applied sciences

Review

A Review: Image Processing Techniques' Roles towards Energy-Efficient and Secure IoT

Abbas M. Al-Ghaili [1,2,3,*], Hairoladenan Kasim [2], Zainuddin Hassan [2], Naif Mohammed Al-Hada [4,5,6,*], Marini Othman [7], Rafiziana Md. Kasmani [5] and Ibraheem Shayea [6,*]

[1] Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Kajang 43000, Selangor, Malaysia
[2] Department of Informatics, College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), Kajang 43000, Selangor, Malaysia
[3] Department of Computing, College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), Kajang 43000, Selangor, Malaysia
[4] Shandong Key Laboratory of Biophysics, Institute of Biophysics, Dezhou University, Dezhou 253023, China
[5] School of Chemical and Energy Engineering, Universiti Teknologi Malaysia, Skudai 81310, Johor Bahru, Malaysia
[6] Electronics and Communication Engineering Department, Faculty of Electrical and Electronics Engineering, Istanbul Technical University, 34467 Sarıyer, Turkey
[7] Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Negeri Sembilan, Malaysia
* Correspondence: abbas@uniten.edu.my (A.M.A.-G.); naifalhada@yahoo.com (N.M.A.-H.); ibr.shayea@gmail.com (I.S.)

Abstract: The goal of this review paper is to highlight the image processing techniques' role in the Internet of Things (IoT), aiming to attain an energy-efficient and secure IoT. 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. Several researchers have made efforts to improve future IoTSs, which are summarized in this article. Day-by-day, proposed methods are developed, and thus IoT deployment has been plainly engaged in our everyday activities. Several efficient image-processing techniques that can be utilized by IoTSs to overcome such issues have been proposed. This review paper aims to highlight those proposed methods that can make contributions in this direction. Thus, this study aims to review numerous research studies on this subject. This study looks at 36 publications relevant to image-processing techniques utilized by several types of IoTSs. The innovative work of this review paper is to provide readers with a map of suitable image processing techniques to be used with certain types of IoT systems (i.e., scenarios). Both methodology and analysis have come out with a suggested mind map highlighting a number of proposed solutions (i.e., image processing techniques) that can be suitable to help design an energy-efficient, secure, and intelligent IoT system. We have made some conclusions and projections for future research work.

Keywords: image processing; energy consumption; IoT systems; location detection; IoT healthcare systems; object detection; IoT monitoring systems; IoT security applications; intelligent IoT

check for updates

Citation: Al-Ghaili, A.M.; Kasim, H.; Hassan, Z.; Al-Hada, N.M.; Othman, M.; Kasmani, R.M.; Shayea, I. A Review: Image Processing Techniques' Roles towards Energy-Efficient and Secure IoT. *Appl. Sci.* **2023**, *13*, 2098. https://doi.org/10.3390/app13042098

Academic Editor: Yoshiyasu Takefuji

Received: 2 September 2022
Revised: 20 November 2022
Accepted: 24 November 2022
Published: 6 February 2023

1. Introduction

Digital images are considered one of the essential elements of Internet of Things (IoT)-dependent systems (IoTSs) [1–8]. Digital image processing with the aid of a number of other technologies, IoT is an example of these technologies, may add greatly to our life's activities and occurrences [6,9,10]. IoT technology can be found in practically every part of our daily lives, from our automobiles to our homes. The IoT might prevent fires, identify and track goods, control and report changes happening in the environment, and capture images in our homes, roadways, and workplaces utilizing IoT apps, to mention just a few of the many helpful aspects they give [11]. Intelligent sensors in self-driving cars may be used to monitor and forecast traffic patterns and to classify objects based on images captured. One of the most promising areas for IoT is image classification using deep neural networks (DNNs) on the cloud. Despite this, the widespread use of "smart" IoT devices and applications may raise questions about their security. Security and encryption of data, feature extraction, and image categorization remain significant challenges to overcome for IoT devices [11].

The effective deployment of services connected to the IoT has expanded at a rapid rate thanks to the assistance of many different fields [12,13]. One of these is digital image processing [14,15]. Image processing, for instance, has been one factor that has led to improvements in IoT application services [16,17]. Images are becoming more and more widely used as a result of the particular qualities and characteristics that they possess [16,18]. Images have been utilized as a tool by IoTSs in order to carry out a wide variety of jobs and duties. For instance, to monitor a location or zone that is quite a distance away, images have been acquired by sensors [19,20]. The field of image processing has been exploited by certain IoTSs in order to determine whether objects are stationary or in motion. On the basis of the item that was recognized, a decision might thereafter be made that is suitable to the characteristics of the IoTS.

However, there are a number of challenges in this regard. The protection of digital assets like images is one of the many difficulties that need to be thoroughly investigated and examined. Based on IoTSs and the goal of the usage, the information that is contained in images may have a high level of sensitivity. As a result, finding and exploiting a large number of attacks will be a primary focus. The number of exploitable flaws is expected to increase as a result of the never-ending and limitless efforts of attackers as well as unique threats and activities. As a result of this, the contents of images and information have been put in jeopardy by IoTSs, and they have also been exposed to a serious risk [21,22].

1.1. Image Processing's Role in the Development of IoT Platforms and Systems

With the support of many areas, the successful implementation of IoT-related services has grown rapidly [23]. Digital image processing is one of these areas [24]. For example, image processing has contributed to the improvement of IoT application services [25,26]. Day-by-day, images have been significantly employed owing to their specific traits and properties. IoTSs have used images as a tool to execute a variety of tasks and functions. Images have been recorded by sensors in order to, for example, monitor a faraway site or zone. Some additional IoTSs have utilized the image processing field to identify static or moving objects. Based on the identified item, a choice might be subsequently taken appropriately to the nature of the IoTS. A step beyond object detection is object recognition, which is helpful for a variety of tasks, including text recognition based on color, texture, and form attributes [27]. Object identification technique has been leveraged additionally by a variety of IoTSs to perform, for example, remote guiding and support to visually-challenged people after things have been detected without the need for a physical supporter. Objects in front of the intended individual are collected by a visual sensor and transferred to a cloud or other distant processing unit for decision-making. Another possibility is that, in case the visually-challenged individual has met unsafe things, the remote assistance center will be alerted where recognized objects would be transported through IoT platforms.

Image processing and the IoT have been integrated to improve our quality of life and a wide range of industries, including healthcare, manufacturing, technology, home security, and entertainment, among others [28,29].

1.2. The Problem of Excessive Energy Use

As discussed earlier, IoTSs deliver digital contents where some of these contain a great quantity of data size, notably a series of images, e.g., videos. As a result, IoT devices must be capable of high-performance processing to handle such massive amounts of data [30]. On the other hand, the time required to deliver such a large quantity of data is considerable. Highly used energy presumably may be caused by these two reasons. Because of this, IoTSs that utilize non-friendly energy are being used. In an effort to address this problem, a number of techniques have been proposed.

This article has looked at a few of the options available. Proposed techniques could contribute to sustainable development objectives for the energy sector and IoT environment. We evaluate a number of IoTSs that rely on the images' transmission between the source, cloud, and destination with optimal performance of energy spent by IoTS. Energy sustainability in the IoT is the goal of this study, which tries to identify many energy-efficient IoTSs.

1.3. A Concern with IoT Security in a Connected World

One of the challenges that has to be fully considered is the security of digital assets, such as images. Images-embedded information may be of high sensitivity depending on the IoTSs and purpose of usage [31]. Hence, plenty of vulnerabilities will be objectives and sought for. The number of vulnerabilities will be of rise owing to endless and infinite efforts of attackers and novel threats and acts. In accordance with this, IoTSs have jeopardized image contents and conveyed information to a genuine hazard. In certain scenarios, this danger may be actual harm to sensitive regions or zones after contents have been illegally updated since such a modification activity might modify the choice made by the remote processing center. Assuming an abnormal event has occurred in a monitored industrial zone, and a taken image has been studied where the detected and identified source-dangerous item is present, and the image has been illegally edited while it was delivered, real harm may then be created. Therefore, there is a huge demand for IoTSs to function in a safe environment [32,33]. That might incorporate communication channels, layers networks, and fog nodes to retain processed and transferred images secure and private as well as to meet security goals for the IoT platform [34]. This article has tried to analyze a variety of potential methods that contribute to the security of IoT-related content and to a safe IoT ecosystem.

1.4. Contributions and Article Organization

1.4.1. Contributions

This article has addressed a variety of contributions, which can be summed up as follows:

(1) It examines a variety of publications and research studies that discuss the designing and building of IoT applications and systems that make use of image-processing techniques. These papers and studies involve the topic of designing and building IoT applications and systems;

(2) It highlights a variety of contributions made by image processing techniques towards other concerns that IoT applications typically face and find difficult to overcome, such as the energy consumption made by IoT systems and the security of IoT data. These issues include: (1) The energy consumption made by IoT systems; and (2) The security of IoT data;

(3) It highlights several different types of IoT applications that depend on image processing techniques, such as image processing-based IoT monitoring applications, image processing-based IoT security applications, image processing-based IoT location detection applications, IoT safety applications, and IoT healthcare applications;

(4) The process of object detection is extremely important and significant since it has an impact on the decision that is made. There won't be much of a focus on it if there isn't an accurate edge detection mechanism, though, because so many reviewed publications have used it to finish the jobs they needed to. This article highlights and reviews a number of IoT applications that rely on the object detection process, which is considered crucial to perform such IoT-related tasks as monitoring, classification, and recognition. The applications are discussed in detail in this article;

(5) It uses the PRISMA 2020 method for systematic reviews in order to emphasize precise steps on the extraction technique of the publications and how that strategy has been performed for various cascade-step phases;

(6) It analyzes the reviewed articles according to various criteria;
(7) It discusses a number of important aspects that made it possible for image processing to act as a connection between us and an intelligent and safe IoT environment;
(8) It suggests a mind map highlighting the most important IoT systems-related issues/concerns and their solutions utilizing image processing techniques; to contribute to future research for potential improvements in this regard;
(9) It provides the readers with a number of significant future trends that need to be taken into consideration by potentially interested researchers and designers.

