**ĐỐI SÁNH KHUÔN MẶT  
FACE MATCHING**

Tác giả: Giảng viên hướng dẫn: **Thầy Lê Phước Hậu**

Thành viên:

1. Lê Đại Dương (nhóm trưởng)

2. Đỗ Mạnh Hà

3. Nguyễn Đắc Nam

Email: [Duong.LD241082M@sis.hust.edu.vn](mailto:Duong.LD241082M@sis.hust.edu.vn), Ha.DM242130M@sis.hust.edu.vn

*Tóm tắt.*

**Mục tiêu nghiên cứu:** Xác định sự tương đồng xác định mức độ tương đồng giữa hai hình ảnh khuôn mặt. Quá trình này dựa trên việc phân tích, mã hóa và so sánh các đặc trưng số học trích xuất từ khuôn mặt của con người.

**Đối tượng và phương pháp nghiên cứu:**

* Đầu vào: bộ dữ liệu người nổi tiếng Việt nam từ Kaggle

+ Tổng số lượng ảnh khuôn mặt: 23105

+ Số lượng ảnh bộ dữ liệu test: 1156

Đầu ra:

* Huấn luyện mô hình trên tập dữ liệu trên  dùng mô hình dự đoán: **vggface2**

Đầu vào: 5 cặp ảnh ngẫu nhiên

Đầu ra: Dựa vào kết quả phân cụm làm tham chiếu, , tính toán độ tương đồng giữa các cặp ảnh được chọn.

**Kết quả:** Kết quả trên tập dữ liệu thực tế cho thấy mô hình **VGGFace2** có hiệu năng dự đoán tốt với ROC AUC Score: 0.9719902398799259.

Mã nguồn và dữ liệu được chia sẻ theo link https://github.com/

**Kết luận:** Nghiên cứu này cho thấy việc sử dụng mô hình dự đoán: vggface2 để xác định sự tương đồng, xác định mức độ tương đồng giữa hai hình ảnh khuôn mặt. Quá trình này dựa trên việc phân tích, mã hóa và so sánh các đặc trưng số học trích xuất từ khuôn mặt của con người là hiệu quả.

Từ khoá/Keywords: vggface2, FaceMatching, Nhận diện khuôn mặt

# Đặt vấn đề

Công nghệ đối sánh khuôn mặt là một nhánh đặc thù của thị giác máy tính (Computer Vision), được thiết kế để xác định mức độ tương đồng giữa hai hình ảnh khuôn mặt. Quá trình này dựa trên việc phân tích, mã hóa và so sánh các đặc trưng số học trích xuất từ khuôn mặt của con người. Đây là nền tảng cho nhiều ứng dụng quan trọng trong an ninh, thương mại, và dịch vụ cá nhân hóa.

1. **Định nghĩa**

****

*Hình 1. Đối sánh khuôn mặt (Face Matching)*

Công nghệ đối sánh khuôn mặt là một nhánh đặc thù của thị giác máy tính (Computer Vision), được thiết kế để xác định mức độ tương đồng giữa hai hình ảnh khuôn mặt. Quá trình này dựa trên việc phân tích, mã hóa và so sánh các đặc trưng số học trích xuất từ khuôn mặt của con người. Đây là nền tảng cho nhiều ứng dụng quan trọng trong an ninh, thương mại, và dịch vụ cá nhân hóa.

1. **Ứng dụng**
   1. **An ninh và giám sát**

* *Phát hiện tội phạm*: Sử dụng để nhận diện tội phạm tại các sân bay, ga tàu, hoặc khu vực công cộng thông qua cơ sở dữ liệu khuôn mặt của cảnh sát.
* *Kiểm soát ra vào*: Ứng dụng trong hệ thống bảo mật tại tòa nhà, văn phòng, hoặc khu vực quân sự.
* *Giám sát đám đông*: Theo dõi hành vi và nhận diện đối tượng trong các sự kiện lớn hoặc khu vực nhạy cảm.
  1. **Thương mại điện tử và tài chính**
* *Thanh toán không tiếp xúc*: Nhận diện khuôn mặt để xác thực giao dịch mà không cần thẻ ngân hàng hay mật khẩu.
* *Phòng chống gian lận*: Đảm bảo tính xác thực của người dùng khi thực hiện giao dịch tài chính hoặc vay vốn.
  1. **Mạng xã hội**
* *Gắn thẻ tự động*: Hỗ trợ nhận diện khuôn mặt trong ảnh và video để gắn thẻ bạn bè (ví dụ: Facebook, Instagram).
* *Cá nhân hóa nội dung*: Cung cấp gợi ý hoặc quảng cáo dựa trên dữ liệu khuôn mặt của người dùng.
* *Ứng dụng AR/VR*: Tích hợp khuôn mặt người dùng vào trò chơi hoặc các trải nghiệm thực tế ảo.
  1. **Chính phủ và dịch vụ công**
* *Quản lý căn cước*: Tích hợp vào hộ chiếu, căn cước công dân, hoặc giấy phép lái xe để đảm bảo danh tính.
* *Bầu cử điện tử*: Nhận diện khuôn mặt để xác thực cử tri, ngăn chặn gian lận bầu cử.
* *Hệ thống cảnh báo*: Giúp nhận diện nhanh các đối tượng có nguy cơ cao trong cộng đồng, như tội phạm truy nã hoặc người mất tích.
  1. **Ứng dụng trong lĩnh vực quân sự**
* *Xác định mục tiêu*: Nhận diện khuôn mặt trong các hoạt động tình báo hoặc tác chiến.
* *Giám sát biên giới*: Nhận diện người di cư hoặc phát hiện đối tượng không được phép nhập cảnh.

1. **Đặc điểm**

*Tính không tiếp xúc (Contactless):* Không yêu cầu chạm vào thiết bị để xác thực danh tính, đảm bảo vệ sinh và thuận tiện hơn so với các công nghệ sinh trắc học khác như vân tay.

*Tính tự động và thời gian thực:* Hệ thống nhận diện khuôn mặt có thể hoạt động tự động, xử lý và đối sánh trong vài mili-giây, phù hợp với các ứng dụng đòi hỏi thời gian thực.

*Độ chính xác cao:* Với sự hỗ trợ của trí tuệ nhân tạo (AI) và học sâu (Deep Learning), độ chính xác của hệ thống ngày càng cao, đặc biệt trong điều kiện môi trường tối ưu.

*Phụ thuộc vào dữ liệu:* Hiệu suất của hệ thống phụ thuộc vào chất lượng và sự đa dạng của dữ liệu khuôn mặt được thu thập và sử dụng trong quá trình đào tạo.

*Phạm vi ứng dụng rộng rãi:* Từ an ninh, y tế, giáo dục, đến thương mại điện tử và dịch vụ khách hàng, nhận diện khuôn mặt có thể được triển khai trong nhiều lĩnh vực khác nhau.

*Tính bền vững:* Các đặc điểm khuôn mặt như hình dáng, cấu trúc không thay đổi nhanh chóng theo thời gian (trừ trường hợp bị tổn thương nghiêm trọng), giúp công nghệ này duy trì độ ổn định lâu dài.

*Nhạy cảm với môi trường:* Hiệu suất có thể giảm trong điều kiện ánh sáng yếu, khuôn mặt bị che khuất (ví dụ: khẩu trang), hoặc góc nhìn không chuẩn hóa.

*Bảo mật và riêng tư:* Dữ liệu khuôn mặt là thông tin nhạy cảm, cần được bảo vệ nghiêm ngặt để tránh lạm dụng và xâm phạm quyền riêng tư.

**Tiềm năng**

*Cách mạng hóa an ninh và giám sát:* Nhận diện khuôn mặt có khả năng cải thiện an ninh công cộng, nhận diện tội phạm và phát hiện các mối đe dọa tiềm tàng trong thời gian thực.

*Đơn giản hóa xác thực và truy cập:* Thay thế các phương pháp xác thực truyền thống như mật khẩu hoặc thẻ từ bằng các giải pháp nhận diện nhanh chóng và tiện lợi.

*Tối ưu hóa dịch vụ khách hàng:* Các hệ thống bán lẻ, ngân hàng, và khách sạn có thể cá nhân hóa dịch vụ dựa trên thông tin nhận diện khuôn mặt của khách hàng.

*Ứng dụng trong IoT và nhà thông minh:* Kết hợp nhận diện khuôn mặt với các thiết bị IoT để mở khóa cửa, điều khiển thiết bị gia dụng, hoặc quản lý an ninh trong nhà.

*Hỗ trợ nghiên cứu và y tế:* Phân tích cảm xúc, theo dõi tâm lý, phát hiện bệnh di truyền hoặc quản lý bệnh nhân một cách hiệu quả hơn.

*Đóng góp cho giao thông thông minh:* Cải thiện an toàn và trải nghiệm người dùng bằng cách nhận diện tài xế, phát hiện hành vi nguy hiểm hoặc quản lý hành khách trong giao thông công cộng.

*Tạo nền tảng cho xã hội số hóa:* Là yếu tố quan trọng trong việc xây dựng các thành phố thông minh, quản lý hành chính số, và triển khai các giải pháp chính phủ điện tử.

*Hỗ trợ nghiên cứu tâm lý và xã hội học:* Phân tích biểu cảm khuôn mặt để hiểu rõ hơn về hành vi con người trong nhiều lĩnh vực nghiên cứu.

1. **Nhược điểm và thách thức**

*Vấn đề riêng tư và đạo đức:*

Cần xây dựng các chính sách bảo vệ dữ liệu cá nhân chặt chẽ, đảm bảo quyền riêng tư của người dùng.

*Khả năng bị giả mạo:*

Các kỹ thuật như Deepfake có thể làm giảm độ tin cậy của công nghệ nhận diện khuôn mặt.

*Yêu cầu cơ sở hạ tầng:*

Để vận hành hiệu quả, công nghệ này đòi hỏi phần cứng mạnh, mạng lưới camera và cơ sở dữ liệu lớn.

# Đối tượng và phương pháp thực hiện

## 2.1 Đối tượng

Bộ dữ liệu người nổi tiếng Việt nam từ kaggle, với cấu trúc thư mục theo danh mục danh tính.

## https://www.kaggle.com/api/v1/datasets/download/hariwu1995/vn-celeb?dataset\_version\_number=1

## 2.2 Phương pháp thực hiện

(1) Đọc ảnh khuôn mặt và gán nhãn cho từng khuôn mặt:

(2). Chia nhỏ tập dữ liệu, sử dụng bộ dữ liệu test để đánh giá mô hình.

(3) Đọc ảnh từ bộ dữ liệu test

# Mô hình lựa chọn: VGGFace2

- Được phát triển vào năm 2017, được đào tạo trên 3,31 triệu hình ảnh, tổng cộng 9131 người

- VGGFace2 sử dụng một tập dữ liệu lớn hơn nhiều và hai mô hình đã được đào tạo bằng cách sử dụng:

+ ResNet-50: Mạng dư thừa 50 lớp với 26M tham số. Mạng dư thừa này là mạng nơ-ron tích chập sâu được Microsoft giới thiệu vào năm 2015.

+ SqueezeNet-ResNet-50: Là một mạng nhỏ hơn được phát triển bởi các nhà nghiên cứu tại DeepScale, Đại học California tại Berkeley và Đại học Stanford. Mục tiêu của SENet là tạo ra một mạng nơ-ron nhỏ hơn có thể dễ dàng phù hợp với bộ nhớ máy tính và dễ dàng truyền qua mạng máy tính.

1. **Luồng thực hiện**
2. Chuẩn hóa

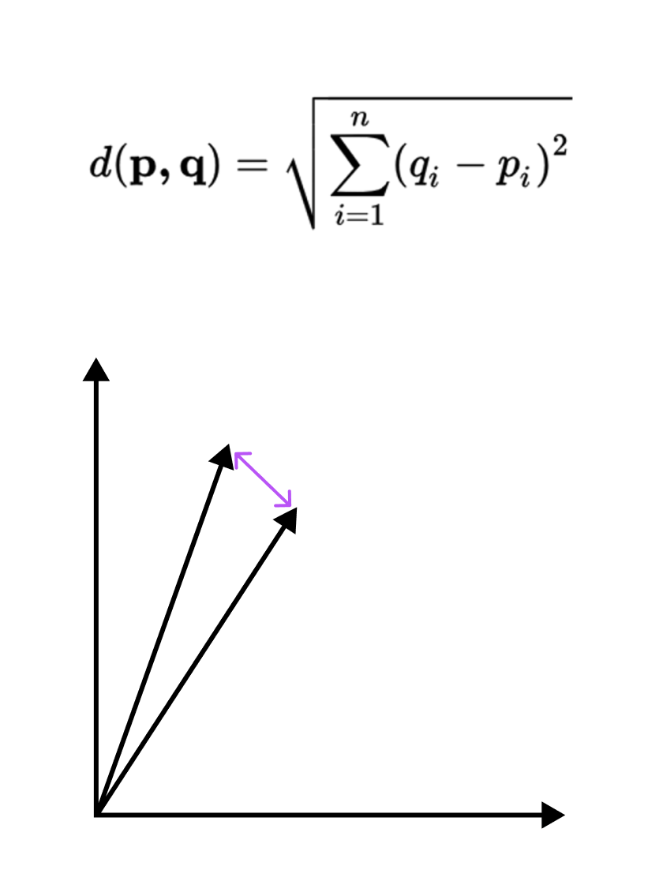
Sử dụng chuẩn hóa dữ liệu bằng NumPy

1. Chuyển sang tensor
2. Trích xuất vector cho toàn bộ khuôn mặt
3. Chọn ngưỡng xác định 2 ảnh có phải của một người
4. **Tính toán độ tương đồng**

Trong nhận diện khuôn mặt, mỗi khuôn mặt được biểu diễn bởi một vector đặc trưng (embedding vector) trong không gian nhiều chiều. Để xác định xem hai vector có cùng danh tính hay không, chúng ta cần đo độ tương đồng giữa chúng. Có 2 hương pháp phổ biến nhất để tính độ tương đồng là Cosine Similarity và Euclidean Distance.

*Euclidean Distance*

Euclidean Distance đo khoảng cách tuyến tính giữa hai vector trong không gian:



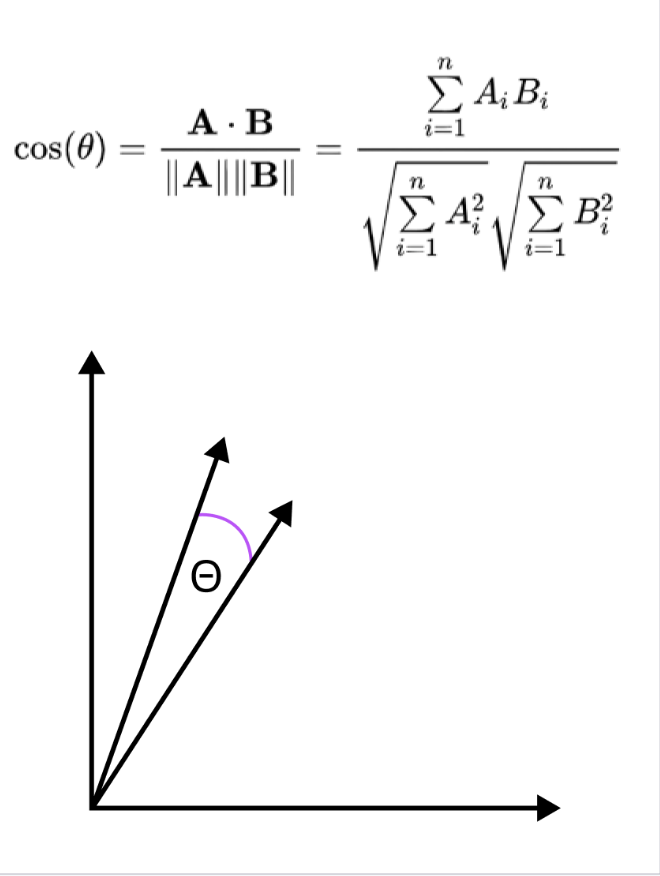
*Hình 8. Euclidean Distance*

Giá trị đầu ra: Một số thực không âm

* 0: Hai vector hoàn toàn giống nhau.
* Giá trị lớn hơn: Hai vector càng khác nhau.
* Ưu điểm: Dễ tính toán và trực quan.
* Nhược điểm: Phụ thuộc vào độ lớn của vector, cần chuẩn hóa trước khi sử dụng.

