CHAPTER ONE

1.0 INTRODUCTION

Fingerprint verification is an important biometric technique for personal identification. Biometrics is a technology that uniquely identifies a person based on his physiological or behavioral characteristics. It relies on an individual's characteristics to make personal identification and therefore can inherently differentiate between an authorized person and an unauthorized person. Any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies the following requirements:

1) **Universality** - This means that every person should have the characteristic.
2) **Uniqueness** - This indicates that no two persons should be the same in terms of the characteristic in question.
3) **Permanence** - This means that the characteristic should be invariant with time. That is, at every point in the lifetime of the individual, this characteristic should be the same.
4) **Collectability** - This indicates that the characteristic can be measured quantitatively.
5) **Performance** – This refers to the achievable identification accuracy, the resource requirements to achieve acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy.
6) **Acceptability** - This indicates to what extent people are willing to accept the biometric system.
7) **Circumvention** – This means that it should be difficult to bypass the system.

The human fingerprint meets these requirements, others being the iris and DNA. However, the latter are harder to implement and usually not as cost friendly as the fingerprint.

Generally, there are two types of systems that help automatically establish the identity of a person:

1) Authentication (verification) systems
2) Identification systems.

In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc. and the system either rejects or accepts the submitted claim of identity.

In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity. This project is channeled towards the development of an examination authentication system that eliminates the pitfalls of a verification system, more specifically, impersonation. It would achieve this by taking advantage of a unique feature of identification – the fingerprint. In our system, the student would not need to provide any means of identification, rather the system will identify whether or not the student is permitted to write the examination using an inherent characteristic (fingerprint) of the student.

1.1 PROBLEM STATEMENT

Authentication has always been a major challenge in all types of examination. Verification of the authentic candidate is not an easy task, and also it consumes a lot of time and process. Often times, the issue of impersonation poses a major challenge to the determination of the performance of candidates the examination was meant for. For this reason, the idea of developing a Fingerprint based exam hall authentication system that is designed to register students for an exam by taking their fingerprints and to pass only users verified by their fingerprint scan and block non verified users from taking the exam, was birthed.

1.2 AIM

The aim of this project is to design and implement a finger print based biometric authentication system for examination purposes.

1.3 OBJECTIVES

To create a system that is capable of tracking impersonators in the examination system using finger print biometrics and mobile device. To reduce rate of corruption in the educational sector and increase the rate of self-confidence on students. To demonstrate the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

1.5 RELEVANCE

With the increasing rate of exam malpractices in the educational sectors, the Universities management decides to incorporate a reliable security means to ensure that these activities of exam impersonators are checkmated. The activities of these exam impersonators have seen the educational sector suffer some serious form of corruption ranging from students to students to students to supervisors. So it became necessary for the educational body to set up strategies to stop this corruption in the educational sector.

The system uses finger prints biometrics and mobile device, that will help ensure that only students with their fingerprints registered during registration period are allowed into the examination hall. As opposed to existing fingerprint biometric systems, this proposed system makes it easier to carry out the authentication process. Existing solutions make use of a laptop or PC device as the interface for registration and authentication. This has a few cons including the size which makes it less portable and the requirement for power. Our system will employ a mobile device for authentication process. The invigilator would no longer need to carry a laptop to the examination hall. Using his mobile phone or any other available mobile phone (with the application installed and the right database files loaded), he can authenticate students smoothly.

This system being easy to deploy and also cost friendly, would contribute in stopping any activity of corruption in the form of impersonation in the educational sector. Hard work would be encouraged as every registered student knows he/she is going to write the exam by him or herself. Consequently, the society will produce more reliable and trustworthy graduates that can match up to their qualifications. The impersonation which has been eating the educational system thereby encouraging laziness among students would be eliminated and standard of student educational performance would be increased.

1.6 SCOPE

This system allows the registration of students with their details such as name and mat number as well as their fingerprint scans. This data is stored in a database and can be extracted as a file and transferred from one device to another. The microcontroller used for the project however, cannot store information exceeding 5MB. Therefore, registration data for a particular examination should not exceed this limit.

The system is designed to work with mobile devices, specifically android phones, through which authentication can be carried out. The system does not work with PC or laptop devices.

This system makes use of a Bluetooth module with a range of 10m. Therefore, the distance between the mobile device and the microcontroller unit should not exceed this limit.

