People Recognition Interface based on Biometric Sensors Connected to an Arduino Mega 2560 Board

Catalin Lupu and Corneliu-Octavian Turcu

"Ștefan cel Mare" University of Suceava, Romania

Summary
Biometric authentication has grown significantly since the events in the United States in 2001. Moreover, during the COVID-19 pandemic, many more researches have been done on contactless biometric authentication or recognition methods. Arduino Mega 2560 is a module often used in designing applications, but most of the time it can only be used as an interface in image processing. During the post-doctoral researches in multimodal biometrics, it was developed a complex application using the Arduino Mega 2560 board and several sensors attached to it, including two fingerprint sensors, an infrared imaging camera, a keyboard and a Bluetooth module that allows communication between this device and a mobile device or a desktop / laptop system. The developed application can be used for registration or authentication to an internet banking system, by entering the biometric features represented by iris and fingerprint, in addition to the classic authentication methods, based on username and a password generated by a digipass. The application and the device only have the role of taking the iris or the fingerprint, these being transmitted via Bluetooth for processing on a mobile or laptop device. Biometric analysis and extraction cannot be performed on the Arduino Mega 2560 due to the low frequency of the processor (12 MHz only) and the relatively small memory space.

Keywords: *iris recognition, COVID-19, SARS-CoV-2, vaccination, digital ceriticate*

1. Introduction

In articles [1] - [8] are presented a lot of information about biometric technologies and their various uses. This article will present an interface for taking the image of the iris and two fingerprints, in order to authenticate to applications such as internet or mobile banking.

2. Theoretical Consideration

The system uses an Arduino Mega 2560 module, to which several sensors are connected, which will be detailed below. This system aims to increase security for access to internet banking applications. Thus, it starts from the idea of a token that generates a certain 6-digit code, after entering a PIN set by the user. This is also used in this project, but in addition to generating an OTP (One Time Password) code, there is also the recognition of people by iris and fingerprint.

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.88

The schematic diagram of this system is shown in Figure 1.

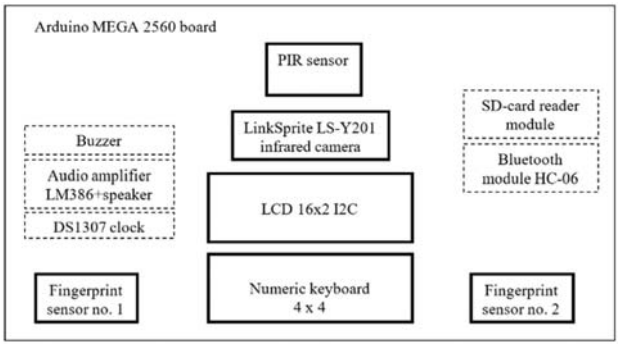

Fig. 1. The main schema for the proposed system

The devices used to carry out the project are shown in Figure 2. Starting from the diagram above, the components in this figure can be easily identified. The figure shows the used devices not connected to the Arduino Mega 2560 development board.

Figure 3 shows the sensors connected to a breadboard that interacts with the development board. The use of a breadboard was chosen because of the large number of sensors, which each require a power supply. Also, two of the sensors use only two pins in addition to the power supply, a technology called I2C (or IIC - Inter-Integrated Circuit).

