Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ 25 (2009) 211-218

Ứng dụng thủy vân số và mã hoá dựa trên định danh trong việc chia sẻ dữ liệu ảnh y sinh học

Đặng Thu Hiền*, Trịnh Nhật Tiến, Trương Thị Thu Hiền

Khoa Công nghệ Thông tin, Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
144 Xuân Thủy, Hà Nội, Việt Nam

Nhận ngày 04 tháng 8 năm 2009

Tóm tắt. Thông tin y học trong các hệ thống E-health được gửi tới cho các bác sỹ chuẩn đoán, phòng thí nghiệm nghiên cứu hoặc trung tâm tư vấn sức khỏe. Việc sử dụng hệ thống chăm sóc y tế điện tử mang lại các lợi ích trong việc truy cập, kiểm soát và chia sẻ thông tin y tế của bệnh nhân, tuy nhiên lại gây ra các nguy cơ xâm phạm tính bí mật và riêng tư tới các thông tin sức khỏe nhạy cảm của người bệnh. Bài báo này tập trung vào ứng dụng của thủy vân số và mã hóa dựa trên định danh trong việc đảm bảo an toàn cho dữ liệu ảnh y sinh học. Các nghiên cứu liên quan về sử dụng thủy vân số ứng dụng trong y sinh học sẽ được trình bày, trên cơ sở đó, một mô hình đề xuất sử dụng thủy vân số kết hợp mã hóa truyền thông dựa trên định danh được trình bày. Phương pháp này giúp đảm bảo tính bí mật và riêng tư cho các thông tin dữ liệu y học.

Từ khoá: thủy vân số, mã hóa truyền thông dựa trên định danh, ảnh y sinh học.

1. Giới thiệu

Nhu cầu về bảo đảm an toàn thông tin trong lĩnh vực y sinh học ngày càng tăng, nhằm phục vụ công tác chăm sóc sức khỏe của cộng đồng và phục vụ các hoạt động nghiên cứu trong lĩnh vực này. Sự phát triển của dữ liệu đa phương tiện đã hỗ trợ tích cực các hoạt động y sinh học như chẩn đoán từ xa, chia sẻ thông tin y tế. Tuy nhiên, việc chia sẻ thông tin y sinh học của mỗi cá nhân (PHR – Patient Health Records) có thể xâm phạm tính riêng tư của người bệnh khi sử dụng các hệ thống E-Health. Do vậy vấn đề bảo đảm an toàn thông tin và chia sẻ thông tin trong hệ thống E-Health càng được đặt ra cấp thiết.

Dù là một trong các kỹ thuật cổ điển nhất để bảo vệ bản quyền tài liệu số hóa, thủy vân số vẫn có nhiều đặc tính phù hợp để bảo vệ dữ liệu E-Health. Nhúng thủy vân số về bản chất là việc chèn một thông điệp vào tài liệu số, thường ở dạng dữ liệu multimedia (ảnh, audio hoặc video). Một số yêu cầu trong kỹ thuật nhúng thủy vân bao gồm: (1) thông tin thủy vân được ẩn giấu với người dùng không có thẩm quyền (tương tự như mã hóa dữ liệu, khóa bí mật được dùng để đọc thông tin thủy vân); (2) bảo đảm tính toàn vẹn và xác thực các dữ liệu thủy vân. Thủy vân số được ứng dụng trong lĩnh vực y học với hai mục tiêu chính: (i) ẩn giấu thông tin trong các ảnh y sinh học nhằm tăng tính khả dụng; (ii) bảo vệ tính toàn vẹn và bí mật của các thông tin y sinh học của từng cá nhân.

