ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO

Môn: Nhận dạng

Fingerprint Recognition

Sinh viên:

Chu Nguyên Đức – 1712352

Bùi Chí Dũng – 1712364

Nguyễn Công Lý - 1712584

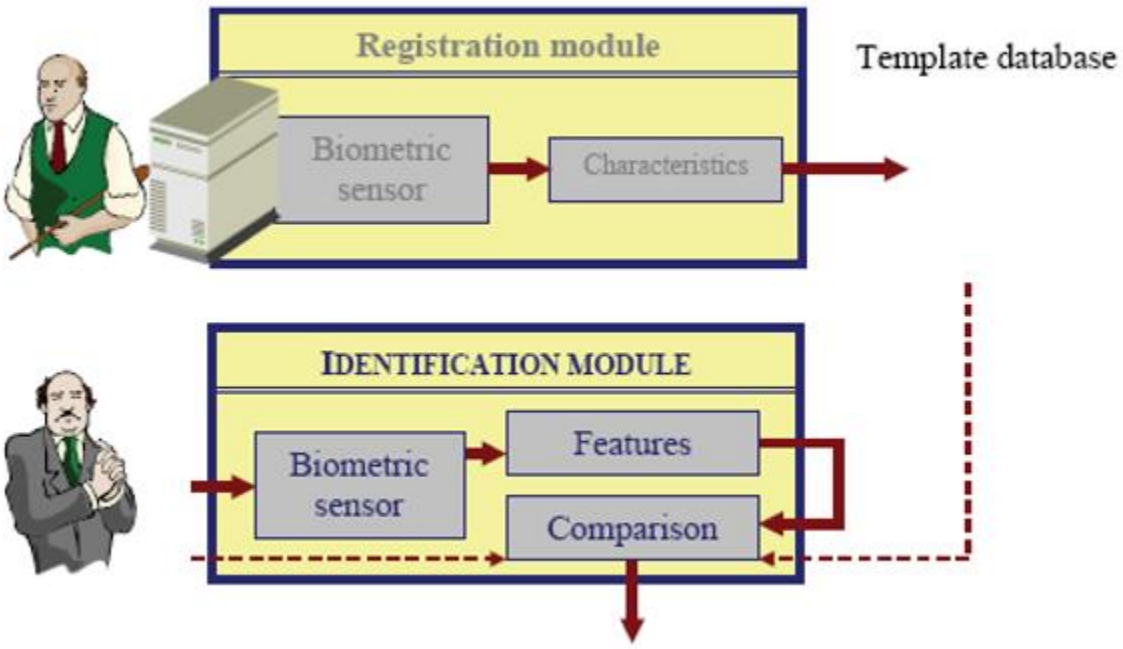
7 / 2020

Sau khi thu thập dữ liệu dấu vân tay dưới dạng hình ảnh, chúng ta tiến hành xử lý ảnh bằng cách tăng cường, làm nổi ảnh, để có thể đến bước tiếp theo là rút trích ra những đặc trưng trên dấu vân tay. Tại đây, các đặc trưng có những đặc điểm đặc biệt có thể được dùng để so sánh các dấu vân tay với nhau để đưa ra được kết luận sau cùng. Tuy vậy, ngày càng có thêm nhiều phương pháp mới trong các bước thực hiện nhận dạng vân tay, giúp cho lời giải của bài toán nhận dạng ngày càng rõ ràng hơn.

1. INTRODUCTION

Ngày càng xuất hiện thêm nhiều kỹ thuật sinh trắc học giúp cho việc bảo mật, cũng như nhận dạng, định danh cá thể người trở nên hiện đại hơn. Tuy có vài kỹ thuật nổi bậc, nhưng để đạt đến mức độ hoàn thiện và đáng tin cậy tối đa thì gần như chưa có một kỹ thuật nào đạt được. Nhưng trong đó, có thể kể đến nhận dạng vân tay – một kỹ thuật được xem là đáng tin cậy nhất được dùng để nhận diện một người, nó rất được quan tâm bởi vì tính bảo mật, đặc trưng riêng biệt về sinh trắc, cũng như ứng dụng với cơ sở dữ liệu nhỏ.

Như chúng ta đã biết, đa số những hệ thống bảo mật từ xưa đến nay là password và mã PIN(Personal Identification Number) vẫn đang rất phổ biến. Tuy nhiên ta có thể thấy nhược điểm quan trọng nhất của nó, đó chính là rất dễ quên, cũng như rất dễ để nhiều người biết được, và bất kì ai biết được những đoạn mã này đều có thể thay mặt bạn sử dụng thiết bị hay tài khoản. Vì vậy mà việc sử dụng kết hợp vân tay cùng mật mã sẽ giúp hệ thống nhận dạng vân tay trở nên bảo mật hơn.



Cấu trúc cơ bản của một hệ thống nhận dạng vân tay

Dấu vân tay được lấy từ một người thông qua một thiết bị có thể lưu lại/chụp lại hình ảnh vân tay, và giữ lại trong cơ sở dữ liệu. Khi có bất cứ nhu cầu nào về việc đối sánh vân tay, chúng

ta lấy dấu vân tay muốn đối sánh, và đối chiếu với dấu vân tay đã lưu trong cơ sở dữ liệu để đưa ra kết quả.

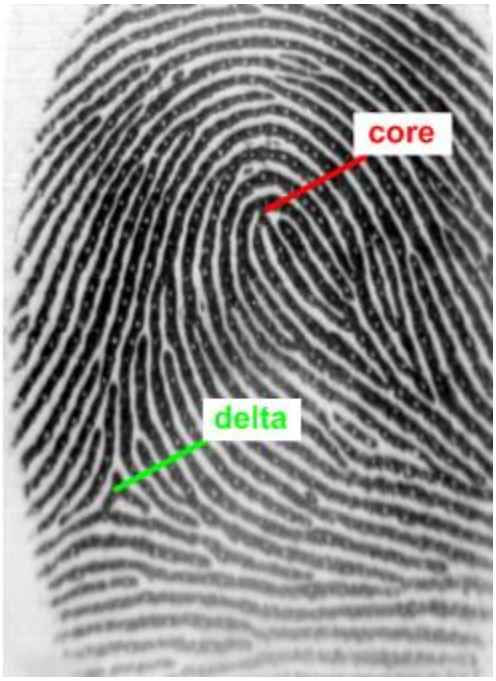
Việc áp dụng kỹ thuật Mạng neural nhân tạo trong việc đối sánh dấu vân tay không phải là một phương pháp mới. Tuy nhiên, việc tối ưu hóa phương pháp này vẫn liên tục được mọi người quan tâm và thực hiện, cho đến nay, khả năng của nó vẫn chưa được khám phá hết sức. Đề tài này được thực hiện để tiếp tục khai phá khả năng của Neural Networks, đặc biệt là trong việc so sánh hai dấu vân tay và được ra xác suất so khớp chính xác nhất có thể.

