**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CMC**



**ĐỀ CƯƠNG NGHIÊN CỨU KHOA HỌC**

**Nghiên cứu và ứng dụng AI Vision phát hiện người xâm nhập trái phép**

***Advanced AI Vision Systems for Intrusion Detection and Security Enhancement***

**Chuyên Ngành : Công Nghệ Thông Tin và Truyền Thông**

**Nhóm sinh viên : Nguyễn Thị Tâm - BIT230372**

**Trần Văn Phúc – BIT220130**

**Người hướng dẫn khoa học : Nguyễn Khánh Sơn**

**Hà Nội, tháng 1 – 2025**

**Hà Nội, tháng 8 năm 2024**

**Hà Nội, tháng năm 2024**

**Mở đầu**

1. **Đặt vấn đề**

Trong thời đại công nghệ 4.0, trí tuệ nhân tạo (AI) đã và đang trở thành một phần quan trọng của nhiều lĩnh vực, đặc biệt trong an ninh và giám sát. Các hệ thống giám sát truyền thống hiện nay thường chỉ đơn thuần lưu trữ dữ liệu hoặc yêu cầu sự can thiệp thủ công của con người để phát hiện và xử lý các tình huống bất thường. Điều này không chỉ gây tốn kém nguồn lực mà còn làm giảm hiệu quả trong việc bảo vệ an ninh, nhất là ở các khu vực nhạy cảm như ngân hàng, khu dân cư cao cấp, nhà máy công nghiệp, và các cơ sở hạ tầng quan trọng. Sự hạn chế về khả năng phát hiện tự động của các hệ thống giám sát truyền thống đã đặt ra nhu cầu cấp thiết về một giải pháp thông minh hơn, hiện đại hơn để giải quyết các thách thức ngày càng phức tạp trong lĩnh vực an ninh.

Thực trạng hiện nay cho thấy, các hành vi xâm nhập trái phép đang diễn ra với mức độ tinh vi cao, không chỉ giới hạn ở các phương thức truyền thống mà còn kết hợp công nghệ để né tránh giám sát. Hệ quả của vấn đề này không chỉ là thiệt hại về tài sản mà còn gây nguy cơ đến tính mạng con người và ảnh hưởng nghiêm trọng đến sự an toàn xã hội. Những thách thức này đòi hỏi một giải pháp tự động hóa với tính chính xác cao, khả năng hoạt động liên tục và đáp ứng nhanh trong thời gian thực để ngăn chặn các hành vi vi phạm.

Nghiên cứu này được thực hiện nhằm phát triển một hệ thống giám sát ứng dụng công nghệ AI Vision tiên tiến, có khả năng tự động phát hiện các hành vi xâm nhập trái phép. Mục tiêu là không chỉ hỗ trợ các tổ chức, doanh nghiệp và cá nhân trong việc giám sát an ninh mà còn giảm thiểu tối đa phụ thuộc vào giám sát thủ công. Hệ thống được kỳ vọng sẽ nâng cao khả năng phòng ngừa, phản ứng nhanh chóng trước các tình huống khẩn cấp, góp phần đảm bảo sự an toàn và an ninh trong nhiều bối cảnh khác nhau.

**2. 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 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 và phân tích các phương pháp, thuật toán AI Vision phù hợp, đảm bảo khả năng nhận diện và phân loại chính xác các hành vi xâm nhập trái phép dựa trên hình ảnh và video.

Thứ hai, xây dựng một hệ thống giám sát tích hợp công nghệ AI Vision với các thiết bị phần cứng như camera an ninh, đồng thời tối ưu hóa khả năng xử lý trong thời gian thực để phát hiện và thông báo kịp thời các tình huống nguy hiểm.

Thứ ba, tiến hành thử nghiệm hệ thống trong các môi trường thực tế khác nhau như khu công nghiệp, khu dân cư, hoặc cơ sở hạ tầng công cộng, nhằm đánh giá hiệu quả hoạt động, độ chính xác và khả năng ứng dụng thực tế của hệ thống.

Thứ tư, trên cơ sở thử nghiệm, đưa ra các đề xuất cải tiến hệ thống để nâng cao độ tin cậy, khả năng xử lý dữ liệu phức tạp, và tính ổn định khi hoạt động trong những môi trường đặc biệt như ban đêm, thời tiết khắc nghiệt hoặc khu vực có mật độ 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.

