DOI: 10.64302/joshusc.v30n1e.1330

HỆ THỐNG KIỂM SOÁT CỬA RA VÀO BẢO MẬT HAI LỚP SỬ DỤNG CAMERA NHẬN DIỆN KHUÔN MẶT VÀ THẺ RFID

Nguyễn Lê Đăng Quang[1], Nguyễn Công Chí Hùng[1], Hồ Thanh Thiên[2], Hồ Đức Tâm Linh[1*]

[1]Khoa Điện, Điện tử và Công nghệ vật liệu, Trường Đại học Khoa học, Đại học Huế

[2]Phòng Tài chính, Hậu cần, Kỹ thuật, Trung tâm giáo dục quốc phòng và an ninh, Đại học Huế

*Email: hdtlinh@husc.edu.vn

Ngày nhận bài: 21/4/2025; ngày hoàn thành phản biện: 9/5/2025; ngày duyệt đăng: 16/5/2025

TÓM TẮT

Bài báo đề xuất một mô hình đơn giản nhận điện khuôn mặt HOG và SVM, kết hợp với hệ thống nhận dạng bằng sóng vô tuyến (RFID) trên nền tảng Raspberry Pi để mở hệ thống cửa. Hệ thống này không chỉ hỗ trợ nhận diện và xác minh danh tính người dùng một cách tự động khi ra vào cửa, mà còn lưu trữ hình ảnh, dữ liệu thời gian và sự kiện để phục vụ công tác quản lý và truy xuất sau này. Từ kết quả đạt được chỉ ra rằng, đối với các hệ thống với cấu hình phần cứng thiết bị hạn chế thì mô hình thuật toán nhận diện khuôn mặt HOG và SVM là lựa chọn tối ưu nhất.

Từ khóa: Raspberry Pi 4, Facial Recognition, MySQL, RFID

1. TỔNG QUAN

Trong bối cảnh phát triển nhanh chóng của công nghệ thông tin và các ứng dụng trí tuệ nhân tạo, việc ứng dụng các phương pháp bảo mật bằng sinh trắc học vào việc kiểm soát truy cập đang ngày càng trở nên cấp thiết trong đời sống con người. Trong số đó, nhận diện khuôn mặt được đánh giá là một trong những phương pháp xác thực sinh trắc học tiềm năng nhất [1].

Một số kỹ thuật kiểm soát ra vào cửa truyền thống như chìa khóa cơ học, khóa số vẫn còn tồn tại nhiều hạn chế đáng kể, bao gồm không thể ghi lại lịch sử truy cập, thiếu linh hoạt và dễ bị sao chép, thất lạc hoặc làm giả. Trước những hạn chế đó, công nghệ nhận diện khuôn mặt đã nổi lên như một phương pháp xác thực sinh trắc học hiệu quả. Nhờ vào tính tiện lợi và khả năng tương thích tốt với các hệ thống camera giám sát

sẵn có, công nghệ này ngày càng được ứng dụng rộng rãi trong các hệ thống kiểm soát truy cập hiện đại [2].

Thách thức lớn nhất là làm sao triển khai phần mềm nhận diện khuôn mặt một cách hiệu quả trên các nền tảng phần cứng giá rẻ, tiêu thụ điện năng thấp như Raspberry Pi, đặc biệt khi hệ thống cần hoạt động hoàn toàn ngoại tuyến để đảm bảo tính riêng tư và an toàn dữ liệu mà không phụ thuộc vào điện toán đám mây. Bài báo này sẽ đề xuất một phương án giải quyết thách thức đó bằng cách thiết kế và xây dựng một hệ thống mở khóa cửa tự động sử dụng thuật toán nhận diện khuôn mặt được tích hợp trực tiếp trên Raspberry Pi 4.

Tuy nhiên, trong điều kiện thực tế, hệ thống nhận diện khuôn mặt có thể gặp phải một số hạn chế như ánh sáng yếu, góc mặt không phù hợp hoặc khuôn mặt bị che khuất, dẫn đến giảm độ chính xác trong việc xác thực người dùng. Để tăng cường độ tin cậy và tính linh hoạt cho hệ thống, việc kết hợp thêm công nghệ thẻ RFID là cần thiết. RFID hoạt động ổn định trong nhiều điều kiện môi trường, không phụ thuộc vào hình ảnh và có tốc độ nhận dạng nhanh. Việc kết hợp hai công nghệ bảo mật này sẽ giúp hệ thống hoạt động ổn định ngay cả khi không có kết nối Internet, đồng thời đảm bảo khả năng mở rộng, chi phí triển khai thấp và thời gian phản hồi đủ nhanh cho các ứng dụng thực tế.

