International Journal of ChemTech Research
CODEN (USA): IJCRGG, ISSN: 0974-4290, ISSN(Online):2455-9555
Vol.10 No.14, pp 265-275, 2017

Microcontroller Based Anti-Theft and Thief Arrest System

D.Poornakumar*, K.Shahanas Banu

Department of Electronics and Communication Engineering, K.S.Rangasamy College of Technology,Tiruchengode.Tamil Nadu, India

Abstract : This paper deals with Anti-theft and thief arrest system. During an unauthorized entry of an intruder inside the shops or stores through shutters or doors, infrared red radiation emits from the intruder's body will be sensed by the Passive Infrared Radiation sensor which possessed with a Fresnel lens at sensor's top layer. Signal Conditioning Unit insists PIC to send AT commands to GSM, for transmitting message and call alert to the recipient's mobile. Serial camera captures the intruder's images and store in any storage element. Using DC motor gate will be closed where the thief can made red-handed.
Keywords : Microcontroller, PIR Sensor, Signal Conditioning Unit, GSM module, DC motor.

Introduction

Embedded system as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. Examples of typical properties of embedded computers when compared with general-purpose ones are low power consumption, small size, rugged operating ranges, and low per-unit cost. However, by building intelligence mechanisms on the top of the hardware, taking advantage of possible existing sensors and the existence of a network of embedded units, one can both optimally manage available resources at the unit and network levels as well as provide augmented functionalities, well beyond those available.

Overview of Anti-Theft System

An anti-theft system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable. Theft is one of the most common and oldest criminal behaviors. From the invention of the first lock and key to the introduction of RFID tags and biometric identification, anti-theft systems have evolved to systems are designed to raise the difficulty of theft to an infeasible level. The kind of system implemented often depends on the acceptable threshold for theft. Because of evolution on both sides and the social aspect of theft of theft, the threshold for theft is very dynamic and heavily dependent on the environment. Doors in quiet suburban neighborhoods are often left unlocked, as the perceived thresholds for theft are very high. Security is often compromised through the lax application of theft-prevention practices and human nature in general. The average anti-theft device does not require any additional effort using the secured item, without reducing the level of security. In practice, users of security may intentionally reduce the effectiveness of an anti-theft system to increase its usability.

Overview of Literature Review

Huaqun Guo, et.al,. proposed an automotive security system to disable an automobile and its key auto systems through remote control when it is stolen. Hence it deters thieves from committing the theft. The most effective automotive security system is probably one that will lead a thief to abandon the idea of stealing the

automobile that he sets his eyes upon. This will be the case if the thief knows that he will gain little economic benefits from his theft in spite of the risks he will be taking. If a theft knows that an automobile and its key auto systems will be disabled when its owner finds that the automobile is stolen, it will deter the theft from committing the theft. Therefore, the automotive security system is presented to disable an automobile and its key auto systems through remote control when it is stolen.

Adnan Ibrahim, et.al., proposed about the design and implementation of a GSM based digital door lock security system using PIC platform. A 5-digit password was used to lock/unlock the doors by employing a gear motor. Three consecutive unsuccessful attempts in entering the correct password results in sending a warning message, was sent to preset mobile numbers, as a means of detecting unauthorized intrusion. SMS Technology was collaborated with GSM/GPRS services to achieve controlling of door lock, where they could lock/unlock the door by receiving a predefined message from the user. In this paper they discuss the design and development of a PIC supported security system prototype with 5 digit passwords and GSM system for sending out intrusion alerts.

Saad Islam, et.al., proposed a secured communication system using GSM. GSM is the most widely spread mobile communication system in the world. An important objective in mobile communication systems is secure speech communication. GSM suffers from various security weaknesses. This system can be made thoroughly secure by encrypting the speech which is to be transmitted on the GSM voice channel. In this paper they have demonstrated a real-time prototype of an end-to-end secure communication system developed in MATLAB Simulink. This is amazing because now the GSM channel will become exclusively concealed and confidential to the two subscribers so that even the company people cannot listen to them.

