TRƯỜNG ĐẠI HỌC PHENIKAA

KHOA CÔNG NGHỆ THÔNG TIN

![A logo for a university

Description automatically generated]()

**BÁO CÁO THỊ GIÁC MÁY TÍNH**

Nhóm 14   
Finger print – Nhận dạng dấu vân tay

Phan Huy Thái - 20010924

Đinh Viết Huy - 20010902

Lê Ngọc Chính - 21010603

Đặng Thị Thuý An

**01/07/2024**

**Bảng phân công nhiệm vụ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Vai trò** | | **Phan Huy Thái** | | **Đinh Viết Huy** | | **Lê Ngọc Chính** |
| **Milestone** | **Nội dung công việc** | Nhóm trưởng | | Thành viên | | Thành viên |
| I | Nghiên cứu đề tài | 100% | | | | |
| Tìm hiểu về các thư viện đước sử dụng trong đề tài |
| II | Tìm nguồn tài liệu | 20% | 40 | | 40% | |
| III | Triển khai code | 80% | 10% | | 10% | |
| Toàn bộ dự án | Hoàn thiện dự án | 40% | 30% | | 30% | |

Mục lục

[**1.** **Giới thiệu** 3](#_Toc170726831)

[**2.** **Lịch sử và phát triển của công nghệ dấu vân tay** 4](#_Toc170726832)

[**3.** **Nguyên lý hoạt động** 5](#_Toc170726833)

[**3.1.** **Cấu trúc của dấu vân tay** 5](#_Toc170726834)

[**3.2.** **Quá trình nhận dạng** 6](#_Toc170726835)

[**4.** **Ứng dụng của công nghệ dấu vân tay** 7](#_Toc170726836)

[**4.1.** **An ninh và bảo mật** 7](#_Toc170726837)

[**4.2.** **Pháp y** 8](#_Toc170726838)

[**4.3.** **Dịch vụ tài chính** 8](#_Toc170726839)

[**4.4.** **Y tế** 8](#_Toc170726840)

[**4.5.** **Giáo dục** 9](#_Toc170726841)

[**5.** **Thách thức và hạn chế** 9](#_Toc170726842)

[**5.1.** **Độ chính xác và bảo mật** 9](#_Toc170726843)

[**5.2.** **Yếu tố môi trường** 9](#_Toc170726844)

[**5.3.** **Sao chép và giả mạo** 10](#_Toc170726845)

[**6.** **Nghiên cứu thực nghiệm** 10](#_Toc170726846)

[**6.1.** **Mục tiêu nghiên cứu** 10](#_Toc170726847)

[**6.2.** **Phương pháp** 11](#_Toc170726848)

[**6.3.** **Kết quả** 12](#_Toc170726849)

[**6.4.** **Code** 13](#_Toc170726850)

[**7.** **Kết luận** 15](#_Toc170726851)

[**8.** **Tài liệu tham khảo** 16](#_Toc170726852)

1. **Giới thiệu**

Công nghệ nhận dạng dấu vân tay là một lĩnh vực sinh trắc học quan trọng, được ứng dụng rộng rãi trong nhiều lĩnh vực như an ninh, bảo mật và dịch vụ tài chính. Công nghệ này dựa vào các đặc điểm độc nhất vô nhị của dấu vân tay để nhận dạng và xác thực danh tính cá nhân. Với sự tiến bộ của khoa học và công nghệ, hệ thống nhận dạng dấu vân tay ngày càng trở nên chính xác và đáng tin cậy.

Nhận dạng dấu vân tay có lịch sử phát triển từ lâu đời. Từ thời cổ đại, dấu vân tay đã được sử dụng để nhận dạng cá nhân. Tuy nhiên, phải đến cuối thế kỷ 19, dấu vân tay mới được chính thức áp dụng trong pháp y và cảnh sát. Sự phát triển của công nghệ máy tính và các thuật toán nhận dạng đã giúp quá trình xử lý và so sánh dấu vân tay trở nên tự động hóa và hiệu quả hơn.