*Cosine Similarity*

Cosine Similarity đo góc giữa hai vector trong không gian nhiều chiều:



*Hình 9. Cosine Similarity*

**Giá trị đầu ra:** Thuộc khoảng [-1, 1].

* + 1: Hai vector hoàn toàn giống nhau.
  + 0: Hai vector vuông góc, không liên quan.
  + -1: Hai vector ngược hướng nhau.
* Ưu điểm:
  + Xét đến mối quan hệ giữa các thành phần vector.
  + Thích hợp với dữ liệu phức tạp.
* Nhược điểm: Tốn kém tính toán do cần tính ma trận nghịch đảo.

**Kết quả**

Trong nhận diện khuôn mặt, ngưỡng (threshold) là giá trị được sử dụng để quyết định xem hai vector đặc trưng khuôn mặt có thuộc cùng một danh tính hay không. Lựa chọn ngưỡng phù hợp là một bước quan trọng để tối ưu hóa độ chính xác của hệ thống và đảm bảo cân bằng giữa tỷ lệ nhận diện đúng và tỷ lệ lỗi.

***Khái niệm Ngưỡng (Threshold)***

* Cosine Similarity:

Ngưỡng là giá trị mà nếu độ tương đồng cosin giữa hai vector lớn hơn hoặc bằng, thì hai khuôn mặt được xác định là thuộc cùng một danh tính.

Ví dụ: Nếu ngưỡng là 0.8, thì Cosine Similarity > 0.8 được xem là cùng một danh tính.

* Euclidean Distance:

Ngưỡng là giá trị mà nếu khoảng cách Euclid giữa hai vector nhỏ hơn hoặc bằng, thì hai khuôn mặt được xác định là thuộc cùng một danh tính.

Ví dụ: Nếu ngưỡng là 0.6, thì Euclidean Distance < 0.6 được xem là cùng một danh tính.

***Tầm Quan Trọng của Ngưỡng***

Ngưỡng ảnh hưởng trực tiếp đến:

* *False Acceptance Rate (FAR):* Tỷ lệ hệ thống chấp nhận nhầm hai khuôn mặt khác nhau là cùng một danh tính.
* *False Rejection Rate (FRR):* Tỷ lệ hệ thống từ chối nhầm hai khuôn mặt thuộc cùng một danh tính.

Việc chọn ngưỡng là tối ưu khi nó cân bằng được giữa FAR và FRR, tùy thuộc vào ứng dụng.

***Quy Trình Lựa Chọn Ngưỡng***

*Bước 1: Thu thập dữ liệu đánh giá*

Sử dụng tập dữ liệu bao gồm:

* Positive pairs: Cặp hình ảnh của cùng một người.
* Negative pairs: Cặp hình ảnh của hai người khác nhau.

*Bước 2: Tính toán độ tương đồng*

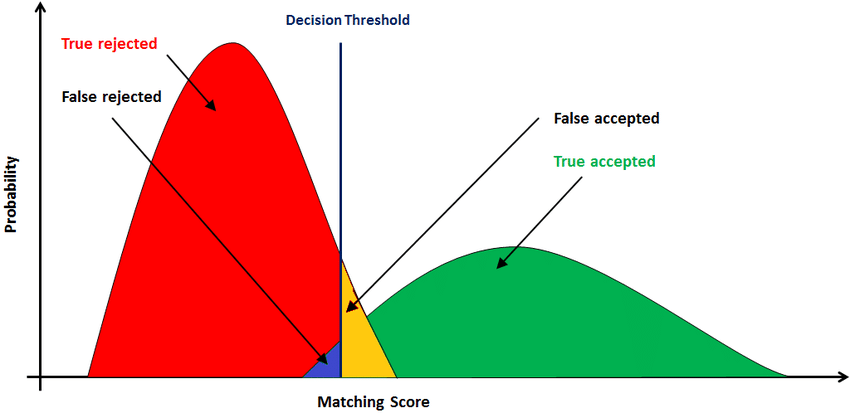
Tính toán Cosine Similarity hoặc Euclidean Distance giữa các cặp khuôn mặt.

*Bước 3: Phân tích phân phối*

Vẽ biểu đồ phân phối giá trị:

* Positive pairs: Độ tương đồng cao hơn (hoặc khoảng cách thấp hơn).
* Negative pairs: Độ tương đồng thấp hơn (hoặc khoảng cách cao hơn).

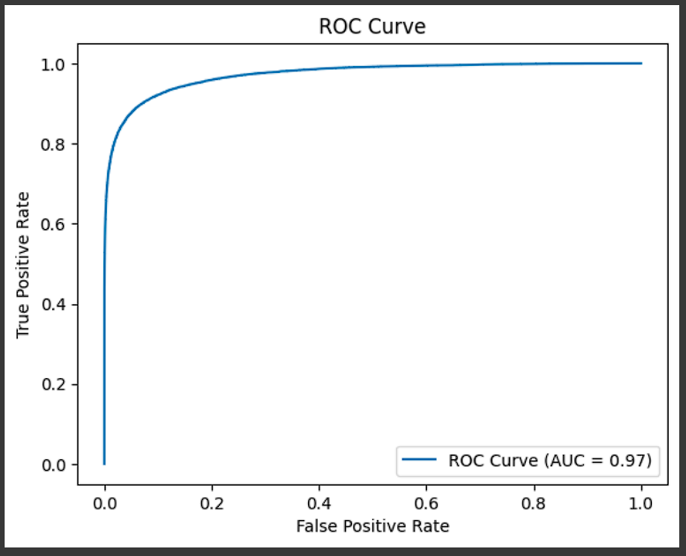
Xác định điểm giao giữa hai phân phối, là vùng mà hệ thống dễ nhầm lẫn.



*Hình 10. Lựa chọn ngưỡng cho face matching*

## 3.3 Kết quả huấn luyện mô hình

Kết quả trên tập dữ liệu thực tế cho thấy mô hình **VGGFace2** có hiệu năng dự đoán tốt với ROC AUC Score: 0.9719902398799259.



# 

# Kết luận

Nhận diện khuôn mặt là một công nghệ tiên tiến và quan trọng trong lĩnh vực thị giác máy tính, với khả năng ứng dụng rộng rãi từ bảo mật, giám sát đến dịch vụ khách hàng và các hệ thống tương tác thông minh. Trong đề tài này, chúng ta đã xây dựng một hệ thống nhận diện khuôn mặt hiệu quả.

Phương pháp đề xuất không chỉ đảm bảo độ chính xác cao trong nhận diện khuôn mặt mà còn tối ưu hóa hiệu năng, đáp ứng tốt các yêu cầu thực tế về thời gian xử lý và độ tin cậy.

* Ý nghĩa: Nhận diện khuôn mặt là một công nghệ tiên tiến và quan trọng trong lĩnh vực thị giác máy tính, với khả năng ứng dụng rộng rãi từ bảo mật, giám sát đến dịch vụ khách hàng và các hệ thống tương tác thông minh. Trong đề tài này, chúng ta đã xây dựng một hệ thống nhận diện khuôn mặt hiệu quả, kết hợp các thành phần hiện đại.
* Hạn chế: Mặc dù hệ thống đạt hiệu suất ấn tượng, vẫn tồn tại một số hạn chế cần khắc phục.
* Hướng phát triển: chống gian lận , Sử dụng học sâu với dữ liệu đa dạng hơn, Tối ưu hóa mô hình trên phần cứng.

# Tên tác giả, địa chỉ, số điện thoại (liên hệ chính)

Lê Đại Dương (nhóm trưởng)

Địa chỉ: C06, Bộ Công an

Số điện thoại: 0989.267.684

# Danh mục tài liệu tham khảo

# VN-celeb: Dữ liệu khuôn mặt người nổi tiếng Việt Nam và bài toán Face recognition

<https://viblo.asia/p/vn-celeb-du-lieu-khuon-mat-nguoi-noi-tieng-viet-nam-va-bai-toan-face-recognition-Az45bG9VKxY>

Implementing Face Recognition Using Deep Learning and Support Vector Machines

<https://www.codemag.com/Article/2205081/Implementing-Face-Recognition-Using-Deep-Learning-and-Support-Vector-Machines>

VGGFace2: A dataset for recognising faces across pose and age

<https://arxiv.org/abs/1710.08092>

Nhận dạng khuôn mặt sử dụng kỹ thuật trí tuệ nhân tạohttps://www.researchgate.net/publication/339221166\_Face\_Recognition\_using\_Artificial\_Intelligent\_Techniques