Azeem Ush Shah Khan, et.al., proposed a technique to improve anti-theft for android based mobile phones by using different services like MMS instead of SMS. Once this software is installed, it will work in a background, stores the current SIM number in a variable and keeps checking continuously for SIM change, whenever SIM gets changed from mobile, it will take snapshots, to an alternate mobile number and an email id, which was provided during installation. The enviable advantage of this software is that it is very easy to configure and it keeps running in the background without interrupting the user. To some extent it helps the owner to identify the thief.

Chee Kyun Ng, et.al., proposed a developed RFID based theft prevention system such that luxurious belongings, such as laptops which are monitored from being stolen. The laptop tag ID and its timer sensed from RFID reader are registered in the system server. When the connectivity is broken when the laptop is taken away by more than its allowable distance, an alarm system will be alerted from server. A short message alerting the owner will be sent via the GSM module within a short period of time. This integrated system of RFID and GSM modules form a robust wireless security system. This system can be improved by using bluetooth pervasive technology such that it can be exploited easily since it is been embedded in most of the mobile devices.

Raj M, et.al., proposed a detailed description about Automated Teller Machines (ATMs) security which is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs and protecting their installations. It provides real-time monitoring and control without the need for human intervention. The Web server can be run on an embedded system having limited resources to serve embedded web page to a web browser. The setup is proposed for ATM security, comprising of the modules namely, authentication of shutter lock, web enabled control, sensors and camera control.

Vinoth Kumar Sadagopan, et.al., proposed a novel anti theft control system for automobiles that tries to prevent the theft of a vehicle. This system makes use of an embedded chip that has an inductive proximity sensor, which senses the key during insertion and sends a text message to the owner's mobile stating that the car is being accessed. The password consists of few characters and the car key number. If the user fails to enter the correct password in three trials, a text message is sent to the police with the vehicle number and the location tracked using a GPS module. The message is also sent to the owner about the unauthorized usage. Further the fuel injector of the car is deactivated so that the user cannot start the car by any smeans. At the same time a secret lock system gets activated and the unauthorized user gets trapped inside the car and only the owner who is equipped with the key to the secret lock system can deactivate the mechanism.

Cao Shunxia, et.al., proposed a secure and reliable wireless intelligent home alarm systems. It consists of anti-theft feature, anti-fire feature and anti-harmful gas leak feature, and can achieve automatic detection and automatic telephone dial-up alarm calls. The system will send out alarm signals when disaster monitored by intelligent detector occurs. It can send the message to alarm host by wireless transmission, control telephone interface circuits, realize analogue hook, automatically dial the alarm call of the relevant departments, and send a voice message for police. They presents a low-cost and reliable security guard based on SCM, and it will play an important role in improvement of performance of security detection system in the current family, district, office, shopping mall, etc.

P. Sathya Ravi Teja, et.al., describe the design and development of a theft control system for security lockers, homes, bank lockers, jewelry outlets, etc. The proposed system consists of an LDR (Light Dependent Resistor) based sensor which acts as an electronic eye for detecting the theft or attempt, and a signaling procedure based on SMS using GSM technology. The GSM based communication helps the owner and concerned authorities to take necessary and timely action in order to prevent the theft. The LDR circuit is interfaced using a relay circuit with an Arduino microcontroller board. Efficacy of the proposed system can be seen in its immediate intimation regarding the incident. The proposed designed system is very effective and inexpensive.

Jer-vui lee, et.al., proposed a detailed description of Multilevel home security system which is basically a multilevel security system which consists of different sensor nodes as the input elements while the output elements react to the signal received from the input elements. The sensor nodes consist of a thief alarm, presence detecting circuit and the break-in camera. A UART is applied as the communication tool between the hardware and the computer. The captured images are delivered to the house owners and the police forces. The task is performed in order to prevent the thieves' invasion.

From the literature review presented above, a clear observation is made to avoid theft in various places such as Banks, ATMs, Homes, Vehicles, etc can be grasped. Electronic gadgets such as PIC kit, Arduino board, RFID tag, etc are used to perform several operations. GSM played an essential role which alerts the user either by Sending Messaging System or by Multimedia Messaging System and those design of the system are quite robust. It gives the keen idea to implement our idea using above furnished Gadgets in order to avoid theft.

