IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 August 2023, accepted 2 September 2023, date of publication 7 September 2023,
date of current version 22 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3312682

TOPICAL REVIEW

A Review on Role of Image Processing Techniques to Enhancing Security of IoT Applications

ABBAS M. AL-GHAILI[1,2], SARASWATHY SHAMINI GUNASEKARAN[2,3], NORZIANA JAMIL[2,4], ZAID ABDI ALKAREEM ALYASSERI[2,5], NAIF MOHAMMED AL-HADA[6,7,8], ZUL-AZRI BIN IBRAHIM[1], ASMIDAR ABU BAKAR[1], HAIROLADENAN KASIM[3], EGHBAL HOSSEINI[2], RIDHA OMAR[3], RAFIZIANA MD. KASMANI[6], AND RINA AZLIN RAZALI[1,2]

[1]Department of Computing, College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), Kajang, Selangor 43000, Malaysia
[2]Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Kajang, Selangor 43000, Malaysia
[3]Department of Informatics, College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), Kajang, Selangor 43000, Malaysia
[4]Department of Information Systems and Security, College of IT, United Arab Emirates University, Al-Ain 15551, United Arab Emirates
[5]Information Technology Research and Development Center, University of Kufa, Kufa, Iraq
[6]Shandong Key Laboratory of Biophysics, Institute of Biophysics, Dezhou University, Dezhou 253023, China
[7]School of Chemical and Energy Engineering, Universiti Teknologi Malaysia, Skudai, Johor 81310, Malaysia
[8]Electronics and Communication Engineering Department, Faculty of Electrical and Electronics Engineering, Istanbul Technical University, 34467 Sarıyer, Turkey

Corresponding authors: Abbas M. Al-Ghaili (abbas@uniten.edu.my), Norziana Jamil (norziana@uaeu.ac.ae), and Naif Mohammed Al-Hada (naifalhada@yahoo.com)

This work was supported in part by the Dato' Low Tuck Kwong International Grant 20238008DLTK, in part by the Tenaga Nasional Berhad (TNB) and Universiti Tenaga Nasional (UNITEN) through the BOLD Refresh Publication Fund through the Centre of Excellence under Project J510050002-IC-6 BOLDREFRESH2025, and in part by the Tan Sri Leo Moggie Chair of Energy Informatics Publication Fund under Grant 20211EICHAIR.

ABSTRACT Once an image has been processed by, for example, a robot machine, for the purpose of, for example, features extraction or meaningful information retrieval, has a secure scheme been applied to preserve security and privacy of such information before sending it to another processing party? A huge number of image-related Internet of Things (IoT) applications face such an issue. But what are applied and potentially being applied image processing techniques that have contributed to enhance the security and privacy of IoT applications? There are numerous IoT applications that utilize image processing techniques in this direction. This article aims to survey and review a number of recently published papers and research studies that encompass proposed methods in which image processing techniques are applied to enhance the security, privacy, and safety of IoT applications. It also aims to help interested researchers in related fields have insights on what the role of image processing in enhancing the security of IoT applications is and what those techniques applied to enhance the security of IoT applications are. A comprehensive framework has been graphically extracted to give readers in the field of IoT security a map with the suitable image processing techniques that serve better to enhancing IoT applications in terms of security and privacy.

INDEX TERMS Image processing, Internet of Things (IoT), secure IoT applications, secure image-related IoT applications, energy IoT.

ABBREVIATIONS

AI	Artificial intelligence.
AOI	Areas-of-interest.
CA	Cellular Automata.
DDoS	Distributed denial of service.
DLs	Digital libraries.
DNNS	Deep neural networks.
H-IoT	Health care Internet of Things.
ID	Identification.
IIoT	Industrial Internet of Things.
IoT	Internet of Things.
MIoT	Multimedia Internet of Things.
OCR	Optical Character Recognition.
OTP	One-time password.

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

PIR	Passive infrared sensor.
RL	Reinforcement learning.
ROI	Region of interest.
SIFT	Scale-invariant feature transform.
VGG-16	Visual Geometry Group.

