Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.4, No.8, 2014

Design of a GSM-Based Biometric Access Control System

[1]Hussaini Habibu, [2]Adamu Murtala Zungeru, [3]Ajagun Abimbola Susan, [4]Ijemaru Gerald Kelechi [5]Oresanya Babajide Oluwatosin

[1,3,5]Department of Electrical and Electronics Engineering
Federal University of Technology Minna, Nigeria

[2,4]Department of Electrical and Electronics Engineering
Federal University Oye-Ekiti, Nigeria

habufarid@futminna.edu.ng, adamuzungeru@ieee.org, bimbo.ajagun@futminna.edu.ng, gerald.ijemaru@fuoye.edu.ng

Abstract

Access control systems restrict access to a secured premise or other secured devices (like a safe) only to authorized persons. In this design a biometric (fingerprint based) access control system was developed with added versatility: remotely Adding/Removing users and monitoring the system's operation via a GSM Phone. The administrator phone sends SMS commands to the system to put it in the desired operating modes (as security situations arise) and to add/remove users of the premise; thus, the system can work both independently and as dictated by the administrator. The main components are a Fingerprint Module, a GSM/GPRS modem, the door & its control circuitry, and an AT89C52 microcontroller. The microcontroller polls the SMS received by the GSM modem, interprets it to puts the system in the desired mode, sends appropriate SCAN/DELETE/ADD command to the fingerprint scanner, opens/closes the door at each access request by any user (registered or not) based on the present system mode and command it receives from the scanner. The microcontroller's code is written in ASSEMBLY language using KEIL MICRO-VISION3 emulator/debugger. At completion, the system quite responded in the four set modes: it adds/deletes user fingerprints appropriately, shuts-off when instructed, opens/closes the door when a registered fingerprint is recognized, displays messages appropriately on the LCD screen and receives/sends the appropriate SMS to the Administrator's phone.

Keywords: Access Control System, Biometric, GSM, SMS, Administrator

1. Introduction

Access Control is a security measure of restricting entrance/exit or the usage of a premise or some other resources only to authorized persons. Electronic access control systems eliminate the problems associated with lost keys; they have the ability to instantly add, allow, restrict or deny someone's access, and to be able to immediately generate an activity report on people's movements. Some of these systems use simple keypads with PIN (personal identification number) codes, "swipe" or insert cards such as magnetic stripe, non-contact "proximity cards" or RFID (Radio Frequency Identification). They are connected to an intelligent door controller which contains stored programming information from an access-control software about who is allowed where and when, as well as other functions that the system can perform. Proximity cards are used in conjunction with an access control card reader connected to the door controller [1].

Current trends are now based on biometric data technology. Biometric data are methods used to uniquely identify an individual; examples amongst many include Fingerprint pattern, Retina Colour, signatures, facial scans, voice pattern etc. Biometrics is the name given to the various methods of capturing, storing, and utilizing biometric data. Two major uses of biometrics include the identification of individuals for the purposes of controlling access, and various applications for tackling and preventing crime [2].

Also, telecommunication has been redefined: applications of mobile phone aren't only restricted to sending SMS (Short Message Services) or making conversations. New innovations which has been generated from it has further enhanced its capabilities making it suitable for remote controlling applications - the GSM/GPRS module; it is used to establish communication between a computer (or an embedded controller) and a GSM phone. GSM: Global System for Mobile Communication is an architecture used for mobile communication in most of the countries. SMS (Short Message Service) is a service available on most digital mobile phones that permits the sending of short messages (also known as text messaging service). Global Packet Radio Service (GPRS) is an extension of GSM that enables higher data transmission rate. GSM/GPRS module consists of a GSM/GPRS

modem assembled together with power supply circuit and communication interfaces (like RS-232, USB, etc.) for a controller.

The GSM based Biometric Access controlled System is a reliable circuit that implements biometric/fingerprint technology along with GSM/GPRS to perform the work of controlling the accessibility of a premise (access control). The purpose of this is to replace current methods with a non-porous and versatile system. This work will help security personnel and owners of a premise to remotely authorize users of the premise and control the accessibility of the premise as security demand requires.

The main aim of this design is to develop a (stand-alone) Access Control unit based on Fingerprint Technology that will be remotely controlled via a GSM phone to meet changing security needs.

The system should fulfil the following objectives:

i. Automatically scan users' fingers when placed on the scanner, hence eliminate the use of buttons.
ii. Add up and store, or delete as many fingerprint data (up to 256) of the users as possible.
iii. Allow registered users access to the premise and totally denying access to an unauthorized person.
iv. The administrator will be able to remotely allow/deny access, add/remove users or even shut- down the system remotely, hence ensuring an optimum security of the premise.
v. The system should be able to work in four modes (Default, Enrolment, Acknowledgment and Shut-off mode); each should be configurable via SMS from the administrator's GSM.
vi. The controller should be able to communicate with the GSM module and the fingerprint module simultaneously.
vii. In the acknowledgement mode, the system will send access-request SMS to the administrator's GSM, Access will be granted only if the Administrator acknowledges such.

2. Review of Relevant Work in Access Control System

Vinay Chada [3] designed a Microcontroller Based Access Control/Security Lock System based on key-codes. He implemented the work using the Motorola 16-pin MC68HC705KJ1 microcontroller, a 4x3 keypad and an external EEPROM memory to store user pins. The system provides means for a user to change his password any number of times using the keypad. Jayanta K. P. and R. N. Das Choudhury in their work [4], interfaced mobile communication with embedded system to prevent/control access to a vehicle ignition system in a work titled an Embedded Automobile Engine - Locking System Using GSM Technology. In the design, an AT89S52 microcontroller was interfaced with a keypad and GSM modem to protect the vehicle from unauthorized access. The car engine can be started only by entering a correct password; entering an incorrect one thrice, the system will deny further access and send an intrusion alert to the owner's mobile via the GSM modem. M. O. Onyesolu and I. M. Ezeani [5] in a paper on ATM (Automated Teller Machines) Security Using Fingerprint Biometric Identifier sought biometric means of accessing ATM machines to replace passwords (key codes) in order to reduce crimes associated with loss/theft of passwords and vulnerability of users account to cyber-crimes. Amurthy and Redddy [6] also developed an embedded fingerprint system also for ATM security applications. A customer's fingerprint and mobile number are collected while registering an account; whenever he access the ATM machine, placing a finger on the fingerprint module, it automatically generates different 4-digit code and sends it as a message to his mobile phone (through a GSM modem connected to the microcontroller). The code is received by the customer and is entered into the ATM machine. After entering, the system checks whether it is a valid one or not and allows the customer further access. In [7], the Authors developed A Prototype of a Fingerprint Based Ignition Systems in Vehicles. In the prototype, an image capturing, enhancement, matching of fingerprints and ignition control was written in visual basic 6.0 and ran on a PC. Users' fingerprints were matched and the result of the match was used to activate the ignition control circuitry. In 2011, M/S Wine yard Technologies [8] developed a project on Fingerprint Based Access Control System. In the system, a fingerprint scanner was interfaced to an ATMEL flash microcontroller to control the scanning process and the door (via an electronic lock) opens for an authorized person and doesn't open for an unauthorized attempt. The work further recommended interfacings with a GSM modem to allow an administrator monitor access activities or remotely control the system.

These past works extensively exploit three technologies: embedded systems, GSM and Biometrics. However, our work is an improvement on them as it implements automatic scanning of users' fingers and it's interfaced with a GSM modem to allow an administrator monitor access activities and remotely control the system.

3. System Design and Implementation

This section will talk about the design procedures and the implementation of the system. The block diagram shown in Figure 1, gives a pictorial view of the working principle of the system.

