Applications of Internet of Things

Subjects: Computer Science, Artificial Intelligence

Contributor: Abbas M. Al-Ghaili, Hairoladenan Kasim, Zainuddin Hassan, Naif Mohammed Al-Hada, Marini Othman, Rafiziana Md. Kasmani , Ibraheem Shayea

IoT-dependent systems (IoTSs) cause heavy usage of energy. This is one of the biggest issues associated with IoTSs. Another issue is that the security of digital content is a big challenge and difficulty. Image processing has recently played an essential role in resolving these difficulties.

Keywords: image processing ; energy consumption ; IoT systems ; location detection

1. IoT Monitoring Applications Based on Image Processing

Video surveillance and monitoring systems are extensive and encompass diverse uses. For example, fire monitoring and detection systems may be of various sorts. There are two linked procedures executed in succession to conduct monitoring and detection operations. For monitoring, smart sensors are employed, while for the second one, image processing techniques are applied, including object detection. Monitoring such a thing or situation that changes over time usually results in many static images (i.e., multi-frame images) whose contents, objects, and regions, including color (image pixels' intensities and/or values), change over time. These grouped images are then processed image by image to identify objects. Monitoring is required to produce multi-frame images to correctly recognize objects. It is possible to operate a camera with a monitoring device that is based on senses, such as smart sensors. In these applications, monitoring process(es) would transmit alerts to a distant center to analyze data or images employing the IoT platform. An example of such uses is described in [1]. Prior to the detection process, a monitoring process employing smart sensors is done. Smart sensors are deployed in various places inside a region of interest (ROI) to transmit alerts. IoT-connected devices such as cameras make a function that remotely transfers collected images to the data processing center. The use of image processing in this context has allowed IoT to better meet human needs while also protecting the environment.

Multi-frame image processing may be seen in a variety of contexts [2][3]. According to [2], a smart camera-based IoT monitoring application is used to track and record certain events based on a predefined set of instructions that allows the camera to consume less energy. The smart camera monitors events based on event detection, and it will be enabled, through its image processing-embedded system, to record only events-of-interest (EOI); therefore, video data will be delivered to a distant processing party employing the IoT. It is recommended that a web server attached to a smart camera be used to allow users to control the camera remotely. Object tracking and identification have aided IoT monitoring applications. In [3], moving background images are processed with the purpose of monitoring, tracking, identifying, and classifying moving objects (vehicles) for road safety. An illustration of IoT monitoring applications based on image processing example is shown in **Figure 1**.

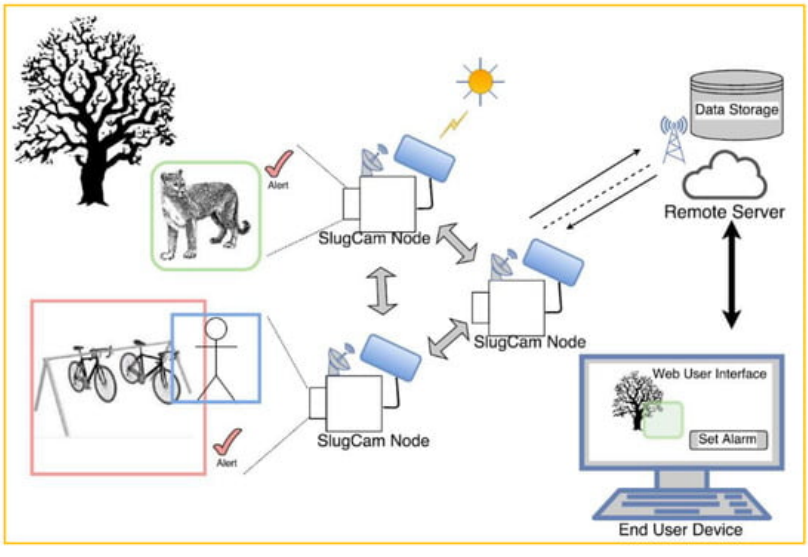

Figure 1. IoT monitoring applications based on image processing—Web-based video server and the Web-based user interface [2].

