Romanian Journal of Petroleum & Gas Technology
VOL. IV (LXXV) • No. 2/2023

INTELLIGENT ACCESS SECURITY SYSTEM

Antonio Costin Dinca [1]

Alexandru Craciun [1]

[1] Petroleum-Gas University of Ploiesti, Romania
e-mail: gbucur@upg-ploiesti.ro

DOI: 10.51865/JPGT.2023.02.04

ABSTRACT

For any person, company or institution, to secure goods, data, information, different methods were sought and thus the idea of access control appeared. Access control can be done by mobile phone, PIN code, access cards and, perhaps, the most secure way, the biometric feature. Once this idea appeared, it was also desired to automate access, in addition to securing it, and thus, the concept of an access control system appeared. These systems are used on a large scale, both in the public and in the private sector, because they ensure the improvement of the level of protection. This work aims to present a fingerprint-based access control system and the steps that are the basis of its implementation, starting from the block diagram, the functional specifications, the electrical diagram and up to the improvements made to the microcontroller program in the system component.

Keywords: fingerprint, security system, biometric sensor, access control

INTRODUCTION

At the moment, access control systems represent a fundamental component of any physical security solution for data or people, being intended to limit the access of unauthorized persons to certain spaces. The basis of current intelligent access systems is the biometric characteristics, i.e. fingerprint sensors.

The pattern formed by the ridges and valleys on the fingertips is called the fingerprint. Unlike the skin on the rest of the body, the skin on the palms and soles consists of ridges and valleys that do not contain hairs and sebaceous glands as found on the rest of the body. These papillary marks, called friction ridges, increase friction and thus help grip objects. The ridges are made up of two components, the dermis (lower layer) and the epidermis (upper layer). Males have approximately 20.7 ridges per centimeter, while females have approximately 23.4 ridges per centimeter.

In addition to being used in grasping objects, papillary ridges are used in biometric recognition. The pattern of ridges on each finger is unique and unchanging, being considered one of the most important distinguishing marks [1].

The reasons why fingerprint techniques have become so useful in identification are related to the fact that no two people have the same fingerprints. Even with identical twins, when two individuals have exactly the same DNA, their fingerprints are different.

This is due to the fact that, although the models have the same genetic basis, they are also affected by the environmental conditions in which they develop. Once the fingerprint pattern has been formed it remains the same throughout life [8].

Today, fingerprint sensors are the most popular forms of biometric security in use, with a variety of systems on the market. Huge and bulky fingerprint scanners are long gone; now a fingerprint scanning device can be small enough to be embedded in a smartphone.

The principle behind the operation of the optical fingerprint sensor is total internal reflection. The sensor uses glass as its contact surface, which geometrically represents a prism. When the finger is not on the surface of the prism, the phenomenon of total internal reflection occurs, thus all the light is captured by the camera of the fingerprint sensor. When the finger is positioned on the fingerprint, the phenomenon of total internal reflection disappears and the phenomenon of failed total reflection occurs, therefore the camera inside the sensor captures the shape of the ridges and the fingerprint is captured.

The captured image is transformed into a graphic model and stored in the database, being then used to identify the person who wants access by analyzing the new captured image with the one in the database. If these data match, the scan result will be positive and access will be allowed [3].

A user's template can be drawn from a single biometric sample or generated by processing multiple samples obtained during enrollment. Thus, the detail template of a finger can be extracted by mosaicking (combining) multiple scans of the same finger. Some systems store multiple templates to account for the large variations that may be seen in a user's biometric data.[4]

Currently, Samsung and Qualcomm have managed to develop the most advanced fingerprint sensor in the world, the 3D Sonic Max ultrasonic scanner. This sensor is able to register the fingerprints of two fingers simultaneously through a secure touch, thus reducing the fingerprint registration time. With the advent of this fingerprint reader, it can be said that the security of access systems has increased exponentially, as the false acceptance rate is 1:250,000. The high costs of this product, however, made the sensor not yet used on such a wide scale, but most likely, in the future, the ultrasonic sensor will capture the market at the expense of the optical sensor. State-of-the-art models used to enhance fingerprints use neural network architectures that remove noise, so that peaks and valleys have improved clarity. [7]

The architecture of a generic biometric system includes the following modules: a sensor used to collect primary information and convert it into digital format; a signal processing algorithm that will extract an appropriate biometric "signature"; a database in which "signatures" from a population of subjects are stored; a procedure for comparing the "signature" corresponding to an unknown person with those stored in the database; a decision procedure (fully automatic or human-assisted) that uses the result of the previous comparison in order to perform an action (Figure 1).

