

# Design and Implementation Embedded System To Generate Random Seed Number

Abdulrafa Hoseen Maree<sup>1</sup>; Omar I. Alsaif<sup>2</sup>; Naqaa L. Mohammed<sup>3</sup>

<sup>1,2,3</sup> Department of Technical of Computer System, Northern Technical University, Mosul, Iraq.

E-mail<sup>1</sup> : [Rafiallwaze@ntu.edu.iq](mailto:Rafiallwaze@ntu.edu.iq)E-mail<sup>2</sup>: [omar.alsaif@ntu.edu.iq](mailto:omar.alsaif@ntu.edu.iq)

## ABSTRACT

The academic community needs a confidentiality system that are ease to use by student and faculty members. This system depends on the generating process of a random identification numbers (ID No.), that are not repeatable and have non-repetitive numerical categories to facilitate their handling. In addition to being highly reliable, these numbers are placed on the exam papers instead of the student's information such as the name and exam material School stage and department. The system was designed using Arduino due microcontroller and its development environment. Arduino webserver monitoring system have many facilities that can be programmed using the C programming language to verify monitoring options.

There are two common ways to generate random numbers, random (Val) represent a classical method that may repeat the generation procedure with the same numbers. If the start seed is matched, it is preferable to use random Seed, which generates random numbers by giving them different seed for one time, in order to avoid matching the random numbers generated by the user. Therefore, it is necessary to take care of this seed and the changes in each process to develop new data. In most previous research, this seed is taken from physiological sensors such as heat or moisture sensor, vibration sensors, wind and light, it is not expected to know the values of change in the reading period. The traditional methods include using a computer device, which contain the database and programs as (Microsoft Office), but in this research, it is used a simple tools, low cost and small size that can be inserted in the pocket and could be portable like mobile, in addition to the high reliability in generating random numbers because it is used Physically altered seeds in each generation process. Finally, the most important in this research are real time property and embedded system characteristics.

**Keywords:** Embedded system, Random seed number,

## 1. INTRODUCTION

There are many types of generation random methods such as true random number generator (TRNG), a random bit generator (RBG), pseudorandom random bit generator (PRBG), and pseudo random number generator (PRNG) [1]. In this research a real time system is designed using AVR- microcontroller to generate random numbers programmed in C ++ language. The length of this number depends on the number of students. If the number of students does not exceed 100, the random number will be (2-Digits) (0 to 99) and so on for the number of students less than (1000). These numbers are generated randomly distinguish the name of the student as the rest of the information [2]. Alphanumeric characters are created before this figure is agreed upon in advance indicating the information of the other student where it is not necessary to hide this information. For example, each student has three subjects Names Such as (F=Mathematics, G=Advanced Statistics, And H=chemistry). The Generator Number Equal (AF235) where (A) is equivalent Classroom Name, (F) Material Name and (235) is ID Student random number consist three Digits [3]. This Table(1) Represent last Example for more students in class Room (A) only. The Data Base contains a number of tables equal the number of classrooms [4].

**Table(1) Data Base for one classroom**

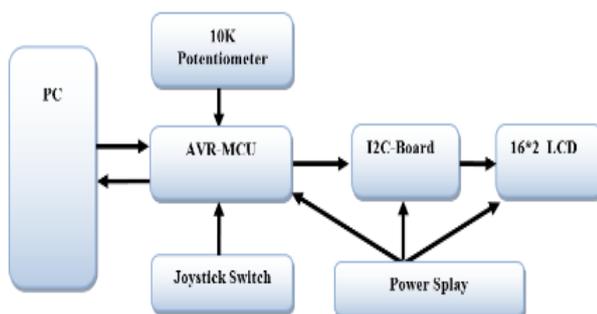
Student Name	Classroom A	Material	ID-No.	random number
Abdulrafa H. Maree	A	F	235	
Abdulrafa H. Maree	A	G	150	
Abdulrafa H. Maree	A	H	77	
Ali M. hasan	A	F	56	
Ali M. hasan	A	G	751	
Ali M. hasan	A	H	255	
-	-	-	-	-

-	-	-	-
-	-	-	-
Noor J. Ali	A	F	154
Noor J. Ali	A	G	66
Noor J. Ali	A	H	841

The programming language (C ++), has been used to program the family-Microcontroller Unite (AVR-MCU), which have special functions for random number generation, such as Random Seed, that contains initial seed. The process of generating random numbers would be more reliable, because of depending to deep function which guaranteed the consistency for this system [5][6].