* Tác giả liên hệ. ĐT.: 84-4-37547813.
E-mail: hienthudang@gmail.com

Mặc dù có nhiều ưu điểm, phương pháp thủy vân vào dữ liệu multimedia vẫn còn một số hạn chế khi áp dụng với ảnh y sinh học. Việc nhúng thủy vân vào ảnh y sinh học thường làm thay đổi ảnh gốc hoặc làm nhiễu một số thông tin quan trọng trong ảnh đó. Vì vậy hầu hết các phương pháp đã đề xuất đều nhằm đến việc duy trì chất lượng ảnh y sinh học sau khi nhúng thủy vân, để tránh mất mát các thông tin quan trọng đã thể hiện trong ảnh.

Một yêu cầu khác đối với hệ thống E-Health là vấn đề kiểm soát truy cập. Thông tin về tình trạng sức khoẻ hay thông tin riêng của bệnh nhân là những dữ liệu riêng tư, không nên tiết lộ công khai. Do đó cần có cơ chế kiểm soát chia sẻ đối với những thông tin này, sao cho chỉ những người dùng hợp lệ mới được phép truy nhập. Một trong các giải pháp thường được sử dụng để bảo đảm an toàn trong chia sẻ thông tin là các kỹ thuật mã hoá truyền thông [1].

Trong bài báo này, chúng tôi trình bày một số giải pháp thủy vân số ứng dụng trong E-Health, từ đó đề xuất một mô hình thủy vân số và mã hóa truyền thông, ứng dụng trong việc đảm bảo an toàn cho các dữ liệu ảnh y sinh học của một cá nhân cụ thể (PHR).

2. Các yêu cầu an toàn cho dữ liệu ảnh y sinh học

Thông tin y sinh học của một bệnh nhân (PHR) bao gồm một tập các thông tin chẩn đoán lâm sàng, kết quả xét nghiệm, các ảnh chụp chiếu, các thông tin khác. Ứng dụng thủy vân số để bảo đảm an toàn dữ liệu ảnh y sinh học, cần đáp ứng các yêu cầu sau:

- Tính bí mật: chỉ người dùng có thẩm quyền mới được phép truy cập thông tin.

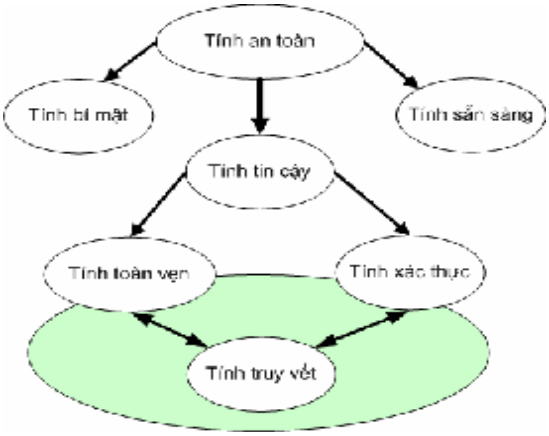
- Tính sẵn sàng: thông tin luôn sẵn sàng trong hệ thống để truy cập và xử lý theo lịch trình.

- Tính tin cậy: dựa trên các yêu cầu:

(i) Toàn vẹn: thông tin không thể bị sửa chữa bởi người dùng không có thẩm quyền;

(ii) Xác thực: có thể chứng minh được thông tin thuộc sở hữu của một người dùng xác định.

Trong các hệ thống thông tin y sinh học, các yêu cầu trên được duy trì bởi các dịch vụ bảo vệ thông tin: bảo mật, bảo toàn, xác thực, sẵn sàng, chống chối bỏ. Nếu các yêu cầu bảo mật, bảo toàn và sẵn sàng có liên quan khá chặt chẽ với nhau, thì yêu cầu về tính xác thực liên quan đến việc xác lập các đường truyền, các cơ chế truy cập để xác minh người dùng nào được phép truy cập thông tin gì. Ngoài ra tính tin cậy liên quan đến vấn đề truy vết thông tin trong quá trình chia sẻ và truyền gửi chúng.



Hình 1. Yêu cầu bảo vệ dữ liệu ảnh y sinh học.

