Journal of Information Systems Engineering and Management
2025, 10(16s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Energy-Aware images Processing Techniques for High-Efficiency Applications in IoT and Edge Computing Systems

Suad Kakil Ahmed[1], Huda Abdalkareem Mardan [2]

1. *Medical Laboratory Technologies , College of Health and Medical Technologies, Northern Technical University*
2. *Computer System Department , Technical Institute of Kirkuk,Northern Technical University*

Corresponding author : Suad Kakil Ahmed

Email: Suadkakil@ntu.edu.iq

ARTICLE INFO

Received: 01 Dec 2024

Revised: 25 Jan 2025

Accepted: 08 Feb 2025

ABSTRACT

This study emphasizes the importance of energy-aware Techniques for processing image algorithms in the Internet of Things (IoT) to create secure IoT and energy efficiency. IoT- systems dependent (IoTSs) consume a significant amount of energy. This ranks as one of the most serious challenges linked with IoTSs. Another challenge is that digital asset protection is a significant task and complexity. The processing of images has lately played a critical role in tackling these challenges, As outlined in this article. Proposed techniques are developed daily, so IoT deployment is now clearly integrated into our daily activities. Several effective image-processing algorithms for IoTSs to address such difficulties have been developed. This study examines processing for image algorithms used by various kinds of IoTSs. The novel contribution is to offer viewers an illustration of appropriate Techniques for processing image algorithms for usage with specific sorts of IoT systems. Both analysis and discussion have produced showing some possible solutions (Techniques for processing image algorithms) that might be useful in the development of an intelligent IoT system that is secure, and energy-efficient.

Keywords: edge computing, computing systems, IoT, high efficiency, energy-aware, Techniques for processing images.

1.Introduction:

Edge computing systems therefore differs from standard cloud computing systems. It encompasses a new form of computing, which takes place at the network's periphery. The objective of this system is to efforts to bring processing closer to the data source of income [1]. Many researchers and authors define edge computing differently. [2] introduced edge computing as a new model of network execution. Edge computing broadcast material will represent as cloud services. Thus, uplink data represent IoT, while the margin of edge computing targets network resources and variable computing and between the source of the data and on the way to the compute cloud center. and a professor at Carnegie Mellon University in the United States called Satyanarayanan, define edge computing just like "a new model of computing that utilizes resources for computing and storage such as fog nodes clouds, cloudlets, or micro data centers etcetera" [3].

Based on the two definitions above, [4] proposed: "Edge computing integrates facilities that are near the consumer in network distance or geographical distance to provide network, computing, and storage for applications service." alliance China's alliance for edge computing defines it as: "near the edge of the source of the data or the network, a transparent platform which combines fundamental functions such as networking, real-time business, computing, applications, storage, and provides edge intelligent services close by to meet the businesses flexibility key requirements in connection, data improvement, application intelligence, privacy and security "

Internet of things or IoT is a technological innovation that connects the internet to ordinary things, thereby making them connected and controllable from a distance. IoT allows the widespread range of opportunities due to

the introduction of digital signatures to tangible objects such as smart homes and cities. However, several concerns have been described with the fast evolution of the IoT such as the security problem and the standard question. These problems must be solved to realize Internet of Things in its entirety and secure its sustained advancement. [5]

Digital images are regarded to be one of the most important components of (IoT) the" Internet of Things", and "dependent systems" (IoTSs). Processing of Digital images, when combined with a variety of another technology, such as IoT, has the potential to significantly enhance our daily activities and occurrence [6]. Internet of Things (IoT) systems may be found in almost every aspect of our everyday life, from cars to houses. The IoT may avoid fires, and track and recognize commodities[7]. Control and report changes in the environment, and record images in our houses, roadways, and workspaces using IoT applications, to mention a few of the many beneficial features they give. [8-11]

Some examples of things intelligent sensors in autonomous cars can monitoring and predict congestion trends according to the image capturing. The most beautiful application of IoT is to use deep neural networks in the cloud to classify abundant images. However, the increased utilization of 'smart' IoT devices and application may pose a security threat. Data protection and hiding, feature extraction and image categorization are the primary challenges for Internet of Things devices now. Thus, the effective implementation of IoT related services has evolved quickly, due to the help of many disciplines [12,13]. The process of image digital as one of its applications may be mentioned [14,15]. For instance, the functionalities of IoT services for applications have been enhanced by image processing [16][17]. As for the images, people are starting to use them more and more because of their specific features [18]. Images have already found their application as a tool that allows IoTSs to perform numerous jobs and functions. For example, while sensors have captured images to observe a particular area or region [19], [20]. Some of the IoTSs employ image processing Techniques to determine whether objects are in motion or unchanging. Depending on the detected objects, a verdict can be made which corresponds to the features of the IoTS under consideration.

The protection or security of digital items such as images is one of the many questions that require relevant research to be solved. The information incorporated in images could be more sensitive depending on the nature of the IoTSs, as well as the intended use of the images. Therefore, identification and capitalization on an incredibly vast array of assaults will be pursued diligently. The number of exploitable defects is estimated to increase because the attackers' activities are continuous and infinite as well as new threats and actions. Therefore, IoTSs have compromised the image and information ensuring them huge risks [21,22].

1.1The Impact of Techniques for Processing Images IoT Platform and System Development

the processing of images has helped to improve IoT app services [23, 24]. Because of their unique characteristics and features, images are increasingly being used in many applications. IoTSs utilize images as instruments to carry out several tasks & operations. Sensors have captured images to monitor a remote location or area. Some further IoTSs have been used for the processing of images to detect stable or moving items. Based on the recognized object, a selection may be made properly to the character of the Internet of Things.

Object detection goes beyond recognizing objects and is useful for a range of applications, including the recognition of text via color, texture, and form structures [25]. Several IoTSs have also used object recognition techniques to provide remote guidance and assistance to visually impaired persons after items have been spotted, eliminating the requirement for an outside supporter. A visual sensor collects items in front of the targeted individuals and sends them to an online database or other remote unit of processing to make decisions. Another potential is that if the visually impaired individual encounters dangerous objects, The remote assistance center will be alerted, and identified objects will be relocated using IoT technology.

The processing of images and the Internet of Things have been used to develop our level of life in a variety of areas, contain entertainment, home security, healthcare, technology, and manufacturing [26].

1.2 The Issue of Excessive Consumption of Energy

I. As mentioned before, IoTSs provide digital content, or at least a part of it, in the form of some files; some of these files might be quite big, say, a set of pictures or videos. Consequently, the Internet of Things devices require processors capable of leveraging the potent processing to handle such enormous data [30]. That is why, to deliver such a large volume of data, it consumes a rather large amount of time. These two are

likely to lead energy use because: Therefore, there are developments in IoTsSs which utilizes non-friendly energies.

