ATM TRANSACTION IS SECURED BY USING STEGNO-PIN AUTHENTICATION SYSTEM

B.Rajitha[1], Venkanna Mood[2]
[1]M. Tech Student, [2]Associate Professor,
Department of ECE, St. Martin's Engineering College, Dhullapally, Hyderabad

Abstract

Users typically reuse the same personalized identification number (PIN) for multiple systems and in numerous sessions. Direct PIN entries are highly susceptible to shoulder-surfing attacks as attackers can effectively observe PIN entry with concealed cameras. Indirect PIN entry methods proposed as countermeasures are rarely deployed because they demand a heavier cognitive workload for users. To achieve security and usability, we present a practical indirect PIN entry method called SteganoPIN. The human–machine interface of SteganoPIN is two numeric keypads, one covered and the other open, designed to physically block shoulder surfing attacks. After locating a long-term PIN in the more typical layout, through the covered permuted keypad, a user generates a one-time PIN that can safely be entered in plain view of attackers. Forty-eight participants were involved in investigating the PIN entry time and error rate of SteganoPIN. Our experimental manipulation used a within-subject factorial design with two independent variables: PIN entry system (standard PIN, SteganoPIN) and PIN type (system-chosen PIN, user-chosen PIN). The PIN entry time in SteganoPIN (5.4–5.7 s) was slower but acceptable, and the error rate (0–2.1%) was not significantly different from that of the standard PIN. SteganoPIN is resilient to camera-based shoulder-surfing attacks over multiple authentication sessions. It remains limited to PIN-based authentication.

Keywords: Authentication, human–machine interaction, personalized identification number (PIN) entry, security, shoulder-surfing

1. INTRODUCTION

- **PIN Entry Security issues**

Individual identification numbers are commonly build and remember, are for the most part utilized as numerical passwords for client confirmation. The application is rising a direct result of current touch screens can make simple appropriate execution of the PIN passage interface on an assortment of administration machines and gadgets, and in addition mechanized teller machines, purpose of-offer and plastic terminals, computerized entryway locks, advanced mobile phones, and tablet PCs. security is effortlessly loses for the most part out in the open spots when client going to enter the discharge PIN. These discharge PIN can be seen by close-by individuals by bear surfing assailants. It could be defined as a frail rival it doesn't have programmed recording gadget, which can be utilize manual instruments might be paper and pencil. These shoulder-surfing assailant is defined as a more grounded rival help by a gadget can work independently of human control, for example, a wearable camera, to record and look at whole exchanges effectively even at long range . The dynamic speculating assailant is an adversary who endeavor figure with PIN hopefuls. Such an aggressor can turn out to be more legitimate when it rehashes camera-based perception of a similar client and framework. High-determination cameras are being scattered and arranged out in the open spots in view of Remote associated perception. The current pattern of focusing on assaults and wearable PCs make visit camera-based shoulder surfing assaults and more sensible risk to the PIN

UI. The quantity of PIN competitors reasonably remains, and reduction in grouping spillage regardless of the possibility that a client's PIN passages are as often as possible saw by foes. At the point when the client enters the PIN in different frameworks then data spillage is destructive.

2. EXISTING SYSTEM

Clients commonly reuse the same customized identification number (PIN) for numerous frameworks and in numerous sessions. At the point when client endeavor to enter the PIN in different framework from numerous points of view, at that point coordinate PIN passages are very disposed to bear surfing assaults as aggressors can proficiently watch PIN section with disguise cameras. Where Indirect PIN passage techniques anticipated as counter activities are once in a while send in light of the fact that they request a heavier psychological workload for clients.

3.PROPOSED SYSTEM

Where commonsense backhanded stick passage technique normally called as a Stegno-PIN with a specific end goal to accomplish security and convenience. This Stegno-PIN as two keypads one keypad is secured and other keypad is open, where PIN can be securely entered on display of assailant. In this undertaking utilizing ARM-11 processor board, Ultrasonic sensor, and camera which is associated with the processor. In this Stegno-PIN, open keypad is a standard format, and secured keypad is an irregular design. The arbitrary format keypad is known as the test keypad since it changes ten numeric keys as an irregular test. By Ultrasonic Sensor, challenge keypad get differs. By utilizing this test keypad we can give an OTP. The client first finds a long haul PIN in normal design and in this manner maps the key areas into the test keypad for OTP determination. We can called the reaction keypad, when client enters an OTP on general format. In the event that we enter the wrong PIN number then client will catch the picture by camera and sends the picture to enroll mail-id.

