ĐẠI HỌC QUỐC GIA TPHCM

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN MÔN HỌC

MÁY HỌC – CS114.K21.KHTN

ĐỀ TÀI:

PHÁT HIỆN KHUÔN MẶT BỊ MẠO DANH BỞI ĐIỆN THOẠI DI ĐỘNG

SINH VIÊN THỰC HIỆN:

Nguyễn Văn Tiến – 18521489

GIẢNG VIÊN HƯỚNG DẪN:

PGS TS. Lê Đình Duy

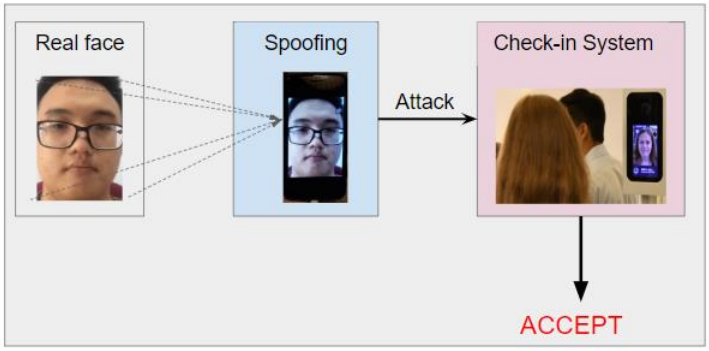
Ths. Phạm Nguyễn Trường An

TP.HCM, ngày 1 tháng 8 năm 2020

Trang này để trống

LỜI MỞ ĐẦU

Ngày nay, sự phát triển của Trí tuệ nhân tạo cùng với các kĩ thuật, nghiên cứu được ứng dụng vào thực tế ngày càng phổ biến. Trong đó, nhận diện khuôn mặt là hướng được nghiên cứu và triển khai phổ biến thành các ứng dụng trong thực tế. Các hệ thống nhận diện bằng khuôn mặt xác nhận danh tính của người dùng với các yêu cầu như thanh toán, check-in. Tuy nhiên, hệ thống nhận diện khuôn mặt có thể bị đánh lừa bởi việc sử dụng hình ảnh của người dùng được ghi lại qua điện thoại hay hình ảnh được in, mặt nạ,… ảnh hưởng nghiêm trọng đến tính bảo mật thông tin người dùng và tính chính xác của hệ thống.



Hình 1. Đánh lừa hệ thống phát hiện khuôn mặt bởi điện thoại di động

Phát hiện khuôn mặt bị mạo danh (Face anti-spoofing detection) sẽ nâng cao tính an toàn cho các hệ thống nhận diện khuôn mặt. Tuy nhiên,. khuôn mặt của người dùng có thể bị mạo danh bởi nhiều hình thức: ảnh chụp của người dùng trong điện thoại di động, ảnh chân dung được in, các kĩ thuật giả mạo khuôn mặt như Deep Face,… đây chính là một trong các thách thức của bài toán. Việc sử dụng điện thoại di động là phương pháp dễ dàng thực hiện, khả năng hệ thống nhận diện khuôn mặt bị tấn công bởi hình thức này rất cao.

Vì vậy, trong đề tài này em sẽ:

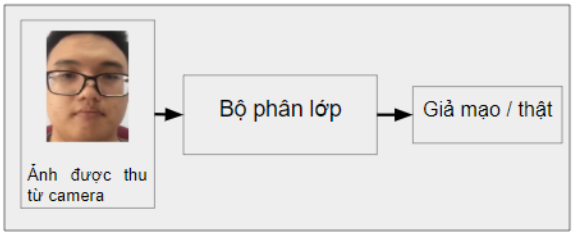
- Tìm hiểu bài toán phát hiện khuôn mặt bị giả mạo bởi điện thoại di động.
- Xây dựng tập dữ liệu cho bài toán.
- Thực nghiệp, đánh giá các phương pháp tiếp cận trên dữ liệu được thu thập và dữ liệu có sẵn trên internet.
- Xây dựng demo minh họa cho bài toán.

MỤC LỤC

I. TỔNG QUAN BÀI TOÁN

1. Mô tả bài toán

Bài toán được phát biểu như sau: xác định mặt người trong hình ảnh được thu bằng camera phải là khuôn mặt được phát từ điện thoại hay không.



