TELKOMNIKA, Vol.16, No.2, April 2018, pp. 755~765
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i2.7572

Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino

Magdin Martin*, Koprda Štefan, Ferenczy Ľubor
Constantine the Philosopher University in Nitra, Faculty of Natural Sciences,
Department of Computer Science, Tr. A. Hlinku 1, 949 74 Nitra, Slovakia
*Corresponding author, e-mail: mmagdin@ukf.sk, skoprda@ukf.sk

Abstract

The idea of security is as old as humanity itself. Between oldest methods of security were included simple mechanical locks whose authentication element was the key. At first, a universal–simple type, later unique for each lock. A long time had mechanical locks been the sole option for protection against unauthorized access. The boom of biometrics has come in the 20th century, and especially in recent years, biometrics is much expanded in the various areas of our life. Opposite of traditional security methods such as passwords, access cards, and hardware keys, it offers many benefits. The main benefits are the uniqueness and the impossibility of their loss. The main benefits are the uniqueness and the impossibility of their loss. Therefore we focussed in this paper on the the design of low cost biometric fingerprint system and subsequent implementation of this system in praxtise. Our main goal was to create a system that is capable of recognizing fingerprints from a user and then processing them. The main part of this system is the microcontroller Arduino Yun with an external interface to the scan of the fingerprint with a name Adafruit R305 (special reader). This microcontroller communicates with the external database, which ensures the exchange of data between Arduino Yun and user application. This application was created for (currently) most widespread mobile operating system-Android.

Keywords*: fingerprint, authentication, arduino yun, pattern, ridge lines*

1. Introduction

The area of biometric recognition is focused to the use of individual biometric characteristics. We can say, that are fingerprint, scan of eyes (pupils) or classification of face features for automatically recognition systems. Especially the fingerprints are uses most widely successful in biometric recognition system [3]. Most often, fingerprint authentication is used to protect the user's personal information [23]. By the concept of biometrics, we mean a set of automated methods designed to identify and verify a person's identity. This set of automated methods is based on physiological and behavioural characteristics, called biometric keys or biometrics features. The advantage of biometric features, unlike other ways of identifying people, is universality and uniqueness. By comparing the biometric features, it is possible to uniquely identify the user. These features are still–not changed in the time. Biometrics refers to various physiological/behavioural traits, not only to the fingerprint. In research, Biometrics area is also iris, face, and keystroke dynamics. The Biometric area removed in latest year's problems with password. Unlike a password, biometrics cannot be forgotten or stolen. This makes biometric modalities more suitable for authentication applications, especially from the perspective of the users [4]. Authentication of people using biometric data is an attractive area of research because the authentication process also examines characteristics that are unique and measurable. Unlike a classic identity management (eg passwords, tokens, or PINs), the biometric security system results in an authentication request to how much similar or dissimilar the biometric query is to its counterpart stored in the database [19]. Therefore these systems present several advantages over classical security methods [7-8], [20]. Classical methods as passwords and PINs must be often changed for purpose holdback of security. The biggest problem is that are difficult to remember [12]. Therefore today has increased impact of the employment of biometrics data (e.g. in social identification as a access control to the network). We can say that this way is accepted a very secure method for identification and people authentication [18]. Authentication systems using biometric traits work in several steps. In the

Received October 14, 2017; Revised February 11, 2018; Accepted February 22, 2018

first step, must be the user enrolled into proposed system. The biometric traits are captured and stored in a form of a reference template. In the second step is stored reference template compared with a sample template. The third step is templates matching. If everything is alright, then output from the system is fully available to the user. However, false denials can lead to frustration and reduce user productivity to repeated verifications, therefore are we using various enhancement techniques for fingerprint images as described in the following section Theoretical background.

2. Theoretical Background

Fingerprinting is one of the basic biometric features. The research area that is dealing with fingerprints is called dactyloscopy. It is a science of the papillary lines on the inside of human fingers. The shapes of the papillary lines, their course and direction, are very different for every person. According to the shapes that the papillary lines create, it is possible to determine several base patterns that serve to sort all of the shapes. For classification of individual fingerprint are used four patterns as a standard [15].

