Tạp chí Tin học và Điều khiển học, T.27, S.2 (2011), 154–165

MÔ HÌNH CHỨNG THỰC DỰA TRÊN ẢNH VÂN TAY

LÊ HOÀI BẮC, NGUYỄN KIM HƯNG, LÊ THỊ HOÀNG NGÂN

Khoa Công Nghệ Thông Tin, Đại Học Khoa Học Tự Nhiên Tp. Hồ Chí Minh

Tóm tắt. Thủy vân số là một trong những phương pháp hữu hiệu trong việc chống xâm phạm bản quyền, bảo vệ, và chứng thực quyền sở hữu trí tuệ sản phẩm. Dữ liệu vân dùng để chứng thực quyền sở hữu hợp pháp thường là những thông tin sở hữu như thông tin tác giả, logo công ty, banner, ... Với một hướng tiếp cận mới, bài báo này đề cập đến một loại tín hiệu vân trắc sinh học - vân tay. Vì những đặc trưng riêng của tín hiệu vân tay nên bài báo áp dụng một số kỹ thuật: thuật toán Gabor, nhị phân mô phỏng cục bộ, kỹ thuật Hilditch, luật heuristic, và độ đo Hamming. Hơn nữa, để nâng cao tính bền vững của mô hình, những hệ số DCT thấp nhất trong mỗi khối sẽ được chọn và nhúng thông tin. Với phương pháp đề xuất, mô hình chứng thực đạt được khả năng chứa cao và chất lượng ảnh tốt. Kết quả thực nghiệm chỉ ra rằng phương pháp đề xuất chống lại các tấn công như nén JPEG, thay đổi độ tương phản, nhiễu Gaussian, làm mờ ảnh, cắt ảnh, quay, tỉ lệ, tịnh tiến ảnh, ảnh cạnh, ảnh nổi, ảnh phình.

Abstract. Digital Watermarking is the art of hiding copyright information to protect host signal from illegal activities. The embedded data can be author identification, company logo and authentication information. In this paper, we proposed a novel scheme in which biometrics watermark, namely fingerprint is used. Because of specific features of fingerprint, to achieve perfect authentication scheme which meets three criteria of watermarking problem, we utilize some techniques like Gabor algorithm, locally adaptive thresholding, Hilditch's thinning method together with heuristic rules, and Hamming measurement. Furthermore, to improve robustness of the scheme, the lowest frequency of DCT blocks is chosen and embedded information. Based on the proposed scheme, the authentication scheme can achieve high capacity and good quatily. The experimental results will show that our algorithm can be robustness against to JPEG compression, brightness and contract modification, Gaussian noise, adding blur, cropping, rotation, scale, translation, edge detection, emboss, bulge image.

1. GIỚI THIỆU

Cùng với sự phát triển mạnh mẽ của Internet và cuộc cách mạng thông tin số thì sự xâm phạm đến quyền sở hữu trí tuệ ngày càng nhiều dưới nhiều hình thức phong phú, đa dạng và tinh vi như: giả mạo, sao chép, mô phỏng, ăn cắp tác phẩm, ... Một trong những bài toán quan trọng đặt ra trong bối cảnh này là làm thế nào để có thể chứng thực quyền sở hữu hợp pháp của một dữ liệu khi có tranh chấp xảy ra. Và thủy vân số (Watermarking) được xem là một trong những giải pháp tốt, có tiềm năng và không ngừng phát triển. Với hướng tiếp cận này, đối tượng cần bảo vệ được gọi là đối tượng chủ. Thông tin được nhúng vào đối tượng chứa, gọi là vân, thường là thông tin về tác giả, tác phẩm, chủ sở hữu hợp

pháp dùng để chứng thực. Ba yêu cầu tiên quyết đặt ra cho bài toán ẩn dữ liệu nói chung và Watermarking nói riêng là: khả năng chứa, độ bền vững và tính vô hình. Mức độ hiệu quả của một giải pháp phụ thuộc vào cả hai yêu tố: đặc điểm của thông tin nhúng và phương pháp ẩn dữ liệu. Có nhiều loại thông tin vân được sử dụng như: thông tin của chính tác giả (chuỗi nhị phân, văn bản), thông tin của chính đối tượng chứa (ảnh nhị phân, ảnh xám) [4], chữ ký của chủ sử hữu (chuỗi nhị phân) [9], thông tin trắc sinh học (mống mắt, vân tay) [1], ... Tuy nhiên, một câu hỏi đặt ra là trong các loại thông tin vân trên thì thông tin nào là tốt nhất giúp người sử dụng chứng thực nếu họ không hiểu rõ về nguồn gốc tác phẩm, đối tượng nào cho độ tin cậy cao nhất, đối tượng nào có tính pháp lý cao nhất cũng như đối tượng nào giúp đáp ứng tốt nhất ba yêu cầu của bài toán Watermarking.