Việc kiểm soát tính toàn vẹn dữ liệu ảnh y sinh học có thể được thực hiện nhờ chữ ký số hoặc mã xác thực thông điệp (Message Authentication Code - MAC), được tính dựa trên toàn bộ dữ liệu ảnh hoặc một vài dữ liệu đặc trưng của ảnh. Ký số được thực hiện trên từng bit của tài liệu cần ký, nên chỉ cần sửa chữa một bít của tài liệu gốc, thì chữ ký đã khác so với chữ ký ban đầu, nhờ đó dễ dàng kiểm soát được tính toàn vẹn của tài liệu gốc. Tình hình tương tự như với MAC.

Về việc phân phối và chia sẻ ảnh y sinh học PHR của các bệnh nhân, có một số giải pháp để xác thực nguồn gốc ảnh. Hầu hết các phương pháp này thao tác trên ảnh theo chuẩn DICOM (Digital Imaging and COmmunication in Medicine). Xác thực ảnh có thể thực hiện bằng việc nhúng thông tin UID (Unique ID) là một phần header của DICOM vào ảnh, nhờ thủy vân có thể xác định nội dung ảnh có bị thay đổi không, dù ảnh lưu trữ ở định dạng nén nào.

Cách hai, nhúng thủy vân là toàn bộ header của ảnh, nhưng do header có thể bị thay đổi liên tục trong khi truyền, nên để đảm bảo nhúng thủy vân, đòi hỏi cấu trúc header tương đối phức tạp.

Cách ba, nhúng chữ ký số trên header vào ảnh. Cách này có thể giúp thu gọn thông tin được nhúng, nhưng lại có hạn chế là header phải được đính kèm ảnh trong quá trình truyền gửi nhằm phục vụ việc kiểm tra tính chính xác của chữ ký, vì vậy khó thay đổi được định dạng của ảnh, làm hạn chế một ưu điểm của phương pháp thủy vân số.

Đã có một số nghiên cứu về tính truy vết cho các ảnh y sinh học trong môi trường làm việc cộng tác như một nhóm người dùng [2]. Người dùng với khóa tương ứng có thể gỡ bỏ một phần thủy vân được nhúng trong ảnh. Người cuối cùng trong chuỗi người dùng sẽ thu được ảnh không có thủy vân (ảnh gốc).

Việc bảo vệ nội dung của PHR cần xem xét tính xác thực liên kết giữa ảnh y sinh học và các nội dung kết quả y tế đi kèm của một bệnh nhân. Các báo cáo y sinh học có chứa kèm thông tin ảnh y sinh học được chụp chiếu, trong khi nội dung ảnh lại chứa các thông tin về báo cáo này nhúng trong đó.

Trong các ứng dụng E-Health, để đảm bảo tính bí mật, có thể chèn các thành phần thông tin PHR vào các ảnh y sinh học. Ưu điểm của thủy vân số là hỗ trợ nâng cao thêm tính bảo mật, mà mật mã đơn thuần không thể đáp ứng được trong việc bảo đảm an toàn dữ liệu ảnh y sinh học.

Ngoài vấn đề bảo vệ bản quyền ảnh y sinh học, có khả năng giấu được nhiều thông tin trong ảnh y sinh học. Tuy nhiên chưa có nhiều nghiên cứu theo hướng này. Một trong những khó khăn của ẩn giấu thông tin là kích thước của thông tin ẩn giấu, tính chất của ảnh, phương pháp giấu tin.

3. Các nghiên cứu liên quan

Hiện nay có 3 cách tiếp cận nhúng thủy vân số được áp dụng cho dữ liệu ảnh y sinh học.

