

ỨNG DỤNG CÔNG NGHỆ XÁC THỰC VÂN TAY ĐA VAI TRÒ TRONG QUẢN LÝ GIÁO DỤC

Trần Thiện Chính*, Trần Huy Long*

* Viện Khoa học Kỹ thuật Bưu điện

Tóm tắt: Công nghệ xác thực vân tay đang được ứng dụng rộng rãi trong hầu hết các lĩnh vực của đời sống - kinh tế - xã hội. Hiện nay các hệ thống sử dụng vân tay làm công cụ xác thực nhận dạng người dùng đã khá phổ biến. Các hệ thống này về cơ bản gồm phần mềm quản lý vân tay và thiết bị phần cứng thu nhận vân tay. Hệ thống có khả năng xác thực theo điều kiện đơn giản bằng cách so sánh một vân tay của người dùng với cơ sở dữ liệu (CSDL) vân tay được lưu trữ trên thiết bị, nếu vân tay của người dùng trùng khớp với vân tay có trong CSDL vân tay trên thiết bị, thì điều kiện xác thực được cho là hợp lệ. Như vậy, hệ thống này không cho phép thiết lập điều kiện xác thực kết hợp, như kết hợp nhiều người dùng với nhiều vai trò đồng thời trong một phiên xác thực. Cũng như không đủ bảo đảm điều kiện an ninh, bảo mật trong môi trường kết nối mạng diện rộng và yêu cầu đòi hỏi phải có sự xác nhận của nhiều vân tay cho phiên xác thực đó. Bài viết này đề xuất ứng dụng công nghệ xác thực bảo mật đa vai trò sử dụng vân tay trong quản lý giáo dục, trên cơ sở kế thừa kết quả nghiên cứu khoa học “Phát triển, ứng dụng hệ thống xác thực bảo mật đa vai trò sử dụng vân tay trong lĩnh vực an ninh, ngân hàng”, mã số 01/2018/CNC-HĐKHNCN, thuộc Chương trình phát triển một số ngành công nghiệp công nghệ cao của Bộ Công thương [1].

Từ khóa: vân tay, xác thực vân tay, nhận dạng vân tay, cơ sở dữ liệu vân tay, xác thực vân tay đa vai trò, điều kiện xác thực, so sánh vân tay, phiên xác thực.

1. MỞ ĐẦU

Những năm gần đây, công nghệ sinh trắc học đã giải quyết được các vấn đề lớn như chi phí, cách thức vận hành và khả năng truy cập, từ đó tạo ra khả năng chính xác cao trong các giải pháp xác thực. Phương pháp xác thực sinh trắc học (Biometric) là một công nghệ sử dụng những thuộc tính vật lý hoặc các mẫu hành vi, các đặc điểm sinh học đặc trưng của con người để nhận diện như dấu vân tay, mẫu móng mắt, giọng nói, khuôn mặt, dáng đi, ... Tương tự như bất kỳ công nghệ bảo mật nào, sinh trắc học không có giải pháp hoàn hảo. Nhưng có một điều chắc chắn rằng sinh trắc học đang trở nên hiện hữu ngày nay. Trong các phương pháp nhận diện bằng đặc điểm sinh trắc học, nhận dạng bằng vân tay đã và đang được sử dụng phổ biến trong nhiều lĩnh vực của đời sống - kinh tế - xã hội.

Bởi vì đáng đi con người, gương mặt, hoặc chữ ký có thể thay đổi với thời gian và có thể được làm giả hoặc mô phỏng theo, nhưng vân tay là đường vân trên da ở đầu các ngón tay và lòng bàn tay người có đặc trưng duy nhất hoàn hảo theo từng cá thể, ổn định không thay đổi theo thời gian, dễ lưu trữ. Vân tay của mỗi người có những nét riêng biệt được giữ nguyên vẹn, cố định từ khi mới sinh ra đến khi chết. Tính riêng biệt này đã minh chứng rằng nhận dạng vân tay là chính xác và hiệu quả hơn các phương pháp nhận dạng khác. Hơn nữa, vân tay có thể được chụp ảnh, được số hóa bằng thiết bị giá thành thấp và nén hiệu quả, nên chỉ cần một dung lượng nhỏ để lưu trữ một lượng lớn dữ liệu thông tin vân tay.

