

DESIGN OF A MULTI-LAYERED ELECTRONIC SECURITY LOCK SYSTEM

Trinh Thuy Ha*, Luong Quang Huy

TNU - University of Information and Communication Technology

ARTICLE INFO		ABSTRACT
Received:	19/4/2023	Users often use mechanical locks to protect their assets, but they can easily be bypassed through various tricks, and losing keys can also cause a lot of inconveniences. With the development of technology, electronic security locks have been created to solve the drawbacks of traditional locks. This article proposes to build an electronic lock that combines functions into one device, including a password input keyboard, fingerprint sensor, and one-time password via SMS sent to the owner's phone, to create a multi-layered security system that allows users to open the door by combining fingerprint with OTP code or entering multiple passwords with a 4x4 keypad. In addition, the lock will also provide unauthorized intrusion warnings in case of violation of administrative access rights or incorrect unlocking procedures. The system's operation is verified through simulation on Proteus software. The research results provide an effective security solution, improving and bringing convenience to the community.
Revised:	23/5/2023	
Published:	23/5/2023	
KEYWORDS		
Electronic lock		
Password lock		
One-time password		
Fingerprint lock		
Multi-layer security		

THIẾT KẾ HỆ THỐNG KHOÁ ĐIỆN TỬ BẢO MẬT ĐA LỚP

Trịnh Thuý Hà*, Lương Quang Huy

Trường Đại học Công nghệ Thông tin và Truyền thông – ĐH Thái Nguyên

THÔNG TIN BÀI BÁO		TÓM TẮT
Ngày nhận bài:	19/4/2023	Người dùng thường sử dụng khoá cơ khí để bảo vệ tài sản, nhưng chúng dễ bị phá thông qua các thủ thuật khác nhau, đồng thời, việc thất lạc khoá cũng gây ra nhiều phiền phức. Với sự phát triển của công nghệ, khoá điện tử bảo mật đã được ra đời giúp giải quyết những bất cập gặp phải ở khoá truyền thống. Bài báo đề xuất xây dựng một khoá điện tử kết hợp các chức năng trong một thiết bị gồm bàn phím nhập mật khẩu, cảm biến vân tay và mật khẩu dùng một lần qua tin nhắn SMS gửi đến điện thoại chủ sở hữu, để tạo lên hệ thống bảo mật đa lớp, cho phép người dùng mở cửa kết hợp vân tay với mã OTP, hay nhập liệu đa mật khẩu với bàn phím 4x4. Bên cạnh đó, bộ khoá cũng sẽ đưa ra cảnh báo xâm nhập trái phép trong trường hợp vi phạm quyền truy cập quản trị hay sai thao tác, quy trình mở khoá cửa. Hoạt động hệ thống được kiểm chứng thông qua mô phỏng trên phần mềm Proteus. Kết quả nghiên cứu cung cấp một giải pháp an ninh hiệu quả, nâng cao và mang lại sự tiện lợi cho cộng đồng.
Ngày hoàn thiện:	23/5/2023	
Ngày đăng:	23/5/2023	
TỪ KHÓA		
Khoá điện tử		
Khoá mật khẩu		
Mật khẩu dùng một lần		
Khoá vân tay		
Bảo mật đa lớp		

DOI: <https://doi.org/10.34238/tnu-jst.7778>

* Corresponding author. Email: ttha@ictu.edu.vn

1. Giới thiệu

Trong thời đại xã hội thông tin phát triển với tốc độ chóng mặt, bảo mật dữ liệu trở nên ngày càng phức tạp và quan trọng hơn bao giờ hết. Các tổ chức, doanh nghiệp hay cá nhân đều muốn bảo vệ tài sản của mình không bị mất mát hay xâm nhập từ bên ngoài. Hệ thống khoá cửa điện tử là một giải pháp hiện đại được sử dụng rộng rãi trong các tòa nhà, văn phòng, căn hộ và các khu dân cư. Với khả năng đảm bảo tính an toàn và bảo mật cho người sử dụng, nó đang ngày càng được ưa chuộng. Vì vậy, việc nghiên cứu và phát triển các khóa bảo mật là một nhu cầu cấp thiết. Tuy nhiên, các công cụ và phương pháp bảo mật hiện có đang phải đối mặt với các mối đe dọa ngày càng phức tạp và tinh vi. Điều này đưa ra vấn đề cần nâng cấp các khóa điện tử để đảm bảo hiệu quả và tính bảo mật cao nhất.

