

# Nghiên cứu phát triển hệ thống xác thực khuôn mặt 2 yếu tố bảo mật sử dụng công nghệ mã F-QR ẩn trên thẻ ID bằng laser 1064 nm và AI camera

Bành Quốc Tuấn<sup>1\*</sup>, Lê Hồng Minh<sup>2</sup>, Lưu Hoàng Đạt<sup>1</sup>, Ngô Hải Long<sup>1</sup>,  
Cao Khắc Thiện<sup>1</sup>, Đỗ Việt Hoàng<sup>1</sup>, Lê Văn Bình<sup>1</sup>

<sup>1</sup>Phòng Thí nghiệm nghiên cứu phát triển ứng dụng fiber laser, Viện Ứng dụng Công nghệ

<sup>2</sup>Trung tâm Vi điện tử và Tin học, Viện Ứng dụng Công nghệ

Ngày nhận bài 1/7/2022; ngày chuyển phản biện 5/7/2022; ngày nhận phản biện 20/7/2022; ngày chấp nhận đăng 25/7/2022

## **Tóm tắt:**

Hệ thống xác thực khuôn mặt sử dụng 2 yếu tố bảo mật là mã F-QR (face QR) ẩn in trên thẻ ID và nhận diện khuôn mặt bằng AI camera được trình bày trong nghiên cứu này. Mã F-QR mang đặc tính gương mặt được tạo ra bởi sự kết hợp của các công nghệ xử lý xác định khuôn mặt, trích xuất đặc trưng khuôn mặt và tạo mã QR. Mã F-QR được in lên thẻ nhựa ID bằng công nghệ in laser sợi quang bước sóng 1064 nm. Thẻ ID được chế tạo bằng vật liệu đặc biệt, trong đó có lớp vật liệu lọc cho phép bước sóng 1064 nm laser truyền qua trong khi cản các ánh sáng nhìn thấy, do đó mã F-QR khi in lên thẻ sẽ không bị nhìn thấy bằng mắt người hay các đầu đọc mã QR thông thường. Xác thực khuôn mặt được triển khai bằng việc sử dụng đầu đọc mã F-QR ẩn chuyên dụng kết hợp với AI camera quyết định độ tương tự Cosine giữa 2 vector đặc trưng của khuôn mặt nhằm đưa ra quyết định chính xác cho việc xác thực.

**Từ khóa:** AI camera, face-ID, ID card, laser quang sợi, QR code.

## **Chỉ số phân loại:** 2.2

## **Mở đầu**

Xác thực người là một trong những yêu cầu quan trọng của hệ thống thị giác máy tính trong nhiều ứng dụng khác nhau như điện thoại thông minh [1], ATM [2], hệ thống chăm sóc sức khỏe cộng đồng [3], hệ thống cấp bằng lái xe [4], giám sát an ninh [5], xác thực hộ chiếu [6]... Xác thực người có thể thông qua một số sinh trắc học [7] có sẵn của con người như mắt, móng tay, vân tay, giọng nói, chữ ký, khuôn mặt... Trong đó, khuôn mặt là một yếu tố thuận tiện để phát triển ứng dụng xác thực người bởi nó không yêu cầu sự phối hợp hành động trực tiếp của con người như những sinh trắc học khác. Nhiều nghiên cứu về xác thực khuôn mặt đã được đưa ra với mục tiêu nâng cao độ chính xác [8-11], trong đó có giải pháp về nâng cao giải thuật [10], giải pháp xác thực 2 yếu tố dùng RFID [8, 9]. Độ chính xác về xác thực có thể lên tới 99% mang đến sự an toàn trong các ứng dụng thực tế. Tuy nhiên, việc triển khai các hệ thống xác thực trên yêu cầu hệ thống cơ sở dữ liệu và máy chủ đủ lớn để lưu trữ và phân tích dữ liệu. Hệ thống nhận diện khuôn mặt cần phải kết nối internet để truy cập vào cơ sở dữ liệu, do đó không tránh khỏi các vấn đề về nghẽn mạng, mất mạng, rủi ro về rò rỉ thông tin trên server cũng như trên thẻ RFID, mất thời gian và chi phí để triển khai hệ thống.