4. BLOCK DIAGRAM

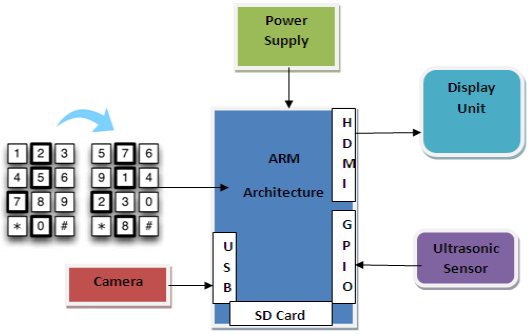


Figure 1:Block Diagram

1. Interfacing IR-sensor to Raspberry-Pi ,getting sensor information by General reason information and yield pin's.

2.These General reason information and yield as absolutely 40 stick's , from this present stick's GPIO - 14 it's a PIN name and physically PIN number is 8 will get associated with the yield of IR-sensor ,and interface GND to GND and Vcc to Vcc.

3. Producing the Standard two keypad in one is open keypad in normal format and the other is canvassed keypad in arbitrary design which is likewise called as test keypad.

4. Test keypad will show when sensor distinguishes, so once individual as enter in the ATM focus sensor will get recognizes and challenge keypad will show.

5.If we know our Security PIN number at that point by observing test keypad we require enter our security PIN number on normal keypad. Along these lines, the PIN number will get show on Display unit in * organize ,to get PIN more secure.

6.Running the camera constantly , if the exchange is fruitful and taking the individual picture and catching the picture and sending to an enlist mail-ID.

7.If exchange bombs at that point additionally taking the individual picture and catching the picture and sending to an enlist mail-ID.

8.Onces this procedure as been finished there is a choice of close, once we tap on close then keypad will arbitrarily changes contrast and past keypad.

9.Again test keypad will show when IR-sensor recognizes and same process as been repeated.

5. HARDWARE IMPLEMENTATION

A. Raspberry Pi Board:

Figure 2:Raspberry Pi Board

1.Where this pi board contains a devices such as General Purpose Input Output pin's, video jack, audio jack, 4 Universal serial Bus, Ethernet, Camera, power supply, and HDMI and so on.
2. Uses of these devices is, where General Purpose Input Output pin's are totally have 40, from these pin's, we are using only three pins for, output, power supply, and GND.
3. From 4 universal serial Bus, we are using 3 universal serial buses, one for keyboard, one for mouse, one for camera.
4. We are using High Definition Multi-media Interface, for the purpose of the display.
5. SD-card is used to store the operating system for the purpose of coding to this project.
6. Power supply is used to get on the board for the working of this project.

B. BCM2835 FEATURES

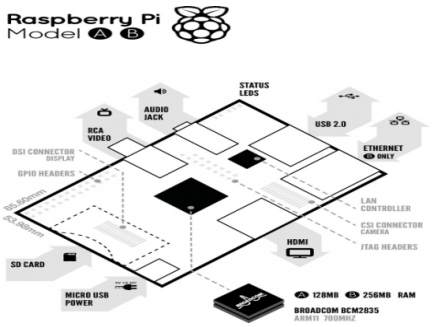


Figure 3: Board features

- AT Raspberry Pi board contains BCM2835 controller which supports ARM11 processing unit which supports following features
- These BCM2835 contains the following peripherals which may safely be accessed by the ARM:

1. supports 700MHZ processing unit frequency
2. Timers
3. General Purpose Input Output
4. Direct Memory Access controller
5. Inter Integrated circuit master
6. Pulse Code Modulation / Inter IC sound
7. Serial Peripheral Interface slave
8. Universal Serial Bus
9. Interrupt controller
10. Pulse Width Modulation
11. SPI0, SPI1, SPI2

6. SOFTWARE REQUIREMENTS

A. Linux Operating System:

- It is a gathering of directions and clarifies the electronic parts of the PC, and it is additionally a free and open source OS. Where the open source and free programming clarifies that every one of the general population as appropriate to utilize it, and alter it. For Linux, there is a cluster of programming and it is a free programming it implies that no of the product will put any permit restricts on client. By this a large number of the general population utilize LINUX.