Từ những phân tích trên, có thể thấy rằng việc kết hợp giữa công nghệ nhận diện khuôn mặt, RFID và nền tảng nhúng như Raspberry Pi mang lại một giải pháp kiểm soát truy cập bảo mật, thông minh, linh hoạt và tiết kiệm chi phí [3]. Hệ thống này có tiềm năng mở rộng rất lớn, không chỉ ứng dụng cho nhà riêng mà còn có thể dùng trong các môi trường doanh nghiệp hoặc cơ sở yêu cầu an ninh cao. Do đó, mô hình này không chỉ là một giải pháp khả thi trong hiện tại, mà còn là nền tảng hứa hẹn cho các ứng dụng bảo mật thông minh trong tương lai.

2. KHẢO SÁT CÁC TÀI LIỆU LIÊN QUAN

2.1. Tìm hiểu về các kỹ thuật nhận diện khuôn mặt

Trong nghiên cứu [4], các tác giả đã tổng hợp lịch sử phát triển và phân loại các phương pháp nhận diện khuôn mặt, nhấn mạnh quá trình chuyển đổi từ phương pháp truyền thống sang các kỹ thuật dựa trên học sâu. Một trong những phương pháp nền tảng tiêu biểu là Eigenfaces. Thuật toán này ứng dụng kỹ thuật phân tích thành phần chính để giảm số chiều dữ liệu ảnh khuôn mặt, chỉ giữ lại các đặc trưng biến thiên quan trọng nhất gọi là "eigenfaces". Khi nhận diện, ảnh khuôn mặt mới sẽ được biểu diễn bằng các giá trị dựa trên tập eigenfaces này, sau đó so sánh với dữ liệu huấn luyện để xác định danh tính. Eigenfaces nổi bật với ưu điểm tính toán nhanh, tiết kiệm bộ nhớ và phù hợp với thiết bị thiếu tài nguyên phần cứng, được ứng dụng rộng rãi trong các hệ

thống quản lý danh tính, điểm danh phòng thí nghiệm hoặc kiểm soát truy cập quy mô nhỏ, nơi nhu cầu về tốc độ cao hơn độ chính xác tuyệt đối.

Một phương pháp khác có tên gọi LBPH (Local Binary Patterns Histogram) khai thác đặc trưng cục bộ bằng cách chia khuôn mặt thành nhiều vùng nhỏ, sau đó với mỗi vùng thực hiện mã hóa các pixel thành chuỗi nhị phân [5]. Sau cùng, biểu đồ phân phối các mã LBP được ghép tạo thành vector đặc trưng đại diện cho toàn bộ khuôn mặt. LBPH có ưu điểm nổi bật là khả năng ổn định trong điều kiện ánh sáng thay đổi hoặc biểu cảm khuôn mặt đa dạng. Điều này giúp LBPH được ứng dụng phổ biến trong các hệ thống điểm danh tự động cho lớp học, công sở hoặc cửa ra vào, đặc biệt tại môi trường có nhiều sự biến thiên ánh sáng và vị trí camera không cố định. Bài báo [3], đã tổng kết kết quả thử nghiệm cho thấy LBPH đảm bảo hiệu quả nhận diện tốt, đồng thời dễ tích hợp lên các nền tảng nhúng.

Trong bài nghiên cứu thực nghiệm [6], một nhóm các tác giả gồm Oscar Deniz, Gloria Bueno, Jesus Salido và Fernando de la Torre đã trình bày chi tiết về đặc trưng của phương pháp HOG (Histogram of Oriented Gradients). HOG thực hiện việc chia nhỏ ảnh thành các khối nhỏ (cells), sau đó tính toán hướng và cường độ của gradient tại từng pixel, từ đó xây dựng biểu đồ phân bố hướng cạnh trong từng vùng. Đặc trưng này giúp HOG nhận diện tốt các đường nét, cạnh và hình khối chủ đạo của khuôn mặt mà không phụ thuộc vào độ tương phản hoặc màu sắc cụ thể. Nhờ sử dụng vector đặc trưng dạng histogram nhỏ gọn, HOG có thể thực thi nhanh trên bộ vi xử lý ARM hoặc các thiết bị nhúng thiếu GPU, trong khi vẫn đủ mạnh để phân biệt các khuôn mặt quen thuộc. Phương pháp này do đó được ứng dụng rộng rãi cho các hệ thống kiểm soát truy cập cửa chính, chấm công tự động quy mô vừa và nhỏ hoặc các trạm kiểm soát thông minh tại những dự án không yêu cầu đầu tư phần cứng đắt tiền.

