SECUREGAZE - EYE-TRACKING PASSWORD AUTHENTICATION SYSTEM

A DISSERTATION II REPORT

Submitted by

ARUNVENKATESH M
(Reg.No. 720722208002)

in partial fulfillment for the award of the degree

of

MASTER OF ENGINEERING

In

EMBEDDED SYSTEMS

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY
An Autonomous Institution, Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai
Accredited by NBA (AERO, AUTO, CIVIL, CSE, ECE, EEE, IT, MECH, MCTS)
Accredited by NAAC 'A++' Grade with CGPA of 3.69 out of 4 in Cycle 2
Valley Campus, Coimbatore – 641 032, Tamil Nadu, India.

JULY 2024

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHOLOGY

An Autonomous Institution, Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai
Accredited by NBA (AERO, AUTO, CIVIL, CSE, ECE, EEE, IT, MECH, MCTS)
Accredited by NAAC 'A++' Grade with CGPA of 3.69 out of 4 in Cycle 2
Valley Campus, Coimbatore – 641 032, Tamil Nadu, India.

BONAFIDE CERTIFICATE

Certified that this project report **"SECUREGAZE - EYE-TRACKING PASSWORD AUTHENTICATION SYSTEM"** is the bonafide work of "**ARUNVENKATESH M"** who carried out the project work under my supervision.

Signature of the Supervisor

SUPERVISOR
Mr.JOSHUA DANIEL S, M.E., (Ph.D).,
Assistant Professor,
Department of Electrical and Electronics Engineering,
Hindusthan College of Engineering and Technology,
Coimbatore – 641032.

Signature of the Head of the Department

HEAD OF DEPARTMENT
Dr. N.P. ANANTHAMOORTHY, M.E., Ph.D.,
Professor & Head
Department of Electrical and Electronics Engineering,
Hindusthan College of Engineering and Technology,
Coimbatore – 641032.

Submitted for Autonomous a Dissertation II Examination project viva-voce examination conducted on …….

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

I express my sincere thanks to **Hindusthan Educational and Charitable Trust** for providing us the necessary facilities to bring out the project successfully. We feel grateful to our thanks to our **Chairman Shri. T.S.R. KHANNAIYANN**, and **Smt. SARASUWATHI KHANNAIYANN,** HICET for all their support and ray of strengthening hope extended.
I extend my thanks to my **CEO Dr. K. KARUNAKARAN, Ph.D.,** for his constant support and motivation.

I am grateful to our **Principal Dr JAYA J, M.E., Ph.D.,** for her invaluable support in enabling us to come out with this project.

At this moment I take this opportunity to convey our deepest regards and sincere thanks to **Dr. N.P. ANANTHAMOORTHY, M.E., Ph.D., Head of the Department**, Electrical and Electronics Engineering for the technical guidance.

I am highly indebted to our **Project Supervisor Mr. JOSHUA DANIEL S, M.E., (Ph.D).,** Assistant Professor, Electrical and Electronics Engineering Department, for his cooperation and valuable guidance from beginning of the project.

I express our grateful thanks to our **Department Project Co-Ordinator Dr MATHAN K, M.E., Ph.D.,** Associate Professor, Electrical and Electronics Engineering Department, for his timely suggestions and encouragement throughout the project.

I deeply express my gratitude to all the faculty members of Department of Electrical and Electronics Engineering, for their encouragement which we received throughout the semester.

I thank all our non-teaching staffs, parents, friends and Almighty God without whose support and blessings, I would never have completed this project.

ABSTRACT

Nowadays Personal Identification Numbers (PIN) are widely used for security and authentication purposes. PIN requires users to enter the manually, which could be an alpha-numeric passcode used as user accessing system, this can be possible to crack the password using Shoulder surfing or Thermal tracking methods.

Shoulder surfing is the technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on the device or sensitive information. So, that are facing security issues, and it is becoming very difficult to overcome this problem.

Thermal tracking is a technique that creates an image using infrared radiation that forms an image using visible light. The practice of capturing and analyzing the data is called thermography. This technique is easy and can see through the PIN which that once enter in ATM or in any other organization which contains PIN-based techniques.

For this problem Gaze based authentication which means to enter the PIN without entering the password manually i.e., Hands off gaze based personal identification number. This technique improves the level of security and helps us to build more authentication for the system.

In Gaze based authentication, will be based on the eye location and eye movement at the different instances of action of the human eye. This is presenting real-time application for PIN entry based on Gaze technique. Using the smart camera, PINs are identified by detecting and tracking the movement of the eye.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

In the prevailing ATM system though the Credit card paves convenient mode of transactions, it is subjected to more jeopardy. As technology extends its limit, the way of hacking and cracking also goes along the road. In this proposed system, in every transaction with the Credit card a handshaking signal is achieved with the cardholder.

The handshaking method is achieved by transferring the transaction details to the mobile of the cardholder by means of a Wi-Fi. From the acknowledgement and authentication received from the cardholder's mobile further transaction proceeds. The message from the cardholder is the major authentication command. At first, the ATM was made to transact for the bank customers but later on the ATMs are connected to interbank network, so that it enables people to deposit, withdraw and transfer amount from the ATM machines not belonging to that particular bank i.e. anyone can access any banks ATM machine to carry out their transactions.

ATMs rely on authorization of a financial transaction by the card issuer or other authorizing institution via the communication network. This is often performed through an ISO 8583 messaging system. Many bank charges ATM usage fees from the customers for the transactions. At present every customer has an individual ATM card for each bank in which he/she maintains account. So, handling the cards, their passwords play a major role here. So, to overcome these difficulties we embedded more than one bank account of the user in a single ATM smart card, so that the user can swipe the card and can select the bank from which he/she are interested to carry out transaction.

In this project, microcontroller accompanied with an interface circuit has been used for ATM transactions fingerprint which is stored in microcontroller itself so that

only authorized person will access the security lock. Introducing concept of synchronization for special form of communication in which control information is exchanged, instead of data, between communicating process residing in the same or different process. Synchronization enforces correct sequencing of processors and ensures mutually exclusive access to shared writable data. Synchronization can be implemented in software, firmware, and hardware through controlled sharing of data and control information in memory. The idea behind this smart card is that the customers can use a single smart card to operate different bank accounts instead of having individual card for each bank account and maintaining their pin's, carrying the cards safely which is a tedious process at present scenario. The technology behind the product of the service is that adding all the user bank accounts to a universal smart card. In this the user swipes his/her smart card in the ATM machine, it requests for authentication on the server side. During this, the data of the user are encrypted and decrypted. A camera which acts as a Eye Tracker is used for authentication process. Once the user is authenticated, then it displays the list of all banks that the user is having account. Now the user can select the bank from which he/she is willing to perform transaction. After selecting the bank, the request is sent to the corresponding bank through a network and links it with the banks server for accessing the database of the user or customer so that the transaction is processed. For unauthorized users there will be a concept of Wi-Fi.

1.2 MOTIVATION

Main Motivation for this project is to avoid frauds happening in bank or other safety zones. Eye Trackers provides better security compared to any other methods. There is a need to provide an Eye Tracking solution which would allow persons with motor disabilities to interact with devices or communicative devices without being exhausted using wearable devices day long. Nowadays everyone could see many cases

of theft from banking sector, it is because of the Personal Identification Number authentication or keypad password. There are many ways to get to know others password, one of that is dropping the silica gel powder coating on the keypad and knowing which all keys were pressed by the user. Another case which happened was "A camera was placed near the keypad inside the ATM machine ", shoulder surfing is most used kind for knowing others password.

All these disadvantages of keypad authentication motivated us to do this project, which increases the security level compared to the keypad password.

1.3 PROBLEM STATEMENT

Keypad based systems which are very easy to hack or easily recognizable. Voice controlled password which is not secure as it can mimicked by others. Hand controlled or gesture-controlled systems where physical movement is required, which will be inconvenient to users. Most of them are sensor dependent systems which are inaccurate with the results obtained.

1.4 OBJECTIVE

Designing a system for tracking face and eye using camera by taking facial image points and retina images respectively. Facial detection using Haar feature-based cascade classifier is an effective object detection method. It is an machine leaning based approach where a cascade function is trained a lot of positive and negative images. It is then used to detect objects in other image

Here that will work with face detection. Initially the algorithm needs a lot of positive images (images with face) and negative images (images without faces) to train the classifier. Then should need to extract features from it. Each feature is a single value obtained by subtracting sum of pixels under the white rectangle from sum of pixels under black rectangle. These are the objectives of this project.

1.5 ORGANIZATION

The Chapter 1 gives a brief description of introduction to the project, motivation which is the major cause of developing this project, problem statement for which this model was developed as a solution. The Chapter 2 gives description of various literature papers referred which helped to gain knowledge of various concepts that could be used to develop the model of this project. The Chapter 3 gives a description of the various Hardware and Software tools necessary to build the model. The Chapter 4 gives detailed description of the generalized methodology for developing the project containing architectures, Data flow diagrams, Flowcharts, etc. The Chapter 5 gives detailed explanation of various algorithms necessary to implement and used to obtain the model. The Chapter 6 concludes the project briefly along with the scope the model can obtain in the future so that it can be used to overcome the odds in the existing system.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

The literature survey chapter provides a comprehensive analysis of existing research papers and journals pertaining to the utilization of gaze pin entry for password authentication using eye tracking. Through a critical and concise examination of earlier studies and literature on eye tracking and eye detection, that have incorporated relevant findings into our project. This chapter outlines the methodology employed, specifically the Haar cascade detection technique, which enables the detection of facial landmarks and subsequently the identification of the eye region. Additionally, also have integrated simulation software to assess the suitability of the detected face and incorporated other pertinent parameters utilized by researchers in our project implementation. By synthesizing and building upon prior research, our study aims to contribute to the advancement of gaze-based password authentication systems.

2.2 LITERATURE SURVEY

The chapter consists of the literature survey of pre-existing research papers and journals relating to the gaze pin entry for password authentication using eye tracking. In this survey, have analyzed critically, and concisely earlier research and literature related to eye tracking, eye detection and utilized them in our project. This chapter gives description of the methodology- Haar cascade detection technique, and made use of the facial landmark to detect the face and then the eye region, simulation software to verify if the face is appropriate or not and also other related parameters which are used by the research is implemented in our project.

2.2.1 SURVEY PAPER ON EYE GAZE TRACKING METHODS AND TECHNIQUES

Puja sorate, Prof. Mrs. G. J. Chhajed "Survey *Paper On Eye Gaze Tracking Methods And Techniques*" International Research Journal of Engineering and Technology e-ISSN: 2395 -0056 Volume: 04 Issue: 06 June -2017.

Face is the key to mind and eyes are the window to the person. Eye movements provide rich information to a person.

The study of eye movement helps to determine people where they are looking. Eye tracking is the measure of eye movement and gaze tracking is the analysis of eye tracking info and head movement info.

The gaze tracking applications like in robotics, psychological studies, cognitive science.

In psychological studies, gaze tracking applications are used to measure behavioral responses. In computer vision as an input device and in making as a tool to obtain optimum location to place an advertisement.

The main application of neuroscience is Eye tracking and is well-organized time and effectual cost, as well as low problem and compare with other neurological methods.

Eye tracking helps the neuroscience Eye movements, such as fixation and smooth pursuit, Visual processing, interaction between eye movements, vision, and performance tasks Object-by-object search mechanisms in attention studies, Eye movement patterns in visual neglect, Neurological functions involved in perceptual decision making.

Attention and brain imaging have been investigated neuroscience.

2.2.2 DESIGN TOWARD EVERYDAY GAZE INPUT: ACCURACY AND PRECESION OF EYE TRACKING AND IMPLICATION FOR DESIGN

Anna Maria Feit1, Shane Williams, Arturo Toledo, Ann Paradiso, Harish Kulkarni, Shaun, Merdith Ringel Morris, Aalto University, Microsoft Research, Toledo "*Design Toward Everyday Gaze Input: Accuracy and Precesion Of Eye Tracking And Implication of Design*" Journal of Eye Movement Research 8,1(2017).

To establish eye gaze as part of everyday interaction with computers, it needs to understand the characteristics and limitations of eye tracking in practice and derive standards for the design of gaze-enabled applications that consider that accuracy and precision can vary widely across different tracking conditions.

It collects calibration style eye tracking data from 80 participants, using two different trackers in two lighting conditions.

In contrast to many eye tracking studies, It does not exclude any participant due to insufficient tracking quality and only calibrated once at the beginning. Finding several contributions for the design and development of gaze- enabled applications:

1. Checking the accuracy and precision ranges overall and for different parts of the screen that characterize the large variation across different tracking conditions.

2. Provides a formal way to derive appropriate target sizes from measures of accuracy and precision. Based on the data the recommendations are given for the minimum size of gaze-aware regions to allow robust interaction.

3. An approach to find optimal parameters for any filter that minimizes target size and signal delay.

2.2.3 EYE TRACKING USING GAZE PIN ENTRY FOR PASSWORD AUTHENTICATION

Mrs. Pavitra S R, Mrs. Pushpalatha S "*Eye Tracking Using Gaze Pin Entry For Password Authentication*", International Journal Innovative Technology and Exploring Engineering, June 2020

In this paper, it comprises of 4 projections for recognizing of eye that are Edge-Projection, Luminance Projection, Chrominance Projection, and Final Projection. This project work was easy and tricky to use and has a more secure approach to enter their pin contrasted with the conventional pin section technique than any other normal techniques.

2.2.4. ityping USING EYE GAZE TO ENHANCE TYPING PRIVACY

Zhenjiang Li1 , Mo L , Prasant Mohapatra , Jinsong Han , Shuaiyu Chen, "*Ityping USING EYE GAZE TO ENHANCE TYPING PRIVACY*",2017.

Mobile devices offer us the most convenient user experience ever, e.g., at anytime and anywhere, but it is unavoidable to face a new potential threat at the same time. The interaction between users and mobile devices may be exposed to public directly, which may leak very sensitive information of the user, e.g., passwords, private data, account information, etc. If the input of such information is not properly protected, the user's privacy can be easily emanated and compromised in public. To overcome this issues iTyping system is proposed. iTyping is for entering the private information using the eye gaze. In iType, the keyboard consists of multiple buttons and each button represents unique character(s) (number or letter).

For the ease of presentation ,it refers password to various kinds of private information for short. To type a password, the user looks at the corresponding buttons

sequentially, and iType essentially solves a decoding puzzle it reads the user's gaze, infers the buttons being looked at, and assembles the password. The iTyping is secure primarily due to the fact that the eye gaze is difficult to eavesdrop. Even an adversary in front of the user could decode the eye gaze, the gaze itself conveys no meaningful information, unless it matches with the keyboard layout, which however can be user-defined and changed.

Advantages:

- iType that uses eye gaze to enhance typing privacy on commodity mobile devices.
- iType system overcomes a challenges accuracy, latency and mobility.

Limitations:

- Quite low precision of gaze tracking for mobiles.
- Issues in the correction of the input errors because of a lack in comparing of the value the true text-entry value.
- The movement of the device along with other noises which could be interfering the precision of the gaze tracking and therefore the efficiency of the iType.

2.2.5 REAL_TIME EYE GAZE DIRECTION CLASSIFICATION USING CONVOLUTIONAL NEURAL NETWORK

Anjith George, Aurobinda Routray, "*Real_Time Eye Gaze Direction Classification Using Convolutional Neural Network*". arXiv:1605.05258v1 [cs.CV] 17 May 2016

Human emotions and cognitive states are essential in developing a natural human-computer interaction system (HCI). Systems which can identify the affective and cognitive states of humans can make the interaction more natural. The knowledge of mental processes can help computer systems to interact intelligently with humans.

Estimation eye gaze direction is useful in various human-computer interaction tasks. Knowledge of gaze direction can give valuable information regarding user's point of attention. A real time framework which can detect eye gaze direction using low-cost cameras in desktops and other smart devices. Estimation of gaze location from webcam often requires cumbersome calibration procedure. Gaze direction classification as a multi-class classification problem, avoiding the need for calibration. The eye directions obtained can be used to find the EAC and thereby infer the user's cognitive process. The information obtained can be useful in the analysis of interrogation videos, human-computer interaction, information retrieval, etc.

The highlights of this system are shown below:

1. Proposes a real-time framework for eye gaze direction classification.

2. Convolutional Neural Network based gaze direction classifier, which is robust against eye localization errors.

3. The proposed approach outperforms state of the art algorithms in gaze direction classification.

The algorithm achieves an average frame rate of 24 fps in desktop environment.

Advantages:

- Increasing the accuracy of eye gaze direction classification.
- Algorithm is robust against noise, blur, and localization errors.
- CNN can improve the accuracy.

Limitations:

The computational complexity of the algorithm in testing phase is less, which makes it suitable for smart devices with low resolution cameras using pre-trained models.