1.4.2. Article's Organization

This article is organized as follows: Section 2 addresses the topics of the existing reviews. The method applied in this review paper has been presented in Section 3. Then, reviewed articles have been presented in Section 4. In Section 5, the analysis part has been provided. The discussion and future trends have been provided in Section 6. In Section 7, a suggested mind map highlighting the scenario and its corresponding solution has been provided. Future trends have been discussed and listed in Section 8. The conclusion has been drawn in Section 9.

2. Existing Reviews

In order to assist readers in distinguishing between the scopes of the existing studies and the scope of this review paper, this paper has provided a concise summary of the issues and subjects raised in the currently published review papers. The first sub-section outlines the subjects and concerns of current evaluations. Research questions have been emphasized in the second sub-section.

2.1. Current Review Articles

A number of existing reviews regarding the topic of this review have been found in the literature, for example, [35–40]. A few major concerns and areas of the current review articles are represented in Table 1.

Table 1. Existing reviews' concerns and areas. Numbers between brackets represent the cited related review articles.

Ref.	Existing Reviews' Concerns	Existing Reviews' Areas
[35]	Deep learning applications for IoT	IoT healthcare
[36]	Techniques related to IoT healthcare	IoT healthcare and e-health
[37]	Industrial solutions applied to developments of IoT technologies	Smart objects integrating IoT
[38]	Multimedia Internet of Things (M-IoT) applications related to road traffic management, security, industry, and health	M-IoT
[39]	Machine learning methods and algorithms assigned to Healthcare Internet of Things (H-IoT)	H-IoT
[40]	Machine learning algorithms for IoT devices	Image classification for IoT in the healthcare sector

This review focuses on IoT, image processing, artificial intelligence, and computer vision applied for the purpose of object detection and recognition to implement a number of related tasks such as monitoring, human and device safety, content security, location detection, and healthcare applications in the era of the IoT. Besides, its field can cover image processing techniques applied for IoTSs to perform security related to internet-based digital contents, monitoring of certain objects, remotely-detected locations, health care management, and a few others. Other related concerns are health care-, medical-, monitoring, safety, and security-related IoTSs for multiple elements in our environment, such as humans, products, and a few others.

2.2. Research Questions

This article aims to answer the following two questions:

RQ1. Can image processing techniques help design energy-efficient and secure IoT systems?

RQ2. What are the most suitable image processing techniques applied to help design such an energy-efficient and secure IoT system?

This review article provides a discussion of the literature followed by an analysis related to these questions. Besides, a suggested map has been highlighted, mentioning a number of proposed solutions (i.e., image processing techniques) that can be suitable to help design an energy-efficient and secure IoT system.

3. Methodology

This section illustrates the major technique employed in the selection process of the extracted papers. The "PRISMA 2020" technique for systematic reviews has been used. Its implemented procedure is shown in Figure 1. The methodology will be presented in three sub-sections. In the first section, the extraction process and filtration phases are explained. Keywords used to extract papers from various DLs will be highlighted. The second section highlights the inclusion and exclusion criteria applied. The third section views the distribution of extracted papers according to digital libraries (DLs).

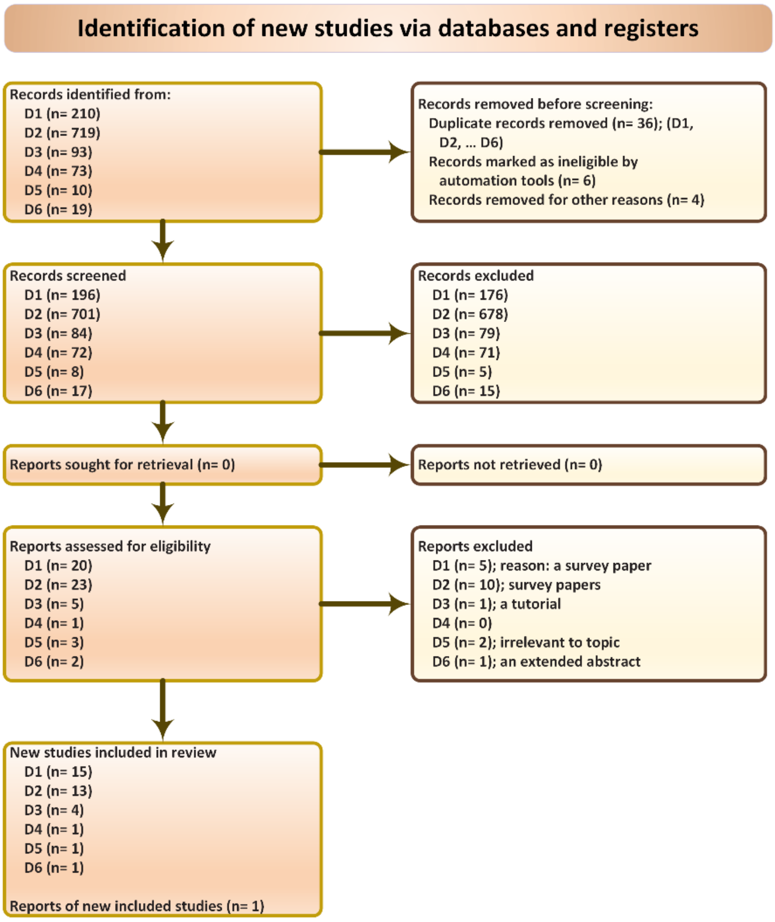
Identification of new studies via databases and registers
Records identified from:
D1 (n= 210)
D2 (n= 719)
D3 (n= 93)
D4 (n= 73)
D5 (n= 10)
D6 (n= 19)
Records removed before screening:
Duplicate records removed (n= 36); (D1, D2, … D6)
Records marked as ineligible by automation tools (n= 6)
Records removed for other reasons (n= 4)
Records screened
D1 (n= 196)
D2 (n= 701)
D3 (n= 84)
D4 (n= 72)
D5 (n= 8)
D6 (n= 17)
Records excluded
D1 (n= 176)
D2 (n= 678)
D3 (n= 79)
D4 (n= 71)
D5 (n= 5)
D6 (n= 15)
Reports sought for retrieval (n= 0)
Reports not retrieved (n= 0)
Reports assessed for eligibility
D1 (n= 20)
D2 (n= 23)
D3 (n= 5)
D4 (n= 1)
D5 (n= 3)
D6 (n= 2)
Reports excluded
D1 (n= 5); reason: a survey paper
D2 (n= 10); survey papers
D3 (n= 1); a tutorial
D4 (n= 0)
D5 (n= 2); irrelevant to topic
D6 (n= 1); an extended abstract
New studies included in review
D1 (n= 15)
D2 (n= 13)
D3 (n= 4)
D4 (n= 1)
D5 (n= 1)
D6 (n= 1)
Reports of new included studies (n= 1)

Figure 1. PRISMA 2020 strategy applied. In this figure, D1 = IEEE Xplore, D2 = ScienceDirect, D3 = SpringerLink, D4 = IOS Press, D5 = MDPI, and D6 = Hindawi.

3.1. Extraction Process and Filtration Phases

Further steps and procedures applied to extract, and select papers from the literature review will be mentioned as follows:

3.1.1. Phase 1

The search is conducted over six digital libraries. During this phase, the following terms have been used as keywords: "image processing" OR "Internet of things" OR "image processing for IoT security" OR "image processing for energy IoT" OR "IoT monitoring applications" OR "Energy consumption with an IoT" OR "IoT healthcare systems" OR "IoT monitoring systems" OR "IoT security applications" OR "Location detection in IoT" OR "IoT systems."

In addition, each extracted paper will initially be examined, and if the scope and keywords of that paper are similar to those listed above, then the paper is taken. This phase produced 1124 papers.

3.1.2. Phase 2

It took into account the possibility of similarity in the findings, and as a consequence, it implemented a procedure for the elimination of duplicated papers. Either it has been discovered that there is a resemblance in titles, or it is regarded to be duplicated documents, in which case it will be deleted. This phase produced a total of 1078 papers.

3.1.3. Phase 3

In this phase, another criterion for filtering has been applied, and it is a combination of previously specified conditions. These conditions include a newspaper, demonstration, poster, expanded abstract, and survey paper. Following the application of these exclusion criteria, the total number of papers that were acquired was equal to 36.

3.2. Inclusion and Exclusion Criteria Strategy

This review article has selected a number of top indexing services. Furthermore, six publishers have been considered, including IEEE, Elsevier, and MDPI. Additional criteria which were considered are listed in Table 2.

Table 2. A list of collection criteria.

Indexing Service	**Scopus OR WOS**
Database names	IEEE Xplore, ScienceDirect, MDPI, SpringerLink, IOS Press, and Hindawi
Search period	25 February 2022 to 10 March 2022
Paper publishing date	2016 to 2021
Type of papers collected	Conference proceedings & Journals
Scope of a candidate paper	IoT systems, Image processing for IoT applications, IoT healthcare, IoT security applications, and IoT monitoring systems utilizing image processing
Image processing related	Image processing techniques considering edge detection, object recognition, video surveillance
IoT systems related	IoT Applications such as healthcare, security, and energy-efficient systems.
IoT and image processing techniques related	IoT systems using image processing techniques such as smart alert, phenomena detection, e.g., fire detection, hazard objects detection
Paper selection	*NOT* a newspaper, demonstration, poster, or extended abstract.

3.3. Distribution of Extracted Papers According to Digital Libraries (DLs)

A limited selection of publishers that have been embraced is profiled in this review study. In addition, a set of indexing services for relevant journals is highlighted, to which the manuscript's peer-reviewed publications all belong. The distribution of papers according to DLs from which papers are retrieved has been illustrated in Figure 2.

