



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

Họ và Tên: Lê Hoàng Thiện

MSSV: 250101066

Lớp: CS2205.RM



<https://github.com/thielh20-UIT/CS2205>

Họ và Tên: Lê Hoàng Thiện

MSSV: 250101066



<https://www.youtube.com/@thienlehoang7458>

Nghiên Cứu Phát Hiện Tấn Công Giả Mạo Khuôn Mặt

Dựa trên Mô Hình Thị Giác Sâu

Nghiên cứu tập trung vào việc ứng dụng các mô hình thị giác sâu hiện đại để phát hiện các hình thức tấn công giả mạo khuôn mặt (PA) như ảnh in, video phát lại, hay mặt nạ 3D, nhằm đảm bảo tính bảo mật cho các hệ thống xác thực sinh trắc học.





Tóm Tắt Nghiên Cứu

Mối Đe Dọa Hiện Hữu

Các hình thức tấn công giả mạo (PA) đang là mối đe dọa nghiêm trọng đối với hệ thống xác thực khuôn mặt.

Ứng Dụng Thị Giác Sâu

Nghiên cứu tập trung vào Phát hiện giả mạo khuôn mặt (FAS) bằng mô hình thị giác sâu.

Đặc Trưng Nổi Bật

Khai thác đặc trưng vi cấu trúc và thông tin chiều sâu từ ảnh đơn để phân biệt thật/giả.

Kết Quả Mong Đợi

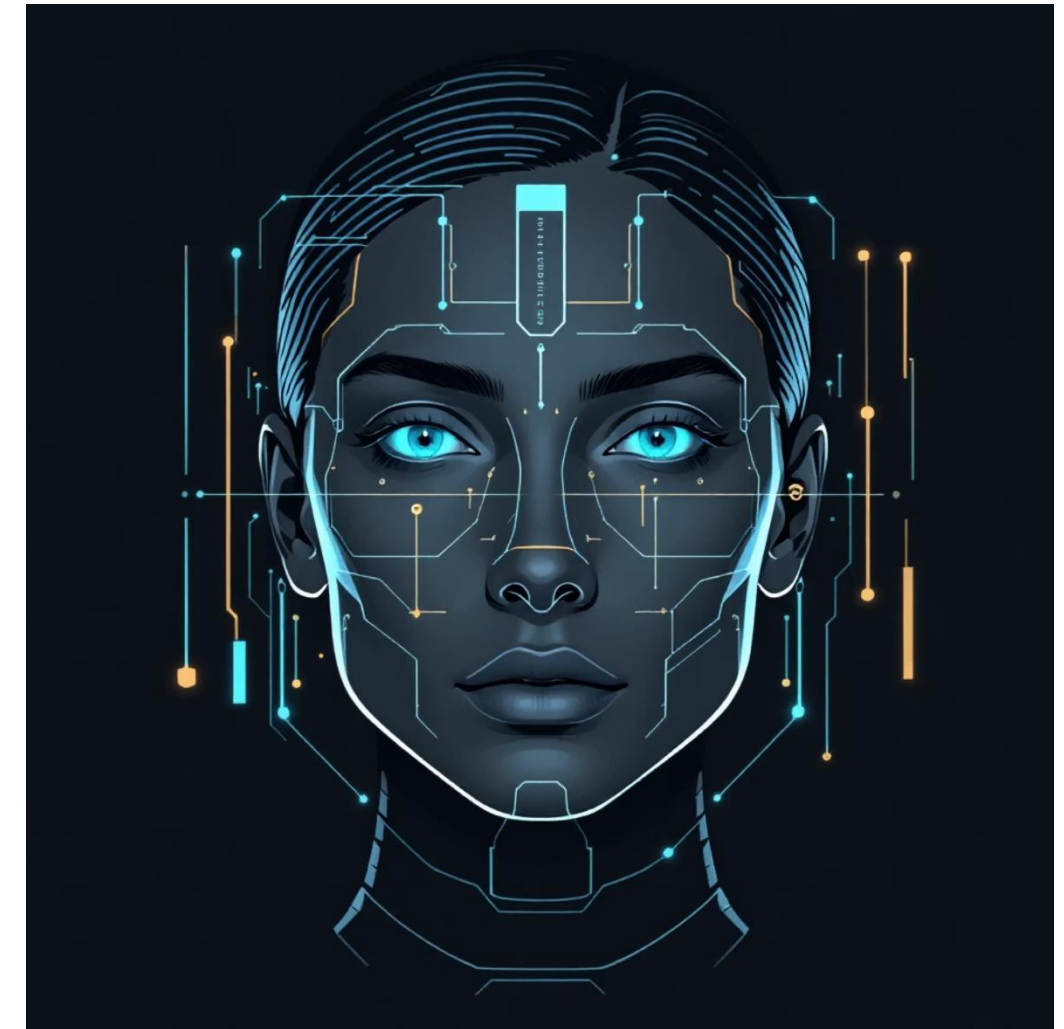
Hệ thống nhận diện chính xác, tỉ lệ sai sót tối thiểu, bảo mật cao cho eKYC và chấm công.

Giới Thiệu

Công nghệ nhận dạng khuôn mặt là yếu tố then chốt trong bảo mật hiện đại. Tuy nhiên, các hệ thống này dễ bị tổn thương bởi các cuộc tấn công giả mạo bằng hình ảnh đơn giản.

Việc bảo vệ hệ thống nhận diện đòi hỏi một lớp kiểm tra thực thể sống (Liveness Detection). Bài toán FAS đã chuyển dịch sang khai thác đặc trưng vi cấu trúc qua mạng học sâu.

Nghiên cứu này giúp tiếp cận kỹ thuật xử lý ảnh tiên tiến, từ phân tích nhiễu moiré đến ước lượng bản đồ chiều sâu từ ảnh 2D.





Mục Tiêu Nghiên Cứu

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.

2

Triển Khai Thực Nghiệm

Xây dựng quy trình huấn luyện và kiểm thử mô hình trên các bộ dữ liệu công khai 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.

Nội Dung Nghiên Cứu

Dữ Liệu

Nghiên cứu và lựa chọn bộ dữ liệu OULU-NPU và SiW.



Thuật Toán

Tìm hiểu cơ chế của Central Difference Convolution (CDC).



Kiến Trúc Mạng

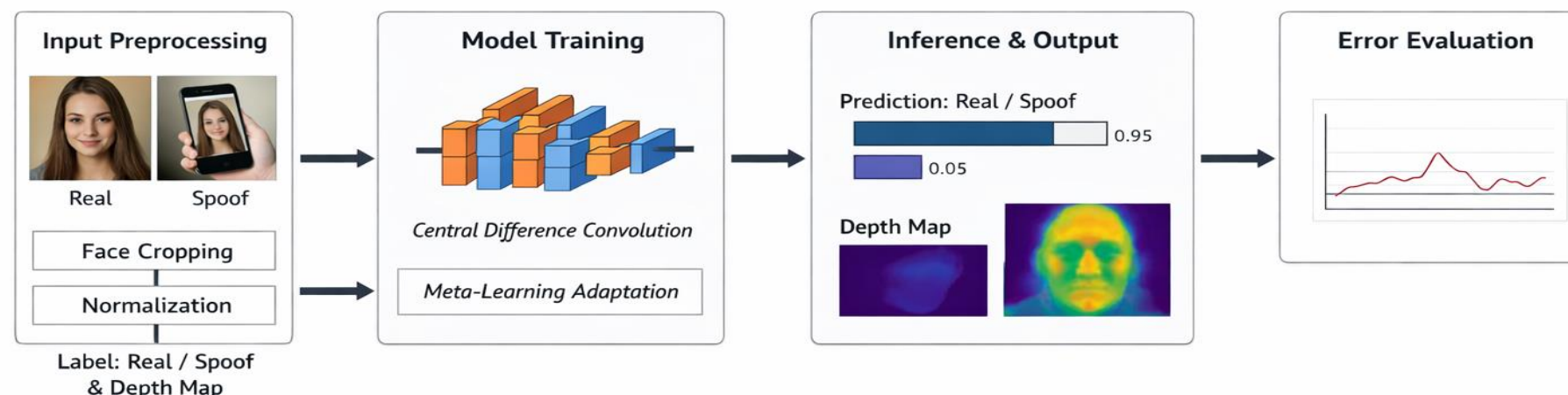
Ứng dụng tìm kiếm kiến trúc mạng (NAS) để tối ưu hóa.



Module Chiều Sâu

Phát triển module ước lượng chiều sâu khuôn mặt.





Phương Pháp Nghiên Cứu



Tiền Xử Lý Dữ Liệu

Cắt vùng khuôn mặt, chuẩn hóa kích thước, gán nhãn nhị phân.



Huấn Luyện Mô Hình

Sử dụng Python, PyTorch, cài đặt kiến trúc CDC, Meta-learning.



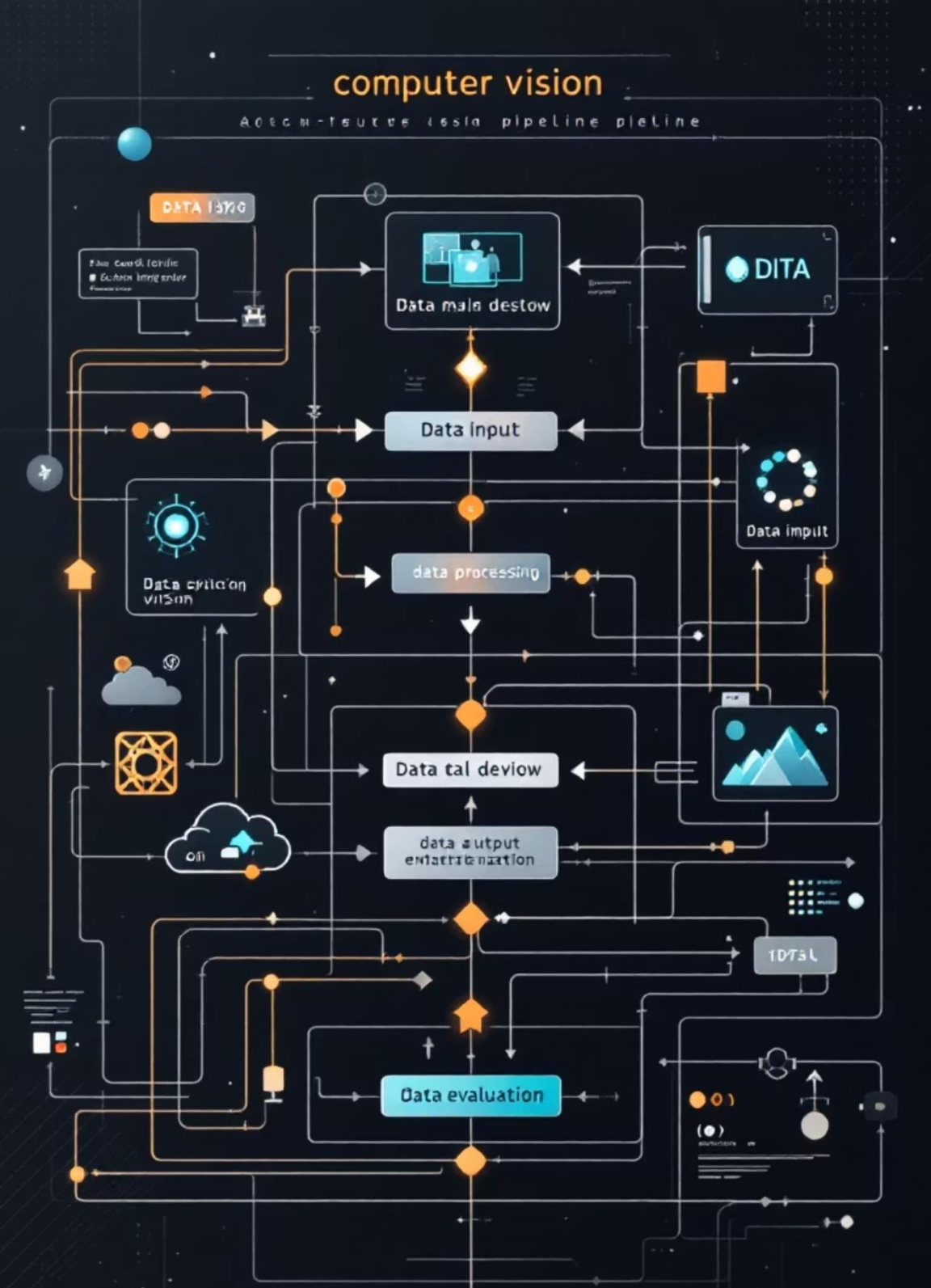
Hậu Xử Lý & Hiển Thị

Hàm Softmax tính xác suất, hiển thị nhãn và bản đồ chiều sâu.



Đánh Giá Sai Số

Tính toán tỉ lệ lỗi ACER để đánh giá hiệu quả.



Quy Trình Kỹ Thuật

Phương pháp thực hiện bài toán được xây dựng dựa trên quy trình kỹ thuật chuẩn của Computer Vision, đảm bảo tính khoa học và hiệu quả.

Kết Quả Mong Đợi

1

Ứng Dụng Thực Nghiệm

Chương trình máy tính hoàn chỉnh cho phép người dùng nhận phản hồi thời gian thực.

2

Độ Chính Xác Cao

Mô hình đạt hiệu suất tối ưu trên tập kiểm thử, thể hiện qua biểu đồ Loss và Accuracy ổn định.

3

Báo Cáo Phân Tích

Tài liệu chi tiết mô tả thuật toán, các trường hợp nhận diện sai và hướng khắc phục.





Tài Liệu Tham Khảo

- 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
- 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
- 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)