Classification pattern number 1, so called ARCH-the papillary lines, more often called as ridge lines, creates simple arcs as shown in Figure 1. Classification pattern number 2, so called RADIAL-the ridge lines create a loop that leads in left side. On right side from the middle of the loop is a mark, the so-called *delta*. Between delta and the middle must be at least 1 line as shown in Figure 2.

Figure. 1. Classification fingerprint pattern ARCH

Figure 2. Classification fingerprint pattern RADIAL

Classification pattern number 3, so called *WHORL*–the ridge lines create circular, oval, spiral, two-loop shapes and contain at least two deltas with at least one line as shown in Figure 3. Classification pattern number 4, so called *ULNAR*–the ridge lines create a loop, that leads in the right side. On the left side from the middle is the delta. Between delta and the middle must be at least 1 line as shown in Figure 4.

Figure 1. Classification fingerprint pattern WHORL

Figure 2. Classification fingerprint pattern ULNAR

These patterns are intended for manual comparison of fingerprints in a classical way - responsible person manually compares two fingerprints between each other and is looking for compliance. Fingerprint images are however rarely in perfect quality, often are corrupted due to

variations in skin. Therefore we must image enhancement techniques are employed for a more reliable estimation of minutiae locations [3]. The image enhancement of fingerprint is a key step for biometric authentication from the reason of elimination different factors. These factors are such as skin condition (very dry or moist, damaged or worn down skin, etc.) but also sensor noise [10]. Fingerprint image quality enhancement techniques are usually preferred, in order to improve the quality of the image. Therefore was development various techniques for reducing noises and increasing the contrast between the ridges and the valleys in the gray-scale fingerprint images. Image enhancement approaches are implemented in spatial domain [21], [5], and in frequency domain [13], [22] or Gabor Filter to improve gray-scale fingerprint first introduced by Daugman and later Hong [1],[2],[6]. Due to the frequency-selective and orientation-selective properties, the Gabor filter achieved a desirable performance on fingerprint enhancement [11].

A completely different approach to fingerprint images processing was chosen by Mahdi Jampour. In your paper with the title *A New Technique in saving Fingerprint with low volume by using Chaos Game and Fractal Theory* explains how is possible by using fractal theory and by the assistance of Chaos Game a new fractal made from fingerprint. Jampour describes we as while making the new fractal by using Chaos Game mechanism some parameters, which can be used in identification process, can be deciphered. For this purpose, a fractal is made for each fingerprint and with this way we save 10 parameters for every fingerprint. The presented technique in this report has been carried out by MATLAB and has been experimented on 600 samples of fingerprint from each of which there are four samples. The advantage of using this technique is the high accuracy of fingerprint images recognition - results which are obtained show 100% success for this technique [9].

Other different approaches in biometrics bring Semwal. According to Semwal, the human gait is considered to be a unique biometric identification tool similar to a fingerprint. It can be used to identify people in various security applications and to detect walking abnormalities before permanent damage occurs. The data used for pattern classification and in the analysis of different walking styles can also be employed to predict the likelihood of diseases by detecting abnormalities in the gait pattern. Furthermore, the gait is a signature of human walking that can be used for personal identification purposes. In his study proposed a new gait identification method. Using the proposed methodology, the gait identification accuracy was improved by employing more accurate spatiotemporal modeling. Extensive simulations demonstrated that this is a highly robust feature extraction technique. The classification rate and activity reorganization activity were improved substantially using the new method [17-18].

However currently exist several complex solutions from various producers. These solutions allow locking or opening the lock with fingerprint. Most widespread system is FAB ENTR, Impresoft FP, and Alarmtel IFP. These solutions include a built-in reader module for fingerprints. Managing of fingerprints is provided via the built-in keyboard or by external application. Often can we use also direct Bluetooth connection between smartphone and the lock. The price range of these solutions ranges from 250 € to 450 € with VAT (in Slovakia).

