International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 150 – 153

DIP Based Smart Door Lock System

Ms. Uzma Fatima Shaikh, Ms. Usha Shinde
AISSMS Institute of Information Technology, Pune, Maharashtra
uzma.fatimah.shaikh@gmail.com
usshinde2014@gmail.com

Prof. M. P. Sardey
Head of Department
AISSMS IOIT, Pune, Maharashtra
sardeymp@yahoo.com

***Abstract*—** In this era of digital development, the requirement of efficient security parameters to safeguard privacy becomes a necessity. In this paper, an effective implementation of security is used by the means of face recognition technology and the widely used One Time Password (OTP) generated with Group Special Mobile (GSM). These technologies when used together help to protect privacy. Conventionally, the modes of security to safeguard privacy are key locks and chains. But these can be sabotaged and the desired area can be open to unauthorized members. With this system, the need for keys can be completely eliminated. This paper provides a cognitive framework to serve the purpose of security with easy utility and cost effectiveness. In order to gain access to a secured area, face recognition technique is used with the help of digital image processing to recognize and allow only authorized users, while the OTP is generated for unauthorized members who can enter this area only if they have been allowed by authorized users to do so by giving them the OTP.

Keywords – *digital image processing, security, One Time Password, GSM SIM800A, solenoid linear actuator, MATLAB, AVR ATMEGA16.*

*****

I. INTRODUCTION

Private areas should be equipped with very strong security system these days, because not doing so, poses a great threat to the safety as well as privacy of the place. The proposed system is divided into two parts:

1. Face Recognition
2. One Time Password generated by GSM

A camera is fixed at the door which captures images of the person outside the door. These images are then matched with those in the database using MATLAB. If there is a match, the door opens. If not, an OTP is sent to the authorized user. After three wrong attempts of entering the password, the alarm starts to ring. The innovative idea is to use these two technologies in one system along with the use of electromagnetic door lock instead of using a motor to open the door.

Human eye can recognize any pattern in a fraction of seconds. Recently, the computers too, have been inculcated with smarter recognition techniques in order to recognize different patterns. Facial recognition came into consideration in late 1960s in order to increase security by having a database. Facial recognition basically recognizes a face and measures the different features that are present of the face. Every human face is different from the other in terms of features. These features can be the arches and valleys in a face which also includes the contour of the face. These are called nodal points. Human faces have about 86 nodal points which can be recognized by a computer. These include various features of a face such as:

- Shape of the jaw line
- Breadth of the nose
- Deepness of eye sockets
- Shape of cheekbones
- Space between the eyes

These nodal points are then converted into a face print by numerical computation to be read by the computer.

Many algorithms have been defined for different recognition processes in computers. One such algorithm for face recognition is Principle Component Analysis (PCA). It is highly efficient and flexible and hence widely used.

PCA is a statistical approach which reduces the number of variables in face recognition. It extracts the most relevant information from the face in the image. In the training set of an image, every information can be obtained in the form of a matrix of weighted eigenvectors which are called eigen faces. This matrix is called covariance matrix and the eigenvectors are its elements. The most relevant eigen faces are used to find out the weights.

A subspace spanned by the eigen faces is then overlapped with a test image for recognition process. After which the classification comes into play. It is effectuated by different measuring methods such as the Euclidean distance.

A 2-D image can be converted to a 1-D vector. Suppose a vector N of size M represents a set of sampled images and p_i represents the value of the pixels,

$$\boldsymbol{w_i = (p_1 + p_M)^T, i = 1.,.,,\ldots,N}$$

Mean centered image is found by subtracting mean image from each image vector. Let n be the mean image.

$$\mathbf{n} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \mathbf{w_i}$$

Then y_i will be the mean centered image,

$$\boldsymbol{y_i = w_i - n}$$

A set e_i should be so chosen that it has maximum projection on each y_i

To find a set of N orthonormal vectors, for which the equation

$$\boldsymbol{\lambda_i = \frac{1}{N}\sum_{m=1}^{N}(e_i^T y_m)^2}$$

should be increased with

$$\boldsymbol{e_1^T e_k = \delta_{lk}}$$

λi and e_i are given by eigen value and eigen vectors of covariance matrix C.

$$\boldsymbol{C = AA^T}$$

Here, A is column matrix of column vectors y_i which are adjacent.

The known faces are transformed into face space. The projection of an image of face is computed onto N

$$\boldsymbol{\Omega = [v_1 v_2 \ldots v_{M'}]^T}$$

Where, $\boldsymbol{v_i = e_i^T y_i}$

Therefore, v_i is the i^{th} co-ordinate of the image in face space. v_i becomes the principle component. Also, e_i is the eigenface. Ω is the set of these eigenfaces.

For face recognition, i.e., to know which face class best fits the given image, a face class, say k, should be so chosen that it should decrease the Euclidean distance

$$\boldsymbol{\epsilon_k = \|\Omega - \Omega_k\|}$$

Ω is the vector wherein k is the face class.

When ϵ_k is less than a preset value, the face image is said to belong to face class k. This is how a face is recognized using PCA.