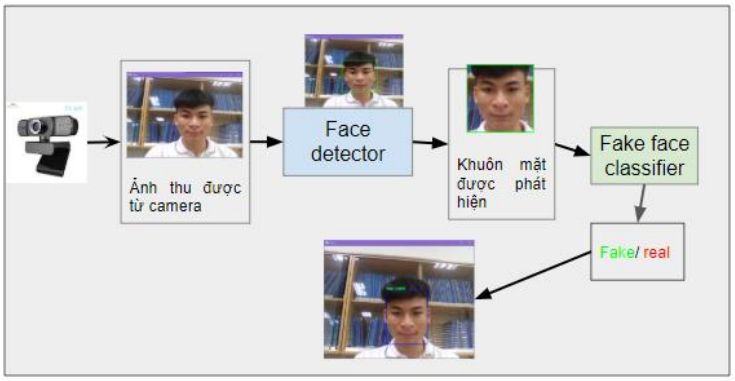
Hình 2. Đầu vào và đầu ra của bài toán

- Đầu vào: đoạn video/ảnh chứa khuôn mặt chưa biết là khuôn mặt của người thật hay khuông mặt mạo danh.

- Đầu ra: Cho ra giá trị 1 (“Giả mạo”), hoặc 0 (“Thật”) thể hiện dự đoán của mô hình cho ảnh đầu vào đang chứa khuôn mặt giả mạo hay mặt của người thật.

2. Quá trình phát hiện khuôn mặt mạo danh

Tại mỗi thời điểm, nếu có mặt người (chưa rõ là mạo danh hay người thật) xuất hiện trong hình ảnh thu được, một detector phát hiện khuôn mặt và gửi hình ảnh của vùng chứa khuôn mặt cho một bộ phân lớp (classifier) để phân loại xem khuôn mặt thu nhận được là mặt giả mạo hay là của người thật.



Hình 3. Quá trình phát hiện khuôn mặt mạo danh

II. DỮ LIỆU CHO BÀI TOÁN

1. Phương pháp xây dựng tập dữ liệu

Cách thức xây dựng dữ liệu

- Dữ liệu được thu thập gồm có hai lớp là ảnh chứa khuôn mặt thật và khuôn mặt mạo danh.
- Dữ liệu ảnh chứa khuôn mặt thật được rút trích từ video selfie ghi lại khuôn mặt thật của đối tượng người thật.
- Dữ liệu khuôn mặt giả mạo danh được rút trích từ video ghi lại khuôn mặt giả mạo của một/nhiều đối tượng.

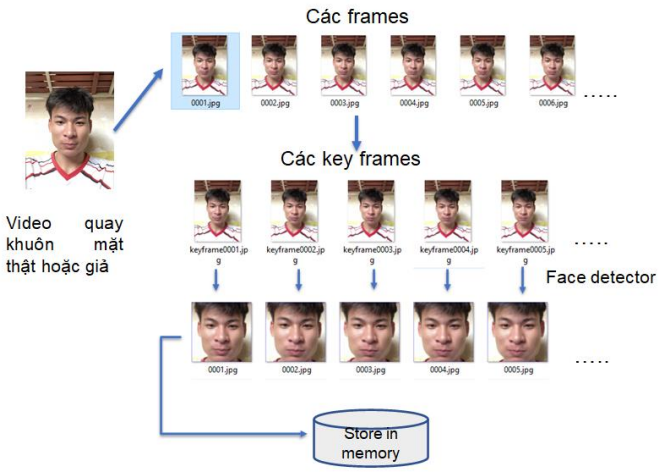
Quy trình xây dựng bộ dữ liệu

Xây dựng bộ dữ liệu khuôn mặt thật

- Bước 1: Sử dụng điện thoại di động ghi lại 30s selfie bản thân khi đang di chuyển (nhằm xây dựng dữ liệu cho lớp dữ liệu khuôn mặt thật).
- Bước 2: Sử dụng thuật toán face detection được hỗ trợ trong thư viện OpenCV để cắt các vùng chứa khuôn mặt trong mỗi fame của 2 video ghi được và lưu tương ứng vào hai thư mục là real.
- Bước 3: Lặp lại bước 1, 2 đối với người khác.

Xây dựng bộ dữ liệu khuôn mặt mạo danh từ dữ liệu thật

- Bước 1: Sử dụng điện thoại di động quay đoạn video ghi khuôn mặt thật ở trên(nhằm xây dựng dữ liệu cho lớp khuôn mặt mạo danh).
- Bước 2: Sử dụng thuật toán face detection được hỗ trợ trong thư viện OpenCV để cắt các vùng chứa khuôn mặt trong mỗi fame của 2 video ghi được và lưu tương ứng vào hai thư mục là fake.
- Bước 3 (giấy in màu): Lặp lại bước 1,2 đối với video khác.