Trong nghiên cứu này, chúng tôi đưa ra phương pháp mới về hệ thống xác thực khuôn mặt sử dụng 2 yếu tố bảo mật là mã QR mang đặc tính của khuôn mặt, được in ẩn trên thẻ ID bằng laser sợi quang 1064 nm và nhận diện khuôn mặt bằng AI camera với các giải thuật xác định khuôn mặt DNN (Deep neural network) [12], biểu diễn khuôn mặt FaceNet [13], xác thực khuôn mặt bằng độ

tương tự Cosine [14]. Dữ liệu khuôn mặt của người dùng sau khi được xử lý bằng các phương pháp DNN và FaceNet thay vì được lưu trữ trên server như các giải pháp truyền thống sẽ được mã hóa thành mã F-QR 2 chiều và lưu trữ trên thẻ ID của người dùng. Thẻ ID này được chế tạo nhiều lớp, bằng vật liệu đặc biệt cho phép sử dụng laser bước sóng 1064 nm để in thông tin lên lớp bên dưới của bề mặt thẻ. Do đó thông tin in lên thẻ là vĩnh viễn, không thể bị xóa, mờ hay bị thay đổi. Bên trong thẻ cũng có một lớp vật liệu lọc đặc biệt, hoạt động như một bộ lọc quang cho phép bước sóng 1064 nm đi qua trong khi cản toàn bộ bước sóng trong vùng nhìn thấy 400-700 nm. Khi mã F-QR được in lên thẻ, mã sẽ hoàn toàn bị ẩn sau lớp vật liệu lọc khiến mắt người, cũng như các đầu đọc mã QR thông thường không thể đọc để lấy thông tin, tránh việc thẻ bị sao chép làm giả. Trong nghiên cứu này, chúng tôi cũng phát triển, chế tạo đầu đọc mã F-QR chuyên dụng để có thể phát hiện và truy xuất thông tin của mã F-QR chìm trên thẻ ID để kết hợp với hệ thống nhận diện khuôn mặt bằng AI camera nhằm xác thực khuôn mặt. Camera bắt khuôn mặt trong thời gian thực, ngay khi người dùng quét thẻ có in mã ẩn F-QR hệ thống sẽ xử lý dữ liệu, đưa ra 2 vector dữ liệu khuôn mặt để làm cơ sở so sánh và xác thực. Ưu điểm của hệ thống này là có thể hoạt động offline, không cần cơ sở dữ liệu, không cần truy cập internet, có thể sử dụng các bộ xử lý dữ liệu (máy tính) và camera thông thường. Đồng thời độ bảo mật trong việc chống sao chép thẻ ID rất cao, mang lại tính tiện dụng cho các ứng dụng của bảo mật không cần sử dụng network. Trong bài báo, chúng tôi sẽ trình bày phương pháp in và đọc mã F-QR chìm trên thẻ ID, phương pháp nhận diện và xác thực khuôn mặt bằng camera AI và các kết quả thực nghiệm tương ứng.

\*Tác giả liên hệ: Email: bqquan@most.gov.vn

# Research and development of a two-factors face authentication system using an invisible F-QR code on ID card by 1064 nm laser and AI camera

Quoc Tuan Banh<sup>1\*</sup>, Hong Minh Le<sup>2</sup>, Hoang Dat Luu<sup>1</sup>,  
Hai Long Ngo<sup>1</sup>, Khắc Thiên Cao<sup>1</sup>,  
Việt Hoàng Do<sup>1</sup>, Van Binh Le<sup>1</sup>

<sup>1</sup>Laboratory for Fiber Laser Research Development and Application,  
National Center for Technological Progress

<sup>2</sup>Center for Microelectronics and Information Technology,  
National Center for Technological Progress

Received 1 July 2022; accepted 25 July 2022

## Abstract:

The face authentication system using two security factors: an invisible F-QR (face QR) code printed on an ID card and face recognition using AI camera is presented in this paper. F-QR codes with facial features are generated by a chain processing of face detection, face property extraction and QR code generation. The F-QR code is printed on a plastic ID card using a 1064 nm fiber laser. The ID card is made of special materials, including a layer of filter material that allows the 1064 nm laser to pass through while blocking visible lights so that the printed F-QR code on the card is invisible to the human eye or conventional QR code readers. Face authentication is implemented using a dedicated invisible F-QR code reader combined with an AI camera to decide the Cosine similarity between two face feature vectors to make an accurate decision for the authentication.