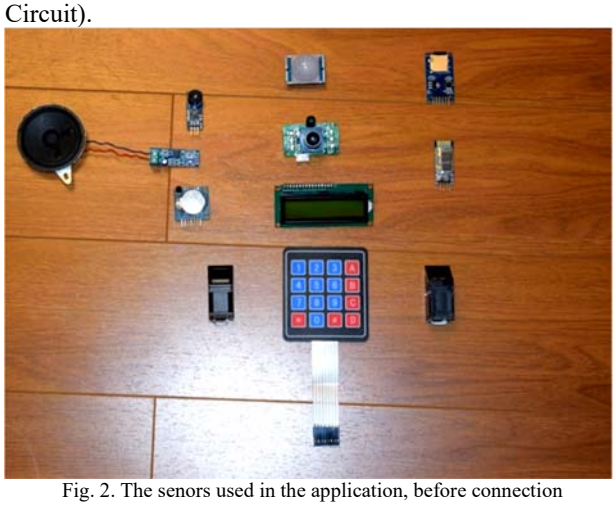

Fig. 2. The senors used in the application, before connection

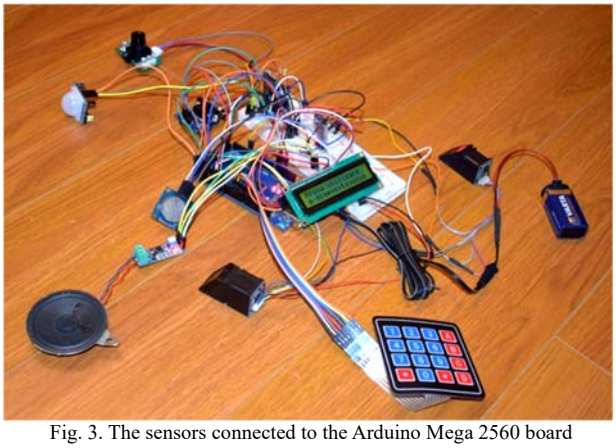

Fig. 3. The sensors connected to the Arduino Mega 2560 board

The sensors that make up the system will be presented below.

2.1. Fingerprint sensors

Adafruit Fingerprint Reader sensor clones were used, namely R307 and R303. The sensor Adafruit Fingerprint R303 are shown in Figure 4.

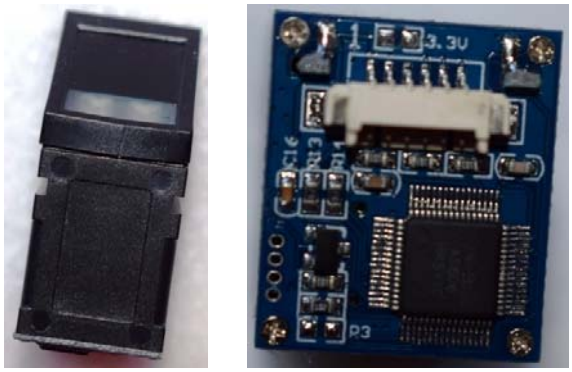

Fig. 4. Fingerprint sensor Adafruit Fingerprint R303

The SFG Demo application produced by Adafruit was used to test the operation of the sensors. Prior to using the application, the Arduino module must be programmed with a code that will initiate serial communication. This is done through the application provided by Arduino. The sequence code for the initialization ("sketch") is shown in Figure 5.

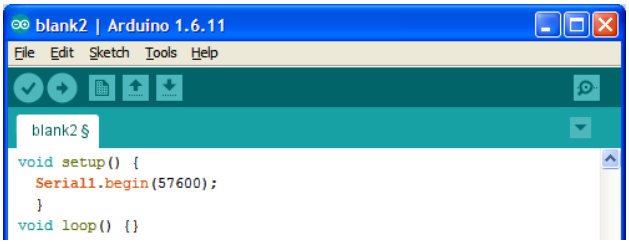

Fig. 5. Arduino initialization

After programming the Arduino device with this code, the SFG Demo application can be opened. In the first phase, press the "Open Device (O)" button, select the serial port to which the device is connected (in this case COM2), then the message to successfully open communication with the device appears in the upper right - Open Device Success). Figure 6 shows the main application window after initiating communication with the device.