2.2.6 GAZE TOUCH PASS SCHEME

Mohamed, Florian, Mariam, Emanuel, Regina and Andreas "*Gaze Touch Pass Scheme*". The 34th ACM SIGCHI Conference on Human Factors in Computing Systems CHI 2016, At San Jose, CA, USA. May 2016

With mobile devices enabling ubiquitous access to sensitive information, there is a need to protect access to such devices. Meanwhile, authentication schemes are prone to shoulder surfing attacks, where a bystander observes a user while authenticating. The attacker then gets hold of the device and tries to authenticate and access sensitive data. To overcome this attacks Gaze Touch Pass, a multimodal authentication scheme in which user define four symbols, each can be entered either via touch (a digits between 0 and 9) or via gaze (gazing to the left and to the right). Consecutive gaze inputs to the same direction would then need to be separated by a gaze to the front and switches between input modalities are used within a single password.

Advantages:

- Gaze Touch Pass is particularly secure against side attack.
- Gaze Touch Pass achieves a balance between security and usability, with low authentication times and high observation resistance.
- Gaze Touch Pass is faster and can work on off-the-shelf mobile devices without additional hardware.
- Gaze Touch Pass shows that multimodal passwords are significantly more secure than single modal ones.

Limitations:

- It's applicable only for mobile devices.
- Gaze Touch Pass can be particularly useful as a secondary authentication mechanism that users can choose to opt to when feeling observed (e.g. public setting),or when accessing critical data (e.g. online banking).

CHAPTER 3
REQUIRED TOOLS

3.1 SOFTWARE REQUIREMENTS

There are few software's that have to be installed for the working of the project model. A brief description of software's and step-by-step procedure for installation of these software's is explained in the following subsection.

3.1.1 COMPUTER VISION

Computer vision is a process by which could understand the images and videos how they are stored and how that can manipulate and retrieve data from them. Computer Vision is the base or mostly used for Artificial Intelligence. Computer Vision is playing a major role in self-driving cars, robotics as well as photo correction apps.

3.1.2 OPEN CV

OpenCV is the huge open-source library for computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's system. By using it, one can process images an videos to identify objects, faces, or even handwriting of a human. When it integrated with various libraries, such as NumPy, python is capable of processing the OpenCV array structure for analysis. To identify image pattern and its various features that use vector space and perform mathematical operations on these features.

The first OpenCV version was 1.0 OpenCV and is released under a BSD license a hence it is free for both academic and commercial use. It has C++, C, Python and Java interfaces and support. Windows, Linux, Mac OS, iOS and Android. When OpenCV was designed the main focus was a real-time application for computational

efficiency. All things are written in optimized C/C++ to take advantage of multi-core processing.

The first alpha version of OpenCV was released to the public at the Conference on Computer Vision and Pattern Recognition in 2000, and five betas were released between 2001 and 2005. The first 1.0 version was released in 2006. A version 1. "pre-release" was released in October 2008.

3.1.3 OPEN CV-PYTHON

OpenCV-Python is a library of Python bindings designed to solve computer vision problems. Python is a general-purpose programming language started by Guido van Rossum that became very popular very quickly, mainly because of its simplicity and code readability. It enables the programmer to express ideas in fewer lines of code without reducing readability. Compared to languages like C/C++, Python is slower. That said, Python can be easily extended with C/C++, which allows us to write computationally intensive code in C/C++ and create Python wrappers that can be used as Python modules.

This gives us two advantages: first, the code is as fast as the original C/C++ code (since it is the actual C++ code working in background) and second, it easier to code in Python than C/C++. OpenCV-Python is a Python wrapper for the original OpenCV C++ implementation.

OpenCV-Python makes use of NumPy, which is a highly optimized library for numerical operations with a MATLAB-style syntax. All the OpenCV array structures are converted to and from NumPy arrays. This also makes it easier to integrate with other libraries that use NumPy such as SciPy and Matplotlib.

3.1.4 OPENCV FUNCTIONALITY

- Image/video I/O, processing, display (core, imgproc, highgui)

- Object/feature detection (objdetect, features2d, nonfree)
- Geometry-based monocular or stereo computer vision (calib3d, stitching, videostab)
- Computational photography (photo, video, superres)
- Machine learning & clustering (ml, flann) CUDA acceleration (gpu)

3.1.5 PROGRAMMING LANGUAGE

Python is an interpreted, high-level and general-purpose programming language. Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear logical code for small and large-scale projects.

Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured(particularly, procedural), object-oriented and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.

Python was created in the late 1980s, and first released in 1991, by Guido van Rossum as a successor to the ABC programming language. Python 2.0, released in 2000, introduced new features, such as list comprehensions, and a garbage collection system with reference counting, and was discontinued with version 2.7 in 2.20.

Python 3.0, released in 2008, was a major revision of the language that is not completely backward compatible an much Python 2 code does not run unmodified on Python 3. With Python 2's end-of-life, only Python 3.6x and later are supported, with older versions still supporting. E.g. Windows 7(and old installers not restricted to 64-bit Windows).

Python interpreters are supported for mainstream operating systems and available for a few more (and in the past supported many more). A global community of programmers develops and maintains CPython, a free and open-source reference

implementation. A non-profit organization, the Python Software Foundation, manages and directs resources for Python and CPython development. As of December 2020 Python ranked third in TIOBE's index of most popular programming languages, behind C and Java.

Python's large standard library, commonly cited as one of its greatest strengths, provides tools suited to many tasks. For Internet-facing applications, many standard formats and protocols such as MIME and HTTP are supported. It includes modules for creating graphical user interfaces, connecting to relational databases, generating pseudorandom numbers, arithmetic with arbitrary-precision decimals, manipulating regular expressions, and unit testing.

3.1.6 IMAGE PROCESSING

Image processing is the technique to convert an image into digital format and perform operations on it to get an enhanced image or extract some useful information from it. Changes that take place in images are usually performed automatically and rely on carefully designed algorithms.

Image processing is a multidisciplinary field, with contributions from different branches of science including mathematics, physics, optical and electrical engineering. Moreover, it overlaps with other areas such as pattern recognition, machine learning, artificial intelligence and human vision research. Different steps involved in image processing include importing the image with an optical scanner or from a digital camera, analyzing and manipulating the image (data compression, image enhancement and filtering), and generating the desired output image.

The need to extract information from images and interpret their content has been the driving factor in the development of image processing. Image processing finds use in numerous sectors, including medicine, industry, military, consumer electronics and soon.

In medicine, it is used for diagnostic imaging modalities such as digital radiography, positron emission tomography (PET), computerized axial tomography (CAT), magnetic resonance imaging (MRI) and functional magnetic resonance imaging (fMRI). Industrial applications include manufacturing systems such as safety systems, quality control and automated guided vehicle control.

Complex image processing algorithms are used in applications ranging from detection of soldiers or vehicles to missile guidance and object recognition and reconnaissance. Biometric techniques including fingerprinting, face, iris and hand recognition are being used extensively in law enforcement and security. Digital cameras and camcorders, high-definition TVs, monitors, DVD players, personal video recorders and cell phones are popular consumer electronics items using image processing.

Digital cameras and camcorders, high-definition TVs, monitors, DVD players, personal video recorders and cell phones are popular consumer electronics items using image processing.

3.1.7 ARDUINO IDE

Arduino is a prototype platform (open source) based on an easy-to-use hardware and software. It consists of a circuit board, which can be programmed (referred to as a microcontroller) and a ready-made software called Arduino IDE (Integrated

Development Environment), which is used to write and upload the computer code to the physical board. Arduino provides a standard form factor that breaks the functions of the micro- controller into a more accessible package.

A program for Arduino may be written in any programming language for a compiler that produces binary machine code for the target processor. Atmel provides a development environment for their microcontrollers, AVR Studio and the newer Atmel Studio.

The Arduino project provides the Arduino integrated development environment (IDE), which is a cross-platform application written in the programming language Java. It originated from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus.

A program written with the IDE for Arduino is called a sketch. Sketches are saved on the development computer as text files with the file extension .ino. Arduino Software (IDE) pre-1.0 saved sketches with the extension .pde.

The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub main() into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution. A minimal Arduino C/C++ sketch, as seen by the Arduino IDE programmer, consist of only two functions:

- **setup():** This function is called once when a sketch starts after power-up or reset. It is used to initialize variables, input and output pin modes, and other libraries needed in the sketch.
- **loop():** After setup() has been called, function loop() is executed repeatedly in the main program. It controls the board until the board is powered off or is reset.

Arduino - Installation

After learning about the main parts of the Arduino UNO board, that are ready to learn how to set up the Arduino IDE.

In this section, will learn in easy steps, how to set up the Arduino IDE on our computer and prepare the board to receive the program via USB cable.

Step 1 − First you must have your Arduino board (you can choose your favorite board) and a USB cable. In case you use Arduino UNO, Arduino Duemilanove, Nano, Arduino Mega 2560, or Diecimila, you will need a standard USB cable (A plug to B plug), the kind you would connect to a USB printer as shown in the following Figure 3.1.

Figure 3.1: USB Printer Cable

In case you use Arduino Nano, you will need an A to Mini-B cable instead as shown in the following Figure 3.2.

Figure 3.2: USB Mini-B Cable

Step 2 − Download Arduino IDE Software.

You can get different versions of Arduino IDE from the Download page on the Arduino Official website. You must select your software, which is compatible with your operating system (Windows, IOS, or Linux). After your file download is complete, unzip the file as shown in the Figure. 3.3.

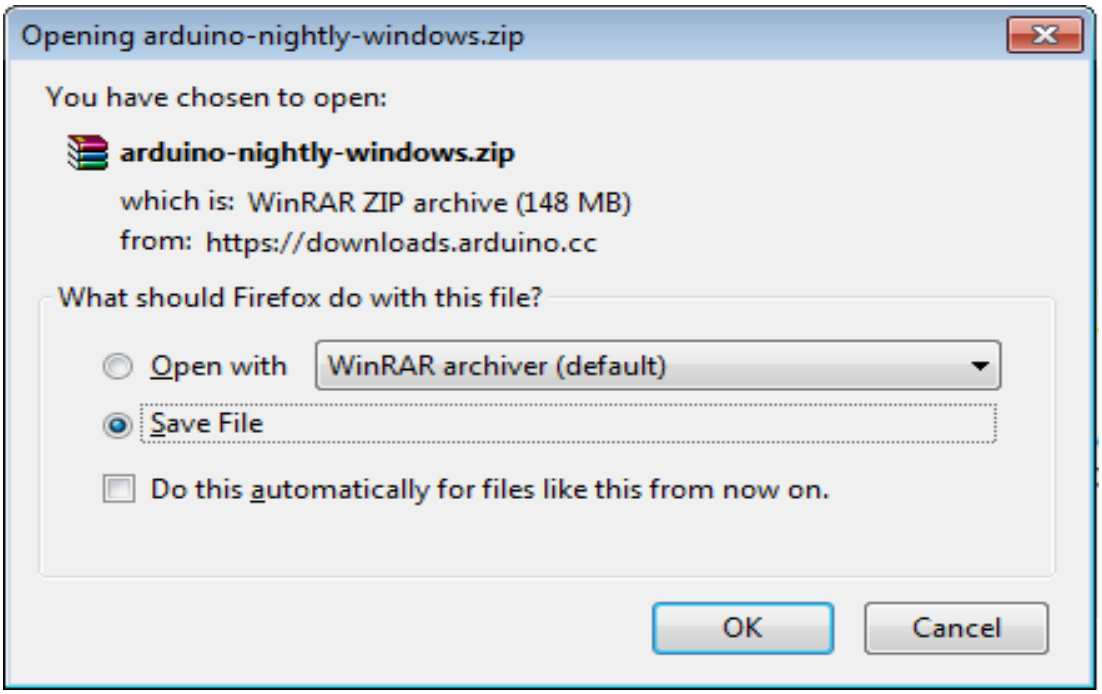


Figure 3.3: Arduino IDE Unzip Window

Step 3 − Power up your board.

The Arduino Uno, Mega, Arduino Nano automatically draw power from either the USB connection to the computer or an external power supply. If you are using an Arduino, you have to make sure that the board is configured to draw power from the USB connection. The power source is selected with a jumper, a small piece of plastic that fits onto two of the three pins between the USB and power jacks. Check that it is on the two pins closest to the USB port.

Connect the Arduino board to your computer using the USB cable. The green power LED (labeled PWR) should glow.

Step 4 − Launch Arduino IDE.

After your Arduino IDE software is downloaded, you need to unzip the folder. Inside the folder, you can find the application icon with an infinity label (application.exe) as shown in the Figure 3.4. Double-click the icon to start the IDE.

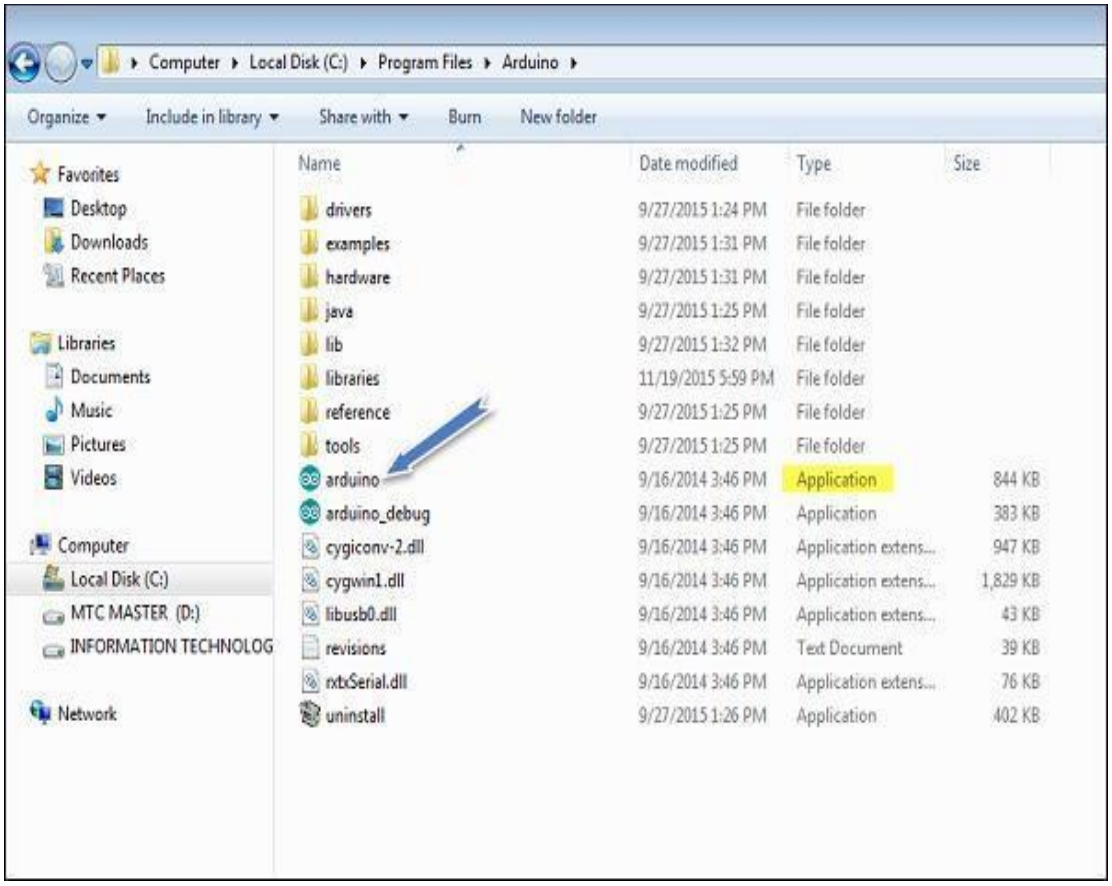


Figure 3.4: Windows Explorer Arduino IDE path

Step 5 − Open your first project.

Once the software starts, you have two options –

- Create a new project. Open an existing project example. To create a new project, select File → **New** as shown in the Figure 3.5.

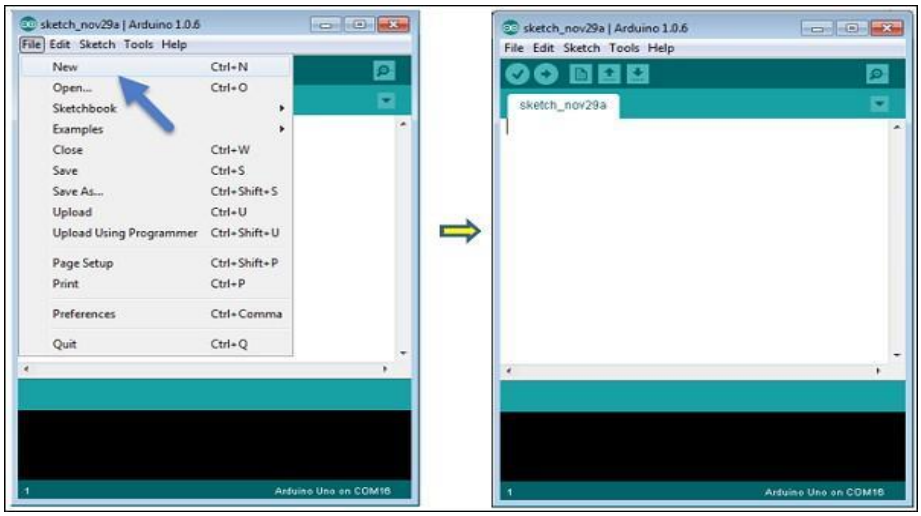
- 

Figure 3.5: Arduino IDE New project File Window

To open an existing project example, select File → Example → Basics → Blink as shown in the Figure 3.6.