Để phát triển về hệ thống khoá cửa điện tử tích hợp các công nghệ mới đảm bảo an ninh cao, các nhà khoa học đã tiến hành nghiên cứu thiết kế, thử nghiệm và đưa ra nhiều công trình, có thể kể đến như: Bài báo [1] cung cấp một hệ thống cho phép chủ nhà có thể kiểm soát cửa ra vào bằng điện thoại thông minh dựa trên công nghệ Bluetooth. Một cơ sở dữ liệu được sử dụng để lưu trữ thông tin ra vào. Tài liệu [2] đề xuất một khóa thông minh có thể nhận cuộc gọi, xác minh bộ số đăng ký để ra lệnh đóng, mở cửa, đồng thời cảnh báo trong trường hợp truy cập trái phép. Các tác giả trong [3] đưa ra trình bày về hệ thống khóa cửa thông minh có thể được giám sát và điều khiển từ xa bằng ứng dụng Android. Khi khách đến và bấm chuông, một camera được kích hoạt để thông báo cho chủ nhà và truyền trực tiếp hình ảnh người đó tới điện thoại qua Internet. Chủ nhà có thể mở/đóng cửa từ xa bằng mật khẩu trước đó và truyền tin nhắn âm thanh cho người đến bằng cách nhập văn bản tương ứng trên điện thoại thông minh. Hệ thống được thiết kế để cung cấp tính năng truy cập từ xa trên một giao diện người dùng đồ họa tương tác trên một máy chủ đám mây. Công trình [4] phát triển một hệ thống khóa cửa sử dụng công nghệ Quick Response (QR) cho phép ghi nhật ký dữ liệu theo dõi vào, ra từ máy chủ web. Nghiên cứu [5] sử dụng công nghệ Internet of Things (IoT) và nhận diện khuôn mặt để mở khóa cửa dựa trên hình ảnh được lưu trong cơ sở dữ liệu. Một email cảnh báo sẽ được gửi cho chủ nhà trong trường hợp có kẻ xâm nhập. Một hệ thống dựa trên RFID được thảo luận trong [6] cung cấp một giải pháp khoá bảo mật cho các hộ gia đình. Hệ thống [7] cho phép khi chuông cửa reo, thông báo sẽ được gửi đến điện thoại, xác định người đứng trước cửa và quyết định cấp quyền vào nhà và một bản phím nhập mật khẩu để mở cửa từ bên ngoài. Báo cáo [8] mô tả giải pháp khóa cửa thông minh cho phép điều khiển đóng, mở cửa bằng khẩu lệnh thông qua Amazon Alexa,...

Tác giả nhận thấy các khóa điện tử trên thị trường hiện nay, hay trong các công trình nghiên cứu được khảo sát sử dụng nhiều kỹ thuật hiện đại, phương pháp bảo mật đa dạng, nhưng đa số đều là bảo mật đơn lớp dẫn đến khả năng bị xâm nhập trái phép khi kẻ xấu phá được lớp bảo vệ, hoặc có thể không kịp thời phát hiện ra và xử lý tình huống. Xuất phát từ yêu cầu thực tiễn, tác giả đề xuất thiết kế một hệ thống khoá bảo mật đa lớp, kết hợp các các thiết bị phổ biến như bàn phím nhập mật khẩu, vân tay và mã OTP (One-Time Password) gửi tin nhắn văn bản SMS tới điện thoại. Kết quả nghiên cứu hệ thống khoá điện tử có ý nghĩa quan trọng trong việc nâng cao bảo mật và tiện ích cho người sử dụng. Hệ thống khoá điện tử giúp người dùng có thể kiểm soát an ninh hiệu quả, tránh được những rủi ro từ việc sử dụng khoá cơ truyền thống.