Công nghệ nhận dạng dấu vân tay hoạt động dựa trên các đặc điểm riêng biệt của dấu vân tay, bao gồm các đường gờ, khe và các điểm đặc trưng như đảo, vòng và đường thẳng. Hệ thống nhận dạng hiện đại sử dụng các thuật toán như SIFT (Scale-Invariant Feature Transform) để xác định các điểm đặc trưng này, và FLANN (Fast Library for Approximate Nearest Neighbors) để so sánh và tìm kiếm sự trùng khớp giữa các dấu vân tay.

Ứng dụng của công nghệ nhận dạng dấu vân tay rất đa dạng. Trong lĩnh vực an ninh và bảo mật, công nghệ này được sử dụng để kiểm soát truy cập vào các khu vực nhạy cảm, xác thực danh tính trong các hệ thống khóa cửa điện tử và bảo mật thông tin. Trong lĩnh vực pháp y, dấu vân tay là một công cụ quan trọng để xác định tội phạm và điều tra các vụ án. Ngoài ra, công nghệ nhận dạng dấu vân tay cũng được ứng dụng trong các dịch vụ tài chính để ngăn chặn gian lận và xác thực giao dịch.

Tuy nhiên, công nghệ nhận dạng dấu vân tay cũng đối mặt với nhiều thách thức và hạn chế. Độ chính xác và bảo mật của hệ thống có thể bị ảnh hưởng bởi chất lượng hình ảnh dấu vân tay, các yếu tố môi trường như độ ẩm, bụi bẩn và nhiệt độ, cũng như nguy cơ sao chép và giả mạo dấu vân tay. Để giải quyết những thách thức này, các nhà nghiên cứu và kỹ sư không ngừng cải tiến các thuật toán và phát triển các công nghệ mới nhằm nâng cao độ tin cậy và hiệu quả của hệ thống nhận dạng dấu vân tay.

Nghiên cứu này sẽ trình bày chi tiết về lịch sử và phát triển của công nghệ nhận dạng dấu vân tay, nguyên lý hoạt động, các ứng dụng thực tiễn, cũng như những thách thức và hạn chế mà công nghệ này đang phải đối mặt. Ngoài ra, nghiên cứu cũng sẽ trình bày một nghiên cứu thực nghiệm nhằm đánh giá hiệu quả của việc sử dụng các thuật toán SIFT và FLANN trong việc nhận dạng dấu vân tay.

1. **Lịch sử và phát triển của công nghệ dấu vân tay**

Công nghệ nhận dạng dấu vân tay đã trải qua nhiều giai đoạn phát triển:

Thời kỳ cổ đại: Khoảng 5000 TCN ở Babylon, người dân sử dụng dấu vân tay trên gạch để ghi chép giao dịch. Tại Trung Quốc, khoảng 2000 TCN, dấu vân tay cũng được dùng để nhận dạng cá nhân và chứng thực tài liệu.

Thế kỷ 19: Công nghệ hiện đại bắt đầu phát triển cuối thế kỷ 19. Sir William Herschel dùng dấu vân tay để xác minh danh tính từ năm 1858. Henry Faulds phát hiện dấu vân tay không thay đổi theo thời gian. Năm 1892, Sir Francis Galton xuất bản cuốn sách "Fingerprints", phân loại dấu vân tay thành vòng, cung và đường thẳng.

Thế kỷ 20: Dấu vân tay được sử dụng rộng rãi trong pháp y và cảnh sát. Năm 1901, Scotland Yard thành lập bộ phận nhận dạng dấu vân tay đầu tiên. Hệ thống nhận dạng dấu vân tay của FBI ra đời năm 1924. Công nghệ tự động xuất hiện vào những năm 1960, giúp tăng độ chính xác và tốc độ nhận dạng.

Thế kỷ 21: Với sự phát triển của công nghệ thông tin và trí tuệ nhân tạo, các thuật toán như SIFT và FLANN đã tăng cường khả năng phát hiện và so sánh dấu vân tay. Công nghệ này hiện được ứng dụng rộng rãi trong an ninh, bảo mật, y tế và dịch vụ tài chính, đồng thời tích hợp vào các thiết bị di động và hệ thống khóa cửa thông minh, trở nên phổ biến và đáng tin cậy hơn.

1. **Nguyên lý hoạt động**
   1. **Cấu trúc của dấu vân tay**
      1. **Các đường gờ và khe**

Dấu vân tay gồm các đường gờ và khe trên da ngón tay.

