

THÔNG TIN CHUNG CỦA NHÓM

- Link YouTube video của báo cáo (tối đa 5 phút):
<https://www.youtube.com/watch?v=-qEFefKJ2rk>
 - Link slides (dạng .pdf) đặt trên Github của nhóm:
(ví dụ: <https://github.com/thielh20-UIT/CS2205/blob/master/CS2205.SEP2025.DeCuong.FinalReport.AIO.Slide.pdf>)
 - Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới
 - Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in
 - Lớp Cao học, mỗi nhóm một thành viên
-
- | | |
|-----------------------------|--|
| • Họ và Tên: Lê Hoàng Thiện | • Lớp: CS2205.RM |
| • MSSV: 250101066 | • Tự đánh giá (điểm tổng kết môn): 8/10 |
| | • Số buổi vắng: 0 |
| | • Số câu hỏi QT cá nhân: 3 |
| | • Số câu hỏi QT của cả nhóm: 0 |
| | • Link Github: https://github.com/thielh20-UIT/CS2205 |

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

NGHIÊN CỨU CÁC PHƯƠNG PHÁP PHÁT HIỆN TÂN CÔNG GIẢ MẠO
KHUÔN MẶT DỰA TRÊN MÔ HÌNH THỊ GIÁC SÂU

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

A STUDY ON DEEP VISION-BASED FACE ANTI-SPOOFING METHODS

TÓM TẮT (*Tối đa 400 từ*)

Trong bối cảnh các hệ thống xác thực sinh trắc học khuôn mặt ngày càng phổ biến, các hình thức tấn công giả mạo (Presentation Attacks - PA) như sử dụng ảnh in (print), video phát lại (replay) hay mặt nạ 3D đang trở thành mối đe dọa nghiêm trọng. Đề tài này tập trung nghiên cứu phương pháp Phát hiện giả mạo khuôn mặt (Face Anti-Spoofing - FAS) bằng cách ứng dụng các mô hình thị giác sâu hiện đại. Trọng tâm của nghiên cứu là khai thác các đặc trưng vi cấu trúc (fine-grained textures) và thông tin chiều sâu được ước lượng từ ảnh đơn (depth-map-based) để phân biệt giữa thực thể sống và vật thể giả mạo. Nghiên cứu sẽ triển khai thực nghiệm trên các bộ dữ liệu chuẩn quốc tế như OULU-NPU và SiW, sử dụng các thuật toán dựa trên mạng Neural tích chập (CNN) kết hợp với cơ chế tìm kiếm kiến trúc mạng (NAS). Kết quả dự kiến là một hệ thống có khả năng nhận diện chính xác các cuộc tấn công với tỉ lệ sai sót tối thiểu, đảm bảo tính bảo mật cao cho các hệ thống eKYC và chấm công thông minh

GIỚI THIỆU (*Tối đa 1 trang A4*)

Công nghệ nhận dạng khuôn mặt đã trở thành một phần không thể thiếu trong các hệ

thống bảo mật hiện đại. Tuy nhiên, các nghiên cứu gần đây đã chỉ ra rằng các hệ thống này rất dễ bị tổn thương trước các cuộc tấn công giả mạo bằng phương tiện hình ảnh đơn giản. Theo các khảo sát toàn diện về lĩnh vực này [3], việc bảo vệ hệ thống nhận diện cần một lớp hàng rào kiểm tra thực thể sống (Liveness Detection).

Tại các hội nghị hàng đầu như CVPR, bài toán FAS đã chuyên dịch từ việc sử dụng các đặc trưng thủ công sang việc khai thác các đặc trưng vi cấu trúc (fine-grained textures) thông qua mạng học sâu [1]. Việc nghiên cứu đề tài này giúp người thực hiện tiếp cận với các kỹ thuật xử lý ảnh tiên tiến, từ việc phân tích nhiễu moiré trên màn hình đến việc ước lượng bản đồ chiều sâu (depth map) từ một ảnh 2D duy nhất [1][2]. Điều này đảm bảo tính logic từ việc nhận diện vẫn đề thực tế đến việc áp dụng các kỹ thuật cao cấp để giải quyết.