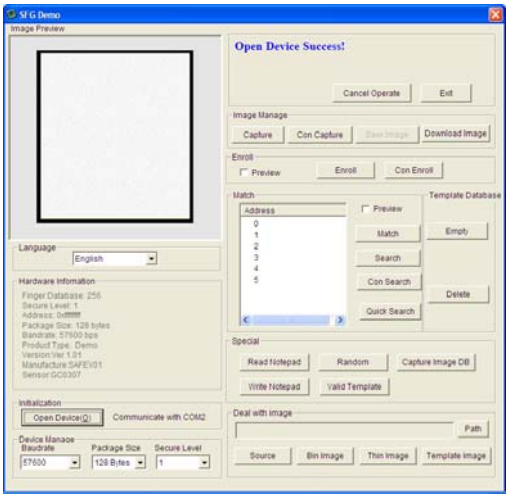

Fig. 6. SFG Demo home page

After initiating communication with the device and the sensor, images can be captured or the person recorded in the system. The fingerprint sensor is equipped with a very fast processor, which provides a very fast response to the captured image in less than a second. However, it takes a much longer time to display the image at the top left of the app - over 5 seconds - due to the low rate of information transfer between the fingerprint picker, the Arduino module, and the computer that is connected to it. via a USB cable that provides a communication of only 57600 bauds.
Figure 7 shows a fingerprint taken from the sensor and transferred to the application.

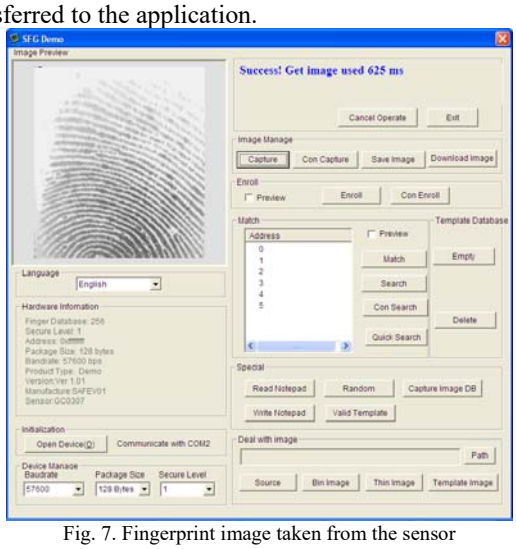

Fig. 7. Fingerprint image taken from the sensor

The purpose of the Arduino module and the fingerprint sensor is to provide fingerprints to a computer, although the sensor has the ability to process a detected fingerprint very quickly (as you can see, fingerprint recognition and image transfer was under a second, 625ms). In the developed project, the image was taken from the sensor and was processed according to those presented in the references [1]-[8].
The sensors are connected to the Serial1 and Serial2 ports of the Arduino module. The "Adafruit_Fingerprint.h" library is used to work with the sensors, and the following sequence is used to initialize them:

```
#define ser1 Serial1
#define ser2 Serial2

Adafruit_Fingerprint finger1 = Adafruit_Fingerprint (& ser1);
Adafruit_Fingerprint finger2 = Adafruit_Fingerprint (& ser2);
```

This module can be programmed to allow access to a vehicle or to start its engine. A similar idea was published by the author in the article [9], presented at the ISCII 2007 conference, and which so far has no less than 32 citations in international journals. The sensors can also be used to access internet banking applications.
The Arduino module can be programmed in two operating modes: for user registration (enrollment) or for checking / identifying user fingerprints (how it works normally).
After programming the module in the person registration mode, when you press the "Serial monitor" button in the programming application of the Arduino device (the version used was 1.8.1) you can see the operation of this application. This can be seen in Figure 8.

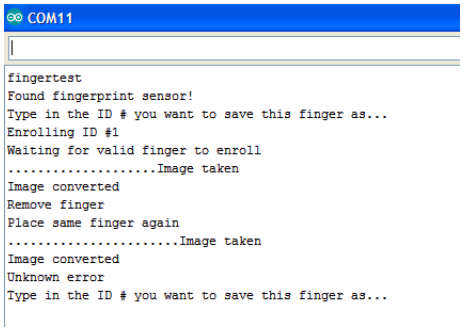

Fig. 8. How the application works in user registration mode

When programming the module for verification / identification mode, it will wait for a finger to appear on the fingerprint sensor during the "loop" routine, and then check or identify the fingerprint in the database previously created in recording mode. If a valid fingerprint is identified, it will grant access to internet banking applications. If an attempt is made to use the fingerprint sensor with a specified number of invalid fingerprints (for example 5), then an SMS may be sent to a registered user to identify the cause.