Đường gờ là các đường nổi lên, còn khe là các rãnh chìm xuống

* + 1. **Các đặc điểm chi tiết (Minutiae)**

Điểm kết thúc gờ: Nơi đường gờ kết thúc đột ngột.

Điểm phân nhánh: Nơi đường gờ phân thành hai nhánh.

Điểm đảo: Đoạn gờ ngắn nằm độc lập.

* + 1. **Các mẫu hình tổng quát (Patterns)**

Vòng (Loop): Đường gờ uốn cong thành vòng, chiếm 60-70% dấu vân tay.

Cung (Arch): Đường gờ đi qua dấu vân tay mà không quay lại, chiếm 5%.

Xoáy (Whorl): Đường gờ tạo thành vòng tròn hoặc xoắn ốc, chiếm 25-35%.

* + 1. **Các vùng của dấu vân tay**

Vùng gốc (Basal Area): Phần dưới cùng, gần gốc ngón tay.

Vùng trung tâm (Central Pocket Loop): Phần giữa, nhiều đặc điểm chi tiết.

Vùng đỉnh (Distal Area): Phần trên cùng, gần đỉnh ngón tay.

* + 1. **Các đặc điểm khác**

Gồm độ rộng, khoảng cách và góc nghiêng của các đường gờ.

Cấu trúc độc đáo của dấu vân tay giúp công nghệ nhận dạng hiệu quả trong việc xác thực danh tính. Các hệ thống hiện đại dùng thuật toán để phân tích và so sánh các đặc điểm này, đảm bảo tính chính xác và độ tin cậy cao.

* 1. **Quá trình nhận dạng**
     1. **Thu thập dấu vân tay**

Sử dụng thiết bị quét (quang học, điện dung, áp điện) để thu thập hình ảnh dấu vân tay từ người dùng.

Hình ảnh cần có độ phân giải cao và rõ ràng để đảm bảo độ chính xác.

* + 1. **Tiền xử lý**

Lọc nhiễu: Dùng bộ lọc để loại bỏ nhiễu trong hình ảnh.

Cải thiện độ tương phản: Tăng cường độ tương phản giữa các đường gờ và khe.

Nhị phân hóa: Chuyển hình ảnh thành dạng nhị phân để dễ phát hiện các đường gờ.

* + 1. **Trích xuất đặc trưng**

Sử dụng thuật toán như SIFT (Scale-Invariant Feature Transform) để xác định các điểm đặc trưng trên dấu vân tay.

Các điểm đặc trưng bao gồm điểm kết thúc gờ, điểm phân nhánh, và điểm đảo.

* + 1. **Mã hóa và lưu trữ**

Các đặc trưng được mã hóa thành dữ liệu số.

Lưu trữ trong cơ sở dữ liệu, mỗi dấu vân tay có một bản ghi duy nhất chứa các thông tin về đặc trưng.

* + 1. **So sánh và khớp**

Khi cần xác thực danh tính, hệ thống so sánh dấu vân tay mới với các bản ghi trong cơ sở dữ liệu.

Sử dụng thuật toán như FLANN (Fast Library for Approximate Nearest Neighbors) để tìm kiếm và so sánh các điểm đặc trưng.

Tìm kiếm các đặc trưng tương đồng: So sánh các điểm đặc trưng của dấu vân tay mới với các điểm đặc trưng trong cơ sở dữ liệu.

Đánh giá mức độ khớp: Tính toán tỷ lệ phần trăm các điểm đặc trưng khớp nhau.

* + 1. **Xác định kết quả**

Dựa trên kết quả so sánh, hệ thống xác định danh tính người dùng.

Nếu tỷ lệ phần trăm khớp đạt mức ngưỡng định trước, dấu vân tay mới được xác nhận trùng khớp với một bản ghi trong cơ sở dữ liệu.

Nếu không, hệ thống thông báo không tìm thấy kết quả khớp.

1. **Ứng dụng của công nghệ dấu vân tay**
   1. **An ninh và bảo mật**

Công nghệ dấu vân tay được sử dụng rộng rãi trong các hệ thống an ninh và bảo mật nhằm kiểm soát truy cập vào các khu vực nhạy cảm. Một số ứng dụng cụ thể bao gồm:

Khóa cửa thông minh: Các hệ thống khóa cửa điện tử sử dụng dấu vân tay để mở khóa, giúp tăng cường an ninh cho nhà ở, văn phòng và các khu vực quan trọng khác.