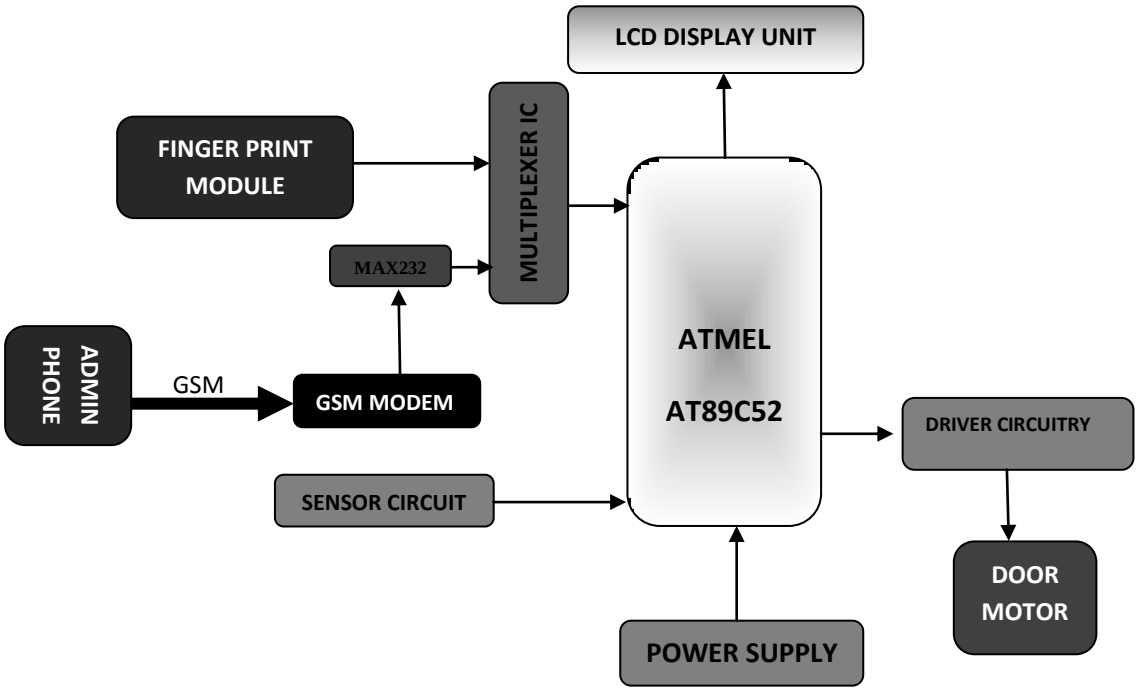


Figure 1. Complete Block diagram of the System

The SMS containing commands to the GSM/GPRS module and are polled by the microcontroller to put the system in any of the four operating modes which are:

Default mode: The Fingerprint Scanner automatically scans a finger placed on it, and compares it against its template. If a match exists, "Access Granted" is displayed on the LCD and the door is opened, otherwise, "access denied" is displayed.

Enrolment Mode: The user places his finger on the module and is scanned automatically. The scanned fingerprint is then stored in the scanner's memory and the microcontroller generates a unique 3-digit for the fingerprint and sends it to the GSM phone (as a means of identifying each user). After a fingerprint is successfully captured, the system returns to default mode.

Acknowledging Mode: If the user's fingerprint is an enrolled one, the GSM module will send an Access Request SMS to the Admin Phone (stating the user's unique 3-digit number), displays "Contacting Admin…" on the LCD and waits for the Admin to acknowledge the request. IF the admin acknowledges the request, the microcontroller opens the door and displays "access granted". If due to network errors or the admin refuses to reply for some time (30 seconds), the system automatically takes it as an access denied.

Shut-off Mode: "System-shut-off" is displayed on the LCD, the fingerprint scanner is switched off and the door is permanently locked.

3.1 *Power Supply Section*

The Microcontroller, GSM modem, Fingerprint scanner require 5V DC while the motor and relay coil require 12V DC for their operation. The 240V AC supply voltage is thus stepped down, rectified, filtered, and regulated to get the desired 5V DC voltage.

- A step down transformer: 12-0-12V center-tap, stepping down 240V to 12V AC.
- Bridge rectifier: four 1N4007 diodes, convert the 12V AC voltage signal to a direct current (DC) voltage.
- Filter capacitors: 2200uF and 440uF. The 12V DC output of the rectifier has lots of ripples. Obtaining a smooth DC voltage at the output, the 12V DC is fed to an electrolytic capacitor which allows DC signals to flow through it, but blocks AC signals. This function makes it very useful in filtering of signals.
- Fixed positive voltage regulator: LM7805 produces a fixed output voltage of 5V from its 12V input voltage.

The output DC voltage ıs gıven by

$$V_{L(dc)} = \frac{\sqrt{2}V_{in}}{\pi K} \quad (1)$$

Where K=10 (transformer Ratıo); V_{IN}= 240V,
Therefore $V_{L(dc)} = \frac{\sqrt{2}\times 240}{\pi \times 10} = 10.79V$

Hence the output Voltage ıs approximately 11V. The relay used in the door control circuitry requires 12V and is still powered with this stage's 11V output.
The filter capacitance value is calculated using:

$$C = \frac{1}{(4VrF\sqrt{3})} \quad (2)$$

Where: V = Supply voltage (12V), r = Ripple factor (0.1), F = Frequency (50Hz)

Hence, $C = \frac{1}{(4 \times 12 \times 0.1 \times 50 \times \sqrt{3})}$

And $C = 0.002405F = 2405\mu F$
Thus a combination of 2200uF and 470uF is used to give an equivalent capacitance value required to produce the smooth DC output.

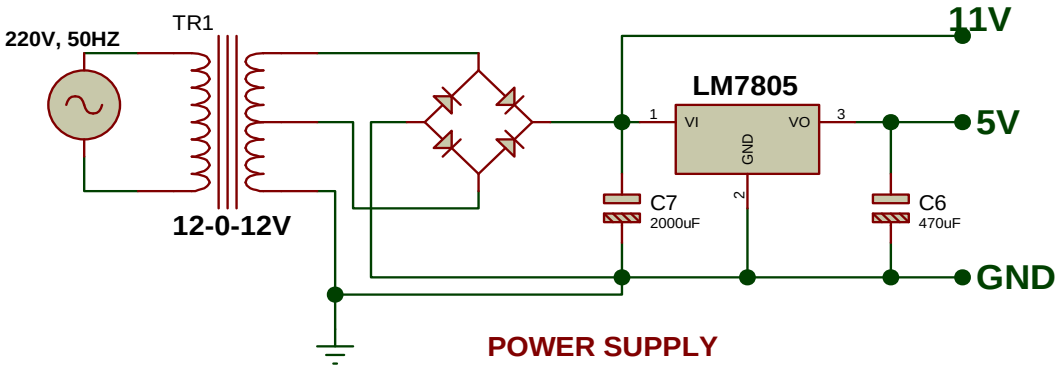


Figure 2. Power supply circuit

3.2 Microcontroller Section
The AT89C52 is an 8-bit microcontroller with 8Kbytes of Flash ROM, 128 Bytes of RAM, 3 Timers/counters, one full-duplex UART channel and up to 1000write/erase cycles. It's a 40-pin device with 32 input/output (I/O) pins making up the four 8-bit ports (P0 to P3). Each port is basically a bi-directional I/O port; some have other additional functions [24].

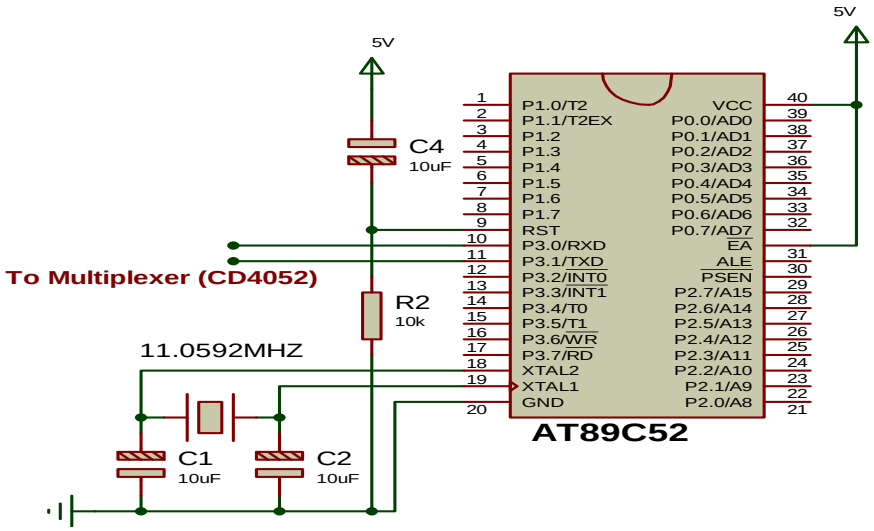


Figure 3. Microcontroller BASIC hardware configuration

The basic external components required to have a working microcontroller are: the crystal oscillator, capacitors and resistors.

Power supply (VCC) = 5V, 50mA. Oscillator frequency = 11.0592MHz

Therefore, 1Machine cycle, $Mc = \frac{number\ of\ instructions\ per\ machinecycle}{oscillator\ frequency}$ (3)

$$\therefore Mc = \frac{12}{11.0592 \times 10^6}$$

$$Mc = 1.086\mu s$$

The 11.0592MHz crystal is chosen as it offers 0% tolerance for serial communication.

The door control circuitry, serial communication circuitry, LCD circuitry respectively connected to ports 2, 3, and 1.