Trong tất cả các thông tin cá nhân, dữ liệu sinh trắc học được đặc biệt quan tâm trong những năm gần đây. Hơn nữa, dữ liệu sinh trắc học của một người là duy nhất, bất biến với thời gian và không thể thay đổi ngay cả khi bị đánh cắp. Những kĩ thuật định danh người dựa trên các đặc trưng sinh trắc học như: vân tay, khuôn mặt, võng mạc, tròng mắt,... ngày càng phổ biến. Bài báo này sử dụng thông tin sinh trắc học - vân tay cho bài toán Watermarking, đặc biệt tập trung vào ứng dụng chứng thực. Đã có một vài công trình nghiên cứu công bố về hướng này nhưng phần lớn tập trung vào việc nghiên cứu đối tượng chứa là ảnh sinh trắc học và dữ liệu ẩn là bất kỳ, còn hướng nghiên cứu ẩn dữ liệu đặc trưng sinh trắc học vào đối tượng chứa bất kỳ là rất ít. Chẳng hạn như hai phương pháp ẩn dữ liệu trên miền không gian đối với ảnh vân được đề xuất bởi Gunsel [3]. Đối với phương pháp thứ nhất, những vùng vân tay quan trọng được đánh dấu thông qua việc phân tích ảnh hướng và dữ liệu ẩn không được nhúng vào những vùng quan trọng đó. Để tránh ảnh hưởng đến giai đoạn phân loại ảnh vân tay, phương pháp thứ hai của Gunsel dùng những đặc trưng vân tay thay vì vùng quan trọng trong vân tay. Một lược đồ ẩn dữ liệu khác được áp dụng trong quá trình nén ảnh vân tay được đề xuất bởi Rath [8]. Quá trình nhúng được thi hành trên chuỗi nén phát sinh bởi Wavelet Scalar Quantizer (WSQ). Những hệ số WSQ được chọn để thay đổi sao cho vẫn đảm bảo chất lượng ảnh. Ghouti [6] đề xuất một phương pháp nhúng dữ liệu vững mạnh vào ảnh vân tay trên miền wavelet bằng cách dựa vào những đặc trưng của vân tay. Jain [2] đề xuất hai ứng dụng dựa trên các phương pháp để thực thi quá trình ẩn dữ liệu sinh trắc học của con người vào các loại đối tượng chứa khác nhau.

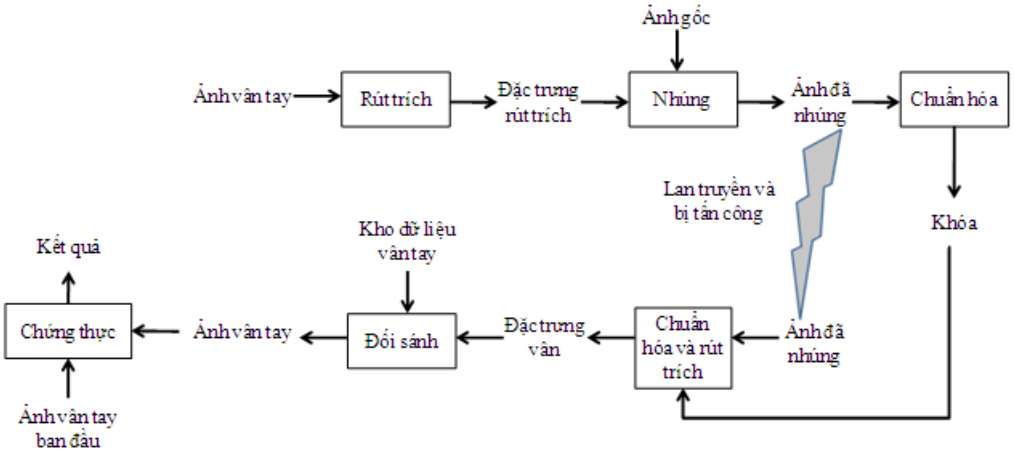
Những phương pháp được đề cập ở trên chỉ vững mạnh trước các tấn công cắt ảnh và nén JPEG, còn tấn công khác thì không được đề cập đến. Hơn nữa, họ vẫn chưa chỉ rõ các ưu điểm khi sử dụng dữ liệu là đặc trưng ảnh vân. Ở đây, ta sẽ dựa vào một đặc điểm quan trọng của vân tay người là mỗi vân tay chỉ có khoảng từ 30 đến 100 đặc trưng [5] để đưa bài toán ẩn ảnh vân tay về bài toán nhúng vector đặc trưng. Hướng tiếp cận này đã không những giải quyết tốt bài toán chọn đối tượng nhúng phù hợp mà vẫn đáp ứng tốt ba yêu cầu của bài toán Watermarking, cụ thể như sau:

(*i*) Dung lượng chứa: Nhờ vào các thao tác tiền xử lý, bài toán nhúng ảnh vân vào ảnh chứa trở thành bài toán nhúng các vector đặc trưng vân vào ảnh chứa. Với phương pháp rút trích đặc trưng hợp lý được chọn, một ảnh vân tay có kích thước vài trăm KB được đại diện bởi các vector đặc trưng có tổng chiều dài vài trăm bit. Điều này có thể cho thấy dung lượng chứa của giải pháp đưa ra là rất cao.

(*ii*) Tính vô hình: Vì vector đặc trưng được nhúng vào ảnh chứa có kích thước khá nhỏ nên độ nhiễu của ảnh trước và sau khi nhúng là không đáng kể.

(*iii*) Khả năng bền vững: Căn cứ trên ưu điểm về kích thước rất nhỏ của vector đặc trưng, giải pháp được chọn trong bài báo này là nhúng vector này vào những vùng quan trọng và bền vững của tín hiệu chứa.

Bố cục bài báo gồm: Mục 1, giới thiệu bài toán Watermarking và động cơ lựa chọn hướng tiếp cận chứng thực ảnh dựa trên sinh trắc học vân tay. Các kỹ thuật liên quan như: tiền xử lý ảnh vân, kỹ thuật rút trích đặc trưng, kỹ thuật đối sánh mẫu được giới thiệu trong Mục 2. Mục 3 trình bày về phương pháp đề xuất với ba giai đoạn: giai đọan nhúng, giai đoạn rút trích và giai đoạn chứng thực. Các kết quả thực nghiệm được trình bày trong Mục 4. Và cuối cùng là đưa ra các kết luận và đánh giá. Phương pháp chứng thực được đề xuất trong bài báo này có thể được mô tả tổng quát qua hình vẽ sau.