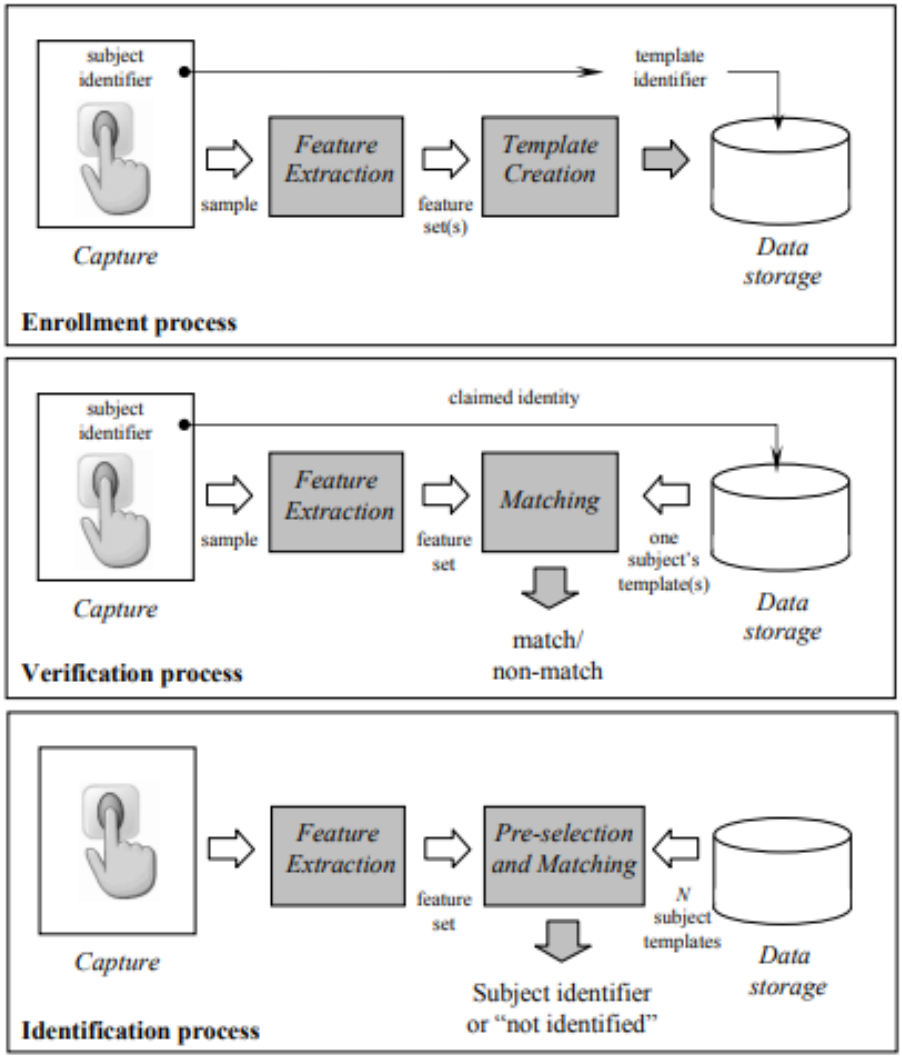

Figure 1. *Enrollment, verification and fingerprint identification processes* [5]

DESIGN AND IMPLEMENTATION OF THE ACCESS SECURITY SYSTEM

The system presented in the work refers to the access to a room through a door, provided with a lock. The door will open only after matching the fingerprint, previously registered and located in the database, the microcontroller sending a signal to the lock that activates its mechanical system and thus, access is allowed. If the fingerprint is recognized, the LCD will show "Fingerprint accepted" and the lock will open, and if the fingerprint does not match, the LCD will show "Idle" and the lock will remain closed [2].

The exit from the considered premises is done by pressing the EXIT button, and thus a signal is sent to the microcontroller, which will command the opening of the door. The message "Activate access" will appear on the LCD. If the EXIT button is not pressed, the door will remain closed.

Since it is desired to use the system in industrial areas, such as refineries, extraction platforms, where gas emissions may occur, the system will be provided with a CO sensor that will warn of exceeding the allowed concentration. In this case, the signal from the

sensor will be transmitted to the microcontroller, the door will open, while the message "CO detected and the respective value" will appear on the LCD. If the CO sensor detects no danger, the door will remain closed.