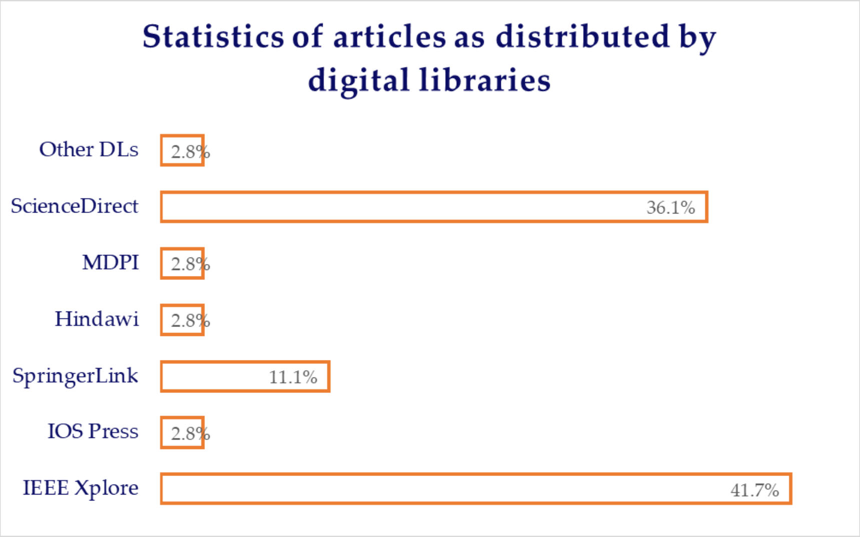

Figure 2. Statistics of articles as distributed by digital libraries (DLs).

4. Literature Review

Different goals required to be processed by IoTSs with the use of image processing techniques might lead to developing a range of classes to which those applications belong. Using image processing techniques, the IoT has been able to take on intelligent and difficult tasks such as remote monitoring, security, healthcare, and UAV. In this study, these aforesaid tasks will be emphasized, and their connected applications from the literature will be explored.

4.1. 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 [41]. 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 [42,43]. According to [42], 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 [43], 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 3.

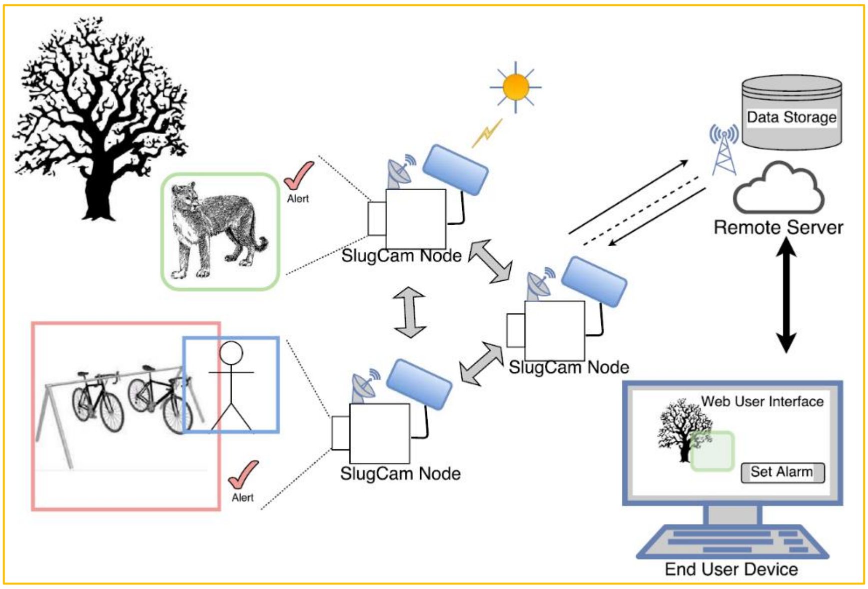

Figure 3. IoT monitoring applications based on image processing—Web-based video server and the Web-based user interface [42].

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 [44], 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 [45] 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 [46,47].

4.2. 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 4.

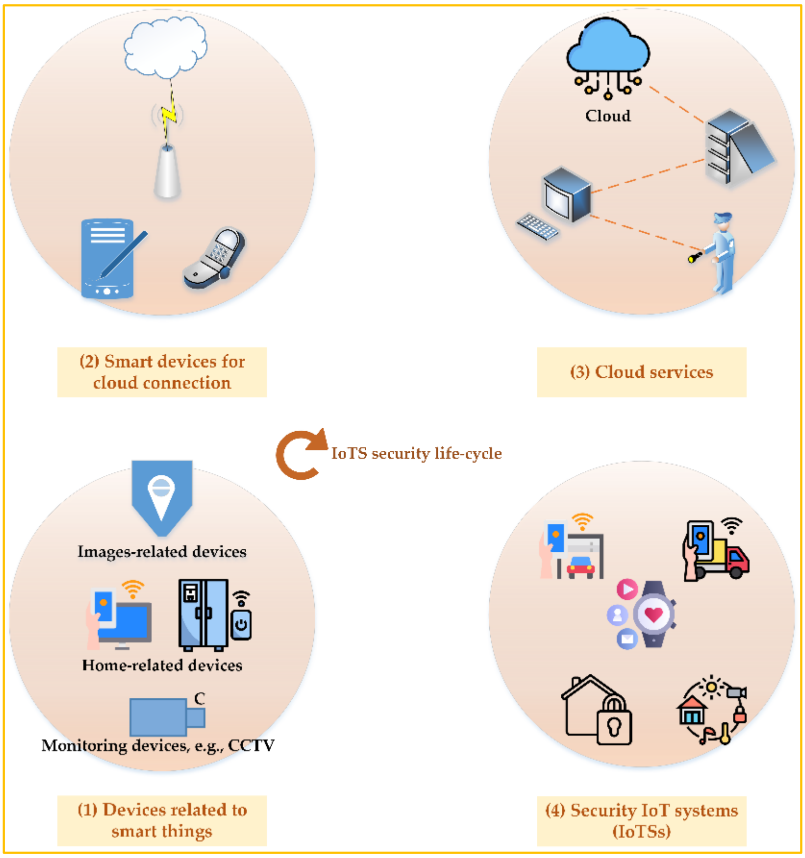
Cloud
(2) Smart devices for cloud connection
(3) Cloud services
IoTS security life-cycle
Images-related devices
Home-related devices
C
Monitoring devices, e.g., CCTV
(1) Devices related to smart things
(4) Security IoT systems (IoTSs)

Figure 4. 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 [48], 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 [29]. 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 [49].

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 [50]. 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 [51].

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 [52].

The research presented in [11] 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 [11] 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.

4.3. 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 [53].

The use of face recognition in an OCR-based smart support system is one such example [54]. 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 [55].

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 [56]. An illustration related to IoT safety applications based on image processing is shown in Figure 5.

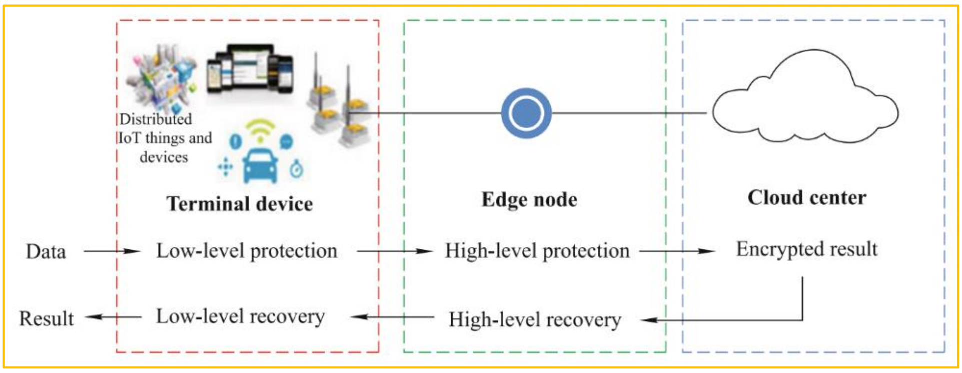

Figure 5. IoT safety applications based on image processing: privacy-preserving outsourced computing architecture [56].

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 [57]. 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 [58], the agricultural industry's plant growth surveillance for improved safety in such a process [59], or the detection of a disease location on plants [60].

4.4. 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 [61], 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 [61] is shown in Figure 6.

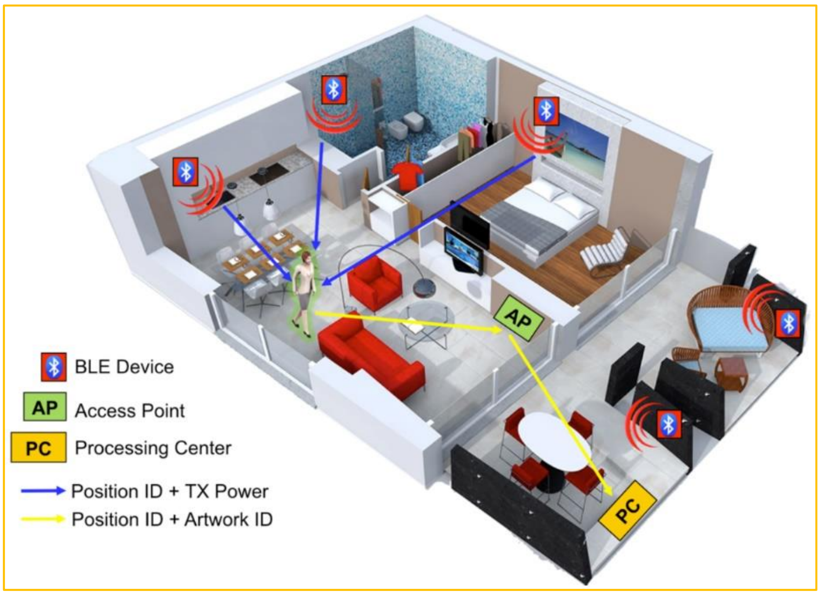

Figure 6. IoT location detection applications based on image processing: localization mechanism elements proposed by [61].

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 [62]. 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].

4.5. IoT Healthcare Applications Based on Image Processing

Medical images used for IoT healthcare are many. One example is described in [63]. 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 [64], 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 7.

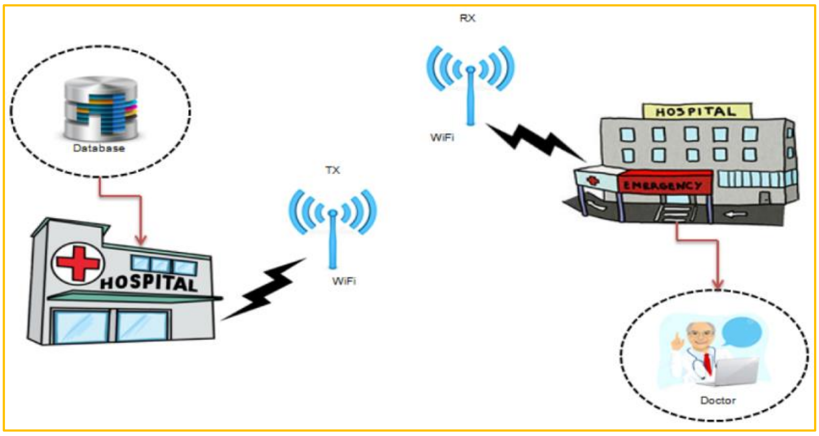

Figure 7. IoT healthcare applications based on image processing: a graphical representation of medical data communication proposed by [64].

