Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ 28 (2012) 158-166

# Tích hợp các kỹ thuật so khớp ảnh trong xác thực hộ chiếu sinh trắc

Dư Phương Hạnh, Nguyễn Ngọc Hoá*

*Trường Đại học Công nghệ, ĐHQGHN, 144 Xuân Thủy, Hà Nội, Việt Nam*

Nhận ngày 16 tháng 5 năm 2012

**Tóm tắt**. Hộ chiếu sinh trắc đã trải qua ba thế hệ phát triển, từ ban đầu chỉ chú trọng lưu ảnh mặt người trên chip; sau đó kết hợp thêm một số nhân tố sinh trắc như ảnh mống mắt, ảnh vân tay cùng cơ chế kiểm soát truy cập mở rộng EAC; và hiện nay bổ xung cơ chế thiết lập kết nối có xác thực mật khẩu PACE. Trong bài báo này, chúng tôi giới thiệu giải pháp tích hợp các kỹ thuật so khớp ảnh sinh trắc vào mô hình xác thực hộ chiếu sinh trắc dựa trên hai cơ chế PACE và EAC. Việc thực nghiệm được tiến hành dựa trên những công cụ mã mở và bước đầu cho phép thử nghiệm toàn bộ quá trình xác thực hộ chiếu sinh trắc.

*Từ khoá:* xác thực sinh trắc học, hộ chiếu sinh trắc, kiểm soát truy cập mở rộng, kiểm soát truy cập cơ bản, RFID, PKI.

## 1. Giới thiệu

Hộ chiếu sinh trắc (biometric passport - HCST), đã và đang được triển khai sử dụng trên nhiều nước trên thế giới [1]. Mục tiêu chính của HCST là nâng cao an ninh/an toàn trong quá trình cấp phát/kiểm duyệt/xác thực hộ chiếu. Mục tiêu này được đảm bảo thông qua việc tăng cường những chuẩn về hộ chiếu thông thường, với (i) các kỹ thuật đảm bảo an ninh/an toàn thông tin, (ii) công nghệ định danh dựa trên tần số radio (Radio Frequency Identification-RFID) và (iii) công nghệ xác thực dựa trên những nhân tố sinh trắc học như ảnh mặt người, vân tay, mống mắt… Hai yếu tố đầu cho phép nâng cao việc chống đánh cắp thông tin cá nhân, chống làm giả hộ chiếu, ..; còn hai yếu tố sau cho phép nâng cao hiệu quả quá trình xác thực công dân mang hộ chiếu sinh trắc [2].

Hiện nay trên thế giới, HCST đã trải qua ba thế hệ phát triển: từ việc mới chỉ sử dụng ảnh mặt người số hoá lưu trên một chip RFID (thế hệ thứ nhất) [1], kết hợp thêm một số nhân tố sinh trắc và cơ chế kiểm soát truy cập mở rộng (Extended Access Control – EAC; thế hệ thứ hai) [2] và bổ xung cơ chế thiết lập kết nối có xác thực mật khẩu (Password Authenticated Connection Establishment – PACE; thế hệ thứ 3, bắt đầu từ cuối năm 2009) [3]. Trong bài báo [3], mô hình xác thực HCST với cơ chế PACE và EAC đã được trình bày chi tiết và đã minh chứng được những ưu điểm của mô hình này so với những HCST ở thế hệ trước.

Trong bài báo này, chúng tôi tập trung nghiên cứu tích hợp các kỹ thuật so khớp ảnh sinh trắc vào mô hình xác thực HCST nêu trên.

* Tác giả liên hệ. ĐT: 84-4-37547813.
E-mail: hoa.nguyen@vnu.edu.vn

Với việc sử dụng ba đặc trưng sinh trắc tiêu biểu, ảnh mặt người, ảnh mống mắtk và ảnh vân tay, cho phép nâng cao được quá trình kiểm soát và xác thực công dân mang HCST.

Các phần còn lại của bài báo được tổ chức như sau: phần 2 giới thiệu mô hình xác thực HCST sử dụng cơ chế PACE và EAC; phần 3 khái quát những kỹ thuật so khớp ảnh ba đặc trưng sinh trắc; phần thử nghiệm và đánh giá được trình bày ở hai phần kế tiếp. Phần cuối cùng là những đánh giá kết luận và một số hướng phát triển kế tiếp.

