International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

Sequencing and Shuffling Technique for Graphical Passwords

[1] Swetha. D [2] Swathi. H, [3] Narendra Kumar
[1][2]PG Scholar, [3] Assistant Professor
RNS Institute of Technology [RNSIT], Bengalore
[1] swetha_d15@yahoo.com, [2] swathih239@gmail.com,[3] nkmsit@gmail.com

Abstract: **Graphical authentication technology is to make the method usable and secure for the user. Pictures are easier to remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. The main security reason for graphical password is harder to guess or broken by brute force, and also if the numbers of images are more then, complexity and security provided for system is very efficient. Image based password authentication for industrial security system with touch screen interfacing provides an image based security system, which can be used in industrial applications. Major goal of this paper work is to reduce the guessing attacks as well as encouraging users to select more random password with multiple images.**

Index Terms **— Global System, Positioning (GPS), Global system for mobile, Communication (GSM),**

I. INTRODUCTION

Here this paper mainly includes Renesas Microcontroller, GLCD, Touchscreen, GSM, PC, Driver Circuit, DC Motor and Buzzer. The touch screen is used to provide an input for the system. The sensed analog data from the touch screen is provided to the inbuilt ADC for the digital conversion. This data is send to the Microcontroller.

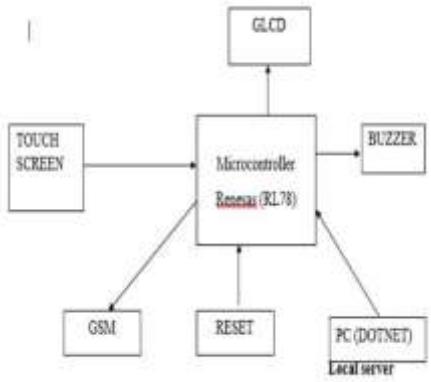

Fig. 1. Block diagram

The GLCD is used for an image display. The Touch screen placed on GLCD is also connected to the microcontroller. When the person enters the password which is in the form of image, this password is compared with the already stored password in database. If it is matched then it allows the user to enter into his account. Here the password need not be a string of characters it can use few images. For each password which is having unique image is provided for the security purpose. This image is displayed on GLCD. If the person enters a password more than 3 times it gives an alert through message using GSM. The DC Motor acts as a gate which allows the user to login with the help of Driver Circuit. All the details of information (password) is stored in the database by using DOTNET. If password is mismatched then the buzzer will beep and send emergency alert to authenticator.

II. RENESAS

Renesas microcontroller consists of General-purpose register: 8 bits × 32 registers. ROM: 512 KB, RAM: 32 KB, Data flash memory: 8 KB. On-chip high-speed oscillator. On-chip single-power-supply flash memory (with prohibition of block erase/writing function). On- chip debug function. Total 11 ports with 58 Input /Output Pins.

On-chip power-on-reset (POR) circuit and voltage detector (LVD). On-chip watchdog timer (operable with the dedicated low-speed on- chip oscillator). I/O ports: 16 to 120 (N-channel open drain: 0 to 4). 16-bit timer: 8 to 16 channels, Watchdog timer: 1 channel. Different potential interface: Can connect to a 1.8/2.5/3 V device. 8/10-bit resolution A/D converter (VDD = EVDD =1.6 to 5.5 V): 6 to 26 channels. Power supply voltage: VDD = 1.6 to 5.5 V.

III. TOUCHSCREEN

A touchscreen is an electronic visual display that can detect the presence and location of a touch within the display area. The term generally refers to touching the display of the device with a finger or hand. Touchscreens can also sense other passive objects, such as a stylus. Touchscreens are common in devices such as game consoles, all-in- one computers, tablet computers, and smartphones.

The touchscreen has two main attributes. First, it enables one to interact directly with what is displayed, rather than indirectly with a pointer controlled by a mouse or touchpad. Secondly, it lets one do so without requiring any intermediate device that would need to be held in the hand (other than a stylus, which is optional for most modern touchscreens).