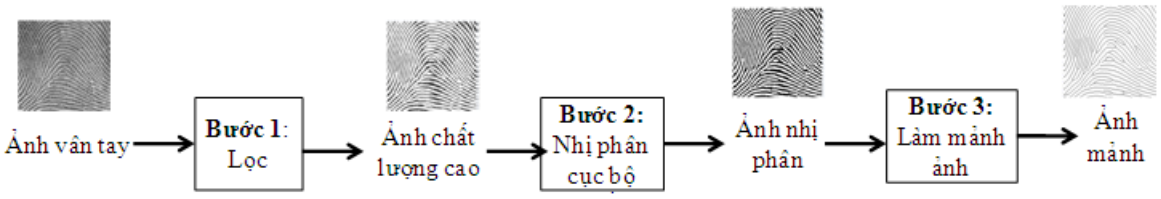


Hình 1.1. Mô hình chứng thực ảnh bằng ảnh vân tay

2. CÁC KỸ THUẬT LIÊN QUAN

2.1. Tiền xử lý ảnh vân

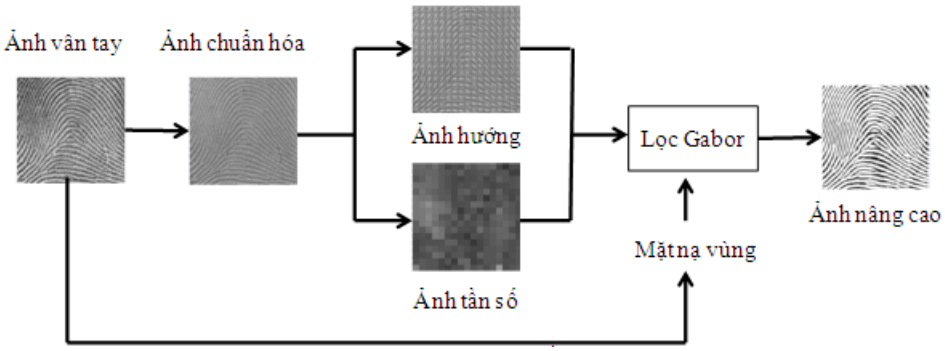
Đầu vào là ảnh vân tay (có thể là ảnh xám hoặc ảnh nhị phân) và kết quả của quá trình này là ảnh nhị phân mảnh chất lượng cao. Quá trình này được tiến hành như sau.



Hình 2.2. Quá trình tiền xử lý ảnh vân

Có thể nói phương pháp tiếp cận trong Hình 2.2 là phương pháp tiếp cận truyền thống đơn giản và hiệu quả nhất đối với quá trình tiền xử lý vân tay như trong [7,10] có đề cập.

Bước 1. (Lọc) Quá trình lọc nhằm giúp nâng cao chất lượng ảnh vân tay, nghĩa là giúp ảnh rõ hơn, nâng cao độ tương phản giữa lằn và lõm, nối những điểm gãy trên cùng một lằn với nhau. Có nhiều phương pháp nâng cao chất lượng ảnh từ đơn giản đến phức tạp, từ miền không gian đến miền tần số. Nhưng phần lớn các kĩ thuật hiện nay đều dựa trên bộ lọc ngữ cảnh mà những tham số của nó phụ thuộc vào tần số lằn và hướng cục bộ. Có bốn bộ lọc phổ biến hiện nay: Gabor, Anisotropic, Watson, và STFT tương ứng với các thao tác lọc trên miền không gian và miền Fourier. Dựa trên kết quả thực nghiệm với ảnh vân tay [7,10], bộ lọc Gabor được chọn trong bài báo này. Quá trình tìm ảnh nâng cao thông qua bộ lọc Gabor được mô tả như sau:



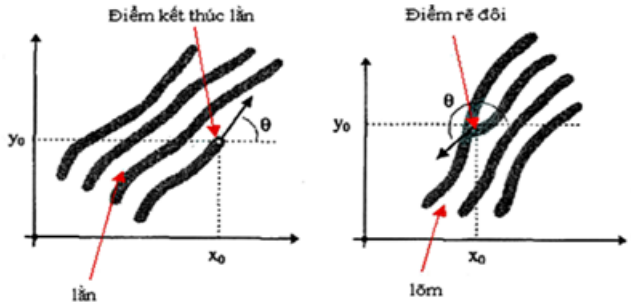
Hình 2.3. Tìm ảnh nâng cao bằng bộ lọc Gabor

Bước 2. (Nhị phân cục bộ) Quá trình này giúp tạo ảnh nhị phần từ một ảnh bất kỳ (xám hay nhị phân). Hướng tiếp cận trực tiếp và đơn giản nhất để có được ảnh nhị phân đó là dựa vào ngưỡng toàn cục T: $I(x,y) = \begin{cases} 1 & I(i,j) > T \\ 0 & I(i,j) \leq T \end{cases}$, trong đó, I là ảnh gốc và I' là ảnh nhị phân. Tuy nhiên, hướng tiếp cận này không tối ưu. Để cải tiến hướng tiếp cận này, thay vì áp dụng ngưỡng toàn cục T trên toàn ảnh thì dùng ngưỡng cục bộ là giá trị mật độ trung bình trên một khối $w \times w$. Nếu giá trị pixel lớn hơn giá trị trung bình của khối hiện tại thì nhận giá trị 1, ngược lại giá trị 0.