CHAPTER TWO

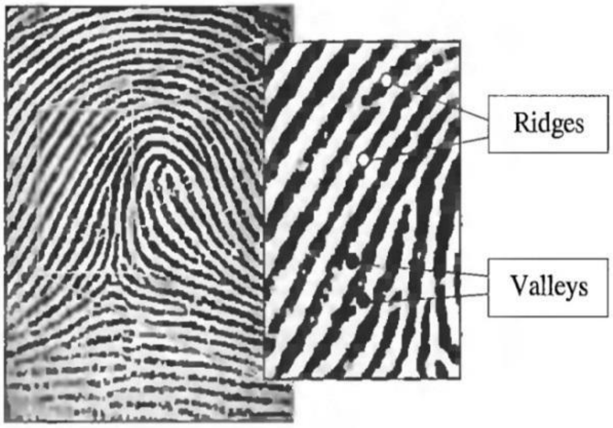
LITERATURE REVIEW

This chapter gives an insight into the theoretical framework as well as previous studies conducted by past researchers relating to this project.

THEORETICAL FRAMEWORK

The Science of Fingerprints

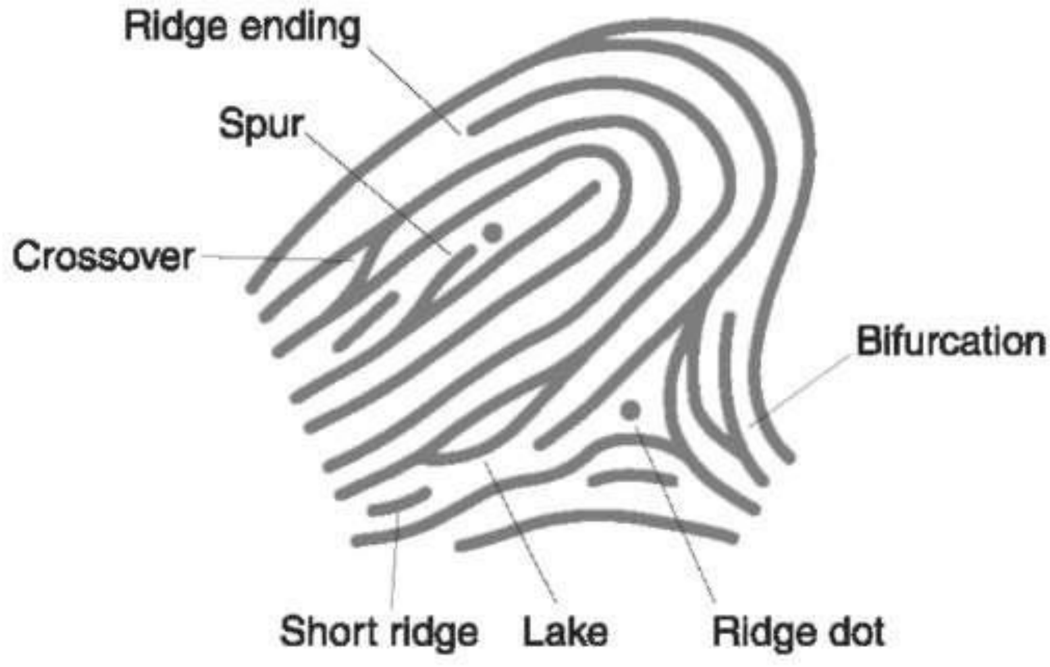
Fingerprints are unique patterns made from friction ridges (raised) and furrows (recessed) which appears on the pads of the fingers and thumbs. A friction ridge is a raised portion of the epidermis on the finger while a furrow is a valley or depression between ridges. These friction ridges, sometimes known as "epidermal ridges" are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges may also assist in gripping rough surfaces and may improve surface contact in wet conditions.



However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows but by a feature known as **Minutia** which are some abnormal points on the ridges. Minutiae are major features of a fingerprint, using which comparisons of one print with another can be made.