## 2. Mô hình xác thực HCST

### *2.1. Các công nghệ trong HCST*

HCST được xây dựng kết hợp chủ yếu ba công nghệ chính: định danh sử dụng tần số vô tuyến (RFID), cơ sở hạ tầng khoá công khai (Public Key Infrastructures – PKI) và xác thực sinh trắc học.

*i. Định danh sử dụng tần số vô tuyến*

RFID là công nghệ nhận dạng đối tượng sử dụng sóng vô tuyến. Công nghệ này cho phép nhận biết các đối tượng thông qua hệ thống thu phát sóng vô tuyến, từ đó có thể giám sát, quản lý hoặc lưu vết từng đối tượng.

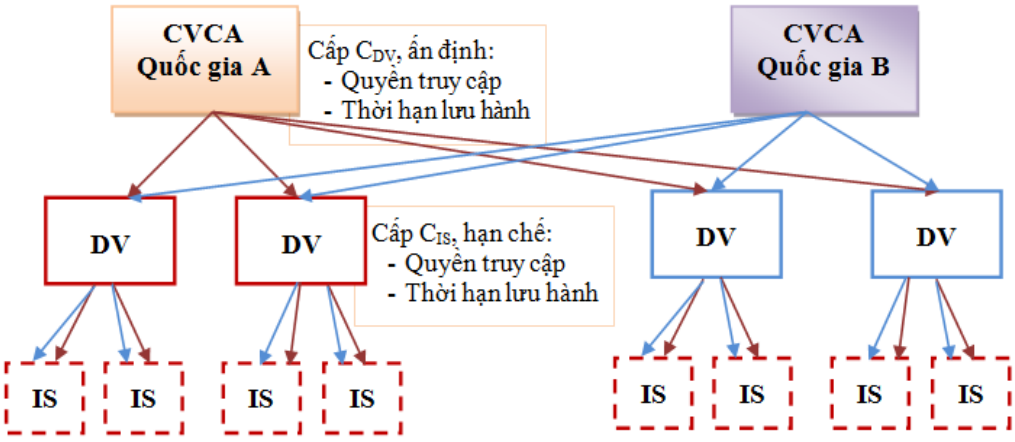
HCST đều sử dụng công nghệ RFID loại thụ động, không cần nguồn nuôi, với đặc tả tuân theo chuẩn ISO 14443 và được tổ chức ICAO miêu tả chi tiết trong [4].

*ii. Cơ sở hạ tầng khoá công khai PKI*

PKI có thể được xem như cơ chế cho phép bên thứ ba (thường là nhà cung cấp chứng chỉ số) cung cấp và xác thực định danh của hai bên tham gia vào quá trình trao đổi thông tin. PKI cho HCST phải cho phép đảm bảo:

- Quá trình đầu đọc thẩm định dữ liệu được lưu trong HCST là xác thực.
- Dữ liệu trong HCST không bị thay đổi hay nhân bản.
- Thẩm định đầu đọc có được phép truy cập dữ liệu trong chip RFID hay không.

Như vậy, mỗi HCST cũng như các hệ thống cấp phát/thẩm định HCST cũng đều phải có chứng chỉ số. Việc trao đổi chứng chỉ của cơ quan cấp hộ chiếu giữa các quốc gia sẽ được thực hiện bằng đường công hàm và thông qua danh mục khoá công khai của ICAO [5-6].




Hình 1. Mô hình PKI cho HCST.

*iii. Xác thực sinh trắc học*

Nói đến sinh trắc học là nói đến nhận dạng và kiểm tra sự giống nhau của con người dựa trên đặc điểm sinh lý nào đó. Các đặc điểm sinh trắc học thường sử dụng bao gồm: vân tay, khuôn mặt, mống mắt, giọng nói, chữ viết tay, hình bàn tay… Trong HCST, ICAO đã đưa ra ba đặc trưng sinh trắc có thể sử dụng là ảnh khuôn mặt, ảnh vân tay và ảnh mống mắt của người mang hộ chiếu [7]. Cả ba đặc trưng này sẽ được sử dụng trong mô hình thực nghiệm trong của bài báo này.