I. INTRODUCTION

In software that is connected to the Internet of Things (IoT), images are one of the most important components [1], [2], [3]. IoT is an ecosystem that consists of a high number of people, a big number of connected objects and connections, and a tremendous quantity of data [4], [5], [6]. Due to the fact that it is suitable for the challenges posed by ''big data'' and the future problems that it addresses, deep learning is particularly suited for these circumstances [6]. Nevertheless, ensuring both security and privacy has quickly become one of the most pressing challenges facing management of the IoT. Without relying to manually designed criteria, deep learning algorithms have been shown to be increasingly effective in a number of recent situations in the process of providing security evaluations for IoT platform and environment [7].

Technology related to the IoT is present in practically every aspect of our day-to-day lives, from the vehicles we drive to the places we reside. IoT might be used to stop the fire, identify and track goods, monitor and report changes happening in the environment, plus take images and videos in our homes [8], on roads [9], and in workplaces, to mention just a few of the many useful functions they are offered in [10]. Examples of this include the monitoring and prediction of traffic [11], as well as the classification of objects based on images gathered by the smart sensors of autonomous automobiles [12]. Image classification with the use of deep neural networks (DNNs) hosted on the cloud is one of the most exciting potential applications for IoT [13]. Despite this fact, the widespread use of ''smart'' IoT devices and applications may give rise to security problems. It still struggles to free IoT devices from severe computational restrictions, such as security and encryption of information, the extraction of features, and the categorization of images [10].

The primary purpose of this review paper is to provide an overview of many efforts that were made by earlier researchers toward enhancing IoT applications with the assistance of image processing techniques. These efforts were done over the course of several years. The provision of intelligent services to users has been the primary emphasis of many IoT applications; however, many applications do not adequately protect the users' security or privacy. This paper aims to review remaining lacks and proposed solutions to these concerns aiming to contribute to the interested researchers to find out the most suitable solutions for relevant scenarios in an attempt to improve solutions for these concerns.

A. IMAGE PROCESSING ROLE TO IoT APPLICATIONS DEVELOPMENT

The rise of successful deployment of services connected to the IoT has corresponded with the assistance of a number of different disciplines. The field of digital image processing and the many methods associated with it is one of these disciplines. The use of image processing has, for example, contributed to the improvement of the services offered by applications for the IoT [14], [15], [16], [17]. Images are becoming more popular as a result of the unique qualities and characteristics that they possess. Many IoT applications now use images as a data format to execute a variety of processes and activities. Sensors have taken images in order to, for example, monitor a faraway site or zone. These images have been recorded [18], [19].

Several further IoT applications have taken use of the image processing industry to identify still or moving objects [20], [21], [22], [23]. Following the detection of the item, a decision might be reached in accordance with the kind of IoT application being used. The object identification process is the next step after the object detection process. It is helpful for a wide variety of applications, including the recognition of text based on color [24], texture, and form attributes, among other things. The process of object recognition has also been utilized by a number of applications related to the IoT in order to provide, for instance, a remote guide and support to visually-challenged individuals once objects have been identified without the requirement of a real supporter being present [25], [26].

In these kinds of applications, a visual sensor is collecting items in front of the intended person. The captured object will be transferred to the cloud or another remote processing unit for them to make a judgment on, and then the intended person will be led [27].

Another possible scenario is that the remote assistance center will be alerted in the event that the visually impaired individual has come into contact with potentially hazardous things. The detected objects will then be transported to the appropriate location using IoT platforms [28].

The integration of image processing and the IoT has made a contribution to our way of life and improved many facets of many different industries, including healthcare [29], industry [30], technology [31], home security [32], entertainment [33], and a great many more [34], [35].

B. IoT-RELATED SECURITY CONCERN

Security of digital contents such as images is one of the issues that needs full consideration. Images-embedded information can be of high sensitivity and low sensitivity depending on the IoT applications and purpose of use [36]. Hence, lots of vulnerabilities will be an aim and searched for. The number of vulnerabilities will be of growth due to unlimited and infinite attempts of attackers and unusual threats [37].

In line with this, IoT related applications have endangered images contents and carried information to a real hazard. In some case, this hazard might be a real damage to sensitive areas or zones once contents have been unauthorized modified because such a modification action might change the decision made by the remote processing center. Suppose that, an abnormal event has happened nearby a monitored industrial zone, and the captured image that was analyzed where the detected and identified source-dangerous object is there; and the image has been unauthorized modified while it was sent, a real damage might be then caused. Therefore, there is a big need for IoT applications to work in a secure environment [38]. That could contain communication channels, layers networks, fog nodes in order to maintain images being transmitted safe and private as well as to achieve security objectives for the IoT platform [39].