Các phương pháp học sâu, đặc biệt với mô hình CNN (Convolutional Neural Networks), đã mang lại bước tiến vượt bậc cho nhận diện khuôn mặt nhờ khả năng tự động trích xuất và học tập các đặc trưng phức tạp từ dữ liệu ảnh lớn. Theo tổng kết [7], bài báo chỉ ra rằng học sâu giúp tăng đáng kể độ chính xác trong bài toán nhận diện khuôn mặt, tiến gần hơn với khả năng của con người nhờ tận dụng khả năng tự động học đặc trưng từ dữ liệu lớn, và đã nhiều lần được kiểm chứng trên các tập dữ liệu chuẩn như LFW, AFLW, Multi-PIE. Tuy nhiên, điều kiện tiên quyết của học sâu là yêu cầu phần cứng mạnh về GPU, dung lượng RAM lớn, cùng dữ liệu huấn luyện phong phú. Nhược điểm này sẽ gia tăng chi phí triển khai, bảo trì và sự phức tạp về phần mềm, dẫn đến khó áp dụng hiệu quả cho các hệ thống nhúng nhỏ gọn như Raspberry Pi, đặc biệt khi yêu cầu hoạt động offline, ổn định lâu dài và chi phí tối ưu. Vì vậy, việc lựa chọn thuật toán cũng cần phải cân nhắc giữa độ chính xác và khả năng triển khai thực tế.

2.2. So sánh và lựa chọn công nghệ phù hợp với phần cứng hiện có

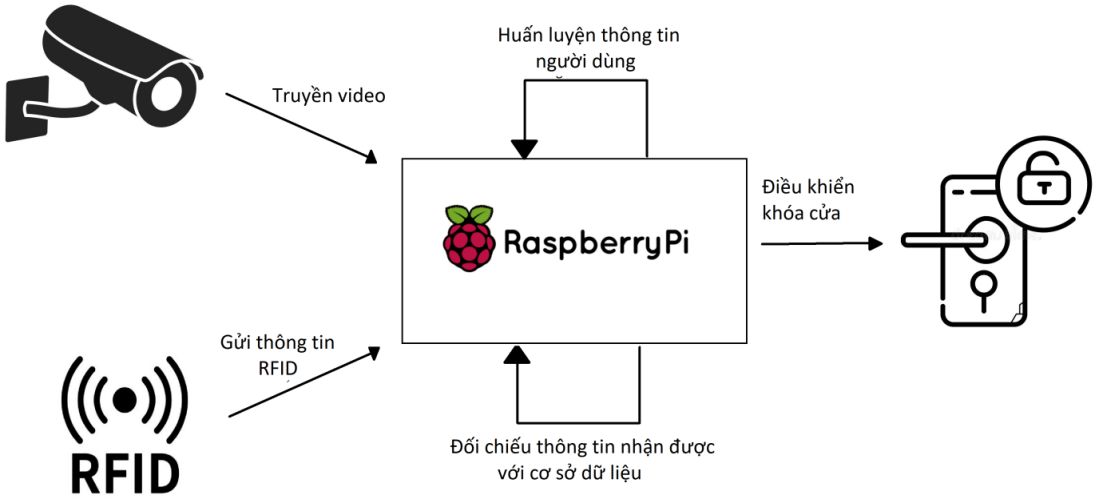
Trong các thuật toán nhận diện khuôn mặt, HOG (Histogram of Oriented

Gradients) kết hợp SVM (Support Vector Machine) được đánh giá là lựa chọn tối ưu cho Raspberry Pi nhờ khả năng cân bằng giữa độ chính xác và hiệu năng trên phần cứng hạn chế. So với các phương pháp chi phí thấp như Eigenfaces, HOG cho kết quả ổn định hơn khi môi trường ánh sáng và vị trí khuôn mặt thay đổi, đồng thời hạn chế lỗi nhận diện giả. Ngược lại, các mô hình dựa trên mạng nơ-ron sâu (CNN) dù đạt độ chính xác rất cao nhưng lại đòi hỏi GPU mạnh và dung lượng bộ nhớ lớn, vượt quá năng lực xử lý của Raspberry Pi trong các ứng dụng hoạt động offline, chi phí thấp. Do đó, giải pháp HOG được khuyến nghị áp dụng vì phù hợp với tiêu chí tối ưu chi phí, hiệu quả xử lý và độ ổn định cho hệ thống nhúng nhỏ gọn.