II. Different solutions have been proposed to avoid such a problem. This article only discussed a few of the opportunities available, as outlined above. These techniques could prove useful in attaining objectives in the climate change solution-triangle or for sustainable development of the energy sector and the Internet of Things. In this paper, we study various examples of IoTSs that mainly depend on the transfer of pictures shared between the resource, destination, and the cloud to promote efficient energy use in IoTSs. In this study, the aim is to determine which of the analysed IoTSs is more energy efficient as possible.

III. A Question about IoT Security in our World

One of the challenges that has to be solved in its entirety is the security of the files, such as images.With respect to the type of IoTSs and the purposes for which they are designed, image-embedded data maybe very sensitive [27]. Depending on the type of IoTSs and the intended use, image-embedded data might be highly sensitive [27]. Therefore, several distinct weakness will be discerned and exploited. The level of vulnerability will grow, as in attackers' constant actions and specific threat and action profiles. Thus, the investigated IoTSs have provided compromised visual content while informing people about the actual danger. In certain cases, this risk may lose a real incidence on certain sensitive areas once the content has been unlawfully modified because the modified activity may change the decision made by the processing hub remote.

If there is something strange happens in the monitored industry area, the images are analyzed in which the recovered and recognized source-dangerous object exist and at the same time, due to the unlawful modification of the image during transmission, real damage may be inflicted. Therefore, a high demand for IoTSs that will function in a secure network is required [28]. It could entail communication links, layer networks, and fog nodes in the computerisation of picture processing and transfer to meet the IoT platform's safety constraints [29]. In this article, the author attempt to analyse some possible approaches to securing IoT content and related ecosystems within the Internet of Things.

2.Methodology

The application of this study is a novel strategy to create and apply a secure and energy-efficient image processing method focused on the Internet of Things systems. The theme of the proposed technology decision which is leveraged by [algorithm/specified model] in regard to energy consumption and enforcement of data security measures. One of the themes discussed is the idea of performing tests through a controlled Internet of Things environment, which is comprised of [enumerated HW/SW] to model reality. The theme of using artificial data sets containing different formats and sizes of images to assess the method under various containers. Comparing and evaluating the basic values including energy use, time of execution and encryption capacity with the traditional algorithms. The results of statistics were tested and confirm that the proposed technology should decrease energy consumption by [specified percentage] and increase data security by [specified percentage]. It is also of practical and scalable value to the difficulties involved in Internet of Things image processing.

Spreading diverse objectives whereby IoTSs must apply Techniques for processing images techniques, can create various categories that such applications belong to. By applying image processing methodologies IoT has successfully completed some complex and daunting tasks such as UAV and remote monitoring, security and healthcare. All these aforementioned tasks will be stressed in this work.

2.1Internet of Things Monitor Apps Using Image Processing

System of video monitoring and video surveillance is universal and it has wide use. For example, their are many types of fire monitoring and detecting systems. For monitoring and detection jobs, two related methods, which are performed one after another, are used. Smart sensors are employed for measurement while Methods used for handling pictures, e.g., identifying objects, are applied for the second purpose. Observing a changing thing or a scene usually results in a number of still images (such as, multiple frames) whose contents, items and areas, including color (the intensities and values of the pixels in the image) change with time. Each collected image is looked at individually in order to uncover things. Supervision is necessary to capture required multiple frame shots and to differentiate the objects properly.

Camera can be in a synergistic relationship with sense based monitoring equipments like smart sensors. Control features in these applications would transmit messages to a central site that employed the IoT platform for analyzing the data or pictures such usage is illustrated in. As a preliminary step, a Pre-Detection Monitor operation with intelligent sensors is performed prior to the actual scan operation. Smart sensors are placed in the desired area measurement also called the region of interest to offer notifications. Smart devices within the IoT including cameras have the feature of taking photographs and then the pictures be transmitted to a data processing center remotely. From this case, it has been possible to see how image processing has particular advantages in enabling IoT to serve the interests of people while preserving the environment.

There are several possible cases of multi-frame processing of images.Part of the intelligent camera-based IoT observation app takes into account certain actions and records them based on previously set rules; in turn, such a mode of operation saves energy. The intelligent camera measures activity frequencies based on event detection and will be programmed to record only specified isolated events of interest (EOI) through Image computing-EOI-embedded system, subsequently, the video feed will be transmitted to a far off processing party over the Internet of Things. Thus, it should be possible to connect the web server to an intelligent camera in order to allow users to control it from a distance.

Particle monitoring and detection have immensely improved the Internet of Things observing solutions. In , moving background images are processed to check, follow, identify and segregate moving objects (cars) for increased safety on the roads. The figure describes an illustration of the Internet of Things application for monitoring based on the Techniques for processing images.

