INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

An Intelligent Quad Level Digital Lock System for Safety Vaults

R Arthi[1], **D Manoj Kumar**[2*], **C Aravindan**[2], **G Vinoth Kumar**[2]

1 Associate Professor, Electronics and Communication Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Ramapuram, Chennai, India
2 Assistant Professor, Electronics and Communication Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Ramapuram, Chennai, India

OPEN ACCESS

Received: 26-06-2023

Accepted: 09-09-2023

Published: 13-10-2023

Citation: Arthi R, Kumar DM, Aravindan C, Kumar GV (2023) An Intelligent Quad Level Digital Lock System for Safety Vaults . Indian Journal of Science and Technology 19(38): 3195-3204. https://doi.org/10.17485/IJST/v16i38.1590

* **Corresponding author**.

manojkud1@srmist.edu.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The current authentication system relates to the wellbeing of safety and security through individual verification of OTP, face or email. The proposed framework guarantees through four level verification such as face recognition, QR code access, OTP and a valid email authentication to access the security lock. **Method:** The methodology uses four step verification process of one time password, password authentication, face recognition of the user and authenticated verification of the user. **Findings:** The significant findings of the proposed computerized code lock framework in the places of the client has been characterized and server produced digits in addition to client that makes figuring out or hacking the code more intricate and furthermore tedious. **Novelty :** The proposed work subsequently describes the novelty of an advanced code lock security framework wherein the client has been granted access with the support of four stages of authentication. The various stages of the authentication includes verification of face recognition, QR code access, OTP generation and valid email verification.

Keywords: Safety Vaults; OTP; QR Code; Face Recognition

1 Introduction

The security code lock frameworks are utilized normally at the banks in wellbeing vaults and even at the private places, for example, houses and lodgings to give wellbeing to the assets and cash and in the interim most ordinarily heard news in the instances of burglary is breaking of the security code lock systems. The existing security code lock frameworks are of both simple and advanced types and are utilized in agreement to the solace and the client comfort. The simple lock frameworks are the frameworks with the mix code lock or the lock and key framework. The advanced code lock frameworks are the ones with the computerized numbering code lock frameworks. The simple blend code lock framework can be broken by knowing the mixes and the lock and key framework can be broken by abusing the key. The advanced security storage spaces can likewise be broken by hacking or deciphering the code. In order to provide safety and security, the proposed system introduces the quad level digital lock by verification of face recognition, QR code access, OTP generation and valid email verification. In [1] the hybrid geometry copper electrodes are adhered on cellulose paper in a simple do-it-yourself (DIY) based fabrication procedure to create the passive transducer-based touch sensors Sensors and Actuators has used the home passage security framework where the increased possibilities of intrusion leading to home security which includes the traditional door lock, RFID, Bluetooth, gesture-based for door lock security systems has been proposed in[2]. In [3] accordance with our design, the fine security of the main gate of the vault will be provided by a biometric function, such as hand geometry, an iris scanner, a fingerprint scanner, or a heartbeat rate with a password or PIN. ItThe system includes a door lock with functions like OTP password creation, lock remote control, picture storage, and live streaming, as well as a smartphone app with functions like real-time video monitoring, door lock control, and event logging[4]. A mystery thump power for the entryway lock security framework utilizing Arduino and versatile has been proposed in[5]. It works by utilizing a thumb power and send the data to versatile the application through remote organization to open or lock the entryway.

In[6]IR sensor array to use secret gesture pattern to unlock the door, tracking number of transactions from the vault using Sonar sensor, and LDR was used as a switch. Password protected entry to connect with the smartphone using Bluetooth module. The Computerized door lock is an electronic locking structure operated by the fusion of advanced key, security secret key or number codes and developed as a domestic safety structure by the ZigBee system with a gadget.

In[7], the author has proposed the electromagnetic lock on the entryway that has the ability to open the event where the picture was available in the information base. In[8] the system would extract a user's brainwaves using an electroencephalogram device. Frequency domain analysis was used to evaluate the system utilizing cognitive tasks such as selective attention, response to stimuli, long-term memory, sustained attention, and divided attention.