## 2. Hard Ware Architectural System

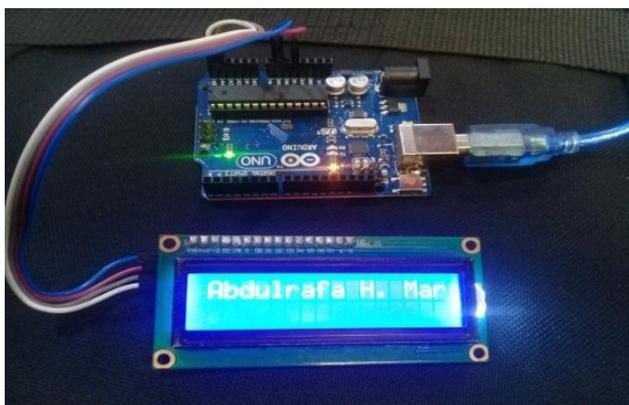
Figure(1) illustrates the basic components of this



system[7].

**Fig 1: Architectural Block Diagram System**

Figure(2) shows the connection of the electronic circuit between Arduino MCU And Liquid Display cell (LCD) [8].

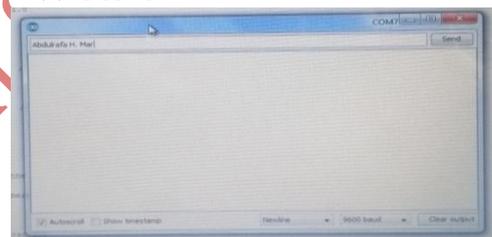


**Fig 2: AVR-Microcontroller and liquid Display**

It is difficult to deal with (AVR-IC) as a unit, where it is required an oscillator circuit and a crystal frequency device to add to the circuit. The programmer task focusing to download the program in hexadecimal system (Hex) on

the integrated circuit (IC) Chips. It is also difficult to enter basic information and data such as students' names, people and materials[9]. These components are simplified, dispensed and inserted in optimum method by Arduino Uno Microcontroller Unit as shown in the diagram above figure (1). The MCU is connected to the input modules via four techniques joystick, a push button, (LCD) and USB port to PC. The last input unit is to connect the variable resistance (10K) as shown in the figure (3) to give a large area of seeds (0 to 1023) different seeds when connected to the terminal (A0) [10].

The role of (PC) deals about using download subprograms and main program to (AVR-MCU), It is also used to read information student from Serial port quickly (9600 bps) and created a database in the (AVR-MCY). This information are displayed from special part (LCD16\*2), which have two-row and sixteen-column as a characteristics of the liquid crystal screen used, as shown in Figure(3). [5][11].



**Fig 3: a: Serial Display (9600)**



**Fig 3: b: Result Liquid Crystal LCD Display**

To reduce the number of wires between the AVR-MCU and the LCD screen to four wires only, we have added and program the board (IC2) as a higher format, that converts data from parallel data to serial data, which designed based on parallel in serial out concept, after adding and loading the libraries in this board with the main program. The following table shows the inputs and outputs of this board [7][12].

**Table (2) Ic2 Board pines**

SDA	SCL	VCC	GND
Data	Clock	5V-Dc	0 V

The most important problems that can be faced by the users of this board is the knowledge about the addresses that are used, so it is important to

[Type text]

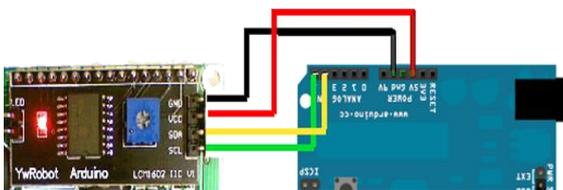
understand each part in the table (3), which shows how to deal with the addresses of each board[9].

**Table (3) knowledge Address in Ic2**

INPUTS			I2C SLAVE ADDRESS
A2	A1	A0	
L	L	L	0x20
L	L	H	0x21
L	H	L	0x22
L	H	H	0x23
H	L	L	0x24
H	L	H	0x25
H	H	L	0x26
H	H	H	0x27

H = Open Jumper L = Close Jumper

From other view, the address can be identified by reading the Serial Port after connecting the terminals (A4, A5) in Arduino Uno board to (SD,SC) in IC2 board [13], as shown in figure(4).



