TẠP CHÍ ĐIỆN TỬ CỦA BỘ XÂY DỰNG
JOURNAL OF CONSTRUCTION

TẠP CHÍ XÂY DỰNG - eISSN 3030-4482

Camera AI giám sát giao thông và các lỗ hổng mất an toàn thông tin cá nhân: Thực trạng và giải pháp

AI traffic surveillance cameras and vulnerabilities in personal data security: Current situation and solutions

➢ **THS Bùi Đình Vũ**
Trường Đại học Hàng hải Việt Nam
Email: vubd@vimaru.edu.vn

THÔNG TIN BÀI BÁO
Chuyên mục: Khoa học công nghệ
Ngày nhận bài: 12/3/2026
Ngày sửa bài: 25/3/2026
Ngày chấp nhận đăng: 14/4/2026
Ngày xuất bản Online: 21/5/2026
Tác giả liên hệ:
Email: vubd@vimaru.edu.vn

TÓM TẮT

Trong bối cảnh đô thị hóa và sự gia tăng nhanh chóng của phương tiện giao thông, nhiều quốc gia đã triển khai hệ thống camera giám sát giao thông tích hợp trí tuệ nhân tạo (AI) nhằm nâng cao hiệu quả quản lý giao thông, giảm tai nạn và hỗ trợ xử lý vi phạm. Các hệ thống này có khả năng nhận diện biển số xe, phát hiện vi phạm giao thông, phân tích mật độ phương tiện và hỗ trợ "phạt nguội". Tuy nhiên, việc sử dụng camera AI cũng đặt ra nhiều vấn đề về an toàn thông tin và quyền riêng tư cá nhân, do hệ thống thu thập và xử lý lượng lớn dữ liệu như hình ảnh khuôn mặt, biển số xe, hành trình di chuyển và các thông tin nhận dạng khác.

Thực tế cho thấy, nhiều hệ thống camera giám sát có thể tồn tại các lỗ hổng bảo mật, chẳng hạn như truy cập trái phép, rò rỉ dữ liệu, khai thác lỗ hổng thiết bị IoT hoặc tấn công vào hệ thống AI. Ngoài ra, các thuật toán nhận diện cũng có thể mắc sai sót dẫn đến nhận diện sai hoặc xử phạt nhầm. Bên cạnh đó, việc thu thập và lưu trữ dữ liệu quy mô lớn cũng làm gia tăng nguy cơ xâm phạm quyền riêng tư và lạm dụng thông tin cá nhân.

Bài báo này trình bày tổng quan về thực trạng ứng dụng camera AI trong quản lý an ninh giao thông, phân tích các lỗ hổng tiềm ẩn gây mất an toàn thông tin cá nhân và đề xuất các giải pháp kỹ thuật, quản lý và pháp lý nhằm nâng cao mức độ bảo mật cho hệ thống. Các giải pháp bao gồm tăng cường bảo mật hệ thống, áp dụng nguyên tắc bảo vệ quyền

riêng tư ngay từ thiết kế, sử dụng các phương pháp ẩn danh dữ liệu, kiểm soát truy cập và hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân.

Từ khóa: Camera AI; giám sát giao thông; an ninh mạng; bảo vệ dữ liệu cá nhân; thành phố thông minh.

A B S T R A C T

In the context of urbanization and the rapid increase in traffic, many countries have deployed AI-integrated traffic surveillance camera systems to improve traffic management efficiency, reduce accidents and assist in handling violations. These systems are capable of license plate recognition, detecting traffic violations, analyzing vehicle density and supporting "on-the-spot" fines. However, the use of AI cameras also raises concerns about information security and personal privacy, as the systems collect and process large amounts of data such as facial images, license plates, travel routes, and other identifying information.

In reality, many surveillance camera systems may have security vulnerabilities, such as unauthorized access, data leaks, exploitation of IoT device vulnerabilities, or attacks on AI systems. Furthermore, recognition algorithms can also make mistakes, leading to misidentification or incorrect penalties. In addition, the large-scale collection and storage of data increases the risk of privacy violations and misuse of personal information.