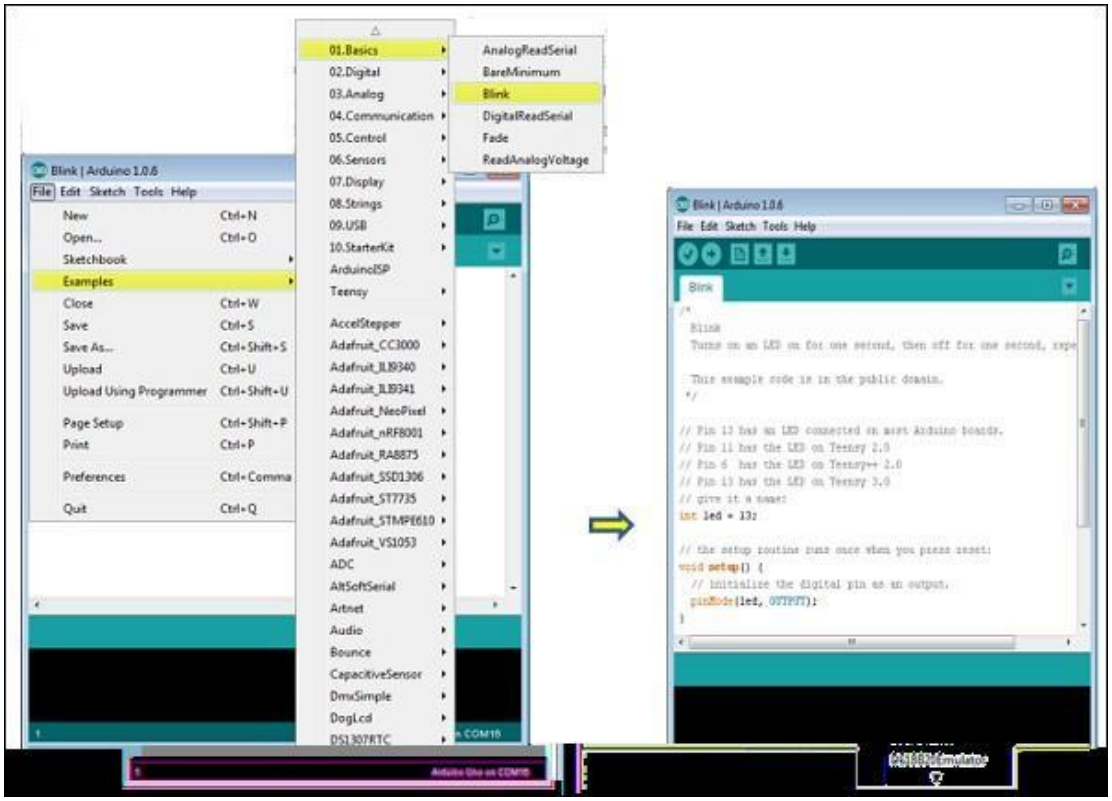


Figure 3.6: Arduino IDE Open project File Window

Here, Once are selecting just one of the examples with the name **Blink**. It turns the LED on and off with some time delay. You can select any other example from the list.

Step 6 − Select your Arduino board.

To avoid any error while uploading your program to the board, you must select the correct Arduino board name, which matches with the board connected to your computer.

Go to Tools → Board and select your board.

Here, also have selected Arduino Uno board according to our tutorial, but you must select the name matching the board that you are using.

Step 7 − Select your serial port.

Select the serial device of the Arduino board. Go to **Tools → Serial Port** menu. This is likely to be COM3 or higher To find out, you can disconnect your Arduino board and re-open the menu, the entry that disappears should be of the Arduino board. Reconnect the board and select that serial port.

Step 8 − Upload the program to your board.

Before explaining how can upload our program to the board, must demonstrate the function of each symbol appearing in the Arduino IDE toolbar.

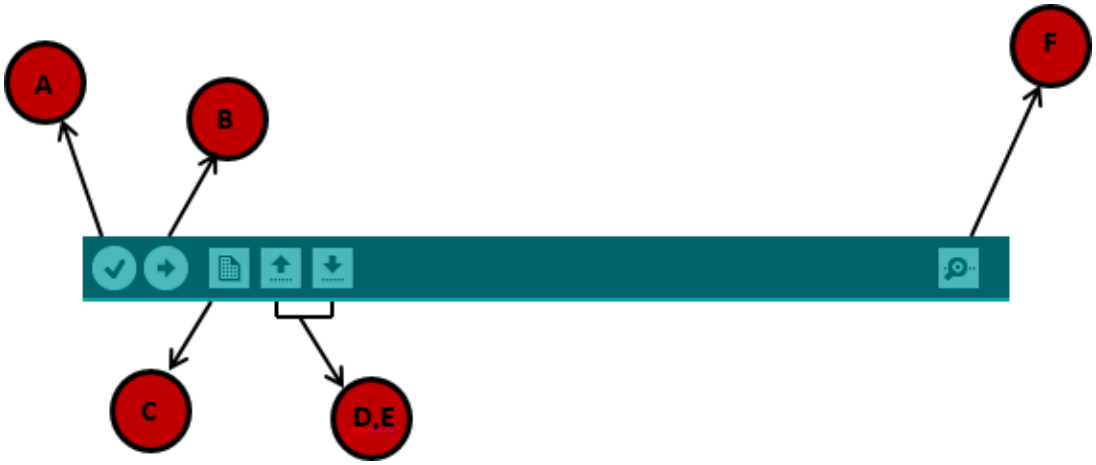


Figure 3.7: Arduino IDE upload program Window

A − Used to check if there is any compilation error. **B** − Used to upload a program to the Arduino board. **C** − Shortcut used to create a new sketch.

D − Used to directly open one of the example sketches.

E − Used to save your sketch.

F − Serial monitor used to receive serial data from the board and send the serial data to the board.

Now, simply click the "Upload" button in the environment. Wait a few seconds; you will see the RX and TX LEDs on the board, flashing. If the upload is successful, the message "Done uploading" will appear in the status bar as shown in the Figure 3.7.

3.1.8 Embedded C:

When designing software for a smaller embedded system with the 8051, it is very commonplace to develop the entire product using assembly code. With many projects, this is a feasible approach since the amount of code that must be generated is typically less than 8 kilobytes and is relatively simple in nature. If a hardware engineer is tasked with designing both the hardware and the software, he or she will frequently be tempted to write the software in assembly language.

The trouble with projects done with assembly code can is that they can be difficult to read and maintain, especially if they are not well commented. Additionally, the amount of code reusable from a typical assembly language project is usually very low. Use of a higher-level language like C can directly address these issues. A program written in C is easier to read than an assembly program.

Since a C program possesses greater structure, it is easier to understand and maintain. Because of its modularity, a C program can better lend itself to reuse of code from project to project. The division of code into functions will force better structure of the software and lead to functions that can be taken from one project and used in another, thus reducing overall development time.

A high order language such as C allows a developer to write code, which resembles a human's thought process more closely than does the equivalent assembly code. The developer can focus more time on designing the algorithms of the system rather than having to concentrate on their individual implementation. This will greatly reduce development time and lower debugging time since the code is more understandable.

By using a language like C, the programmer does not have to be intimately familiar with the architecture of the processor. This means that someone new to a given processor can get a project up and running quicker, since the internals and organization of the target processor do not have to be learned. Additionally, code developed in C will be more portable to other systems than code developed in assembly. Many target processors have C compilers available, which support ANSI C.

All of this is not to say that assembly language does not have its place. In fact, many embedded systems (particularly real time systems) have a combination of C and assembly code. For time critical operations, assembly code is frequently the only way to go. One of the great things about the C language is that it allows you to perform low-level manipulations of the hardware if need be, yet provides you the functionality and abstraction of a higher order language.

3.2 HARDWARE REQUIREMENTS

There are few hardware components required to develop the project model. A brief description of all the hardware components used along with their configurations is explained in the following subsection.

3.2.1 ARDUINO MEGA 2560:

The main reason behind this is the additional features that are inbuilt with this board. First feature is the large I/O system design with inbuilt 16 analog transducers

and 54 digital transducers that supports with USART and other communication modes all details are shown in the table 3.1 Secondly, it has inbuilt RTC and other features like analog comparator, advanced timer, interrupt for controller wakeup mechanism to save more power and fast speed with 16 MHz crystal clock to get 16 MIBS. It has more than 5 pins for Vcc and Gnd to connect other devices to Arduino Mega.

Other features include JTAG support for programming, debugging and troubleshooting. With large FLASH memory and SRAM, this board can handle large system program with ease. It is also compatible with the different type of boards like high-level signal (5V) or low-level signal (3.3V) with I/O ref pin. Brownout and watchdog help to make the system more reliable and robust. It supports ICSP as well as USB microcontroller programming with PC and details are shown in table 3.2.

The Arduino Mega 2560 shown in the Figure 3.8, is a replacement of the old Arduino Mega, and so in general reference, it will be called without the '2560' extension. Due to the many numbers of pins, it is not usually used for common projects but you can find them in much more complex ones like Radon detectors, 3D printers, temperature sensing, IOT applications, real-time data monitoring applications etc.

Figure 3.8: Arduino Mega 2560

Table 3.1: Arduino Mega 2560 Specifications

Arduino Mega	Features
Microcontroller	AVR AT mega 2560 (8bit)
Power Supply	7-12V (Inbuilt Regulator for Controller)
Digital I/O Pins	54
Analog I/O Pins	16
Total Digital I/O	70 (Digital + Analog)
Clock Speed	16 MHz (Factory set to 1Mhz)
Flash Memory	128 KB
SRAM	8 KB
Communication	USB (Programming with AT mega 8), ICSP (programming) SPI, I2C and USAR

Table 3.2: Advanced Features of Arduino Mega

Arduino Mega	Advanced Features
Timer	2 (8bit) + 4 (16bit) = 6 timer
PWM	12 (2-16 bit)
ADC	16 (10 bit)
USART	4
Pin Change Interrupt	24

Arduino Mega Pinout

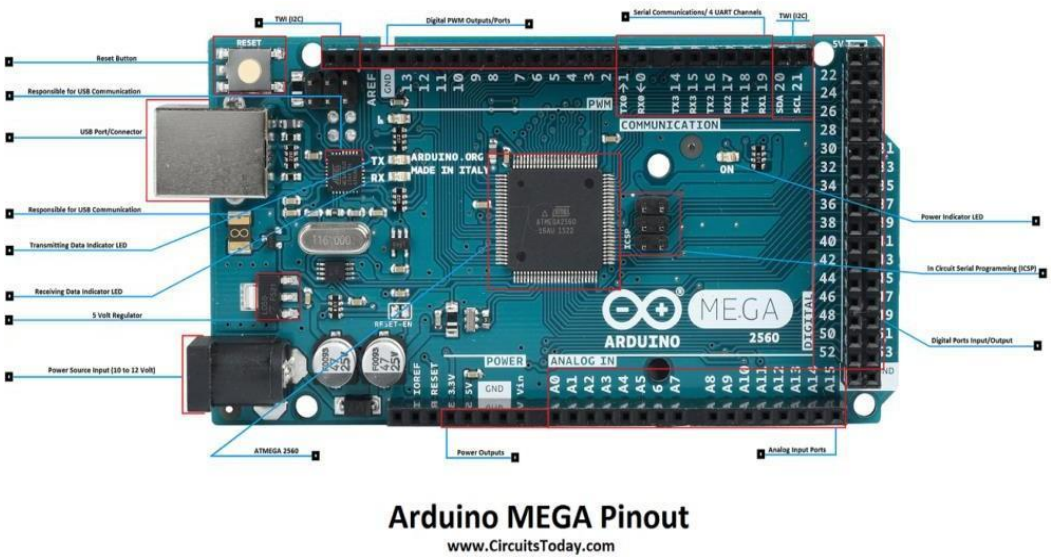


Figure 3.9 Arduino Mega Pinout

Analog Pins (16):

Analog pins: From 0-15(analog) can be used as analog input pin for adc, if not used than it work as normal digital pin. It can be used by pin Mode() for pin direction, analog Read() to read pin status and get digital value for analog signal. Pinout are shown in the Figure 3.9.

Application:

Input devices: Ntc thermistor, sensors (like ldr, irled and humidity) and others

Table 3.3: Arduino Power pins

Arduino Mega	Power Pins
VIN	Supply voltage (7-12V)
GND	Ground
5V Supply	For External hardware device power supply
3.3V Supply	For External low voltage hardware device power supply

SPI Pins:

Pin 22 – SS, Pin 23 SCK, Pin 24 – MOSI, Pin 25 - MISO

Application:

Programming AVR controller, communication with others peripheral like LCD and SD card with four-line communication at high speed.

I2C Pins:

Digital pin 20 for SDA and 21 for SCK (speed 400kHz) to enable two wire communication with other devices. Function used are wire.begin() to start I2C conversation, with wire.Read() to read I2C data and wire.Write() I2C data.

Applications:

Output devices : LCD and communication between multiple devices with two wire. Input devices : Rtc and others.

PWM Pins:

Digital pin 2-13 can be used as PWM output with analogWrite() to write PWM value from 0-255. It's alternative of DAC for low cost system to get analog signal at output by using filter.

Application:

Output devices: speed control of motor, light dimmer, pid for efficient control system.

USART Pins :

Pin 0 -RXD0, pin 1 -TXD0 Pin 19 – RXD1, pin18 – TXD1

Pin 17 – RXD2, pin 16 – TXD2 Pin 15 – RXD3, pin 14 -TXD3

This pin is used for serial usart communication with pc or other system for data sharing and logging. It is used with serialBegin() to set baud rate setting and start communication with serial.Println() to print array of char on other device output.

Application:

Two controller communication, pc and controller communication, debugging with usart by serial monitor.

Pin change Interrupt Pins:

This pin is used for pin change interrupt. Enable bit of pin change interrupt must be set with global interrupt enable.

Application:

Rotary encoder, push button-based interrupt and others.

Hardware Interrupt Pins:

Digital pin 18 – 21,2,3 hardware interrupt is used for interrupt services. Hardware interrupt must be enabled with global interrupt enable to get interrupt from other devices.

Application:

Push button for ISR program, wake up controller with external devices, sensors like ultrasonic and others.

Arduino Mega Schematic Components:

DC Jack Power Supply:

External Supply for Arduino Mega from range 7-12 volt is given with this port. Arduino Mega R3 has a voltage regulator for 5v and 3.3v supply for Arduino controller and sensor supply.

AVR 2560:

This is the main controller used to program and run task for the system. This is the brain of the system to control all other devices on board.

ATmega8 :

This controller is used for communication between the main controller and other devices. This controller is programmed for USB communication and serial programming features.

ICSP 1 (ATmega8) and 2 (AVR 2560):

It has features of programming using serial bus with AVR programmer using SPI communication. AVR 2560 shown in Figure 3.10, is programmed to run the system and AT mega 8 is programmed for serial communication and programming.

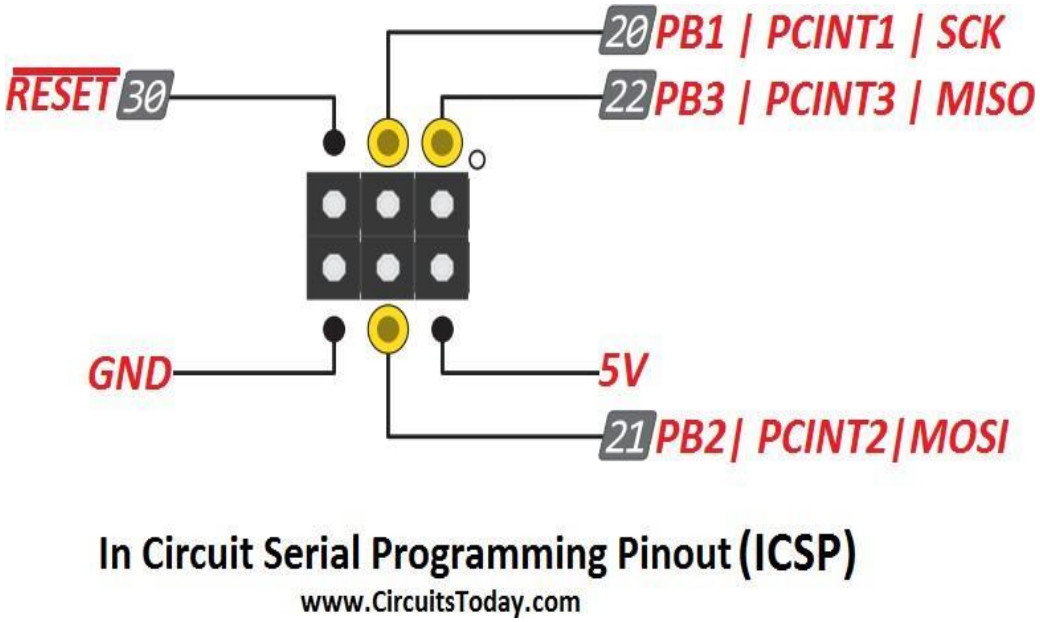


Figure 3.10: Mega ICSP Pinout for AT mega 2560

Reset:

It has reset circuit with capacitor, button and resistor to reset the controller. A push button is used to get 4 cycle low signal on reset pin to get the controller in reset mode.