The block diagram of the system is presented in figure 2.

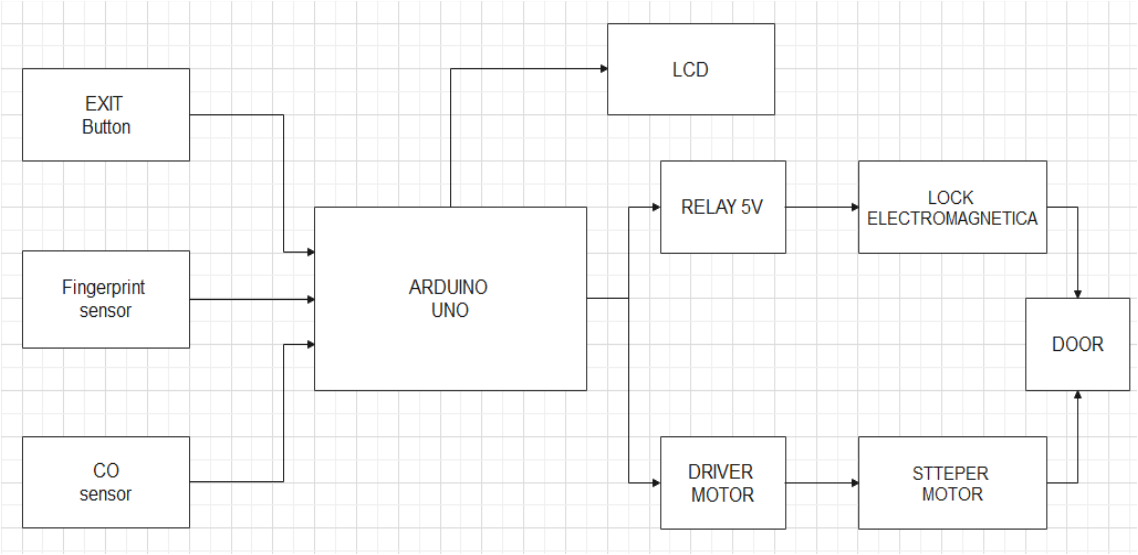

***Figure 2**. Block diagram of the system*

The components of the indoor access control system will be presented in the following.

The fingerprint sensor. The ZFM-20 optical sensor is a very simple all-in-one optical fingerprint sensor module that includes two parts, one for fingerprint registration, and the second part includes matching the fingerprint with those in the library, the matching can be 1:1 or 1:N.

The ZFM-20 sensor module has a fingerprint resolution of 256x288 pixels and can be accessed via the serial interface. Thanks to this feature, the module can connect to Arduino or any other microcontroller. Also, this module has built-in DSP for fingerprint processing and verification.

Arduino Uno R3 development board. This is an open-source platform, based on software and hardware, very easy to use. This is based on a signal processor capable of receiving data from different sensors and transmitting certain actions to the other components connected to the board. The processor is capable of executing commands following programming in a C++-like language. For USB communication, the board uses the CH340g chip.

Liquid crystal LCD screen. The 2004 LCD module displays 2 lines of 16 characters each. It can be used easily even in low light conditions because it also has a background light. Also, the background light must be protected by a resistor or a 2k potentiometer. An I2C module can be used to reduce the number of pins used to connect the LCD to the controller.

5V relay. The module with a relay needs a supply voltage of 5V DC and can be controlled by switching the voltage on the "IN" pin.

12V lock. The lock is opened when it is powered for less than 15 seconds: the door tongue is in normal state when no current flows => the door is closed; the door tongue contracts when powered => the door is open.

Stepper Nema 17. The Nema 17 stepper motor is usually used in 3D printers as it provides high torque and minimizes vibration and noise, but it is also used in various applications due to its very good features and easy to use with a driver. It uses a current of 12v.

Driver A4988. The driver is used to control the stepper motor, it connects via the DIR and STEP pins to the Arduino development board and thus the motor can be controlled easily. It is powered by a 5v supply, but also uses a 12v current required by the stepper motor.

CO sensor – MQ-7. The MQ-7 sensor is a highly sensitive sensor capable of detecting carbon monoxide concentrations between 10 and 10000 ppm in air. The sensor can use only one analog input of the Arduino development board.

The electrical connection diagram of the access system elements is presented in figure 3.

