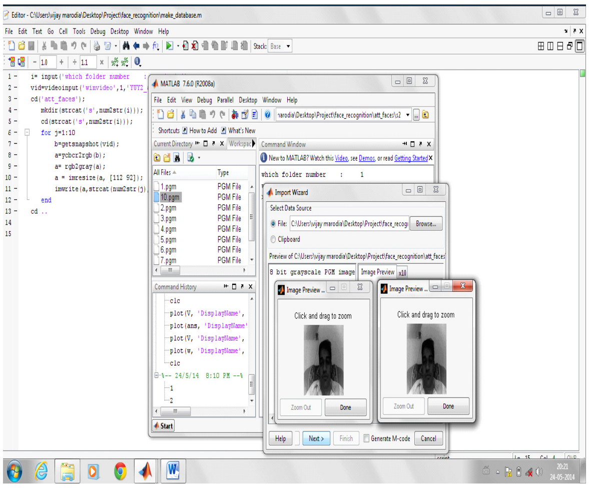
WORKING

The input is 230V AC which is step down using the transformer (12-0-12). The 12V ac input is fed to the bridge diode to gives 12V pulsating DC. This DC voltage is filtered through the capacitor to remove the ripples. The filtered DC is fed to 7805 regulator to fetch +5v regulated output. This regulated voltage is given to all the components to function properly.

SOFTWARE PART

In the software section we are using MATLAB to design the interface between the user and the computer. As shown in figure 1 first a folder is made and 10 random images is taken to be stored in data base.

Now in real world a picture is taken from the webcam and will be converted in to matrix form.



Editor - C:\Users\vijay marodia\Desktop\Project\face_recognition\make_database.m

```
i= input('which folder number    :
vid=videoinput('winvideo',1,'YUY2_
cd('att_faces');
   mkdir(strcat('s',num2str(i)));
   cd(strcat('s',num2str(i)));
   for j=1:10
       b=getsnapshot(vid);
       a=ycbcr2rgb(b);
       a= rgb2gray(a);
       a = imresize(a, [112 92]);
       imwrite(a,strcat(num2str(j),
   end
cd ..
```

MATLAB 7.6.0 (R2008a)

Command Window

```
which folder number    :    1
```

Command History

```
clc
plot(V, 'DisplayName',
plot(ans, 'DisplayName'
plot(V, 'DisplayName',
plot(w, 'DisplayName',
clc
%-- 24/5/14  8:10 PM --%
1
2
```

Import Wizard

Select Data Source

● File: C:\Users\vijay marodia\Desktop\Project\face_recogi

○ Clipboard

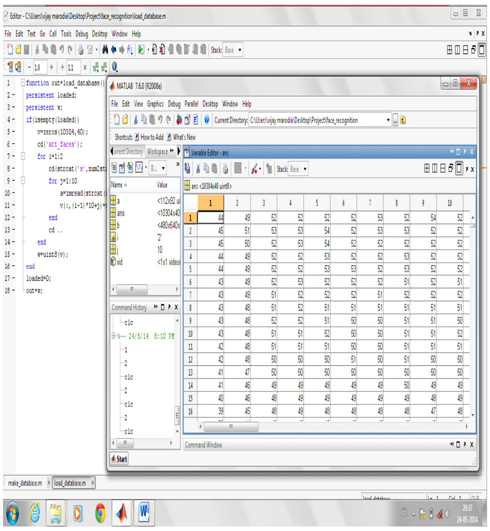
Preview of C:\Users\vijay marodia\Desktop\Project\face_recognition\att_faces

8 bit grayscale PGM image

Figure 1: Capturing a Real Time Image Using Webcam

As shown in figure, MATLAB program is written to covert the images stored in databse, into matrix form so that the eigen values and eigen vectors of the image are calculated as it is more comfortable & accurate to process the data/picture in matrix form. After converting the data in matrix form, mean of the matrix is calculated to remove useless information or we can say the "Noise". In the program, eigen values are restricted to upto 10 which is called as Dominant Eigen values composed of highly detailed information of the face. Now, a correlation technique is applied to compare the real time image with that stored in the database.

