Sử dụng vân tay và hệ mật RSA để bảo mật HỆ THỐNG CƠ SỞ DỮ LIỆU DÂN TỘC

>HOÀNG VĨNH HÀ*, TRỊNH VĂN ANH**

Công nghệ thông tin ngày càng trở thành một trong những động lực quan trọng đối với sự phát triển kinh tế - xã hội. Cùng với sự phát triển của máy tính điện tử, truyền thông phát triển kéo theo sự ra đời và phát triển của mạng máy tính, từ các mạng cục bộ, mạng diện rộng cho tới mạng toàn cầu Internet và xa lộ thông tin. Việc thông tin chuyển sang dạng số và kết nối mạng đã làm thay đổi sự chuyển hóa của nền kinh tế, các dạng thể chế, các mối quan hệ và bản chất của hoạt động kinh tế - xã hội và có ảnh hưởng sâu sắc đến hầu hết các lĩnh vực hoạt động và đời sống con người, trong đó có hoạt động giao dịch cơ sở dữ liệu. Để những giao dịch cơ sở dữ liệu đạt được lợi ích tối đa, việc tìm lời giải cho bài toán đảm bảo an ninh an toàn thông tin cho dữ liệu là rất quan trọng. Trong đó, có 9 yếu tố cần được đảm bảo đó là: Bảo vệ toàn vẹn cơ sở dữ liệu; Bảo vệ chống truy cập trái phép; Bảo vệ chống suy diễn; Toàn vẹn dữ liệu thao tác; Toàn vẹn ngữ nghĩa của dữ liệu; Khả năng lưu vết và kiểm tra; Xác thực người dùng; Bảo vệ dữ liệu nhạy cảm; và Bảo vệ nhiều mức.

Dựa trên những nguyên tắc chung đối với việc bảo vệ cơ sở dữ liệu, nhóm tác giả đề xuất giải pháp kết hợp sinh trắc học (cụ thể là nhận dạng vân tay) và hệ mã công khai RSA để hệ thống cơ sở dữ liệu Dân tộc có tính an toàn cao hơn.

1. TỔNG QUAN VỀ HỆ MÃ RSA VÀ NHẬN DẠNG VÂN TAY

Hệ mã RSA

RSA là một trong những cơ chế khoá công khai đầu tiên được phát triển vào năm 1977 bởi Ron Rivest, Adi Shamir và Len Adleman tại MIT và xuất bản lần đầu vào năm 1978 là RSA (tên viết tắt của ba tác giả). RSA là một thuật toán mã hóa khối, trong đó các bản rõ và bản mã là các số nguyên giữa 0 và n - 1.

* Trung tâm Thông tin - Ủy ban Dân tộc

** Trường Đại học Văn hóa Thể thao và Du lịch Thanh Hóa

Thuật toán tạo khoá như sau:

1. Để tạo ra một cặp khóa RSA, trước hết, chọn hai số nguyên tố đủ lớn p và q. Tính n=p*q và Φ(n) = (p-1)(q-1)
2. Chọn một số e sao cho e và Φ(n) = (p-1)(q-1) là hai số nguyên tố cùng nhau. Tìm số d sao cho ed = 1 mod Φ(n). Ký hiệu "mod m" biểu diễn phép modulo trên cơ số m.
3. Khoá Công bố số n và khóa công khai (Public key): (n, e) trong danh bạ khoá công khai Khóa bí mật (Private) là tổ hợp (n, d).
4. Việc mã hóa một khối thông tin gốc M được thực hiện theo công thức:

   Người gửi A nhận khoá công khai của người nhận (n, e)