Theo kết quả nghiên cứu của Dự án ứng dụng công nghệ cao “Phát triển, ứng dụng hệ thống xác thực bảo mật đa vai trò sử dụng vân tay trong lĩnh vực an ninh, ngân hàng”, mã số 01/2018/CNC-HĐKHNCN, thuộc Chương trình phát triển một số ngành công nghiệp công nghệ cao của Bộ Công thương [1], hệ thống này đã đạt được các yêu cầu đa dạng như:

i) Kiểm soát tuân thủ quy trình: Khi cần truy cập một địa điểm phải có xác thực đồng thời nhiều vân tay của những người có trách nhiệm trong quy trình thì xác thực mới hợp lệ. Ví dụ, theo quy định của quy trình quản lý tiền mặt, giấy tờ có giá, tài sản quý trong hệ thống Ngân hàng/Kho bạc Nhà nước, vấn đề đảm bảo an toàn cho các loại tài sản có giá trị này được đặc biệt quan tâm. Do vậy, mỗi lần vào/ra kho cất giữ, từng người phải ký xác nhận vào “Sổ theo dõi vào-ra”. Trước khi vào và sau khi ra, các thành viên giữ chìa khóa phải có mặt đầy đủ để chứng kiến việc mở/đóng cửa kho. Thành viên giữ chìa khóa phải tự bảo vệ bí mật mã số, chìa khóa cửa kho khi mở/đóng cửa. Nhưng khi sử dụng hệ thống truy cập đa vai trò bằng vân tay, có thể kiểm soát tuân thủ quy trình vào/ra kho bằng xác thực vân tay đồng thời của từng người có trách nhiệm liên quan (thủ kho, thủ quỹ, kế toán, người phụ trách, ...).

ii) Xác thực vân tay sử dụng thiết bị di động/cảm tay: theo đó khi cần xác định/nhận dạng một người nào đó đang không ở một địa điểm cố định (đang di chuyển), thì có thể xác định nhanh nhận dạng của người đó thông qua thiết bị cảm tay/di động để thu nhận, xác thực vân tay và thông qua kết nối mạng 3G/4G để xác thực với hệ thống trung tâm.

iii) Xác thực vân tay thay cho mã khóa số: Với mỗi khóa số có thể yêu cầu nhiều người cùng mở khóa với các mã khóa khác nhau nhằm bảo đảm an ninh, bảo mật. Nhưng đi kèm với mã khóa số chính là phải nhớ mật khẩu, mà hiện nay mật khẩu đã có nhiều phương pháp bị

Tác giả liên hệ: Trần Thiện Chính,

Email: trthchinh@gmail.com

Đến tòa soạn: 9/2020, chỉnh sửa: 10/2020, chấp nhận đăng: 10/2020.

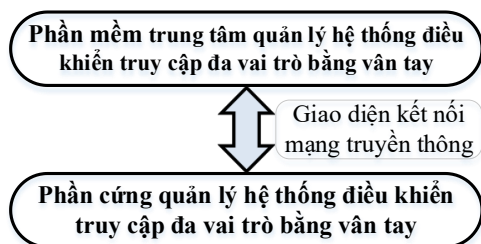
tấn công và đánh cắp khá dễ dàng. Các mật khẩu dài, phức tạp đảm bảo độ an toàn cao, nhưng lại khiến người dùng khó nhớ. Do vậy, khi sử dụng vân tay thay cho mã khóa số, mỗi thành viên tham gia mở khóa sử dụng vân tay của mình để mở khóa thay cho mật khẩu (tương ứng với mỗi chìa khóa để mở) và kết hợp với sử dụng mỗi lần cho nhiều hơn một vân tay để xác thực truy nhập (tương ứng với nhiều mã khóa số khác nhau).