This article has attempted to review a number of proposed solutions that contribute to the security of IoT related contents and towards a secure IoT environment.

C. IoT-RELATED PRIVACY CONCERN

Deep learning is a prominent application in robot systems that can learn and train the outcomes according to needs. However, the training process gathers sensitive information, which may easily lead to leaking of users' private information. To this day, there has been very little research done on deep learning models that protect users' privacy in robot systems [40].

In this day and age of the Industrial IoT (IIoT), enormous volumes of data are being produced, and businesses are under intense pressure to store the data on cloud servers so that they may save money and improve their application efficiency. Despite this, the data collected by IIoT are always quite valuable. The direct outsourcing of such data might lead to vital company information being leaked, which can result in significant financial losses for the organizations. Thus, the privacy concern is of high importance due to above mentioned reasons and considerations [41].

The issue of the privacy of digital images has been linked to many IoT applications, and one of the most important of these applications is the Internet of Medical Things applications due to the privacy of information and data available in medical images that are periodically stored to update the patient's condition. The kind of medical images and the total number of them have both greatly risen with the introduction of medical IoT devices. It is very important to be able to retrieve medical images in order to increase the effectiveness of illness diagnosis and therapy. However, this might cause people to be concerned about their privacy, given that medical images include sensitive and confidential information about patients. The currently available research on the retrieval of medical data either does not safeguard the sensitive information included in medical images or is restricted to a single image data source [42].

D. ROLE OF DEEP LEARNING IN PRIVACY-PRESERVING FOR IMAGE-BASED IoT APPLICATIONS

Deep learning algorithms, which are based on neural networks, have had a great deal of success and are currently seeing widespread use in a wide variety of application domains. These domains include image classification, automatic driving, clinical diagnosis, and intrusion detection, to name just a few [43], [44], [45], [46]. However, the privacy and security flaws of deep learning have recently come to light. It has been shown that the deep learning model may be lifted or reverse-engineered, that sensitive training data can be deduced, and that even a facial image of the victim that can be recognized can be retrieved. In addition, new research has shown that the deep learning model is susceptible to adversarial instances that are tainted by undetectable noise, which may cause the deep learning model to make incorrect predictions with a high level of confidence [47].

E. ROLE OF EDGE COMPUTING IN ENHANCING SECURITY OF IMAGE-PROCESSED IoT APPLICATIONS

In recent years, there has been a lot of focus placed on the IoT. Nevertheless, the image data that are recorded by IoT devices connected are intimately tied to the personal information of users. As such, these image data remain critical and must be secured. Even if classic privacy-preserving outsourced computing alternatives like homomorphic cryptographic primitives are able to enable privacy-preserving computing, the amount of CPU and storage resources that they need is enormous. Therefore, it places a significant pressure on IoT terminal devices, which often have very little resources [48].

Edge computing is a promising approach that, if implemented correctly, has the potential to significantly improve the data security provided by IoT applications and systems [49], [50].

F. BASIC CONTEXT OF THE EVOLUTION OF IMAGE PROCESSING TO ENHANCING SECURITY, PRIVACY, AND SAFETY OF IoT APPLICATIONS

Think about how our lives have changed because of all those smart devices around us – from smart homes to industries. This big change is called the IoT, where devices connect and share data. It's pretty cool, but it also brings some challenges. These devices are vulnerable to hackers and other threats. Our old ways of security just don't cut it anymore. This is where image processing steps in to help make things safer.

G. REASONS FOR IMAGE PROCESSING TECHNIQUES INTEGRATION IN THE FIELD OF IoT APPLICATIONS-RELATED SECURITY ENHANCEMENT

A lot of enhancement and improvement associated with security of IoT applications was made by image processing techniques integration. Reasons of this integration is to increase security. It is known, that new tricks are always changing. But image processing can change too to overcome potential treats. This makes sure our data stays safe and protected with the help of image processing techniques. Highlighted is a list of related examples that made such integration to be performed. One of them is that, image processing has helped provide better security with more or big data. IoT applications and systems make all sorts of data. Some is text, numbers, and some is images or videos. Image processing lets us analyze all these types together. It's like looking at the whole picture, which helps us catch bad stuff more accurately.