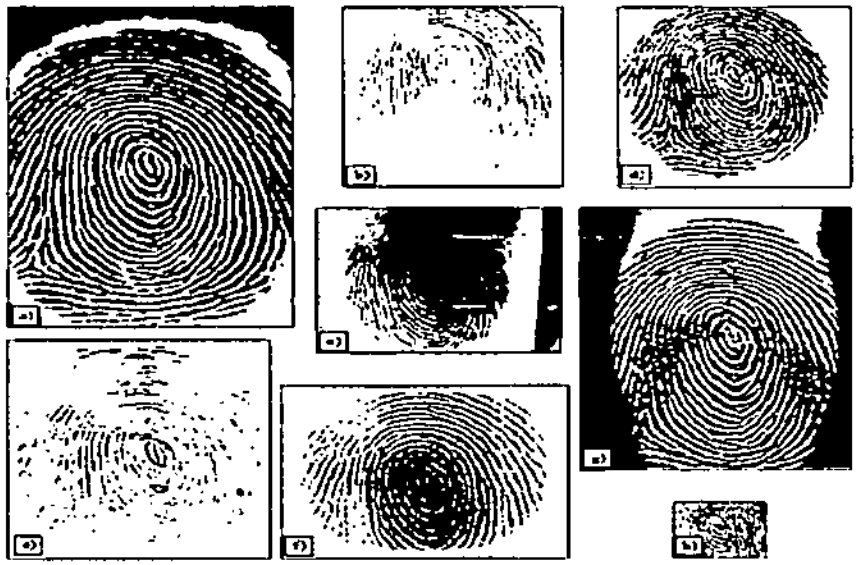
   Người gửi A biểu diễn thông tin cần gửi thành số M (0 ≤ M ≤ n-1)

   Mã hoá C = $M^e \bmod n$
5. Và quá trình giải mã C được thực hiện theo công thức:

   M = $C^d \bmod n$

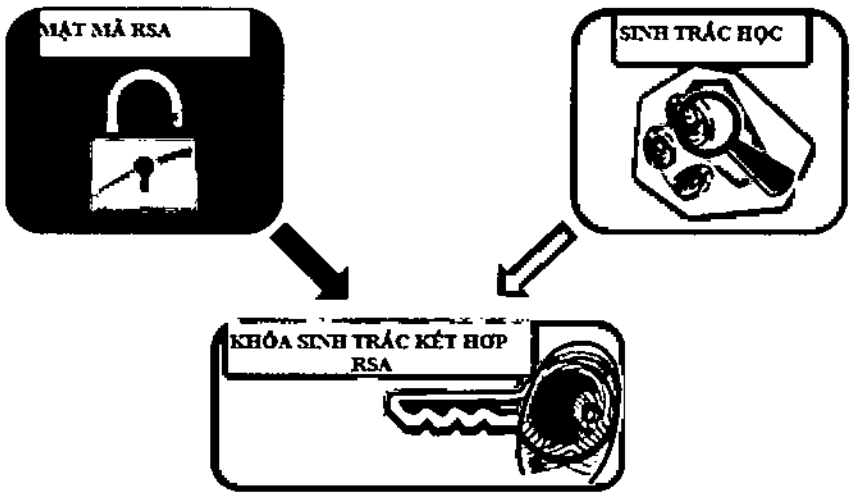
Nhận dạng vân tay

Vân tay là một đặc điểm sinh trắc học của con người, nhận dạng vân tay là hệ thống xác thực một cá nhân bằng cách tìm kiếm và đối sánh đặc tính dấu vân tay của người dùng với toàn bộ các mẫu sinh trắc được lưu giữ trong cơ sở dữ liệu. Cơ sở nhận dạng vân tay là những đặc điểm riêng biệt trong cấu tạo của các vân tay khác nhau. Dấu vân tay của mỗi cá nhân là độc nhất. Xác suất hai cá nhân - thậm chí ngay cả anh em (hoặc chị em) sinh đôi cùng trứng - có cùng một bộ dấu vân tay là 1 trên 64 tỉ. Ngay cả các ngón trên cùng bàn tay cũng có vân khác nhau. Dấu vân tay của mỗi người là không đổi trong suốt cuộc đời. Người ta có thể làm phẫu thuật thay da ngón tay, nhưng chỉ sau một thời gian dấu vân tay lại được hồi phục như ban đầu.

