

VISVESWARAYA TECHNOLOGICAL UNIVERSITY
“Jnana Sangama”, Belgaum-590 018



PROJECT REPORT ON

“ONLINE DIGITAL VOTING POLL”

*Submitted in partial fulfillment of the requirement for the 8th Semester
Bachelor of Engineering in Computer Science and Engineering.*

Submitted by

MANOJ R [1CC18CS026]

NIKITA [1CC20CS009]

PRAMOD J [1CC20CS012]

SHAKUNTALA [1CC20CS015]

Under the Guidance of

Mrs. Sheela C R, BE., M.E.,

Assistant Professor

Dept. of CSE

Dr. SMCE, Bangalore.



Department of Computer Science and Engineering
Dr. SRI. SRI. SRI. SHIVAKUMARA MAHASWAMY
COLLEGE OF ENGINEERING

Byranayakanahalli, Nelamangala Taluk, Bangalore Rural Dist.-562132

2023-2024



**Dr. Sri. Sri. Sri. Shivakumara Mahaswamy
College of Engineering**

(Affiliated to VTU, Belagum & Approved by AICTE, New Delhi)

Fax: 080 - 2773 9250 Ph: 080 - 2770 1250 / 2773 9251/ 52/ 53/ 54 E-mail:principaldrsmce@gmail.com



CERTIFICATE

This is to certify that the Project entitled “**ONLINE DIGITAL VOTING POLL**” was carried out by **MANOJ R (1CC18CS026), NIKITA (1CC20CS009), PRAMOD J (1CC20CS012), SHAKUNTALA (1CC20CS009)** is a bonafide student of **Dr. Sri. Sri. Sri. Shivakumara Mahaswamy College of Engineering, Bangalore** in partial fulfillment for the award of degree of **Bachelor of Engineering in Computer Science & Engineering** of **Visveswaraya Technological University, Belgaum**, during the academic year 2023-2024.

Signature of the Guide

Mrs. Sheela C R, BE., M.E.,
Assistant Professor
Dept. of CSE
Dr. SMCE, Bangalore.

Signature of the HOD

Prof. Renukaradhya P C, BE., M.Tech., (Ph.D)
Head of Department
Dept. of CSE,
Dr. SMCE, Bangalore.

Signature of the Principal

Dr. H.D Ramesh B.E., M.E., Ph.D., MISTE
Dr. SMCE, Bangalore.

External Viva

Examiners

1. _____

2. _____

Name with Signature

DECLARATION

We are **MANOJ R (1CC18CS026)**, **NIKITA (1CC20CS009)**, **PRAMOD J (1CC20CS012)**, **SHAKUNTALA (1CC20CS015)**, the student of 8th semester Bachelor of Engineering in Computer science and Engineering, Dr. Sri. Sri. Sri. Shivakumara Mahaswamy College of Engineering.

We are here by declare that the Project Report work has been carried out by under the guidance of **Asst. Prof. Sheela C R**, Dept. of Computer science and Engineering.

The Project Report submitted to **Visvesvaraya Technological University, Belgaum**, in the partial fulfillment of the requirement of the award of the degree of Bachelor of Engineering in Computer Science and Engineering during the academic year 2023-24.

Place: Bangalore

Date:

MANOJ R (1CC18CS026)

NIKITA (1CC20CS009)

PRAMOD J (1CC20CS012)

SHAKUNTALA (1CC20CS015)

ACKNOWLEDGEMENT

While presenting this Project Report. We feel that it is our duty to acknowledge the help rendered to us by various personalities.

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible and whose constant encouragement and guidance crowned our efforts with success.

We consider ourselves proud, to be part of **Dr. Sri. Sri. Sri. Shivakumara Mahaswamy College of Engineering** family, the institution which stood by our way in endeavours.

We have a great pleasure in expressing our deep sense of gratitude to our honorable Founder chairman **Sri Chennigappa** and Chairman **Sri D.C Venugopal** for providing us a good infrastructure and facility to carry out our Project work.

We express our deep and sincere thanks to our principal **Dr. H.D. Ramesh** for encouraging, inspiring and providing moral support to me.

We like to express our thanks to **Prof. Renukaradhya P C**, HOD of CSE for having extended cooperation and help during the Project work.

We wish to thank our internal guide **Asst. Prof. Sheela C R**, Dept. of CSE for guiding and correcting various documents of ours with attention and care. She has taken the lot of pain to go through documents and make necessary corrections as and when needed.

We would like the faculty member and supporting staff of the Department of CSE, Dr. Sri. Sri. Sri. Shivakumara Mahaswamy College of Engineering for providing all the support for completing the Project work.

Finally, We are grateful to our parents and friends for their unconditional support and help during the course of our Project work.

MANOJ R (1CC18CS026)
NIKITA (1CC20CS009)
PRAMOD J (1CC20CS012)
SHAKUNTALA (1CC20CS015)

ABSTRACT

Highly advanced security methods are necessary to introduce effective online voting system in the whole world. The aspect of security and transparency is a threat from global election with the conventional system.

Fundamental right to vote or simply voting in elections forms the basis of democracy. The conduct of periodic, competitive, participatory, credible and non-violent elections is one of the main yardsticks used to determine the democratic condition of a state.

In Nigeria, elections have been conducted using the manual system of voting ever since we started practicing democracy in 1999, but these elections using the manual means have been marred with a lot of electoral malpractices and hitches.

General elections still use a centralized system where one organization that manages it. Some of the problems that can occur in traditional electoral systems are with an organization that has full control over the database and system, it is possible to manipulate with the database. This paper presents a survey on some previous voting system that is used by different countries and organizations.

These includes violent attack on the voters, result manipulations, vote buying, remoteness of polling centers etc. These are enough reasons that necessitates the design and construction of an electronic voting system, that goes a long way in addressing most of these problems.

Table of Contents

SL no.	Contents	Page no.
CHAPTER 1	Introduction -----	1
CHAPTER 2	Literature Survey -----	4
	2.1 Balloting System -----	4
	2.2 Marking System -----	5
	2.3 Existing System -----	6
	2.4 Proposed System-----	8
CHAPTER 3	System Requirements-----	11
	3.1 Hardware Requirements-----	11
	3.2 Software Requirements-----	11
	3.3 Functional Requirements-----	11
CHAPTER 4	System Design-----	12
	4.1 Methodology -----	13
	4.2 RFID -----	15
	4.3 RFID Concepts-----	16
	4.4 The four components of RFID system-----	17
	4.5 RFID Tags -----	18
	4.5.1 RFID Interrogators (Reader) -----	19
	4.5.2 Specification -----	20
	4.5.3 Components of RFID system -----	21
	4.6 ARM (ARM LPC 2418) -----	24
	4.6.1 General Description -----	25
	4.6.2 Pin Diagram-----	26
	4.7 Functional Description -----	28
	4.7.1 Functional Overview -----	28
	4.7.2 On-chip Flash Memory -----	29
	4.7.3 On-Chip Static RAM -----	29
	4.7.4 Interrupt Controller-----	30
	4.8 Pin Control Block -----	31
	4.9 Fast General Purpose Parallel I/O (GPIO) -----	32

CHAPTER 5	Fingerprint Recognition-----	38
	5.1 Fingerprint Reader -----	38
	5.1.1 Specification of Finger Print reader -----	39
	5.2 Operation Principle of Fingerprint Reader-----	40
	5.3 Power Supply -----	41
	5.4 Circuit Description -----	42
	5.5 Buffer and Driver -----	44
	5.5.1 Pin Description -----	44
	5.5.2 Features of IC ULN in 2004-----	45
	5.5.3 ULN 2004 -----	46
	5.6 Principle Component Analysis for Face recognition -----	47
	5.7 Web Page Developing -----	50
	5.7.1 Html (Hypertext Markup Language) -----	51
	5.7.2 JavaScript -----	52
	5.7.3 Java Technology -----	53
CHAPTER 6	Implementation-----	64
	6.1 RFID Module -----	64
	6.2 Face Recognition Module -----	66
	6.3 Voting Module -----	70
CHAPTER 7	Testing and Results-----	72
	7.1 Unit Testing -----	72
	7.2 Functional Testing -----	74
	Advantages and Applications-----	75
	Conclusion-----	76
	Future Enhancement-----	77
	Reference-----	78

LIST OF FIGURES

Sl.no.	Figures	Page no.
CHAPTER 1	Fig.1.1. RFID Card -----	2
	Fig. 1.2. Face Recognition using PCA algorithm -----	3
CHAPTER 2	Fig.2.1. Representing Balloting system-----	4
	Fig.2.2. Represents Marked Voting System-----	5
	Fig.2.3. Existing electronic voting machine-----	7
CHAPTER3	Fig.3.1. System Design -----	12
	Fig.3.2. Basic Building blocks of an RFID system -----	18
	Fig.3.3. RFID Tag -----	18
	Fig.3.4. RFID Tag Components-----	18
	Fig.3.5. Pin Diagram-----	26
CHAPTER5	Fig.5.1. Fingerprint Reader -----	38
	Fig.5.2. Voltage Regulator IC KIA 78xx -----	41
	Fig.5.3. Circuit Diagram of +5V & +12V Regulated Power Supply -----	41
	Fig.5.4. Pin Description of Buffer IC 4050 -----	44
	Fig.5.5. Basic Darlington Pair Circuit-----	44
	Fig.5.6. Pin Description of IC ULN 2004 -----	46
	Fig.5.7. Structure of Face Recognition System-----	49
	Fig.5.8. Representing How the face is matched with data-----	50
	Fig.5.9. Representation of Servlet-----	55
	Fig.5.10. Developing Application using JSP model -----	57
CHAPTER6	Fig.5.11. Capturing and cropping of Face-----	66
	Fig.5.12. Training the PCA Algorithm -----	67
	Fig.5.13. Face authentication using PCA algorithm -----	67
	Fig.6.4. Login page for booth level officer-----	70
	Fig.6.5. Voter's voting page -----	71
	Fig.6.6. Representing status of voter after voting and if tries to revote-----	71

CHAPTER 1

INTRODUCTION

India is a Democratic country every citizen above 18 years of age is eligible to elect their leaders. When a person attains the age of 18 has the constitutional right to voluntarily enroll for voter id given by the Indian Election Commission (IEC). Voter ID is only used for electing purpose once in 5 years or on occurrence and voter card will not provide any government facility like Aadhaar, Citizens miss out to enroll for Voter card and even after getting the Voter card during the election time the voter may miss out the voting due to voter may neglect voting because voter is living in some other region which is far from his resident and voter is not ready to travel such a distance. To avail constitutional voting right to every citizen, Aadhaar and Web based Voting System using Face Recognition, Fingerprint Technique is the best solution.

Nowadays with the rise in population the need for checking the validity of the voters has become a problem. As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. In the past, usually, information security was used mostly in military and government institutions. But, now need for this type of security is growing in everyday usage. In computing, e-services and information security it is necessary to ensure that data, communications or documents (electronic or physical) are enough secure and privacy enabled. Advances in cryptographic techniques allow pretty good privacy one voting systems. Security is a heart of e-voting process. Therefore, the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters.

This project provides the security by means of RFID, Face recognition and respective booth level officer login which is stored already in the data base. Radio frequency identification (RFID) technology is a wireless communication technology that enables users to uniquely identify tagged objects or people.

When the RFID card shown in Fig.1.1 is swiped on RFID reader [3], the RFID reader reads and sends the unique character from RFID card to ARM [4] shown in Fig.1.2.

The ARM waits to receive a character from MatLab. After RFID authentication the MatLab recognizes the face here the Face Authentication is done by using the principle Component Analysis [5] and searches for the match in stored database. Once it finds the match as shown in Fig.1.3 MatLab sends the respective character of matched face to ARM. It receives the character from MatLab and try to match with the character received from RFID reader.

If both character matched the ARM sends the respective character to the cloud to unlock vote button for voter. Once the admin login is done the respective voter's constitution will be displayed. If the character sent by the RFID reader and the MatLab is unmatched then the ARM will not send any character still if the admin gives a login, the web page will display an error message. In a particular nation or organization, it is very important to elect a person who is efficient to lead that particular organization or nation. So, here there is a need for election to elect the person from group of people. In old voting machines there are chances of rigging. So to overcome this problem here we are using an Aadhaar and Web based voting system by using which there is less chance for rigging.

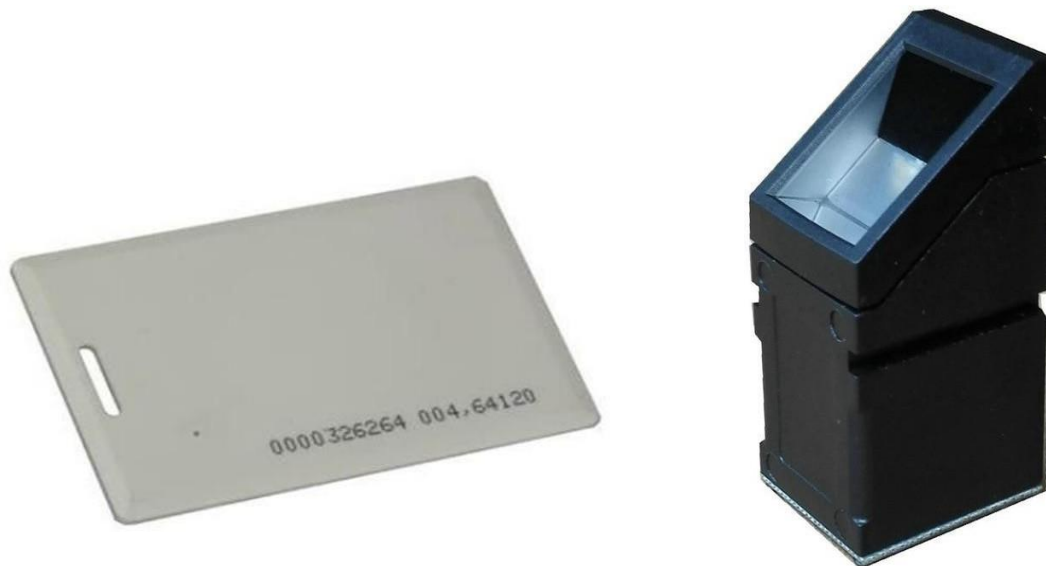


Fig.1.1. RFID Card

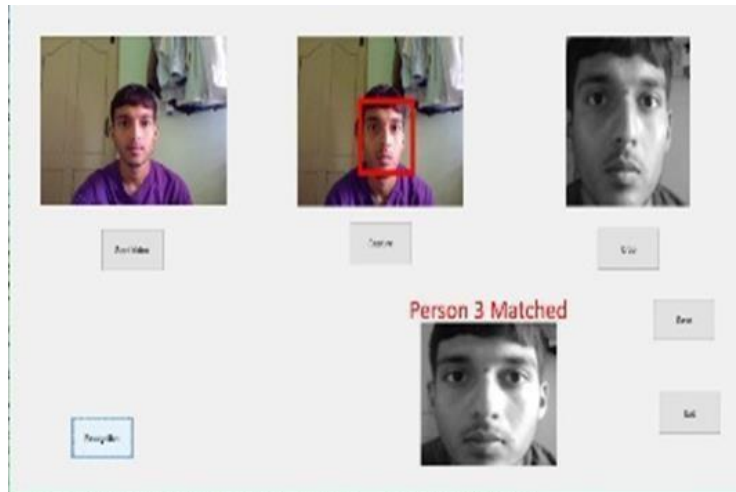


Fig. 1.2. Face Recognition using PCA algorithm

In “Aadhaar and Web based Voting System using Fingerprint and Face Recognition” if a person tries to vote once again using same RFID card the web page will display as your vote casted successfully until the Election Commission officer resets it. If the person enters to vote with some other person’s RFID card during Face Recognition the character generated will be sent to ARM. The ARM compares the character sent by RFID reader and MatLab if both are different then the ARM won’t send the respective character to the Server and the server won’t provide permission to next page to vote.

CHAPTER 2

LITERATURE SURVEY

India is one of the world's largest democracies with a community of 1.1 billion; India has an electorate of 714 million persons over 828 thousand polling stations, 1.37 million voting machines and 5.5 million polling officials cover 543 parliamentary constituencies. Past experience of electoral process enforced us to focus on the use of latest technology in E-voting process. The current voting mechanism has many security problems, and it is very difficult to prove even simple security aspects about them. A voting system that can be demonstrated correct has many considerations.

2.1 Balloting System

For the first and second General Election in 1951-52 and 1957, the Election Commission adopted the 'Balloting System' of voting.