To reduce all frequent dangers, it makes use of the finest cloud security principles, appropriate cryptographic usage, and trusted computing. To securely authenticate utilizing Fast IDentity Online (FIDO2) requirements, the cloud architecture runs a Virtual Machine (VM). For security reasons, the information from the physical authenticator is kept in the cloud and is only accessed when an unlock is required.[9]. The user's access is discovered and verified by the RFID card reader. When the card is in close proximity to the reader, it detects the card's radio frequency and validates its authenticity. The key also activates an LCD display and an LED that blinks[10]. In[11], the author has proposed a hand signal acknowledgment based advanced lock framework. The author has planned a useful lock framework utilizing Human-Computer Interaction (HCI) show for the training reason. A minimal expense shrewd entryway locking framework fit[12] for settling on choices in light of facial acknowledgment innovation. The framework works through a mix of Arduino UNO and the Android-based cell phone. It is fit for playing out all the facial acknowledgment stages all alone, for example, face location, highlights extraction, face acknowledgment applying the OpenCV library. An advancement of minimal expense, solid arrangement valuable[13] for both in home robotization and security by utilizing the Node MCU and Google Assistant. This framework can screen and control different boundaries like temperature, dampness, light power. It will take vocal orders from the google partner also the information from the sensors that got broke down in the cloud server IFTTT.

The NFC entryway lock execution[14] that is minimal expense and easy to understand in light of Arduino sheets as the microcontroller. In[15] the author has proposed a LoRa innovation that can interminably screen the situation with the entryway. Lora Technology has reconfigured the IoT by empowering significant distance information associations while utilizing next to no power. LoRa WAN fills a specialized hole for portable based and a WiFi networks which needs higher power or high transfer speed, or even the failure to enter into profound indoor regions. In[16], the author has proposed a procedure by considering the monetary state of individuals of an agricultural nation like Bangladesh. The author has proposed an IoT based savvy home security and computerization framework named 'Facebook courier Chatbot' which has made involving Raspberry PI as the focal processor. It will empower its clients to utilize it liberated from cost as Facebook courier application is free in Bangladesh.

A way to deal with distinguish a human face utilizing surface examination which incorporates[17] figuring a Histogram of Gradients (HOG) over an area of the face and afterward utilizes Support Vector Machines (SVMs) to perceive a face. A squint discovery instrument utilized in this article guarantees the energy of the individual, making the framework more dependable. This model can accomplish a most extreme precision of 92.68% and accomplishes ideal outcomes during the evening, taking a sum of 9.89 seconds for face acknowledgment and flicker location. In[18], the author has proposed a dual authenticated digital code lock system wherein the digital code is of total the 8 digits in which 4 digits of the code are user-defined and the remaining 4 are server generated digits and changes for every individual entry [commonly known as OTP(One Time Password)].

In[19] the work centers around an issue infusion into involved pieces of Instruction Memory (IMEM) and Data Memory (DMEM). Moreover, the long-lasting disappointments of processors has got reproduced by shortcoming infusion of Look-up Tables (LUTs) of the processor plan on the FPGA. The outcome shows the use of specific SW-executed adaptation to internal failure strategies may, in inverse, debase the hardness of the framework. The examinations suggest that the IMEM is the touchiest to blame infusion, while there were less opportunities for a possible self-fix. On account of DMEM, incorrect qualities might be perhaps fixed when the variable is revamped back to the memory, somewhat bringing the DMEM responsiveness down to blame infusions. The actual CPU is the most un-vulnerable. Despite the fact that deficiencies are infused to the used substance just, for the CPU LUTs, a specific piece of the rationale may not be utilized to execute the expected capacity.

In [20] suggests a dual authenticated digital code lock system with an 8-digit total digital code, 4 of which are user-defined and the other 4 generated by a server.

2 Methodology

The existing literature pertaining to the safety and security either deals individual verification of the system, while the novelty of the proposed system ensures safety and security through four level authentication.

The proposed work basically thought about the genuineness of safety passwords, telephone numbers or security data.Increasing the safety to houses, valuables in safety vaults, and depositories are the leading purpose of the recommended method.

The recommended framework has a four-venture verification process in Figure 1 . The initial step verification process has been finished by sending a warning to the enlisted portable number of the proprietor to affirm assuming that the client who is attempting to get approved one or not. On the off chance that the proprietor endorses, the framework will be continuing on to the subsequent stage else the nearby cops, the security authorities and the proprietor will be educated that unapproved access has being finished.

