DESIGNING AN ARDUINO-BASED SMART FINGERPRINT AUTHENTICATION MECHATRONIC MODEL

Ergashev Odiljon Alijon o‘g‘li
Intern teacher of the department "Automation of machine building production" of the Andijan State Technical Institute
Email:ergashevodiljon944@gmail.com
Inomjonov Umar Inomjon o’g’li
Andijan State Technical Institute,
"Automation of Machine Building Production" Department, "Mechatronics and Robotics" 4th ear student
e-mail: bookmedia75@gmail.com

Annotation. This article explores the development of an Arduino-based smart fingerprint authentication mechatronic model for secure access control. The study highlights the integration of biometric technology with mechatronic modules to enhance security and automation. The proposed system utilizes fingerprint recognition, microcontrollers, and IoT-based connectivity to ensure efficient and reliable authentication. Experimental results demonstrate that the system significantly improves access control efficiency, reduces unauthorized access risks, and enhances operational reliability. The findings emphasize the high potential of mechatronic and biometric technologies in various security applications, suggesting future adaptability in different sectors, including smart homes, industrial security, and financial institutions.

In Uzbekistan, modernization of industrial processes and implementation of high-precision measurement methods align with the Presidential Action Strategy for 2017–2021. This project provides practical recommendations for integrating innovative technologies into local industries. The research holds significant value in the development of intelligent systems for high-precision sorting based on robotic manipulators

Keywords: Smart authentication, fingerprint recognition, mechatronics, Arduino, IoT security, biometric access control, automation, secure identification systems.

Аннотация. В данной статье рассматривается разработка мехатронной модели умной аутентификации по отпечатку пальца на базе Arduino для безопасного контроля доступа. Исследование подчеркивает интеграцию биометрических технологий с мехатронными модулями для повышения уровня безопасности и автоматизации. Предлагаемая система использует распознавание отпечатков пальцев, микроконтроллеры и IoT-подключение для обеспечения эффективной и надежной аутентификации. Экспериментальные результаты показывают, что система значительно

ISSN 3030-3907

повышает эффективность контроля доступа, снижает риски несанкционированного проникновения и улучшает надежность работы. Выводы исследования подчеркивают высокий потенциал мехатронных и биометрических технологий в различных сферах безопасности, предполагая их будущую адаптацию в таких областях, как умные дома, промышленная безопасность и финансовые учреждения.

В Узбекистане модернизация производственных процессов и внедрение методов высокоточного измерения соответствуют Стратегии действий Президента на 2017–2021 годы. В рамках данного проекта даны практические рекомендации по интеграции инновационных технологий в локальную промышленность. Исследование имеет важное значение для разработки интеллектуальных систем с высокой точностью сортировки на основе роботизированных манипуляторов.

Ключевые слова: Умная аутентификация, распознавание отпечатков пальцев, мехатроника, Arduino, безопасность IoT, биометрический контроль доступа, автоматизация, системы безопасной идентификации.

Anotatsiya. Ushbu maqolada Arduino asosida aqlli barmoq izi autentifikatsiyasi uchun mexatronik modelni ishlab chiqish masalasi ko‘rib chiqiladi. Tadqiqotda xavfsizlik va avtomatlashtirishni oshirish uchun biometrik texnologiyalar va mexatronik modullarning integratsiyasi ta’kidlangan. Taklif etilgan tizim barmoq izi identifikatsiyasi, mikrokontrollerlar va IoT orqali bog‘lanishni qo‘llab-quvvatlab, samarali va ishonchli autentifikatsiyani ta’minlaydi. Eksperimental natijalar shuni ko‘rsatdiki, tizim kirishni boshqarish samaradorligini sezilarli darajada oshiradi, ruxsatsiz kirish xavfini kamaytiradi va tizimning ishonchliligini yaxshilaydi. Tadqiqot natijalari shuni ko‘rsatadiki, mexatronika va biometrik texnologiyalarning xavfsizlik sohasidagi yuqori samaradorligi kelajakda aqlli uylar, sanoat xavfsizligi va moliyaviy institutlarda qo‘llanishi mumkin.