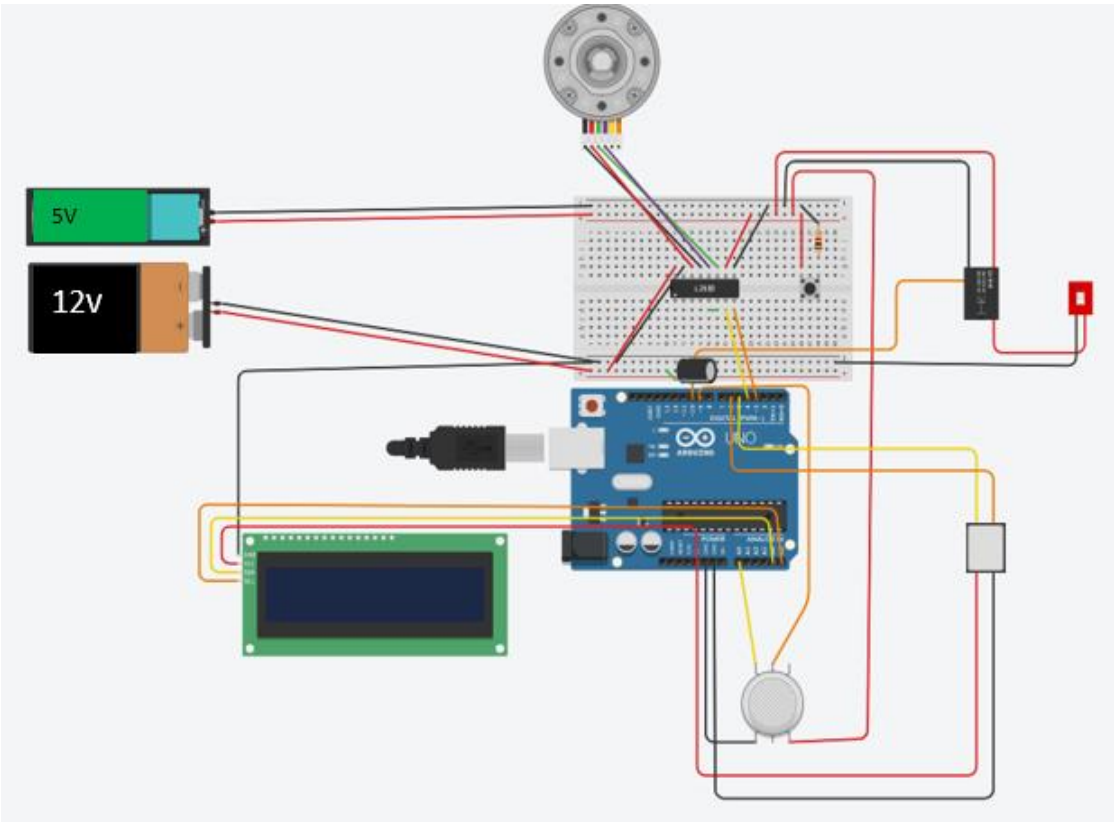

***Figure 3**. Circuit diagram*

The circuit is powered by a multiple power source, which has 3.3v, 5v and 12v outputs. The top line of the breadboard will be powered by 5v and the bottom line by 12v. A 100 µF, 25v capacitor is also found on the 12v line.

The button that triggers the door to open is connected to pin 8 of the Arduino expansion board and 5v to the breadboard.

The CO sensor is connected to the 5v power supply on the breadboard, while pin A0 is connected to pin A0 on the Arduino expansion board and pin D0 is connected to pin 9 of the expansion board.

The fingerprint sensor is connected as follows: V+ to 3.3v on the Arduino board, GND to GND on the Arduino board, TX to pin 5 of the board and RX to pin 6 of the board.

The LCD is connected to the Arduino development board via the I2C adapter, as follows: VCC to 5v on the board, GND to GND board, SDA to pin A4 and SCL to pin A5 on the Arduino board.

The 5v relay is connected as follows: VCC to 5v on the Arduino board, GND to GND on the board, IN to pin 10 on the Arduino board, COM to 12v on the breadboard, and NO to the PLUS of the lock.

The lock is connected to the minus of the breadboard, while the plus is connected to the NO of the 5v relay.

