BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CMC

ĐỀ CƯƠNG ĐỀ TÀI NCKH SINH VIÊN
NĂM HỌC 2024 – 2025

1. Họ và tên nhóm sinh viên tham gia thực hiện đề tài.
    1) Trần Văn Phúc, Mã SV:BIT220130, Lớp: 22IT-SE1.2
    2) Nguyễn Thị Tâm, Mã SV:BIT230372, Lớp: 23IT2
2. Tên đề tài (tiếng Việt): Nghiên cứu và ứng dụng AI Vision phát hiện người xâm nhập trái phép.
3. Tên đề tài (tiếng Anh): Advanced AI Vision System for Intrusion Detection and Security Enhancement.
4. Tính cấp thiết:

Trong cuộc cách mạng công nghiệp 4.0, ứng dụng công nghệ thông minh vào an ninh trở thành xu hướng tất yếu. Các hệ thống giám sát truyền thống ngày càng lộ rõ hạn chế trong việc phát hiện và xử lý xâm nhập trái phép, đặc biệt trong môi trường phức tạp hoặc ánh sáng kém.

Công nghệ AI Vision, với khả năng xử lý hình ảnh thời gian thực và nhận diện chính xác, đã chứng minh hiệu quả vượt trội trong giám sát an ninh. Tuy nhiên, tại Việt Nam, việc nghiên cứu và ứng dụng công nghệ này vào phát hiện xâm nhập trái phép vẫn chưa được khai thác đúng mức, dù nhu cầu bảo vệ an ninh cho khu công nghiệp và cơ sở hạ tầng ngày càng tăng.

Nghiên cứu AI Vision không chỉ đáp ứng nhu cầu cấp thiết về an ninh mà còn thúc đẩy phát triển công nghệ bảo mật tại Việt Nam.

5. Mục tiêu nghiên cứu:

Mục tiêu chung của nghiên cứu là xây dựng và ứng dụng một hệ thống AI Vision tiên tiến, giúp tự động phát hiện các hành vi xâm nhập trái phép một cách chính xác và hiệu quả. Hệ thống này sẽ được thiết kế để hỗ trợ đắc lực cho công tác giám sát an ninh tại các khu vực nhạy cảm, nâng cao tính tự động hóa trong quản lý và đảm bảo an toàn ở mức độ cao nhất.

Mục tiêu cụ thể bao gồm bốn điểm chính:

Thứ nhất, nghiên cứu các phương pháp, thuật toán AI Vision phù hợp để nhận diện và phân loại chính xác hành vi xâm nhập trái phép qua hình ảnh và video.

Thứ hai, xây dựng hệ thống giám sát tích hợp AI Vision với camera an ninh, tối ưu khả năng xử lý thời gian thực để phát hiện và thông báo kịp thời các nguy cơ.

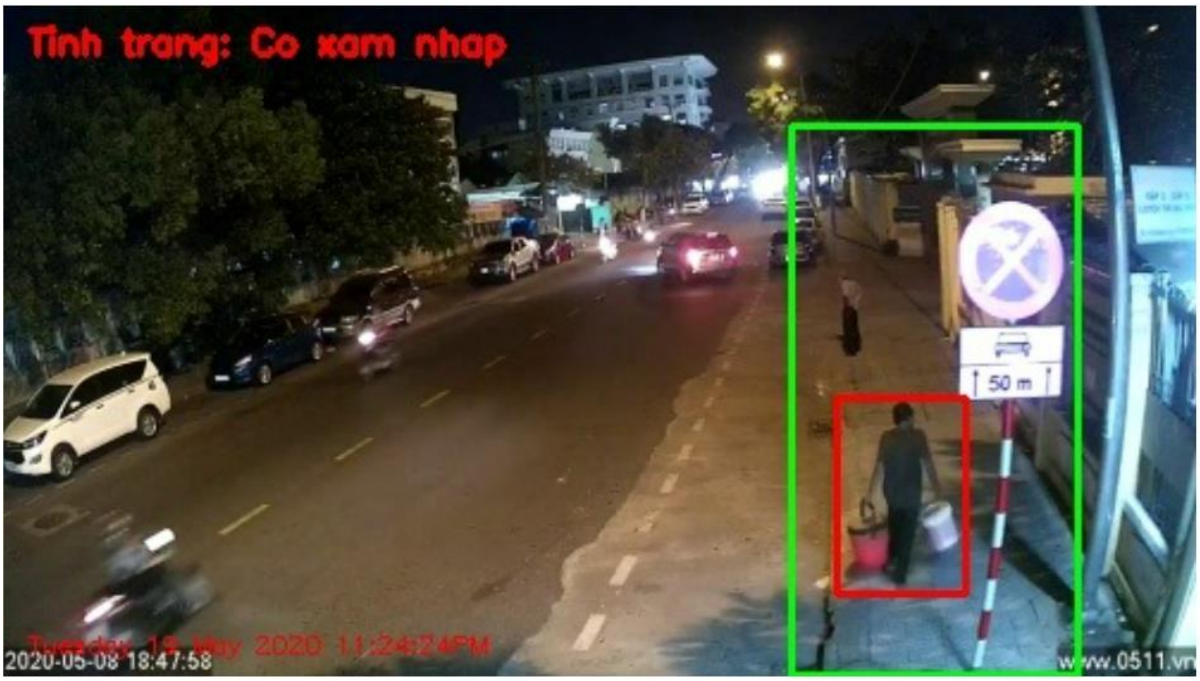
Thứ ba, thử nghiệm hệ thống trong môi trường thực tế như khu công nghiệp, dân cư hoặc hạ tầng công cộng để đánh giá hiệu quả, độ chính xác và tính ứng dụng.