One Time Password is a password applicable for one time use only, hence called One Time Password.

OTP is a string of characters that are randomly selected. The length of the string can be up to 7 characters long. In this paper, 4 characters are used.

The randomness guarantees security, as it is very difficult to make different combinations and crack down the password.
OTPs are safe from replay attacks. If an intruder was able to save a previously generated OTP, he cannot reuse it as it will not be valid.

The algorithms used for the generation of the OTPs use pseudo randomness and hash functions.

These algorithms can be based on:

1. Time-synchronization
2. Previous passwords generated
3. A mathematical challenge

OTPs can be delivered by multiple means such as text message, tokens or even mobile phones.

II. OBJECTIVE OF SYSTEM

- To design a program for image processing in MATLAB using a camera. If the person is recognized and matches images in database, the door will open, if not, an SMS along with an OTP will be sent to the authorized user.
- To apply GSM system which will notify the authorized user through SMS if some unauthorized person tries to gain access to the locked area.
- An OTP will be generated which will be sent through SMS.
- To design a door lock system that uses electromagnetic lock that opens when it receives confirmation.
- If the authorized person knows this person, he can forward this OTP to the user which the user has to put in using the keypad.

III. PROPOSED SYSTEM

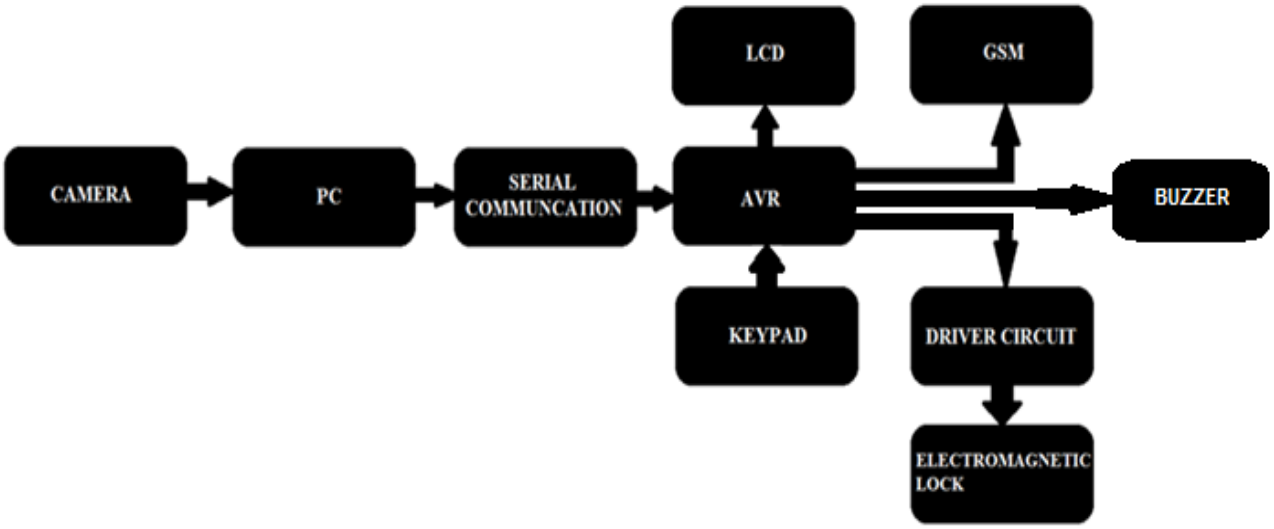
The main components used in this system are

1. Microcontroller – AVR Atmega16
2. Computer
3. Camera- Webcam
4. GSM- SIM800A
5. KEYPAD
6. LCD interface
7. Serial interface
8. Relay – HE JQC3FC
9. Electromagnetic lock- linear solenoid actuator

The Microcontroller AVR Atmega16 controls all the functions.
The computer processes the messages from the microcontroller.

The microcontroller and computer have serial interface between them to communicate with each other.
The relay drives the electromagnetic lock, which is a linear solenoid actuator

 ISSN: 2321-8169
150 – 153



BLOCK DIAGRAM

IV. WORKING AND EXPLANATION

1. MICROCONTROLLER AVR ATMEGA16:

Program memory type of ATMEGA16 is flash with program memory of high speed 16 kb. CPU speed in 16 MIPS. There is only 1 ram byte. There are 512 bytes of data eeprom. Digital communication peripherals include 1-uart, 1-spi, 1-i2c. Capture/compare/pwm peripherals include 1 input capture, 1 ccp, 4pwm. Operating voltage range is 2.7 to 5.5 volts. It has 44 pins.

2. CAMERA:

The camera is used to capture the image of the person standing outside the door. The image is then sent to the PC for database matching.

3. COMPUTER:

Computer is required for total processing of image and face recognition. The program is fed into the system through MATLAB. This programming is done in the computer.

4. SERIAL INTERFACE:

RS232 has been used for serial interface. It provides effective data transmission with less cables and is inexpensive. RS232 provides three links:

i. Link 1 for transmits.
ii. Link 2 for receives.
iii. A common ground.