2. DATA

2.1. Vân tay [1]

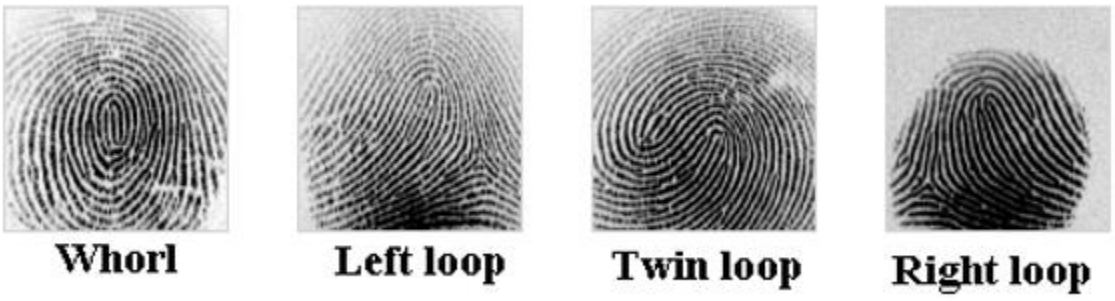
Vân tay là một đặc điểm sinh trắc đặc biệt xuất hiện trên đầu ngón tay của mỗi người. Đặc điểm này là riêng biệt đối với mỗi người, xác suất gặp được hai vân tay giống nhau từ hai người khác nhau gần như bằng không. Đặc điểm làm nên điều này chính là các vị trí không bị trùng lặp trên vân tay được phân ra thành hai loại: **singularity và minutiae**.

Singularity là những vùng cấu trúc khác thường so với những vùng bình thường khác (có dạng cấu trúc song song) và có hai loại là **core** và **delta**.



Singularity

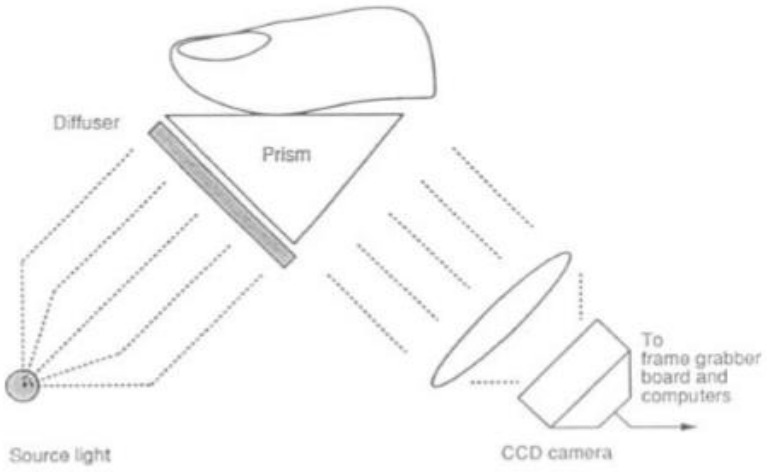
Một số dạng **Core:**



Minutiae là những điểm đường vân kết thúc (Ridge Ending) hoặc rẽ nhánh (Bifurcation).

2.2. Thu thập dấu vân tay [1]

Thông thường, dấu vân tay sẽ được thu bằng phương pháp lăn mực (ink-technique) như trong việc lăn dấu vân tay để công chứng giấy tờ, hay làm chứng minh thư, … Tuy nhiên có một nhược điểm khá lớn, đó là phương pháp này cho ảnh khá xấu và mờ, gây nhiều khó khăn trong việc đối sánh. Vì vậy mà cảm biến vân tay được sinh ra, khắc phục các yếu điểm của phương pháp lăn mực thông thường. Cảm biến vân tay cho hình ảnh chất lượng, rõ nét hơn rất nhiều so với ink-technique. Kỹ thuật này có ba loại chính đó là: **optical, solid-state** và **ultrasound.**



Dưới đây là một số ảnh chụp từ các thiết bị cảm biến:

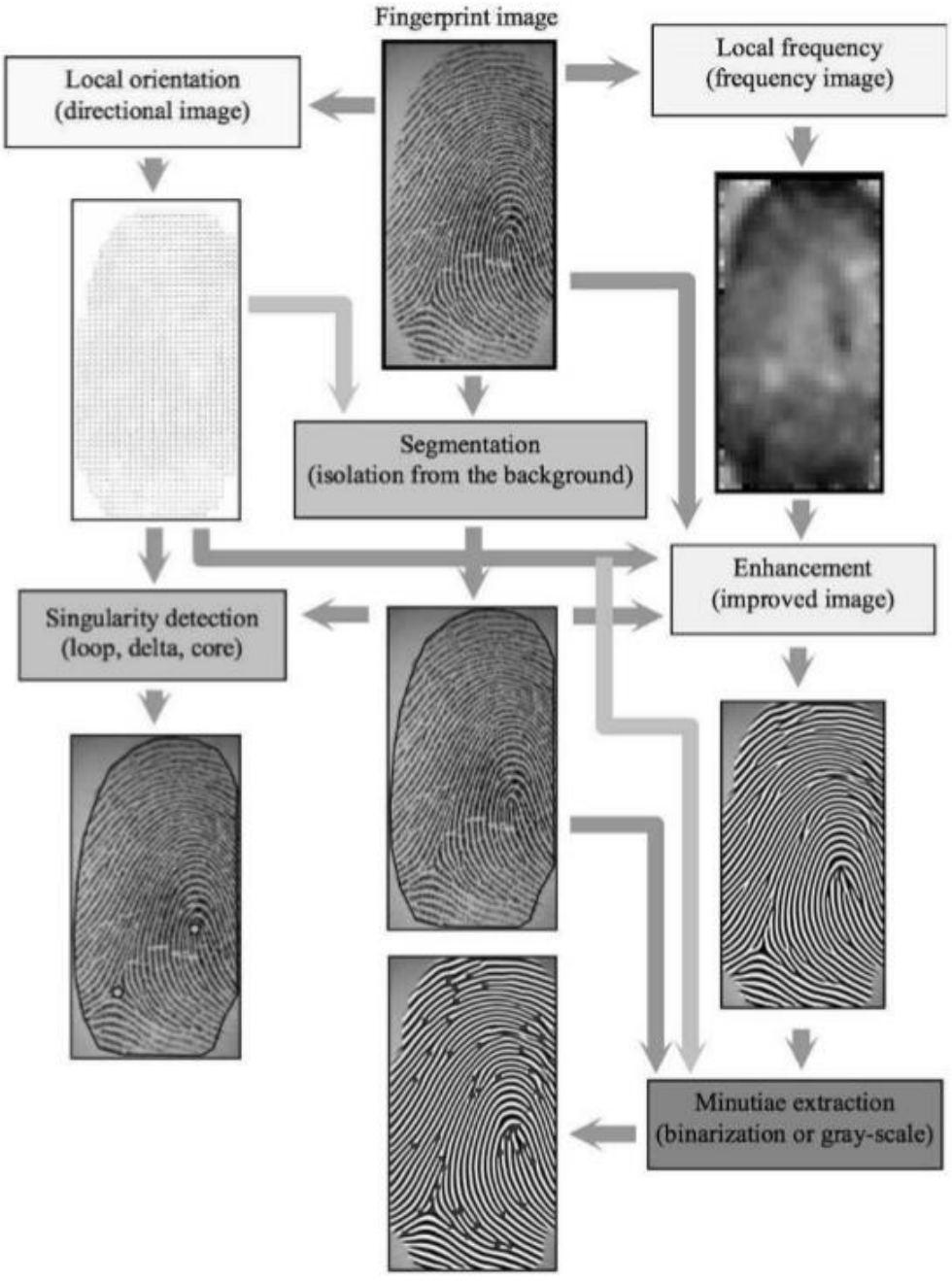
Hình 1.2: Ảnh vân tay được chụp từ các thiết bị trên: a) Biometrika FX2000,
b) Digital Persona UareU2000, c) Identix DFR200,
d) Ethentica TactilSense T-FPM,
e) STMicroelectronics TouchChip TCS1AD, f) Veridicom FPS110,
g) Atmel FingerChip AT77C101B, h) Authentec AES4000.

Tuy cho chất lượng hình ảnh cao, nhưng cảm biến vân tay không tránh khỏi những yếu điểm gây khó chịu cho người sử dụng. Cảm biến sẽ không hoạt động tốt trong điều kiện tay bị ẩm, ước hay quá khô, áp lực bề mặt lúc quét vân tay, hay thậm chị là có thể bị làm giả gây ảnh

hưởng đến vấn đề bảo mật, mặc dù đặc tính sinh trắc của vân tay rất đặc biệt nhưng vẫn không thể loại trừ khả năng làm giả dấu vân tay.

3. RÚT TRÍCH ĐẶC TRƯNG

Bằng các phương pháp xử lý ảnh, tăng cường ảnh, ta sẽ tìm ra được điểm đặc trưng trên dấu vân tay, lấy đó làm dữ liệu so sánh trong bước tiếp theo của quá trình nhận dạng.

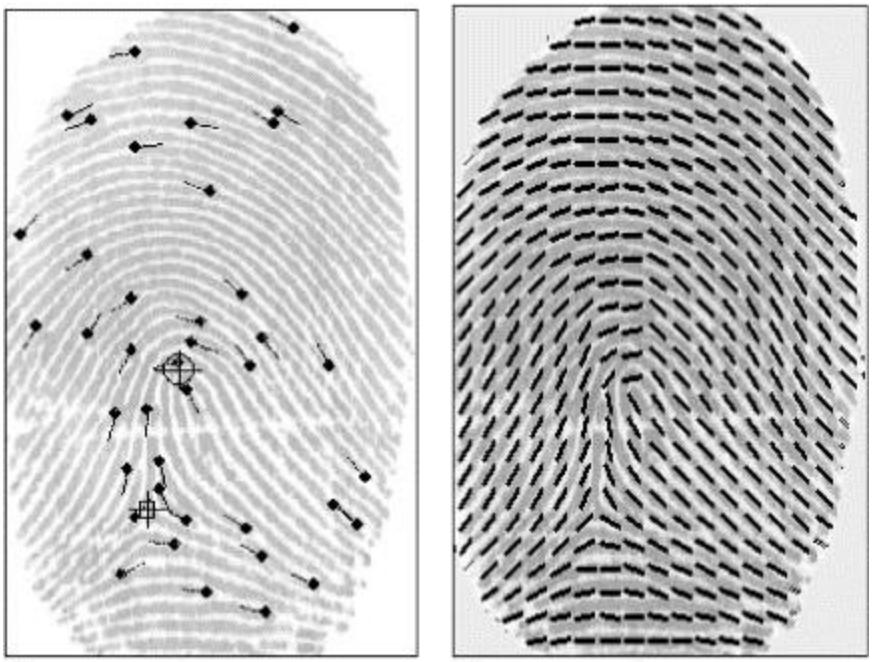


Các bước trong quá trình rút trích đặc trưng

3.1. Trích điểm singularity

3.1.1. Trường định hướng (Orientation field) [3] [6]

Ảnh vân tay là một ảnh mang tính định hướng, trong đó các đường vân (ridge) chính là các đường cong theo hướng xác định. Một điểm trên đường vân và phương ngang tạo thành một góc gọi là hướng của điểm đó. Trường định hướng là tập hợp hướng của các điểm trên dấu vân tay.