Cách tiếp cận 1: Nhúng thủy vân vào các vùng ảnh ít quan trọng – RONI [3], để tránh làm ảnh hưởng chất lượng thông tin trong ảnh, thông thường là các vùng nền màu đen, đôi khi cũng có thể là các điểm màu xám. Mặc dù không làm ảnh hưởng đến nội dung quan trọng trong ảnh phục vụ cho mục đích chuẩn đoán, những vùng được nhúng thủy vân có thể làm thay đổi các vùng nền màu đen trên ảnh, do đó gây nhiễu cho các chuyên gia chuẩn đoán dựa trên nội dung ảnh đã nhúng thông tin thủy vân.

Cách tiếp cận 2: Thủy vân số có thể được gỡ bỏ, theo nghĩa là khi thông tin nhúng được đọc, nó được gỡ bỏ khỏi ảnh, cho phép thu được ảnh gốc (trước khi nhúng thủy vân) [4]. Có một số nghiên cứu theo cách tiếp cận này, nhưng vẫn còn hạn chế về dung lượng thông tin được nhúng. Cách tiếp cận này thường ứng dụng trong ẩn giấu thông tin.

Cách tiếp cận 3: Sử dụng kỹ thuật thủy vân số truyền thống sao cho việc nhúng thủy vân không làm bóp méo hay thay đổi nội dung của ảnh. Kỹ thuật truyền thống phổ biến là thủy vân được thay thế vào các bít ít quan trọng của ảnh [5], hoặc các thông tin có thể bị mất trong trường hợp nén ảnh có mất mát [6, 7].

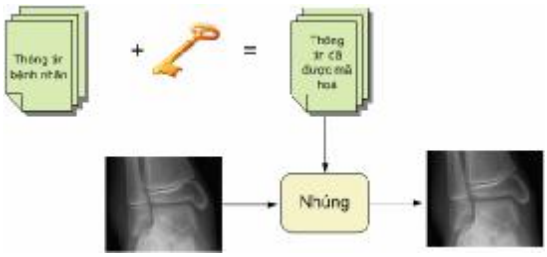
Tùy thuộc vào các miền ứng dụng khác nhau, ví dụ dữ liệu ảnh y sinh học được dùng phục vụ việc chuẩn đoán của chuyên gia, hoặc dữ liệu ảnh y sinh học được dùng cho mục đích giảng dạy, nghiên cứu, mà cân bằng giữa các đặc trưng về tính mạnh, tính ẩn giấu, dung lượng thông tin được nhúng.

Các ứng dụng liên quan trực tiếp đến việc chăm sóc sức khỏe cho bệnh nhân thì có yêu cầu khắt khe hơn trong việc thay đổi dữ liệu ảnh gốc, trong khi các ứng dụng nghiên cứu giảng dạy liên quan đến dữ liệu y sinh học thì có thể cho phép thay đổi nội dung dễ dàng hơn. Vì đặc điểm này mà khi thiết kế cần lựa chọn các kỹ thuật thủy vân số thích hợp. Phương pháp RONI hoàn toàn không làm ảnh hưởng đến dữ liệu ảnh được dùng để chẩn đoán, tuy nhiên ta cũng chỉ áp dụng được phương pháp này với những bức ảnh có RONI, đồng thời dung lượng thông tin giấu cũng phụ thuộc vào kích thước vùng RONI.

Với cách tiếp cận 2, ảnh gốc vẫn không được bảo vệ khi thủy vân đã gỡ bỏ. Với phương pháp này, dung lượng thủy vân có thể rất lớn, do đó trước khi sử dụng ảnh gốc cần gỡ bỏ thủy vân. Việc này tương tự như việc giải mã thông điệp, khi muốn lấy thông điệp gốc. Tuy nhiên, phương pháp này có ưu điểm hơn phương pháp mã hóa ở chỗ hỗ trợ tính xác thực cho ảnh. Hơn nữa, dù phương pháp nào được áp dụng, vấn đề thời gian xử lý tránh ảnh hưởng đến việc chuẩn đoán của các chuyên gia, đặc biệt với các ảnh y sinh học có dung lượng lớn.

