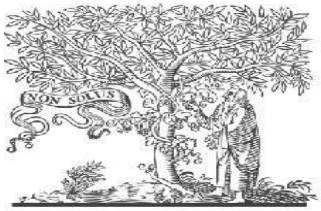
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

2023 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 1st Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/01

Title **Fingerprint Laser Security Alarm**

Volume 12, ISSUE 08, Pages: 1-5

Paper Authors **Madhu Kumar Vanteru, G.Jithin , K.Leela , G.Anjali , T.Bharath , B.Nagasai Balaramasetty**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Fingerprint Laser Security Alarm

Madhu Kumar Vanteru[1] , G.Jithin[2] , K.Leela[3] , G.Anjali[4] , T.Bharath[5] , B.Nagasai Balaramasetty[6]
[1]Assistant Professor, Dept. of Electronics & Communication Engineering, Balaji Institute of Technology and Science, Warangal, Telangana, India
[2,3,4,5,6]UG Student, Dept. of Electronics & Communication Engineering, Balaji Institute of Technology and Science, Warangal, Telangana, India

Abstract—This project focuses on developing a design model for an alarm system based on fingerprint laser security. Installation and accessibility of fingerprint laser security alarms are challenging, limited only to the ultra-wealthy. The objective of this undertaking is to create a security system utilizing lasers, a fingerprint sensor, and an LDR (Light Dependent Resistor). Why Opt for Lasers? Laser beams possess the remarkable capability to travel considerable distances without dispersing, making them suitable for integration into security systems. In this analysis, we examine the light source using the LDR sensor. Our project additionally employs a fingerprint scanner to grant access to registered users. By utilizing these components, we design a security system incorporating fingerprint recognition and laser technology. A laser diode emits a continuous laser beam that consistently impinges upon the LDR sensor. When an unauthorized individual crosses its path, the laser is obstructed from reaching the LDR, causing the sensor to produce a low value. The controller detects this value, activating the buzzer and transmitting an alert to the user. Upon successful authentication of an authorized person's fingerprint**,** the laser deactivates, and the lock opens temporarily for a few seconds to allow for resumed operation.

Keywords—Fingerprint sensor, LDR, Laser, Buzzer

I. INTRODUCTION

The requirement for security is an innate necessity for every individual. Ensuring our safety and the tranquility of our surroundings is vital for living in harmony. However, in this era of uncertainty, when crime, terrorism, and threats reach their peak, attaining peace of mind becomes challenging. This is precisely where laser security systems come into play, providing an increasingly sought-after solution that helps people safeguard themselves. This is why you are considering its installation. Various electronic security systems can be employed in homes and other critical workplaces to fulfill security objectives.

A fingerprint laser security alarm serves as a valuable device for ensuring security. It possesses a broad range of applications in the realms of security and defense, encompassing both everyday household items and highly valuable organizational assets. In the past, it used to be an expensive resolution for security needs. However, the declining costs and rapid technological advancements have rendered this type of security system increasingly affordable.

Laser technology differs from conventional light sources in significant ways, holding two key properties relevant to any security system. Unlike light bulbs and flashlights, laser light forms a narrow beam instead of dispersing. Moreover, laser light is predominantly monochromatic. Due to its limited spread, laser light can be transmitted over long distances while retaining sufficient energy within a small area to trigger detectors in security systems. Additionally, its single wavelength nature allows the use of rejection filters on the detectors, permitting the passage of laser light while preventing background light from entering the detector.

Laser light follows a straight trajectory. For instance, to protect the front yard, positioning the laser in one corner and the detector in the opposite corner would suffice. Nonetheless, such a configuration is often impractical. Typically, a laser security system is implemented to secure the perimeter of a room or at least an extension of it. To achieve this, the system begins by directing a laser beam towards a small mirror. The first mirror is angled to redirect the beam to a second, smaller mirror, and this pattern continues until the final mirror guides the beam towards the detector. Any interruption of the beam between the laser and detector triggers a warning signal from the electronic components.

Fingerprint recognition stands as one of the most secure systems due to the uniqueness of each individual's fingerprint. Unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users, granting access only upon finding a match. The authentication of biometric data has demonstrated its excellence, as the grooves on our fingertips form a distinct and consistent pattern. This distinctiveness makes fingerprints an unparalleled identifier for each person. The popularity and reliability of fingerprint scanners can be easily observed through their integration into modern portable devices like mobile phones and laptops.