Also, image processing has locked things down with one's face. It has made unlocking a phone with one's face easier and real. It's like having a super secure lock that only opens for the authorized person. This makes sure only the right people get into those devices. Plus, one's personal data stays on the device - no need to send it to a faraway server.

Image processing techniques can hide secrets in photos. Sometimes, we need to send private stuff online. Image processing can hide it in photos. Imagine your message hidden inside a photo of your cat. Only the right person knows where to look to find the secret message. This keeps your private stuff safe from prying eyes.

It has helped catch trouble with one's eyes to increase the privacy. Imagine if your smart camera saw someone trying to mess with it. Image processing can help these cameras see and understand when something's wrong. If anyone tries to mess with your camera, you will know right away.

Besides, it can spot weird behaviors for safety. In big factories or even in cities, IoT devices are watching. They use cameras to see things. Image processing can tell when something strange happens. It's like the devices have a sixth sense and can warn us if something unsafe is going on.

Image processing also can make sense of what is around. Sometimes, IoT devices need to understand what's happening around them. Image processing helps them see and make sense of it. This is really useful for self-driving cars – they can see and avoid obstacles.

Additionally, image processing makes security and safety easier for people. We humans are good at understanding images and scenes. So, using images for security and safety makes things easier for us. We are less likely to mess up and make things unsafe when we can see what is happening.

H. CONTRIBUTIONS

This paper has covered a set of contributions, summarized as follows:

1) It reviews a number of papers and research studies that concern designing IoT applications in which image processing techniques have been utilized.
2) It highlights a number of contributions made by image processing techniques towards several issues that IoT applications usually face and find difficulties to overcome them, such as IoT data security, privacy, and safety.
3) It highlights several types of IoT applications that depend on image processing techniques e.g., image processing-based IoT monitoring applications, and image processing-based IoT security applications.
4) It reviews a number of IoT applications that depend on object detection process that is considered crucial to perform such IoT-related tasks e.g., monitoring, classification, and recognition.
5) It adopts PRISMA 2020 methodology for systematic reviews to highlight detailed steps on the papers' extraction procedure and how that has been implemented for different cascade-step phases.
6) It supports the explanation with graphical representation(s) for a more clarification.
7) It adds to results obtained from reviewed literature a set of illustrations and graphical representations to make the paper easily understandable.
8) It discusses the role of image processing techniques in the direction of construction a secure IoT application.
9) It discusses the role of edge computing towards data security of IoT applications.
10) It gives readers a number of important future trends that need to be considered by potentially interested researchers and designers.
11) It analyzes the obtained results according to the research questions arisen from this review.
12) It highlights a number of key contributions of employing image processing techniques in IoT applications.
13) It suggests a framework and mapping road for the future trends of suitability of applying an image processing technique to the purpose of addressing an issue faced by an IoT application (Figure 8). Both techniques (as solutions) and IoT-related issues (as concerns) are highlighted using simple graphing shapes to make the framework easily understandable to readers and applicable by interested researchers, designers, and developers.

I. ARTICLE ORGANIZATION

Sections and sub-sections of this article's organization could be shown in a graphical representation as illustrated in Figure 1.

II. RESEARCH DESIGN

The purpose of this article is to provide readers with additional clarification that may assist them in differentiating between the scopes of the current papers and the scope of this review paper by providing a summarized overview regarding the concerns raised in the currently published review papers. This is detailed in the first sub-section that follows. Research topics that have been emphasized in the currently published reviews from literature will be highlighted as well. Research questions are mentioned in the third sub-section. Finally, research objectives will be listed.

A. CURRENT PUBLISHED REVIEW ARTICLES

Table 1 provides a summary of the most important elements with relation to the scopes and focuses of the most recent review publications. In addition to that, areas that are being addressed by recent review articles have been mentioned.

