Computer Vision and Web Framework for Bank Security Locker System Using Arm Processor

R.Bala Bhaskar, A.Murali Krishna, Dr. K.Sreenivasa Ravi

Abstract— Internet and Digitalization is everywhere and that is the next and running revolution running around the globe. Everything is digitalized, and the market trends on it. E-commerce plays a vital role in marketing the product, purchasing the product, reviewing the product and mainly in India there were too many start- ups running on E-commerce. The purchase with internet is the most feasible way and reaches the customer satisfaction in majority possible cases. When you see the market, there were Android Smartphones coming up with the new emerging applications that moves the e-Market to next gen. Collecting signature from the customer is the digitalization concept that anyone wants to see. That topic is our main agenda, which is to collect signature from the user and to check whether it is her/his own signature or not. Signature is collected with the help of Android Smartphone from the user and it is uploaded to the dynamic web server for image processing using OpenCV with Python (Histogram Evaluation). If it matches with the original signature then SMS will be sent to the user. The same application can also be used in accessing the locker at Banks. This application is demonstrated here with a simple security system.

Index Terms— Android Application, OpenCV, Signature Verification, Histogram Evaluation, Smart Phone, Bank Locker, Security

1 INTRODUCTION

Now-a-days, the bank lockers were accessed through a key and there were some demerits by doing that. Out of which, the main demerit is anyone can access the locker if they have a key with them. In this paper, we proposed a solution for bank lockers. A security system is designed with 2-step authentication (Step–1: Password Recognition, Step-2: Pattern Recognition). Pattern Recognition is done with the help of user signature verification using image processing. OpenCV installed with Microsoft Visual Studio 2012 is used for processing the signature and a simple customized web bank interface is also designed along with the android application.

Signature Verification can be done in two ways:

Static: In this verification method, users deliver their signature on a bank document and digitalize it through a scanner. Bankers will recognizes it through a shape analysis. Thus, this method is termed as offline system.

Dynamic: In this verification method, users deliver their signature on an android smartphone/any digitalized device and that signature will be given for image processing with the previous original signature where pattern recognition plays a vital role and making it as an online system.

SYSTEM ARCHITECTURE

The system architecture of this proposed system is divided into three different and independent blocks.

ARM7 END: Hardware implementation for this proposed system is shown below with the simple blocks. Power Supply block is designed and developed to generate power source for the ARM processor and its relevant components. Reset Circuit is designed and developed to reset the program whenever necessary and interfaced to the ARM processor for greater stable response. Clock Circuit is designed and developed to generate oscillations and interfaced to the ARM processor for needy response. LCD Display is interfaced to the ARM processor for displaying the status of the system for better understanding. Keypad is used to enter the password as a first step authentication for bank lockers which plays a key role in accessing the locker. The GSM module is the main important peripheral which sends information to the owner asking him to sign on his own android smartphone, the system which we proposed here seems to look like a present OTP system. Laptop is interfaced for processing the image.