O‘zbekistonda ishlab chiqarish jarayonlarini modernizatsiya qilish va yuqori aniqlikdagi o‘lchov usullarini qo‘llash bo‘yicha Prezidentning 2017-2021 yillarga mo‘ljallangan Harakatlar strategiyasiga muvofiq, mazkur loyihada innovatsion texnologiyalarning mahalliy sanoatga tatbiq etilishi bo‘yicha amaliy tavsiyalar berilgan. Bu tadqiqot robot manipulyatorlar asosida yuqori aniqlikdagi aqlli tizimlarni ishlab chiqishda muhim ahamiyatga ega.

Kalit so‘zlar: Aqlli autentifikatsiya, barmoq izi identifikatsiyasi, mexatronika, Arduino, IoT xavfsizligi, biometrik kirish nazorati, avtomatlashtirish, xavfsiz identifikatsiya tizimlari.

Introduction

ISSN 3030-3907

Security has always been a concern of paramount importance to human beings. When it comes to security, it is one of the most pressing problems in today's hectic, competitive environment, where a human being is unable to offer protection for his possessions daily. Keeping our staff safe has always been at the top of our priority list. Today's security includes a wide range of software and hardware, such as web-based security services, biometrics, and personal gadgets with built-in security levels[1].

A traditional lock with a key was the favored locking mechanism. This is an old-fashioned locking mechanism with a few flaws, such as the key being easily copied and the lock being easily opened by an unauthorized person. Several approaches have been reported in the literature for security solutions, such as a radio-frequency identification (RFID) card, keypad, pin, password, or Internet of Things (IoT) by unlocking the device with a mobile phone. These systems have the same advantages and disadvantages, and this form of security lock may open the system from any security level. To unlock the system, the user either enters a Personal Identification Number (PIN) or swipes an RFID card[2].

This system lacks a security level chain, which would improve security. An RFID card, which stands for radio frequency identification, can be used to unlock the system. The scanner scans the radio frequency to determine if the identity is allowed or unauthorized. However, the primary drawback of this approach is that the passwords could be hacked, and a card may be stolen or lost. As a result, the user must handle it with caution. Besides, this system also has no alert system in case of a break-in, or an unauthorized person trying to unlock the door.

IoT is an abbreviation for the Internet of Things, which is used in door locks through a wireless connection. The user can utilize IoT-enabled applications on his smartphone to unlock the door lock. With a single touch, the user may simply open or lock the system. However, IoT is supported only by an internet connection. The most striking problem for those models operating with smartphones is the risk of being unable to open the door if the smartphone's battery runs out. Unfortunately, the autonomy of these gadgets is limited, and whenever the user is unable to charge their smartphone, they will face the risk of being unable to open the door[3].

Biometrics provides a natural and dependable approach to some elements of identity management by employing fully automated or semi-automated systems to recognize persons based on biological features. It is possible to create an identity based on who you are rather than what you own, such as an identification (ID) card, or what you know, such as passwords, by utilizing biometrics. Biometrics may be used to augment ID cards and passwords in some applications, adding an extra

ISSN 3030-3907

layer of protection. This type of setup is sometimes referred to as a dual-factor authentication method[4].

Therefore, an Arduino-Based Smart Fingerprint Authentication System for Key Security Locker was proposed and developed in this research. The proposed method is more efficient because biometric identifiers cannot be readily misplaced, faked, or shared, making them more trustworthy for person recognition than traditional token-based techniques (e.g., keys or ID cards) or knowledge-based techniques (e.g., passwords or PINs).

Fingerprint technology is the most generally recognized and established biometric approach. It is the most user-friendly and provides a higher level of protection. Fingerprint recognition improves security, increases efficiency, and enhances user convenience. Furthermore, fingerprint recognition is the most commonly used biometric feature. It is often assumed that each finger has a distinct pattern. Given that there are around 6.5 billion people in the world and assuming that each person has ten fingers, there are 65 billion distinct fingerprints!

Fingerprints were originally used as a form of identification over a century ago. Fingerprint recognition is one of the most secure systems because each person has a unique fingerprint pattern. Unauthorized access can be restricted by creating a lock that saves the fingerprints of one or more authorized users and opens the system when a match is detected.

The Arduino serves as a data storage device for users. The skin on our hands and soles has a flow-like pattern of ridges on each fingertip that is unique and unchangeable, making biometric authorization one of the most reliable security methods. As a result, fingerprints are a one-of-a-kind form of identification for everyone[5].