3. THIẾT KẾ HỆ THỐNG

3.1. Hoạt động của hệ thống

a. Sơ đồ hoạt động của hệ thống

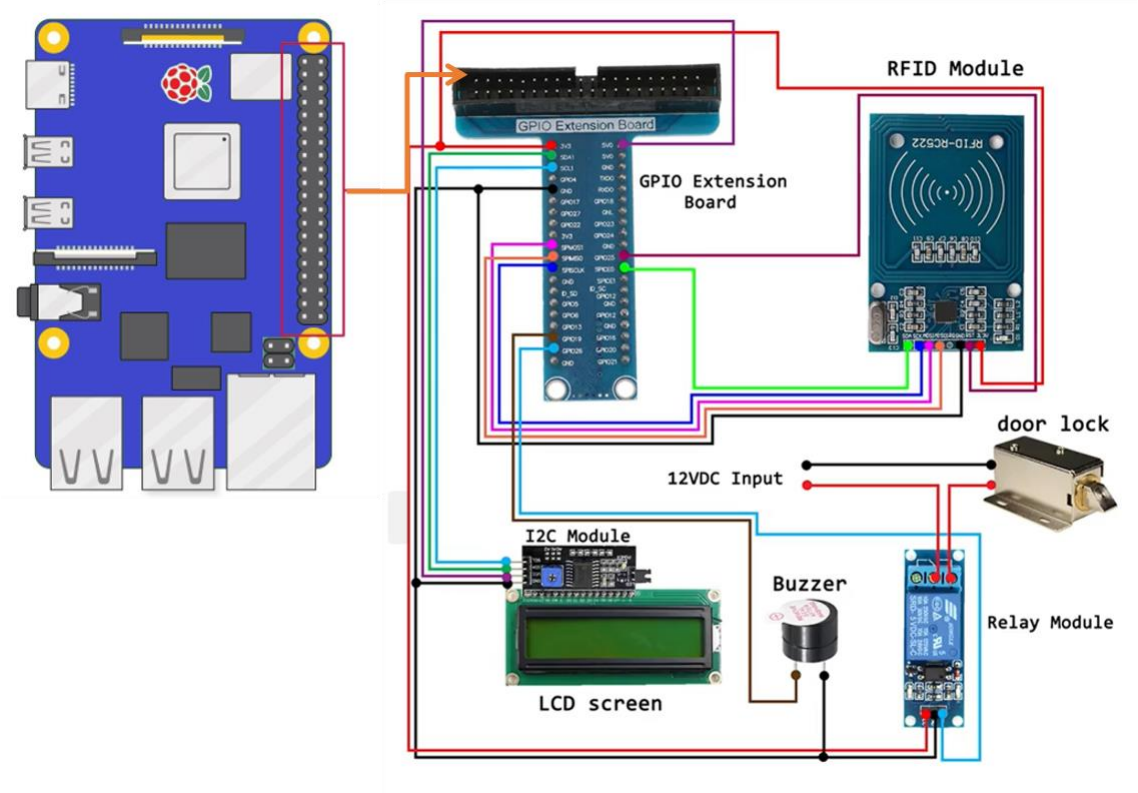


Hình 1. Sơ đồ hoạt động của hệ thống

Hệ thống bắt đầu với hai nguồn đầu vào chính: camera giám sát và thiết bị đọc thẻ RFID (Hình 1). Camera sẽ liên tục truyền dữ liệu video đến Raspberry Pi. Tại đây, hệ thống xử lý hình ảnh để phát hiện và nhận diện khuôn mặt người dùng. Đồng thời, thiết bị đọc RFID cũng gửi dữ liệu mã thẻ đến Raspberry Pi, đây là một phương thức xác thực thứ hai.