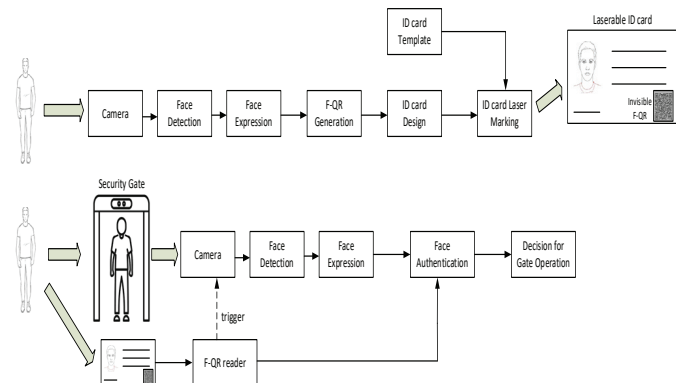
**Keywords:** AI camera, face-ID, fiber laser, ID card, QR code.

**Classification number:** 2.2

## Phương pháp nghiên cứu

Hình 1 miêu tả sơ đồ khối hệ thống xác thực khuôn mặt 2 yếu tố và quy trình tạo mã F-QR để in lên thẻ ID. Đối với quy trình tạo và in mã F-QR lên thẻ ID, mỗi người dùng được cấp một thẻ ID với mã F-QR mang đặc trưng của khuôn mặt. Mã F-QR được tạo ra từ nguồn dữ liệu ảnh khuôn mặt, hoặc chụp khuôn mặt từ máy ảnh. Khối xác định khuôn mặt có chức năng lọc vùng điểm ảnh chỉ bao gồm dữ liệu của khuôn mặt sử dụng thuật toán DNN. Từ ảnh khuôn mặt, khối biểu diễn khuôn mặt chuyển hóa các đặc trưng của khuôn mặt tạo thành một vector đặc trưng N phần tử. Đối với mỗi góc cạnh khác nhau của cùng một khuôn mặt sẽ có một vector đặc trưng N phần tử riêng, tuy nhiên sự khác nhau giữa phần tử trong vector này là ít hơn so với vector đặc trưng N phần tử của khuôn mặt khác. Vector đặc trưng N phần tử có thể coi như chuỗi dữ liệu, cho phép khối tạo mã F-QR tạo ra mã F-QR 2 chiều ở dạng dữ liệu ảnh để có thể sử dụng máy in laser in/khắc trên

thẻ ID. Hiện nay có khá nhiều công cụ tạo mã QR [15, 16]. Phôi thẻ ID đặc biệt có thể dùng laser để in/khắc thông tin lên thẻ kết hợp với phần mềm thiết kế thẻ cho phép tạo ra thẻ ID đặc trưng cho mỗi người dùng.



**Hình 1. Sơ đồ khối hệ thống xác thực khuôn mặt 2 yếu tố bảo mật thẻ ID kết hợp mã F-QR chìm và AI camera.**

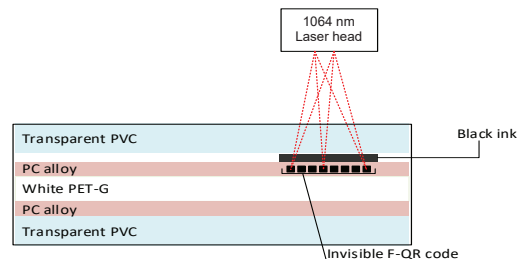
Đối với hệ thống xác thực khuôn mặt, hệ thống sẽ so sánh 2 nguồn dữ liệu của người dùng là đầu đọc thẻ F-QR chìm và camera AI. Với camera, khung hình có khuôn mặt của người dùng sẽ được chụp sau khi có tín hiệu kích hoạt từ việc đọc mã F-QR trên thẻ. Ảnh chụp về cũng được xử lý qua các giai đoạn xác định khuôn mặt và biểu diễn khuôn mặt giống như quy trình tạo mã F-QR. Tại khối biểu diễn khuôn mặt, vector đặc trưng N phần tử được tạo ra. Một vector đặc trưng N phần tử khác cũng được tạo ra bởi đầu đọc F-QR sau khi đọc và chuyển đổi dữ liệu từ thẻ ID. Việc so sánh sự tương đồng giữa 2 vector đặc trưng N phần tử được thực hiện tại khối xác thực khuôn mặt. Tại đây, phương pháp kiểm tra độ tương đồng Cosine được áp dụng. Quyết định đồng nhất được đưa ra dựa trên thực nghiệm xác định giá trị ngưỡng. Như vậy hệ thống hoàn toàn hoạt động offline mà không cần internet để truy cập cơ sở dữ liệu, trong khi vẫn giữ được các lợi thế của các công nghệ nhận dạng khuôn mặt tiên tiến hiện nay.