Such displays can be attached to computers, or to networks as terminals. They also play a prominent role in the design of digital appliances such as the personal digital assistant (PDA), satellite navigation devices, mobile phones, and video games. The first touch screen was a capacitive touch screen developed by E.A. Johnson at the Royal Radar Establishment, Malvern, UK.

Fig. 2. Touch Sensitive Pad

This touch sensitive pad on the Acer Aspire 8920 laptop can increase and reduce the volume of the speakers. Touchscreens have subsequently become familiar in everyday life. Companies use touchscreens for kiosk systems in retail and tourist settings, point of sale systems, ATMs, and PDAs, where a stylus is sometimes used to manipulate the GUI and to enter data.

IV. GRAPHIC LCD DISPLAY

The Graphic LCD display used in this project is 128x64 pixels, where it has 128 columns and 64 rows. Supply voltage is 5V matching the voltage for most microcontrollers. The LCD controller is Samsung KS0108B. JHD12864J module uses 8-bit data bus (DB0 – DB7) Nevertheless, it is a straight forward module comparing to other LCD series like T6963C. JHD12864J is split logically in half with controller #1 (CS1) driving the left half of the display, and controller #2 (CS2) driving the right half. These two portions map directly to the physical display area. Refer figure 3

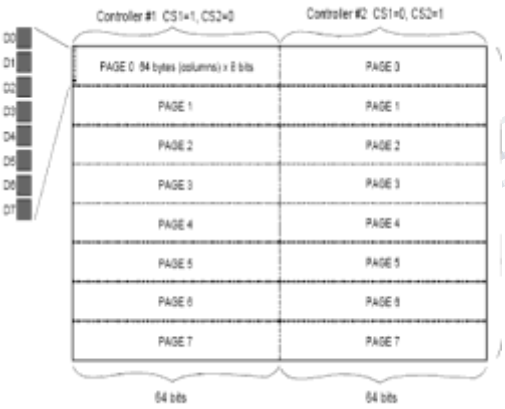

Fig. 3. Chip Selection

RS is equivalent to PIN D/I as stated on JHD12864J data sheet. It controls data or command action (D/I=LOW _ command; D/I=HIGH _ data). Horizontal pixel addressed by Y address counter (0-63). The nomenclature is not the same as our convention of Cartesian coordinate system (x-y). The Y address indicates the column position in the horizontal direction. Why only 64 pixels but not 128 pixels? Because the LCD is spitted logically in half with controller #1 (CS1) driving the left half of the display, and controller #2 (CS2) driving the right half. We need to handle each half individually.

R/W controls data READ/WRITE (R/W=LOW _ write; R/W=HIGH _ read). The reason of writing bytes to the LCD is obvious we need to display something on the LCD. However, being capable of reading from the module is also important because it is only possible to write to a whole Page in 8-bit format. As an example, we want to display a single pixel at the 10th column on

3rd pixel down the top Page where there is an existing byte 0xAB. If we simply output 0x40 (0b0000 0100), the byte pattern 0xAB would be erased. One possible way is to perform a data read first, store the byte in background to a temporary variable, and do a bitwise OR operation with 0x40. This makes a new byte value of 0xAF.

Besides D/I, and R/W pins, there are other control pins to take care including CS1, CS2, E, and RST pins. Direct low-level access and signal timing requirement will be taken care by hardware dependent functions. The application interface function (API) is hardware-independent. This idea is to allow easy porting to other microcontrollers since we only have to re-write the hardware interface for other microcontrollers or compliers.