2. Phương pháp nghiên cứu

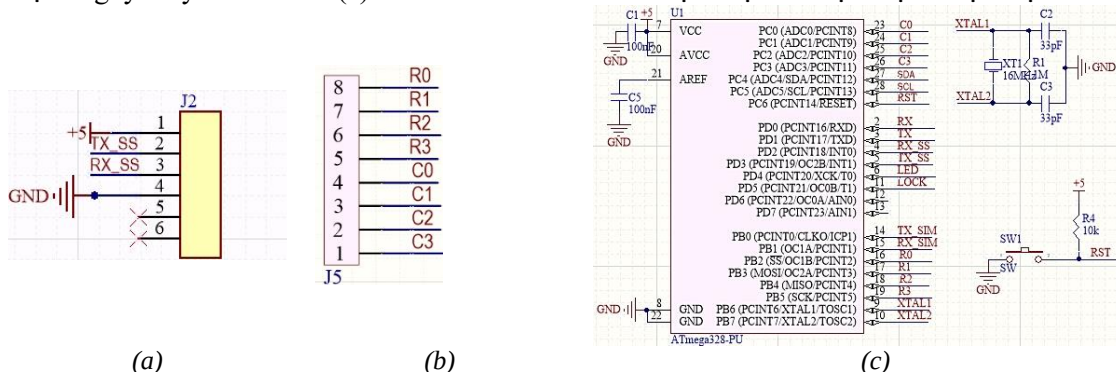
2.1. Thiết kế phần cứng cho hệ thống khoá bảo mật đa lớp

Thiết bị bảo mật đa lớp được xây dựng gồm các khối chính sau:

- Khối thu thập dữ liệu vân tay: chuyển dữ liệu vân tay về cho khối xử lý trung tâm, khối này có mạch nguyên lý như Hình 1(a), với module cảm biến vân tay AS608 sử dụng giao thức truyền thông nối tiếp bất đồng bộ UART để giao tiếp với vi điều khiển.

- Khối ma trận bàn phím: dùng để nhập mật khẩu, số điện thoại và mã OTP, khối này có mạch nguyên lý như Hình 1(b), sử dụng keypad 4x4.

- Khối xử lý trung tâm: có chức năng xử lý và giải mã thông tin từ các khối như cảm biến vân tay, module sim gửi mã OTP và ma trận phím để điều khiển khối cơ cấu chấp hành, khối này có mạch nguyên lý như Hình 1(c). Module Arduino Uno được chọn để thực hiện nhiệm vụ của khối.



(a)

(b)

(c)

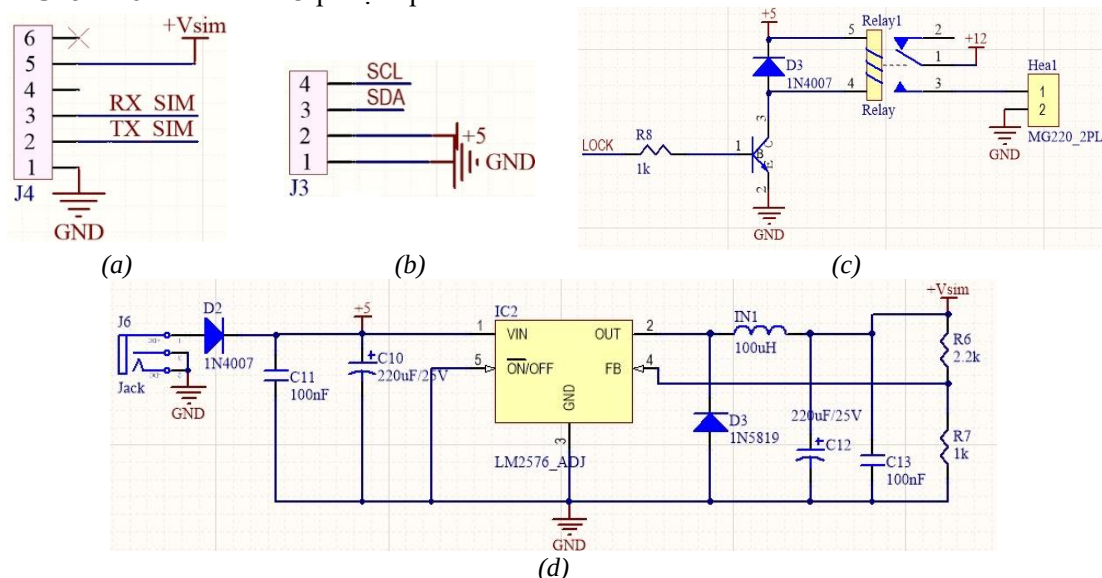
Hình 1. Sơ đồ mạch nguyên lý: (a) Khối thu thập dữ liệu vân tay; (b) Khối ma trận bàn phím; (c) Khối xử lý trung tâm

- Khối module sim gửi mã OTP: được sử dụng để gửi mã OTP về điện thoại, khối này có mạch nguyên lý như Hình 2(a). Module sim 800L sử dụng giao thức UART để giao tiếp với MCU. Chân TX và RX của module sim sẽ được kết nối với các chân tương ứng trên MCU để truyền và nhận dữ liệu giữa hai thiết bị.