Figure 3. Biometric locks from producers Alarmtel, Impresoft and FAB ENTR

3. Proposal of System for Authentication using Fingerprint

The disadvantage of referred systems as shown in Figure 5 is relatively expensive price and missing versatility of the solution. These solutions cannot be used for common human

activity. As an example, can be seen authentication of user to access the car or activation of the car engine, control of the industrial robot only on the basis of fingerprint authentication and the like. Therefore, we focused in our proposal of solution not only summary price (max. 130 €) but also versatility of overall solution. Based on the current state (see please section *Theoretical background*) we have decided to use a number of non-related systems, and to link them together, so that the user authentication has been accomplished using a fingerprint biometric and that the versatility and simplicity of this solution was maintained.
Based on this reason, we have decided for the following hardware equipment of the system:
a. Microcontroller Arduino Yun,
b. Fingerprint reader R305 (FPM10).
Functional requirements for the system are as follows:
a. The system can load, process, and store fingerprints,
b. After successfully processing of the fingerprint, the system simulates the open/close state of the lock, respectively reject the access for unauthorized person,
c. The system contains mobile application for a control,
d. All parts of the system communicate with each other through a local network or the Internet,
e. The system evaluates fingerprints very quickly (max up to 1-2 seconds),
f. The hardware part works in conjunction with the mobile application but also can function independently (e.g. in the network failure case) i.e., on the hybrid principle.
Other system requirements are as follows:
a. The authentication part of the system is built on the Arduino platform,
b. The mobile app is programmed for Android platform,
c. The interface element between the hardware - authentication part of the system and the mobile application of the system is the server with the database,
d. The system has low power consumption,
e. The hardware components of the system are selected with the best price/performance ratio of the system.
Every part of the system is made up from several different types of devices. From a global viewpoint, we can draw our system as the following scheme as shown in Figure 6.

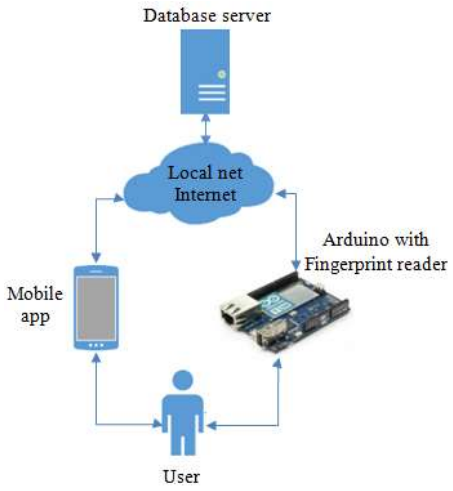

Figure 6. Global Scheme of Our Proposed System

As a data repository for the authentication system, we chose the database. When choosing a database system, we followed the following criteria that the database system had to meet:
a. Relational database system,
b. Support for transactional processing,
c. Low hardware requirements,
d. Low purchase price, ideal free database system.

Based on these requirements we chose database system MySQL that is available with license GPL-for our need is available free. The database structure was then designed using the MySQL Workbench development tool. The database has the following structure of Tables, relationships and attributes as shown in Figure 7.

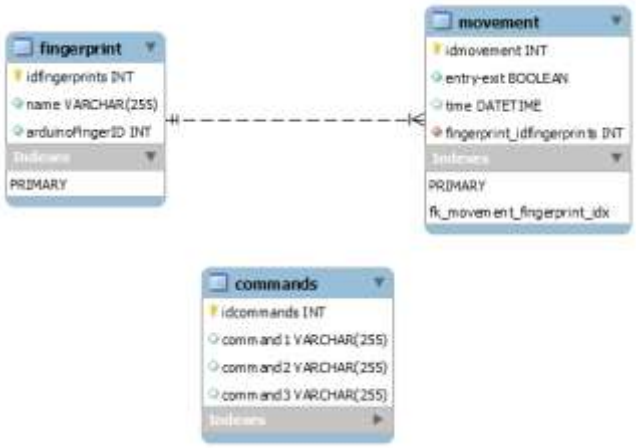

Figure 7. The structure of MySQL tables

As a method of data transfer (to and from the database server), we considered in the design of database the following connectivity:

a. Direct connection of Arduino Yun via MySQL connector,
b. Direct connection via MSQL connector through an encrypted VPN tunnel,
c. Sending data via PHP parameters in the URL (GET and POST).