Working: Every candidate was allotted a separate ballot box at each polling station in a screened compartment and voter was required only to drop his ballot paper, the centrally pre-printed ballot paper into the ballot box the candidate of his choice. For results, all votes were counted and maximum vote gainer was declared as winner.



Fig.2.1. Representing Balloting system

Disadvantage:

- Manual elections are very expensive and time consuming.
- A nationwide ballot consumed thousands of tons of stationary paper including about 4 lacs phials of indelible ink and required about 3 million strongboxes to store them under heavy security until the votes were counted.
- Balloting system takes up to three – four days to count the votes, with hired personnel spending day and night in secured areas manually counting each ballot.
- Sometimes demanding for repeat the counting resulting for the minimum margin difference of the votes between the top two candidates coupled with large number of invalid and uncertain votes.

2.2 Marking System

From the 3rd General Election in 1962 onwards, the commission switched over to 'Marking system' of voting.

Working: Under this system, a common ballot paper containing the names and election symbols of all contesting candidates is printed on the voter has to put a mark with an arrow cross mark rubber stamp on or near the symbol of the candidate of this choice, All the marked ballot papers are put into a common ballot box.



Fig.2.2. Represents Marked Voting System

Disadvantage:

- There is no scope for automation in paper ballot system.
- The people who are physically challenged find it difficult to cast their votes through the paper ballot and even if they cast their votes using paper ballot they require someone to cast their vote on behalf.
- Greatest challenge is that one could never use historic reference in case of the paper ballot.
- In few places where the governance is corrupt, they can easily insert several bogus paper votes in the ballot and then it becomes impossible to track the honest votes.

2.3 Existing System

For first time in part of Parur Assembly Constituency in Kerala in 1982, on experimental basis. Later, the extensive use of EVMs started in 1998. The EVMs were used at all polling stations in the country in the 14th General Elections to the Loka Sabha in 2004 for the first time. Since then all elections to Loka Sabha and Legislative Assemblies have been held using EVMs.

Working: The control unit is with the presiding officer or a polling officer and the balloting Unit is placed inside the voting compartment. The balloting unit presents the voter with blue buttons (momentary switch) horizontally labeled with corresponding party symbol and candidate names. The Control Unit on the other hand provides the officer in-charge with a "Ballot" marked button to proceed to the next voter, instead of issuing a ballot paper to them. This activates the ballot unit for a single vote from the next voter in queue. The voter has to cast his vote by once pressing the blue button on the balloting unit against the candidate and symbol of his choice.

As soon as the last voter has voted, the Polling Officer in-charge of the Control Unit will press the 'Close' Button. Thereafter, the EVM will not accept any votes. Further, after the close of poll, the Balloting Unit is disconnected from the Control Unit and kept separately. Votes can be recorded only through the Balloting Unit. Again the Presiding officer, at the close of the poll, will hand over to each polling agent present an account of votes recorded. At the time of counting of votes, the total will be tallied with this account and if there is any discrepancy, this will be pointed out by the Counting Agents. During the counting of votes, the results are displayed by pressing the 'Result' button.

There are two safeguards to prevent the be pressed till the 'Close' button is pressed by the Polling Officer in-charge at the end of the 'Result' button from being pressed before the counting of votes officially begins. (a) This button cannot be voting process in the polling booth. (b) This button is hidden and sealed; this can be broken only at the counting centre in the presence of designated office.

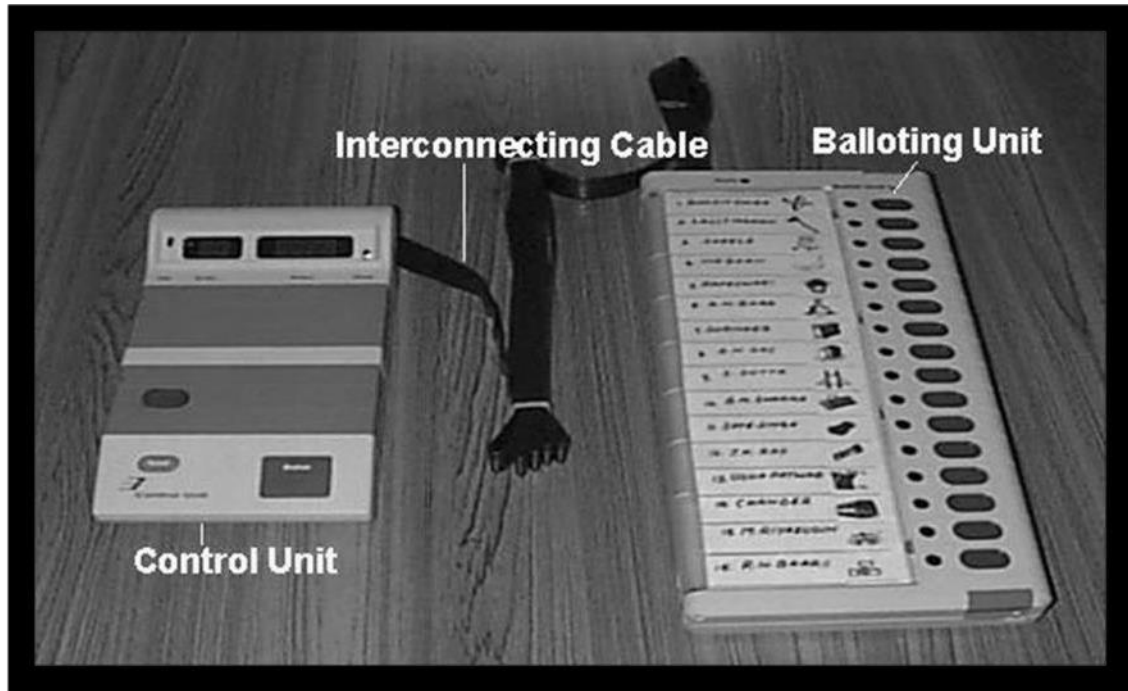


Fig 2.3. Existing electronic voting machine

The machine and the process is in this context that the solution offered by Bharat Electronics Ltd (BEL) in India stands out as perhaps the best of available alternatives. The Electronic Voting Machine (EVM) from BEL consists of two interconnected units, the Ballot Unit where the voter casts his vote by pressing a button alongside the name of the candidate and symbol of the party for whom the person chooses to vote for and the Control Unit by which the polling official enables the Ballot Unit for the voter to cast his vote and where all related data like number of votes polled for each candidate, total number of votes cast etc. resides. The voting sequence using the EVM has been kept as close to the traditional Voting process as possible.

Once the validity of the voter has been ensured, the Polling official enables the Ballot Unit and the voter is asked to go to the secluded area where the Ballot Unit is placed. There, the voter scrutinizes the names of the candidates / parties displayed on the Ballot Unit and cast his vote by pressing the blue button beside the chosen candidates' name / symbol.

The corresponding LED is lit and an audible beep is heard confirming the registration of vote in the system. This process is repeated for the next voter. At the end of polling, the process is completed by the official by pressing the Close button on the Control Unit. On operation of the result button of the Control Unit, the display indicates the results of the poll including total number of votes cast and the number of votes polled for each candidate.

Disadvantage:

- Many software programmers have claimed that the electronic voting machines are vulnerable to malicious programming and if it gets affected then any hacker can hack the machine and can tamper the vote counts easily.
- Fake display units could be installed in the electronic voting machines which would show manipulated numbers but originally fake votes could be generated from the back end. This process does not need any hacker to hack the software. Such fake display units are easily available in the market.
- Electronic voting machines can be tampered during its manufacturing and in such cases, it does not even require any hacker or malware to manipulate the actual voting.
- The biggest change with technology is that no matter how much data it records but a single virus can destroy the entire data storage. The electronic voting machines which were used during the elections are susceptible to damage which will result in loss of data.

2.4 PROPOSED SYSTEM

This project aims to build an Aadhaar and Web based Voting System using Fingerprint and Face Recognition. This project is used to maintain High level security. The voter details are stored in database in computer. Before entering the premises that person should swipe RFID card on to RFID reader, the RFID reader sends a character associated with the RFID card. After sending the character to the ARM, the ARM uploads the character to MATLAB.

After receiving the character from ARM the MATLAB asks for face authentication if the character obtained from the MATLAB and the ARM is same then he is valid person, he will be allowed to vote. In this project we can overcome the problem prevalent in the existing system, such as proxy votes, missing identity, security, high cost and helps people to vote from any booth to his respective constituency.

To overcome above stated problems we are proposing a voting system which is more secure, time saving and provide two level of authentication by electronic means based on individual Face pattern recognition, Fingerprint of voters. The new system will use face pattern of the voter as authentication by which at the time of election if scanned face pattern data of the voter matches with that of saved in the system then he is allowed to vote otherwise he is rejected a reported as fake voter and law breaker. Face pattern properties of any individual are unique universally, which cannot be matched with anybody like fingerprint, iris, gaits, voice, face etc. Out of these, fingerprints, face images and iris samples are saved in national Aadhaar (U-id) database of Indian government. So, there is no need to create an extra database which contains only face pattern data. The need is to connect with the U-id database. The proposed approach is time saving and provides much better authentication from paper based authentication

To overcome above stated problems we are proposing a voting system which is more secure, time saving and provide two level of authentication by electronic means based on individual Face pattern recognition, Fingerprint of voters. The new system will use face pattern of the voter as authentication by which at the time of election if scanned face pattern data of the voter matches with that of saved in the system then he is allowed to vote otherwise he is rejected a reported as fake voter and law breaker. Face pattern properties of any individual are unique universally, which cannot be matched with anybody like fingerprint, iris, gaits, voice, face etc. Out of these, fingerprints, face images and iris samples are saved in national Aadhaar (U-id) database of Indian government. So, there is no need to create an extra database which contains only face pattern data. The need is to connect with the U-id database. The proposed approach is time saving and provides much better authentication from paper based authentication

CHAPTER 3

SYSTEM REQUIREMENTS

All computer software needs certain hardware components or other software resources to be present on a computer. These prerequisites are known as system requirements. In other words, system requirements are giving to be met in the design of a system or sub-system.

3.1 Hardware Requirements

- RFID Tag
- RFID Reader
- ARM
- Fingerprint
- WIFI Module
- Camera
- 5v 2A power supply

3.2 Software Requirements

- 3.2.1 Embedded C
- 3.2.2 MatLab
- 3.2.3 HTML
- 3.2.4 SQL
- 3.2.5 Java Script

3.3 Functional Requirements

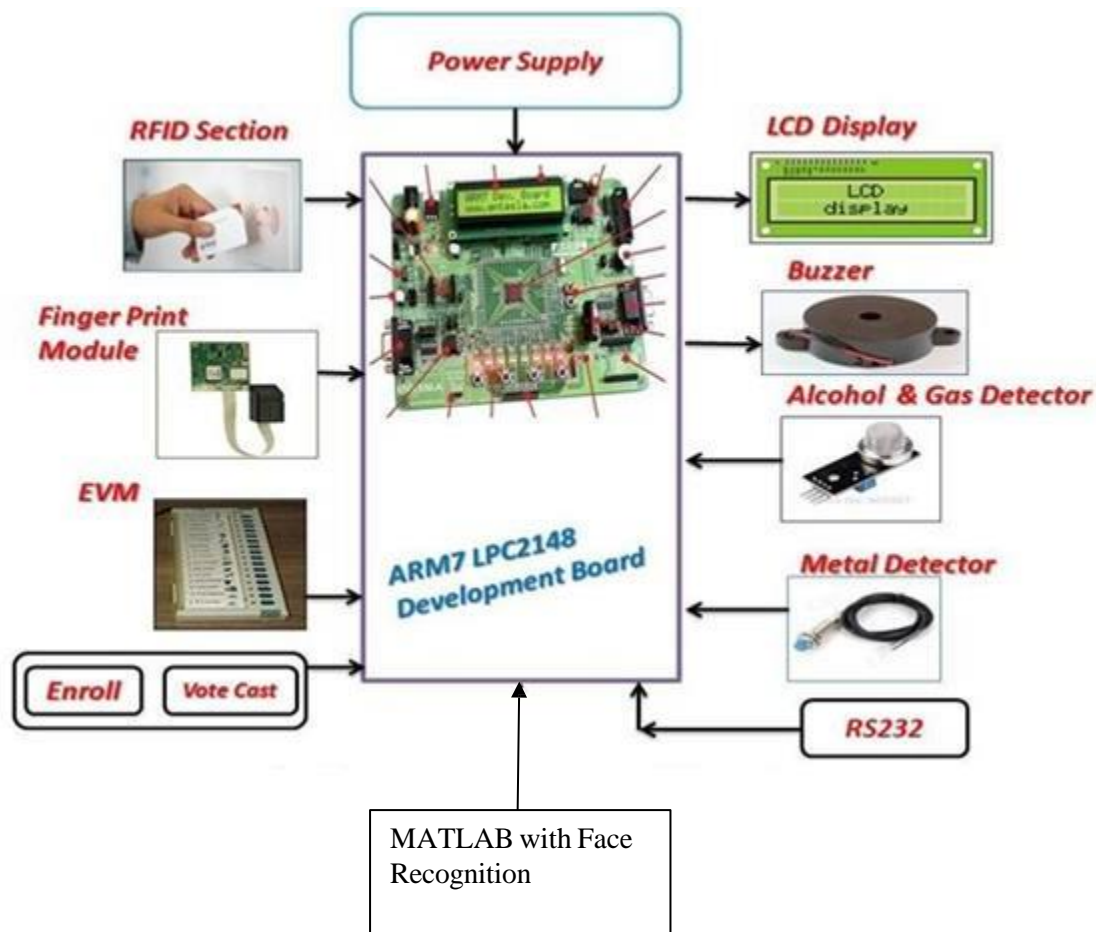
Functional requirement can be defined as user requirement that include a function which must be performed by the system. With the help of functional specification, in development phase different accessibility options are given according to the role of users. Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform. The functional requirements of the project are as shown below:

- 3.3.1 An interactive user interface to take input from the user in the form of RFID tag scanning.
- 3.3.2 Interface to take Face patterns from the Voter for authentication.
- 3.3.3 Interface to give login page to booth level officer.

CHAPTER 4

SYSTEM DESIGN

All computer software needs certain hardware components or other software resources to be present on a computer. These prerequisites are known as system requirements. In other words, system requirements are giving to be met in the design of a system or sub-system.



4.1 Methodology:

1. Aadhar Card Scanning
2. Connect to Server Fetch and Display Aadhar Card Related details
3. User Authentication Using Face Recognition
4. Matching Database and Live Detected Face
5. Face Recognition Using PCA Algorithm
6. If Face Matches showing the constituency details and allowing person to vote
7. If face doesn't match person will not be allowed to vote
8. Storing in Database

The proposed face recognition system overcomes certain limitations of the existing face recognition system. It is based on extracting the dominating features of a set of human faces stored in the database and performing mathematical operations on the values corresponding to them. Hence when a new image is fed into the system for recognition the main features are extracted and computed to find the distance between the input image and the stored images. Thus, some variations in the new face image to be recognized can be tolerated. When the new image of a person differs from the images of that person stored in the database, the system will be able to recognize the new face and identify who the person is.

System design is the process of defining the architecture, modules, interfaces and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development "blends the perspective of marketing, design, and manufacturing into a single approach to product development," then design is the act of taking the marketing information and creating the design of the product to be manufactured.

System design is therefore the process of defining and developing systems to satisfy specified requirements of the user. Until the 1990s, systems design had a crucial and respected role in the data processing industry. In the 1990s, standardization of hardware and software resulted in the ability to build modular systems. The increasing importance of software running on generic platforms has enhanced the discipline of software engineering. Object-oriented analysis and design methods are becoming the most widely used methods for computer systems design. The UML has become the standard language in object-oriented analysis and design.

It is widely used for modelling software systems and is increasingly used for high designing non-software systems and organizations. It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently. System Design focuses on how to accomplish the objective of the system.

The System Design Document is a required document for every project. It should include a high level description of why the System Design Document has been created, provide what the new system is intended for or is intended to replace and contain detailed descriptions of the architecture and system components of the system. Based on the user requirements and the detailed analysis of the existing system, the new system must be designed. This is the phase of system designing. It is the most crucial phase in the developments of a system. The logical system design arrived at as a result of systems analysis is converted into physical design. System design is the phase that bridges the gap between problem domain and the existing system in a manageable way.

This phase focuses on the solution domain, i.e. -how to implement? It is the phase where the SRS document is converted into a format that can be implemented and decides how the system will operate.

In this phase, the complex activity of system development is divided into several smaller sub-activities, which coordinate with each other to achieve the main objective of system development.