The usage of fingerprint scanners in modern hand-held devices such as mobile phones and computers demonstrates their popularity and dependability.

Method

ISSN 3030-3907

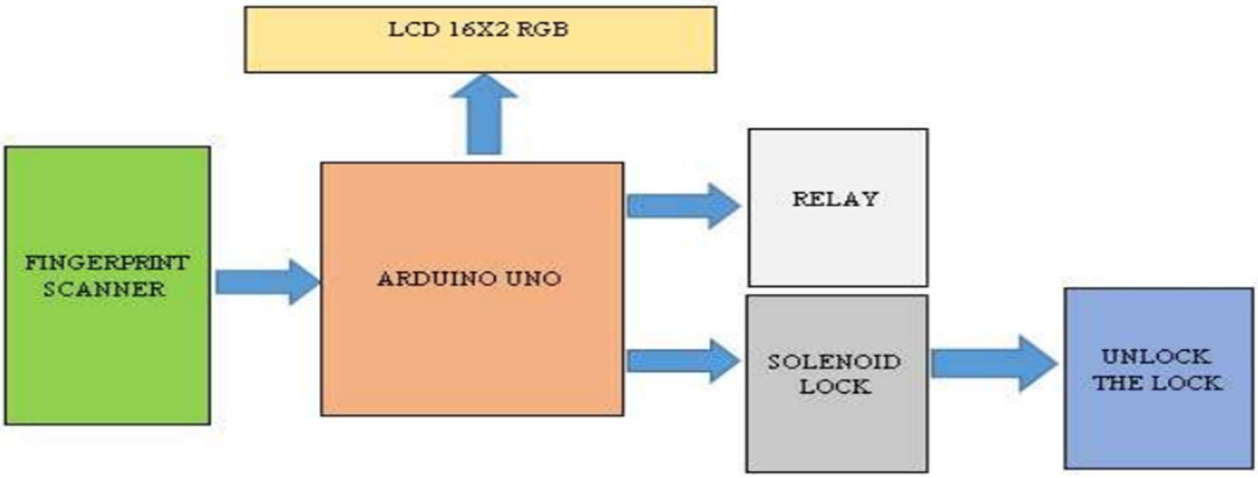


Fig. 1. Block diagram

The block diagram of an Arduino-based Smart Fingerprint Authentication System for Key Security Locker is shown in Fig. 1. To use the fingerprint scanner, the user must place their finger on it. The fingerprint scanner captures the fingerprint image and sends it to the Arduino Uno. The Arduino Uno then searches for the original fingerprint data already saved on the board. If the fingerprint matches one previously saved in Arduino, the Liquid-Crystal Display (LCD) will display "Fingerprint Match." The microcontroller will then instruct the relay and solenoid lock to open the locker door. If the fingerprint does not match, the LCD will display "Not Matching," and the locker door will remain locked[6].

The Arduino is an open-source physical computing platform based on a single microcontroller board. It is used when there are interactions between inputs and outputs. The Arduino has 14 digital Input/Output (I/O) pins, six of which can be used as pulse width modulation (PWM) outputs, six analog inputs, a reset button, a power connector, a USB connection, and other features. It includes everything needed to support the microcontroller; simply connect it to a personal computer (PC) through a USB cable and power it up using an AC-to-DC adapter or battery. It is used to control outputs based on input directives, such as using a switch to control a light or motor[7].

The optical finger reader sensor, commonly known as a fingerprint reader, is a technological device that captures a digital image of the fingerprint pattern. The captured image is known as a live scan, which is then digitally processed. The distinctive features of the fingerprint are extracted, and a fingerprint biometric template is created. This biometric template is saved and will be used for matching in the future.

The relay is an electrically operated switch consisting of two main parts: an electromagnetic coil and a mechanical set of switches. The electromagnet requires

ISSN 3030-3907

a low voltage to activate, which is supplied by the Arduino. Once triggered, the electromagnet pulls the contact to complete the high voltage circuit.

Solenoids are electromagnets made from a large copper wire coil with an armature in the middle. The slug is drawn into the center of the coil when it is charged. This allows the solenoid to pull from only one end.

An LCD is an electrical display module that uses liquid crystals to create a visible image. The main advantages of using this module are its low cost, ease of programming, ability to display animations, and the fact that there are no restrictions on displaying unique characters, special animations, etc.