Bước 3. (Làm mảnh ảnh) Quá trình này giúp làm mảnh các đường lằn, loại bỏ những pixel thừa của đường lằn cho đến khi bề rộng của nó chỉ còn một pixel mà vẫn giữ được cấu trúc hình học của ảnh. Có nhiều thuật toán làm mảnh như Stentiford, Zhang-Suen, Holt,... Tuy nhiên kết quả thực nghiệm cho thấy với ảnh vân tay, thuật toán Hilditch đơn giản và cho kết quả tốt. Với thuật toán này, tại mỗi điểm P1 nằm trên lằn, xem xét lân cận 8 của pixel P1. Sau đó tính A(P1) và B(P1), với A(P1) là số lượng cặp pixel (0, 1) trong chuỗi P2, P3, P4, P5, P6, P7, P8, P9, P2 và B(P1) là số lượng pixel P1 lân cận khác 0. Pixel tại P1 sẽ chuyển từ 1 (black) sang 0 (white) nếu thỏa mãn 4 điều kiện: (1) $2 \leq$ B(P1) ≤ 6; (2) A(P1) $= 1$; (3) P2.P4.P8 $= 0$ hoặc A(P2) != 1; (4) P2.P4.P6 $= 0$ hoặc A(P4) != 1.

2.2. Rút trích đặc trưng vân

Đầu vào là ảnh nhị phân mảnh chất lượng cao và kết quả của quá trình này là vector đặc trưng vân. Có hai đặc trưng được rút trích trong quá trình này là: điểm kết thúc lằn và điểm rẽ đôi nhánh. Hai điểm này có thể được minh họa thông qua hình vẽ sau:



Hình 2.4. Điểm kết thúc lằn và điểm rẽ đô

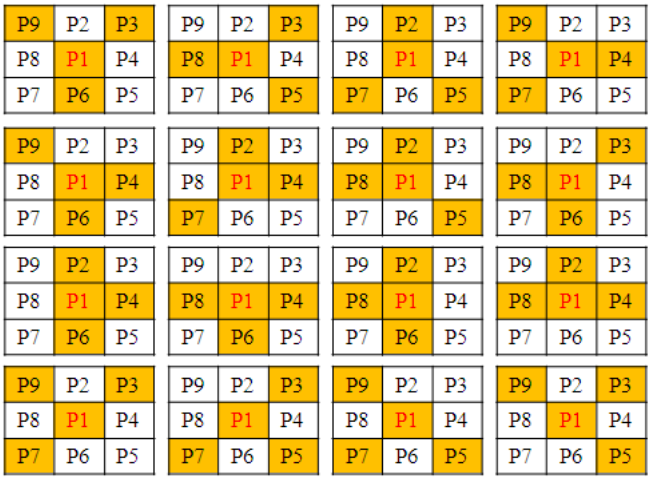
Bằng cách chia ảnh nhị phân mảnh thành các khối ảnh xếp chồng nhau, kích thước 3×3, điểm P1 nằm trung tâm khối được xác định là điểm kết thúc lằn nếu các lân cận P1 thoải một trong các trường hợp sau:

Hình 2.5. Trường hợp P1 là điểm kết thúc lằn

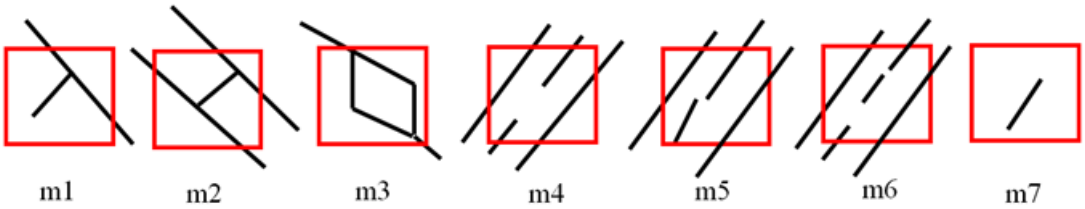
Dựa trên định nghĩa, điểm P1 được xác định là điểm rẽ đôi nếu các lân cận P1 thuộc các trường hợp sau:

Tuy nhiên, một số lằn gãy sai vì không đủ mực hay lằn cắt nhau vì mực loang sẽ tạo ra các đặc trưng sai trong quá trình rút trích đặc trưng vân tay như các trường hợp sau:

Tương ứng với các trường hợp trên: (m1): lằn đi ngang qua lõm, (m2): một lằn sai kết nối hai lằn, (m3): hai rẽ đôi gần nhau trong cùng một lằn, (m4): hai điểm gãy trong lằn có hướng giống nhau và gần nhau, (m5) giống (m4) ngoại trừ một phần lằn gãy quá ngắn đến nỗi một rẽ đôi có thể phát sinh, (m6) mở rộng (m4) với lằn thứ ba được tìm thấy ở giữa của



Hình 2.6. Trường hợp P1 là điểm rẽ đôi



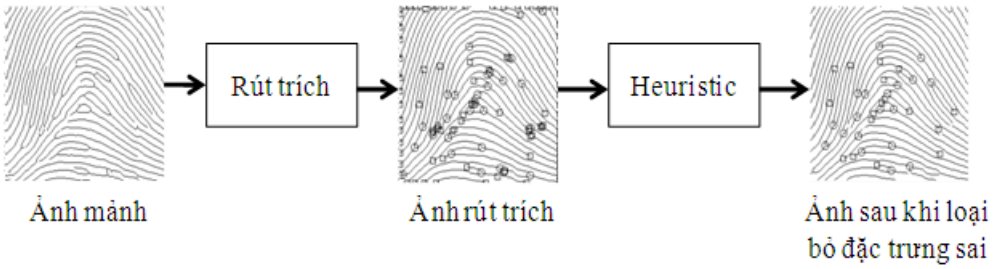
Hình 2.7. Một số trường hợp khiến quá trình rút trích vân sai

hai lằn gãy, (m7) có một lằn ngắn. Do đó, để tránh ảnh hưởng tới kết quả, một số đặc trưng thừa sẽ được loại bỏ thông qua một số luật heuristic như sau:

- Nếu khoảng cách giữa điểm rẽ nhánh và lằn kết thúc nhỏ hơn D thì hai điểm này được xem là cùng một lằn (trường hợp m1) và loại bỏ chúng.
- Nếu khoảng cách giữa hai điểm rẽ đôi lằn là nhỏ hơn D và chúng thuộc cùng về một lằn thì loại bỏ chúng đi (trường hợp m2, m3).
- Nếu hai điểm kết thúc lằn có khoảng cách nhỏ hơn D và hướng của chúng lệch với nhau một khoảng nhỏ. Đồng thời không có điểm kết thúc lằn nào xen vào giữa. Thì hai điểm kết thúc đó được xem là đặc trưng sai nhận từ lằn gãy và loại bỏ đi. (trường hợp m4, m5, m6).
- Nếu hai điểm kết thúc nằm trên một lằn ngắn với chiều dài nhỏ hơn D, thì loại bỏ hai điểm kết thúc đó đi (trường hợp m7).
- Nếu hướng của đặc trưng là không phù hợp với hướng của lằn cục bộ thì loại bỏ đi. Điều này loại bỏ đi những đặc trưng xuất hiện như nhiễu trong ảnh.

- Loại bỏ tất cả đặc trưng mà có khoảng cách nhỏ hơn ngưỡng T so với đường bao quanh của ảnh vân tay. Luật này sẽ loại bỏ những đặc trưng giả tạo mà nó xuất hiện dọc theo đường bao quanh của ảnh vân tay.

Trong đó, D là bề rộng hay khoảng cách trung bình giữa hai lần lân cận. Hình vẽ sau minh họa cho quá trình rút trích đặc trưng vân.



Hình 2.8. Quá trình rút trích đặc trưng vân tay

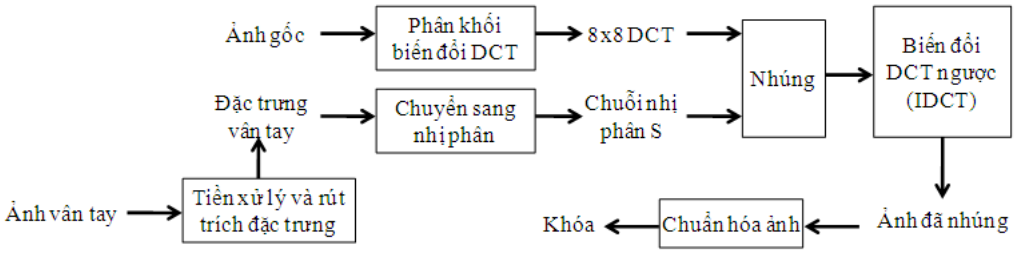
Lưu ý trong hình minh họa trên, hình tròn tương ứng với điểm rẽ đôi, hình vuông tương ứng với điểm kết thúc lằn.

3. PHƯƠNG PHÁP ĐỀ XUẤT

Phương pháp chứng thực bằng ảnh vân tay được đề xuất trong bài báo này gồm có ba giai đoạn, giai đoạn nhúng, giai đoạn trích, và giai đoạn chứng thực như sau.

3.1. Giai đoạn nhúng

Giai đoạn nhúng có thể tóm lược thông qua sơ đồ như trong Hình 3.9:



Hình 3.9. Quá trình rút trích đặc trưng vân tay

Tại thời điểm ban đầu, ảnh chứa gốc được phân thành các khối không trùng khớp nhau, kích thước 8×8. Áp dụng phép biến đổi Cosin rời rạc - DCT lên các khối này. Kết quả ta sẽ thu được một tập các hệ số Cosin từ mỗi khối. Song song với quá trình ảnh vân tay sau khi được tiền xử lý và rút trích đặc trưng. Vì mỗi đặc trưng chứa ba thông tin: (1) tọa độ

x, (2) tọa độ y, và (3) loại. Lưu ý rằng loại đặc trưng mang giá trị 1 nếu là lần đôi và mang giá trị 0 nếu là lần kết thúc. Thông tin đặc trưng được chuyển sang dạng nhị phân (gọi là chuỗi S). Chẳng hạn, ta có một đặc trưng rẽ đôi (30, 40, 1) thì mỗi giá trị trong đặc trưng chuyển sang nhị phân 8-bit và kết quả đạt được là 000111110001010000000001. Do chuỗi tín hiệu dạng nhị phân khá nhỏ so với kích thước ảnh chứa nên ở đây ta có thể chọn nhúng một bit trong chuỗi S vào một khối ảnh chứa 8×8. Để thực hiện thao tác nhúng một bit Sk và khối anh Bk, ta tiến hành các bước sau:

Bước 1. Chọn hai hệ số ở vị trí bất kỳ trong miền tần số giữa của hệ số Cosin, giả sử đó là $B_k(i,j)$ và $B_k(p,q)$. Gọi a là tham số thỏa mãn điều kiện $a = 2(2t+1)$ với t là một số nguyên dương ($0 \leq$ t ≤ 127). Trong chương trình thực nghiệm chọn $t = 4$.

Bước 2. Tính khoảng cách giữa hai hệ số, $d = |B_k(i,j) - B_k(p,q)| \, (mod\, a)$.

Bước 3. Xét giá trị S_k. Nếu S_k là bit '1' và $d \geq 2t+1$ thì ta không cần thay đổi gì cả. Ngược lại, nếu $d < 2t+1$ thì một trong hai hệ số $B_k(i,j)$ hoặc $B_k(p,q)$ sẽ được thay đổi để $d \geq 2t+1$ theo công thức sau:

$$MAX(B_k(i,j), B_k(p,q)) = MAX(B_k(i,j), B_k(p,q)) + INT(0.75 \times a) - d,$$

trong đó,

$$MAX(B_k(i,j), B_k(p,q)) = \begin{cases} B_k(i,j) & if\ B_k(i,j) \geq B_k(p,q) \\ B_k(p,q) & if\ B_k(i,j) < B_k(p,q) \end{cases},$$

INT(0.75×a) là giá trị nguyên nhỏ nhất mà nhỏ hơn 0.75×a.