Trong bài báo này, chúng tôi tập trung vào các công nghệ:

- 1) Thẻ ID và công nghệ in F-QR chìm bằng laser 1064 nm trên thẻ ID;
- 2) Tạo mã F-QR và xác thực khuôn mặt bằng AI camera.

## Thẻ ID và công nghệ in F-QR chìm bằng laser 1064 nm

Công nghệ laser sợi quang [17] đã được phát triển rộng rãi trong những năm gần đây trong các lĩnh vực công nghiệp, đo lường, bảo mật. Đặc biệt, gần đây một số quốc gia đã bắt đầu sử dụng thẻ căn cước, bằng lái xe, hay hộ chiếu dùng laser sợi quang để in thông tin trên thẻ với mục đích nâng cao bảo mật chống giả và tăng tuổi thọ của thẻ ID [18-20]. Hình 2 miêu tả cấu trúc thẻ ID được sử dụng trong nghiên cứu.



**Hình 2. Cấu trúc thẻ ID có thể dùng laser để in/khắc thông tin.**

Các loại thẻ ID bình thường chỉ bao gồm 3 lớp vật liệu PVC cơ bản, trong đó 2 lớp ngoài cùng để in thông tin bằng mực trên bề mặt. Do đó, thông tin dễ bị xóa do va chạm vật lý thường xảy ra. Để chống thông tin in trên thẻ bị mất, thông tin cần được in trên một lớp vật liệu nằm bên dưới một lớp bảo vệ vật liệu PVC trong suốt không thể sử dụng các máy in mực thông thường để in. Đặc tính của laser sợi quang 1064 nm là truyền qua vật liệu trong suốt, tương tác với vật liệu Polycarbonat cản quang thông qua hiệu ứng nhiệt. Tia laser với công suất đỉnh phù hợp tạo ra nhiệt lượng vừa đủ để điểm tương tác trên vật liệu Polycarbonat cản quang thay đổi độ xám từ màu nguyên thủy trắng mà không gây hiện tượng bốc hơi vật liệu. Độ xám có thể tùy chỉnh dựa vào điều khiển công suất đỉnh của tia laser. Thông qua việc quét tia laser trong 2 chiều ngang, dọc trên mặt phẳng thẻ, thông tin (ký tự, hình ảnh) có thể được in vĩnh viễn trên vật liệu Polycarbonat cản quang. Sử dụng laser 1064 nm có thể in thông tin trên thẻ, tuy nhiên thông tin này có thể nhìn thấy đôi mắt người khi có ánh sáng trắng (ánh sáng đèn hoặc mặt trời). Để có thể ẩn thông tin in bằng laser, một lớp lọc quang được chèn thêm vào giữa lớp vật liệu PVC trong suốt và lớp vật liệu Polycarbonat cản quang. Vật liệu lọc là một loại mực có màu đen, không chứa carbon, cản quang đối với ánh sáng trắng và trong suốt đối với tia laser 1064 nm. Như vậy, có thể in thông tin bằng laser 1064 nm bên dưới lớp lọc và bên trên bề mặt lớp Polycarbonat cản quang. Trong trường hợp thông tin là một loại mã QR, nó sẽ trở nên ẩn với mắt người và các đầu đọc mã QR phổ thông, vì mắt người hay đầu đọc chỉ đọc được thông tin tại bước sóng nhìn thấy. Bảng 1 miêu tả thông tin các lớp vật liệu sử dụng trong thẻ bảo mật.

**Bảng 1. Cấu trúc và thông số các lớp trong thẻ bảo mật.**

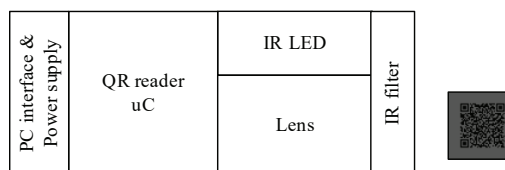
| Vật liệu        | Độ dày                 | Công dụng         |
|-----------------|------------------------|-------------------|
| Transparent PVC | PVC trong suốt         | 100 $\mu\text{m}$ |
| Black ink       | Mực đen không carbon   | 50 $\mu\text{m}$  |
| PC alloy        | Polycarbonat cản quang | 100 $\mu\text{m}$ |
| White PET-G     | PET-G                  | 300 $\mu\text{m}$ |
| PC alloy        | Polycarbonat cản quang | 100 $\mu\text{m}$ |
| Transparent PVC | PVC trong suốt         | 100 $\mu\text{m}$ |