Another example may be discussed in [65]. 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 [65] 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 [66]. The proposed algorithm exceeds the competition and may be put to good use in diagnosing medical images [66,67].

5. Analysis

There are three types of analysis. The first one is the analysis of papers according to the type of IoT application. The second is the analysis of papers according to IoT applications according to the date of publishing. The third one will be the analysis of papers according to IoT application vs. the utilized image processing technique in order to find out what the suitable image processing techniques for IoT applications are.

5.1. Distribution of Papers According to the Type of IoT Application

In this type of analysis, the papers are classified into groups based on the type of IoT applications in which image-processing techniques are exploited. According to the reviewed literature, there are five types of IoT applications. In Figure 8, the distribution of papers according to the IoT application type is shown.

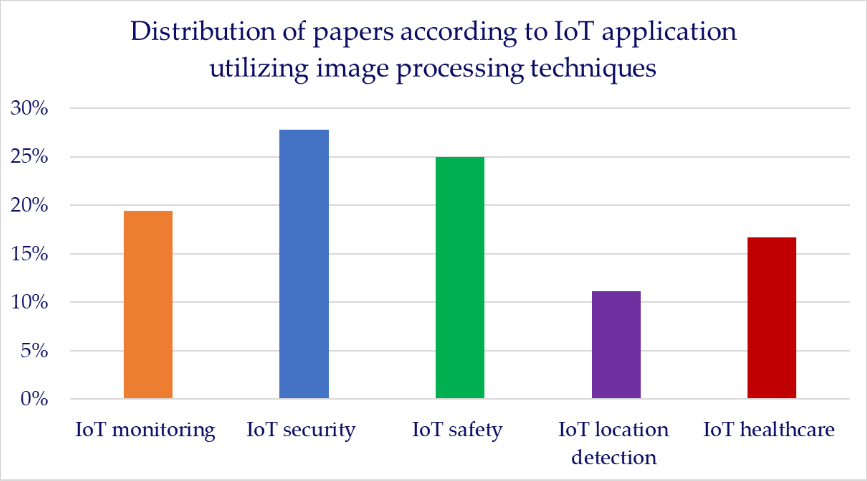

Figure 8. Distribution of reviewed papers according to the type of IoT application.

It is shown in Figure 8 that the most frequently applied image processing techniques can occur with the IoT security applications with a percentage of about 28% amongst other IoT applications, including IoT safety applications that ranked second and have 25% of the frequency.

5.2. Distribution of Papers According to IoT Application According to the Data of Publishing

This analysis is going to show the distribution of papers according to the IoT application. Distribution(s) of analyzed papers related to IoT monitoring, security, safety, location detection, and healthcare applications according to publishing year(s) are shown in Figure 9.

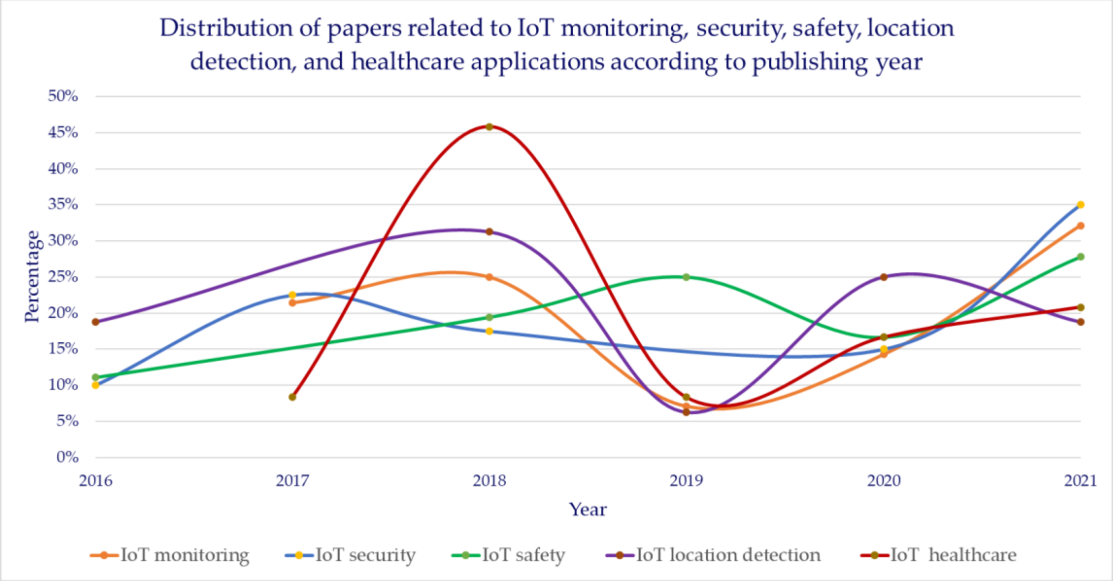

Figure 9. Distribution of reviewed papers related to various types of IoT applications according to publishing year.

5.3. Distribution of Papers According to IoT Application vs. the Utilized Image Processing Technique

In this type of analysis, the distribution of papers according to IoT applications utilizing specific kinds of image-processing techniques will be the focus: meaning what types of image-processing techniques are applied by each type of IoT application. This indicates the suitability of image processing techniques for certain scenarios. The distribution(s) of reviewed papers according to IoT monitoring, security, safety, location detection and healthcare applications vs. applied image processing technique(s) are shown in Figures 10–14, respectively.

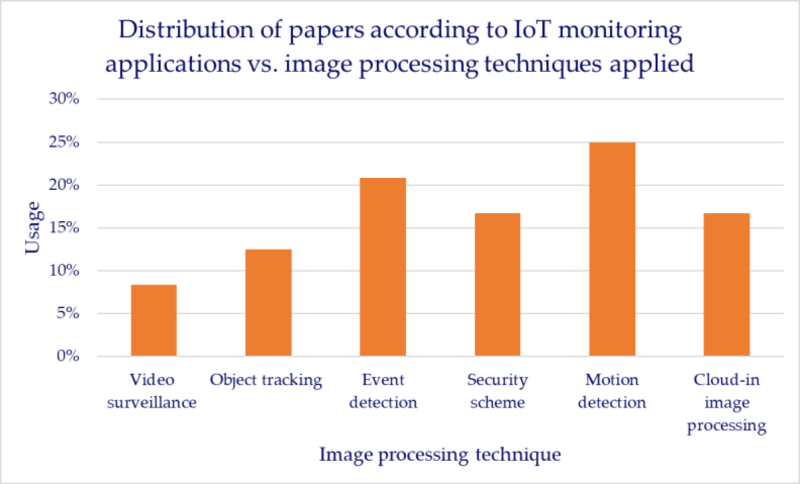

Figure 10. Distribution of papers according to IoT monitoring application vs. applied image processing technique(s).

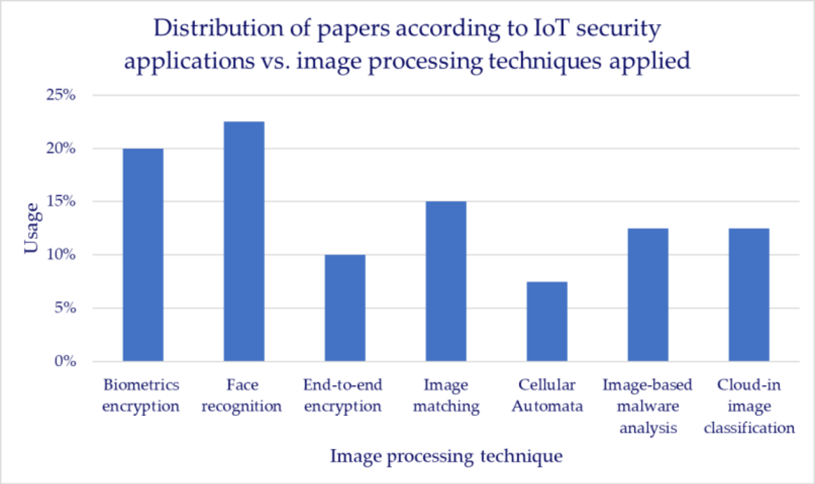

Figure 11. Distribution of papers according to IoT security application vs. applied image processing technique(s).

It is shown in Figures 10–14 that there is a varied set of image processing techniques utilized by those corresponding IoT applications depending on the needs of the IoT application's purpose. For example, in Figure 10, "motion detection" has been utilized by the "monitoring IoT applications" with a percentage of 25% amongst other applications. Another example is that, in Figure 11, the "face recognition" technique has been used in order to do a security purpose for such an IoT application. The use of this technique has been present in more than 20% of the analyzed papers that consider the security of IoT applications.

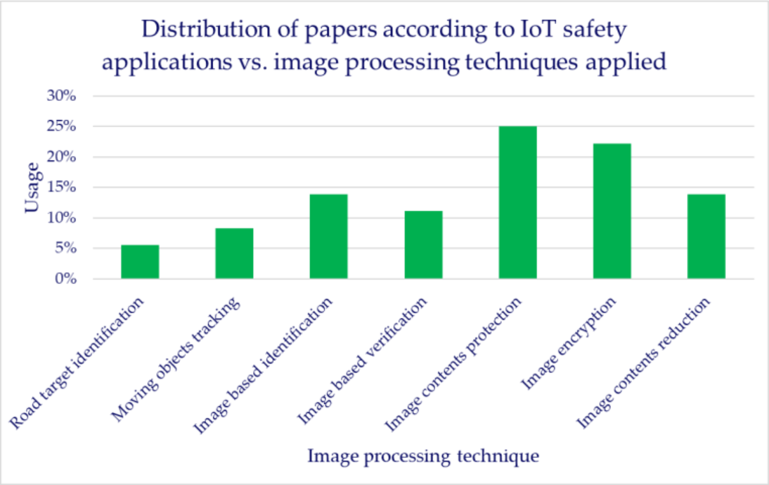

Figure 12. Distribution of papers according to IoT safety application vs. applied image processing technique(s).