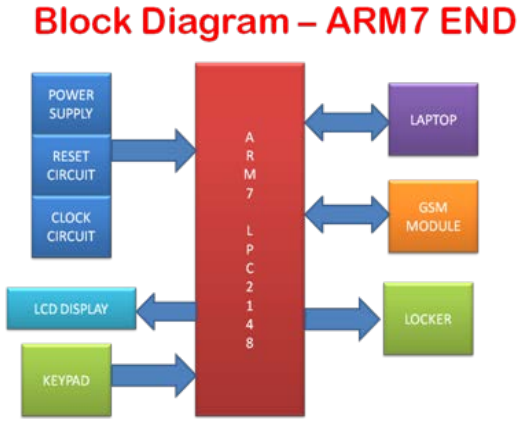

Figure – 1: Block Diagram of ARM7 END

- *R.BALA BHASKAR is currently working as Associate Professor, Department of ECE, Bhoj Reddy College Engineering College for Women, Hyderabad – 500 059, Telangana, INDIA. E-mail: bhaskar.rallabhandi@gmail.com*
- *A.MURALI KRISHNA is currently working as Assistant Professor, Department of ECE, RVR & JC College of Engineering, GUNTUR, Andhra Pradesh, INDIA. E-mail: muralikrishna.atmakuri80@gmail.com*
- *Dr. K.SREENIVASA RAVI is currently as Professor, Department of ECM, K.L.University, Green Fields, Vaddeswaram, Vijayawada 520 010, Andhra Pradesh, INDIA, E-mail: ravi.kavuluri@kluniversity.in*

ANDROID END: The GSM module interfaced at ARM will send a simple SMS stating that someone is accessing the locker, and please authenticate it with the help of your signature. A simple customized Android application is designed and installed manually in the user's android smartphone/tablet. The GSM module of android smartphone will receive a SMS coming from ARM end, upon a SMS coming from the bank server a simple android application will be opened automatically. In the application, it will ask you to enter your name and followed by a canvas where the user has to sign there. The signed image will be uploaded to the bank server for signature verification.

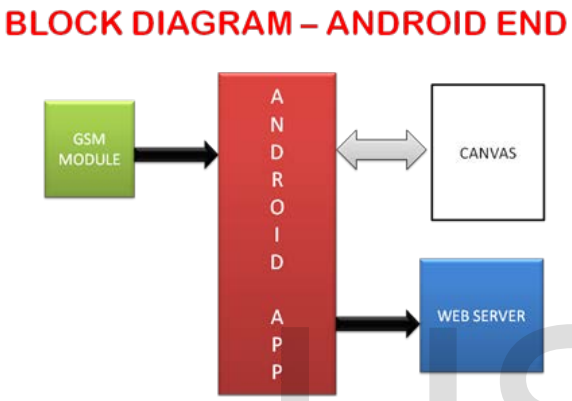

Figure – 2: Block Diagram of ANDROID END

SERVER END: A WEB SERVER is designed and developed for collecting the user signature from the application. A simple UI is designed for better understanding by the bankers and when the signature is received, the bankers will perform the signature verification using openCV. Manual UI is designed for understanding of process with the help of HTML and PHP.

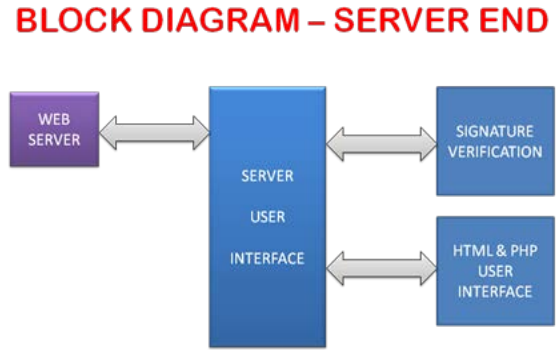

Figure – 3: Block Diagram of Server END

2 IMPLEMENTATION

HARDWARE:

In hardware implementation, ARM processor plays a key role in monitoring and controlling the security system. Low-power consumption ARM processor (LPC2148) operating at 3.3V, 50uA is designed and mounted on a PCB along with Reset Circuit and a Clock Circuit. LPC2148, a 32-bit microcontroller with advanced RISC architecture and having 48 GPIO lines with a program memory of 32KB and a data memory of 512Bytes.