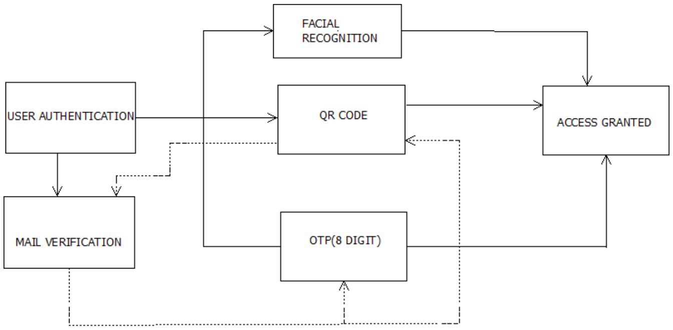


Fig 1. Architecture of the system

In the secondary session, a 4-digit OTP is shipped off the enlisted versatile number of the proprietor. The more elevated level security to the framework has been given in this separate advance, in light of the fact that the OTP produced in this progression has been created utilizing our proposed calculation that makes it challenging to an unapproved clients to decipher the code. The OTP created changes for each individual passage and furthermore would be sent uniquely to the enlisted proprietor's versatile hand set just and consequently it has been kept up with secretly. The client likewise needs to keep a 4-digit fixed code. Consequently, the client would have a 4-digit OTP and a 4-digit fixed for example, client characterized code. The client has additionally furnished with a choice to change the places of the client characterized with 4-digit code and the OTP. For example, the client can fix the positions to such an extent that 1,3,5,7 digits of the 8-digit code ought to have the client characterized for example, fixed code and 2,4,6,8 digits ought to have the OTP which is gotten in the enlisted proprietor's portable hand set. In the third step, the process of facial recognition has been used. Facial liveness has arisen as an approach to stop extortion and guarantee the honesty of face biometrics as a methods for validation. Though face acknowledgment for verification can precisely respond to the inquiry ”Is this the correct individual?” it doesn't address the inquiry, ”Is this a genuine individual?”. This is the job of liveness recognition. Facial liveness location works with a biometric framework to quantify and dissect actual attributes and responses to decide whether a biometric test is being caught from a living subject who is available at the place of catch.

In our proposed framework, an informational collection of 8 photos of the proprietor (client) has been taken care of to the framework to get prepared. When the essence of client gets prepared and confirmed, then, at that point, the QR code is shipped off the client's enlisted mail id. In the fourth and the last advance, the QR code has been acquired by the client in the clients enlisted mail id and the client should check the QR code in the framework. The QR code uses RS Algorithm for code generation and lastly the client gets approved for the client to gain admittance to the framework.

In this segment, the inward work stream of the framework has been made sense of with the assistance of flow graph in Figure 2 . First the entrance demand has been shipped off the enlisted client versatile number, in the event that it awards verification, the client would be handled with 4-digit OTP and 4-digit fixed code. When the confirmation falls flat in the initial step, prompt ready hint would be shipped off the neighborhood cops and security authorities to safeguard the framework. Next interaction