Bước 4. Ngược lại nếu S_k là bit '0' và $d < 2t+1$ thì ta không cần thay đổi gì cả. Ngược lại, nếu $d \geq 2t+1$ và $S_k = 0$ thì một trong hai hệ số $B_k(i,j)$ hoặc $B_k(p,q)$ sẽ được thay đổi để $d < 2t+1$ theo công thức sau.

Quá trình trên sẽ được tiến hành cho đến khi chuỗi nhị phân S được nhúng hết vào ảnh chứa tập tại các hệ số Cosin của các khối ảnh chứa. Để có được ảnh sau khi nhúng, phép biến đổi Cosin ngược sẽ được áp dụng cùng với phép ghép các khối ảnh.

Để tăng khả năng an toàn dữ liệu cũng như phục hồi dữ liệu khi có tấn công, một số tham số sẽ được rút trích và được sử dụng như là khóa mật của hệ thống. Với hướng tiếp cận đề xuất này, ta cần rút trích ra ba tham số m_{00}, y, φ tương ứng là moment zero của ảnh sau khi nhúng, tỉ lệ kích thước (dài và rộng) của ảnh sau nhúng, và góc quay của ảnh sau khi nhúng so với ảnh chuẩn hóa.

Giả sử ảnh sau khi nhúng có kích thước là $l_x \times l_y$ thì $y = l_y / l_x$.

Moment cấp $p+q$ của một ảnh sau khi nhúng $f(x,y)$ là: $m_{pq} = \sum_x \sum_y x^p x^q f(x,y)$. Khi đó moment zero m_{00} của ảnh sẽ tương ứng với $p = 0, q = 0$, tức $m_{00} = \sum_x \sum_y f(x,y)$. Moment trung tâm cấp $p+q$ của ảnh sau khi nhúng được định nghĩa như sau

$$\mu_{pq} = \sum_x \sum_y (x - \overline{x})^p (y - \overline{y})^p f(x,y), \text{trong đó: } \overline{x} = \frac{m_{10}}{m_{00}}, \overline{y} = \frac{m_{01}}{m_{00}}.$$

Góc quay φ của ảnh sau khi nhúng so với ảnh chuẩn hóa được tính như sau:

$$\begin{cases} \varphi = \tan^{-1}\left(-\frac{t_1}{t_2}\right) \\ -t_1 \sin\varphi + t_2 \cos\varphi > 0 \end{cases},$$

trong đó, $t_1 = \mu_{12} + \mu_{30},\ t_2 = \mu_{21} + \mu_{03}$.

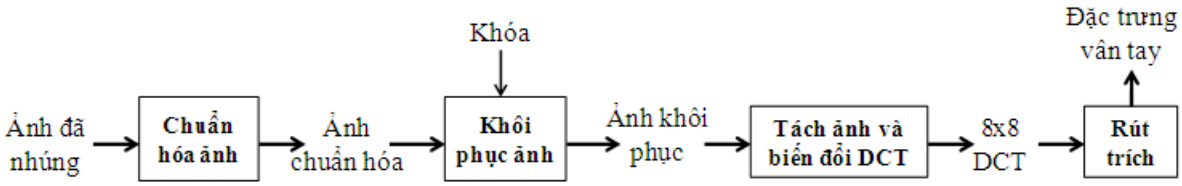
3.2. Giai đoạn rút trích

Giai đoạn rút trích được chia thành hai trường hợp.

Trường hợp thứ nhất: Người gửi và người nhận cùng thực hiện trên cùng một đối tượng, có nghĩa là không có tấn công trên đường truyền vào ảnh sau nhúng không thay đổi.

Trường hợp thứ hai: Có tấn công trên đường truyền vào ảnh sau nhúng bị thay đổi khi đến chuyển tới người nhận.

Thông thường người nhận không biết chính xác ảnh chứa có bị tấn công hay không nên một cách tổng quát ta sẽ xem xét quá trình rút trích khi có tấn công và được mô tả qua Hình 3.10 như sau.

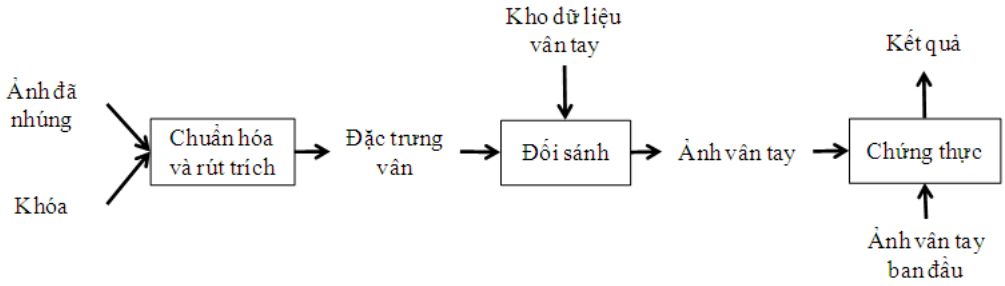


Hình 3.10. Quá trình rút trích đặc trưng vân tay

Đầu tiên, người nhận sẽ chuẩn hóa ảnh. Ảnh chuẩn hóa kết hợp với ba tham số m_{00}, y, φ để khôi phục lại ảnh. Ảnh sau khi được khôi phục sẽ được chia thành các khối không trùng lắp nhau, mỗi khối kích thước 8×8. Áp dụng phép biến đổi DCT lên mỗi khối, kết quả được tập hệ số DCT. Quá trình rút trích đặc trưng được tiến hành bằng cách lựa chọn các cặp hệ số giữa trong miền tần số giữa, giả sử đó là $B_k(i,j)$ và $B_k(p,q)$. Tính khoảng cách giữa hai hệ số với a là giá trị được chọn trong quá trình nhúng. Dựa vào giá trị của độ khác biệt này, thông tin watermark được rút trích như sau: Nếu $d \geq 2t+1$ thì gán $s_i = 1$. Ngược lại nếu $d < 2t+1$ thì gán $s_i = 0$.