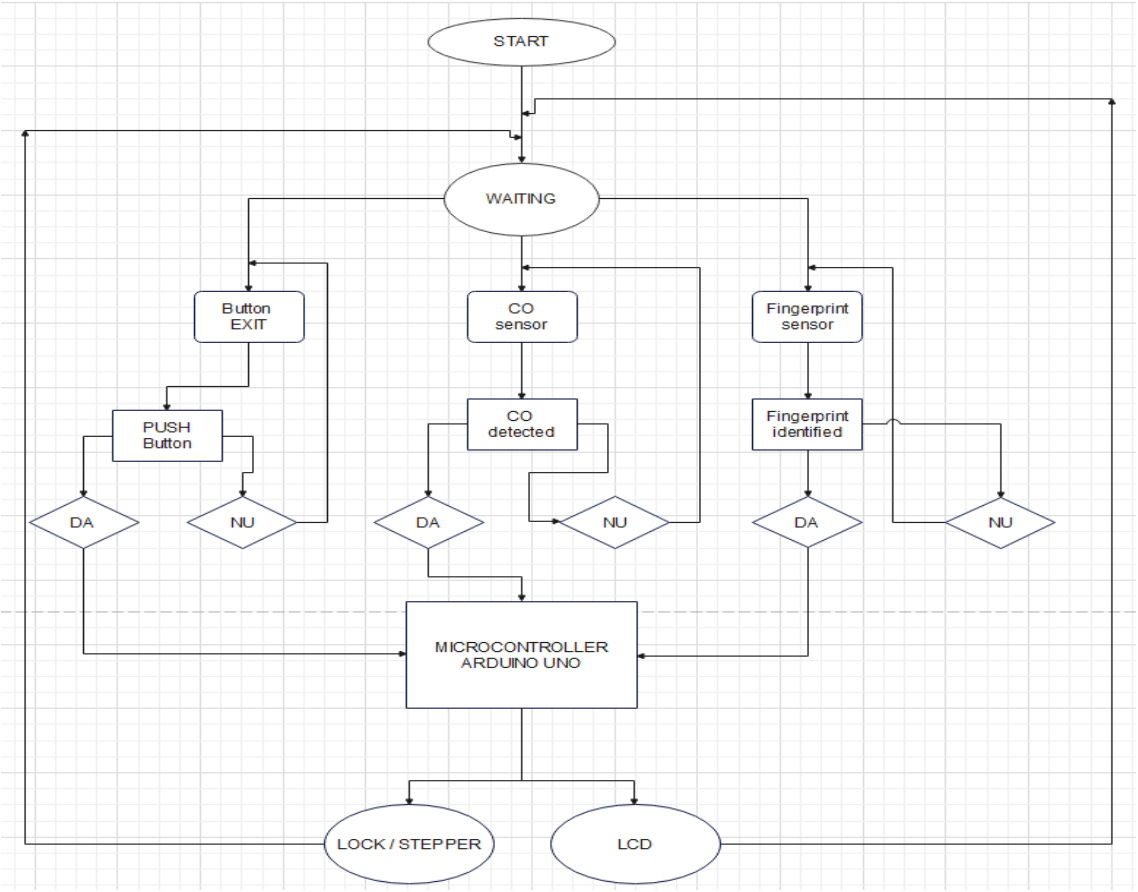

***Figure 4**. Logic diagram of the system*

The stepper motor is connected to the system via the A4988 driver, as follows: A+ (green) to B1 driver, B- (blue) to A1 driver, A- (black) to A2 driver, B+ (red) to B2 driver. In turn the driver is connected to the Arduino development board, DIR to pin 3 and STEP to pin 4. Sleep of the driver is connected to its Reset. The driver power supplies are connected like this: VDD to 5v on the breadboard, GND to GND on the breadboard, and VMOT to 12v on the breadboard and GND to GND on the breadboard.

When all the connections and wiring have been made, it's time to write the code. The logical scheme of the programme operation system is presented in Figure 4.

EXPERIMENTAL RESULTS

In order to validate the correct operation of the created system, a set of 50 tests was performed, using a fingerprint previously registered and stored in the database. The sensor recognized the fingerprint in each of the 50 experiments. According to catalog data, the sensor has an accuracy of 99.9% and a failure rate of only 0.1%.

Thus, the precision obtained was 100%, but this precision is not a real one, since if more attempts had been made, errors would have appeared.

In Figure 4 you can see the result of a test in which the fingerprint is valid and the message "Fingerprint accepted" appears on the screen.