5. KEYPAD 4X4:

The OTP is fed using the keypad. At most three attempts are allowed to feed the password. After third attempt, the alarm buzzer will be activated.

6. LCD 16X2:

The LCD screen displays whether the person is recognized or not. If not, then it asks for the OTP. This OTP is then shown on display when typed.

7. GSM SIM800A:

It is a dual-band 900/1800MHz GSM. It can be controlled AT commands. The advantage of using SIM800A is that it has low power consumption. It has very good network reception. It is used to send the OTP to the authorized user.

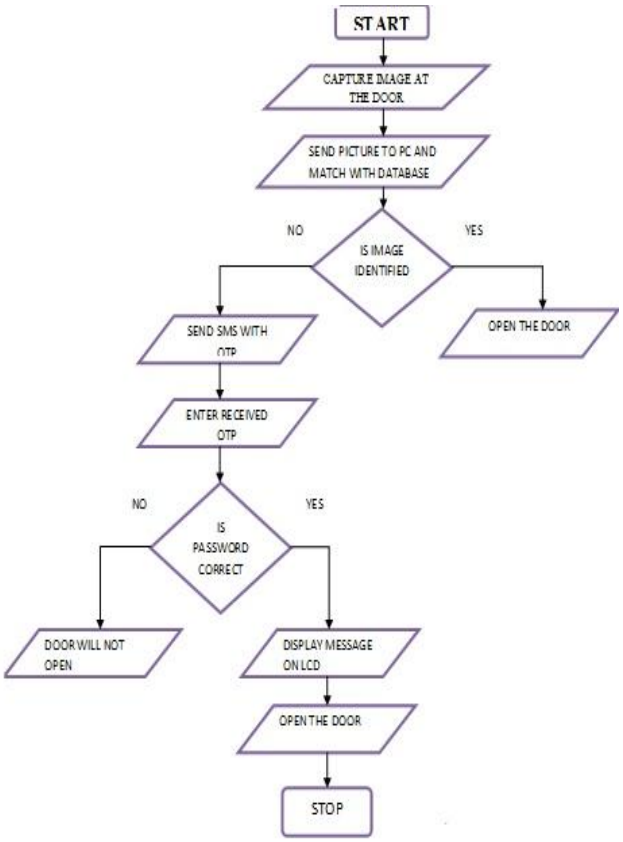
8. ELECTROMAGNETIC LOCK:

The linear solenoid actuator is used to keep the door locked. It converts electrical energy into a mechanical pushing or pulling motion. Generally, in automatic door lock systems, motors are used to open the door. But electromagnetic locks are better option as they require less power and can be battery operated.

9. BUZZER- PIEZO INDICATOR:

The buzzer is used as an alarm to alert the people around in case of unauthorized use. This will protect the secured area from theft as well.

V. FLOWCHART



VI. FUTURE SCOPE

- This system can use advanced communication systems such as WI-FI
- Biometric recognition systems like iris scanner can be added
- This system can be superiorly advanced by the use of a DSP processor
- Internet of Things (IoT) can be implemented for better access

VII. EXPECTED RESULTS

- This system aims at allowing the rightful user to deploy platform to any property that requires protection.
- It must protect the privacy of a secured area; hence it must not allow entry of unauthorized persons.
- Also there must be successful recognition of authenticated members.
- In case of unauthorized use, an OTP must be generated and sent via the GSM.
- Activation of alarm if the password is wrong up to three attempts.

VIII. CONCLUSIONS

This paper proposes an electronic system that takes into account security parameters by means of face recognition and OTP, hence making it highly effective for any secured area as compared to the conventional key and lock systems. This system, however, can be improved and made more reliable by future technologies.

IX. REFERENCES

[1] P. Vigneswari, V. Indhu, R. R. Narmatha, A. Sathinisha, J. M. Subashini, “Automated security system using surveillance” International journal of current engineering and technology,vol.5,no.2, pp. 882-884, April 2015.
[2] G. Sushma, M. Joseph, A. R. Tabitha, M. B. Yokesh, ”Image tracking based home security using arduino microcontroller” Internal journal of innovative research on computer and communication Engineering, vol.3, no.8, pp. 117-122, October 2015.
[3] Pratiksha Misal, Madhura Karule, Dhanshree Birdwade, Anjali Deshmukh, Mrunal Pathak, “Door locking/unlocking sytem using SMS technology with GSM or GPRS service.” International Journal of Electronics Communication and Computer Engineering. 2014
[4] Bhalekar Pandurang, Garge Rahul, “Smart lock: unlocking system using Bluetooth technology and camera verification.”
[5] Jolliffe, I.T. (2002). Principal Component Analysis, second edition (Springer).

DATASHEETS:

[6] Microchip Datasheet for ATMEGA16
[7] Maxim Integrated Products data sheet for multichannel RS232 drivers
[8] Simcom documents for GSM SIM800
[9] MikreElektrenika keypad 4x4 product sheet.

WEBSITES:

[10] https://www.engineersgarage.com
[11] http://www.electronics-tutorials.ws
[12] www.wikipwedia.com