Portable and efficient fingerprint authentication system based on a microcontroller

Mauricio García Vargas[1], Fredy E. Hoyos[2], John E. Candelo[3]
[1,2]Escuela de Física, Facultad de Ciencias, Sede Medellín, Universidad Nacional de Colombia, Colombia
[3]Departmento de Energía Eléctrica y Automática, Facultad de Minas, Sede Medellín,
Universidad Nacional de Colombia, Colombia

Article Info

Article history:

Received Apr 12, 2018
Revised Mar 5, 2019
Accepted Mar 11, 2019

Keywords:

Authentication
Fingerprint sensor
Microcontroller

ABSTRACT

This paper presents the design of a fingerprint authentication system based on a simple microcontroller and the fingerprint sensor. The circuit diagram and details regarding the procedure are included. The system was programed in MPLAB and then embedded into the microcontroller. Communication between the PIC and sensor is by RS232 protocol. The results show that the system recognizes the fingerprint in less than 1 second. It is portable and there is no need for image processing. Furthermore, the system shows a high effectiveness when storing and verifying fingerprints.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Fredy Edimer Hoyos
Universidad Nacional de Colombia, Sede Medellín
Calle 59A No. 63-20, Medellín, Colombia.
Telephone: (574) 4309327
Email: fehoyosve@unal.edu.co

1. INTRODUCTION

Nowadays, security is one of the most significant necessities in society and the demand for highly secure authentication systems is increasing all over the world. In this context, biometrics plays an important role. Biometrics refers to the use of distinctive anatomical and behavioral characteristics for automatically recognizing individuals [1]. The importance of biometrics is in the fact that the anatomical and behavioral characteristics of an individual cannot be misplaced, shared, or copied. Among all biometric technologies, fingerprint analysis is universally used due to its easy acquisition, high distinctiveness, persistence, and acceptance by the public [2, 3]; however, other technologies, such as ECG waveform features, are also found in the literature [4]. Fingerprint recognition has been used in home safety, forensic applications, smartphones, security boxes, smart homes, and even as a work or classroom attendance system [5-9]. Any fingerprint recognition system includes four phases: acquisition, representation (template), feature extraction, and matching [10]. Because the sensor used in this paper carries out the pre- and post-processing of the digital image independently, we can talk about two phases: the enrollment and the matching phase. During the enrollment process, the fingerprint is captured and stored in a database and during the recognition process the fingerprint is captured and compared with all the fingerprints that are stored in that database. This is known as (1:N) matching and helps identify a particular person's fingerprint (1:1). Matching refers to comparing the captured fingerprint with another fingerprint previously enrolled in the database [11] and is commonly used for authentication.

There are several publications about fingerprint recognition. In [12], a fingerprint authentication system is implemented and applied in distance education where courses are developed in learning management systems. A pre-processing of the image was carried out to remove noise and apply a filter to the pattern. In [13], a feature extraction method using minutiae points is proposed. Minutiae points are also used in this paper for fingerprint authentication. In [14], a biometric fingerprint system is designed using Arduino and a fingerprint sensor R305. In [15], a fingerprint system is proposed and tested using an image filtering technique that improves the speed of the system. For real-time implementation, the system is tested using an FPGA (Field Programmable Gate Array). In [16], authors present a fingerprint verification system using a sweep, tactile fingerprint sensor, and an FPGA. The functioning of the system is explained in detail. In [17], an authentication system is implemented using a capacitive fingerprint sensor that embeds a 32-bit microcontroller. In [7], the authors demonstrate the performance of a fingerprint recognition system implemented with an ARM Cortex-M3 microcontroller and an FPC1011F3 capacitive sensor; the final algorithm was also tried in a Raspberry Pi 2 to display the matching results in a Graphical User Interface (GUI). In [18], a fingerprint authentication system is implemented using an FPGA and the processing of the image is carried out. The authors suggest the low cost of the system is due to using the FPGA. Finally, in [19], a fingerprint-based user authentication system is implemented using a T1050.3 Xtensa processor and an AES3400 fingerprint sensor. The sensor is connected to the processor, where the processing of the image is carried out using specific software. Matching results are shown in the processor; however, none of these publications show the schematic of the corresponding circuits and details of the procedure to carry out the hardware implementation. Additionally, [12, 13, 15, 18, 19, 20] carry out an image processing phase that makes the system complex and reduces its portability. This image processing phase is internally carried out by the fingerprint sensor FZ1036G used for this paper. This is possible due to an embedded microcontroller. In [14, 17], the authors also use a fingerprint sensor with an embedded microcontroller to perform image processing.