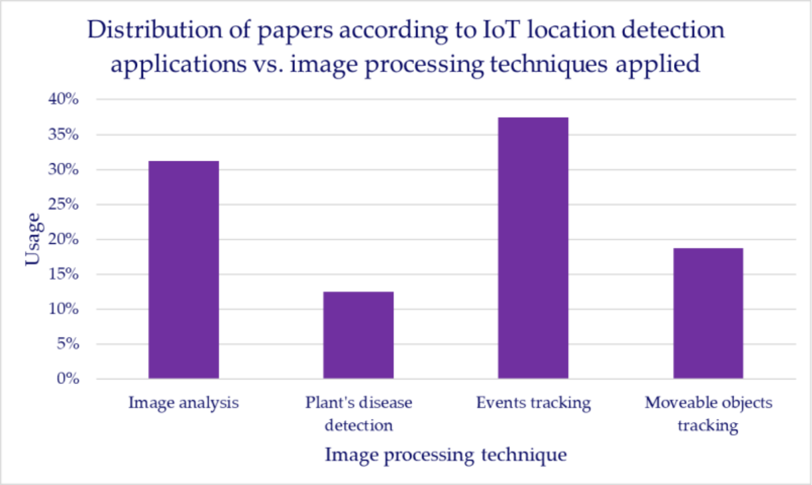

Figure 13. Distribution of papers according to IoT location detection application vs. applied image processing technique(s).

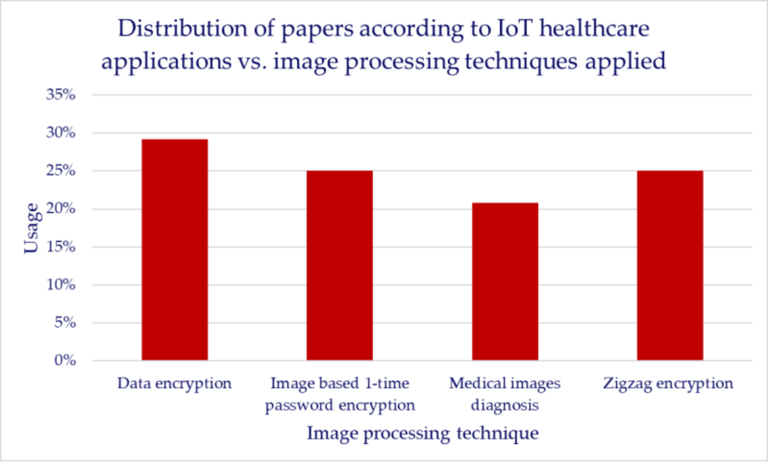

Figure 14. Distribution of papers according to IoT healthcare application vs. applied image processing technique(s).

6. Discussion

The goal of using image processing techniques exploited by IoTSs is to have such feasibility of contributing to generating energy-efficient and secure IoTSs. Hence, there are two major considerations which are: (1) the purpose of using image processing techniques exploited by IoTSs, (2) the possibility that image processing techniques could contribute to the production of IoT applications and systems that are more energy-efficient and secure. It is important to note that IoTSs have been applying image-processing techniques to use to accomplish a wide range of goals.

Image processing techniques, particularly those that have the potential to increase the amount of energy that is used by IoTSs, need to be investigated. Using image processing to help reduce power consumption and ensure data security will be covered in this section.

6.1. Image Processing Techniques' Roles to Address Energy Consumption for IoTSs

In relation to this, there are several examples that demonstrate successful implementations of associated image-processing algorithms with several IoTSs. These examples show that the energy consumption rates of these IoTSs are superior to those of other applications, resulting in greater energy savings. There are several instances examined in this article that proved that image processing techniques had helped design IoTSs that utilize less energy and more security. When it comes to information processing, volume and energy use are closely related. Therefore, the cost of storing in the cloud will impact energy use. The following are some of the roles that image processing techniques have had in enhancing and decreasing the rate of energy consumption produced by IoTSs:

1. Images will be uploaded to the cloud if they include information that is useful. That minimizes energy use by reducing transmission time spent [45];
2. Because of advancements in image processing, transmission times have become significantly shorter. If all of the obtained multi-frame images are transmitted, it will be significantly less time than that;
3. With the aid of image processing, a mathematical model for the intensity of compressed pixels such as CA has been developed, enabling the development of energy-efficient IoTSs that may minimize energy usage [45,49];
4. Lightweight security measures may be applied before images are sent to the IoT cloud via image processing [57]. As a direct result of this, a significant amount of processing time and available computer resources will be preserved. Thus, achieving long-term energy security is a goal.

6.2. Image Processing Techniques' Roles to Address Security for IoTSs

6.2.1. Security of Networks

1. Image processing has proposed various methods [32,68,69] to address concerns about the safety of the communication channel that runs between the image processing and the final destination. It is said that image processing techniques have a role in strengthening the security of communication channels [68].
2. The technique of matching images [29,55] has been used in cloud-stored images, where it has been shown to be effective in maintaining the confidentiality of data storage and communication networks. It has helped to ensure the security and confidentiality of the image that was retrieved from its storage in the cloud. As a result of the matching procedure, communications have been made more secure [29].
3. Numerous IoTSs have established a connection between image encryption, image transfer, and cloud storage [67,70]. There has been an increase in the level of security provided to the proposed communication channels [50].

6.2.2. Security of Contents

Image processing techniques have greatly improved the security of contents and channels required for transmission. Image processing techniques have contributed to the development of a variety of security procedures for IoTSs, which we examine.

1. Zigzag image encryption may be more resistant to data attacks [66];
2. As a result of advancements in image processing, IoT devices and networks are now able to transmit data safely. The current conventional security scheme, in particular the two-step authentication, has been proposed to be replaced by a biometric encryption scheme that uses image processing [48];
3. IoTSs stored on a server and hence subject to attack at the server level benefit from image block splitting as a security measure. Increased security and decreased attack likelihood are two benefits of block-based image encryption schemes [68];
4. Encryption of images may improve the safety of the contents of images. However, improvements to this method are currently being made to enhance the functionality of privacy protection for contents of images connected to IoTSs [50];
5. The matching procedure helps to increase the safety of image data associated with the IoT [29].

7. A Suggested Mind Map

In this section, a mind map mentioning and highlighting the suitable image processing techniques applied by such an IoT application will be suggested and graphically represented. For each IoT application (i.e., scenario), there will be a number of image processing technique(s) that might be applied and can produce a high level of energy-efficient and secure IoT system/application. Shown in Figure 15 is the suggested mind map.

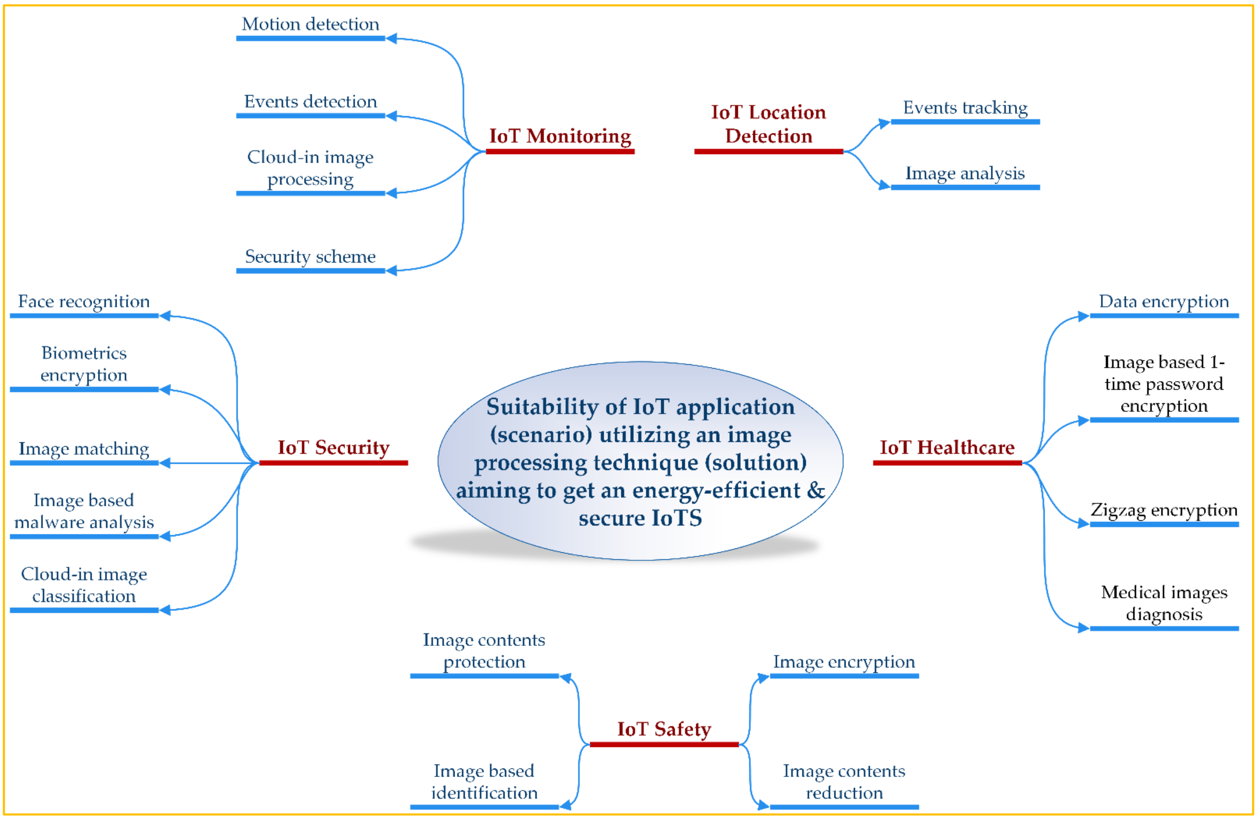
Motion detection
Events detection
Cloud-in image processing
Security scheme
IoT Monitoring
IoT Location Detection
Events tracking
Image analysis
Face recognition
Biometrics encryption
Image matching
Image based malware analysis
Cloud-in image classification
IoT Security
Suitability of IoT application (scenario) utilizing an image processing technique (solution) aiming to get an energy-efficient & secure IoTS
IoT Healthcare
Data encryption
Image based 1-time password encryption
Zigzag encryption
Medical images diagnosis
Image contents protection
Image based identification
IoT Safety
Image encryption
Image contents reduction

Figure 15. A suggested mind map highlighting the concern, which is the scenario (IoT application marked in a red-colored font) and the corresponding and most suitable solution (image processing technique marked in a blue-colored font) for such a concern. Starting from the scenario, applying a solution, aiming to attain an energy-efficient and secure IoTS.