UART Configuration: Data/commands to and from the GSM modem, Fingerprint scanner and the microcontroller is via serial transfer. Since the AT89C52 has only one serial channel, both devices share the channel using a multiplexer IC – hence, pin 3 and 13 of the multiplexer is soldered directly to pin10 (TX) and pin11(RX) of the microcontroller. The Baud Rate is generated using Timer1 in 8-bit mode, the value to be loaded into the TH1 register is determined by the formula:

$$TH1 = 256 - \frac{2^{SMOD} \times Oscilator\ Frequency}{192 \times Baud\ Rate} \quad (4)$$

$$TH1 = 256 - \frac{2^0 \times 11.0592}{192 \times 96500}$$

For a 96,500bps Baud rate (for the GSM modem), using a 11.0592MHz Crystal Oscillator and the SMOD bit of the PCON register at zero, i.e., SMOD=0. Thus, in the assembly language programming, the TH1 register is loaded with 0FAH. Same calculation is done for a 11,000bps baud rate (for the fingerprint scanner). The RX pin (P3.0) and TX pin (P3.1) are respectively connected to pins 13 (common X) and 3 (Common Y) of the multiplexer IC (see 3.2.4).

3.3. Lcd Display Section

A HITACHI 44780 16x2 Liquid Crystal Display (LCD) is interfaced with the microcontroller (Port1). The LCD has 14 pins (Fig. 4) with the functions highlighted in Table 1 as:

Table 1. LCD Pin descriptions

Pin	Symbol	I/O	Description
1	V_{SS}	---	Ground
2	V_{CC}	---	+5V power supply
3.	V_{EE}	---	Power supply to control contrast (screen brightness)
4.	RS	I	If RS=0, LCD command register is selected and RS=1 selects data register.
5.	R/W	I	Allows data to be written or read from the LCD. R/W=0 (for write) R/W=1 (for read).
6.	E	I/O	Enable pin. Used by the LCD to latch information presented to its data bus. A high-to-low pulse must be sent to this pin for the LCD to latch the data presented.
7 – 14	DB0 to DB7	I/O	The LCD's 8-bit data bus: used to send data to the LCD or read content of its registers.

Some Configuration commands (Hexadecimal) used

01	to clear the screen
06	shift cursor to the right
08	turn off display and cursor
0A	off display, turn on cursor
0C	on display, turn off cursor
0E	display on, cursor blinks
18	shift entire display leftward
1C	shift entire display rightward
80	take cursor row1 column1
C0	take cursor to row2 column1
38	configure the LCD as a 2-line 5x7 matrix character display

The microcontroller is programmed to send the configuration commands to the LCD (with RS=0) and the data to be displayed (with RS=1). Pin R/W is grounded (data is continously written to the LCD), pins D0 – D7 are connected to Port1, EN to P3.4, RS to P3.5. And V_{EE} pin to 5V power rail through a 1K variable resistor in order to vary the LCD screen intensity.

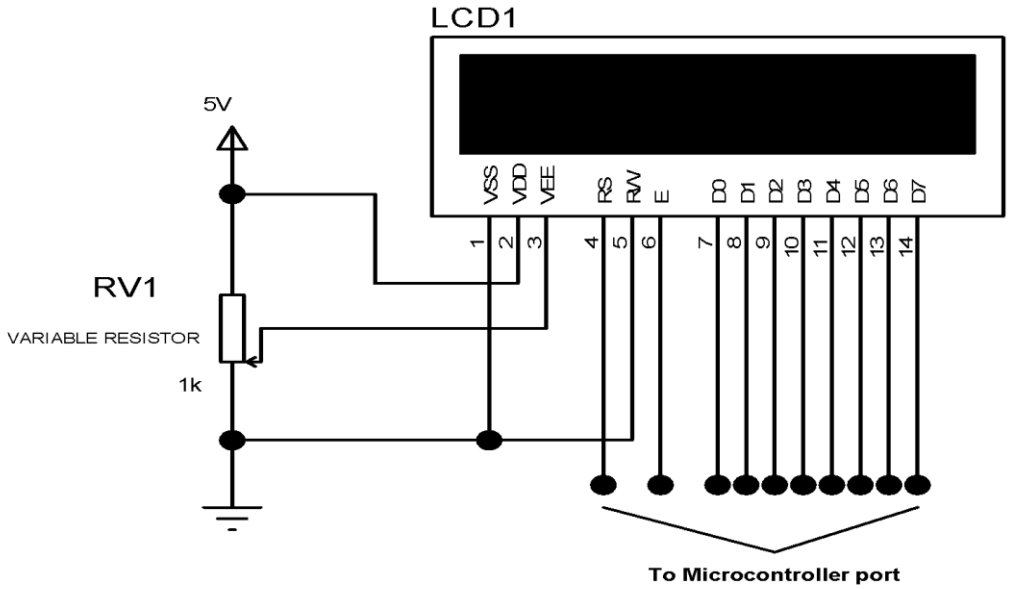
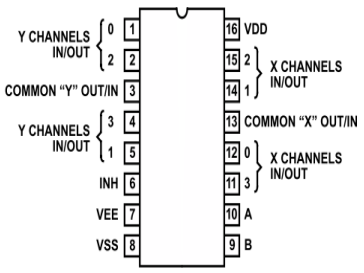


Figure 4. LCD Terminations.

3.4. The (CD4052) Multiplexer IC

The GMS modem as well as the fingerprint module both sends and receive instructions serially to and from the microcontroller, i.e., both using the microcontroller's serial pins. The AT89C52 microcontroller used in this project has a SINGLE UART feature (just a pair of RXD and TXD pins). This single UART pins are thus multiplexed between both devices using an analogue/Digital multiplexer IC – CD4052. The CD4052BC is a 4-channel multiplexer with two binary control inputs, (A and B) and an inhibit input. The two binary input signals select 1 or 4 pairs of channels to be turned on and routes the inputs to the selected outputs [25].

Table 2. CD4052 Truth Table



INPUT STATES			ON-CHANNELS
Inhibit	B	A	
0	0	0	0X & 0Y
0	0	1	1X & 1Y
0	1	0	2X & 2Y
0	1	1	3X & 3Y
1	*	*	NONE

Figure 5.CD4052 Multiplexer IC

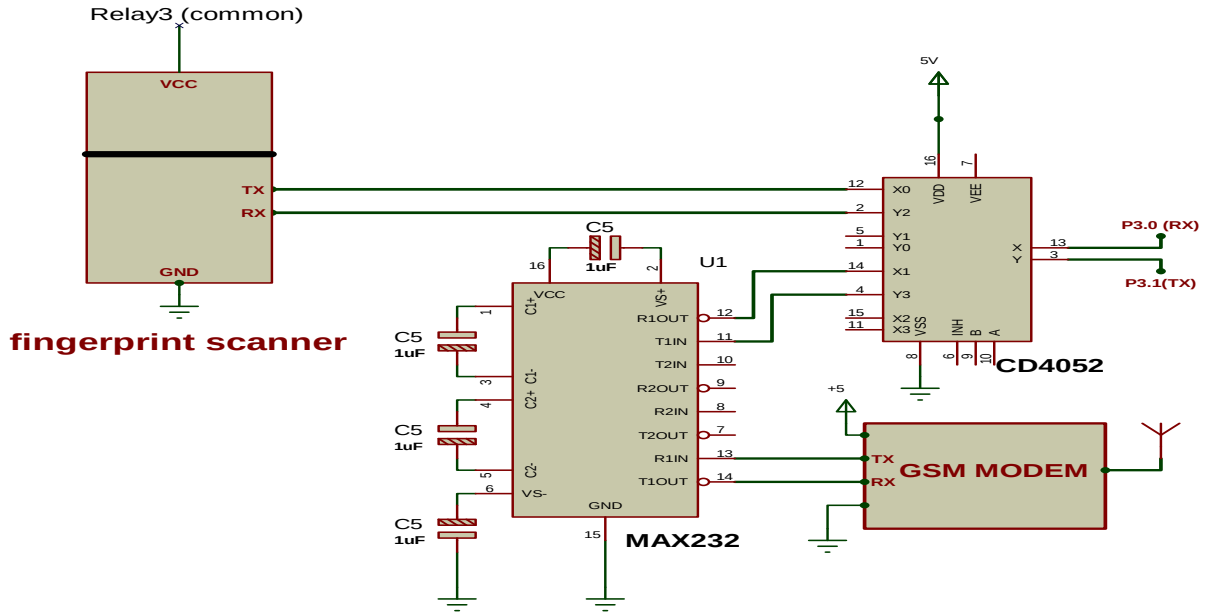


Figure 6. Multiplexing Circuit for the fingerprint scanner and the GSM modem

3.5. The GSM/GPRS Modem

The GSM modem used is the WAVECOM 2004a Modem. The features are: DC input voltage (5 – 30V), supports **Extended AT commands**, RS232 interface (DB9 type, female), Dual band GSM 900/1800Hz, supports all SIM cards and fully compliant with the ETSI GSM specifications.