4. Mô hình đề xuất cho PHR

Đối với ảnh y sinh học, các thông tin của mỗi bệnh nhân thường được gắn với từng bức ảnh để việc lưu trữ, quản lý và xử lý được thuận tiện. Hiện nay thông tin về bệnh nhân thường được in tại góc của ảnh, nên ai cũng có thể đọc được thông tin này khi xem ảnh. Trong một số trường hợp, thông tin về tình trạng sức khoẻ của bệnh nhân được coi là thông tin nhạy cảm. Nếu những thông tin này bị tiết lộ có thể gây ảnh hưởng trong đời sống xã hội và tình trạng sức khoẻ của những người liên quan. Do vậy, để đảm bảo tính an toàn và bí mật, những thông tin này cần được mã hoá và nhúng vào ảnh. Sơ đồ chung của quá trình này được biểu diễn như hình 2.



Hình 2. Sơ đồ mã hóa và nhúng thông tin.

Bác sỹ cũng như bệnh nhân và người nhà của họ cần biết được thông tin về bệnh nhân khi chẩn đoán, điều trị và chăm sóc sức khoẻ cho bệnh nhân đó. Như vậy những người dùng hợp lệ trên có quyền truy cập các thông tin này. Việc sử dụng các hệ mã hoá khoá công khai thông thường cũng đảm bảo được yêu cầu trên, nhưng gặp phải một số hạn chế như: phải lưu trữ nhiều cặp khoá của từng người dùng tham gia vào hệ thống, phải tạo ra số bản mã tương ứng với số lượng người dùng hợp lệ, dẫn đến tốn thời gian và không gian lưu trữ.

Để khắc phục vấn đề trên, trong bài báo này chúng tôi sử dụng kỹ thuật mã hoá truyền thông dựa trên định danh (Identity-Based Broadcast Encryption – IBBE) [8-10] cho quá trình mã hoá thông tin của bệnh nhân, sau đó nhúng bản mã thu được vào ảnh y sinh học sử dụng kỹ thuật thuỷ vân số. Những ưu điểm của cách kết hợp này sẽ được phân tích kỹ hơn ở phần tiếp theo.

4.1. Các trường thông tin trong PHR

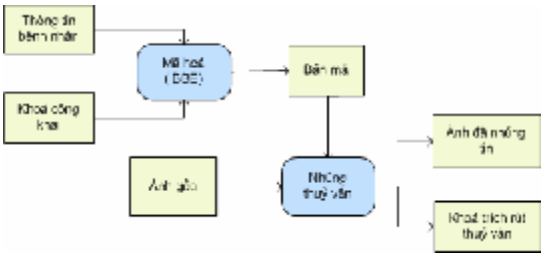
Dữ liệu y tế của mỗi bệnh nhân cần được thu thập và lưu trữ qua nhiều năm, tập hợp thành hồ sơ sức khoẻ của bệnh nhân. Việc lưu trữ dữ liệu y tế của mỗi người không chỉ phục vụ cho mục đích chăm sóc và chữa trị cho bệnh nhân khi cần thiết, mà về lâu dài, còn rất quan trọng trong các nghiên cứu dịch tễ học, lập phác đồ điều trị hay kinh doanh bảo hiểm y tế. Trong báo cáo này, chúng tôi giới thiệu một số trường thông tin thường dùng khi nhúng vào ảnh y tế.