2.2. Motion detector sensor (PIR)

The term PIR stands for “Pyroelectric ("Passive") InfraRed Sensors”. The HC-SR501 presence sensor was used in the developed application. This module has a power consumption of 65 mA and contains a plastic cover above the sensor that acts as a divergent lens, which allows the sensor to detect objects over a much longer radius, up to 7 meters. The sensitivity of the sensor can be adjusted from a potentiometer. The PIR sensor can be seen in the Figure 9.
The purpose of using this sensor is to determine if a person is near the module or is attempting to defraud the system through a remote Bluetooth connection. It can also be used to exit the system from standby.
The sensor is connected to port 26 of the Arduino Mega 2560 mode, and the declaration of the variables for the presence sensor is done as follows:

```
int inputPinPIR = 26; // choose the pin for the presence sensor
int pirState = LOW; // at first, no motion is assumed to be detected
```

The sensor status is read using the *digitalRead function* . If the returned value has the value HIGH, then it means that motion has been detected.

Fig. 9. HC-SR501 PIR Sensor

2.3. 4x4 keyboard

The 4x4 matrix keyboard with a female pin connector is used to enter or set the PIN when using the system for the first time. This keyboard has 4 lines and 4 columns, being similar to that of the token for generating unique passwords, with the observation that it has an extra column (the one on the right). Figure 10 shows this keyboard. The connection to Arduino is made on 8 wires, in this project using the PWM inputs 4-11. Pressing a key generates a pulse on the row and column pins. The "Keypad" library was used for this use, the declaration of the keyboard variable being the following:

```
const byte ROWS = 4; // Four lines
const byte COLS = 4; // Four columns
// Key position
char keys [ROWS] [COLS] = {
{,1 ',' 4 ',' 7 ',' * '},
{,2 ',' 5 ',' 8 ',' 0 '},
{,3 ',' 6 ',' 9 ',' # '},
{,A B C D'}};
// Define the lines ROW0, ROW1, ROW2 and ROW3, which connect to
// these pins.
```

```
Byte rowPins [ROWS] = {7,6,5,4};
// Columns COL0, COL1 and COL2.
Byte colPins [COLS] = {11,10,9,8};

// Create the Keypad kpd variable
Keypad kpd = Keypad (makeKeymap (keys), rowPins, colPins, ROWS,
COLS);
```

Fig. 10. 4x4 matrix keyboard with connector

2.4. LinkSprite LS-Y201 camera

Figure 11 shows the LinkSprite LS-Y201 camera. It contains a lens that can capture images in up to 640x480 format, a light sensor (at the top of the lens) and 6 infrared LEDs. The LEDs light up only if the light sensor does not detect a high enough light intensity. In order to always be lit in order to take the infrared image, the light sensor was covered, to be misled and to believe that the light intensity is very low.

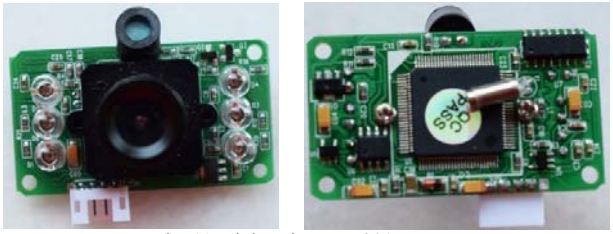

Fig. 11. LinkSprite LS-Y201 camera

An image taken with this camera can be seen in Figure 12. One of the advantage of this camera is that the picture can be taken in infrared light and can be used by iris recognition systems. Classically, the image used by these systems is in taken in near-infrared light.