As a transfer method, we chose to send data via HTTP parameters that will be performed on the server side from PHP scripts. This solution does not require a publicly open MySQL port. Potential attacker in this case does not know our system structure and the attack would be more demanding. The security advantage is also that the templates of fingerprints are not transmitted through the network. The user works directly with only two parts of the system: with the hardware module (contains the fingerprint reader) or the mobile application. The mobile application and the hardware part of the system communicate with one another using a database server and a local network or the Internet. The system therefore requires network connection. As the most appropriate of Arduino board is Arduino Yun with native network support. It includes network microprocessor Atheros, which is controlled via a Linux kernel, based on OpenWRT under the full name OpenWrt-Yun. The board of microcontroller Arduino contains RJ-45 port for Ethernet, USB-A port, WIFI module (with various standards 802.11 b/g/n), slot for microSD card and other important connectors and modules for I/O communication.

For authentication of user based on the biometrics fingerprint, we choose the fingerprint reader with a mark R305. This module realizes the processing of fingerprint, image processing of fingerprint, searching and assigning of fingerprint and saving of the pattern of the fingerprint. For communication with Arduino it uses an UART protocol and can communicate with the speed from 9600 to 115200bps. Module of the fingerprint reader uses the graphical memory and two others 512 bytes memories (short memory term and permanent for saving of the pattern of the fingerprint and various settings).

Usage of the fingerprint reader is automatic. The fingerprint reader can reliably extract minutiae from the input fingerprint images. Quality of a minutiae extraction relies especially from the quality of the input fingerprint images. Therefore is essential using a fingerprint enhancement algorithm directly in the minutiae extraction module. For this step was development various enhancement techniques for processing of the fingerprint images where consist of five main stages: segmentation, normalization, orientation estimation, ridge frequency estimation, and Gabor filtering [3].

Figure 8. The board of microcontroller arduino YUN

Figure 9. The module of fingerprint reader Adafruit R305

3.1. Segmentation

In a fingerprint image are various areas with the background that generally exhibit a very low grey-scale variance value. Some the foreground regions however have a very high variance. Therefore we must the image divided into blocks and calculated the grey-scale variance for each block in the image. The grey-level variance for a block of size *WxW* is defined as:

$$\mathrm{V(k)} = \frac{1}{\mathrm{W}^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}(I(i,j)-M(k))^2 \quad (1)$$

where *V(k)* is the variance for block k, *I(i, j)* is the grey-level value at pixel *(i, j)*, and *M(k)* is the mean grey-level value for the block *k*.

3.2. Normalization

Uses a process that changes the range of pixel intensity values. The normalization is a very simple pre-processing step to improve the image quality (noise reducing from image). The basis of image normalization consists of the changing intensity of each pixel [14]. Normalization is used to standardize the intensity values in an image by adjusting the range of grey-level values so that it lies within a desired range of values. Let *I(i, j)* represent the grey-level value at pixel *(i, j)*, and *N(i, j)* represent the normalized grey-level value at pixel *(i, j)*. The normalized image is defined as:

$$N(i,j) = M_0 + \sqrt{((VAR_0((I(i,j)-M)^2))/VAR} \quad (2)$$

otherwise

$$N(i,j) = M_0 - \sqrt{((VAR_0((I(i,j)-M)^2))/VAR} \quad (3)$$

where M_0 and VAR_0 are the desired mean and variance of the given image and M and VAR are the computed mean and variance of the given image.

3.3. Orientation estimation

The orientation field of a fingerprint image defines the local orientation of the ridges contained in the fingerprint. The least mean square estimation method is used to compute the orientation image [6].

3.4. Ridge frequency estimation

Represents important parameter that is used in the construction of the Gabor filter. The ridge frequency *F(i, j)* for a block centred at pixel *(i, j)* is defined as:

$$F(i, j) = \frac{1}{S(i, j)} \quad (4)$$

where the ridge spacing *S(i, j)* is then computed by counting the median number of pixels between consecutive minima points in the projected waveform. The last step is using Gabor filter.