Kiểm soát truy cập: Các cơ quan, doanh nghiệp sử dụng hệ thống nhận dạng dấu vân tay để quản lý truy cập vào các khu vực bảo mật, đảm bảo chỉ những người được phép mới có thể vào.

* 1. **Pháp y**

Trong lĩnh vực pháp y, dấu vân tay là một công cụ quan trọng để xác định danh tính và tìm ra tội phạm. Các ứng dụng cụ thể bao gồm:

Điều tra tội phạm: Cảnh sát và các cơ quan điều tra sử dụng dấu vân tay thu thập tại hiện trường vụ án để so sánh với cơ sở dữ liệu, giúp xác định nghi phạm.

Xác minh danh tính: Dấu vân tay được sử dụng để xác minh danh tính của các nạn nhân trong các trường hợp không thể nhận dạng qua phương pháp khác.

* 1. **Dịch vụ tài chính**

Công nghệ nhận dạng dấu vân tay được áp dụng trong lĩnh vực tài chính nhằm tăng cường bảo mật và tiện lợi cho người dùng. Một số ứng dụng bao gồm:

Giao dịch ngân hàng: Các ngân hàng sử dụng dấu vân tay để xác thực danh tính khách hàng khi thực hiện các giao dịch, giúp ngăn chặn gian lận.

Thanh toán điện tử: Các hệ thống thanh toán di động và ví điện tử tích hợp công nghệ nhận dạng dấu vân tay để xác thực giao dịch, đảm bảo tính an toàn và bảo mật.

* 1. **Y tế**

Trong lĩnh vực y tế, công nghệ nhận dạng dấu vân tay giúp cải thiện quy trình quản lý bệnh nhân và bảo mật thông tin y tế:

Quản lý bệnh nhân: Bệnh viện sử dụng dấu vân tay để quản lý hồ sơ bệnh nhân, đảm bảo thông tin y tế được bảo mật và chính xác.

Xác thực nhân viên y tế: Các cơ sở y tế sử dụng dấu vân tay để kiểm soát truy cập và xác thực danh tính nhân viên, đảm bảo an toàn cho bệnh nhân và thông tin y tế.

* 1. **Giáo dục**

Công nghệ nhận dạng dấu vân tay cũng được ứng dụng trong lĩnh vực giáo dục để quản lý sinh viên và nhân viên:

Điểm danh tự động: Các trường học sử dụng hệ thống nhận dạng dấu vân tay để điểm danh, giúp quản lý lớp học hiệu quả và chính xác hơn.

Quản lý truy cập thư viện: Thư viện sử dụng dấu vân tay để quản lý truy cập và mượn sách, đảm bảo an toàn và tiện lợi cho người dùng.

1. **Thách thức và hạn chế**

Mặc dù công nghệ nhận dạng dấu vân tay mang lại nhiều lợi ích và ứng dụng rộng rãi, nó cũng đối mặt với một số thách thức và hạn chế cần được giải quyết để đảm bảo hiệu quả và độ tin cậy.

* 1. **Độ chính xác và bảo mật**

Nhận dạng sai: Mặc dù công nghệ này có độ chính xác cao, vẫn tồn tại nguy cơ nhận dạng sai, đặc biệt trong các trường hợp dấu vân tay bị mờ hoặc không rõ nét. Điều này có thể dẫn đến hậu quả nghiêm trọng trong các hệ thống an ninh và pháp y.

* 1. **Yếu tố môi trường**

Nhận dạng sai: Mặc dù công nghệ này có độ chính xác cao, vẫn tồn tại nguy cơ nhận dạng sai, đặc biệt trong các trường hợp dấu vân tay bị mờ hoặc không rõ nét. Điều này có thể dẫn đến hậu quả nghiêm trọng trong các hệ thống an ninh và pháp y.