Experimental Setup

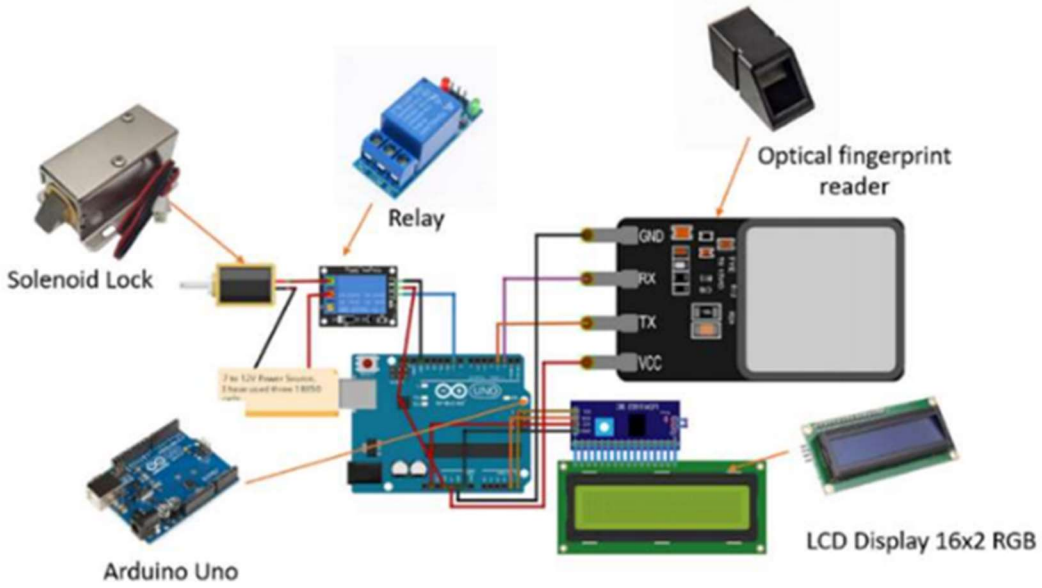
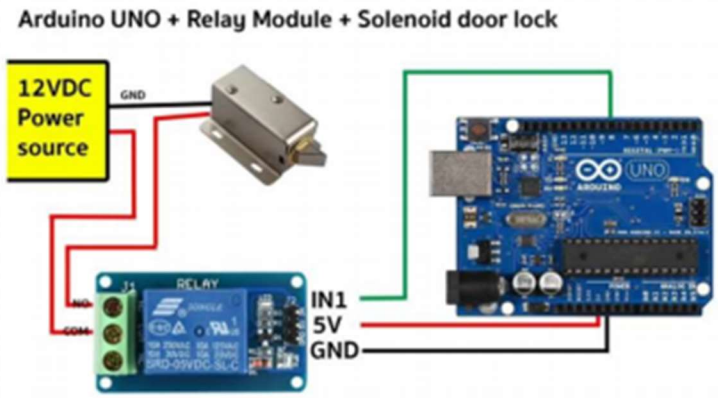


Fig. 2. Experimental setup for the proposed system

Fig.2 presents the experimental setup for an Arduino-Based Smart Fingerprint Authentication System for Key Security Locker. Based on Fig. 4, the optical fingerprint scanner serves as an input and is connected to the Arduino board. Pin 2 is assigned to the transmitter (Tx), while Pin 3 is assigned to the receiver (Rx). The Arduino Uno supplies 5V power to the fingerprint reader.



ISSN 3030-3907

Fig. 3. The connection between an Arduino with a relay module, and a solenoid lock

Fig. 3 illustrates the connection between the Arduino board, the relay module, and the solenoid lock. The relay module acts as an on/off switch. IN1 is connected to pin 9, and 5V power is supplied to the relay module from the Arduino board. Additionally, the Normally Open (NO) terminal is connected to the solenoid lock's anode. The negative terminal of the solenoid lock and the Common (COM) pin are both connected to a 12V power source[8].