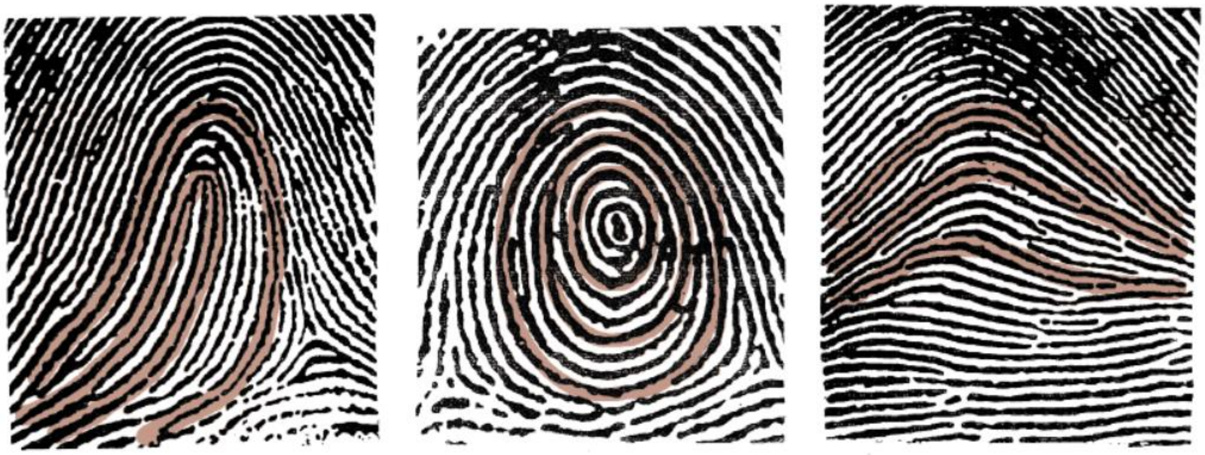
There exist a variety of minutia types including ridge ending, ridge bifurcation, short ridge, island, spur, crossover, delta, core, etc of which ridge ending and ridge bifurcation are the most significant and heavy in usage.

1. **Ridge Ending:** The abrupt end of a ridge.
2. **Ridge Bifurcation:** A single ridge that divides into two ridges.



Fingerprint Recognition

Fingerprint recognition is the process of comparing questioned fingerprint against another to determine if the impressions are from the same finger or palm. A person's fingerprint pattern (the print left when an inked finger is pressed onto paper), is that of the friction ridges on that particular finger. Friction Ridge patterns are grouped into three distinct types—loops, whorls, and arches—each with unique variations, depending on the shape and relationship of the ridges:



- **Loops -** prints that recurve back on themselves to form a loop shape. Divided into radial loops (pointing towards the radius bone, or thumb) and ulnar loops (pointing towards the ulna bone, or pinky), loops account for approximately 60 percent of pattern types.
- **Whorls -** form circular or spiral patterns, like tiny whirlpools. There are four groups of whorls: plain (concentric circles), central pocket loop (a loop with a whorl at the end), double loop (two loops that create an S-like pattern) and accidental loop (irregular shaped). Whorls make up about 35 percent of pattern types.

- **Arches –** create a wave-like pattern and include plain arches and tented arches. Tented arches rise to a sharper point than plain arches. Arches make up about 5 percent of all pattern types.

The general pattern types (loop, whorl or arch) help us group fingerprints into categories for proper and further analysis. Analysts use these general pattern types to make initial comparisons and include or exclude a know fingerprint from other further analysis. To match a print, the analyst uses the minutiae to identify specific points on the unknown fingerprint with the same information in a known fingerprint. Several researches and algorithms have been developed over the decades to create more accurate and efficient matching systems to ascertain the origin (match) of a given fingerprint.

Sandeep Kuma Panda et al (2014) in their research identified three major stages for fingerprint recognition – Preprocessing stage, Minutia Extraction and Minutia Match. The preprocessing stage involved a technique known as Histogram Equalization which entailed improving the global contrast of an image by adjusting the intensity distribution on a histogram. Further enhancement was done using Fourier transform:

$$g(x,y) = F^{-1}\left\{F(u,v) \times \left|F(u,v)\right|^{k}\right\}$$

Where,

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

for x=0,1,2,…….,31 and y=0,1,2,…….,31.

Thereafter, the 8-bit Gray fingerprint image was transformed into a 1-bit image with 0-value for ridges and 1-value for furrows. Further preprocessing techniques such as Block direction Estimation and ROI (Region of Interest) to remove noise were also carried out.

The Minutia extraction process involved Ridge Thinning – which is the elimination of redundant pixels of ridges till the ridges are just one pixel wide. This was achieved by iterative, parallel thinning algorithm. Thereafter, Minutia marking was done using the concept of Crossing Number (CN) which is a widely used technique for minutia extraction.

The Minutia matching stage involved two sub stages: -

- Alignment stage: - Given two fingerprint images to be matched, any one minutia from each image is chosen and the similarity of the two ridges associated with the two referenced minutia points is calculated.
- Match stage: After obtaining two sets of transformed minutia points, the elastic match algorithm is used to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.

$$match\ score = \frac{num(matched\ minutiae)}{\max(num\ of\ minutiae\ in\ i1\ and\ i2)}$$

At the end of their project, they were able to achieve a match score of 0.67 for the same finger and 0.37 for different fingers which is adequate enough to identify a correct fingerprint.