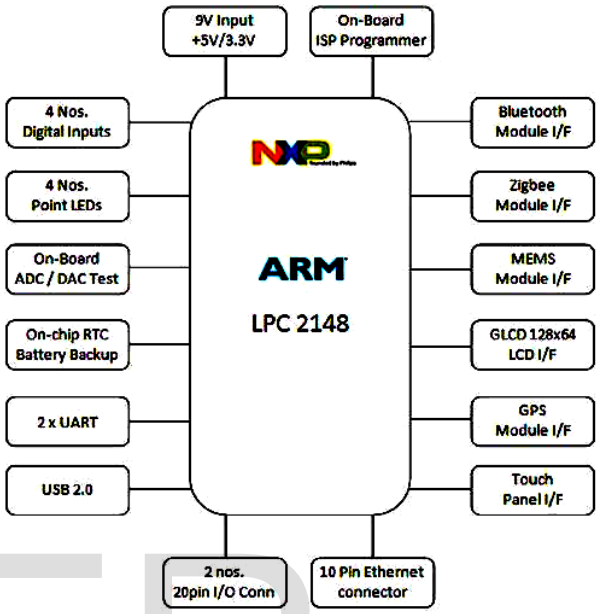

Figure – 4: ARM Overview [LPC2148]

Figure – 5: LPC2148 Development Board

Here, in the above figure the clock circuit and reset circuits were assembled along with the LCD display circuit. A 16 X 2 LCD display is used for displaying the status of the system. A keypad is also designed as per below the schematic diagram, and interfaced to P0.16 – P0.23 of LPC2148.

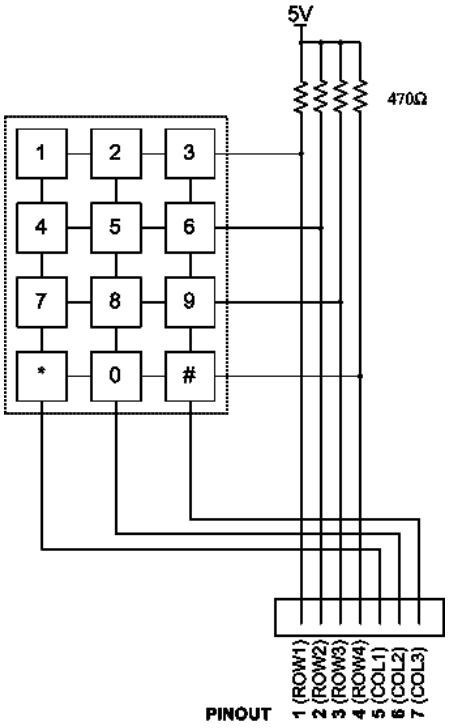

Figure – 6: Keypad Interfacing with LPC2148

The remaining modules like GSM, Motor Driver for controlling the locker were assembled as per the following schematic diagram:

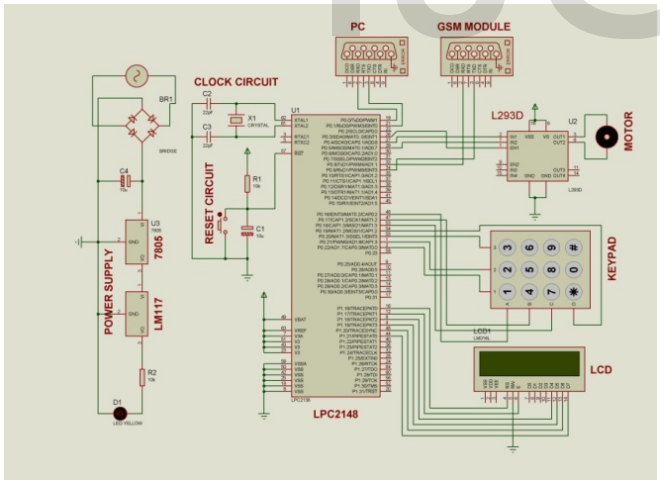

Figure – 7: PC Interface

PC/Laptop was interfaced at UART0 of LPC2148 as per Figure – 7. Motor was interfaced to L293D (Motor Driver) at P0.3 – P0.5 of LPC2148 as per Figure – 8 which enables the locker action. GSM Module was interfaced to UART1 for SMS communication. Keypad (4 * 3) was interfaced at P0.16 – P0.23 of LPC2148. LCD Display (16 * 2) was also interfaced at P1.6 – P1.22 of LPC2148. Reset Circuit and Clock Circuits were interfaced at RST, XTAL1, and XTAL2 of LPC2148.