3.3. Giai đoạn chứng thực

Vì dữ liệu đặc trưng vân tay được chuyển sang chuỗi nhị phân trước khi nhúng vào ảnh và quá trình rút trích dữ liệu từ ảnh cũng cho ra một chuỗi nhị phân nên để quá trình chứng thực đạt độ chính xác cao, ở đây, ta dùng khoảng cách Hamming xác định độ khác biệt giữa hai chuỗi bit rút trích $A = a_1a_2...a_n$ và chuỗi bit cần so sánh $B = b_1b_2...b_n$. Khi đó độ khác nhau giữa hai chuỗi bit là: Nếu D nhỏ hơn một ngưỡng $D = \frac{1}{n}\sum_{i=1}^{n}|a_i - b_i|$ thì hai chuỗi khớp với nhau. Ngược lại thì hai chuỗi không khớp với nhau. Trong trường hợp có nhiều chuỗi



Hình 3.11. Quá trình rút trích đặc trưng vân tay

khớp với chuỗi bit rút trích thì sẽ chọn chuỗi mà có giá trị D nhỏ nhất. Tương ứng với D nhỏ nhất, ta sẽ có được một ảnh vân tay tương ứng. Ảnh vân tay sẽ được so sánh với ảnh vân tay ban đầu xem có giống nhau không. Nếu giống nhau thì quá trình chứng thực đúng, còn ngược lại thì sai.

3.4. Kết quả thực nghiệm

Kết quả thực nghiệm được tiến hành trên máy tính có cấu hình Intel(R) Core(TM)2 CPU T5800 2.00GHz, RAM 4GB, với hệ điều hành là Windows Vista 32-bit. Chương trình được cài đặt trên VC++ 6.0 với bộ thư viện hỗ trợ OpenCV. Bộ dữ liệu vân tay thực nghiệm là 1500 mẫu lấy từ Bộ Công An. Trong đó, ảnh vân kiểm thử là 1.tif, 1.jpg, 2.tif, 2.jpg, 3.tif, 3.jpg, 4.tif, 4.jpg, 5.tif, 5.jpg, tương ứng với kích thước 64.2KB, 13.9KB, 8.89KB, 64.5KB, 12.3KB, 64.5KB, 12.2KB, 64.5KB, 11.7KB, 64.5KB. Ảnh cần bảo vệ trong trường hợp này là Lena.jpg và Cameraman.bmp tương ứng với kích thước 34.1KB, 65KB.

Để xác định chất lượng ảnh sau nhúng, bài báo sử dụng độ đo PSRN (Peak Signal-to-Noise Ratio) được xác định theo công thức $PSNR = 10 \times \log_{10} \frac{255^2}{MSE}$ (dB) trong đó MSE (Mean Square Error) là không gian lỗi trung bình giữa ảnh gốc và ảnh sau khi nhúng. Với ảnh xám gốc, kích thước $w \times h$, giá trị MSE được xác định như sau: $MSE_{grayscale} = \frac{1}{w \times h} \sum_{x=1}^{h} \sum_{y=1}^{w}$ trong công thức trên, G_{xy} và $G'xy$ là giá trị pixel tại vị trí (x, y) của ảnh gốc và ảnh sau khi nhúng.

Trong phần này, ảnh sau khi nhúng sẽ được tiến hành thực nghiệm qua hai trường hợp. Trường hợp thứ nhất là không có tấn công. Kết quả chứng thực được ghi nhận lại như sau.

Trường hợp thứ hai được xem xét khi có các tấn công. Các tấn công được tiến hành trong phần này bao gồm quay (R), tịnh tiến (T), tỉ lệ (S), thêm nhiễu (Median, Gaussian), làm mờ. Kết quả chứng thực được ghi nhận lại như sau.

Ngoài ra phương pháp đề xuất trong bài báo này cho khả năng nhúng cao cùng với chất lượng ảnh sau nhúng tốt. Điều này thể hiện thông qua kết quả thực nghiệm sau:

Bảng 1. Kết quả chứng thực khi không có tấn công

Ảnh vân	Kích thước ảnh vân (KB)	Kích thước vector đặc trưng nhúng (bit)	Kích thước vector đặc trưng rút trích (bit)	D	Chứng thực
1.tif	64.2	1088	1088	0	Đúng
1.jpg	13.9	3904	3904	0	Đúng
2.jpg	8.89	1440	1440	0	Đúng
2.tif	64.5	992	992	0	Đúng
3.jpg	12.3	2016	2016	0	Đúng
3.tif	64.5	960	960	0	Đúng
4.jpg	12.2	1824	1824	0	Đúng
4.tif	64.5	1312	1312	0	Đúng
5.jpg	11.7	1536	1536	0	Đúng
5.tif	64.5	823	823	0	Đúng