4.2 RFID

In 1946, a Russian invented an espionage tool called the Covert Listening Device. This device retransmitted incident radio waves with audio information. Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency.

This passive device was attributed to be the first known device and a predecessor of the RFID technology. The British invented a similar system during the World War II to identify enemy aircraft. It was called the Identification of Friend or Foe (IFF).

Initial application was during World War II-The United Kingdom used RFID devices to distinguish returning English airplanes from inbound German ones. RADAR was only able to signal the presence of a plane, not the kind of plane it was. It was invented in 1948 by Harry Stockman. In 1971, an RFID device that was passive, powered by the interrogating signal, with a 16-bit memory transponder was invented. This device was the true ancestor to modern RFID and was patented in 1973 in the USA that had demonstrated its uses in: Transportation (automotive vehicle identification, automatic toll system, electronic license plate, electronic manifest, vehicle routing, and vehicle performance monitoring) Banking (electronic check book, electronic credit card), security (personnel identification, automatic gates, surveillance), Medical (identification, patient history). It came into commercial use only in 1990s.

Radio frequency identification (RFID) technology is a wireless communication technology that enables users to uniquely identify tagged objects or people. RFID is rapidly becoming a cost-effective technology. This is in large part due to the efforts of Wal-Mart and the Department of Defence (DoD) to incorporate RFID technology into their supply chains. Although the foundation of the Radio Frequency Identification (RFID) technology was laid by past generations, only recent advances opened an expanding application range to its practical implementation.

RFID is only one of numerous technologies grouped under the term Automatic

Identification (Auto ID), such as bar code, magnetic inks, optical character recognition, voice recognition, touch memory, smart cards, biometrics etc. Auto ID technologies are a new way of controlling information and material flow, especially suitable for large production networks.

4.3 RFID Concept

The RFID technology is a means of gathering data about a certain item without the need of touching or seeing the data carrier, through the use of inductive coupling or electromagnetic waves.

One important feature enabling RFID for tracking objects is its capability to provide unique identification. One possible approach to item identification is the EPC (Electronic Product Code), providing a standardized number in the EPC global Network, with an Object Name Service (ONS) providing the adequate Internet addresses to access or update instance-specific data. However, currently, ONS cannot be used in a global environment, and since it is a proprietary service, its use is relatively expensive, especially for participants with limited resources such as SMEs. As an alternative, researchers from the Helsinki University have proposed the notation ID@URI, where ID stands for an identity code, and URI stands for a corresponding Internet address. This allows several partners to use the system and still guarantee unique identification. The project 'Identity-Based Tracking and Web-Services for SMEs' (<http://www.traser-project.eu>) is currently working on further development of this concept.

RFID tags or radio-frequency identification tags are helping streamline distribution, logistics and asset tracking and rapidly replacing traditional barcode technology as the solution of choice for companies in nearly every industry sector globally. With the increasing success and popularity of RFID more demands are being placed on its performance. Additional capabilities are required for RFID tag design and functionality including the ability to package and encapsulate tags and incorporate sensor based technology. RFID tags are being used increasingly in extreme environments requiring exposure to harsh chemicals, high moisture and high heat.

The data carrier is a microchip attached to an antenna (together called transponder or tag), the latter enabling the chip to transmit information to a reader (or transceiver) within a given range, which can forward the information to a host computer.

The middleware (software for reading and writing tags) and the tag can be enhanced by data encryption for security-critical application at an extra cost, and anti-collision algorithms may be implemented for the tags if several of them are to be read simultaneously.

One important feature enabling RFID for tracking objects is its capability to provide unique identification. One possible approach to item identification is the EPC (Electronic Product Code), providing a standardized number in the EPC global Network, with an Object Name Service (ONS) providing the adequate Internet addresses to access or update instance-specific data. However, currently, ONS cannot be used in a global environment, and since it is a proprietary service, its use is relatively expensive, especially for participants with limited resources such as SMEs. As an alternative, researchers from the Helsinki University have proposed the notation ID@URI, where ID stands for an identity code, and URI stands for a corresponding Internet address. This allows several partners to use the system and still guarantee unique identification. The project 'Identity-Based Tracking and Web-Services for SMEs' (<http://www.traser-project.eu>) is currently working on further development of this concept.

RFID tags or radio-frequency identification tags are helping streamline distribution, logistics and asset tracking and rapidly replacing traditional barcode technology as the solution of choice for companies in nearly every industry sector globally. With the increasing success and popularity of RFID more demands are being placed on its performance. Additional capabilities are required for RFID tag design and functionality including the ability to package and encapsulate tags and incorporate sensor based technology. RFID tags are being used increasingly in extreme environments requiring exposure to harsh chemicals, high moisture and high heat.

4.4 The Four Core Components of an RFID System

An RFID system has four basic components: A tag which is composed of a semiconductor chip and an antenna. An interrogator (sometimes called a read/write device), which is composed of an antenna, a RF electronics module, and a control electronics module.

A controller (sometimes called a host), which most often takes the form of a PC or a workstation running database and control (often called middleware) software. An antenna, which converts electrical power to RF power.

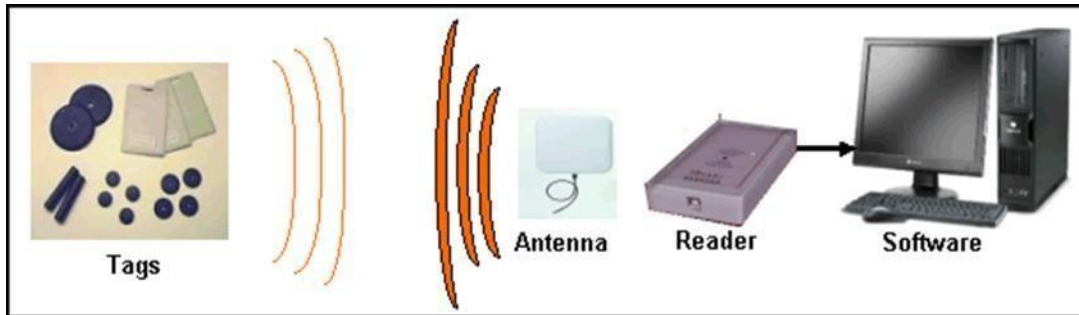


Fig.4.5. Basic Building blocks of an RFID system

4.5 RFID tags

The basic function of an RFID tag is to store data and transmit data to the interrogator. At its most basic, a tag consists of an electronics chip and an antenna encapsulated in a package to form a usable tag as shown in Fig.3.2, such as a packing label that might be attached to a box.

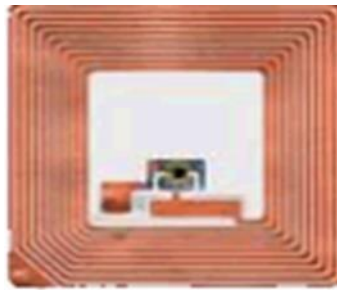


Fig.4.6. RFID Tag

Generally, the chip contains memory where data may be stored and read from and sometimes written, too, in addition to other important circuitry as shown in Fig.4.6. Some tags also contain batteries, and this is what differentiates active tags from passive tags. In our project we use passive tag.

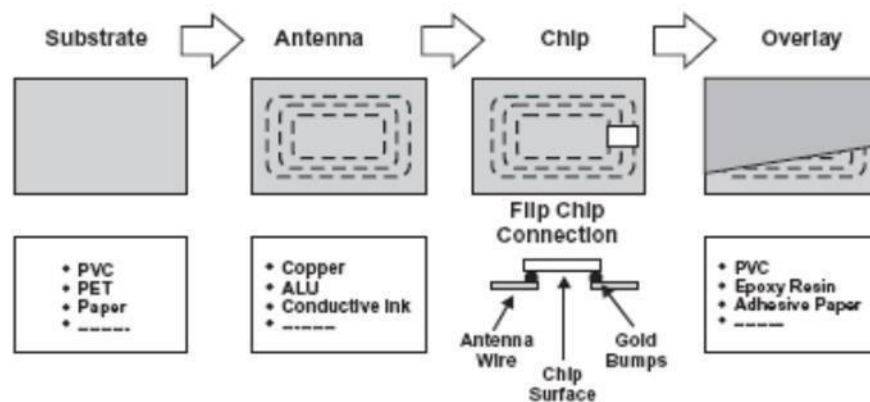


Fig.4.7. RFID Tag Components

Types of Tags and Readers

RFID tags and readers can be grouped under a number of categories as shown in Fig.3.4. Their classification is presented Classification of RFID tags Passive Also called ‘pure passive’, ‘reflective’ or ‘beam powered’ obtains operating power from the reader the reader sends electromagnetic waves that induce current in the tag’s antenna, the tag reflects the RF signal transmitted and adds information by modulating the reflected signal Semi-passive uses a battery to maintain memory in the tag or power the electronics that enable the tag to modulate the reflected signal communicates in the same method, as the other passive tags Active powered by an internal battery, used to run the microchip’s circuitry and to broadcast a signal to the reader Generally ensures a longer read range than passive tags More expensive than passive tags (especial because usually are read/write).

The batteries must be replaced periodically By the tag’s memory type Read-only - the memory is factory programmed, cannot be modified after its manufacture Its data is static Very limited quantity of data can be stored, usually 96 bits of information can be easily integrated with data collection systems Typically are cheaper than read-write tags Read-write - can be as well read as written into Its data can be dynamically altered can store a larger amount of data, typically ranging from 32 Kbytes to 128 Kbytes being more expensive than read-only chips, is impractical for tracking inexpensive items.

By the method of wireless signal used for communication between the tag and reader Induction Close proximity electromagnetic or inductive coupling—near field Generally use, LF and HF frequency bands Propagation. Propagating electromagnetic waves—far field Operate in the UHF and microwaves frequency bands Tags can take a variety of forms like: Smart labels Keys and Key Fobs Watches Smart Cards Disks and Coins Mount-on-metal.

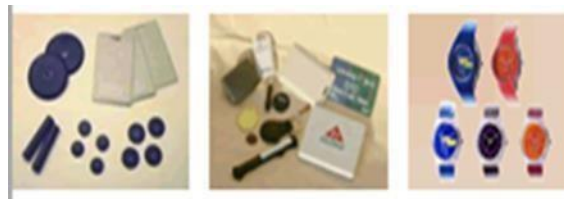


Fig.4.8. Various Forms of Tag

4.5.1 RFID Interrogators (Reader)

An RFID interrogator acts as a bridge between the RFID tag and the controller.

It has a few basic functions to perform: Read the data contents of an RFID tag Write data to the tag (in the case of smart tags) Relay data to and from the controller Power-up the tag (in the case of passive tags).

RFID interrogators are composed of roughly three parts: an antenna, an RF electronics module, responsible for communicating with the RFID tag, and a controller electronics module, responsible for communicating with the controller. A number of factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gains, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have an impact on the RFID system's read range. The reader either continuously (in case of fixed readers) or on demand (as in handheld readers) sends out electromagnetic waves to inquire the presence of any tags in its active read field. On receiving the signals from the tags, the reader decodes the signal and forwards it to the host information processing system.

Classification of Readers

By design and technology used Read - only reads data from the tag-Usually a micro-controller- based unit with a wound output coil, Peak detector hardware, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation- Different types for different protocols, frequencies and standards exist.

- 4.5.1.1 **Read/write:** reads and writes data from/on the tag by fixation of the device Stationary The device is attached in a fixed way, for example at the entrance gate, respectively at the exit gate of products Mobile in this case the reader is a handy, movable device.
- 4.5.1.2 **RFID Read/Module:** DT125R Series the DT125R series proximity OEM RFID Read modules work at the industry-standard 125 kHz frequency. Designed to detect and read/write Hitag2 and TK5561 tags Built-in antenna and pin out for external antenna.

4.5.2 Specifications

TABLE I
Specification for RFID Reader

Frequency	125 KHz
Reading distance	≥ 50 mm
Interface	UART
Antenna	Built in / External
Supply Voltage	5V
Operating Temperature	-10°C to +50°C
Tag Types	Unique, TK 5530
Output Format	ASCII, Wiegand 26

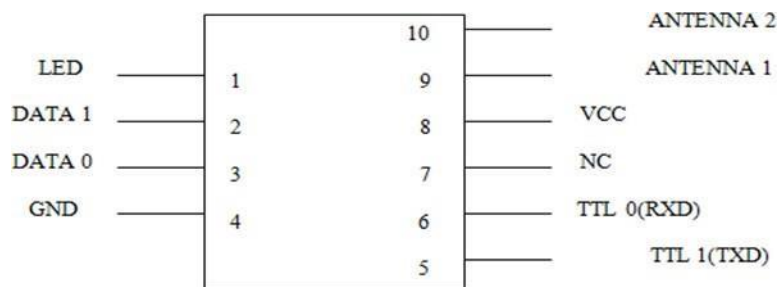


Fig. 4.9. Pin Out Diagram of DT 125R

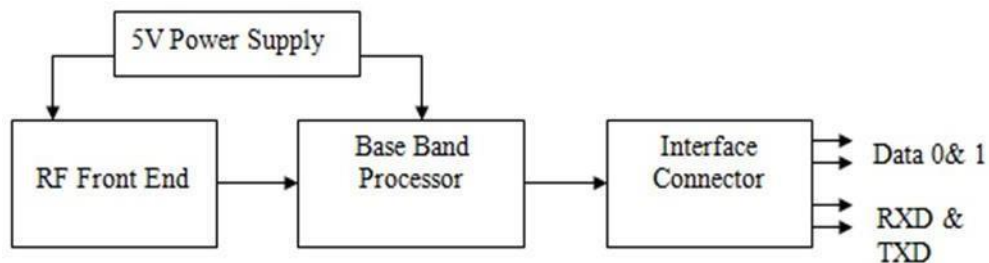


Fig. 4.10. Block Diagram of DT 125R

The LF DT125R reader consists of a RF front end interfaced with the baseband processor that operates with +5V power supply.

An antenna is interfaced with the RF front end, and tuned at 125 kHz to detect a tag (transponder) that comes in the vicinity of the reader field as shown in Fig. 4.9. The data read from the tag by the front end is detected and decoded by the baseband processor and is then sent to the UART interface.

The DATA 0 & DATA 1 (pins 3 & 4) provide tag information in Weygand 26 format. The TXD & RXD (pins 5 & 6) provide tag information in ASCII format. DT125R has a built-in circuitry for noise reduction as shown in Fig. 4.10.

4.5.3 Components of RFID Systems

An RFID system is always made up of two components

- The Transponder, which is located on the object to be identified.
- The interrogator or reader, which, depending upon the design and the technology Used, may be a read or write/read device.

A practical example is shown in Fig. 4.11. A reader typically contains a radio frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, RS 485, etc.) to enable them to forward the data received to another system (PC, robot control system, etc.). The transponder, which represents the actual data-carrying device of an RFID system, normally consists of a coupling element and an electronic microchip as shown in Fig. 4.11.

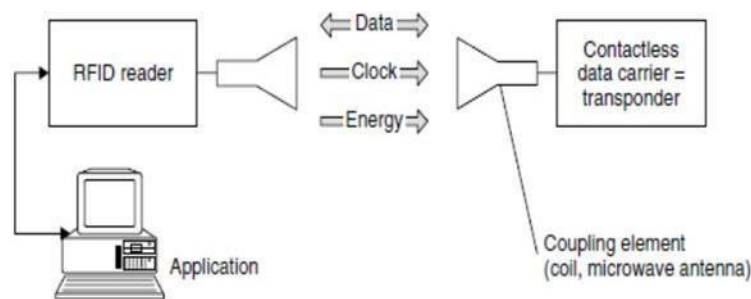


Fig. 4.11. RFID System Consisting of Transponder and Receiver



Fig. 4.12. RFID Card Showing the Microchip and Antenna

When the transponder, which does not usually possess its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive. The transponder is only activated when it is within the interrogation zone of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.

Fundamental Operating Principles of 1-Bit Transponder: A bit is the smallest unit of information that can be represented and has only two states: 1 and 0. This means that only two states can be represented by systems based upon a 1-bit transponder: ‘transponder in interrogation zone’ and ‘no transponder in interrogation zone’. Despite this limitation, 1-bit transponders are very widespread — their main field of application is in electronic anti-theft devices in shops (EAS, electronic article surveillance). The Block Diagram of Transponder is shown in Fig.4.13.