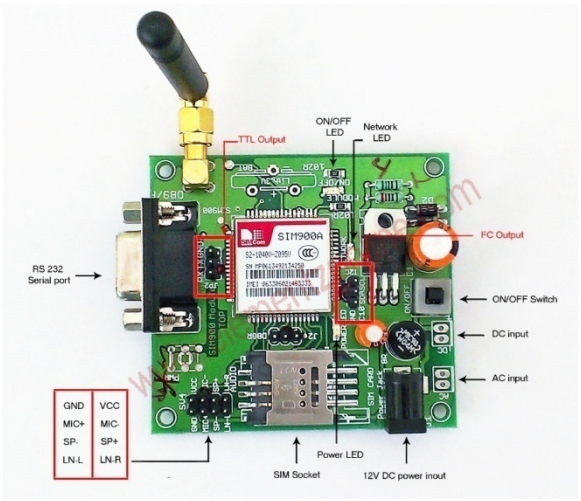

Figure – 8: GSM Module

SOFTWARE:

Here, to program ARM processor Keil uVision 4 was used as a cross-compiler and Flash Magic was used as a programmer. Signature evaluation is done using openCV with Visual Studio 2012, and the web server interface was designed using HTML and PHP. Android application was designed using Android Developer Tools with Eclipse.

3 ALGORITHM, FLOWCHART & RESULTS

ALGORITHM:

Step – 1: Initialize ARM, LCD and GSM Module.
Step – 2: Wait until you see READY on LCD.
Step – 3: PRESS '0' TO ACCESS LOCKER.
Step – 4: ENTER PASSWORD AND PRESS '#'.
Step – 5: If the password is authorized, send OTP to owner mobile.
Step – 6: If the password is unauthorized, display you can't access locker and send SMS to the owner stating that someone is accessing locker.
Step – 7: Whenever OTP has received by the owner mobile, then immediately a built-in android application will be opened.
Step – 8: There, he has to enter name and have to sign on the space allocated and move to next page.
Step – 9: There, he has to upload the signature into the bank server make sure that smartphone is having valid internet connection.
Step – 10: Display the status "SUCCESS" on banker's web user interface.
Step – 11: Banker will process the signature by using a predefined image processing technique (Histogram Evaluation with the previous signatures).
Step – 12: If the signature is matched, then send data from the

server to the system stating that you can access it and a simple SMS will be sent to the owner for intimation.
Step – 13: The status of the processing will also be displayed on bankers web user interface for better understanding.
Step – 14: If the signature is not matched, then also a data will be sent to the ARM processor for intimating the owner stating that someone is trying to access locker without your information.
Step – 15: Locker will be opened successfully with a two-step authentication.
Step – 16: Repeat Step – 3 to Step – 15 for infinite times until the server shut down.

FLOWCHART:

The flowchart of this paper is shown below:

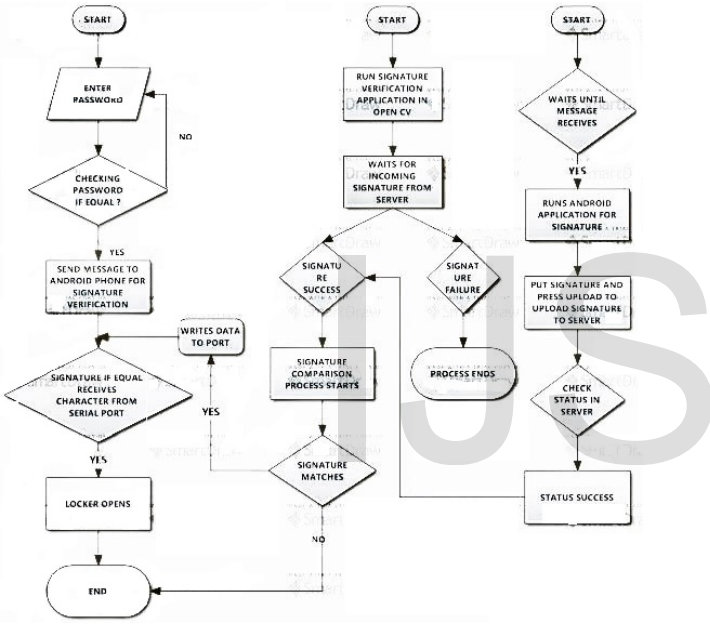

Figure – 9: Flow Chart

RESULTS

Figure – 10: Server Login of Bank

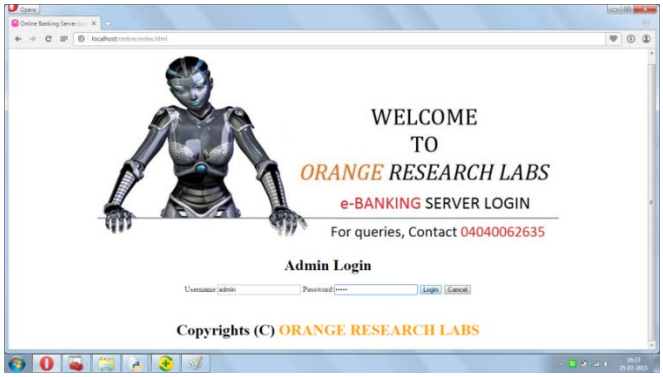

Figure – 11: Login ID and Password

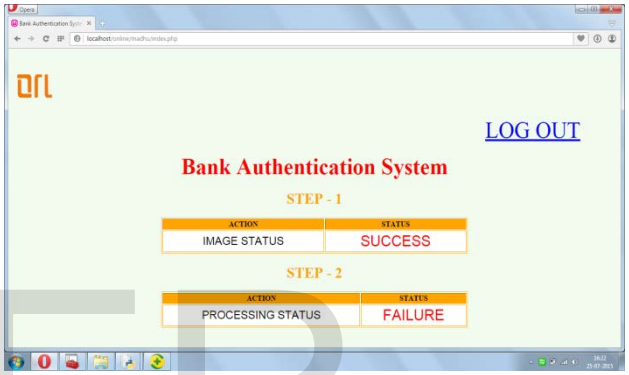

Figure – 12: Status of the Process

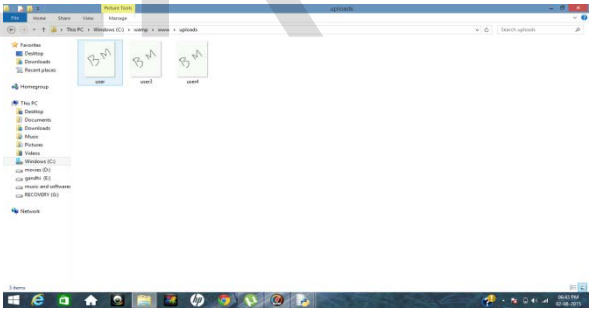

Figure – 13: Signature Uploaded to the server

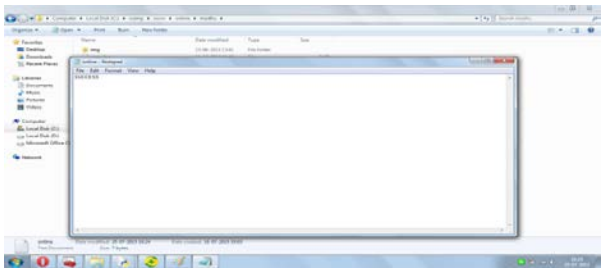

Figure – 14: Text Bridge between the HTML and Image Processing

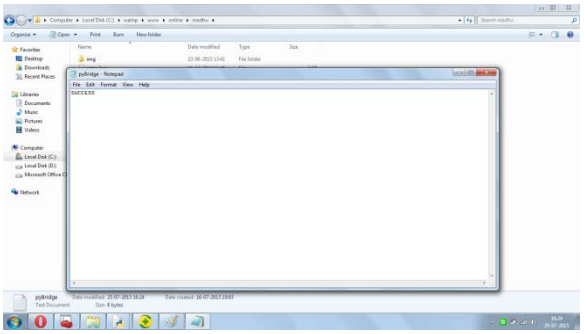

Figure – 15: Python Bridge between the Python Program and Serial Communication

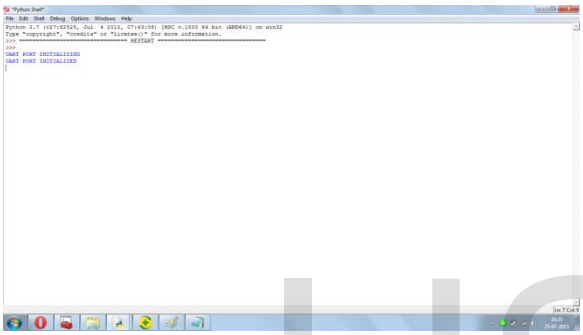

Figure – 16: Python Web Server

Figure – 17: Hardware Assembled for the system

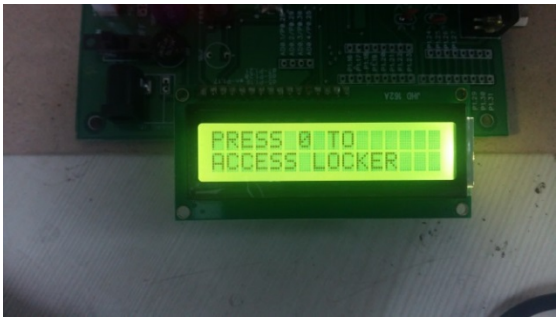

Figure – 18: Asking to access the locker

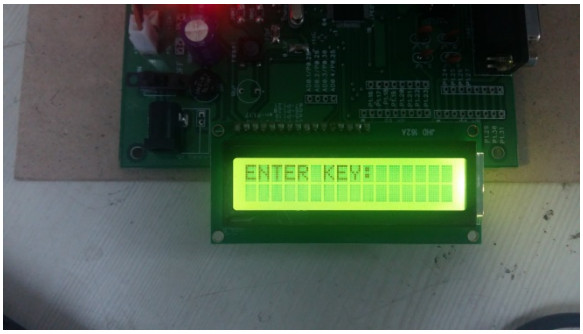

Figure – 19: Enter the password

Figure – 20: Entering the password

Figure – 21: Authorized and going to second authentication

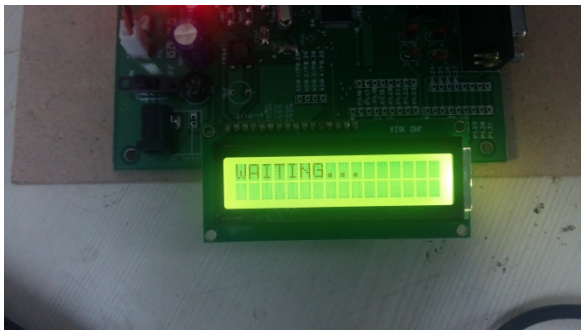