Raspberry Pi giữ vai trò là trung tâm xử lý. Nó tiến hành đối chiếu thông tin khuôn mặt và RFID nhận được với cơ sở dữ liệu đã được huấn luyện từ trước. Việc huấn luyện thông tin người dùng (bao gồm ảnh khuôn mặt và mã thẻ hợp lệ) cũng được thực hiện và lưu trữ ngay trên Raspberry Pi hoặc thông qua hệ thống quản lý dữ liệu đi kèm.

b. Kết nối phần cứng và lựa chọn phần mềm



Hình 2. Sơ đồ kết nối phần cứng các thiết bị

Về phần cứng, hệ thống triển khai các kết nối linh hoạt thông qua các chân GPIO đa năng của Raspberry Pi (Hình 2). Kết nối module RFID với GPIO qua bus SPI và đấu dây chính xác các chân (RST, MISO, MOSI, SCK, NSS, GND, 3.3V), đầu đọc RFID hoạt động qua giao thức SPI, đáp ứng yêu cầu tương tác nhanh và ổn định. Camera được kết nối qua cổng USB hoặc giao diện CSI tùy theo loại sử dụng. Lắp module LCD bằng dây I2C vào chân SDA/SCL và cấp nguồn. Đấu dây nguồn và dây điều khiển khóa điện với relay (dây COM, NO của relay tới dây điện của khóa, GND nối với board), bộ điều khiển relay đảm nhận việc điều khiển lưu thông dòng điện cho khóa điện nhằm thực hiện chức năng đóng/mở cửa.

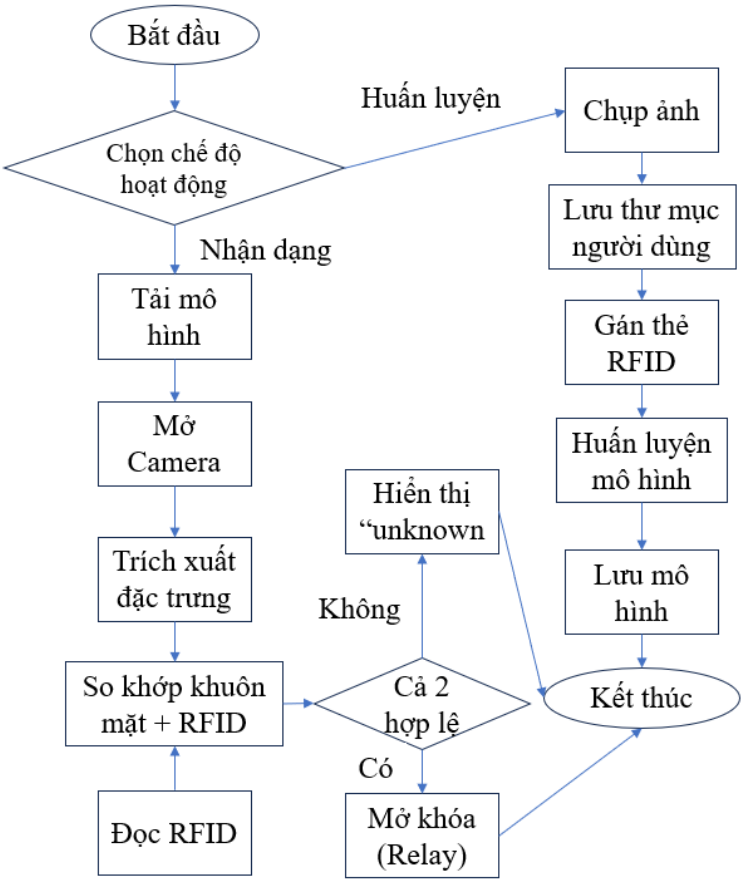
Về phần mềm, hệ thống vận hành trên nền tảng hệ điều hành Raspberry Pi OS (được phát triển dựa trên Debian Linux). Hệ sinh thái phần mềm tích hợp các thư viện chính như OpenCV phục vụ xử lý ảnh, thư viện face_recognition chuyên dùng cho nhận diện khuôn mặt dựa trên thuật toán HOG, RPi.GPIO để quản lý điều khiển chân GPIO, cùng các thư viện hỗ trợ xử lý và giao tiếp với đầu đọc RFID cũng như màn hình hiển thị LCD. Các phần mềm điều khiển hoạt động theo mô-đun, bao gồm các script có các chức năng như sau: script dùng để chụp và lưu trữ ảnh khuôn mặt (chia thư mục theo tên người dùng); script để thu nhận mã số thẻ RFID và gán với từng người dùng; script huấn luyện hệ thống nhận diện khuôn mặt với dữ liệu đã thu thập được, có chức năng trích xuất đặc trưng khuôn mặt với HOG và lưu vector mã hóa vào dữ liệu hệ thống;

script để vận hành hệ thống nói chung ví dụ như hiển thị lên LCD, so sánh dữ liệu khuôn mặt và RFID, điều khiển chốt khóa cửa.