In this paper, we present the design of a fingerprint authentication system using the microcontroller PIC18f252 and the fingerprint sensor FZ1036G, and implement (1:1) matching. The program is made in MPLAB X IDE v3.65 and then burned into the microcontroller. Once the microcontroller is programmed, the system consists only of the microcontroller and the fingerprint sensor, thus making it portable and efficient. Communication between the PIC and the sensor is by RS232 protocol. The main contribution of this paper is that due to the sensor capacity, the proposed system is able to acquire or match a fingerprint image in less than 1 s. In addition, because the fingerprint sensor has an embedded microcontroller that is in charge of the image processing, there is no need to implement an image processing phase. Moreover, the circuit diagram and details regarding the procedure are shown. The rest of the paper is divided into four sections. Section 2 presents the model used in fingerprint recognition. Section 3 describes the materials, methods used to build the fingerprint recognition system, and the procedures. Section 4 presents the tests, the results, the analysis, and discussion. Finally, Section 5 concludes.

2. MODELING OF FINGERPRINT RECOGNITION SYSTEM

Fingerprints are graphical patterns of ridges and valleys on the surface of fingertips. As illustrated in Figure 1, ridge endings and ridge bifurcation are called “minutiae.” These features define the difference between two individuals’ fingerprints, making this technology possible. Fingerprint recognition systems are possible thanks to two fingerprint characteristics: invariance and singularity. These characteristics basically imply that the fingerprint is unique and it does not change through life [11].

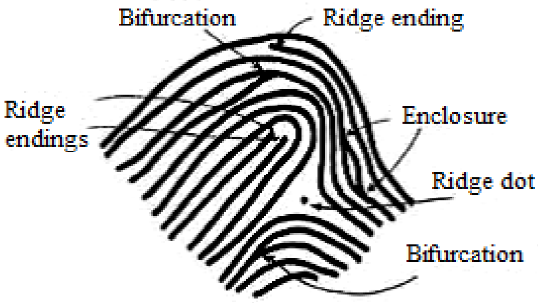

Figure 1. Different ridge features on a fingerprint image [11]

A fingerprint sensor is an electronic device used to capture an image of the fingerprint pattern. The captured image is digitally processed to create a biometric template (a collection of extracted features) that is stored and used for matching. Typical fingerprint sensor technologies include optical sensors, capacitive sensors, RF capacitive sensors, pressure sensors, thermal sensors, and ultra-sound sensors. The optical fingerprint sensors use frustrated refraction over a glass prism (when the skin touches the glass, the light is not reflected but absorbed). The finger is illuminated from one side by an LED while the other side transmits the image through a lens to a camera as shown in Figure 2 [21].

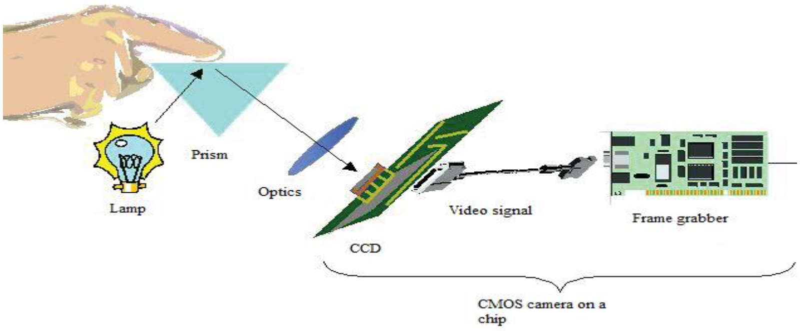

Figure 2. Optical fingerprint sensor technology [21]

2.1. Image processing stages

The FZ1036G is an optical fingerprint sensor with an embedded microcontroller that carries out the image processing phase. The next three stages are as follows [21]:

2.1.1. Image acquisition

This stage refers to capturing the image of the fingerprint pattern.