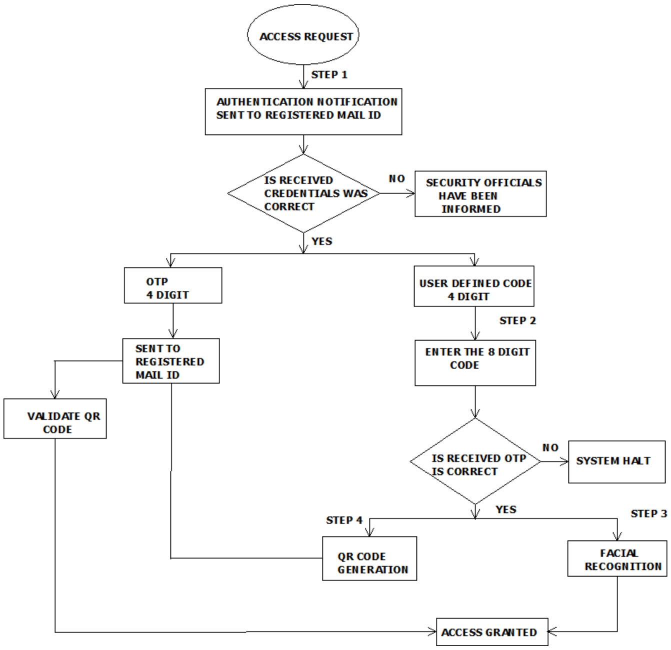

ACCESS REQUEST
STEP 1
AUTHENTICATION NOTIFICATION SENT TO REGISTERED MAIL ID
IS RECEIVED CREDENTIALS WAS CORRECT
NO
SECURITY OFFICIALS HAVE BEEN INFORMED
YES
OTP 4 DIGIT
USER DEFINED CODE 4 DIGIT
STEP 2
SENT TO REGISTERED MAIL ID
ENTER THE 8 DIGIT CODE
VALIDATE QR CODE
IS RECEIVED OTP IS CORRECT
NO
SYSTEM HALT
YES
STEP 4
STEP 3
QR CODE GENERATION
FACIAL RECOGNITION
ACCESS GRANTED

Fig 2. Process of User Authentication to access the security system

is acquiring the 8-digit security code (OTP and client characterized code). In the event that the got security code is right, it continues to create the QR code that must be sent to the enlisted mail id. Presently the QR gets approved by the client to allow the entrance. In the event that the got code is erroneous, the framework stops and won't continue further. The last verification would be facial acknowledgment to concede the entrance. Thus, to get to the security framework, the cycle needs to go through all the four-way confirmation to make each progression effective. The proposed work can be used in practice for safety vaults in banks and cash withdrawal in ATM etc.

2.1 Proposed Algorithm

```
function otp
    open 4 digit.txt
    open secret.txt
    step1
    read 4 digit.txt and store in n
    read secret.txt and store in secret_code
    n=n-
    set next number=middle four digits of square of n
    if,
    next number is less than 1000
    next number=next number+1000
    write next number in 4 digit.txt
    return next number
    initialize
    get userid from the user
    if
    the userid is invalid
    then
    go to step 1
    Step 2
    set max retry=3
```

```
send an one time password via registered email id
get the passcode from the user
if
the passcode is invalid
if
max retry>0
then
max retry-=1
else
maximum limit is exceeded
System Halts
return
Step 3
capture the face of user
set max retry=3
if
the captured face is mismatching with the owner’s face
if
max retry>0
then
max retry-=1
go to step 3
else
maximum limit is exceeded
go back to step 1
set max allowed time=3
step 4
generate a QR code
send the generated QR code to the registered email id
if
the authentication is successful
then
the QR scan is validated
then
access is given
```

2.2 Training the system

Initially the system has been trained with username and password. As soon as the user opens the training window, the space in which the username has to be given pops up and the operator will have to enter the username. Then the very next responsibility of the operator has to train the system with the 4-digit user defined code that could have to be used in the second step of the authentication process. So, the system trains itself with the 4-digit one time password and the user defined code of 4 digits was generated while the 8-digit code gets stored in the system and waits for the user to enter the password in the predefined order.

If the password generated in the second step matches with the password stored in the system, then proceeds to the next step of authentication else the system halts at the same point where the system identifies the malicious usage.

The third step of training process was to train the faces of the user. The most crucial step of training was that the accuracy completely depends on the training part. Here the proposed work has been trained with a data set of 8 pictures to increase the accuracy of the system.

As soon as the system authorizes the face with the support of Training, then the authentication process starts to validate and thereby the access has been granted for the safety lock to function**.**

3 Results and Discussion

The working model of the RFID-based door lock system has been discussed[21]. An RFID-based door lock system along with OTP driven technology is discussed to provide a high-security solution for households. The author has designed[22] in such a way that the OTP is generated for door access and this OTP will expire after the expiration time provided and designed a real-time face recognition security door lock system connected with raspberry pi as an implication of the proposed method.

The various authentication processes such as OTP Verification, Password Authentication, Facial Recognition and QR code Authentication is being simulated and discussed in this section.