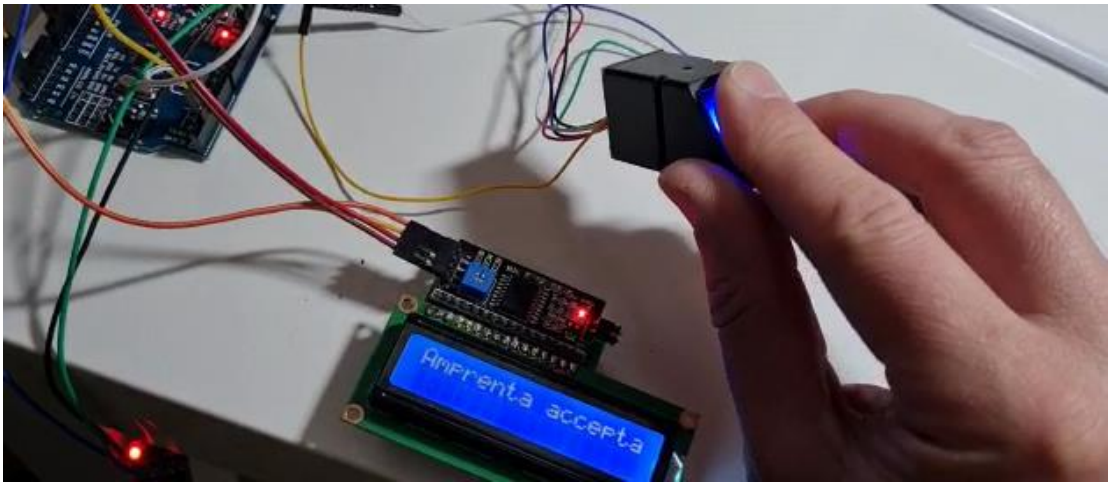

***Figure 4**. The fingerprint recognition message*

CONCLUSIONS

Through this project, it was desired to design and implement a fingerprint-based access system, used to secure a door, more precisely to lock and unlock it with the fingerprint.

This intelligent security system can be used in many fields, among which we mention its applicability in the military field, facilitating access to safes and local security rooms. At the same time, this security system can be used in large companies to verify the presence of employees at work by scanning their fingerprints upon entering the company. Also, the fingerprint-based security system is used for access to homes and to secure access to

gadgets such as a laptop, tablet or phone. And last but not least, the industrial sphere should be mentioned, especially if the premises are located in areas with potentially explosive gas emissions: refineries, gas exploitations, marine platforms.

As a future trend, verification (authentication) applications must ensure a reasonable compromise between the two major types of errors (acceptance rate and false rejection rate respectively), so as to minimize the probability of access to protected resources/spaces by some unauthorized persons without excessively disturbing the authorized users. The concrete choice of limit values for these errors depends directly on the considered application and the related restrictions, because, in reality, there will always be "doorways" that can be used in fraud attempts.

REFERENCES

[1] Bucur G., Sisteme inteligente de masurare – structuri de baza si aplicatii, Editura UPG Ploiesti, 2018; https://drive.google.com/file/d/1kkhIiewvTiBm4hCfeWv2FX4MVK10-5vm/view

[2] Dinca A., Craciun A., Sistem inteligent de acces, Proiect la disciplina Măsurări și Traductoare, anul III, AIA IFR, coordonator conf. G. Bucur, UPG Ploiești, 2022

[3] Pricop E., Summary of the doctoral thesis – Research on the security of automatic systems, https://doctorat.upg-ploiesti.ro/images/Doctorat/Anunturi_doctorat/2017/PE/Rezumatul_tezei_de_doctorat.pdf

[4] Jain, A.K., Ross A.A., Nandakumar K., Introduction to Biometrics, Ed. Springer, 2011, https://link.springer.com/book/10.1007/978-0-387-77326-1

[5] Maltoni D., Maio D., Jain A.K., Prabhakar S., Handbook of Fingerprint Recognition, 2nd edition, Ed. Springer, 2009, https://nguyenthihanh.files.wordpress.com/2015/08/handbook-of-fingerprint-recognition.pdf

[6] https://learn.adafruit.com/adafruit-optical-fingerprint-sensor

[7] https://www.sciencedirect.com/science/article/abs/pii/B9780323983709000093

[8] https://www.dreamstime.com/stock-photography-finger-print-image4921282

Received: April 2023; Revised: June 2023; Accepted: July 2023; Published: July 2023