Crystal :

It has a crystal circuit with two capacitors and one 16 MHz crystal for xtal pins 1 and 2 interfacing with avr 2560.

I2C:

It has features of I2C (two wire communication) with an external pull-up resistor.

USART:

It has TXD and RXD pin for serial communication with LED indicator.

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 flavors: 78xx for positive voltage output and 79xx for negative voltage output. For example, 7812 gives +12V output and 7912 gives - 12V stabilized output. These regulator ICs have in-built short-circuit protection and auto- thermal cutout provisions. If the load current is very high the IC needs ‘heat sink’ to dissipate the internally generated power.

Transformer:

A transformer is a device that transfers electrical energy from one circuit to another through inductively coupled conductors without changing its frequency. A varying current in the first or primary winding creates a varying magnetic flux in the transformer's core, and thus a varying magnetic field through the secondary winding. This varying magnetic field induces a varying electromotive force (EMF) or "voltage" in the secondary winding. This effect is called mutual induction. If a load is connected to the secondary, an electric current will flow in the secondary winding and electrical energy will be transferred from the primary circuit through the transformer to the load. This field is made up from lines of force and has the same shape as a bar magnet. If the

current is increased, the lines of force move outwards from the coil. If the current is reduced, the lines of force move inwards. If another coil is placed adjacent to the first coil then, as the field moves out or in, the moving lines of force will "cut" the turns of the second coil. As it does this, a voltage is induced in the second coil. With the 50 Hz AC mains supply, this will happen 50 times a second. This is called MUTUAL INDUCTION and forms the basis of the transformer.

Rectifier:

Rectifier is an electrical device that converts alternating current (AC) to direct current (DC), a process known as rectification. Rectifiers have many uses including as components of power supplies and as detectors of radio signals. Rectifiers may be made of solid-state diodes, vacuum tube diodes, mercury arc valves, and other components. A device that it can perform the opposite function (converting DC to AC) is known as an inverter. When only one diode is used to rectify AC (by blocking the negative or positive portion of the waveform), the difference between the term diode and the term rectifier is merely one of usage, i.e., the term rectifier describes a diode that is being used to convert AC to DC. Almost all rectifiers comprise a number of diodes in a specific arrangement for more efficiently converting AC to DC than is possible with only one diode. Before the development of silicon semiconductor rectifiers, vacuum tube diodes and copper (I) oxide or selenium rectifier stacks were used.

Filter:

The process of converting a pulsating direct current to a pure direct current using filters is called as filtration. Electronic filters are electronic circuits, which perform signal- processing functions, specifically to remove unwanted frequency components from the signal, to enhance wanted ones.

Regulator:

A voltage regulator (also called a _regulator ‘) with only three terminals appears to be a simple device, but it is in fact a very complex integrated circuit. It converts a varying input voltage into a constant _regulated ‘output voltage. Voltage Regulators are available in a variety of outputs like 5V, 6V, 9V, 12V and 15V. The LM78XX series of voltage regulators are designed for positive input. For applications requiring negative input, the LM79XX series is used. Using a pair of _voltage-divider‘ resistors can increase the output voltage of a regulator circuit. You cannot use a 12V regulator to make a 5V power supply. Voltage regulators are very robust. These can withstand over- current draw due to short circuits and also over-heating. In both cases, the regulator will cut off before any damage occurs. The only way to destroy a regulator is to apply reverse voltage to its input. Reverse polarity destroys the regulator almost instantly.

3.2.2S RFID HISTORY:

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, 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 Defense (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.

3.2.3 RFID CONCEPT:

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. 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.

The FOUR CORE Components of an RFID System

An RFID system has four basic components as shown in the Figure 3.11.

- 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.

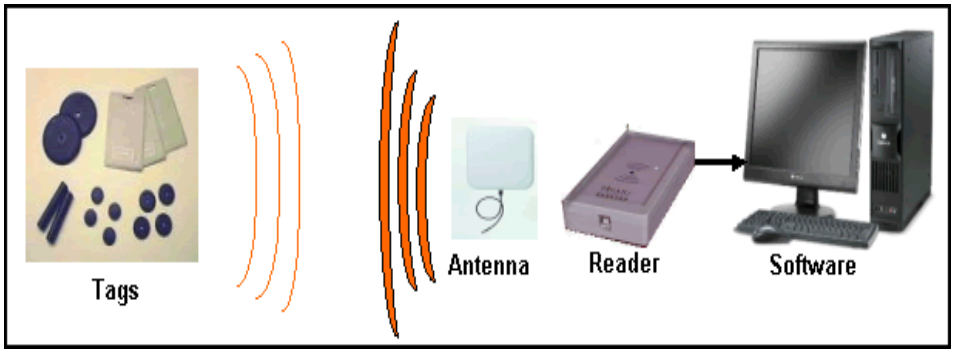


Figure 3.11: Basic Building blocks of an RFID system

3.2.4 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, such as a packing label that might be attached to a box. The components are shown in the Figure 3.12.

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

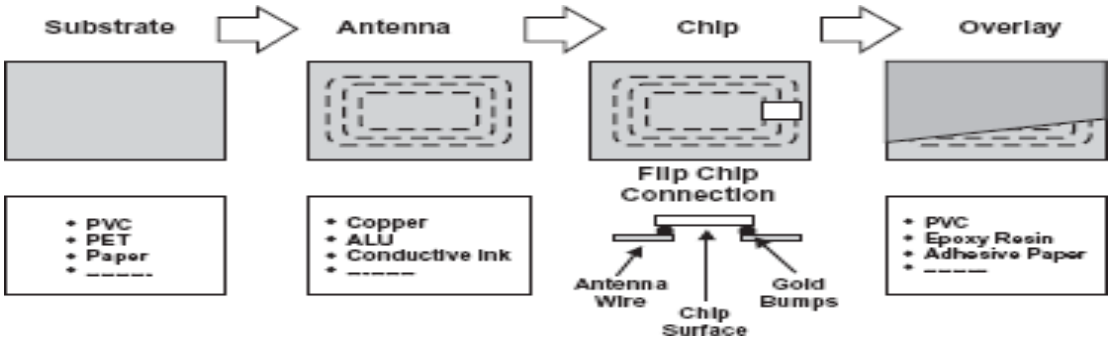


Figure 3.12: RFID Tag Components

3.2.5 TYPES OF TAGS AND READERS

RFID tags and readers can be grouped under several categories. Their classification is presented.

3.2.6 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 read as well 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.
- Proximity electromagnetic or inductive coupling - near field
- Generally, use LF and HF frequency bands.
- Propagating electromagnetic waves - far field

RFID Interrogators (Reader)

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

3.2.6 CLASSIFICATION 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.

- 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.

3.2.7 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.

Specifications:

Table 3.4: Specification of RFID

Frequency	125KHz
Reading distance	>=50
Interface	UART
Antenna	Built in/External
Supply Voltage	5V
Operating Temperature	-10°C to +50°C
Tag Types	Unique, TK 5530
Output Format	ASCII, Wiegand26

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. 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. It is also shown in the table 3.4.

Components of RFID Systems:

An RFID system is always made up of two components as shown in the figure 3.13.

- 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 3.6. 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.

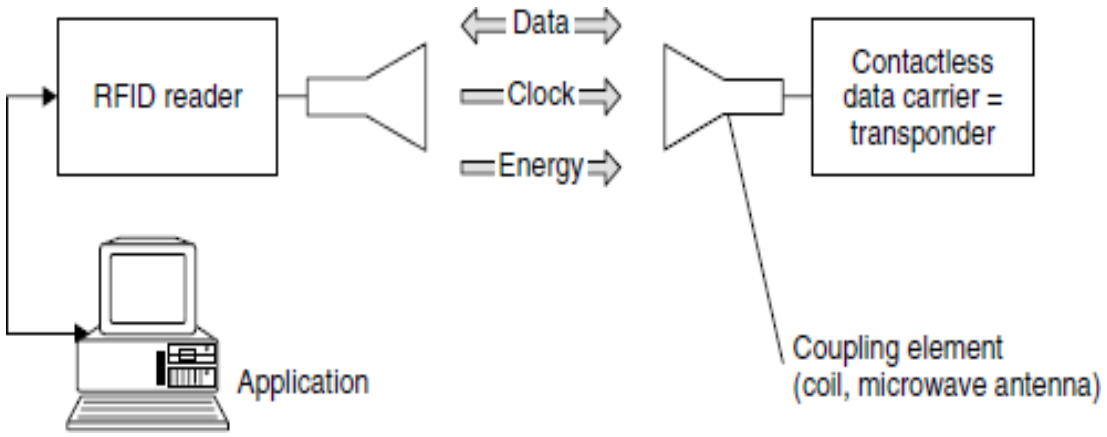


Figure 3.13: RFID System consisting of transponder and receiver.

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 shown in the Figure 3.14.

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 radio frequency (RF) procedure is based upon LC resonant circuits adjusted to a defined resonant frequency. Early versions employed inductive resistors made of wound enameled 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 aluminum conduction tracks on the 25μm thick polyethylene foil must be at least 50μm. Intermediate foils of 10μm 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 of the alternating field corresponds with the resonant frequency 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 because 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 shown in the Figure 3.15.

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).

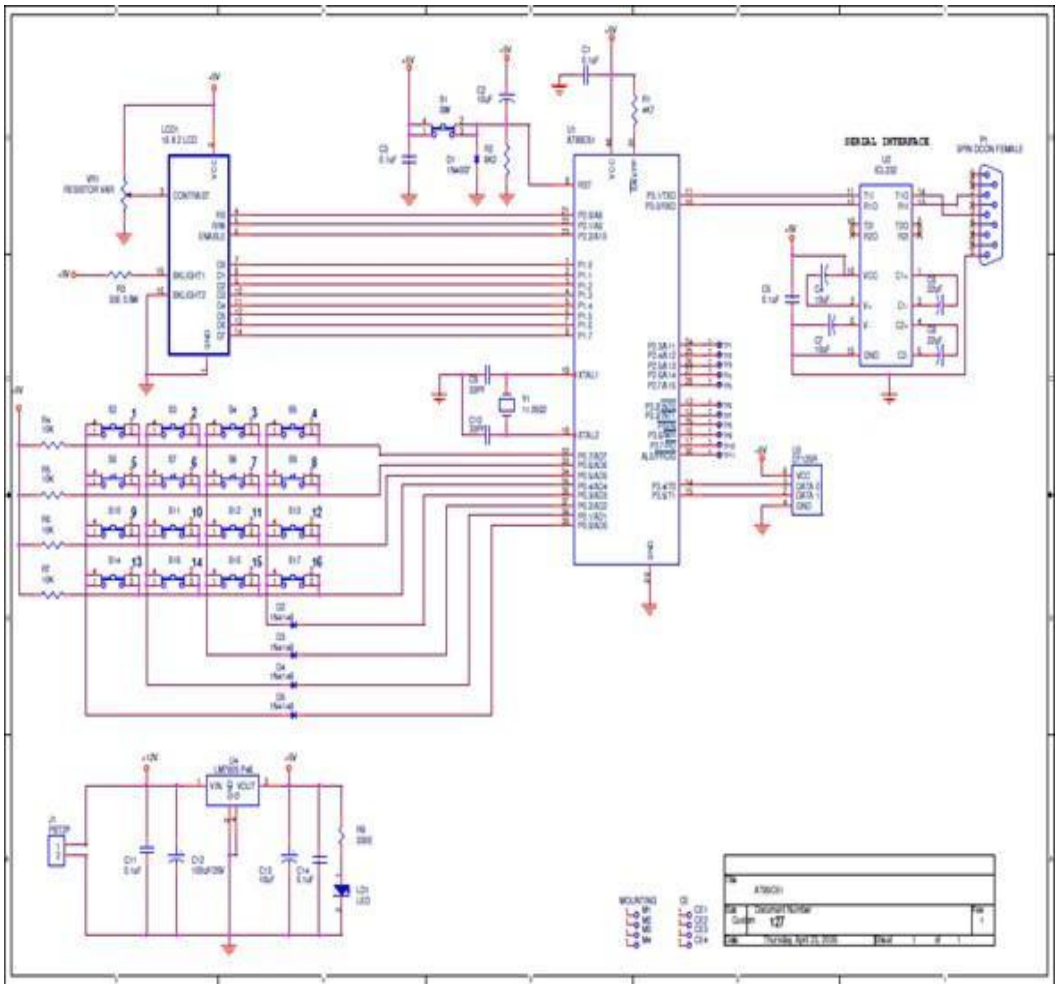


Figure 3.14: Schematic circuit diagram of RFID

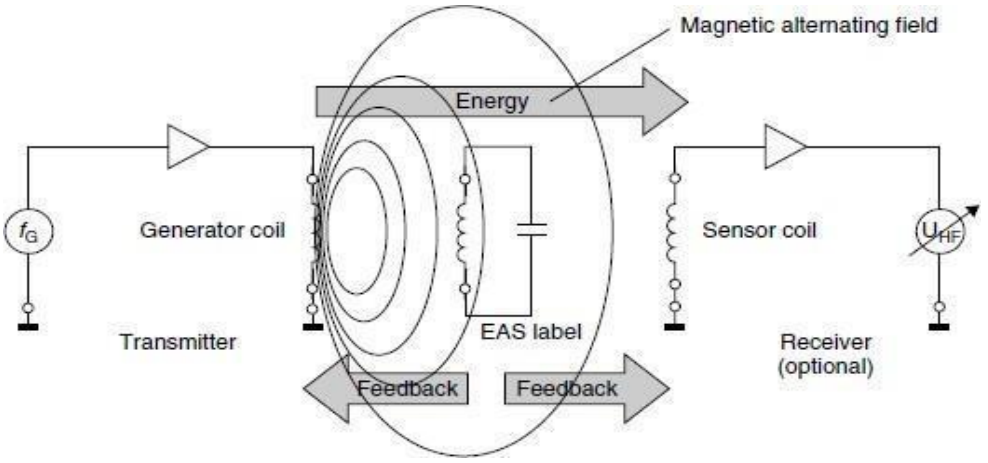


Figure 3.15: Operating principle of EAS radio frequency procedure.

3.2.8 LIQUID CRYSTAL DISPLAY:

A liquid-crystal display shown in the Figure 3.16 is a flat-panel display or other electronically modulated optical . LCDs are available to display arbitrary images or fixed images with low information content, which can be displayed or hidden. For instance: pre-set words, digits, and seven- segment displays, as in a digital clock, are all good examples of devices with these displays. LCDs can either be normally on (positive) or off (negative), depending on the polarizer arrangement. For example, a character positive LCD with a backlight will have black lettering on a background that is the colour of the backlight, and a character negative LCD will have a black background with the letters being of the same colour as the backlight. Optical filters are added to white on blue LCDs to give them their characteristic appearance.

In recent years the LCD is finding widespread use replacing LEDs this is due to following reasons:

1. The declining prices of LCDs.

2. The ability to display numbers, characters and graphics. This is in contrast to LEDs, which are limited to numbers and few characters.

3. Incorporation of a refreshing controller in to LCD, there by relieving the CPU of the task of refreshing the LCD. In contrast LCD must be refreshed by CPU to keep displaying the data.

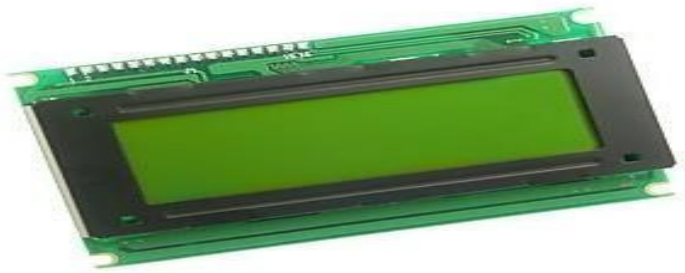


Figure 3.16: Liquid Crystal Display

Basic reading:

This section deals with the character-based LCD module which use Hitachi HD44780 controller chip. These modules are not quite as advanced as the latest generation, full size, full color, back lit types used in today's laptop computers, but far from being "phased out", Character based LCDs, are still used extensively in commercial and industrial equipment, particularly where display requirements are reasonably simple.

Shapes and sizes:

Even limited to character-based modules, there is still a wide variety of shapes and Sizes available. Line lengths 8, 16,2,024,32 and 40 characters are all standard, in one, two- and 4-lines versions.

Several different liquid crystal technologies based exist. "Supertwist" types, for Example, offer improved contrast and viewing angle over the older "twisted pneumatic" types. Some modules are available with backlighting, so that they can view in dimly lit conditions.

Connections:

A 14-pin access is provided having 8 data lines,3 control lines and 3 power lines. The connections are laid out in one of two common configurations, either two row of seven pins, or a single row of 14 pins shown in the Figure 3.17.