In Figure 15, a number of solutions (image processing techniques) are proposed to enhance the scenario (IoT application) by increasing the security and reducing the energy consumption by such an IoTS. To read and understand this figure, suppose that an IoT system is needed to be proposed for the purpose of security where images are a core element in this system; it is suitable to apply face recognition, biometrics encryption, or image matching for the purpose of verification, depending on the nature of the application and the necessity of that IoT system/application. One important thing to consider in this supposed scenario is that it is a must to reach a high level of energy-use reduction and security. This could lead to contribute to interested researchers getting benefits for designing and establishing such a potential IoTS.

Figure 15 also shows that there can be a use of more than an "image processing technique" with two different "IoT scenarios." For example, in monitoring IoT applications, Cloud-in image processing can be used, while this technique can also be used with some other IoT applications, such as IoT security applications. Similarly, IoT security and monitoring applications can use, for example, biometrics and face recognition for almost the same purpose, which is the increase of protection of digital content. In addition, images can be analyzed using two IoT applications which are IoT security and location detection applications. In some other scenarios (i.e., IoT applications), there might be a difference in using such a solution (image processing technique).

There are, however, commonalities between these techniques utilizing solutions, where they can be structured as briefly highlighted in Table 3.

Table 3. Commonalities between solutions and scenarios.

		IoT System or Application (Scenario)				
		Monitoring	**Security**	**Safety**	**Location Detection**	**Healthcare**
Image processing technique (Solution)	Motion detection	×				
	Events detection & tracking	×			×	
	Cloud image processing & analysis	×	×			
	Security scheme	×	×			
	Face recognition	×	×	×		
	Biometrics encryption	×				
	Image matching	×				
	Image analysis	×			×	
	Image contents protection			×		
	Image-based identification			×		
	Image content reduction					
	Image encryption	×		×		×
	Medical image diagnosis					×

In Table 3, it is shown that there might be an occurrence of commonalities between more than a single scenario (IoT system/application) to utilize one solution (image processing technique), such as with "image encryption" or "image analysis." That depends on the nature of the design of the IoT system. For more clarification, shown in Figure 16 is a graphical representation highlighting these commonalities.

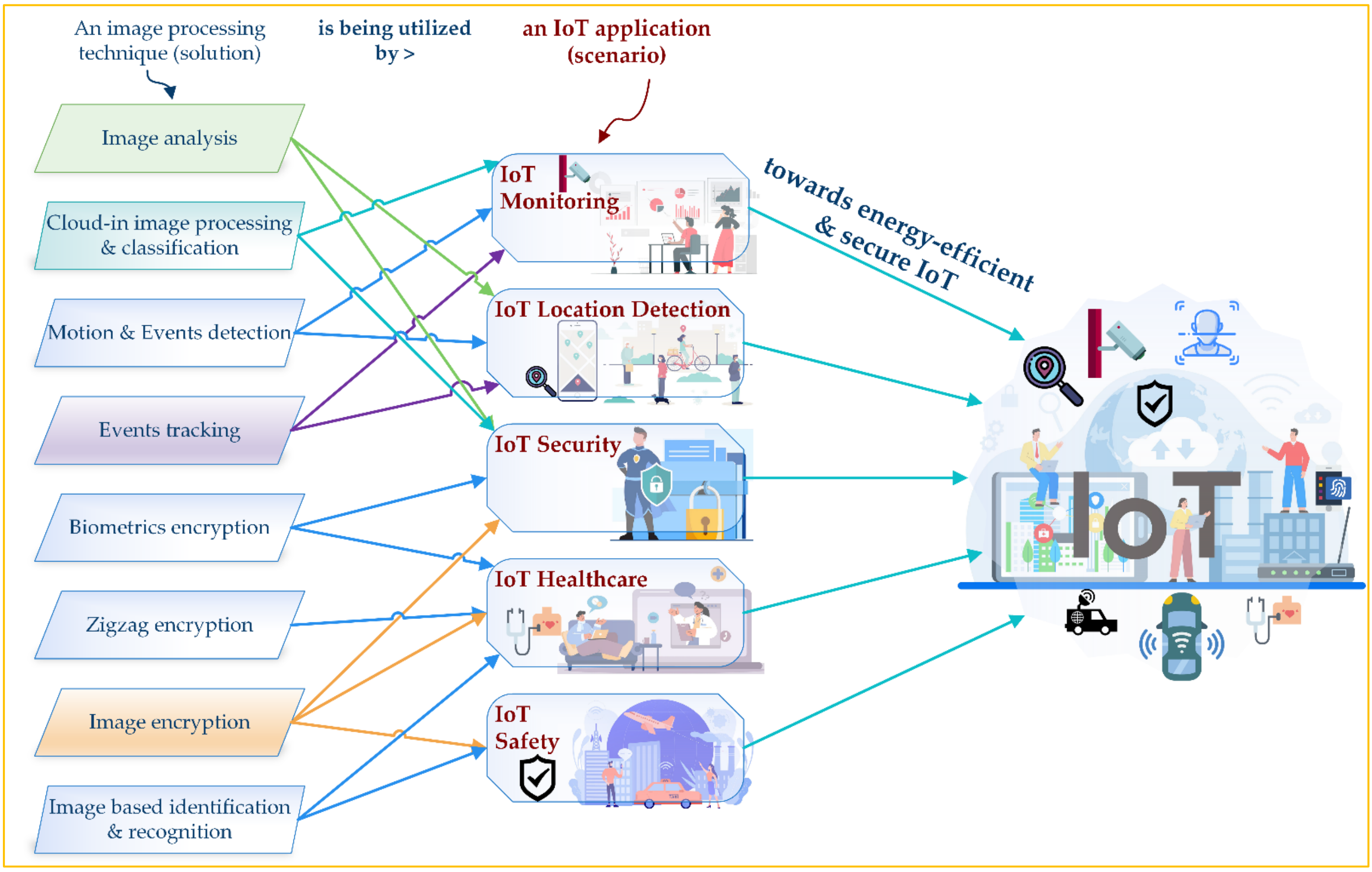
An image processing technique (solution)
is being utilized by >
an IoT application (scenario)
Image analysis
Cloud-in image processing & classification
Motion & Events detection
Events tracking
Biometrics encryption
Zigzag encryption
Image encryption
Image based identification & recognition
IoT Monitoring
IoT Location Detection
IoT Security
IoT Healthcare
IoT Safety
towards energy-efficient & secure IoT
IoT

Figure 16. A graphical representation highlighting a number of commonalities between solutions (image processing techniques) and scenarios (IoTSs). In this simple representation, a solution (listed on the left side) can be utilized by an IoTS (listed in the middle—in a red-colored font) in order to attain such an energy-efficient and secure IoT environment. Images are licensed. Design is made by authors.

8. Future Trends

We will look forward to the future trends in this part, where we will talk about how image processing may help us make important improvements in the IoT. In general, IoTS have relied on a wide array of developing and emerging technologies. Digital image processing is one example of these technologies. The following are some predicted developments in image processing related to the IoT:

1. Image processing seeks to help IoT be more secure, wherein all items linked with its infrastructure are engaged. Therefore, image processing techniques are continually being improved, and as a result, research that is devoted to improving image processing techniques should also try to reflect this improvement towards the growth of IoT in terms of various factors, including the security and safety of data [48];
2. When attempting to match images from both the collected and previously stored in-cloud images, it is essential that the data storage and communication networks used to do this be secure. Hence, the security of communication between the cloud and image-matching processing portion, on the one hand, and the safety and privacy of the remembered in-cloud-stored image, on the other hand, is a major concern and is a future trend of interaction between and integration of IoT and image processing;
    a. In the case of IoTSs, the entire system will fail if there is an issue with the security of image matching processing or with the safety of image content, regardless of whether or not the fault is discovered;

   b. As a result, researchers need to have been concerned with this problem and ought to have either enhanced the security of communication between IoT parties [29];

3. Image processing can contribute to IoT by decreasing the distance between two distant and remote workplaces;
   a. In the very near future, various programs will be employed for the objective of accessing digital and sensitive workplaces;
   b. An authentication and verification process by a third party, which might be the owner of the digital asset, as an example, is required to guarantee not just permitted access but also the security and confidentiality of its contents;
   c. So, initially, the first party will apply for authorized entry to the workplace. Secondly, a captured image is transmitted to the other party for verification purposes; however, a matching process is employed to help the decision-making. The third possibility is that the other party will permit such authorized access to keep the contents secure;
   d. For example, security improvement and computation time required to analyze either a single image or multi-frame images will be emphasized. An IoTS may either allow or deny an access request made by the authorized person [55];
4. Recently, the problem of image encryption has been extensively considered to execute an image transfer to cloud storage. For the purpose of this operation, having a secure communication method is equally as vital as having secure image content. Image-based encryption is yet to progress to serve better and help in this goal. There is a requirement to boost the performance of the IoTS that wants to transmit images to cloud storage or to a distant portion. The most crucial problem to be addressed regarding IoTS performance is the security of the images' contents [50];
5. Sending multi-frame images to the cloud with a little file size will be an important challenge in the future of IoT implementation. This is one of the key issues for both image processing and IoTSs owing to the massive storage created in the cloud. For IoTSs requiring the transmission of multi-frame images via IoT networks, a solution to this problem is to provide a system that prioritizes the transfer of particular frames depending on analysis decisions made by image processes. Images containing significant content will be uploaded to the cloud [45];
6. Another important barrier to image processing in the setting of IoT-implemented systems is connected to the security of the communication channel between the source of image processing and the destination. Because of the importance of transferring digital material while maintaining the safety of the communication route, this problem is still difficult to solve. Hence, presently proposed studies are tackling this problem by observing that the security system is essential to reach a high degree of lightweight;
7. In accordance with [57], a smaller image is better for IoT-cloud image transfer. The data size across IoT communication channels will be decreased as a consequence, helping to minimize overall energy usage. This will contribute to shifting energy-friendly IoT seeking to realize the vision of the development of sustainable energy. One of the future trends towards sustainable energy in the IoT environment is to use effective security schemes that serve to considerably decrease the size of the image to minimize both transmission time and size;
8. One method for increasing the security of images stored in the IoT cloud or on other servers is to divide them into blocks of images, which may be used to create a double-phase security scheme for images;
9. Embedding a password mechanism should have helped the attainment of the integrity target of encrypted medical images [64]. As long as you embed an OTP in the encrypted medical image, the authorized person may verify the embedded OTP by comparing it to another OTP that was transmitted via a secure channel.