- It is carry on like OS. In span of the 1980s its principle convictions are built up in UNIX. Solid portion utilized by framework, the procedure control by the Linux Kernel, fringe, and systems administration. Drivers are specifically incorporated with the portion and modules are stacked while the framework is running.

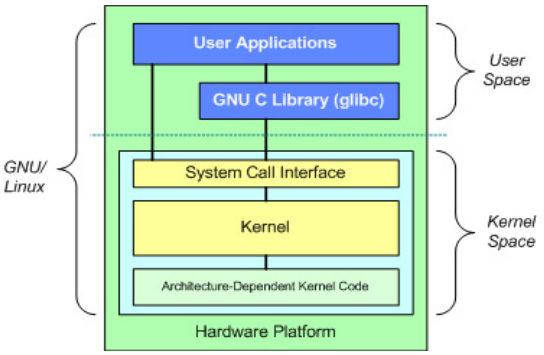


Figure 4: Architecture of Linux Operating System

B. Qt for Embedded Linux:

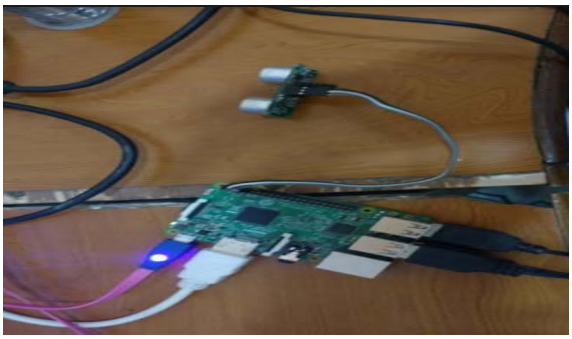
- It is a cross-stage application structure , by utilizing graphical client it builds application programming

- Increasing non-Graphical User Interface projects such a charge line apparatuses and reassures for servers.
- It makes far reaching utilization of a unique code generator all in all with a few macros to enhance the dialect.
- Programming dialects are broadly utilized.
- It keeps running on the significant versatile stages and desktop stages. Internationalization bolster is influenced by substantial region.

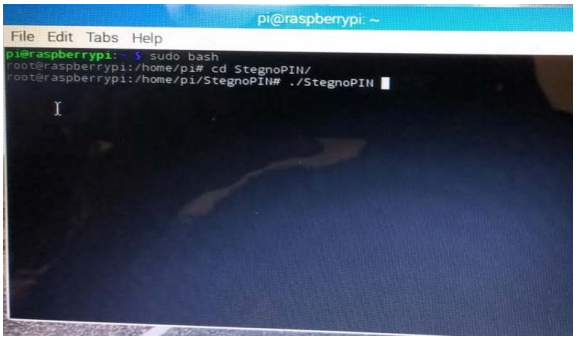
C. Open CV Library:

Open CV (Open Source Computer Vision) is a library of programming capacities for continuous PC vision. It is made by Willow Garage, the association behind the celebrated Robot Operating System (ROS). Presently you'd say MATLAB additionally can do Image Processing, at that point why Open CV? Expressed underneath are a few contrasts between both. When you experience them, you can choose for yourself.