3.1 Step 1: OTP Verification

As discussed, the underlying User Interface demands admittance to the security lock framework , the client would get a notice in his/that's what her enlisted portable number on the off chance that the solicitation is an approved one or not. In the event that the proprietor supports, the framework would prompt a higher-level else the instant message will be shipped off the neighborhood security work force that an unauthenticated client is attempting to break the security lock system.

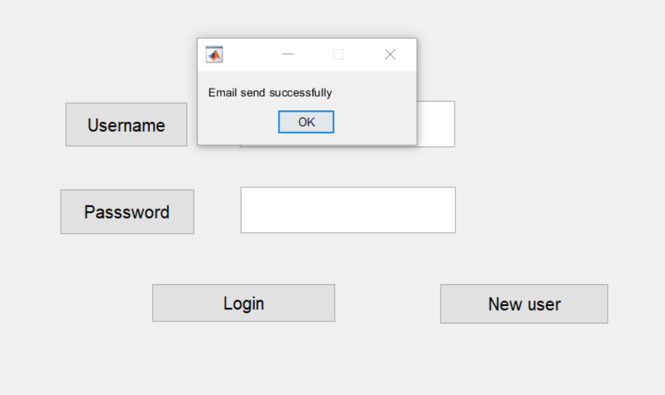
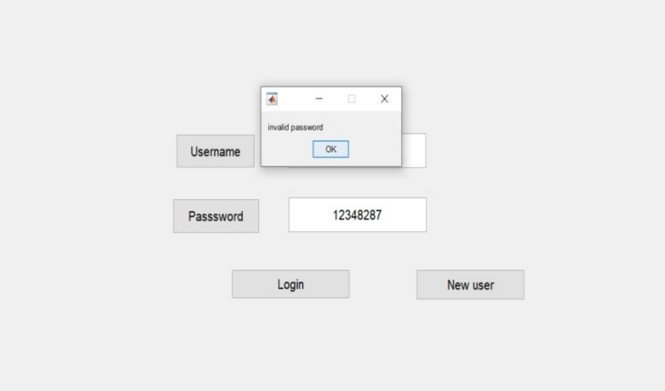

Email send successfully

Fig 3. Email Notification

As soon as the client approves his/her client id the email is shipped off the client's enrolled mail id in Figure 3 and the client should engage a similar OTP in the following stage of the cycle

3.2 Step2 : Password Authentication


invalid password

Passsword: 12348287

Fig 4. Invalid Password

In the subsequent procedure, a 4-digit OTP has been shipped off enrolled portable number of the client. The more significant level security to the framework has been given in this particular advance in light of the fact that the OTP created utilizes our proposed calculation that makes it hard to the unapproved clients to decipher the code in Figure 4 . The OTP produced changes for each individual section and furthermore would be sent just to the enlisted proprietor's mobile handset just and consequently was kept up with privately. The client additionally needs to keep a 4-digit client characterized code. So the client will have a 4-digit OTP and a 4-digit fixed i.e.; client characterized code. The client was additionally given a choice to change the places of the client characterized 4 digit code and the OTP. For example the client can fix the positions with the end goal that 1,3,5,7 digits of the 8-digit code ought to have the client characterized i.e.; fixed code and 2,4,6,8 digits ought to have the OTP which is gotten in the enlisted proprietor's portable.

3.3 Step 3: Facial Recognition

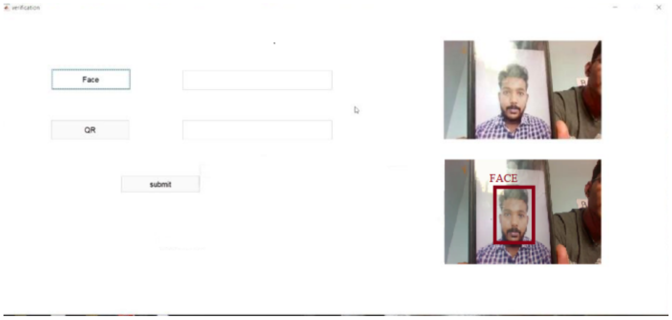
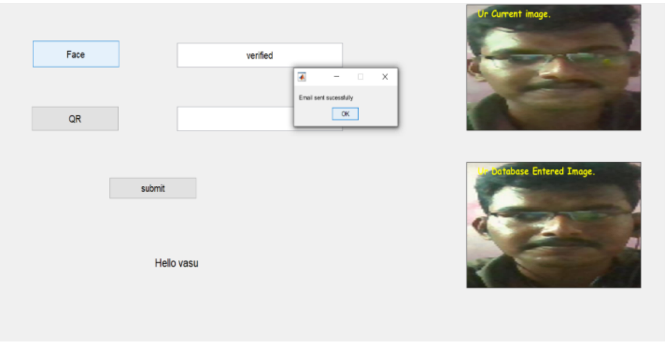