(a) (b)

Phương pháp xác định trường định hướng:

- Chia ảnh vân tay thành các thành phần nhỏ hơn với kích thước là WxW

- Tính gradient theo hướng x và y là Gx, Gy tại mỗi pixel trong phần nhỏ đó

- Khi đó thì hướng của điểm chính giữa phần được xác định theo công thức:

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

3.1.2. Xác định các điểm singularity bằng chỉ số Poincare [3]:

Cho (i,j) là một điểm bất kì lấy trên ảnh vân tay, gọi C là đường cong khép kín xung quanh điểm cho trước, khi đó chỉ số Poincare tại điểm cho trước là tổng đại số các độ lệch hướng của các điểm liền kề nhau trên đường cong C:

$$Poincare(i,j) = \sum_{k=0}^{Np-1} \Delta(k)$$

$$\Delta(k) = \begin{cases} d(k) & |d(k)| < \pi/2 \\ d(k)+\pi & d(k) \le -\pi/2 \\ d(k)-\pi & \end{cases}$$

$$d(k) = \varphi(x_{k+1}, y_{k+1}) - \varphi(x_k, y_k)$$

Trong đó Np là tông số điểm trên đường cong C, $\phi(x,y)$ là hướng tại điểm (x,y)

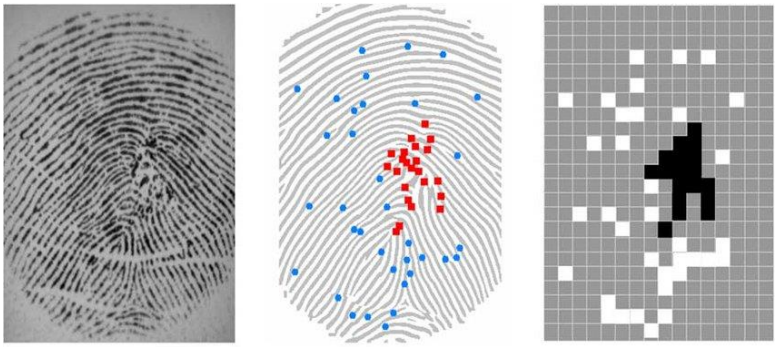
Dựa vào chỉ số Poincare ta biết được các điểm singularity theo quy luật sau:

$$Poincare(i,j) = \begin{cases} 0^0 & \text{(i,j) không phải là điểm singularity} \\ 360^0 & \text{(i,j) là điểm whorl} \\ 180^0 & \text{(i,j) là điểm loop} \\ -180^0 & \text{(i,j) là điểm delta} \end{cases}$$

3.2. Trích các điểm minutiae

Để trích điểm minutiae trên vân tay ta có hai phương pháp chính đó là trích từ ảnh binary hoặc trích trực tiếp từ ảnh xám thu được trước đó mà không phải qua xử lý.

3.2.1. Trích từ ảnh binary [5]



(a) (b) (c)

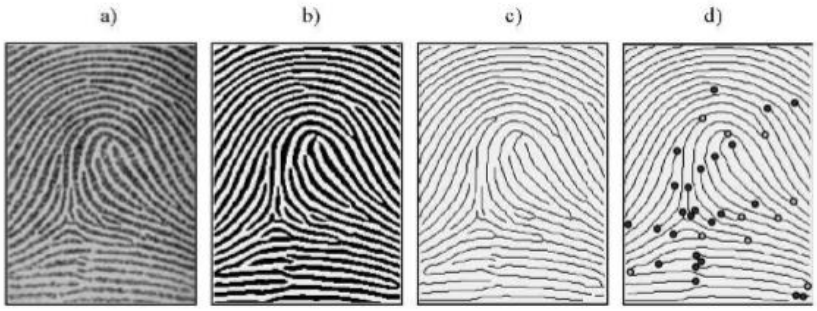


Fig. 2.6. a) A fingerprint gray-scale image; b) the image obtained after enhancement and binarization; c) the image obtained after thinning; d) termination and bifurcation minutiae detected through the pixel-wise computation of the crossing number.

Sử dụng các bộ lọc thích hợp để phát hiện và làm mảnh đường vân dưới dạng một pixel (ridge detection), biến đổi ảnh xám ban đầu thành ảnh binary có giá trị 0 hoặc 1 tương ứng. Sau đó các điểm minutiae sẽ được trích như sau: cho (x,y) là một điểm trên đường vân đã được làm mảnh và Ni(i=0:8) là 8 điểm quanh nó thì:

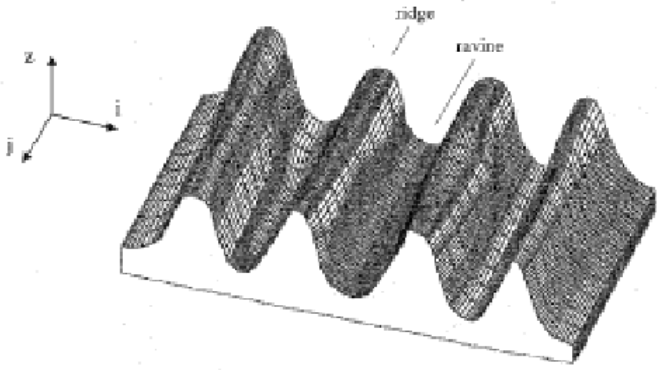
- (x,y) là một điểm kết thúc nếu $\sum_0^7 \boldsymbol{Ni} = \mathbf{1}$

- (x,y) là một điểm rẽ nhánh nếu $\sum_0^7 \boldsymbol{Ni} > \mathbf{2}$

3.2.2. Trích trực tiếp từ ảnh xám [2]

- Dò theo đường vân (Ridge line following)

Giả sử một ảnh xám có kích thước mXn, coi chiều thứ ba z là mức xám tại điểm (i,j) thì bề mặt của ảnh có dạng:



Đường vân là tập hợp các điểm dọc theo hướng xác định, việc xác định minutiae trực tiếp từ ảnh xám sẽ dựa trên thuật toán dò đường vân, thuật toán này xác định các điểm cực đại dọc theo hướng đi của đường vân.