Hình 4. Quá trình xây dựng dữ liệu

Tiền xử lý dữ liệu

Phát hiện mờ

Khi khuôn mặt được cắt ra bởi thuật toán face detection, ta sử dụng một classifier phát hiện xem ảnh có mờ hay không để loại bỏ.

Rút trích đặc trưng và lưu xuống file

Với cách tiếp cận sử dụng các đặc trưng LBPs (sẽ được trình bày ở phần sau), lưu các vector đặc trưng của tập dữ liệu thành một file để khi cần xử lý thì load lên nhanh chóng.

2. Tập dữ liệu Collection

Tập dữ liệu Collection được thu thập với thông tin như sau:

- Số lượng dữ liệu: 1912 ảnh
- Số lượng dữ liệu của mỗi lớp:
  - Mạo danh (fake): 1115 ảnh.
  - Thật (real): 797 ảnh.

Video selfie gồm có 5 video tương ứng với 5 người khác nhau. Mỗi video được ghi lại với điều kiện chiếu sáng khác nhau với background ít thay đổi.

3. Tập dữ liệu ROSE-Youtu

Tập dữ liệu ROSE-Youtu được lấy từ internet với thông tin như sau:

- Số lượng dữ liệu: 10604 ảnh
- Số lượng dữ liệu mỗi lớp:
    - Mạo danh (fake): 2382 ảnh.
    - Thật (real): 8222 ảnh.

Tập dữ liệu ROSE-Youtu là một tập dữ liệu video lớn cho bài toán chống mạo danh khuôn mặt, dữ liệu bao gồm các trường hợp mạo danh như dùng điện thoại di động, sử dụng mặt nạ, … Tập dữ liệu được dùng trong bài toán được rút trích từ những video liên giả mạo qua điện thoại di động được cung cấp.

III. CÁC PHƯƠNG PHÁP TIẾP CẬN BÀI TOÁN

1. Phương pháp dựa trên đặc trưng do chuyên gia đề xuất.

Đặc trưng do chuyên gia đề xuất (hand-crafted features)

Khi giải quyết một bài toán máy học, ta phải trải qua các bước để đạt được mô hình sau cùng cho ta độ tốt có thể chập nhận được. Trong quy trình máy học, hai giai đoạn Feature engineering (chế tác đặc trưng) và Training model (huấn luyện mô hình) được xử lý riêng biệt. Các phương pháp sử dụng để chế tác đặc trưng từ ảnh như một số phương pháp:

- SIFT(Scale Invariant Feature Transform).
- SURF (Speeded-Up Robust Features).
- HOG (Histogram of Oriented Gradients).
- LBP (Local Binary Pattern).

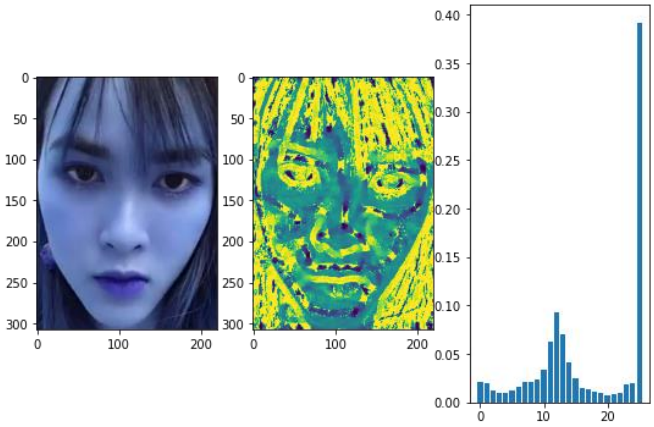
Các phương pháp chế tác đặc trưng được nêu bên trên được gọi là đặc trưng chế tác một cách thủ công vì các đặc trưng này dựa trên các quan sát về đặc tính riêng của ảnh (còn gọi là đặc trưng do chuyên gia đề xuất). Sau quá trình rút trích đặt trưng, ta đi đến giai đoạn huấn luyện bộ phân lớp (training classifier).

Local Binary Patterns

Phương pháp Local Binary Patterns là một phương pháp dùng để rút trích các đặc trưng bên trong hình ảnh dựa trên các phép toán trên các pixel lân cận (local operation). Input là một ảnh, output là một vector đặc trưng. Dưới đây là quá trình tính toán của phương pháp LBPs.

- Bước 1: Chuyển hình ảnh đầu vào về ảnh thang độ xám (grayscale).
- Bước 2: Với mỗi pixel tại vị trí (i,j) ta thực hiện các bước:
- Bước 3: Chọn vùng lân cận pixel đó với kích thước là r , với tâm là pixel hiện tại.
- Bước 4: Tính giá trị LBPs của pixel đó, outut của bước này là một mảng hai chiều có kích thước $r \times r$.

- Bước 5: Duỗi mảng hai chiều ở bước trên thành một chuỗi nhị phân (theo chiều kim đồng hồ hoặc ngược chiều kim).
- Bước 6: Chuyển giá trị chuỗi nhị phân về hệ cơ số 10 và lưu vào một ma trận M tại vị trí (i,j) giá trị vừa lấy được.
- Bước 7: Tính histogram của ma trận ở bước 6, ta thu được một vector đặc trưng.



Hình 5. Mô tả quá trình rút trích đặc trưng bằng LBPs.

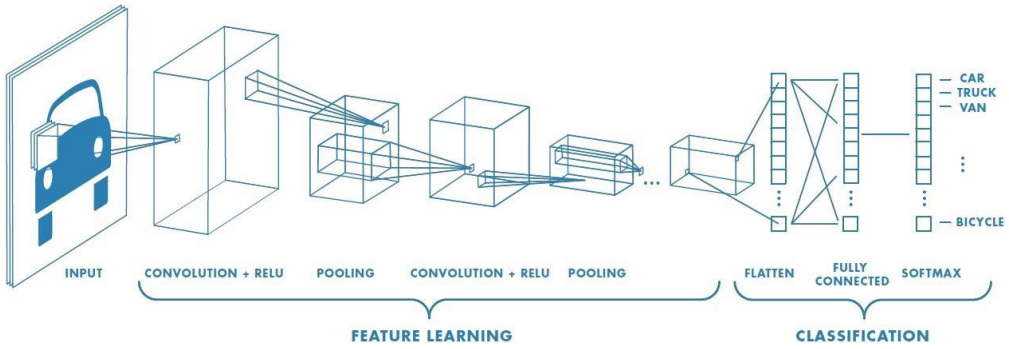
Các tham số liên quan đến việc rút trích đặt trưng bằng phương pháp Local Binary Patterns đó là (p, r), trong đó:

- p là số lượng giá trị được quan xét đến xung quanh pixel hiện tại.
- r là bán kính của đường tròn với tâm là pixel đang xét.

2. Phương pháp dựa trên đặc trưng học sâu.

Thay vì phân biệt hai giai đoạn: rút trích đặc trưng và huấn luyện mô hình phân lớp, phương pháp dựa trên đặc trưng học sâu sẽ nhận dữ liệu đầu vào và **học** được các đặc trưng bên trong hình ảnh và dùng đặ trưng đó đi huấn luyện bộ phân lớp. Phương pháp deep learning có độ chính xác cao trong hầu hết các bài toán của máy học nên thường được xem là giải pháp cho các hệ thống yêu cầu độ hiệu năng cao.

Mạng neuron tích chập (Convolutional Neuron Networks - CNNs) là xương sống của các kiến trúc mạng điển hình của phương pháp deep learning, tầng của mô hình được xếp chồng lên nhau giúp cho việc học được các đặc trưng tốt hơn.



Hình 6. Phương pháp dựa trên deep learning sử dụng CNNs.

3. Mô tả phương phép thử nghiệm

Dưới đây là mô tả các phép thử bằng hai phương pháp tiếp cận và 3 bộ dữ liệu.

Đối với phương pháp dựa trên đặc trưng do chuyên gia đề xuất.

- Với mỗi tập dữ liệu:
  - Rút trích đặt trưng từ của tất cả các ảnh bằng phương pháp Local Binary Patterns với các tham số (p, r) bên dưới và lưu xuống file kèm theo nhãn của từng vector đặc trưng:

p	**r**
8	1
8	2
8	4
16	4
16	6
24	6
24	8

  - Với mỗi bộ vector đặc trưng rút trích tương ứng từ tập dữ liệu, huấn luyện các bộ phân lớp sử dụng thư viện scikit-learn, bao gồm:
    - Logistic regression.
    - K-nearest neighbor.
    - Random forest.

        - Decision tree.
        - Naïve bayes.
        - Support vector machine (SVMs)
        - Multilayer Perceptron.
- Một số tham số thử nghiệm:
    - Test size (kích thước tập dữ liệu kiểm thử):
        - 25% đối với 3 bộ dữ liệu với 7 bộ tham số (p, r).

Đối với phương pháp deep learning

- Với mỗi tập dữ liệu:
    - Chia thành 2 phần riêng biệt:
        - Dữ liệu huấn luyện(training set) dùng để huấn luyện mô hình.

Dữ liệu kiểm thử (test set) dùng để đánh giá mô hình sau khi huấn luyện.

    - Phần huấn luyện mô hình:
        - Load dữ liệu vào bộ nhớ và resize ảnh về kích thước $n \times n \times 3$, và tiến huấn huấn luyện mô hình.
        - Các tham số của mô hình được sử dụng là:
            - Learning rate $\eta = 10^{-4}$.
            - Tỉ lệ phân chia dữ liệu: 75% dữ liệu huấn luyện, 25 % dữ liệu kiểm thử.
            - Kích thước ảnh được resize là 64x64.
            - Số lượng Epochs (số lần duyệt qua toàn bộ dữ liệu) là 50.
            - Batch size (số lượng mẫu dữ liệu cho một lần huấn luyện mô hình) là 32 ảnh.

IV. THỰC NGHIỆM VÀ ĐÁNH GIÁ

1. Kết quả thực nghiệm

Sử dụng đặc trưng LBPs

Bộ dữ liệu Collection

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.91	0.91	0.87	1	0.93
kNN	1	0.99	1.0	1.0	1
Random forest	0.97	0.96	0.95	0.99	0.97
Decision tree	1	0.98	0.98	0.99	0.99
Naive bayes	0.96	0.96	0.95	0.98	0.97
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	0.98	0.98	0.98	1	0.99

Bộ tham số (8, 1)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.99	0.98	0.98	1	0.99
kNN	1.0	1.0	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	0.99	0.99	0.99	1.0	0.99
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	1.0	0.99	1	1	1.0

Bộ tham số (8, 2)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.99	0.99	1.0	0.99	0.99
kNN	1.0	1.0	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	1.0	1.0	1.0	0.99	1.0
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	0.99	0.98	0.99	0.99	0.99

Bộ tham số (8, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.99	0.99	1.0	0.99	0.99
kNN	1.0	1.0	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	1.0	1.0	1.0	0.99	1.0
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	0.99	0.98	0.99	0.99	0.99

Bộ tham số (16, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.99	0.98	0.99	0.99	0.99
kNN	1.0	1.0	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	0.99	0.99	1.0	0.99	1.0
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	1.0	1.0	1.0	1.0	1.0

Bộ tham số (16, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.99	0.98	0.99	0.99	0.99
kNN	1.0	0.99	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	0.99	0.99	1.0	0.98	0.99
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	0.58	0.59	0.59	1.0	0.74

Bộ tham số (24, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.98	0.98	0.99	0.98	0.99
kNN	1.0	1.0	1.0	1.0	1.0
Random forest	1.0	1.0	1.0	1.0	1.0
Decision tree	1.0	1.0	1.0	1.0	1.0
Naive bayes	0.99	0.99	1.0	0.99	0.99
SVMs	1.0	1.0	1.0	1.0	1.0
MLPs	0.58	0.59	0.59	1.0	0.74

Bộ tham số (24, 6)

Bộ dữ liệu ROSE-Youtu

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.77	0.78	0.97	0.03	0.05
kNN	0.99	0.95	0.86	0.98	0.91
Random forest	0.81	0.82	0.98	0.18	0.3
Decision tree	1.0	0.97	0.95	0.94	0.94
Naive bayes	0.74	0.75	0.43	0.42	0.43
SVMs	0.90	0.90	0.87	0.69	0.77
MLPs	0.80	0.81	0.80	0.19	0.3

Bộ tham số (8, 1)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.77	0.78	0.75	0.00	0.01
kNN	0.99	0.96	0.89	0.98	0.93
Random forest	0.79	0.80	0.99	0.1	0.18
Decision tree	1.0	0.97	0.94	0.94	0.94
Naive bayes	0.65	0.66	0.36	0.62	0.45
SVMs	0.88	0.88	0.91	0.53	0.67
MLPs	0.80	0.81	0.79	0.24	0.37

Bộ tham số (8, 2)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.78	0.78	0.95	0.05	0.09
kNN	0.99	0.98	0.94	0.98	0.96
Random forest	0.81	0.81	0.86	0.22	0.35
Decision tree	1.0	0.98	0.96	0.96	0.96
Naive bayes	0.66	0.67	0.37	0.61	0.46
SVMs	0.88	0.88	0.94	0.53	0.68
MLPs	0.81	0.82	0.79	0.29	0.42

Bộ tham số (8, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.77	0.78	0.9	0.02	0.05
kNN	0.99	0.98	0.94	0.98	0.96
Random forest	0.81	0.82	0.88	0.24	0.38
Decision tree	1.0	0.97	0.94	0.95	0.94
Naive bayes	0.67	0.67	0.37	0.64	0.47
SVMs	0.95	0.94	0.93	0.79	0.85
MLPs	0.81	0.82	0.71	0.31	0.43

Bộ tham số (16, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.79	0.76	0.13	0.23
kNN	1.0	1.0	0.97	0.99	0.98
Random forest	0.81	0.82	0.86	0.22	0.35
Decision tree	1.0	0.98	0.97	0.96	0.97
Naive bayes	0.69	0.70	0.39	0.61	0.48
SVMs	0.95	0.95	0.94	0.83	0.88
MLPs	0.79	0.80	0.68	0.19	0.29

Bộ tham số (16, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.79	0.76	0.11	0.2
kNN	0.99	0.99	0.96	0.99	0.98
Random forest	0.81	0.81	0.94	0.19	0.31
Decision tree	1.0	0.97	0.95	0.95	0.95
Naive bayes	0.68	0.69	0.38	0.63	0.48
SVMs	0.97	0.95	0.95	0.86	0.9
MLPs	0.79	0.79	0.78	0.11	0.2

Bộ tham số (24, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.80	0.7	0.17	0.27
kNN	1.0	0.99	0.97	0.99	0.98
Random forest	0.82	0.82	0.88	0.24	0.38
Decision tree	1.0	0.98	0.96	0.95	0.95
Naive bayes	0.71	0.73	0.43	0.67	0.52
SVMs	0.97	0.96	0.95	0.9	0.93
MLPs	0.79	0.79	0.74	0.13	0.21

Bộ tham số (24, 8)

Bộ dữ liệu ROSE-Youtu+Collection

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.78	0.79	1.0	0.02	0.03
kNN	0.97	0.92	0.76	0.9	0.82
Random forest	0.82	0.82	0.97	0.15	0.26
Decision tree	1.0	0.89	0.76	0.76	0.76
Naive bayes	0.74	0.74	0.4	0.38	0.39
SVMs	0.89	0.89	0.86	0.59	0.7
MLPs	0.81	0.81	0.65	0.30	0.41

Bộ tham số (8, 1)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.8	0.8	0.99	0.22	0.35
kNN	0.99	0.95	0.87	0.98	0.92
Random forest	0.8	0.8	0.99	0.22	0.36
Decision tree	1.0	0.96	0.93	0.95	0.94
Naive bayes	0.77	0.77	0.63	0.25	0.36
SVMs	0.86	0.87	0.92	0.53	0.68
MLPs	0.8	0.8	0.87	0.25	0.39

Bộ tham số (8, 2)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.79	1.0	0.2	0.33
kNN	1.0	0.98	0.92	0.99	0.96
Random forest	0.82	0.82	0.9	0.33	0.49
Decision tree	1.0	0.97	0.95	0.96	0.95
Naive bayes	0.79	0.79	0.71	0.3	0.42
SVMs	0.86	0.86	0.95	0.47	0.63
MLPs	0.8	0.8	0.75	0.33	0.46

Bộ tham số (8, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.79	1.0	0.19	0.32
kNN	0.97	0.98	0.95	1.0	0.97
Random forest	0.82	0.82	0.93	0.32	0.48
Decision tree	1.0	0.98	0.96	0.96	0.96
Naive bayes	0.79	0.79	0.73	0.31	0.43
SVMs	0.89	0.89	0.94	0.60	0.73
MLPs	0.8	0.8	0.75	0.33	0.46

Bộ tham số (16, 4)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.8	1.0	0.21	0.35
kNN	1.0	1.0	0.96	1.0	0.98
Random forest	0.82	0.82	0.96	0.31	0.47
Decision tree	1.0	0.98	0.96	0.96	0.96
Naive bayes	0.8	0.8	0.79	0.33	0.47
SVMs	0.9	0.9	0.94	0.65	0.77
MLPs	0.83	0.82	0.75	0.46	0.57

Bộ tham số (16, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.79	1.0	0.2	0.33
kNN	1.0	0.99	0.95	1.0	0.98
Random forest	0.82	0.82	0.98	0.3	0.45
Decision tree	1.0	0.98	0.95	0.96	0.96
Naive bayes	0.81	0.8	0.76	0.33	0.46
SVMs	0.93	0.92	0.93	0.75	0.83
MLPs	0.83	0.82	0.79	0.40	0.53

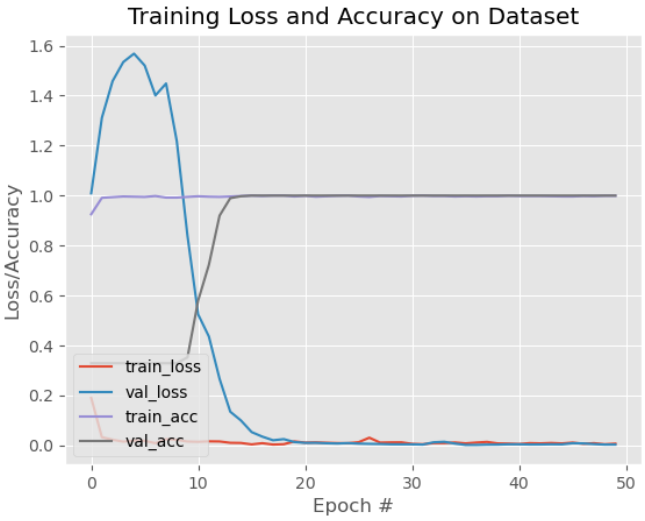
Bộ tham số (24, 6)

Model	Accuracy training set	Accuracy	Precision	Recall	F1
Logistic reg	0.79	0.8	1.0	0.19	0.32
kNN	1.0	1.0	0.97	1.0	0.98
Random forest	0.81	0.81	0.98	0.27	0.42
Decision tree	1.0	0.98	0.96	0.96	0.96
Naive bayes	0.81	0.81	0.78	0.35	0.48
SVMs	0.94	0.32	0.93	0.79	0.86
MLPs	0.83	0.82	0.75	0.44	0.56

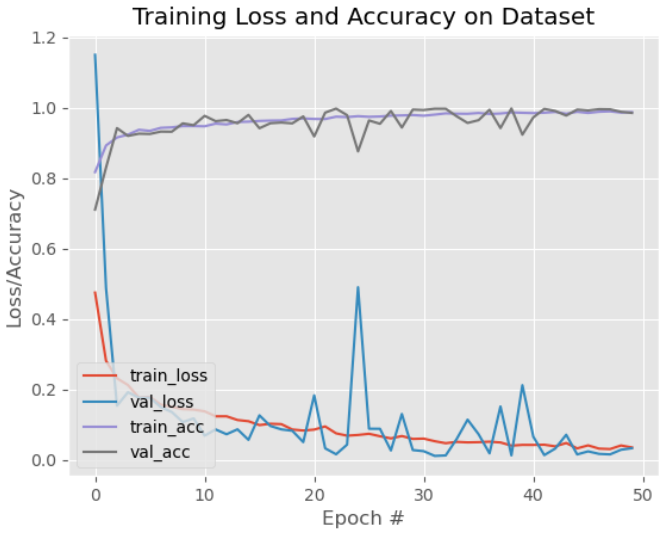
Bộ tham số (24, 8)

Phương pháp dựa trên đặc trưng học sâu

Dataset	Accuracy (training set)	Accuracy	Precision	Recall	$F_{1_{score}}$
Collection	0.99	0.22	0.2	1.0	0.36
ROSE-Youtu	0.98	0.19	0.2	1.0	0.33
ROSE-Youtu+Collection	0.98	0.2	0.2	1.0	0.33



a. Tập dữ liệu Colection



b. Tập dữ liệu ROSE-Youtu

c. Tập dữ liệu ROSE-Youtu+Collection

Hình 7. Quá trình huấn luyện trên các tập dữ liệu.

2. Đánh giá

Vấn đề về dữ liệu

- Tập dữ liệu được thu thập được chưa đủ lớn, đủ đa dạng nên các bộ phân lớp sau huấn luyện luôn có độ chính xác cao (ở Collection dataset, ta thấy với các bộ tham số khác nhau thì các bộ phân lớp đều cho độ chính xác từ 0.99 trở lên), trong khi

đối với tập dữ liệu ROSE-Youtu thì độ chính xác không còn cao và ổn định. Phép thử dùng một mô hình huấn luyện trên Collection dataset sau đó test trên một phần dữ liệu của tập dữ liệu ROSE-Youtu có thể chứng tỏ được vấn đề.

