

Nhận dạng vân tay trong hệ thống bảo mật Sinh trắc học

Bùi Thị Hương

ThS. Trường Đại học Hải Phòng

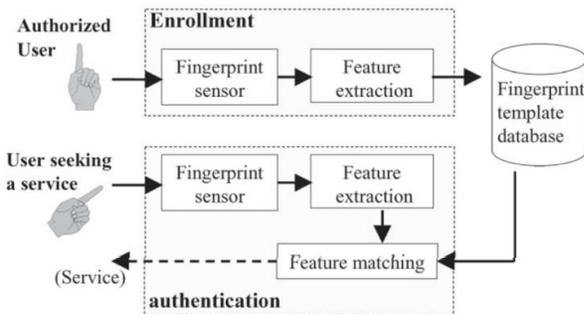
Received: 15/2/2024; Accepted: 23/2/2024; Published: 26/2/2024

Abstract: The most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in order to design a fingerprint Identification in Biometric Security Systems.

Keywords: Biometric Security, Systems Fingerprint Identification, matching image, select image features.

1. Đặt vấn đề

Hệ thống an ninh thông thường sử dụng một trong hai phương pháp (PP) dựa trên tri thức (mật khẩu hoặc mã PIN), và PP token-based (hộ chiếu, bằng lái xe, thẻ ID) và nó dễ bị gian lận vì số PIN có thể bị quên hoặc bị tấn công và các thẻ có thể bị mất, nhân đôi hoặc bị đánh cắp. Bằng cách sử dụng kết hợp vân tay và mật khẩu, việc xác nhận một người có thể thực hiện bằng một hệ thống nhận dạng vân tay an toàn và thuận tiện.



Hình 1: Cấu trúc cơ bản của hệ thống nhận dạng [1]

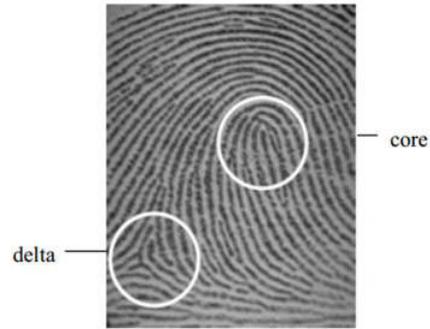
2. Nội dung nghiên cứu

2.1. Các điểm đặc trưng trên ảnh vân tay

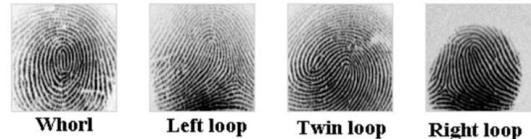
Trên các ảnh vân tay có các điểm đặc trưng (là những điểm đặc biệt mà vị trí của nó không trùng lặp trên vân tay người khác) Được phân thành hai loại: *singularity* và *minutiae*

Singularity: Trên vân tay có những vùng có cấu trúc khác thường so với những vùng bình thường khác (thường có cấu trúc song song), những vùng như vậy gọi là singularity. Có hai loại singularity là core và delta.

Core thường có một số dạng như sau:

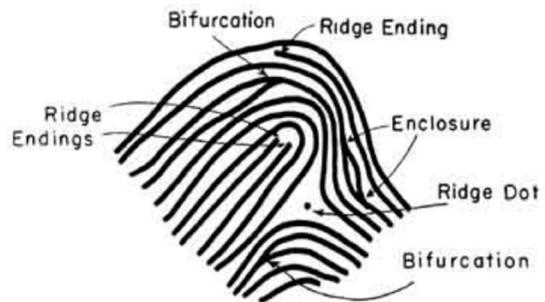


Hình 2: Mô tả singularity.



Hình 3: Mô tả Core.

Minutiae: Khi dò theo từng đường vân ta sẽ thấy có những điểm đường vân kết thúc (Ridge Ending) hoặc rẽ nhánh (Bifurcation), những điểm này được gọi chung là minutiae.



Hình 4: Mô tả minutiae.

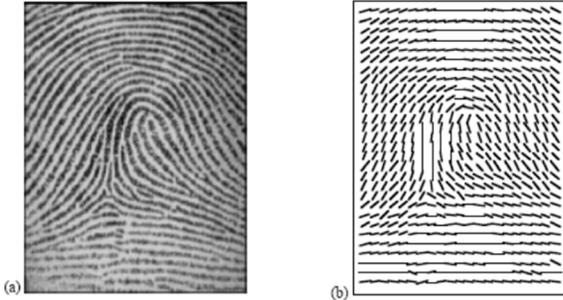
Trích các điểm đặc trưng

Bằng các PP xử lý ảnh ta có thể tìm được vị trí các

điểm đặc trưng trên các ảnh vân tay.