- Khối hiển thị LCD: chịu trách nhiệm hiển thị thông tin trên màn hình LCD1602, khối này có mạch nguyên lý như Hình 2(b).

- Khối cơ cấu chấp hành: nhận tín hiệu từ khối xử lý trung tâm để thực hiện các hành động như đóng mở cửa, khối này có mạch nguyên lý như Hình 2(c) sử dụng module Relay 5VDC.

- Khối cung cấp nguồn: chịu trách nhiệm cung cấp nguồn cho toàn bộ hệ thống, khối này có mạch nguyên lý như Hình 2(d). Nguồn cung cấp là DC 5V-2A. Mạch sử dụng IC nguồn LM2576-ADJ ở đầu ra để cấp điện áp cho module sim.



(a)

(b)

(c)

(d)

Hình 2. Sơ đồ mạch nguyên lý: (a) Khối module sim gửi mã OTP; (b) Khối hiển thị LCD; (c) Khối cơ cấu chấp hành; (d) Khối cung cấp nguồn

Yêu cầu thiết kế của hệ thống khoa điện tử bảo mật đa lớp như sau:

+ Cho phép quản trị viên cài đặt lựa chọn đăng ký, thêm, sửa, xóa vân tay để mở khoá và số điện thoại để nhận mã OTP.

+ Để có quyền quản trị viên thì cần có mật khẩu đăng nhập (từ bàn phím). Khi nhập mật khẩu trong mỗi lần sai quá 3 lần thì cửa vẫn khoá đồng thời gửi SMS đến các số đã đăng ký cảnh báo truy cập trái phép. Sau khi đăng nhập có thể thay đổi mật khẩu truy cập quyền quản lý.

+ Khoá cửa sẽ được mở nếu thực hiện từng bước xác thực: vân tay đúng, tiếp đến nhập chính xác số điện thoại đã đăng ký và mã OTP đã gửi về số đó đúng ngược lại cửa vẫn khoá đồng thời gửi SMS đến các số đã đăng ký cảnh báo truy cập trái phép.

+ Trường hợp dự phòng khi vân tay không thể xác thực (do tai nạn, do cảm biến vân tay lỗi, do tay ẩm ướt, bụi,...) hoặc không có mang theo điện thoại đã đăng ký có thể lựa chọn tính năng nhập mật khẩu để mở khoá. Khi nhập mật khẩu trong mỗi lần sai quá 3 lần thì cửa vẫn khoá đồng thời gửi SMS đến các số đã đăng ký cảnh báo truy cập trái phép. Với quyền quản trị viên thì các mật khẩu mở cửa này cũng có thể thay đổi.

+ Sau khi cửa mở sẽ tự động khoá lại sau 1 khoảng thời gian cài đặt bởi quản trị viên.

2.2. Thiết kế phần mềm cho hệ thống khoá bảo mật đa lớp

Hệ thống khoá bảo mật đa lớp được thiết kế theo thuật toán như sau:

- Bước 1: Cấu hình tiền xử lý: Bắt đầu chương trình cần khai báo các thư viện LCD I2C, Keypad, Wire, Fingerprint sensor AS608, GSM, định nghĩa các biến, các định danh, tạo các kết nối giữa ngoại vi với Arduino,...

- Bước 2: Khai báo các hàm chính:

+ Hàm đăng ký, thêm, sửa, xoá vân tay.

+ Hàm thêm, sửa, xoá số điện thoại và Hàm gửi mã OTP về số đã đăng ký.