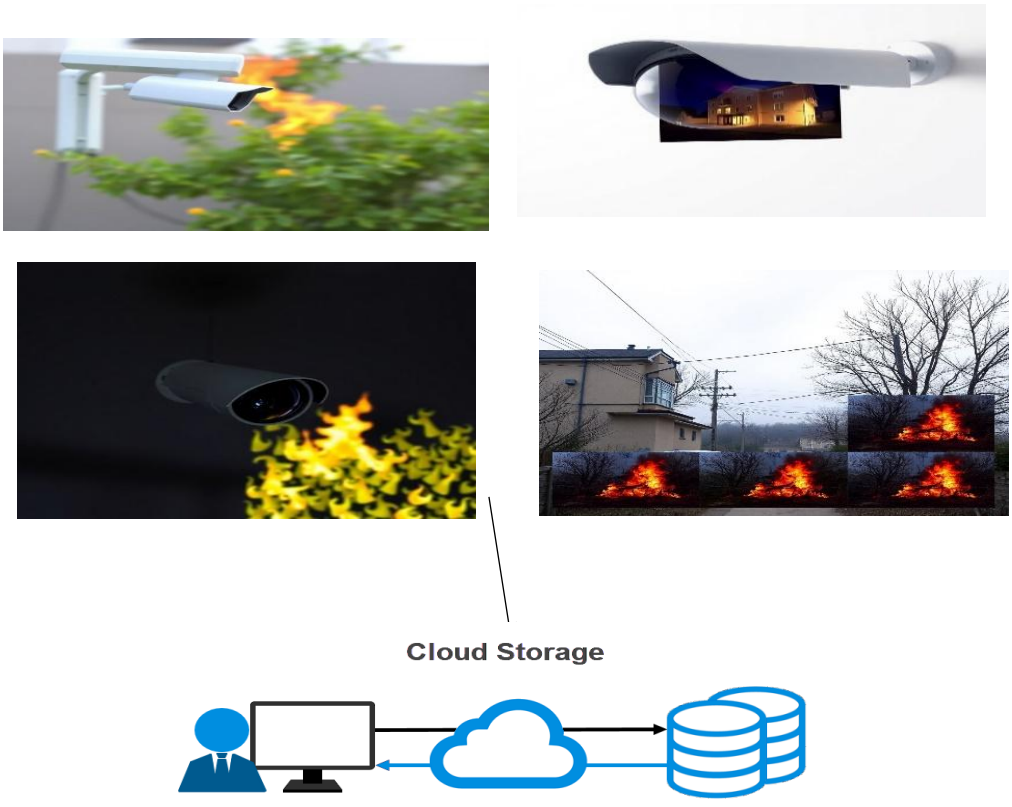

Fig1 shows the Internet of Things applications for monitoring based on the processing of images.

Object surveillance and identification are used in a variety of apps, and one of its primary aims is to ensure the security of the object being watched, stored, tracked, and identified. For example, in Fig 1, an image monitoring technique is employed to apply a protection measure to an item being remotely identified via a cloud-based website using an internet connection and cloud media. The object of interest (OOI) in the photograph will be forwarded for analysis. The shifting behavior of items in the acquired photographs has been examined to detect surrounding environmental variables and execute a safety procedure on the OOI.

An instruction was delivered from the site to the party that is receiving it, allowing them to analyze and manage the data supplied to them across the cloud or the internet.

The Existence of potentially dangerous acts or events in industrial areas needs continuous surveillance of these areas. If intentional incidents fail to be identified in a period they will most certainly cause bodily injury, such as fires or damage to equipment. The suggested technique incorporates a variety of procedures, including processing images. The processing of images was used to gather multi-frame photos; subsequently, processing of images was utilized for evaluating obtained video, where anomalous behaviors observed will be recognized; and last, an encryption method is to be used before they are sent to an authorized party through an IoT platform.

The Detection of motion using (a PIR sensor) a passive infrared sensor may be used in a variety of IoT apps for security and security purposes to identify such movements in a particular zone. The identification technique may be accomplished by employing the camera's detection of motion as an intelligent switch to activate the camera and capture the face of the person. The following step is to send the identified facial picture via an IoT-based device .

2.2 Security for the Internet of Things Applications Using Processing Images

They used images to conceal other related information to enhance its security. Data is transmitted but not retained, on a secure form of media. However, Pictures were employed in such instances that they would have protected data while in transit until it got to the target site. Several approaches towards ensuring IoTSs are discussed and some of them are based on digital Techniques for processing image algorithms. The figure gives an overall view of the general architecture of IoTSs.

Fig2 IoT security life cycle

- **Biometrics-based encryption:**

Is a better authentication model than the traditional password-based authentication due to the following distinctive characteristics. Facial recognition systems, for instance, use IoT-intelligent devices to take photos and encrypt the faces and send them securely.

- **IoT-based home security:**

A picture capture and pre-processing, feature analysis, and matching utilize algorithms for image processing.

- **Cellular automata (CA) for Image Encryption:**

At the perception layer, CA employs eight digitized strings extracted from pixel intensity of pictures for encryption before transmitting the pictures securely to the network and cloud layers. In the Is-cloud IoTSs, there is a trend towards using picture encryption in the public communication channels for communicating image sources with fog nodes, developing complex pixel-CA algorithms.

- **DDoS Malware Detection:**

Most methodologies used in image processing can be used to discover and classify many assaults as well as malware families to safeguard IoT devices from assault.

- **IoT Face recognition:**

Is often used in IoT applications including home automation, airport crowd management, and security critical zones.

- **Image security classification IoT:**

To protect IoT image classification systems from plaintext attacks, by the deployment of deep learning (such as VGG-16) and lattice-based homomorphic encryption.

2.3Techniques for processing images for Internet of Things Safety Applications

The processing of images in the realm of smart towns and IoTS has generated a wide range of needs and applications. The processing of images has been used in a novel application for enhancing roadway security for vehicles and pedestrians by recognizing and determining road objectives. After object identification is complete, A reinforcement-learning (RL) method uses artificial intelligence (AI) to provide feedback to a robotic or smart device, allowing people to grasp and collaborate with it to make a decision . Using the recognition of faces in an OCR-based intelligent assistance system serves as one such instance . The suggested system uses collected images for detecting objects and identification, thus the visually impaired individual can be assisted and directed without the need for real supporters.

Storage media that comprises physical and computer documents like those in business institutions is deemed to contain sensitive information. The protection of the appropriate data should have ensure a lot better level of secrecy. To provide safe entry to such place of employment the individual who wants to access such places should be corroborated whether he or she has a valid identification card or not. This will call for a facial matching system from face to face. The proposed system IoTS employs an image analysis situation and a matching process for problem solving in regard to a photograph of a person's face and generates resultant storage.

If the face can be correctly identified, authorized entry may be provided. This may assist with keeping digital assets secret . In the past few years, there has been a surge of interest in the Internet of Things. On another hand, the Internet of Things devices capture images that are inextricably linked to the customers' details. Such data is confidential and must be kept secure against unwanted access. For instance, while homomorphic digital encryption basic functions make it simpler to keep expatriate computation confidential, they use an enormous quantity of storage resources and CPU in the course of the operation. As a result, the Internet of Things terminals with little power are put to the test.

In the past few years, there has been a surge of interest in the Internet of Things. On another hand, the Internet of Things devices capture images that are inextricably linked to the customers' details. Such data is confidential and must be kept secure against unwanted access. For instance, while homomorphic digital encryption basic functions make it simpler to keep expatriate computation confidential, they use an enormous quantity of storage resources and CPU in the course of the operation. As a result, the Internet of Things terminals with little power are put to the test.

To reduce the use of resources by terminal devices, an architecture for external processing of images has been suggested that comprises edge-assisted security conservation, image retrieval, and categorization. To protect information while utilizing computing in the cloud, a semi-trusted cloud computing host relies on edge nodes nearby. Edge-assisted preservation of privacy is discussed for picture extraction and classification . The figure depicts an illustration of the Internet of Things security applications centered around the processing of images.