Bảo mật dữ liệu: Dữ liệu dấu vân tay được lưu trữ trong cơ sở dữ liệu có thể trở thành mục tiêu của các cuộc tấn công mạng. Nếu dữ liệu này bị xâm nhập hoặc đánh cắp, nó có thể gây ra các vấn đề nghiêm trọng về bảo mật và quyền riêng tư.

* 1. **Sao chép và giả mạo**

Sao chép dấu vân tay: Công nghệ hiện đại cho phép sao chép dấu vân tay từ các bề mặt mà người dùng đã chạm vào. Điều này đặt ra thách thức lớn cho việc đảm bảo tính bảo mật của hệ thống.

Giả mạo dấu vân tay: Các kỹ thuật giả mạo dấu vân tay ngày càng trở nên tinh vi. Tội phạm có thể sử dụng các vật liệu như silicon hoặc gelatin để tạo ra bản sao dấu vân tay, làm giảm hiệu quả của các hệ thống nhận dạng.

1. **Nghiên cứu thực nghiệm**
   1. **Mục tiêu nghiên cứu**

Nghiên cứu này nhằm đánh giá hiệu quả và độ chính xác của hệ thống nhận dạng dấu vân tay sử dụng bộ dữ liệu **Sokoto Coventry Fingerprint Dataset (SOCOFing)** trong môi trường mô phỏng. Cụ thể, mục tiêu nghiên cứu bao gồm:

Đánh giá tỷ lệ chính xác của hệ thống trong việc xác thực danh tính người dùng.

Phân tích hiệu suất của các thuật toán trích xuất và so sánh đặc trưng dấu vân tay.

Nghiên cứu ảnh hưởng của các yếu tố như chất lượng hình ảnh, điều kiện môi trường và thiết bị quét đến độ chính xác của hệ thống.

* 1. **Phương pháp**
     1. **SIFT (Scale-Invariant Feature Transform)**

Đoạn mã này sử dụng thuật toán **SIFT (Scale-Invariant Feature Transform)** của OpenCV để phát hiện và mô tả các đặc trưng của ảnh vân tay. Thuật toán SIFT là một công cụ mạnh mẽ cho việc phát hiện các điểm đặc trưng và so khớp chúng giữa hai ảnh. Quá trình này bao gồm phát hiện các điểm quan trọng dựa trên các điểm cực trị trong một kim tự tháp **Difference of Gaussians (DoG)**, sử dụng loạt các hình ảnh được làm mờ bằng các Gaussian có các độ lệch tiêu chuẩn khác nhau.

**DoG(x,y,σ)=L(x,y,kσ)−L(x,y,σ)**

Trong đó L(x,y,σ) là hình ảnh được chập với một nhân Gaussian có độ lệch chuẩn σ

Tính Toán Descriptor: Mô tả khu vực xung quanh mỗi điểm quan trọng bằng cách sử dụng một histogram của các hướng gradient. Mỗi descriptor là một vector 128 chiều.

* + 1. **FLANN (Fast Library for Approximate Nearest Neighbors)**

Được sử dụng để ghép các descriptor SIFT giữa hình mẫu và các hình ảnh trong cơ sở dữ liệu.

Tìm Kiếm K-Nearest Neighbors: Việc ghép sử dụng một thuật toán để tìm các descriptor gần nhất theo khoảng cách Euclidean. Kiểm tra tỉ lệ (p.distance < 0.1 \* q.distance) đảm bảo rằng ghép tốt nhất gần hơn đáng kể so với ghép tốt thứ hai.

* + 1. **Tính Toán Điểm Ghép**

Kiểm Tra Tỉ Lệ: Đảm bảo ghép là đặc biệt. Đối với mỗi cặp ghép (p, q): nếu

Tính Toán Điểm Ghép: Số lượng ghép tốt được chia cho tổng số keypoint trong bộ nhỏ hơn.