+ Ngoài ra còn có các Hàm:

- ✓ Hàm truy cập quyền quản trị: Mật khẩu này gồm 2 lớp bảo vệ, mỗi một lớp yêu cầu mã với 2 mật khẩu khác nhau, nhập đúng lớp 1 mới cho nhập tiếp lớp 2.
- ✓ Hàm thay đổi mật khẩu đăng nhập quyền quản trị: Sau khi đăng nhập thành công có thể thay đổi mật khẩu truy cập quyền quản lý, với mỗi lớp sẽ yêu cầu nhập mật khẩu mới và nhập lại, trùng khớp mới cho xác nhận cập nhật mã.
- ✓ Hàm nhập mật khẩu để mở cửa: Mật khẩu này gồm 2 lớp bảo vệ, mỗi một lớp yêu cầu mã với 2 mật khẩu khác nhau, nhập đúng lớp 1 mới cho nhập tiếp lớp 2.
- ✓ Hàm gửi SMS cảnh báo (truy cập quyền quản trị, mở cửa).
- ✓ Hàm đọc vân tay, hàm đọc giá trị từ bàn phím, hàm hiển thị lên LCD,...

- Bước 3: Cài đặt ban đầu chương trình chính: LCD tắt để tiết kiệm năng lượng, cửa khoá.

- Bước 4:

+ Kiểm tra điều kiện nhập liệu từ bàn phím dãy ký tự: *101#, nếu đúng: LCD sáng, hiển thị thông báo yêu cầu quét vân tay. Nếu vân tay không đúng, thì hiển thị yêu cầu quét lại vân tay, nếu quá 3 lần mà vẫn không trùng với vân tay đã đăng ký thì tắt LCD, cửa vẫn khoá và gửi SMS cảnh báo truy cập trái phép. Nếu vân tay khớp thì LCD hiển thị nhập số điện thoại, nếu nhập không đúng số được đăng ký quá 3 lần, thì tắt LCD, cửa vẫn khoá và gửi SMS cảnh báo truy cập trái phép. Nếu nhập đúng số thì hệ thống sẽ gửi mã OTP về, người dùng nhập 4 số từ mã OTP vào, nếu nhập sai trên 3 lần thì tắt LCD, cửa vẫn khoá và gửi SMS cảnh báo truy cập trái phép. Nếu đúng thì cửa mở, LCD hiển thị thông tin chào mừng. Sau 10 giây thì tự động tắt LCD và khoá cửa.

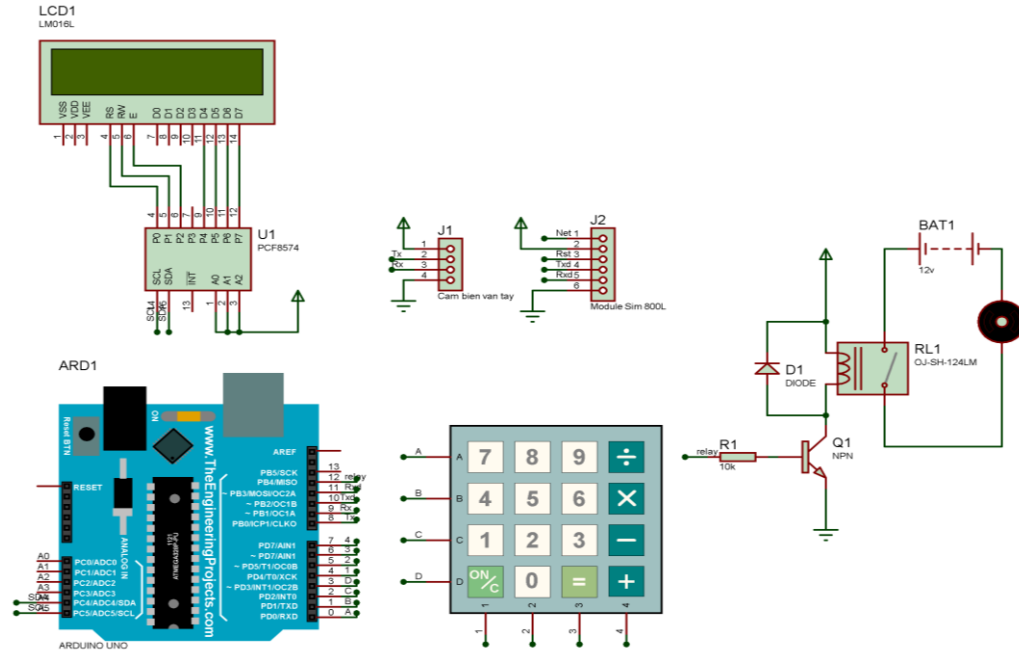
+ Xét điều kiện nhập truy cập quyền quản trị: Nếu nhập mật khẩu lớp 1 đúng thì màn hình LCD hiển thị thông báo yêu cầu nhập khoá lớp 2 để vào cài đặt hệ thống. Nếu nhập sai quá 3 lần thì tắt LCD, cửa vẫn khoá và gửi SMS cảnh báo truy cập trái phép. Nếu nhập mã đúng thì cho phép quản trị viên thực hiện các công việc theo yêu cầu thiết kế.