Lukasz Wieclaw (2014) in his study made comparison between different minutiae-based matching algorithms. One of the popular extraction methods he explored was the Direct Grey-Scale Method by Maio and Maltoni [5]. Their basic idea is ridge tracing, by sailing according to the local orientation. The ridge line algorithm attempts to locate at each step, the local maxima, relative to a section perpendicular to the local ridge direction. The algorithm avoids revisiting the same ridge, by keeping track of the points traced so far. They also compared their method to binarization and thinning approaches and concluded that ridge following, significantly reduce computation time.

He also highlighted the Linear Symmetry (LS) filter method by Nilsson and Bigun [6] who proposed that this algorithm based on the concept that minutiae are local discontinuities of the LS vector field. Two types of symmetries - parabolic symmetry and linear symmetry are adapted to model and locate the points in the grey-scale image, where there is lack of symmetry.

In modern days, these extraction and matching process are abstracted and carried out by dedicated electronic devices. We now have complete modules that handle fingerprint recognition. Mobile devices, laptops, locks, etc now have fingerprint sensors that obtain, process and compare prints. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS. The fingerprint module we are going to employ is an optical biometric fingerprint reader/sensor (R307) module with TTL UART interface for direct connections to a microcontroller UART. It can store the fingerprint data in the module and can be configured in 1:1 or 1: N mode for identifying a person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other function.

REVIEW OF SIMILAR PAST PROJECTS

Anil J. and Hong L. [1] compared different biometric technologies and found out that fingerprint is the most widely used technology in the world as it accounts for approximately $100 million of forensic applications. They developed a fingerprint matching algorithm based on point matching (minutiae matching) instead of the traditional image based and ridge-pattern matching. The reason for their choice is the need to develop a robust, simple and fast verification algorithm and to keep the template (image prints) size small.

O. Akinola and A. Abayomi-Alli [2] developed a microcontroller-based fingerprint examination pass system using C# programming language and Futronic FS80 scanner. The system and its interface was developed using Microsoft Visual Studio 2010. Their system worked in two modes: enrollment/registration mode during which the student's information alongside fingerprint is stored into the database and authentication mode during which a print is compared with the data available in the database to determine if the owner of the print is eligible for the exam. Their system gave a convenience value of 98.67% when tested with 75 students.

Another interesting research work which illuminates the world of fingerprint identification is the work of James Stephen, and Prasad Reddy [3]. This work identifies the flaws in minutiae-based fingerprint system. The study proposed the Singular Value Decomposition system (SVD) for the acquisition of images, extraction of features and matching of patterns. The first stage involved acquiring of images through a fingerprint user interface while the feature extraction stage involved the extraction of the features from the images through the Singular Value Decomposition algorithm by splitting it into vectors and taking into consideration, their vectoral positions. The matching stage was achieved through the Euclidean distance algorithm.

Oyediran Mayowa Oyedepo and Wahab Wajeed Bolanle [4] proposed a standalone handheld biometric system. Their system uses Arduino MEGA, Adafruit fingerprint sensor, HC-05 Bluetooth module. The Arduino microcontroller acts as a link between the sensor and the Bluetooth module and converts the data received from the fingerprint sensor to a string that can be sent over Bluetooth. It also parses the data received from the PC and sends appropriate commands to the FPS. They used Arduino because it has multiple serial ports to communicate with both the Bluetooth module and the fingerprint sensor. Like most biometrics system, it has two modes of operation also, registration and verification. Their system successfully identified and verified registered students and also generates a report of registered students in real time.

Although these systems proposed in the above project appear flawless and without a need for improvement, one particular problem that is prevalent in these systems is its dependability on a PC or laptop device for the verification process. This poses as a problem of portability and high dependability on the need for a power supply. Our system will make use a microcontroller and mobile device along with the FPS (fingerprint sensor) to register/enroll students and thereafter verify them for the examination. It will solve the problem of portability and convenience for administrators carrying out authentication process, by eliminating the requirement of a PC, and replacing it with a mobile device.

OBSOLETE

SECTION…

Fingerprint Module

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS. The fingerprint module we are going to employ is an optical biometric fingerprint reader/sensor (R307) module with TTL UART interface for direct connections to a microcontroller UART. It can store the fingerprint data in the module and can be configured in 1:1 or 1: N mode for identifying a person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other function.

Fingerprint processing includes two parts, fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through the sensor and system will generate a template of the finger and compare it with templates of the finger library (database in this case).

For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

The module itself does all complex tasks behind reading and identifying the fingerprints with an on-board optical sensor and fingerprint algorithm. When simple commands are sent, the fingerprint scanner can store different fingerprints.