- Xác định điểm cực đại

Giả sử **Ω((i$_t$,j$_t$), ϕ, σ))** là thiết diện của đường vân có điểm chính giữa là (i$_t$,j$_t$), hướng của thiết diện là **ϕ = φ$_t$ + π/2** (φ$_t$ là hướng của đường vân tại (i$_t$,j$_t$) và bề rộng của thiết diện m = 2σ + 1 pixel. Khi đó, Ω được xác định như sau:

Ω = {(i,j) | (i,j) ∈ I, (i,j) ∈ segment((i$_{start}$,j$_{start}$),(i$_{end}$,j$_{end}$))}

(i$_{start}$,j$_{start}$)= (round(it – σ.cosϕ), round(jt - σ.sinϕ))

(i$_{end}$,j$_{end}$) = (round(it + σ.cosϕ), round(jt + σ.sinϕ))

$$\text{round(x)} = \begin{cases} x + 0.5 \; if \; x \geq 0 \\ x + 0.5 \; otherwise \end{cases}$$

và điểm cực đại được xác định bằng cách so sánh mức xám giữa các điểm trong Ω

Nhiều học giả cho rằng phương pháp trích xuất minutiae từ ảnh nhị phân đã được chuyển đổi sẽ phần nào làm chúng ta mất mát dữ liệu, thông tin trên vân tay, cũng như phương pháp làm mảnh sẽ tạo ra một số lượng khá lớn minutiae, khi xử lý với ảnh có chất lượng thấp thì phương pháp chuẩn hóa thành ảnh nhị phân không cho kết quả thỏa đáng. Họ cũng cho rằng làm việc với ảnh xám ban đầu vẫn cho kết quả khả quan mà không cần xử lý ảnh trước.

4. LÀM NỔI ẢNH VÂN TAY [10]

Như đã đề cập, ảnh vân tay thu được từ phương pháp lăn mực cho ảnh kém chất lượng, vì vậy cần xử lý ảnh sao cho ảnh thể hiện được rõ và đầy đủ các điểm đặc trưng của vân tay để có thể rút trích đặc trưng trọn vẹn, mà không hề làm thay đổi nội dung ảnh.

Ảnh đã chuẩn hóa (phải) và ảnh gốc (trái)

Kết quả sau khi lọc bằng Gabor

5. ĐỐI SÁNH

Khó khăn lớn nhất của bước so sánh đó chính là phải so sánh với mẫu ảnh có chất lượng kém, chính điều đó sẽ gây rất nhiều khó khăn, gây nhiễu hay thậm chí làm sai lệch kết quả so sánh.

Đa số các phương pháp nhận dạng vân tay hiện nay đều dựa vào việc đối sánh vị trí các điểm đặc trưng trên hình ảnh vân tay, ta cũng có thể tham khảo thêm một số kĩ thuật như: **correlation-based , Minutiae-based , Ridge Feature-based.**

1. Correlation-based techniques

Đặt I (delta_x, delta_y, θ) đại diện cho một hình ảnh đầu vào I theo góc θ (thường là tâm hình ảnh), thay đổi lần lượt delta x và delta y theo hướng x và y. Từ đó sự giống nhau giữa I và T sẽ là:

$$S(T,I) = \max(delta\_x, delta\_y, \theta)*CC(T,I(delta\_x,delta\_y, \theta))$$

Trong đó $CC(T,I) = T^TI$ là mối tương quan chéo (cross-corelation) giữa T và I. Mối tương quan này được hiểu như là một thước đo độ giống nhau của hình ảnh.

2. Minutiae-based methods

Minutiae-based chính là kỹ thuật được áp dụng phổ biến nhất, việc so sánh dấu vân tay này dựa trên các tập kiểm tra. Minutiae được trích xuất từ hai dấu vân tay, và được lưu trữ lại thành một tập hợp các điểm trong không gian 2-Dimentional. Thuật toán sẽ quy định một bộ ba gồm m = {x, y, θ }, có nghĩa tọa độ của minutia tại vị trí (x,y) và với góc hợp bởi mặt phẳng ngang là θ. Hough transform-based là một kỹ thuật phổ biến nhất để so khớp minutiae, tìm hiểu thêm trong tài liệu tham khảo [1]

3. Ridge Feature-based techniques

Rút trích minutiae từ ảnh có chất lượng kém là một vấn đề khó chấp nhận; rất tốn thời gian là những lý do khiến chúng ta phải suy nghĩ và tìm thêm kỹ thuật mới hay cải tiến các thuật toán trước đó. Một nhóm tác giả đã đưa ra đề xuất về một ky thuật phân tích kết cấu cục bộ trong đó khu vực được quan tâm đó chính là điểm cốt lõi. Chi tiết về kỹ thuật này chúng ta sẽ hiểu rõ trong tài liệu tham khảo [1].