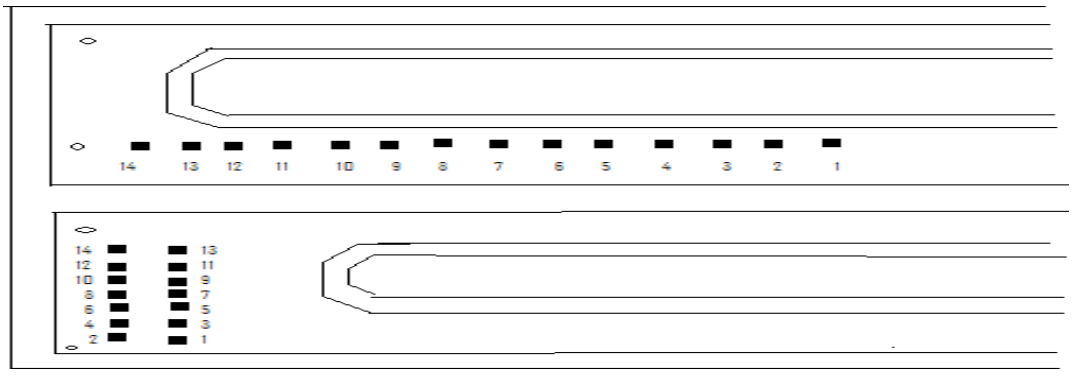


Figure 3.17: Pin out of the basic LCD formats.

On most displays, the pins are numbered on the LCD's PCB, but if not, it is quite easy to locate pin1.Since this pin is connected to ground, it often has a thicker PCB track connected to it and it is generally connected to the metal work at some point.

Pins 1 and 2 are the power supply lines, Vss and Vdd. The Vdd pin should be connected to positive supply and Vss to 0V supply or ground. Although the LCD module data sheets specify a 5VDC supply, supplies of 6V and 4-5V both works well, and even 3V is sufficient for some modules.

Pin 3 is a control pin, Vee, which is used to alter the contrast of the display. Ideally, this pin should be connected to a variable voltage supply.

Pin 4 is the (RS) register select line. When this line is low, data bytes transferred to the display are treated as commands and data bytes read from the display indicate its status. By setting the RS line high, character data can be transferred to and from the module.

Pin 5 is read/write line. This line is pulled low in order to write commands or character data to the module, or pulled high to read character data or status information from its registers.

Pin 6 is the enable line. This input is used to initiate the actual transfer of commands or character data between the module and the data lines. When writing to the display, data is transferred only on high to low transition of this signal.

Pin 7 to 14 are data bus lines (D0 to D7).data can be transferred to and from the display either as a single 8 bit byte or two 4 bit nibbles. The other two pins LED+ and LED- is used for back light of the LCD.

Now let us try to display a single character on LCD. When powered up, the display should show a series of dark squares, possibly on a part of the display. These character cells are actually in their off state, so the contrast control should be adjusted anti clock wise until the squares are only just visible.

The display module resets itself to an initial state when power is applied, which curiously the display has blanked off, so that even if the characters are entered, they cannot be seen. It is therefore necessary to issue a command at this point, to switch the display on.

The display on/off and cursor command turns on the display, but also determines the cursor style at the same time. Initially it is better to select a blinking cursor with under line, so that its position can be clearly seen. ie code 00001111(0F).set the data switches
(s1 to s8)to 00001111(0F) and ensure that RS switch (S10)is “down”(logic 0).so that the device is in command mode.

Now press E switch (S9) momentarily, which enables the chip to accept the data. Now set RS switch to “up” position (logic 1), switching the chip from command mode to character mode and enter the binary value 01000001(41) on data switches. This is ASCII code for a capital A. Press the switch and marvel as the display fills up with capital as. Clearly, something is not right.

Interfacing LCD with microcontroller is very easy task. You just have to know the proper LCD programming algorithm. LCD used here has HD44780u dot matrix LCD controller. LCD module has 8-bit data interface and control pins. One can send data as 8- bit or in pair of two 4-bit nibbles.

To display any character on LCD micro controller has to send its ASCII value to the data bus of LCD. For e.g. to display 'AB' microcontroller has to send two hex bytes 41h and 42h respectively. LCD display used here is having 16x2 size. It means 2 lines each with 16 characters. Interfacing is shown in the Figure 3.18.

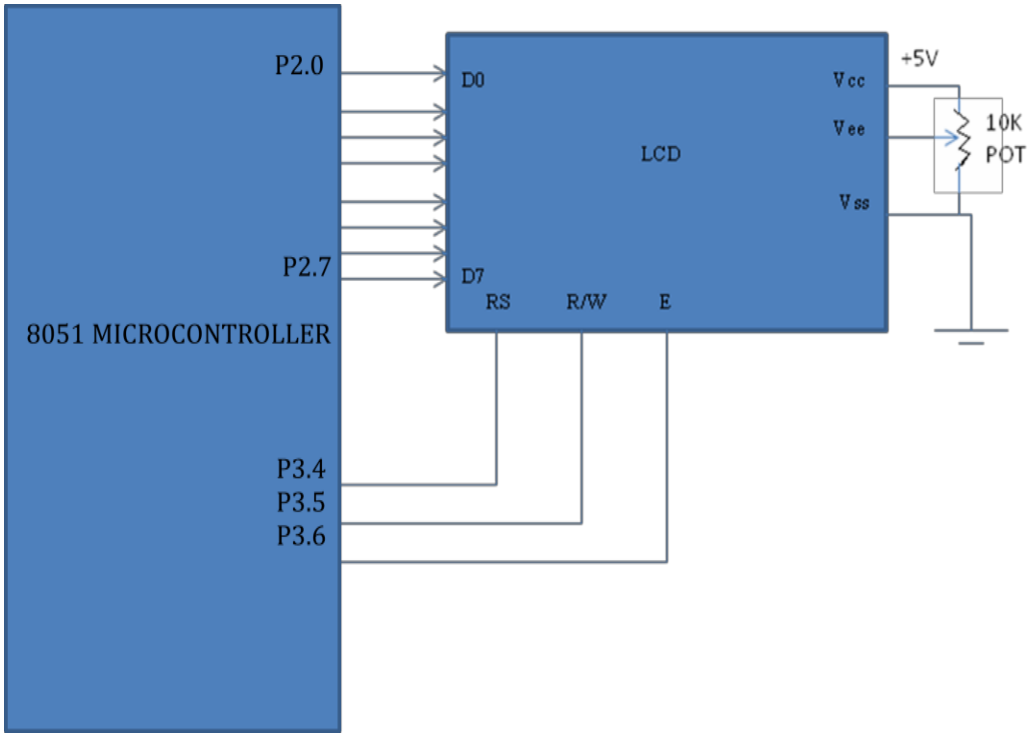


Figure 3.18: Interfacing LCD with the microcontroller

3.2.9 ROLE OF LCD:

The LCD module is used in the vehicle anti-collision system to display the range information which is calculated by LV Max Sonar-EZ1 and also to display one of the three zones in which the vehicle is present. If the distance displayed is above 20 inches it displays “safe” zone. If the distance is between 15 and 19 inches, then it displays “alert” zone. If the distance is below 15 inches, the LCD will display “stop” zone.

16X2 LCD : This LCD can be used to display 16 characters in 2 rows. It has the ability to display numbers, characters and graphics. It has an inbuilt refreshing circuit, thereby relieving the CPU from the task of refreshing. LCD discussed has total of 14 pins. Pinout of the LCD is shown in the Figure 3.19.

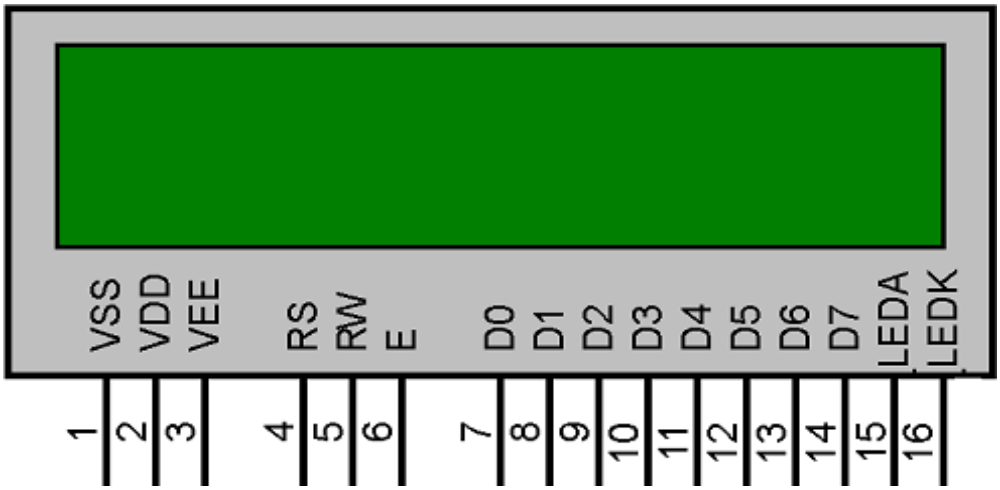


Figure 3.19: Pin out of a generic 16x2 LCD

In recent years the LCD is finding widespread use replacing LEDs this is due to following reasons:

1. The declining prices of LCDs.

2. The ability to display numbers, characters and graphics. This is in contrast to LEDs, which are limited to numbers and few characters.

3. Incorporation of a refreshing controller in to LCD, there by relieving the CPU of the task of refreshing the LCD. In contrast LCD must be refreshed by CPU to keep displaying the data.

3.2.10 NODEMCU:

The ESP8266 NodeMCU has 16 GPIO pins and one analog input pin shown in the image bellow.

However, only 10 of these GPIO pins can be used for digital input and output operations. These are listed on the Table below. It is shown in the Figure 3.20.

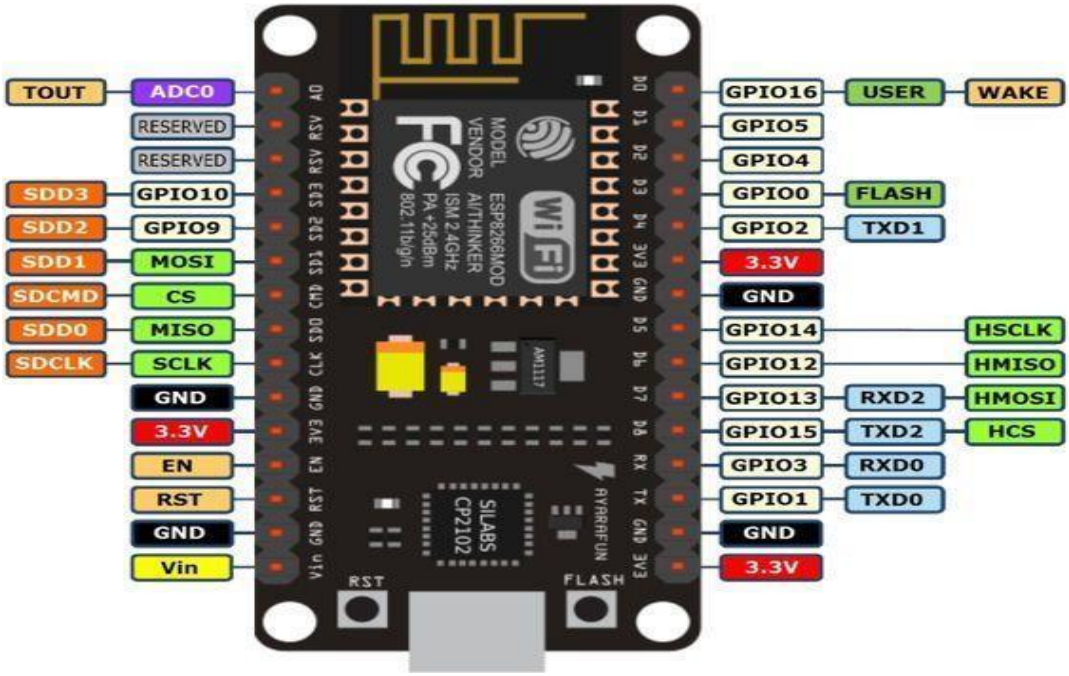


Figure 3.20: ESP 8266 NodeMCU Pin diagram

In the ESP8266 firmware for the Arduino IDE pin numbers are defined in the table 3.5.

Table 3.5: ESP8266 firmware for the Arduino IDE pin numbers

Pin Name on the Board	Function	Pin Number in Arduino IDE	Alias Name in Arduino IDE
D3	GPIO 0	0	D3
TX	GPIO 1	1	D10
D4	GPIO 2	2	D4
RX	GPIO 3	3	D9
D2	GPIO 4	4	D2
D1	GPIO 5	5	D1
D6	GPIO 12	12	D6

D7	GPIO 13	13	D7
D5	GPIO 14	14	D5
D8	GPIO 15	15	D8
D0	GPIO 16	16	D0, LED_BUILTIN
A0	ADC0	A0	analog_ip

Pin numbers in the Arduino IDE correspond directly to the ESP8266 GPIO pin numbers. **Pin Mode**, **digital Read**, and **digital Write** functions work as usual, so to read GPIO2, call **digital Read (2)** or its alias name **digital Read(D10)**.

At startup, pins are configured as **INPUT**. Digital pins 0-15 can be **INPUT**, **OUTPUT**, or **INPUT_PULLUP.**

Pin 16 can be **INPUT**, **OUTPUT** or **INPUT_PULLDOWN_16** and is connected to the build-in LED. It can be addressed with **digital Read (D0)**, **digital Read (16)** or **digital Read (LED_BUILDIN)**.

Pins may also serve other functions, like Serial, I2C, SPI. These functions are normally activated by the corresponding library. The diagram above shows the pin mapping for the popular ESP8266 NodeMcu module.

Pin interrupts are supported through **attach Interrupt**, functions. Interrupts may be attached to any GPIO pin, except GPIO16. Standard Arduino interrupt types are supported: **CHANGE**, **RISING**, **FALLING**.

Reserved Pins:

GPIO pins 6—11 is not shown on this diagram because they are used to connect flash memory chip on most modules. Trying to use these pins as IOs will likely cause the program to crash.

Note that some boards and modules (ESP-12ED, NodeMCU 1.0) also break out pins 9 and 11. These may be used as IO if flash chip works in DIO mode (as opposed to QIO, which is the default one).

Vin,3V3, GND:

Vin is the NodeMCU' S voltage input that is connected to its internal voltage regulator allowing an input voltage range of 4.75V to10V. It will be regulated to 3.3V. NodeMCU' S 3V3 pins. The 3V3 pin can be also a voltage source to other components such as LEDs. GND is the common ground of the board.

Analog Input:

ESP8266 has a single ADC channel available to users. It may be used either to read voltage at ADC pin, or to read module supply voltage (VCC).To read external voltage applied to ADC pin, use **analog Read(A0)**. Input voltage range is 0 — 1.0V. To read VCC voltage, use **ESP.getVcc()** while the ADC pin must be kept unconnected. Additionally, the following line has to be added to the sketch.

ADC_MODE(ADC_VCC);

This line has to appear outside of any functions, for instance right after the **#include** lines of your sketch.

Analog Output:

analogWrite(pin,value) enables software PWM on the given pin. PWM may be used on pins 0 to 16. Call **analogWrite(pin,0)** to disable PWM on the pin. **value** may be in range from 0 to **PWMRANGE**, which is equal to 1023 by default. A value of 0, 512 and 1023 sets the PWM duty cycle to 0%, 50% and 100%, respectively. Optionally, the PWM range may be changed by calling **analogWriteRange(new_range)**.

PWM frequency is 1kHz by default. Call **analogWriteFreq(new_frequency)** to change the frequency. The unit representation is in [Hz].

CHAPTER 4
METHODOLOGY

In this chapter, explained about the generalized steps of implementing the project model to be developed. It describes architecture, dataflow diagrams, sequence diagrams, flowcharts, etc.

4.1 SYSTEM ARCHITECTURE

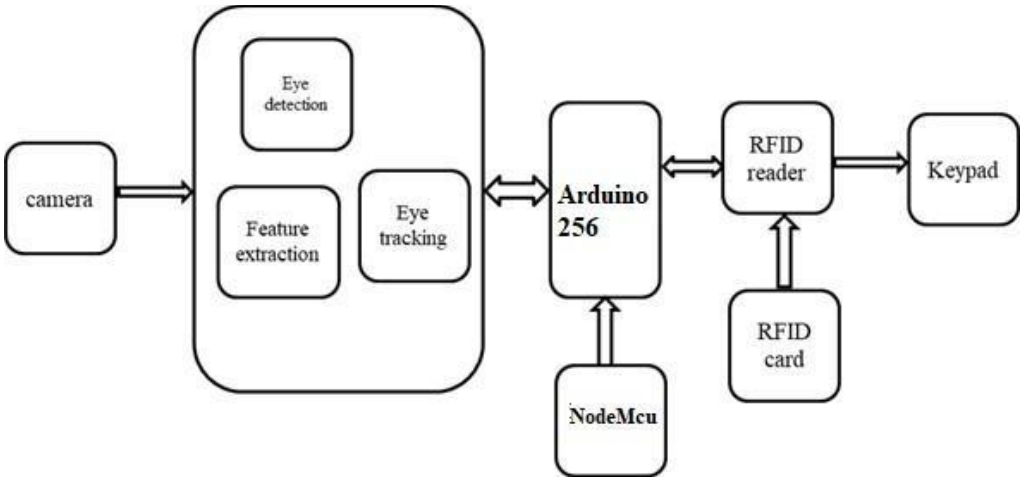


Figure 4.1: Block Diagram of the proposed system.