2.1.2. Image pre-processing

The purpose of this stage is to increase the clarity of the captured fingerprint pattern. Some typical image pre-processing techniques are image segmentation, binarization, elimination of noise, smoothing, and thinning. These techniques basically help remove unwanted data from the pattern [21].

2.1.3. Feature extraction

This stage refers to extracting the features that make fingerprints unique with respect to ridge endings and bifurcations. The most common method to extract these features is called the "crossing number" (CN) approach. This method involves skeletonization of the image and extraction of the minutiae. The CN value is then computed. The CN is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood pixels. Mathematically, the CN for a pixel P is given by (1) [22]:

$$CN = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i-1}|, P_9 = P_1, \qquad (1)$$

where P_i is the pixel value in the neighborhood of P. Once the CN is computed, the corresponding pixel can be classified as a minutiae or non-minutiae point using Table 1.

Table 1. Crossing number property [22]

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

2.1.4. Matching

This is the stage where the comparison between the acquired pattern and the patterns stored in the database is carried out.

2.2. Proposed fingerprint recognition system

The proposed fingerprint authentication system is divided into three blocks as shown in Figure 3. Software and hardware implementation are implied. The system allows the user to choose between three function modes: store fingerprint, delete fingerprint, and verify fingerprint. The modes can be selected by pressing some hardware buttons. Image acquisition, which consists of creating the fingerprint and creating a pattern, is done by the sensor. In the store fingerprint mode, this pattern is stored in the database; however, in the verify fingerprint mode, the pattern is compared with the pattern that was previously stored in the database. The desired function mode and the user`s fingerprint refer as system inputs or the variables that are in charge of the user so that the system can perform the desired actions.

In the verification mode, the system generates an output authentication result. This is the block where a device to be controlled is also implemented. There are three devices to be controlled that comprise the output of the system: a buzzer, an LCD display, and a motor. The motor is in charge of opening and closing the door depending on the result of the authentication. The buzzer is activated when the fingerprint that is verified is not stored in the database and the LCD display shows the result of the authentication. The program, made in MPLAB X IDE v3.65 and then burned into the microcontroller, consists of the logical processes that the system has to perform.

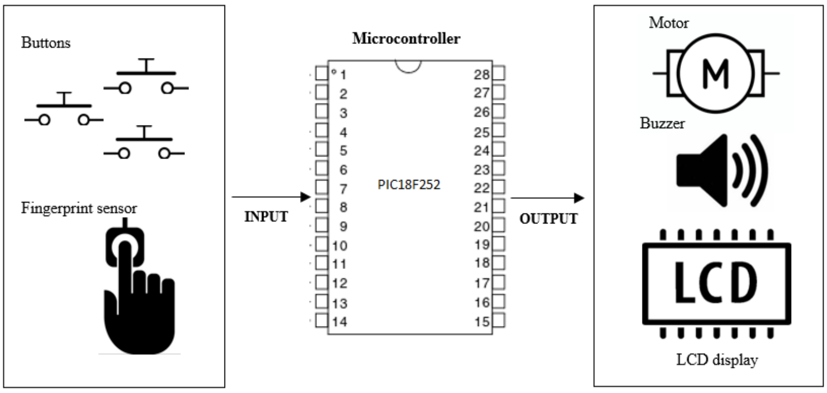

Figure 3. Block diagrams

3. MATERIALS AND METHODS

The circuit used is shown in Figure 4. The system is powered by a 5 V DC source. The buttons are used select the function mode. The button and output results use the I/O ports of the microcontroller. The LCD is used so that the user can observe the state of the system. After the verification process, the system displays a message to indicate whether the fingerprint image is stored in the database or not.