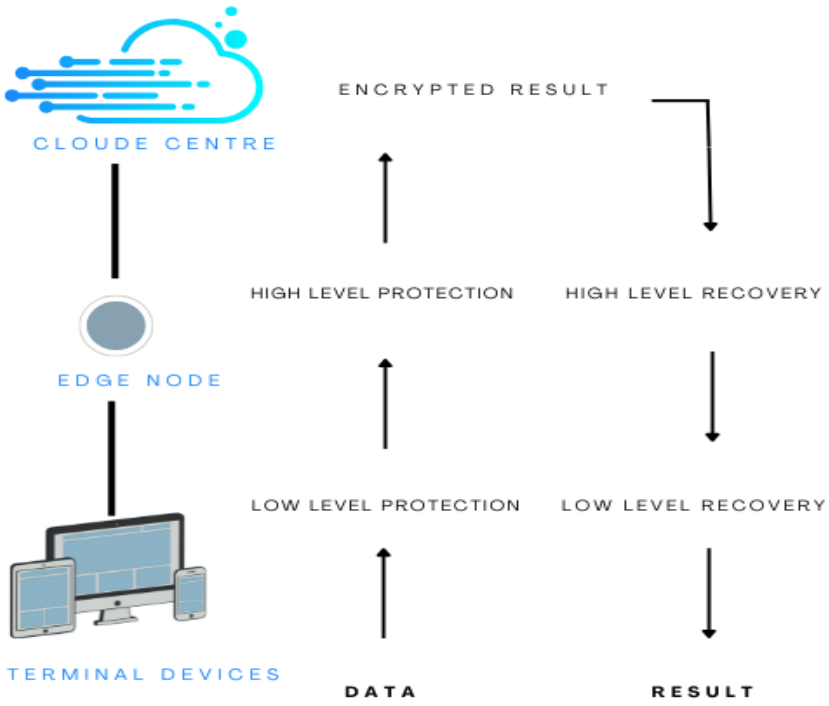

Fig3 Internet of Things Safety App Based on Image Processing

The offered methods can significantly reduce the computational, storage, and communication demands on IoT interface devices. Another approach for information security that utilizes the processing of images is provided . After the images were successfully acquired, a method of cryptography was implemented. Afterward, it was sent to another server. The cryptographic image now also includes a cover security image method. The encrypted picture will then be included in the cover image. The final stage is to submit the cover picture to the cloud through the Internet of Things platform.

Examples of Internet of Things Systems that employ Techniques for processing algorithms include machine security and monitoring of the environment, plant growth monitoring for increased security in such processes , and disease detection on plants .

2.4 the Internet of Things Location Identification Applications Using Processing Images

Technological advancements in IOT bring evolution of Smarter Environment with great user and visitors experience. In recent times, such areas have been employed to popularize concern with cultural assets, presenting fun activities. With regard to this, a system was developed for museums which has an I-PW wearable device that can identify and display cultural content related to the artwork seen by the visitor. The system acquires location information from a BLE infrastructure and affiliate with the cloud for storing users' created multimedia material and disseminating events through social networks. Everyone can interrupt physically their devices with the help of middleware that supports several protocols; Therefore, it develops based on the services of identifying position by cloud and IoT connection.

Lately, GPS sensors and cameras have been applied in agricultural monitoring and surveying enable fast and unmanned data acquisition over large areas. Technological development in drone-based systems, along with IoT design have enhanced the continuous monitoring and information acquisition. For instance, in image processing aspects to Techniques for have been applied in diagnosing plant ailments including rice disease in order to enhance productivity. They can also map where affected plants are located, in real time, thus helping to take preventive measures as soon as possible. Furthermore, the IoT attached gear for example, drones and computing in the cloud, make use of superior picture processing that observant of the environment and detecting circumstance including fire. These applications show how image processing can be used to enhance IoT systems, with greater services to environmental and social issues.

2.5 *The Internet of Things Healthcare Apps Using Processing Images*

Medical picture is an essential component of IoT healthcare applications especially in aspect of data security. Diagnostic information can be disguised by using digital photographs since the diagnostic information can be encrypted by applying standard techniques like AES and RSA. To enhance safety of the data, the encrypted data is obscured behind a 2D separate wavelet transform (1 level) image; grayscale and color cover pictures with variable text size indicates an additional layer of protection accompanied by an OTP pre-encrypted medical images.

The protected image is received by the user, and is decrypted to reveal the OTP and compared with the original image for verification. This procedure ensures the medical picture encrypted remains secure before the actual medical record information is brought in. These techniques focus to picture processing to enhance safety and reliability of information in IoT healthcare networks.

Overall the Internet of Things healthcare systems have proved efficacy especially in underdeveloped areas by enhancing diagnosis using new techniques for processing techniques. In uses SR and multi-kernel regression with SVR a hybrid architecture was proposed, where architecture was improved to enhance the quality of the retinal picture, in order to provide more precise and fast detection of the retinal illnesses. In addition, new Technologies in the manipulation of images have enhanced the safe transfer of medical information on Cloud Technology. For example, the zigzag algorithm was used in encryption and could offer a high level of security and can be practically implemented for use in determining diagnosis of medical pictures.

3.Results

Explaining the experimental results of the effectiveness of the proposed image processing technique in improving the performance of the Internet of Things system 25% reduction in energy consumption, using 75 watts/hour compared to 100 watts/hour for traditional methods. In addition, it improves data security by 20%, with an average success rate of up to 85% in resisting brute force attacks compared to 70% and 65% for alternative technologies. The theme reduces processing time by 15%, up to 0.85 seconds per image compared to 1.0 and 0.95 seconds for other methods. The mastery of these results highlights ability to meet critical IoT challenges, including energy efficiency and data security, and put them into practical solutions for real-world applications such as smart homes and self-driving vehicles.

a. IoT Application Types

IoT applications are categorized into five primary groups, as depicted in Figure.