3.2. Lưu đồ thuật toán và kết quả hoạt động

a. Lưu đồ thuật toán

Hình 3 trình bày lưu đồ thuật toán mô tả nguyên lý hoạt động của hệ thống. Ban đầu, hệ thống kiểm soát truy cập bằng nhận diện khuôn mặt và RFID hoạt động theo hai chế độ chính: chế độ huấn luyện (Training Mode) và chế độ nhận dạng (Recognition Mode). Trong chế độ huấn luyện, người dùng được hướng dẫn cung cấp dữ liệu khuôn mặt thông qua camera tích hợp. Mỗi lần nhấn phím cách (Space), một ảnh được chụp và tự động lưu trữ vào thư mục mang tên người dùng trong cây thư mục. Các thư mục con này đại diện cho nhãn phân loại tương ứng, phục vụ làm đầu vào cho giai đoạn huấn luyện mô hình.



Hình 3. Lưu đồ thuật toán nguyên lý hoạt động của hệ thống

Sau khi thu thập ảnh, hệ thống sử dụng các thư viện như face_recognition hoặc Dlib để phát hiện khuôn mặt trong từng ảnh, trích xuất vector đặc trưng (face encoding) và gán nhãn tương ứng. Tập hợp các vector này được sử dụng để huấn luyện mô hình nhận diện khuôn mặt. Mô hình đầu ra sau huấn luyện được lưu lại dưới dạng tệp .pkl

hoặc .dat, phục vụ cho quá trình nhận dạng thời gian thực sau này.

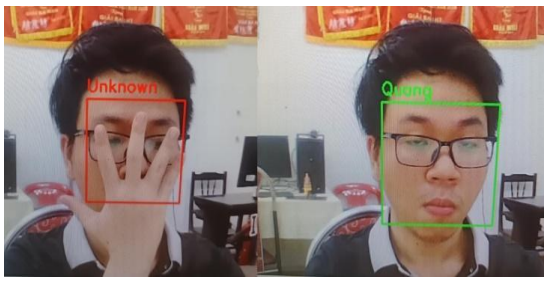
Trong chế độ nhận dạng, hệ thống tải mô hình đã huấn luyện và kích hoạt camera để thu thập ảnh liên tục theo thời gian thực. Mỗi khung hình được xử lý nhằm phát hiện và mã hóa khuôn mặt thành vector đặc trưng, sau đó so khớp với các vector đã được lưu trong cơ sở dữ liệu MySQL. Đồng thời, hệ thống đọc thẻ RFID thông qua module giao tiếp UART như RDM6300 để xác định mã thẻ người dùng. Việc xác thực chỉ được coi là hợp lệ khi cả khuôn mặt và mã RFID đều trùng khớp với dữ liệu đã đăng ký. Điều này cho phép triển khai cơ chế xác thực kép (two-factor authentication), giúp nâng cao mức độ bảo mật trong môi trường triển khai thực tế.

Khi cả hai điều kiện được thỏa mãn, Raspberry Pi sẽ gửi tín hiệu thông qua chân GPIO để kích hoạt ro-le điều khiển khóa điện tử (thường là loại Normally Open). Khóa sẽ mở trong một khoảng thời gian định sẵn (ví dụ 5 giây) trước khi tự động đóng lại. Toàn bộ quy trình điều khiển thiết bị ngoại vi được lập trình bằng Python, sử dụng các thư viện như RPi.GPIO hoặc gpiozero để đảm bảo khả năng mở rộng, dễ bảo trì và tích hợp với các chức năng nâng cao khác trong tương lai như ghi lịch sử truy cập hoặc phân quyền người dùng. Hệ thống cũng hiển thị thông tin phản hồi thời gian thực như tên người dùng, trạng thái xác thực, hoặc cảnh báo "Unknown" nếu phát hiện truy cập trái phép.

b. Kết quả sau khi vận hành hệ thống

Quy trình bắt đầu khi người dùng tiến tới khu vực mà camera tích hợp (Pi Camera hoặc webcam USB) có thể nhận diện được, đồng thời đưa thẻ RFID vào vùng đọc của đầu đọc RC522, kết nối với cổng UART của Raspberry Pi. Trong điều kiện hoạt động bình thường, hệ thống luôn xác thực được 100% khuôn mặt được lưu trữ trong cơ sở dữ liệu và tính hợp lệ của mã thẻ RFID. Lúc này khóa cửa sẽ được mở. Hệ thống được thiết lập sau 30 giây sau cửa sẽ tự động khóa lại nếu không có tác động gì ở bước tiếp theo.