II. PROBLEM STATEMENT

Now, with crime rates on the rise, security can be considered one of the most important things. There are many different types of security systems that most people use today. Closed-circuit television (CCTV), alarms, etc., are visible to the naked eye and warn intruders to circumvent or disable these security systems.

III. EXISTING SYSTEM

This study conducted an analysis of the current locking systems employed in homes and offices. While initially useful, these methods have been discovered to become outdated over time, posing significant security

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

risks. Additionally, it has been confirmed that these systems are highly costly. Below, we will explore the advantages and disadvantages of the existing systems.

A. Deadbolt system

This system followed a security protocol of "one key for one lock." While satisfactory initially, it was proven incorrect when it was found that one lock could easily be opened by multiple keys. Consequently, this system is now considered vulnerable and obsolete.

B. Password authentication

In this system, passwords of authorized users are stored for verification purposes, ensuring a substantial level of security. The power consumption was efficient, and the usage is user-friendly. Anyhow, unauthorized users can easily acquire passwords through various means such as hacking or guessing.

C. RFID reader authentication

Radio Frequency Identification (RFID) is a cost-effective technology that facilitates wireless data transmission. With RFID, wireless automatic identification becomes possible, whereby an object, place, or person is marked with a unique identification code stored in an RFID tag attached to or embedded in the target. This system offers several advantages as the data on the RFID card can only be read by specialized equipment, ensuring the safety of the recorded information. However, RFID systems can be easily cloned, and the cards can be misused.

D. Face detector lock

These systems encounter difficulties in recognizing faces from images captured under different lighting conditions or from distinct angles. It remains questionable whether facial recognition alone is sufficient for accurately identifying a person among numerous identities, particularly in the absence of contextual information.

E. Retinal scanner

The retinal vasculature is believed to possess distinct and individual characteristics for each person and eye. Image acquisition requires the subject to focus on a specific point within the field of view, enabling the imaging of a particular portion of the retinal vasculature. Although this device is commonly employed for security purposes and exhibits low false positive and rejection rates, it is not user-friendly and comes with a significant equipment cost.

F. Iris scanner

Iris authentication involves extracting unique characteristics from the iris of the human eye. Each individual has a distinct iris pattern, even among identical twins, and variations can exist between the right and left eyes of the same person. The advantage of using an iris scanner lies in its high accuracy, although changes in lighting conditions can affect its performance. However, one limitation of iris recognition technology is that scanners tend to be expensive and require ample memory for data storage.

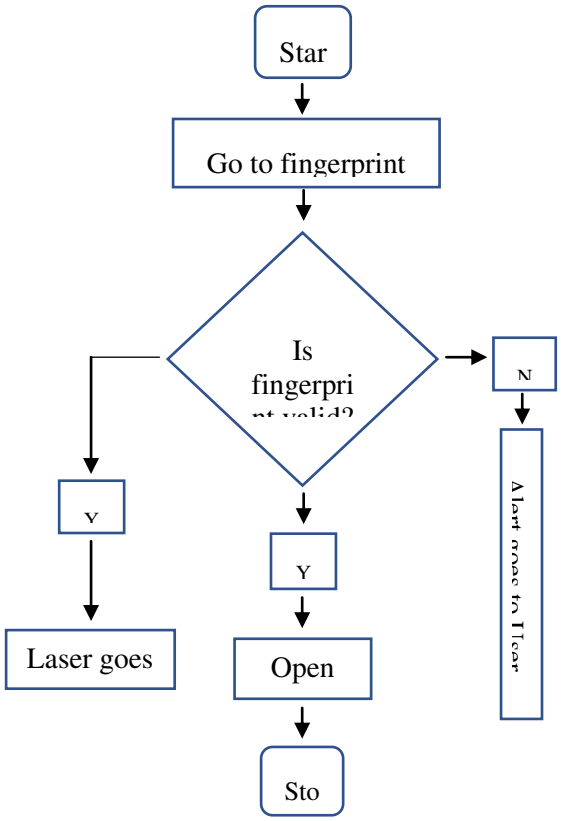
G. Voice recognition

Speech or speaker recognition refers to the identification of individuals based on their vocal characteristics through biometric authentication technology. Acoustic features of the voice differ from person to person and encompass both anatomical factors (such as throat and mouth size and shape) and learned behavioural patterns (such as pitch and speaking style). A drawback of speech-based recognition is its susceptibility to factors like background noise, which can affect the accuracy of the system.