Figure 7. WAVECOM GSM modem

Installation Steps:

i. Press the SIM notch to eject the SIM card holder and insert the SIM card

ii. Connect the antenna to the antenna holder and connect the DC power supply.

iii. Connect the RS232 cable to the DB9 connector for interfacing the AT commands.

The GSM modem is interfaced with the microcontroller through the voltage-level converter (MAX232) and then connected to the multiplexer IC. Only three signals of the serial interface of the modem are needed for the serial communication i.e., the TXD, RXD and GND: the TX and RX pins are connected respectively to pins 13 and 14 of the MAX232.

3.6 The Logic Level Converter And DB9 Cable

The GSM modem serial communication requires TIA/EIA-232-F voltage levels but the microcontroller is a standard TTL logic device; hence a voltage level converter is used to convert between the TTL and RS232 voltage levels. The MAX232 is a 16-pin DIL chip incorporating two receivers and two transmitters with a capacitive voltage generator made up of four 1uF capacitors (to supply the TIA/EIA-232-F voltage levels) and the IC operates with a 5V supply. Each receiver can accept ±30V TIA/EIA-232-F inputs and converts to 5-V TTL/CMOS levels. Each driver converts TTL/CMOS input levels into TIA/EIA-232-F levels [26]. Hence, the microcontroller outputs TTL logic level RS232 signals from its TX pin (P3.1) and can receive TTL level RS232 signals from its RX pin (P3.0). Thus, the MAX232 converts TTL logic signals of the microcontroller to the TIA/EIA-232-F voltage levels required for the GSM modem.

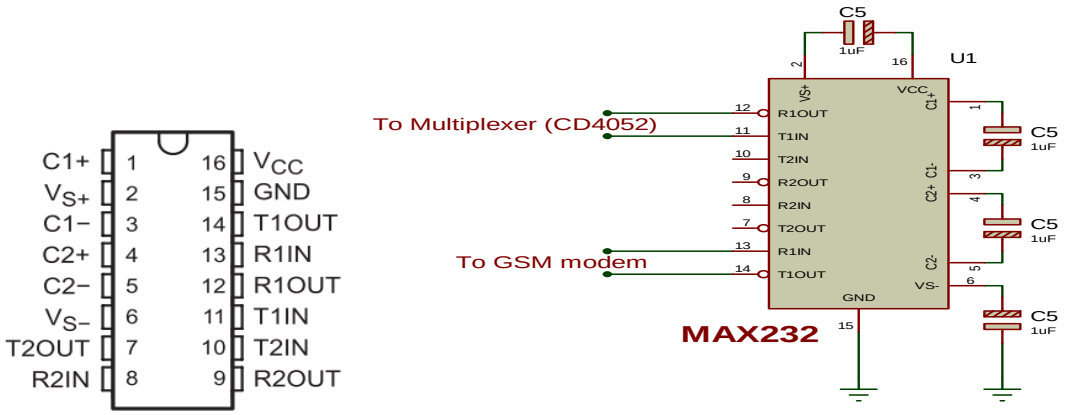


Figure 8. MAX232 Voltage-level converter.

The serial communication cable/connector (DB9) has eight data bits (lines), three of which are used to establish connection between the modem and MAX232, i.e. Transmit (TX), Receive (RX), and ground (GND). These three pins are identified using a multi-meter: Pin 5 is ground, pin 3 TX pin, while pin 2 is the RX pin. Pins 13 (R1IN) and 14 (T1OUT) of MAX232 are connected to the GSM modem's TX and RX respectively. Pins 11 (T_{in}) and 12 (R_{out}) of MAX232 are connected to the RX and TX pins of the multiplexer IC (pins).

3.7 The Fingerprint Scanner

SM630 is an Optical fingerprint verification module consisting of an optical sensor, high-performance DSP and a 64KB flash memory. The operating voltage is 4.3 to 6.5V and an operating current of less than 80 mA when operated at 5V. The communication interface is via standard serial interface at TTL logic at a baud rate of 57600Bps. The module has a fingerprint template of 768. There are only four cables to connect the module to the microcontroller:

Pin1= Positive power supply connected to the common terminal of relay3
Pin2 = Module serial Transmit pin (TX) connected to pin of the CD4052 multiplexer
Pin3 = module serial Receive pin (RX) connected to pin of the CD4052 multiplexer
Pin4 = Negative power supply connected to ground). The pin to the edge of the board is pin4.

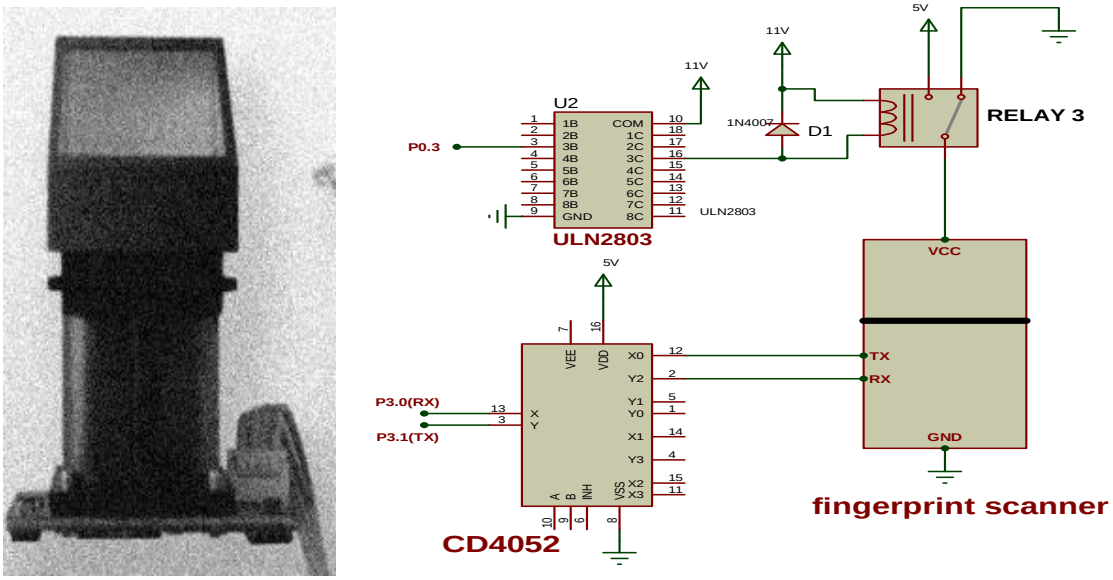


Figure 9. SM630 Fingerprint scanner.

Communication between the microcontroller and the module is coded as an **Information Packet**. In writing the Assembly program to communicate with the module, the format of each packet is as follows:

- **Packet head** (1byte): 0x4D and 0x58
- **Packet flag** (1byte): 0x10 (for command); 0x20 (for data); 0x30 (for response)
- **Packet length** (1byte): length of the content in the packet

- **Content** (N-byte) **Checksum** (1byte) [24].

Typical formats of instruction packets is found in the Table 3 (since the packet head is constant throughout, it is omitted in Table 2).

- **Adding fingerprint**: the microcontroller sends the ADD packet (containing the start location of the to-be-added fingerprint), if received, the module responds with RECEIVE CORRECT, else PARAMETER ERROR. After processing the fingerprint, it responds with OPERATION SUCCESSFUL and if no finger is presented, it responds TIME OUT.
- **Deleting fingerprint**: on receipt of the delete packet containing the ID of the fingerprint to be deleted, Module responds with RECEIVE CORRECT and OPERATION SUCCESSFUL after successful delete. Else, it responds with PARAMETER ERROR.

Table 3. Content of instruction packets sent to and received from the Scanner for various operations and responses.

Function	**Description**	**Packet flag**	**Length**	**Content**	**Checksum**
Scan fingerprint	Scan	0x10	0x30	0x40+0x00+0x00	0Xf8
	"Receive correct" response	0x30	0x01	0x01	0xD7
	Parameter error	0x30	0x02	0x40+0x35	0x4C
	"operation Successful"	0x30	0x02	0x04+0x31	0x48
	processing failure	0x30	0x02	0x40+0x34	0x4B
	Time-out	0x30	0x02	0x40+0x33	0x4A
Delete Fingerprint	delete	0x10	0x03	0x42+0x00+0x00	0xFA
Search fingerprint	search	0x10	0x05	0x44+0x00+0x00+0x00+0x10	0x0E
	Fingerprint found	0x30	0x04	0x44+0x39+hig & low bytes of the found fingerprint	0x..
	No match	0x30	0x02	0x44+0x3A	0x55
	processing failure	0x30	0x02	0x44+0x34	0x4F

- **Searching fingerprint**: on receiving a SEARCH instruction, the module waits for a finger to be placed on its screen and responds with OPERATION SUCCESSFUL. If a match is found, it again responds with FINGERPRINT FOUND else with NO MATCH. If the fingerprint quality is poor, it responds with PROCESSING ERROR [27].