From scan process of the fingerprint are required at least two identical fingerprints. We need these two fingerprints to eliminate potential errors in the scanning process. These scans are stored in the buffer and are converted to a character file and saved. The image processor determines whether both scans are from the same finger. If yes, then system generates a template of the fingerprint and saves this template. If the scans do not match, the template will not be created and the system will send the return packet with the error code. The whole process can be illustrated by the following flowchart as shown in Figure 10.

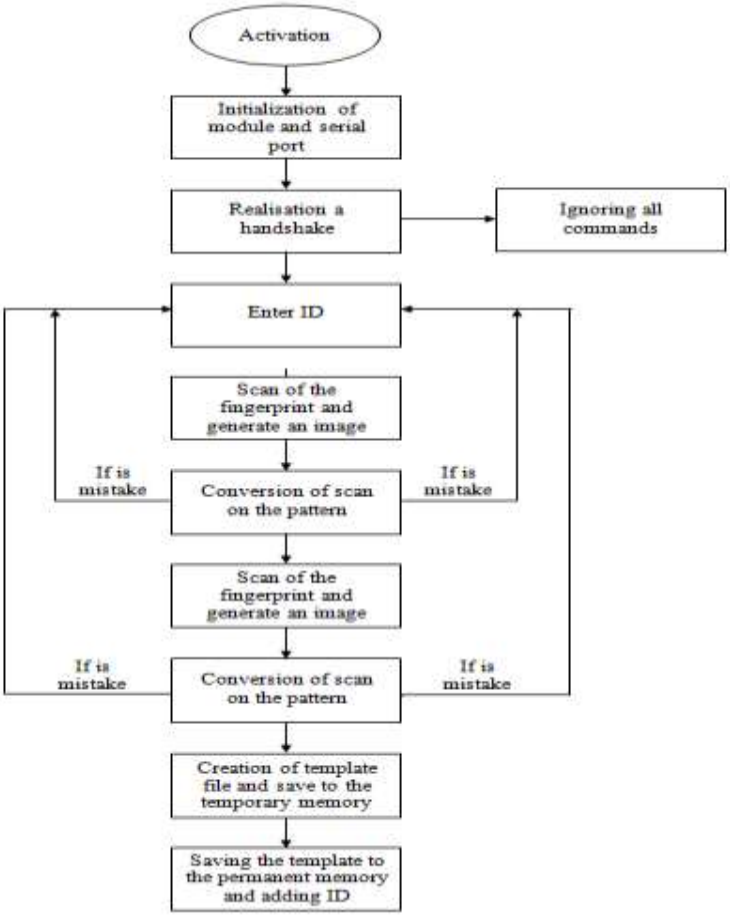

Figure 10. Flowchart of process fingerprint reader–the process of save the template of fingerprint

4. Development of the Mobile App for Android OS and the hardware part–Arduino with Peripherals

Another part of this proposed system is the mobile application. The requirements for the mobile application were as follows:

a. The ability to add new fingerprints to the system,
b. The ability to remove existing fingerprints from the system,
c. Overview about action open/close, people ID, access time,
d. Low hardware requirements of the running application,

e. User-friendly environment to control.
f. As a development environment, we used software Android Studio in version 2.3.1.

The key part of the biometric authentication system is its hardware part controlled by the Arduino Yun microcontroller. In general, however, it is possible after adequate edits of the program to use any Arduino board with support of the network connection. In addition to microcontroller Arduino and the fingerprint reader R305 we used components as LCD (information element), various colours of LED diodes, motion sensor, transistor, the potentiometer, resistors and connecting wires. The motion sensor SparkFun PIR was used for creating of saving mode of the complete device. Saving mode is activated when motion sensor does not detect motion. With this step, we can economize total consumption of electric energy (if we used power supply from battery). We used LED diodes as signal elements for simulation of physical output. Other components are used for protective function, e.g. bipolar transistor BC547B is dedicated for activation or deactivation of the LCD display in activation or deactivation of saving mode. The potentiometer ensures correct adjustment of contrast for font of the LCD display.