Dưới đây là hình ảnh xác thực đúng khi nhận diện khuôn mặt và đọc đúng thẻ RFID, chốt cửa được mở.



Hình 4. Chương trình nhận diện đúng khuôn mặt

Hình 5. Màn hình LCD hiển thị đã nhận diện thành công khuôn mặt và thẻ RFID, khóa điện cho phép mở cửa.

3.3. Thảo luận trường hợp xác thực người dùng không thành công

Trong quá trình vận hành hệ thống kiểm soát truy cập sử dụng xác thực kép bằng nhận diện khuôn mặt và thẻ RFID, một loạt các tình huống xác thực không hợp lệ có thể xảy ra, phản ánh tính thực tiễn và khả năng ứng phó của hệ thống trước các trạng thái lỗi hoặc truy cập không được ủy quyền. Ba tình huống lỗi phổ biến nhất có thể được liệt kê như sau: thẻ RFID không hợp lệ, hoặc nhận diện khuôn mặt không khớp với dữ liệu đã huấn luyện, hoặc người dùng không quét thẻ RFID khi thực hiện xác thực.

Trường hợp thứ nhất là khi người dùng quét một thẻ RFID không nằm trong cơ sở dữ liệu hợp lệ (ví dụ: ID không tồn tại trong bảng user_rfid). Hệ thống lập tức phát hiện sự sai lệch này thông qua truy vấn SQL, từ đó đưa ra cảnh báo và ngăn chặn bước xác thực khuôn mặt tiếp theo. Điều này giúp loại bỏ những trường hợp sử dụng thẻ giả mạo hoặc thẻ không được cấp phát chính thức.

Trường hợp thứ hai xảy ra khi người dùng sở hữu thẻ RFID hợp lệ nhưng khuôn mặt được nhận diện không khớp với mẫu đã lưu. Trong quy trình xử lý, hệ thống sau khi xác thực RFID thành công sẽ truy xuất ảnh từ camera và trích xuất vector đặc trưng khuôn mặt trong thời gian thực. Vector này sau đó được so sánh với các vector đã lưu trong tệp huấn luyện hoặc cơ sở dữ liệu. Nếu không đạt được độ tương đồng theo ngưỡng định sẵn (khoảng cách Euclidean > 0.6), hệ thống sẽ từ chối xác thực và không kích hoạt Rơ-le mở khóa. Tình huống này thường phản ánh các rủi ro như người mạo danh, chất lượng ảnh kém hoặc điều kiện ánh sáng không đảm bảo.

Trường hợp thứ ba là khi người dùng chỉ trình diện khuôn mặt trước camera mà không quét thẻ RFID. Điều này có thể xảy ra do thiếu nhận thức về quy trình hoặc cố tình lách hệ thống. Trong thiết kế hiện tại, quy trình xác thực chỉ được khởi động đầy đủ khi cả hai yếu tố (RFID và khuôn mặt) được cung cấp. Do đó, hệ thống sẽ không tiến hành nhận diện khuôn mặt nếu không có tín hiệu đầu vào từ bộ đọc RFID, nhằm giảm thiểu rủi ro bị khai thác bằng ảnh giả hoặc video giả mạo (spoofing).

Tổng hợp các tình huống trên cho thấy tính nghiêm ngặt và khả năng xử lý lỗi của hệ thống xác thực kép. Kết quả đánh giá chỉ ra rằng, thời gian nhận diện trung bình hình ảnh người trước máy quét và đưa ra phản hồi mở cửa là 0.5s, tỉ lệ nhận diện chính xác 99% trên tập dữ liệu phân biệt 10 người và tỉ lệ từ chối sai nhỏ hơn 0.01%.

Bằng cách phân tích và phản ứng riêng biệt cho từng dạng sai lệch, hệ thống không chỉ đảm bảo tính bảo mật mà còn tăng khả năng chẩn đoán lỗi và nâng cao trải nghiệm người dùng thông qua phản hồi rõ ràng và kịp thời. Những kịch bản này đóng vai trò quan trọng trong việc kiểm chứng hiệu quả của hệ thống trước khi triển khai trong môi trường thực tế có yêu cầu bảo mật cao.