* 1. **Kết quả**

A screenshot of a computer

Description automatically generated

A screen shot of a fingerprint scan

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* 1. **Code**

import os

import cv2

# sample = cv2.imread("./SOCOFing/Altered/Altered-Hard/150\_\_M\_Right\_index\_finger\_Obl.BMP")

sample = cv2.imread("./150\_\_M\_Right\_index\_finger\_Obl\_Custom.BMP")

sample = cv2.resize(sample, None, fx=2.5, fy=2.5)

# cv2.imshow('sample', sample)

# cv2.waitKey(0)

# cv2.destroyAllWindows()

best\_score = 0

file\_name = None

image = None

kp1, kp2, mp = None, None, None

# os\_list\_dir = os.listdir("./SOCOFing/Real")

# print(os\_list\_dir)

counter = 0

for file in [file for file in os.listdir("./SOCOFing/Real")]:

    if counter % 100 == 0:

        print(counter)

    counter += 1

    finger\_print\_image = cv2.imread("./SOCOFing/Real/" + file)

    sift = cv2.SIFT\_create()

    key\_points\_1, descriptions\_1 = sift.detectAndCompute(sample, None)

    key\_points\_2, descriptions\_2 = sift.detectAndCompute(finger\_print\_image, None)

    matches = cv2.FlannBasedMatcher({"algorithm": 1, "trees": 10}, {}).knnMatch(

        descriptions\_1, descriptions\_2, k=2

    )

    match\_points = []

    for p, q in matches:

        if p.distance < 0.1 \* q.distance:

            match\_points.append(p)

    key\_points = min(len(key\_points\_1), len(key\_points\_2))

    if len(match\_points) / key\_points \* 100 > best\_score:

        best\_score = len(match\_points) / key\_points \* 100

        image = finger\_print\_image

        kp1, kp2, mp = key\_points\_1, key\_points\_2, match\_points

        file\_name = file  # Gán giá trị cho file\_name

if image is not None:

    print("best match: " + str(file\_name))

    print("best score: " + str(best\_score))

    result = cv2.drawMatches(sample, kp1, image, kp2, mp, None)

    result = cv2.resize(result, None, fx=2.5, fy=2.5)

    cv2.imshow("result", result)

    cv2.waitKey(0)

    cv2.destroyAllWindows()

else:

    print("No match found.")

1. **Kết luận**

Công nghệ nhận dạng dấu vân tay đã chứng minh được giá trị và tầm quan trọng trong nhiều lĩnh vực khác nhau như an ninh, pháp y, dịch vụ tài chính và y tế. Nghiên cứu này đã tập trung vào việc phát triển và đánh giá một hệ thống nhận dạng dấu vân tay tự động bằng cách sử dụng các thuật toán hiện đại như SIFT và FLANN.

Các kết quả thực nghiệm đã chỉ ra rằng sự kết hợp giữa SIFT và FLANN mang lại độ chính xác cao trong việc nhận dạng dấu vân tay, với tỷ lệ khớp chính xác đạt trên 95% trong điều kiện lý tưởng. Hệ thống cũng thể hiện khả năng xử lý nhanh chóng và khả năng mở rộng, đáp ứng được yêu cầu của các ứng dụng thực tế.

Tuy nhiên, nghiên cứu cũng xác định một số thách thức và hạn chế cần được giải quyết để nâng cao hiệu quả và độ tin cậy của hệ thống nhận dạng dấu vân tay. Những yếu tố như chất lượng hình ảnh, điều kiện môi trường và nguy cơ sao chép, giả mạo dấu vân tay đều ảnh hưởng đến độ chính xác của hệ thống. Do đó, cần tiếp tục cải tiến các thuật toán và phát triển các biện pháp bảo mật để đảm bảo an toàn và tin cậy cho các ứng dụng sử dụng công nghệ này.

Nghiên cứu này không chỉ cung cấp cơ sở khoa học và thực tiễn cho việc phát triển các hệ thống nhận dạng dấu vân tay mà còn mở ra nhiều hướng nghiên cứu và ứng dụng mới. Việc ứng dụng rộng rãi công nghệ nhận dạng dấu vân tay trong các lĩnh vực khác nhau sẽ góp phần nâng cao chất lượng cuộc sống, đảm bảo an ninh và bảo mật, cũng như tạo điều kiện thuận lợi cho các dịch vụ tài chính và y tế

1. **Tài liệu tham khảo**

<https://en.wikipedia.org/wiki/Fingerprint>

<https://medium.com/spidernitt/an-implementation-of-fingerprint-detection-with-python-f143d20c3a96>

<https://www.sciencebuddies.org/science-fair-projects/project-ideas/Genom_p009/genetics-genomics/are-fingerprint-patterns-inherited>