Design and Implementation of A Digital Code Lock System using 'C' Programme

Pinaki Satpathy
Department of Electronics and Communication Engineering
Haldia Institute Of Technology, Haldia, West Bengal, India

Surajit Mukherjee
Department of Electronics and Communication Engineering
Haldia Institute Of Technology, Haldia, West Bengal, India

Moumita Jana
Department of Electronics and Communication Engineering
Haldia Institute Of Technology, Haldia, West Bengal, India

Raj Kumar Maity
Department of Electronics and Communication Engineering
Haldia Institute Of Technology, Haldia, West Bengal, India

Abstract- The purpose of this paper is to create a 'C'-programme based Digital Code Lock that serves the purpose of security. The 'C' programme based Digital Code Lock is an access control system that allows only authorized persons to access a restricted area. Security is a prime concern in our day-today life. Everyone wants to be as much secure as possible. An access control for doors forms a vital link in a security chain. The system comprises of a push button keypad connected to the 8 bit microcontroller ATmega16. The system will allow you to preset a password. The lock will open if and only if the entered password matches the preset one. If the entered password is wrong a buzzer will be activated.

Keywords – Digital Code Lock, Microcontroller, LCD Display Interface

I. INTRODUCTION

"Digital Code Lock" is a concept which has been put to use by us after exploiting the needs and demands of modern digitized world. The simple concept of pattern recognition has been implemented by us using IR sensor pairs and LM358 comparator IC.

Home network is a residential local network, and is used to connect multiple devices within the house or apartment. It may consist of a broadband modem, a router, PCs, a wireless access point, entertainment peripherals, and other electronics. It allows users to remotely monitor and control consumer electronics through the external network such as Internet. Until recently, the home network has been greatly getting a lot of attention in both commercial and research sectors. The home network has become the network of consumer related electronics for various useful applications such as entertainments, telecommunications, automation systems, and remote control and monitoring systems. Owing to the rapid growth of personal computers and the Internet, high advanced telecommunication technologies, the importance of the home network has increasingly emphasized in the both domains.

Since it is in early stage market, there are little practical products for the home network [1]-[3].

The IR sensor pair detects the human touch and sends the required input to the LM358 comparator IC, which already has a fixed threshold manually set by the use of potentiometer. When the signal input from the IR sensor pair exceeds the threshold then as a reliable output we trigger a LED on. Now, the above method is in common for all the nine IR sensor pairs which have been utilized to make a grid of 3x3 touchpad.

II. PROPOSED ALGORITHM

In this paper we have used this code for some advanced security purposes. It has many other applications in various domains and the concept is pretty fluid and easy enough to be implemented in them.

On the basis of such considerations, the algorithm uses a different color image multiplied by the weighting coefficients of different ways to solve the visual distortion, and by embedding the watermark, wavelet coefficients of many ways, enhance the robustness of the watermark.

Figure 1. Confirm saved pattern

III. WORKING AND CIRCUIT DIAGRAM

The circuit uses an comparator to compare the value detected and output logic ‘1’ or ‘0’ or ON and OFF.

We use an IR LED which will emit Infrared light and it will be reflected by the surface. The detector acts as a variable resistor whose value depends on the intensity of light falling on its surface. The higher the intensity, the lower is the resistance of the detector. The detector and R2 act as a potential divider. When the intensity is high (reflected from white surface), the resistance of detector is low and so the value of the potential is high. Similarly when the intensity is low (reflected from black surface), the resistance of the detector is high and so the potential is low.

This potential is compared with a reference potential. The reference can be varied by the potentiometer (pot). Calibration is required. You have to record potentials of the white as well as black surface and then find their ranges. According these potentials ten set the reference so that for white surface output is. high and for white black surface output is low.

An LED can also be used as a visual detector so that you can see whether the surface is black or white.

R3 resistor prevents excessive current to pass through the LED. The value of the resistor depends on the size and the colour of the LED. More the diameter of the LED, more is the current it will sink in. R1 should be chosen according to the LED. Usually for 3mm Red LED and 5V supply 330Ω is enough. R2 should be larger than the maximum resistance of the detector.