Laser 1064 nm sử dụng trong nghiên cứu là loại laser xung MOPA. Xung laser có thể điều chỉnh từ 4 đến 200 ns. Do thời gian phát xung ngắn nên vật liệu tương tác ít bị sinh nhiệt gây cháy hoặc ảnh hưởng đến độ phân giải. Nhiệt chỉ xảy ra trong quá trình tương tác laser và vật liệu tạo ra độ xám (thông tin). Thông số về laser được miêu tả ở bảng 2.

**Bảng 2. 1064 nm laser và thông số kỹ thuật.**

| Tên                      | Thông số kỹ thuật |
|--------------------------|-------------------|
| Bước sóng (nm)           | 1064              |
| Chế độ làm việc          | Xung              |
| Công suất trung bình (W) | 10                |
| Độ rộng xung (ns)        | 4-200             |
| Tần số phát xung (kHz)   | 2-500             |
| Năng lượng xung (mJ)     | <1 mJ             |

Mã F-QR khi được in bằng laser lên thẻ sẽ không nhìn thấy bằng mắt người cũng như các đầu đọc QR thông thường. Trong nghiên cứu này, chúng tôi phát triển đầu đọc mã QR cho phép lấy được thông tin từ mã F-QR chìm bên dưới lớp vật liệu lọc. Để đầu đọc có thể nhìn thấy mã F-QR bên dưới lớp vật liệu lọc, một nguồn sáng hồng ngoại có bước sóng phù hợp và một bộ lọc quang highpass tương ứng được sử dụng để lọc thông tin chỉ của mã F-QR đưa đến cảm biến đọc mã QR. Hình 3 miêu tả sơ đồ khối của đầu đọc F-QR ẩn. Mã F-QR ẩn được chiếu ánh sáng hồng ngoại bước sóng >850 nm, bước sóng này xuyên qua vật liệu lọc màu đen trên thẻ và tương tác với mã F-QR, tia phản xạ đi ngược lại đầu đọc, qua tấm lọc hồng ngoại, qua thấu kính đi vào cảm biến giải mã QR. Tấm lọc hồng ngoại trên đầu đọc để ngăn các ánh sáng nhìn thấy đi vào cảm biến gây ảnh hưởng đến độ nhạy của đầu đọc. Truyền thông và cấp nguồn cho đầu đọc được lấy từ máy tính thông qua giao tiếp micro-USB. Dữ liệu lấy được từ mã F-QR được sử dụng cho việc xác thực khuôn mặt.



**Hình 3. Sơ đồ khối đầu đọc mã F-QR chìm.**

### Tạo mã F-QR và xác thực khuôn mặt bằng AI camera

Quy trình tạo mã F-QR được thực hiện thông qua 3 quá trình: xác định khuôn mặt, biểu diễn khuôn mặt và chuyển đổi mã QR. Trong xác định khuôn mặt, phương pháp DNN được lựa chọn do các ưu điểm về tốc độ, phù hợp với ảnh có 1 khuôn mặt và kích thước ảnh lớn hơn 100x100 pixels [21]. Thư viện của thuật giải này được cung cấp ở [22]. Biểu diễn khuôn mặt quyết định độ chính xác của quá trình nhận dạng khuôn mặt. Ở bước này, mỗi khuôn mặt sẽ được biểu diễn thành một véc tơ đặc trưng N phần tử. Thông qua việc đánh giá các mô hình, thuật giải AI để biểu diễn khuôn mặt như mô hình VGG-Face CNN của Oxford [23] (đầu vào: ảnh màu 224x224 pixels; đầu ra: vector 2622 phần tử; mô hình: ResNet-50, có 145.022.878 tham số), mô hình FaceNet của Google [13] (đầu vào: ảnh màu 160x160 pixels; đầu ra: vector 128 phần tử; mô hình: InceptionResNetV2, có 22.808.144 tham số), mô hình OpenFace của Carnegie Mellon University [24] (đầu vào: ảnh màu 96x96 pixels; đầu ra: vector 128 phần tử; mô hình: có 3.743.280 tham số), mô hình DeepFace của Facebook [25] (đầu