3.8 The Sensor Circuitry.

The sensor circuitry is made up of an LDR (light dependent resistor) biased with a 50K variable resistor to trigger pulse generation through a 555timer configured in Monostable mode. On receiving the pulse at P2.3 of the microcontroller, the microcontroller recognizes that a finger is placed on the fingerprint scanner and thus sends the SCAN packet to it.

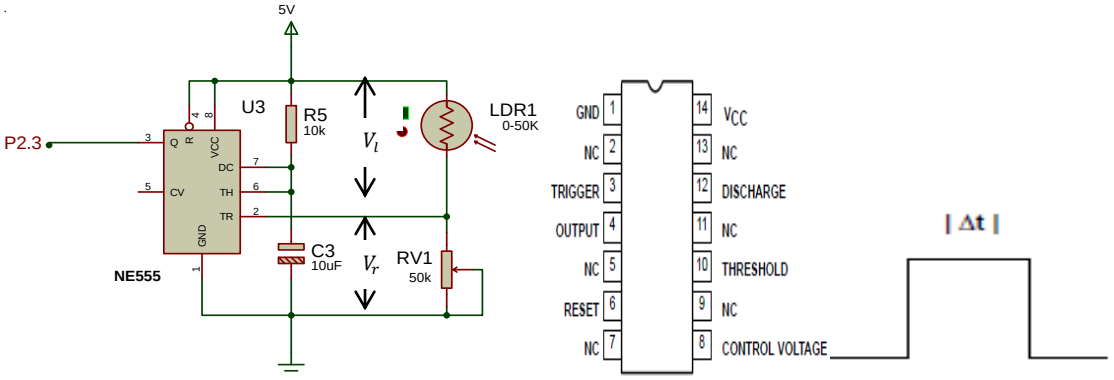


Figure 10. (a) sensor circuitry (b) NE555 timer IC (c) output pulse generated

$$\Delta t = 1.1R_5C_3 \tag{5}$$

Hence for $R_5 = 10K$ and $C_3 = 10\mu F$, $\Delta t = 0.11sec$.

$V_l = voltage\ across\ the\ LDR$ and $V_r = volt\ across\ the\ variable\ tesistor = volt\ at\ pin\ 2$ and R_l is the resistance of the LDR (R_l varies inversely with light intensity).

$\therefore V_r = 5 \times \frac{R_l}{R_l+50K}$ and as soon as the LDR is obstructed by a finger, light intensity on it becomes low, R_l becomes extremely high causing V_r to become low ($<<4V$) and hence, the timer pin2 is triggered (a high-to-low pulse on pin2 triggers the timer) and the timer generates a pulse of width Δt on pin3 (shown in Fig. 10 (c)). The microcontroller thus sends a scan command to the fingerprint scanner.

3.8.1 Door Control and Switching Circuitry.

Made up of three Relays (12V DC), one 12V DC motor, three 1N4001 diodes and the UNL2803 relay Driver IC.

- The ULN28023A contains eight Darlington transistors (common emitters) and suppression diodes for inductive loads. Each Darlington has a peak current rating of 600mA and can withstand at least 50V in the off state. It has a 2.7kW input resistor for 5V TTL and CMOS. Input pins (IN1 – 8) are opposite output pins (OUT1 – 8) to simplify layout
- IN1 and 2 connected to P0.1 and P0.2 of the microcontroller. A Low on p0.1 (simultaneously a High on P0.2) activates relay1 and the door motor turns clock-wisely (opens the door); the other way around, the door turns anticlockwise.
- IN3 is connected to P0.3, whenever the system is put in SLEEP MODE, a High is sent to P0.3, hence Relay3 de-energizes and the scanner is turned off in this mode.