Fig 5. Capture of Unauthorized Face



verified

Email sent sucessfully

Hello vasu

Fig 6. Authentication of authorized Face

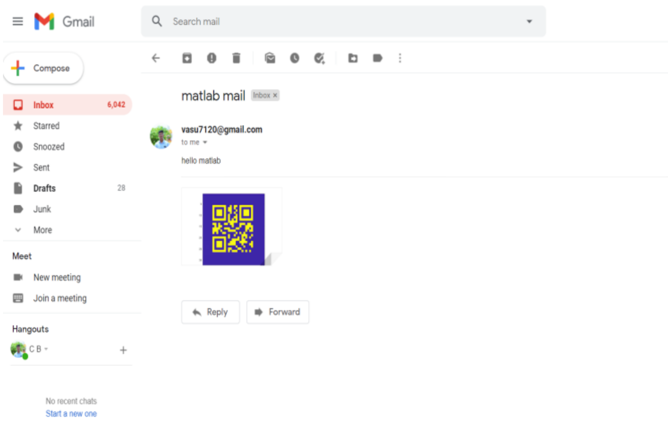
The Figure 5 explains the process of facial recognition. Eigen face Algorithm for facial recognition and PCA for dimensionality reduction towards obtaining the accuracy. The process of facial image capture and authentication process is dealt clearly with the simulated output**.**

3.4 Step 4: QR code Authentication

Once the user gets authenticated by facial recognition , then it has to be verified by QR code. In this process, as soon as the face of the user is authorized then QR code that is encrypted using the 8-digit password entered in the second step of the authentication is sent to the registered email id of the owner .

The user now has to scan the QR code received in the registered email id using the camera of the system so that the camera could match the QR code in the database . If the QR code matches then the system says that the usage is an authorized usage and gives the access to the user . If the QR code is not matched with the QR code in the database then the access will not be given to the user. When the user gets successfully authenticated in all the steps, then the access is given to the user else not.

The Figures 9 and 10 shows the hardware output for displaying the process of Authorization. The time taken for the whole process to complete was 3 minutes and 50 seconds. The accuracy levels of each process have also been calculated for the first, second and the last steps are 100% accurate as they are just being matched with the actual text or the picture from the database.