Figure – 22: Waiting for the server to communicate

ess

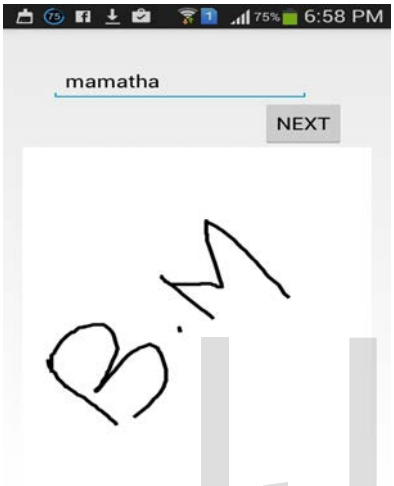

Figure – 24: Signature collected from Android Smartphone

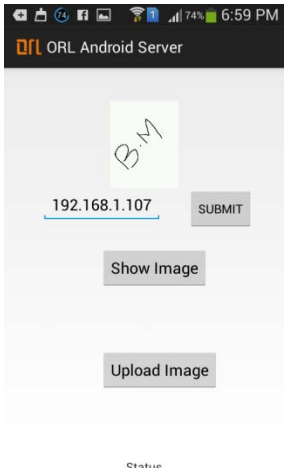

Figure – 25: Signature Stored

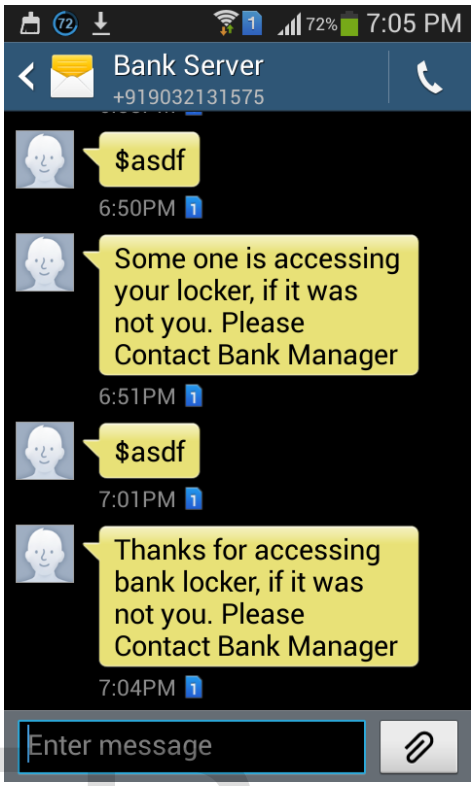

Figure – 26: SMS Feedback from the server

4 Conclusion

Here, in this paper computer vision based framework is designed and developed for providing security system to bank lockers. Now-a-days, digitalization is everywhere and in every digital product that designed and purchased. Making a signature on a digital device plays a key role in making authentications for various applications and field areas.

References

[1] [1] L. Nanni and A. Lumini, "A novel local online signature verification system", vol 29. No 5 pp – 599-568, 2008.

[2] [2]E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application toon-line signature recognition," IEEE Trans. Syst., Man, Cybern. A, Syst.,Humans, vol. 40, no. 3, pp. 525–538, May 2010.

[3] H. Feng and C. C. Wah, "Online signature verification using a newextreme points warping technique," Pattern Recognit. Lett., vol. 24,no. 16, pp. 2943–2951, 2003.

[4] DataGenetics. (2012, Aug. 14). Pin Analysis [Online]. Available:http://www.datagenetics.com/blog/september32012/

[5] Python Reference – Guido Van Rossum, Fred L. Drake, Jr., editor, Available: https://docs.python.org/2.0/ref/ref.html

[6] Py Serial – Documented for Python Serial. Available: http://pythonhosted.org/pyserial/

[7] PHP References manual for Beginners, Available: http://code.stephenmorley.org/php/references-tutorial/
[8] Managing Android Projects for Beginners, Available: https://www.edx.org/course/introduction-mobile-application-hkustx-comp107x?gclid=CKawudvN-8YCFYcHvAodMeYGLw
[9] Referenced GSM, AT COMMANDS Available: http://www.zeeman.de/wp-content/uploads/2007/09/ubinetics-at-command-set.pdf
[10] ARMv7 Reference and System Architecture Manual, Available: https://web.eecs.umich.edu/~prabal/teaching/eecs373-f10/readings/ARMv7-M_ARM.pdf