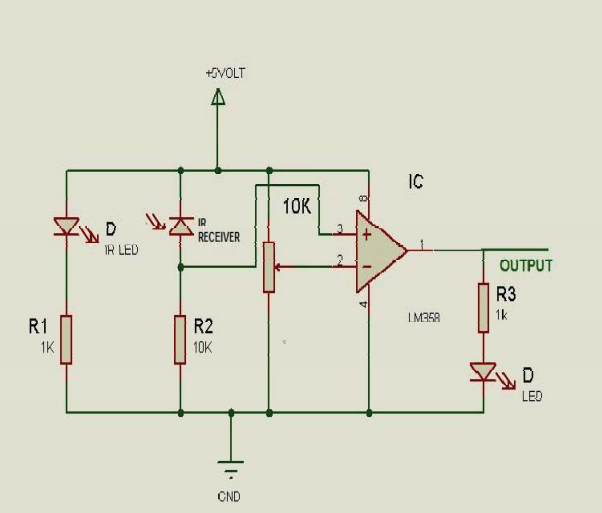


Figure 2. Circuit Diagram

The authentication method used here is a four digit numeric code which is entered through the keypad. The code entered this way is then compared to the password stored in memory. The microcontroller continuously monitors the keypad for a match with the stored password. As and when there is a match the output line is enabled which can then be used to trigger an LED. A buzzer is triggered if the entered code doesn't match the stored password, as an audio indication that the lock has not been opened. An LCD display is also used to display whether the entered password is correct or not.

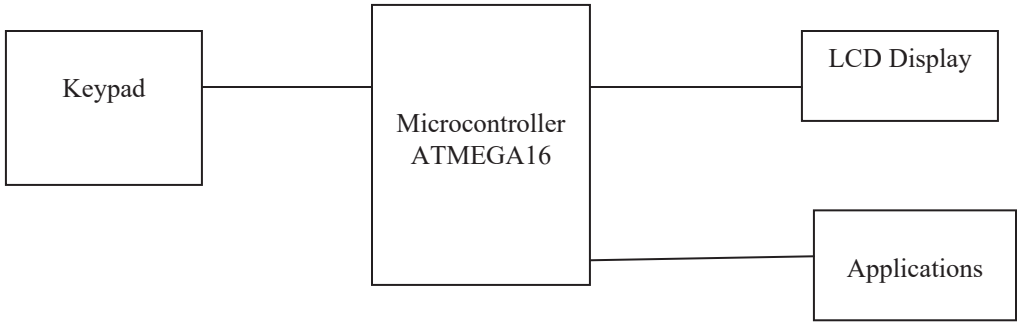


Figure 3. Block Diagram Diagram

When the circuit is switched on a message on the LCD prompts us to 'enter password'. The entered code is read from the keypad and checked against the original password stored in the microcontroller memory. If it is a match an LED is switched ON and if it is not a match, a buzzer is triggered and a message on the LCD prompts us to re-enter the password. The whole procedure is then repeated.

IV. Experiment and Result

The LED and detector have very narrow emission and detection angles, so keep them close so that the circuit functions properly. Metallic or glossy surfaces reflect more tend to reflect more light, so make sure you calibrate the device properly.

Many objects are opaque to visible light (that means light doesn't pass through it, like wood, black plastic, metal), but are transparent to IR light. If you work in the sunlight make sure it doesn't interfere with the function of the circuit. Usually sensors placed below the body of the robot are the least affected by it. Depending on resistor values,

your IR circuit can be tweaked to better detect color instead of distance.

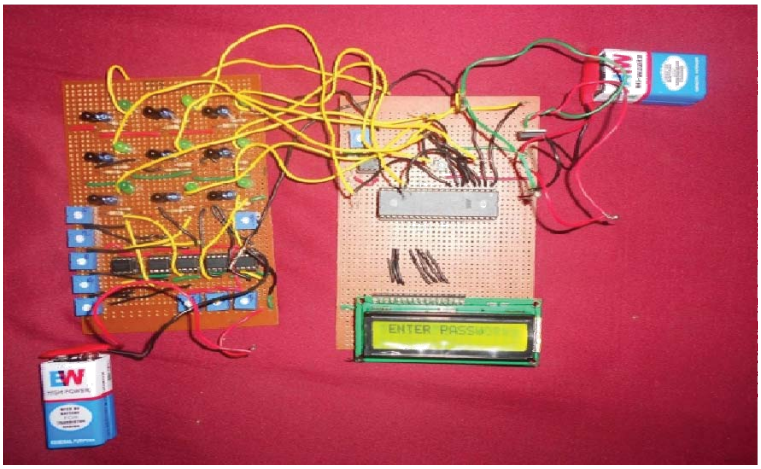
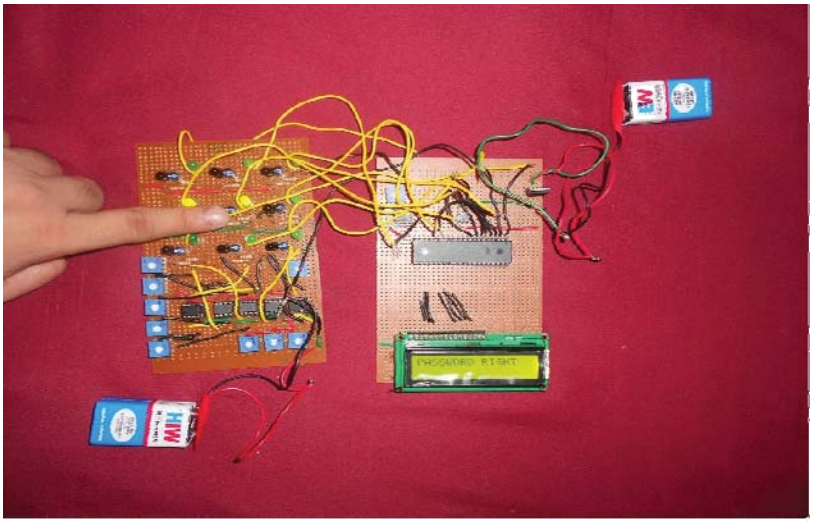