The Radio Frequency (RF) procedure is based upon LC resonant circuits adjusted to a defined resonant frequency f_R . early versions employed inductive resistors made of wound enamelled copper wire with a soldered on capacitor in a plastic housing (hard tag). Modern systems employ coils etched between foils in the form of stick-on labels. To ensure that the damping resistance does not become too high and reduce the quality of the resonant circuit to an unacceptable level, the thickness of 1-BIT TRANSPONDER the aluminium conduction tracks on the 25 μm thick polyethylene foil must be at least 50 μm . Intermediate foils of 10 μm thickness are used to manufacture the capacitor plates. The reader (detector) generates a magnetic alternating field in the radio frequency Range. If the LC resonant circuit is moved into the vicinity of the magnetic alternating field, energy from the alternating field can be induced in the resonant circuit via its coils (Faraday’s law).

If the frequency f_G of the alternating field corresponds with the resonant frequency f_R of the LC resonant circuit the resonant circuit produces a sympathetic oscillation. The current that flows in the resonant circuit as a result of this acts against its cause, i.e. it acts against the external magnetic alternating field. This effect is noticeable as a result of a small change in the voltage drop across the transmitter's generator coil and ultimately leads to a weakening of the measurable magnetic field strength. A change to the induced voltage can also be detected in an optional sensor coil as soon as a resonant oscillating circuit is brought into the magnetic field of the generator coil. The relative magnitude of this dip is dependent upon the gap between the two coils (generator coil — security element, security element — sensor coil) and the quality Q of the induced resonant circuit (in the security element)

4.6 ARM

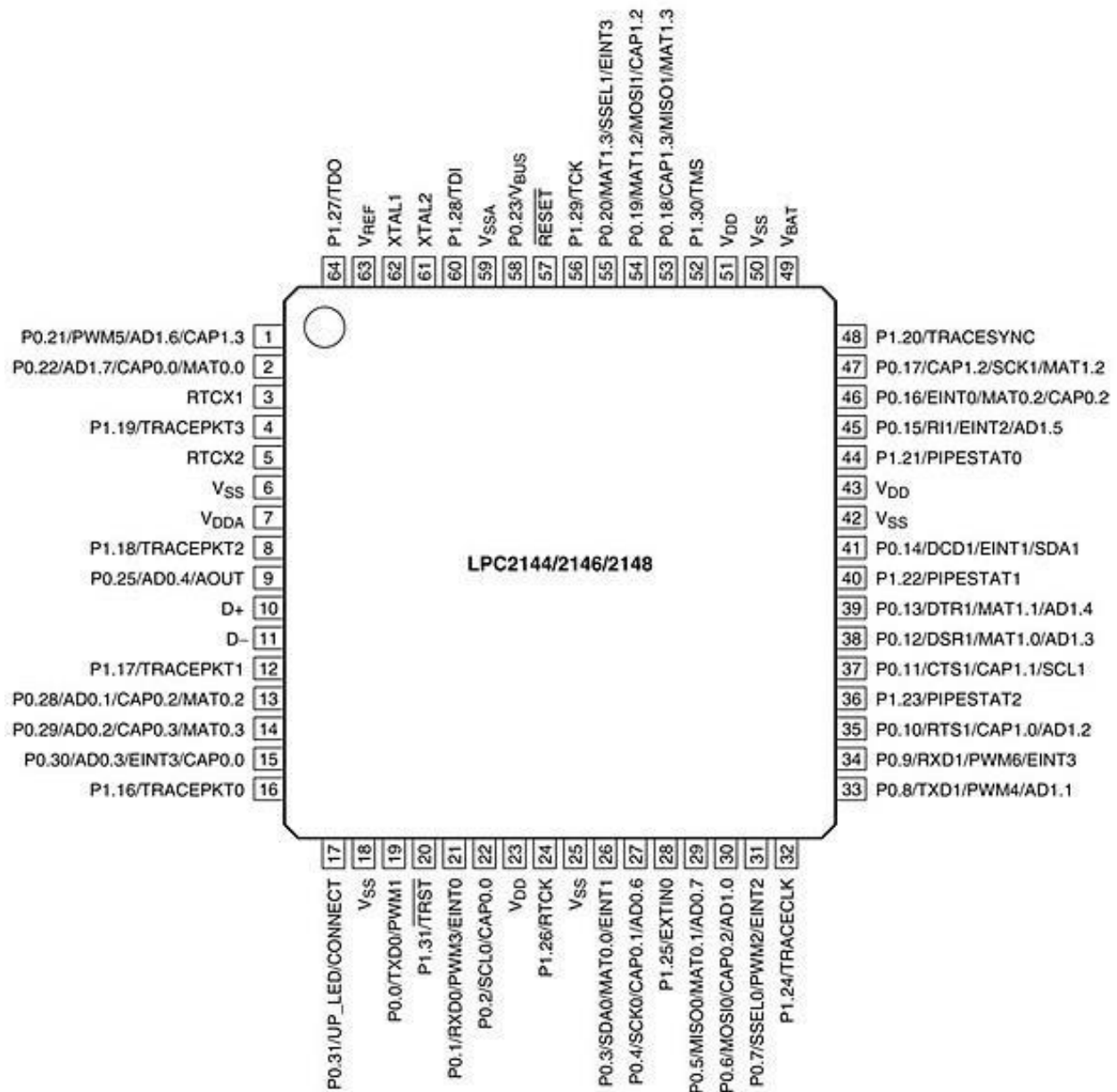
ARM LPC 2148

4.6.1 General Description:

The LPC2141/42/44/46/48 microcontrollers are based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and a unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty.

Due to their tiny size and low power consumption, LPC2141/42/44/46/48 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. Serial communications interfaces ranging from a USB 2.0 Full-speed device, multiple UARTs, SPI, SSP to I2C-bus and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit. ADC(s), 10-bit DAC, PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers suitable for industrial control and medical systems.

4.6.2 Pin Diagram:



Features:

- 16-bit/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
- 8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash memory. 128-bit wide interface/accelerator enables high-speed 60 MHz operation.
- In-System Programming/In-Application Programming (ISP/IAP) via on-chip boot loader software. Single flash sector or full chip erase in 400 ms and programming of 256 bytes in 1 ms.
- Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction execution.
- USB 2.0 Full-speed compliant device controller with 2 kB of endpoint RAM. In addition, the LPC2146/48 provides 8 kB of on-chip RAM accessible to USB by DMA.
- One or two (LPC2141/42 vs. LPC2144/46/48) 10-bit ADCs provide a total of 6/14 analog inputs, with conversion times as low as 2.44 μ s per channel.
- Single 10-bit DAC provides variable analog output (LPC2142/44/46/48 only).
- Two 32-bit timers/external event counters (with four capture and four compare channels each), PWM unit (six outputs) and watchdog.
- Low power Real-Time Clock (RTC) with independent power and 32 kHz clock input.
- Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities.
- Vectored Interrupt Controller (VIC) with configurable priorities and vector addresses.
- Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package,.
- Up to 21 external interrupt pins available.
- 60 MHz maximum CPU clock available from programmable on-chip PLL with Settling time of 100 μ s.
- On-chip integrated oscillator operates with an external crystal from 1 MHz to 25 MHz.
- Power saving modes include Idle and Power-down.

- Individual enable/disable of peripheral functions as well as peripheral clock
- Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction execution.
- USB 2.0 Full-speed compliant device controller with 2 kB of endpoint RAM. In addition, the LPC2146/48 provides 8 kB of on-chip RAM accessible to USB by DMA.
- One or two (LPC2141/42 vs. LPC2144/46/48) 10-bit ADCs provide a total of 6/14 analog inputs, with conversion times as low as 2.44 μ s per channel.
- Single 10-bit DAC provides variable analog output (LPC2142/44/46/48 only).
- Two 32-bit timers/external event counters (with four capture and four compare channels each), PWM unit (six outputs) and watchdog.
- Low power Real-Time Clock (RTC) with independent power and 32 kHz clock input.

- Processor wake-up from Power-down mode via external interrupt or BOD.
- Single power supply chip with POR and BOD circuits:
- CPU operating voltage range of 3.0 V to 3.6 V ($3.3\text{ V} \pm 10\%$)

with 5 V tolerant I/O pads.

4.7 Functional Description:

4.7.1 Architecture Overview:

The ARM7TDMI-S is a general purpose 32-bit microprocessor, which offers high performance and very low power consumption. The ARM architecture is based on Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are much simpler than those of microprogrammed Complex Instruction Set Computers (CISC). This simplicity results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective processor core.

Pipeline techniques are employed so that all parts of the processing and memory systems can operate continuously. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory.

The ARM7TDMI-S processor also employs a unique architectural strategy known as Thumb, which makes it ideally suited to high-volume applications with memory restrictions, or applications where code density is an issue. The key idea behind Thumb is that of a super-reduced instruction set.

The ARM7TDMI-S processor has two instruction sets:

- The standard 32-bit ARM set.
- A 16-bit Thumb set.

The Thumb set's 16-bit instruction length allows it to approach twice the density of standard ARM code while retaining most of the ARM's performance advantage over a traditional 16-bit processor using 16-bit registers. This is possible because Thumb code operates on the same 32-bit register set as ARM code. Thumb code is able to provide up to 65 % of the code size of ARM, and 160 % of the performance of an equivalent ARM processor connected to a 16-bit memory system. The particular flash implementation in the LPC2141/42/44/46/48 allows for full speed execution also in ARM mode. It is recommended to program performance critical and short code sections (such as interrupt service routines and DSP algorithms) in ARM mode. The impact on the overall code size

4.7.2 On-chip Flash Memory:

The LPC2141/42/44/46/48 incorporate a 32 kB, 64 kB, 128 kB, 256 kB and 512 kB flash memory system respectively. This memory may be used for both code and data storage. Programming of the flash memory may be accomplished in several ways. It may be programmed In System via the serial port. The application program may also erase and/or program the flash while the application is running, allowing a great degree of flexibility for data storage field firmware upgrades, etc. Due to the architectural solution chosen for an on- chip boot loader, flash memory available for user's code on LPC2141/42/44/46/48 is 32 kB, 64 kB, 128 kB, 256 kB and 500 kB respectively. The LPC2141/42/44/46/48 flash memory provides a minimum of 100,000 erase/write cycles and 20 years of data-retention.

4.7.3 On-Chip Static RAM:

On-chip static RAM may be used for code and/or data storage. The SRAM may be accessed as 8-bit, 16-bit, and 32-bit. The LPC2141, LPC2142/44 and LPC2146/48 provide 8 kB, 16 kB and 32 kB of static RAM respectively. In case of LPC2146/48 only, an 8 kB SRAM block intended to be utilized mainly by the USB can also be used as a general purpose RAM for data storage and code storage and execution.

4.7.4 Interrupt Controller:

The Vectored Interrupt Controller (VIC) accepts all of the interrupt request inputs and categorizes them as Fast Interrupt Request (FIQ), vectored Interrupt Request (IRQ), and non-vectored IRQ as defined by programmable settings. The programmable assignment scheme means that priorities of interrupts from the various peripherals can be dynamically assigned and adjusted.

Fast interrupt request (FIQ) has the highest priority. If more than one request is assigned to FIQ, the VIC combines the requests to produce the FIQ signal to the ARM processor. The fastest possible FIQ latency is achieved when only one request is classified as FIQ, because then the FIQ service routine does not need to branch into the interrupt service routine but can run from the interrupt vector location. If more than one request is assigned to the FIQ class, the FIQ service routine will read a word from the VIC that identifies which FIQ source(s) is (are) requesting an interrupt.

Vectored IRQs have the middle priority. Sixteen of the interrupt requests can be assigned to this category. Any of the interrupt requests can be assigned to any of the 16 vectored IRQ slots,

among which slot 0 has the highest priority and slot 15 has the lowest. Non-vectored IRQs have the lowest priority.

The VIC combines the requests from all the vectored and non-vectored IRQs to produce the IRQ signal to the ARM processor. The IRQ service routine can start by reading a register from the VIC and jumping there. If any of the vectored IRQs are pending, the VIC provides the address of the highest-priority requesting IRQs service routine, otherwise it provides the address of a default routine that is shared by all the non- vectored IRQs. The default routine can read another VIC register to see what IRQs are active

Interrupt sources:

Each peripheral device has one interrupt line connected to the Vectored Interrupt Controller, but may have several internal interrupt flags. Individual interrupt flags may also represent more than one interrupt source.

4.8 Pin Control Block:

The pin connect block allows selected pins of the microcontroller to have more than one function. Configuration registers control the multiplexers to allow connection between the pin and the on chip peripherals. Peripherals should be connected to the appropriate pins prior to being activated, and prior to any related interrupt(s) being enabled. Activity of any enabled peripheral function that is not mapped to a related pin should be considered undefined.

The Pin Control Module with its pin select registers defines the functionality of the microcontroller in a given hardware environment. After reset all pins of Port 0 and 1 are configured as input with the following exceptions: If debug is enabled, the JTAG pins will assume their JTAG functionality; if trace is enabled, the Trace pins will assume their trace functionality. The pins associated with the I2C0 and I2C1 interface are open drain.

4.9 Fast General Purpose Parallel I/O (GPIO):

Device pins that are not connected to a specific peripheral function are controlled by the GPIO registers. Pins may be dynamically configured as inputs or outputs. Separate registers allow setting or clearing any number of outputs simultaneously. The value of the output register may be read back, as well as the current state of the port pins. LPC2141/42/44/46/48 introduce accelerated GPIO functions over prior LPC2000

- Mask registers allow treating sets of port bits as a group, leaving other bits unchanged.
- All GPIO registers are byte addressable.
- Entire port value can be written in one instruction

Features:

- Bit-level set and clear registers allow a single instruction set or clear of any number of bits in one port.
- Direction control of individual bits.
- Separate control of output set and clear.
- All I/O default to inputs after reset.

10-Bit ADC:

The LPC2141/42 contain one and the LPC2144/46/48 contain two analog to digital converters. These converters are single 10-bit successive approximation analog to digital converters. While ADC0 has six channels, ADC1 has eight channels. Therefore, total number of available ADC inputs for LPC2141/42 is 6 and for LPC2144/46/48 is 14.

Features:

- 10 bit successive approximation analog to digital converter.
- Measurement range of 0 V to VREF ($2.0\text{ V} \leq \text{VREF} \leq \text{VDDA}$).
- Each converter capable of performing more than 400,000 10-bit samples per second.
- Every analog input has a dedicated result register to reduce interrupt overhead.
- Burst conversion mode for single or multiple inputs.
- Optional conversion on transition on input pin or timer match signal.
- Global Start command for both converters (LPC2142/44/46/48 only).

10-Bit DAC:

The DAC enables the LPC2141/42/44/46/48 to generate a variable analog output. The maximum DAC output voltage is the VREF voltage.

USB 2.0 Device Controller:

The USB is a 4-wire serial bus that supports communication between a host and a number (127 max) of peripherals. The host controller allocates the USB bandwidth to attached devices through a token based protocol. The bus supports hot plugging, unplugging, and dynamic configuration of the devices. All transactions are initiated by the host controller.

The LPC2141/42/44/46/48 is equipped with a USB device controller that enables 12 Mbit/s data exchange with a USB host controller. It consists of a register interface, serial interface engine, endpoint buffer memory and DMA controller. The serial interface engine decodes the USB data stream and writes data to the appropriate end point buffer memory. The status of a completed USB transfer or error condition is indicated via status registers. An interrupt is also generated if enabled.

A DMA controller (available in LPC2146/48 only) can transfer data between an endpoint buffer and the USB RAM.

Features:

- Fully compliant with USB 2.0 Full-speed specification.
- Supports 32 physical (16 logical) endpoints.
- Supports control, bulk, interrupt and isochronous endpoints.
- Scalable realization of endpoints at run time.
- Endpoint maximum packet size selection (up to USB maximum specification) by software at run time.
- RAM message buffer size based on endpoint realization and maximum packet size.
- Supports Soft Connect and Good Link LED indicator. These two functions are sharing one pin.
- Supports bus-powered capability with low suspend current.
- Supports DMA transfer on all non-control endpoints (LPC2146/48 only).

- One duplex DMA channel serves all endpoints (LPC2146/48 only).
- Allows dynamic switching between CPU controlled and DMA modes
(only in LPC2146/48).
- Double buffer implementation for bulk and isochronous endpoints

UARTs:

The LPC2141/42/44/46/48 each contain two UARTs. In addition to standard transmit and receive data lines, the LPC2144/46/48 UART1 also provides a full modem control handshake interface. Compared to previous LPC2000 microcontrollers, UARTs in PC2141/42/44/46/48 introduce a fractional baud rate generator for both UARTs, enabling these microcontrollers to achieve standard baud rates such as 115200 with any crystal frequency above 2 MHz. In addition, auto-CTS/RTS flow-control functions are fully implemented in hardware (UART1 in LPC2144/46/48 only).