Object tracking and detection are used in a variety of applications, and one of their primary purposes is to ensure the security of the item that is currently monitored, recorded, tracked, and detected. For example, in [4], a monitoring process is performed on images to apply a protective action through the Internet and cloud media to the item being remotely identified via a cloud-based website. The object of interest (OOI) in the image will be transmitted for analysis. The movement of objects in the acquired images has been processed to identify surrounding environmental factors to apply a security operation to the OOI. A command is sent from a website to the receiving party in order for them to be able to evaluate and control the data that has been transferred to them over the Internet or in the cloud.

The presence of potentially harmful actions or occurrences in industrial zones [5] necessitates constant surveillance in these places. If malicious occurrences are not identified in time, they will most likely result in bodily harm like fires or equipment damage. The proposed method has incorporated various processes in which image processing has been applied. Image processing was used to acquire multi-frame images; then, image processing was used to analyze obtained video, where abnormal actions discovered will be identified; after that, an encryption scheme is to be applied before they are sent to an authorized party through an IoT platform.

Motion detection utilizing a passive infrared sensor (PIR sensor) may be leveraged from numerous IoT applications for monitoring and security reasons to recognize such a movement in a given region. The detection procedure may be completed by using the camera's motion detection as a smart switch to turn the camera on and capture a person's face. The next step is to use an IoT-based device to communicate the image in which the face is detected [6][7].

2. IoT Security Applications Based on Image Processing

Images were used as a means of encrypting and protecting other relevant data. While data is transferred, it is stored on a medium that is not considered to be secure. However, images have been used in such a way that they should have secured data while it was sent until it arrived safely at its destination. Reviewed are several attempts of proposed methods in which digital image processing techniques have been utilized to help secure IoTSs. The overall architecture for IoTSs is illustrated in **Figure 2**.

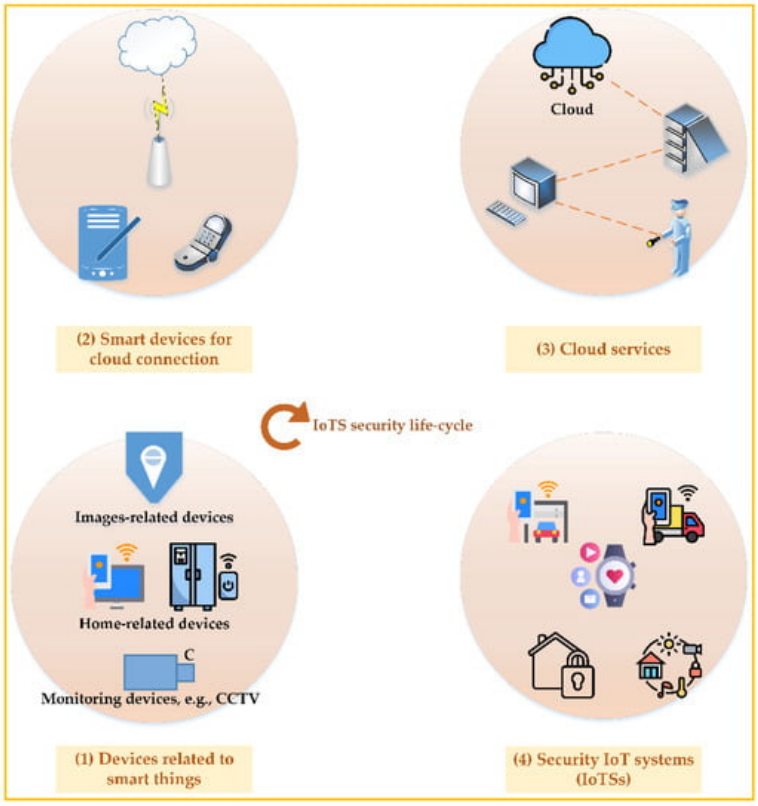

Figure 2. IoTSs security lifecycle: conception and systems.