Figure 4. Enter the password



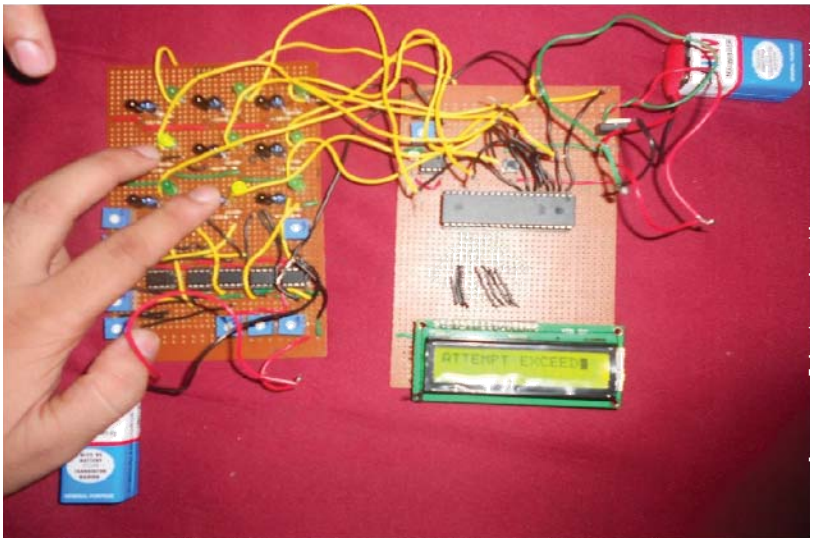


Figure 5. (a) Password enter cottect, (b) Password enter attempt exceed

IV.CONCLUSION

The digital code lock performed as expected. We were able to implement all the functions specified in our proposal. The biggest hurdle we had to overcome with this project was interfacing the micro controller with the hardware components. We feel that this digital code lock is very marketable because it is easy to use, comparatively inexpensive due to low power consumption, and highly reliable. This digital code lock is therefore particularly useful in applications such as door locks and equipment locks.

This simple digital code lock using microcontroller can be enhanced by incorporating new means of authentication. Most prevalent form of digital lock is that using a numerical code for authentication; the correct code must be entered in order for the lock to deactivate. Such locks typically provide a keypad, and some feature an audible response to each press. Combination lengths are usually between 4 and 6 digits long.

Another means of authenticating users is to require them to scan or "swipe" a security token such as a smart card or similar, or to interact a token with the lock.

As biometrics become more and more prominent as a recognized means of positive identification, their use in security systems increases. Some new digital locks take advantage of technologies such as fingerprint scanning, retinal scanning and iris scanning, and voiceprint identification to authenticate users.

Radio frequency identification (RFID) is the use of an object (typically referred to as an RFID tag) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. This technology is also used in modern digital locks.

REFERENCES

[1] S. Conner and R. Gryder, “Building a wireless world with mesh networking technology,” Technology@Intel Magazine, November 2003.

[2] N. Kokkos, A. Floros, N. Tatlas, and J. Mourjopoulos, “A paradigm for wireless digital audio home entertainment,” Audio Engineering Society 120th Convention, Paris, May 2006.

[3] T.B. Zahariadis and A.K. Sakintzis, “Introduction to special feature on wireless home networks,” ACM Mobile Computing and Communications Review, vol. 7, no. 2, April 2003.

[4] J. Choi, B. Ahn, Y. Cha, and T. Kuc, “Remote-controlled Home Robot Server with Zigbee Sensor Network,” SCIE - ICASE International Joint Conference, pp. 3739-3743, October 2006.

[5] ZigBee Alliance, ZigBee Specification, ZigBee Document 053474r06 Version 1.0, April 2004.

[6] L. Zheng, “ZigBee wireless sensor network in industrial Applications”, SICE-ICASE International Joint Conference, pp. 1067-1070, October 2006.

[7] A. Wheeler, “Commercial applications of wireless sensor networks using, ZigBee,” IEEE Communications Magazine, pp. 70-77, April 2007.

[8] N. Baker, “Bluetooth strengths and weaknesses for industrial applications,” IEE Computing & Control Engineering, pp. 21-25, April 2006.

[9] I. Poole, “What exactly is ZigBee?,” Communications Engineer, vol. 2, no. 4, pp. 44-45, August 2004.