*2.2. Mô hình xác thực HCST thử nghiệm ứng dụng cơ chế PACE và EAC*

Dựa trên mô hình HCST thế hệ thứ ba [3], mô hình xác thực HCST tích hợp cả hai cơ chế PACE và EAC sẽ được sử dụng trong bài báo này. Mô hình này bao gồm các bước chính sau:

**B1:** Người mang hộ chiếu xuất trình hộ chiếu cho cơ quan kiểm tra, cơ quan tiến hành thu nhận các đặc tính sinh trắc học từ người xuất trình hộ chiếu.

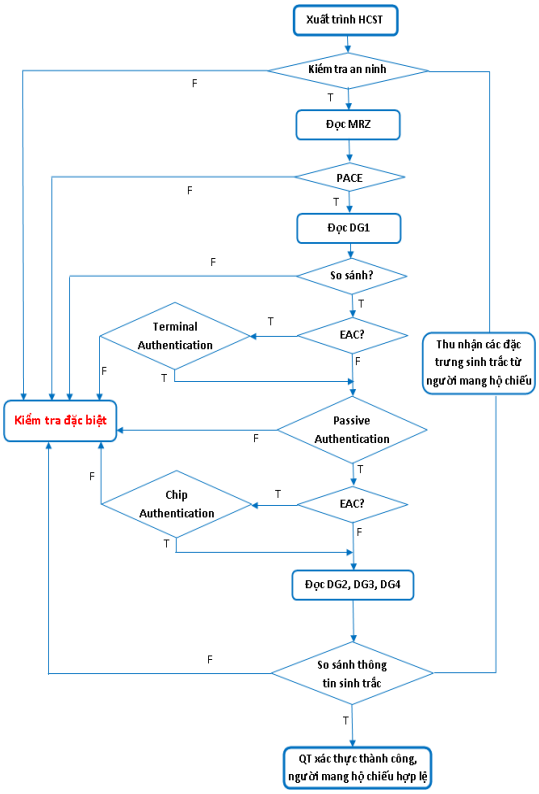
**B2:** Kiểm tra các đặc tính bảo mật trên trang hộ chiếu giấy thông qua các đặc điểm an ninh truyền thống đã biết: thuỷ ấn, dải quang học, lớp bảo vệ ảnh…

**B3:** IS và chip thực hiện quá trình PACE. Sau khi PACE thành công, IS có thể đọc các thông tin trong chip ngoại trừ DG3, DG4 (ảnh vân tay và mống mắt), mọi thông tin trao đổi giữa đầu đọc và chip được truyền thông báo bảo mật, mã hoá sau đó là xác thực theo cặp khoá ($K_{ENC}$, $K_{MAC}$) có được từ quá trình PACE.

**B4:** Tiến hành quá trình TA để chứng minh quyền truy cập của đầu đọc đến phần dữ liệu DG3, DG4.

**B5:** Thực hiện PA để kiểm tra tính xác thực và toàn vẹn của các thông tin lưu trong chip thông qua kiểm tra chữ ký trong $SO_D$ bằng khoá công khai của cơ quan cấp hộ chiếu. Việc trao đổi khoá thông qua chứng chỉ số theo mô hình khuyến cáo của ICAO.

**B6:** Tiến hành CA để chứng minh được tính nguyên gốc của chip đồng thời cung cấp khoá phiên mạnh cho truyền thông báo bảo mật.




Hình 2. Mô hình xác thực Hộ chiếu sinh trắc.

**B7:** IS đối sánh dữ liệu sinh trắc thu nhận được trực tiếp từ người xuất trình hộ chiếu với dữ liệu sinh trắc lưu trong chip. Nếu quá trình đối sánh thành công và kết hợp với các chứng thực trên, cơ quan kiểm tra hộ chiếu có đủ điều kiện để tin tưởng hộ chiếu là xác thực và người mang hộ chiếu đúng là con người mô tả trong hộ chiếu. Nếu cơ quan kiểm tra hộ chiếu không