The RFID reader will read the card and the unique number will be generated which is considered as the password. This generated password is sent to OpenCV where the password is stored and then the password is entered through the eye movement and eye blinking. Further the authentication process will be done based on the generated password and the entered password. Web camera is used to capture the continuous images. The captured image acts as input to OpenCV. This captured image is sent to Eye detection module. The image from the camera is fed into OpenCV. This image is sent to eye detection module in OpenCV where the face and eye region in the image would be captured and the respective window location is sent to feature detection

module, here the co-ordinates of the eye region is will be the output. Lastly in the eye tracking module the eye movements will be tracked to get the gaze ratio and the eye blinks will be detected to get the blinking ratio. Based on these two ratios the password would be updated.

Global systems for mobile communications are used to describe the protocols for cellular networks used by mobile devices. Here Message is used to send alert system to the user. Eye detection module is used to detect the eye region in the input image. Image that is captured from the camera is sent to eye detection module where the haar cascade algorithm is used to detect the face in the image and in that face region the eye region will be detected the architecture is shown in the Figure 4.1.

In Feature detection, based on the window location of the face the key facial structures of the face i.e., eye, nose, mouth, ears would be found and the specific (x,y) co-ordinates would be given to the facial structures starting from 1 to 68. Then the co-ordinates of the left and right eye will be used to draw the polygon over the eye region. Eye tracking is used to track the eye movement and to detect the eye blinking for updating the password. The co-ordinates of the eye will be used to find the midpoint of the eye and through the midpoint the horizontal and vertical line will be drawn based on these line the tracking of the eye movement will takes place to update the password.

4.2 SYSTEM ANALYSIS

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. While a use case itself might drill into a lot of detail about every possibility, a use case diagram can help provide a higher-level view of the system. It

has been said before that "Use case diagrams are the blueprints for your system". They provide the simplified and graphical representation of what the system does.

- Customer- Scans the RFID card through the RFID reader and enters pin through eye tracker.
- Transaction System -Verifies the PIN and displays the banks.
- OTP generation- For unauthorized users.
- Withdrawal – After successful completion of authentication the customer will be able to withdraw the money. Use diagram is shown in Figure 4.2.

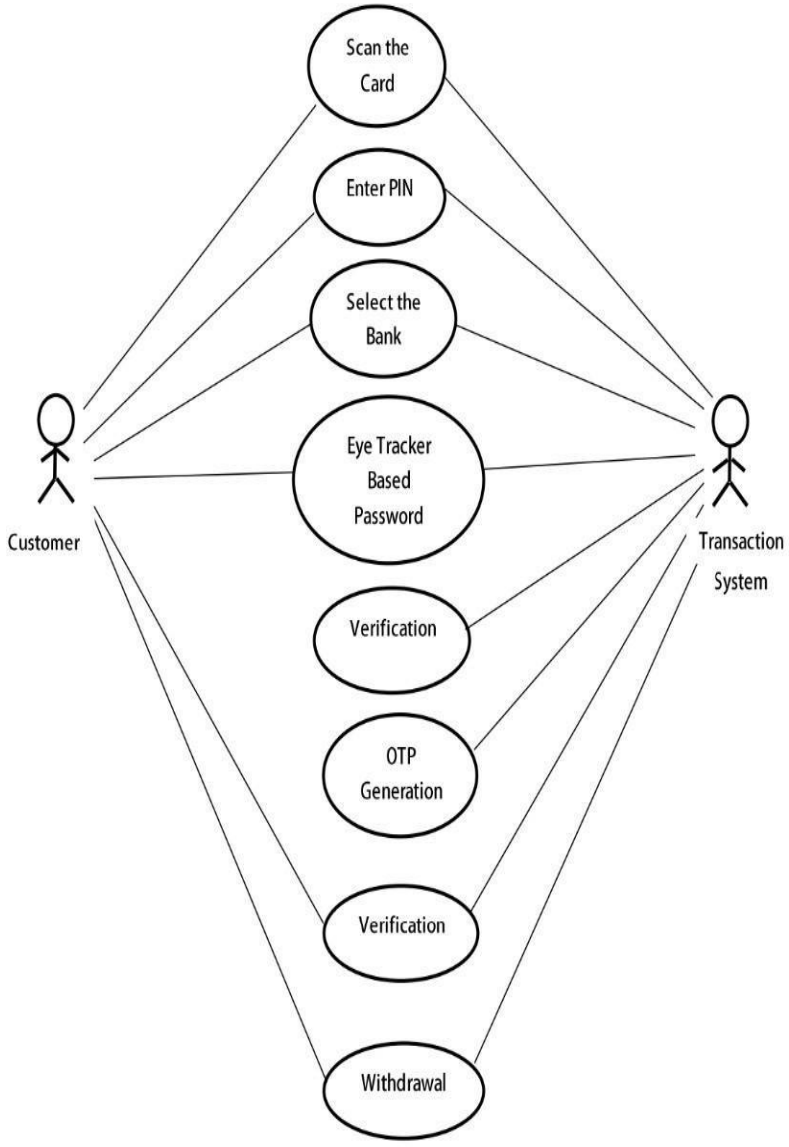


Figure 4.2: Use Case Diagram

4.3 SEQUENCE DIAGRAM

This diagram gives representation of the sequential exchange of information/data between the user, atm console, server and the bank shown in the Figure 4.3.

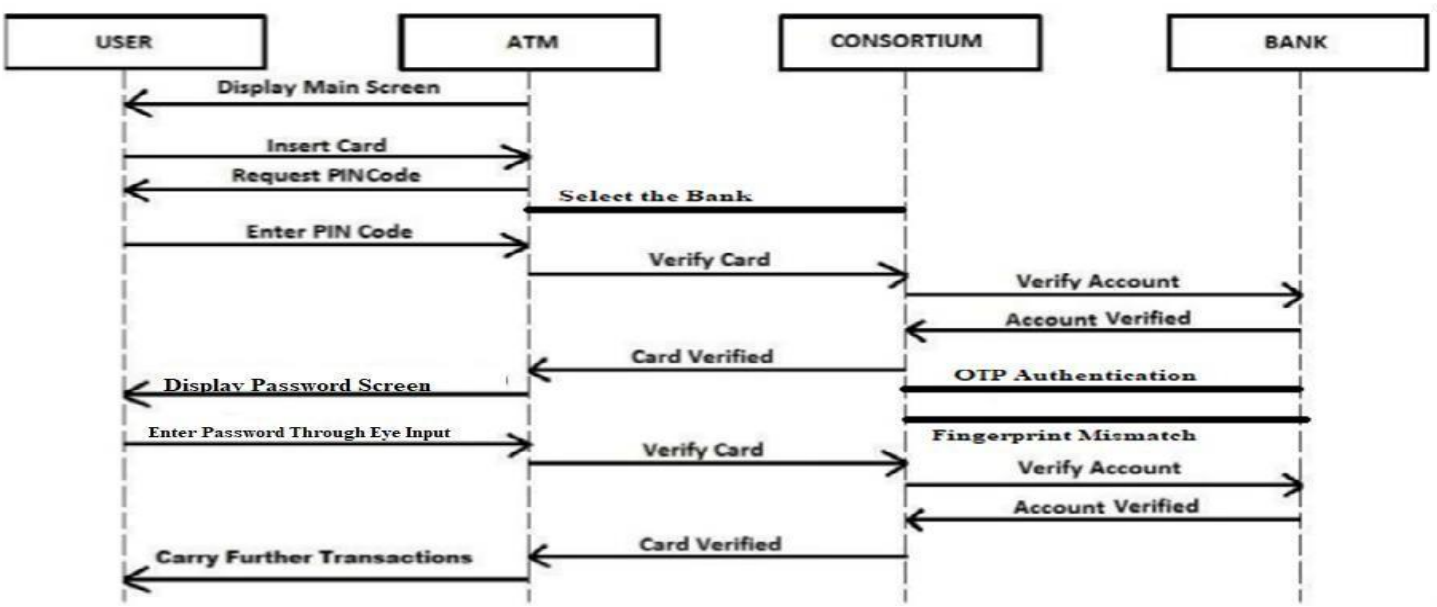


Figure 4.3: Sequence Diagram

4.4 DATAFLOW DIAGRAM

A dataflow diagram is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing. A DFD shows what kind of information will be input to and output from the system, how the data will advance through the system, and where the data will be stored.

1. DFD LEVEL 0:

This figure 4.4 represents a generalized flow of data between customer and the transaction system.

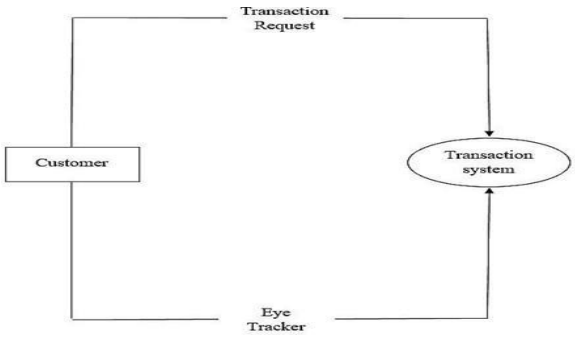


Figure 4.4: Data Flow Diagram Level 0

2. DFD LEVEL 1:

This figure 4.5 represents the detailed flow of data between the user and the ATM server with database.

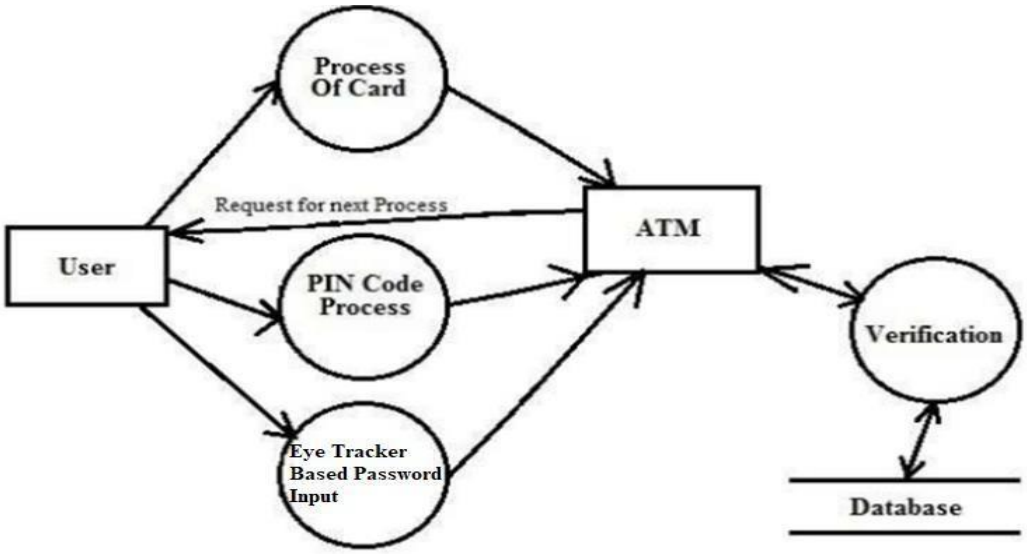


Figure 4.5: Data flow Diagram Level 1

3. DFD LEVEL 2:

In addition to DFD Level 1, this figure 4.6 represents the entire process of authentication of password for cash withdrawal from the bank.

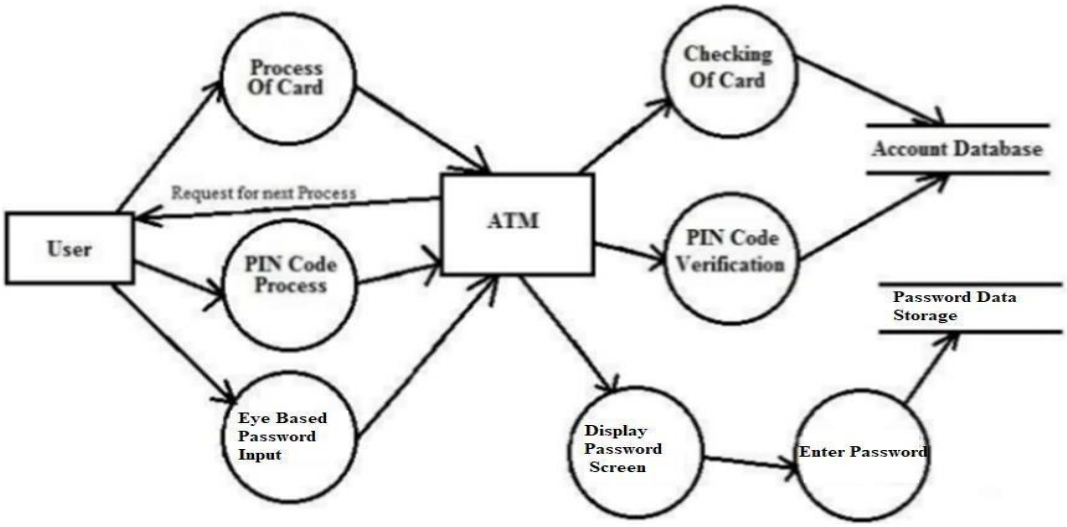


Figure 4.6: Data flow Diagram Level 2

5. FLOWCHART

The flowchart shown in the Figure 4.7 represents the entire step-by-step procedure for password authentication of the transaction system for withdrawal of money from the respective bank.

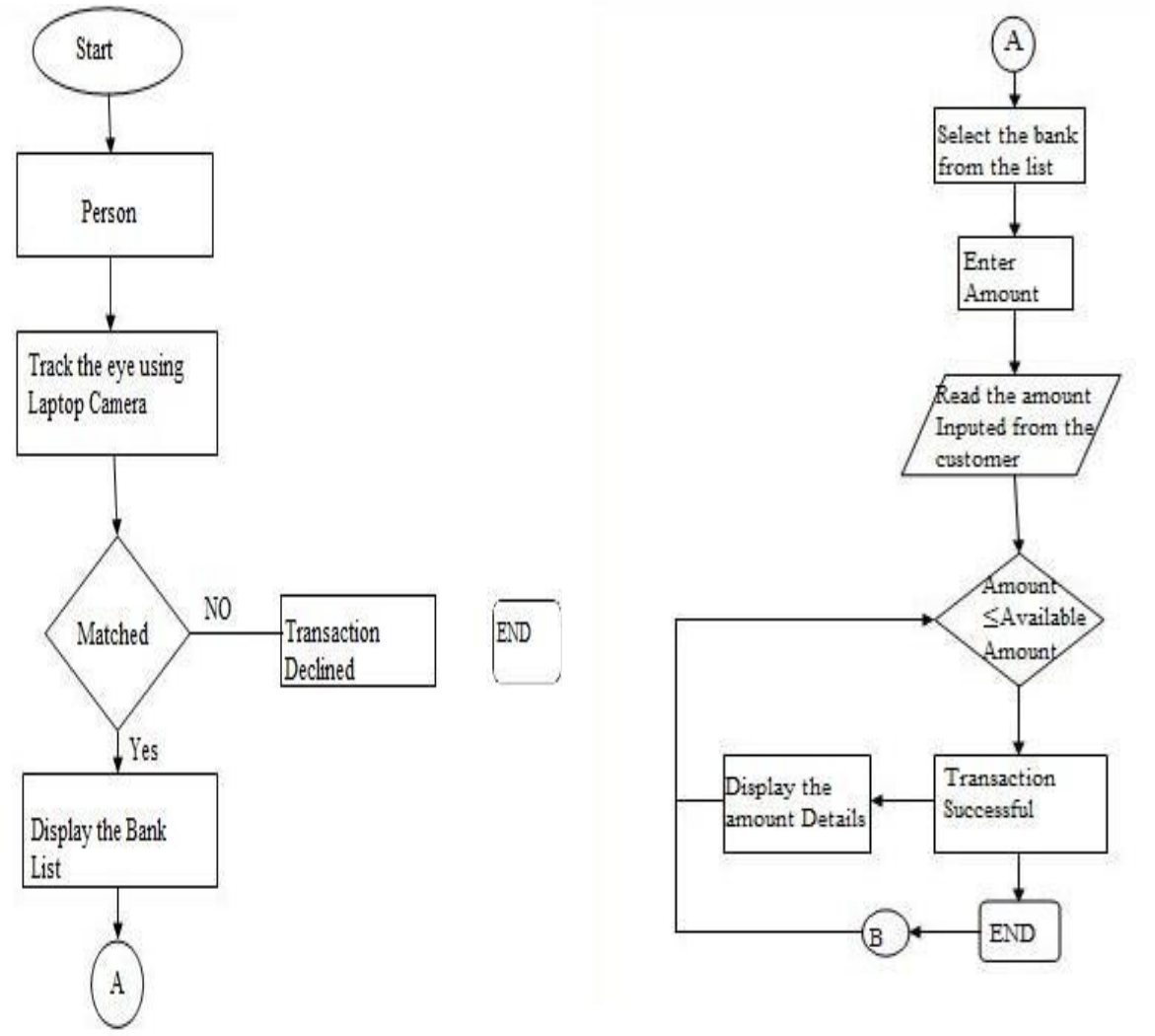


Figure 4.7: Flowchart of Multi-account ATM System

CHAPTER 5
IMPLEMENTATION

Here for demo purpose, in project using RFID cards as ATM cards. When user brings RFID card near RFID reader then on the touch screen authentication page will display. If the correct user password based on eye tracker is given then security eye tracking password will be sent to user mobile, then use has to enter the received number on the screen.