Trong lĩnh vực giáo dục, chẳng hạn để quản lý các thí sinh tham dự thi, hiện đang sử dụng hệ thống thẻ/phiếu dự thi có ảnh của thí sinh kèm theo. Việc nhận dạng thí sinh phụ thuộc hoàn toàn vào giám thị và gần như chưa có hệ thống giám sát, kiểm soát đủ tin cậy. Gần đây một số nghiên cứu đang đề xuất sử dụng “thẻ thông minh - Smart card” có gắn định danh của đối tượng kết hợp với camera nhận diện khuôn mặt để quản lý đối tượng. Mặc dù ứng dụng này đang trong giai đoạn nghiên cứu, thử nghiệm, nhưng nếu như có thể triển khai được thì cũng sẽ khá phức tạp trong khâu phát hành thẻ, hệ thống đọc thẻ và lưu trữ, hệ thống nhận diện khuôn mặt, ... cũng đòi hỏi phải đồng bộ. Điều này chắc chắn sẽ rất phức tạp và tốn kém chi phí. Ngoài ra, nếu sử dụng hệ thống nhận dạng vân tay thông dụng hiện có trên thị trường để quản lý thí sinh dự thi, thì sự đơn giản, kém bảo mật cũng như độ tin cậy không cao của hệ thống sẽ khó có thể cho phép đáp ứng được yêu cầu quản lý. Bởi các sản phẩm nhận dạng vân tay hiện có đều dựa trên khả năng xác thực “đơn vân tay” theo điều kiện đơn giản, bằng cách so sánh vân tay của một người dùng/thí sinh với CSDL vân tay trên máy chủ CSDL, nếu vân tay của thí sinh trùng khớp với vân tay có trong CSDL vân tay trên thiết bị, thì điều kiện xác thực được cho là hợp lệ. Nhưng khi mà số lượng thí sinh tham dự rất lớn, tập trung trong thời gian ngắn thì hệ thống khó có thể đảm bảo đáp ứng yêu cầu.

Do vậy, nếu áp dụng hệ thống xác thực đa vai trò sử dụng vân tay trong quản lý đối tượng/thí sinh tham dự kỳ thi, thì việc nhận dạng có thể sử dụng vân tay (thay cho thẻ/phiếu dự thi), hơn nữa có thể sử dụng nhiều vân tay của thí sinh (có thể xác thực lên tới 10 vân tay). Trường hợp cần bảo đảm an ninh, an toàn hơn có thể kết hợp với xác nhận của những người quản lý liên quan để nhận dạng đúng chính xác thí sinh của trường, lớp, địa phương, khi này cần có xác nhận thêm như: của các giáo viên chủ nhiệm, giáo viên phụ trách bộ môn, giám hiệu, trường, người giám hộ (nếu có), ... Việc xác nhận này thông qua sử dụng xác thực vân tay của những người có trách nhiệm liên quan, đó chính là yếu tố đa vai trò trong quản lý đối tượng/thí sinh.

II. KHÁI QUÁT HỆ THỐNG XÁC THỰC VÂN TAY ĐA VAI TRÒ

Thiết kế kiến trúc hệ thống xác thực vân tay đa vai trò gồm hai phần như Hình 1 [1]:



Hình 1. Kiến trúc hệ thống xác thực đa vai trò bằng vân tay



Hình 2. Thiết bị xác thực vân tay đa vai trò UCS-MFA-Fix

Phần cứng thiết bị nhận dạng vân tay (Hình 2): Với thành phần cốt lõi là phần mềm nhúng ứng dụng (phần mềm sụn) nạp trong chip vi điều khiển; bên cạnh đó còn có các thành phần khác như: bo mạch chủ xử lý với các chip vi điều khiển và các vi mạch IC phụ trợ; đầu đọc vân tay cảm biến quang; màn hình hiển thị; loa, bàn phím; các cổng điều khiển vào ra; các cổng giao diện mạng truyền thông; v.v... Ngoài ra, phần cứng hệ thống cũng có thể bao gồm hệ thống máy chủ trung tâm được cài đặt ứng dụng giao diện web, truyền thông qua mạng với bo mạch chủ xử lý để giám sát, cấu hình từ xa bo mạch chủ và các thiết bị phần cứng khác. Việc truyền thông giữa máy chủ trung tâm và bo mạch chủ xử lý thông qua các phương tiện truyền thông có dây/hữu tuyến hoặc không dây/vô tuyến, qua mạng IP (ví dụ, mạng Ethernet, LAN, WLAN, 3G/4G, ...), hoặc kết nối trực tiếp. Phần cứng cho phép cấu hình nhiều người dùng với nhiều vai trò khác nhau. Truy cập hệ thống được xem như hợp lệ khi đồng thời nhiều người dùng với đầy đủ các vai trò cùng truy cập xác thực bằng vân tay trong một khoảng thời gian xác định, được cấu hình bởi nhà quản trị. Các truy cập hệ thống không hợp lệ khi những người dùng xác thực không đủ các vai trò, hoặc quá thời hạn xác thực. Khi truy cập hệ thống không hợp lệ, phần cứng sẽ gửi cảnh báo thông qua kết nối mạng đến phần mềm trung tâm quản lý (sử dụng giao thức truyền thông chuẩn). Phần mềm nhúng các ứng dụng tùy chỉnh động chuyên biệt gồm: xác thực bảo mật đa vai trò; cảnh báo cục bộ và trung tâm; ghi thông tin theo dõi cục bộ; hỗ trợ 10 vân tay cho mỗi người dùng; hỗ trợ tối thiểu 50 người dùng (với thiết bị đơn lẻ tại chỗ); thêm, sửa, xóa, gán vai trò người dùng; đăng ký liên tục trong một phiên đăng ký; bảo mật bằng mật khẩu; cấu hình thông qua giao diện Web; hủy phiên xác thực; bảo toàn dữ liệu khi mất nguồn; hiển thị thông tin; kiểm tra tình trạng kết nối mạng; xác thực hợp lệ khi đồng thời nhiều người dùng, với nhiều vai trò đồng thời được xác thực bằng vân tay; bất hợp lệ phiên xác thực sau một khoảng thời gian.

