## TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

**Viện Công nghệ thông tin và Truyền thông**

**---oOo---**

****

BÁO CÁO

**Nhập môn An toàn thông tin**

# **Mã lớp: 115655**

Nhóm 25

Giảng viên hướng dẫn: PGS. TS. NGUYỄN LINH GIANG

Sinh viên thực hiện:

1. Vũ Khắc Chinh : 20172979

2. Vũ Quốc Dũng : 20173053

3. Nguyễn Trung Kiên : 20173214

4. Phạm Trí Ninh : 20173295

**Hà Nội, 2020**

**MỤC LỤC**

**1. Tổng quan về sinh trắc học…………………………………………4**

**2. Đặc trưng sinh trắc học khuôn mặt………………………………...5**

**2.1. Các đặc trưng sinh trắc khuôn mặt………………………………5**

**2.2. Các phương pháp xác định đặc trưng**

**khuôn mặt………………………………………………………….5**

**2.2.1. Phương pháp xác định màu da…………………………………5**

**2.2.2. Phương pháp phân tách, phân vùng  
 đặc trưng khuôn mặt…………………………………………….6**

**2.2.3. Phương pháp tiếp cận theo mô hình**

**đường viền linh hoạt……………………………………………..7**

**2.2.4. Phương pháp tiếp cận theo mô hình**

**xuất hiện linh hoạt……………………………………………….7**

**2.3. Nhận dạng 3D……………………………………………………...7**

**2.4. Thuật toán facenet………………………………………………...9**

**2.4.1. Khái quát thuật toán…………………………………………….9**

**2.4.2. Triple loss……………………………………………………….10**

**2.4.3. Lựa chọn Triple images input…………………………………11**

**2.5. Vấn đề bảo mật trong các hệ thống**

**sinh trắc học………………………………………………………12**

**2.5.1. Những cách thức, thủ đoạn xâm**

**nhập trái phép………………………………………………….12**

**2.5.2. Các biện pháp bảo mật………………………………………13**

**1. Tổng quan về sinh trắc học**

- Mỗi con người có một nét đặc trưng riêng, không ai giống ai. Những đặc điểm như dấu vân tay, khuôn mặt, giọng nói, nhịp điệu, màu mắt, màu tóc, cách gõ phím máy tính, ... làm cho họ có nét riêng biệt với những người khác. Các đặc trưng sinh trắc được chia làm hai loại:

+ Đặc trưng sinh lí: là các đặc trưng cho cấu tạo và hình dạng của cơ thể như khuôn mặt, vân tay. Các đặc trưng này để phân biệt mỗi người và khó bị mất đi từ khi sinh ra đến khi chết đi trừ trường hợp như: phẫu thuật thẩm mĩ, tai nạn…

+ Đặc trưng hành vi: là những đặc trưng như: cách nói chuyện, di chuyển, ứng xử, chữ kí…

- Dựa vào những đặc điểm sinh trắc của con người, các hệ thống sinh trắc ra đời nhằm giải quyết vấn đề an ninh mạng, khoa học, xác nhận một người ,…

- Một hệ thống sinh trắc học cơ bản gồm các thành phần sau:

+ Thiết bị thu nhận đặc trưng(Sensor): Là thiết bị thu nhận các đặc trưng sinh trắc của người dung như bộ cảm biến vân tay, camera chụp ảnh khuôn mặt…

+ Xử lý: Đây là phần trích chọn đặc trưng của mỗi người, nếu người dùng lần đầu sử dụng thì đặc trưng này sẽ được thêm vào cơ sở dữ liệu. Từ lần thứ hai sử dụng thì đặc trưng của người dung sẽ được so sánh với đặc trưng có sẵn trong cơ sở dữ liệu. Nếu trong cơ sở dữ liệu có chứa mẫu trùng với mẫu thu thập thì hệ thống sẽ đưa ra quyết định xác thực danh tính của mẫu thu nhận được.