Trích các điểm singularity

Ảnh vân tay là ảnh định hướng, các đường vân là các đường cong theo các hướng xác định. Góc hợp bởi phương của một điểm trên đường vân với phương ngang được gọi là hướng của điểm đó. Tập hợp các hướng của các điểm trên ảnh vân tay gọi là trường định hướng của ảnh vân tay đó.



Hình 4: Trường định hướng của ảnh vân tay.

PP xác định trường định hướng như sau:

Chia ảnh vân tay thành các khối nhỏ hơn kích thước $W \times W$

Tính gradient theo hai hướng x, y là G_x, G_y tại mỗi điểm (pixel) trong khối

$$\varphi = \frac{1}{2} \tan^{-1} \left(\frac{\sum_{i=1}^W \sum_{j=1}^W 2G_x(i, j)G_y(i, j)}{\sum_{i=1}^W \sum_{j=1}^W (G_x^2(i, j) - G_y^2(i, j))} \right)$$

Khi đó hướng của điểm chính giữa của khối được xác định theo công thức:

Trích các điểm minutiae

Có hai PP chính để tìm các điểm minutiae: trích các điểm minutiae từ ảnh binary và trích các điểm minutiae trực tiếp từ ảnh xám.

Trích các điểm minutiae từ ảnh binary

$$\sum_{i=0}^7 N_i = 1$$

Ý tưởng chính của PP này là từ ảnh

xám ban đầu ta sử dụng các bộ lọc thích hợp để phát hiện và làm mảnh đường vân dưới dạng một pixel, biến đổi ảnh xám ban đầu thành ảnh binary (có giá trị là 0 hoặc 1) tương ứng. Sau đó, các điểm minutiae sẽ được trích như sau: giả sử (x, y) là một điểm trên đường vân đã được làm mảnh và N_0, N_1, \dots, N_7 là 8 điểm xung quanh nó thì

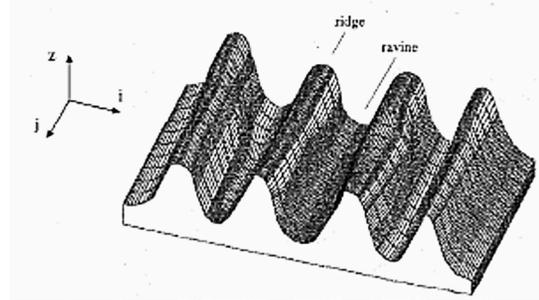
(x, y) là một điểm kết thúc nếu;

(x, y) là một điểm rẽ nhánh nếu $\sum_{i=0}^7 N_i > 2$.

Trích các điểm minutiae trực tiếp từ ảnh xám

Dò theo đường vân giả sử I là một ảnh xám có

kích thước là $m \times n$ và nếu coi chiều thứ ba z là mức xám tại điểm (i, j) thì bề mặt của ảnh vân tay I có dạng như sau:



Hình 2.5: Bề mặt của ảnh vân tay.

Theo quan điểm toán học thì đường vân là tập hợp các điểm cực đại dọc theo một hướng xác định. Việc xác định các điểm minutiae trực tiếp từ ảnh xám dựa vào thuật toán dò theo đường vân. Thuật toán này dựa vào việc xác định các điểm cực đại dọc theo hướng của đường vân.

Tóm lại việc tìm các điểm minutiae bằng thuật toán dò theo đường vân được thực hiện như sau:

Lấy một điểm bất kì (i_s, j_s) trên ảnh I

Tìm hướng φ_s tại điểm (i_s, j_s)

Tìm điểm cực đại (i_c, j_c) gần (i_s, j_s) nhất

Tìm hướng φ_c tại điểm (i_c, j_c)

Dịch chuyển theo hướng φ_c một đoạn μ

Tính chính lại điểm cực đại (i_c, j_c) và hướng φ_s

Tiếp tục quá trình này để dò theo đường vân cho đến khi không phát hiện được điểm cực đại (i_c, j_c) thì đó là điểm Ridge Ending hoặc chạm vào một đường vân khác thì đó là điểm Bifurcation (mỗi đường vân sau khi được dò sẽ được gán nhãn)

Tiếp theo chọn một điểm (i_s, j_s) khác và thực hiện lại quá trình trên cho đến khi dò hết tất cả các đường vân.

2.2. Kiểm nghiệm thuật toán nhận dạng

Thực hiện đúng các quá trình nhận dạng vân tay: Mở ảnh vân tay hoặc quét từ thiết bị quét vân tay.



Hình 6: Kết quả quét từ thiết bị quét vân tay.