Features:

- 16 byte Receive and Transmit FIFOs.
- Register locations conform to '550 industry standard.
- Receiver FIFO trigger points at 1, 4, 8, and 14 bytes
- Built-in fractional baud rate generator covering wide range of baud rates
without a need for external crystals of particular values.
- Transmission FIFO control enables implementation of software
(XON/XOFF) flow control on both UARTs.
- LPC2144/46/48 UART1 equipped with standard modem interface
signals. This module also provides full support for hardware flow control
(auto-CTS/RTS).

• I2C-Bus Serial I/O Controller:

The LPC2141/42/44/46/48 each contain two I2C-bus controllers. The I2C-bus is bidirectional, for inter-IC control using only two wires: a serial clock line (SCL), and a serial data line (SDA). Each device is recognized by a unique address and can operate as either a receiver-only device (e.g., an LCD driver or a transmitter with the capability to both receive and send information (such as memory)).

receivers can operate in either master or slave mode, depending on whether the chip has to initiate a data transfer or is only addressed. The I2C-bus is a multi-master bus, it can be controlled by more than one bus master connected to it. The I2C-bus implemented in LPC2141/42/44/46/48 supports bit rates up to 400 kbit/s (Fast I2C-bus).

Features:

- Compliant with standard I2C-bus interface.
- Easy to configure as master, slave, or master/slave.
- Programmable clocks allow versatile rate control.
- Bidirectional data transfer between masters and slaves.
- Multi-master bus (no central master).
- Arbitration between simultaneously transmitting masters without corruption of serial data on the bus.
- Serial clock synchronization allows devices with different bit rates to communicate via one serial bus.
- Serial clock synchronization can be used as a handshake mechanism to suspend and resume serial transfer.
- The I2C-bus cost effective purposes

SSI Serial I/O Controller:

The LPC2141/42/44/46/48 each contain one SPI controller. The SPI is a full duplex Serial interface, designed to handle multiple masters and slaves connected to a given bus. Only a single master and a single slave can communicate on the interface during a given. Data transfer. During a data transfer the master always sends a byte of data to the slave, And the slave always sends a byte of data to the master.

Features:

- Compliant with Serial Peripheral Interface (SPI) specification.
- Synchronous, Serial, Full Duplex, Communication.
- Combined SPI master and slave.
- Maximum data bit rate of one eighth of the input clock rate.

SSP Serial I/O Controller:

The LPC2141/42/44/46/48 each contain one SSP. The SSP controller is capable of operation on a SPI, 4-wire SSI, or Microwire bus. It can interact with multiple masters and slaves on the bus. However, only a single master and a single slave can communicate on the bus during a given data transfer. The SSP supports full duplex transfers, with data frames of 4 bits to 16 bits of data flowing from the master to the slave and from the slave to the master. Often only one of these data flows carries meaningful data.

Features:

- Compatible with Motorola's SPI, TI's 4-wire SSI and National Semiconductor's Micro wire buses.
- Synchronous serial communication.
- Master or slave operation.
- 8-frame FIFOs for both transmit and receive.
- Four bits to 16 bits per frame.

General Purpose Timers/External Event Counters:

The Timer/Counter is designed to count cycles of the peripheral clock (PCLK) or an externally supplied clock and optionally generate interrupts or perform other actions at specified timer values, based on four match registers. It also includes four capture inputs to trap the timer value when an input signal transitions, optionally generating an interrupt. Multiple pins can be selected to perform a single capture or match function, providing an application with 'or' and 'and', as well as 'broadcast' functions among them. The LPC2141/42/44/46/48 can count external events on one of the capture inputs if the minimum external pulse is equal or longer than a period of the PCLK. In this configuration, unused capture lines can be selected as regular timer capture inputs, or used as external interrupts.

Features:

- A 32-bit timer/counter with a programmable 32-bit pre scaler.
- External event counter or timer operation.
- Four 32-bit capture channels per timer/counter that can take a snapshot of the timer

value when an input signal transitions. A capture event may also optionally generate an interrupt.

- Four 32-bit match registers that allow:

Continuous operation with optional interrupt generation on match. Stop timer on match with optional interrupt generation. Reset timer on match with optional interrupt generation.

- Four external outputs per timer/counter corresponding to match registers, with the following capabilities:

Watchdog Timer:

The purpose of the watchdog is to reset the microcontroller within a reasonable amount of time if it enters an erroneous state. When enabled, the watchdog will generate a system reset if the user program fails to ‘feed’ (or reload) the watchdog within a predetermined amount of time.

Features:

- Internally resets chip if not periodically reloaded.
- Debug mode.
- Enabled by software but requires a hardware reset or a watchdog reset/interrupt to be disabled.
- Incorrect/Incomplete feed sequence causes reset/interrupt if enabled.
- Flag to indicate watchdog reset.
- Programmable 32-bit timer with internal pre-scaler.
- Selectable time period from $(TPCLK \times 256 \times 4)$ to $(TPCLK \times 232 \times 4)$ in multiples of $TPCLK \times 4$.

4.12 Real-Time Clocks:

The RTC is designed to provide a set of counters to measure time when normal or idle operating mode is selected. The RTC has been designed to use little power, making it suitable for battery powered systems where the CPU is not running continuously (Idle mode).

Features:

- Measures the passage of time to maintain a calendar and clock.
- Ultra-low power design to support battery powered systems.
- Provides Seconds, Minutes, Hours, Day of Month, Month, Year, Day of Week, and Day of Year.
- Can use either the RTC dedicated 32 kHz oscillator input or clock derived from the external crystal/oscillator input at XTAL1. Programmable reference clock divider allows fine adjustment of the RTC.
- Dedicated power supply pin can be connected to a battery or the main 3.3 V.

CHAPTER 5

FINGERPRINT RECOGNITION

5.1 FINGERPRINT READER



Fig 4.15 Fingerprint Reader

5.1.1 Specification of Finger Print reader:

- DC power: 3.6V-6V.
- Current working rate: 100mA-150mA.
- Time taken to acquire: <0.5sec.
- Average searching time: <0.8sec.
- Working environment: Temp -10°C - +40°C.
- Matching mode: 1:1 and 1: n matching.

5.2 Operation Principle OF Fingerprint Reader

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

Fingerprint- processing instructions

➤ **To collect finger image GenImg**

Detecting finger and store the detected finger image in Image Buffer while returning successful confirmation code; If there is no finger, returned confirmation code would be “can’t detect finger”.

➤ **Upload image Up Image**

To upload the image in Img_Buffer to upper computer.

➤ **Download the image Down Image**

To download image from upper computer to Img_Buffer.

➤ **To generate character file from image Img2Tz**

To generate character file from the original finger image in Image Buffer and store the file in CharBuffer1 or CharBuffer2.

➤ **To generate Template**

To combine information of character files from CharBuffer1 and CharBuffer2 and generate a template which is store back in both CharBuffer1 and CharBuffer2.

➤ **To store template**

To store the template of specified buffer (Buffer1/Buffer2) at the designated location of Flash library.

➤ **To read template from Flash library**

To load template at the specified location of Flash library to template buffer

CharBuffer1/CharBuffer2

➤ **To delete template**

To delete a segment (N) of templates of Flash library started from the specified location

➤ **To empty finger library**

To delete all the templates in the Flash library.

➤ **To search finger library**

To search the whole finger library for the template that matches the one in CharBuffer1

or CharBuffer2. When found, Page ID will be returned.

5.3 Power Supply Unit

The circuit needs two different voltages, +5V & +12V, to work. These dual voltages are supplied by this specially designed power supply. The power supply, unsung hero of every electronic circuit, plays very important role in smooth running of the connected circuit. The main object of this 'power supply' is, as the name itself implies, to deliver the required amount of stabilized and pure power to the circuit.

The stabilization of DC output is achieved by using the three terminal voltage regulator IC. This regulator IC comes in two flavours: 78xx for positive voltage output and 79xx for negative voltage output is as shown in Fig.3.12. For example, 7812 gives +12V output and 7912 gives -12V stabilized output. These regulator ICs have in-built short-circuit protection and auto-thermal cut-out provisions. If the load current is very high the IC needs 'heat sink' to dissipate the internally generated power.

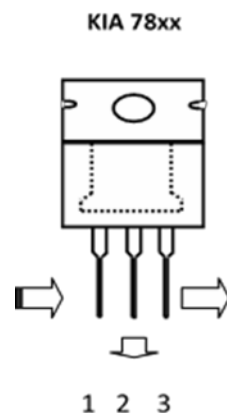


Fig 4.16. Voltage Regulator IC KIA 78xx

Circuit Diagram of +5v & +12v Full Wave Regulated Power Supply

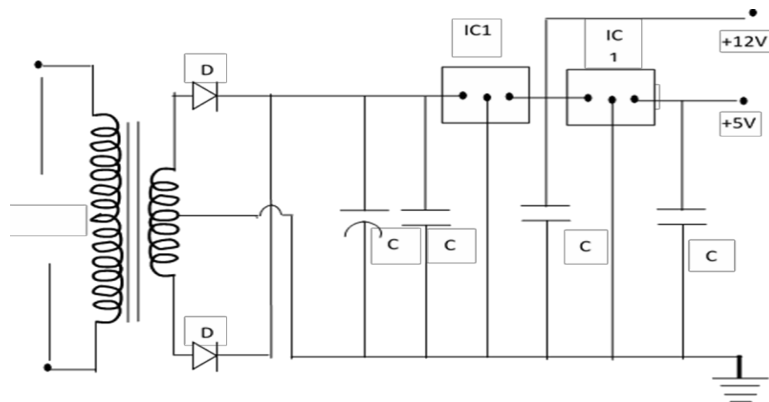


Fig 4.17. Circuit Diagram of +5V & +12V Regulated Power Supply

Components List

TABLE II
Components Required for Power Supply

Semiconductors		
IC1	7812 Regulator IC	1
IC2	7805 Regulator IC	1
D1& D2	1N4007 Rectifier Diodes	2
Capacitors		
C1	1000 μ f/25V Electrolytic	1
C2 to C4	0.1 μ F Ceramic Disc type	3
Miscellaneous		
X1	230V AC Pri,14-0-14 1Amp Sec Transformer	1

5.4 Circuit Description

A DC power supply which maintains the output voltage constant irrespective of AC. mains fluctuations or load variations is known as regulated DC power supply. It is also referred as full-wave regulated power.

Supply as it uses two diodes with the transformer. This laboratory power supply offers excellent line and load regulation and output voltages of +5V & +12 V at output currents up to one ampere.

- Step-down Transformer: The transformer rating is 230V AC at Primary and 12-0-12V, 1Amps across secondary winding. This transformer has a capability to deliver a current of 1Ampere, which is more than enough to drive any electronic circuit or varying load. The 12VAC appearing across the secondary is the RMS value of the waveform and the peak value would be $12 \times 1.414 = 16.8$ volts. This value limits our choice of rectifier diode as 1N4007, which is having PIV rating more than 16 Volts. [3]
- Rectifier Stage: The two diodes D1 & D2 are connected across the secondary winding of the transformer as a full-wave rectifier. During the positive half-cycle

of secondary voltage, the end A of the secondary winding becomes positive and end B negative. This makes the diode D1 forward biased and diode D2 reverse biased. Therefore, diode D1 conducts while diode D2 does not. During the negative half-cycle, end A of the secondary winding becomes negative and end B positive. Therefore, diode D2 conducts while diode D1 does not. Note that current across the center tap terminal is in the same direction for both half-cycles of input AC. voltage. Therefore, pulsating DC. is obtained at point 'C' with respect to Ground. [3]

- **Filter Stage:** Here Capacitor C1 is used for filtering purpose and connected across the rectifier output. It filters the AC. components present in the rectified DC and gives steady DC voltage. As the rectifier voltage increases, it charges the capacitor and also supplies current to the load. When capacitor is charged to the peak value of the rectifier voltage, rectifier voltage starts to decrease. As the next voltage peak immediately recharges the capacitor, the discharge period is of very small duration. Due to this continuous charge-discharge-recharge cycle very little ripple is observed in the filtered output. Moreover, output voltage is higher as it remains substantially near the peak value of rectifier output voltage. This phenomenon is also explained in other form as: the shunt capacitor offers a low reactance path to the AC. components of current and open circuit to DC component. During positive half cycle the capacitor stores energy in the form of electrostatic field. During negative half cycle, the filter capacitor releases stored energy to the load.
- **Voltage Regulation Stage:** Across the point 'D' and Ground there is rectified and filtered DC. In the present circuit KIA 7812 three terminal voltage regulator IC is used to get +12V and KIA 7805 voltage regulator IC is used to get +5V regulated DC output. In the three terminals, pin 1 is input i.e., rectified & filtered DC is connected to this pin. Pin 2 is common pin and is grounded. The pin 3 gives the stabilized DC output to the load. The circuit shows two more decoupling capacitors C2 & C3, which provides ground path to the high frequency noise signals. Across the point 'E' and 'F' with respect to ground +5V & +12V stabilized or regulated DC output is measured, which can be connected to the required circuit.

5.5 Buffer and Driver

Buffer Circuit

The BUFFER IC used is IC 4050 which is a voltage amplifier; it's a non-inverting buffer. A buffer doesn't change the logical state and it also provides an extra voltage drive. This 16-pin DIL packaged IC 4050 acts as Buffer as-well-as a Converter. The input signals may be of 2.5 to 5V digital TTL compatible or DC analogue the IC gives constant output voltage. The IC acts as buffer and provides isolation to the main circuit from varying input signals. Here the IC is use to increase the voltage. It acts as a voltage amplifier. Typically, a voltage buffer amplifier is used to transfer a voltage from a first circuit, having a low output impedance level, to a second circuit with a high input impedance level. The ideal characteristic of a voltage buffer is to have an infinite input resistance and zero output resistance.

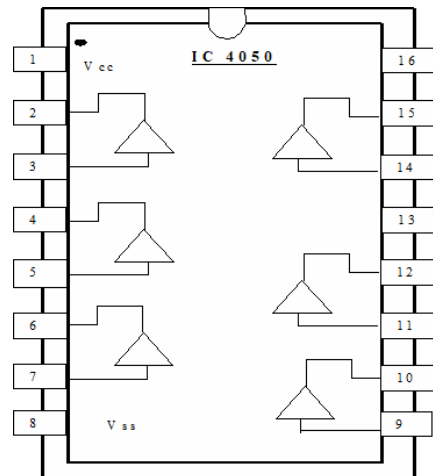


Fig 4.18. Pin Description of Buffer IC 4050

DriverCircuit

The driver circuit is used to enhance the current handling capacity in the circuit. Moreover its acts as a driving circuit for the relays. The IC ULN 2004 is used, this IC consist of an array of emitter-follower circuits as shown in Fig. 4.19.

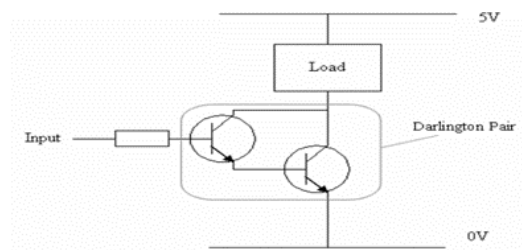


Fig.4.19. Basic Darlington Pair Circuit

Normally to turn on a transistor the base input voltage of the transistor will need to be greater than 0.7V. As two transistors are used in Darlington Pair this value is doubled. Therefore, the base voltage will need to be greater than $0.7V \times 2 = 1.4V$. [6] The output current $I_c = \text{total gain } (\beta) * \text{input current}$. The DRIVER IC used is ULN 2004 [6].

5.5.1 Pin Description

The UTC ULN2004 are high-voltage, high-current Darlington drivers comprised of NPN Darlington pairs. All units feature integral clamp diodes for switching inductive loads. Applications include relay, hammer, lamp and display (LED) drivers.

5.5.2 Features of IC Uln2004

Output current (single output): 500mA (MAX.)

High sustaining voltage output: 50V (MIN.)

Output clamp diodes

Inputs compatible with various types of logic.

5.5.3 ULN 2004

Since the digital outputs of some circuits cannot sink much current, they are not capable of driving relays directly. So, high-voltage high-current Darlington arrays are designed for interfacing low-level logic circuitry and multiple peripheral power loads.

The series ULN2000A/L ICs drive seven relays with continuous load current ratings to 600mA for each input. At an appropriate duty cycle depending on ambient temperature and number of drivers turned ON simultaneously, typical power loads totalling over 260W [$400mA \times 7, 95V$] can be controlled. Typical loads include relays, solenoids, stepping motors, magnetic print hammers, multiplexed LED and incandescent displays, and heaters.