The materials used to build the fingerprint recognition system and their detailed descriptions are listed in Table 2. Because the current requirement of the buzzer is low, it can be activated directly from the output of the microcontroller. However, due to the motor current requirement, a transistor and an independent DC voltage source are implemented to control power dissipated in the motor.

Communication between the fingerprint sensor and the microcontroller is by RS232 protocol. Therefore, the reception pin of the sensor is connected to the transmission pin of the microcontroller and vice versa. When communicating, the command/data/results are bundled in a data package format as described in Table 3. Once the fingerprint sensor receives the commands, it will report the result by sending back an “acknowledge” packet. This packet includes a 1-byte confirmation code that confirms whether the fingerprint has been stored or not and if there is a matching result.

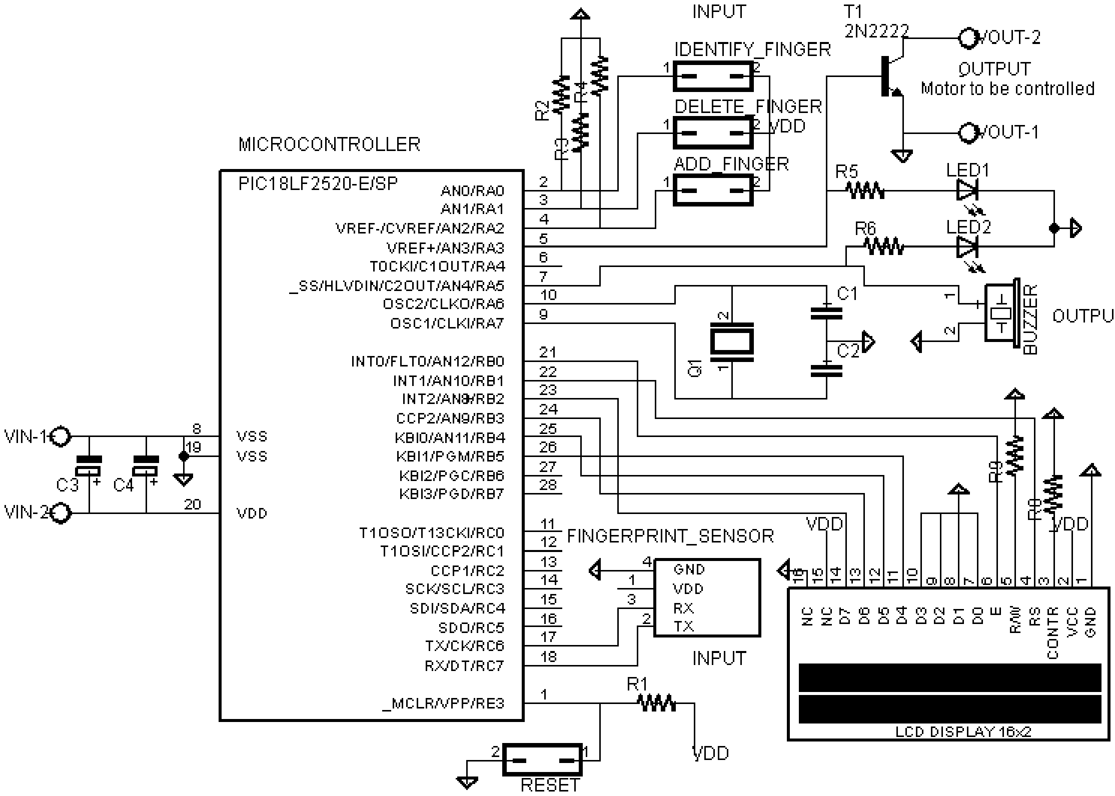

Figure 4. System schematics

Table 2. Materials

Component	Characteristics
Microcontroller PIC18f252	Operating frequency 20 MHz; serial communications: MSSP, addressable USART; I/O ports
Fingerprint sensor FZ1036G	Interface: UART (TTL logical level); Baud rate: 9600 (default)
I2C LCD 16x2	Ref: DRF0063
Buzzer	Variable voltage 3 V-15 V DC
Crystal	20 MHz
Button	Normally open
Door prototype	3–5 V DC motor
Resistors, capacitors, LEDs	Different values
Transistor	NPN transistor; Ref: 2N2222