vào: ảnh màu 152x152 pixels; đầu ra: vector 4096 phần tử; mô hình: có 137.774.071 tham số), căn cứ vào các đánh giá về độ chính xác của phương pháp (99,63% trên Labeled Faces in the Wild - LFW dataset; 95,12% trên YouTube Faces DB) và căn cứ vào tốc độ tính toán và các kết quả khảo sát theo khuôn mặt và ảnh thực tế và yêu cầu lưu trữ, mô hình FaceNet của Google được sử dụng trong nghiên cứu này. Mô hình này đã được cung cấp dạng thư viện trong [26] với bộ trọng số đã được huấn luyện và đánh giá đạt độ chính xác cao. Vector đặc trưng 128 phần tử của mô hình FaceNet được chuyển đổi, mã hóa sang dạng F-QR code sử dụng các thư viện mở [27].

Xác thực khuôn mặt được thực hiện bởi 2 hoạt động: 1) Đọc mã F-QR ẩn bằng đầu đọc và chuyển thành vector đặc trưng N phần tử; 2) Tạo vector đặc trưng N phần tử AI camera. Việc so sánh 2 vector đặc trưng này được thực hiện thông qua việc tính toán độ tương tự Cosine theo công thức sau:

$$\text{Cosine}(x, y) = \frac{\sum_{i=1}^n x_i y_i}{\sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2}} \quad (1)$$

trong đó: x, y là 2 vector đặc trưng của 2 khuôn mặt thu về từ đầu đọc mã F-QR và từ AI camera; n là số lượng phần tử của vector đặc trưng (trong trường hợp này n=128); i chạy từ 1-n.

Quyết định giống hay khác nhau của khuôn mặt được xác định tùy theo các ứng dụng khác nhau thông qua một mức ngưỡng so sánh. Thông thường mức ngưỡng được lựa chọn một cách thực nghiệm dựa trên các điều kiện thực tế nơi thiết lập hệ thống như không gian, môi trường, ánh sáng...

## Kết quả thực nghiệm

### Thiết lập hệ thống

Trong phạm vi phòng thí nghiệm, chúng tôi chỉ sử dụng những thiết bị phổ thông nhằm đánh giá sự khả thi của hệ thống. Camera webcam USB2.0 được sử dụng để chụp khuôn mặt, tạo mã F-QR code và xác thực khuôn mặt. Dữ liệu được xử lý bởi máy tính desktop có cấu hình (Intel Core i5 3,2 GHz, 8,0 GB RAM, với board VGA HD Graphics 4600). Máy in thẻ laser sử dụng nguồn MOPA IPG YLPN-1-1x350-20 in trên thẻ Kobayashi Create laserable. Đầu đọc mã F-QR tự thiết kế chế tạo kết nối với máy tính qua cổng USB. Phần mềm mô phỏng hệ thống được thiết kế với tính năng vừa tạo mã F-QR để cho máy in thẻ, vừa kiểm tra xác thực khuôn mặt khi cùng kết nối USB camera và đầu đọc vào máy tính. Hình 4 miêu tả các thiết bị được sử dụng trong thử nghiệm.



Hình 4. Thiết bị sử dụng trong thử nghiệm.

### Kết quả thực nghiệm

Hình 5 là giao diện phần mềm tạo mã F-QR theo 1 trong 2 phương án: 1) Chụp ảnh từ webcam và tạo mã F-QR; 2) Tạo mã F-QR từ ảnh đã được chụp từ trước.



Hình 5. Giao diện phần mềm tạo mã F-QR từ camera (hoặc từ ảnh tĩnh).

Hình 6 là kết quả tạo mã F-QR đối với các khuôn mặt khác nhau.



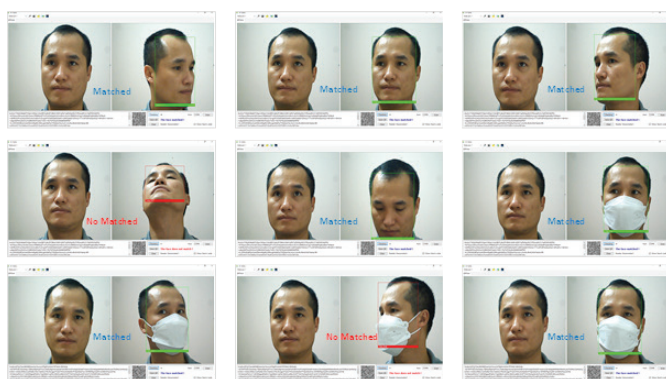
Hình 6. Kết quả tạo mã F-QR của những người dùng khác nhau.