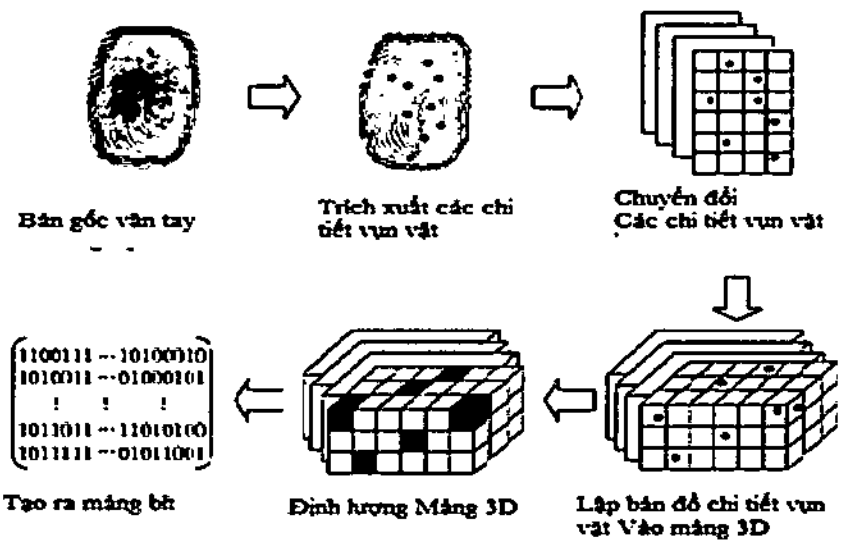


Hình 1. Ảnh vân tay được chụp từ các thiết bị tương ứng

Đầu tiên một người sẽ cung cấp dấu vân tay cùng với thông tin hoặc đặc điểm cá nhân của người đó như họ tên, ngày sinh, quê quán... (trong chứng minh thư) hoặc là User name, tên tài khoản, các quyền hạn của người đó,... (trong bảo mật). Bước này nhằm tạo ra một cơ sở dữ liệu tương ứng dấu vân tay và các đặc điểm liên quan. Nguyên lý cơ bản của hệ thống này là sử dụng các diot phát sáng để truyền các tia gần hồng ngoại (Near Infrared NIR) tới ngón tay và chúng sẽ được hấp thụ lại bởi hồng cầu trong máu. Vùng các tia bị hấp thụ trở thành vùng tối trong hình ảnh và được chụp lại bởi camera CCD. Sau đó, hình ảnh được xử lý và tạo ra mẫu vân tay. Mẫu vân tay được chuyển đổi thành tín hiệu số và là dữ liệu để nhận dạng người sử dụng chỉ trong vòng chưa đến 2 giây. Công nghệ truyền ánh sáng của Hitachi cho phép ghi lại rõ nét sơ đồ vân nhờ độ tương phản cao và khả năng tương thích với mọi loại da tay, kể cả da khô, da dầu hay có vết bẩn, vết nhăn hoặc bị khiếm khuyết do tạo hoá trên bề mặt của các ngón tay. Lượng dữ liệu nhỏ đó là căn cứ cho việc nhận dạng và tạo nên một hệ thống nhỏ gọn, an toàn, thân thiện và nhanh nhất trên thế giới. Hệ thống này có thể lưu trữ từ 6.000 - 8.000 vân ngón tay trong một máy và mỗi người có thể được nhận dạng bởi 1 trong 5 vân ngón tay khác nhau đã đăng ký trước đó. Ưu điểm vượt trội của hệ thống này là chỉ tương tác với cơ thể sống nên việc bắt chước, giả mạo hoặc ăn cắp dữ liệu là điều hoàn toàn bất khả thi. FVB ra đời hồi đầu năm 2006, đã nhanh chóng thành công tại thị trường Nhật Bản, Singapor, Trung Quốc... Hiện nay, trên thị trường thế giới đã có bán nhiều loại thiết bị chụp vân tay (fingerprint reader, fingerprint scanner) với các chất lượng khác



Hình 2. Hệ thống được đề xuất



Hình 3. Quá trình tạo bít từ dấu vân tay

nhau. Một số ảnh vân tay được chụp từ các thiết bị này trong Hình 1.