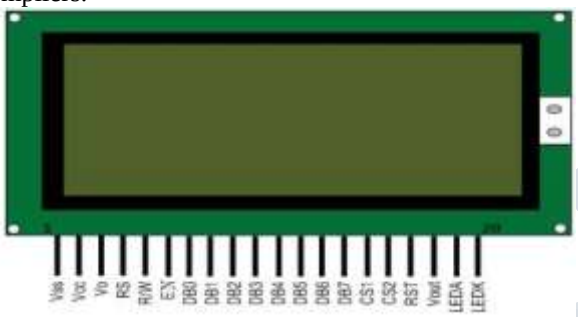

Fig. 4. Graphical LCD Pin Diagram

1	2	3	4	5	6	7	8	9	10
Vss	VDD	Vo	D/I	R/W	E	DB0	DB1	DB2	DB3
11	12	13	14	15	16	17	18	19	20
DB4	DB5	DB6	DB7	CS1	CS2	RST	VEE	LEDA	LEDK

Fig. 5. Pin Configuration

V. GSM

GSM stands for Global System for Mobile Communications formerly called as Groupe Special Mobile**.** Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900MHz. It is estimated that many countries outside of Europe will join the GSM partnership.

GSM is used by over 3 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs from its predecessors in that both signaling and speech channels are digital, and thus is considered a second generation (2G) mobile phone system. This has also meant that data communication was easy to build into the system.

SIM900 is a Tri-band GSM/GPRS engine that works on frequencies EGSM 900 MHz, DCS 1800 MHz and PCS 1900MHz. SIM900 features GPRS multi-slot class 10/ class 8 (optional) and supports the GPRS coding schemes CS-1, CS-2, CS-3 and CS-4.

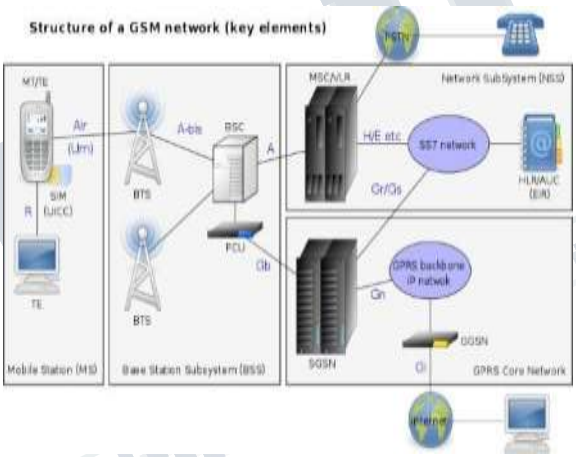

Fig. 6. Structure of GSM Network

You can use AT Command to get information in SIM card. The SIM interface supports the functionality of the GSM Phase 1 specification and also supports the functionality of the new GSM Phase 2+ specification for FAST 64 kbps SIM (intended for use with a SIM application Tool-kit).Both 1.8V and 3.0V SIM Cards are supported. The SIM interface is powered from an internal regulator in the module having nominal voltage 2.8V. All pins reset as outputs driving low.

The "AT" or "at" prefix must be set at the beginning of each command line. To terminate a command line enter <CR>. Commands are usually followed by a response that includes, "<CR><LF><response><CR><LF" Throughout this document, only the responses are presented, <CR><LF> are omitted intentionally.

VI. PIEZO BUZZER

A buzzer or beeper is an audio signalling device, which may be mechanical, electromechanical, or piezoelectric. Typical uses of buzzers and beepers include alarm devices, timers and confirmation of user input such as a mouse click or keystroke.

Fig. 7. Buzzer

Piezo buzzer is an electronic device commonly used to produce sound. Light weight, simple construction and low price make it usable in various applications like car/truck reversing indicator, computers, call bells etc. Piezo buzzer is based on the inverse principle of piezo electricity discovered in 1880 by Jacques and Pierre Curie. It is the phenomena of generating electricity when mechanical pressure is applied to certain materials and the vice versa is also true. Such materials are called piezo electric materials.

VII. TEST RESULT

The implementation of this graphical passwords using sequencing and shuffling technique is obtained and result is verified on the display. The figure 8 shows the data base of the person when they are registering for the first time. During registration the person's password is selected in sequence of icons and in some random order.