After successful login, Debit / Credit Option will display, once user selects the required option bank symbols will be displayed on the screen, and then user has to select the corresponding bank to perform transaction. Before any transaction again security number is sent to confirm the transaction.

5.1 EYE DETECTION

Eye detection module shown in the Figure 5.1 is used to detect the eye region in the input image. Image that is captured from the camera is sent to eye detection module where the haar cascade algorithm is used to detect the face in the image and in that face region the eye region will be detected. The specific window location is sent to next module.

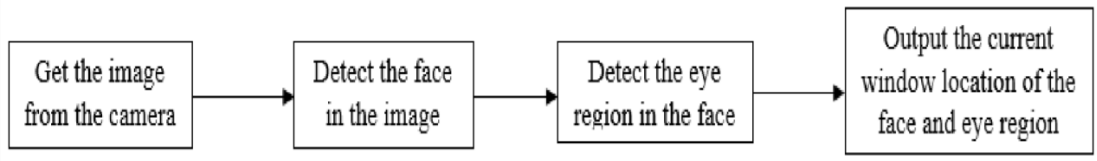


Figure 5.1: Block Diagram of Eye Detection module

Algorithm used:

The Haar cascade algorithm is a machine learning object detection algorithm used to identify objects in an image or video based on the concept of features. Haar cascade algorithm had four steps:

1. Haar feature Selection
2. Creating integral image
3. Ada boost training
4. Cascading Classifiers

5.1.1 Haar Feature Selection

Haar like Features are the digital image features used in object recognition. It is showed in the Figure 5.2. Haar feature selection is a cascade classifier. Initially the algorithm need ti train with lots of positive images (images of face) and negative images to train the classifier. Haar features shown in below image are used.

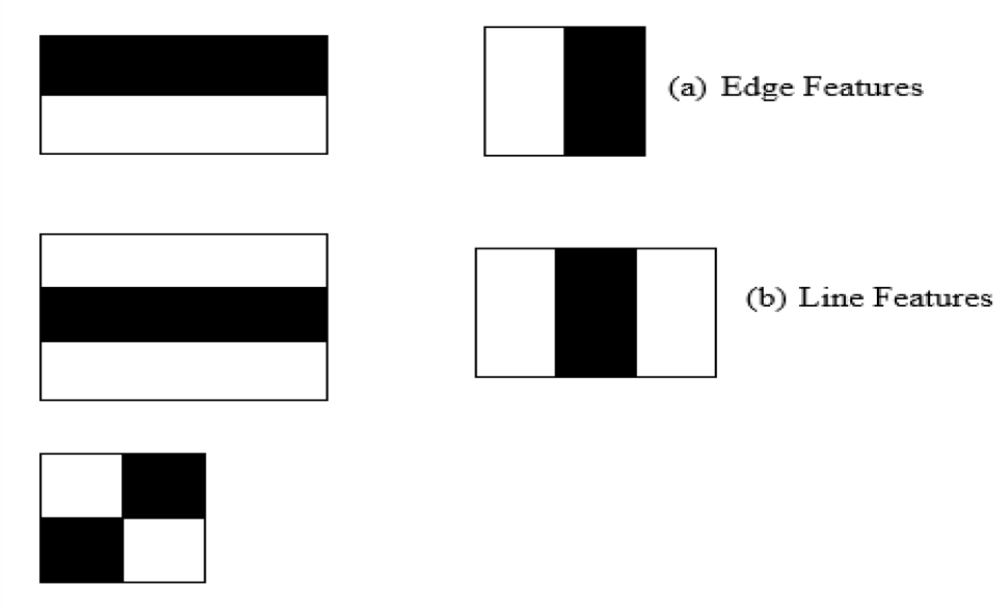


Figure 5.2: THREE DIFFERENT HAAR FEATURES

Each feature is a single value obtained by subtracting sum of pixels under white rectangle from the sum of pixels under black rectangles.

The eye region in the face is detected by using the edge feature detection since the eye region is darker than the other region that is nose and cheeks.

5.1.2 Creating Integral Images

Integral image are those images in which the pixel value at any (x,y) location is the sum of the all pixel values present before the current pixel. Its use can be understood by the following example shown in the Figure 5.3.

5	4	3	8	3
3	9	1	2	6
9	6	0	5	7
7	3	6	5	9
1	2	2	8	3

5	9	12	20	23
8	21	25	35	44
17	36	40	55	71
24	46	56	76	101
25	49	61	89	117

Assume a matrix ‘A’ of Size 5x5 representing an image, as shown here:

5	4	3	8	3
3	9	1	2	6
9	6	0	5	7
7	3	6	5	9
1	2	2	8	3

Figure 5.3: 5x5 representation of the image

Calculate the average intensity over the are highlighted in the figure 5.4.

5	4	3	8	3
3	9	1	2	6
9	6	0	5	7
7	3	6	5	9
1	2	2	8	3

Figure 5.4: Region of addition normally

To do the following:

9+1+2+6+0+5+3+6+5 = 37

37/9 = 4.11

This requires a total of 9 operations. Doing the same for 100 such operations would require:

100 * 9 = 900 operation.

Now, first make integral image of the preceding Figure 5.5.

5	9	12	20	23
8	21	25	35	44
17	36	40	55	71
24	46	56	76	101
25	49	61	89	117

Figure 5.5: Integral image for the preceding image making this image require a total of 56 operations.

Again, focus on the highlighted figure 5.6.

5	9	12	20	23
8	21	25	35	44
17	36	40	55	71
24	46	56	76	101
25	49	61	89	117

Figure 5.6: Integral image with highlighted portion

To calculate the avg intensity:

(76 – 20) – (24 - 5) = 37

37/9 = 4.11

This required a total of 4 operation.

To do this for 100 such operation, would require:

56 + 100 * 4 = 456 operations.

For just a hundred operations over a 5x5 matrix, using an integral image requires about 50% less computations. Imagine the difference it makes for large images and other such operations.

Creation of an integral image changes other sum difference operations by almost O(1) time complexity, thereby decreasing the number of calculations.

It simplifies the calculation of the sum of pixels, no matter how large the number of pixels to an operation involving just four pixels.

5.1.3 Adaboost training

The process selects only those features known to improve the predictive power of the model, reducing dimensionality and potentiality improving execution time as irrelevant features need not computed.

During this window of the specific size moved over the image and for each subsection of the image the haar features are calculated. The difference is then compared to a learned threshold that separates non-object form objects.

5.1.4 Cascade Classifier

It consists of collection of storage, where each storage is an ensemble of week learner. The week learners are simple classifiers called decision stumps. Each stage is trained using a technique called boosting.

Boosting provides the ability to train a highly accurate classifier by taking a weighted average of the decisions made by the weak learners.

While the window slides, it detects whether the region is positive or negative. If the positive region is detected, then it considers that the object is found and pass it on to the next stage. If the negative region is detected, then the sliding window considers the next smaller region of the image.

After the classifier passes the region to the next stage. The detector reports an object found at the current window location when the final stage classifies the region as positive.

5.2 FEATURE DETECTION

The output of the above module is taken as input in this module. Based on the window location of the face the key facial structures of the face i.e., eye, nose, mouth, ears would be found and the specific (x,y) co-ordinates would be given to the facial structures starting from 1 to 68. Then the co-ordinates of the left and right eye will be used to draw the polygon over the eye region.

Algorithm used.

Facial landmark detector: This is used to detect and label the facial landmarks of the image.

- Input the window location where the face and eye region is found.
- Detect the key facial structures in the image.
- Locate the key facial structures with specific (x,y) co-ordinates.
- Start with for the first (x,y) co-ordinate.
- End with 68 for the last (x,y) co-ordinate.

Facial Landmark detector is used to achieve the above process. The Facial Land Marks is shown in the Figure 5.7.

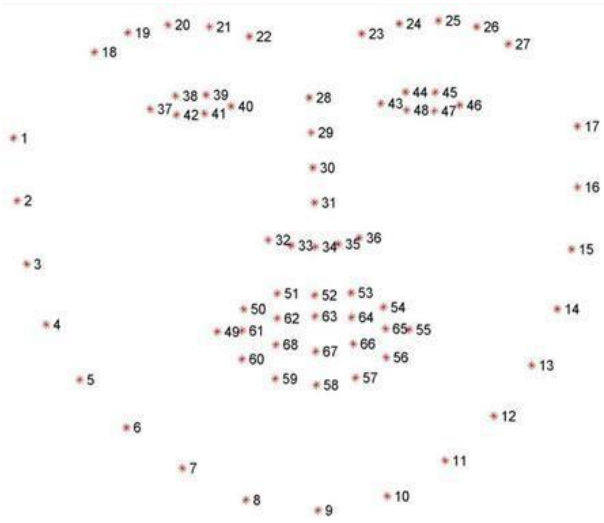


Figure 5.7: 68 Facial Landmark points

To draw the polygon over the eye region as shown in the Figure 5.8.

Get the co-ordinates value of the left and right eye.

eye_region = np.array([(facial_landmaeks.part(eye_points[36])]).x,

facial _landmakrs.part(eye_points[36]).y),

(facial_landmarks.part(eye_points[37]).x, Facial_landmark.part(eye_points[37]).y),

(facial_landmarks.part(eye_points[38]).x, Facial_landmark.part(eye_points[38]).y),

(facial_landmarks.part(eye_points[39]).x, Facial_landmark.part(eye_points[39]).y),

(facial_landmarks.part(eye_points[40]).x, Facial_landmark.part(eye_points[40]).y),

(facial_landmarks.part(eye_points[41]).x,

Facial_landmark.part(eye_points[41]).y)],np.int32)

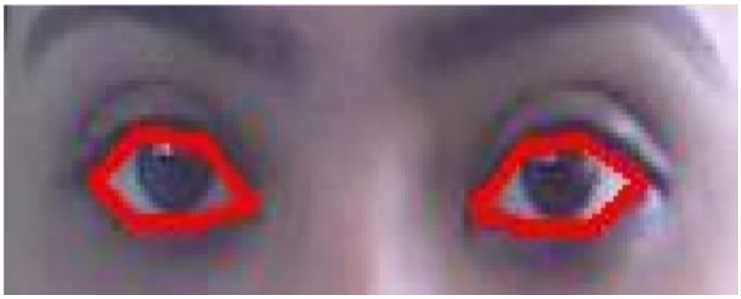


Figure 5.8: Polygon drawn over the eye region

Table 5.1: Co-ordinates values of left eye

	X	Y
36	403	321
37	415	313
38	430	313
39	443	323
40	430	326
41	415	326

Table 5.2: Co-ordinates values of right eye

	X	Y
42	495	320
43	508	311
44	521	311
45	533	316
46	523	321
47	509	322

Based on the above table 5.1 and table 5.2 pixel values the polygon is drawn over the eye region.

5.3 EYE TRACKING

Eye tracking is used to track the eye movement and to detect the eye blinking for updating the password. The co-ordinates of the eye will be used to find the midpoint of the eye and through the midpoint the horizontal and vertical line will be drawn based on this line the tracking of the eye movement will takes place to update the password.

Methodology

- Obtain the midpoint.
- Draw the horizontal and vertical line passing through the midpoint.
- Calculate the number of white pixels on each eye to the left and right of vertical line to get the gaze ratio.
- Calculate the length of the horizontal and vertical line to get the blinking ratio.

Based on the Gaze Ratio the Left or Right Side of the keyboard is selected. After selecting the keyboard, the Blinking Ratio of the eye is calculated. Based on the Blinking Ratio the password is updated, and further authentication process is performed. In case of valid authentication, the relay is opened else it remains close.

Algorithm:

To calculate the gaze ratio

1. Input the pixel values of the eye region.
2. Get only the eye region.
3. Divide each eye region into left and right side.
4. Convert the eye image into grayscale.
5. Get the number of white pixels on both sides i.e left and right side of each eye.
6. Calculate the Gaze Ratio:

Gaze Ratio of left eye = Number of white pixels on right side

Number of white pixels on left side

Gaze Ratio of right eye = Number of white pixels on right side

Number of white pixels on left side

Gaze Ratio = Gaze Ratio of left eye + Gaze Ratio of right eye

2

7. If Gaze Ratio <= 0.9 then select the right keyboard

Else: Then select the left keyboard and the algorithm is shown in the Figure 5.9.

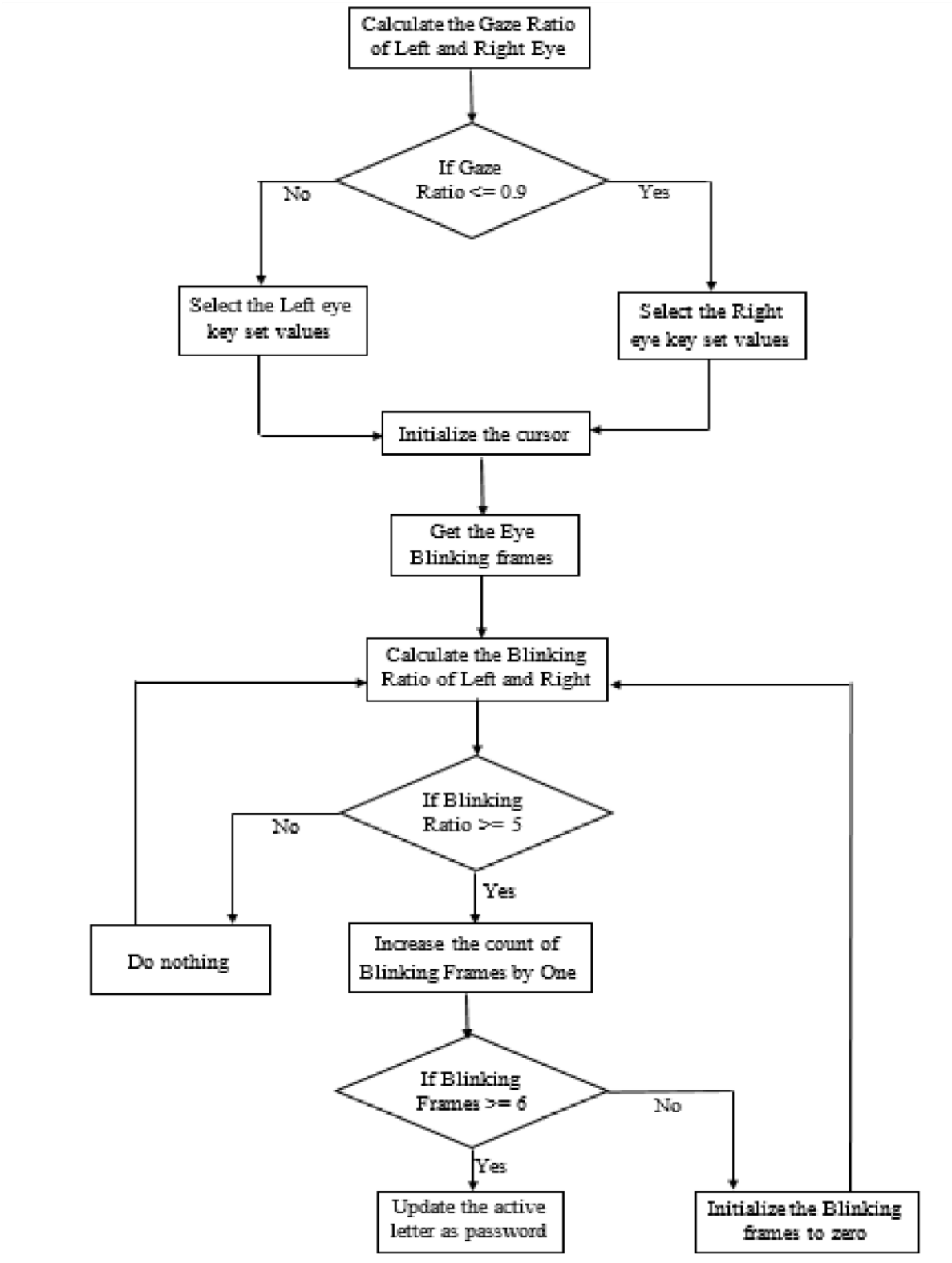


Fig 5.9: Algorithm to Find Gaze Ratio

5.4 Working

The Table value are taken as the input here. The corresponding eye region is converted into gray scale which is shown in the below Figure 5.10 and Figure 5.11.

Figure 5.10: Gray Scale Image

Figure 5.11: The menu keyboards.

Then the midpoint between 37th and 38th co-ordinate is calculated and midpoint of 40th and 41st co-ordinate is calculated, and those midpoints are joined to divide the eye region into two parts as shown in the figure 5.12.