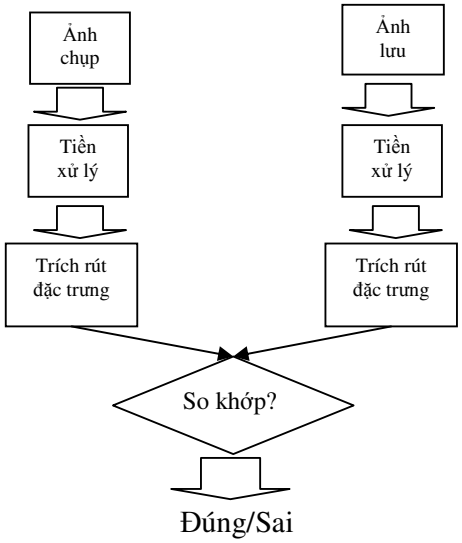
triển khai EAC thì IS đó không có quyền truy cập DG3 và DG4. Thông tin sinh trắc học duy nhất dùng để đối sánh chỉ là ảnh khuôn mặt.

Chi tiết về bảy bước này được trình bày cụ thể trong [3]. Để thực hiện bước 7, các kỹ thuật so khớp ảnh sinh trắc sẽ được sử dụng.

## 3. Các kỹ thuật so khớp ảnh đặc trưng sinh trắc

Trong mô hình xác thực HCST nêu trên, bước cuối cùng chính là so khớp những ảnh đặc trưng sinh trắc đã lưu trong HCST với những ảnh thu chụp trực tiếp từ người mang HCST. Với việc sử dụng cả ba đặc trưng - vân tay, mống mắt, khuôn mặt – việc tỷ lệ xác thực kiểm tra chính xác định danh công dân sẽ được nâng cao.

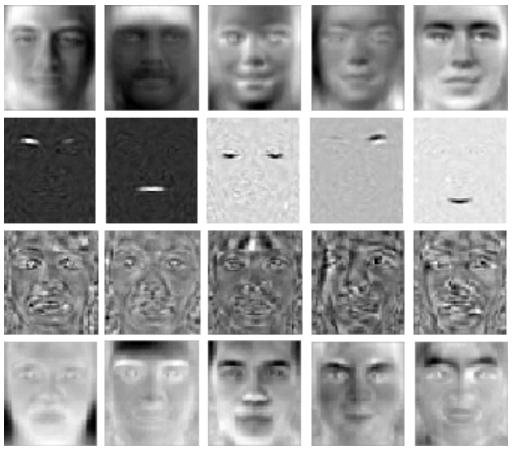
Quy trình chung của việc so khớp của cả ba ảnh sinh trắc được minh hoạ như hình dưới đây:




Hình 3. Quy trình so khớp ảnh.

### *3.1. So khớp ảnh khuôn mặt*

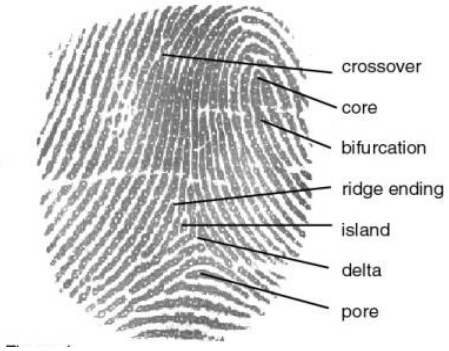
Trong HCST, ảnh khuôn mặt được lưu vào vùng dữ liệu DG2 với định dạng ảnh là JPEG hoặc JPEG2000, kích thước ảnh nằm trong khoảng từ 12-15KB. Tại các điểm xuất nhập cảnh sẽ có các camera chuyên dụng để quét ảnh khuôn mặt của mỗi người. Việc so khớp giữa ảnh thu chụp trực tiếp tại của khẩu với ảnh lưu trong HCST sẽ dựa trên kỹ thuật so khớp thông dụng nhất: sử dụng kỹ thuật eigenface [8].



Hình 4. Nhận dạng khuôn mặt sử dụng eigenface.

### *3.2. So khớp ảnh vân tay*

Vân tay là một trong những nhân tố sinh trắc hoàn toàn tự nhiên, có những đặc trưng riêng của con người và từ lâu đã được coi là bằng chứng hợp pháp trên toàn thế giới. Các điểm đặc trưng thường được sử dụng trong anh vân tay được minh hoạ như hình dưới đây.