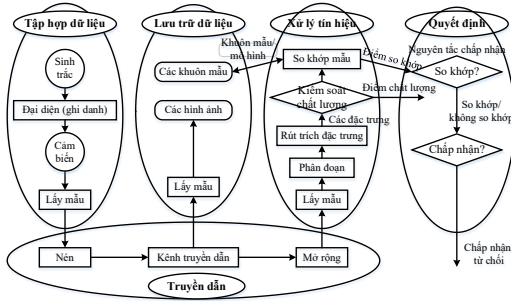
Phần mềm Trung tâm quản lý hệ thống điều khiển truy cập đa vai trò bằng vân tay thực hiện chức năng: quản lý nhóm người dùng (có khả năng mở rộng lên hàng triệu người dùng); Phân quyền sử dụng cho người dùng; nhập và lựa chọn ưu tiên từng vai trò (thành phần) trong nhóm xác thực; giám sát, cảnh báo tức thời về thành phần truy cập, thời gian thực hiện xác thực truy cập; tạo các báo cáo dữ liệu truy cập, cảnh báo (theo thời gian và mã truy cập); lọc dữ liệu theo thời gian và chiết xuất File lưu trữ dưới dạng “.pdf” có hiển thị ngày, giờ chiết xuất File từ hệ thống; lưu trữ dữ liệu trong thời gian 1 năm (12 tháng); cấu hình thiết bị xác thực vân tay từ xa qua kết nối mạng Internet; khả năng quản lý tối thiểu 300 thiết bị xác thực bảo mật vân tay đa vai trò.

III. ĐỀ XUẤT ỨNG DỤNG CÔNG NGHỆ XÁC THỰC ĐA VAI TRÒ SỬ DỤNG VÂN TAY TRONG QUẢN LÝ GIÁO DỤC

1. Mô hình hệ thống xác thực sinh trắc học tổng quát

Một hệ thống xác thực sinh trắc học tổng quát được chia thành 5 phân hệ dựa trên các chức năng của nó như thể hiện trên Hình 3: 1) Tập hợp dữ liệu; 2) Truyền phát dữ liệu; 3) Xử lý dữ liệu; 4) Quyết định; 5) Lưu trữ dữ liệu [2].

Ở mức cơ bản nhất, công nghệ sinh trắc là hệ thống nhận dạng mẫu, ở đó hoặc là sử dụng thiết bị thu thập hình ảnh (như máy quét hoặc máy ảnh trong trường hợp công nghệ nhận dạng vân tay hoặc móng mắt), hoặc là thiết bị thu nhận âm thanh/chuyển động (như micro hoặc đĩa trong trường hợp công nghệ nhận dạng giọng nói/chữ ký) để thu thập các mẫu hoặc đặc điểm sinh trắc học. Đặc điểm của các mẫu thu được xem như khác biệt nhất giữa những người dùng và ổn định nhất đối với mỗi người dùng đã được trích xuất, mã hóa thành một tham chiếu hoặc mẫu sinh trắc học biểu diễn toàn học đặc trưng sinh trắc học một người. Các mẫu này được lưu trữ trong CSDL, hoặc trên thẻ thông minh, hoặc thẻ xác thực khác và được sử dụng để so sánh khi bảo đảm an toàn nhận dạng. Hệ thống sinh trắc học được tự động hóa bởi phần cứng và phần mềm, cho phép đưa ra quyết định nhanh chóng, theo thời gian thực.