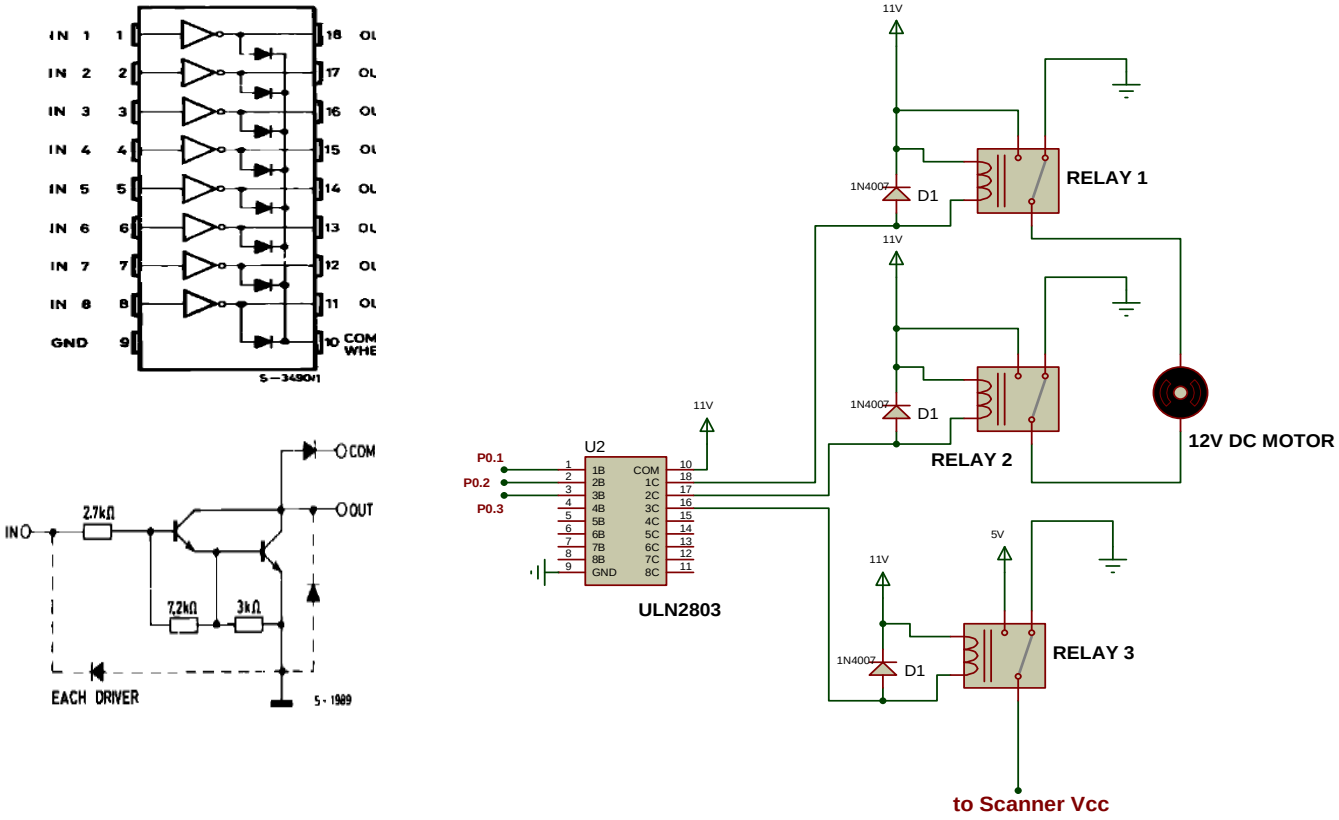


Figure 11. (a). UNL2803 relay driver. (b). Door Control/switching Circuitry

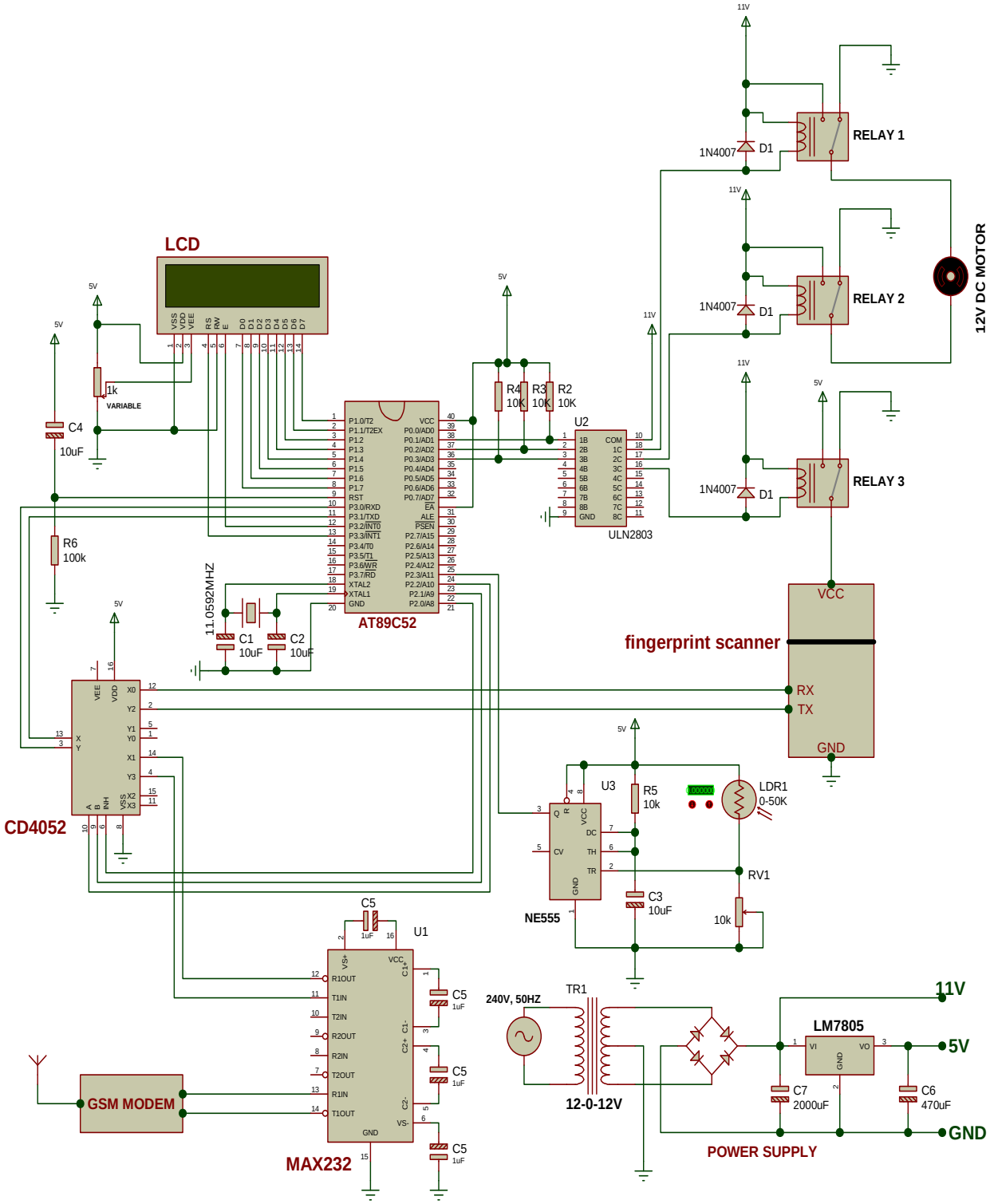


Figure 12. Complete Circuit Diagram of the GSM- Based Biometric Access Control System.

4. Testing, Results and Discussion of Results

4.1. Testing

4.1.1. Testing the Gsm Modem in Hyperterminal

The modem's RS232 Cable is connected to a PC's serial port and its Power supply plugged to 220V mains. HyperTerminal is a free terminal-software that comes with most Microsoft Windows XP operating systems. It is launched from the windows/desktop accessories and configured for communicating with the GSM modem as follows:

i. A new session was created and named. The com-port associated with the computer was then selected (COM1).
ii. Clicking the OK button, properties of the selected communications were displayed and settings matching those of the modem were selected from the dialog box. The hardware flow control option is disabled by selecting NONE in the combo box.
iii. After clicking the OK button, the HyperTerminal window is opened and the commands are entered. Some of the commands used and their respective responses are listed in Table 4.

Table 4. List of some AT commands used

S/N	COMMAND SENT	RESPONSE RECEIVED	COMMENT
1.	AT	OK	Check if serial interface and GSM modem is working
2.	ATE0	OK	Turn off ECHO (less traffic on serial line)
3.	AT+CMGF=1	+CMGF: 1 OK	Message format: text mode
4.	AT+CMGR=X	+CMGR: X, "REC UNREAD","081234569" OK	Read a specific SMS from SIM
5.	AT+CMGD=X	OK	Delete a specific SMS from SIM
6.	AT+CMGS="+27829876543" >Access Request…[Ctrl+Z]	> +CMGS: 23 OK	Send an SMS

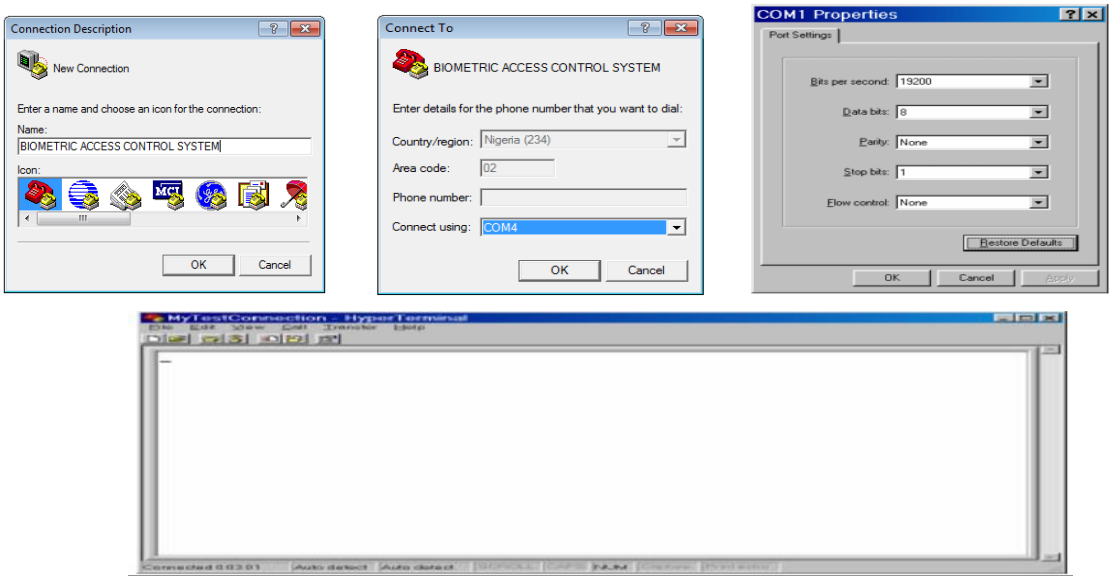


Figure 13. Screen Shots of the HyperTerminal interface

4.1.2. Assembler and Chip Programmer

Programming of the controller (AT89C52) was carried out in two stages: writing and compiling the code; burning the generated Hex file on the controller's ROM.

The code was written and compiled using an evaluation version of KEIL u-Vision3 software which could be used for programming in both C and assembly language (however, Assembly Language was employed in this project).

The application was launched and the appropriate steps for writing the assembly language codes for the operations of the microcontroller were followed. AT89C52 was chosen, an Oscillating frequency of 11.0592Mhz was selected and on the output option, "create HEX file" was also selected – this will enable the compiler create the HEX file after compiling the code.

After successfully compiling and generating the HEX file, it was burnt into the microcontroller's ROM via the TOP2048 USB universal programmer. The programmer is connected to the computer via the USB port and its window-based software – TOPWIN is launched. TOPWIN accepts the generated Hex file from the KEIL compiler and sends it to the TOP2048 programmer upon which the target chip (microcontroller) has been plugged.

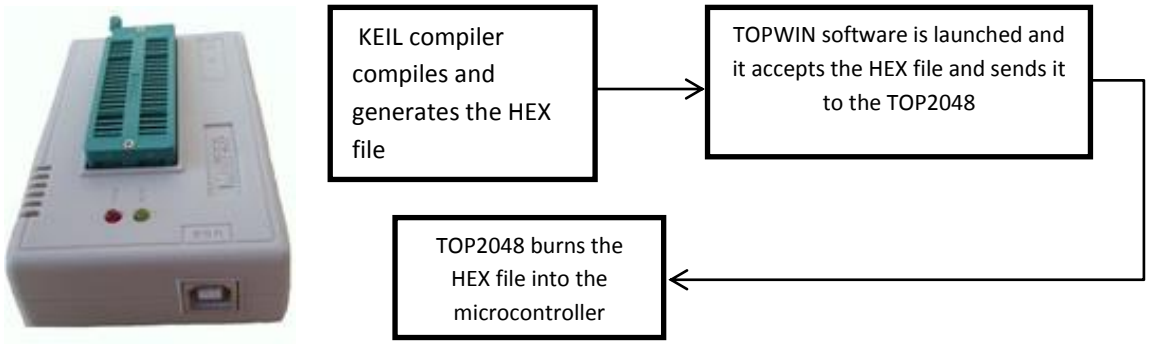


Figure 14. (a) TOP2048 USB universal programmer (b) steps to programming the microcontroller.