The database of prints can be downloaded from the unit and distributed to other modules. Although a number of fingerprint reader/sensor modules with slight variations are available now, most have a 4-pin external connection interface. By way of the serial interface, fingerprint reader/sensor module can communicate with a microcontroller that runs on 3.3V or 5V power supply. TX/TD pin of the module connects with RXD (RX-IN pin of the microcontroller), and RX/RD pin connects with TXD (TX-OUT pin of the microcontroller).

Microcontroller

A microcontroller is a self-contained system with peripherals, memory and a processor that can be used as an embedded system. A microcontroller contains one or more CPUs (processor cores) along with memory and programmable input/output peripherals. In this work arduino microcontroller (ATmega328) is used. Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. The board can be told what to do by sending a set of instructions to the microcontroller on the board. To do so the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing are used. Arduino is used in this project because of the advantages it offers which include:

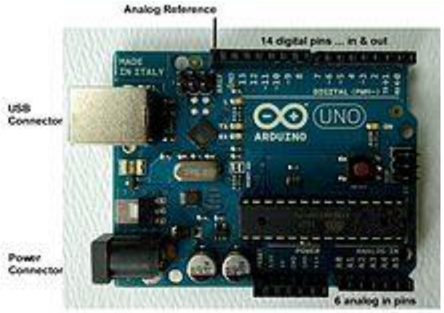
- **Inexpensive** - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50

- **Cross-platform** - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- **Simple, clear programming environment** - The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well.
- **Open source and extensible software** - The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- **Open source and extensible hardware** - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

2.2.1 HARDWARE

Most Arduino boards consist of an Atmel 8-bit AVR microcontroller (ATmega8, ATmega168, ATmega328, ATmega1280, ATmega2560) with varying amounts of flash memory, pins, and features. The 32-bit Arduino Due, based on the Atmel SAM3X8E was introduced in 2012. The boards use single or double-row pins or female headers that facilitate connections for programming and incorporation into other circuits. These may connect with add-on modules termed *shields*. Multiple and possibly stacked shields may be individually addressable via an I²C serial bus. Most boards include a 5V linear regulator and a 16 MHz crystal oscillator or ceramic resonator. Some designs, such as the LilyPad, run at 8 MHz and dispense with the onboard voltage regulator due to specific form-factor restrictions.

Arduino microcontrollers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default bootloader of the Arduino UNO is the optiboot bootloader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor–transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header. Other variants, such as the Arduino Mini and the unofficial Boarduino, use a detachable USB-to-serial adapter board or cable, Bluetooth or other methods. When used with traditional microcontroller tools, instead of the Arduino IDE, standard AVR in-system programming (ISP) programming is used.



An official Arduino Uno R2 with descriptions of the I/O locations

The Arduino board exposes most of the microcontroller's I/O pins for use by other circuits. The *Diecimila, Duemilanove*, and current *Uno* provide 14 digital I/O pins, six of which can produce pulse-width modulated signals, and six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commercially available. The Arduino Nano, and Arduino-compatible Bare Bones Board and Boarduino boards may provide male header pins on the underside of the board that can plug into solderless breadboards. The Atmel 8-bit AVR RISC-based microcontroller used in this project combines 32 kB ISP flash memory with read-while-write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz.

2.2.2 SOFTWARE

A program for Arduino hardware may be written in any programming language with compilers that produce binary machine code for the target processor. Atmel provides a development environment for their 8-bit AVR and 32-bit ARM Cortex-M based microcontrollers: AVR Studio (older) and Atmel Studio (newer).

IDE

The Arduino integrated development environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in the Java programming language. 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. The source code for the IDE is released under the GNU General Public License, version 2.

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. The Arduino IDE employs the program *avrdude* to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware.

A program written with the Arduino IDE 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**.

A minimal Arduino C/C++ program 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()* function exits (ends), the *loop()* function is executed repeatedly in the main program. It controls the board until the board is powered off or is reset

1.1 Bluetooth module

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by Dutch electrical engineer Jaap Haartsen, working for telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables.

Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. This is in the globally unlicensed (but not unregulated) industrial, scientific and medical (ISM) 2.4 GHz short-range radio frequency band.

Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 800 hops per second, with Adaptive Frequency-Hopping (AFH) enabled.

A master BR/EDR Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone necessarily begins as master—as initiator of the connection—but may subsequently operate as slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The specification is vague as to required behavior in scatternets.

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other; however, a quasi-optical wireless path must be viable. Range is power-class-dependent, but effective ranges vary in practice.