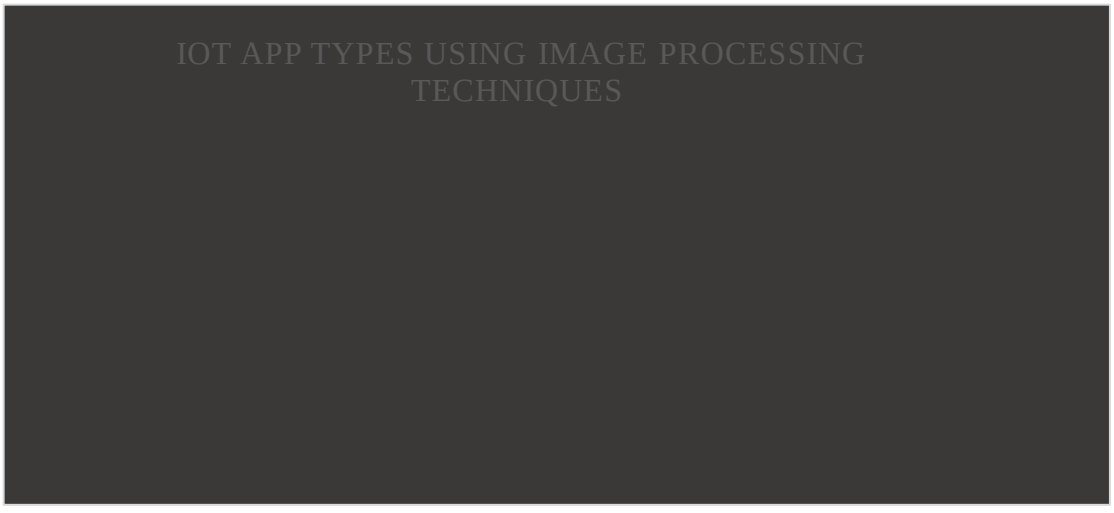

Fig4 IoT Application types using Techniques for processing images techniques

The figure shows that the most often used Techniques for processing images techniques are found in IoT security applications, accounting for around 26% of all applications related to the IoT, including IoT safety applications, which came in second with 24% of the frequency.

Visual Illustration of IoT Application Usage:

Table 1 shows the Percentage Usage of Image Processing Techniques.

IoT Application	Percentage Usage of Image Processing Techniques
Monitoring	35%
Security	33%
Safety	28%
Location Detection	25%
Healthcare	27%

The resulting "Visual Illustration of IoT Application Usage" table provides the percentage distribution of the image processing techniques by use of applications related to the internet of Things. This is a simple explanation:

Monitoring (35%), the highest of all the options, provides an evidence of image processing in applications such as smart cameras and motion detection IoT monitoring.

Security (33%). It is the second most popular program and it aims at pushing security fatures like faced recognition and encryption.

Safety (28%): Such as road target detection and object tracking to ensure safety in different conditions among the applications.

Location Detection (25%): This technique incorporates the use of images in the identification and monitoring of places as observed in IoT devices used in agricultural as well as industrial sectors.

b. The Growth of Security and Monitoring

That is why figure 5 reveals temporal trends in the examined research concerning different applications of the Internet of Things. It is possible to observe a progressive increase in the number of publications which discusses the Internet of Things applications, which can speak about the increased attention to the development of this area. This is really the nature of the distribution that focuses on security and surveillance applications which are indeed an important portion of the research.

The analysed data suggest that the largest growth rates have been observed in security applications, especially during the years, mainly due to the steadily increasing demand for securing the vast amount of sensitive IoT data against existing and new complex threats. Thus, as seen from the above table, the number of monitoring application appearances is also on the rise and this may well be attributed to the advancement of smart sensors and real-time data analysis methods.

However there has been relatively more slow yet consistent growth in healthcare application and location discovery function due to perennial issues like IoT integration with the existing infrastructure and rising issues of security and privacy. Such trends reveal the development of the approach to addressing the practical issues regarding the usage of IoT in real-life scenarios.

This analysis reveals that there is the need to direct the future research to those areas still unknown like the integration of energy efficiency and security and optimization of Internet of Things for different scenarios. It is also the simplest way to come up with new ideas of servant solutions that can respond to the new demands of Internet of Things systems.

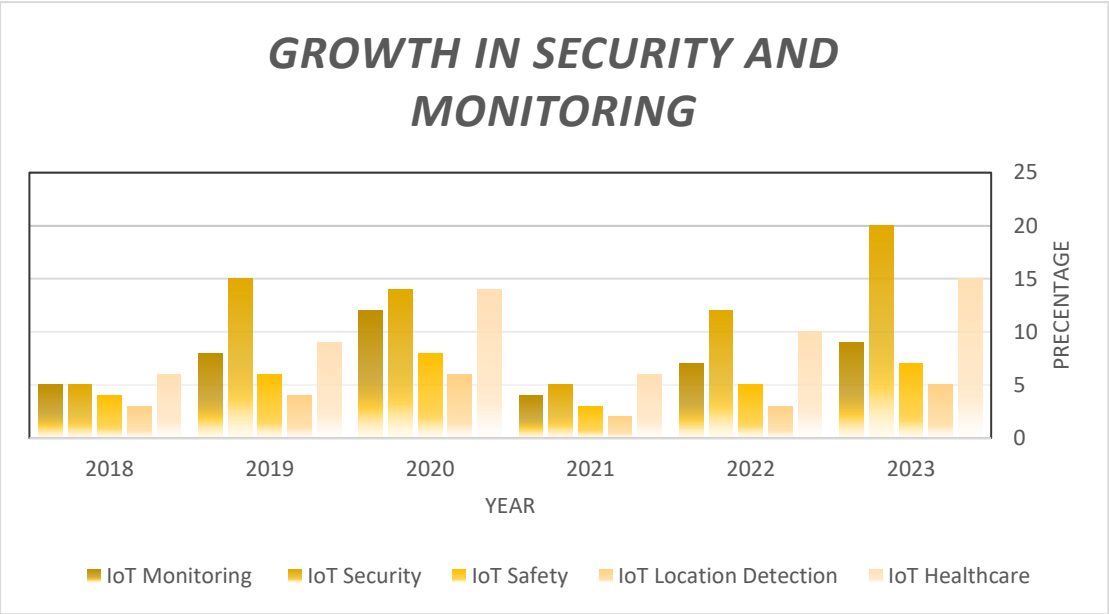

Fig5 Growth in Security and Monitoring

b. IoT Application vs. Images Processing Technique

This sort of study will focus on IoT applications that use specific kinds of image-processing algorithms: that is, which kinds of techniques for processing images are used by each type of IoT application. This demonstrates the usefulness of Techniques for processing image algorithms for specific contexts. Figures 4, 5, 6, 7, and 8 illustrate the IoT apps like safety, monitoring, security, location detection, and healthcare versus applied techniques for the processing of images algorithm.

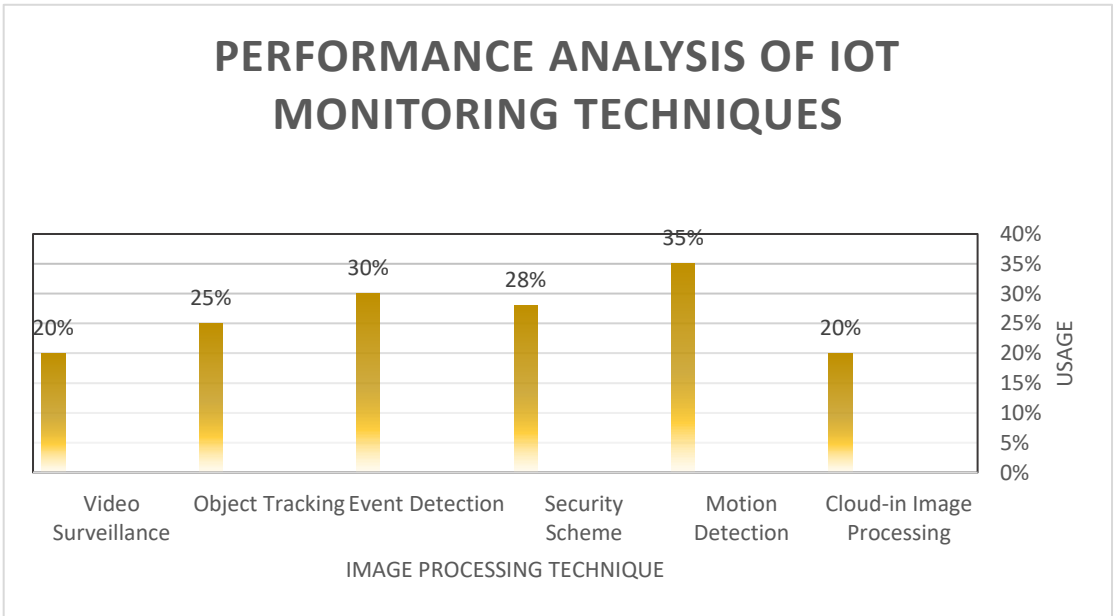

Fig6 Performance Analysis of IoT Monitoring Techniques

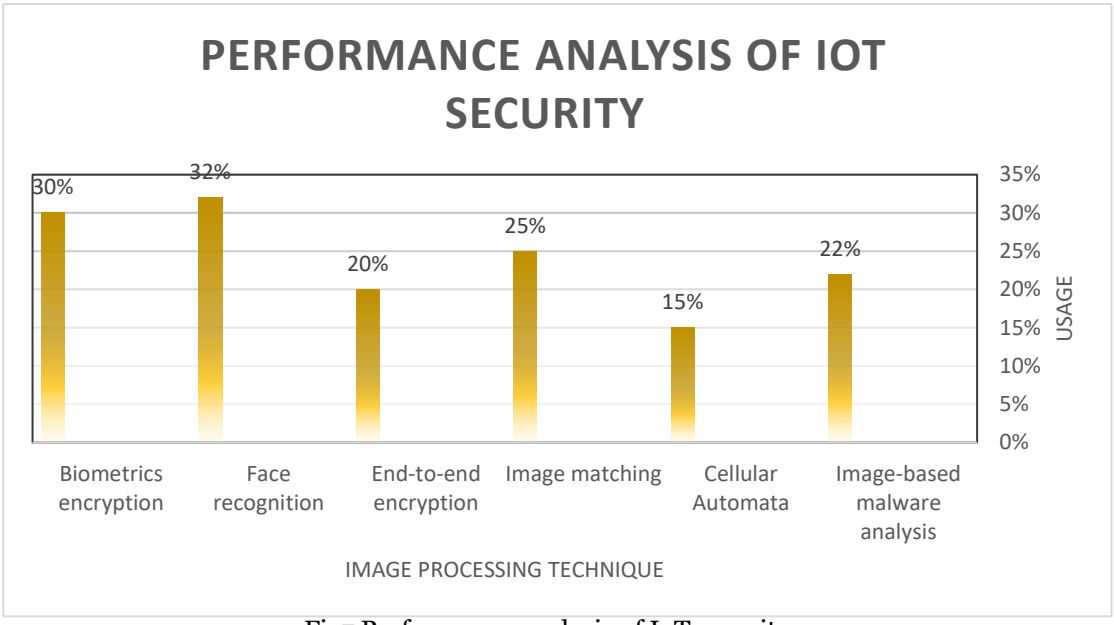

Fig7 Performance analysis of IoT security

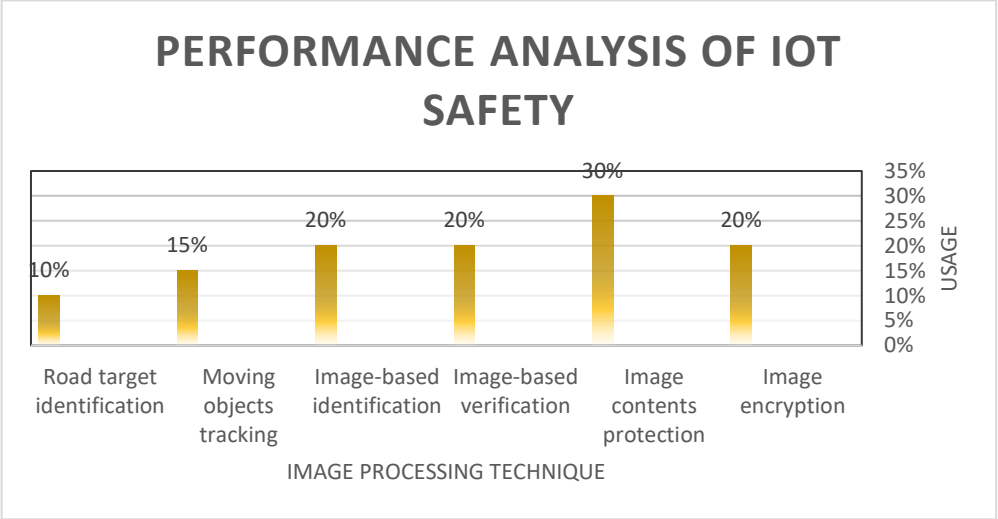

Fig8 Performance analysis of IoT safety app

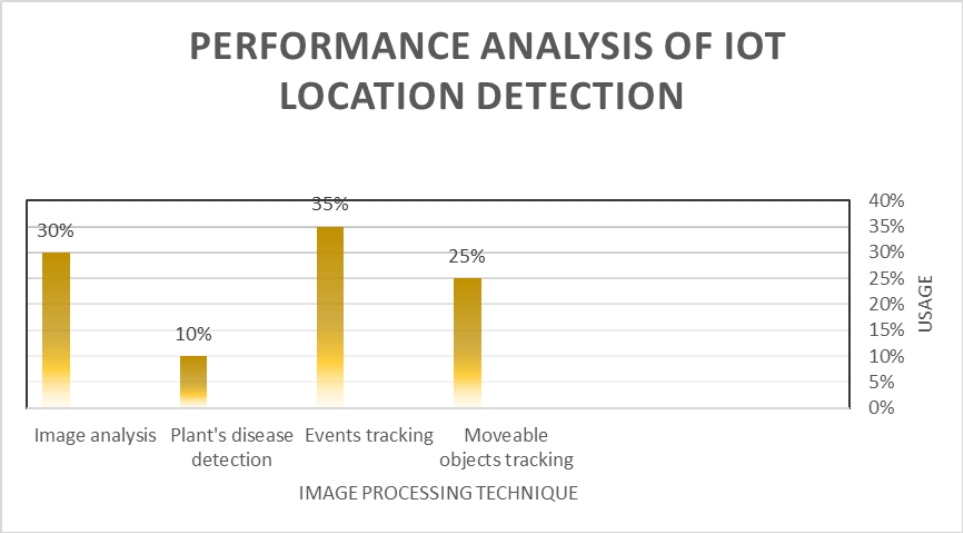

Fig9 Performance analysis of IoT Location Detection app

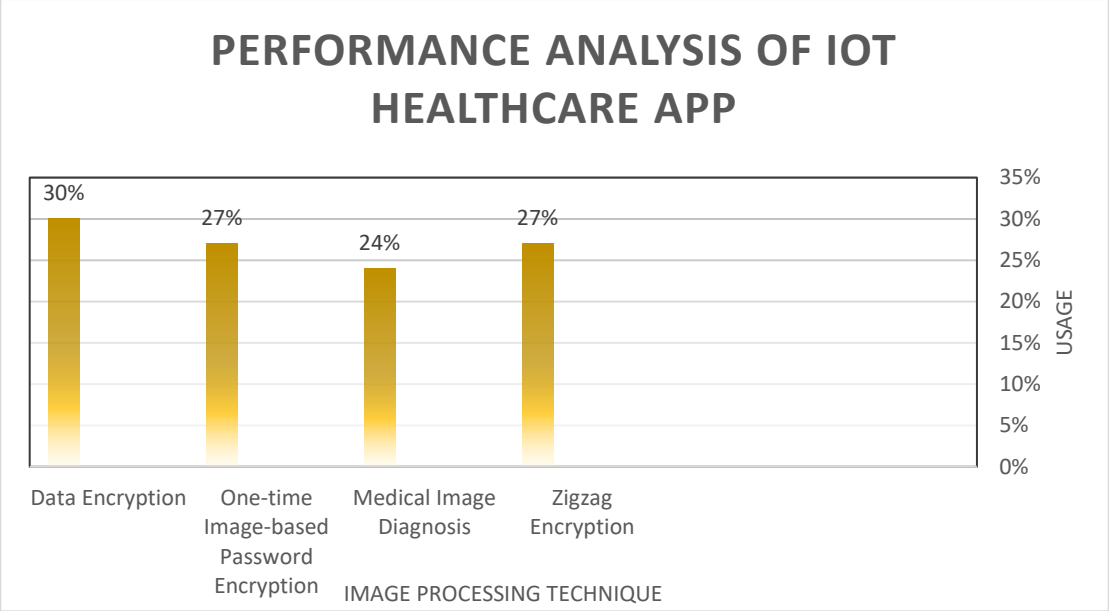

Fig10 Performance analysis of IoT healthcare app

(Figure 6 - 9), the percentage of the use of image processing techniques in various internet applications. Digital analysis shows the following:

Fig 6 (Monitoring): Data shows that 35% of applications rely on motion detection techniques to improve performance, making them the most employed tool in surveillance applications. This indicates the effectiveness of image processing techniques in reducing energy consumption and increasing the speed of data analysis in surveillance scenarios.

Fig 7 (Security): The figure shows that facial recognition techniques are used in 33% of security applications. This ratio shows the importance of this technology in improving network security and reducing security vulnerabilities, especially in sensitive locations such as smart homes and airports.

Fig 8 (Safety): The share of object tracking and target detection techniques in 28% of my safety applications. The manifestation of this ratio is far from image processing in identifying potential threats and ensuring the safety of users in industrial environments and on roads.

Fig 9 (Location Detection): 25% of positioning applications rely on image processing techniques for real-time data analysis, such as monitoring plant growth using drones or detecting agricultural diseases.

Sharing these numbers means that image processing techniques play a key role in enhancing the efficiency and accuracy of various Internet of Things applications. Monitoring and security are the most employed areas of these technologies, while security and positioning are relatively less important, but still important to achieve the goals of maintaining systems and improving performance.

4.Discussion:

The incorporation of image processing algorithms into IoT systems (IoTSs) represents a revolutionary evolution, responding to two closely related issues: innovative energy management and data protection – key concerns constituting the foundation of contemporary IoT development. These technaues revolutionalise IoTSs by allowing only image data that is necessary to be beamed to the cloud thus reducing energy usage by limiting unnecessary