4.1.3. Testing The System

The prototype GSM Based Biometric (fingerprint) Access Control system was tested using ten test fingerprints (seven of which were enrolled in the database) and a GSM phone as the Administrator's phone. Each modes of the system were tested using the 10 fingerprints in the steps below:

(1). Power-up, the system was in the DEFAULT MODE and access request is performed by placing each finger on the fingerprint scanner and then pressing the scan button.

(2). The system is SHUT-DOWN by sending the following SMS from the admin Phone: **#MODE2.**

Then access request is then performed by the fingers as in (1) above.

(3). The SMS **#POWER** was then sent to put back the system into operation.

(4). Some of the registered fingerprints are then DELETED by sending the following SMS from the administrator phone:

#DEL 004 **#DEL 006** **#DEL 008**

Access request are then performed by the deleted fingers (users)

(5). SMS **#DEL ALL** below is sent from the Admin phone to delete all the fingerprints

Access request is then performed by all fingerprints

(6). SMS **#MODE4** is sent from the admin GSM to add a new user (fingerprint):

Access request is then performed by the new fingerprint.

(7). The system was put into the ACKNOWLEDGEMENT MODE by sending the SMS **#MODE5**

Access requests are then performed by all the 10 fingerprints.

4.2. Test Results

- The fingerprint scanner did not switch ON until GSM initialization was successful. In the Default mode: "SCAN FINGER" was displayed on the LCD screen. On scanning each of the seven enrolled fingerprints, the door opened and "access Granted" displayed on the screen; otherwise, "access denied" was displayed.
- Step 2: "SHUT-DOWN" was displayed on the display screen, the Fingerprint scanner was switched off and there was no response to every access request by any of the ten fingers.
- Step3: the system came up into DEFAULT MODE and the fingerprint scanner was switched on.

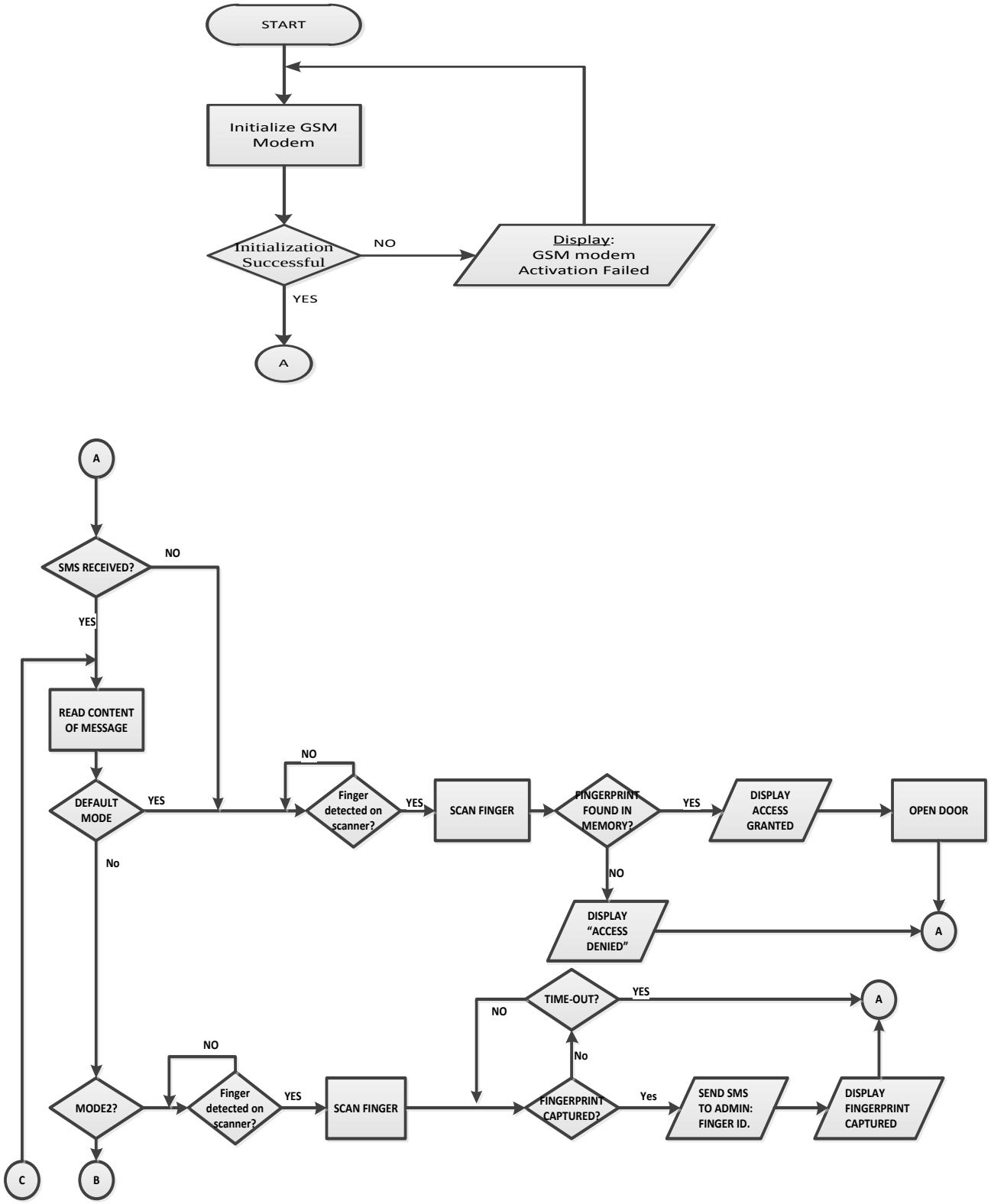
- Step4: SMS was sent to the phone as: "DELETE SUCCESSFUL", access was denied for the deleted fingerprints.
- Step5: an SMS reply "ALL USERS DELETED" was sent received on the GSM phone and also displayed on the screen for 5-seconds. After this, this, the system returns to the default mode and access was denied for all the fingerprints.
- Step6: when the fingerprint was successfully captured, a reply SMS (e.g. "fingerprint captured 007") was received on the GSM phone, the 3-digits indicate the location of the fingerprint in memory and "FINGERPRINT CAPTURED" was displayed on the screen for 5-seconds. Afterwards, the system returned to the Default Mode.
- Step7: At access request by un-enrolled fingerprints, "ACCESS DENIED" was displayed on the screen. At access request by enrolled ones, an SMS is sent to the phone in the format: **007 request access** Indicating that user with ID 007 is requesting access. When a response **ACKNOWLEDGE** was received before 30seconds, "ACCESS GRANTED" was displayed and the door opens, otherwise, at a response **DENY** received, "ACCESS DENIED" was displayed. After 30seconds without the acknowledgment SMS received, "ACCESS DENIED" is also displayed.

Figure 15. Snapshots during design and test stages

4.3. Discussion of Results.

SM630 fingerprint module responded with an excellent correction and tolerance to deformed and poor-quality fingerprint, the response time to each command (scan, delete e.t.c.) was very quick. The system functioned appropriately as designed for all four operation modes. There were however, minor delays in reception of SMS by both the GSM modem and phone due to GSM network errors. At each access granted, the door motor rolls opens then closes after 7seconds.

4.4. Operation Flow-Chart


START
Initialize GSM Modem
Initialization Successful
NO
Display: GSM modem Activation Failed
YES
A
A
SMS RECEIVED?
NO
YES
READ CONTENT OF MESSAGE
DEFAULT MODE
YES
NO
Finger detected on scanner?
YES
SCAN FINGER
FINGERPRINT FOUND IN MEMORY?
YES
DISPLAY ACCESS GRANTED
OPEN DOOR
NO
DISPLAY "ACCESS DENIED"
A
No
TIME-OUT?
YES
A
NO
No
MODE2?
NO
Finger detected on scanner?
YES
SCAN FINGER
FINGERPRINT CAPTURED?
Yes
SEND SMS TO ADMIN: FINGER ID.
DISPLAY FINGERPRINT CAPTURED
C
B