Class	Max. permitted power		Typ. range (m)
	(mW)	(dBm)	
1	100	20	~100
2	2.5	4	~10
3	1	0	~1
4	0.5	−3	~0.5

Table 2.1 Ranges of Bluetooth devices by class

Officially Class 3 radios have a range of up to 1 meter (3 ft.), Class 2, most commonly found in mobile devices, 10 meters (33 ft.), and Class 1, primarily for industrial use cases,100 meters (300 ft.).[2] Bluetooth Marketing qualifies that Class 1 range is in most cases 20–30 meters (66–98 ft.), and Class 2 range 5–10 meters (16–33 ft.). The actual range achieved by a given link will depend on the qualities of the devices at both ends of the link, as well as the air conditions in between, and other factors.

The effective range varies depending on propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. Most Bluetooth applications are for indoor conditions, where attenuation of walls and signal fading due to signal reflections make the range far lower than specified line-of-sight ranges of the Bluetooth products.

HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup. The HC-05 Bluetooth Module can be used in a Master or Slave configuration, making it a great solution for wireless communication. This serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband. It uses CSR Bluecore 04-External single chip Rluetooth system with CMOS technology and with AFH (Adaptive Frequency Hopping Feature). By default the factory setting is SLAVE. The Role of the module (Master or Slave) can be configured only by AT COMMANDS. The slave modules cannot initiate a connection to another Bluetooth device, but can accept connections. Master module can initiate a connection to other devices.

1.1.1 PIN DESCRIPTION

The HC-05 Bluetooth Module has 6 pins. They are as follows:

ENABLE:

When enable is pulled LOW, the module is disabled which means the module will not turn on and it fails to communicate. When enable is left open or connected to 3.3V, the module is enabled i.e the module remains on and communication also takes place.

Vcc:

Supply Voltage 3.3V to 5V

GND:

Ground pin

TXD & RXD:

These two pins acts as an UART interface for communication

STATE:

It acts as a status indicator. When the module is not connected to/paired with any other Bluetooth device, signal goes Low. At this low state, the led flashes continuously which denotes that the module is not paired with other device. When this module is connected to/paired with any other Bluetooth device, the signal goes High. At this high state, the led blinks with a constant delay say for example 2s delay which indicates that the module is paired.

BUTTON SWITCH:

This is used to switch the module into AT command mode. To enable AT command mode, press the button switch for a second. With the help of AT commands, the user can change the parameters of this module but only when the module is not paired with any other BT device. If the module is connected to any other bluetooth device, it starts to communicate with that device and fails to work in AT command mode.

1.2 Crystal Oscillator

A crystal oscillator is an electronic oscillator circuit that uses the mechanical resonance of a vibrating crystal of piezoelectric material to create an electrical signal with a precise frequency. This frequency is often used to keep track of time, as in quartz wristwatches, to provide a stable clock signal for digital integrated circuits, and to stabilize frequencies for radio transmitters and receivers. A crystal oscillator, particularly one made of quartz crystal, works by being distorted by an electric field when voltage is applied to an electrode near or on the crystal. This property is known as electrostriction or inverse piezoelectricity. When the field is removed, the quartz - which oscillates in a precise frequency - generates an electric field as it returns to its previous shape, and this can generate a voltage. The result is that a quartz crystal behaves like an RLC circuit.

Crystal oscillator circuit usually works on the principle of the inverse piezoelectric effect. The applied electric field will produce a mechanical deformation across some materials. Thus, it utilizes the vibrating crystal's mechanical resonance that is made with a piezoelectric material for generating an electrical signal of a particular frequency.

Usually quartz crystal oscillators are highly stable, consists of good quality factor (Q), they are small in size, and are economically related. Hence, quartz crystal oscillator circuits are more superior compared to other resonators like LC circuits, turning forks.