The input of ULN 2004 is TTL-compatible open-collector outputs. As each of these outputs can sink a maximum collector current of 500 mA, miniature PCB relays can be easily driven using ULN 2004. No additional free-wheeling clamp diode is required to be connected across the relay since each of the outputs has inbuilt free-wheeling diodes. The Series ULN20x4A/L features series input resistors for operation directly from 6 to 15V CMOS or PMOS logic outputs.

1N4148 signal diode: Signal diodes are used to process information (electrical signals) in circuits, so they are only required to pass small currents of up to 100mA. General purpose signal diodes such as the 1N4148 are made from silicon and have a forward voltage drop of 0.7V as shown in Fig. 4.20.

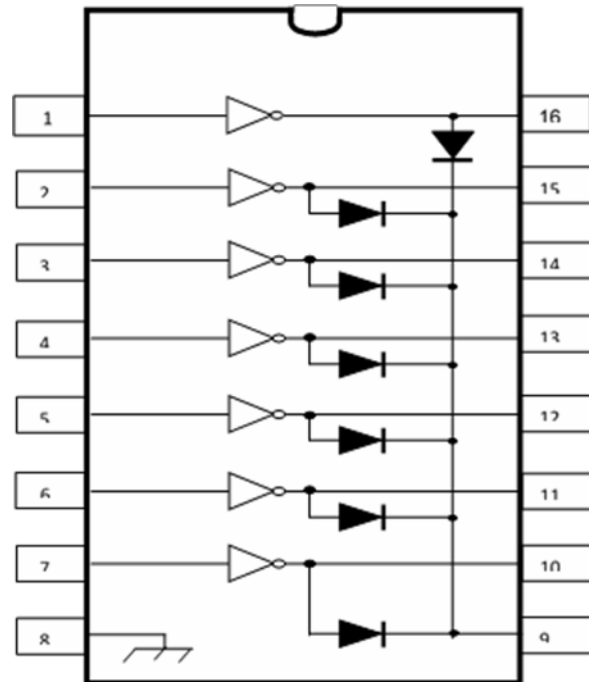


Fig 4.20. Pin Description of IC ULN 2004

Relay

A relay is an electrically operated switch. Current flowing through the coil of the relay creates a magnetic field which attracts a lever and changes the switch contacts. The coil current can be on or off so relays have two switch positions and they are double throw (changeover) switches.

Relays allow one circuit to switch a second circuit which can be completely separate from the first. For example, a low voltage battery circuit can use a relay to switch a 230V AC mains circuit. There is no electrical connection inside the relay between the two circuits; the link is magnetic and mechanical as shown in Fig.4.21. The coils, which provide the necessary magnetic flux to operate a relay, are available for operation on a variety of voltages between 5V and 115V DC and 12V to 250V AC. at currents of between 5 mA and 400 mA.

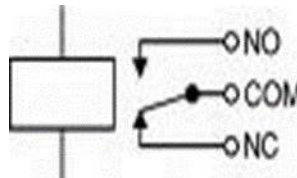


Fig 4.21. Schematic Representation of Relay

5.6 Principle Component Analysis for Face recognition

One instance of a PCA implementation of a face detection/recognition system was done by H. Ando, N. Fuchigami, M. Sasaki, and A. Iwata [5]. The first stages of implementation were tested on prototype software running on a PC. This software reads in an RGB image, reduced in size to 100 x 100 pixels. Face detection is then performed by detecting skin colour, and the PCA algorithm is applied to the face area detected. The prototype software was designed on a XEON-based multi-CPU system using Visual C++ as the programming language. The input to the system was a USB camera device connected to the PC [5].

The next step was to implement the face recognition system. As such, custom hardware blocks were designed in order to carry out the functionality of the PCA algorithm discussed previously. Specifically, the database of images was pre-processed, storing the average face and eigenvectors. For face recognition, an input image vector is fed into the subtraction unit for normalization with respect to the average face. The processed image is then passed to a multiplier/accumulator unit that reads the eigenvectors from memory and performs the projection required by the algorithm. The next stage involves passing this Eigen space projection into the matching block, which contains an evaluation block that reads the Eigen space projections of known faces from memory and performs the necessary Euclidean distance calculations. Finally, a decision unit reads in these distances and makes the face recognition decision based on the requirements of the algorithm.

Having researched the various algorithms for face recognition, we found that the two most popular hardware implementations are PCA and Neural Networks. As stated before, the advantage of PCA is its robustness, parallelizability, and relative simplicity.

Its disadvantages are its sensitivity to lighting and pose variations. On the other hand, the Neural Networks approach provides strong accuracy but limits the number of individuals that can be included in the database due to the long training periods involved.

The PCA algorithm have chosen to adopt for face recognition for several reasons. Firstly, the environment that will be used to obtain the individual face images is controlled and hence lighting and pose variation effects can be minimized. Secondly, since a face can be subdivided into multiple regions, pattern recognition can be applied in parallel, resulting in faster face recognition. Lastly, PCA allows us to quickly add individuals to the face database, making it better suited for real time applications.

Algorithm

Step1: Let I1, I2, I3, I4, IN be the face images from data set (training faces). The face images must be centered and of the same size.

Step 2: Prepare the data set each face image I in the database is transformed into a vector and placed into a training set S.

$$S = \{\Gamma_1, \Gamma_2, \Gamma_3, \dots, \Gamma_N\} \quad (1)$$

Step 3: compute the average or normalized face vector. The average face vector (Ψ) has to be calculated by using the following formula:

$$\Psi = \frac{1}{N} \sum_{i=1}^N \Gamma_i \quad (2)$$

Step 4: Subtract the average face vector. The average face vector is subtracted from the original faces and the result stored in the variable,

$$\Gamma_i = \Gamma_i - \Psi \quad (3)$$

Step 5: Calculate the covariance matrix and obtain the covariance M

$$M = S \cdot S^T \quad (4)$$

Step 6: Obtain the most significant Eigen faces for feature set.

Step 7: Calculate the standard deviation

$$\text{std} = \left(\frac{1}{N-1} \sum_{i=1}^N (\Gamma_i - \Psi)^2 \right)^{1/2} \quad (5)$$

Inputs and Outputs

The inputs of our system consist of bit streams representing the image to be analysed, an average face, an Eigenvector matrix, and a set of projections. The image to be analysed, as well as the average face, will consist of $150 \times 125 = 18,750$ pixels, each being 8-bit grayscale (28 = 256 shades of gray, ranging from 0 to 255). These figures were chosen because they provide a good balance between size and accuracy. Additionally, these values were used successfully by many research groups. In a database with M faces, the Eigenvector matrix will be of size 18,750 by M. Finally, the set of projections will consist of M vectors, each having M values. The outputs of our system will consist of the face ID with the closest match, as well as a value representing how close this match is (a distance value). Furthermore, the system outputs execution times to gauge the speed of the system, as well as each of the functions involved in the recognition stage. All this information will be displayed on the MATLAB.

As discussed earlier that the robust system catering the needs of real world situation is a challenging task. The images will be scanned by scanner and stored into database. Again the image will be scanned and stored into the database. Now two images of the same candidate will be stored into the database. The first step is to select desired images from the database then for comparisons them the next step is to detect faces from each image. The next step is to recognize that images as of the same candidate or not.

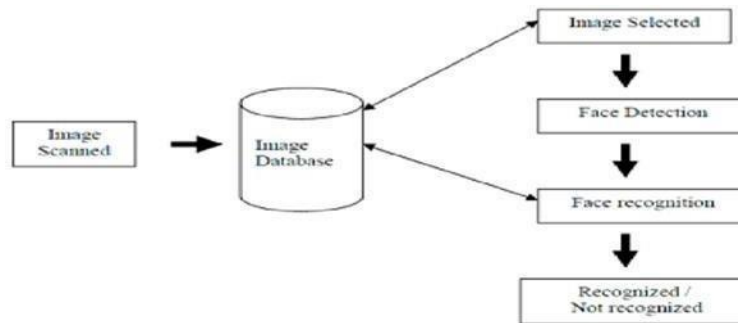
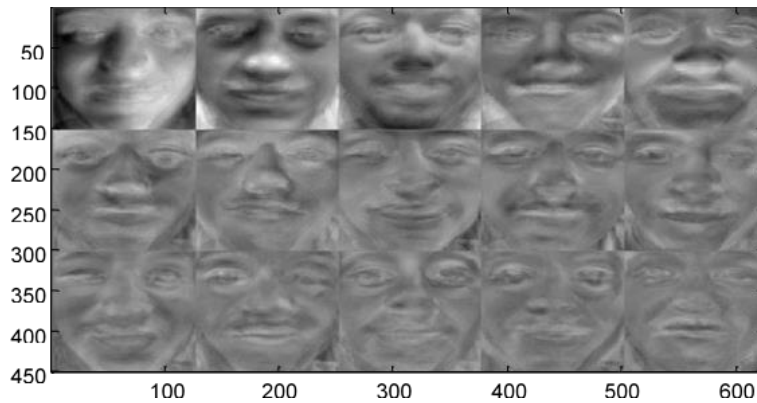


Fig. 4.22. Structure of Face Recognition System

A free database of faces, non faces, and new faces was used as a means to test the implementation developed. The database of faces consists of 51 images each having dimensions of 150×125 pixels represented as row vectors. Each pixel contains an 8-bit grayscale value representing 1 of 256 possible shades of gray. The MATLAB implementation followed the algorithm details outlined above and used built-in MATLAB functions to achieve functionality. Some of these functions are outline in the table below.

TABLE III
Some Functions of MatLab

MATLAB Function	Description
mean (A)	Calculates the mean of matrix A
A'	Calculates the transpose of matrix A
eigs (A, k)	Determines the first k eigenvectors and eigenvalues of A
dist (A, B)	Determines the Euclidean distance between matrices A and B

**(a) Sample Face****(b) Average Face****(c) Eigenface****Fig.4.23. Representing How the face is matched with data**

5.7 Web Page Developing

5.7.1 Html (Hypertext Markup Language)

It is the predominant Mark-up language for web pages. It provides a means to describe the structure of text-based information in a document by denoting certain text as headings, paragraphs, lists, and so on and to supplement that text with interactive forms, embedded images, and other objects. HTML is written in the form of labels (known as tags), surrounded by angle brackets. HTML can also describe, to some degree, the appearance and semantics of a document, and can include embedded scripting language code which can affect the behaviour of web browsers and other HTML processors.

HTML can be used to display any type of document on the host computer, which can be geographically at a different location. It is a versatile language and can be used on any platform or desktop. HTML provides tags (special codes) to make the document look attractive. HTML tags are not case-sensitive. Using graphics, fonts, different sizes, colour, etc., can enhance the presentation of the document. Anything that is not a tag is part of the document itself.

TABLE IV
Basic HTML Tags

<! -- -->	Specifies comments
<A>.....	Creates hypertext links
.....	Formats text as bold
<BIG>.....</BIG>	<BIG>.....</BIG>
<BODY>...</BODY>	Contains all tags and text in the HTML document
<CENTER>...</CENTER>	Align the text at center
<DD>...</DD>	Definition of a term
<DL>...</DL>	Creates definition list
<DL>...</DL>	Creates definition list
...	Formats text with a particular font
<FORM>...</FORM>	Encloses a fill-out form
<FRAME>...</FRAME>	Defines a particular frame in a set of frames
<H#>...</H#>	Creates heading of different levels(1 – 6)
<HEAD>...</HEAD>	Contains tags that specify information about a document
<HR>...</HR>	Creates a horizontal rule
<HTML>...</HTML>	Contains all other HTML tags
<META>...</META>	Provides meta-information about a document
<SCRIPT>...</SCRIPT>	Contains client-side or server-side script
<TABLE>...</TABLE>	Creates a table
<TD>...</TD>	Indicates table data in a table
<TR>...</TR>	Designates a table row
<TH>...</TH>	Creates a heading in a table

5.7.2 JavaScript

JavaScript is a script-based programming language that was developed by Netscape Communication Corporation. JavaScript was originally called Live Script and renamed as JavaScript to indicate its relationship with Java.

JavaScript supports the development of both client and server components of Web-based applications. On the client side, it can be used to write programs that are executed by a Web browser within the context of a Web page. On the server side, it can be used to write Web server programs that can process information submitted by a Web browser and then update the browser's display accordingly.

Even though JavaScript supports both client and server Web programming, we prefer JavaScript at client side programming since most of the browsers supports it. JavaScript is almost as easy to learn as HTML, and JavaScript statements can be included in HTML documents by enclosing the statements between a pair of scripting tags

```
<Script>.....</Script>  
<Script Language = "JavaScript">  
    JavaScript statements  
</Script>
```

Here are a few things we can do with JavaScript

- Validate the contents of a form and make calculations.
- Add scrolling or changing messages to the Browser's status line.
- Animate images or rotate images that change when we move the mouse over them.
- Detect the browser in use and display different content for different browsers.
- Detect installed plug-ins and notify the user if a plug-in is required.
- We can do much more with JavaScript, including creating entire application.

5.7.3 Java Technology

Initially the language was called as "oak" but it was renamed as "Java" in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices.

- Java is a programmer's language.
- Java is cohesive and consistent.
- Except for those constraints imposed by the Internet environment, Java gives the programmer, full control.
- Finally, Java is to Internet programming where C was to system programming.

Importance of Java to the Internet

Java has had a profound effect on the Internet. This is because; Java expands the Universe of objects that can move about freely in Cyberspace. In a network, two categories of objects are transmitted between the Server and the Personal computer. They are: Passive information and Dynamic active programs.

Java can be used to create two types of Programs

Applications and Applets: An application is a program that runs on our Computer under the operating system of that computer. It is more or less like one creating using C or C++. Java's ability to create Applets makes it important. An Applet is an application designed to be transmitted over the Internet and executed by a Java –compatible web browser. An applet is actually a tiny Java program, dynamically downloaded across the network, just like an image. But the difference is, it is an intelligent program, not just a media file. It can react to the user input and dynamically change.

The Byte Code

The key that allows the Java to solve the security and portability problems is that the output of Java compiler is Byte code. Byte code is a highly optimized set of instructions designed to be executed by the Java run-time system, which is called the Java Virtual Machine (JVM). That is, in its standard form, the JVM is an interpreter for byte code. Translating a Java program into byte code helps makes it much easier to run a program in a wide variety of environments. The reason is, once the run-time package exists for a given system, any Java program can run on it.

Servlets

Servlets provide a Java (TM)-based solution used to address the problems currently associated with doing server-side programming, including inextensible scripting solutions, platform-specific APIs, and incomplete interfaces.

Use Servlets instead of CGI Scripts

Servlets are an effective replacement for CGI scripts. They provide a way to generate dynamic documents that is both easier to write and faster to run. Servlets also address the problem of doing server-side programming with platform-specific APIs: they are developed with the Java Servlet API, a standard Java extension. So use Servlets to handle HTTP client requests. For example, have Servlets process data posted over HTTPS using an HTML form, including purchase order or credit card data.

Client Interaction

- When a servlet accepts a call from a client, it receives two objects:
- A `ServletRequest`, which encapsulates the communication from the client to the server.
- A `ServletResponse`, which encapsulates the communication from the servlet back to the client.
- `ServletRequest` and `ServletResponse` are interfaces defined by the `javax.servlet` package.

The ServletRequest Interface

The `ServletRequest` interface allows the servlet access to: Information such as the names of the parameters passed in by the client, the protocol (scheme) being used by the client, and the names of the remote host that made the request and the server that receive the input stream, `ServletInputStream`. Servlets use the input stream to get data from clients that use application protocols such as the HTTP POST and PUT methods.

Interfaces that extend `ServletRequest` interface allow the servlet to retrieve more protocol-specific data. For example, the `HttpServletRequest` interface contains methods for accessing HTTP-specific header information.

The ServletResponse Interface

The `ServletResponse` interface gives the servlet methods for replying to the client. It

- Allows the servlet to set the content length and MIME type of the reply.
- Provides an output stream, `ServletOutputStream`, and a `Writer` through which the servlet can send the reply data.

Interfaces that extend the `ServletResponse` interface give the servlet more protocol-specific capabilities. For example, the `HttpServletResponse` interface contains methods that allow the servlet to manipulate HTTP-specific header information.