Biometrics-based encryption is recommended as an alternative to the commonly employed strategies for protecting data exchanged between IoTSs and parties. In [8], it is stated that the proposed method is stronger against vulnerabilities than other strategies, such as password-based authentication, owing to the unique qualities the biometrics-based techniques

have. The proposed method is backed up by a case study that uses pertinent biometrics to accomplish facial recognition. The face image is captured by an IoT-connected device such as a smartphone. IoT platform will be used to send the captured image to the intended destination across a communication network. End-to-end encryption with the aid of image processing techniques may be accomplished.

Image processing techniques have been employed in order to execute a security scheme for an IoT-based home management system [9]. The primary purpose of the proposed system is to conduct a security scheme for the home through an IoT platform by capturing an image at the site the camera-embedded system is put at. Image initialization and pre-processing, analysis, and image matching stored in a database are performed.

To encrypt images, Cellular Automata (CA) was utilized in conjunction with image processing. An 8-bit string series will be generated from pixel intensity values (image elements). These images contain critical information since the camera initially takes an image that will be encrypted at the perception layer. As a result, at this level, they are also encrypted. Secondly, such images will be forwarded to network layers. Once they have been decoded, they can be read. This security strategy has been implemented on sensitive images to provide a secure route between the network and perception levels. The network layer is where the fog nodes are placed. Fog nodes are in charge at this point of sending any images they receive to the Cloud for further processing if that becomes necessary [10].

Since so much data is being delivered in the form of images over the Cloud via IoTSs, image encryption has become more popular in recent years. Therefore, image-based encryption is yet to be developed to serve better [11]. In order for there to be a safe and reliable public connection between the source of the image capture and the fog node, the image must first be encrypted before it can be sent. The combination of pixel intensities with CA-generated values is an intriguing encryption technique.

Security of IoT devices has leveraged image processing by categorizing distributed denial of service (DDoS) malware assaults. Gray-scale images may be initially categorized according to the families. DDoS malware assaults may also be identified, which is the second benefit of monitoring. An additional security scheme may be accomplished with the aid of image processing techniques [12].

For security considerations, the face recognition process is essential. This has been used in a wide range of IoTSs. Face recognition may be utilized with smart homes for numerous functions, such as control and security. Other applications and IoTS are specialized to conduct a face recognition process for the purpose of crowd surveillance in specified places and zones such as airports [13].

The research presented in [14] is an example of another IoT security application that makes use of image processing. To secure IoT image classification against plaintext attacks, the research in [14] has proposed a system that is almost indistinguishable. An IoT device is not necessary to continually connect with the cloud-based image classification system. Using DNNs, a technique for the safe evaluation of linear functions was developed, such as divide-and-conquer and a set of unified ideal protocols. The lattice-based homomorphic method contributes to keeping contents hidden. Pre-trained deep convolutional neural network model of Visual Geometry Group (VGG-16) is used to extract deep information from an image.

3. IoT Safety Applications Based on Image Processing

Image processing in the field of smart cities and IoTS has given rise to a variety of demands and purposes. Image processing has been put to use in an innovative application that aims to improve road safety for motorists and pedestrians by detecting and identifying road targets. Once object recognition has been performed, a reinforcement learning (RL) algorithm based on artificial intelligence (AI) is used to send information to a robot or wearable device so that the user can understand and interact with it to make a decision [15].

The use of face recognition in an OCR-based smart support system is one such example [16]. The proposed system relies on captured images for object detection and recognition so that the visually-challenged person would be supported and led without the requirement for an actual supporter.

Precious and digital assets, such as in workplaces, are deemed to contain sensitive data. A higher level of confidentiality for the relevant information should have been attained via their protection. To provide secure access to such workplaces, there should be a verification of the identity (ID) of the person who is attempting to access them. A face-based matching mechanism will be necessary. Using an image analysis method and a matching process, the proposed IoTS analyzes an

image of a person's face and stores the results. Authorized access may be granted if the face is accurately identified. By doing this, digital assets may be kept private [17].