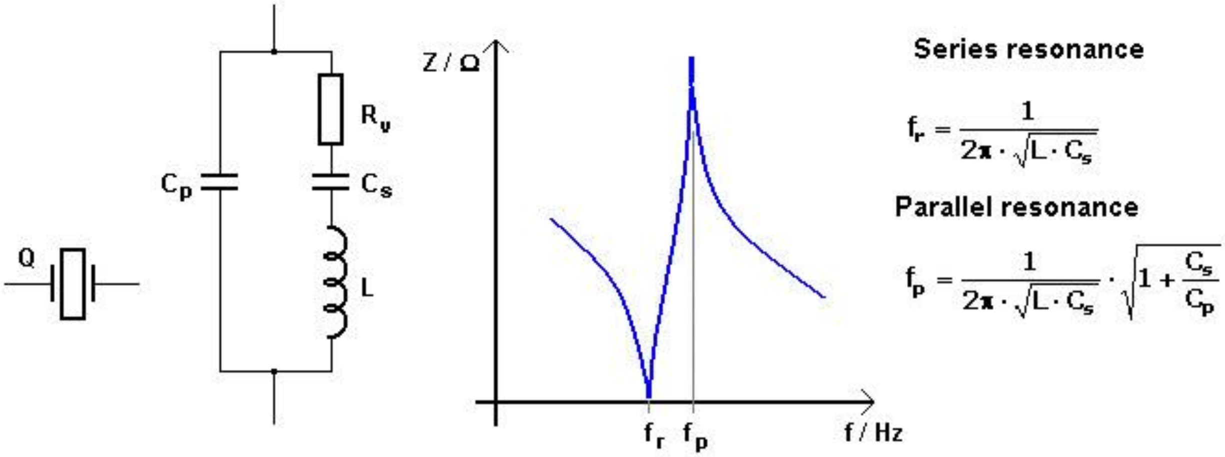

Q
C_p
R_v
C_s
L
Z / Ω
f_r
f_p
f / Hz
Series resonance
$f_r = \frac{1}{2\pi \cdot \sqrt{L \cdot C_s}}$
Parallel resonance
$f_p = \frac{1}{2\pi \cdot \sqrt{L \cdot C_s}} \cdot \sqrt{1 + \frac{C_s}{C_p}}$

Diagram of the crystal and equivalent circuit

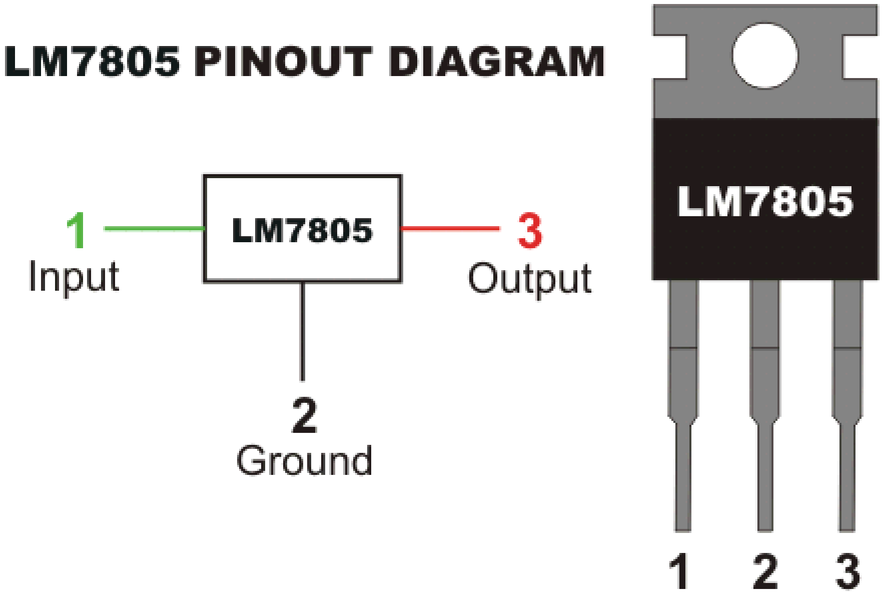
The equivalent electrical circuit also describes the crystal action of the crystal. This is shown above. The basic components used in the circuit, inductance L represents crystal mass, capacitance Cs represents compliance, and Cp is used to represent the capacitance that is formed because of crystal's mechanical moulding, resistance R represents the crystal's internal structure friction, The quartz crystal oscillator circuit diagram consists of two resonances such as series and parallel resonance, i.e., two resonant frequencies.

Generally, in the design of microprocessors and microcontrollers, crystal oscillators are used for the sake of providing the clock signals. A 16MHz crystal ships in with the ATMega328 microcontroller. This particular crystal oscillator which is having cycle rate at 16MHzis used to generate clock pulses which are required for the synchronization of all the internal operations in the microcontroller.

1.3 Voltage Regulator

A voltage regulator is an electronic circuit that provides a stable DC voltage independent of the load current, temperature and AC line voltage variations. A voltage regulator may use a simple feed-forward design or may include negative feedback. There are two types of voltage regulators. Linear and switching voltage regulators. Linear voltage regulator acts as a voltage divider and it's the most commonly used type when designing low power and low cost circuit. Switching regulators are used when there is a large difference between input and output voltage.

The **voltage regulator IC 7805** is actually a member of 78xx series of voltage regulator ICs. It is a fixed linear voltage regulator. The xx present in 78xx represents the value of the fixed output voltage that the particular IC provides. For 7805 IC, it is +5V DC regulated power supply. This regulator IC also adds a provision for a heat sink. The input voltage to this voltage regulator can be up to 35V, and this IC can give a constant 5V for any value of input less than or equal to 35V which is the threshold limit.