4. KẾT LUẬN

Bài báo này đã đề xuất và triển khai một hệ thống kiểm soát truy cập bảo mật hai lớp sử dụng công nghệ nhận diện khuôn mặt kết hợp RFID trên nền tảng Raspberry Pi. Thông qua việc tích hợp giữa sinh trắc học (biometric authentication) và xác thực vật lý (RFID), hệ thống không chỉ đảm bảo tính tiện lợi, chi phí thấp mà còn nâng cao đáng kể mức độ an toàn và khả năng ứng dụng trong thực tế. Các phân tích thực nghiệm đã cho thấy mô hình HOG + SVM là lựa chọn phù hợp nhất trong bối cảnh phần cứng hạn chế, đáp ứng tốt yêu cầu về độ chính xác, tốc độ xử lý và khả năng triển khai đơn giản. Tổng thể, kết quả đạt được trong nghiên cứu này cho thấy tiềm năng mở rộng ứng dụng của hệ thống không chỉ giới hạn trong quy mô gia đình hoặc văn phòng nhỏ, mà còn có thể thích nghi với các môi trường yêu cầu kiểm soát truy cập chặt chẽ hơn như phòng máy chủ, phòng thí nghiệm, trường học hoặc doanh nghiệp vừa và nhỏ. Trong tương lai, hệ thống có thể được nâng cấp để hỗ trợ thêm các yếu tố xác thực như mã PIN, vân tay hoặc tích hợp AI để phát hiện hành vi bất thường, hướng tới xây dựng các mô hình kiểm soát an ninh thông minh và toàn diện hơn.

TÀI LIỆU THAM KHẢO

[1] Rahaman, Md, & Noman, Md. Abdullah & Ali, Muhammad & Rahman, Mahfuzur, "Design and Implementation of a Face Recognition Based Door Access Security System using Raspberry Pi". 8. (2021).

[2] Suman Pandit, Shakyanand Kamble, Vinit Vasudevan, "Home Security Alarm System Using Arduino" Vidyalankar Institute of Technology, Wadala (E), Mumbai – 400 037, 7, 2024.

[3] Praveen Kumar, Umesh Chandra Pati ' IoT Based Monitoring and Control of Appliances for Smart Home' IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India, (pg - 1145 to 1150)

[4] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, Chung-Horng Lung 'Smart Home: Integrating Internet of Things with Web Services and Cloud Computing' 2013 IEEE International Conference on Cloud Computing Technology and Science, (pg -317 to 320).

[5] Leyla G. Muradkhanli1, Eshgin A. Mammadov2, "Real-Time Face Recognition on Raspberry Pi Using HOG and SVM" – arXiv.org, arXiv:1909.03461

[6] Elnozahy, Seifeldin Sherif Fathy Ali, Senthill C. Pari, and Lee Chu Liang. 2025. "Raspberry Pi-Based Face Recognition Door Lock System" *IoT* 6, no. 2: 31. https://doi.org/10.3390/iot6020031

[7] Battaglia, Filippo & Iannizzotto, Giancarlo & Lo Bello, Lucia, "A biometric authentication system based on face recognition and RFID tags". 13. 2024.

DOOR ACCESS CONTROL SYSTEM WITH DUAL-LAYER SECURITY USING FACIAL RECOGNITION CAMERA AND RFID CARDS

Nguyen Le Dang Quang[1], Le Cong Chi Hung[1],
Ho Thanh Thien[2], Ho Duc Tam Linh[1*]

[1]Faculty of Electronics, Electrical Engineering and Material Technology,
University of Sciences, Hue University

[2]Department of Finance, Logistics and Engineering,
Defense Education Center of Hue University

*Email: hdtlinh@husc.edu.vn

ABSTRACT

The paper presents a face recognition model employing Histogram of Oriented Gradients (HOG) features and a Support Vector Machine (SVM) classifier, integrated with a radio-frequency identification (RFID) system on the Raspberry Pi platform for door access control. The proposed system enables automatic identification and authentication of users during entry and exit, while simultaneously recording images, timestamps, and event logs to support subsequent management and data retrieval. The results show that for systems with limited hardware configurations, the HOG and SVM face recognition model is the most optimal choice.

Keywords: Raspberry Pi 4, Facial Recognition, MySQL, RFID.