Dấu vân tay sẽ được đưa thu thập từ một cảm biến (sensor) để đối chiếu với cơ sở dữ liệu các vân tay để truy ra các đặc điểm muốn truy xuất. Việc đối sánh ảnh vân tay cần nhận dạng chỉ cần được tiến hành trên các vân tay (có trong cơ sở dữ liệu) thuộc loại đã được xác định nhờ quá trình phân loại. Đây là giai đoạn quyết định xem hai ảnh vân tay có hoàn toàn giống nhau hay không và đưa ra kết quả nhận dạng, tức là ảnh vân tay cần nhận dạng tương ứng với vân tay của cá thể nào đã được lưu trữ trong cơ sở dữ liệu.

2. HỆ THỐNG AN TOÀN KẾT HỢP SINH TRẮC HỌC VÀ HỆ MÃ RSA CHO CƠ SỞ DỮ LIỆU DÂN TỘC

Mô hình

Hệ thống vân tay RSA bao gồm 2 modul chính là modul vân tay và hệ mật mã RSA. Để tạo ra được hệ thống an toàn dựa trên đặc điểm sinh học trên cơ thể người kết hợp với hệ mật mã khóa công khai RSA như Hình 2, các modul vân tay dựa trên các đặc điểm riêng, vụn vặt của vân tay như điểm chết, điểm cao, tần số vân. Modul tổng hợp là modul kết hợp giữa Mật mã RSA và Sinh trắc học, tại modul này sự kết hợp giữa sinh trắc học và mật mã RSA tạo nên hệ thống khóa sinh trắc kết hợp RSA.

Quá trình tạo bít từ dấu vân tay

Bản gốc vân tay được lưu trữ lấy theo định danh vân tay xác thực chủ thể người có vân tay gốc sau đó chuyển hóa, lọc, tách các chi tiết vụn vặt, các đặc điểm khác nhau. Chuyển đổi các chi tiết vụn vặt và lập bản đồ chi tiết vụn vặt vào mảng 3D. Từ mảng 3D đế định lượng Mảng và chuyển hóa sang mảng bít (Hình 3).

Hệ thống xác thực vân tay

Bước 1: Dấu vân tay được kết hợp với thuật toán RSA mã hóa công khai (ở đây dấu vân tay được xác thực định danh) sau đó kết hợp RSA.