IV. PROPOSED SYSTEM

Our proposed system effectively addresses all security concerns associated with existing systems, delivering both high security and efficiency. It presents the ideal solution for safeguarding against the inconvenience of stolen or lost keys and unauthorized entry. Fingerprinting emerges as an excellent solution to these problems, offering a remarkable level of recognition accuracy. The surface of our palms and soles features a unique pattern of grooves known as friction ridges. Each finger possesses an individual and unchanging arrangement of these friction

Figure 1. Flowchart



bridges. Consequently, fingerprints serve as distinct identifiers for every individual. To ensure authentication, our system utilizes a fingerprint scanner to capture and

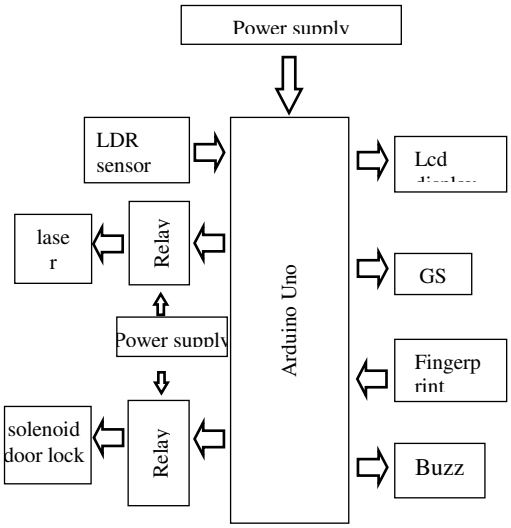
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

analyze a user's fingerprint. Fingerprint scanning proves to be a highly precise and cost-effective method, virtually impossible to duplicate. The fingerprint recognition system simplifies the process of authentication. During verification, the system compares the entered fingerprint with the enrolled fingerprints of a specific user, determining if they match the same finger's print.

V. WORKING OF PROPOSED MODEL

A. Flowchart

Figure 2. Block Diagram



B. Block Diagram

C. Working

Our project "Fingerprint Laser Security System" works by the usage of laser and fingerprint authentication technology to provide both security and accessibility respectively to the authorized users. The security system works by keep on transmitting a narrow beam of light through LASER in the air. The transmitted light travels in the air until it is blocked by a fixed object. The property of light is to get reflected when the trajectory of it gets blocked by an object. Hence, the beam of light on hitting the fixed object gets reflected. The reflected beam of light is allowed into the device consisting of a detector, the detector continuously keeps on measuring the light falling on it.

When any intruder comes in the path of the light beam, the path of light and the amount of the reflected light falling on the detector gets disturbed. When the detector detects it, it triggers a signal that activates the alarm unit to generate the alarm and an alert through GSM module. The alarm goas off with a loud sound to alert the security personnel of the premises and alerts the authorized users of the intrusion by sending an alert through GSM.

When an authorized person wants access, he can put his fingerprint in the fingerprint scanner and the security algorithm involved compares the fingerprint just scanned with the ones that are registered in the database for authentication. When the fingerprint is verified then the laser turns off for a few seconds and the door lock opens, giving access to the user.

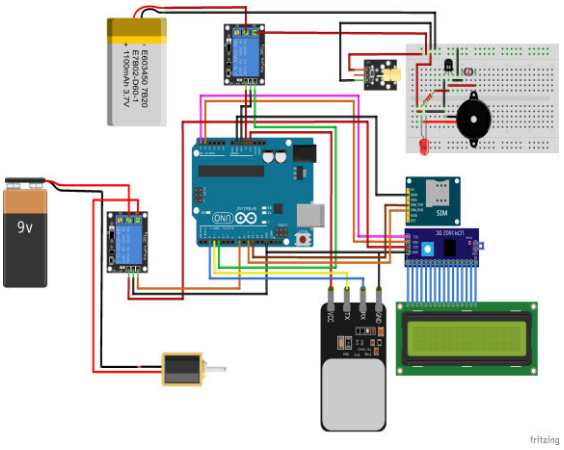


Figure 3. Circuit Diagram

VI. RESULT

The Fingerprint module is interfaced with the Arduino. The laser continuously incident light on the LDR. If anyone interrupt the laser beam then the LDR detects low light and it gives alert to the user through buzzer and also sends an SMS alert to the user. When the authorized user scans his fingerprint, the door opens for few minutes and at the same time the laser module goes off simultaneously. If an unauthorized user tries to enter an alert goes to the user.