**3. Mục đích nghiên cứu**

Hệ thống AI Vision đang được triển khai rộng rãi trên toàn thế giới, với nhiều ứng dụng trong an ninh, giao thông, và quản lý công cộng. Theo thống kê từ các tổ chức công nghệ hàng đầu, việc ứng dụng công nghệ nhận diện hình ảnh đã giúp giảm thiểu 30-50% các vụ vi phạm an ninh tại những khu vực được triển khai.

Tại Việt Nam, AI Vision bắt đầu nhận được sự quan tâm, đặc biệt trong lĩnh vực giao thông và an ninh khu vực. Một số thành phố lớn như Hà Nội và TP.HCM đã thử nghiệm ứng dụng AI trong nhận diện phương tiện hoặc phát hiện hành vi vi phạm giao thông. Tuy nhiên, việc áp dụng công nghệ vào mục tiêu phát hiện xâm nhập trái phép vẫn còn khá mới mẻ, đặc biệt tại các địa phương.

**4. Các 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.



Phổ biến như FPT Camera sử dụng công nghệ nhận diện khuôn mặt AI để phát hiện sự xâm nhập trái phép trong khu vực giám sát. Khi có ai đó xâm nhập vào khu vực hạn chế hoặc không được phép, hệ thống sẽ tự động gửi cảnh báo đến người quản lý, giúp doanh nghiệp phản ứng nhanh chóng và đảm bảo an ninh. 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.

**II. NỘI DUNG**

**1. Kế hoạch nghiên cứu dự kiến**

|  |  |  |
| --- | --- | --- |
| **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 | 27/12/2024 - 06/01/2025 |
| 2 | Nộp đề cương nghiên cứu khoa học | 07/01/2025 |
| 3 | Thiết kế và phát triển đề tài | 08/01/2025 - 28/02/2025 |
| 4 | Phát triển ứng dụng | 21/02/2025 - 15/03/2025 |
| 5 | Viết,  hoàn thiện báo cáo đề tài nghiên cứu | 16/03/2025 - 10/04/2025 |
|  |  |  |

**2. Đối tượng nghiên cứu**

Đối tượng nghiên cứu của đề tài bao gồm:

**Con người và hành vi:** Hành vi của con người khi xâm nhập trái phép vào các khu vực được giám sát. Các hành vi đặc trưng có thể bao gồm vượt rào, phá hoại, hoặc di chuyển bất thường.

**Hệ thống giám sát an ninh:** Các thiết bị camera và cảm biến hiện có tại địa bàn nghiên cứu, đồng thời tích hợp với các công cụ xử lý AI Vision.

**Dữ liệu hình ảnh/video:** Các tập dữ liệu hình ảnh/video thu thập được từ hệ thống giám sát để phục vụ cho quá trình trích xuất đặc trưng và huấn luyện mô hình.

**3. Phương pháp nghiên cứu**

**Thu thập dữ liệu**

Thu thập hình ảnh/video từ hệ thống camera thực tế và bộ dữ liệu công khai.

Tiền xử lý dữ liệu: chuẩn hóa, gắn nhãn và loại bỏ nhiễu.

**Xử lý và trích xuất đặc trưng**

Sử dụng OpenCV để xử lý ảnh (lọc nhiễu, phát hiện cạnh).

Huấn luyện mô hình YOLOv8 với dữ liệu qua framework PyTorch.

**Thiết kế và phát triển hệ thống**

Tích hợp YOLOv8 vào hệ thống và kết nối cơ sở dữ liệu SQLite/SQL Server.

**Thử nghiệm và đánh giá**

Kiểm tra hệ thống thực tế, đo hiệu năng (Precision, Recall, F1-Score).

Thu thập phản hồi từ người dùng để cải tiến.

**Báo cáo và tài liệu**

Tổng hợp kết quả thành báo cáo khoa học.

Soạn tài liệu hướng dẫn cài đặt, sử dụng và bảo trì hệ thống.

**III. THỬ NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ**

**1.  Sản phẩm cần đạt dự kiến của đề tài**

Hệ thống AI Vision được phát triển dựa trên mô hình YOLOv8 (You Only Look Once, phiên bản 8), 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.

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.

**Tài liệu tham khảo**