Thứ tư, đề xuất cải tiến nhằm nâng cao độ tin cậy, khả năng xử lý dữ liệu phức tạp và tính ổn định trong điều kiện đặc biệt như ban đêm, thời tiết xấu hoặc khu vực giao thông cao.

Hệ thống được kỳ vọng không chỉ đáp ứng các yêu cầu kỹ thuật mà còn mang lại giá trị thực tiễn cao trong việc bảo vệ an ninh, đảm bảo an toàn cho con người và tài sản trong bối cảnh các thách thức an ninh ngày càng gia tăng.

6. Tổng quan tình hình nghiên cứu trong và ngoài nước:

Trên thế giới, các nghiên cứu về ứng dụng AI Vision trong an ninh tập trung vào nhận diện khuôn mặt, phát hiện chuyển động bất thường, và phân loại hành vi con người. Ví dụ, nghiên cứu của nhóm tác giả tại Đại học Stanford (2021) đã áp dụng Deep Learning vào phát hiện hành vi khả nghi tại khu vực công cộng, đạt độ chính xác trên 90%. Một nghiên cứu khác từ Trung Quốc đã tích hợp hệ thống AI Vision vào mạng lưới camera giao thông để phát hiện người đi bộ xâm nhập trái phép vào các khu vực cấm.



Tại Việt Nam, nghiên cứu của Viện Nghiên cứu Ứng dụng Công nghệ CMC ATI đã chính thức ra mắt hai sản phẩm AI mới: CMC AIVISION và CMC AIBOX, khẳng định vị thế tiên phong trong nghiên cứu và phát triển công nghệ AI tại Việt Nam. CMC AIVISION là thiết bị AI camera xử lý tại biên, phục vụ các ứng dụng nhận diện khuôn mặt, phát hiện hành vi bất thường, cảnh báo cháy nổ, vi phạm giao thông và nhận diện biển số xe. CMC AIBOX là thiết bị giúp camera thường trở thành camera AI, nhận diện khuôn mặt, phát hiện hành vi, xác định độ tuổi, và có thể được tùy biến thành AIoT Gateway, Home Server hoặc Office Server để lưu trữ, chia sẻ tài liệu như thiết bị NAS. Tính năng linh hoạt trong thu thập dữ liệu từ các thiết bị IoT qua nhiều giao thức như Bluetooth, 4G, Zigbee và phân tích xử lý AI tại biên mà không cần kết nối AI Server.

Hạn chế chính của các nghiên cứu trong và ngoài nước là yêu cầu cơ sở hạ tầng hiện đại, chi phí cao, và khả năng nhận diện còn phụ thuộc vào điều kiện ánh sáng và góc nhìn. Những vấn đề này tạo khoảng trống nghiên cứu mà đề tài "Ứng dụng AI Vision phát hiện người xâm nhập trái phép" hướng tới giải quyết đặc biệt cải thiện các điều kiện tác động và cải thiện tốc độ phát hiện đối tượng xâm nhập .

7. Nội dung nghiên cứu:

Cấu trúc chính của báo cáo dự kiến bao gồm 5 phần:

PHẦN I. MỞ ĐẦU

Trong phần I, bài báo trình bày tổng quan về đề tài nghiên cứu ứng dụng AI Vision trong phát hiện xâm nhập: giới thiệu bài toán, đối tượng nghiên cứu của đề tài, tổng quan các bài nghiên cứu đã được giải quyết ở trong và ngoài nước, đồng thời đưa ra những vấn đề tồn tại cần được nghiên cứu và đóng góp của đề tài nghiên cứu.

Giới thiệu bài toán: Bài toán phát hiện xâm nhập trái phép sử dụng AI Vision là một hệ thống xử lý dữ liệu video và hình ảnh theo thời gian thực từ camera giám sát, kết hợp với các thông số về thời gian và điều kiện môi trường làm đầu vào. Hệ thống sử dụng các thuật toán AI Vision như object detection, person tracking và classification để xử lý thông tin và tạo ra đầu ra bao gồm: khả năng phát hiện, định vị và phân loại đối tượng trong vùng giám sát, kích hoạt cảnh báo real-time khi phát hiện xâm nhập trái phép, đồng thời lưu trữ thông tin chi tiết về các sự kiện xâm nhập như thời gian, vị trí và hình ảnh đối tượng để phục vụ công tác theo dõi và xử lý sau này.

Kết luận phần I.