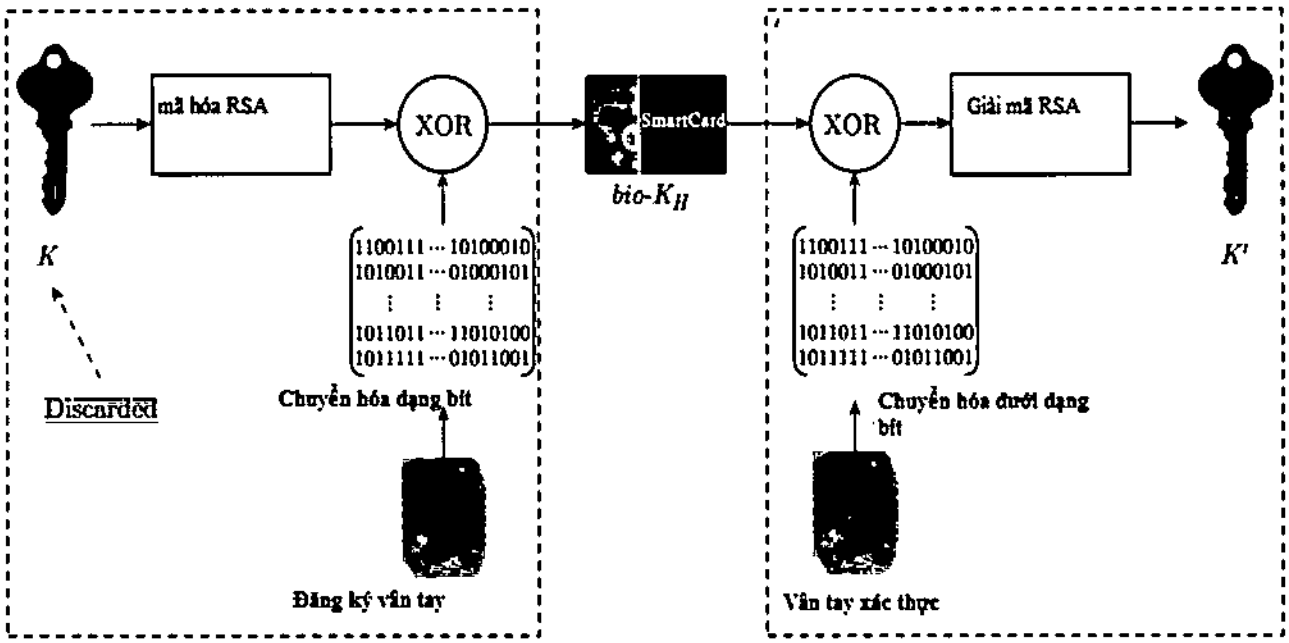
Bước 2: Sau khi khóa được kết hợp hình thành được tích hợp trong thẻ Bio như Hình 4.

Bước 3: Dữ liệu tích hợp trong thẻ Bio được xác thực lại bằng khóa vân tay xác thực (nếu xác thực thành công) cho phép giải mã khóa K để đăng nhập vào hệ thống cơ sở dữ liệu.

Hoạt động của Hệ thống kết hợp sinh trắc học và mật mã học

Hoạt động của hệ thống như sau:

1. Người dùng quét vân tay.



Hình 4. Quá trình xác thực vân tay

2. Đặc trưng vân tay (Minutiae) của người dùng được sinh ra.

3. Minutiae được gửi cho User Registration.

4. Minutiae được mã hóa bằng password của người dùng.

5. Băm password của người dùng.

6. Gửi user cho Database access.

7. Gửi mã băm password cho Database Access.

8. Tạo profile từ thông tin của người dùng.

9. Gửi profile cho Database Access.

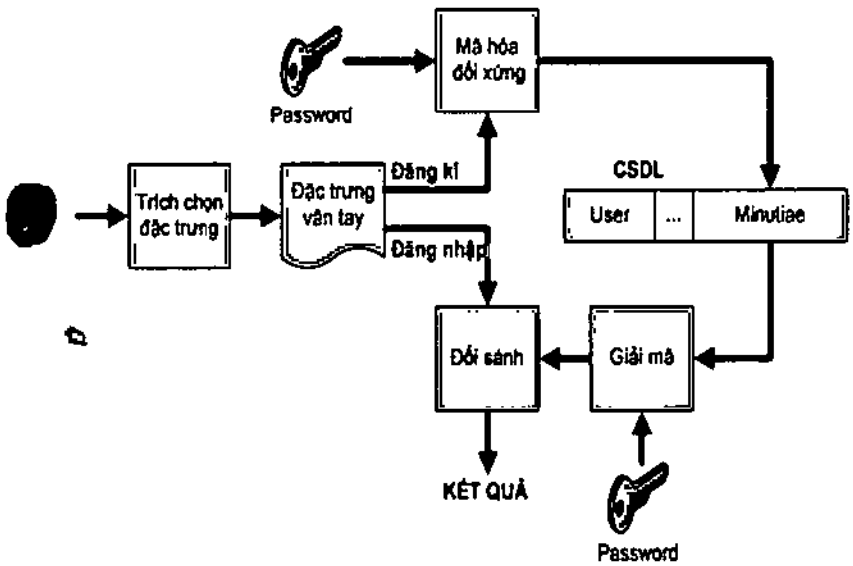
10. Gửi Minutiae đã mã hóa cho Database Access.