Table 3. Definition of data package taken from the fingerprint sensor datasheet

Name	Symbol	Length	Description
Header	START	2 bytes	Fixed value of EF01H; High byte transferred first.
Adder	ADDR	4 bytes	Default value is 0xFFFFFFFF, which can be modified by command. High byte is transferred first and at wrong adder value, module will reject to transfer.
Package identifier	PID	1 byte	01H: Command packet 02H: Data packet; Data packet shall not appear alone in the executing process, must follow command packet or acknowledge packet. 07H: Acknowledge packet 08H: End of data package
Package Length	Length	2 bytes	Refers to the length of package content (command packets and data packets) plus the length of checksum (2 bytes). Unit is byte. Max. length is 256 bytes, and high byte is transferred first.
Package contents	DATA	-	It can be commands, data, command parameters, acknowledge result, etc. (fingerprint character value, template are all deemed as data).
Checksum	SUM	2 bytes	The arithmetic sum of package identifier, package length, and all package contents. Overflowing bits are omitted. High byte is transferred first.

4. RESULTS AND ANALYSIS

The experimental set-up is shown in Figure 5. It was designed as a door prototype to illustrate the system's functionality. The DC voltage source is used as the voltage source for the entire system including the fingerprint sensor, the LCD display, and the microcontroller.

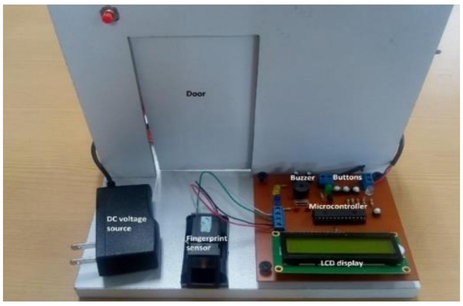

Figure 5. Experimental set-up

As explained in Section 2.2, an independent DC voltage source and a transistor were implemented to control the power dissipated in the motor. The interesting fact about this is that it is possible to use any kind of motor by simply replacing the independent voltage source with the corresponding one and using an element such as a relay or a power transistor to control the power dissipated in the motor. The importance of this resides in being able to implement the system in any kind of application that uses any kind of motor. Three trials were conducted to test the functioning of the system.

4.1. Storing mode test

To carry out this test, four people were chosen-two females and two males. The idea was to measure the effectiveness of the system when storing a fingerprint. Each person made 30 attempts to store their fingerprint. The results are shown in Table 4.

Table 4. Storing test results

Person	Gender	Attempts	Stored	Not Stored	Percentage Stored
Person 1	Male	30	27	3	90%
Person 2	Male	30	28	2	93.3%
Person 3	Female	30	28	2	93.3%
Person 4	Female	30	27	3	90%
				Average	91.7%

The results show that the system is effective when storing fingerprints; moreover, no relation was found between the gender of the people and the effectiveness. When storing a fingerprint, the user has to place their finger on the scanner twice in succession to allow the device to compare them and store the better image. This may explain the times the fingerprint was not stored as the fingerprints must be exactly the same both times for it to be stored. It could also be due to inconsistent finger placement.

4.2. Verification mode test

Four people two females and two males were used also to test the system's fingerprint verification function (i.e., verification mode). Each person made 30 attempts to verify their print (the fingerprint of each system was previously stored). The time to perform the verification was found to be less than 1 s. The results are shown in Table 5.

Table 5. Verification test results

Person	Gender	Attempts	Verified	Not Verified	Percentage Verified
Person 1	Male	30	29	1	96.6 %
Person 2	Male	30	28	2	93.3 %
Person 3	Female	30	29	2	96.6 %
Person 4	Female	30	29	1	96.6 %
				Average	95.8 %

The results show that the system is more effective when verifying fingerprints; moreover, no relation between the gender of the people and the effectiveness was found. When verifying the fingerprint, the user only has to place their finger once, which makes it easier for the system to verify. The times the fingerprint was not verified can be due to inconsistent finger placement.