Thông tin về bệnh nhân
Mã số bệnh nhân, Họ tên, Ngày sinh, Giới tính, Địa chỉ, Ngày chụp ảnh
Thông tin về tình trạng sức khoẻ
Biểu hiện, Kết quả xét nghiệm, Chẩn đoán, Phương pháp điều trị, Tiền sử bệnh tật
Thông tin về bác sĩ điều trị
ID và họ tên của bác sĩ điều trị chính, ID và họ tên của các bác sĩ, chuyên gia cộng tác

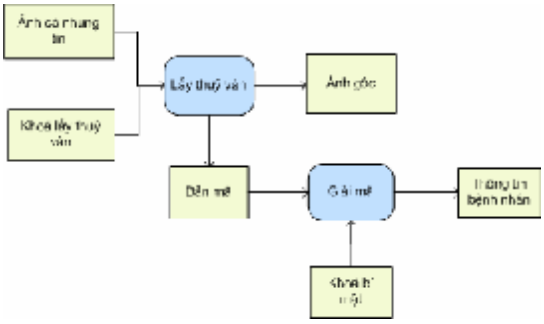
Ngoài ra, trong một số trường hợp cần thiết, có thể thêm các thông tin về bố mẹ, con cái hoặc anh chị em của bệnh nhân để phục vụ cho một số mục đích như nghiên cứu, chữa trị các chứng bệnh liên quan đến di truyền.

4.2. Sơ đồ mã hóa và thủy vân số

Bài báo này sử dụng sơ đồ mã hoá truyền thông dựa trên định danh để mã hoá các thông tin về bệnh nhân, sau đó nhúng thông tin này vào ảnh y tế sử dụng kỹ thuật thuỷ vân số. Mã hoá dựa trên định danh là hệ mã hoá sử dụng các thông tin đơn nhất và không thể chối cãi của mỗi người dùng (chẳng hạn như tên, địa chỉ email) để xây dựng khóa công khai cho họ [11]. Việc mã hoá các thông tin sử dụng định danh không chỉ đảm bảo tính an toàn mà còn giảm bớt được độ phức tạp cũng như chi phí thiết lập, bảo trì do không cần có hạ tầng cơ sở khoá công khai để phân phối và quản lý khoá. Chính vì vậy, áp dụng mã hoá truyền thông dựa trên định danh trong đảm bảo an toàn dữ liệu y sinh học giúp cho việc chia sẻ thông tin giữa bệnh nhân và hội đồng bác sĩ, các chuyên gia sức khoẻ được thuận tiện và dễ dàng hơn.



Hình 3. Sơ đồ mã hóa và nhúng thủy vân.



Hình 4. Sơ đồ lấy thủy vân và giải mã.

Cặp khoá công khai/bí mật dùng trong bước mã hoá và giải mã của sơ đồ được xây dựng theo đề xuất của C. Delerablee [10], sử dụng định danh của đối tượng. Các tham số của hệ thống được lựa chọn như sau:

+ Chọn một tham số bảo mật m và một số nguyên n.

+ Sinh một số nguyên tố q, hai nhóm $(G_1, +)$, $(G_2, *)$ bậc q và một ánh xạ song tuyến tính $e: G_1 x G_2 \rightarrow G_2$

+ g và h là hai phần tử sinh của G_1 và G_2.

+ Chọn ngẫu nhiên $s \hat{I} Z_q^*$

+ Chọn hàm băm $H: (0, 1)^* \to Z_q^*$

Khoá công khai là $P_{pub} = (w, v, h, h^s, \ldots, h^{sn})$ với $w = g^s$, $v = e(g, h)$.

Các tham số hệ thống là: $Params = (g, G_1, G_2, e, n, P_{pub}, H)$. Khoá chủ là s.

Với khoá chủ s và một định danh $ID \hat{I} \{0, 1\}^*$, khoá bí mật là: $s_{ID} = g^{\frac{1}{s+H(ID)}}$

Các bước của quá trình mã hoá và nhúng thuỷ vân:

- Mã hoá: Một người dùng thuộc nhóm chia sẻ thông tin chọn ngẫu nhiên $r \hat{I} Z_q^*$ và tính:

$$C_1 = w^{-r}, C_2 = h^{r \cdot \prod_{i=1}^{n} s+H(ID_i)}, k_{IBE} = v^{-r}$$

Sau đó, sử dụng k_{IBE} làm khoá bí mật để mã hoá thông tin bệnh nhân P bằng một trong các hệ mã đối xứng như DES3, AES,… ta thu được $C_3 = enc_{DES3, k_{IBE}}(P)$.