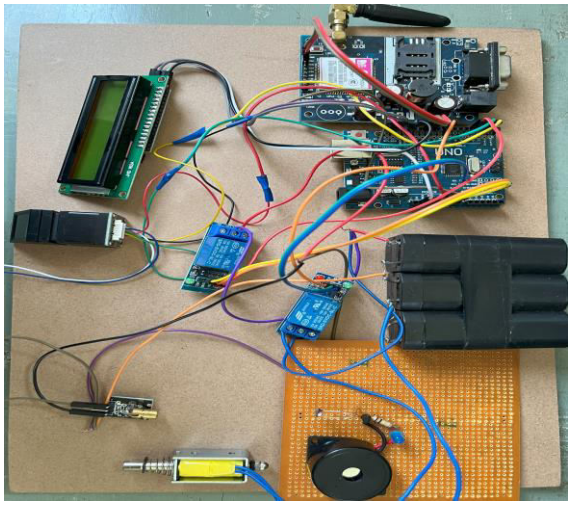


Figure 3. Result

VII. ADVANTAGES AND APPLICATIONS

A. Applications

- It can be used in safety lockers in our homes.
- It can be used in Office Security.
- It can be used in Banking and financial systems.
- It can be used in E-commerce/e-business security.

B. Advantages

- No password or PIN is remembered as it can only be opened if an authenticated user was present.
- More secure and accurate than traditional passwords.
- It is User-Friendly.
- Password-based security systems are always at risk of theft or access by unauthorized users, but here they can only be opened in the presence of an authorized user.

VIII. CONCLUSION

Based on the results of the developed biometric locker system, the program uploaded to the microcontroller successfully facilitated its operation. Components used in the system were compatible with the microcontroller unit. You have effectively performed the following functions:

1. Properly register, store, and scan the user's thumb and index finger prints.
2. Fix fingerprint and passcode recognition and recognition to open locker magnetic lock.
3. Correct establishment of the connection between the microcontroller unit and the GSM module. This allows you to send an auto-generated passcode text message to the user when an unrecognized fingerprint is recognized. The system accepted the autopasscode entered into the system

REFERENCES

[1] Subhash H. Jadhav, "Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391, Paper ID: ART20162571

[2] Omidiora E. O.(2011) "A Prototype of a Fingerprint Based Ignition Systems in Vehicles" Published in European Journal of Scientific Research ISSN 1450-216X Vol.62 No.2 (2011), pp. 164-171 EuroJournals Publishing, Inc. 2011

[3] Crystalynne D. Cortez, "Development of Microcontroller-Based Biometric Locker System with Short Message Service", Lecture Notes on Software Engineering, Vol. 4, No. 2, May 2016, DOI: 10.7763/LNSE.2016.V4.233

[4] Sagar S. Palsodkar, "Bank Lockers Security System using Biometric and GSM Technology", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – Volume 2 Issue 4–April 2015

[5] H. Dong, N. Giakoumidis, J. Juma, D. Tretyakov, & N. Mavridis, "A Fast Laser Motion Detection and Approaching Behavior Monitoring Method for Moving Object Alarm System (MOAS), Procedia Engineering," Volume 41, 2012, Pages 749- 756, ISSN 1877-7058, https://doi.org/10.1016/j.proeng.2012.07.23 9

[6] S. Singha, & D. Maji, "LASER SECURITY SYSTEM", International Journal of Scientific & Engineering Research, Volume 7, Issue 4, April-2016, ISSN 2229-5518.

[7] Mohammed, Ayad. (2015). Design and Construction of a Smart Security System by Laser Fence Technique. FONDAZIONE GIORGIO RONCHI. 6. 699-713.

[8] Meenakshi N, Dikshit KJ, Monish M, Bharath S. Arduino based totally smart Fingerprint Authentication device. In 2019 1st global convention on innovations in facts and communique technology (ICIICT) 2019 Apr 25 (pp. 17). IEEE.

[9] Moyashir R, Baidya J, Saha T, Palit R. layout and implementation of a fingerprint-primarily based key device for shared access. 2017 IEEE seventh Annual laptop and conversation conference and conference (CCWC) 2017 January 9 (pp. 1-6).IEEE.

[10] Gupta RP. Implementation of Biometric Security in Smartphone Based Domotics. 2018 International Conference on Computer Development, Communication and Network Management (CCWC) 2018 Oct 12 (pp. 80-85). IEEE

[11] Atar Nasrin, "Fingerprint Based Security System For Banks", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 – 0056 Volume: 03 Issue: 04 | Apr-2016

[12] Jordi Sapes, "FingerScanner: Embedding a Fingerprint Scanner in a Raspberry Pi", Sensors 2016, 16, 220; doi:10.3390/s16020220

[13] Kumar, V. & Ramana, T.. (2022). Fully scheduled decomposition channel estimation based MIMO-POMA structured LTE. International Journal of Communication Systems. 35. 10.1002/dac.4263.

