Special section on emerging multimedia technology for smart surveillance system with IoT environment

- Brian Kim
- Kostas Psannis
- Harish Bhaskar

The internet-of-things (IoT) can be defined as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects) is expected to usher in automation covering all major engineering fields, while also enabling advanced applications such as smart grid and smart surveillance.

Smart surveillance system is mainly composed of automatic video/audio analysis. Therefore, an emerging surveillance system must consider multimedia information for monitoring activities and extracting meaningful information from the environment. Researchers are working to solve a number of challenging questions that are often encountered during the designing of smart surveillance systems. Some of those interesting questions are tough and fundamental, but unavoidable: what are the applications of smart surveillance? What are the possible system architectures for smart surveillance? What are the core technologies? What are key technical challenges? What are the implications of smart surveillance, both to security and privacy?

As we anticipate, surveillance technology will be soon adopted to large networked system, we believe the role of IoT becomes very important in this context. This Special Issue aims to highlight the latest research results and advances on various signal processing algorithms, architectures, and technologies for multimedia-based smart surveillance system, and especially their applications in the IoT environment.

In response to the call-for-papers of this Special Issue, we received very interesting submissions, from both industry and academia. Specifically, 20 papers were submitted, which have been assessed by many reviewers. All the reviewers are experts of the highest level, from both industry and academia, and their collaboration has been essential for the success of this Special Issue.

As a result of the review process, we have selected 13 papers among them, which reflect prominent efforts and advances in the design and development of smart

surveillance system and architecture with the internet-of-things (IoT). There are three categories: architecture (system), networks, and advanced algorithm.

For architecture (system), Park et al. present an improved scalable architecture for an automated surveillance system using edge computing. They provide an alternative way of reducing the server resource and wireless network limitation. The paper by Lim et al. develops an ultra-HD (UHD) HEVC encoding system using SIMD implementation. Through this implementation, they make fast encoding schemes (about 192 times faster) for real-time smart surveillance system. A frameNet extension which is called as AspectFrameNet, is proposed for analysis of sentiments around product aspects by Chatterji et al. AspectFrameNet provides a framework that helps the semantic analysis of text inputs from social feeds and news (Voice of Customer) by disambiguating the contexts in which the lexical units are used. Alsmirat et al. develop a cloud-supported large-scale wireless surveillance system. This paper designs and evaluates a reliable IoT-based wireless video surveillance system that provides an optimal bandwidth distribution and allocation to minimize the overall surveillance video distortion.

For networks for smart surveillance system with IoT, Batalla et al. propose an evolutionary multi-objective optimization algorithm for multimedia delivery using two-phase EMO algorithm, especially in critical applications through Content-Aware Network. Also, Seo et al. suggest improved error-resilient surveillance video transmission based on a practical joint source-channel distortion computing model, especially for ultra-high quality video application. Through simulations, they show that the proposed method can accurately estimate the channel loss threshold set, resulting in an optimal FEC code rate with low computational complexity. A real-time wireless multisensory smart surveillance with 3D-HEVC streams is proposed by Kokkonis et al., especially for internet-of-things (IoT). In this paper, an adaptive packet frame grouping (APFG) and adaptive quantization are deployed in order to maximize the quality-of-experience (QoE).

As the part of advanced algorithm, Kim et al. propose a fast coding unit (CU) determination algorithm for high-efficiency video coding (HEVC) in smart surveillance application. This paper focuses on developing fast mechanism HEVC encoding system based on spatial and temporal information in which 13 neighboring coding tree units (CTUs) are present. Also, Gupta et al. propose a cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. This paper deals with authentication scheme with IoT environment. A geocasting-based synchronization of Almanac on the maritime cloud is suggested for distributed smart surveillance, by Park et al. The proposed method ensures integrity based on block ID and supports delta update, thereby minimizing bandwidth and boosting performance. The paper by Singh et al. presents an efficient method for moving object detection in smart surveillance environment. They use the modified temporal differencing and local fuzzy thresholding to improve the detection accuracy. The paper by Kim et al., proposes national cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment. To provide reliable IoT services for critical infrastructure utilizing IoT devices, the present paper proposes methods for predicting errors that may occur in physical situations where things are connected to each other and analyzing and modeling the errors as a functional

requirement. Lee et al. propose a block chain-based secure firmware update for embedded devices in IoT environment. This paper introduces a new scheme for firmware update, in which a blockchain technology is proposed to securely check a firmware version, validate the correctness of firmware, and download the latest firmware for the embedded devices.

In our opinion, both the scope and the high technical quality of the accepted papers make them very relevant for anyone involved, or just interested, in the smart surveillance system and architecture with the internet-of-things (IoT), especially in terms of architecture, networks, and advances in algorithm.

The guest editors would like to thank the authors, reviewers, the editorial staff at Springer and the editors-in-chief for supporting this Special Issue for its success. We hope that this Special Issue will have a broad impact on the smart surveillance system and architecture expert groups in the internet-of-things (IoT) environment, especially in terms of architecture, networks, and advances in algorithm.