Figure 11. The main control menu of mobile app

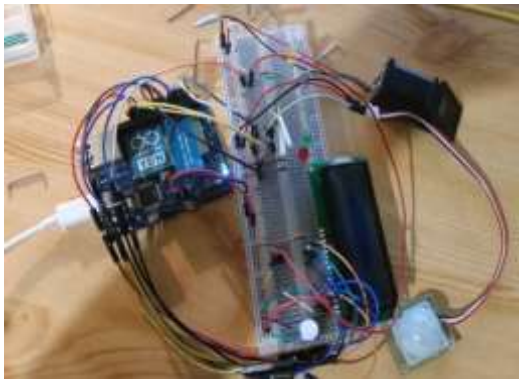

Figure 12. Prototype of hardware part

5. Simple Experiment of Reliability of the Authentication System

To test the reliability of fingerprint recognition we created the following simple test:

a. To the memory of the fingerprint reader we recorded a total of six patterns of fingerprints from three different people, each of these people had two recorded fingerprints,
b. Each of fingerprint was tested with 10x,
c. We realized total 60 authentication attempts.
d. The results of successful authentication testing are summarized as shown in Table 1:

Table 1. Results of Authentication Attempts

	Person 1		Person 2		Person 3	
Attempt numb.	Fingerprint 1	Fingerprint 2	Fingerprint 3	Fingerprint 4	Fingerprint 5	Fingerprint 5
1.	x	□	□	x	□	□
2.	□	x	□	□	x	□
3.	□	□	□	□	□	□
4.	□	x	□	x	□	□
5.	□	x	□	□	□	□
6.	□	□	□	□	□	□
7.	x	□	□	□	x	□
8.	□	□	□	□	□	□
9.	□	□	□	□	□	□
10.	□	□	x	□	□	□
Success	8	7	9	8	8	10

The Legend: X=Unsuccessful attempt, □=Successful attempt

The total authentication success rate is 50 successful attempts out of a total of 60 attempts, a success rate of 83.3%. From the measurements, we can see that most unsuccessful attempts were during the first attempts. This initial lower success was caused because of the human factor. Tested humans must have to become accustomed to the force of finger pressure, immobility during scanning and other minor subjectively caused motions that prevent successful authentication. We also tested the system on the fingerprint patterns that were not saved in the database. Of the total of 50 attempts with 6 different unauthorized fingerprints patterns, there was not even one false authentication, which means 100% resistance to access by not authorized users. Another factor of possible system unreliability that occurred during the testing process was sensitivity to Wi-Fi signal quality. In locations where the smartphone Samsung Galaxy S5 reported about 50% signal strength, the Arduino Yun board was experiencing sporadic Wi-Fi connection failure (as we noticed by the mobile application connection error messages). The reason was the smaller size and hence the weaker gain of the built-in antenna of Arduino Yun (only 0,5dBi). One of the parameters in designing the biometric authentication system was the lowest acquisition cost of the components used but with the emphasis on maintaining the overall functionality of the system.

Total acquisition costs are amounted to approximately 134 € with VAT. A lower price can be obtained by ordering these components from abroad, especially from some Asian countries. However, such a purchase may represent a risk of purchasing non-original components without any compatibility with the original components. This was also our case. We bought a fingerprint reader with the mark R308, but we had problems with its initialization with the Arduino microcontroller.

6. Discussion and Conclusion

Based on the theoretical analysis of current trends in biometrics security, we chose from all the currently used biometrics features for further research of the fingerprints. This form of biometric feature has been selected on the basis of most ideal ratio of properties as: simplicity, easy use for the end-user, the cost of hardware needed to acquire the properties of a given biometric feature, and the support of the hardware on the selected open-source Arduino platform. We proposed and realized a system with the impact on an emphasis of easy use for the end-user. This system consists of two user parts. First part is mobile app, which is programmed currently for mobile OS Android. The app was written in Java and in the IDE Android Studio. For the end user, it offers the ability to manage fingerprints, specifically adding new fingerprint patterns and removing existing fingerprints. The last option of the application is to view report of user's accesses on the basis on the attributed names to the individual fingerprint patterns. The exchange of data between the authentication hardware and the application takes place via a relational MySQL database.