transfers and time taken [30,31]. As the disciplines of multi-frame image analysis and pixel intensity compression undergo constant development, these kinds of approaches lead to extraordinary levels of energy conservation while achieving the highest possible utility of the system resources without negating the efficiency of its operation [32]. In addition to it, compression algorithms designed specifically for IoTSs and the pre-transfer lightweight encryption procedure which do not demand many computational resources but help in saving both the computational capability and bandwidth in due course contributing to the sustainability in low energy domains [33].

At the same time, those techniques have transformed the approach to IoTS security architectures by adding such as block-based and zigzag encryption techniques, which are extremely effective to protect against server level attacks and data interception [34,35]. Far more revolutionary is bringing biometric encryption systems despite the fact they outcompete conventional security models, presenting unique, individual security solutions capable of adaptation in regards to appearing cyber threats [36]. Hence image matching algorithms have since been establish as vital to the security of cloud storage protocols to keep data secret and secure, to enable the recovery and transfer of data and hence tighten the security of information networks [37]. The mentioned techniques establish a synergy between energy enhancement and better security and tie between improved dependability and the addition of extra resources towards optimum energy utilization achieving a more powerful protective shield by preserving energy.

These innovations are not simply for effectiveness and protection; they point to graceful, flexible IoTSs that adequately respond to the ever-expanding connectivity and information exchange required and anticipated in the future. However, computational complexity and/or the integration with other significant network management components continue to be a problem that needs to be solved through the development of new, simple combined models with both increased computational load and flexibility [39]. They not only revolutionalise core IoT structures but also introduce new incubator paradigms of limitation and safety for sustainable IoT environments. Lastly, owing to the advanced image processing techniques, IoTSs go beyond the traditional conventional approaches, and turn into robust, green, and inherently secured systems ready for tackling the world connectivity issues [27].