**Fig 4: connection method between LCD and AVR-MCU**

### 3. Device Programming Process

AVR-MCU is programmed in C ++ language as sub-routines based on the following steps:

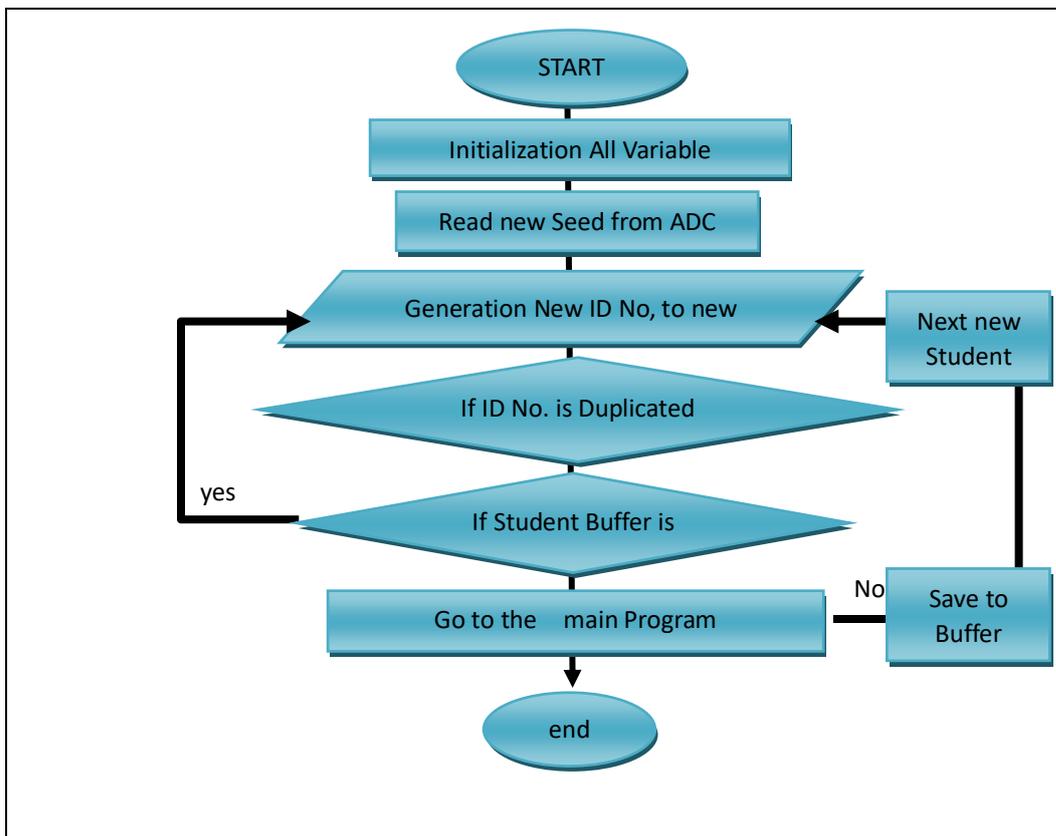
1. The first subprogram is used to generate random numbers with a constant dimensions (2 or 3 -Digit)m

which have significant property that is non-repeatable. These two or three digits are variable seed that read (A0) port of analog signal to convert to digital (Analog to Digital Converter), which represents the variable resistance (10K) whose value must be changed at each new generation. The flow chart below, figure (5) illustrate the algorithm for generating random numbers in a subprogram [2] [13].

2- The program which responsible of enter the database that generated from previous step into (MCU) containing the student's triple name and stage ( level ), in addition to the exam material would be entered by (PC-Serial Port 9600)

to the internal memory in the system. The last step of this program are generate a unique number for each student and tested if there is duplicate in their value, otherwise will save it in the buffer. This number does not match or interfere with any other student number and the various numbered materials. Figure (6) shows how the (MCU) insert the database [1] [12].

The main program have to collect a previous programs and calls each one as needed, in addition to configure the sub-libraries, the printers, the variables, the input and output ports. The main program control to the speed of data transfer from and to the MCU, and the joystick control to review information displayed on the LCD screen using the four ports. The following flowchart illustrates the main program tasks [2].