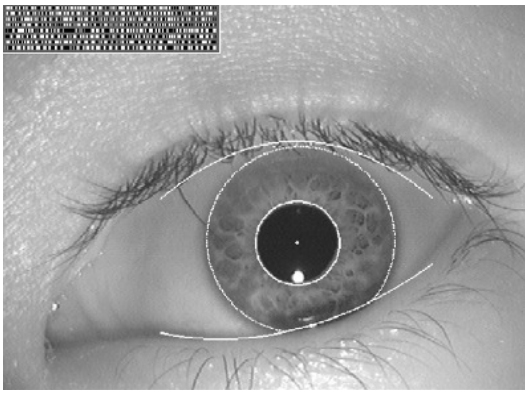

Hình 5. Ảnh vân tay và các điểm đặc trưng.

Dữ liệu ảnh vân tay sẽ được lưu trong vùng DG3 của HCST. Mỗi ảnh vân tay sẽ được lưu với chuẩn WSQ và có kích thước tối đa là 10KB. Tuỳ thuộc dung lượng của chip RFID sử dụng trong HCST mà mỗi quốc gia có thể quy định số vân tay lưu trong HCST. Thông tin về số lượng và vị trí vân tay cũng được lưu trong DG3 [5].

Việc so khớp hai ảnh vân tay sẽ được thực hiện với kỹ thuật trích rút các điểm chi tiết (minutiaes) và so khớp các tham số như khoảng cách giữa các điểm, góc lệch, thông tin về các điểm lân cận khác … [9].

*3.3. So khớp ảnh mống mắt*

Mống mắt cũng giống như vân tay, là những đặc trưng sinh trắc của mỗi con người, được duy trì và ổn định trong suốt cuộc đời của họ. Mống mắt là một cơ trong mắt điều chỉnh kích thước đồng tử, điều chỉnh số lượng ánh sáng vào mắt. Nó phân chia màu mắt với màu sắc dựa trên số lượng sắc tố melatonin trong cơ. Các đặc tính của mống mắt được bảo vệ từ môi trường và khá ổn định so với các đặc tính sinh trắc khác của con người.



Hình 6. Ảnh mống mắt và đặc trưng được trích.

Tại các điểm xuất nhập cảnh hoặc các điểm kiểm tra, người dùng đứng trước một camera để chụp hoặc sử dụng tia laser để thu được ảnh mống mắt. Mỗi ảnh mống mắt sẽ được lưu với dung lượng tối đa là 30KB trong DG4 [5].

Việc trích rút các đặc trưng trong ảnh mống mắt sẽ được thực hiện với kỹ thuật sử dụng bộ lọc 2D Gabor [10].

## 4. Thực nghiệm

Do điều kiện có hạn về cơ sở vật chất, chúng tôi đã tiến hành thử nghiệm mô hình trên theo hướng kiểm thử quy trình xác thực với dữ liệu mô phỏng. Các phần liên quan đến những bước cần xử lý trên chip RFID sẽ được thử nghiệm trong thời gian tới.

Chương trình thử nghiệm chúng tôi phát triển sẽ tập chung vào các chức năng sau:

- Phân tích vùng MRZ trên HCST.
- Đọc vùng DG1 lưu trên chip và so khớp với vùng MRZ vừa đọc trên.
- Mô phỏng quá trình xác thực với cơ chế PACE và EAC (bao gồm cả xác thực đầu đọc và xác thực chip).
- So khớp các đặc trưng sinh trắc.

Dựa trên số thư viện mã hoá như Org.BouncyCastle, CryptoSys PKI và bộ thư viện xử lý ảnh OpenCV [11] chúng tôi đã tiến hành xây dựng chương trình cung cấp các chức năng nêu trên, phục vụ quá trình kiểm thử mô hình xác thực.

Chương trình thử nghiệm thu được đã có khả năng tiến hành các bước đã nêu trong mô hình xác thực nêu trên. Cụ thể:

- Phân tích và hiển thị thông tin trong vùng MRZ

- Tiến hành PACE, lưu vết kết quả. Nếu thành công, tiến hành tiếp bước sau.

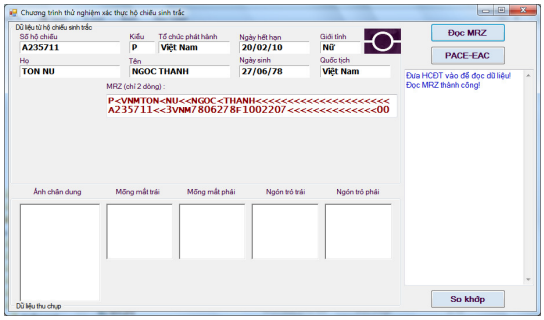
- Đọc DG1 và so khớp với thông tin MRZ như trong mô hình đã nêu.