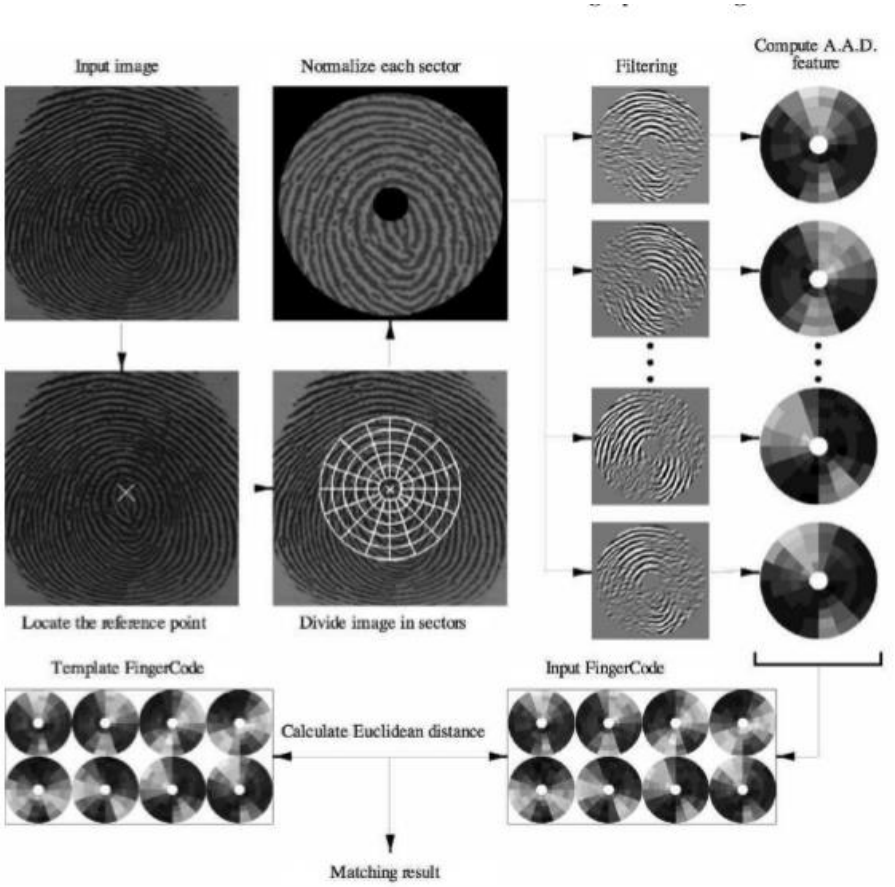
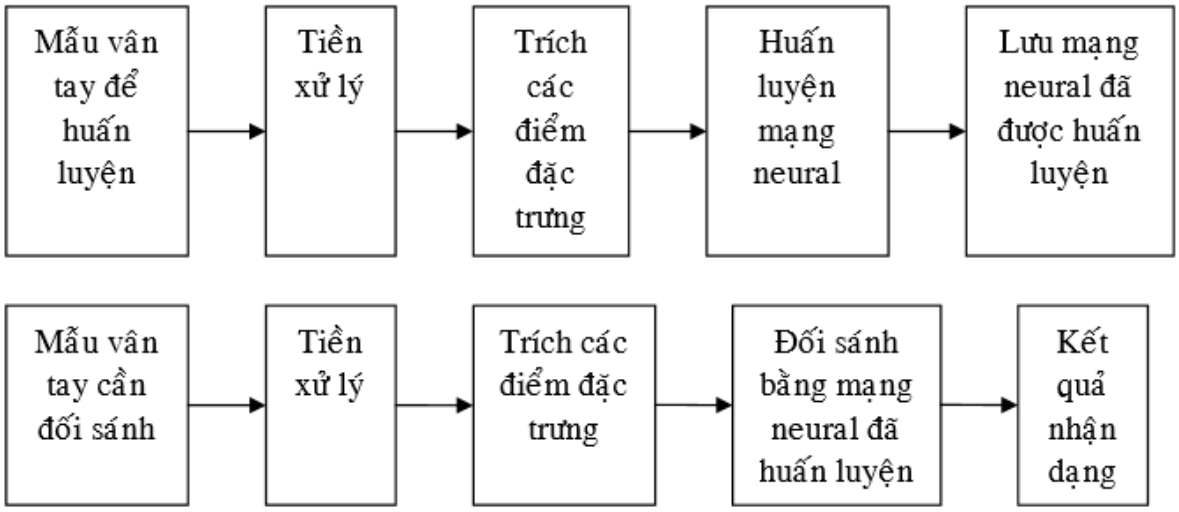


Fig. 2.9. System diagram of Jain et al.'s FingerCode approach [25].

6. SỬ DỤNG NEURAL NETWORKS TRONG NHẬN DẠNG VÂN TAY [6]

Ý tưởng của phương pháp này là huấn luyện mạng neural dựa vào các mẫu dữ liệu đầu vào là vị trí của các điểm đặc trưng trên ảnh vân tay. Sau khi huấn luyện, mạng neural được dùng để đối sánh các mẫu vân tay cần nhận dạng.

Dưới đây là lưu đồ thực hiện:



1. Lựa chọn mạng

Ở đây, sử dụng mạng truyền thẳng Perceptron một ngõ ra, mỗi mạng tương ứng với một mẫu. Khi cần đối sánh một mẫu ta phải so sánh mẫu đó qua tất cả các mạng trong cơ sở dữ liệu. Việc so sánh một mẫu qua các mạng đơn giản và tối ưu hóa được thời gian. Đối với hàm kích hoạt lớp ra là hàm tuyến tính và được huấn luyện về 0 đối với từng mẫu.

2. Xây dựng tập mẫu đầu vào

Đầu vào của mạng là vị trí của các điểm đặc trưng trên ảnh vân tay đã rút trích trước đó. Để xác định vị trí này ta phải có một điểm gốc tương đối cố định. Trong phương pháp này, điểm **core** được chọn làm gốc tọa độ, vì điểm này luôn tồn tại và cố định trong ảnh vân tay.

Vì phương pháp này dựa trên việc so sánh các vị trí, vì vậy không thể sai lệch dù chỉ một vị trí, điều đó sẽ làm cho toàn bộ mạng bị sai. Tuy nhiên sai lệch là không tránh khỏi trong quá trình xác định các điểm đặc trưng đối với ảnh có chất lượng kém. Để khắc phục nhược điểm này, thay vì đưa trực tiếp vị trí các điểm minutiae vào mạng mà sử dụng trung bình cộng các điểm minutiae lại:

- **Core** là gốc tọa độ, khi đó **core** sẽ chia mặt phẳng ảnh thành bốn phần.

- Mỗi một phần tư của mặt phẳng ảnh, ta tìm vị trí trung bình các điểm minutiae trong đó. Ta được bốn vị trí trung bình đối với 4 gốc phần tư, sau đó sử dụng Decart để đưa 4 vị trí này vào theo 8 đầu vào của mạng.

- Ta cũng có thể đưa thêm số điểm minutiae trong mỗi phần tư của mặt phẳng ảnh vào bốn đầu vào khác của mạng.

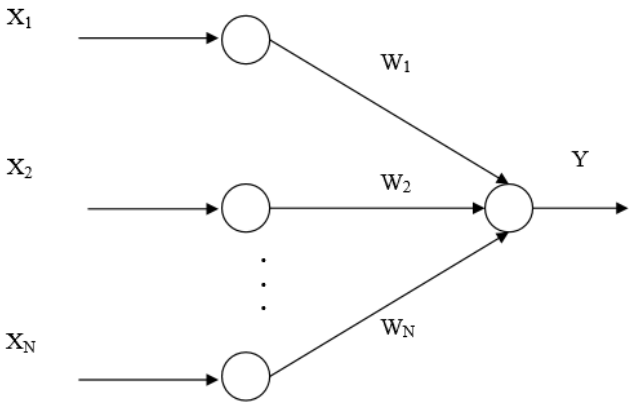
3. Số lớp

Số lớp sử dụng trong bài toán này sẽ là **một** và **hai**.