5.Conclusion:

This article explored techniques to improve the energy utilization of image algorithms for higher efficiency IoT and edge computing systems applications. Methods of processing images have been useful in providing solutions in particular disciplines. To identify whether they might aid in such issues, several different image processing techniques were examined in this study for utility in creating a secure Internet of Things and low-energy-consuming system for experts in related fields. Image processing techniques may be helpful to IoTSs when applying techniques for processing images techniques. Processing techniques in image algorithms have enhanced the aspect of security and gains in the IoT framework impressively. Such methods help minimize discontinuity in the image flow between IoT devices and networks using image encryption methods and models such as the cellular automata (CAs). These strategies increase privacy by tamper proofing information that requires protection such as medical files by placing it under password protected protection through algorithms. They also help identify malware through categorizing malicious pictures and this assist in such attacks like DDoS. Image processing methods are also required in modulation and demodulation to monitor processes and secure messaging channels in edge computing cases. It encourages the use of energy efficient designs of systems through control of factors like the transfer time and bandwidth among others while guaranteeing safety of picture transfer to the cloud. The use of technologies such as quadcopters, GPS and wireless sensors enhances items identification and also enhances the assessment of the general environment. Methods of image regulating in health care help in distant evaluation, and can include a fast diagnostic test and disease prognosis based on encrypted medical images stored on cloud. However, the technique has drawback like the size of the data and specific energy usage issues are not solved, and this reveal that more research should be done.

Reference

[1] Benjamin H. Klimko, Yanne K. Chembo, "Demonstration of Reservoir Computing Using Optoelectronic Oscillators With Direct Laser Modulation", IEEE Photonics Technology Letters, vol.36, no.23, pp.1353-1356, 2024.

[2] Yuki Kubo, Masaharu Yonezawa, Hisashi Shima, Yasuhisa Naitoh, Hiroyuki Akinaga, Toshiki Nokami, Toshiyuki Itoh, Kentaro Kinoshita, "Quantitative Relationship Between Data Dimensionality and Information Processing Capability Revealed via Principal Component Analysis for Non-Linear Current Waveforms With Non-Ideality Derived From Ionic Liquid-Based Physical Reservoir Device", IEEE Access, vol.12, pp.153809-153821, 2024.

[3] Rio Nurtantyana, Wu-Yuin Hwang, Uun Hariyanti, "Education of Things (XoT): Harnessing AI and Edge Computing to Educate All Things", IEEE Access, vol.12, pp.147138-147155, 2024.

[4] H. A. Mardan and S. K. Ahmed, "Using AI in wireless communication system for resource management and optimisation," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 8, no. 4, pp. 2068–2074, 2020.

[5] S. K. Ahmed and H. A. Mardan, "Improve a technique for searching and indexing images utilizing content investigation," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 1, pp. 59–70, 2021.
[6] L. E. George and S. K. Ahmad, "Hiding image in image using iterated function system (IFS)," in *Proceedings of the European Conference of Systems, European Conference of Circuits Technology and Devices, European Conference of Communications, and European Conference on Computer Science*, Nov. 2010, pp. 68–74.
[7] 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]
[8] 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. [Google Scholar] [CrossRef]
[9] 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. [Google Scholar]
[10] 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. [Google Scholar] [CrossRef]
[11] Jacoby, M.; Usländer, T. Digital twin and internet of things—Current standards landscape. Appl. Sci. 2020, 10, 6519. [Google Scholar] [CrossRef]
[12] Gu, Z.; Li, H.; Khan, S.; Deng, L.; Du, X.; Guizani, M.; Tian, Z. IEPSBP: A cost-efficient image encryption algorithm based on the parallel chaotic system for green IoT. IEEE Trans. Green Commun. Netw. 2021, 6, 89–106. [Google Scholar] [CrossRef]
[13] 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]
[14] Hassan, A.; Liu, F.; Wang, F.; Wang, Y. Secure image classification with deep neural networks for IoT applications. J. Ambient. Intell. Humans. Comput. 2021, 12, 8319–8337. [Google Scholar] [CrossRef]
[15] 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. [Google Scholar]
[16] 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.; Acade.mic Press: Cambridge, MA, USA, 2022; pp. 123–141. [Google Scholar]
[17] 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]
[18] 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]
[19] 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. [Google Scholar]
[20] Rahmani, A.M.; Bayramov, S.; Kiani Kalejahi, B. Internet of things applications: Opportunities and threats. Wirel. Pers. Commun. 2022, 122, 451–476. [Google Scholar] [CrossRef]
[21] Esposito, M.; Palma, L.; Belli, A.; Sabbatini, L.; Pierleoni, P. Recent Advances in the 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]

[22] 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. [Google Scholar] [CrossRef]
[23] 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]
[24] 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. [Google Scholar]
[25] Smmarwar, S.K.; Gupta, G.P.; Kumar, S. Deep malware detection framework for IoT-based smart agriculture. Comput. Electr. Eng. 2022, 104, 108410. [Google Scholar] [CrossRef]
[26] 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]
[27] 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]
[28] Sharma, A.; Singh, P.K.; Kumar, Y. An integrated fire detection system using IoT and Techniques for processing imagestechnique for smart cities. Sustain. Cities Soc. 2020, 61, 102332. [Google Scholar] [CrossRef]
[29] 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]
[30] 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]
[31] 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]
[32] Dorothy, A.B.; Kumar, S.B.R.; Sharmila, J.J. IoT Based Home Security through Digital Techniques for processing imagesAlgorithms. In Proceedings of the 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, India, 2–4 February 2017; pp. 20–23. [Google Scholar] [CrossRef]
[33] 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]
[34] 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. [Google Scholar] [CrossRef]
[35] 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. [Google Scholar]
[36] Kapoor, A.; Bhat, S.I.; Shidnal, S.; Mehra, A. Implementation of IoT (Internet of Things) and Techniques for processing imagesin 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. [Google Scholar]
[37] 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. [Google Scholar]
[38] Bolhasani, H.; Mohseni, M.; Rahmani, A.M. Deep learning applications for IoT in health care: A systematic review. Inform. Med. Unlocked 2021, 23, 100550. [Google Scholar] [CrossRef]

[39] 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. [Google Scholar] [CrossRef]
[40] 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. [Google Scholar] [CrossRef].