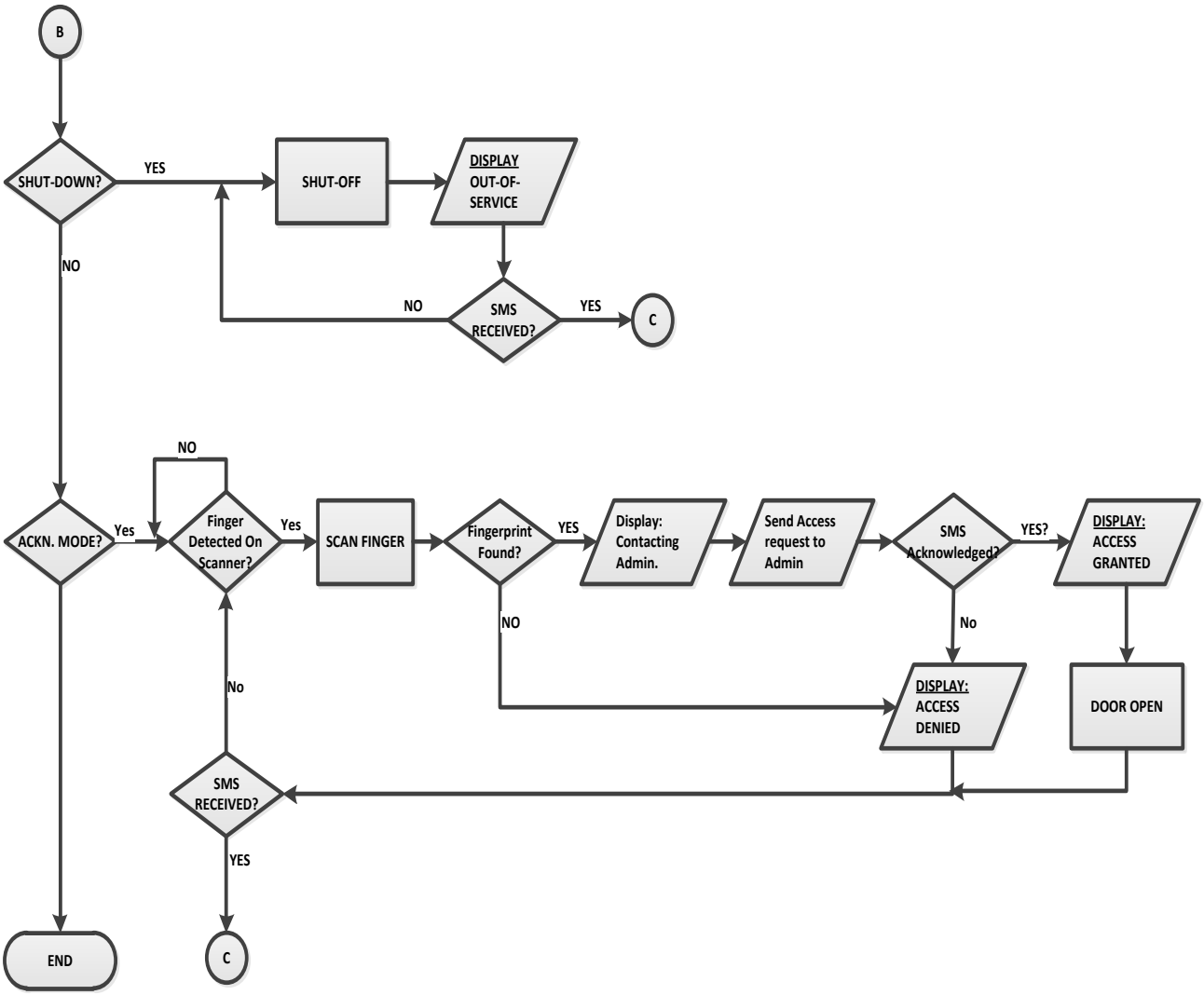


Figure 16. Operation Flow-chart for the System

5. Conclusion and Future Work

5.1 Major Constranits/Limitations

The limitations and challenges encountered in the implementation of this work as proposed include:

- Choice of Fingerprint Scanner: due to the sensitivity of this project, the Scanner has to be reliable in terms of scanning response and less failure rate. This disqualified most common fingerprint scanners and getting the SM630 in local markets was quite difficult.
- Automatic Scan: the scanner module has no command to enable it scan fingers automatically; configuring the LDR to sense fingers placed on the scanner requires precision which wasn't easily achieved.
- The Microcontroller and Choice of programming Language: AT89C52 has only one UART channel which has to be shared between the GSM modem and the Fingerprint scanner. It seems almost unachievable at first, but was achieved using the CD4052 multiplexer IC; this however resulted in longer Code body. Since AT89C52 has only 2KB of code memory, the C-language was thus inappropriate in the programming as very large Hex file larger than 2KB would result.
- GSM Network: The operation of the system depends largely on the GSM network. Poor and unreliable network affects communications between the administrator and the system, and this is a major burden to the Acknowledging mode of operation.

5.2. Conclusion

The design met its stated aims and objectives: it automatically scanned, captured and stored users' fingerprints, granted/denied access appropriately, sent/responded to administrator's SMS effectively and worked in the four modes earlier listed. The system is dependent on GSM network availability and did not start-up when connection with the network couldn't be established. The system is an improvement on conventional Access control systems (especially via key-codes) as fingerprints are unique and possibilities of security compromise completely eliminated and can be configured by the administrator to the desired modes. It is therefore recommended that, the design be implemented using more powerful controllers with larger ROM space and two (or more Serial Ports) like the PIC18F series microcontrollers; the code could then be written in more friendly languages (C, C++, Java or BASIC). In this design, a routine for verifying the administrator's Phone number was not included in the code, instead, delimiting character "#" was always included in the SMS sent to authenticate that the SMS is from the administrator phone. The verifying routine can be effectively written using the appropriate AT commands to verify the phone number, which we intend to work on in the near future. Also, to further optimize this design and make it more compact, the choice of a built-in GSM module can be considered instead of an external GSM modem; external memory should be interfaced with the microcontroller to store and keep track of present mode whenever there's a power outage and a back-up battery added to prevent power outage.

References

http://www.kerisys.com/pages/products/why-access-control/
http://science.howstuffworks.com/biometrics.htm
Vinay Chaddha, "Microcontroller-based access control system", www.electronicsforyou.com, Oct. 2002.
Jayanta Kumar Pany & R. N. Das Choudhury, "Embedded Automobile Engine Locking System, Using GSM Technology", International Journal of Instrumentation, Control and Automation (IJICA) ISSN : 2231-1890 Volume-1, Issue-2, 2011.
M.O.Onyesolu and I.M.Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, pp. 68-70, 2012.
P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

Omidiora E. O. Fakolujo O. A. Arulogun O. T. Aborisade D. O. "A Prototype of a Fingerprint Based Ignition Systems in Vehicles", European Journal of Scientific Research, ISSN 1450-216X Vol.62 No.2 (2011), pp. 164-171. http://www.eurojournals.com/ejsr.htm

http://www.wineyard.in.ph/wk314.pdf

Jain, Anil. "Biometrics." Microsoft Encarta 2009 [DVD]. Redmond, WA: Microsoft Corporation, 2008.

M. A. Mazidi, J. G. Mazidi, R. D. McKinlay "The 8051 Microcontroller & Embedded Systems using Assembly and C", Pearson Education Asia, India, 2nd edition, 2008.

Deshpande, Nikhil, "Matlab implementation of GSM traffic channel", 2003,Graduate School Theses and Dissertations. http://scholarcommons.usf.edu/etd/1354

www.bioenabletech.com/technical_introduction_to_GSM_Modem_technology.htm

Global System for Mobile communication. The international Engineering Consortium.

http://www.iec.org

PETER MARWEDEL. Embedded System Design, University of Dortmund, Germany Published by Springer, P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

David Calcutt, Fred Cowan Hassan Parchizadeh, 8051 Microcontrollers: An Applications-Based Introduction, The Netherlands: Krips BV.

Steven F. Barrett and Daniel J. Pack, Microcontrollers Fundamentals for Engineers and Scientists, A Publication in the Morgan & Claypool Publishers' series.

"Modem." Microsoft Encarta 2009 [DVD]. Redmond, WA: Microsoft Corporation, 2008.

http://www.nowsms.com/faq/what-is-a-gsm-modem

Ashraf El-Sisi, "Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter", The International Arab Journal of Information Technology, Vol. 8, No. 4, October 2011

Mohammad Omar Derawi, Bian Yang, and Christoph Busch, "Fingerprint Recognition with Embedded Cameras on Mobile Phones", Norwegian Information Security Laboratory, Gjvik University College, Norway, http://www.nislab.no/

www.cs.ucla.edu/honors/uploads/andrews/thesis.pdf

"Design of low power Electronic voting machine using AVR microprocessors", International Journal of Emerging Trends in Engineering and Development, Issue 2, Vol.6 (September 2012) ISSN 2249-6149. (http://www.rspublication.com/ijeted_index.htm)

http://smallbusiness.chron.com/finger-print-scanner-work-26552.html

AT89C55 Microcontroller datasheet, ATMEL Corp.

CD4052 Dual 4-Channel Analogue Multiplexer, Fairchild Semiconductor, 2002.

MAX232 dual Driver/Receiver datasheet. © 2004, TEXAS instruments Inc., March 2004
SM630 series fingerprint identification module user manual. Web Portal (http//:www.maxis.com/…./.pdf).

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar