Phạm Văn Hào – Nguyễn Thành Chính – Nguyễn Văn Cường TÊN ĐỀ TÀI : XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME 2022

ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT
KHOA ĐIỆN – ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP
ĐẠI HỌC

NGÀNH: ĐIỆN-ĐIỆN TỬ

CHUYÊN NGÀNH: KỸ THUẬT ĐIỆN TỬ

ĐỀ TÀI:

XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME

Người hướng dẫn: **ThS. Lê Hữu Duy**
Sinh viên thực hiện: **Phạm Văn Hào**
Nguyễn Thành Chính
Nguyễn Văn Cường
Mã sinh viên: **1711505110110**
1711505110105
1711505210105
Lớp**: 17KTDT1**

Đà Nẵng, …../20.

ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT
KHOA ĐIỆN – ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP
ĐẠI HỌC

NGÀNH: ĐIỆN-ĐIỆN TỬ

CHUYÊN NGÀNH: KỸ THUẬT ĐIỆN TỬ

ĐỀ TÀI:

XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME

Người hướng dẫn: **ThS. Lê Hữu Duy**
Sinh viên thực hiện: **Phạm Văn Hào**
Nguyễn Thành Chính
Nguyễn Văn Cường
Mã sinh viên: **1711505110110**
1711505110105
1711505210105
Lớp**: 17KTDT1**

Đà Nẵng, …../20….

NHẬN XÉT CỦA NGƯỜI HƯỚNG DẪN

NHẬN XÉT CỦA NGƯỜI PHẢN BIỆN

TÓM TẮT

Tên đề tài: Xây dựng hệ thống bảo mật sinh trắc học dựa trên nhận dạng khuôn mặt và vân tay ứng dụng vào Smart Home

Sinh viên thực hiện: Phạm Văn Hào

Nguyễn Thành Chính

Nguyễn Văn Cường

Mã SV: 1711505110110

1711505110105

1711505210105

Lớp: 17KTDT1

Đề tài "Xây dựng hệ thống bảo mật sinh trắc học dựa trên nhận dạng khuôn mặt và vân tay ứng dụng vào Smart Home" nhằm tạo ra một hệ thống bảo mật có thể ứng dụng cho cửa ra vào trong nhà . Nội dung báo cáo là các kiến thức về lập trình nhúng chương trình xử lý hình ảnh vào Raspberry Pi bằng ngôn ngữ python. Sản phẩm của đề tài này bao gồm một bộ xử lý trung tâm và các thiết bị đầu ra khác trong ngôi nhà. Bên cạnh đó báo cáo cũng cung cấp các số liệu thử nghiệm và đánh giá thực tế của sản phẩm từ đó đưa ra nhận xét.

LỜI NÓI ĐẦU

Thời gian vừa qua đã tạo cơ hội cho chúng em tổng hợp và hệ thống hóa lại những kiến thức đã học, đồng thời kết hợp với thực tế để nâng cao kiến thức chuyên môn. Qua quá trình nghiên cứu đề tài, chúng em đã được mở rộng tầm nhìn và tiếp thu rất nhiều kiến thức thực tế. Từ đó chúng em nhận thấy, việc tham gia nghiên cứu và thực hành thực tế là vô cùng quan trọng nó giúp sinh viên xây dựng nền tảng lý thuyết được học ở trường vững chắc hơn, đồng thời tiếp thu được thêm nhiều kiến thức mới. Trong quá trình thực hiện đồ án, chúng em đã gặp phải rất nhiều khó khăn nhưng với sự giúp đỡ tận tình của thầy Lê Hữu Duy đã giúp em có thể hoàn thành tốt đồ án này cũng như viết lên bài báo cáo đồ án tốt nghiệp.

Xin chân thành cảm ơn thầy cô giáo trong Trường Đại học Sư phạm Kỹ thuật Đà Nẵng nói chung và các thầy cô trong khoa Điện - Điện tử nói riêng đã tận tình giảng dạy, truyền đạt cho chúng em những kiến thức quý báu và tạo điều kiện giúp đỡ trong suốt quá trình học tập trong những năm học vừa qua, giúp chúng em có được cơ sở lý thuyết vững vàng để hoàn thành tốt đồ án tốt nghiệp này.

Tuy nhiên do thời gian có hạn cộng với kiến thức còn hạn chế nên Bài báo đồ án tốt nghiệp của chúng em không sao tránh khỏi có những thiếu sót. Vì thế em rất mong nhận được sự đóng góp ý kiến, chỉ bảo thêm từ phía thầy cô cũng như các bạn.

Chúng em xin chân thành cảm ơn!

CAM ĐOAN

Chúng em xin cam đoan đề tài: "Xây dựng hệ thống bảo mật sinh trắc học dựa trên nhận dạng khuôn mặt và vân tay ứng dụng vào Smart Home" là một công trình nghiên cứu độc lập dưới sự hướng dẫn của giáo viên hướng dẫn: ThS. Lê Hữu Duy. Ngoài ra không có bất cứ sự sao chép của người khác. Đề tài, nội dung báo cáo tốt nghiệp là sản phẩm mà nhóm chúng em đã nỗ lực nghiên cứu trong thời gian qua. Các số liệu, kết quả trình bày trong báo cáo là hoàn toàn trung thực, em xin chịu hoàn toàn trách nhiệm, kỷ luật của bộ môn và nhà trường đề ra nếu như có vấn đề xảy ra.

Đà Nẵng, ngày… tháng… năm 202..

Sinh viên thực hiện 1	Sinh viên thực hiện 2	Sinh viên thực hiện 3
Phạm Văn Hào	**Nguyễn Thành Chính**	**Nguyễn Văn Cường**

MỤC LỤC

DANH SÁCH CÁC BẢNG, HÌNH VẼ

HÌNH ẢNH CHƯƠNG 3

HÌNH ẢNH CHƯƠNG 4

HÌNH ẢNH CHƯƠNG 5

DANH SÁCH CÁC KÝ HIỆU, CHỮ VIẾT TẮT

KÝ HIỆU:

……

……

……

……

……

……

CHỮ VIẾT TẮT:

Công nghệ Lice-scan: phương pháp đạt được hình ảnh vân tay không sử dụng mực in

……

……

……

……

MỞ ĐẦU

Hiện nay, vấn đề an toàn bảo mật và an ninh là một vấn đề cực kì quan trọng và cần thiết trong cuộc sống, ta có thể thấy hàng loạt các công nghệ có liên quan và ảnh hưởng đến vấn đề này đang được thúc đẩy ra đời và phát triển một cách mạnh mẽ. Từ vấn đề an ninh của các cơ quan, trụ sở cho tới việc bảo đảm an toàn các thiết bị, nhà cửa, công trình, VV... Điển hình như việc thiết lập một hệ thống bảo vệ nhà cửa tránh sự xâm nhập của kẻ lạ cũng như vấn đề trộm cướp. Hệ thống bảo vệ có thể là một ổ khóa thông minh được người dùng cài đặt mật khẩu bằng các dãy số, hay là hệ thống được tạo nên dựa trên cơ sở của công nghệ sinh trắc học như là nhận diện khuôn mặt, giọng nói, vân tay,... Trong đề tài này, chúng ta sẽ nói về một hệ thống bảo mật đóng mở cửa bằng phương pháp nhận diện dựa trên công nghệ sinh trắc học. Và cụ thể đó là hệ thống sử dụng nhận dạng khuôn mặt, vân tay

Mục tiêu của đồ án này là đem lại các tính năng bảo mật hệ thống cửa ra vào nhưng phải đảm bảo được gia thành rẻ và tiện lợi. Để hoàn thành mục tiêu này nhóm đã tập trung nghiên cứu các kiến thức về lập trình nhúng cho Raspberry, các kiến thức về xử lý hình ảnh, lập trình python,

Trong quá trình nghiên cứu nhóm đã sử dụng nhiều phương pháp nghiên cứu khác nhau nhằm đạt hiệu quả cao nhất có thể liệt kê sơ qua:

- Phân tích và tổng hợp lý thuyết.
- Nghiên cứu sách báo, qua mạng internet.
- Xây dựng thuật toán, viết chương trình.
- Lắp ráp và chạy thử thiết bị.

Báo cáo đồ án tốt nghiệp "Xây dựng hệ thống bảo mật sinh trắc học dựa trên nhận dạng khuôn mặt và vân tay ứng dụng vào Smart Home" sẽ bao gồm các nội dung sau:

- Phần I: Mở đầu
- Phần II: Giới thiệu đề tài
- Phần III: Tổng quan hệ thống bảo mật ứng dụng cho nhà thông minh
- Phần IV: Thiết kế hệ thống bảo mật sử dụng khuôn mặt, vân tay
- Phần V: Thiết kế thực thi
- Phần VI: Đánh giá hệ thống

Chương 1: MỞ ĐẦU

1.1. Đặt vấn đề

Nhận dạng sinh trắc học đề cập đến việc sử dụng các thuộc tính duy nhất của hành vi và đặc điểm thể chất chẳng hạn như dấu vân tay, khuôn mặt, chữ ký, mống mắt để tự động nhận dạng một người. Trong các tổ chức, cơ quan hành chính, nghiên cứu khoa học luôn phải kiểm tra và trả lời các câu hỏi: "Con người có quyền ra vào và sử dụng thiết bị không?", "Cá nhân có quyền tiếp cận thiết bị. "Bạn có quyền truy cập thông tin bí mật không?. "Nghiên cứu cho thấy rằng các đặc điểm sinh học không thể dễ dàng thay thế, chia sẻ hoặc giả mạo . Chúng được coi là đáng tin cậy hơn các phương pháp dựa trên thẻ truyền thống như sử dụng khóa , các phương pháp dựa trên kiến thức chẳng hạn như sử dụng mật khẩu. Sinh trắc học ngày càng cung cấp cho người dùng mức độ bảo mật cao hơn, hiệu quả cao hơn và tiện lợi hơn. Nhiều quốc gia trên thế giới đã và đang phát triển nhiều công nghệ sinh trắc học, một số công nghệ đã được đưa vào ứng dụng thực tế. Sinh trắc học thường được sử dụng là dấu vân tay, khuôn mặt, mống mắt, giọng nói, ... Mỗi sinh trắc học đều có những ưu điểm và nhược điểm, vì vậy việc sử dụng các sinh trắc học cụ thể phụ thuộc vào yêu cầu của một ứng dụng nhất định. Các đặc điểm sinh học có thể được so sánh dựa trên các yếu tố sau: tính phổ biến, tính duy nhất, tính ổn định, khả năng thu thập, tính hợp lệ và khả năng chấp nhận. Dấu vân tay được biết đến với sự độc đáo tính cách và ổn định theo thời gian, và là đặc điểm sinh học được sử dụng rộng rãi nhất. Bảo mật bằng mật khẩu là một trong những hình thức truyền thống trước đây, thường được sử dụng để kiểm soát truy cập. Tuy nhiên, với sự phát triển kinh tế và xã hội như hiện nay, những hình thức truyền thống này không còn mang lại hiệu quả cao về độ an toàn. Dần dần phương pháp này đã được thay thế bởi công nghệ tiên tiến hơn đó là việc ứng dụng công nghệ sinh trắc học.

Trong thời gian ngắn thực hiện đề tài, cộng với việc đề tài tại Việt Nam rất ít người làm nên kiến thức còn hạn chế, trong tập đồ án thiếu sót là điều không thể tránh khỏi, nhóm thực hiện rất mong sự đóng góp ý kiến của thầy cô và bạn bè.

1.2. Mục tiêu

Mục tiêu của đề tài là thiết kế và lắp đặt được 1 hệ thống bảo mật sử dụng sinh trắc học và vân tay ứng dụng vào smarthome thông qua xử lý hình ảnh. Hệ thống

cần đáp ứng đầy đủ được các chức năng cơ bản của một hệ thống nhà thông minh tương tác thông dụng hiện nay. Nhưng với giá thành phù hợp với tính ứng dụng cao.

Để đạt yêu cầu trên nhóm đặt ra mục tiêu nghiên cứu cụ thể như sau:

- Tìm hiểu về nguyên tắc hoạt động của Raspberry Pi. Biết cách cài đặt và lập trình cho Raspberry Pi.
- Tìm hiểu về ngôn ngữ lập trình python và lập trình nhúng Raspberry Pi bằng python.
- Tìm hiểu và lập trình thị giác máy tính với OpenCV.
- Thiết kế, cấu hình và lắp đặt thiết bị sinh trắc học và vân tay.
- Tìm hiểu về ngôn ngữ lập trình điều khiển cho vân tay dựa trên nền tảng Arduino.

1.3. Phương pháp nghiên cứu

Nhóm khi thực hiện đề tài đã sử dụng các phương pháp nghiên cứu như sau:

- Phân tích và tổng hợp lý thuyết
- Sách báo, qua mạng internet
- Tham khảo tài liệu
- Viết chương trình
- Lắp ráp và chạy thử thiết bị

1.4. Nội dung đề tài

Đồ án tốt nghiệp "XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME" được trình bày trong 6 chương như sau:

- **Chương 1: Mở đầu**
  - Tổng quan về đề tài: đặt vấn đề, mục tiêu nghiên cứu, nội dung đề tài.
- **Chương 2: Giới thiệu đề tài**
  - Tổng quan về hệ thống nhà thông minh, cấu tạo nguyên lý.
  - Khảo sát một số hệ thống nhà thông minh hiện nay.
- **Chương 3: Tổng quan hệ thống bảo mật dành cho nhà thông minh**
  - Tổng quan về hệ thống bảo mật truyền thống, bảo mật hiên nay…
  - Trình bày ý tưởng dựa trên 1 số hệ thống bảo mật nhà có sẵn.

- **Chương 4: Thiết kế hệ thống bảo mật sử dụng khuôn mặt, vân tay**
  - Trình bày sơ đồ nguyên lý hoạt động tổng quát của hệ thống
  - Trình bày và phân tích sơ đồ thuật toán.
  - Thiết kế và lựa chọn phần cứng.
- **Chương 5: Thiết kế thực thi**
  - Chạy thử nghiệm trong 1 số môi trường.
  - Phân tích, đánh giá và nhận xét kết quả nhận được.
- **Chương 6: Đánh giá hệ thống**
  - Kết quả đạt được của đồ án.
  - Hướng phát triển cho hệ thống.

Chương 2: GIỚI THIỆU ĐỀ TÀI

Xã hội thế kỷ 21 chứng kiến sự phát triển vượt bậc của công nghệ và đánh dấu sự mở đầu của những thiết bị thông minh. Smart phone, Smart Tivi đều là những thiết bị ngày càng phổ biến, thông dụng trong đời sống hằng ngày của con người. Đúng như tên gọi, những thiết bị này không những có khả năng đáp ứng những yêu cầu cơ bản của con người, mà còn hơn thế, các thiết bị smart ra đời đã thay thế con người trong việc kiểm soát và điều khiển các chức năng khác 1 cách chuyên nghiệp, dễ dàng và hiệu quả.

Tiếp nối thành công của những thiết bị thông minh ấy, Smart home ra đời như một sự khởi đầu táo bạo về tư duy làm chủ công nghệ ngay trong cuộc sống của con người. Một ngôi nhà thông minh với khả năng thấu hiểu tư duy điều khiển của con người nhanh chóng trở thành đề tài công nghệ có sức hấp dẫn.

Nhà thông minh là một đề tài rộng và có nhiều vấn đề đặt ra. Tùy theo mục đích sử dụng của chủ nhân để thiết kế, một phần quan trọng trong hệ thống nhà thông minh là hệ thống điều khiển và giám sát.

Bên cạnh đó, vấn đề an toàn bảo mật và an ninh là một vấn đề cực kì quan trọng và cần thiết trong cuộc sống, ta có thể thấy hàng loạt các công nghệ có liên quan và ảnh hưởng đến vấn đề này đang được thúc đẩy ra đời và phát triển một cách mạnh mẽ. Từ vấn đề an ninh của các cơ quan, trụ sở cho tới việc bảo đảm an toàn các thiết bị, nhà cửa, công trình, VV... Điển hình như việc thiết lập một hệ thống bảo vệ nhà cửa tránh sự xâm nhập của kẻ lạ cũng như vấn đề trộm cướp. Hệ thống bảo vệ để có thể là một ổ khóa thông minh được người dùng cài đặt mật khẩu bằng các dãy số, hay là hệ thống được tạo nên dựa trên cơ sở của công nghệ sinh trắc học như là nhận diện khuôn mặt, giọng nói, vân tay,... Như đã nêu ở trên, hiện tại những nơi như nhà máy, xí nghiệp, cơ quan, nhà cửa hay những nơi có sự an toàn, bảo mật đặt hàng đầu thì một hệ thống bảo vệ lối ra vào hay là phát hiện được sự xâm nhập của kẻ lạ, khả nghi, giả mạo đặc biệt đối với các cơ quan an ninh, bệnh viện hoặc những nơi đông người,...) là vô cùng cần thiết.

Trong đồ án này, chúng em trình bày một hệ thống bảo vệ đóng mở cửa bằng phương pháp nhận diện dựa trên công nghệ sinh trắc, và cụ thể đó là hệ thống sử dụng cảm biến vân tay, xử lý ảnh nhận dạng khuôn mặt.

Đề tài là một sản phẩm có tính thực tế cao dựa trên nhu cầu công nghệ hiện nay, được nghiên cứu, chế tạo dựa trên những kiến thức chúng em đã học, kế thừa và phát huy những kết quả của các công trình nghiên cứu trước đây.

Em xin cảm ơn gia đình, bạn bè đã tạo điều kiện, giúp đỡ cho bản thân em hoàn thành được đồ án tốt nghiệp này

Em xin chân thành cảm ơn các thầy cô trong bộ môn Điện Tử đã tận tình chỉ bảo để nhóm em có thể hoàn thành đề tài nghiên cứu này. Bên cạnh đó là sự hướng dẫn, góp ý của giáo viên hướng dẫn Th.S Lê Hữu Duy và sự giúp đỡ của giáo viên phản biện TS. ……..

Do thời gian và kiến thức còn nhiều hạn chế, đề tài của em sẽ không tránh khỏi những sai sót, em mong thầy cô góp ý, chỉnh sửa để có thể hoàn thiện hơn.

Đà Nẵng, ngày tháng năm 2021

Sinh viên thực hiện

Phạm Văn Hào

Nguyễn Thành Chính

Nguyễn Văn Cường

Chương 3: TỔNG QUAN HỆ THỐNG BẢO MẬT ỨNG DỤNG CHO NHÀ THÔNG MINH

3.1. Bảo mật truyền thống

3.1.1. Khóa cơ

3.1.1.1 Tính tiện dụng của khóa

Khóa cơ: thông thường bạn cần có chìa khóa để mở cửa. Nếu không may bỏ quên chìa khóa ở trong nhà và chốt cửa lại .

Khi làm mất chìa khóa thì cách duy nhất để bạn có thể vào nhà là tìm đến những người thợ sửa khóa hoặc phá khóa. Đôi khi có thể khiến người khác hiểu lầm rằng bạn đang cố tình đột nhập vào nhà người khác.

Hình 3.1: Khóa cơ

3.1.1.2 Tính bảo mật

Khóa cơ: với những chiếc khóa cơ thông thường có rất nhiều cách. Để kẻ xấu mở cửa đột nhập vào nhà bạn chỉ với chiếc chìa vạn năng. Một chiếc kìm công lực, một thanh kẽm hay một chút axit mạnh để phá khóa. Do đó, khóa cơ gần như không còn khả năng bảo vệ khi đứng trước những tên trộm ranh mãnh.

3.1.1.3. Tính thẩm mỹ

Khóa cơ: đa số các loại khóa cơ đều có vẻ ngoài tầm thường, đơn giản, nhiều loại còn dễ bị hoen gỉ sau một thời gian sử dụng. Chính những chiếc khóa này làm giảm đi vẻ đẹp thẩm mỹ cho ngôi nhà của bạn.

3.1.1.4. Hệ thống khóa cửa

Khóa cơ: Cơ chế hoạt động dựa vào sự ăn khớp giữa hốc lõm và vết rãnh của chìa khóa và các đường rãnh bên trong ổ khóa. Có thể nói khóa cơ không có khả năng quản lý và phân quyền do chỉ cần có chìa khóa của đúng ổ khóa là có thể mở được cửa.

3.1.2. Camera an ninh

3.1.2.1 Quyền riêng tư là một vấn đề

Trước đây đã có một vài trường hợp camera an ninh gây tranh cãi, đặc biệt là trong các thiết lập chuyên nghiệp. Đã có trường hợp nhân viên phản đối việc bị giám sát liên tục mà không có sự cho phép của họ và lấy lý do là 'xâm phạm quyền riêng tư'. Một số người cũng đã dùng đến hành động pháp lý chống lại người sử dụng lao động của họ liên quan đến việc này.

Những người chỉ trích hệ thống camera an ninh đã xúc phạm đến việc họ được đặt trong văn phòng và lập luận rằng làm như vậy có nghĩa là người sử dụng lao động đã giả định hoặc tin rằng nhân viên của mình không tốt và sẽ làm điều gì đó sai trái, đó là lý do tại sao các hoạt động của họ cần phải được ghi lại.

3.1.2.2 Chi phí cho thiết bị đắt tiền

Mặc dù camera giả có thể không đắt, nhưng camera thật có giá hàng trăm, thậm chí hàng nghìn USD tùy thuộc vào tính năng và số lượng camera, hệ thống giám sát mà bạn mua. Việc cài đặt chúng và bảo trì chúng đồng nghĩa với việc tăng thêm chi phí. Nếu bạn đang nghĩ đến việc tự lắp đặt chúng, hãy tạm dừng ý tưởng đó trừ khi bạn có kiến thức tốt về hệ thống dây dẫn, nếu không bạn có thể làm hỏng camera.

Hình 3.2: Camera an ninh

3.1.2.3 Họ có thể dễ bị tổn thương

Khi chúng ta, là người sử dụng camera an ninh, cố gắng cập nhật những thông tin mới nhất về hệ thống an ninh, chúng ta không nên quên rằng những kẻ xâm nhập và tội phạm cũng đang làm như vậy. Một kẻ xâm phạm thông minh có thể sẽ biết tất cả về chúng và có thể đã tìm ra cách để không bị phát hiện.

Hơn nữa, những tên tội phạm am hiểu công nghệ có thể đã hiểu công nghệ và tìm ra cách để vô hiệu hóa ngắt kết nối chúng khỏi nguồn điện của chúng. Ngoài ra, nếu anh ta phát hiện máy ảnh của bạn là giả hình nộm, chúng có thể hoàn toàn vô dụng trong bất kỳ công tác phòng chống tội phạm nào.

Trong trường hợp xấu nhất, tin tặc có thể phá hoại hệ thống camera an ninh của bạn bằng cách sử dụng Internet và sử dụng chúng để theo dõi bạn.

Điều này làm cho camera an ninh dễ bị hư hỏng và hoặc sử dụng sai mục đích.

3.1.2.4. Không thể ngăn chặn trộm cắp

Máy ảnh cho phép người dùng ghi lại cảnh quay để xem sau, đồng thời giúp truy bắt tội phạm và nhận công lý từ pháp luật. Tuy nhiên, họ không thể ngăn chặn tội ác khi nó đang diễn ra. Họ không cảnh báo hàng xóm hoặc cảnh sát như một hệ thống báo động. Điều này có nghĩa là bạn sẽ phải chịu tổn thất ngay cả khi bạn chạy ra tòa,

yêu cầu bảo hiểm và sắp xếp lại hàng tồn kho bị đánh cắp, điều này có thể khiến bạn không còn cảm thấy an toàn tuyệt đối và thậm chí khiến bạn mất niềm tin vào chúng.

Hình 3.3: Camera hãng HIK VISION

3.2. Các hệ thống bảo mật an ninh hiện nay

3.2.1. Vân tay

Bảo mật vân tay ngày càng được ứng dụng rộng rãi trong đời sống. Sự hiện diện của bảo mật vân tay trên vào các thiết bị thường nhật giúp người tiêu dùng tận hưởng một cuộc sống nhiều tiện ích và thoải mái hơn.

Nghiên cứu về vân tay đã xuất hiện cách đây 200 năm, kết hợp cùng sự phát triển khoa học kỹ thuật, hàng triệu thông tin dần được số hoá và ứng dụng công nghệ sinh trắc vân tay nhằm mục đích lưu trữ dữ liệu một cách dễ dàng. Khi nhu cầu bảo mật, nhận diện ngày một cao, công nghệ sinh trắc vân tay được chú trọng phát triển và dần phổ biến thông qua các thiết bị sử dụng hằng ngày: điện thoại, máy tính, máy chấm công,...

Hình 3.4: Khóa vân tay

Nguyên tắc hoạt động của công nghệ nhận dạng vân tay: Khi vân tay được đặt lên máy quét, ngay lập tức hình ảnh vân tay được đối chiếu các đặc điểm của ngón tay đó với dữ liệu đã được lưu trữ trong hệ thống, qua quá trình xử lý để đưa ra thông báo rằng dấu vân tay đó là hợp lệ hay không hợp lệ.

Với đặc tính sinh học phụ thuộc vào di truyền và môi trường, vân tay của mỗi người là duy nhất. Đến nay khoa học vẫn chưa xác nhận trường hợp trùng vân tay nào kể cả các cặp song sinh. Vì đặc tính trên, công nghệ sinh trắc vân tay được người dùng ứng dụng rộng rãi vào đời sống con người.

Chức năng mở khoá bằng dấu vân tay gần như đã xuất hiện trên toàn bộ các dòng điện thoại di động để dễ dàng mở khóa, thanh toán về bảo mật dữ liệu tốt hơn. Máy chấm công bằng vân tay cũng được nhiều công ty sử dụng vì thao tác thực hiện nhanh chóng và chính xác, giúp công việc quản lý dễ dàng hơn.

Bảo mật vân tay như một bức tường lửa, nâng cao sự an toàn cho người dùng. Cụ thể:

- Đặc điểm sinh học khó sao chép hơn so với các loại thẻ từ.
- Không thể đoán cầu may như password.

- Vân tay của mỗi người là cá biệt, không thể nhầm lẫn.
- Không có tình trạng quên mất vân tay như quên chìa khoá hay các loại thẻ từ.

3.2.2. Nhận diện khuôn mặt

Công nghệ nhận diện khuôn mặt là một loại phần mềm sinh trắc học ánh xạ các đặc điểm khuôn mặt của một cá nhân về mặt toán học và lưu trữ dữ liệu dưới dạng faceprint (dấu khuôn mặt). Công nghệ sử dụng các thuật toán Deep Learning để so sánh ảnh chụp trực tiếp hoặc hình ảnh kỹ thuật số với faceprint được lưu trữ để xác minh danh tính của một cá nhân.

Công nghệ nhận diện khuôn mặt hoạt động như thế nào?

Phần mềm xác định 80 điểm nút trên khuôn mặt người. Các điểm nút được sử dụng để đo các biến trên khuôn mặt người, như chiều dài hoặc chiều rộng của mũi, độ sâu của hốc mắt và hình dạng của xương gò má. Hệ thống hoạt động bằng cách thu thập dữ liệu cho các điểm nút trên hình ảnh kỹ thuật số của khuôn mặt và lưu trữ dữ liệu kết quả dưới dạng faceprint. Faceprint sau đó được sử dụng làm cơ sở để so sánh với dữ liệu được chụp từ các khuôn mặt trong một hình ảnh hoặc video.

Mặc dù hệ thống nhận diện khuôn mặt chỉ sử dụng 80 điểm nút, nhưng nó có thể xác định nhanh chóng và chính xác mục tiêu khi điều kiện thuận lợi. Tuy nhiên, nếu khuôn mặt của chủ thể bị che khuất một phần, loại phần mềm này trở nên ít đáng tin cậy hơn.

Những trường hợp sử dụng của công nghệ nhận diện khuôn mặt

Công nghệ nhận diện khuôn mặt có thể được sử dụng cho vô số ứng dụng, từ bảo mật đến quảng cáo. Một số trường hợp sử dụng bao gồm:

- Bảo mật trên thiết bị di động.
- Mạng xã hội (chẳng hạn như Facebook, để gắn thẻ các cá nhân trong ảnh).
- Bảo mật doanh nghiệp, vì các doanh nghiệp có thể sử dụng nhận dạng khuôn mặt để vào tòa nhà.
- Tiếp thị. Các nhà tiếp thị có thể sử dụng nhận dạng khuôn mặt để xác định độ tuổi, giới tính và dân tộc để nhắm mục tiêu tới đối tượng cụ thể.

Những lợi ích của nhận dạng khuôn mặt

Với việc sử dụng công nghệ nhận diện khuôn mặt có thể mang đến một loạt các lợi ích tiềm năng, bao gồm:

- Không cần phải trực tiếp tiếp xúc với thiết bị để xác thực (các kỹ thuật xác thực sinh trắc học dựa trên tiếp xúc khác như máy quét dấu vân tay, có thể không hoạt động chính xác nếu có vết bẩn trên tay của một người).
- Cải thiện mức độ bảo mật.
- Yêu cầu xử lý ít hơn so với các kỹ thuật xác thực sinh trắc học khác.
- Dễ dàng tích hợp với các tính năng bảo mật hiện có.
- Độ chính xác được cải thiện theo thời gian.
- Có thể được sử dụng để giúp tự động hóa việc xác thực.

3.2.3. Giọng nói

Giải pháp nhà thông minh điều khiển bằng giọng nói được hiểu là tất cả các hệ thống thiết bị của ngôi nhà như chiếu sáng, rèm cửa, bình nóng lạnh, điều hòa, âm thanh, truyền hình… đều được gắn các bộ điều khiển điện tử để có thể kết nối với Internet và điện thoại di động, cho phép chủ nhà điều khiển bằng giọng nói của chính mình. Điều khiển nhà bằng giọng nói lần đầu tiên xuất hiện tại Việt Nam.
Đây được xem là một bước đột phá vượt trội trong hệ thống nhà thông minh ở Việt Nam.

Hình 3.5: Hình tượng trưng giải pháp nhà thông minh điều khiển bằng giọng nói

Ứng dụng giải pháp nhà thông minh điều khiển bằng giọng nói và tính năng của chúng Khi bạn đang bận làm bất kì công việc gì mà không thể cầm điện thoại hay ipad để điều khiển. Lúc này bạn chỉ cần ra lệnh, mọi thiết bị sẽ "vâng lời" theo ý muốn của bạn.

Các giải pháp có khả năng "hỗ trợ Alexa", tất cả đều sẵn sàng nhận lệnh bằng giọng nói của người dùng với những câu lệnh bắt đầu bằng "Alexa".

Ví dụ**:** khi bạn muốn bật đèn, bạn chỉ cần nói câu lệnh: Alexa, turn on the lights" thông tin sẽ được truyền đến server Amazon, rồi qua sever của nhà thông minh. Tại đây, bộ điều khiển trung tâm sẽ truyền lệnh cho đèn bật sáng và mở rèm trong tích tắc.

Lợi ích mà nhà thông minh điều khiển bằng giọng nói mang lại cho người sử dụng an toàn cho trẻ nhỏ: Bạn không còn phải lo lắng khi con leo trèo bật đèn hay tay ướt chạm vào công tắc điện, thật đơn giản, chỉ cần ra lệnh cho thiết bị nhận diện giọng nói, ngay lập tức đèn đã bật lên.

Tiện ích cho người cao tuổi: Bố mẹ bạn đã có tuổi và khó khăn trong việc di chuyển, để bật tắt các thiết bị hay đơn giản kéo rèm khi đọc sách mà không muốn phiền đến bạn, thiết bị nhận diện giọng nói sẽ thay bạn làm điều đó.

Cho giấc ngủ thêm ngon giấc: Ánh sáng trong phòng không phù hợp, có thể do đèn ngủ hay rèm cửa. Thật khó chịu với việc chui ra khỏi chăn ấm, nhảy xuống đất để tắt đèn hoặc kéo rèm. Với nhà thông minh điều khiển bằng giọng nói, bạn chỉ cần ra lệnh, lập tức phòng ngủ sẽ có ánh sáng hợp lý.

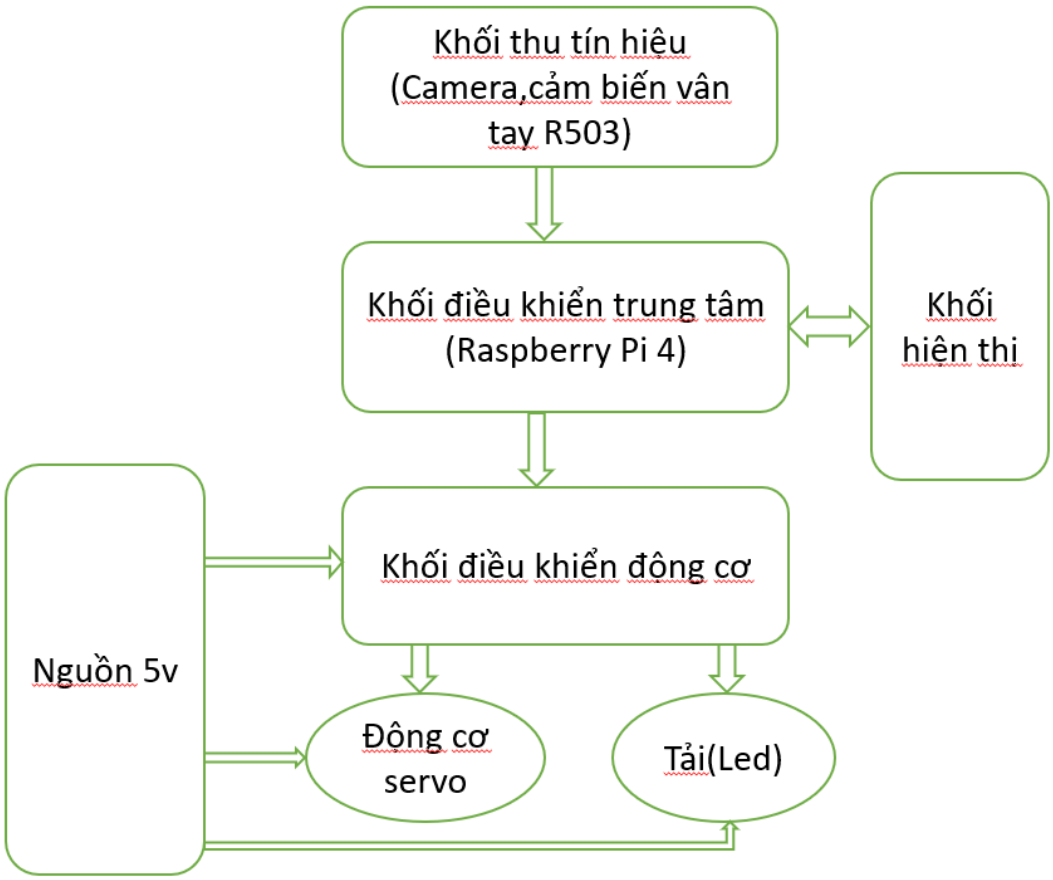
Thiết lập hoạt cảnh: Thay vì phải đi lần lượt các phòng để kiểm tra các thiết bị điện trước khi ngủ. Giờ đây chỉ cần nằm trên giường và ra lệnh, mọi thiết bị sẽ tự động theo ý bạn… Ngoài ra, các thiết bị trong nhà có thể tự động bật tắt nếu chuyển sang chế độ hẹn giờ.

Âm thanh đa vùng: Mùa đông, bạn muốn nghe một bản nhạc, nhưng lại không muốn chui ra khỏi chăn. Với nhà thông minh điều khiển bằng giọng nói, công việc duy nhất bạn phải làm là nằm trong chăn yêu cầu bài hát yêu thích.

Dựa trên các hệ thống tham khảo như thế, nhóm em mong muốn xây dựng hệ thống bảo mật khuôn mặt + vân tay cho cửa ra vào. Vì lý do: Thay thế hệ thống mở cửa truyền thống bằng bảo mật sinh trắc học tăng tính bảo mật nhằm tránh ké xấu muốn đột nhập,

Chương 4: THIẾT KẾ HỆ THỐNG BẢO MẬT SỬ DỤNG VÂN TAY , KHUÔN MẶT

4.1 Sơ đồ khối hệ thống



Hình 4.0 Sơ đồ khối hệ thống

Khối xử lý trung tâm sẽ lấy tín hiệu từ khối thu tín hiệu hình ảnh để xử lý rồi gửi tín hiệu qua khối điều khiển động cơ và khối hiển thị để điều khiển động cơ và hiển thị thông tin người dùng trên màn hình deskop.

Chức năng từng khối:

Khối xử lý trung tâm: Là bộ xử lý chính, nhận tín từ khối thu tín hiệu hình ảnh, sau đó xử lý hình ảnh và phân tích nhận dạng, đem so sánh để đưa kết quả. Sử dụng kit Raspberry Pi 4 Model B làm bộ xử lý trung tâm. Sử dụng thêm bàn phím và chuột máy cho kit Raspberry.

Khối thu tín hiệu hình ảnh: Có chức năng thu nhận tín hiệu hình ảnh từ thực tế chuyển về tín hiệu điện và gửi dữ liệu cho Khối xử lý trung tâm. Ở đây dùng Camera USB làm khối thu tín hiệu hình ảnh.

Khối hiển thị: nhận tín hiệu từ khối xử lý trung tâm để hiển thị trên màn hình desktop

Khối điều khiển động cơ: Relay 1 kênh 5V sẽ giao tiếp với khối xử lý trung tâm thông qua giao tiếp I2C của Raspberry nếu Raspberry truyền ký tự '1' qua chân GPIO, và sẽ tiến hành cho chân tín hiệu của động cơ lên mức cao để mở cửa sau khi mở cửa 5s thì tự đóng lại

Khối nguồn: Dùng nguồn 5V để nuôi khối xử lý trung tâm.

4.2 Vân tay

4.2.1. Giới thiệu sơ lược về dấu vân tay và nhận dạng vân tay

Khái niệm về dấu vân tay

Dấu vân tay là một đường vân nằm trên ngón tay người và nó thể hiện sự phản ánh chính xác số lượng nếp nhăn trên não.

Dấu vân tay của con người rất chi tiết, gần như là duy nhất, khó thay đổi và tồn tại trong suốt cuộc đời của một cá nhân, điều này làm cho chúng thích hợp làm dấu ấn vĩnh viễn của danh tính con người.

Sinh trắc vân tay là phương pháp sử dụng công nghệ để phân tích mật độ, độ dài và hình dạng của dấu vân tay, các nghiên cứu đã chỉ ra rằng các chỉ số phát triển thần kinh não có liên quan mật thiết đến sự gia tăng của thượng bì và biểu bì, do đó, sinh trắc vân tay dần trở thành giải pháp hữu hiệu cho con người.

4.2.2. Lịch sử của công nghệ vân tay

Việc bắt đầu sử dụng vân tay là ở thời gian rất xa xưa. Theo lịch sử tìm thấy, vân tay đã được sử dụng trên những tấm thẻ bằng đất sét cho việc giao dịch kinh doanh ở thời Babylon cổ xưa. Ở Trung Quốc, dấu vân tay được tìm thấy trên những con dấu bằng đất sét. Nhưng mãi đến thế kỷ 19 những kết quả nghiên cứu khoa học mới được phổ biến và công nghệ vân tay mới bắt đầu được xem xét hàng loạt.

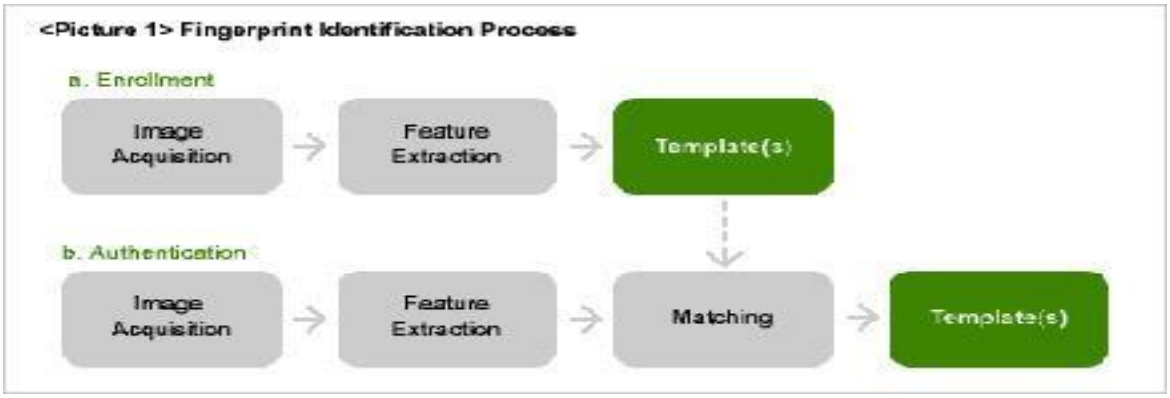
Việc sử dụng những nghiên cứu khoa học ở những năm 1800 như là một phát minh, công nghệ vân tay đã được ứng dụng vào đầu thế kỷ 20. Vào năm 1924, FBI (Federal Bureau of Investigation) đã biết lưu trữ 250 tỉ vân tay của công dân cho mục đích điều tra tội phạm và nhận dạng những người bị chết mà không biết rõ họ tên. Vào đầu những năm 1900, công nghệ vân tay đã gặp một bước ngoặt lớn khi nó cho ra đời "live-scan", một phương pháp đạt được hình ảnh vân tay không sử dụng mực in. Khi

FBI loan báo rằng đó là kế hoạch để ngưng sử dụng những thẻ vân tay bằng giấy cho những thành viên mới gia nhập AFIS (IAFIS) nội bộ của họ. Đó là thực tế đang công bố gây một bước nhảy vọt cho công nghệ Live-Scan ngày hôm nay.

Nhưng công nghệ nhận dạng vân tay không dừng lại chỉ cho mục đích pháp lý. Nó đã được sử dụng một cách chính thức cho mục đích kinh doanh vào năm 1968 tại một nhóm kinh doanh về an ninh tại đường Wall. Vân tay ngày nay đang được sử dụng như là một phương pháp nhận dạng hiệu quả và chắc chắn trong nhiều lĩnh vực, bao gồm tài chính, y học, kinh tế điện tử và ứng dụng điều khiển truy nhập và khóa cửa. Ứng dụng hiện đại nhất của công nghệ vân tay là nhờ vào phần lớn của sự phát triển của mắt đọc vân tay dạng nén một cách phi thường.

4.2.3. Xử lý nhận dạng vân tay

Xử lí nhận dạng vân tay bao gồm hai quy trình thiết yếu: Sự đăng ký (Enrollment) và sự nhận dạng (Authentication). Xem các bước thủ tục theo sơ đồ bên dưới, hệ thống nhận dạng vân tay so sánh giữa hình ảnh vân tay đầu vào và dữ liệu đã đăng ký trước để xác định vân tay đúng. Tất cả các bước được mô tả ở trên là chỉ ra tính hoàn thiện của hệ thống toàn vẹn, nhưng gánh nặng của máy điện toán của các bước sau đây có thể được cắt giảm một phạm vi lớn bằng việc thu được một hình ảnh vân tay chất lượng cao cho bước đầu tiên.



Hình 4.1. Quy trình lấy vân tay

Bước 1. Thu gom hình ảnh vân tay

Phương pháp thu gom hình ảnh thời gian thực là sự phân lớp một cách đại khái là thuộc quang học (optical) và không thuộc quang học (non-optical). Phương pháp thuộc

về quang học là dựa vào hiện tượng phản xạ tuyệt đối trên bề mặt kiến hoặc tăng cường thêm một lớp chất dẻo ở nơi mà ngón tay tiếp xúc. Mắt đọc thông thường bao gồm một lăng kính và một khối CCD(Charged Coupled Device) hoặc là mắt đọc hình ảnh CMOS. Trong sự tương phản, mắt đọc bán dẫn, ví dụ tiêu biểu như những mắt đọc không thuộc quang học, khai thác những đặc tính thuộc về điện của ngón tay chẳng hạn như là điện dung. Sóng siêu âm, nhiệt, và áp suất cũng được sử dụng để đạt được hình ảnh đối với mắt đọc vân tay không thuộc quang học. Những mắt đọc không thuộc quang học được nói rằng thích hợp một cách tương đối hơn đối với sự sản xuất quy mô lớn và hạn chế về kích thước chẳng hạn như tích hợp với thiết bị di động.

Xem bảng 1 là chi tiết so sánh.

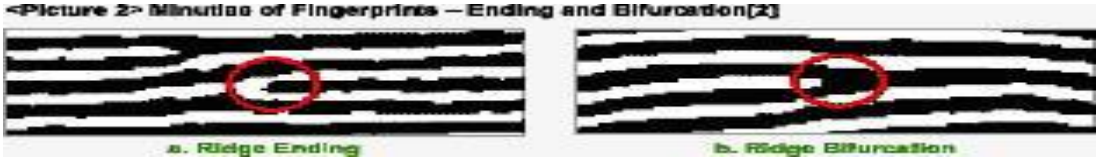
	Thuộc về quang học	Không thuộc về quang học
Phương pháp đo lường	Ánh sáng	Ánh sáng, nhiệt độ, điện dung, sóng siêu âm
Ưu điểm	Thực thi tính ổn định cao và hình ảnh chất lượng cao	Giá thành thấp với tích hợp kích cỡ nhỏ, tiêu thụ nguồn thấp
Khuyết điểm	Tranh giới giá thành cao để giảm bớt về kích thước Dể nhằm lẫn với ngón tay có vết tích hoặc ngón tay giả	Dễ bị hư bề mặt điện và gặp khó khăn với nhiệt độ và ngón tay khô
Ứng dụng	Hệ thống chấm công và điều khiển ra vào, điều khiển dịch vụ ngân hàng và bảo mật máy vi tính	Bảo mật máy vi tính, nhận dạng tài chính điện tử, thiết bị cầm tay và thẻ thông minh.

Bảng 1. Chi tiết so sánh thuộc và không thuộc về quang học

Bước 2. Sự rút trích đặc điểm riêng.

Có hai cách chính để so sánh hình ảnh đầu vào và dữ liệu đã đăng ký. Một là so sánh một hình ảnh này với hình ảnh khác một cách trực tiếp. Cách khác là so sánh đặc tính đoạn trích từ mỗi hình ảnh vân tay. Sau cùng là được gọi là việc kết nối so sánh đặc tính cơ bản (feature-based)/ minutia-based. Mỗi ngón tay có duy nhất một hình thể riêng theo các đường nổi thành dòng gọi là "ridges" và những vùng lổ giữa chúng gọi

là "valleys". Như thể hiện ở hình bên dưới, ridges được đại diện là những đường màu đen, trong đó valleys là trắng.



Hình 4.2. So sánh các đường vân tay

Bước 3. Sự kết nối so sánh– Matching

Các bước đối sánh được chia nhỏ thành đối sánh 1: 1 và đối sánh 1: N tùy theo mục đích và hoặc số lượng trích dẫn. So khớp 1: 1 còn được gọi là kiểm tra và xác định từng cá nhân. Đây là một chương trình yêu cầu người dùng chỉ định anh ta hoặc cô ta, tức là sử dụng dấu vân tay để chỉ định một ID. Chỉ có một phép so sánh giữa ảnh vân tay đầu vào và ảnh vân tay được chọn từ dữ liệu do người dùng khai báo. Ngược lại, đối sánh 1: N thể hiện quá trình hệ thống so sánh vân tay đầu vào với thông tin trong dữ liệu để nhận dạng người dùng mà không cần khai báo của người dùng. Một ví dụ hoàn hảo là AFIS (Hệ thống Nhận dạng Vân tay Tự động) thường được sử dụng trong điều tra tội phạm. Vậy, quá trình kết hợp được biểu diễn bằng các con số như thế nào? Các biện pháp đơn giản nhất là FRR (tỷ lệ từ chối sai) và FAR (tỷ lệ chấp nhận sai).

4.2.4. Thị trường ứng dụng vân tay

Thị trường ứng dụng vân tay đối với công nghệ vân tay bao gồm điều khiển truy nhập và ứng dung khóa cửa, chuột nhận dạng vân tay, điện thoại di động vân tay, và nhiều ứng dụng khác. Thị trường vân tay được phân lớp như hình bên dưới:

Hình 4.3 . Thị trường ứng dụng vân tay

Theo công nghệ tiến bộ cho phép kích cỡ mắt đọc vân tay ngày càng thu nhỏ nhiều hơn, dãy ứng dụng được trải rộng cho thị trường di động. Xem xét kênh phát triển của thị trường di động hiện tại, tiềm năng của nó là lớn nhất của toàn bộ thị trường ứng dụng.

4.2.5 Giới thiệu phần cứng

Thiết bị đầu vào: module cảm biến vân tay r503
Thiết bị đầu ra: động cơ servo SG90,relay
Thiết bị điều khiển trung tâm: Board arduino uno r3,raspberry pi4
Các chuẩn truyền dữ liệu: UART

4.2.6. Giới thiệu phần cứng

Arduino UNO R3 có thể sử dụng 3 vi điều khiển họ 8bit AVR là ATmega8, ATmega168, ATmega328. Bộ não này có thể xử lí những tác vụ đơn giản như điều khiển đèn LED nhấp nháy, xử lí tín hiệu cho xe điều khiển từ xa, làm một trạm đo nhiệt độ - độ ẩm và hiển thị lên màn hình LCD,… hay những ứng dụng khác mà bạn đã được xem.

Thiết kế tiêu chuẩn của Arduino UNO sử dụng vi điều khiển ATmega328 với giá khoảng 90.000đ. Tuy nhiên nếu yêu cầu phần cứng của bạn không cao hoặc túi tiền không cho phép, bạn có thể sử dụng các loại vi điều khiển khác có chức năng tương đương nhưng rẻ hơn như ATmega8 (bộ nhớ flash 8KB) với giá khoảng 45.000đ hoặc ATmega168 (bộ nhớ flash 16KB) với giá khoảng 65.000đ.

Các chân input - output của Arduino Uno R3

Hình 4.4. Sơ đồ chân Arduino Uno R3

Có một số chân I / O Digital và Analog được đặt trên bo mạch hoạt động ở mức logic 5V với dòng từ khoảng từ 20mA đến 40mA

- *Thông số kỹ thuật:*

Chíp ATMEGA328P-PU

Nguồn Cấp : 7-12V

Dòng Max chân 5V : 500mA

Dòng Max 3.3V : 50mA

Dòng Max Chân I/O : 30mA

14 Chân Digital I/O (6 chân PWM)

6 Chân Analog Inputs

32k Flash Memory

16Mhz Clock Speed

SRAM 2 KB

EEPROM 1 KB

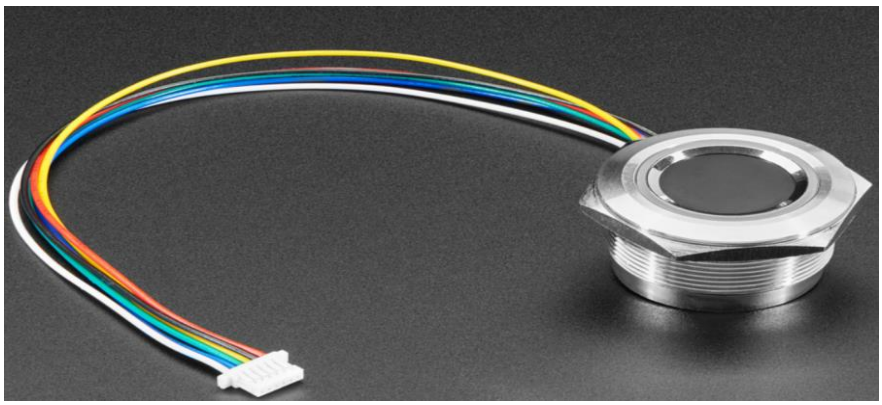
4.3. Module cảm biến vân tay R503(Fingprint r503)

4.3.1. Miêu tả vân tay R503(Fingprint r503)

Sử dụng công nghệ sinh trắc học để bảo vệ dự án của bạn - cảm biến vân tay quang học tất cả trong một ngày giúp bạn dễ dàng thêm tính năng nhận diện và xác

minh dấu vân tay. Nó thậm chí còn có một vòng đèn LED tích hợp xung quanh bàn phím phát hiện, có thể được đặt thành màu đỏ, xanh lam hoặc tím (và một số hiệu ứng mờ dần / nhấp nháy) để mang lại trải nghiệm người dùng cảm giác thú vị hơn.

Các mô-đun này thường được sử dụng trong két sắt - có một chip DSP công suất cao thực hiện việc kết xuất hình ảnh, tính toán, tìm kiếm đặc điểm và tìm kiếm. Kết nối với bất kỳ bộ vi điều khiển hoặc hệ thống nào có nối tiếp TTL và gửi các gói dữ liệu để chụp ảnh, phát hiện bản in, băm và tìm kiếm. Bạn cũng có thể đăng ký các ngón tay mới trực tiếp - có thể lưu trữ tối đa 200 dấu vân tay trong bộ nhớ FLASH tích hợp.



Hình 4.5. Cảm biến vân tay R503

4.3.1.1 Nguyên lí hoạt động

Nguyên lý hoạt động cảm biến vân tay cơ bản có 2 phần:

Lấy dữ liệu hình ảnh của vân tay: Khi lấy dữ liệu,người dùng cần phải thực hiện quét dấu vân tay hai lần thông qua cảm biến quang học.Hệ thống sẽ tiến hành thuật toán xử lý hình ảnh của 2 lần quét vân tay,tạo ra một khuôn mẫu của các vân tay dựa trên kết quả xử lý và lưu lại các bản mẫu

So sánh dấu vân tay(có thể theo chế độ 1:1 hoặc 1:N): Khi người dùng thực hiện quét dấu vân tay,module sẽ chụp lại hình ảnh dữ liệu vân tay và so sánh với các mẫu vân tay đã được lưu trữ sẵn trong thư viện.Đối với 1:1,hệ thống sẽ trực tiếp so sánh vân tay với mẫu được chỉ định cụ thể trong module,đối với 1:N hoặc tìm kiếm,hệ thống sẽ tìm kiếm trong thư viện để tìm vân tay phù hợp.Sau đó trả về kết quả đúng nếu trùng khớp hoặc sai nếu không trùng khớp với dữ liệu đã được lưu trữ

4.3.1.2 Các đặc tính

Module tích hợp nhiều loại chip xử lí trong cùng 1 module : cảm biến vân tay quang học,bộ vi xử lý DSP tốc độ cao,bộ nhớ FLASH...

Dễ dàng sử dụng với các tính năng bảo mật cao,thông minh.Mức độ bảo mật điều chỉnh được: thích hợp cho các ứng dụng khác nhau,mức độ bảo mật có thể được thiết lập bởi người sử dụng

Người dùng có thể kết hợp với các module khác để làm ra một loạt sản phẩm cuối cùng,chẳng hạn như kiểm soát quyền truy cập,điểm danh vào lớp học và chấm công,két an toàn ,khóa cửa nhà hay xe.

Tiêu thụ điện năng thấp,giá thành không cao,kích thước nhỏ gọn,hiệu năng tuyệt vời

Khả năng chống tĩnh điện mạnh mẽ,xử lí hình ảnh tốt.

4.3.1.3 Chi tiết kỹ thuật

Thông số kỹ thuật:

• Mô hình: R503

• Mô-đun vân tay điện dung

• Giao diện: TTL UART

• Độ phân giải: 508 DPI

• Điện áp: 3.3VDC

• Dung lượng: 200 dấu vân tay

• Mảng cảm biến: 192x192 pixel

• Làm việc hiện tại: 20mA

• Dòng điện chờ: Điện áp chờ cảm ứng điển hình: 3,3V, Dòng điện trung bình: 2uA

• Kích thước mô-đun: 28mm (đường kính ngoài) / 23,5mm (đường kính trong)

• Chiều cao mô-đun: 15,5mm

• Vùng cảm biến: 15,5mm

• Màu sắc LED: Xanh lam và đỏ

• Tốc độ quét: <0,2 giây

• Tốc độ xác minh: <0,3 giây

• Phương pháp so khớp: 1: 1; 1: N

• FRR: ≤1%

• FAR: ≤0,001%

• Môi trường làm việc: -20ºC - 60ºC

• Độ ẩm làm việc: 10-85%

• Công suất chống tĩnh điện: 15KV

• Cường độ chống mài mòn: 1 triệu lần

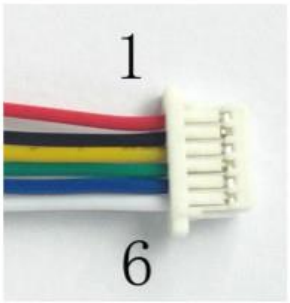
• Tốc độ baud truyền thông (UART): (9600 × N) bps trong đó N = 1 ~ 12 (mặc định là 57600bps)

Trọng lượng : 35.0g / 1.2oz

4.3.1.4 Giao tiếp phần cứng

Cảm biến vân tay R503 có tất cả 6 chân ,như các chân cấp nguồn với điện áp hoạt động ở mức 3.3V,các chân truyền và nhận tín hiệu từ cảm biến.

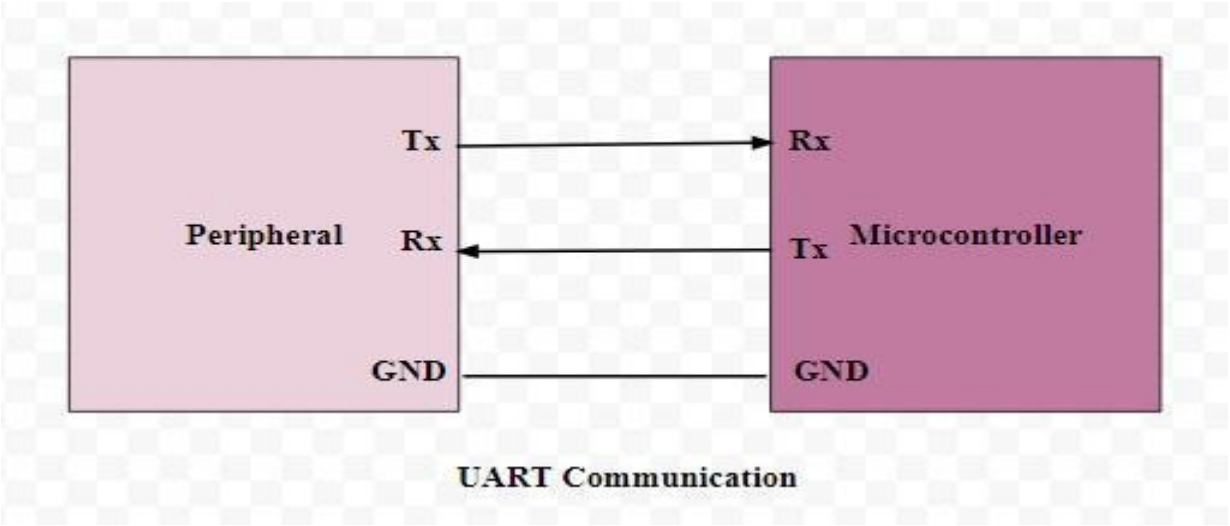
Connector: MX1.0--6P

Pin	Name	Description	Pic
1	Power Supply	DC3.3V	
2	GND	Signal ground. Connected to power ground.	
3	TXD	Data output. TTL logical level	
4	RXD	Data input. TTL logical level	
5	WAKEUP	Finger Detection Signal	
6	3.3VT	Touch induction power supply, DC3—6V	

Hình 4.6. Các chân cảm biến R503

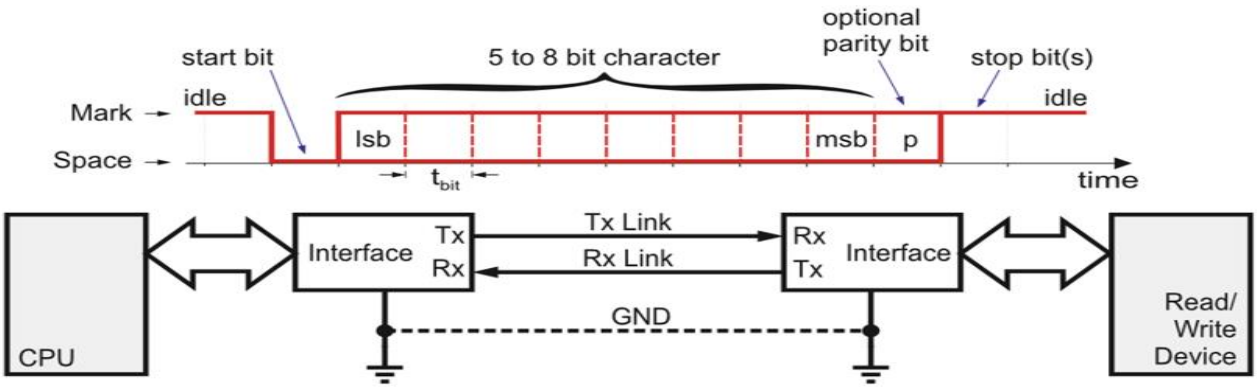
4.3.1.5 Giao thức truyền thông nối tiếp không đồng bộ UART(Universal Asynchronous Receiver / Transmitter)

UART hay Universal Asynchronous Receiver Transmitter là giao tiếp nối tiếp được chuyển đổi từ giao tiếp song song – quá trình chuyển đổi này được thực hiện trước khi truyền ở thiết bị truyền và sau khi nhận ở thiết bị nhận dữ liệu. Nó là giao tiếp phổ biến tại vì các thông số như: tốc độ truyền, kiểu dữ liệu,… đều có thể thay đổi được.



Hình 4.7. Sơ đồ khối truyền dữ liệu giữa 2 thiết bị

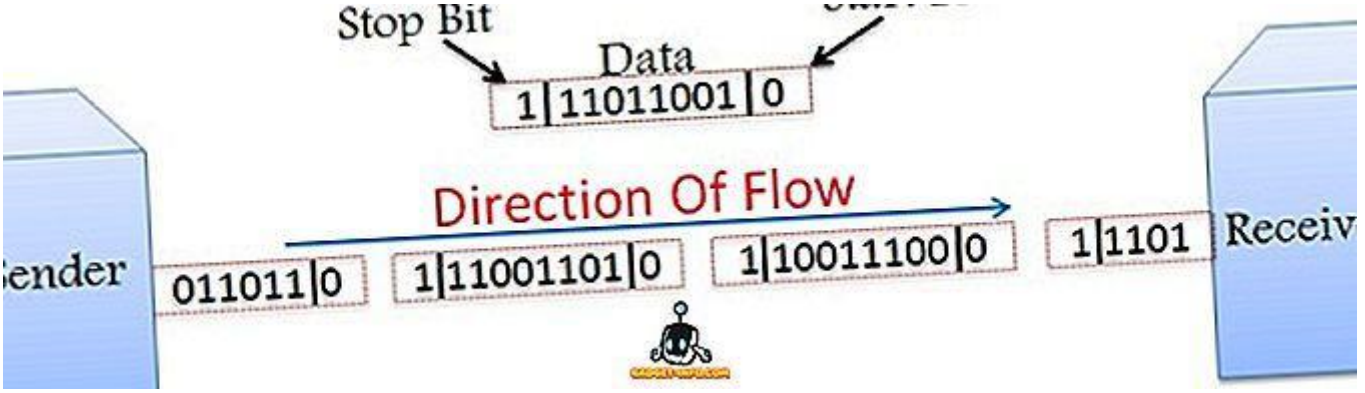
Trong giao tiếp UART cơ bản, thiết bị truyền và thiết bị nhận giao tiếp theo cách thức như sau: Phần cứng – hardware- UART sẽ chuyển đổi dữ liệu song song nhận được từ vi xử lý, vi điều khiển và chuyển chúng thành dữ liệu nối tiếp. Dữ liệu nối tiếp này sẽ được truyền đến thiết bị nhận và tại đây, hardware UART sẽ chuyển đổi ngược lại thành dữ liệu song song để truyền về vi điều khiển, vi xử lý của thiết bị nhận.



Hình 4.8. Giao thức truyền thông R503

Các chân sử dụng cho giao tiếp UART được gọi là TX ở thiết bị truyền và RX ở thiết bị nhận. Đồng thời, có các thanh ghi – shift registers – được hiểu như là một phần của UART hardware (2 loại thanh ghi được sử dụng ở đây là: Transmitter Shift Register và Receiver Shift Register).

Trong dữ liệu Truyền không đồng bộ chảy ở chế độ song công, 1 byte hoặc một ký tự tại một thời điểm. Nó truyền dữ liệu trong một luồng byte liên tục. Nói chung, kích thước của một ký tự được gửi là 8 bit được thêm vào một bit chẵn lẻ, tức là một bit start và bit stop cung cấp tổng cộng 10 bit. Nó không yêu cầu đồng hồ để đồng bộ hóa; thay vào đó, nó sử dụng các bit chẵn lẻ để cho người nhận biết cách diễn giải dữ liệu.



Hình 4.9. Truyền dữ liệu trên 1 byte

Nó đơn giản, nhanh chóng, tiết kiệm và không cần giao tiếp 2 chiều. Thư, email, diễn đàn, TV và radio là một số ví dụ về Truyền không đồng bộ.

4.3.1.6 Giao thức truyền gói dữ liệu

Khi module R503 thực hiện việc giao tiếp,truyền và nhận các câu lệnh dữ liệu,kết quả thì tất cả được định dạng qua 1 gói dữ liệu được thể hiện chi tiết:

Tên	Ký hiệu	Độ dài	Mô tả
Header	START	2 bytes	Có 2 byte được truyền đầu tiên trong gói dữ liệu. Được mặc định giá trị 0xEF01.
Adder	ADDER	4 bytes	Có 4 byte địa chỉ của module. Giá trị mặc định ban đầu là 0XFFFFFFFF, nhưng nó có thể được sửa đổi bởi lệnh. Byte cao sẽ được chuyển vào đầu tiên và nếu giá trị adder sai, module sẽ từ chối để chuyển.
Package indentifier	PID	1 bytes	Định dạng loại gói dữ liệu 0x01: Gói lệnh. 0x02: Gói dữ liệu. 0x07: Gói xác nhận. 0x08: Gói kết thúc dữ liệu.
Package length	LENGTH	2 bytes	Chiều dài gói dữ liệu tính từ Package content đến Checksum. Đơn vị chiều dài là byte (tối đa 256 bytes).
Package contents	DATA	-	Nội dung dữ liệu. Có thể là lệnh, dữ liệu, kết quả được xác nhận...(như giá trị ký tự dấu vân tay).
Checksum	SUM	2 bytes	Là tổng số học của Package identifier, Package length, Package content. Bit tràn được bỏ qua, bit cao được truyền đầu tiên.

Hình 4.10. Định dạng gói dữ liệu

4.3.1.7 Kiểm tra và xác nhận gói dữ liệu

Mô tả ý nghĩa các lệnh:

0x00:thực hiện lệnh hoàn tất hoặc ok

0x01:lỗi nhận gói tin

0x02:không có ngón tay trên cảm biến

0x03:hình ảnh dấu vân tay đầu vào không thành công

0x06:hình ảnh dấu vân tay quá lộn xộn

0x07:hình ảnh vân tay bình thường nhưng quá ít điểm đặc trưng

0x08:dấu vân tay không trùng khớp

0x09:không tìm thấy dấu vân tay

0x0a:hợp nhất đặc điểm không thành công

0x0b:số seri địa chỉ truy cập cở sở dữ liệu vân tay ngoài phạm vi của cơ sở dữ liệu vân tay

0x0c:đọc mẫu từ cơ sở dữ liệu vân tay bị lỗi hoặc không hợp lệ

0x0d:cho biết các đặc điểm tải lên không thành công

0x0e:mô đun không thể chấp nhận các gói tiếp theo

0x0f:hình ảnh tải lên không thành công

0x10:xóa mẫu không thành công

0x11:cơ sở dữ liệu dấu vân tay trống không thành công

0x13:mật khẩu không chính xác

0x15:vùng đệm không có hình ảnh gốc hợp lệ

0x18:đọc và ghi lỗi FLASH

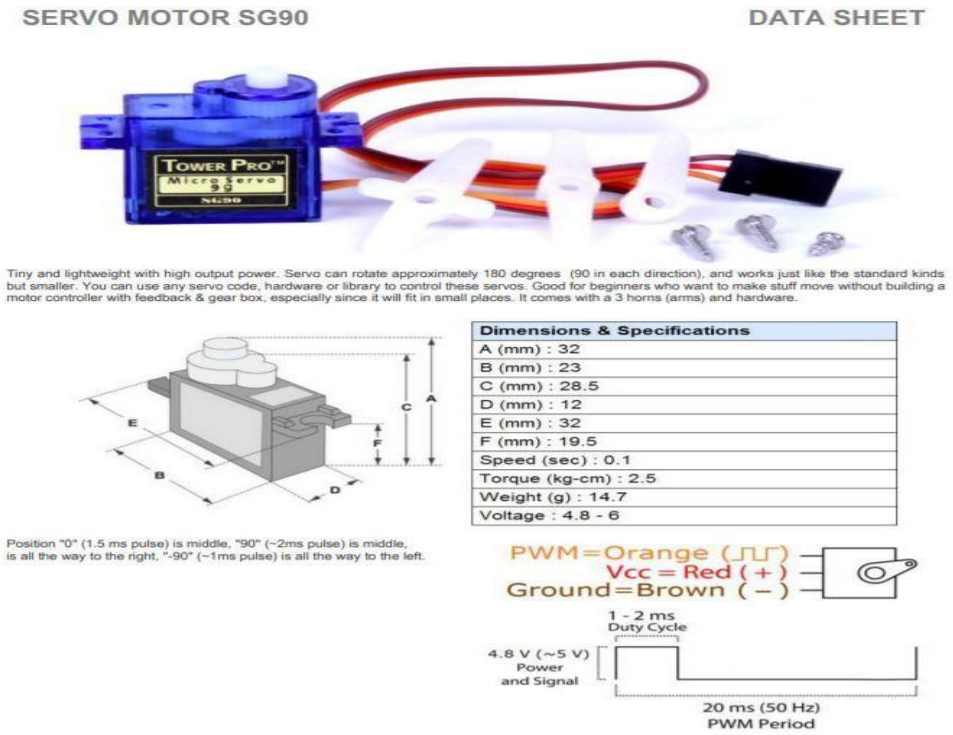
0x1a:số đăng kí không hợp lệ

0x20:sai mã địa chỉ

0x21:phải xác minh mật khẩu

others:dự phòng

4.3.1.8 Giới thiệu động cơ servo SG90 micro



Hình 4.11. Servo sg90 micro

4.3.1.9 Thông số kỹ thuật của Servo sg90 micro

Khối lượng:9g

Kích thước:22.2x11.8.32mm

Momen xoắn:1.8kg/1cm

Tốc độ hoạt động:60 độ trong 0.1s

Điện áp hoạt động:4.8V-5V

Nhiệt độ hoạt động:0-55˚C

4.3.1.10 Điều khiển và kết nối:

Kết nối dây màu đỏ với 5V,dây màu nâu với mass,dây màu cam với chân phát xung của vi điều khiển.Ở chân xung cấp cấp 1 xung từ 1ms-2ms theo để điều khiển góc quay mong muốn.

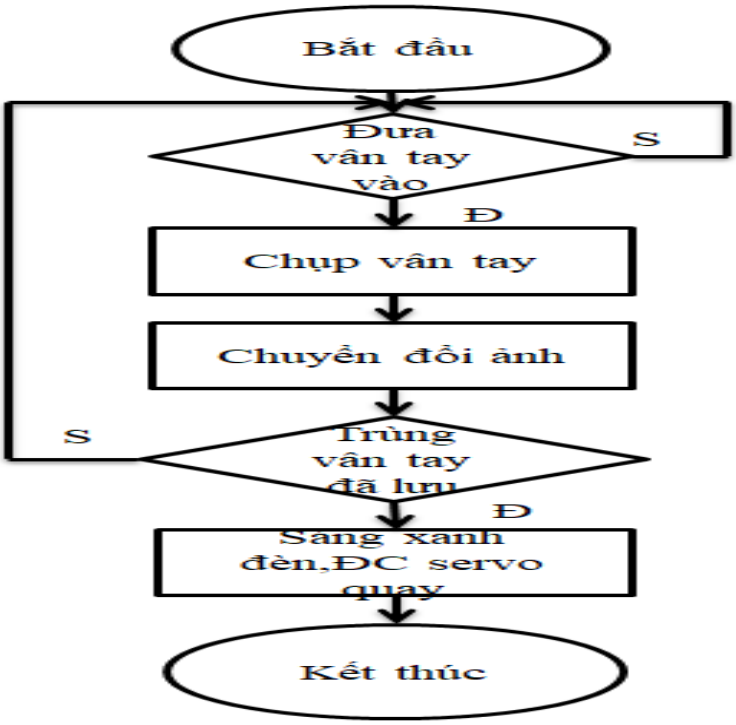
4.3.2. Lập trình hệ thống

Mục đích: Hệ thống sẽ thực hiện các chức năng như thêm dấu vân tay ,quét dấu vân tay xem trùng khớp với dấu vân tay đã lưu hay chưa ,xóa các dấu vân tay ko sử dụng nữa.

Lưu đồ giải thuật

Hệ thống thực hiện các chức năng là quét vân tay và thêm vân tay để quản lý người ra vào nhà.Sau khi quét vân tay,dữ liệu ID của người quét sẽ được lưu lại vào bộ nhớ ,thống kê danh sách.Hệ thống cho phép thêm vân tay và xóa vân tay dễ dàng.Khi cấp điện vào hệ thống,khởi động Arduino,cảm biến vân tay,servo...Sau khi khởi động xong ta thực hiện quét vân tay nếu trùng đèn led cảm biến sáng xanh ,servo quay và ngược lại

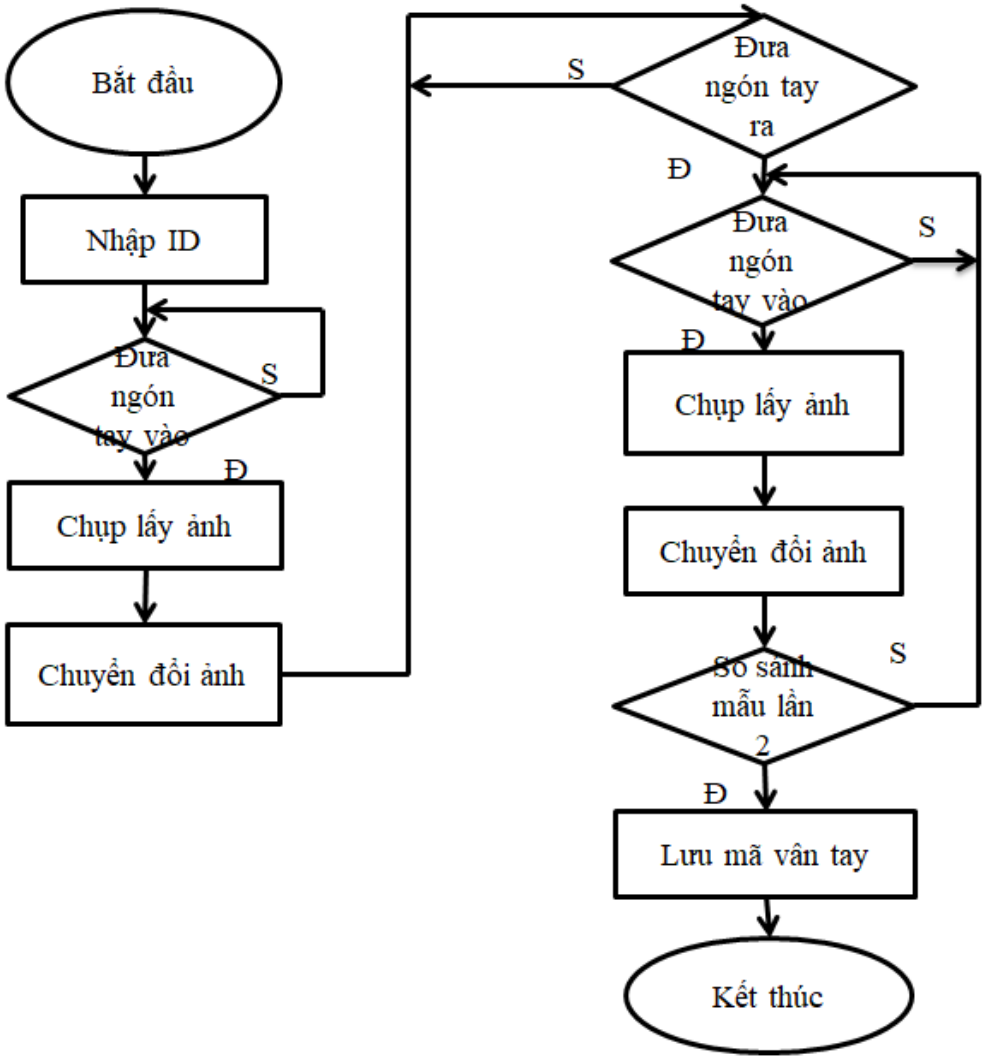
Lưu đồ quét vân tay:



Hình 4.12. Lưu đồ quét vân tay

Giải thích lưu đồ quét vân tay: Quá trình quét vân tay được thực hiện theo lưu đồ hình trên. Nếu vân tay trùng với vân tay đã lưu thì cảm biến sáng xanh đèn, servo quay thông báo đã quét vân tay thành công.

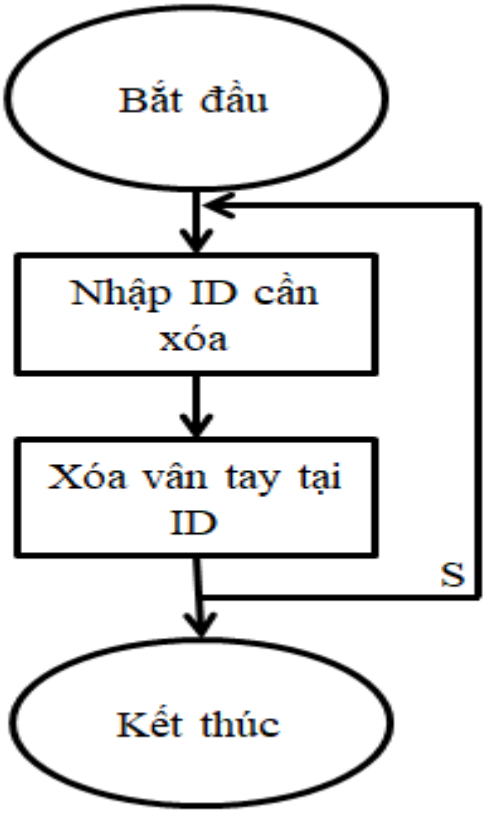
Lưu đồ thêm vân tay:



Hình 4.13. Lưu đồ thêm vân tay

Giải thích lưu đồ thêm vân tay: Quy trình lấy mẫu thêm vân tay người dùng được thực hiện như lưu đồ trên.Khi nhập ID nơi lưu trữ dấu vân tay thì cảm biến sẽ sáng trong khi đợi ta đưa vân tay vào.Ta đưa vân tay vào cảm biến để tiến hành lấy mẫu lần một và tương tự lần hai.Vân tay ta đưa vào lần thứ hai mà không giống lần một thì ta sẽ cho lấy đến khi nào trùng khớp thì lưu dấu vân tay lại.Tiếp tục lưu dấu vân tay với những mẫu khác tương tự như trên cho đến khi kết thúc việc lấy mẫu .

Lưu đồ xóa vân tay:



Hình 4.14. Lưu đồ xóa vân tay

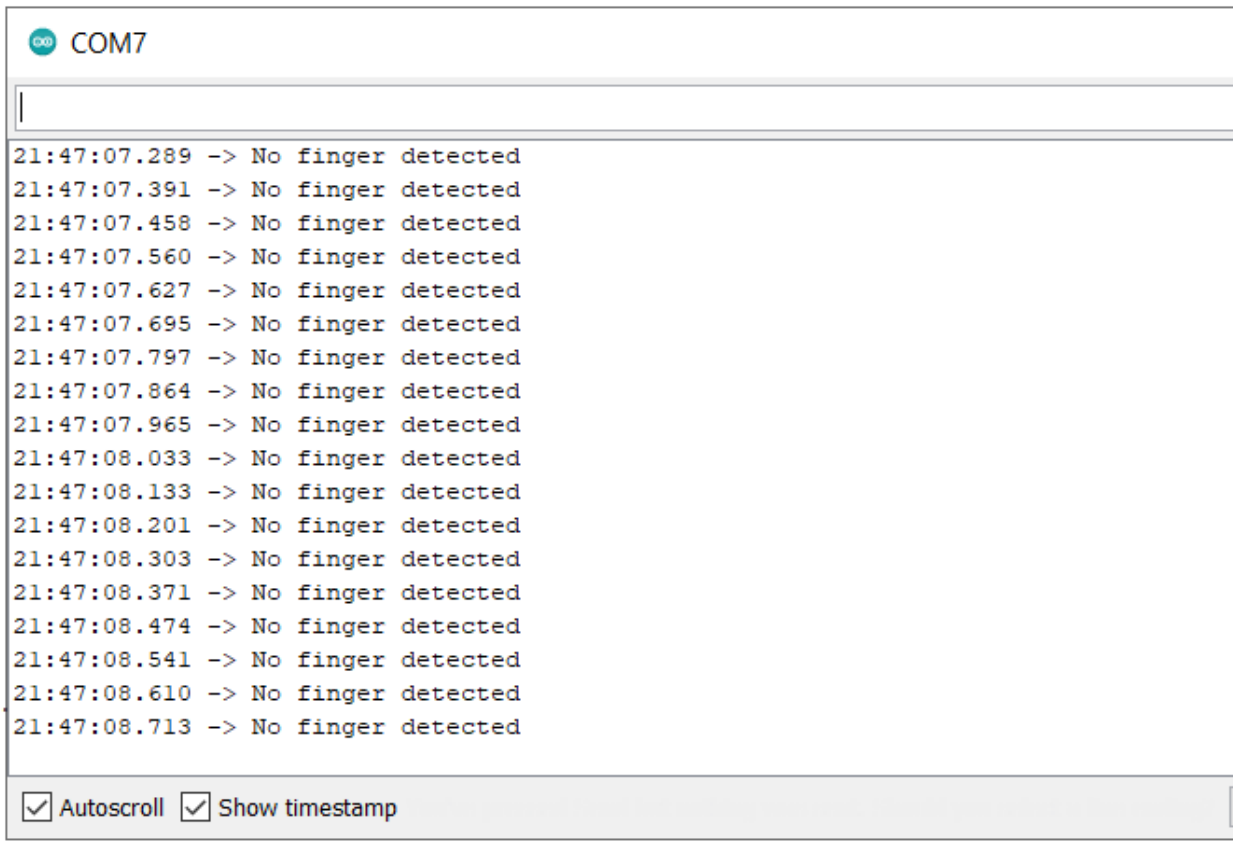
Giải thích lưu đồ xóa vân tay:Quy trình xóa vân tay người dùng như lưu đồ trên.Nhập ID cần xóa,thực hiện cho đến khi kết thúc chương trình cần xóa rồi quay về ban đầu.

4.3.3. Phần mềm lập trình cho vi điều khiển

4.3.3.1 Giới thiệu phần mềm lập trình Arduino IDE

Arduino IDE là phần mềm giúp ta lập trình cho các dòng sản phẩm của Arduino như Uno,mega,nano,...Lập trình trên Arduino IDE là cách tiếp cận đơn giản cho những người đam mê điện tử và muốn tạo ra sản phẩm nhúng ấn tượng mà không cần quá nhiều kiến thức chuyên sâu về điện tử.Môi trường phát triển tích hợp Arduino IDE là 1 ứng dụng đa nền tảng được viết bằng Java.

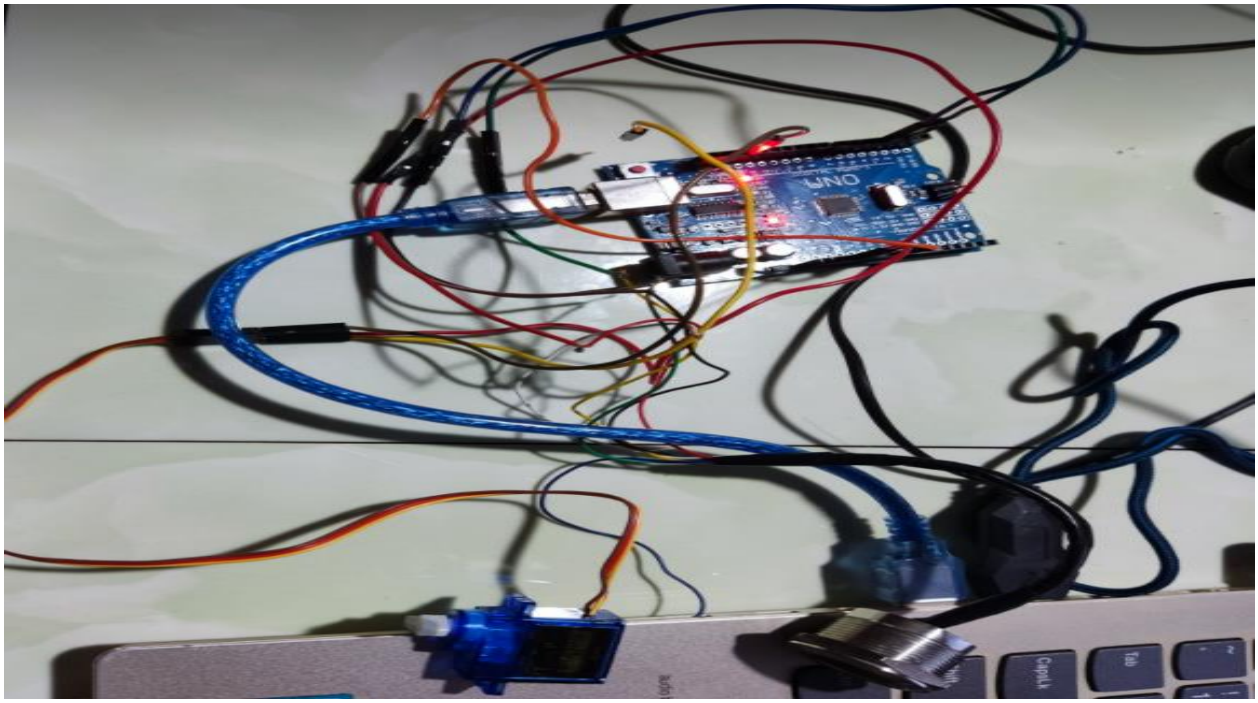
4.3.3.2 Thực hiện



Hình 4.15. Lấy dấu vân tay

```
773 -> No finger detected
342 -> No finger detected
945 -> No finger detected
014 -> No finger detected
319 -> Image taken
799 -> Image converted
970 -> Found a print match!
176 -> Found ID #1 with confidence of 164
245 -> No finger detected
347 -> No finger detected
415 -> No finger detected
518 -> No finger detected
586 -> No finger detected
556 -> No finger detected
760 -> No finger detected
328 -> No finger detected
932 -> No finger detected
```

Hình 4.16. Tìm thấy dấu vân tay trong thư viện



Hình 4.17. Board mạch kết nối arduino ,vân tay với servo

4.4. Khuôn mặt

4.4.1. Bài toán nhận dạng khuôn mặt

Nhận dạng là một bài toán quan trọng trong lĩnh vực Computer Vision, thuật toán nhận dạng khuôn mặt là một bài toán khá phức tạp, nó đòi hỏi một loạt các vấn đề cần thực hiện:

Việc làm đầu tiên đó là cần phải tìm kiếm tất cả những khuôn mặt có trong bức hình

Tập trung vào từng khuôn mặt chắc chắn rằng bạn có thể nhận ra cùng một người từ các góc nhìn hoặc điều kiện sáng tối khác nhau.

Lựa chọn những đặc trưng đặc trưng trên từng khuôn mặt -VD như đôi mắt to, khuôn mặt dài...

So sánh những đặc trưng này với những người khác để chúng ta có thể biết được tên của họ.

Giải quyết bài toán từng bước, ở mỗi bước sẽ có các thuật toán học máy khác nhau:

4.4.1.1 Tìm kiếm khuôn mặt (Face Detection):

Có thể thấy rõ đầu tiên chúng ta cần xác định vị trí của khuôn mặt có trong bức hình trước khi xác định người đó là ai.

Để tìm kiếm khuôn mặt trong một bức hình, ta cần làm cho bức hình trở thành ảnh đen trắng. Về cơ bản thì một bức ảnh màu không có tác dụng gì lắm cho việc xác định khuôn mặt

Sau đó, vẽ các vector chỉ hướng tối dần đi của các điểm ảnh của bức ảnh đen trắng đó. Tạo ra các khung tỉ lệ để xác định các đặc điểm cơ bản của khuôn mặt thông qua các vecto này

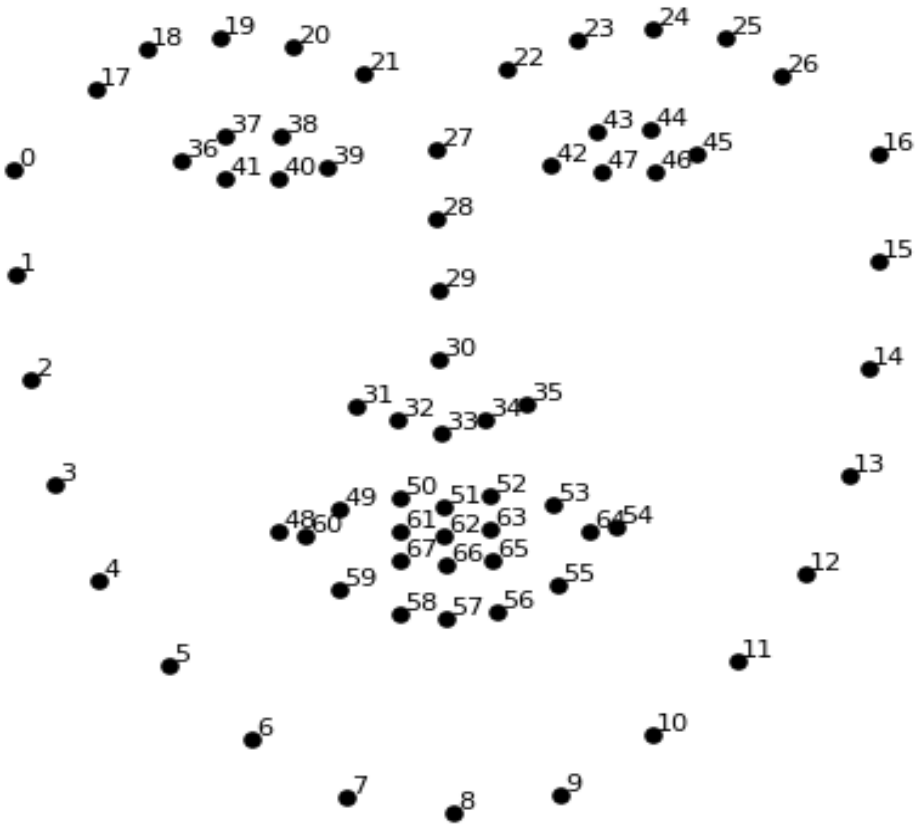
4.4.1.2 Trích rút đặc trưng (Feature Extraction):

Sau khi phát hiện ra khuôn mặt trong bức ảnh, chúng ta tiến hành trích rút những đặc trưng của khuôn mặt. Bước này trích xuất ra một vector đặc trưng đại diện cho một khuôn mặt. Nó phải đảm bảo được tính duy nhất của một khuôn mặt.

Có những khuôn mặt thì nghiêng sang trái, nghiêng sang phải, khiến bạn chỉ nhìn thấy một phần khuôn mặt của họ, hay có những bức hình thì lại hơi nghiêng đầu, khiến cho bức ảnh bị lệch khỏi khung nhìn. Do đó, chúng ta cần phải cố gắng làm cong bức hình để đôi mắt, bờ môi luôn ở vị trí mẫu trong ảnh. Điều này sẽ làm cho việc so sánh khuôn mặt ở các bước tiếp theo dễ dàng hơn nhiều.

Để làm điều này, chúng ta sẽ sử dụng một thuật toán được gọi là face landmark estimation. Ý tưởng cơ bản của thuật toán là tìm ra 68 điểm cụ thể (được gọi là mốc) tồn tại trên mỗi khuôn mặt - đầu cằm, cạnh bên ngoài của mỗi mắt, cạnh bên trong của mỗi lông mày ... Sau đó, chúng ta sẽ dùng một thuật toán machine learning để training để có thể tìm thấy 68 điểm cụ thể trên từng khuôn mặt.

Sau đó, chỉ cần xoay và cắt ảnh để mắt và miệng được căn giữa là xong



Hình 4.18. 68 điểm trong thuật toán face landmark estimation

4.4.1.3 Nhận dạng khuôn mặt (Face Recognition):

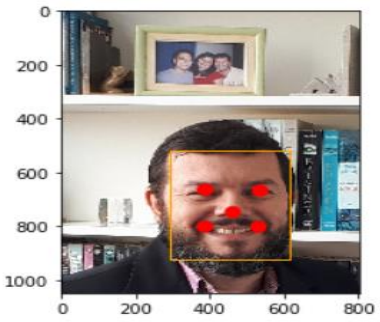
Với hình ảnh đầu vào sau khi phát hiện ra khuôn mặt, trích rút các đặc trưng của khuôn mặt và đem so sánh các đặc trưng này với cơ sở dữ liệu khuôn mặt

Phương pháp tiếp cận đơn giản nhất để nhận biết khuôn mặt là so sánh trực tiếp khuôn mặt mà chúng ta đã tìm được ở bước 2 với tất cả các hình ảnh của những người đã được training trước đó trong cơ sở dữ liệu. Kiểm tra các đặc điểm trên khuôn mặt rồi từ đó nhận diện được khuôn mặt người trong webcam là ai.

4.4.1.4 Xây dựng ứng dụng và triển khai cài đặt

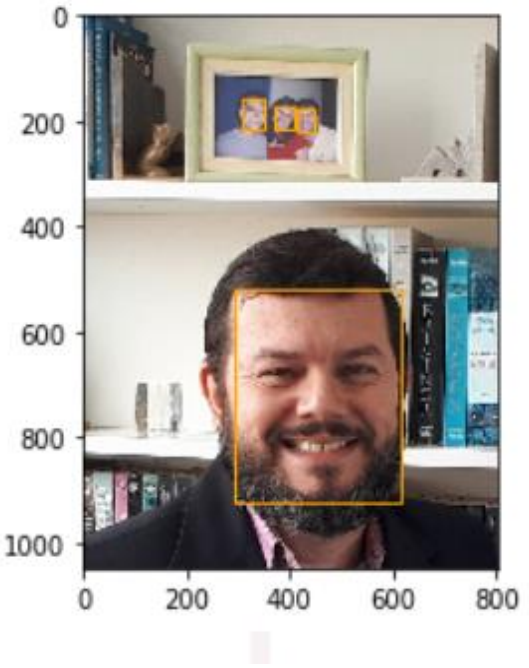
MTCNN là một thư viện Python được viết bởi người dùng. Nhận dạng khuôn mặt chung và căn chỉnh bằng cách sử dụng mạng nhiều dây xếp tầng. Nhận dạng khuôn mặt là một vấn đề về thị giác máy tính được sử dụng để tìm khuôn mặt trong ảnh, thông qua các kỹ thuật dựa trên tính năng cổ điển.

Nhận diện khuôn mặt là một vấn đề về thị giác máy tính được sử dụng để tìm khuôn mặt trong hình ảnh. Đây là một vấn đề nhỏ mà con người cần giải quyết, và nó đã được giải quyết một cách hợp lý thông qua các kỹ thuật dựa trên tính năng cổ điển (chẳng hạn như bộ phân loại tầng). Gần đây, các phương pháp học sâu đã đạt được kết quả tiên tiến nhất trên bộ dữ liệu nhận dạng khuôn mặt điểm chuẩn tiêu chuẩn. Một ví dụ là mạng nơ-ron tích tụ phân cấp đa nhiệm vụ, gọi tắt là MTCNN.



Hình 4.19. Ví dụ về hộp ranh giới MTCNN

```
# draw an image with detected objects
def draw_facebox(filename, result_list):
# load the image
data = plt.imread(filename)
# plot the image
plt.imshow(data)
# get the context for drawing boxes
ax = plt.gca()
# plot each box
for result in result_list:
# get coordinates
x, y, width, height = result['box']
# create the shape
rect = plt.Rectangle((x, y), width, height,fill=False, color='orange')
# draw the box
ax.add_patch(rect)
# draw the dots
for key, value in result['keypoints'].items():
# create and draw dot
dot = plt.Circle(value, radius=20, color='red')
ax.add_patch(dot)
# show the plot
plt.show()
# filename = 'test1.jpg' # filename is defined above, otherwise uncomment
# load image from file
# pixels = plt.imread(filename) # defined above, otherwise uncomment
# detector is defined above, otherwise uncomment
#detector = mtcnn.MTCNN()
# detect faces in the image
faces = detector.detect_faces(pixels)
# display faces on the original image
draw_facebox(filename, faces)
```



Hình 4.20: Vẽ hộp xung quanh khuôn mặt

```
def run_detection(fast_mtcnn, filenames):
frames = []
frames_processed = 0
faces_detected = 0
batch_size = 60
start = time.time()
for filename in tqdm(filenames):
v_cap = FileVideoStream(filename).start()
v_len = int(v_cap.stream.get(cv2.CAP_PROP_FRAME_COUNT))
for j in range(v_len):
frame = v_cap.read()
frame = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
frames.append(frame)
if len(frames) >= batch_size or j == v_len - 1:
faces = fast_mtcnn(frames)
frames_processed += len(frames)
faces_detected += len(faces)
frames = []
print(
f'Frames per second: {frames_processed / (time.time() - start):.3f},',
f'faces detected: {faces_detected}\r',
end=''
)
v_cap.stop()
run_detection(fast_mtcnn, filenames)
```

```
100% ████████████████████████████████████████ 100/100 [07:35<00:00, 4.56s/it]
Frames per second: 65.815, faces detected: 32681
```

Hình 4.21:Chạy script trích xuất khuôn mặt

Để bị xử lý hàng triệu bức ảnh, cần phải tăng tốc MTCNN, nếu không CPU sẽ bị cháy trước khi xử lý xong. Nếu chạy đoạn mã trên quá trình này sẽ mất khoảng một giây, sẽ xử lý khoảng một ảnh mỗi giây còn với việc chạy MTCNN trên GPU và sử dụng phiên bản tăng tốc, nó sẽ đạt được khoảng 60–100 hình ảnh / khung hình một giây.

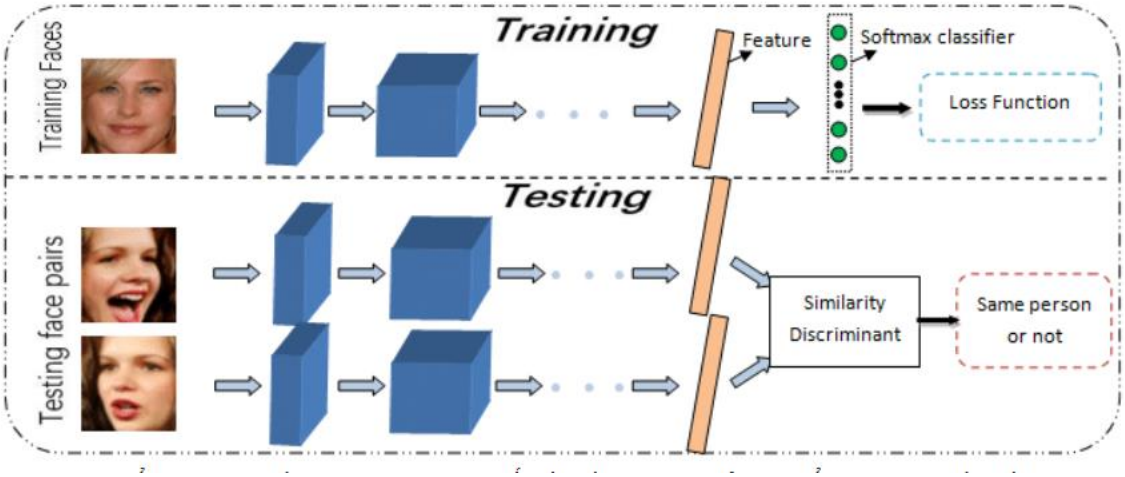
4.4.2. Trích rút đặc trưng(arcface)

4.4.2.1 Nhúng tính năng

Một CNN điển hình được sử dụng để phân loại bao gồm trích xuất và phân loại đối tượng địa lý. Trong quá trình đào tạo, người mẫu sẽ học các đặc điểm khuôn mặt độc đáo và tạo các nhúng đặc trưng trong quá trình trích xuất đặc điểm. Sau khi quá trình đào tạo hoàn tất, bạn có thể bỏ qua việc phân loại và tạo các tính năng nhúng cho từng hình ảnh khuôn mặt, chẳng hạn như "dấu vân tay" kỹ thuật số.

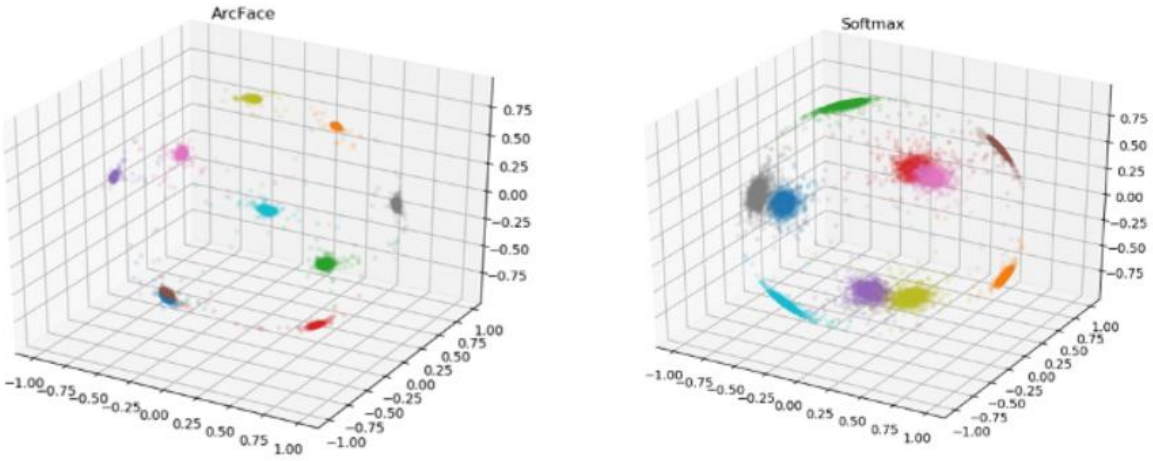
Độ giống nhau về vectơ của hai ảnh khác nhau của cùng một người là cao nhưng khoảng cách nhỏ và độ giống nhau của hai ảnh khác nhau là thấp nhưng bình phương khoảng cách lớn.

Sau khi chúng tôi phát hiện và cắt khuôn mặt, chúng tôi có thể xử lý nó thông qua mô hình arc face, mô hình này sẽ tạo ra hai tính năng được nhúng. Khi chúng ta có được hai vectơ nhúng, chúng ta sẽ có thể tính toán độ tương đồng cosine hoặc khoảng cách bình phương giữa chúng và xác định xem hai hình ảnh có thuộc về cùng một người hay không.



Hình 4.22:Quy trình chung để xác minh khuôn mặt

So sánh SoftMax và Arc Face :Trong mạng phân loại tiêu chuẩn, SoftMax và Loss of Categorical Cross Entropy thường được sử dụng ở cuối mạng. SoftMax chuyển đổi số thành xác suất. Đối với mỗi đối tượng, cho một xác suất để mỗi lớp có tổng là 1. Huấn luyện hoàn tất, lớp có xác suất cao nhất được chọn. Categorical Loss Cross Entropy tính toán sự khác biệt giữa hai phân phối xác suất và được giảm thiểu trong quá trình truyền ngược trong quá trình huấn luyện. Nhược điểm của SoftMax là nó không tạo ra một giới hạn an toàn, có nghĩa là các đường viền hơi mờ. Chúng ta muốn vectơ của hai ảnh của cùng một người càng giống nhau càng tốt và vectơ của hai ảnh của hai người khác nhau. Càng khác biệt càng tốt.



Hình 4.23: Tính năng nhúng các chữ số MNIST

Chúng ta thấy các đơn vị nhúng chữ số MNIST. Cần lưu ý rằng giới hạn của các chức năng SoftMax tương đối mờ so với các chức năng Arc Face được nhúng: Thay vì sử dụng khoảng cách Euclide, Arc Face tính toán khoảng cách trắc địa trong siêu cầu. không gian là không gian trong đó tất cả các khoảng cách được đo bằng đường ray. Đường thu được giữa hai điểm được gọi là đường trắc địa. Mô tả khoảng cách ngắn nhất. giữa các điểm, còn được gọi là khoảng cách trắc địa.

Hàm mất mát Arc Face:

$$-\frac{1}{N}\sum_{i=1}^{N} \quad log\frac{e^{S*(coscos\,(\theta_{y_i}+m)}}{e^{S*(coscos\,(\theta_{y_i}+m)} + \sum_{j=1,j\neq 1}^{n} \quad e^{S*coscos\,\theta_j}}$$

4.4.2.2 Kết luận

Trên thực tế, việc mất Arc face thay đổi logit khỏi SoftMax và do sự tương ứng chính xác với việc loại bỏ quốc gia trên Siêu cầu và tiêu chuẩn hóa có tính năng giải thích rõ ràng về hình học và các tính năng được tiêu chuẩn hóa, sự mất mát của Arc Face tươi của Biên độ tối đa, là biên giới quyết định trong những người được hỏi.

4.4.3. Thuật toán tìm kiếm(Faiss)

Faiss là một thư viện sử dụng tính năng tìm kiếm sự giống nhau kết hợp với nhóm vectơ. Faiss được nghiên cứu và phát triển bởi nhóm nghiên cứu AI của Facebook; Được viết bằng C ++ và được đóng gói trong môi trường Python. Thư viện bao gồm các thuật toán tìm kiếm vectơ đa chiều trong việc tìm kiếm các điểm tương đồng. Tìm điểm tương đồng Hiện nay, phương pháp phổ biến nhất để tìm hình ảnh là tìm điểm tương đồng. tạo cấu trúc dữ liệu từ RAM. Sau đó, một vectơ mới xx được tính.

Hiện nay, phương pháp phổ biến nhất trong Image Retrieval là dùng Similarity

$i = argmin_{i||x-x_i||} i = argmin_i ||x - x_i||$

Trong Faiss, đây được gọi là tạo ra *index*, một object có khả năng add các vector x-i*xi*

Phần tính toán argmax argmin, được gọi là tìm kiếm chỉ mục Faiss, cho phép: Trả về nhiều kết quả tương tự Tìm kiếm nhiều vectơ cùng một lúc (còn được gọi là xử lý hàng loạt) Chọn giữa độ chính xác và tốc độ (độ chính xác). Ví dụ: bạn có thể giảm độ chính xác 10% để tăng tốc độ lên 10 lần hoặc giảm bộ nhớ đi 10 lần. Khoảng cách Euclidean L2 là Index Flash L2.

Tìm kiếm

- Bước đầu tiên là xử lý ảnh: đọc ảnh
- Resize về kích thước đầu vào của mạng (384, 384)
- Trích xuất ra feature vector 128 chiều qua mạng CNN
- Search và đưa ra top khung ảnh có distance nhỏ nhất

Kết luận:

Model hoạt động tốt nhưng vẫn còn có thể cải tiến:

Saliency sẽ detect chủ thể của bức ảnh nên nếu ví dụ bức ảnh chụp hoa có ong hoặc động vật khác, rất có thể chúng ta sẽ không thu được ảnh crop chuẩn => Thực hiện flower classify trước khi đưa vào saliency.Độ chính xác được cải thiện thêm khi áp dụng kỹ thuật dropout.

4.4.4. Face Detection với MTCNN

4.4.4.1 Detect Face bằng OpenCV và MTCNN

Trước hết, ta cần khai báo thư viện và check xem sẽ sử dụng CPU hay GPU. Thực tế cho thấy mạng MTCNN rất nhẹ, có thể dễ dàng chạy trên GPUcủa Raspbery.

face.py > ...

```
1   import numpy as np
2   import cv2
3   import MNN
4   import sys
```

Hình 4.24. Khai báo thư viện MNN

Tiếp theo, ta sẽ gọi 1 object từ class MTCNN đi kèm 1 số config như sau:

```
mtcnn = MTCNN(thresholds= [0.7, 0.7, 0.8] ,keep_all=True, device = device)
```

Hình 4.25. Hiển thị độ chính xác

Thresholds chính là mức thresholds cho 3 lớp mạng P, R và O. Mặc định là [0.6, 0.6, 0.7] nhưng vì muốn tăng độ chính xác nên truyền vào mức 3 cao hơn như trên. Keep_all để xác định việc chúng ta có detect hết và trả về tất cả mặt có thể trong bức hình hay không.

Về việc load video từ webcam, ta sẽ sử dụng hàm cv2.VideoCapture() của OpenCV để gọi webcam và ghi lại từng frame ảnh. Set cho kích thước của webcam về theo kích thước mong muốn và tiến hành khoanh box cho từng frame:

```
cap = cv2.VideoCapture(0)
cap.set(cv2.CAP_PROP_FRAME_WIDTH,640)
cap.set(cv2.CAP_PROP_FRAME_HEIGHT,480)
while cap.isOpened():
    isSuccess, frame = cap.read()
    if isSuccess:
        boxes, _ = mtcnn.detect(frame)
        if boxes is not None:
            for box in boxes:
                bbox = list(map(int,box.tolist()))
                frame = cv2.rectangle(frame,(bbox[0],bbox[1]),(bbox[2],bbox[
    cv2.imshow('Face Detection', frame)
    if cv2.waitKey(1)&0xFF == 27:
        break
```

Hình 4.26. Face detect với ảnh

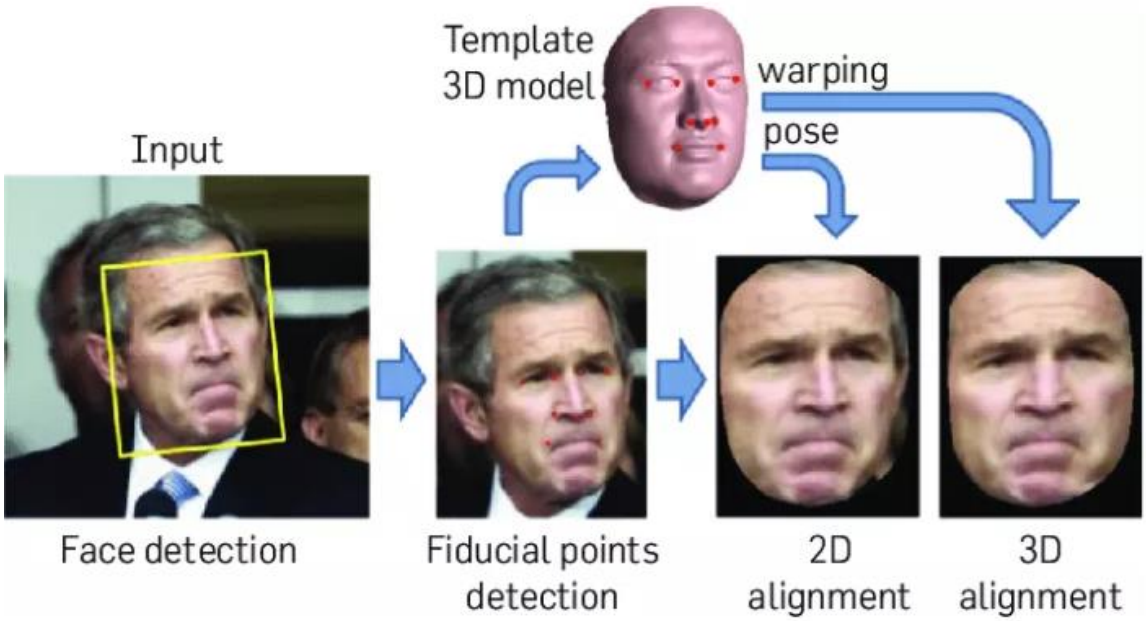
4.4.4.2 Capture Face

Phần code của Capture sẽ không khác gì lắm so với phần Detect, chỉ thêm vào một số biến như *count* - dùng để đếm số lượng ảnh; *leap* - bước nhảy, tức máy sẽ lấy ảnh sau mỗi frame.

```
import cv2
from facenet_pytorch import MTCNN
import torch
from datetime import datetime
import os

device =  torch.device('cuda:0' if torch.cuda.is_available() else 'cpu')
print(device)

IMG_PATH = './data/test_images/'
count = 50
usr_name = input("Input ur name: ")
USR_PATH = os.path.join(IMG_PATH, usr_name)
leap = 1

mtcnn = MTCNN(margin = 20, keep_all=False, post_process=False, device = dev
cap = cv2.VideoCapture(0)
cap.set(cv2.CAP_PROP_FRAME_WIDTH,640)
cap.set(cv2.CAP_PROP_FRAME_HEIGHT,480)
while cap.isOpened() and count:
    isSuccess, frame = cap.read()
    if mtcnn(frame) is not None and leap%2:
        path = str(USR_PATH+'/{}.jpg'.format(str(datetime.now())[:-7].repla
        face_img = mtcnn(frame, save_path = path)
        count-=1
    leap+=1
    cv2.imshow('Face Capturing', frame)
    if cv2.waitKey(1)&0xFF == 27:
        break
```

Hình 4.27 Crop ảnh theo từng id

Ta sẽ không dùng hàm detect() có trong class nữa, mà dùng hàm forward thẳng qua class. Hàm này sẽ trả về ảnh dựa trên 2 tọa độ góc của box chứa mặt người, sau khi đã crop&resize ảnh về đúng kích thước đầu ra mong muốn của mạng FaceNet



Hình 4.28 Face Alignment dựa theo phương pháp 2D Alignment và 3D Alignment

4.4.5. Xây dựng ứng dụng

4.4.5.1 Mô hình tổng quan

Mô hình tổng thể của hệ thống bao gồm:

- Tạo face.py dùng để nhận diện
- Tạo DatabaseManagement.py sử dụng để training dữ liệu
- Tạo lớp config.py để lấy dữ liệu

4.4.5.2 Xây dựng chi tiết ứng dụng

4.4.5.3 Lấy ID qua từng Khung ảnh

```
105     def find(self,vector):
106         idx,d  (parameter) self: Self@DatabaseManager
107         ID = self.index2ID(str(idx[0]))
108         name = self.id2Name(str(ID))
109         return name, distance[0], idx[0], ID
110
111     def index2ID(self,index):
112         return self.__index2id[index]
113
114     def id2Name(self,ID):
115         return self.__id2name[ID]
```

Hình 4.29. Train dữ liệu lấy id

Hình 4.30. Dữ liệu khuôn mặt

4.4.5.4 Tạo lớp training dữ liệu

Toàn bộ file code DatabaseManagement.py

DatabaseManagement.py > get_json_dict

```python
from FaceSearch import FaceSearch
import os
import numpy

def get_json_dict(path):
    import os
    from os.path import exists
    from json import load

    if exists(path):
        with open(path, 'r',encoding='utf-8') as _f:
            try:
                data = load(_f)
                print('Load from {} succesfully'.format(path))
                return data
            except:
                print("File is an empty structure")
                return {}
    else:
        return {}

def write_json_dict(path,data_dict):
    import json
    with open(path, 'w+', encoding='utf-8') as f:
        json.dump(data_dict, f, ensure_ascii=False, indent=4)


class DatabaseManager():
    def __init__(self,config):
        if config.bin_path is not None:
            self.core = FaceSearch(index_path = config.bin_path)
        else:
            self.core = FaceSearch()
```

Hình 4.31. Code train dữ liệu

4.4.5.5 Lớp DatabaseManagement.py nhận diện khuôn mặt đã training

```
        if name in self.__id2name.values(): # current name is existed in database
            # if face (from file_path) is not extracted => save to name
            # Else skip
            if file_path not in self.__index2path.values():
                self.__index2id[len(self.__index2id)] = currentID
                self.__index2path[len(self.__index2path)] = file_path
                embeddings.append(emb)
                print('Exist ID - New Path {}: index:{} - ID: {} - name: {} <-> process at path {}'.format(currentID,len(self.__index2id),len(sel

            else:
                print('Exist ID, Exist Path - {}: index:{} - ID: {} - name: {} <-> process at path {}'.format(currentID,len(self.__index2id),len(
        else:
            print('---------------New user found')
            currentID += 1
            self.__index2id[len(self.__index2id)] = currentID
            self.__index2path[len(self.__index2path)] = file_path
            self.__id2name[currentID] = name
            print('New ID - New Path {}: index:{} - ID: {} - name: {} <-> process at path {}'.format(currentID,len(self.__index2id),len(self.__id
            embeddings.append(emb)

        # self.core.addVectorAndIndexing(embeddings)
        write_json_dict(self.config.id2name_path,self.__id2name)
        write_json_dict(self.config.index2id_path,self.__index2id)
        write_json_dict(self.config.index2path_path,self.__index2path)
    print(len(embeddings),len(self.__index2path),len(self.__index2id))
    embeddings = numpy.concatenate(embeddings,axis=0)
    self.core.addVectorAndIndexing(embeddings)
    self.core.saveBin('library_face.bin')
```

Hình 4.32. Code train dữ liệu theo từng id

4.4.6. Chạy ứng dụng và kiểm tra kết quả

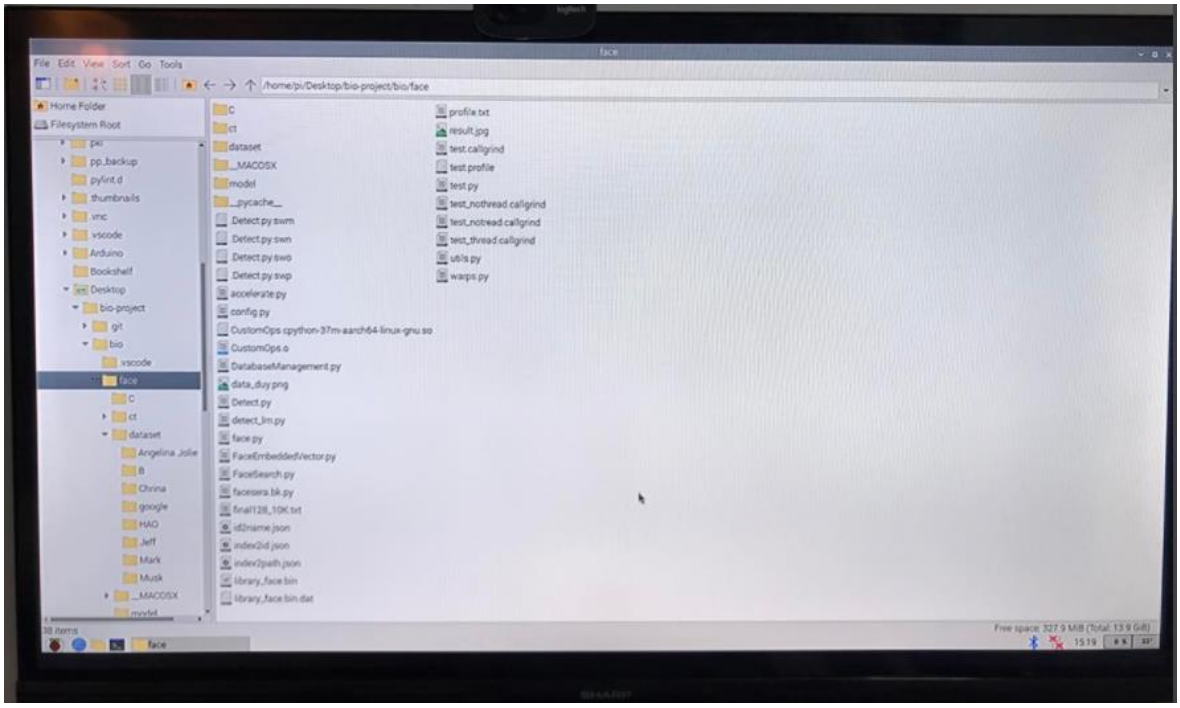
4.4.6.1 Chạy ứng dụng

Đầu tiên, ta chạy file config.py

```
config.py > ...
1   id2name_path = 'id2name.json'
2   index2id_path = 'index2id.json'
3   index2path_path = 'index2path.json'
4   bin_path = 'library_face.bin'
5   # bin_path = None
```

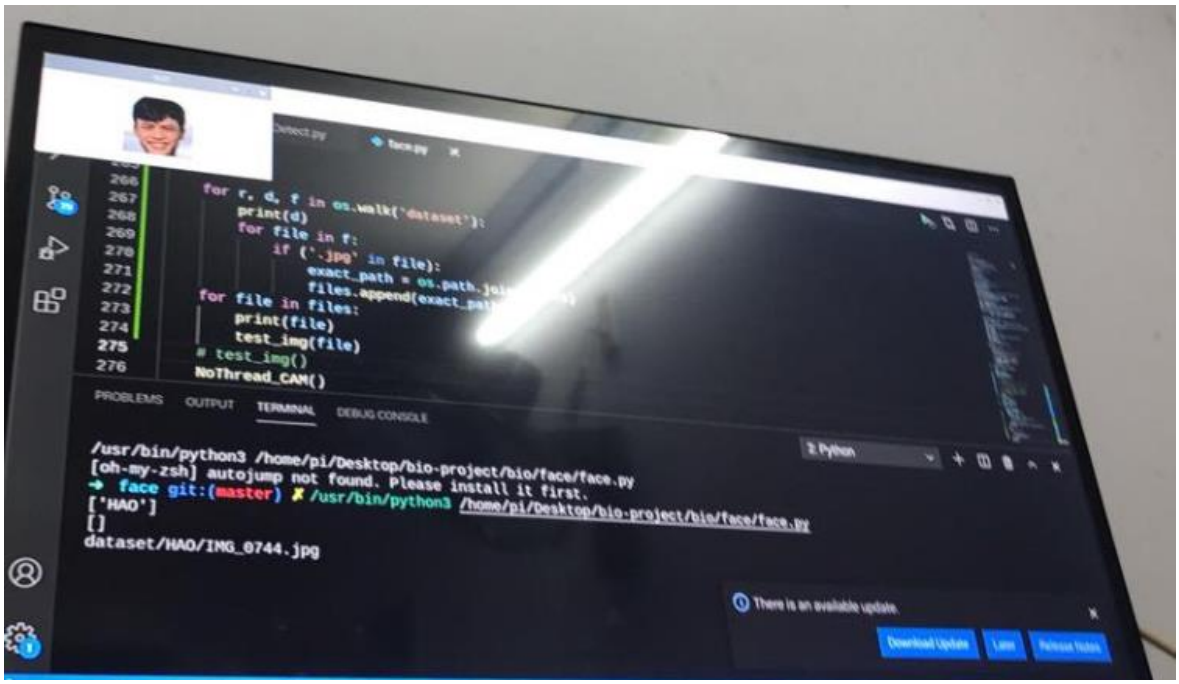
Hình 4.33. Code đưa dữ liệu vào

Sau khi lấy dữ liệu xong thì dữ liệu tập hợp các bức ảnh chụp khuôn mặt người nhận diện sẽ ở trong thư mục datashet:



Hình 4.34. File ảnh

Tiếp đến, chạy file DatabaseManagement.py để training dữ liệu các khuôn mặt đã được lấy ở trên:

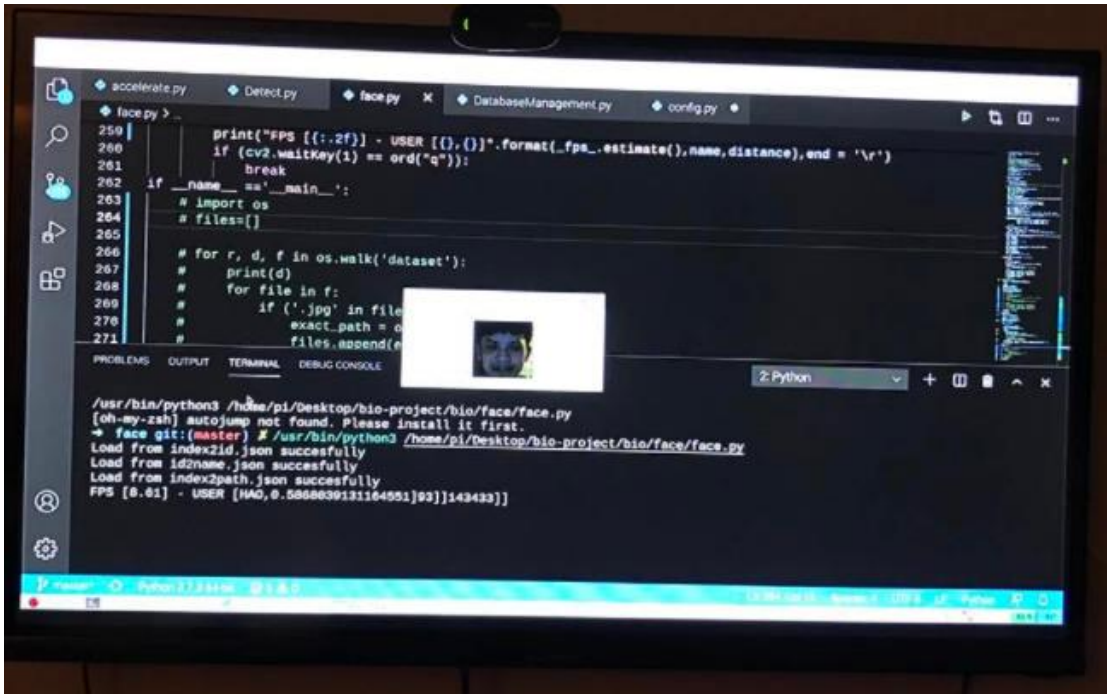


Hình 4.35. Train ảnh

4.4.6.2 Kết quả thu được:

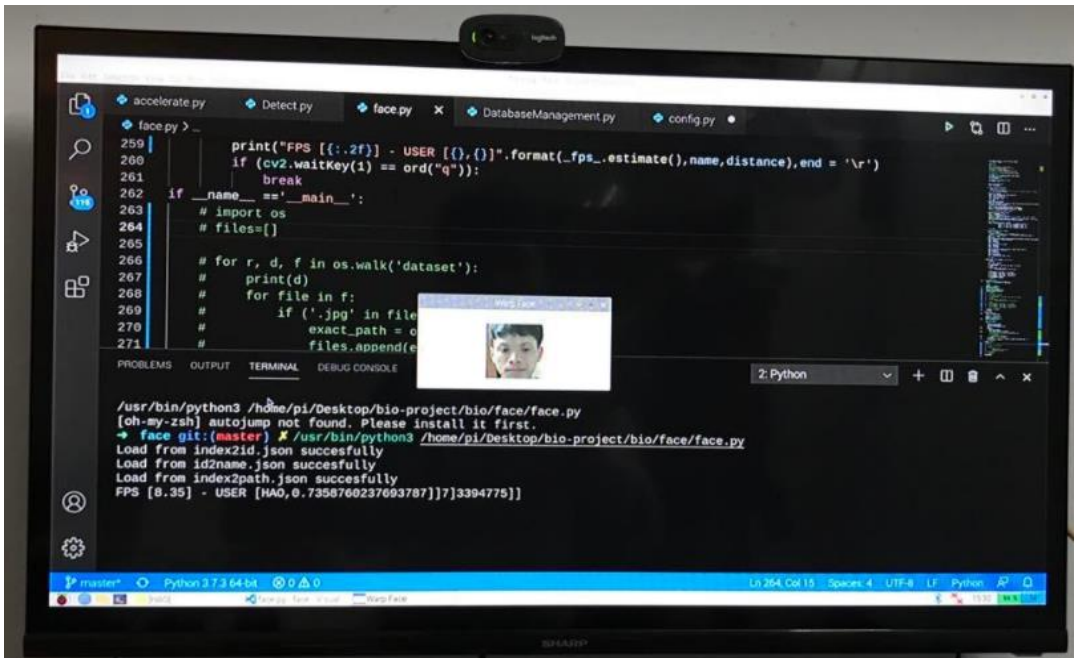
Chạy file face.py để nhận diện khuôn mặt

Trường hợp: khi ở điều kiện ánh sáng tối, không đảm bảo chất lượng ánh sáng hệ thống vẫn nhận diện đưa dữ liệu đúng.