The IoT has garnered increasingly more attention in recent years. On the other hand, IoT terminal devices take images that are intimately connected to the users' personal information. This information is private and must be protected from unauthorized access. For example, homomorphic encryption primitives may make it easier to keep outsourced computing private, but they use a significant amount of CPU and storage resources in the process. Because of this, IoT terminals with limited resources are put to the test. An architecture for outsourced image processing that includes edge-assisted privacy preservation, image retrieval and classification has been proposed here in order to minimize the amount of resource consumption by terminal devices. To safeguard data while using cloud computing, a semi-trusted cloud server relies on nearby edge nodes. Edge-assisted privacy preservation is presented for image retrieval and classification [18]. An illustration related to IoT safety applications based on image processing is shown in **Figure 3**.

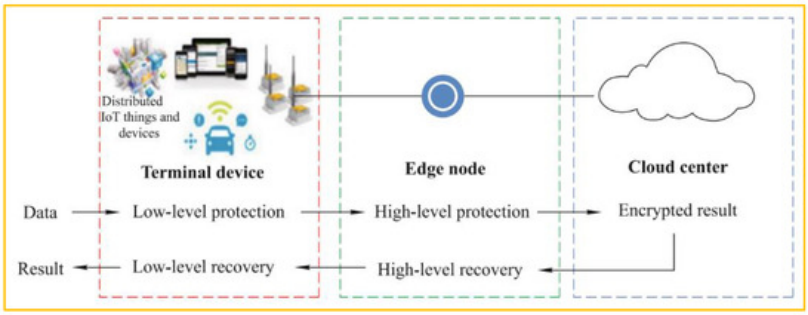

Figure 3. IoT safety applications based on image processing: privacy-preserving outsourced computing architecture [18].

IoT terminal devices' computation, communication, and storage loads may be greatly lowered by the recommended ways. Another method of content security based on image processing is presented [19]. Once the image has been captured, a cryptographic strategy is employed. Then, it was transmitted to another server. In addition, a cover image security mechanism is added to the cryptographic image. A cover image will then include the encrypted image. The last step is to upload the cover image to the cloud via the IoT platform.

Examples of IoTSs that use image processing techniques could include machine safety and environmental monitoring [20], the agricultural industry's plant growth surveillance for improved safety in such a process [21], or the detection of a disease location on plants [22].

4. IoT Location Detection Applications Based on Image Processing

The IoT's growing breakthroughs allow for the building of truly smart settings that can provide first-rate amenities to its occupants and visitors alike. Lately, such smart settings have also been employed to reignite consumers' interest in cultural heritage by presenting them with real, interactive cultural experiences that they can engage in. In [23], an indoor site architecture has been built to enhance the user experience in a museum context. As a result, an image-processing wearable device would be useful for identifying and pinpointing the contents of an image. Therefore, the proposed system could be configured in such a way as to supply users with cultural content that is related to the artworks that they are currently viewing. A Bluetooth low energy (BLE) infrastructure was set up at the museum to get the location data. Furthermore, the system interfaces with the Cloud to preserve multimedia content generated by the user and to publish events made by the environment through social networks. These services connect with physical devices via a middleware that supports numerous protocols. Improvements have been made to cloud-based and IoT-connected location detection services thanks to image processing. The proposed localization mechanism proposed by [23] is shown in **Figure 4**.

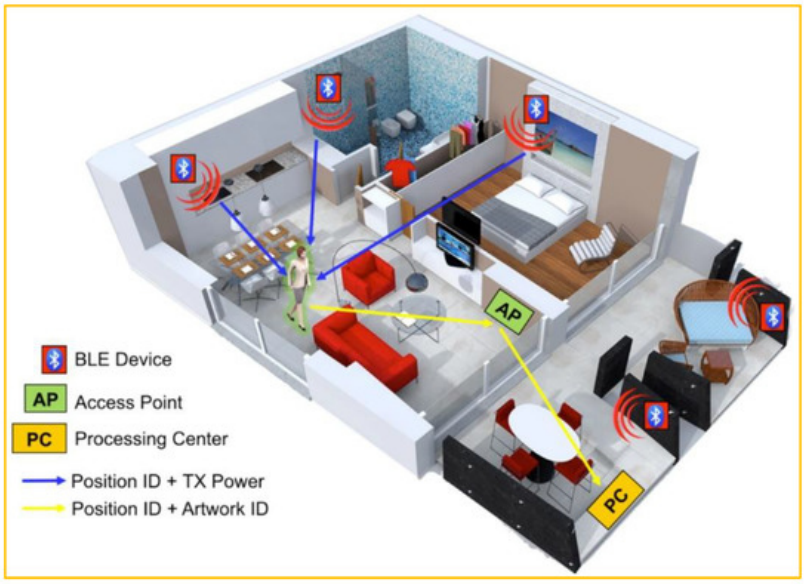

Figure 4. IoT location detection applications based on image processing: localization mechanism elements proposed by [23].

A combination of a camera and a GPS sensor has recently been deployed in agricultural monitoring. It is novel to acquire data in a big area swiftly and independently. Production of such a plant may be improved by employing a drone-based system where the IoT architecture was utilized to help retrieve information in a real-time situation. The detection and classification methods dedicated to plant (e.g., rice) diseases by applying image processing techniques have been reported in [24]. This was done to enhance the rice production process. With the use of a GPS sensor, the proposed system may reveal the location of ill rice plants in a real-time on a map. An earlier and real-time sickness detection system based on IoT architecture has been conceived to contribute to illness detection and prevention systems. Image processing in this example has garnered interest from other systems owing to its object identification abilities.

Similarly, sensors and IoTSs are utilized to monitor environmental parameters. Drones and cloud computing are all components of this detecting system's wireless sensor technology mix. Multiple image processing processes could be integrated to detect, for example, fire occurrence. The proposed system has demonstrated that image processing can be used and exploited to increase the detection of events in places, which can lead to advancements and enhancements in IoTSs that provide greater services to our lives and our green environment [25].

5. IoT Healthcare Applications Based on Image Processing

Medical images used for IoT healthcare are many. One example is described in [26]. It illustrates that the image may be utilized to mask a textual version of diagnostic data. Images are employed to cover data. Since data has been encrypted using industry-standard techniques such as AES and RSA, which stands for Advanced Encryption Standard. Using a 2D discrete wavelet transform (1 level) image, the ciphertext is concealed. The text scale has been suppressed to conceal its contents. To accomplish this, two distinct cover images made from gray-scale and color images have been created, resulting in two distinct font sizes.

Another example of this concept can be found in [27], in which pre-encrypted medical images have been provided, producing an additional layer of protection by having a one-time password (OTP) embedded into them. The encrypted image with the OTP will be transmitted to the same user. After that, the encrypted medical image will be decrypted to reveal the encoded OTP. Finally, the two OTPs, previously retrieved from the medical image, are compared. This verification step is necessary to check the encrypted medical image's integrity. Once the verification procedure is completed, original medical data will be extracted. An illustration related to IoT healthcare applications based on image processing is shown in **Figure 5**.

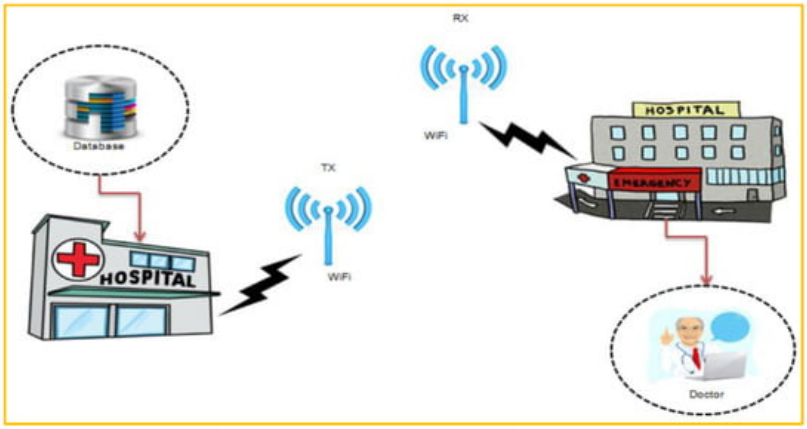

Figure 5. IoT healthcare applications based on image processing: a graphical representation of medical data communication proposed by [27].

Another example may be discussed in [28]. People in less developed countries, where medical care is scarce, may benefit greatly from IoTSs that place a high priority on human vision. The proposed system in [28] proposes a hybrid IoT healthcare architecture that analyzes retinal images. By considering the retinal images, the proposed super-resolution (SR) work makes use of multi-kernel support vector regression (SVR) to improve the overall image quality that is recorded. This is done to better diagnose retinal diseases. By producing high-resolution retinal images, the hybrid architecture enables ophthalmologists to establish more accurate diagnoses more rapidly.

The healthcare industry has gained considerably from digital image processing technology, notably medical images and health-related information. This use may be noticeable when there is a requirement to send the information securely via communication channels such as the cloud for storage and/or processing reasons. Zigzag encryption of medical images is one of these advantages [29]. The proposed algorithm exceeds the competition and may be put to good use in diagnosing medical images [29][30].

References

1. Cui, F. Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment. Comput. Commun. 2020, 150, 818–827.
2. Abas, K.; Obraczka, K.; Miller, L. Solar-powered, wireless smart camera network: An IoT solution for outdoor video monitoring. Comput. Commun. 2018, 118, 217–233.
3. Punyavathi, G.; Neeladri, M.; Singh, M.K. Vehicle tracking and detection techniques using IoT. Mater. Today Proc. 2021, 51, 909–913.
4. Santhanakrishnan, C.; Annapurani, K.; Singh, R.; Krishnaveni, C. An IOT based system for monitoring environmental and physiological conditions. Mater. Today Proc. 2021, 46, 3832–3840.
5. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.; Baik, S.W. Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption. IEEE Trans. Ind. Inform. 2018, 14, 3679–3689.
6. Aydin, I.; Othman, N.A. A new IoT combined face detection of people by using computer vision for security application. In Proceedings of the 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 16–17 September 2017; pp. 1–6.
7. Patil, N.; Ambatkar, S.; Kakde, S. IoT based smart surveillance security system using raspberry Pi. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017; pp. 344–348.
8. Hossain, M.S.; Muhammad, G.; Rahman, S.M.M.; Abdul, W.; Alelaiwi, A.; Alamri, A. Toward end-to-end biomet rics-based security for IoT infrastructure. IEEE Wirel. Commun. 2016, 23, 44–51.
9. Dorothy, A.B.; Kumar, S.B.R.; Sharmila, J.J. IoT Based Home Security through Digital Image Processing Algorithms. In Proceedings of the 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, India, 2–4 February 2017; pp. 20–23.
10. Roy, S.; Rawat, U.; Sareen, H.A.; Nayak, S.K. IECA: An efficient IoT friendly image encryption technique using programmable cellular automata. J. Ambient. Intell. Humaniz. Comput. 2020, 11, 5083–5102.