The second part is a hardware system, which is controlled via microcontroller Arduino Yun (could be possible with also other microcontroller with network connection). The authentication hardware applies hybrid principle of activity-in standard mode it works using network connection with session to database but in case of power cut it can work also as a standalone authentication element. The most important peripheral component of microcontroller Arduino is the fingerprint reader module Adafruit R305. For the notification of the person, that is trying to authenticate, is used a specific monochrome LCD display. Since there is an amount of specific types of locks and locking devices, we simulated the locking and unlocking activity with LED diodes. In practical applications, they can be completely replaced by switching relays or stepping motors. This system has low energy requirement–max. 0.7W in activity and 0.4W in saving mode. The saving mode works on the principle of motion detection on the basis motion PIR sensor in neighbour of the fingerprint reader module. In case of motion absence, system is in the "sleep" mode, i.e. the components with the largest electricity consumption (LCD and fingerprint reader) are shut down. This shutdown of components is realized using bipolar transistor of type NPN. After motion detection is system activated and ready for scanning of the fingerprint.

Total price of this system is maximum 134 € with VAT. The system can be connected to the external system of power supply. However, such a backup power supply will only be relevant if the power supply of the locking mechanism and in ideally, the network devices that provide a network connection–Wi-Fi router or other router/switch, is cut. The potential problem of this system could be its sensitivity of extreme temperatures outside the interior. The most sensitive component of the system is the LCD display that has trouble-free operation at temperatures between -10 °C and +40 °C. Also, possible moisture would rapidly reduce the life of the system in the outdoor environment. The solution would be to create a suitable enclosure with the minimum degree of protection IP64.

The system in comparison to the existing solutions from companies like FAB ENTR, Impresoft FP and Alarmtel IFP, offers the benefit of a lower acquisition price (134 € vs. 250 €) and better adaptability also to the non-traditional locking mechanism. When creating our system, we also encountered a problem with incompatible, probably non-original hardware. On the market exists also fingerprint reader with a mark R308 that is visually completely identical as the R305 but uses two more signal wires (6 wires at R305 vs. 4 wires at R308). For this fingerprint reader was not possible to reliably initiate almost any kind of communication using library Adafruit or others. The manufacturer however described the full compatibility with the Arduino microcontroller in the technical description. This incompatible hardware of the fingerprint reader module is probably a non-original imitation with problematic functionality, and therefore we had to replace this R308 module with the R305 fingerprint reader module that was fully functional during the implementation process. Overall success of authentication from all attempts was 83.3%.

References

[1] Daugman, JG. Uncertainty Relation for Resolution in Space, Spatial Frequency, and Orientation Optimized by Two-Dimensional Visual Cortical Filters. *Journal of the Optical Society of America A: Optics and Image Science, and Vision,* 1985; 2(7): 1160-1169. 10.1364/JOSAA.2.001160

[2] Daugman, JG. Complete discrete 2D Gabor transforms by neural networks for image analysis and compression. *IEEE Transactions on Acoustics, Speech and Signal P (ASASP),* 1988; 16(7): 1988, 1169–1179.

[3] El-Sisi, A. Design and implementation biometric access control system using fingerprint for restricted area based on Gabor filter. *International Arab Journal of Information Technology,* 2011; 8(4), 355-363.

[4] Ghouzali, S, Lafkih, M, Abdul, W, Mikram, M, El Haziti, M, Aboutajdine, D. Trace attack against biometric mobile applications. *Mobile Information Systems,* 2016.10.1155/2016/2065948

[5] Greenberg, S, Aladjem, M, Kogan, D. Fingerprint image enhancement using filtering techniques. *Real-Time Imaging,* 2002; 8(3): 227-236.