Sau khi có mã F-QR của từng người dùng, mã F-QR được in chìm lên thẻ ID bằng 1064 nm laser. Hình 7 là thẻ ID của 2 người dùng mặt trước và mặt sau. Mặt trước in ảnh và thông tin, mặt sau in mã F-QR chìm.



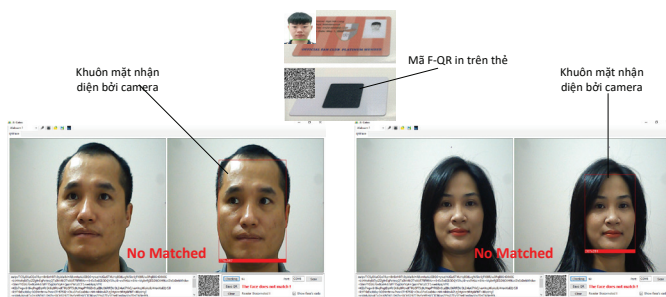
Hình 7. Thẻ ID in mã F-QR chìm của 2 người dùng.

Việc xác thực khuôn mặt từ 2 yếu tố bảo mật thẻ ID và AI camera được thực hiện như trong hình 8. Mỗi khi đầu đọc nhận được dữ liệu từ việc đọc mã F-QR chìm trên thẻ, hệ thống sẽ kích hoạt webcam để chụp ảnh người xuất hiện tại vùng quan sát và phân tích dữ liệu. Nếu trùng hoặc không trùng khuôn mặt, hệ thống sẽ thông báo tương ứng. Hình 8 thể hiện các kết quả xác thực đối với các góc cạnh khác nhau của khuôn mặt chụp bởi camera và so sánh với F-QR tính trong thẻ ID. Kết quả cho thấy, hệ thống nhận diện một cách chính xác nếu như khuôn mặt chụp bởi camera không quá nghiêng so với hướng nhìn của camera. Kết quả cũng cho thấy, mặc dù mã F-QR in trong thẻ được tạo trong trường hợp không đeo khẩu trang nhưng hệ thống vẫn xác thực được đúng người kể cả khi người dùng đeo khẩu trang không quá che kín khuôn mặt.



**Hình 8. Kết quả xác thực của cùng khuôn mặt tại các góc độ khác nhau và trường hợp có/không có khẩu trang (mã F-QR in trên thẻ ID là không có khẩu trang).**

Hình 9 chỉ ra kết quả xác thực khuôn mặt trong trường hợp mã F-QR trên thẻ ID khác với các khuôn mặt chụp từ camera. Kết quả cho thấy, hệ thống nhận biết sự khác biệt khá rõ, cho kết quả không trùng khuôn mặt một cách chính xác. Tổng thời gian xử lý và xác thực khuôn mặt của hệ thống khoảng 0,3 s, đủ nhanh cho các ứng dụng của an ninh nơi yêu cầu người dùng cần dừng lại và có hành động dứt khoát vào khe đọc thẻ để kích hoạt hệ thống.



**Hình 9. Kết quả xác thực khuôn mặt khác với mã F-QR in trên thẻ ID.**

Bên cạnh đó, từ kết quả thực nghiệm cho thấy, để phân biệt khuôn mặt thực 3D và ảnh 2D cần phải bổ sung các giải pháp như: nhận dạng đối tượng đúng là người trước khi capture khuôn mặt; tích hợp cảm biến nhiệt độ để phân biệt người và ảnh.

## Kết luận

Nghiên cứu đã trình bày hệ thống xác thực khuôn mặt mới sử dụng 2 yếu tố xác thực là mã F-QR in trên thẻ ID và AI camera. Kết quả tiên khả thi cũng được trình bày trong bài báo. Hệ thống này thích hợp với những ứng dụng của ra vào an toàn không cần phải xây dựng hệ thống phức tạp như kết nối sever, internet và thiết bị cần thông số kỹ thuật cao. Giảm thiểu được rủi ro rò rỉ thông tin do phụ thuộc vào server cũng như sao chép thông tin trên thẻ. Bên cạnh đó, sử dụng laser 1064 nm trên thẻ nhựa cho phép tăng độ bảo mật, tiết kiệm chi phí do không cần mực in thẻ là một điểm mạnh của hệ thống. Nếu áp dụng hệ thống xử lý ảnh kết hợp với GPU tốc độ cao, tốc độ xử lý của hệ thống sẽ được cải thiện, đạt tới tốc độ xác thực <0,1 s, phù hợp với nhiều ứng dụng thực tế.