Hình 3. Mô hình hệ thống sinh trắc học tổng quát

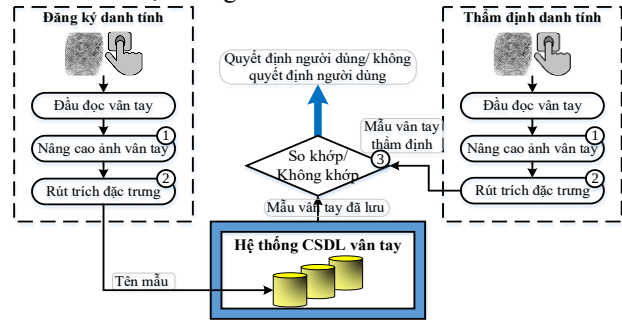
2. Mô hình Hệ thống nhận dạng vân tay tự động (AFIS)

Mô hình Hệ thống nhận dạng vân tay tự động (AFIS) như Hình 4 thể hiện 3 bước chính của AFIS, bước (1) “Kỹ thuật nâng cao ảnh vân tay”, bước 2 “Kỹ thuật rút trích đặc trưng”, bước 3 “Kỹ thuật so khớp đặc trưng” [3].

1) Bước 1 “Kỹ thuật nâng cao ảnh vân tay”: Chụp ảnh dấu vân tay bằng thiết bị cảm biến, có thể cho chất lượng hình ảnh khác nhau tùy thuộc vào loại thiết bị cảm biến hoặc nhiễu của môi trường. Do đó, mục tiêu cơ bản của kỹ thuật nâng cao ảnh là cải thiện chất lượng hình ảnh và loại bỏ nhiễu, sử dụng hai kỹ thuật: i) “Kỹ thuật lọc Gabor cô điển” gồm 6 bước để cho chất lượng ảnh tốt hơn gồm chuẩn hóa, lọc biến đổi Fourier nhanh (FFT), phân đoạn, hướng rãnh vân tay, tần số vân tay, bộ lọc Gabor; ii) “Kỹ thuật lọc biến đổi Fourier nhanh”.

2) Bước 2 “Kỹ thuật rút trích đặc trưng”: Một ảnh vân tay được nâng cao, các đặc trưng vân tay có thể được rút trích và biểu diễn theo các điểm ảnh và đường vân. Kỹ thuật này có 3 bước chính là nhị phân hóa, làm mỏng, rút trích các điểm đặc trưng.

3) Bước 3 “Kỹ thuật so khớp đặc trưng”: Kỹ thuật này là bước cuối cùng trong AFIS và được sử dụng để quyết định xem hai dấu vân tay có khớp hay không bằng cách so sánh các đặc trưng của nó.



Hình 4. Mô hình hệ thống nhận dạng vân tay tự động

3. Đề xuất xây dựng kiến trúc AFIS trong quản lý giáo dục

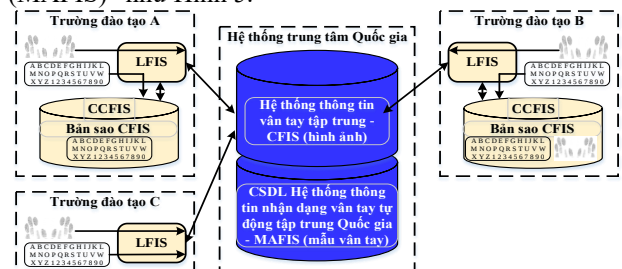
Kiến trúc AFIS trong quản lý giáo dục ở cấp độ Quốc gia được đề xuất trên hai khía cạnh: tương tác giữa các Trường đào tạo với Hệ thống tập trung Quốc gia (Bộ Giáo dục và Đào tạo) và tổ chức quản lý nội bộ của chính hệ thống AFIS. Các lựa chọn tiềm năng cho kiến trúc khả thi các chức năng AFIS dựa trên các yếu tố sau [4]:

- Kiến trúc của AFIS gồm một hệ thống tập trung xử lý 20% truy vấn chung và truy vấn từ xa của các Trường đào tạo không có bản sao dữ liệu tại chỗ. 80% truy vấn của các Trường đào tạo còn lại không có quyền truy cập trực tiếp vào hệ thống tập trung, do các Trường đào tạo này vẫn có bản sao dữ liệu cục bộ. Do vậy, cần phải có AFIS tại hệ thống tập trung, để cung cấp chức năng truy vấn từ xa cho những Trường đào tạo không có bản sao dữ liệu cục bộ và cho các Trường có thể bị xảy ra sự cố kỹ thuật tạm thời với bản sao dữ liệu cục bộ.