Fig. 12. Image taken by the LS-Y201 camera

The downloaded images will be transferred to a mobile device or computer, which will process it and try to extract the iris code, as described in papers [1]-[9]. Below are some screenshots made with the applications available in the Google Play Store - "Arduino bluetooth controller" (version 1.3 - figure 13) and "S2 Terminal for Bluetooth (F)" (version 4.0.3 - figure 14).

Fig. 13. Captured image via Arduino Bluetooth controller

Fig. 14. Capture the image via S2 Terminal for Bluetooth (F)

2.5. Bluetooth HC-06

The module, shown in Figure 15, is used to provide communication between the Arduino Mega 2560 development module and a mobile device or computer equipped with Bluetooth. It connects to the A8 and A9 pins of the Arduino, the communication being done by using the "SoftwareSerial.h" library. The declaration of the variable for bluetooth is done as follows:

```
#define RxD A8
#define TxD A9

SoftwareSerial bth (RxD, TxD);
```

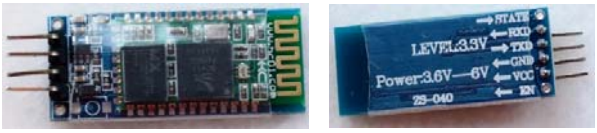

Fig. 15. HC-06 bluetooth module

3. Experimental Consideration

The logic diagram in Figure 16 shows the steps taken to initialize the communication between the Arduino Mega 2560 development module and the sensors that are connected to it.
In the case of the first use of the device (determined by reading the value 1 from position 2003 in the EEPROM) the user will be registered, according to the logic diagram in figure 17.
The recording scenario is as follows:

- the bank clerk connects to the device registration application on the bank's server;
- communication is made via Bluetooth with the device;
- a 4-digit password is set for PIN and Bluetooth communication;
- the fingerprint is recorded on sensor 1 and then on sensor 2;
- the iris is recorded using the LinkSprite LS-Y201 camera;
- the official disconnects from Bluetooth and the registration application and configures the client's phone to make the connection via Bluetooth.

After registration or if it is not the first use of the device, enter the LOOP loop, where events from the serial port, bluetooth or keyboard are expected. Upon receipt of an event in any of these ways, the event is processed. If the device is not used for 5 minutes, it will enter standby mode. The logical scheme of this process is presented in figure 18.