- Tiến hành xác thực đầu đọc và lưu/hiển thị toàn bộ vết các bước đã thực tiện trong quá trình này.

- Thực hiện xác thực chip với 7 bước và lưu/hiển thị các vết thực hiện. Ở đây, quá trình PA tạm thời chưa tích hợp vào hệ thống vì lý do thiếu hạ tầng khoá công khai PKI.

### *4.1. Đọc thông tin từ MRZ*

Chức năng này thực hiện việc đọc vùng MRZ (gồm 2 dòng dữ liệu trong vùng MRZ) và hiển thị các thông tin tương ứng lên vùng dữ liệu từ HCST của giao diện chính. Đồng thời hiển thị thông báo việc đọc thành công hay thất bại ở bên khung bên phải của giao diện.




Hình 7. Thực nghiệm đọc MRZ.

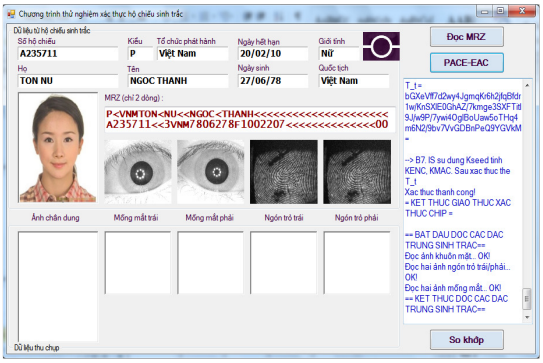
### *4.2. Thực hiện cơ chế PACE-EAC*

Trước khi đầu đọc có quyền đọc các vùng dữ liệu trong Chip, cả hai phải thực hiện giao thức xác thực PACE trước tiên. Giao thức này thiết lập các thông báo bảo mật giữa Chip MRTD và IS dựa trên các *weak (short) password*, và cho phép Chip thẩm định xem đầu đọc có quyền truy cập vào vùng dữ liệu ít nhạy cảm hay không (ví dụ DG1, …). Trường hợp thất bại, sẽ có thông báo và yêu cầu chuyển sang tác vụ "***Kiểm tra đặc biệt***".

Sau khi thực hiện PACE thành công, hệ thống có quyền truy cập và đọc vùng DG1 lưu trong Chip. Từ đó, hệ thống sẽ so sánh dữ liệu trong DG1 có khớp với MRZ mà đã đọc ở bên trên hay không.

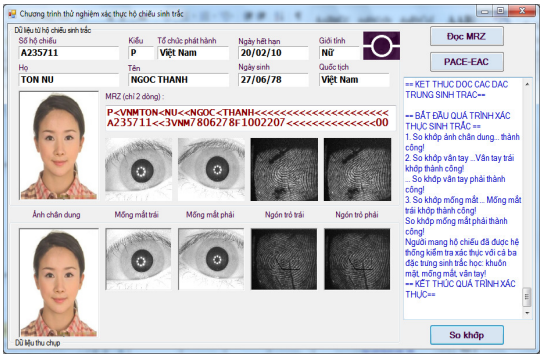
Xác thực đầu đọc được tiến hành tiếp theo để đảm bảo chứng minh với Chip là có quyền truy cập vào vùng dữ liệu nhạy cảm (DG3, DG4). Giao thức này được miêu tả qua tám bước, các bước tương ứng được hiển thị chi tiết trong khung vết thực hiện [3]. Nếu thành công, sẽ thực hiện tiếp xác thực Chip, nếu không phải chuyển sang bước ***kiểm tra đặc biệt***.

Xác thực Chip thiết lập thông báo bảo mật giữa chip MRTD và IS dựa trên cặp khoá tĩnh được lưu trữ trên chip (được sử dụng thay thế cơ chế Active Authentication mà ICAO đã đưa ra). Mục đích cho phép đầu đọc (hệ thống) thẩm định chip RFID là nguyên bản hay không. Khi giao thức này được thực hiện thành công, cùng với giả thiết cơ chế Xác thực thụ động (Passive Authentication) và các dữ liệu sinh trắc (ảnh mặt người, vân tay, mống mắt) sẽ được hiển thị lên màn hình.