- Các hệ thống sinh trắc học đem lại sự an toàn cho việc bảo mật vì:

+ Tính duy nhất: Các đặc trưng sinh trắc của mỗi người khác nhau là khác nhau tức đặc trưng sinh trắc của mỗi người là duy nhất.

+ Không thể chia sẻ: Các đặc trưng sinh trắc là thuộc tính riêng gắn với mỗi người vì vậy không thể chia sẻ việc sử dụng đặc trưng đó cho người khác.

+ Không thể sao chép: Các đặc trưng sinh trắc không thể bị sao chép

+ Không thể mất: các đặc trưng sinh trắc không thể mất đi trừ trường hợp phẫu thuật, tai nạn

Qua những đặc điểm trên cho thấy việc bảo mật bằng nhận diện sinh trắc cho thấy tính an toàn cao và cho phép xác định hành vi của con người. Chính vì những ưu điểm đó mà ngày nay các hệ thống bảo mật sinh trắc đang được phát triển.

- Ứng dụng của hệ thống nhận diện sinh trắc học:

+ Thi hành pháp luật: Được thực hiện bằng hệ thống nhận diện vân tay để xác nhận dấu vân tay tội phạm để lại trên đồ vật hoặc dung hệ thống nhận diện khuôn mặt để tìm ra hung thủ.

+ Giám sát: Được sử dụng để định vị và theo dõi người trong một khu vực nhất định. Bằng cách sử dụng các camera để nhận diện sinh trắc khuôn mặt sẽ xác định được danh tính của người trong phạm vi 200 mét, tròng mặt cũng được sử dụng nhưng do kích thước nhỏ nên khoảng cách để xác định danh tính đối tượng là 15 mét

+ Xuất nhập cảnh: Được sử dụng để xác nhận danh tính của người xuất nhập cảnh khi số lượng người xuất nhập cảnh ngày càng nhiều, sử dụng hộ chiếu điện tử - một công nghệ sinh trắc học cho phép xác thực danh tính đối tượng bằng sinh trắc khuôn mặt, vân tay, tròng mắt

+ Chống gian lận: Được sử dụng để chống các cá nhân hưởng lợi từ việc đăng kí nhiều danh tính khác nhau, hiện nay liên hợp quốc sử dụng vân tay để chống trường hợp một các nhân dung nhiều danh tính để hưởng lương trợ cấp nhiều lần

+ Điểm danh: được sử dụng tại các trường học để điểm danh bằng khuôn mặt, vân tay…

+ Bảo vệ tài sản: sử dụng vân tay để khóa tủ…

**2. Đặc trưng sinh trắc học khuôn mặt**

**2.1. Các đặc trưng sinh trắc khuôn mặt**

- Các đặc trưng sinh trắc khuôn mặt là những đặc điểm trên khuôn mặt mỗi người hầu như không thay đổi theo thời gian( ngoại trừ trường hợp tai nạn, phẫu thuật…), các đặc điểm này đối với mỗi người là khác nhau, chính vì vậy nó giúp phân biệt người này với người khác, hầu như không thể tìm được những người có đặc điểm khuôn mặt giống hết nhau ( kể cả sinh đôi ). Con người có thể xác định được người khác cho dù khuôn mặt ở các góc độ khác nhau, ánh sáng khác nhau nếu đặc trưng khuôn mặt không đổi vì vậy việc xác định danh tính bằng sinh trắc khuôn mặt sẽ cho độ chính xác cao.

- Một số đặc điểm sinh trắc học khuôn mặt như: Màu da, mắt, chán. mũi, miệng, cằm, má, lông mày, tai.

- Hiện nay các hệ thống sinh trắc học nhận diện khuôn mặt thông qua việc phân tích và xử lí các đặc điểm sinh trắc trên khuôn mặt.

**2.2. Các phương pháp xác định đặc trưng khuôn mặt**

**2.2.1 Phương pháp xác định màu da**

- Phương pháp này sẽ xác định một bức ảnh đầu vào có khuôn mặt hay không và nếu có sẽ xác định vị trí của khuôn mặt.

- Ý tưởng của phương pháp là phân vùng rõ rang giữa vùng có da và vùng không có da. Ngày nay có nhiều kỹ thuật để xử lý nhiệm vụ này. Các điểm ảnh sẽ được biểu diễn trong không gian màu thích hợp để phân vùng da.

- Một số phương pháp:

+ Phân cụm theo da của Kovac:

* B1: Giảm độ phân dải của ảnh đầu vào thành 160 x 120 pixels
* B2: Loại bỏ các pixels được xác định là không thể hiện khuôn mặt
* B3: Khoanh vùng các điểm ảnh thể hiện phần khuôn mặt
* B4: Loại bỏ các vùng không thể hiện khuôn mặt

+ Phương pháp phát hiện vùng da dựa trên xác suất của Kakumanu: Vấn đề đặt ra của phương pháp này là xác định đâu là vùng không có da người, Kakumanu đề xuất phương pháp phân tích histogram của ảnh để phân chia dựa trên lý thuyết xác xuất Bayes. Không gian màu được lượng tử hóa thành các màu cụ thể. Mỗi một mức màu sẽ bao gồm số lượng các điểm ảnh nhất định nằm trong tập dữ liệu các điểm ảnh đã được mã hóa. Từ ý tưởng đó Kakumanu sẽ chuyển đổi ngẫu nhiên các điểm ảnh mang mức màu cụ thể sang giá trị xác suất:

**P(a) = count(a)/S**

Trong đó:

* Count(a) là số lượng các điểm ảnh mang giá trị mức màu a
* S là tổng các mức màu đã được lượng tử hóa trong quá trình mã hóa

Các giá trị xác suất này sẽ được so sánh với các mức xác định màu da hoặc không phải màu da cho trước rồi đưa ra kết luận

+ Dai và Nakano sử dụng phân bố của thành phần màu I trong không gian màu YIQ để phát hiện các pixcels trong ảnh có chứa phần da người (màu da vàng). Màu I bao gồm dải màu từ orange đến cyan, tất cả các điểm ảnh có giá trị từ 0 đến 50 đều dùng để thể hiện màu da con người.

**2.2.2 Phương pháp phân tách, phân vùng đặc trưng khuôn mặt**

- Ý tưởng của phương pháp này là việc xây dựng và trích chọn các đặc trưng sinh trắc theo cấu trúc khuôn mặt, từ đó so sánh với mẫu trong cơ sở dữ liệu rồi đưa ra kết luận. Các đặc trưng như: độ rộng của thán, khoảng cách giữa hai mắt, độ rộng của mũi, miệng, gò má, viền khuôn mặt.

- Một số phương pháp:

+ Mô hình mạng thần kinh do H.Rowley đề xuất

+ Mô hình nhận dạng khuôn mặt thời gian thực do P.Viola và M.Jones đề xuất: Ở đây tác giả xây dựng các đặc trưng Haar-like, sau đó tỉnh tổng giá trị chênh lệch của các vùng đen và các vùng trắng rồi dung giá trị này so sánh với giá trị các pixels thô, các giá trị Haar-like có thể tăng giảm (bên trong hoặc bên ngoài vùng mặt người) do đó làm cho bộ phân loại dễ hơn. Dựa trên ý tưởng đó ta phân loại các vùng riêng biệt trên khuôn mặt.

+ AdaBoost là bộ phân loại mạnh phi tuyến phức dựa trên hướng tiếp cận boosting được Freund và Schapire đưa ra vào năm 1995. Adaboost cũng hoặc động dựa trên nguyên tắc kết hợp tuyến tính các weak classifiers để hình thành các strong classifiers. Là một cải tiến của tiếp cận boosting, AdaBoost sử dụng thêm khái niệm trọng số để đánh dấu các mẫu khó nhận dạng.

+ Phân tích các thành phần chính: là một phương pháp trích chọn các đặc điểm. Thuật toán cung cấp một mô hình thực tiễn trên các mẫu đặc trưng của một lớp, có thể sử dụng để chia các lớp từ các mẫu chưa được phân lớp.

**2.2.3 Phương pháp tiếp cận theo mô hình đường viền linh hoạt.**

- Ý tưởng của phương pháp này là dựng ra các đường viền khung khuôn mặt bao gồm đường viền bao quanh khuôn mặt, các đường viền bao quanh các bộ phận đặc trưng trên khuôn mặt như: mắt, mũi miệng. Từ đó với một bức ảnh đầu vào người ta sẽ đem so khớp ảnh khuôn mặt với các mẫu đường viền đó dựa trên thuật toán phù hợp, nếu tỷ lệ trùng khớp đủ lớn hơn một ngưỡng nào đó thì sẽ kết luận khuôn mặt đầu vào trùng khớp với khuôn mặt nào đó.

- Việc thực hiện thuật toán PCA trên khuôn mặt có thể không hiệu quả bằng việc so khớp các đường viền vì vậy mô hình ASM áp dụng thuật toán PCA một cách hiệu quả.

- Một số phương pháp:

**+** Yuile sử dụng mô hình phân vùng khuôn mặt theo mắt, miệng dựa vào ý tưởng xây dựng các khung từ các dạng hình học cơ bản như vòng tròn, đường kẻ, hình đa giác… cho phép khoanh vùng những mảng hình đặc trưng.

+ Kass đề xuất mô hình linh hoạt hơn, đó là tập trung vào các đặc trưng sinh trắc khuôn mặt, các đặc trưng khuôn mặt được vẽ bởi các đường cong với mức độ bám sát tối đa, những khoảng thừa được giảm xuống mức nhỏ nhất để xác định vùng liên quan tới đặc trưng sinh trắc khuôn mặt.

**2.2.4 Phương pháp tiếp cận theo mô hình xuất hiện linh hoạt.**

- Đây là mô hình được cải tiến từ mô hình ASM, mô hình này sẽ tập trung vào cấu trúc của ảnh, đặc biệt vào hình dạng các vùng trên khuôn mặt được xác định bởi các điểm mốc dựa trên thuật toán PCA với:

+ v: các tham số đường viền

+ g: các tham số cho cấu trúc

+ Tập học PCA bao gồm các vector c = (v,g)

+ Sai số của mô hình năm trong khoảng giá trị: ||c||

+ Đánh giá: tốc độ tìm kiếm của mô hình/ viền được đánh dấu rất nhanh

**2.3. Nhận dạng 3D**

- Ngày nay, với sự phát triển của công nghệ và với xu hướng 3D đang thịnh hành, chúng ta có nhận dạng khuôn mặt 3 chiều. Kỹ thuật này sẽ nâng cao độ chính xác nhờ phân tích được nhiều thông tin hơn. Kỹ thuật này sử dụng các cảm biến 3D để nắm bắt thông tin về hình dạng của khuôn mặt, rồi dùng các điểm nổi bật trên khuôn mặt – nơi những mô cứng và xương nhìn thấy rõ nhất như đường cong của hốc mắt, mũi và cằm -- để nhận ra đối tượng. Các đặc điểm này là độc nhất đối với mỗi khuôn mặt và không thay đổi theo thời gian.

- Cách thức sử dụng độ sâu và trục của các phần trên khuôn mặt không bị ảnh hưởng bởi ánh sáng, vì thế việc nhận dạng khuôn mặt 3D có thể được sử dụng cả trong bóng tối và có thể nhận ra khuôn mặt từ nhiều góc độ khác nhau với độ chênh lệch lên tới 90 độ. Và nhờ có việc xác định khuôn mặt dựa trên hình ảnh 3 chiều, nên nhận dạng 3D có khả năng xác định 1 khuôn mặt từ nhiều góc nhìn hơn. Số lượng các điểm dữ liệu 3 chiều khiến cho độ chính xác tăng lên đáng kể bởi sự phát triển của các bộ cảm biến tinh vi giúp nắm bắt hình ảnh chụp khuôn mặt 3D được tốt hơn. Các cảm biến hoạt động bằng cách chiếu ánh sáng có cấu trúc lên gương mặt. Hàng chục hoặc nhiều hơn nữa các bộ cảm biến hình ảnh này có thể được đặt lên trên cùng một con chip CMOS-mỗi cảm biến sẽ thu một phần khác nhau của hình ảnh.

- Để có thể nhận dạng 3 chiều, ngoài việc phải sử dụng phần mềm 3D, hệ thống nhận diện này cần trải qua một loạt bước để nhận diện một đối tượng:

+ Nhận dạng: Việc ghi lại một hình ảnh có thể thực hiện bằng cách quét một tấm ảnh 2D sẵn có, hoặc sử dụng video để có được một hình ảnh 3D sống của đối tượng.

+ Liên kết: Sau khi đã ghi lại một khuôn mặt, hệ thống này sẽ tính toán vị trí, kích cỡ và tư thế của đầu. Như đã đề cập từ trước, hệ thống có thể nhận ra một khuôn mặt ở góc lệch lên tới 90 độ, trong khi với hình ảnh 2D, khuôn mặt của đối tượng phải nghiêng ít nhất là 35 độ về phía camera.

+ Đo đạc: Sau đó, hệ thống này sẽ đo đạc những đường cong trên khuôn mặt với độ chính xác lên tới dưới 1 milimet, rồi tạo một khuôn mẫu.

+ Tái hiện: Sau đó, hệ thống sẽ chuyển khuôn mẫu này thành một mã độc nhất với từng người. Với mỗi khuôn mẫu, mã này có dạng một nhóm các con số đại diện cho khuôn mặt của một đối tượng.

+ So sánh: Nếu như hình ảnh này có dạng 3D và cơ sở dữ liệu cũng chứa các hình ảnh 3D, thì việc đối chiếu có thể tiến hành mà không phải thực hiện bất kỳ thay đổi nào đối với hình ảnh đó. Tuy vậy, nếu như hình ảnh vẫn ở dạng 2D thì sẽ có đôi chút khó khăn hơn, bởi công nghệ 3D đem lại hình ảnh thực và sống động hơn so với một hình ảnh 2D phẳng lì, bất động. Nhưng công nghệ mới có thể giải quyết được khó khăn này. Ví dụ, phần bên ngoài và bên trong của con mắt cùng với phần đỉnh mũi sẽ được lấy ra đo đạc. Sau khi việc đo đạc này hoàn tất, một thuật toán sẽ được áp dụng để chuyển hình ảnh trong cơ sở dữ liệu sang dạng 2D. Sau khi chuyển đổi, phần mềm sẽ so sánh hai hình ảnh 2D này với nhau để tìm ra đối tượng.

+ Xác minh và nhận diện:

* Xác minh có nghĩa là một hình ảnh sẽ được đối chiếu với chỉ 1 hình ảnh trong cơ sở dữ liệu (tỉ lệ 1:1). Ví dụ như, một hình ảnh của một đối tượng nào đó sẽ được đối chiếu với một hình ảnh trong cơ sở dữ liệu của Uỷ ban phương tiện giao thông để xác minh xem đối tượng đó là ai.
* Nhận diện có nghĩa là một hình ảnh sẽ được đối chiếu với tất cả các hình ảnh trong cơ sở dữ liệu để tìm ra đối tượng. Khi đó, bạn phải ghi lại hình ảnh đối tượng và so sánh với toàn bộ cơ sở dữ liệu để biết được đối tượng đó là ai.

**2.4. Thuật toán facenet**

- Facenet chính là một dạng siam network có tác dụng biểu diễn các bức ảnh trong một không gian eucledean nchiều (thường là 128) sao cho khoảng cách giữa các véc tơ embedding càng nhỏ, mức độ tương đồng giữa chúng càng lớn.

**2.4.1. Khái quát thuật toán**

- Hầu hết các thuật toán nhận diện khuôn mặt trước facenet đều tìm cách biểu diễn khuôn mặt bằng một véc tơ embedding thông qua một layer bottle neck có tác dụng giảm chiều dữ liệu.

* Tuy nhiên hạn chế của các thuật toán đó là số lượng chiều embedding tương đối lớn (thường >= 1000) và ảnh hưởng tới performance của thuật toán. Thường chúng ta phải áp dụng thêm thuật toán PCA để giảm chiều dữ liệu.
* Hàm loss function chỉ đo lường khoảng cách giữa 2 bức ảnh. Như vậy trong một đầu vào huấn luyện chỉ học được một trong 2 khả năng là sự giống nhau nếu chúng cùng 1 class hoặc sự khác nhau nếu chúng khác class giữa 2 bức ảnh.

Facenet đã giải quyết cả 2 vấn đề trên bằng các hiệu chỉnh nhỏ nhưng mang lại hiệu quả rất lớn:

* Base network áp dụng một mạng convolutional neural network và giảm chiều dữ liệu xuống chỉ còn 128 chiều. Do đó thuật toán classification ở những layer sau hoạt động nhanh hơn và đồng thời độ chính xác vẫn được đảm bảo.
* Sử dụng một hàm loss function đặc biệt có khả năng đánh mức độ khác biệt giữa các bức ảnh sao cho giá trị loss function của chúng càng lớn, sự khác biệt giữa chúng càng cao. Đó chính là triplot loss function.
* Hàm triplot loss có khả năng học được đồng thời sự giống nhau giữa 2 bức ảnh cùng nhóm và tìm cách phân biệt các bức ảnh nếu chúng không cùng nhóm. Do đó hiệu quả hơn rất nhiều so với các phương phát trước đây.

## 2.4.2. Triple loss

Trong facenet, quá trình encoding của mạng convolutional neural network đã giúp ta mã hóa bức ảnh về 128 chiều. Sau đó những véc tơ này sẽ làm đầu vào cho hàm loss function mà có tác dụng phân biệt tốt các véc tơ giống hoặc khác nhau. Đó chính là hàm loss function.

Để áp dụng triple loss, chúng ta cần lấy ra 3 bức ảnh trong đó có một bức ảnh là anchor. Anchor image cũng có tác dụng gần như vậy. Trong 3 ảnh thì ảnh anchor được cố định trước. Chúng ta sẽ lựa chọn 2 ảnh còn lại sao cho một ảnh là negative (của một người khác với anchor) và một ảnh là positive (cùng một người với anchor).

Kí hiệu ảnh Anchor, Positive, Negative lần lượt là A,P,N.

Mục tiêu của hàm loss function là tối thiểu hóa khoảng cách giữa 2 ảnh khi chúng là negative và tối đa hóa khoảng cách khi chúng là positive. Như vậy chúng ta kì vọng rằng:

* Ảnh Anchor và Positive giống nhau: khoảng cách d(A,P) sẽ nhỏ.
* Ảnh Anchor và Negative khác nhau: khoảng cách d(A,N) sẽ lớn.

Triplot loss function luôn lấy 3 bức ảnh làm input và trong mọi trường hợp ta kì vọng:

d(A,P)<d(A,N)(1)

Để làm cho khoảng cách giữa vế trái và vế phải lớn hơn, chúng ta sẽ cộng thêm vào vế trái một hệ số α không âm rất nhỏ. Khi đó (1) trở thành:

d(A,P)+α→||f(A)−f(P)||22+α≤≤d(A,N)||f(A)−f(N)||22

→||f(A)−f(P)||22−||f(A)−f(N)||22+α≤0

Như vậy hàm loss function sẽ là:

L(A,P,N)=∑i=0n||f(Ai)−f(Pi)||22−||f(Ai)−f(Ni)||22+α

Trong đó n là số lượng các bộ 3 hình ảnh được đưa vào huấn luyện.

Mục tiêu của chúng ta là giảm thiểu các trường hợp hợp mô hình nhận diện sai ảnh Negative thành Postive nhất có thể. Do đó để aloại bỏ ảnh hưởng của các trường hợp nhận diện đúng Negative và Positive. Ta sẽ điều chỉnh giá trị đóng góp của nó vào hàm loss function về 0.

Tức là nếu:

||f(A)−f(P)||22−||f(A)−f(N)||22+α≤0

sẽ được điều chỉnh về 0. Khi đó hàm loss function trở thành:

L(A,P,N)=∑i=0nmax(||f(Ai)−f(Pi)||22−||f(Ai)−f(Ni)||22+α,0)

Như vậy chúng ta có thể áp dụng Triple loss vào các mô hình convolutional neural network để tạo ra những thuật toán có tác dụng phát hiện ra những ảnh thuộc về cùng một người trong bộ 3 các ảnh đầu vào trong quá trình huấn luyện mô hình. Khi đó tại layer gần cuối cùng của siam network ta sẽ thu được những véc tơ biểu diễn ảnh tốt nhất cho một hình ảnh.

Một chú ý quan trọng khi huấn luyện mô hình siam network với triplot function đó là chúng ta luôn phải xác định trước cặp ảnh (A,P) thuộc về cùng một người. Ảnh N sẽ được lựa chọn ngẫu nhiên từ các bức ảnh thuộc các nhãn còn lại.

Do đó cần thu thập ít nhất 2 bức ảnh/1 người để có thể chuẩn bị được dữ liệu huấn luyện.

## 2.4.3. Lựa chọn triple images input

Nếu lựa chọn triple input một cách ngẫu nhiên có thể ảnh khiến cho bất đẳng thức (1) dễ dàng xảy ra vì trong các ảnh ngẫu nhiên, khả năng giống nhau giữa 2 ảnh là rất khó. Hầu hết các trường hợp đều thỏa mãn bất đẳng thức (1) và không gây ảnh hưởng đến giá trị của loss function do giá trị của chúng được set về 0. Như vật việc học những bức ảnh Negative quá khác biệt với Anchor sẽ không có nhiều ý nghĩa.

Để mô hình khó học hơn và đồng thời cũng giúp mô hình phân biệt chuẩn xác hơn mức độ giống và khác nhau giữa các khuôn mặt, chúng ta cần lựa chọn các input theo các bộ 3 khó học (hard triplets).

Ý tưởng là chúng ta cần tìm ra bộ ba (A,N,P) sao cho (1) là gần đạt được đẳng thức (xảy ra dấu =) nhất. Tức là d(A,P) lớn nhất và d(A,N) nhỏ nhất. Hay nói cách khác với mỗi Anchor A cần xác định:

* Hard Positive: Bức ảnh Positive có khoảng cách xa nhất với Anchor tương ứng với nghiệm:

argmaxPi(d(A,Pi))

* Hard Negative: Bức ảnh Negative có khoảng cách gần nhất với Anchor tương ứng với nghiệm:

argminNj(d(A,Nj))

Việc tính toán các trường hợp Hard Positive và Hard Negative có thể được thực hiện offline và lưu vào checkpoint hoặc có thể tính toán online trên mỗi mini-batch.

Chiến lược lựa chọn Triple images sẽ có ảnh hưởng rất lớn tới chất lượng của mô hình Facenet. Nếu lựa chọn Triplet images tốt, Facenet sẽ hội tụ nhanh hơn và đồng thời kết quả dự báo chuẩn xác hơn. Lựa chọn ngẫu nhiên dễ dẫn tới thuật toán không hội tụ.