**Fig 5: Flow Chart for Random Seed Generator Subprogram**

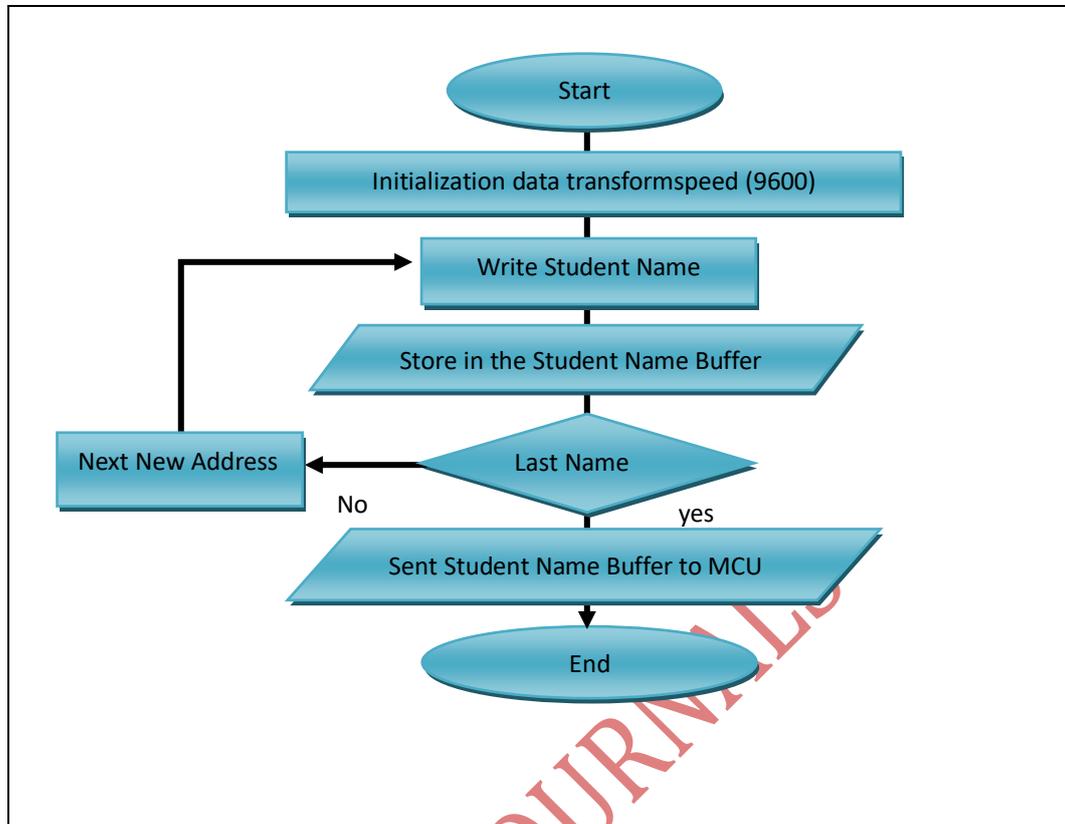
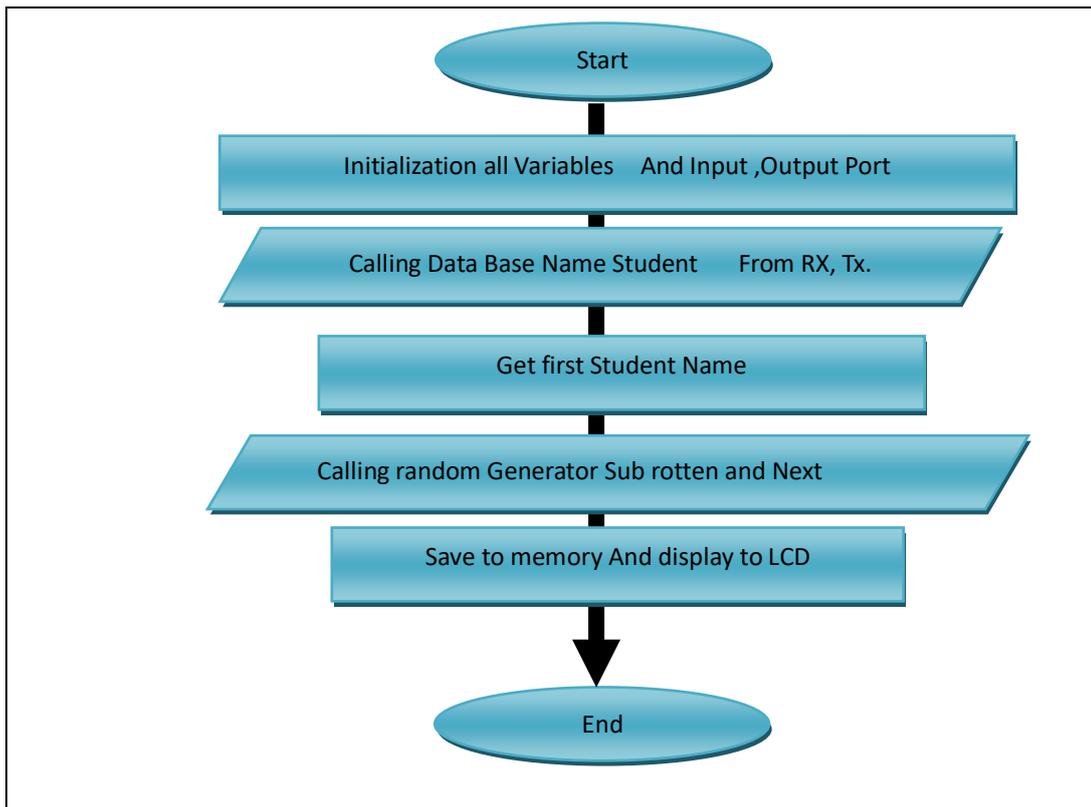