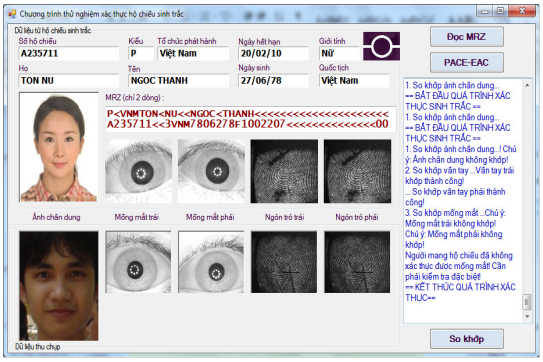

Hình 8. Kết quả thực hiện PACE-EAC.

### *4.3. So khớp các đặc trưng sinh trắc*




Hình 9. Kết quả so khớp các đặc trưng sinh trắc thành công.

Sau khi thu chụp được những đặc trưng sinh trắc từ phía người mang hộ chiếu, hệ thống tiến hành so khớp các đặc trưng này với những đặc trưng đã lưu trong HCST. Hình dưới minh hoạ cho quá trình so khớp chính xác với HCST của công dân thông thường.




Hình 10. Kết quả so khớp các đặc trưng sinh trắc không thành công.

Trong trường hợp những đặc trưng thu chụp không khớp với những đặc trưng lưu trong HCST, hệ thống sẽ đưa ra thông báo yêu cầu kiểm tra đặc biệt. Các đặc trưng cũng được xếp độ ưu tiên từ cao đến thấp (mống mắt, vân tay, khuôn mặt) để phục vụ kết hợp các kết quả so khớp. Tuy nhiên, tất cả các vết kết quả so khớp đều được hiển thị trong hệ thống nhằm phục vụ nhân viên tác nghiệp.

## 5. Đánh giá kết quả

Về hiệu năng tính toán, do phần tính toán trên chip không nhiều và được hạn chế đến mức tối đa, thế nên việc triển khai thực tế là hoàn toàn khả thi [3]. Hơn nữa, với việc sử dụng hệ mật dựa trên đường cong Elliptic (ECC) [12]- hệ mật được đánh giá có độ an toàn cao trong khi kích thước khoá nhỏ, thời gian tính toán nhanh và rất phù hợp để triển khai trên các thiết bị tính toán có năng lực xử lý yếu [13]. Đây là điều kiện tiên quyết đảm bảo hiệu năng của mô hình xác thực.

Ngoài ra, mô hình nêu trên hoàn toàn đáp ứng được những yêu cầu đặt ra đối với HCST như: đảm bảo tính chân thực (quy trình rõ rang); tính không thể nhân bản (sử dụng CA và PA); tính nguyên vẹn và xác thực (PA và PKI), tính liên kết công dân-HCST (sử dụng ba đặc trưng sinh trắc có độ xác thực cao nhất); kiểm soát được truy cập (PACE và EAC).

Với việc sử dụng cả ba đặc trưng sinh trắc, độ chính xác của quá trình so khớp xác thực được nâng lên. Mặc dù vậy, mô hình xác thực HCST này vẫn tồn tại nhược điểm liên quan đến vấn đề hết hạn của đầu đọc [3].

## 6. Kết luận

Việc sử dụng HCST đã minh chứng được những tính ưu việt trong việc nâng cao quá trình cấp phát và kiểm soát hộ chiếu. Với những nghiên cứu và phân tích những thế hệ đã có của HCST, chúng ta có thể nắm bắt tốt hơn ưu/nhược của từng thế hệ, từ đó có được những giải pháp phù hợp với từng loại hộ chiếu.

Với việc thử nghiệm toàn bộ chức năng trong mô hình đề xuất, chúng tôi hy vọng những kết quả này sẽ là tiền đề cho những nghiên cứu/đầu tư chuyên sâu hơn, từ đó có thể

xây dựng và sản xuất được HCST cho công dân Việt Nam mà không cần phải sử dụng lại những sản phẩm nước ngoài.