9. Conclusions

This paper has looked at one of the common problems with IoTSs, such as security. Image processing techniques have played a significant role in providing solutions. Several alternative techniques of image processing have been investigated to determine whether or not they could contribute to the solution of such issues. This review's primary goal is to help researchers in related domains to design an energy-efficient and secure IoTS. It has been shown in these publications that image-processing techniques may contribute to IoTSs.

In this section, two main sub-sections are discussed. Firstly, detailed concluding notes on papers evaluated, in which the benefits and drawbacks of systems and papers are discussed. Other important IoT-related challenges, such as energy usage and security, have been discussed. The final sub-section lists a number of limitations related to this article.

9.1. Final Thoughts and Remarks

1. Image processing has been used in IoT monitoring applications, according to [42];
2. Image processing techniques have made a significant contribution to IoT's ability to protect data transferred between devices and networks;
3. By using a variety of image processing techniques, image processing techniques have reinforced the encryption idea applied to digital data. When comparing an image processing-based security solution to a non-image processing-based method, the number of vulnerabilities is decreased [48];
4. The use of sensors and cameras for detecting movement and collecting images helps improve home safety [29];
5. At the perception layer, image processing has contributed to the safe transmission of sensitive material to the network layer. Cloud-based storage will be used for the images. It is thus possible to use the proposed security strategy for a wide range of IoTSs, including cloud-enabled IoT, that require encrypting images using random and sophisticated patterns with the aid of CAs [49];
6. Image encryption has been utilized by many proposed systems and applications described in the literature to improve the security and privacy of the material that an image conveys [49,50];
7. By grouping the infected images into groups, image processing has helped identify malware assaults. Malware binaries are used to create malware images. Because malware images are classified, IoT devices impacted by an assault will be better protected in terms of security; as a result, the DDoS virus is a well-known assault against IoT devices [51];
8. IoTSs have been able to benefit greatly from image processing. An image processing technique may be used to record images (as a video stream) for the purpose of performing monitoring tasks for an area or environment, such as an industrial zone containing sensitive equipment. Image processing can be used not only to analyze acquired images at the site or at the fog nodes but it can also be used to secure the communication channel between regions where images are captured and fog nodes before any transferring of these images have taken place. Creating an energy-friendly system design might lower other parameters like transmission time, bandwidth, storage, and transmission cost. In addition, image protection is a second responsibility. With the use of various image processing techniques and other mathematical models, such as the CA rule conception, it may be implemented in which images themselves can be encrypted;
9. A lot of processing and computing resources will be saved using lightweight security solutions before images are sent to the IoT Cloud [57];
10. According to [68], maintaining secure communication channels during image transmission isn't enough; IoT servers devoted to image storage must also be kept at a high level of security. The probability of the secret image (or any other IoT-associated

data) being hacked is reduced, and the content's safety is improved when it is divided up into blocks;

11. Embedding a password into an encrypted image that conceals medical data is possible [64]. Using a verification technique performed to the encrypted image's embedded password and sending that password to the authorized individual improves image content security in terms of integrity;
12. Many IoTSs employ image processing as a monitoring and security tool. Several related smart systems have integrated image processing-based security schemes with non-image processing-based schemes in terms of security [46,47] since image processing has played an effective role in strengthening security;
13. Many IoTSs that provide location detection services have made use of image processing techniques;
    (a) IoTSs will be able to provide improved services in terms of object localization if image processing is used in conjunction with the cloud and IoT settings [61];
    (b) It is mentioned that image processing and position detection methods like GPS have been employed and exploited to increase a variety of services that are significant and critical in our everyday activities, such as the identification and prevention of plant catastrophes [62];
    (c) UAVs, wireless sensors, drones, cloud computing, and other technologies have all been used in conjunction with image processing to improve position recognition in open areas that may be covered by the image capture process using UAVs [25];
14. Many IoT healthcare applications use image processing, such as [65]. To make IoT-related services more convenient, image processing has been used, where collected images may be analyzed remotely by people; then the necessary action can be taken via the IoT platform;
15. Performing computations via the cloud in recent years, an increased emphasis has been made on the need for security in relation to both the preservation of medical data and images as well as disease prediction. The healthcare business creates enormous amounts of data on a daily basis as a result of the progress of medical technologies. Cloud computing allows for the storage and management of these enormous amounts of data in a manner that is exceptionally secure. A more secure zigzag image encryption technique is utilized to identify illnesses utilizing image processing in a safe cloud computing environment [66].

9.2. Limitations

In this sub-section, a number of limitations of this article will be listed.

1. The search period is within a certain period of time; thus, there are a number of studies;
2. There is a portion of articles that have not been included in this review due to the publishing date(s) being beyond this article's search period;
3. This review has considered two factors which means some other factors have not been considered;
    a. It has considered the energy consumption caused by the processing of contents-heavy images;
    b. It has considered the security of images' contents;
    c. It has not considered the data size of digital content;
    d. It has considered the roles of image processing techniques in reducing energy consumption and increasing security;
4. In future investigations, researchers can take into account the recently published papers and publications.

Author Contributions: A.M.A.-G. wrote and designed the paper. H.K. proposed the idea of the paper and wrote the paper. Z.H. designed the paper's conception. N.M.A.-H. wrote the paper. M.O., R.M.K. and I.S. contributed to the paper's flow. All authors have read and agreed to the published version of the manuscript.

Funding: This article is funded by Tenaga Nasional Berhad (TNB), Malaysia with TNB SEED FUND with a grant code: U-TL-RD-21. Also, this research is funded by Universiti Tenaga Nasional (UNITEN) with J510050002-IC-6 BOLDREFRESH2025-CENTRE OF EXCELLENCE.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the team at freepik.com. Licensed images are borrowed from https://www.freepik.com/ (accessed on 10 November 2022).

Conflicts of Interest: The authors declare that they have no competing interest.

List of Abbreviations

AI	Artificial intelligence
BLE	Bluetooth low energy
CA	Cellular Automata
DDoS	Denial of service
DLs	Digital libraries
DNNs	Deep neural networks
EOI	Events-of-interest
ID	Identity
IoT	Internet of Things
IoTSs	Internet of Things (IoT)-dependent systems
OOI	Object-of-interest
OTP	One-time password
PIR sensor	Passive infrared sensor
RL	Reinforcement learning
ROI	Region of interest
SVR	Support vector regression
UAVs	Unmanned aerial vehicles
VGG	Visual Geometry Group

References

1. Hsu, C.-H.; Cheng, S.-J.; Chang, T.-J.; Huang, Y.-M.; Fung, C.-P.; Chen, S.-F. Low-Cost and High-Efficiency Electromechanical Integration for Smart Factories of IoT with CNN and FOPID Controller Design under the Impact of COVID-19. *Appl. Sci.* **2022**, *12*, 3231. Available online: https://www.mdpi.com/2076-3417/12/7/3231 (accessed on 11 November 2022). [CrossRef]
2. Quy, V.K.; Hau, N.V.; Anh, D.V.; Quy, N.M.; Ban, N.T.; Lanza, S.; Randazzo, G.; Muzirafuti, A. IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Appl. Sci.* **2022**, *12*, 3396. Available online: https://www.mdpi.com/2076-3417/12/7/3396 (accessed on 11 November 2022). [CrossRef]
3. Sepasgozar, S.; Karimi, R.; Farahzadi, L.; Moezzi, F.; Shirowzhan, S.; Ebrahimzadeh, S.M.; Hui, F.; Aye, L. A Systematic Content Review of Artificial Intelligence and the Internet of Things Applications in Smart Home. *Appl. Sci.* **2020**, *10*, 3074. Available online: https://www.mdpi.com/2076-3417/10/9/3074 (accessed on 11 November 2022). [CrossRef]
4. Othman, N.A.; Aydin, I. A face recognition method in the Internet of Things for security applications in smart homes and cities. In Proceedings of the 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 25–26 April 2018; pp. 20–24. [CrossRef]
5. Taştan, M.; Gökozan, H. Real-Time Monitoring of Indoor Air Quality with Internet of Things-Based E-Nose. *Appl. Sci.* **2019**, *9*, 3435. Available online: https://www.mdpi.com/2076-3417/9/16/3435 (accessed on 11 November 2022). [CrossRef]
6. Zhang, M.; Peng, B.; Chen, Y. An efficient image encryption scheme for industrial Internet-of-Things devices. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, London, UK, 15 November 2019; pp. 38–43.
7. Mat, I.; Kassim, M.R.M.; Harun, A.N.; Yusoff, I.M. Smart Agriculture Using Internet of Things. In Proceedings of the 2018 IEEE Conference on Open Systems (ICOS), Langkawi, Malaysia, 21–22 November 2018; pp. 54–59. [CrossRef]

