We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

6,300
Open access books available

170,000
International authors and editors

185M
Downloads

154
Countries delivered to

Our authors are among the
TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

Introductory Chapter: Intelligent Video Surveillance – What's Next?

Pier Luigi Mazzeo

1. Introduction

Most of the biggest urban areas are speedily translating into smart cities with structures able to handle huge quantity of data shaped by the Internet of Things apparatus for intelligent analysis. Decreasing human contribution and improving people's life quality are two main objectives that smart cities proposed to reach. A concrete research field and its applications that satisfy both of these principles is smart video surveillance [1].

Intelligent video surveillance systems aim to analyze the observed scenario using machine learning, computer vision, and data analytics in order to minimize or completely eradicate human contribution.

The request for such intelligent security systems qualified for recognizing both natural emergencies, such as fire, floods, earthquakes, and human-made emergencies, such as violence, traffic accidents, and weapon threats, is growing solidly [2].

Intelligent video surveillance systems are usually adopted in different contexts, spreading from public areas and infrastructures to commercial buildings. They are often used for a double scope: i) real-time monitoring of physical estates and areas and ii) for reviewing collected video information to estimate security indicators and plan safety measures, consequently.

In the last decades, intelligent video surveillance systems are deeply employed in the public and security sectors, but now a significant interest in these topics has quickly been raised by other stakeholders. This interest has been caused by the constant increase in crime rates and security national and international threats, which are conducting incredible growth in the market of video surveillance and security systems. A report redacted by Mordor Intelligence [3] estimates that the video surveillance market has been valued at 30 billion dollars in 2016, but is expected to reach a value of 72 billion dollars by the end of 2022. A boost to the market perspective is also given by the recent results obtained in artificial intelligence and digital technologies—introducing intelligence, scalability, and higher accuracy in video surveillance solutions. Some spontaneous questions arise—what are the main technology trends in smart video surveillance and how can they be best used?

2. Technology trends in intelligent video surveillance solutions

- **Scene-aware intelligent video data gathering:** The obtained results in signal and image digital processing bring great progress to intelligent video surveillance systems, in particular, those that can be smarting adapt to the video data collection frame acquisition rate. When a security anomaly is detected, the data acquisition frame rate is increased accordingly in order to pick up richer and higher definition information for having more accurate and reliable results.

- **Big data infrastructures:** Advances in big data infrastructures have created more opportunities for video data storage and access, based on the four Vs of big data: volume, velocity, variety, and veracity. This way, gathering huge quantities of data from numerous cameras, taking into account high congestion streaming data rates, is much more efficient with respect to last year. Studying novel big data solutions increments the creation and deployment of smart video surveillance architectures that scale unceasingly and cost-effectively.

- **Streaming data devices:** Varying solutions in streaming systems have arisen in the last few years. These systems enable streaming management and analysis skills and are crucial portions of the big data systems examined.

- **Proactive analytics and artificial intelligence (AI):** Artificial intelligence and machine learning have given a new impulse for introducing new features in the smart surveillance systems, thanks to the materialization of disrupting deep learning methodologies, such as those introduced by Google's Alpha AI engine [4] and DeepMind. The growth of deep neural networks can be openly integrated into video surveillance systems to arm them with outstanding intelligence and able to boost more effective surveillance activities. As an interesting AI application includes predictive analytics, which helps security operators to foresee security events and act proactively.

- **UAV and the Internet of Things (IoT):** Next generation of smart surveillance systems and security includes the fusion of Internet of Things equipment and smart entities. Employing unmanned aerial vehicles (UAVs) (i.e., drones) in smart video surveillance introduces such versatility reaching some areas that are problematic to reach using traditional fixed cameras.

- **Physical and cyber security interaction:** Industrial assets' digital transformation with the innovation process is incrementally merging physical and digital security measures. New smart video surveillance solutions act as a protagonist in this merging because they express IT architectures employed to inspect wide physical areas. This way, they can be directly included in different cybersecurity structures for a universal and unified approach to security, safety, and surveillance.

3. Designing and developing of video surveillance systems

All the technologies described above open new challenges and possibilities in the expansion, application, and function of new generation of intelligent video surveillance systems. An important role is played by the developers and implementers of this intelligent surveillance systems, who should integrate and use full features of the mentioned cutting-edge technologies. To reach this objective, it is crucial to design and realize the right architecture for the video surveillance framework. Novel intelligent video surveillance solutions respect the **edge/fog-computing paradigm** [5] (see **Figure 1**) to elaborate video data sources earlier directly near the observed scene. Using this paradigm permits to save bandwidth performing real-time security supervising. Smart cameras are placed at the edge of the designed network and become edge nodes, where frames are grabbed and processed "in situ." This way, the intelligence is decentralized and these edge nodes can realize data collection intelligence and tuning frame rate, according to the recognized security context. Furthermore, they are linked to the cloud architecture, where information from multiple cameras is merged, assessed, and processed on higher time scales.

Choosing edge/fog-computing architectures [5] is the best choice for supporting the integration of past video surveillance systems with the actual technologies. IoT-driven drones will be combined with suitable edge nodes and they will be part of a mobile edge-computing infrastructure. It is strongly recommended that real-time processing of the acquired streaming flow should be computed at the edge, instead of in the cloud of the video surveillance architecture. Contrarily, deep learning computing can be performed both at the edge and in the cloud of the video surveillance infrastructure: If deep neural networks are placed at the edge, they can extract complex feature patterns in real time. However, the extraction of complex feature patterns and information over wider areas observed by several edge nodes (e.g., city-level structure) should be done only if deep learning is implemented in the cloud.

In general, it is difficult to find the right balance among the functionality to place in the cloud or on the edge. The decisions are done by making a trade-off among some opposite features (e.g., processing speed versus obtained results accuracy for some surveillance tasks).

All the smart video surveillance solutions should take some advantages of open equipment from different cameras and device vendors. In fact, a surveillance system may contain different devices and video capture means (e.g., high-definition cameras,

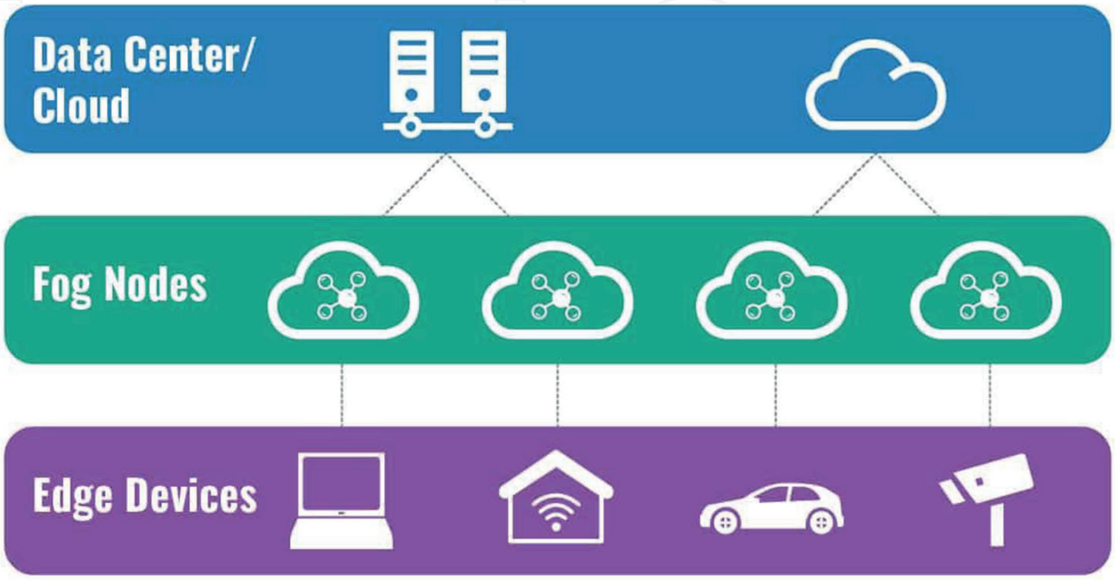

Figure 1.
Edge/fog-computing paradigm.

wired or wireless cameras, cameras in drones/UAVs, and so on). There are many benefit to have an open architecture because we can obtain flexibility, elasticity, and technological durability. In the last years, some energies have been spent to present an open, standards-based architecture for edge/fog computing in order to have video surveillance as the principal example of the use of fog computing.

4. Discussion and future works in intelligent video surveillance solutions

Choosing the right configuration when an edge-computing architecture is designed for implementing a video surveillance system that meets other kinds of challenges. These kinds of challenges include privacy preservation and data protection compliance. For example, producing surveillance devices is subjected to many privacy and data protection regulations and directives emanating from different countries. This often forces some restrictions in designing smart video surveillance systems. Stronger limitation are also applied in the use of drones that must respect some tighter regulations.

Another type of challenge interests the automation rate reached by the proposed solution. Considering that automation is commonly required for covering and monitoring wider spaces and saving further human workers, but human involvement in assessing is still necessary for the trustworthiness of the designed solution. Furthermore, it should be considered that nowadays new cyber-physical threats and attacks are arising against surveillance systems. Notice that a physical attack is often supported by a cyberattack on the video surveillance framework, which completely compromise the capacity to detect the physical assault that is happening.

The implementation of intelligence is data-driven (e.g., proactive threat prediction and AI analysis) needs large amounts of data that include examples of security threats that are very difficult to have. The study and design of artificial intelligence algorithms (e.g., lightweight and easy-to-use deep neural networks) is taking its first steps, although numerous innovative start-ups with cutting-edge AI products and services are already emerging.

Facing the many new challenges described above by developers and distributors of intelligent video surveillance solutions forces them to better comply with standards and regulations while adopting a phased approach to deployment. This gradual process should enable a transition from manual, that is, human-mediated, systems to fully automated video surveillance based on artificial intelligence.

Overcoming the challenges, we face requires a gradual implementation of data-driven intelligence. Starting with simple supervised training rules and moving on to more sophisticated machine learning techniques capable of detecting more complex asymmetric attack patterns. Another important outcome that could be achieved is the implementation of open architectures capable of accommodating innovative surveillance sensors by making them coexist with older ones, so as to exploit new advanced capabilities while obtaining the best value for money.

In conclusion, it can be said that all future smart video surveillance solutions may include many innovative features and functionalities, as they may employ new cutting-edge IT and artificial intelligence technologies.

IntechOpen

IntechOpen

Author details

Pier Luigi Mazzeo
National Research Council of Italy (CNR), Institute of Applied Sciences and Intelligent Systems (ISASI), Lecce, Italy

*Address all correspondence to: pierluigi.mazzeo@cnr.it

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. cc BY

References

[1] Porikli F, Brémond F, Dockstader SL, Ferryman J, Hoogs A, Lovell BCS, et al. Video surveillance: Past, present, and now the future dsp forum. IEEE Signal Processing Magazine. 2013;**30**(3):190-198

[2] Xu Z, Hu C, Mei L. Video structured description technology based intelligence analysis of surveillance videos for public security applications. Multimedia Tools and Applications. 2016;**75**(19):12155-12172

[3] Available from: https://www.marketsandmarkets.com/Market-Reports/video-surveillance-market-645.html

[4] Available from: https://www.deepmind.com/research/highlighted-research/alphago

[5] Raj P, Saini K, Surianarayanan C, editors. Edge/Fog Computing Paradigm: The Concept, Platforms and Applications. Vol. 127. Advances in Computers Series; 2022. ISBN: 9780128245064

IntechOpen

IntechOpen