+ Xét điều kiện mật khẩu để mở cửa: Nếu nhập mật khẩu lớp 1 đúng thì màn hình LCD hiển thị thông báo yêu cầu nhập khoá lớp 2 để mở cửa. Nếu nhập sai quá 3 lần thì tắt LCD, cửa vẫn khoá và gửi SMS cảnh báo truy cập trái phép. Nếu mã đúng thì cửa mở, LCD hiển thị thông tin chào mừng. Sau 10 giây thì tự động tắt LCD và khoá cửa.

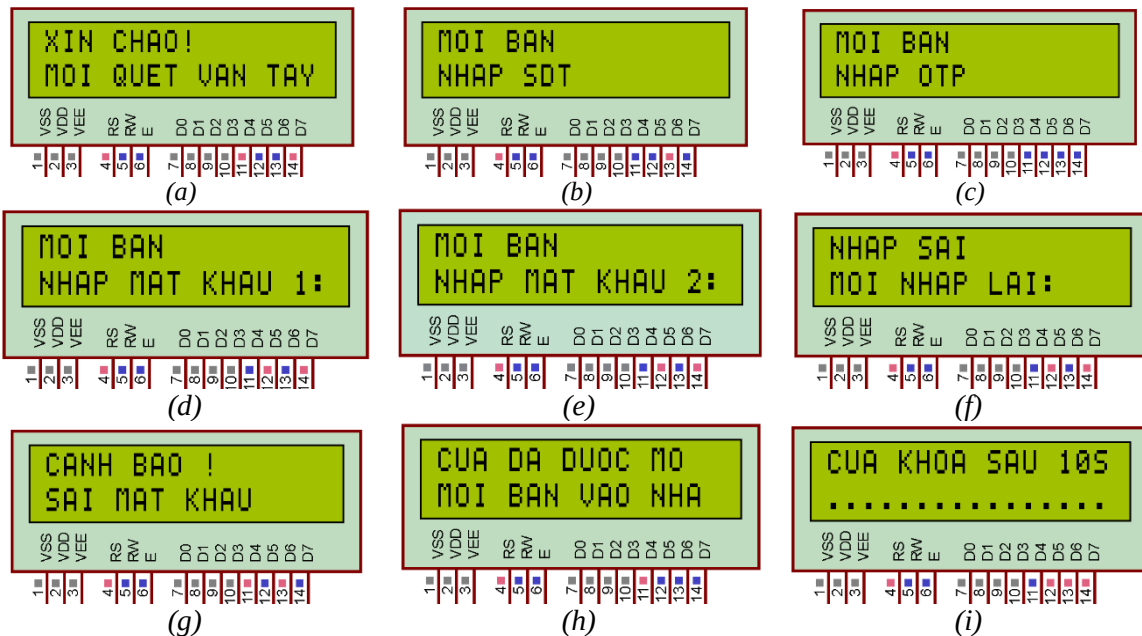
Nếu các điều kiện trong Bước 4 không thỏa mãn thì mặc định LCD tắt và cửa khoá.

3. Kết quả mô phỏng hệ thống

Để kiểm chứng lại hoạt động của hệ thống đảm bảo các yêu cầu thiết kế đặt ra và tuân theo thuật toán điều khiển, tác giả tiến hành mô phỏng khoá bảo mật đa lớp trên phần mềm Proteus. Toàn bộ các linh kiện chính được đưa ra trong sơ đồ nguyên lý ở Hình 3.