[6] Hong, L, Wan, Y, Jain, A. Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 1998: 20(8): 777-789. 10.1109/34.709565

[7] Indrawan, G, Sitohang, B, Akbar, S. Review of sequential access method for fingerprint identification. *TELKOMNIKA (Telecommunication Computing Electronics and Control),* 2012; 10(2): 335-342.

[8] Jain, AK, Ross, A, Pankanti, S. Biometrics: A tool for information security. *IEEE Transactions on*

Information Forensics and Security, 2006; 1(2), 125-143. 10.1109/TIFS.2006.873653
[9] Jampour, M, Javidi, MM, Nejad, AS, Ashourzadeh, M, Yaghoobi, M. A new technique in saving fingerprint with low volume by using chaos game and fractal theory. *International Journal of Interactive Multimedia and Artificial Intelligence*, 2010; 1(3): 28–32.
[10] Kocevar, M, Klampfer, S, Chowdhury, A, Kacic, Z. Low-quality fingerprint image enhancement on the basis of oriented diffusion and ridge compensation. *Elektronika Ir Elektrotechnika,* 2014; 20(8), 49-54. 10.5755/j01.eee.20.8.8440
[11] Li, X, Zhang, L, Yin, Y. *A Novel Fingerprint Enhancement Algorithm using Curve Mask.* 10.1007/978-3-642-33506-8_38. 2012.
[12] Nikam, SB, Agarwal, S. Ridgelet-based fake fingerprint detection. *Neurocomputing,* 2009; 72(10-12), 2491-2506. 10.1016/j.neucom.2008.11.003
[13] Sivaranjani, R. Gabor Filter Based Finger Print Enhancement Techniques: A Comparative Study, *International Journal of Advance Research in Computer Science and Management Studies*, 2015; 3(4): 390-399.
[14] Saddique, S, Khiya, MSH, Khan, A, Khanum, M. Modified sequential algorithm using euclidean distance function for seed filling. *Journal of Theoretical and Applied Information Technology,* 2010; 19(1): 9-14.
[15] Saparudin, Sulong, G. A technique to improve ridge flows of fingerprint orientation field's estimation. *TELKOMNIKA (Telecommunication Computing Electronics and Control),* 2016; 14(3): 987-998. 10.12928/TELKOMNIKA.v14i3.3112
[16] Sepasian, M, Mares, C, Balachandran, W. Vitality detection in fingerprint identification. *WSEAS Transactions on Information Science and Applications,* 2010; *7*(4): 498-507.
[17] Semwal, VB, Raj, M, Nandi, GC. Biometric gait identification based on a multilayer perceptron. *Robotics and Autonomous Systems,* 2015; 65: 65-75. 10.1016/j.robot.2014.11.010
[18] Semwal, VB, Singha, J, Sharma, PK, Chauhan, A, Behera, B. An optimized feature selection technique based on incremental feature analysis for bio-metric gait data classification. *Multimedia Tools and Applications,* 2017; 76(22): 24457-24475. 10.1007/s11042-016-4110-y
[19] Singh, YN, Singh, SK. A taxonomy of biometric system vulnerabilities and defences. *International Journal of Biometrics,* 2013; 5(2): 137-159. 10.1504/IJBM.2013.052964
[20] Wayman, JL. Biometrics in identity management systems. *IEEE Security and Privacy*. 2008; 6(2): 30-37. 10.1109/MSP.2008.28
[21] Yang J, Liu L, Jiang T, Fan Y. A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognition Letters,* 2003; 24(12): 1805-1817. 10.1016/S0167-8655(03)00005-9
[22] Yin YL, Zhan XS. An Algorithm Based on Gabor Function for Fingerprint Enhancement and Its Application. *Journal of Software*. 2003; 14(3): 484–489.
[23] Zafar, MR, Ali Shah, M. *Fingerprint authentication and security risks in smart devices*. Paper presented at the 2016 22nd International Conference on Automation and Computing, ICAC 2016: Tackling the New Challenges in Automation and Computing, 2016: 548-553. 10.1109/IConAC.2016.7604977.