4.3. Angle placement test

The functioning of the system is dependent on the angle at which the person places their finger. To test this dependence, a finger was gradually place on the sensor at different angles with the purpose of verifying or storing its fingerprint. It was found out that there is no relation between the angle at which the user places their finger and the verification or storage functions; that is, it does not matter how the user places their finger on the fingerprint sensor as it does not affect the results. This is explained by the way the system performs the matching process. As explained in Section 2.1.3, during the feature extraction, the system extracts the minutiae from the fingerprint pattern and uses this to perform the matching. It is important to mention that even though the angle of placement changes during the test, the user always places the same area of their finger on the fingerprint sensor, which means the system always extracts the same minutiae and the matching result is not affected.

5. CONCLUSION

In this work, we have developed a portable and efficient fingerprint authentication system. The system employs an optical fingerprint sensor with an embedded microcontroller that performs effective image processing. Moreover, the system can be easily implemented to supply any kind of authentication such as for home safety, automobile safety, and security boxes. The performance evaluation shows encouraging results. There is no effect of user gender or the angle at which they place their finger on the verification and storage of the fingerprint. The system is effective when verifying and storing fingerprints and the process of matching takes no more than 1 second. The results show that the percentage of verified fingerprints (95.8%) was higher than the percentage stored (91.7%). This is because when storing a fingerprint, the user has to place their finger on the sensors in two successive motions, creating a higher possibility of failure in storing the fingerprint.

ACKNOWLEDGEMENTS

The authors thank to the School of Physics, and the Department of Electrical Engineering and Automation for the valuable support to conduct this research. This work was supported by the Universidad Nacional de Colombia, Sede Medellín under the projects HERMES-34671 and HERMES-36911.

REFERENCES

[1] P. Schuch and S. Schulz, and C. Busch. “Survey on the impact of fingerprint image enhancement," *IET Biometrics*, vol. 7, pp. 102-115, 2018.

[2] H. Xu, R. Veldhuis, T. Kevenaar and T. Akkermans. “A Fast Minutiae-Based Fingerprint Recognition System," *IEEE systems journal*, vol. 3, No. 4 pp. 418-427, December 2009.

[3] M. Ghafoor, S. Iqbal, S. Tariq, I. Taj and N. Jafri. “Efficient fingerprint matching using GPU," *IET image process*, vol. 12, pp. 274-284, 2018.

[4] A. Y. Shdefat, M. Joo, S. Choi, H. Kim, “Utilizing ECG Waveform Features as New Biometric Authentication Method,” *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 2, pp. 658~665, April 2018.

[5] I. Dror and J. Mnookin. “The use of technology in human expert domains: challenges and risks arising from the use of automated fingerprint identification systems in forensic science," *Oxfords journals*, vol. 9, pp. 47-67, January 22, 2010.

[6] F. Ishengoma. “Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies," 2014.

[7] J. Arcenegui, R. Arjona, and I. Baturone. “*Demonstrator of a fingerprint recognition algorithm into a low-power microcontroller*," Conference on *Design and Architectures for Signal and Image Processing (DASIP)*, pp. 1-2, 2017.

[8] Fahad-Bin-Mazhar, O. Ahamed, and M. Rasedujjaman, “Biometric smart attendance kit with fingerprint scanner by using microcontroller," *International Conference on Electrical and Electronic Engineering (ICEEE)*, pp. 13-16, 2015.

[9] J. Han, “Fingerprint Authentication Schemes for Mobile Devices,” *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 5, No. 3, pp. 579~585, June 2015.

[10] A. Jain, L. Hong, S. Pankanti and R. Bolle. "*An Identity-Authentication System Using Fingerprints*," Proceedings of the *IEEE*, vol. 85, No. 9, September 1997.