**2.5. Vấn đề bảo mật trong các hệ thống sinh trắc học**

**2.5.1. Những cách thức, thủ đoạn xâm nhập trái phép**

Dữ liệu sinh trắc học của bạn tồn tại vĩnh viễn và duy nhất chỉ là của bạn. Việc để dữ liệu này bị lọt vào tay “hacker” sẽ làm mất tính bảo mật riêng tư cũng như an ninh của một hệ thống sinh trắc học.

Nếu các hacker muốn tiếp cận một hệ thống bảo mật bằng vân tay hoặc nhận diện khuôn mặt, họ có thể áp dụng các cách sau:

1. Thay vân tay hoặc nhận diện khuôn mặt của bạn (dữ liệu mẫu) bằng dữ liệu khác để giành quyền tiếp cận hệ thống
2. Tạo ra một bản sao vân tay hoặc khuôn mặt của bạn để giành quyền tiếp cận hệ thống
3. Đánh cắp dữ liệu mẫu để tái sử dụng để giành quyền tiếp cận hệ thống
4. Đánh cắp dữ liệu mẫu để theo dõi bất hợp pháp một cá nhân từ hệ thống này sang hệ thống khác.

**2.5.2. Các biện pháp bảo mật**

Ngày nay để bảo mật dữ liệu trong sinh trắc học, người ta đưa ra một loại các kỹ thuật mã hóa. các kỹ thuật này được chia làm hai loại: sinh trắc học giản ước được và các hệ thống mã hóa sinh trắc học

Kĩ thuật sinh trắc học giản ước được sẽ sử dụng các hàm số toán học phức hợp để chuyển đổi dữ liệu mẫu gốc khi vân tay hoặc khuôn mặt của bạn được quét. Một khi đã chuyển đổi thì dữ liệu không thể chuyển ngược lại được nữa, có nghĩa là dữ liệu mẫu là vân tay hoặc khuôn mặt bạn đã chuyển đổi thành dạng dữ liệu khác thì không có cách gì để chuyển dữ liệu này ngược trở lại thành dấu vân tay hoặc khuôn mặt bạn được nữa.

Trong trường hợp cơ sở dữ liệu lưu trữ dữ liệu đã chuyển đổi bị đột nhập thì các dữ liệu lưu trữ có thể bị xóa đi. Thêm vào đó, khi bạn quét vân tay hoặc khuôn mặt lại một lần nữa thì hình ảnh quét sẽ cho ra một dữ liệu mới tinh không hề trùng với dữ liệu cũ, ngay cả khi bạn quét lại cùng một ngón tay hoặc đúng khuôn mặt bạn ngay sau lần quét trước.

Đối với các hệ thống mã hóa sinh trắc học, dữ liệu mẫu gốc được kết hợp với một khóa mật mã để tạo ra một “hộp đen”.Khóa mật mã là “bí mật” và dữ liệu truy vấn là “chìa khóa” mở “hộp đen” để lấy lại được “bí mật”. Khóa mật mã chỉ được cung cấp sau khi xác thực thành công.

Ngăn chặn những mối đe dọa này là một trong những vấn đề áp lực nhất mà các nhà thiết kế gặp phải khi họ thiết kế các hệ thống anh ninh nhận diện sinh trắc học dựa vào AI.

Các kĩ thuật mã hóa đang áp dụng cho các hệ thống sinh trắc học không dựa vào AI hiện nay không tương thích với các hệ thống sinh trắc học dựa vào AI, vì thế cần phải có kĩ thuật bảo vệ mới.

Các nhà nghiên cứu khoa học và các nhà sản xuất máy quét sinh trắc học nên phối hợp với nhau để đảm bảo an toàn cho dữ liệu mẫu sinh trắc học nhạy cảm của người dùng thiết bị, như vậy mới có thể giảm thiểu rủi ro cho người dùng.