7805 pin diagram

PIN 1-INPUT

The function of this pin is to give the input voltage. It should be in the range of 7V to 35V. We apply an unregulated voltage to this pin for regulation. For 7.2V input, the PIN achieves a maximum efficiency.

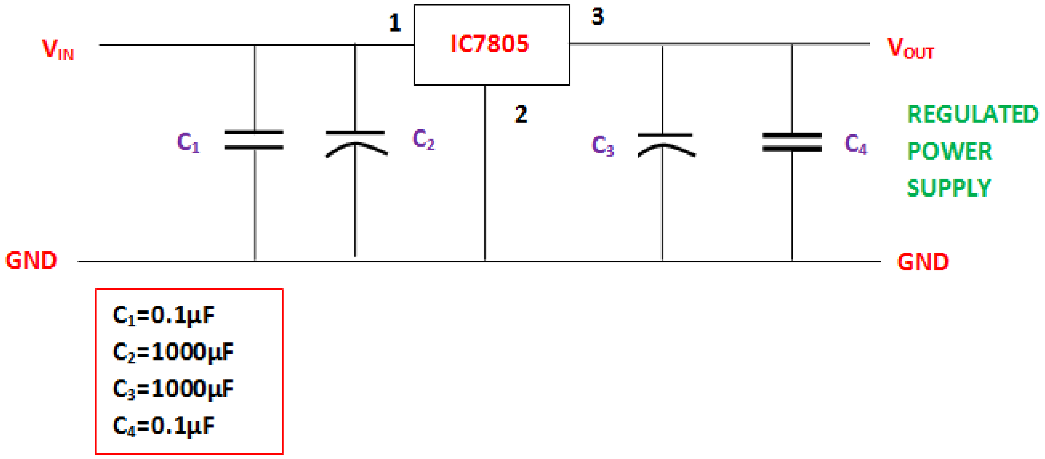
PIN 2-GROUND

For output and input, this pin is equally neutral (0V).

PIN 3-OUTPUT

This pin is used to take the regulated output.

Voltage regulator is used in the power supply circuit to provide a constant 5V dc supply to the microcontroller, fingerprint module and the bluetooth module.



Power supply circuit

1.4 Capacitors

A capacitor is a passive two-terminal electrical component that stores potential energy in an electric field. The physical form and construction of practical capacitors vary widely and many capacitor types are in common use. Most capacitors contain at least two electrical conductors often in the form of metallic plates or surfaces separated by a dielectric medium. A conductor may be a foil, thin film, sintered bead of metal, or an electrolyte. The non-conducting dielectric acts to increase the capacitor's charge capacity. Materials commonly used as dielectrics include glass, ceramic, plastic film, paper, mica, and oxide layers. Capacitors are widely used as parts of electrical circuits in many common electrical devices. Unlike a resistor, an ideal capacitor does not dissipate energy.

Capacitor

In this project, capacitors are used in two major areas – decoupling (bypass) in the IC and power supply filtering. A decoupling capacitor’s job is to suppress high-frequency noise in power supply signals. They take tiny voltage ripples, which could otherwise be harmful to delicate ICs, out of the voltage supply. Also since they resist a sudden change in voltage, they are connected in parallel in the power supply circuit to reduce ripples in the power supply.

2.7 Resistors

A resistor is a passive two-terminal electrical component that implements electrical resistance as a circuit element. In electronic circuits, resistors are used to reduce current flow, adjust signal levels, to divide voltages, bias active elements, and terminate transmission lines, among other uses.

In this project, resistors are used in LED current limiting. Resistors are key in making sure LEDs don't blow up when power is applied. By connecting a resistor in series with the LED, current flowing through the two components can be limited to a safe value.

REFERENCES

[1] Anil Jain, Lin Hong. An Identity Authentication System Using Fingerprints.

[2] O. A. Akinola1, A. Abayomi-Alli (August, 2015). Development of a Microcontroller Based Fingerprint Examination Access Control System.

[3] James Stephen, Prasad Reddy (2012). Implementation of Easy Fingerprint Authentication with Euclidean and Singular Value Decomposition Algorithm. International Journal of Software Computer Application, 3(2), 1-15.

[4] Oyediran Mayowa Oyedepo, Wahab Wajeed Bolanle. Development of An Examination Authentication Embedded System Based on Fingerprint Approach.

[5] MAIO D., MALTONI D., Direct Gray-Scale Minutiae Detection In Fingerprints, IEEE Trans. Pattern Anal. Machine. Intell., vol 19, pp. 27-40, USA, 1997.

[6] BIGUN J., NILSSON K., Using linear symmetry features as a pre-processing step for fingerprint images, Conf. Audio and Video Based Biometric Person Authentication, pp.247–252, Sweden, 2001.