[11] Mouad. Ali, Vivek. H, Pravin. Y, and Gaikwad A., "*Overview of fingerprint recognition system*," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1334-1338, 2016.

[12] R. Gil, G. Orueta, M. Tawfik, F. Garcia-Loro, A. Pesquera, E. Sancristobal, S. Martín and M. Castro. "Fingerprint Verification System in Tests in Moodle," *IEEE journal of Latin America Learning Technologies*, vol. 8, No. 1, February 2013.

[13] N. A. Rakib, SM Z. Farhan, Md M. B. Sobhan, J. Uddin, A. Habib, "A Novel 2D Feature Extraction Method for Fingerprints Using Minutiae Points and Their Intersections," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No. 5, pp. 2547~2554, October 2017.

[14] M. Martin, K. Štefan, F. Ľubor, "Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino," *TELKOMNIKA Telecommunication Computing Electronics and Control*, Vol.16, No.2, pp. 755~765, April 2018.

[15] T. Khan, D. Bailey, M.Khan and Y. Kong. "Efficient Hardware Implementation For Fingerprint Image Enhancement Using Anisotropic Gaussian Filter," *IEEE transactions on image processing*, vol. 14, No. 8, June 2016.

[16] N. Galy, B. Charlot and B. Courtois. "A Full Fingerprint Verification System for a Single-Line Sweep Sensor," *IEEE sensor journal*, vol. 7, No. 7, July 2007.

[17] S. Jung, J. Nam, D. Yang, and M. Lee. "A CMOS Integrated Capacitive Fingerprint Sensor With 32-bit RISC Microcontroller," *IEEE journal of solid-state circuits*, vol. 40, no. 8, August 2005.

[18] A. S. Shinde and V. Bendre, "An Embedded Fingerprint Authentication System," *International Conference on Computing Communication Control and Automation*, pp. 205-208, 2015.

[19] P. Gupta, S. Ravi, A. Raghunathan, and N. K. Jha, "*Efficient fingerprint-based user authentication for embedded systems*," Proceedings of the 42nd annual conference on Design automation - DAC `05, pp. 244, 2005.

[20] S. R. Borra, G. J. Reddy, E. S. Reddy, "An Efficient Fingerprint Identification using Neural Network and BAT Algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 2, pp. 1194~1213, April 2018.

[21] Lunji Qiu. "Fingerprint sensor technology," *IEEE 9th Conference on Industrial Electronics and Applications (ICIEA)*, Shanghai, China, 2014.

[22] A. Chaudhari, G. Patnaik, S. Patil. "Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept," *Informatica Economica*, vol. 18, No. 1, 2014.

BIOGRAPHIES OF AUTHORS

Mauricio García Vargas Engineering physics student, Science Faculty, Universidad Nacional de Colombia, Medellín, Colombia, E-mail: maugarciavar@unal.edu.co. His research interests include applied electronics and physics.

Fredy Edimer Hoyos Electrical Engineer, MEng Industrial Automation, Ph.D in Automation. Assistant professor, Science Faculty, School of Physics, Universidad Nacional de Colombia Sede Medellín, Colombia, E-mail: fehoyosve@unal.edu.co. His research interests include nonlinear control, nonlinear dynamics of nonsmooth systems, and power electronic applications. He is a member of the Applied Technologies Research Group-GITA, at the Universidad Nacional de Colombia.
https://orcid.org/0000-0001-8766-5192

John Candelo received his BS degree in Electrical Engineering in 2002 and his PhD in Engineering with emphasis in Electrical Engineering in 2009 from the Universidad del Valle, Cali - Colombia. His employment experiences include the Empresa de Energía del Pacífico EPSA, Universidad del Norte, and the Universidad Nacional de Colombia - Sede Medellín. He is now an Assistant Professor of the Universidad Nacional de Colombia - Sede Medellín, Colombia. His research interests include: engineering education, planning, operation, and control of power systems; artificial intelligence; and smart grids. He is a member of the Applied Technologies Research Group-GITA, at the Universidad Nacional de Colombia. https://orcid.org/0000-0002-9784-9494.