- Tất cả các Trường đào tạo sử dụng hệ thống tập trung để tạo, cập nhật và xóa (CUD) cảnh báo. Việc đưa ra một cảnh báo sẽ yêu cầu, chẳng hạn như một vấn đề nhất quán, kiểm tra chất lượng tại hệ thống tập trung do AFIS vận hành. Bất kỳ xử lý một cảnh báo nào đều được gửi đến hệ thống tập trung, sau đó sẽ truyền phát tới các bản sao dữ liệu cục bộ hiện có.

- Việc tìm kiếm trong bản sao dữ liệu cục bộ tạo ra kết quả tương đương với kết quả tìm kiếm trong CSDL tập trung. AFIS hoạt động trên bản sao dữ liệu cục bộ sẽ phải cung cấp cùng một kết quả nhận dạng (độ chính xác, hành vi) như trên hệ thống CSDL tập trung.

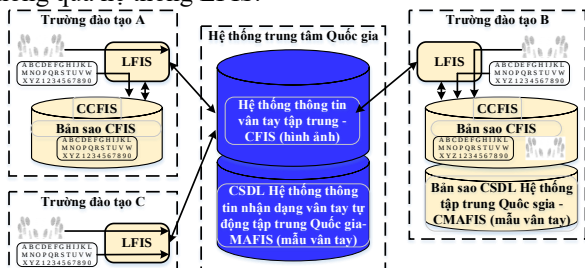
1) Đề xuất 1 “Chỉ duy nhất AFIS hoạt động trên Hệ thống thông tin nhận dạng vân tay tập trung Quốc gia (MAFIS)” như Hình 5.



Hình 5. Mô hình AFIS hoạt động trên hệ thống tập trung Quốc gia (MAFIS)

Trong đề xuất này dự kiến chỉ duy nhất chức năng MAFIS được cung cấp bởi Hệ thống thông tin vân tay tập trung (CFIS). Với Trường đào tạo B có bản sao dữ liệu của hệ thống thông tin vân tay tập trung (CCFIS), sẽ thực hiện truy vấn vào Hệ thống MAFIS bất cứ khi nào cần nhận dạng vân tay thông qua Hệ thống thông tin vân tay cục bộ (LFIS). Tuy nhiên, khi sử dụng chuyên gia để xác nhận kết quả thủ công, thì ảnh vân tay được lưu trữ trong CCFIS cũng có thể được sử dụng để giảm bớt lưu lượng truy cập tới hệ thống MAFIS. Với Trường đào tạo A chỉ có bản sao dữ liệu chữ và số, hoặc Trường đào tạo C thậm chí không có bản sao dữ liệu, sẽ hoàn toàn dựa vào hệ thống MAFIS thông qua hệ thống truy nhập LFIS. CCFIS chỉ chứa ảnh vân tay, còn hệ thống trung tâm MAFIS sẽ lưu trữ toàn bộ mẫu vân tay (vân tay đã mã hóa) của tất cả các Trường đào tạo.

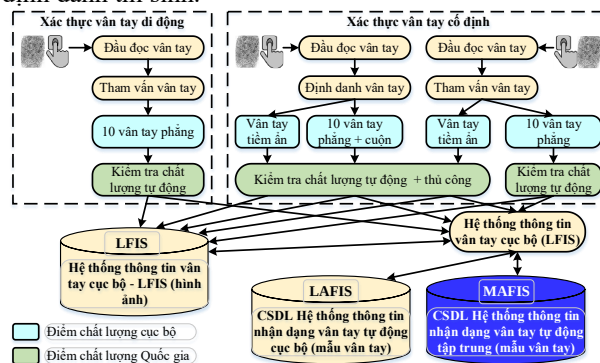
2) Đề xuất 2 “AFIS hoạt động trên hệ thống thông tin nhận dạng vân tay tập trung Quốc gia (MAFIS) và bản sao CSDL hệ thống thông tin nhận dạng vân tay tự động tập trung (CMAFIS)”: Như Hình 6, trong đề xuất này dự kiến cũng chỉ duy nhất chức năng MAFIS được cung cấp bởi Hệ thống CFIS. Với Trường đào tạo B đã có bản sao CSDL đầy đủ của Hệ thống MAFIS, khi cần nhận dạng vân tay sẽ truy vấn vào CMAFIS thông qua Hệ thống LFIS, mà không cần phải truy nhập vào hệ thống MAFIS. Tương tự như trên, với Trường đào tạo A chỉ có bản sao dữ liệu chữ và số, hoặc với Trường đào tạo C không có bản sao dữ liệu, sẽ hoàn toàn dựa vào hệ thống MAFIS thông qua hệ thống LFIS.