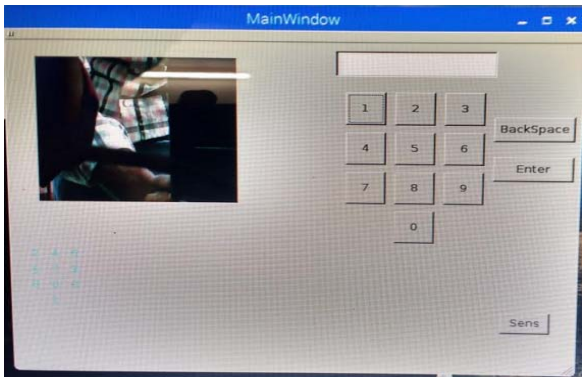
6. RESULT



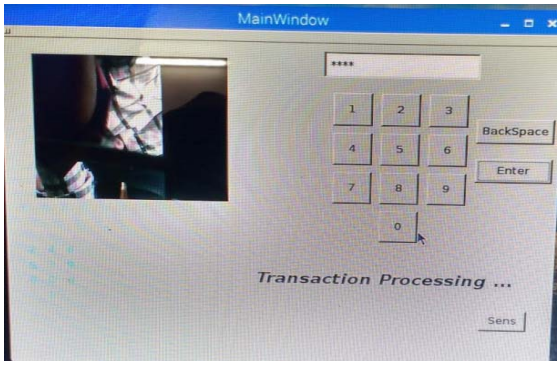
- First connect the IR-sensor to the Raspberry-pi board of General purpose input and output pin's , i.e. output of the IR-sensor will be get connected to the General purpose input and output of GPIO14 pin (PIN name)physically pin no is 8 and connect GND to GND and Vcc to Vcc.



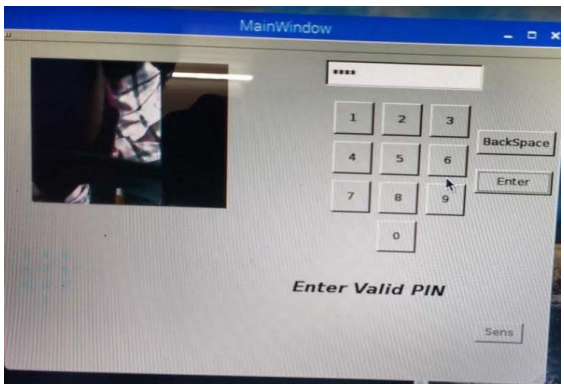
- Where this is the terminal of Linux enter the command (cd StegnoPIN) cd is the change directory , StegnoPIN is the name of this project.



- Once the sensor detects then challenge keypad will display , by seeing challenge keypad we need to enter the password on regular keypad.
- After entering password click on enter button, if there may wrong password enter, there is a option backspace button.



- Once the password is correct it shows as a transaction is completed, at the same time came will continuously runs onces transaction is completed camera will take the pic and capture the image and sends to register mail ID.



- If we enter wrong password it shows enter valid PIN and shows transaction fails , still camera continuously runs camera will take the pic and capture the image and sends to register mail ID.

- Once this process as been completed challenge keypad will get hide , and again keypad will display when sensor detects and same process will repeat.

7. ADVANTAGES:

- Low cost, easy to implement.
- Low power consumption.

8. APPLICATIONS:

- PIN-based authentication

9. CONCLUSION

The undertaking ATM exchange secured by utilizing stegnoPIN Authentication framework has been effectively composed and tried. It has been produced by incorporating part of something of all the equipment segments and programming utilized. Nearness of each module has been founded on rationale and set painstakingly in this manner adding to the best working of the unit. Also, utilizing very propelled Raspberry pi board and with the assistance of developing innovation the task has been effectively executed.

10. REFERENCES

[1] J. Long and J. Wiles, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.

[2] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance," Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/.

[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM Comput.Commun. Security, 2004, pp. 236–245.

[4] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

[5] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.

[6] A. Parti and F. Z. Qureshi, "Integrating consumer smart cameras into camera networks: Opportunities and obstacles," IEEE Comput., vol. 47, no. 5, pp. 45–51, May 2014.

[7] B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-chowdhury, "Distributed camera networks," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 20–31, Apr. 2011.

[8] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security—A field study of real world ATM use," in Proc. ACM Symp. Usable Privacy Security, 2010, pp. 1–10.

[9] J. Rogers, "Please enter your 4-digit PIN," Financial Services Technology, U.S. Edition, vol. no. 4, Mar. 2007.

[10] T. Matsumoto and H. Imai, "Human identification through insecure channel," in Proc. Adv. Cryptol., 1991, pp. 409–421.