Hardware Platform

GSM uses a variation of time division multiple access and is the most widely used in three digital wireless technologies such as TDMA, GSM and CDMA. GSM digitizes and compresses data, then send it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency. PIC16F877A acts as a controller to control the flow of working. PIR acts as a sensor element. Process of GSM, Serial Camera, DC motor, are coded and dumped within the PIC16F877A Controller. It also acts as a decision maker which decides the priority of operation of different electronic gadgets.

Concepts of Microcontroller

Microcontroller is a general purpose device, which integrates a number of the components of a microprocessor system on to single chip. It has inbuilt CPU, memory and peripherals to make it as a mini computer. A microcontroller combines on to the same microchip:

- The CPU core
- Memory(both ROM and RAM)
- Some parallel digital I/O

Microcontrollers will combine other devices such as:

- A timer module to allow the microcontroller to perform tasks for certain time periods.
- A serial I/O port to allow data to flow between the controller and other devices such as a PIC or another microcontroller.
- An ADC to allow the microcontroller to accept analogue input data for processing.

Features of Microcontroller

- Smaller in size
- Consumes less power
- Inexpensive

Microcontroller is a standalone unit, which can perform functions on its own without any requirement for additional hardware like I/O ports and external memory.

The heart of the microcontroller is the CPU core. In the past, this has traditionally been based on an 8-bit microprocessor unit.

In the recent years, microcontrollers have been developed around specifically designed CPU cores, for example the microchip PIC range of microcontrollers.

Introduction to Pic

The microcontroller that has been used here is from PIC series. PIC microcontroller is the first RISC based microcontroller fabricated in CMOS (complementary metal oxide semiconductor) that uses separate bus for instruction and data allowing simultaneous access of program and data memory.

The main advantage of CMOS and RISC combination is low power consumption resulting in a very small chip size with a small pin count. The main advantage of CMOS is that it has immunity to noise than other fabrication techniques.

C**PIC 16F877A**

Various microcontrollers offer different kinds of memories. EEPROM, EPROM, FLASH etc. are some of the memories of which FLASH is the most recently developed. Technology that is used in pic16F877A is flash technology, so that data is retained even when the power is switched off. Easy Programming and Erasing are other features of PIC 16F877A.

CMOS Technology

- Low-power, high-speed Flash/EEPROM technology which is full of static design
- Wide operating voltage range (2.0V to 5.5V)
- Commercial and Industrial temperature ranges
- Low-power consumption

PIR Sensor

An individual PIR sensor detects changes in the amount of infrared radiation impinging upon it, which varies depending on the temperature and surface characteristics of the objects in front of the sensor. When an object, such as a human, passes in front of the background, such as a wall, the temperature at that point in the sensor's field of view will rise from room temperature to body temperature, and then back again. The sensor converts the resulting change in the incoming infrared radiation into a change in the output voltage, and this triggers the detection. Objects of similar temperature but different surface characteristics may also have a different infrared emission pattern, and thus moving them with respect to the background may trigger the detector as well.

PIR comes in many configurations for a wide variety of applications. The most common models have numerous Fresnel lenses or mirror segments, an effective range of about ten meters (thirty feet), and a field of view less than 180 degrees. There are also PIRs designed with reversible orientation mirrors which allow either broad coverage (110° wide) or very narrow "curtain" coverage, or with individually selectable segments to "shape" the coverage.

Differential Detection

Pairs of sensor elements may be wired as opposite inputs to a differential amplifier. In such a configuration, the PIR measurements cancel each other so that the average temperature of the field of view is removed from the electrical signal; an increase of IR energy across the entire sensor is self-cancelling and will not trigger the device. This allows the device to resist false indications of change in the event of being exposed to brief flashes of light or field-wide illumination. At the same time, this differential arrangement minimizes common-mode interference, allowing the device to resist triggering due to nearby electric fields. However, a differential pair of sensors cannot measure temperature in this configuration, and therefore is only useful for motion detection.

Passive Infrared sensors are electronic devices which measure infrared light radiating from objects in the field of view. PIRs are often used in the construction of PIR based motion detectors. Apparent motion is detected when an infrared emitting source with one temperature, such as a human body, passes in front of a source with another temperature, such as a wall.

The term 'passive' in this instance means the PIR does not emit any energy of any type but merely sits 'passive' accepting infrared energy through the front of the sensor, known as the sensor face. At the core of a PIR is a solid state sensor or set of sensors, with approximately 1/4 inch square area. The sensor areas are made from a pyroelectric material.