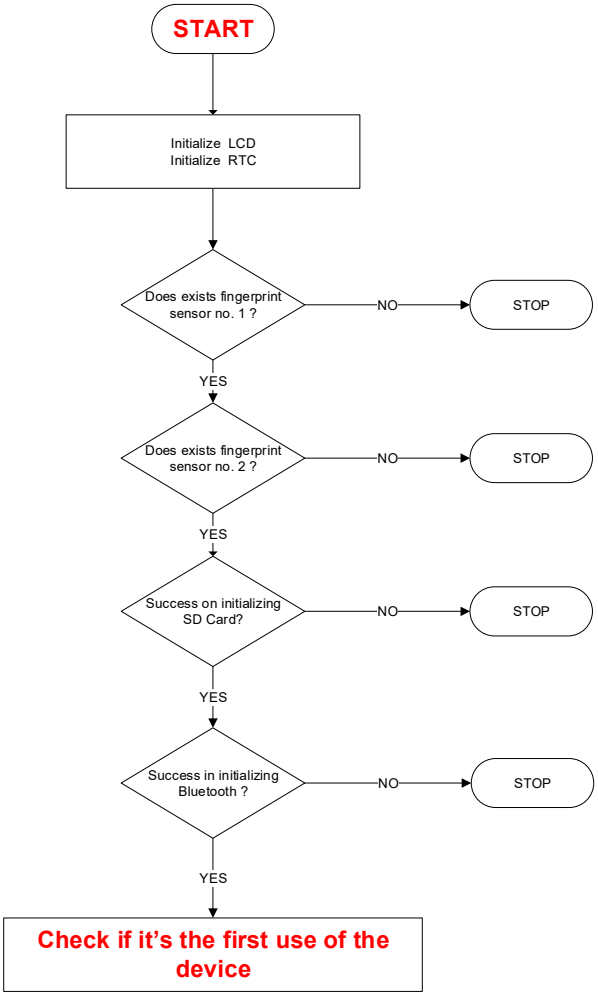

Fig. 16. System initialization steps

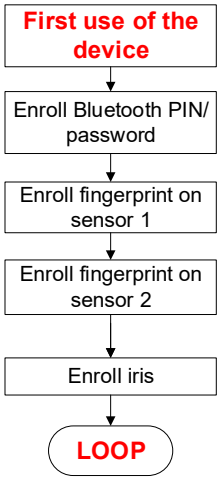

Fig. 17. Flowchart for the first use of the device

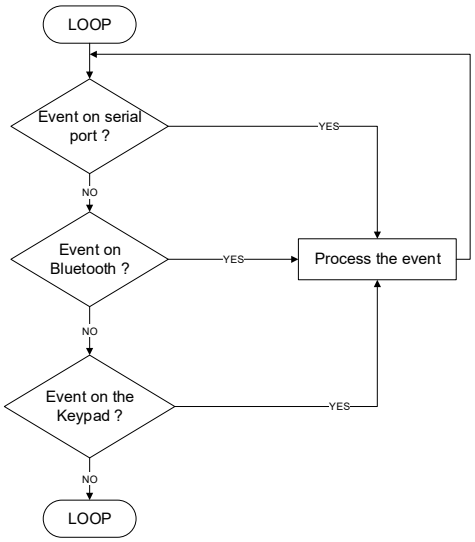

Fig. 18. Waiting for events in the LOOP loop

The logic diagram in figure 19 is used to process the events.

The security of the system is ensured by several checks, among which the most important would be:

- the MAC address of the bluetooth device is checked with the one registered in the database;
- read certain values from the EEPROM memory, from default addresses, to see if they are identical to the user's private key stored on the server.

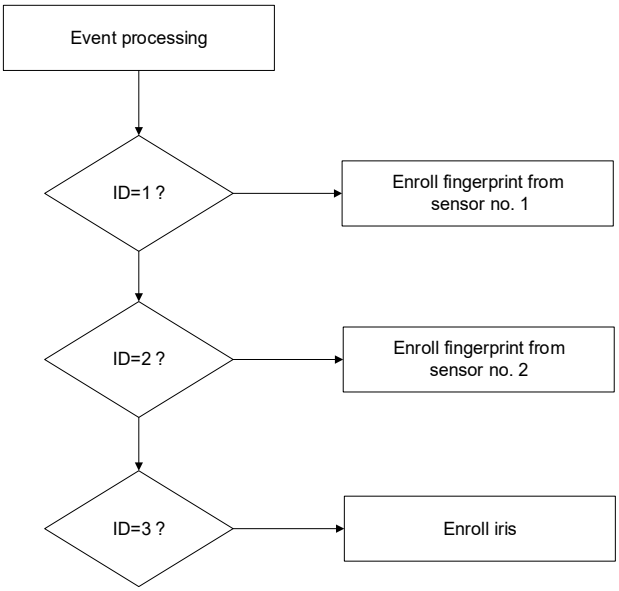

Fig. 19. Event processing

On the figure 20 it can be seen the main flowchart of the online banking application. The schema was largely discussed in papers [2] and [5].