Servlet Lifecycle

Each servlet has the same life cycle

- A server loads and initializes the servlet
- The servlet handles zero or more client requests
- The server removes the servlet

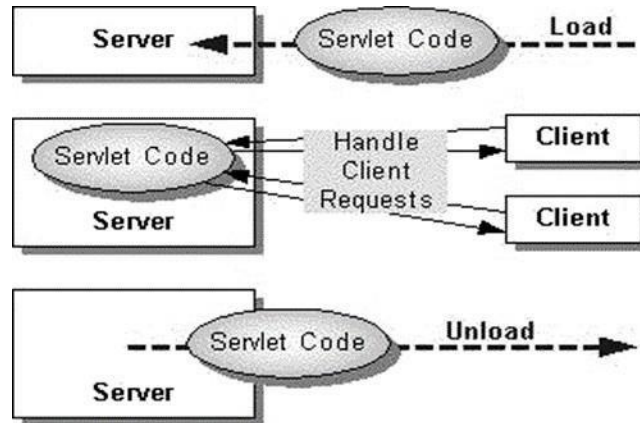


Fig.4.24 Representation of Servlet

Initializing a Servlet

When a server loads a servlet, the server runs the servlet's init method. Initialization completes before client requests are handled and before the servlet is destroyed. Even though most Servlets are run in multi-threaded servers, Servlets have no concurrency issues during servlet initialization. The server calls the init method once, when the server loads the servlet, and will not call the init method again unless the server is reloading the servlet. The server cannot reload a servlet until after the server has destroyed the servlet by calling the destroy method.

The init Method:

The init method provided by the HttpServlet class initializes the servlet and logs the initialization. To do initialization specific to your servlet, override the init () method following these rules, If an initialization error occurs that renders the servlet incapable of handling client requests, throw an Unavailable Exception.

Initialization Parameters:

The second version of the init method calls the getInitParameter method. This method takes the parameter name as an argument and returns a String representation of the parameter's value. The specification of initialization parameters is server-specific. In the Java Web Server, the parameters are specified with a servlet is added then configured in the Administration Tool. For an explanation of the Administration screen where this setup is performed, see the Administration Tool: Adding Servlets online help document. In some cases, if we need to get the parameter names, we can use the getParameterNames method.

Destroying a Servlet:

Servlets run until the server destroys them, for example at the request of a system administrator. When a server destroys a servlet, the server runs the servlets destroy method. The method is run once; the server will not run that servlet again until after the server reloads and reinitializes the servlet. When the destroy method runs, another thread might be running a service request. The Handling Service Threads at Servlet Termination section shows you how to provide a clean shutdown when there could be long-running threads still running service requests.

Using the Destroy Method:

The destroy method provided by the HttpServlet class destroys the servlet and logs the destruction. To destroy any resources specific to your servlet, override the destroy method. The destroy method should undo any initialization work and synchronize persistent state with the current in-memory state. A server calls the destroy method after all service calls have been completed, or a server-specific number of seconds have passed, whichever comes first. If your servlet handles any long-running operations, service methods might still be running when the server calls the destroy method. You are responsible for making sure those threads complete. The next section shows you how. The destroy method shown above expects all client interactions to be completed when the destroy method is called, because the servlet has no long-running operations.

Java Server Pages

Java Server Pages technology lets you put snippets of servlet code directly into a text-based document. A JSP page is a text-based document that contains two types of text: static template data, which can be expressed in any text-based format such as HTML, WML, and XML, and JSP elements, which determine how the page constructs dynamic content.

Java Server Page™ (JSP)

An extensible Web technology that uses template data, custom elements, scripting languages, and server-side Java objects to return dynamic content to a client. Typically, the template data is HTML or XML elements, and in many cases the client is a Web browser.

According to JSP model1 one can develop the application as,

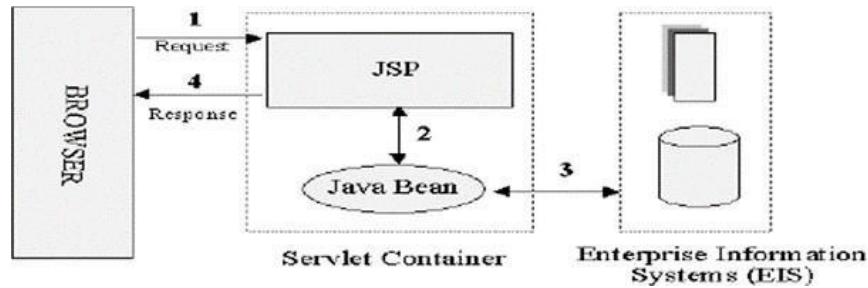


Fig. 4.25 Developing Application using JSP model

According to above model the presentation logic has to be implemented in JSP page and the business logic has to be implemented as part of Java bean This model help us in separating the presentation and business logic. For large-scale projects instead of using model1 it is better to use model2 (MVC).

Java Server Pages (JSP) lets you separate the dynamic part of your pages from the static HTML. You simply write the regular HTML in the normal manner, using whatever Web-page-building tools you normally use. You then enclose the code for the dynamic parts in special tags, most of which start with "<%" and end with "%>". For example, here is a section of a JSP page that results in something like "Thanks for ordering Core Web Programming.

For URL of

[http://host/OrderConfirmation.jsp?title=Core+Web+Programming:](http://host/OrderConfirmation.jsp?title=Core+Web+Programming)

Thanks for ordering

```
<I><%= request.getParameter("title") %></I>
```

You normally give your file a .jsp extension, and typically install it in any place you could place a normal Web page. Although what you write often looks more like a regular HTML file than a servlet, behind the scenes, the JSP page just gets converted to a normal servlet, with the static HTML simply being printed to the output stream associated with the servlet's service method. This is normally done the first time the page is requested, and developers can simply request the page themselves when first installing it if they want to be sure that the first real user doesn't get a momentary delay when the JSP page is translated to a servlet and the servlet is compiled and loaded. Note also that many Web servers let you define aliases that so that a URL that appears to reference an HTML file really points to a servlet or JSP page. Aside from the regular HTML, there are three main types of JSP constructs that you embed in a page: scripting elements, directives, and actions.

Scripting elements let you specify Java code that will become part of the resultant servlet, directives let you control the overall structure of the servlet, and actions let you specify existing components that should be used, and otherwise control the behaviour of the JSP engine. To simplify the scripting elements, you have access to a number of predefined variables such as request in the snippet above.

J2EE Platform Overview

The J2EE platform is designed to provide server-side and client-side support for developing distributed, multi-tier applications. Such applications are typically configured as a client tier to provide the user interface, one or more middle-tier modules that provide client services and business logic for an application, and back-end enterprise information systems providing data management.

Communication Technologies

Communication technologies provide mechanisms for communication between clients and servers and between collaborating objects hosted by different servers. The J2EE specification requires support for the following types of communication technologies.

Internet protocols

- Remote method invocation protocols
- Object Management Group protocols
- Messaging technologies
- Data formats

Internet protocols define the standards by which the different pieces of the J2EE platform communicate with each other and with remote entities. The J2EE platform supports the following

Internet protocols:

- TCP/IP—Transport Control Protocol over Internet Protocol. These two protocols provide for the reliable delivery of streams of data from one host to another. Internet Protocol (IP), the basic protocol of the Internet, enables the unreliable delivery of individual packets from one host to another. IP makes no guarantees as to whether the packet will be delivered, how long it will take, or if multiple packets will arrive in the order they were sent. The Transport Control Protocol (TCP) adds the notions of connection and reliability.

- HTTP 1.0—Hypertext Transfer Protocol. The Internet protocol used to fetch hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client.
- SSL 3.0—Secure Socket Layer. A security protocol that provides privacy over the Internet. The protocol allows client-server applications to communicate in a way that cannot be eavesdropped or tampered with. Servers are always authenticated and clients are optionally authenticated.

Remote Method Invocation Protocols

Remote Method Invocation (RMI) is a set of APIs that allow developers to build distributed applications in the Java programming language. RMI uses Java language interfaces to define remote objects and a combination of Java serialization technology and the Java Remote Method Protocol (JRMP) to turn local method invocations into remote method invocations. The J2EE platform supports the JRMP protocol, the transport mechanism for communication between objects in the Java language in different address spaces.

Object Management Group Protocols

Object Management Group (OMG) protocols allow objects hosted by the J2EE platform to access remote objects developed using the OMG's Common Object Request Broker Architecture (CORBA) technologies and vice versa. CORBA objects are defined using the Interface Definition Language (IDL).

An application component provider defines the interface of a remote object in IDL and then uses an IDL compiler to generate client and server stubs that connect object implementations to an Object Request Broker (ORB), a library that enables CORBA objects to locate and communicate with one another. ORBs communicate with each other using the Internet Inter-ORB Protocol (IIOP). The OMG technologies required by the J2EE platform are Java IDL and RMI- IIOP.

Java IDL

Java IDL allows Java clients to invoke operations on CORBA objects that have been defined using IDL and implemented in any language with a CORBA mapping. Java IDL is part of the J2SE platform. It consists of a CORBA API and ORB. An application component provider uses the idlj IDL compiler to generate a Java client stub for a CORBA object defined in IDL. The Java client is linked with the stub and uses the CORBA API to access the CORBA object.

RMI-IIOP

RMI-IIOP is an implementation of the RMI API over IIOP. RMI-IIOP allows application component providers to write remote interfaces in the Java programming language. The remote interface can be converted to IDL and implemented in any other language that is supported by an OMG mapping and an ORB for that language. Clients and servers can be written in any language using IDL derived from the RMI interfaces. When remote interfaces are defined as Java RMI interfaces, RMI over IIOP provides interoperability with CORBA objects implemented in any language.

RMI-IIOP contains:

The rmic compiler, which generates: - Client and server stubs that work with any ORB. An IDL file compatible with the RMI interface. To create a C++ server object, an application component provider would use an IDL compiler to produce the server stub and skeleton for the server object. A CORBA API and ORB. Application clients must use RMI-IIOP to communicate with enterprise beans.

MySql

MySQL is a relational database management system, which organizes data in the form of tables. MySQL is one of many databases servers based on RDBMS model, which manages a seer of data that attends three specific things-data structures, data integrity and data manipulation. With MySQL cooperative server technology, one can realize the benefits of open, relational systems for all the applications. MySQL makes efficient use of all systems resources, on all hardware architecture; to deliver unmatched performance, price performance and scalability. Any DBMS to be called as RDBMS has to satisfy Dr.E.F.Codd's rules.

Distinct Features of MySql:

- MySQL is Portable:
- The MySQL RDBMS is available on wide range of platforms ranging from PCs to super computers and as a multi user loadable module for Novel NetWare, if you develop application on system you can run the same application on other systems without any modifications.
- MySQL is Compatible:
- MySQL commands can be used for communicating with IBM DB2 mainframe RDBMS that is different from MySQL, that is MySQL compatible with DB2.

MySQL RDBMS is a high performance fault tolerant DBMS, which is specially designed for online transaction processing and for handling large database applications.

Multithreaded Server Architecture:

MySQL adaptable multithreaded server architecture delivers scalable high performance for very large number of users on all hardware architecture including symmetric multiprocessors (sumps) and loosely coupled multiprocessors. Performance is achieved by eliminating CPU, I/O, memory and operating system bottlenecks and by optimizing the MySQL DBMS server code to eliminate all internal bottlenecks

Most popular RDBMS in the market because of its ease of use

- Client/server architecture.
- Data independence.
- Ensuring data integrity and data security.
- Managing data concurrency.
- Parallel processing support for speed up data entry and online transaction processing used for applications.
- DB procedures, functions and packages

5.7.4 Dr. E. F. OCDD's Rules

These rules are used for valuating a product to be called as relational database management systems. Out of 12 rules, a RDBMS product should satisfy at least 8 rules +rule called rule 0 that must be satisfied.

Rule 0: Foundation Rule:

For any system that is to be advertised as, or claimed to be relational DBMS. That system should manage database with in self, without using an external language.

Rule 1: Information Rule

All information in relational database is represented at logical level in only one way as values in tables.

Rule 2: Guaranteed Access

Each and every data in a relational database is guaranteed to be logically accessibility by using to a combination of table name, primary key value and column name.

Rule 3: Systematic Treatment of null values

values are supported for representing missing information and inapplicable information.

They must be handled in systematic way, independent of data types.

Rule 4: Dynamic Online Catalog Based Relation Model

The database description is represented at the logical level in the same way as ordinary data so that authorized users can apply the same relational language to its interrogation as they do to the regular data.

Rule 5: Comprehensive Data Sub Language

A relational system may support several languages and various models of terminal use. However, there must be one language whose statement can express all of the following: Data Definitions, View Definitions, Data Manipulations, Integrity, Constraints, and Authorization and transaction boundaries.

Rule 6: View Updating

Any view that is theoretically that updatable if changes can be made to the tables that effect the desired changes in the view.

Rule 7: High Level Update, Insert and Delete

The capability of handling a base relational or derived relational as a single operand applies not only retrieval of data also to its insertion, updating, and deletion.

Rule 8: Physical Data Independence

Application program and terminal activities remain logically unimpaired whenever any changes are made in either storage representation or access method.

Rule 9: Logical Data Independence

Application programs and terminal activities remain logically unimpaired whenever any changes are made in either storage representation or access methods.

Rule 10: Integrity Independence

Integrity constraints specific to particular database must be definable in the relational data stored in the catalogue, not in application program.

Rule 11: Distributed Independence

Whether or not a system support data base distribution, it must have a data sub-language that can support distributed databases without changing the application.

Rule 12: Non Sub-Version

If a relational system has low level language, that low language cannot use to subversion or by pass the integrity rules and constraints expressed in the higher level.

MySql Supports the Following Codd's Rules:

Rule 1: Information Rule (Representation of information)-YES.

Rule 2: Guaranteed Access-YES.

Rule 3: Systematic treatment of Null values-YES.

Rule 4: Dynamic on-line catalog-based Relational Model-YES.

Rule 5: Comprehensive data sub language-YES.

Rule 6: View Updating-PARTIAL.

Rule 7: High-level Update, Insert and Delete-YES.

Rule 8: Physical data Independence-PARTIAL.

Rule 9: Logical data Independence-PARTIAL.

Rule 10: Integrity Independence-PARTIAL.

Rule 11: Distributed Independence-YES.

Rule 12: Non-subversion-YES.

Chapter 6

IMPLEMENTATION

Implementation deals with the detailed specification of the concept with all the modules that are used in the approach.

6.1 RFID Module

When a user enters the voting booth he/she has to scan RFID Card on RFID reader. Once the RFID card is scanned on the RFID reader, the Arduino waits to receive for a character from MatLab.

The pseudo code is shown below.

```
if(!(strcmp(buff,"$00021281" )))
{
    Serial.print("VALID PERSON 1");
    Serial.print("Face recognition waiting.....");
    While(1)
    {
        FACE_VERIFYING_1();    //receives the character from MatLab
        WIFI_UPLOAD_RFID1();    //uploads to the RFID Aurdino
        WIFI_READ();
    }
}
```

Once the RFID receives the character, it verifies the character by comparing with the character obtained from the RFID card. If both the character matches, then RFID uploads it to a server. Void FACE_VERIFYING_1(void)

```
{
    x= Serial.read();
    Switch(x)
    {
        case 'A':    Serial.print("Valid User");
                    WIFI_UPLOD_RFID1();//Function used to upload the character to
                    an server
                    Break;
    }
```

```
        case 'B':      Serial.print("Invalid User");
                        loop();
                        break;
    }
}
```

The WIFI_UPLOAD_RFID1 () function is used to update the character to the server.

6.2 Face Recognition Module

The face recognition of a voter is done by using PCA algorithm by using the MatLab software.