[14] V. M. Kumar and T. V. Ramana, "Position-based Fully-Scheduled Precoder Channel Strategy for POMA Structured LTE Network," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-8, doi: 10.1109/ICECCT.2019.8869133.

[15] M. K. Vanteru, T. V. Ramana, A. C. Naik, C. Adupa, A. Battula and D. Prasad, "Modeling and Simulation of propagation models for selected LTE propagation scenarios," 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), Hyderabad, India, 2022. 10.1109/ICMACC54824.2022.10093514.

[16] Madhu Kumar Vanteru, K.A. Jayabalaji, Suja G. P, Poonguzhali Ilango, Bhaskar Nautiyal, A. Yasmine

Begum,Multi-Sensor Based healthcare monitoring system by LoWPAN-based architecture,Measurement: Sensors,Volume 28,2023,100826,ISSN 2665-9174.

[17] Dr.M.Supriya, Dr.R.Mohandas. (2022). Multi Constraint Multicasting Analysis with fault Tolerance Routing Mechanism. Telematique, 21(1), 3544-3554.

[18] N.Sivapriya, T.N.Ravi. (2019). Efficient Fuzzy based Multi-constraint Multicast Routing with Multi-criteria Enhanced Optimal Capacity-delay Trade off. International journal of Scientific & Technology Research, 8(8), 1468-1473.

[19] N.Sivapriya, T.N.Ravi. (2019). A framework for fuzzy-based Fault Tolerant Routing Mechanism with Capacity Delay Tradeoff in MANET. International Journal of advanced Science & Technology, 28(17), 420-429.

[20] P. Kiran Kumar, B.Balaji , K.Srinivasa Rao, Performance analysis of sub 10 nm regime source halo symmetric and asymmetric nanowire MOSFET with underlap engineering. Silicon 14, 10423–10436 (2022).

[21] K. K. Vaigandla, "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis," 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2022, pp. 27-31, doi: 10.1109/ICIPTM54933.2022.9753990.

[22] Karthik Kumar Vaigandla , Dr.J.Benita, "Study and Analysis of Various PAPR Minimization Methods," International Journal of Early Childhood Special Education (INT-JECS), Vol 14, Issue 03 2022, pp.1731-1740.

[23] P.Kiran Kumar, B.Balaji, K.Srinivasa Rao, Halo-Doped Hetero Dielectric Nanowire MOSFET Scaled to the Sub-10 nm Node. Transactions on Electrical and Electronic Materials (2023). https://doi.org/10.1007/s42341-023-00448-6

[24] Padakanti Kiran Kumar, Bukya Balaji, K.Srinivasa Rao, Design and analysis of asymmetrical low-k source side spacer halo doped nanowire metal oxide semiconductor field effect transistor, IJECE, Vol 13, No 3 DOI: http://doi.org/10.11591/ijece.v13i3.pp3519-3529.

[25] P. K. Kumar, K. Srikanth, N. K. Boddukuri, N. Suresh and B. V. Vani, "Lattice Heating Effects on Electric Field and Potential for a Silicon on Insulator (SOI) MOSFET for MIMO Applications," 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON), Rajpura, India, 2023, pp. 1-4, doi: 10.1109/DELCON57910.2023.10127385.

[26] P. K. Kumar, P. P. Rao and K. H. Kishore, "Optimal design of reversible parity preserving new Full adder / Full subtractor," 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 368-373, doi: 10.1109/ISCO.2017.7856019.

[27] V.Madhu Kumar,Dr.T.V.Ramana" Virtual Iterative Precoding Based LTE POMA Channel Estimation Technique in Dynamic Fading Environments" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6, April 2019

[28] V.Madhu Kumar,Dr.T.V.Ramana, Rajidi Sahithi" User Content Delivery Service for Efficient POMA based LTE Channel Spectrum Scheduling Algorithm" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S3, December 2019.

[29] P. K. Kumar, P. P. Rao and K. H. Kishore, "Optimal design of reversible parity preserving new Full adder / Full subtractor," 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 368-373, doi: 10.1109/ISCO.2017.7856019.

[30] V.Madhu Kumar,Dr.T.V.Ramana" Virtual Iterative Precoding Based LTE POMA Channel Estimation Technique in Dynamic Fading Environments" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6, April 2019