Như vậy, bản mã C thu được gồm 3 thành phần $C = <C_1, C_2, C_3>$.

- Nhúng thuỷ vân: Thông tin thuỷ vân C được nhúng vào ảnh y sinh học I bằng một trong số các phương pháp nhúng thuỷ vân sử dụng các kỹ thuật LSB, DCT. Bước này sẽ cho kết quả là một ảnh đã được nhúng thuỷ vân I' và một khoá trích rút thuỷ vân k_w.

$$(I', k_w) = W(I, C)$$

Các bước của quá trình trích rút thuỷ vân và giải mã:

- Trích rút thuỷ vân: Với ảnh đã nhúng thuỷ vân I' và khoá trích rút thuỷ vân k_w thu được, sử dụng phương pháp trích rút thuỷ vân (LSB, DCT,…) ta thu được ảnh I và thông tin thuỷ vân C. Đây chính là thông tin về bệnh nhân đã được mã hoá.

- Giải mã: Một người dùng có định danh ID_i muốn đọc được nội dung thông tin về bệnh nhân P cần tính được khoá K_{IBE} để giải mã được thông tin đã bị mã hoá. Khoá K_{IBE} được tính theo công thức:

$$k_{IBE} = (e(C_1, h^{p_{i,S(s)}}).e(s_{ID_i}, C_2))^{\frac{1}{\prod_{j=1, j\neq i}^{n} H(ID_j)}}$$

Với:

$$p_{i,S(s)} = \frac{1}{s}\left(\prod_{j=1, j\neq i}^{n}(s+H(ID_j)) - \prod_{j=1, j\neq i}^{n} H(ID_j)\right) \quad \backslash\backslash$$

Với khoá k_{IBE} thu được, sử dụng hệ DES3 để giải mã C_3 ta thu được bản rõ về thông tin bệnh nhân $P = dec(C_3, k_{IBE})$.

Theo sơ đồ này, khoá công khai được dùng chung cho mọi người thuộc nhóm chia sẻ thông tin, khoá bí mật là của riêng từng người. Việc mã hoá chỉ cần thực hiện một lần sử dụng khoá công khai, và chỉ có một bản mã duy nhất, nhưng tất cả những người dùng có định danh hợp lệ đều có thể dùng khoá bí mật của riêng mình để giải mã và đọc được thông tin. Việc này tiết kiệm được rất nhiều thời gian cũng như không gian lưu trữ khóa, không cần có hệ thống chia sẻ và quản lý khoá, thuận tiện trong việc trao đổi các tài liệu về y tế trên mạng mà vẫn đảm bảo được tính an toàn, bí mật cho các thông tin cần thiết.

Sơ đồ đề xuất trong bài báo này đáp ứng được các yêu cầu về bảo đảm an toàn cho dữ liệu ảnh y sinh học như đã nêu trong mục 2. Nhờ việc sử dụng mã hóa truyền thông nên các thông tin PHR được đảm bảo bí mật hoàn toàn, chỉ những người dùng có thẩm quyền mới có thể truy cập. Bằng cách sử dụng kỹ thuật thủy vân số, tính toàn vẹn cũng được đáp ứng, khi thông tin về bệnh nhân cùng bức ảnh y sinh học của họ được lưu trữ trong một đối tượng thống nhất.

