


MẪU BÁO CÁO LUẬN VĂN

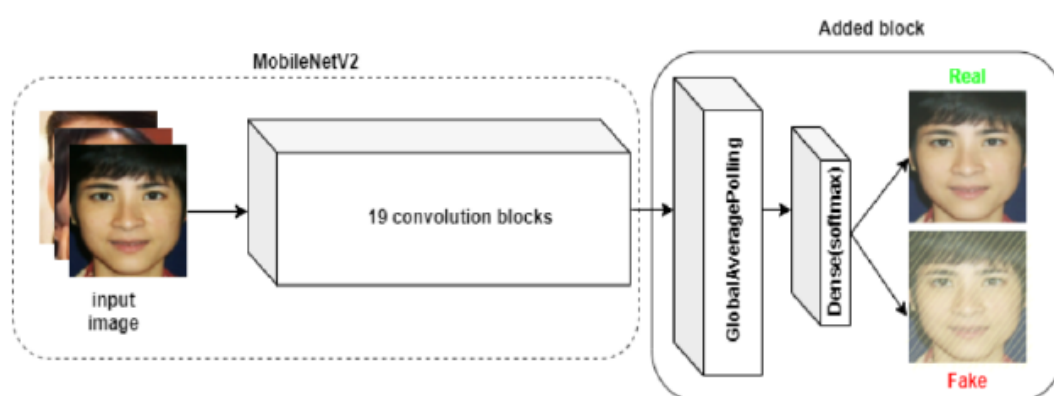
Họ và tên (IN HOA)	TRẦN VĂN BẢO
Ảnh	
Số buổi vắng	0
Bonus	5
Tên đề tài (VN)	XÂY DỰNG KIẾN TRÚC MẠNG NƠ-RON TRONG PHÁT HIỆN GIẢ MẠO KHUÔN MẶT DỰA TRÊN MẠNG NƠ-RON MOBILENETV2
Tên đề tài (EN)	OPTIONAL - KHÔNG BẮT BUỘC
Giới thiệu	<p><i>Hướng dẫn:</i></p> <ul style="list-style-type: none"><i>Bài toán/vấn đề mà đề tài muốn giải quyết</i> <p>Hiện tại, nhận dạng khuôn mặt là một trong những yếu tố quan trọng nhất đối với cách hệ thống xác thực danh tính. Tuy nhiên nó phải đối mặt với rất nhiều thách thức gây ra bởi các cuộc tấn công giả mạo. Do đó, các hệ thống xác thực cần sử dụng những thuật toán chống giả mạo mạnh mẽ và có khả năng chạy được với các thiết bị có cấu hình thấp.</p> <ul style="list-style-type: none"><i>Lí do chọn đề tài, khả năng ứng dụng thực tế, tính thời sự</i>

Các cuộc tấn công giả mạo đã trở thành mối đe dọa bảo mật nghiêm trọng cho các hệ thống xác thực, do chúng có thể truy cập trái phép vào hệ thống bằng cách mạo danh người được ủy quyền. Nhằm đối phó với những thách thức này, một số kỹ thuật chống giả mạo đã được phát triển để phát hiện những hành vi giả mạo. Các hệ thống chống giả mạo dựa trên mạng nơ-ron tích chập gần đây đã thể hiện sự hiệu quả vượt trội của chúng so với các phương pháp truyền thống.

Tuy nhiên, có một xu hướng mới là nhận dạng khuôn mặt đang dần chuyển sang các thiết bị di động hoặc thiết bị nhúng. Điều này yêu cầu thuật toán chống giả mạo khuôn mặt cần được cải tiến để chạy với chi phí tính toán và lưu trữ ít hơn. Từ quan điểm này, việc thiết kế các thuật toán chống giả mạo dựa trên mạng nơ-ron tích chập trở nên thách thức hơn trong môi trường di động hoặc nhúng. Do đó, phát triển một thuật toán học sâu đủ tốt để có thể chạy được trên các thiết bị cấu hình thấp nhưng vẫn đáp ứng được độ chính xác của thuật toán vẫn đang cần nhiều đầu tư nghiên cứu.

Vì thế đề tài này đề xuất một mạng nơ-ron phát triển từ mô hình MobileNetV2 được phát triển bởi Google có khả năng chạy trên các thiết bị cấu hình thấp nhưng vẫn đáp ứng được độ chính xác.

- *Mô tả input và output, nên có hình minh họa*



Input: Hình ảnh khuôn mặt cần kiểm tra

Output: Kết quả kiểm tra là thực hay giả.

Mục tiêu	<ul style="list-style-type: none"> • Trong vòng 3 ý • Lưu ý viết sao cho có thể đánh giá/lượng hoá được như thế nào là đạt được mục tiêu <p>Nghiên cứu phương pháp phát hiện giả mạo khuôn mặt bằng phương pháp truyền thống.</p> <p>Nghiên cứu phương pháp phát hiện giả mạo khuôn mặt bằng phương pháp sử dụng mạng nơ-ron tích chập CNNs.</p> <p>Đề xuất một mạng nơ-ron dựa trên một mô hình mạng đã được huấn luyện của Google là MobilenetV2</p>
Nội dung và phương pháp thực hiện	<ul style="list-style-type: none"> - Viết chi tiết các nội dung và phương pháp để đạt mục tiêu - Lưu ý Mục tiêu → Nội dung → Phương pháp phải có kết nối với nhau. <p>Nội dung 1: Phân loại nhị phân bằng phương pháp sử dụng vector hỗ trợ (Support Vector Machine -SVM).</p> <ul style="list-style-type: none"> - Nghiên cứu trích chọn các đặc trưng bằng các bộ lọc khác nhau - Phân loại ảnh thật hay giả bằng thuật toán SVM hoặc Random Forest <p>Nội dung 2: Sử dụng mạng nơ-ron tích chập CNNs.</p> <ul style="list-style-type: none"> - Sử dụng duy nhất một khung hình màu RGB kết hợp với bộ phân loại. - Sử dụng mạng CNN với nhiều khung ảnh RGB kết hợp với phương pháp đo áp lực tĩnh mạch Remote Photoplethysmography (rPPG) để đưa ra quyết định. - Kết hợp nhiều loại ảnh RGB, ảnh hồng ngoại, ảnh 3D trên cùng một đối tượng để truyền vào mạng CNN nhằm trích chọn đặc trưng và đưa ra quyết định. <p>Nội dung 3:</p> <ul style="list-style-type: none"> - Xây dựng mô hình mạng đã được huấn luyện của Google là MobilenetV2 - Tinh chỉnh và tối ưu mạng vừa xây dựng - Thực nghiệm - Đánh giá

	<ul style="list-style-type: none"> ✚ Sử dụng 2 tập dữ liệu chính LCC_FASD và NUAA cho các quá trình training và thực nghiệm. ✚ Môi trường thực nghiệm: <ul style="list-style-type: none"> - Cài đặt bằng ngôn ngữ python trên thư viện hỗ trợ phát triển thuật toán học sâu Keras. ✚ Tiền xử lý dữ liệu: <ul style="list-style-type: none"> - Thực hiện co, giãn ảnh về kích thước chung 128x128. Khác với mạng MobileNetV2 yêu cầu 224x224, do đó giảm được chi phí tính toán trong mạng nơ-ron. - Thu thập thêm các video quay chụp từ camera an ninh, thiết bị di động, Sử dụng thuật toán phát hiện khuôn mặt để cắt vùng khuôn mặt để tạo một bộ dữ liệu riêng với kích thước 128x128.
Kết quả dự kiến	<ul style="list-style-type: none"> ● <i>Phần mềm ứng dụng</i> ● <i>Thuật toán,</i> ● <i>So sánh giữa các phương pháp</i> ● <i>Bộ dữ liệu, etc</i> <p>Xây dựng được một kiến trúc mạng đủ nhẹ với số lượng tham số ít có khả năng chạy trên các thiết bị có cấu hình thấp.</p> <p>Có khả năng phát hiện giả mạo khuôn mặt với độ chính xác cao.</p>
Tài liệu tham khảo	<ul style="list-style-type: none"> ● Theo định dạng DBLP ● Điền sai format sẽ bị trừ điểm <p>[1] Peng Zhang, Fuhao Zou, Zhiwen Wu, Nengli Dai, Skarpness Mark, Michael Fu, Juan Zhao, Kai Li. FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-spoofing. arXiv preprint arXiv:1904.09290, 2019.</p>

- | | |
|--|--|
| | <ul style="list-style-type: none">[2] Zinelabidine Boulkenafet, Jukka Komulainen, and Abdenour Hadid. Face antispoofing using speeded-up robust features and fisher vector encoding. <i>IEEE Signal Processing Letters</i>, 2017.[3] Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Face anti-spoofing using patch and depth-based cnns. In <i>2017 IEEE International Joint Conference on Biometrics (IJCB)</i>. IEEE, 2017.[4] Litong Feng, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, and Kwok-Wai Cheung. Integration of image quality and motion cues for face antispoofing: A neural network approach. <i>Journal of Visual Communication and Image Representation</i>, 2016.[5] Shifeng Zhang, Xiaobo Wang, Ajian Liu, Chenxu Zhao, Jun Wan, Sergio Escalera, Hailin Shi, Zezheng Wang, and Stan Z Li. Casia-surf: A dataset and benchmark for large-scale multi-modal face anti-spoofing. <i>arXiv preprint arXiv:1812.00408</i>, 2018.[6] Zezheng Wang, Chenxu Zhao, Yunxiao Qin, Qiusheng Zhou, and Zhen Lei. Exploiting temporal and depth information for multi-frame face anti-spoofing. <i>arXiv preprint arXiv:1811.05118</i>, 2018.[7] Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In <i>Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition</i>, 2018[8] Andrew G Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam. Mobilenets: Efficient |
|--|--|

	<p>convolutional neural networks for mobile vision applications. arXiv preprint arXiv:1704.04861, 2017</p> <p>[9] Chi Nhan Duong, Kha Gia Quach, Ngan Le, Nghia Nguyen, and Khoa Luu. Mobiface: A lightweight deep learning face recognition on mobile devices. arXiv preprint arXiv:1811.11080, 2018</p>
--	---