8. Jacoby, M.; Usländer, T. Digital twin and internet of things—Current standards landscape. *Appl. Sci.* **2020**, *10*, 6519. [CrossRef]
9. Gu, Z.; Li, H.; Khan, S.; Deng, L.; Du, X.; Guizani, M.; Tian, Z. IEPSBP: A cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 89–106. [CrossRef]
10. Lin, C.-H.; Hu, G.-H.; Chan, C.-Y.; Yan, J.-J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm. *Appl. Sci.* **2021**, *11*, 1329. Available online: https://www.mdpi.com/2076-3417/11/3/1329 (accessed on 1 September 2022). [CrossRef]
11. 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. [CrossRef]
12. Vermesan, O.; Friess, P.; Guillemin, P.; Giaffreda, R.; Grindvoll, H.; Eisenhauer, M.; Serrano, M.; Moessner, K.; Spirito, M.; Blystad, L.-C. Internet of things beyond the hype: Research, innovation and deployment. In *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*; River Publishers: Gistrup, Denmark, 2022; pp. 15–118.
13. Bale, A.S.; Saravana Kumar, S.; Varun Yogi, S.; Vura, S.; Baby Chithra, R.; Vinay, N.; Pravesh, P. Chapter 8—Network and security leveraging IoT and image processing: A quantum leap forward. In *System Assurances*; Johri, P., Anand, A., Vain, J., Singh, J., Quasim, M., Eds.; Academic Press: Cambridge, MA, USA, 2022; pp. 123–141.
14. Cruz, M.; Mafra, S.; Teixeira, E.; Figueiredo, F. Smart Strawberry Farming Using Edge Computing and IoT. *Sensors* **2022**, *22*, 5866. Available online: https://www.mdpi.com/1424-8220/22/15/5866 (accessed on 11 November 2022). [CrossRef]
15. Debauche, O.; Mahmoudi, S.; Guttadauria, A. A New Edge Computing Architecture for IoT and Multimedia Data Management. *Information* **2022**, *13*, 89. Available online: https://www.mdpi.com/2078-2489/13/2/89 (accessed on 12 November 2022). [CrossRef]
16. Malik, S.; Tyagi, A.K.; Mahajan, S. Architecture, Generative Model, and Deep Reinforcement Learning for IoT Applications: Deep Learning Perspective. In *Artificial Intelligence-Based Internet of Things Systems*; Pal, S., De, D., Buyya, R., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 243–265.
17. Rahmani, A.M.; Bayramov, S.; Kiani Kalejahi, B. Internet of things applications: Opportunities and threats. *Wirel. Pers. Commun.* **2022**, *122*, 451–476. [CrossRef]
18. Esposito, M.; Palma, L.; Belli, A.; Sabbatini, L.; Pierleoni, P. Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review. *Sensors* **2022**, *22*, 2124. Available online: https://www.mdpi.com/1424-8220/22/6/2124 (accessed on 1 November 2022). [CrossRef] [PubMed]
19. KhoKhar, F.A.; Shah, J.H.; Khan, M.A.; Sharif, M.; Tariq, U.; Kadry, S. A review on federated learning towards image processing. *Comput. Electr. Eng.* **2022**, *99*, 107818. [CrossRef]
20. Rehman, A.; Saba, T.; Kashif, M.; Fati, S.M.; Bahaj, S.A.; Chaudhry, H. A Revisit of Internet of Things Technologies for Monitoring and Control Strategies in Smart Agriculture. *Agronomy* **2022**, *12*, 127. Available online: https://www.mdpi.com/2073-4395/12/1/127 (accessed on 17 November 2022). [CrossRef]
21. Bhardwaj, A.; Kaushik, K.; Kumar, M. Taxonomy of Security Attacks on Internet of Things. In *Security and Privacy in Cyberspace*; Kaiwartya, O., Kaushik, K., Gupta, S.K., Mishra, A., Kumar, M., Eds.; Springer Nature: Singapore, 2022; pp. 1–24.
22. Smmarwar, S.K.; Gupta, G.P.; Kumar, S. Deep malware detection framework for IoT-based smart agriculture. *Comput. Electr. Eng.* **2022**, *104*, 108410. [CrossRef]
23. Park, S.; Park, S.H.; Park, L.W.; Park, S.; Lee, S.; Lee, T.; Lee, S.H.; Jang, H.; Kim, S.M.; Chang, H.; et al. Design and Implementation of a Smart IoT Based Building and Town Disaster Management System in Smart City Infrastructure. *Appl. Sci.* **2018**, *8*, 2239. Available online: https://www.mdpi.com/2076-3417/8/11/2239 (accessed on 20 February 2022). [CrossRef]
24. Hsu, T.-C.; Tsai, Y.-H.; Chang, D.-M. The Vision-Based Data Reader in IoT System for Smart Factory. *Appl. Sci.* **2022**, *12*, 6586. Available online: https://www.mdpi.com/2076-3417/12/13/6586 (accessed on 1 November 2022). [CrossRef]
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. [CrossRef]
26. Wang, C.; Han, Y.; Wang, W. An End-to-End Deep Learning Image Compression Framework Based on Semantic Analysis. *Appl. Sci.* **2019**, *9*, 3580. Available online: https://www.mdpi.com/2076-3417/9/17/3580 (accessed on 26 February 2022). [CrossRef]
27. Jia, Z.; Xu, S.; Mu, S.; Tao, Y. Learning-Based Text Image Quality Assessment with Texture Feature and Embedding Robustness. *Electronics* **2022**, *11*, 1611. Available online: https://www.mdpi.com/2079-9292/11/10/1611 (accessed on 11 November 2022). [CrossRef]
28. Barriga, J.J.; Sulca, J.; León, J.L.; Ulloa, A.; Portero, D.; Andrade, R.; Yoo, S.G. Smart Parking: A Literature Review from the Technological Perspective. *Appl. Sci.* **2019**, *9*, 4569. Available online: https://www.mdpi.com/2076-3417/9/21/4569 (accessed on 27 February 2022). [CrossRef]
29. 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. [CrossRef]
30. Awan, M.J.; Bilal, M.H.; Yasin, A.; Nobanee, H.; Khan, N.S.; Zain, A.M. Detection of COVID-19 in Chest X-ray Images: A Big Data Enabled Deep Learning Approach. *Int. J. Environ. Res. Public Health* **2021**, *18*, 10147. Available online: https://www.mdpi.com/1660-4601/18/19/10147 (accessed on 3 March 2022). [CrossRef]

31. Anuradha, M.; Jayasankar, T.; Prakash, N.B.; Sikkandar, M.Y.; Hemalakshmi, G.R.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocess. Microsyst.* **2021**, *80*, 103301. [CrossRef]
32. Godavarthi, B.; Nalajala, P.; Ganapuram, V. Design and implementation of vehicle navigation system in urban environments using internet of things (IoT). In Proceedings of the IOP Conference Series: Materials Science and Engineering, Hyderabad, India, 3–4 July 2017; p. 012262.
33. Kapoor, A.; Bhat, S.I.; Shidnal, S.; Mehra, A. Implementation of IoT (Internet of Things) and Image processing in smart agriculture. In Proceedings of the 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 12 December 2016; pp. 21–26.
34. Bharath, V.; Adyanth, H.; Shreekanth, T.; Suresh, N.; Ananya, M. Intelligent sockets for home automation and security: An approach through IoT and image processing. In *The IoT and the Next Revolutions Automating the World*; IGI Global: Hershey, PA, USA, 2019; pp. 252–279.
35. Bolhasani, H.; Mohseni, M.; Rahmani, A.M. Deep learning applications for IoT in health care: A systematic review. *Inform. Med. Unlocked* **2021**, *23*, 100550. [CrossRef]
36. Haghi Kashani, M.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A systematic review of IoT in healthcare: Applications, techniques, and trends. *J. Netw. Comput. Appl.* **2021**, *192*, 103164. [CrossRef]
37. Gnoni, M.G.; Bragatto, P.A.; Milazzo, M.F.; Setola, R. Integrating IoT technologies for an "intelligent" safety management in the process industry. *Procedia Manuf.* **2020**, *42*, 511–515. [CrossRef]
38. Nauman, A.; Qadri, Y.A.; Amjad, M.; Zikria, Y.B.; Afzal, M.K.; Kim, S.W. Multimedia Internet of Things: A Comprehensive Survey. *IEEE Access* **2020**, *8*, 8202–8250. [CrossRef]
39. Bharadwaj, H.K.; Agarwal, A.; Chamola, V.; Lakkaniga, N.R.; Hassija, V.; Guizani, M.; Sikdar, B. A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications. *IEEE Access* **2021**, *9*, 38859–38890. [CrossRef]
40. Al-Dhief, F.T.; Latiff, N.M.A.; Malik, N.N.N.A.; Salim, N.S.; Baki, M.M.; Albadr, M.A.A.; Mohammed, M.A. A Survey of Voice Pathology Surveillance Systems Based on Internet of Things and Machine Learning Algorithms. *IEEE Access* **2020**, *8*, 64514–64533. [CrossRef]
41. Cui, F. Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment. *Comput. Commun.* **2020**, *150*, 818–827. [CrossRef]
42. 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. [CrossRef]
43. Punyavathi, G.; Neeladri, M.; Singh, M.K. Vehicle tracking and detection techniques using IoT. *Mater. Today Proc.* **2021**, *51*, 909–913. [CrossRef]
44. 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. [CrossRef]
45. 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. [CrossRef]
46. 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.
47. 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. [CrossRef]
48. 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. [CrossRef]
49. 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. [CrossRef]
50. 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. [CrossRef]
51. 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. [CrossRef]
52. 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. [CrossRef]
53. 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. [CrossRef]
54. 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**. [CrossRef]
55. 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. [CrossRef]

56. 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. [CrossRef]
57. 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. [CrossRef]
58. 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. [CrossRef]
59. 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. [CrossRef]
60. 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**. [CrossRef]
61. 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. [CrossRef]
62. 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. [CrossRef]
63. 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. [CrossRef]
64. 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. [CrossRef]
65. 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. [CrossRef]
66. 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. [CrossRef]
67. 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.
68. Li, Y.; Tu, Y.; Lu, J.; Wang, Y. A Security Transmission and Storage Solution about Sensing Image for Blockchain in the Internet of Things. *Sensors* **2020**, *20*, 916. [CrossRef]
69. Zadobrischi, E. Analysis and Experiment of Wireless Optical Communications in Applications Dedicated to Mobile Devices with Applicability in the Field of Road and Pedestrian Safety. *Sensors* **2022**, *22*, 1023. Available online: https://www.mdpi.com/1424-8220/22/3/1023 (accessed on 11 November 2022). [CrossRef] [PubMed]
70. Vanitha, V.; Akila, D. Efficient Computation of Hepatitis Blood Smear Image Encryption Using Enhanced Chaotic Technique for Cloud Storage. In *Soft Computing: Theories and Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 845–855.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.