MỤC TIÊU (*Viết trong vòng 3 mục tiêu*)

1. Nghiên cứu lý thuyết: Tìm hiểu các kiến trúc mạng Deep Learning chuyên biệt cho Face Anti-Spoofing, đặc biệt là các biến thể của mạng tích chập trung tâm [1][2].
2. Triển khai thực nghiệm: Xây dựng quy trình huấn luyện và kiểm thử mô hình trên các bộ dữ liệu công khai có sẵn để đánh giá tính khả thi.
3. Đánh giá hiệu năng: Phân tích độ chính xác của mô hình thông qua các chỉ số chuyên dụng để khẳng định hiệu quả của phương pháp so với các phương pháp truyền thống.

NỘI DUNG VÀ PHƯƠNG PHÁP

Khuôn Mặt Thật Hay Giả? Giải Pháp Chống Giả Mạo Bằng Trí Tuệ Nhân Tạo

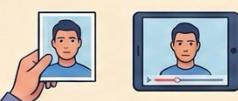
Vấn Đề: Mối Đe Dọa Từ Tấn Công Giả Mạo



Tấn công giả mạo (Presentation Attack) là gì?
Là hành vi sử dụng vật thể giả để đánh lừa hệ thống nhận dạng sinh trắc học.



Các hình thức tấn công phổ biến
Bao gồm ảnh in, video phát lại trên màn hình, và mặt nạ 3D.

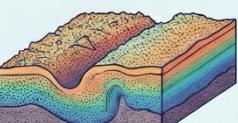


Tại sao chúng lại nguy hiểm?
Các hệ thống nhận dạng thông thường dễ bị qua mặt, đòi hỏi lớp kiểm tra thực thế sống.



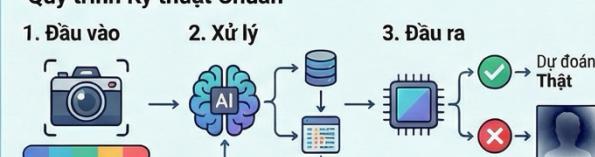
Giải Pháp: Phát Hiện Giả Mạo Bằng Thị Giác Sâu



Phân tích các đặc trưng vi mô và chiều sâu

Hệ thống tập trung vào cấu trúc bề mặt và bản đồ chiều sâu để phân biệt thật/giả.

Công nghệ cốt lõi:
Tích chập Trung tâm (CDC)

Thuật toán giúp làm nổi bật cấu trúc vật liệu, loại bỏ nhiễu từ môi trường xung quanh.

Quy trình Kỹ thuật Chuẩn
1. Đầu vào
2. Xử lý
3. Đầu ra

Dữ liệu khuôn mặt được cắt, chuẩn hóa
Huấn luyện mô hình AI để học cách phân biệt dựa trên cấu trúc và chiều sâu.
Đưa ra dự đoán (Thật/Giả) kèm bản đồ chiều sâu để giải thích quyết định.

NotebookLM

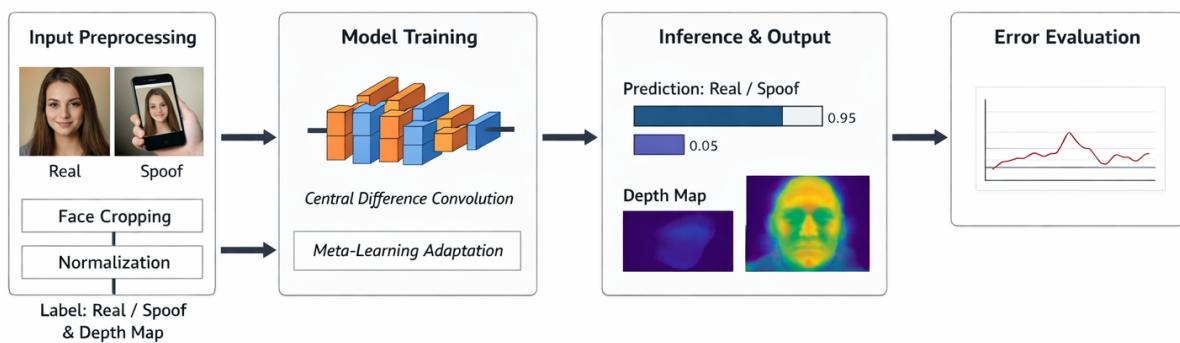
Nội dung nghiên cứu

Nội dung nghiên cứu tập trung vào việc hiện thực hóa các mục tiêu đã đề ra thông qua các bước cụ thể:

- Nghiên cứu và lựa chọn dữ liệu:** Chúng tôi sẽ tập trung vào bộ dữ liệu OULU-NPU và SiW. Đây là các bộ dữ liệu công khai (Public dataset) chứa hàng ngàn video tấn công giả mạo trong các điều kiện môi trường khác nhau, giúp mô hình học được tính tổng quát hóa.
- Nghiên cứu thuật toán chủ đạo:** Trọng tâm là việc tìm hiểu cơ chế của Central Difference Convolution (CDC) [1]. Khác với tích chập thông thường, CDC tập trung vào sự khác biệt cường độ giữa điểm ảnh trung tâm và các điểm lân cận, giúp loại bỏ nhiễu môi trường và làm nổi bật cấu trúc bề mặt vật liệu [1].
- Nghiên cứu kiến trúc mạng tự động:** Chúng tôi sẽ tìm hiểu cách ứng dụng tìm kiếm kiến trúc mạng (NAS) để tối ưu hóa mô hình FAS, giúp hệ thống vừa đạt độ chính xác cao vừa đảm bảo tốc độ xử lý nhanh [2].
- Phát triển module ước lượng chiều sâu:** Nội dung này tập trung vào việc thiết

kết một nhánh phụ trong mạng Neural để dự đoán bản đồ chiều sâu của khuôn mặt, từ đó loại bỏ các cuộc tấn công dựa trên mặt phẳng (ảnh in, iPad) [1][3].

Phương pháp nghiên cứu



Phương pháp thực hiện bài toán được xây dựng dựa trên quy trình kỹ thuật chuẩn của Computer Vision:

- **Tiền xử lý dữ liệu (Input):** Sử dụng các thư viện hỗ trợ để cắt vùng khuôn mặt và chuẩn hóa về cùng một kích thước không gian. Dữ liệu sẽ được gắn nhãn nhị phân (Real/Spoof) kết hợp với bản đồ chiều sâu giả định (ground-truth depth) [1].
- **Huấn luyện mô hình (Algorithms):** Sử dụng ngôn ngữ lập trình Python và thư viện PyTorch để cài đặt kiến trúc CDC [1]. Quá trình huấn luyện sẽ sử dụng kỹ thuật Meta-learning [2] để mô hình có thể thích nghi nhanh với các kịch bản tấn công mới chưa từng thấy trong tập huấn luyện.
- **Hậu xử lý và Hiển thị (Output):** Kết quả từ mạng sẽ được đưa qua một hàm

Softmax để tính toán xác suất thực thể sống. Output cuối cùng bao gồm nhãn dự đoán và bản đồ chiều sâu trực quan giúp người dùng hiểu được tại sao hệ thống đưa ra quyết định đó.

- **Đánh giá sai số:** Sử dụng phương pháp thống kê để tính toán tỉ lệ lỗi ACER (Average Classification Error Rate) – một tiêu chuẩn đánh giá khắt khe trong các cuộc thi FAS toàn cầu [1][3].

KẾT QUẢ MONG ĐỢI

Dựa trên việc triển khai các nội dung và phương pháp nêu trên, nghiên cứu dự kiến đạt được:

- **Ứng dụng thực nghiệm:** Một chương trình máy tính hoàn chỉnh cho phép người dùng đưa khuôn mặt trước camera và nhận kết quả phản hồi thời gian thực.
- **Độ chính xác:** Mô hình đạt được hiệu suất tối ưu trên tập kiểm thử, thể hiện qua các biểu đồ Loss và Accuracy ổn định.
- **Báo cáo phân tích:** Một tài liệu chi tiết mô tả cách thức thuật toán hoạt động, các trường hợp mô hình nhận diện sai và hướng khắc phục trong tương lai.

TÀI LIỆU THAM KHẢO (*Định dạng DBLP*)

[1]. Zitong Yu, Chenxu Zhao, Zhen Le, Yunxiao Qin, Qibin Hou, Guoying Zhao: Searching Central Difference Convolutional Networks for Face Anti-Spoofing. CVPR

2020: 5294-5304

[2]. Yunxiao Qin, Zitong Yu, Longyin Wen, Guoying Zhao, Dewei Fu, Jingang Shi:
Meta-learning for Network Architecture Search: A Case Study on Face Anti-spoofing.
CVPR 2020: 1-10

[3]. Zitong Yu, Yunxiao Qin, Xiaobai Li, Chenxu Zhao, Zhen Lei, Guoying Zhao:
Deep Learning for Face Anti-Spoofing: A Survey. IEEE Trans. Pattern Anal. Mach.
Intell. 45(5): 5609-5633 (2023)