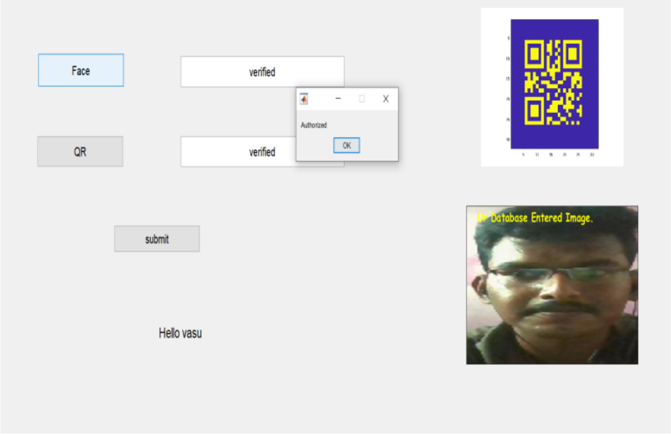


matlab mail Inbox ×

vasu7120@gmail.com
to me

hello matlab

Fig 7. Encrypted QR code received in the mail



Face: verified

QR: verified

Authorized

Hello vasu

Fig 8. User Authorized

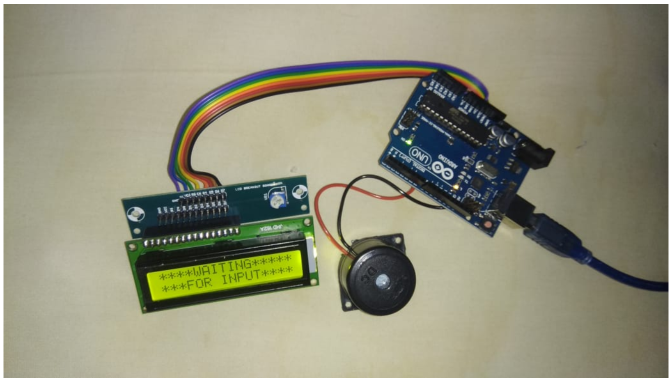


Fig 9. Hardware Output displaying the process

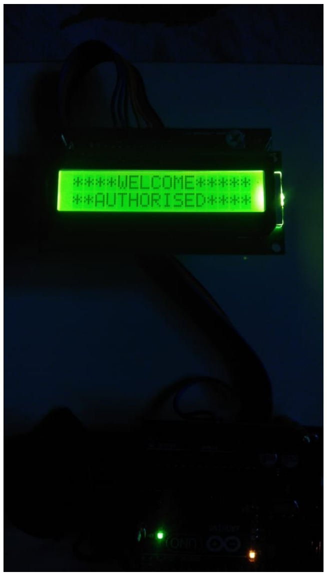


Fig 10. LCD Display for Authorization

The third step that includes the facial recognition was 90% accurate as the camera fails to detect the faces in the highly lightened places and that is the only reason of failure of 1 test case amongst the 10 test cases.

4 Conclusion

A design frame work of an electronic safe has been proposed with security measures of the assets placed inside the safety vaults against the hacking techniques by an unauthorized users that can be prevented and protected. The electronic safe system has a quad level authentication mechanism that is more secure than existing techniques, where the security code under goes multi-level authentication . This makes the proposed digital code security system safe and non-penetrable. The various stages of the authentication includes verification of face recognition, QR code access, OTP generation and valid email verification by providing security to the safety vaults. The efficiency and safety of the system has been authenticated with quad level security to access the vault.

Future Scope

In near future many more number of security levels can be added and the system can be upgraded with Finger and Iris Biometric with proper training and testing with the support of data set. Few such considerations are providing a strong firewall which cannot be penetrated by malicious operators and users.

References

1) Mehmood MQ, Malik MS, Zulfiqar MH, Khan MA, Zubair M, Massoud Y. Invisible Touch Sensors-Based Smart and Disposable Door Locking System for Security Applications. *SSRN Electronic Journal*. 2023;9(2):793–797. Available from: https://doi.org/10.1016/j.heliyon.2023.e13586.
2) Shetty S, Shetty S, Vishwakarma V, Patil S. Review Paper on Door Lock Security Systems. *2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW)*. 2020;p. 1–4. Available from: https://doi.org/10.1109/ICCDW45521.2020.9318636.
3) Dutta M, Islam MA, Mamun MH, Psyche KK, Mamun MA. Bank vault security system based on infrared radiation and GSM technology. Springer International Publishing. 2019. Available from: https://link.springer.com/chapter/10.1007/978-3-030-34080-3_14.
4) Kook J. Design and Implementation of a OTP-based IoT Digital Door-lock System and Applications. *International Journal of Engineering Research and Technology*. 2019;12:1841–1847. Available from: https://www.ripublication.com/irph/ijert19/ijertv12n11_02.pdf.
5) Rhunn TCH, Raffei AFM, Rahman NSA. Internet of Things (IoT) Based Door Lock Security System. *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*. 2021;p. 6–9. Available from: https://doi.org/10.1109/ICSECS52883.2021.00008.
6) Joy MHC, Karim MMA, Choudhury AH, Razin M, Ahmed SNM. An IoT Based Smart Vault Security and Monitoring System with Zero UI. *2023 3rd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*. 2023;p. 95–100. Available from: https://doi.org/10.1109/ICREST57604.2023.10070057.

7) Shanthini M, Vidya G, Arun R. IoT Enhanced Smart Door Locking System. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2020;p. 92–96. Available from: https://doi.org/10.1109/ICSSIT48917.2020.9214288.