Correlation converts 2D image values into 1D image values so that comparison becomes bit easier. If the values match with the values stored in the database then the access to that person is given.



Editor - C:\Users\vijay marodia\Desktop\Project\face_recognition\load_database.m

```
function out=load_database()
persistent loaded;
persistent w;
if(isempty(loaded))
    v=zeros(10304,40);
    cd('att_faces');
    for i=1:2
        cd(strcat('s',num2st
        for j=1:10
            a=imread(strcat(
            v(:,(i-1)*10+j)=
        end
        cd ..
    end
    w=uint8(v);
end
loaded=0;
out=w;
```

Current Directory: C:\Users\vijay marodia\Desktop\Project\face_recognition

Variable Editor - ans

ans <10304x40 uint8>

	1	2	3	4	5	6	7	8	9	10
1	44	49	52	52	52	52	53	52	54	52
2	45	51	53	53	54	52	53	53	52	52
3	45	50	52	53	54	52	52	52	52	52
4	44	49	52	52	53	52	52	53	52	52
5	44	49	52	52	53	53	52	53	52	52
6	43	49	52	53	52	52	52	51	52	51
7	43	49	51	52	52	52	51	52	52	52
8	43	48	51	52	51	51	51	51	51	51
9	43	48	52	52	51	50	50	51	51	50
10	43	48	51	51	52	50	50	51	51	52
11	42	48	51	51	51	50	50	51	51	51
12	42	48	50	50	50	51	50	51	50	50
13	41	47	50	50	50	50	50	50	50	50
14	41	46	49	49	49	49	49	50	49	49
15	40	46	48	49	49	49	49	49	48	49
16	39	45	48	49	48	48	48	48	47	48

Figure 2: Creating Matrix of the Image Data

HARDWARE PART

In the Hardware part, from computer we send the data at the COM port of the computer that is basically a communication port through which hardware part will communicate/access the software to run the system. The serial data port of computer is USB based. The UART MODULE converts this standard into the TTL standard of the microcontroller. The microcontroller reads the data from the computer turns on door accordingly. To open the door and close it, we are using MATLAB for face recognition (0-1) and generate the serial event on matching of face.

Microcontroller Used AT89S8253

Features

- 8K Bytes of In-System Reprogrammable Flash Memory
- Endurance: 1,000 Write/Erase Cycles
- Fully Static Operation: 0 Hz to 33 MHz
- Three-level Program Memory Lock
- 256 x 8-bit Internal RAM
- 32 Programmable digital I/O Lines
- Three 16-bit Timer/Counters

The AT89s8253 is a low power, high performance CMOS 8-bit micro computer with 8K bytes of flash programmable and erasable read only memory(PEROM).The device is manufactured using Atmel’s high density nonvolatile memory technology and is compatible with the industry standard 80c51 and 80C52 instruction set and pin out. Atmel AT89s8253 is a powerful microcomputer which provides a highly flexible and cost effective solution to many embedded control applications.

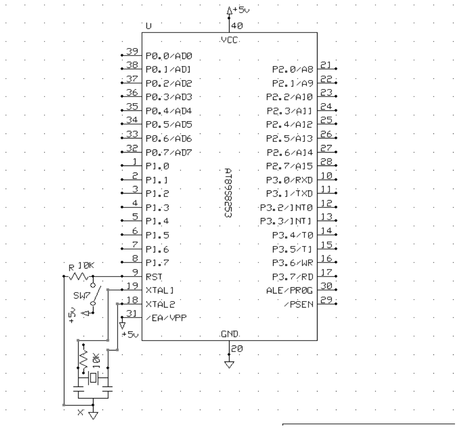


Figure 3

PCB Layout

A PCB layout is required to place components on the PCB so that the component area can be minimized and the components can be placed in an efficient manner. The components can be placed in two ways, either manually or by software. The manual procedure is quiet cumbersome and is very inefficient. The other method is by the use of computer software. This method is advantageous as it saves time and valuable copper area.

Many of them are loaded with auto routing and auto placement facility. The software that we have used here is EXPRESS PCB**.** This software has a good interface, easy editing options and a wide range of components.