The PIR device can be thought of as a kind of infrared 'camera' which remembers the amount of infrared energy focused on its surface. A person entering the monitored area is detected when the infrared energy emitted from the intruder's body is focused by a Fresnel lens.

Most PIR modules have a 3-pin connection at the side or bottom. Sometimes larger modules don't have direct output and instead just operate a relay in which case there is ground, power and the two switch connections. The output of some relays may be 'open collector' which means that it requires a pullup resistor.

PIR sensor itself has two slots in it, each slot is made of a special material that is sensitive to Infrared Radiation. Fresnel lens is mounted on the upper covering of PIR sensor. When the sensor is idle, both slots detect the same amount of IR, the ambient amount radiated from the room or walls or outdoors. When the warm body leaves the sensing area, the reverse happens, whereby the sensor generates a negative differential change. The Fresnel lens condenses light, providing a larger range of IR to the sensor.

The PIR sensor is typically mounted on a printed circuit board containing the necessary electronics required to interpret the signals from the sensor itself. The complete assembly is usually contained within a housing, mounted in a location where the sensor can cover area to be monitored. The housing will usually have a plastic "window" through which the infrared energy can enter. Despite often being only translucent to visible light, infrared energy is able to reach the sensor through the window because the plastic used is transparent to infrared radiation. The plastic window reduces the chance of foreign objects (dust, insects, etc.) from obscuring the sensor's field of view, damaging the mechanism, and/or causing false alarms. The window may be used as a filter, to limit the wavelengths to 8-14 micro meters, which is closest to the infrared radiation emitted by humans.

Opening and closing of doors is always a tedious job, especially in places like shopping malls, hotels and theatres where a person is always required to open the door for visitors. An automatic door opening system consists of a pir sensor which senses the presence of human being and sends pulses to the microcontroller which controls the motor driver by sending appropriate pulses to its input pins and enable pin.

Generally, human body emits infrared energy which is sensed by the PIR sensor from a considerable distance. The output from the PIR sensor i.e., passive infrared detector is amplified to a transistor BC547, the output of which at the collector is connected to pin 1 of the microcontroller. While any moving object is sensed by the PIR it develops logic high at its output which gets inverted by the transistor used to develop a logic low at pin 1 of microcontroller.

In other words, the current signal from the SPDT switch sends a interrupt signal to the microcontroller and it sends a output of logic low to the enable pin input of the motor IC, thus stopping the motor.

After few seconds the microcontroller sends reverse logic to the motor driver IC such that the motor rotates in the opposite direction representing closing of the door.

This happens as the microcontroller sends a logic low to pin2 and logic high to pin7and the motor reverses its direction and door gets automatically closed. This happens few seconds after the person crosses the door path. Thus the door can be closed or opened automatically as a person approaches it or leaves through it.

GSM Module

In this case, PIC microcontroller is interfaced with GSM module by connecting the transmitter pin of controller with the receiver pin of GSM module and the transmitter pin of GSM module is then connected with the receiver pin of Micro controller. Power supply about 5V has been given to the microcontroller whereas the same supply is provided to the GSM module which is interfaced with the PIC microcontroller. AT commands are used to initialize the GSM to perform a particular function to send SMS.

In order to send SMS text mode is selected from the GSM features using AT commands. AT+CMGF command is to select the mode to send SMS in GSM. AT+CMGS command is to select number of message recipient and message that needs to be send to recipient. AT+CSCA is used to set message center number of sim which had inserted in GSM module sim jacket. AT+CSMP is used to set parameter of text mode. Instead of PIR sensor to be used , switch has been used. When the switch is in open condition the call and SMS been sent to the recipients mobile number.

Interfacing GSM Modem With PIC Microcontrollers

It is very easy to interface a GSM MODEM to a PIC Microcontroller as most GSM modems have a serial interface. The USART serial input pin receiver and transmitter of the microcontroller are connected to the transmitter and receiver pins of the GSM module. This is a wired communication to send data from one device to another. There are many methods of wired communication but PIC and GSM interfaced through 2 wire serial communication. Serial communication mean to send data bit by bit. There is only one important key to consider while using serial communication which is baud rate. Baud rate compatibility between two devices should be checked. SIM900D GSM module supports 9600 baud rate with UART type serial communication. PIC microcontroller have built in hardware to implement UART serial communication process between PIC microcontroller and GSM module. SIM900D GSM module also support UART serial communication.