PHẦN II. NGHIÊN CỨU NÂNG CAO VỀ AI VISION VÀ ỨNG DỤNG TRONG PHÁT HIỆN NGƯỜI XÂM NHẬP

Phần II trình bày về nội dung nghiên cứu, phương pháp nghiên cứu đã được sử dụng trong đề tài, đưa ra những kiến thức lý thuyết liên quan về kiến trúc tổng quát, chi tiết mô hình được sử dụng để giải quyết bài toán của đề tài nghiên cứu: kiến trúc mạng nơ-ron tích chập CNN, mô hình Yolov8,....:

YOLOv8 là mô hình object detection mới nhất từ Ultralytics, cải tiến đáng kể về tốc độ và độ chính xác so với các phiên bản trước. Mô hình hỗ trợ object detection, segmentation và classification với khả năng xử lý real-time, sử dụng anchor-free detection và các kỹ thuật tối ưu như mosaic augmentation. YOLOv8 đặc biệt phù hợp cho các ứng dụng giám sát an ninh thời gian thực.

Convolutional Neural Network (CNN) là mạng neural chuyên dụng để xử lý dữ liệu dạng lưới, đặc biệt là hình ảnh. Cấu trúc chính gồm lớp tích chập để trích xuất đặc trưng, lớp gộp để giảm kích thước, và lớp fully connected để phân loại. CNN tự động học các pattern trong ảnh từ đơn giản đến phức tạp, giúp giải quyết hiệu quả các bài toán computer vision.

Kết luận phần II.

PHẦN III. THỰC NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

Phần III trình bày chi tiết về quá trình thực nghiệm phát hiện xâm nhập, bao gồm dữ liệu sử dụng, quy trình huấn luyện mô hình, thiết kế và thiết lập thực nghiệm hệ thống. Dự kiến bộ dữ liệu sử dụng sẽ do nhóm sinh viên tự tiến hành thu thập và gán nhãn dữ liệu. Kết quả thực nghiệm được thống kê với các chỉ số đánh giá mô hình cho bài toán nhằm phục vụ cho việc so sánh, đánh giá sâu hơn. Đồng thời, tiến hành thảo luận sâu hơn về các kết quả đạt được như: ý nghĩa, tác động kinh tế - xã hội,...

PHẦN IV. KẾT LUẬN

Phần IV trình bày các kết quả đạt được: Nghiên cứu ứng dụng mô hình AI Vision vào giải quyết bài toán phát hiện người xâm nhập trái phép. Đưa ra được đánh giá về những điểm cần cải tiến trong bài toán và các khuyến nghị, định hướng nghiên cứu sâu hơn trong tương lai.

PHẦN V. DANH MỤC TÀI LIỆU THAM KHẢO

8. Phương pháp nghiên cứu:

Về mặt lý thuyết:

i. Thu thập, khảo sát tài liệu, bài báo, nghiên cứu có liên quan tới phát hiện xâm nhập.

ii. Thu thập, tiền xử lý dữ liệu ảnh / video thực tế và bộ dữ liệu công khai.

Về mặt thực nghiệm:

iii. Huấn luyện mô hình với dữ liệu ảnh sau khi xử lý.

iv. Thực nghiệm tích hợp mô hình với hệ thống dữ liệu thực tế và đánh giá kết quả.

9. Sản phẩm cần đạt của đề tài:

Hệ thống AI Vision được phát triển dựa trên mô hình YOLOv8, có khả năng phát hiện xâm nhập trái phép một cách nhanh chóng và chính xác. Mô hình này sử dụng mạng nơ-ron tích chập sâu (CNN) để trích xuất đặc trưng và phân loại các đối tượng hoặc hành vi trong hình ảnh/video, cho phép nhận diện hành vi bất thường theo thời gian thực, kết quả phát hiện bất thường được tối ưu hóa thời gian phản hồi của mô hình dưới 0,5s.

Ứng dụng này tích hợp hệ thống AI Vision vào một nền tảng giám sát thông minh, giúp giám sát các khu vực quan trọng và tự động đưa ra cảnh báo khi phát hiện xâm nhập. Ứng dụng có giao diện thân thiện với người dùng, hỗ trợ hiển thị video trực tiếp, ghi nhận các cảnh báo, và cung cấp tính năng quản lý dữ liệu giám sát.

10.Kế hoạch thực hiện

STT	Nội dung	Thời gian thực hiện dự kiến
1	Nghiên cứu tổng quan bài toán, xây dựng, sửa chữa kế hoạch và đề cương	20/12/2024 - 06/01/2025
2	Nộp đề cương nghiên cứu khoa học	07/01/2025
3	Sửa chữa hoàn thiện đề cương	08/01/2025 - 09/01/2025
4	Nghiên cứu, phát triển mô hình, hoàn thiện hệ thống	10/01/2025 - 15/03/2025
5	Viết, hoàn thiện báo cáo đề tài nghiên cứu	16/03/2025 - 10/04/2025

Hà Nội, ngày 07 tháng 01 năm 2025

Xác nhận của giảng viên hướng dẫn

Nhóm sinh viên

(Ký và ghi rõ họ tên từng thành viên)