11. Database lưu trữ tất cả các thông tin nhận được của người dùng và cho phép vào hệ thống.

3. MÔ HÌNH HỆ THỐNG CSDL DÂN TỘC

Căn cứ từ bài toán trên, biểu đồ phân tích hệ thống như sau:

Người sử dụng A có khóa chung



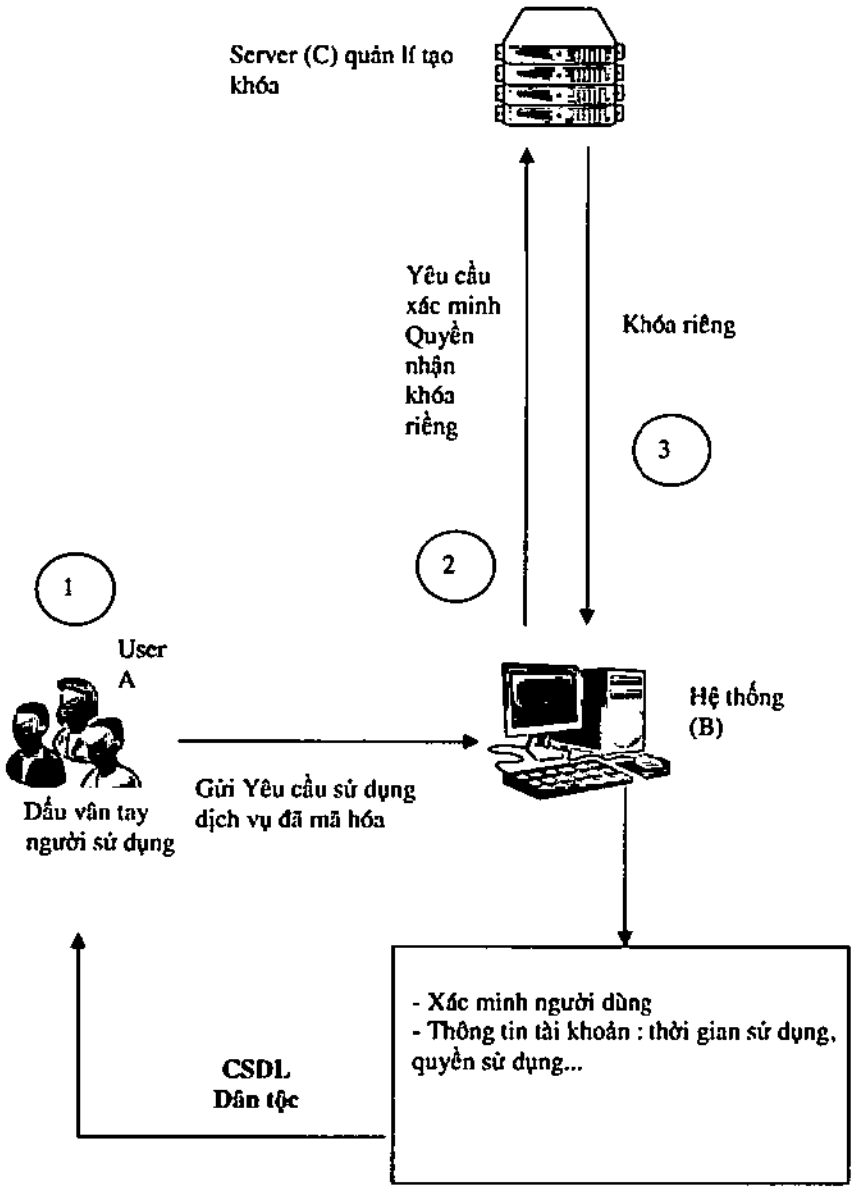
Hình 5. Sơ đồ hệ thống đảm bảo an toàn cơ sở dữ liệu tích hợp sinh trắc học

là "abcxyzz" (do được cấp) mã hóa dữ liệu (thông tin tài khoản và mật khẩu) gửi tới hệ thống kiểm soát quyền truy cập B.