Hình 6. Mô hình AFIS hoạt động trên hệ thống tập trung Quốc gia (MAFIS) và bản sao CSDL hệ thống tập trung (CMAFIS)

3) Đề xuất 3 “Kiến trúc Hệ thống xác thực vân tay ứng dụng trong quản lý giáo dục”: Hình 7 mô tả kiến trúc hệ thống xác thực vân tay ứng dụng trong quản lý giáo dục. Hệ thống được thực hiện dưới hai hình thức, xác thực vân tay cố định (tại điểm tập trung Quốc gia, trường, địa phương, ...) và xác thực vân tay di động (tại điểm thi có chức năng xác thực). Trường hợp xác thực vân tay cố định, nếu trong CSDL hệ thống thông tin nhận dạng vân tay tự động cục bộ (của Trường đào tạo) đã có chứa bản sao dấu vân tay đầy đủ của thí sinh, thì hệ thống sẽ kiểm tra chất lượng dấu vân tay tự động với các dạng vân tay tiềm ẩn (là những hình ảnh vân tay vô tình để lại do ngón tay để lại trên bề mặt vật thể) và dạng vân tay phẳng (là những hình ảnh vân tay để lại do ngón tay ấn xuống bề mặt phẳng), vân tay cuộn để tự động định danh thí sinh. Nếu trong CSDL hệ thống của Trường đào tạo không chứa bản sao dấu vân tay đầy đủ, hoặc có nhưng không đầy đủ, hoặc phải truy vấn từ CSDL hệ thống thông tin nhận dạng vân tay tự động Quốc gia (của Bộ Giáo dục và Đào tạo), thì hệ thống sẽ kiểm tra chất lượng dấu vân tay thủ công với các dạng vân tay tiềm ẩn và dạng vân tay

phẳng thông qua tham vấn chuyên gia để định danh thí sinh. Trường hợp xác thực vân tay di động, hệ thống sẽ kiểm tra chất lượng dấu vân tay tự động với dạng vân tay phẳng dưới sự kiểm soát/tham vấn của chuyên gia để định danh thí sinh.



Hình 7. Kiến trúc Hệ thống đăng ký vân tay ứng dụng trong quản lý giáo dục

4) Đề xuất 4 “Kết hợp hệ thống xác thực vân tay với hệ thống nhận diện khuôn mặt ứng dụng trong quản lý giáo dục”: Theo đó, ngoài việc sử dụng hệ thống xác thực vân tay dạng theo các đề xuất ở trên, sẽ kết hợp/tích hợp với hệ thống camera nhận diện khuôn mặt để tăng cường thêm độ chính xác, an toàn của hoạt động xác thực và bảo mật đối với thí sinh.

IV. KẾT LUẬN

Hệ thống xác thực vân tay đa vai trò đã được nghiên cứu và hoàn thiện trên cơ sở kết quả của Dự án ứng dụng công nghệ cao “Phát triển, ứng dụng hệ thống xác thực bảo mật đa vai trò sử dụng vân tay trong lĩnh vực an ninh, ngân hàng”, mã số 01/2018/CNC-HĐKHNC, thuộc Chương trình phát triển một số ngành công nghiệp công nghệ cao của Bộ Công thương [1]. Từ kết quả nghiên cứu đã đạt được, nhóm thực hiện đề tài đề xuất mô hình và kiến trúc ứng dụng công nghệ xác thực, bảo mật đa vai trò sử dụng vân tay trong quản lý giáo dục. Cụ thể là trong quản lý thí sinh dự thi, nhằm thay thế việc chứng nhận và xác thực thí sinh bằng hệ thống thẻ/phiếu dự thi có ảnh của thí sinh kèm theo thông qua giám thị, vừa phức tạp, tốn kém vừa chưa đủ độ tin cậy. Khi sử dụng hệ thống xác thực đa vai trò sử dụng vân tay, sẽ cho phép thí sinh dự thi chỉ cần đăng ký dấu vân tay (thay cho đăng ký lấy phiếu/thẻ dự thi), khi tham dự thi, thí sinh sẽ sử dụng vân tay của mình để xác thực định danh vào phòng thi (thay cho xuất trình thẻ/phiếu dự thi để giám thị kiểm tra cho vào phòng thi). Đồng thời, có thể kết hợp với việc xác nhận/chứng thực của nhà trường thông qua xác thực đa vai trò sử dụng vân tay của giáo viên chủ nhiệm, hoặc Ban giám hiệu, hoặc người giám hộ, ... (tránh được gian lận trong đăng ký dự thi). Điều này vừa đơn giản, ít tốn kém chi phí tổ chức dự thi, vừa có khả năng bảo mật, lưu trữ dữ liệu “dưới dạng số” và nhất là tránh phiền phức cho thí sinh trong việc bị quên hoặc làm mất thẻ/phiếu dự thi. Hơn nữa, nếu hệ thống xác thực quản lý thí sinh được liên kết với hệ thống CSDL quản lý dân cư (đã lưu trữ sẵn định danh của thí sinh trên 14 tuổi), thì sẽ rất thuận tiện và đơn giản hóa thủ tục đăng ký dự thi.