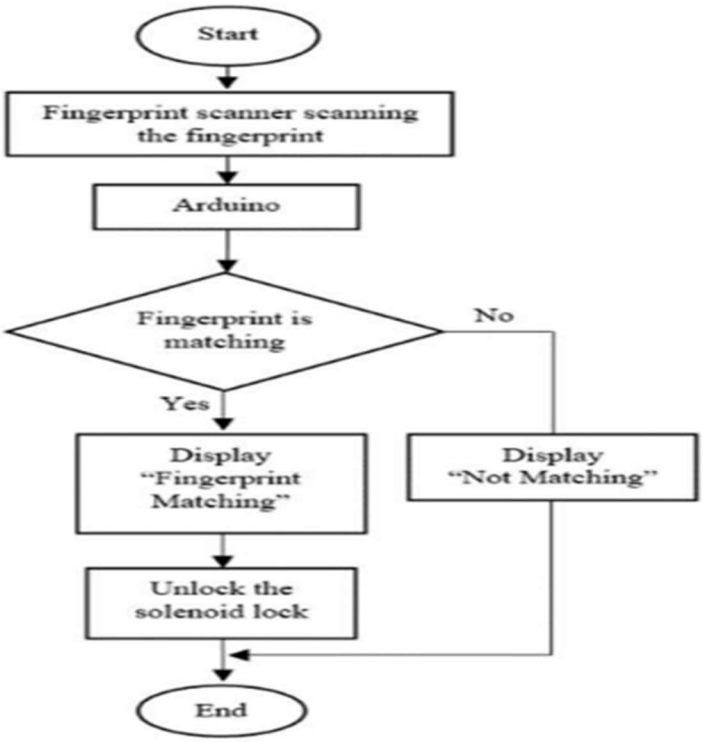


Fig. 4. Flow chart of the proposed system

Fig. 4 depicts the flowchart for the proposed system. When the user places a finger on the scanner, the fingerprint sensor illuminates the surface of the finger and records the minutiae using a charge-coupled device (CCD) with an 8-bit per dot resolution of 500 dpi (dots per inch) in grayscale. The collected data is converted into a digital signal and saved in a local database. Every time a fingerprint is scanned, a new minutia is captured. This new fingerprint data is then compared with the stored database to determine whether the individual is authorized or not[9].

ISSN 3030-3907

Software Arduino (IDE).

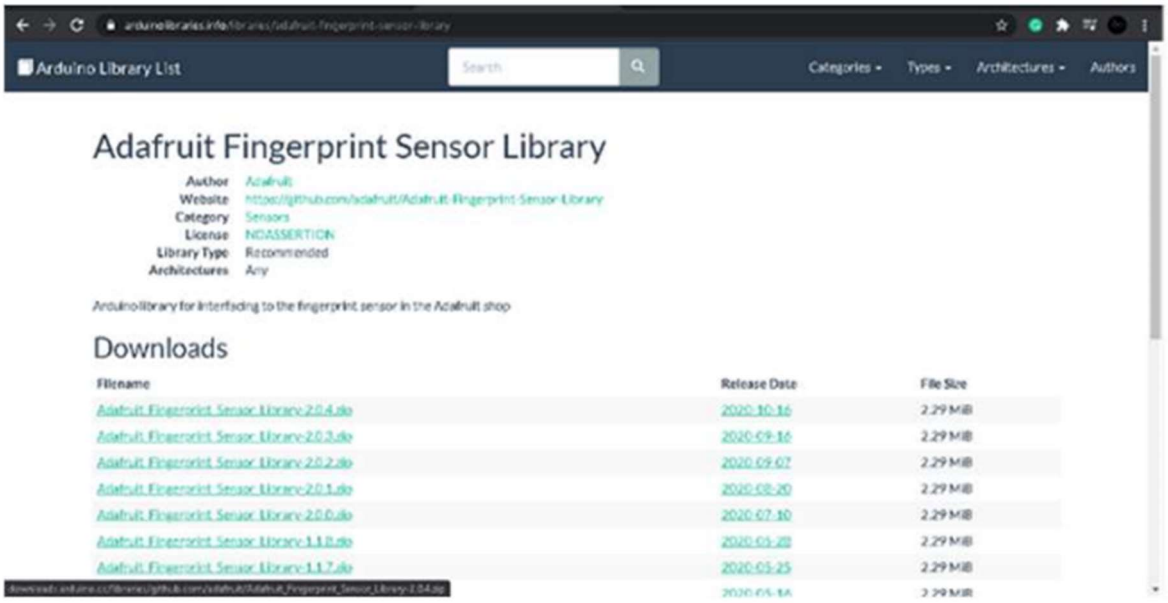


Fig. 5. Adafruit fingerprint library in Google.