Figure 5.12: Vertical line drawn over the image to divide the eye region.

The gaze ratio of both left and right eye will be calculated and then the average of both the left and right eye is taken to obtain the Gaze ratio.

Gaze ratio is shown below: Gaze Ratio of the left eye shown in Figure 5.13.

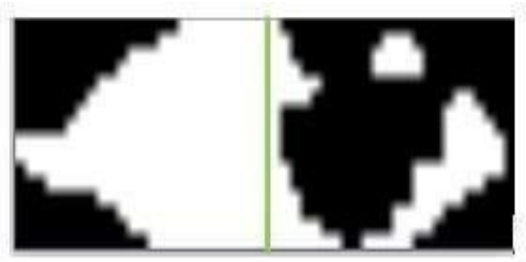


Figure 5.13: Gaze of the left eye

Number of white pixels on the left side = 7187

Number of white pixels on the right side = 2701

Gaze ratio of left eye = $\frac{\text{Number of white pixels on right side}}{\text{Number of white pixels on left side}}$

$= \frac{2701}{7187}$

$= 0.376$

Gaze ratio is shown below: Gaze Ratio of the left eye shown in Figure 5.14.

Figure 5.14: Gaze of the right eye

Number of white pixels on the left side = 4759

Number of white pixels on the right side = 398

Gaze ratio of left eye = $\frac{\text{Number of white pixels on right side}}{\text{Number of white pixels on left side}}$

$$= \frac{398}{4759}$$

$$=0.0836$$

Gaze Ratio = Gaze Ratio of left eye + Gaze Ratio of right eye

$$= \frac{0.376 + 0.0836}{2} = 0.2297$$

The gaze ratio obtained above is less 0.9. Similarly the gaze ratio is obtained for 15 frames continuously. If all the obtained gaze ratio of the 15 frames is less than 0.9 then the right keyboard is selected. If the obtained gaze ratio is more then 0.9 then the left keyboard is selected as shown in the figure 5.15.

Figure 5.15: Right Keyboard

When the keyboard is displayed the eye blinking is calculated to update the password.

5.5 Algorithm:

To calculate the Blinking ratio

1. Input is the co-ordinate values of the eye region.
2. Obtain the horizontal and vertical line of left eye:
   i. Calculate the midpoint of 37^{th}, 38^{th} co-ordinate and 40^{th} , 41^{st} co- ordinate.
   ii. Join the points to the vertical line.
   iii. Join the 36^{th} and 39^{th} point to get the horizontal line.
3. Obtain the horizontal and vertical line of the right eye:
   i. Calculate the midpoint of 43^{rd}, 44^{th} co-ordinate and 45^{th} , 46st co- ordinate.
   ii. Join the points to the vertical line.
   iii. Join the 42^{nd} and 47^{th} point to get the horizontal line.
4. Calculate the Blinking ratio:
   i. Blinking Ratio of the left eye:

$$\text{Blinking ratio of the left eye} = \frac{\text{Length of the horizontal line}}{\text{Length of the vertical line}}$$

   ii. Blinking Ratio of the right eye:

$$\text{Blinking ratio of the right eye} = \frac{\text{Length of the horizontal line}}{\text{Length of the vertical line}}$$

   iii. $$\text{Blinking Ratio} = \frac{\text{Blinking ratio of left eye + blinking ratio of right eye}}{2}$$

5. Initialize the blinking frame to zero.

6. If the Blinking ratio >= 5

Increase the blinking frames value by one.

7. If Blinking frames == 6

Then update the letter as password.

Working

Consider the midpoints to obtain the horizontal and vertical line. Consider the left eye co-ordinates points as shown in above Table For obtaining the vertical line:

Midpoint of 37^{th} ,38^{th} co-ordinate = ((415 + 430) / 2), ((313 + 313) / 2)

= 422.5,313

Midpoint of 40^{th} ,41^{st} co-ordinate = ((430 + 415) / 2), ((326 + 326) / 2)

= 422.5,326

Join the above points i.e., (422.5,313) and (422.5,326) to get the vertical lin.

For obtaining horizontal line:

Join the 36^{th} and 37^{th} co-ordinate i.e., (403,321) and (443,323) to get the horizontal line.

The Figure 5.16 shown below will show how the horizontal and vertical line is drawn on the eye.

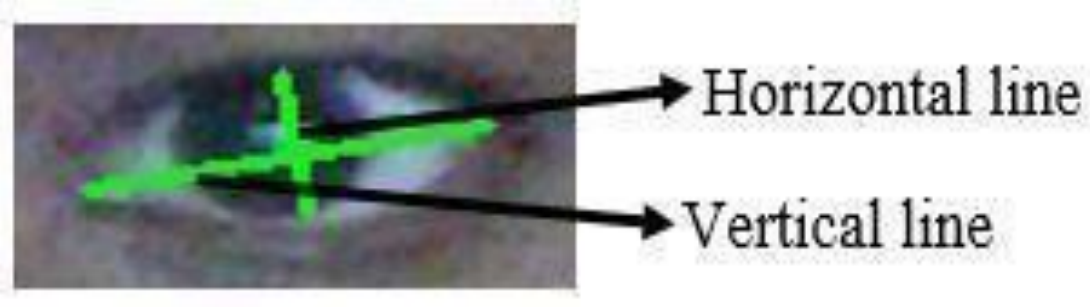


Figure 5.16: The horizontal and vertical line drawn on the eye

Figure 5.17: Horizontal and vertical line when eye is blinked

The calculation of the Blinking ratio of the above Figure 5.17 is shown below Calculating he is blinking ratio:

Blinking Ratio of left eye:

Length of the horizontal line = 48.0936

Length of the vertical line = 8.0

Blinking ratio of left eye = $\frac{48.0936}{8.0}$

= 6.0117

Blinking Ratio of left eye:

Length of the horizontal line = 49.09175

Length of the vertical line = 10.0498

Blinking ratio of left eye = $\frac{49.09175}{10.0498}$

= 4.8848

Blinking ratio = $\frac{\text{Blinking ratio of left eye + Blinking ratio of right eye}}{2}$

Here the blinking ratio is greater than 5. This blinking ratio computation is done continuously for 6 frames if in all the frames the blinking ratio obtained is greater than 5 then the letter pointed by the cursor will be updated as the password, else the blinking frames will be made zero and the process repeats.

CHAPTER 6

RESULTS AND DISCUSSIONS

The following figures represent the images after execution of each step-by-step procedure of entire process.

6.1 ATM used by Authorized person:

The Figure 6.1, shows two options the user must choose the appropriate one.

Figure 6.1: Options to choose for the User role.

If the user is validated and then the workflow starts. Once the selected option and entered value by the user is valid then the further steps will follow as shown in the figure 6.2.

Figure 6.2: Selection of bank from the list

The user needs to select his/her bank from the given list of banks to make the transactions from the list of Predefined banks displayed on the LCD.

Figure 6.3: Listing all bank names.

After selecting a particular bank, a welcome message will be displayed with respect to that bank as shown in the Figure 6.4.

Figure 6.4: Welcome message from Bank

The user must enter the amount that needs to be withdrawn from the bank as show in the Figure 6.5.

Figure 6.5: Enter Amount Dialog Screen

Once the desired amount is entered and fed into the system. In the background the system verifies the transaction and dispenses the cash and displays the message to collect the money as shown in the Figure 6.6.

Figure 6.6: Collect Cash Dialog Screen

Finally, once the dispensed cash is collected from the machine it detects as the cash is collected and displays the transaction end thanks greet message as shown in the Figure 6.7

Figure 6.7: End Transaction Dialog Screen

6.2ATM USED BY UNAUTHORIZED PERSON

The next method going to be discussed is unauthorized person action. And the Figure 6.8 shows two options must choose the appropriate one.

Figure 6.8: Options to choose for the User role.

Once the user selects the above option as Unauthorized and enters the value it will ask the user to swipe the card to check the identity as shown in the figure 6.9.

Figure 6.9: Swiping Card Dialog Screen

The user swipes the card as shown in the Figure 6.10.

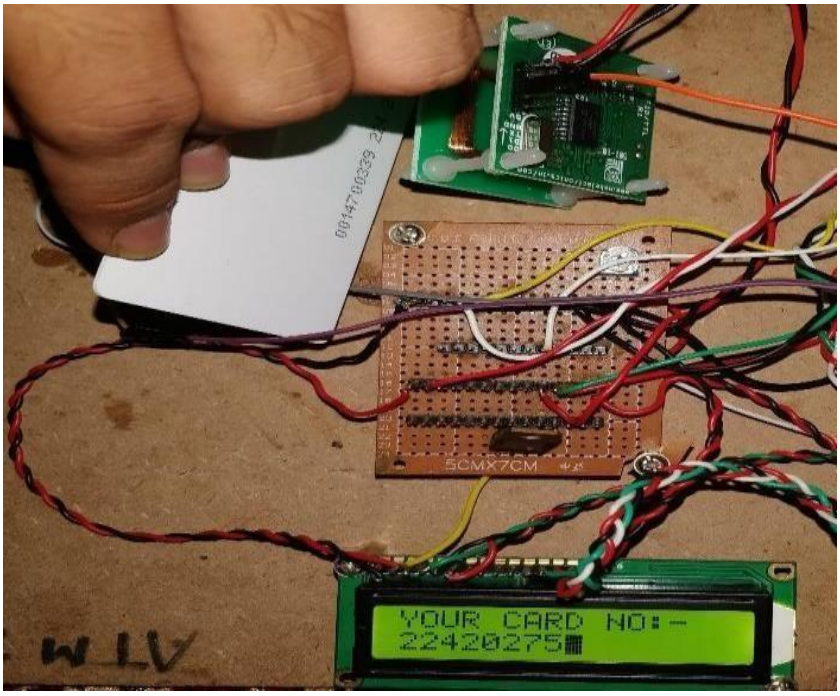


Figure 6.10: Swiping Card

After the validation of the card, the system will ask the user to enter the PIN for the authorization as shown in the Figure 6.11.

Figure 6.11: OTP Dialog Screen

After a valid PIN is entered in the system, and if found valid, it will proceed for the next step displaying all bank names as shown in the Figure 6.12.

Figure 6.12: Selection of bank name from the list

The user needs to select his/her bank from the given list of banks to make the transactions from the list of Predefined banks displayed on the LCD Figure. 6.13

Figure 6.13: Listing bank name.

After selecting a particular bank, a welcome message will be displayed with respect to that bank as shown in the Figure 6.14.

Figure 6.14: Welcome Bank message

The user must enter the amount that need to be withdrawn from the bank as the LCD Display shows the below Figure 6.15 output.

Figure 6.15: Please Enter Amount Dialog Screen

Once the desired amount is entered and fed into the system. In the background the system verifies the transaction and dispenses the cash. And displays the message to collect the money as shown in the Figure 6.16.

Figure 6.16: Please Collect Cash Dialog Screen

Finally, the dispensed cash is collected from the machine it detects as the cash is collected, 1display the transaction end thanks greet message shown in the Figure 6.17

Figure 6.17: Transaction end Dialog Screen

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

7.1 CONCLUSION

The method using for handling multiple accounts here is more efficient than existing system. This Reduces transaction cost of handling multiple accounts of a single user. This makes banking system more efficient than the existing system. Using this the users can perform transactions for all bank accounts using single smart ATM card with enhanced security system such as OTP (one time password) and eye recognition. Thus, the user can manage his multiple accounts in various banks with the help of this single smart card which provides access and reduces the complexity of managing more than one ATM card and passwords.

7.2 FUTURE SCOPE

- This project can be implemented for office security also.
- Also, to colleges, hospitals and in parking system.
- Future research will help to do away with PINs completely dwarf ATM card authorization by introducing palm and finger vein authentication, which is fast, accurate and difficult to fake.
- Since more than one bank accounts being added, the existing PIN security are not sufficient, so that it can use a biometric scan in the smart card i.e., multi component card.
- So that the user holds the card such that the face recognition on the biometric scan reader while he swipes the registered card, and the image is authenticated at the real time.
- No one other than the user and their family can use the card. Only if the face matches, the user can enter the PIN number otherwise the transaction will not be allowed until the user is authenticated.

REFERENCES

[1] "*Smart Card & Security Basics*" – Card Logix, paper no.:710030

[2] "*Smart card based Identity Card And Survey*"-White Paper JKCSH (Jan Kremer Consulting Services).

[3] "*Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta*"-Douglas King, Jan 2012.

[4] "*Examining Smart-Card Security under the Threat of Power Analysis Attacks*"-Thomas S. Messaerges member IEEE, Ezzat A. Dabbish member IEEE, and Robert H. Sloan senior member IEEE vol.51, No. 5, MAY 2002.

[5] "*Secure Internet Banking Application*"-Alain Hiltgen, Thorsten Kramp.

[6] Fingerprint Verification Using Smart Cards for Access Control Systems, Raul Sanchez-Riello, IEEE AESS Systems Magazine , September 2002 [7] "*Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application*"-Smart card Alliance 2011.

[7] Katakam Swathi, Prof. M. Sudhakar "*Multi Account Embedded ATM Card with Enhanced Security*" IOSR Journal of Electronics and Communication Engineering IOSR Journal of Electronics and Communication Engineering, Volume 10, Issue 3, Ver. I (May-Jun 2015)

[8] Tahaseen Taj I S, Dr Suresh M B "*An Embedded Approach: For Handling Multiple Accounts With Smart Atm Card*" International Conference on Computer Science, Electronics & Electrical Engineering-2015

[9] Nair Vinu Uthaman, Pratiksha Shetty, Rashmi, Mr. Balapradeep K N "*MAASC Multiple Account Access using Single ATM Card*" International Journal of Science,Engineering and Technology Research(IJSETR), Volume 3, Issue 6, June 2014.

[10] Youjung Ko, Insuk Hong, Hyunsoon Shin, Yoonjoong Kim "*Development of HMM- based Snoring Recognition System for Web Services*" 2016 IEEE

[11] Ashutosh Gupta, Prerna Medhi, Sujata Pandey, Pradeep Kumar, Saket Kumar, H. P. Singh "*An Efficient Multistage Security System for User Authentication*" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[12] Archana. Darchanadheenadayalan, Aarthi. R Angelin. A "*Secured Smart Card For Multi Banking*" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 09761353 Volume 21 Issue 3 – APRIL 2016.634

[13] Sree Rekha G, V. K. Agrawal "*A Scheme for Integrated Multi-banking Solution*" International Journal of Computer Applications (0975 – 8887) Volume 29– No.7, September 2011

[14] Gokul. R, Godwin Rose Samuel. W, Arul. M, Sankari. C, "*Multi account Embedded ATM card*", "*International Journal of Scientific and Engineering Research*", Volume4 , Issue-4, April-2013.

[15] S. Alazmi, A. R. Khan and Q. Yu, "A Comprehensively Secure Smart card access controls," *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, 2018, pp. 1-4, doi: 10.1109/NCG.2018.8592961.

[16] T. Abdurahmonov, E. -T. Yeoh and H. M. Hussain, "The implementation of Elliptic Curve binary finite field (F2m) for the global smart card," *2010 IEEE Student Conference on Research and Development (SCOReD)*, Kuala Lumpur, Malaysia, 2010, pp. 169-173, doi: 10.1109/SCORED.2010.5703995.

[17] Tadiwa, N. E., and H. Halabi. "Multi-level security algorithm for randon zigbee wireless sensor network." *4th International Symposium on Information Technology 2010 (ITSim'10)*. 2010.

[18] Zhang Peng and Jia Jian Fang, "Comparing and implementation of public key cryptography algorithms on smart card," *2010 International Conference on*

Computer Application and System Modeling (ICCASM 2010), Taiyuan, 2010, pp. V12-508-V12-510, doi: 10.1109/ICCASM.2010.5622377.

[19] C. Sanchez-Avila and R. Sanchez-Reillol, "The Rijndael block cipher (AES proposal) : a comparison with DES," *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186)*, London, UK, 2001, pp. 229-234, doi: 10.1109/CCST.2001.962837.

[20] Al Tamimi, Abdel-Karim. "Performance analysis of data encryption algorithms." *available at weblink: http://www. cse. wustl. edu/~ jain/cse567-06/ftp/encryption_perf/index. html* (2006).

[21] M. Mehrubeoglu and V. Nguyen, "Real-time eye tracking for password authentication," *2018 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2018, pp. 1-4, doi: 10.1109/ICCE.2018.8326302.

[22] M. Corbett, J. Shang and B. Ji, "GazePair: Efficient Pairing of Augmented Reality Devices Using Gaze Tracking," in *IEEE Transactions on Mobile Computing*, vol. 23, no. 3, pp. 2407-2421, March 2024, doi: 10.1109/TMC.2023.3255841.

[23] Y. Cheng, H. Wang, Y. Bao and F. Lu, "Appearance-based Gaze Estimation with Deep Learning: A Review and Benchmark," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, doi: 10.1109/TPAMI.2024.3393571.

[24] N. Jesani, N. Gupta, S. Bhatt, P. Singh and A. Saxena, "Smart Card For Various Application In Institution," *2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, 2020, pp. 1-5, doi: 10.1109/SCEECS48394.2020.26.