Bảng 2. Kết quả chứng thực sau khi thực hiện tấn công RST trên ảnh đã nhúng

Ảnh vân: 1.tif Kích thước vector đặc trưng nhúng: 1088 Kích thước vector đặc trưng rút trích: 1088			Ảnh vân: 296.jpg Kích thước vector đặc trưng nhúng: 3904 Kích thước vector đặc trưng rút trích: 3904		
Tấn công	**D (%)**	**Chứng thực**	**Tấn công**	**D (%)**	**Chứng thực**
R (30)	0.372243	Đúng	T(40,50) R(45)	0.367572	Đúng
R (-45) S (0.8)	0.367647	Đúng	T(30,50) R(110) S(0.7)	0.364754	Đúng
R (157) S (0.6) T(40,40)	0.372243	Đúng	R (-300) S(1.1)	0.367828	Đúng
R (-125) S(1.2)	0.339154	Đúng	R(180)	0.371158	Đúng
R (226) T(100,50)	0.357537	Đúng	R(90) S(1.2)	0.367572	Đúng
S(0.4)	0.375	Đúng	S(1.5) T(100,100)	0.366547	Đúng

Bảng 3. Kết quả chứng thực sau khi thực hiện tấn công nhiễu và làm mờ

Ảnh vân: 1.tif Kích thước vector đặc trưng nhúng: 1088 bits Kích thước vector đặc trưng rút trích: 1088 bits					
Tấn công	**D**	**Chứng thực**	**Tấn công**	**D**	**Chứng thực**
Gaussian Noise(3)	0.389706	Đúng	Add Noise (20)	0.372243	Đúng
Gaussian Noise(7)	0.386029	Đúng	Add Noise (50)	0.384191	Đúng
Gaussian Noise(9)	0.390625	Đúng	Add Noise (75)	0.386029	Đúng
Simple Blur(3)	0.383272	Đúng	Add Noise (100)	0.368566	Đúng
Simple Blur(7)	0.383272	Đúng	Frosted Glass (3)	0.373162	Đúng
Simple Blur(9)	0.397978	Sai	Frosted Glass (5)	0.386029	Đúng
Frosted Glass (3) R(35)	0.391544	Đúng	R(25) S(0.7) Gaussian Blur(9)	0.391544	Đúng
Add Noise (50) R(-45)S(0.9)	0.397059	Sai	R(25) S(0.7) Blur(9)	0.395221	Sai

Bảng 4. Khả năng nhúng và chất lượng ảnh sau khi nhúng

Ảnh cần chứng thực Lena.jpg (512×512): 34.1KB			Ảnh cần chứng thực Cameraman.bmp(256×256):65KB		
Ảnh vân tay	Kích thước ảnh vân	PSNR (dB)	Ảnh vân tay	Kích thước ảnh vân	PSNR (dB)
1.tif	64.2KB	55.135506	1.tif	64.2KB	49.16818
1.jpg	13.9KB	49.662246	296.jpg	13.9KB	43.525588
2.jpg	9.41KB	53.79492	2.jpg	9.41KB	47.91026
2.tif	64.5KB	55.370502	2.tif	64.5KB	49.924009
3.jpg	12.3KB	52.082649	3.jpg	12.3KB	46.286146
3.tif	64.5KB	55.417789	3.tif	64.5KB	49.431832
4.jpg	12.2KB	52.581738	4.jpg	12.2KB	46.894973
4.tif	64.5KB	54.096616	4.tif	64.5KB	48.350862

4. KẾT LUẬN

Bài báo đã đề xuất một phương pháp chứng thực ảnh bằng sinh trắc học vân tay. Kết quả thực nghiệm cho thấy mô hình này có khả năng bền vững với các tấn công quay, tỉ lệ, tịnh tiến, thêm nhiễu Gaussian và làm mờ ảnh. Hơn thế nữa, hướng tiếp cận này cho phép nhúng vân ảnh có kích thước lớn hơn ảnh cần chứng thực với chất lượng ảnh sau nhúng khá tốt (PSNR>43.5dB).

TÀI LIỆU THAM KHẢO

[1] A. E. Hassanien, Hiding iris data for authentication of digital images using wavelet theory, *Pattern Recognition and Image Analysis* (December 2006) 637–643.

[2] A. K. Jane, and U. Uludag, Hiding fingerprint minutiae in images, *Proceeding of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2002.

[3] B. Gunsel, U. Uludag, and A. M. Tekalp, Robust watermarking of fingerprint images, *Pattern Recognition* **35** (12) (Dec. 2002) 2739—2747.

[4] C. C. Ramos, R. R. Reyes, M. N. Miyatake, and H. P. Meana, Image authentication scheme based on self-embedding watermarking, *Lecture Notes In Computer Science* **5856** (2009) 1005–1012.

[5] Federal Bureau of Investigation (FBI) John Edgar Hoover, "The Science of fingerprints: classification and uses", U.S. Government Printing Office, Washington D.C, 2006.

[6] L. Ghouti, and A. Bouridane, Data hiding in fingerprint images, *European Signal Processing Conference (Eusipco)*, Warsaw, Poland, September 2006.

[7] L. Hong, Y. Wang, and A. K. Jain, Fingerprint image enhancement: Algorithm and performance evaluation, *Transactions on PAMI* **20** (8) (August 1998) 777–789.

[8] N. K. Ratha, J. H. Connell, and R. M. Bolle, Secure data hiding in wavelet compressed fingerprint images, *Proc. ACM Multimedia*, Oct. 2000 (127—130).

[9] P. MeenakshiDevi, M. Venkatesan, and K. Duraiswamy, A fragile watermarking scheme for image authentication with tamper localization using integer wavelet transform, *Journal of Computer Science* **5** (11) (2009) 831–837.

[10] R. Thai, "Fingerprint image enhancement and minutiae extraction", Report, School of Computer and Software Engineering, University of Western Australia, Perth, 2003.

Ngày nhận bài 28 - 4 - 2010
Nhận lại sau sửa 13 - 5 - 2011