## TÀI LIỆU THAM KHẢO

- [1] S. Hassan, et al. (2013), "Face recognition in mobile devices", *International Journal of Computer Applications*, **73**(2), pp.13-20.
- [2] M. Karovaliya, et al. (2015), "Enhanced security for ATM machine with OTP and facial recognition features", *Procedia Computer Science*, **45**, pp.390-396.
- [3] C. Libby, J. Ehrenfeld (2021), "Facial recognition technology in 2021: Masks, bias, and the future of healthcare", *Journal of Medical Systems*, **45**(39), DOI: 10.1007/s10916-021-01723-w.
- [4] I.A. Ziegen, et al. (2021), "License verification system with face recognition using IOT", *International Journal of Advanced Research in Science*, **4**, pp.656-670.
- [5] F.P. Mahdi, et al. (2017), "Face recognition-based real-time system for surveillance", *Intelligent Decision Technologies*, **11**(1), pp.79-92.
- [6] A. Clark, T. Bourlai (2013), "Enhancing passport images for face recognition", *SPIE Newsroom*, DOI: 10.1117/2.1201310.005112.
- [7] S. Prabhakar, et al. (2003), "Biometric recognition: Security and privacy concerns", *IEEE Security and Privacy Magazine*, **1**, pp.33-42.
- [8] C.Y. Chang, J.J. Liao (2015), "Combination of RFID and face recognition for access control system", *2015 International Conference on Consumer Electronics-Taiwan*, pp.470-471.
- [9] A.V. Phapale, et al. (2016), "Automated attendance system using RFID and face recognition", *International Journal of Innovative Research in Computer and Communication Engineering*, **4**(3), pp.3983-3990.
- [10] S. Singh, S.V.A. Prasad (2018), "Techniques and challenges of face recognition: A critical review", *Procedia Computer Science*, **143**, pp.536-543.
- [11] A. Dirin, et al. (2020), "Comparisons of facial recognition algorithms through a case study application", *International Journal of Interactive Mobile Technologies*, **14**(14), pp.121-133.
- [12] S. Baek, et al. (2021), "Face detection in untrained deep neural networks", *Nat. Commun.*, **12**, DOI: 10.1038/s41467-021-27606-9.
- [13] F. Schroff, et al. (2015), "FaceNet: A unified embedding for face recognition and clustering", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp.815-823.
- [14] I.A. Taie, et al. (2017), "The effect of distance similarity measures on the performance of face, ear and palm biometric systems", *2017 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*, DOI: 10.1109/dicta.2017.8227495.
- [15] P. Suthesbanjard, W. Premchaiswadi (2010), "QR-code generator", *2010 Eighth International Conference on ICT and Knowledge Engineering*, DOI: 10.1109/ICTKE.2010.5692920.
- [16] <http://www.denso-wave.com/qrcode/aboutqre.html>.
- [17] S. Fu, et al. (2017), "Review of recent progress on single-frequency fiber lasers", *Journal of the Optical Society of America B*, **34**(3), DOI: 10.1364/josab.34.000a49.
- [18] <https://www.maticacorp.com/2018/03/laser-personalization-for-high-security-id-cards/>.
- [19] <https://www.enraversjournal.com/articles/online/engraving-plastic-with-a-fiber-laser>.
- [20] <https://www.iai.nl/cases/swedish-passports-id-cards/>.
- [21] Lê Hồng Minh và cs (2021), "Tích hợp nhận dạng khuôn mặt để tự động xác thực người mang thẻ, ứng dụng vào kiểm soát người vào/ra hầm lò mỏ than", *Kỷ yếu Hội nghị khoa học và Triển lãm quốc tế lần thứ 6 về điều khiển và tự động hoá - VCCA'2021*.
- [22] <https://opencv.org/>.
- [23] [https://www.robots.ox.ac.uk/~vgg/software/vgg\\_face/](https://www.robots.ox.ac.uk/~vgg/software/vgg_face/).
- [24] <http://multicomp.cs.cmu.edu/resources/openface>.
- [25] Y. Taigman, et al. (2014), "DeepFace: Closing the gap to human-level performance in face verification", *Proceedings of the Conference on Computer Vision and Pattern Recognition (CVPR)*.
- [26] <http://dlib.net/>.
- [27] <https://github.com/nayuki/QR-Code-generator>.