8) Alipio MI. Development, evaluation, and analysis of biometric-based bank vault user authentication system through brainwaves. *Journal of Ambient Intelligence and Humanized Computing*. 2023;14(8):10165–10179. Available from: https://doi.org/10.1007/s12652-021-03679-8.

9) Sethuraman SC, Mitra A, Li KC, Ghosh A, Gopinath M, Sukhija N. Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets. IEEE Access. 2022. Available from: https://doi.org/10.1109/ACCESS.2022.3216665.

10) Guntur J, Raju SS, Niranjan T, Kilaru SK, Dronavalli R, Kumar NSS. IoT-Enhanced Smart Door Locking System with Security. *SN Computer Science*. 2023;4(2):209. Available from: https://doi.org/10.1007/s42979-022-01641-9.

11) Yaseen L, Mousa O, Alawani R, Qaisar SM. Design and Implementation of a Hand Gesture Based Digital Lock Demonstrator. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. 2020;p. 1–4. Available from: https://doi.org/10.1109/ICCIS49240.2020.9257688.

12) Khalimov R, Rakhimbayeva Z, Shokayev A, Kamalov B, Ali MH. Development of Intelligent Door Locking System Based on Face Recognition Technology. *2020 11th International Conference on Mechanical and Aerospace Engineering (ICMAE)*. 2020;p. 244–248. Available from: https://doi.org/10.1109/ICMAE50897.2020.9178866.

13) Javvaji KSS, Nelakuditi UR, Dadi BP. IoT Based Cost Effective Home Automation and Security System. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2020;p. 1–5. Available from: https://doi.org/10.1109/ICCCNT49239.2020.9225557.

14) Pacheco J, Miranda K. Design of a low-cost NFC Door Lock for a Smart Home System. *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. 2020;p. 1–5. Available from: https://doi.org/10.1109/IEMTRONICS51293.2020.9216409.

15) Venkatraman S, Varshaa RR, Vigneshwary P. IoT based Door open or close monitoring for home security with emergency notification system using LoRa Technology. *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*. 2021;1:173–178. Available from: https://doi.org/10.1109/ICACCS51430.2021.9441890.

16) Ahmed S, Paul D, Masnun R, Shanto MU, Farah T. Smart Home Shield and Automation System Using Facebook Messenger Chatbot. IEEE. 2020. Available from: https://doi.org/10.1109/TENSYMP50017.2020.9230716.

17) Ganjoo R, Purohit A. Anti-Spoofing Door Lock Using Face Recognition and Blink Detection. *2021 6th International Conference on Inventive Computation Technologies (ICICT)*. 2021;p. 1090–1096. Available from: https://doi.org/10.1109/ICICT50816.2021.9358795.

18) Arthi R, Manojkumar D, Abraham A, Kishan AR, Sattenapalli A. Deep Learning Based Multi-Modal Biometric Security System Using Visible Light Communication. *WSEAS Transactions on Systems and Control* . 2022;17:34–41. Available from: https://wseas.com/journals/sac/2022/a085103-002(2022).pdf.

19) Lojda J, Panek R, Podivinsky J, Cekan O, Krcma M, Kotasek Z. Hardening of Smart Electronic Lock Software against Random and Deliberate Faults. *2020 23rd Euromicro Conference on Digital System Design (DSD)*. 2020;p. 680–683. Available from: https://doi.org/10.1109/DSD51259.2020.00110.

20) Arthi R, Kumar DM, Vasu CB, Asan RA, Pradeep S. A Dual Authenticated Safety Vault for Cryopreservation Center. *Turkish Journal of Computer and Mathematics Education*. 2021;12(9):2378–2384. Available from: https://doi.org/10.17762/turcomat.v12i9.3715.

21) Aswini D, Rohindh R, Ragavendhara KSM, Mridula CS. Smart Door Locking System. *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*. 2021;8:1–5. Available from: https://doi.org/10.1109/ICAECA52838.2021.9675590.

22) Waseem M, Khowaja SA, Ayyasamy RK, Bashir F. Face Recognition for Smart Door Lock System using Hierarchical Network. *2020 International Conference on Computational Intelligence (ICCI)*. 2020;8:51–56. Available from: https://doi.org/10.1109/ICCI51257.2020.9247836.