Hình 4.36. Kết quả nhận diện ở điều kiện ánh sáng không tốt

Trường hợp: khi ở điều kiện ánh sáng tốt, đảm bảo chất lượng ánh sáng hệ thống nhận diện đưa dữ liệu đúng.



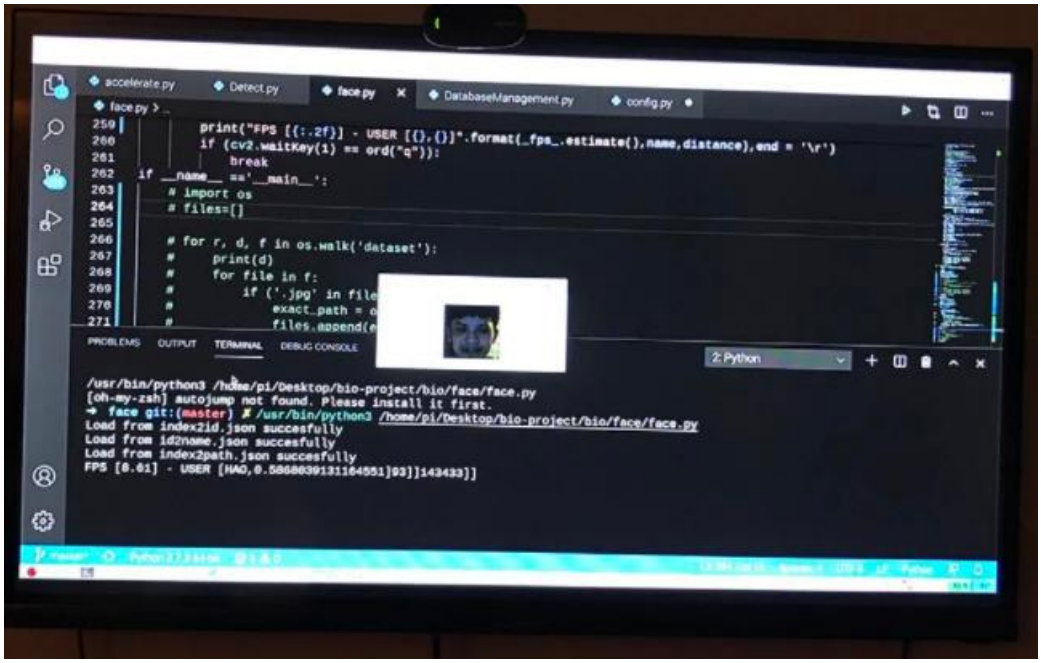
Hình 4.37. Kết quả nhận diện ở ánh sáng tốt

Chương 5: THIẾT KẾ THỰC THI

5.1. Thiết kế nhận diện khuôn mặt và vân tay

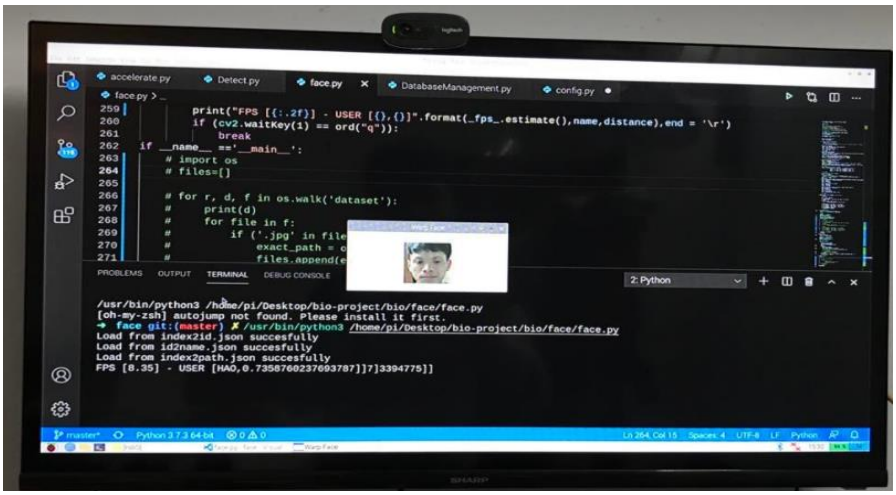
Thiết kế nhận diện khuôn mặt:

Trường hợp: khi ở điều kiện ánh sáng tối, không đảm bảo chất lượng ánh sáng hệ thống vẫn nhận diện đưa dữ liệu đúng



Hình 5.1. Kết quả nhận diện ở điều kiện ánh sáng không tốt

Trường hợp: khi ở điều kiện ánh sáng tốt, đảm bảo chất lượng ánh sáng hệ thống nhận diện đưa dữ liệu đúng.

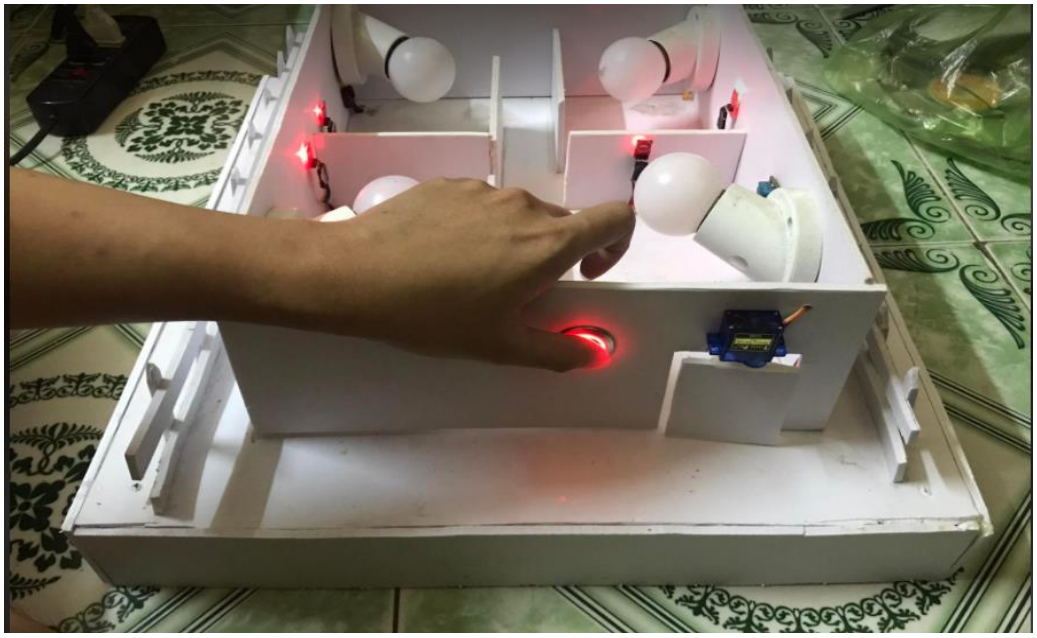


Hình 5.2. Kết quả nhận diện ở ánh sáng tốt

Nhìn chung hệ thống khi ở các trường hợp khác nhau, khả năng nhận diện vẫn hoạt động tốt, cho ra kết quả nhận diện đúng theo cơ sở dữ liệu đã lưu trước. Cải thiện tình trạng giật lag trên khung hình nhận diện.

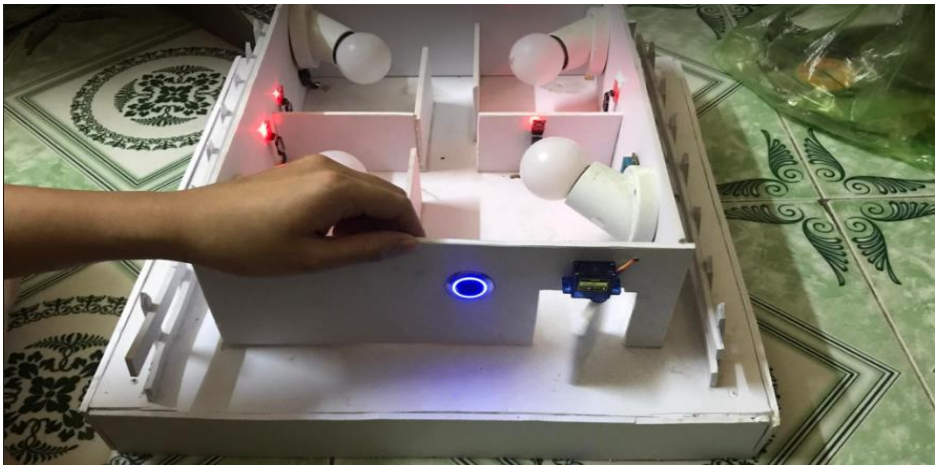
Nhận dạng vân tay:

Trường hợp vân tay không hợp lệ



Hình 5.3. Hình ảnh vân tay không hợp lệ

Trường hợp vân tay hợp lệ



Hình 5.4. Hình ảnh vân tay hợp lệ

Cảm biến vân tay trong hệ thống hoạt động ổn, kịch bản đóng và mở cửa so với thời gian đúng theo mục tiêu của nhóm.

5.2. Kết quả đạt được

Mục tiêu ban đầu của đề tài "XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME" là xây dựng hai đề tài nghiên cứu là: nhận diện khuôn mặt và vân tay ứng dụng mở cửa cho mô hình nhà thông minh. Dựa trên ngôn ngữ Python với thư viện chính là OpenCV và được thực hiện trên Kit Raspberry Pi 4.

Sau quá trình nghiên cứu và thực hiện đề tài, nhóm đã rút ra được nhiều vấn đề khác nhau, từ việc sử dụng phần mềm, các phương pháp giải thuật, cho tới sử dụng phần cứng. Thời gian thực hiện trong khoảng thời gian 15 tuần. Trong đó, gồm các vấn đề sau:

Đối với phần cứng: Biết sử dụng Kit Raspberry, cài đặt hệ điều hành cho Raspberry, biết sử dụng Camera kết nối với Raspberry, các thư viện dành cho Raspberry.

Đối với phần mềm: Biết cách lập trình cơ bản trên Python cùng với thư viện OpenCV, và các giải thuật liên quan đến đề tài như: phương pháp nhận dạng khuôn mặt. Đọc thông tin vân tay và ghi vào dữ liệu

Qua quá trình chạy thực thi có được một số kết quả:

Phát hiện được khuôn mặt người.

So sánh được với ảnh mẫu trong cơ sở dữ liệu để đưa ra quyết định với độ tương thích được đặt trước.

Hiển thị được các thông báo của hệ thống, thông tin người dùng,…

Đóng mở cửa đúng với hành động mong muốn của người dùng.

Chương 6: ĐÁNH GIÁ HỆ THỐNG

6.1. Kết quả đạt được của đồ án

Sau 15 tuần thực hiện đề tài, tìm hiểu và đọc các tài liệu chuyên ngành có liên quan ở các trang mạng, diễn đàn, cộng đồng trong nước và quốc tế thông qua mạng Internet, tổng hợp các kiến thức đã được học xuyên suốt 4 năm cũng như được sự hướng dẫn tận hình của thầy GVHD Th.S Lê Hữu Duy, nhóm thực hiện đồ án chúng em cuối cùng cũng đã hoàn thành được đề tài "XÂY DỰNG HỆ THỐNG BẢO MẬT SINH TRẮC HỌC DỰA TRÊN NHẬN DẠNG KHUÔN MẶT VÀ VÂN TAY ỨNG DỤNG VÀO SMART HOME"

Qua quá trình thực hiện, nhóm cảm thấy đã đúc kết, nâng cao và học được thêm một số kỹ năng như: kỹ năng giao tiếp,làm việc nhóm,kỹ năng phân tích và xử lí vấn đề,...

Thiết kế được hoàn thành có thể ứng dụng cho lắp đặt thay thế các loại khóa cửa dân dụng hay các loại khóa bằng mật khẩu số tại cửa cổng ở các cơ quan, xí nghiệp,..

Hệ thống đóng cửa dùng cảm biến vân tay được thực hiện như đề tài có thể được xem là một hệ thống thông minh với các chức năng đã đạt được như:

Nhận diện được người dung qua xác minh hình ảnh vân tay so với thư viện vân tay đã được lưu trữ để đóng mở cửa chính xác, giảm bớt nguy cơ khi có kẻ gian xâm nhập. Tuy nhiên bên cạnh ưu điểm có được thì hệ thống còn có nhược điểm hạn chế đó là dễ bị phá hoại, vấn đề bảo vệ còn chưa tốt.

Thiết kế thành công mô hình ngôi nhà thông minh.

Tìm hiểu được cơ sở, ý nghĩa của việc điều khiển thiết bị qua internet.

Hiểu được nguyên lí làm việc của các module trong hệ thống và cách ghép nối chúng như thế nào.

Hiểu rộng hơn về Raspberry và môi trường làm việc đa dạng của nó.

Cải thiện được các vấn đề về làm việc nhóm, cũng như các kỹ năng có liên quan (Visual studio code, Word, Power Point…).

Tiến hành chạy thực nghiệm, đánh giá kết quả.

Sau quá trình tìm hiểu môi trường Python và thư viện Opencv cùng một số kĩ thuật có liên quan, đề tài đã đạt được mục tiêu đề ra là xây dựng ứng dụng trí tuệ nhân tạo trong việc nhận dạng khuôn mặt người.

Nhìn chung, hệ thống hoạt động tương đối sự ổn định, có thể làm việc liên tục và đạt các yêu cầu đã đặt ra ban đầu. Bên cạnh đó hệ thống còn được nâng cao thêm một số tính năng giúp cải thiện trải nghiệm người dùng, nâng cao được tính bảo mật dài lâu của hệ thống, đảm bảo được an toàn và giữ vững độ tin cậy.

Hệ thông sử dụng nguồn 12V-5V trở xuống nên rất an toàn cho người sử dụng nếu có xảy ra các tình trạng chạm vỏ, rò điện,… hoặc các tai nạn về điện của hệ thống.

Tuy nhiên, do giới hạn về thời gian và sự hạn chế về mặt kiến thức nên ứng dụng chỉ mới ở giai đoạn ban đầu, cũng như môi trường, nguồn tài liệu tham khảo ở môi trường trong nước không thực sự nhiều, vá lỗi chủ yếu là từ các tài liệu quốc tế, nên hệ thống không tránh khỏi một số hạn chế nhất định và cần phát triển:

Hạn chế đầu tiên là chưa có nguồn dự trữ để duy trì hoạt động cho hệ thống trong trường hợp mất điện.

Các điều kiện về kinh phí cũng như thời gian thực hiện mà tính thẩm mỹ của hệ thống không cao (mô hình to và cồng kềnh, các đường dán keo thô và không đều)

6.2. Hướng phát triển cho hệ thống

Qua đồ án này em xin đề xuất một số hướng phát triển cho hệ thống:

Hệ thống có thể phát triển thêm theo hướng bảo mật nhiều lớp, kết hợp thêm nhiều phương thức bảo mật trong thực tế hơn nữa để tạo ra một hệ thống có tính bảo mật cao hơn và hơn nữa.

Ngoài ra cũng có thể nâng cao khả năng nhận dạng khuôn mặt bằng phương pháp nhận dạng bằng camera kép, một camera nhận dạng và một camera đo chiều sâu để nâng cao khả năng nhận dạng nhiều góc độ cũng như là tăng độ tin cậy của hệ thống lên cao.

Có thể kết hợp với các hệ thống cảnh báo nhằm gửi các thông báo hay báo cáo đến người dùng mỗi lần có người lạ cố tình đột nhập vào nhà, đồng thời cũng nhằm khai thác triệt để module camera của hệ thống.

Xem được ngày giờ xác nhận vân tay.

Có thể thực hiện thay đổi trực tiếp vân tay hoặc xóa bỏ được vân tay ngay trên hệ thống cảm biến.

KẾT LUẬN

Sau khi thực hiện đồ án "Xây dựng hệ thống bảo mật sinh trắc học dựa trên nhận dạng khuôn mặt và vân tay ứng dụng vào Smart Home", sản phẩm cuối cùng đã đạt được các mục tiêu ban đầu được đề ra và nhóm đã hoàn thành tốt báo cáo đồ án này.

Trong quá trình thực hiện đề tài này nhóm cũng đã cũng cố được nhiều kiến thức cũ, đồng thời cũng biết được thêm nhiều kiến thức mới về xử lý hình ảnh bằng python, lập trình C#... Bên cạnh đó nhóm cũng đã rút ra được nhiều kinh nghiệm về nghiên cứu và chế tạo sản phẩm.

Về kết quả, quá trình thử nghiệm cho các kết quả tốt và đáp ứng được yêu cầu của nhóm đề ra. Mặc dù vẫn còn một số hạn chế tuy nhiên nhóm cũng đã tìm ra được nguyên nhân và cách khắc phục. Bên cạnh đó nhóm cũng nhận thấy đề tài có thể phát triển thêm nhiều tính năng hơn nữa.

Do kiến thức của chúng em còn nhiều hạn chế nên nội dung báo cáo có thể có nhiều sai sót. Vì vậy em mong được sự đóng góp ý kiến của các thầy cô và các bạn để bài báo cáo của chúng em được hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

[1] Ngô Diên Tập, Lập trình C cho vi điều khiển NXB KHKT, 2003.

[2] Chu Văn Hoành, Giáo trính Thiết kế Web NXB GDVN, 2005.

[3] Arduino.vn

[4] https://techtalk.vn/xay-dung-he-thong-kiem-soat-nhan-dang-khuon-mat-voi-opencv-dlib-va-deep-learning.html

[5] https://www.adafruit.com/product/4651?fbclid=IwAR2LoLp1aTjMI8jP0vQC8tAf3h9ypMz4XZUzTo_UMChwmrd6rVq0915sok8

[6] https://2kvn.com/nhan-dien-khuon-mat-voi-mang-mtcnn-va-facenet-phan-2-p5f33353636?fbclid=IwAR1aZUUUn_eRRWOwbDyKDjI1PxZgeCGmN82LeMM_EfL5aW7btwoywxumyak

[7] https://viblo.asia/p/arcface-mot-buoc-tien-trong-nhan-dien-khuon-mat-LzD5dW7EljY

[8] https://viblo.asia/p/image-retrieval-voi-thu-vien-faiss-LzD5ddJo5jY