THUẬT TOÁN HUẤN LUYỆN:

Thuật toán huấn luyện được sử dụng là thuật toán lan truyền ngược suy giảm sai số gradient.

1. Mạng Perceptron một lớp



Trong đó, $X = [X_1, X_2 \dots X_N]^T$ là vector tín hiệu đầu vào, Y là tín hiệu ra, $W = [W_1, W_2 \dots W_H]^T$ là vector trọng số.

Thuật toán huấn luyện:

Bước 1:

Khởi động trị W(0)

Chọn hằng số học η

Bước 2: lan truyền thuận

Tính:

$Y(k) = net(k) = W^T X(k)$

Bước 3: lan truyền ngược

Tính:

$$W(k+1) = W(k) + \eta[D(k) - Y(k)]\frac{\partial a(net(k))}{\partial net(k)}$$ (a(.) là hàm kích hoạt)

Bước 4: lặp lại bước 3 K lần (một epoch), với K là số mẫu dữ liệu vào.

Bước 5: tính $J(K) = \frac{1}{2}[D(K) - Y(K)]^2$

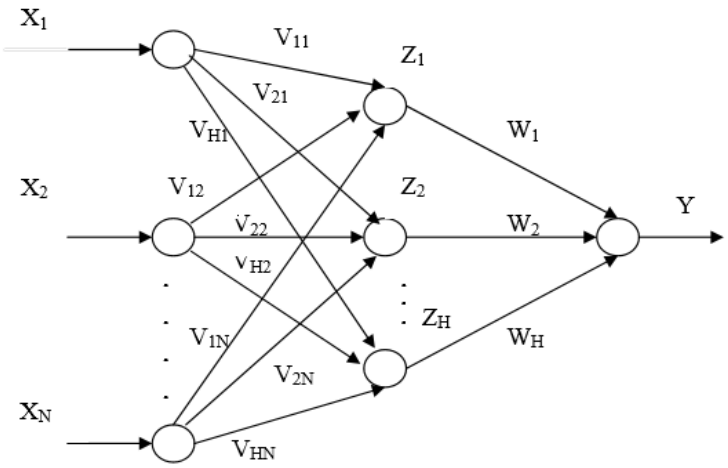
Bước 6: kiểm tra nếu J(K) đủ bé:

Đủ bé: kết thúc (lưu W)

Chưa: lặp lại bước 1 với các giá trị khởi động W(0) được cập nhật từ bước 4

2. Mạng Perceptron hai lớp

Bao gồm một lớp ẩn và một lớp ra được huấn luyện bằng giải thuật lan truyền ngược suy giảm sai số. Hàm kích hoạt lớp ẩn được chọn làm hàm sigmoid, hàm kích hoạt lớp ra là hàm tuyến tính.



Trong đó, $X = [X_1, X_2 \dots X_N]^T$ là vector tín hiệu đầu vào, Y là tín hiệu ra, $W = [W_1, W_2 \dots W_H]^T$ là vector trọng số lớp ra, $Vq = [V_{q1}\ V_{q2} \dots V_{qN}]^T$ là các vector trọng số lớp ẩn (q = 1:H), $Z = [Z_1\ Z_2 \dots Z_H]^T$ là vector tín hiệu ra lớp ẩn.

Thuật toán huấn luyện:

Bước 1:

Khởi động trị $W(0)$, $V_q(0)$

Chọn hằng số học η

Bước 2: lan truyền thuận

Tính:

$Z_q(k) = \text{sigmoid}(net_q) = \text{sigmoid}(V_q^T.X(k))$

$Y(k) = neto = W^T Z(k)$

Bước 3: lan truyền ngược

Tính:

$$\delta_O = D(k) - Y(k)$$

$$W(k+1) = W(k) + \eta.\delta_O.Z(k)$$

$$\delta_{hq} = \delta_O.W_q.\frac{e^{-netq}}{(1+e^{-netq})^2}$$

$$V_q(k+1) = V_q(k) + \eta.\delta_{hq}.X(k)$$

Bước 4: lặp lại bước 3 K lần (một epoch), với K là số mẫu dữ liệu vào.

Bước 5: tính $J(K) = \frac{1}{2}[D(K) - Y(K)]^2$

Bước 6: kiểm tra nếu J(K) đủ bé:

Đủ bé: kết thúc (lưu W, V_q)

Chưa: lặp lại bước 1 với các giá trị khởi động $W(0)$, $V_q(0)$ được cập nhật từ bước 4

7. PERFORMANCE EVALUATION

Dù độ chính xác của phương pháp nhận dạng dựa trên dấu vân tay rất cao, tuy nhiên không phương pháp nhận dạng nào hoàn hảo. Để biết được mức độ hoàn hảo của phương pháp

nhận dạng, performance evaluation là bước làm không thể thiếu trong tất cả các bài toán nhận dạng. Chương trình đánh giá hiệu suất từng được biết tới rộng rãi đó là Fingerprint Technology Evaluation (FpVTE), cùng các sáng kiến hiện thời như NIST SDK Testing và MINEX. Fingerprint Verification Competition (FVC2000) lần đầu tiên được tổ chức bởi the Biometric System Laboratory of the University of Bologna, cùng với Biometric Test Center of the San Jose State University và the Pattern Recognition and Image Processing Laboratory of the Michigan State University. Mục đích của việc tổ chức những cuộc thi như thế này là để tìm kiếm, cũng như thúc đẩy các sáng kiến mới mẻ từ nhiều cá nhân, tổ chức, từ đó thiết lặp một chuẩn mực chung để so sánh các thuật toán phù hợp với dấu vân tay.