It is used to send SMS, make and receive calls, and do other GSM operation by simple AT commands through a serial interface from microcontrollers and computers. All modem operations (sending and receiving messages, calls, etc) can be carried out by sending AT commands to this virtual serial port through a serial terminal program. Most programming languages allow sending and receiving serial command to the serial port and can be used to write software that can operate the modem without the need to implement any complex interface.

AT Commands to Send Sms to The Mobile Phone

There are two modes to send SMS in GSM as follows

- In text mode
- PDU in binary format which is easier to send SMS using text mode.

To set GSM to text mode:

AT+CMGF=1

AT+CMCS

The above command is used to select character mode to,

AT+CMCS=”GSM”

This command is used to select number of message recipient and message that the user want to send to recipient. To select number and message the following command should be followed,

AT+CMGS=”+090078601”

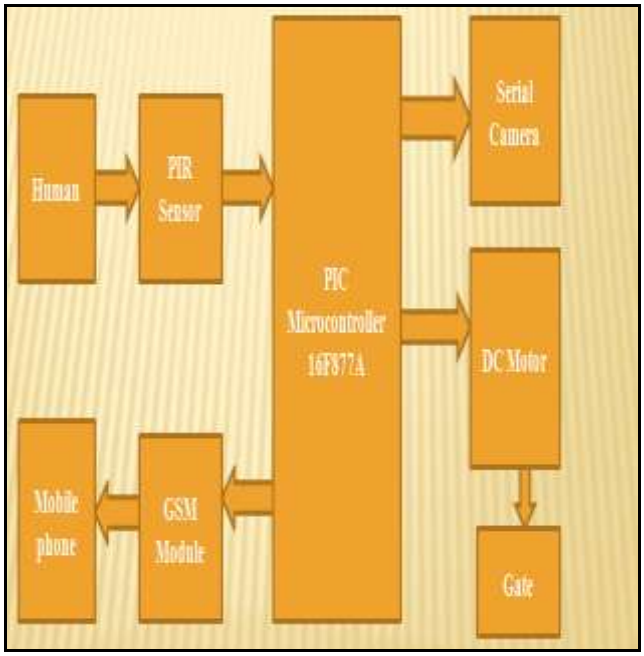


Figure 1: Block Diagram of the Proposed Work

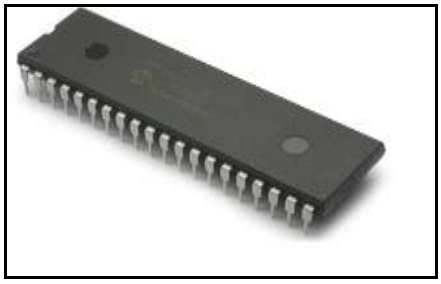


Figure 2: PIC 16F877A

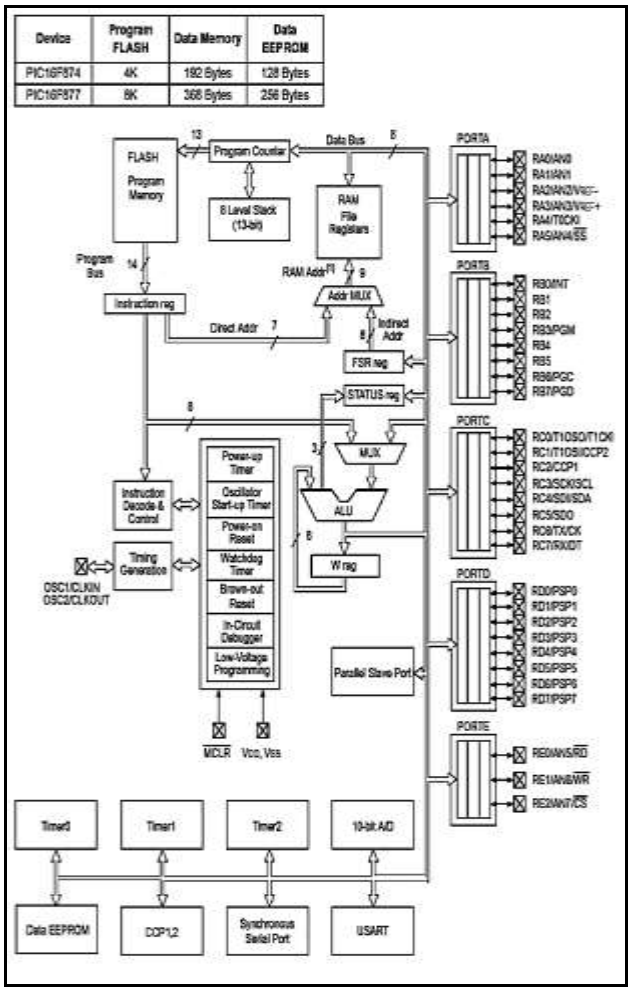


Figure 3. Architecture of PIC 16F877A

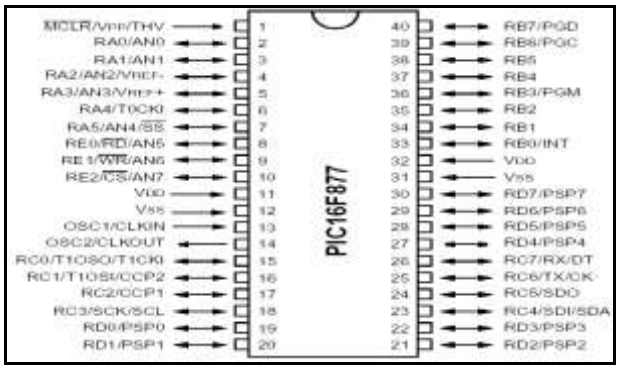


Figure 4: Pin Diagram of PIC16F877A

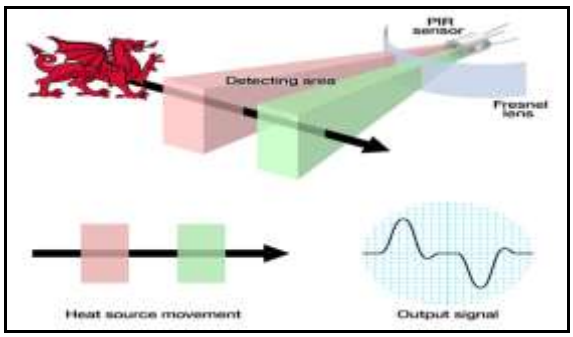


Figure 5: Function of PIR Sensor

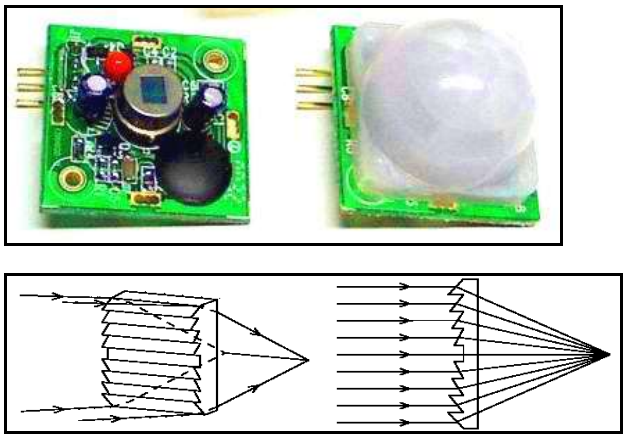
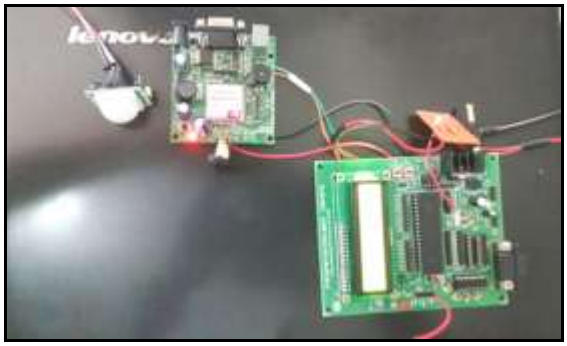


Figure 6: Fresnel Lens

Figure 7: PIR Sensor (Pyro electric material)