Hình 3. Sơ đồ mạch nguyên lý mạch mô phỏng khoá bảo mật đa lớp trên Proteus



Hình 4. Hoạt động của hệ thống: (a) Yêu cầu quét vân tay; (b) Yêu cầu nhập số điện thoại đã đăng ký; (c) Yêu cầu điền mã OTP gửi về số điện thoại; (d) Yêu cầu nhập mật khẩu lớp 1; (e) Yêu cầu nhập mật khẩu lớp 2; (f) Cảnh báo nhập sai; (g) Cảnh báo truy cập trái phép; (h) Thông tin về cửa được mở khoá thành công; (i) Thông báo cửa sẽ được khoá lại sau 10 giây

Các thông báo trên LCD về yêu cầu quét vân tay, nhập số điện thoại đã đăng ký, điền mã OTP, nhập mật khẩu truy cập lớp 1, mật khẩu truy cập lớp 2, yêu cầu nhập lại thông tin, cảnh báo truy cập trái phép, hiển thị thông tin về cửa được mở, thông báo về tình trạng cửa sẽ khoá lại sau 10 giây, lần lượt được trình bày ở Hình 4 (a), Hình 4 (b), Hình 4 (c), Hình 4 (d), Hình 4 (e), Hình 4 (f), Hình 4 (g), Hình 4 (h), Hình 4 (i).

4. Kết luận

Hệ thống khoá điện tử được tác giả thiết kế đã sử dụng một loạt các lớp bảo mật để đảm bảo tính an toàn và bảo mật cho người sử dụng. Việc kết hợp các phương pháp mã hoá từ bàn phím, mật khẩu dùng 1 lần OTP và vân tay đã tạo ra một hệ thống khoá điện tử đa lớp, nâng cao đáng kể tính bảo mật và khả năng chống lại các hình thức tấn công khác nhau. Hệ thống khoá điện tử này cũng được thiết kế để đáp ứng các yêu cầu nhập liệu nghiêm ngặt và truy cập cần thiết để bảo vệ thông tin và tài sản của người sử dụng. Ngoài ra, hệ thống còn cung cấp cảnh báo trái phép, giúp người dùng phát hiện và ngăn chặn các hành vi không hợp lệ hoặc nguy hiểm đối với khu vực lắp đặt thiết bị. Kết quả mô phỏng trên Proteus cho thấy hoạt động của khoá bảo mật đa lớp thoả mãn yêu cầu thiết kế đặt ra và tuân theo thuật toán điều khiển.

Hệ thống có thể được nghiên cứu và phát triển thêm khi sử dụng các công nghệ sinh trắc học như mống mắt, quét 3D khuôn mặt sử dụng LiDAR,... Các kỹ thuật này kết hợp với vân tay vừa tăng khả năng bảo mật vừa khiến cho quá trình mở khoá được nhanh chóng, tiện lợi.

TÀI LIỆU THAM KHẢO/ REFERENCES

- [1] S. Kavde, R. Kavde, S. Bodare, and G. Bhagat, "Smart digital door lock system using Bluetooth technology," *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2017, pp. 1-4.
- [2] N. G. Raju, J. Vikas, S. Appaji, and A. S. Hanuman, "Smart Lock Controlled using Voice Call," *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2018, pp. 97-103.
- [3] S. R. Pinjala and S. Gupta, "Remotely Accessible Smart Lock Security System with Essential Features," *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, Chennai, India, 2019, pp. 44-47.
- [4] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, "Development of Web-Based Smart Security Door Using QR Code System," *2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Shah Alam, Malaysia, 2020, pp. 13-17.
- [5] R. Priyakanth, N. M. S. Krishna, G. Karanam, M. L. Prassna, S. Baby Poojitha, and J. Mounika, "IoT Based Smart Door Unlock and Intruder Alert System," *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2021, pp. 6-11.
- [6] D. Aswini, R. Rohindh, K. S. Manoj Ragavendhara, and C. S. Mridula, "Smart Door Locking System," *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, Coimbatore, India, 2021, pp. 1-5.
- [7] P. Prabakaran, I. Sumedha, L. Umashankar, M. M. Rai, and M. Swathi, "Smart Door Lock System For The Elderly And Disabled," *2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C)*, Bangalore, India, 2021, pp. 229-233.
- [8] D-Robotics UK, "DHT11 Humidity & Temperature Sensor," DHT11 sensor datasheet, 2010.