5. Kết luận

Sự kết hợp của thủy vân số và mật mã học là một hướng nghiên cứu hứa hẹn xây dựng các

dịch vụ bảo mật thông tin trong lĩnh vực y sinh học (E-Health) cho đến khi tìm được một kỹ thuật thủy vân số đơn thuần mà vẫn đảm bảo được các yêu cầu về bảo mật. Trong bài báo này chúng tôi đã trình bày các yêu cầu bảo mật và kỹ thuật thủy vân số, mã hóa thông tin đính kèm dữ liệu ảnh y sinh học, qua đó đề xuất mô hình kết hợp giữa mật mã học và thủy vân số với các trường thông tin nhúng. Việc kết hợp giữa mã hoá truyền thông và thuỷ vân số đem lại nhiều lợi ích trong việc đảm bảo tính an toàn và tính riêng tư cho các thông tin cần được chia sẻ. Hướng nghiên cứu tiếp theo là tiến hành các thực nghiệm đánh giá mô hình đề xuất, từ kết quả đánh giá phát triển các dịch vụ y sinh học cho hệ thống E-Health dựa trên mô hình này.

Lời cảm ơn

Công trình này được tài trợ một phần từ đề tài mang mã số QC.07.11 Đại học Quốc Gia Hà Nội.

Tài liệu tham khảo

[1] Amos Fiat and Moni Naor. Broadcast encryption. In Douglas R. Stinson, editor, CRYPTO'93, volume 773 of LNCS, pages 480–491, Santa Barbara, CA, USA, August 22–26, 1994. Springer-Verlag, Berlin, Germany

[2] M. Li, R. Poovendran, S. Narayanan, Protecting patient privacy against unauthorized release of medical images in a group communication environment, Computerized Medical Imaging and Graphics, vol. 29, no.5, pp. 367-383, 2005.

[3] G. Coatrieux, B. Sankur, H. Maître, Strict Integrity Control of Biomedical Images, in Proc. Electronic Imaging, Security and Watermarking of Multimedia Contents, SPIE, USA, 2001, pp.229- 240.

[4] B. Macq, F. Dewey, Trusted Headers for Medical Images, in DFG VIII-DII Watermarking Workshop, Erlangen, Germany, 1999.

[5] D. Anand, U.C. Niranjan, Watermarking Medical Images with Patient Information, in Proc. Int. Conf. IEEE-EMBS, 1998, pp. 703–706.

[6] A. Piva, M. Barni, F. Bartolini, A. De Rosa, Data hiding technologies for digital radiography, in IEE Proc. Vision, Image and Signal Processing, vol. 152, n°5, pp.604-610, 2005.

[7] Deepthi Anand, U.C. Niranjan, Watermarking medical images with patient information, Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 20, No 2, 1998.

[8] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, CRYPTO 2001, volume 2139 of LNCS, pages 213– 229, Santa Barbara, CA, USA, August 19–23, 2001. Springer-Verlag, Berlin, Germany.

[9] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, CRYPTO 2005, volume 3621 of LNCS, pages 258–275, Santa Barbara, CA, USA, August 14–18, 2005. Springer-Verlag, Berlin, Germany

[10] Cecile Delerablee, Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys, Proceedings of Asia Crypt 2007.

[11] A.Shamir, "Identity-based cryptosystems and signature schemes", in Advances in Cryptology – Crypto '84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag,pp.47–53,1984

An application of watermarking and identity-based encryption for sharing medical image

Dang Thu Hien, Trinh Nhat Tien, Truong Thi Thu Hien

Faculty of Information Technology, College of Technology, VNU, 144 Xuan Thuy, Hanoi, Vietnam

Medical information in e-health system is sent to a laboratory or consulting physician. Relevant information may be transmitted to your health insurer or pharmacy. By making information more readily available to those who need it, greater use of computerized health information can help improve the quality of health care and reduce its costs. While the recent advances in information and communication technologies provide new means to access, handle and share medical information, they also compromise their security due to their ease of manipulation and replication. In this paper, we focus on the complementary role of watermarking with respect to medical information security. The main objectives for medical image watermarking are that the watermarks are imperceptible and act as a mean of authentication and integrity control. We review existing approaches of watermarking for protection of medical images, for secure sharing and handling of medical images. We then propose a model that combines the watermarking with encryption technique to address the issue of security and privacy for personal healthcare record.