This paper presents an overview of the current state of AI camera applications in traffic security management, analyzes potential vulnerabilities that compromise personal information security and proposes technical, managerial and legal solutions to enhance system security. These solutions include strengthening system security, applying privacy protection principles from the design stage, using data anonymization methods, access control and improving the legal framework for personal data protection.

Keywords: AI camera; traffic surveillance; cybersecurity; personal data protection; smart city.

1. ĐẶT VẤN ĐỀ

Hình 1. Camera AI an ninh giao thông

Sự phát triển của đô thị hóa và sự gia tăng nhanh chóng của phương tiện giao thông đã đặt ra nhiều thách thức cho công tác quản lý giao thông tại các thành phố lớn. Trong bối cảnh đó, nhiều quốc gia đã triển khai các hệ thống camera giám sát giao thông tích hợp trí tuệ nhân tạo (AI) nhằm nâng cao hiệu quả giám sát và quản lý giao thông.

Camera AI có khả năng:

- Nhận diện biển số xe;
- Phát hiện vi phạm giao thông;
- Phân tích lưu lượng phương tiện;
- Phát hiện tai nạn giao thông.

Nhờ các công nghệ như computer vision, machine learning và big data, hệ thống này có thể xử lý dữ liệu video theo thời gian thực và hỗ trợ cơ quan chức năng đưa ra các quyết định nhanh chóng.

Tuy nhiên, bên cạnh những lợi ích, việc triển khai camera AI cũng đặt ra nhiều thách thức liên quan đến:

- Bảo mật hệ thống;
- Quyền riêng tư cá nhân;
- Nguy cơ lạm dụng dữ liệu.

2. THỰC TRẠNG CAMERA AI GIÁM SÁT GIAO THÔNG

2.1. Kiến trúc tổng thể hệ thống camera AI giám sát giao thông

Hệ thống camera AI giao thông thường được thiết kế theo kiến trúc nhiều lớp, bao gồm:

2.1.1. Lớp thu thập dữ liệu (Data Acquisition Layer)

Đây là lớp đầu tiên của hệ thống, chịu trách nhiệm thu thập dữ liệu từ môi trường giao thông.

Các thiết bị gồm:

- Camera giao thông AI;
- Camera nhận diện biển số (ANPR);
- Radar đo tốc độ;
- Cảm biến giao thông.

Dữ liệu thu thập:

- Video giao thông;
- Hình ảnh phương tiện;
- Biển số xe;
- Mật độ lưu lượng.

2.1.2. Lớp xử lý biên - Edge Computing Layer

Tại lớp này, dữ liệu được xử lý ngay tại thiết bị hoặc gần thiết bị nhằm giảm tải cho hệ thống trung tâm.

Các chức năng:

- Phát hiện phương tiện;
- Nhận diện biển số;
- Nhát hiện vi phạm;
- Lọc dữ liệu.

Ưu điểm:

- Giảm độ trễ;
- Giảm băng thông truyền dữ liệu;
- Tăng bảo mật dữ liệu.

2.1.3. Lớp truyền dữ liệu (Network Layer)

Dữ liệu được truyền về trung tâm thông qua các hạ tầng mạng:

- Mạng cáp quang;
- Mạng 4G/5G;
- Mạng IoT;
- Mạng chuyên dụng của thành phố.

2.1.4. Lớp xử lý trung tâm (Cloud/Data Center Layer)

Tại đây hệ thống thực hiện:

- Phân tích dữ liệu lớn;
- Lưu trữ dữ liệu video;
- Chạy thuật toán AI;
- Phát hiện vi phạm giao thông.

Các công nghệ sử dụng:

- Big Data;
- AI Analytics;
- Machine Learning;
- Video Management System (VMS).

2.1.5. Lớp ứng dụng (Application Layer)

Lớp này cung cấp các dịch vụ cho cơ quan quản lý giao thông.

Các ứng dụng gồm:

- Hệ thống phạt nguội;
- Giám sát giao thông thời gian thực;
- Phân tích ùn tắc;
- Điều khiển đèn giao thông thông minh.

2.2. Xu hướng ứng dụng camera AI trong giao thông

Trong những năm gần đây, sự phát triển của trí tuệ nhân tạo, thị giác máy tính và công nghệ IoT đã thúc đẩy sự ra đời của các hệ thống camera giám sát giao thông thông minh. Những hệ thống này không chỉ ghi hình như camera truyền thống mà còn có khả năng phân tích dữ liệu video theo thời gian thực, từ đó phát hiện các hành vi vi phạm giao thông hoặc tình huống bất thường.

Camera AI thường được tích hợp các công nghệ như:

- Nhận diện biển số xe (Automatic Number Plate Recognition - ANPR);
- Nhận diện khuôn mặt;
- Phát hiện hành vi vi phạm giao thông;
- Phân tích lưu lượng giao thông;
- Phát hiện tai nạn hoặc sự cố.

Các hệ thống này có thể hoạt động trong mô hình trung tâm điều hành giao thông thông minh (ITS - Intelligent Transportation Systems), nơi dữ liệu từ hàng trăm hoặc hàng nghìn camera được thu thập và xử lý tập trung.

Theo nhiều nghiên cứu, hệ thống giám sát giao thông sử dụng AI có thể thực hiện nhiều nhiệm vụ nhận dạng như phát hiện đối tượng, nhận dạng hành vi và phân tích sự kiện bất thường từ video giám sát nhằm nâng cao an toàn công cộng.

2.3. Ứng dụng camera AI trong quản lý giao thông tại Việt Nam

Tại Việt Nam, nhiều thành phố lớn đã triển khai hệ thống camera AI để phục vụ công tác giám sát giao thông và xử lý vi phạm.

Ví dụ: Tại TP.HCM, hệ thống camera giao thông bao gồm:

- Hàng trăm camera quan sát giao thông;

- Camera giám sát tốc độ;

- Camera nhận diện biển số;

- Camera phát hiện vi phạm tại các giao lộ.

Chỉ trong khoảng một tháng triển khai, hệ thống đã phát hiện hơn 3.000 trường hợp vi phạm giao thông như vượt đèn đỏ, đi sai làn hoặc dừng, đỗ sai quy định.

Ngoài ra, tại Hà Nội, hệ thống camera AI đã ghi nhận hơn 6.300 trường hợp vi phạm giao thông chỉ sau một tháng vận hành, trong đó phổ biến nhất là lỗi vượt đèn đỏ và không đội mũ bảo hiểm.

Những con số này cho thấy camera AI đang đóng vai trò quan trọng trong việc:

- Nâng cao ý thức chấp hành luật giao thông;

- Hỗ trợ xử lý vi phạm tự động;

- Giảm áp lực cho lực lượng cảnh sát giao thông.

2.4. Lợi ích của hệ thống camera AI giao thông

Việc ứng dụng camera AI trong giao thông mang lại nhiều lợi ích đáng kể:

- Tăng hiệu quả giám sát giao thông:

Camera AI có thể hoạt động liên tục 24/7 và giám sát nhiều khu vực cùng lúc.

- Hỗ trợ xử phạt tự động:

Hệ thống có thể tự động phát hiện vi phạm và lưu bằng chứng hình ảnh.

- Giảm tai nạn giao thông:

Việc giám sát chặt chẽ giúp nâng cao ý thức người tham gia giao thông.

- Hỗ trợ quản lý đô thị thông minh:

Dữ liệu giao thông thu thập từ camera AI giúp phân tích:

+ Mật độ phương tiện;

+ Thời gian ùn tắc;

+ Tối ưu hóa hệ thống đèn giao thông.

2.5. Những thách thức trong triển khai

Mặc dù mang lại nhiều lợi ích, hệ thống camera AI cũng đặt ra nhiều thách thức:

- Chi phí đầu tư lớn;

- Yêu cầu hạ tầng mạng mạnh;

- Quản lý dữ liệu phức tạp;

- Rủi ro về quyền riêng tư.

Các nghiên cứu cho thấy, việc sử dụng hệ thống giám sát AI có thể gây ra cảm giác "luôn bị theo dõi", từ đó làm gia tăng lo ngại về quyền riêng tư và tự do cá nhân.

3. NHỮNG LỖ HỔNG TIỀM ẨN TỪ CAMERA AI GIÁM SÁT GIAO THÔNG

3.1. Rò rỉ dữ liệu cá nhân

Camera AI thu thập nhiều dữ liệu nhạy cảm như:

- Hình ảnh khuôn mặt;

- Biển số xe;

- Vị trí và thời gian di chuyển;

- Video hành trình.

Nếu hệ thống bảo mật kém, dữ liệu này có thể bị rò rỉ hoặc bị truy cập trái phép.

Các hệ thống camera kết nối Internet có thể bị tin tặc xâm nhập để chiếm quyền điều khiển và thu thập dữ liệu cá nhân của người dùng.

3.2. Tấn công mạng vào hệ thống camera

Camera giám sát thường được kết nối với mạng Internet hoặc mạng nội bộ.

Những lỗ hổng phổ biến bao gồm:

- Mật khẩu mặc định;

- Firmware lỗi thời;

- Giao thức truyền dữ liệu không mã hóa;

- Cổng mạng mở.

Khi bị tấn công, hacker có thể:

- Truy cập dữ liệu video;

- Thay đổi cấu hình hệ thống;

- Sử dụng camera làm điểm tấn công vào mạng nội bộ.

3.3. Phân tích dữ liệu từ lưu lượng mạng

Ngay cả khi dữ liệu camera được mã hóa, thông tin riêng tư vẫn có thể bị suy đoán thông qua phân tích lưu lượng mạng.

Một nghiên cứu cho thấy, các nhà nghiên cứu có thể suy ra hoạt động trong khu vực giám sát thông qua kích thước gói tin và thời gian truyền dữ liệu, ngay cả khi dữ liệu video được mã hóa.

Điều này cho thấy việc mã hóa dữ liệu thôi là chưa đủ để bảo vệ hoàn toàn quyền riêng tư.

3.4. Sai sót của thuật toán AI

Các hệ thống AI nhận diện hình ảnh có thể mắc lỗi trong nhiều trường hợp:

- Ánh sáng yếu;

- Biển số bị che khuất;

- Góc quay không phù hợp.

Ngoài ra, các nghiên cứu chỉ ra rằng, hệ thống nhận diện khuôn mặt có thể nhận diện sai đối tượng do dữ liệu huấn luyện không đầy đủ hoặc thiên lệch.

Sai sót này có thể dẫn đến:

- Phạt nhầm người;

- Nhận diện sai phương tiện;

- Ảnh hưởng đến quyền lợi cá nhân.

3.5. Tấn công AI (Adversarial Attack)

Một số nghiên cứu đã chứng minh rằng, các hệ thống nhận diện dựa trên học máy có thể bị đánh lừa bằng các mẫu nhiễu đặc biệt (adversarial patch).

Các mẫu này có thể làm giảm đáng kể khả năng phát hiện của hệ thống giám sát hoặc khiến hệ thống nhận diện sai đối tượng.

Điều này đặt ra thách thức lớn đối với độ tin cậy của các hệ thống camera AI.

3.6. Lạm dụng dữ liệu và giám sát quá mức

Một trong những vấn đề lớn của camera AI là nguy cơ giám sát quá mức (mass surveillance).

Một số trường hợp trên thế giới cho thấy hệ thống nhận diện khuôn mặt đã được sử dụng để theo dõi người dân mà không có sự minh bạch hoặc giám sát pháp lý đầy đủ, làm dấy lên nhiều tranh cãi về quyền riêng tư và quyền tự do cá nhân.

4. GIẢI PHÁP KHẮC PHỤC

4.1. Tăng cường bảo mật hệ thống

Các biện pháp kỹ thuật cần áp dụng bao gồm:

- Mã hóa dữ liệu truyền tải (TLS/SSL);

- Cập nhật firmware thường xuyên;

- Sử dụng mật khẩu mạnh;

- Thiết lập tường lửa mạng;

- Phân tách mạng camera với mạng nội bộ.

4.2. Áp dụng nguyên tắc Privacy by Design

Privacy by Design là phương pháp tích hợp bảo vệ quyền riêng tư ngay từ giai đoạn thiết kế hệ thống.

Các biện pháp bao gồm:

- Giảm thiểu dữ liệu thu thập;

- Ẩn danh dữ liệu;

- Làm mờ khuôn mặt khi không cần thiết;

- Chỉ lưu dữ liệu trong thời gian cần thiết.

4.3. Kiểm soát truy cập dữ liệu

Hệ thống cần triển khai:

- Xác thực đa yếu tố (MFA);

- Phân quyền truy cập dữ liệu;

- Ghi nhật ký truy cập (audit log);

- Giám sát truy cập bất thường.

4.4. Áp dụng công nghệ bảo vệ dữ liệu

Một số công nghệ có thể áp dụng:

- *Edge computing:* Xử lý dữ liệu tại thiết bị camera thay vì gửi toàn bộ dữ liệu về trung tâm.

- *Differential privacy:* Bảo vệ dữ liệu cá nhân khi phân tích dữ liệu.

- *Homomorphic encryption:* Xử lý dữ liệu khi đang mã hóa.

4.5. Kiểm thử và đánh giá an ninh

Cần thực hiện:

- Kiểm thử xâm nhập (penetration testing);

- Đánh giá lỗ hổng bảo mật;

- Kiểm tra hệ thống định kỳ.

4.6. Hoàn thiện khung pháp lý

Ngoài giải pháp kỹ thuật, cần xây dựng các quy định pháp lý như:

- Luật bảo vệ dữ liệu cá nhân;

- Quy định thời gian lưu trữ dữ liệu;

- Quy trình xử lý khi xảy ra rò rỉ dữ liệu;

- Cơ chế khiếu nại khi xử phạt nhầm.

5. KẾT LUẬN

Camera AI đang trở thành một công cụ quan trọng trong quản lý giao thông và xây dựng đô thị thông minh. Nhờ khả năng phân tích dữ liệu video theo thời gian thực, hệ thống này giúp nâng cao hiệu quả giám sát giao thông, phát hiện vi phạm và hỗ trợ lực lượng chức năng trong công tác quản lý trật tự an toàn giao thông.

Tuy nhiên, việc triển khai camera AI cũng đặt ra nhiều thách thức liên quan đến an toàn thông tin và quyền riêng tư cá nhân. Các lỗ hổng bảo mật trong thiết bị, hệ thống mạng hoặc thuật toán AI có thể dẫn đến rò rỉ dữ liệu, nhận diện sai hoặc bị tấn công mạng. Ngoài ra, việc thu thập và xử lý dữ liệu quy mô lớn cũng làm gia tăng nguy cơ giám sát quá mức và lạm dụng thông tin cá nhân.

Do đó, để đảm bảo hệ thống camera AI hoạt động hiệu quả và an toàn, cần kết hợp đồng thời nhiều giải pháp:

- Tăng cường bảo mật kỹ thuật;

- Áp dụng nguyên tắc bảo vệ quyền riêng tư ngay từ thiết kế;

- Kiểm soát chặt chẽ việc truy cập dữ liệu;

- Hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân.

Việc cân bằng giữa an ninh giao thông và bảo vệ quyền riêng tư là yếu tố quan trọng để đảm bảo sự chấp nhận của xã hội đối với các hệ thống giám sát thông minh trong tương lai.

TÀI LIỆU THAM KHẢO

[1] Bộ Công an. Triển khai hệ thống camera AI phục vụ xử lý vi phạm giao thông, 2026.

[2] Báo Thanh Niên. Camera AI phát hiện hơn 3.000 trường hợp vi phạm giao thông tại TP.HCM, 2025.

[3] Chính phủ Việt Nam. Mở rộng ứng dụng camera AI phạt nguội trong quản lý đô thị, 2026.

[4] Công an Nghệ An. Cảnh giác nguy cơ mất an toàn thông tin từ camera giám sát, 2024.

[5] ScienceDirect. Invisible Eyes: Real-time Activity Detection through Encrypted Wi-Fi Traffic, 2025.

[6] Blockchain Council. AI and the Ethics of Surveillance, 2025.

[7] Rahimi Ardabili et al. Understanding Policy and Technical Aspects of AI-Enabled Smart Video Surveillance, 2023.

[8] Thys et al. Fooling Automated Surveillance Cameras: Adversarial Patches to Attack Person Detection, 2019.

[9] Wang et al. AI Eyes on the Road: Cross-Cultural Perspectives on Traffic Surveillance, 2025.