The pseudo code for Face Recognition using PCA is given below:

The pseudo-code for PCA is as follows:

- Set image resolution parameter 4 (imres)
- Set PCA dimensionality parameter (PCADIM)
- Read training images
- Form training data matrix (Mtraindata)
- Form training class labels matrix (Mtrainlabels)
- Calculate PCA transformation matrix (tmatrix)
- Calculate feature vectors of all training images using tmatrix
- Store training feature vectors in a matrix
- Read test faces
- For each test face do
 - Calculate the feature vector of a test face using t matrix
 - Compute the distances between test feature vector and all training vectors
 - Store the distances together with the training class labels
 - Initialize error count to zero.
 - For each test face do
 - Using the distance data, determine the person ID of the most similar training vector
 - If the found ID is not equal to the ID of the test image increment error count
 - Output the correct recognition accuracy: $(1 - (\text{error count} / \text{total test image count})) * 100$

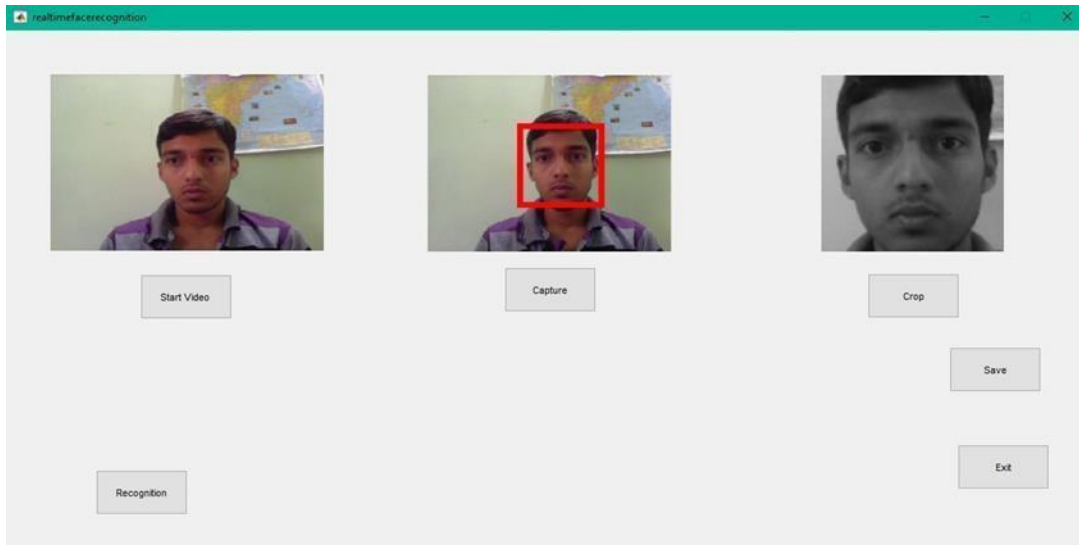


Fig.5.1. Capturing and cropping of Face

To start a webcam to make a video and to take snapshot of an image and to set a resolution of an image.

The pseudo code is given below

```
{  
    vidobj = videoinput('winvideo', 1, 'YUY2_320x240');    // to take an video as an input  
    vidRes = get(vidobj, 'VideoResolution');    // To set the resolution of an video  
    handles.webcam_image = getsnapshot(handles.vidobj); // To get a snapshot from an video  
    handles.imgCrop = crop_image(handles.webcam_image, 1);    //To crop an obtained  
    image  
}
```

Training the PCA algorithm by providing train data set:

Pseudo code to train the PCA algorithm

```
{  
    TrainImage = inputdlg(prompt,dg_title,num_lines,def); // giving input to train data  
    TrainImage = strcat(TrainDatabasePath,'\char(TrainImage)'.jpg); //path to store train  
    img  
}
```

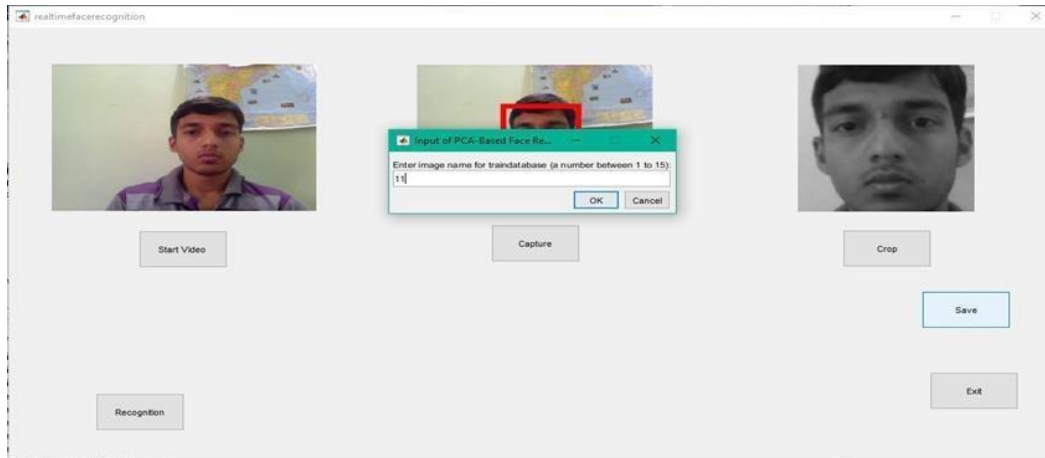


Fig.5.2 Training the PCA Algorithm

Pseudo code for selecting the Face image of voter from the train data is given below

```
{
    if index<6% && nose_eye1_diff<124&& nose_eye1_diff>120 && nose_eye2_diff<125
    && nose_eye2_diff>120
    disp('Person 1 matched')
    axes(handles.axes1);
    imshow(SelectedImage);
    title('Equivalent Image using PCA');
    d='Person1 matched';
    set(handles.text2,'string',d);
    fwrite(s,'A')
}
```

// if the values obtained from the face recognition matched with the trained data set

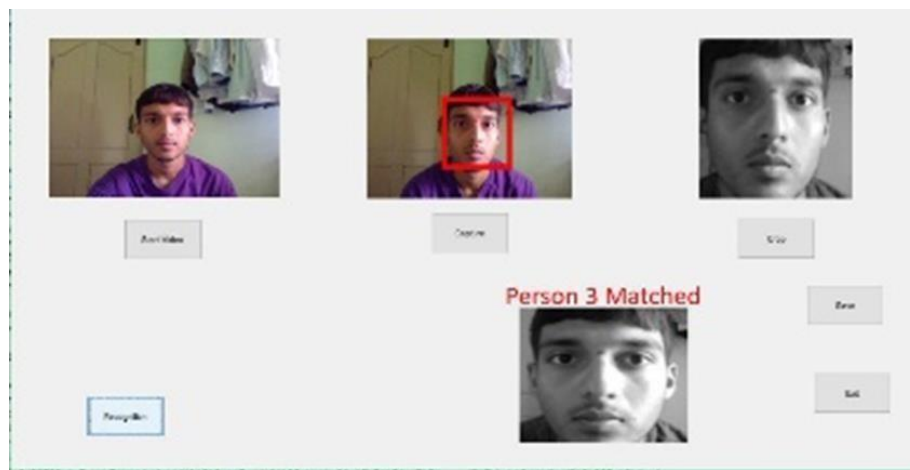


Fig.5.3. Face authentication using PCA algorithm

6 Fingerprint Module:

7

8 This is a finger print sensor module with TTL UART interface. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 Microcontroller. A level converter (like MAX232) is required for interfacing with PC.

9 R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions.

10 The R307 fingerprint module has two interface TTL UART and USB2.0, USB2.0 interface can be connected to the computer; RS232 interface is a TTL level, the default baud rate is 57600, can be changed, refer to a communication protocol; can and microcontroller, such as ARM, DSP and other serial devices with a connection, 3.3V 5V microcontroller can be connected directly. Needs to connect the computer level conversion, level conversion note, embodiments such as a MAX232 circuit.

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26 Pinouts :**27**

Pin# Pin Name Details

1 5V Regulated 5V DC

- 2 GND Common Ground
- 3 TXD Data output - Connect to MCU RX
- 4 RXD Data Input - Connect to MCU TX
- 5 TOUCH Active Low output when there is touch on sensor by finger
- 6 3.3V Use this wire to give 3.3V to sensor instead of 5V

28 USB Cable Connections are 5V/D+/D-/GND (Optional)

29

30 Features:

31

32

- 33 • Supply voltage: DC 4.2 ~ 6.0V
- Supply current: Working current: 50mA (typical) Peak current: 80mA
- Fingerprint image input time: <0.3 seconds
- Window area: 14x18 mm
- Matching method: Comparison method (1: 1)
- Search method (1: N)
- Characteristic file: 256 bytes
- Template file: 512 bytes
- Storage capacity: 1000 pieces
- Security Level: Five (from low to high: 1,2,3,4,5)
- Fake rate (FAR): <0.001%
- Refusal rate (FRR): <1.0%
- Search time: <1.0 seconds (1: 1000 hours, mean value)
- Host interface: UART \ USB1.1
- Communication baud rate (UART): (9600xN) bps Where N = 1 ~ 12 (default N = 6, ie 57600bps)
- Working environment: Temperature: -20 °C - +40 °C Relative humidity: 40% RH-85% RH (no condensation)
- Storage environment: Temperature: -40 °C - +85 °C Relative humidity: <85% H (no condensation)

6.3 Voting Module

To permit a voter to vote the booth level officer has to provide Login to server through web page by Logging in.

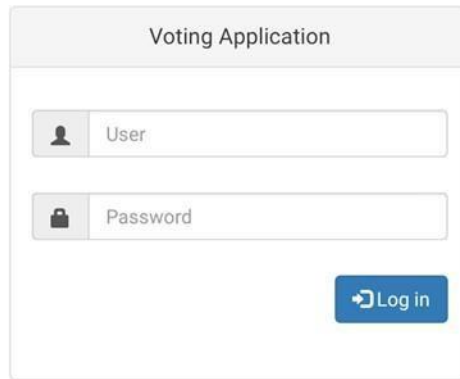


Fig.5.4. Login page for booth level officer

Pseudocode for login web page and redirecting to the respective voter voting page

```
@RequestMapping(value = "/login", method = RequestMethod.GET)
Public ModelAndView showLogin(HttpServletRequest request, HttpServletResponse response)
{
    ModelAndView mav = new ModelAndView("login");
    mav.addObject("login", new Login()); //For new login
    return mav;
}

@ModelAttribute("login") Login login, HttpSession session) {
    if(login.getUsername().equalsIgnoreCase("admin") &&
    login.getPassword().equalsIgnoreCase("admin")) {
        int id1 = userService.getVotingUser();
        System.out.println("id1===="+id1);
        if(id1 == 1) {
            return new ModelAndView("redirect:/user1"); //redirecting to the
            respective user page
        }
    }
}
```

Voter's voting page with status:

Pseudocode to check the user status

```
VoterUser voterUser = new VoterUser();  
    int status=0;  
    voterUser.setStatus(1);  
    if(Name.equalsIgnoreCase("a")){  
        voterUser.setVoterId(1);  
        status = userService.getStatus(1);//updating the user respective character to the  
        web page  
    }  
    if(status !=2 ) {  
        userService.updateVotingUser(voterUser);//if user is already voted then it has to  
        display that vote caste status  
    }  
}
```

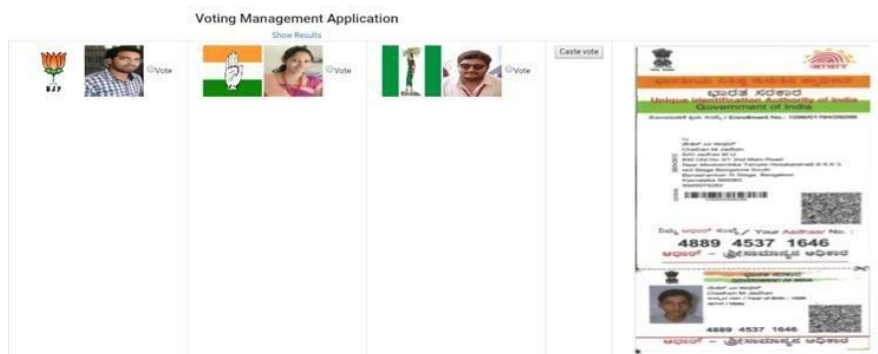


Fig.5.5 Voter's voting page



Fig.5.6 Representing status of voter after voting and if tries to revote

Chapter 7

TESTING AND RESULTS

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable faults or weakness in a work product. It provides a way to check the functionality of component, sub-assemblies, assemblies and a finished product. It is a process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner.

7.1 Unit Testing

Unit testing is a software development process in which the smallest testable parts of an application, called Unit. A unit is the smallest testable part of any software. It usually has one or a few inputs and usually a single output.

TEST CASE 1:

TABLE V

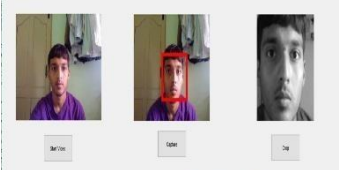

Test Case for Admin Log IN Still if No User Authenticated

INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
Admin should Log In with out any User Authenticated	Should Display “No User Authenticated” on web page.	<small>Show Results</small> No User Authenticated	Pass


TEST CASE 2:

TABLE VI



Test Case for Face Recognition Authentication

INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
	Should Display the Matched person from the Trained Data Set.		Pass

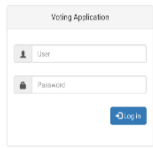

TEST CASE 3:**Table VII****Test Case to Pop Up the Voter's Voting Window after Authentication and Admin Log In**

INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
The matched Character from RFID and Face Recognition is sent to the Server and Admin is Logged In.	The Web page should Display the respective Voter's Aadhaar Card and Provide a "Vote Cast" button to Vote.		Pass

TEST CASE 4:**Table VIII****Test Case for After Vote Casted by Voter**


INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
	The Web Page should show "Vote Casted Successfully" in the place of "Vote Cast" Button.		Pass

TEST CASE 5:**Table IX****Test Case for Admin Login after Voter Casted Vote and Logged Out**

INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
	Should display a message "No User Authenticated" on Web page.		Pass

TEST CASE 6:

Table X
Test Case for When Voter tries to Revote

INPUT	ACTUAL OUTPUT	EXPECTED OUTPUT	RESULT
The matched Character from RFID and Face Recognition is sent to the Server and Admin is Logged In.	The Web page should Display the respective Voter's Aadhaar Card and Message "Vote Casted Successfully".		Pass

7.2 Functional Testing

Functional Testing is a software testing process used within software development in which software is tested to ensure that it conforms to all requirements. Functional testing is a way of checking software to ensure that has all the required functionality that's specified within its functional requirements.

The Voter enters the booth with the RFID card. Voter Swipes the RFID card on RFID reader, the RFID reader reads the respective character stored in the card and waits to receive the character from MatLab for face recognition. Once after the character sent from the MatLab, the RFID reader will Uploads the respective character to the server if both the character is same. If both the character is not same then it won't send the character to the web page. Once it uploads to the server the admin gives login to the web page then the respective voter's web page will pop up on window with vote button. After voting the message will be displayed as vote casted successfully.

Advantages and Applications

- Elimination of fraud votes
- Cost savings
- Faster counts
- Economical
- Tamper proof storage
- Machines are easily accessible
- Scanned fingerprint can be used for Govt applications

Applications:

- Can be used for college and university election
- Used for applications such as ration card, driving license and many more
- Used inside the parliament
- Used to maintain account in the bank

CONCLUSIONS

The proposed method is to develop a secure internet voting system based on face recognition which tried to overcome all the drawback occurs in traditional or current voting system. The proposed system has many strong features like correctness, verifiability, convenience etc. For this system no requirement of an election officer, paper ballot or any electronic voting machine only the internet connection and Face scanners are required one can vote from anywhere securely.

The proposed system provides two phase of authentication. First is through RFID and second is Face Recognition and third is fingerprint recognition. In this system no voter can vote twice because the voters fingerprint, Facial patterns will be linked to their Aadhaar Card. So that any user tries to vote twice with some other person's RFID card it is not possible due to RFID linked to the Aadhaar card and the respective Fingerprint and Facial Patterns stored in data storage will not be matched with the Voter trying to voting with some other person's RFID.

Also the proposed method provides the voter to vote from any region with in India to their Residential Constituency from the nearest Voting Booth with a secure voting process without neglecting to vote.

Future Enhancement

- Future EVM
- Socket to PC interface
- Password to access the count value
- Touch screen as ballot unit
- Photo verification

REFERENCES

- [1]. Alaguvel.R, Gnanavel.G, Jagadhambal.K “Biometrics using Electronic Voting System with Embedded Security”.
- [2]. D.Jennifer, S.K.akshaya, J.ash3, H.swethasalaksshi “Aadhaar based electronic voting system and providing authentication on INTERNET OF THINGS” International Journal of Engineering Science & Advanced Technology, volume-4, Issue-2.
- [3]. The 8051 Micro controller and Embedded Systems- Muhammad Ali Mazidi and Janice Gillespie Mazidi.
- [4]. Programming and Customizing the 8051 Microcontroller-Predko.
- [5]. Prof. Pritika, V. Mamankar, Prof. Sonika A, Prof. Rachana S “Face Recognition Using Principal Component Analysis”. IJSER, volume 7, issue2, February-2016.
- [6]. General information about electronic voting machine

Links Referred:

www.eci.gov.in

www.eci.gov.in/faq/evm.asp

www.eci.gov.in/Audio_VideoClips/presentation/EVM.ppt

www.rajasthan.net/election/guide/evm.htm

www.indian-elections.com/electoralsystem/electricvotingmachine.html