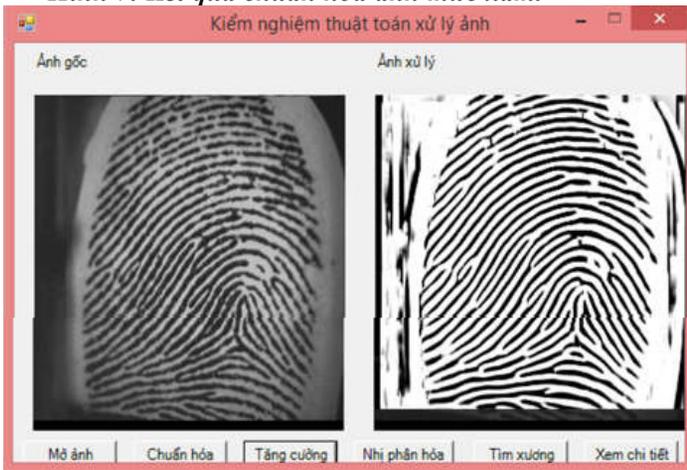
Chuẩn hóa ảnh mức xám của ảnh, đồng thời tìm vùng có vân tay

3. Kết luận

Bài báo đã mô tả tổng quan nhận dạng vân tay và công nghệ quét ảnh cũng như các PP trích chọn đặc trưng của ảnh. Vấn đề lựa chọn của một thuật toán tối ưu cho phù hợp với dấu vân tay để thiết kế một hệ thống phù hợp với hiệu suất mong đợi và độ chính xác là mối quan tâm lớn cho các nhà thiết kế. Nó là điều cần thiết đầu tiên để hiểu được kiến trúc cơ bản của một hệ thống bảo mật sinh trắc học cơ bản và sau đó tiến vào tìm hiểu làm thế nào một hệ thống xác thực dấu vân tay diễn hình hoạt động.



Hình 7: Kết quả chuẩn hóa ảnh mức xám.



Tăng cường ảnh bằng hàm Gabor

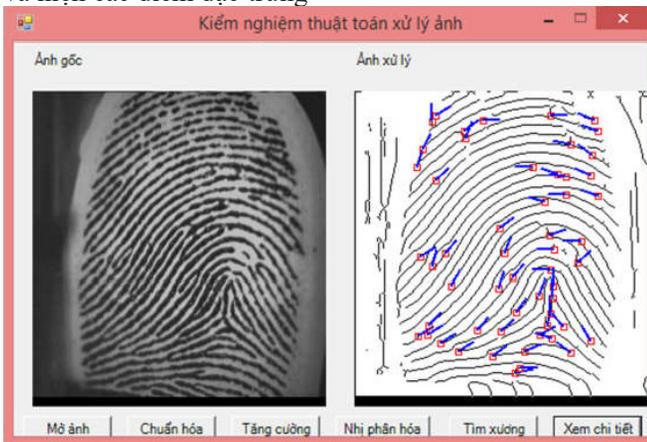
Hình 8: Kết quả tăng cường ảnh bằng hàm Gabor. Nhị phân hóa để tìm trường định hướng, tìm xương và hiện các điểm đặc trưng

Từ phần mềm miễn phí có sẵn trên Internet, hộp công cụ xử lý hình ảnh và phần mềm MATLAB tác giả đã tạo ra một hệ thống chứng thực cá nhân quy mô nhỏ. Kết quả với 25 cặp dấu vân tay (chất lượng cao) đã được đưa vào phần mềm sử dụng thuật toán lọc kết quả như sau: (Giá trị Threshold = 35)

Số lần chấp nhận sai = 2 (8%) Số lần từ chối sai = 1 (4%)

Nguyên nhân của độ lệch trong trường hợp này có thể là do thực tế là các cơ sở dữ liệu đã được sử dụng là nhỏ, và không đại diện cho quy ước tối thiểu cần thiết cho các chức năng thích hợp của phần mềm. Có lẽ, điều này có thể được khắc phục bằng cách sử dụng một số lượng lớn các bản in trên đó lỗi này có thể dần dần giảm tới giới hạn chấp nhận được.

Tài liệu tham khảo



Hình 9: Kết quả nhị phân hóa.

1. Arya, S., and Mount, D.M. (1993). *Approximate nearest neighbor queries in fixed dimensions. In Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'93), pp. 271- 280.*

2. Arya, S., Mount, D.M., Netanyahu, N.S., Silverman, R., and Wu, A.Y. (1998). *An optimal algorithm for approximate nearest neighbor searching. Journal of the ACM, 45:891-923.*

3. Ballard, D.H. (1981). *Generalizing the Hough transform to detect arbitrary patterns. Pattern Recognition, 13(2):111-122.*