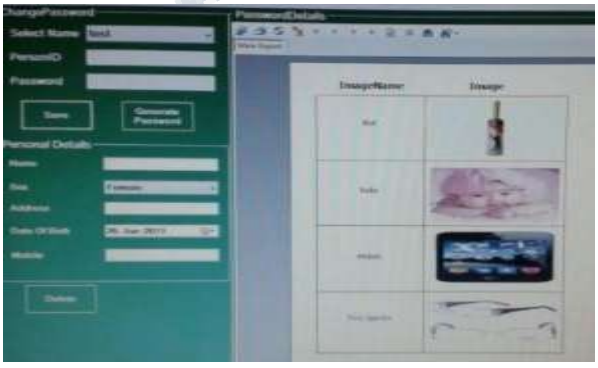

Fig. 8. New data base of the person

The person must set the password in such a way that he/she can remember it easily and also must be difficult to hack by the hackers. After registering in the data base the person can also view their entered details whenever they required the information about the password entries. In figure 9 we can see the details displayed when the password entered by the person is correct.

Suppose the password entered is incorrect for three times then the security alert is send through the GSM to the person and also the buzzer is activated. Once the entered password is correct the message is displayed on the GLCD display and further process is continued.

Fig. 9. Details of the person displayed in data base

VIII. RELATED WORK

There are many different techniques present in graphical password technology. Pass- faces technique is easier to remember compared to textual passwords. It is the combination of attractive password faces but it also takes too much longer time than password faces. The next scheme consist of pass-objects scheme but it consist of 1000 objects on the login process and this make display more crowded and making it difficult to find the pass objects and if number of objects is reduced the size of password space will become smaller and it becomes easier to crack and guess.

The repeating process several times by clicking or rotating it randomly and this become confusing and time consuming since it consist of two many pass objects. The Dhamija and Perrig password system Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel based image [3]. To log in, a user must click within some system-defined tolerance region for each click-point.

This acts as a cue to help users remember their password click-points and for this sequence of click points provided. And if you click on wrong sequence then click points will get blocked. This drawback of the pass point system that clicks points will get blocked. But as per security point of view it is the strong system but finding click points sequence is time consuming task so this graphical password technique using sequencing and shuffling system will help user to come out from this drawback and surely this will provide more security also.

In cued click point technique which is a next graphical password scheme where users select one point per image for five images but it is sequence defined with combination of number of images in the defined sequence of cue. The interface of click point displays only one image at a time and then image will get replaced by the next image. But it is necessary that point should be correct and after that only it will get correct sequence of cue.

The next technique is persuasive cued click point consist of concept of shuffling. For accepting password user must select click point within view port area. If user unable to find the view port then user can press the shuffle button. But this is time consuming task to find the click point in the shuffle button so the new technique defined in this paper will help to overcome from these disadvantages will surely make system safe and secure.

IX. CONCLUSION

The main aim of this paper is to provide a security system for illiterates. This provides user- friendly environment for the users with a kind of image interaction. The system provides complexity for which it will make the system more safe and secure. We can have more than four images as our password for high security. Both images and characters can be used together in order to make the password stronger and to avoid guessing attacks. An extra enhancement can be done by storing user's code words in images as passwords, as it is convenient for the user to remember the images. In order to avoid hacking of character passwords, we have introduced image based password but this can also be hacked. So to avoid this we can use more improvised techniques in future. The output of proposed system will help to make a system secure and safe. This new Click point password makes the system more secure. The output system is combination of sequencing and shuffling together.

REFERENCES

[1] Innovative Graphical Passwords using Sequencing and Shuffling Together Rashmi Wable1, Dr.Suhas Raut2 N.K. Orchid College of Engineering and Technology, Solapur

[2] A.Adams and M.A.Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol.42, pp. 41-46 1999

[3] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[5] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R., "Picture Password: A Visual Login Technique for Mobile Devices"

[6] Suresh Pagidala, C. Shoba Bindu Improved Persuasive Cued Click Points for Knowledge-Based Authentication

[7] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by using Gaze based Password Entry", Symposium on Usable Privacy and Security (SOUPS), July 18-20, 2007, Pittsburgh, PA, USA.

[8] Alain Forget Sonia Chiasson Robert Biddle P.C. van Oorschot "Influencing Users towards Better Passwords Persuasive Cued Click-Points"

[9] Real User Corporation www.realuser.com