	FVC2004	FpVTE2003
Algorithms Evaluated	*Open Category*: 41 *Light Category*: 26	*Large Scale Test (LST)*: 13 *Medium Scale Test (MST)*: 18 *Small Scale Test (SST)*: 3 (SST only)
Subject population	Students (24 years old on the average)	Operational fingerprint data from a variety of U.S. Government sources including low-quality fingers and low-quality sources
Fingerprint format	Single finger flat impressions acquired through low-cost commercial fingerprint scanners (including small area and sweeping sensors)	Mixed formats (flat, slap, and rolled from different sources; scanned paper cards, and from FBI-compliant fingerprint scanners)
Perturbations	Deliberately exaggerated perturbations (rotation, distortion, dry/wet fingers, ...)	Difficulties mainly due to intrinsic low-quality fingers of some subjects and sometimes due to non-cooperative users
Database availability	Databases are available to the scientific community	Databases are not available due to data protection and privacy issues
Data collection	All the data were acquired for this event	Data coming from existing U.S. Government sources
Database size	4 databases, each containing 800 fingerprints from 100 fingers	48,105 fingerprint sets from 25,309 subjects
Evaluation type	Independent Strongly supervised	Independent Supervised
Anonymous participation	Allowed	Not allowed
Best EER	Best average EER: 2.07% (in the Open Category)	Best EER on MST: 0.2% (MST is the FpVTE2003 test closest to FVC2004 Open Category)

So sánh giữa FVC2004 và FpVTE2003

Việc đánh giá hiệu suất hoạt động của hệ thống nhận dạng phụ thuộc khá nhiều vào dữ liệu. Thông thương để có được tỉ lệ lỗi thấp cũng như thời gian chính xác thì hệ thống cần có một cơ sở dữ liệu lớn về hình ảnh. Một khi cơ sở dữ liệu đã từng được sử dụng để kiểm tra và tối ưu hóa hệ thống thì trong những lần kiểm tra tiếp theo, hệ thống yêu cầu một bộ cơ sở dữ liệu hoàn toàn mới mà chưa từng được thêm vào trước đây. Để có được những cơ sở dữ liệu lớn không chỉ tốn kém về thời gian, tiền bạc, mà còn có nhiều vấn đề phát sinh khác, dễ chán nản, công việc lặp đi lặp lại, lỗi thu thập, luật bảo mật sử dụng dữ liệu cá nhân. Vì vậy mà hệ thống tổng hợp hình ảnh thực tế ra đời giúp giải quyết những khó khăn trên. Thuộc tính mong muốn nhất của một công cụ tạo ra dấu vân tay tổng hợp là mô hình chính xác các biến thể giữa các lớp và giữa các lớp khác nhau trong hình ảnh dấu quan tay quan sát được trong tự nhiên. Nó tạo ra một dấu vân

tay ảo chân thực bằng cách mô phỏng: những ngón tay khác nhau chạm vào cảm biến, biến đổi phi tuyến được tạo ra bởi áp lực không trực giao của ngón tay trên cảm biến, sự thay đổi độ dày của đường vân do áp suất hoặc độ ẩm của da hay những vết cắt nhỏ trên đầu ngón tay và những loại nhiễu khác.

8. KẾT LUẬN

Nhận dạng vân tay tự động là một trong những ứng dụng đầu tiên của nhận dạng mẫu máy, tuy vậy đây vẫn là bài toán tìm nghiệm gần đúng, vẫn chưa có một nghiệm chính xác hoàn hảo cho bài toán này. Không chỉ vậy nó còn là bài toán nhận dạng mẫu phức tạp và rất nhiều thách thức. Đặc biệt là trong việc cải thiện thuật toán rút trích đặc trưng, và đối sánh. Việc tối ưu thuật toán rút trích sao cho mạnh mẽ, rút trích chính xác thành phần đặc trưng, không có lỗi và lấy được đầy đủ thông tin là điều gần như không thể, nhất là khi mà hình ảnh thu được có chất lượng không đảm bảo. Mặc dù có cả thuật toán tăng cường chất lượng ảnh, tuy nhiên càng có nhiều bước thực hiền thì càng có nhiều sai số, mỗi phương pháp có sai số riêng của nó thì sau các phương pháp đó kết quả nhận dạng sẽ càng bị sai lệch. Không thể phủ nhận rằng các phương pháp tiên tiến nhất hiện nay đã dần trở nên rất hiệu quả, ở cả tốc độ nhận dạng rất cao. Trong tương lai, cần nhiều hơn những nghiên cứu mới về phát triển kĩ thuật rút trích đặc trưng tiếp cận các công nghệ, cũng như tiếp cận nguồn thông tin, dữ liệu dồi dào hơn, và đào tạo những thuật toán này có thể giải quyết vấn đề như một chuyên gia.

Và cũng như các hệ thống nhận dạng khác, hệ thống nhận dạng vân tay không tránh khỏi việc bị làm giả. Có rất nhiều con đường tấn công nhắm vào hệ thống này như: tấn công các kênh liên lạc, tấn công module phần mềm (thay thế, trích xuất, hay sao chép các so khớp), tấn công cơ sở dữ liệu vân tay đã đăng ký, …

Chính vì vậy, ngoài việc nâng cao hiệu quả hệ thống nhận dạng vân tay, chúng ta cần đặc biệt quan tâm đến vấn đề bảo mật cơ sở dữ liệu, cũng như bảo mật hệ thống một cách an toàn hơn.

9. REFERENCES

[1]. James L. Wayman, Anil K. Jain, Patrick Flynn and Arun A. Ross, “Handbook of Biometrics”, 2007

[2] Dario Maio and Davide Maltoni,”Direct Gray-Scale Minutiae Detection In Fingerprints”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 1, January 1997.

[3] D.Maltoni, D.Maio, A.K.Jain, S.Prabhakar, ”Singularity and Core Detection” Extract from “Handbook of Fingerprint Recognition”, Springer, New York, 2003.

[4] D.Maltoni, D.Maio, A.K.Jain, S.Prabhakar, ”Minutiae-based Methods” Extract from “Handbook of Fingerprint Recognition”, Springer, New York, 2003. .

[5]. Nguyễn Hoàng Huy, “Luận văn thạc sĩ – Nhận dạng vân tay”, 07/2007

[6]. Pavol Marák and Alexander Hambalík, “Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation”, 2006

[7] Pierre Baldi, Yves Chauvin and Richard Lippman, “Neural Networks for Fingerprint Recognition”, 1993

[8] Karthik Nandakumar, Anil K. Jain, “Local Correlation-based Fingerprint Matching”, To Appear in Proceedings of ICVGIP, Kolkata, December 2004.

[9] Anil Jain, Sharathcha Pankanti, “Fingerprint Classification and Matching”.

[10] Anil Jain, Lin Hong, Yifei Wan, ”Fingerprint Image Enhancement: Algorithm and Performance Evaluation ”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, 1998.

HẾT