The Arduino Adafruit fingerprint library can be downloaded from the Google website, as shown in Fig.5. After downloading the library, it should be copied and pasted into the Arduino library folder. Fig. 6 illustrates the coding for Adafruit_Fingerprint.h, while Fig. 7 presents the coding for the proposed system in the Arduino software.

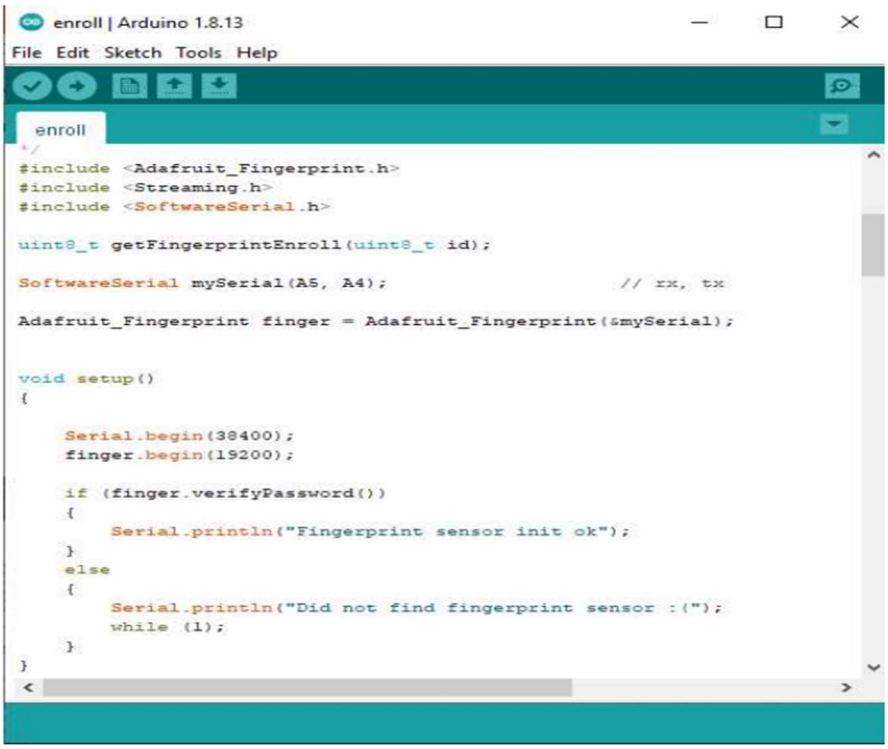