USB TO UART MODULE

USB to RS232 TTL Module contains a CP2102 single-chip USB to UART bridge which converts data traffic between USB and UART formats. The chip includes a complete USB 2.0 full-speed function controller; bridge control logic and a UART interface with transmit/receive buffers and modem handshake signals. The Module interfaces to microcontrollers through a 6 Pin 2.54mm single row pin header interface can easily be connected to any microcontroller or FPGA and DSPs.

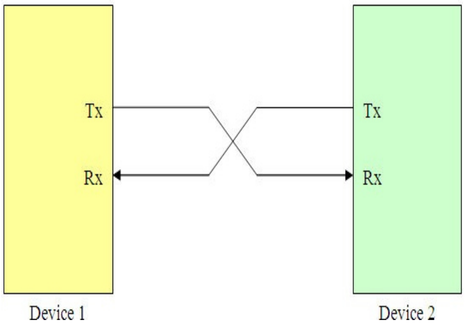


Figure 4

ADVANTAGES OF FACE DETECTION TECHNOLOGY

- The physiological properties of faces are major advantages to use them as a method of authentication.
- Uniqueness of the face patterns.
- One key advantage is that it does not require the cooperation of the test subject to work.
- It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless the user actually engages it.
- The accurateness of the scanning technology is a major benefit with low error rates, hence resulting in a highly reliable system for authentication.
- Scalability and speed of the technology are a major advantage.
- The technology is designed to be used with large-scale applications such as with ATMs.
- Ability of the system to scan and compare the face within a matter of minutes is a major benefit.

DISADVANTAGES OF FACE DETECTION TECHNOLOGY

As with any technology, there are challenges with face detection as well.

- Face recognition is not perfect and struggles to perform under certain conditions.
- Conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject’s face, and low resolution images.
- The camera used in the process needs to have the correct amount of illumination. Without this, it is very difficult to capture an accurate image of the face.
- Along with illumination, problem with reflective surfaces, within the range of the camera & unusual lighting may occur.
- Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective.
- Normal day-to-day problems such as system failures, power failures, network problems, and software problems can contribute to rendering a biometric system unusable.

CONCLUSIONS

Biometric technology is increasingly being used in various applications specially for the smooth flow of cross-border traffic, for authentication of criminal identities and controlled access to military facilities. In addition, more and more consumer market players are using biometrics for effective identification. This includes airlines, gyms and self-service convenience stores aiming to increase their efficiency, as well as pharmacies using it to secure their medicine stocks.

Face detection came into existence due to uniqueness of the face structure as even genetically identical individuals have completely independent face textures.

- High speed of matching with existing templates.
- Extreme resistance to False Matches
- Increased security.
- Eliminate problems caused by lost IDs or forgotten passwords
- Replace hard-to-remember passwords which may be shared/disclosed.

REFERENCES

1. Poulami Das, Debnath Bhattacharya, Samir Kumar Bandyopadhyay, Tai-hoon Kim “Person identification through Face detection”, International Journal of security & its applications (vol. 3, No. 1), January 2009, pg. 129-147.
2. Michael Negin, Thomas A.Chmielewski, Jr. Marcos Salganicoff, Theodore A. Camus, Ulf M. Cahn von Seelen, Peter L. Venetianer, Guanghua G. Zhang “ An Face Biometric System for Public and Personal Use”, 2000 IEEE, pg. 70-75.
3. Harley Geiger, "Facial Recognition and Privacy". Center for Democracy & Technology. Retrieved 2012-01-10.
4. Jon Krueger, Marshall Robinson, Doug Kochelek, Mathew Escarra, “Obtaining The Eigenface Basis” version 1.3: Dec 17, 2004.
5. Jonathon Shlens, “A Tutorial on Principal Component Analysis”, Syaytems Neurobiology Laboratory, version 2, 2005. Books
6. Cryptography and Network Security by Behrouz A. Forouzan, Debdeep Mukhopadhyay.
7. Data Communication and Networking by Behrouz A. Forouzan.