ALIF SEMICONDUCTOR

Enhancing Computer Vision Accuracy in Security Cameras with Ensemble Family MCUs

Smart security camera. Photo credit: Shutterstock

In the last decade, the surveillance field has undergone a significant transformation, evolving from basic video monitoring to intelligent systems capable of recognizing and interpreting visual data. This case study delves into the evolution of security cameras, the rising demand for AI and Machine Learning (ML) capabilities in security systems, and highlights the need for enhanced computer vision accuracy. It also explores how the Ensemble Family of Microcontrollers (MCU) can be pivotal in achieving this enhancement while ensuring reliable, efficient security systems.

Evolution of Security Cameras: From Basic Surveillance to Intelligent Monitoring

Conventional surveillance cameras are designed as passive devices to record video footage for subsequent review. The first generation of surveillance cameras were Closed-Circuit Television (CCTV) systems, characterized by their low resolution and limited functionality. However, with increased adoption of AI/ML technologies, security cameras have transitioned into sophisticated monitoring devices for real-time monitoring, high-definition imaging, cloud storage, and more.

Today's security cameras are not just capable of recording, but also of analyzing captured footage in real-time. Embedded with intelligent algorithms, they can identify, track, and analyze objects and behaviors in their field of view. This shift from passive recording to proactive monitoring has paved the way for applications like facial recognition, motion detection, and anomaly detection, adding a new dimension to security and surveillance.

AI/ML Capabilities in Security Cameras

Traditional surveillance systems require human monitoring, which is labor-intensive and prone to errors. AI/ML algorithms can analyze and process vast amounts of data quickly and accurately, identifying potential threats or anomalies that can be missed by a human observer. AI-powered security cameras, for instance, can be programmed to recognize patterns like unattended bags in public spaces, or to identify or track individuals across multiple camera feeds. These capabilities are invaluable in enhancing public safety and ensuring timely responses to security incidents. Moreover, while facility and residential surveillance are popular use cases, potential applications are nearly unlimited. As an example, AI-powered security cameras can detect and

monitor wildlife, such as endangered species, by capturing high-resolution pictures and video footage that can be used to study their behaviors in the wild.

The Importance of Computer Vision Accuracy

Enhancing the computer vision accuracy of AI-powered security cameras is crucial for several reasons. False positives, where a non-threatening situation is incorrectly identified as a threat, can lead to unnecessary panic and resource allocation. False negatives, meanwhile — where a legitimate threat goes undetected — can have serious implications. Enhanced accuracy can be achieved by improving AI/ML algorithms for image processing, object detection, and pattern recognition. This involves optimizing the software to better interpret the data from the camera's sensors and make accurate predictions or identifications.

Microcontrollers are the heart of many embedded systems, including security cameras. They are responsible for processing data from camera sensors, running algorithms to detect and analyze objects, and making decisions based on analysis. As computer vision algorithms become more sophisticated, the demand on processing power increases and traditional MCUs may struggle to keep up, leading to reduced accuracy and slower response times.

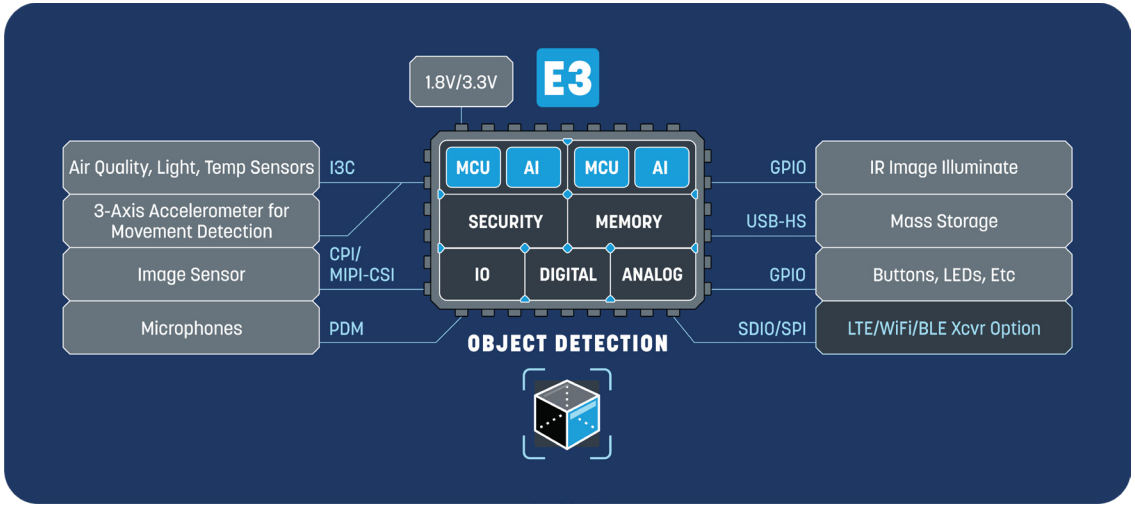
Computer vision challenges in AI-enabled security cameras include the following:

- Latency: Delays in data processing might lead to the inability to capture essential scenes or trigger alarms in real-time.
- False Positives/False Negatives: Without the ability to process algorithms, cameras may either wrongly recognize or overlook objects, resulting in unwarranted alarms.
- Low-light Performance: Security cameras might encounter difficulties in precisely detecting and tracking objects under insufficient lighting conditions.
- Insufficient Computational Capabilities: Security cameras may employ MCUs that lack the adequate processing power to execute computer vision algorithms.

By integrating advanced MCUs with AI/ML capabilities, manufacturers can significantly improve the vision accuracy of their security cameras.

E3 Series MCU block Image. Image credit: Alif Semiconductor

Ensemble MCUs Enhance Computer Vision Accuracy in Security Cameras



E3 Series MCU block diagram. Image credit: Alif Semiconductor

Alif Semiconductor is a leading provider of scalable and secure AI-enabled, 32-bit embedded microcontrollers. Alif's Ensemble MCUs offer high performance and reduced power consumption while enhancing the vision accuracy of AI-enabled cameras. Ensemble MCUs are equipped with powerful processors, integrated memory, and a range of peripherals that make them suitable for running complex algorithms.

Alif's E3 Series MCUs are engineered to provide a perfect blend of performance, power efficiency, and AI/ML capabilities, enabling security cameras to perform the most complex computer vision tasks with high accuracy and minimal latency.

Below are some key features:

High-Performance MCU Core and Optional NPU

The E3 Series is equipped with a high-performance MCU core that can operate at frequencies of up to 400 MHz. This ensures that the system can handle computationally intensive tasks such as image processing, video analytics, and real-time data processing.

To further enhance the real-time processing capabilities, the E3 Series offers two optional micro Neural Processing Unit (microNPU) for parallel processing, boosting the security camera's ability to perform multiple tasks simultaneously.

Advanced Object and Event Classification

The E3 Series MCU advanced object and event classification allows security cameras to not only detect movement, but also identify and classify the object in question — whether it's a person, vehicle, or animal. This level of classification is crucial for security applications where different responses are required based on the identified object or event.

Real-Time Processing and Fast Response Times

The combination of two high-performance MCU cores and up to two microNPU ensures that E3 MCUs process data efficiently in real-time, which is suitable for applications where fast response times are crucial. By processing and analyzing data on the edge, the system can trigger alarms or notifications instantaneously, ensuring timely intervention when necessary.

Autonomous Power Management

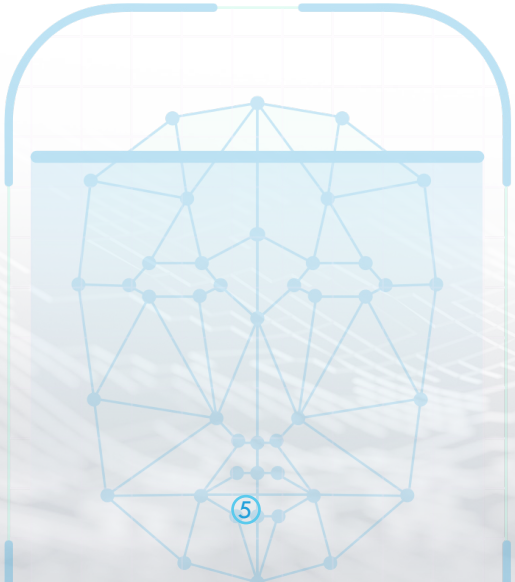
The E3 Series is designed with aiPM™ technology, which offers autonomous power management features that optimize energy consumption based on workloads. This ensures that cameras can operate for extended periods without frequent battery replacements, making it ideal for remote or hard-to-reach installations.

Person Detection and Gesture Recognition

With the integration of E3 MCUs, security cameras can be equipped with person detection and gesture recognition capabilities. This feature allows the cameras to distinguish between humans and other objects and even interpret specific gestures or actions. Such features can be used for user interactions or to trigger specific responses based on the detected gestures.

Enhanced Optical Character Recognition

Alif's E3 Ensemble MCUs enhance Optical Character Recognition (OCR) capabilities in security cameras by leveraging advanced image processing and ML algorithms. This allows cameras to accurately detect and monitor objects from various surfaces and at different angles, minimizing the likelihood of false positives or false negatives.

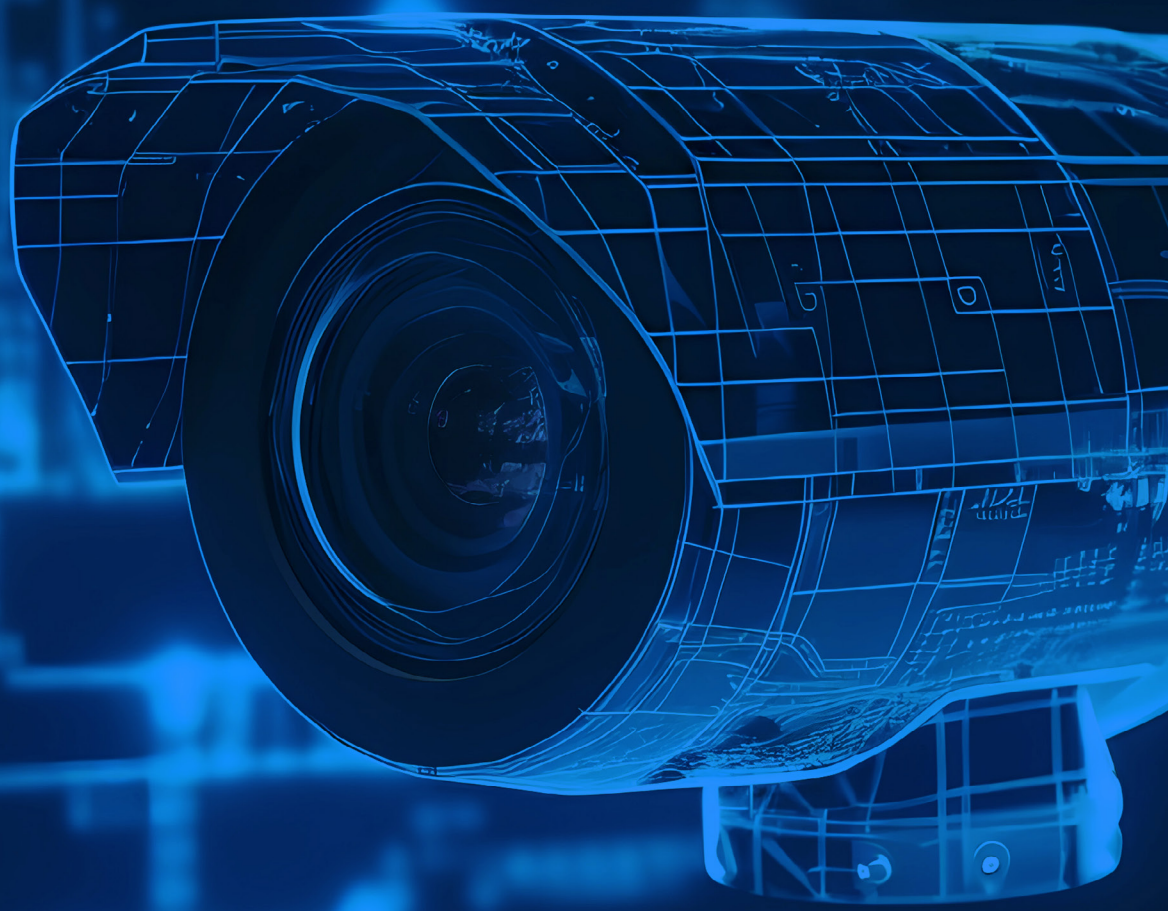


Smart security camera for wildlife monitoring

Image credit: Shutterstock

Conclusion

Security cameras have evolved from basic surveillance tools into intelligent monitoring systems. With the increasing demand for AI/ML capabilities in these cameras, there is a pressing need to enhance the accuracy of computer vision in these systems. By integrating AI/ML-capable MCUs, developers can significantly enhance the accuracy and reliability of computer vision applications. This ensures robust and dependable security systems for improved monitoring and protection of people and assets. Alif Semiconductor's Ensemble Family of MCUs, with its powerful processing capabilities, energy efficiency, and flexibility, offer an excellent solution to meet these demands and ensure the continued evolution of intelligent security systems.



For more information on Ensemble MCUs and technical specifications, please visit: https://alifsemi.com/products/ensemble/