Hệ thống B gửi tới server C xác nhận quyền nhận khóa bí mật MK. Server C xác nhận hệ thống B, cấp một lần duy nhất khóa riêng bí mật MK chỉ được sử dụng cho A. Hệ thống B lưu lại khóa riêng và giải mã dữ liệu mỗi khi nhận dữ liệu đã được mã hóa từ A.

Giải mã xong dữ liệu (thông tin tài khoản và mật khẩu), hệ thống B so sánh với dữ liệu đã được lưu trữ trước đó của A.

Nếu đúng cho phép sử dụng dịch vụ. Sai thì từ chối dịch vụ.



Hình 6. Sơ đồ phân tích hệ thống CSDL Dân tộc

KẾT LUẬN

Trong khuôn khổ các nghiên cứu của Đề tài "Nghiên cứu giải pháp tăng cường ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội và bảo đảm quốc phòng, an ninh vùng dân tộc thiểu số và miền núi", bài báo đề xuất phương pháp kết hợp nhận dạng vân tay và hệ mã RSA để đảm bảo an ninh cho Hệ thống cơ sở dữ liệu Dân tộc. Phương pháp này kết hợp được ưu điểm của dấu vân tay và RSA trong việc nhận thực người dùng, giúp Hệ thống cơ sở dữ liệu Dân tộc được xác thực an toàn hơn và bảo mật tốt hơn. Tuy nhiên, trong phương pháp của mình, nhóm tác giả có hạn chế trong cách xử lý dấu vân tay rõ nét, chính xác và cách kiểm tra chương trình dấu vân tay sau khi mã hóa. Trong tương lai, nhóm tác giả sẽ tiếp tục nghiên cứu cách kiểm tra, kiểm soát lại quá trình mã hóa kết hợp RSA và sinh trắc học bằng thuật toán tính toán nhiều bước; Giảm thiểu nhiễu do ảnh vân tay, chất lọc chính xác dấu vân tay. Đồng thời sẽ nghiên cứu sâu hơn để tích hợp các thiết bị PKI (Public Key Infrastructure) tạo thành hệ thống BioPKI hoàn chỉnh đảm bảo an toàn an ninh dữ liệu bằng sinh khóa, bảo mật khóa qua PKI.❖

Tài liệu tham khảo

[1] A. K. JAIN, A. ROSS, Introduction to Biometrics, In "Handbook of Biometrics", A. Jain et al. (Eds), Springer, 2008

[2] Y. C. FENG, P. C. YUEN, A. K. JAIN, A Hybrid Approach for Face Template Protection, In Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, pp. 325, 2008

[3] P. BALAKUMAR, R. VENKATESAN, A Survey on Biometrics-based Cryptographic Key Generation Schemes, International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80 - 85, 2012

[4] RSA Algorithm Based On Fingerprint Traits, 1Sona K.H. Computer science and Engineering, Vidya Academy of Science and Technology, Thrissur, India, February 2016 IJSDR | Volume 1, Issue 2

[5] Luận văn Thạc sĩ Nghiên cứu mã hóa dựa trên IBE và ứng dụng để quản lý đề thi của Trường Đại học Văn hóa Thể thao và Du lịch Thanh Hóa. ThS. Trịnh Văn Anh, Học viện Công nghệ Bưu chính Viễn thông Hà Nội

[6] Đồ án tốt nghiệp SVTH: Nhóm Cảm biến Nhận dạng vân tay Lớp ĐH Cơ điện tử - K2, ĐH Công nghiệp Hà Nội

[7] Giáo trình mạng máy tính, TS. Phạm Thế Quế, Học viện Công nghệ Bưu chính Viễn thông