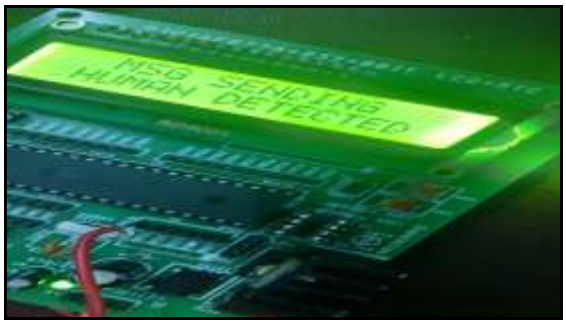


Figure 8: Results and Output

Result and Discussion

PIR sensor detects changes in the amount of infrared radiation depends on the temperature of the human in front of the sensor. The sensor converts the resulting change in the incoming infrared radiation into a change in the output voltage, and this triggers the detection. Human body emits infrared energy which is sensed by the PIR sensor from a considerable distance. The output of PIR sensor is connected to base of the transistor BC547 of SCU (Signal Condition Unit) and it is used to gain the output. Output from the collector pin which is placed in SCU is then transmitted to the microcontroller. While any moving object is sensed by the PIR it develops logic high as its output which gets inverted by the transistor used to develop a logic low at pin 1 of microcontroller. PIC microcontroller is interfaced with GSM module by connecting the transmitter pin of controller with the receiver pin of GSM module and the transmitter pin of GSM module is then connected with the receiver pin of Micro controller. Power supply is about 5V is given to the microcontroller and same supply is provided to the GSM module . AT commands are used to initialize the GSM to perform a particular function to send SMS. AT+CMGF(Message Format) is used to select the text mode to send SMS in GSM. AT+CMGS(Sending Messages) command is to select number of message recipient and message that needs to be send to recipient. AT+CSCA(Service Center Address) is used to set message centre number of sim which is to be inserted in GSM module sim jacket. AT+CSMP(Set Parameter Mode) is used to set parameter of text mode. Using software program has been coded and then dumped in the Peripheral Interface Controller which is used to make calls and send SMS to the recipient mobile using GSM module. The message is displayed on the LCD for every action at the time of initialization, monitoring, calling and message sending.

References

1. H. S. Cheng, H.Q. Guo and Y.D. Wu, “A Method and System For Tamper Proofing A System of Interconnected Electronic Devices,” US PCT patent application No. 60/900,317. Feb 2008.
2. Yanbo Zhao, Zhaohui Ye,”A low cost GSM/GPRS based wireless home security system”, Consumer Electronics, IEEE Transactions on (Vol: 54 , Issue: 2), May 2008.
3. C. Lo and Y. Chen, “Secure communication mechanisms for GSM networks,” IEEE Transactions on Consumer Electronics, Vol. 45, No. 4, pp. 1074-1079, November 1999.
4. Salim, Mohammad, M. Sana Akhtar, and Mohammed A. Qadeer. "Data Retrieval and Security Using Lightweight Directory Access Protocol." In Knowledge Discovery 2009. Second International Workshop on, pp. 685-688. IEEE, 2009.
5. C. C. Tan, B. Sheng and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1400 - 1407, April 2008.
6. Huaqun Guo Lek Heng Ngoh Yong Dong Wu Teo, J.C.M: ‘Secure wireless Vehicle Monitoring and control’, IEEE Asia-Pacific Conference on Services Computing APSCC 2009, pp-81.
7. Zhu Zhiqiang, Xu Lin Construction Method of the Link Equation in Viral Mobile Communication Based on Cross Entropy. 3rd IEEE International Conference on Computer Science and Information Technology, 2010(8):610-613
8. Md. Yusof H., Toha, S.F., Azlan N.Z., Zainuddin F., Muhida R., M. Kazim M.N.F, “Prototype Modeling of Security System with Metal Detector”, Second IEEE Conference on Industrial Electronics and Applications(2007).

9. C. K. Ng, K. S. Wee, N. K. Noordin, M. I. Saripan and R. Syamsul and A. R. Abdullah, "Theft Prevention using Wireless Security System (WSS)", IEEE International RF and Microwave Conference, (2008), pp. 257-261.

*****