Trong thời gian tới, chúng tôi sẽ có những đánh giá cụ thể hơn về hiệu năng của mô hình xác thực, độ chính xác của quá trình xác thực các đặc trưng sinh trắc. Ngoài ra, những vấn đề như cấp/quản lý chứng chỉ số; quản lý cơ sở dữ liệu công dân có kèm theo những đặc trưng sinh trắc, cũng sẽ được chú trọng trong những hướng phát triển tiếp theo của bài báo này.

## Lời cảm ơn

Công trình này được tài trợ một phần từ đề tài nghiên cứu đặc biệt mang mã số QG.09.28, Đại học Quốc gia Hà Nội.

## References

[1] Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. *ePassport: Securing international contacts with contactless chips*. In Financial Cryptography 2008, LNCS.Springer-Verlag, 2008.

[2] Moses, T.: The Evolution of E-Passports: Extended Access Control - Protecting Biometric Data with Extended Access Control. Entrust. (August 2008)

[3] V.T.H. Minh, N.N. Hoa, "Xác thực hộ chiếu sinh trắc với cơ chế PACE và EAC", *Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ* 27 (2011) 37-51. Wikipedia, "*Biometric Passport*", http://en.wikipedia.org/wiki/Biometric_passpor, truy cập ngày 16/10/2011

[4] ICAO, *Machine Readable Travel Documents: Document 9303*, Part 1, Volumes 1 and 2, 6th edition, 2006.

[5] ICAO, *Machine Readable Travel Documents*: *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*. Version 1.1. 2004. http://www.icao.int/mrtd/download/technical.cfm

[6] R. Nithyanand. *A survey on the evolution of cryptographic protocols in epassports*. Cryptology ePrint Archive, Report 2009/200, 2009.

[7] P.T. Long, N.N. Hoa, "*Mô hình xác thực hộ chiếu điện tử*", tại Hội thảo Quốc gia "Một số vấn đề chọn lọc trong CNTT, 06/2008, Huế, Việt Nam.

[8] Delac, K., Grgic, M., Liatsis, P. (2005). "Appearance-based Statistical Methods for Face Recognition". *Proceedings of the 47th International Symposium ELMAR-2005 focused on Multimedia Systems and Applications*, Zadar, Croatia, 08-10 June 2005, pp. 151-158

[9] Mazumdar, Subhra; Dhulipala, Venkata (2008). "Biometric Security Using Finger Print Recognition". University of California, San Diego. 2010.

[10] N.N. Hoá, "*Iris Recognition for biometric passport authentication*", VNU Journal of Science, Natural Sciences and Technology 26 (2010) 14-20.

[11] Một số thư viện được sử dụng trong ứng dụng thử nghiệm: BouncyCastle - http://www.bouncycastle.org/csharp/ và CryptoSys PKI - http://www.cryptosys.net/pki/pkidotnet.html, OpenCV-http://opencv.willowgarage.com/wiki/

[12] N.N. Hoa, et al., "Mutual Authentication for RFID tag-reader by using the elliptic curve cryptography", Vietnam National University Journal of Science, Natural Sciences and Technology 24 (2008) 36-43.

[13] Dagdelen and Marc Fischlin. *Security analysis of the extended access control protocol for machine readable travel documents*. In Proceedings of the 13th international conference on Information security (ISC'10), Mike Burmester, Gene Tsudik, Spyros Magliveras, and Ivana Ili (Eds.). Springer-Verlag, Berlin, Heidelberg, 54-68, 2010.

# Image matching for the biometric passport authentication

Du Phuong Hanh, Nguyen Ngoc Hoa

*VNU University of Engineering and Technology, 144 Xuan Thuy, Hanoi, Vietnam*

Biometric passports have gone through three generations of development, initially focused on saving the image on the chip, then combining a number of factors such as image biometric iris, fingerprint image with the extended access control mechanisms and actually adding the connection established mechanism with password authentication. In this paper, we introduce our experiment to validate the third generation including also the three biometric matching techniques for authenticating a biometric passport. This experiment was performed based on different open source tools and allows us to verify the entire biometric passports authentication process. The obtained results show a good performance from both a biometric point of view and the biometric passport security.

*Keywords*: biometric passport, Extended Access Control, Password Authenticated Connenction Establishment, RFID, PKI.