Vấn đề về phương pháp tiếp cận

- Phương pháp tiếp cận sử dụng đặc trưng LBPs kết hợp với bộ phân lớp kNN (K-nearest Neighbor) cho hiệu quả tốt hơn so với các bộ phân lớp khác được thử trong thí nghiệm trên cả 3 tập dữ liệu
- Phương pháp tiếp cận sử dụng đặc trưng học sâu không có kết quả tốt trên 3 tập dữ liệu.
- Khi đưa ra ngoài thực tế sử dụng, mô hình dựa trên đặc trưng học sâu cho độ chính xác cao và đáp ứng thời gian thực thi tốt hơn mô hình kNN.

Vấn đề về thử nghiệm tham số cho mô hình

- Các bộ tham số khác nhau trong việc rút đặc trưng bằng phương pháp Local Binary Patterns có ảnh hưởng đến hiệu quả của bộ phân lớp.

V. TỔNG KẾT ĐỀ TÀI

1. Nội dung đề tài thực hiện

Đề tài ứng dụng máy học bài toán trong thực tế, cụ thể là dùng phương pháp máy học giải quyết bài toán Phát hiện khuôn mặt mạo danh qua điện thoai di động. Quá trình thực hiện đề tài trải qua các giai đoạn:

- Khảo sát các hướng tiếp cận của bài toán
- Khảo sát cách xây dựng dữ liệu, xây dựng dữ liệu.
- Thực nghiệm và đánh giá với một số bộ tham số cho các mô hình phân lớp trên bộ dữ liệu tự xây dựng và bộ dữ liệu thu thập từ internet.
- Xây dựng demo minh họa cho bài toán chạy trên máy tính cá nhân.

Các thông tin tài liệu liên quan đến đề tài

- Tập dữ liệu được dùng trong đề tài: https://drive.google.com/drive/folders/1aN2imtjYQW9PwljJGO5Zu4HwXBFEB7hl?usp=sharing
- Repository chứa source code của đồ án: https://github.com/tiennvuit/CS114.K21.KHTN/tree/master/Capstone_FakeFaceDetection
- Video demo:

2. Bàn luận

Bài toán Phát hiện mạo danh khuôn mặt có vai trò quan trọng trong các hệ thống hiện đại ngày nay. Phương pháp này có thể ngăn chặn các hành vi lạm dụng dữ liệu lưu trữ trong điện thoại để dánh cấp thông tin của cá nhân khác.

Tuy nhiên chúng ta có thể đánh lừa một hệ thống trí tuệ nhân tạo một cách dễ dàng nên các hệ thống tích hợp phát hiện khuôn mặt phải có khả năng đưa ra các phán đoán chính xác trước các tình huống. Đề tài này chỉ xoay quanh vấn đề về mạo danh qua hình ảnh cá

nhân được lưu trong điện thoại nên chưa khái quát hóa các trường hợp trong thực tế, vì vậy một số hướng phát triển của đề tài có thể là:

- Xây dựng dữ liệu cho các trường hợp khác như sử dụng ảnh chân dung được in, sử dụng mặt na, các vật che đậy, các kỹ thuật mới trong xây dựng khuôn mặt mạo danh như Deep Face, FaceSwap.
- Về mặt phương pháp cần phải thử nghiệm nhiều phương pháp tốt hơn có thể sử dụng cho bài toán này như:
    - Các thuật toán dựa trên Heuristic
    - Thuật toán Optical Flow.
    - Face 3D.

-

TÀI LIỆU THAM KHẢO

[1] Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing, Joel Stehouwer, Amin Jourabloo, Yaojie Liu, Xiaoming Liu, IEEE, 2020.

[2] H. Li, W. Li, H. Cao, S. Wang, F. Huang and A. C. Kot, "Unsupervised Domain Adaptation for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1794-1809, July 2018, doi: 10.1109/TIFS.2018.2801312.

[3] A. Khodabakhsh, R. Ramachandra, K. Raja, P. Wasnik and C. Busch, "Fake Face Detection Methods: Can They Be Generalized?," 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, 2018, pp. 1-6, doi: 10.23919/BIOSIG.2018.8553251.