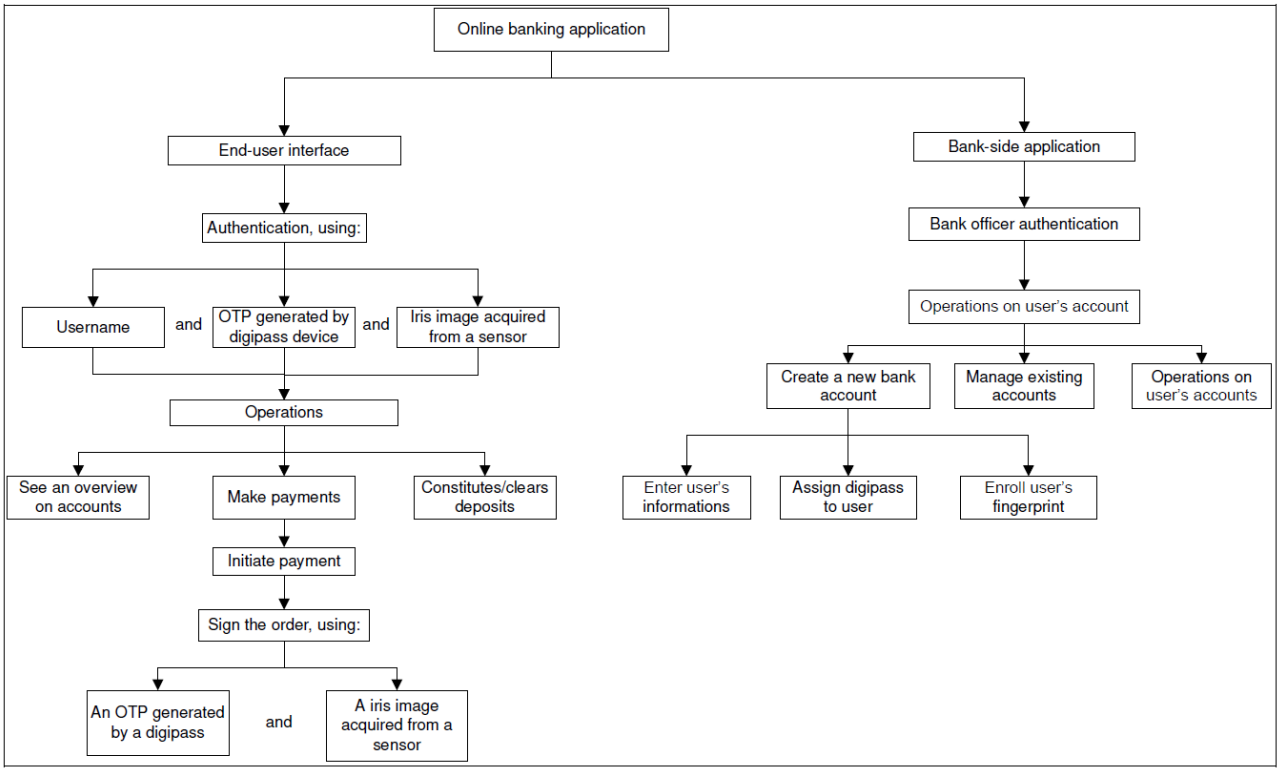

Fig. 20. Main flowchart for online banking registration or authentication

4. Conclusion

The developed application was used to register fingerprints and irises from a great number of persons. Also, it was used to acquire fingerprints and irises in order to perform personal recognition. The board Arduino Mega 2560 was a good interface between the sensors and the computer or a mobile device. The main problem of the board is that complex graphical processing cannot be performed on it because of low memory and very slow clock speed.

Acknowledgment

This work is supported by the project ANTREPRENORDOC, in the framework of Human Resources Development Operational Programme 2014-2020, financed from the European Social Fund under the contract number 36355/23.05.2019 HRD OP /380/6/13 – SMIS Code: 123847.