Fig. 6. Coding for Adafruit_Fingerprint.h

ISSN 3030-3907

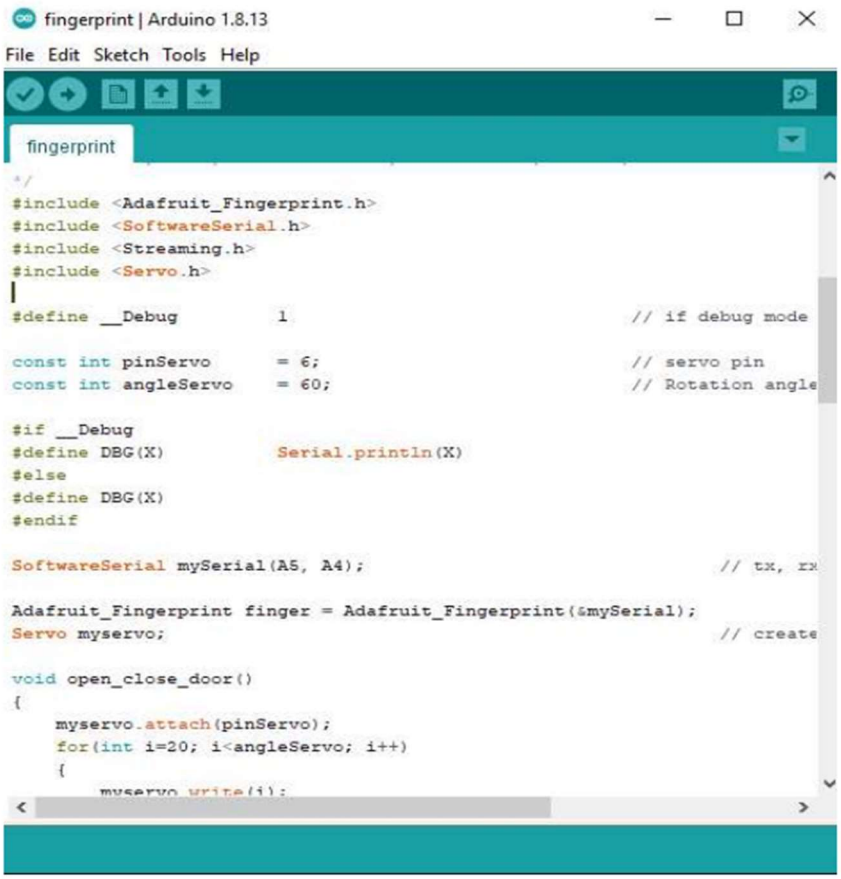


Fig. 7. Coding for Fingerprint

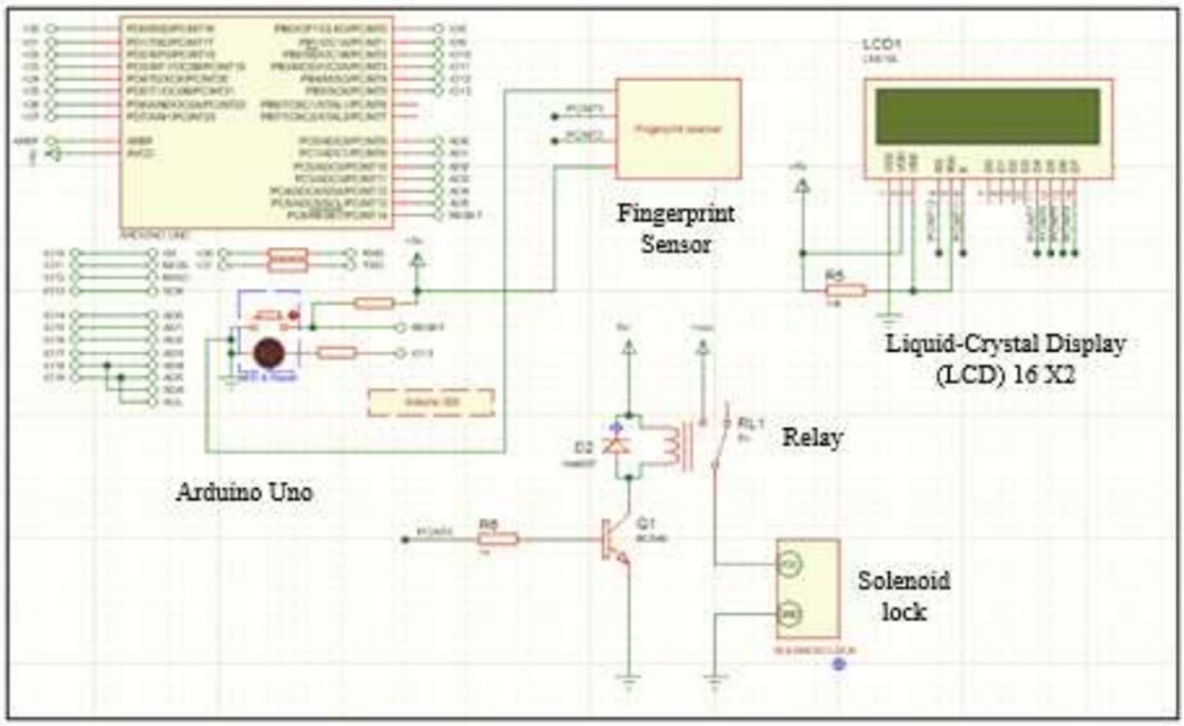


Fig. 8. Schematic design.

The schematic diagram for an Arduino-based Smart Fingerprint Authentication System for Key Security Locker is shown in Fig. 8. The input voltage for the Arduino Uno is 5V, while the solenoid electric lock requires 12V.