Fig 6: Data transmit from buffer to ( MCU )

[Type text]



**Fig 7: Maine Flow Chart Program in MCU**

#### **4. . RESULTS AND CONCLUSION**

This system is characterized by important specifications in terms of cost and ease of use when compared to the traditional systems like analog to digital converter ( ADC ), which converts the voltage difference from ( 0 - 5v ) to digital values and represented as seed at the beginning of each random seed generator process. This technique has been implemented using computer based technologies such as ( ACCESS software ) which installed within operating system ( windows ), so the embedded systems technique proved its effectiveness and high efficiency when compared with previous traditional technologies. This system is more reliable compared to other database programs because it is hiding the information within (MCU), which gives it more secure and no one can enter to this data and execute piracy process. The control process beside develop and change are very extremes by the specific authorized programmer, because the program are written in c++ language which already encoded into hexadecimal number system that entered to ( MCU ), so it is not possible to manipulate and change the specifications of the program. The

cost of manufacturing has been reduced to the minimum material cost possible and the computer mission ended after downloading the program and entering the data. Finally this system is small in size, portable and does not need electrical source (220v) but operates on a battery (5v DC), whom does not consume much energy.

#### **5. Future Work**

This seed can be expanded by connecting more than one output ports like (A0 & A1), which can be inserted and modulated into a mathematical or logical process, so the seed generation process will be expanded and more complex. The search was used in a two dimension screen (16 \* 2), which is suitable for this purpose. If the database become very big, a screen can be used with large dimensions as (20 \* 4) or others. To reduce the physical size of the device, Arduino Uno can be replaced with a smaller type such as Microcontroller, there are many options for changing the seed by connecting other physiological sensors in addition to variable resistance such as

(gyroscope, vibration, heat, humidity, light and noise).

## 6. References

- [1] Bashar S. Mohamad-Ali, Abdulsfs H. Maree "LOW COST MEDICAL DATA ACQUISITION SYSTEM USING AVR-MCU AND PC," Journal of Theoretical and Applied Information Technology, Vol. 42 No.2 , 31 August 2012.
- [2] Benedikt Kristinsson, Reykjavik University. Ardrand, "The Arduino as a Hardware Random-Number Generator," December, 2011.
- [3] Arduino Home Page. <http://www.arduino.cc/>.
- [4] <http://www.atmel.com>, "8-bit AVR Microcontroller with 16K Bytes In-System Programmable Flash", 2002.
- [5] Evans, B. 2011. Beginning Arduino Programming. 2-3. New York: Apress.
- [6] Fraden, J. "Handbook of Modern Sensors: Physics, Designs, and Applications". Pringer Science & Business Media. 2010.
- [7] MA Yahya, O.I. Alsaif, I .A. Saleh, AM Abdulkhaleq, N Ojaroudi Parchin. " Noise Cancellation for HIPERLAN/2 with Open Loop Transmit Diversity Technique", Inventions vol. 4, Issue (3), page 46. 2019
- [8] O. I. Alsaif, I. Saleh, D Ali. "Evaluating The Performance of Nodes Mobility For Zigbee Wireless Sensor Network". International Conference on Computing and Information Science . May, 2019
- [9] Kifaa H. Thanoon." Morphological Properties for Feature Extraction of Geometrical shapes" International Journal of Engineering and Innovative Technology (IJEIT). Vol.7, Issue 6, page 43- 49. 2017
- [10] Fritzing. "a tool for advancing electronic prototyping for designers". Available: <http://fritz-ing.org/home/>. Accessed: 26 March 2016.
- [11] Karvinen, T. & Karvinen, K. "Getting Started with Sensors: Measure the World with Electronics, Arduino, and Raspberry". Pi.Maker Media, Inc. 2014.
- [12] Noergaard, T. "Embedded Systems Architecture : A Comprehensive Guide for Engineers and Programmers". Burlington, MA, USA: Newnes. ProQuest ebrary. 2005.
- [13] Vizcayno, D. "The Future of Technology, Privacy, Security and Risks" (part 3 of 5). Available: <https://dcvizcayno.files.wordpress.com/2015/08/as1.png>. Accessed: 19 March 2016.