References

[1] LUPU, Cătălin; Valeriu Lupu, " *Biometrics used for authentication in internet-banking applications* ", Annals of the "Contantin Brâncuşi" University of Târgu Jiu / Annals of the "Constantin Brâncuşi" University of Târgu Jiu, Engineering Series, Nr. 3/2014, ISSN 1842-4856, B + cod 718, pp. 57-63, 2014

[2] LUPU, Cătălin ; Valeriu Lupu, Gheorghe Gîlcă, " *Securing online banking services using iris recognition* ", Annals of the "Contantin Brâncuşi" University of Târgu Jiu / Annals of the "Constantin Brâncuşi" University of Târgu Jiu, Engineering Series, Nr. 4/2015, ISSN 1842-4856, pp. 69-75, 2015

[3] LUPU, Cătălin ; Valeriu Lupu, Gheorghe Gîlcă, " *Overview on a personal recognition system that uses iris images as main biometric characteristic* ", Annals of "Contantin Brâncuşi" University of Târgu Jiu / Annals of the "Constantin Brâncuşi" University of Târgu Jiu, Engineering Series , Nr. 4/2015, ISSN 1842-4856, pp. 76-79, 2015

[4] LUPU, Cătălin; GĂITAN, Vasile-Gheorghiţă; LUPU, Valeriu, "*Security enhancement of internet banking applications by using multimodal biometrics*", SAMI 2015, Herl'any, Slovakia, pp. 47-52, ISBN 978-1-4799-8220-2, DOI: 10.1109 / SAMI.2015.7061904 7301177, 2015

[5] LUPU, Cătălin ; Vasile-Gheorghiţă GĂITAN, Valeriu LUPU, " *Fingerprints used for security enhancement of online banking authentication process* ", IEEE 7th International Conference on Electronics, Computers and Artificial Intelligence - ECAI 2015, vol. 7, no. 1, pp. 217-220, ISSN 1843-2115, 2015

[6] LUPU, Cătălin; Valeriu Lupu, „ *The beginnings of using fingerprints as biometric characteristics for personal identification purposes*", Annals of „Contantin Brâncuşi" University from Târgu Jiu / Annals of the „Constantin Brâncuşi" University of Târgu Jiu, Engineering Series, Nr. 3/2014, ISSN 1842-4856, pp. 53-56, 2014

[7] LUPU, Cătălin, "*Development of optimal filters obtained through convolution methods, used for fingerprint image enhancement and restoration*", The USV Annals of Economics and Public Administration, Section 5: Statistics, economic informatics and mathematics, vol. 14, no. 2 (20) / 2014, pp. 156-167, ISSN 2285-3332, Online ISSN 2344-3847, 2014

[8] LUPU, Cătălin; Vasile-Gheorghiţă Găitan, Valeriu Lupu, "*Improving the Security of Internet Banking Applications by Using Multimodal Biometrics*", Journal of Applied Computer Science & Mathematics, no. 19 (9) / 2015, Suceava, pp. 37-42, ISSN 2066-4273, 2015

[9] Lupu, C., and V. Lupu. "*Multimodal biometrics for access control in an intelligent car*", 2007 International Symposium on Computational Intellgence and Intelligent Informatics. IEEE, 2007.

Cătălin LUPU received the B.Sc. degree from "Ștefan cel Mare University" from Suceava in 2003. He received the Dr. Eng. degree from the same University 14 years later, in 2017. He has been a research assistant and a university assistant at "Ștefan cel Mare" University from 2003 until now. His research interest includes biometric technologies, recognition of persons, iris and fingerprint matching and programming techniques.

Prof. Cornel Turcu was born in 1966 in Adjud, Romania. He received the B.Sc. and Ph.D. degrees in automatic systems, from the University of Iasi, Romania, in 1991, and 1999, respectively. Since 1991, he has been with the Faculty of Electrical Engineering and Computer Science, University of Suceava (USV), where he is a full professor of System Theory and Intelligent Systems. At USV he is also a supervisor for Ph.D. and MS theses. He has published over 70 research papers and 4 books. His research interests include intelligent systems, RFID systems and automatic control system design.