TÀI LIỆU THAM KHẢO

- [1] Trần Thiện Chính và các cộng sự, Báo cáo tổng hợp và Báo cáo các chuyên đề NCKH thuộc Dự án ứng dụng công nghệ cao “Phát triển, ứng dụng hệ thống xác thực bảo mật đa vai trò sử dụng vân tay trong lĩnh vực an ninh, ngân hàng”, mã số 01/2018/CNC-HĐKHCN, Viện Khoa học Kỹ thuật Bưu điện, 03/2020.
- [2] James Wayman, Anil Jain, Davide Matoni and Dario Maio (Eds), Biometric Systems: Technology, Design and Performance Evaluation, ISBN 1-85233-596-3 Springer-Verlag London Berlin Heidelberg, @ Springer-Verlag London Limited 2005.
- [3] Ezdihar N. Bifari, Lamiaa A. Elrefaei, Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm, 978-1-4799-3080-7114/\$31.00 ©2014 IEEE.
- [4] Laurent Beslay, Javier Galbally, Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II), JRC Science for Policy Report, JRC 33516-2014.

MULTI-ROLE FINGERPRINT AUTHENTICATION TECHNOLOGY APPLYING TO EDUCATION MANAGEMENT

Abstract: Fingerprint authentication technology is being widely applied in almost all fields of life - economy - society. Currently, systems using fingerprints as tools to authenticate users' identification are quite popular. These systems are basically two parts as fingerprint management software and hardware device to recognize/authentication fingerprint with the ability to authenticate under simple conditions by comparing a pattern of user's fingerprint with the fingerprint database (database) stored on the device, if the user's fingerprint matches the one in the fingerprint database on the device, then authentication condition is considered valid. As such, this system does not allow to set up association authentication conditions such as combining multiple users with many concurrent roles in one authentication session. Also inadequate to ensure security and confidentiality in a wide area network connection environment and requires multiple fingerprint authentication for that authentication session. This article proposes the application of multi-role fingerprint security authentication technology in educational management, on the basis of inheriting scientific research results “Development and application of multi-role security authentication system using fingerprints in the security and banking sector”, code No. 01/2018/CNC-HĐKHCN, under the Program on developing a number of high-tech industries of the Ministry of Industry and Trade.

Keywords: fingerprint, fingerprint authentication, fingerprint identification, fingerprint database, multi-role fingerprint authentication, authentication conditions, fingerprint comparison, session authentication.



Tran Thien Chinh was born in 1967. He got Bachelor degree in University of Transport and Communications (UTC) in 1991 and hold visiting lecturers at the at the University. He then got a PhD. specialist "Networks and Communications" from Posts and Telecommunications Institute of Technology in 2005. Currently he is deputy director of the Research Institute of Posts and Telecommunications. Main research directions: Research and development of Internet of Things (IoT) applications in the fields of telecommunications, smart transportation, smart agriculture, intelligent environment management, smart health, etc. Research and development of security and security applications in information communication technology (ICT), in which focus on wireless sensor network (WSN). Research and develop processing, control and automation systems for the application of economic and communal fields festival. In which focus on smart city, smart transportation.

Email: trthcinhh@gmail.com



Tran Huy Long received the B.E degree in Telecommunications Engineering from Electric Power University, in 2013 and the Master degree from Posts and Telecommunications Institute of Technology in 2015. Currently, he is a postgraduate of University of Communications and Transport, Hanoi. He is a researcher in Research Institute of Posts and Telecommunications. His current research interest is information security, Routing security, wireless communications, WSN.

Email: huylong.ript@gmail.com