ISSN 3030-3907

The Arduino Uno microcontroller (MCU) board serves as the brain of the circuit. It features 14 digital I/O pins, six analog inputs, 32k flash memory, a 16MHz crystal oscillator, a USB connection, a power connector, an In-Circuit Serial Programming (ICSP) header, and a reset button. The board can be programmed using the Arduino Integrated Development Environment (IDE) software[10].

The fingerprint sensor, an optical fingerprint scanner, acts as an input device. Users can store fingerprint data in the module and configure it for 1:1 or 1:N identification mode. The sensor's Tx and Rx pins are connected to the Arduino's digital pins 2 and 3 for serial communication. The LCD is used to display output messages.

A 5V relay (RL1) is required to control the lock. The Normally Open (N/O) contacts of RL1 are connected to Ground through connector CON3 (GND). Connector CON3 links to the electronic door-lock solenoid. The solenoid is an electromagnet consisting of a large copper wire coil and an armature at its center. When the coil is electrified, the slug is drawn into the center, allowing the solenoid to move to one end[11].

Conclusion

An Arduino-based Smart Fingerprint Authentication System for Key Security Lockers has been developed, providing enhanced security, efficiency, and user convenience. This innovative system allows keys to be stored in a more organized and secure manner. Only authorized users can unlock the key security locker to access the keys inside.

By utilizing biometric technologies such as fingerprint scanning, authentication becomes more secure and convenient. The adoption of biometric technology is expected to grow in the future, expanding into more sectors that impact daily life.

References

1. Odiljon, E., Muhammaddiyor, O. va Ahmadali, U., 2024. Cnc moshinalarda sezish element va elektr diskning sinxron ishlatini loyihalash. *Fan, jamiyat va innovatsiyalar* , *1* (10), 30-35-betlar.

2. Odiljon, E. va Ahmadali, M., 2024. Akilli piyodalar kechasini loyihalash. *Fan, jamiyat va innovatsiyalar* , *1* (10), 66-69-betlar.

3. Odiljon, E., 2024. Sut maxsulotlari ishlab chiqarish zavodlarida ultrtovushli dizinfeksiyalash tizimini loyihalsh. *Fan, jamiyat va innovatsiyalar* , *1* (9), 24-28-betlar.

ISSN 3030-3907

4.H. Hassan, R. A. Bakar, and A. T. F. Mokhtar, “Face recognition based on auto-switching magnetic door lock system using microcontroller,” in 2012 International Conference on System Engineering and Technology (ICSET), IEEE, 2012.
5.Y. T. Park, P. Sthapit, and J.-Y. Pyun, “Smart digital door lock for the home automation,” in TENCON 2009-2009 IEEE Region 10 Conference, IEEE, 2009.
6.Keriya, F.R.B., “Development of IoT–based locking system,” B.S. dissestation, Dept. Faculty of Electrical and Electronic Engineering (UTHM), Johor, Malaysia 2019.
7.Z. Mumtaz, Z. Ilyas, A. Sohaib, S. Ullah, and H. A. Madni, “Design and implementation of user-friendly and low-cost multiple-application system for smart city using microcontrollers,” arXiv preprint arXiv:2010.07016, 2020.
8.Y. Motwani, S. Seth, D. Dixit, A. Bagubali, and R. Rajesh, “Multifactor door locking systems: A review,” Materials Today: Proceedings, 2021.
9.S. Goyal, P. Desai, and V. Swaminathan, “Multi-level security embedded with surveillance system,” IEEE Sensors Journal, vol. 17, no.22, pp. 7497-7501, 2017.
10.S. Hossain, M. I. Ahmed, and M. N. Mostakim, “A prototype of automated vault locker solution for industrial application,” in 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), IEEE, pp. 1-7, 2019. E-ISSN : 2798 – 4664 160
11.A. M. A. Bakry, and D. R. Rajaa, “Smart phone-Arduino based of smart door lock/unlock using RC4 stream cipher implemented in smart home,”International Journal of Advanced Computer Technology, vol. 5, no. 5, pp. 14-18, 2016.
12.G. K. Verma, and P. Tripathi, “A digital security system with door lock system using RFID technology,” International Journal of Computer Applications, vol. 5, no. 11, pp. 6-8, 2010.
13.N. Meenakshi, M. Monish, KJ. Dikshit, and S. Bharath, “Arduino based smart fingerprint authentication system,” in 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), IEEE, pp. 1-7, 2019.

ISSN 3030-3907