11. Roy, S.; Shrivastava, M.; Pandey, C.V.; Nayak, S.K.; Rawat, U. IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata. Multimed. Tools Appl. 2021, 80, 31529–31567.
12. Su, J.; Vasconcellos, D.V.; Prasad, S.; Sgandurra, D.; Feng, Y.; Sakurai, K. Lightweight Classification of IoT Malware Based on Image Recognition. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; pp. 664–669.
13. Balla, P.B.; Jadhao, K.T. IoT Based Facial Recognition Security System. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; pp. 1–4.
14. Hassan, A.; Liu, F.; Wang, F.; Wang, Y. Secure image classification with deep neural networks for IoT applications. J. Ambient. Intell. Humaniz. Comput. 2021, 12, 8319–8337.
15. Wang, K.; Chen, C.-M.; Hossain, M.S.; Muhammad, G.; Kumar, S.; Kumari, S. Transfer reinforcement learning-based road object detection in next generation IoT domain. Comput. Netw. 2021, 193, 108078.
16. Sharmila, V.; Rejin Paul, N.R.; Ezhumalai, P.; Reetha, S.; Naresh Kumar, S. IOT enabled smart assistance system using face detection and recognition for visually challenged people. Mater. Today Proc. 2020.
17. Nag, A.; Nikhilendra, J.N.; Kalmath, M. IOT Based Door Access Control Using Face Recognition. In Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–3.
18. Li, X.; Li, J.; Yiu, S.; Gao, C.; Xiong, J. Privacy-preserving edge-assisted image retrieval and classification in IoT. Front. Comput. Sci. 2019, 13, 1136–1147.
19. Arunkumar, S.; Vairavasundaram, S.; Ravichandran, K.S.; Ravi, L. RIWT and QR factorization based hybrid robust image steganography using block selection algorithm for IoT devices. J. Intell. Fuzzy Syst. 2019, 36, 4265–4276.
20. Rukmani, P.; Teja, G.K.; Vinay, M.S. Industrial Monitoring Using Image Processing, IoT and Analyzing the Sensor Values Using Big Data. Procedia Comput. Sci. 2018, 133, 991–997.
21. Franco, J.D.; Ramirez-delReal, T.A.; Villanueva, D.; Gárate-García, A.; Armenta-Medina, D. Monitoring of Ocimum basilicum seeds growth with image processing and fuzzy logic techniques based on Cloudino-IoT and FIWARE platforms. Comput. Electron. Agric. 2020, 173, 105389.
22. Mahesh, N.; Baluprithviraj, K.N.; Anbarasu, L.; Balaji, B.; Saravana Kumar, U.; Sathish Kumar, S. Quality inspection system using IoT and image processing. Mater. Today: Proc. 2021.
23. Alletto, S.; Cucchiara, R.; Fiore, G.D.; Mainetti, L.; Mighali, V.; Patrono, L.; Serra, G. An Indoor Location-Aware System for an IoT-Based Smart Museum. IEEE Internet Things J. 2016, 3, 244–253.
24. Kitpo, N.; Inoue, M. Early Rice Disease Detection and Position Mapping System using Drone and IoT Architecture. In Proceedings of the 2018 12th South East Asian Technical University Consortium (SEATUC), Yogyakarta, Indonesia, 12–13 March 2018; pp. 1–5.
25. Sharma, A.; Singh, P.K.; Kumar, Y. An integrated fire detection system using IoT and image processing technique for smart cities. Sustain. Cities Soc. 2020, 61, 102332.
26. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. IEEE Access 2018, 6, 20596–20608.
27. Rajagopalan, S.; Janakiraman, S.; Rengarajan, A.; Rethinam, S.; Arumugham, S.; Saravanan, G. IoT Framework for Secure Medical Image Transmission. In Proceedings of the 2018 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 4–6 January 2018; pp. 1–5.
28. Jebadurai, J.; Dinesh Peter, J. Super-resolution of retinal images using multi-kernel SVR for IoT healthcare applications. Future Gener. Comput. Syst. 2018, 83, 338–346.
29. Deepika, J.; Rajan, C.; Senthil, T. Security and Privacy of Cloud- and IoT-Based Medical Image Diagnosis Using Fuzzy Convolutional Neural Network. Comput. Intell. Neurosci. 2021, 2021, 6615411.
30. Anandkumar, R.; Dinesh, K.; Obaid, A.J.; Malik, P.; Sharma, R.; Dumka, A.; Singh, R.; Khatak, S. Securing e-Health application of cloud computing using hyperchaotic image encryption framework. Comput. Electr. Eng. 2022, 100, 107860.