B. RESEARCH QUESTIONS

There are two main research questions for this review article, highlighted as follows:

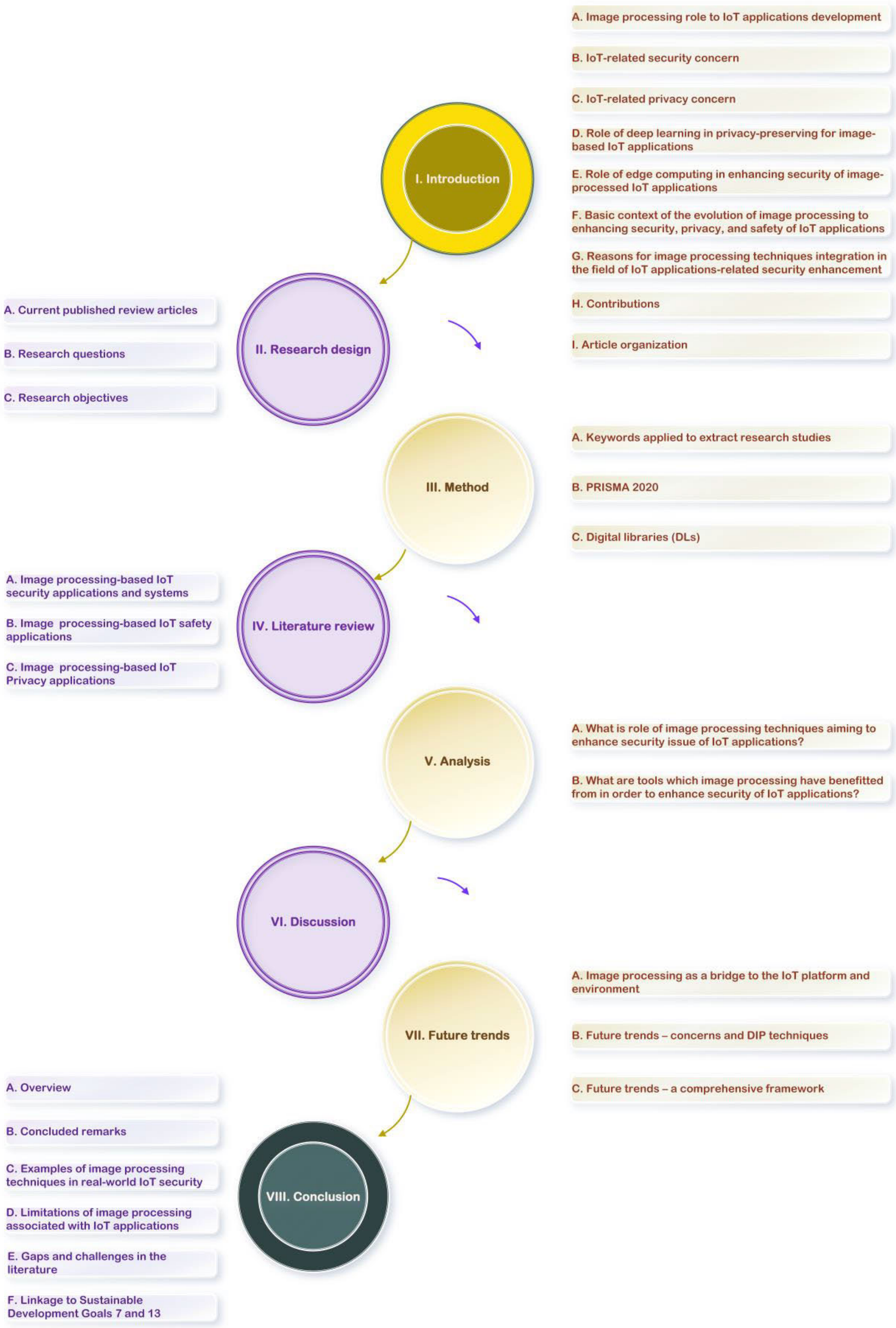

I. Introduction
A. Image processing role to IoT applications development
B. IoT-related security concern
C. IoT-related privacy concern
D. Role of deep learning in privacy-preserving for image-based IoT applications
E. Role of edge computing in enhancing security of image-processed IoT applications
F. Basic context of the evolution of image processing to enhancing security, privacy, and safety of IoT applications
G. Reasons for image processing techniques integration in the field of IoT applications-related security enhancement
H. Contributions
I. Article organization
II. Research design
A. Current published review articles
B. Research questions
C. Research objectives
III. Method
A. Keywords applied to extract research studies
B. PRISMA 2020
C. Digital libraries (DLs)
IV. Literature review
A. Image processing-based IoT security applications and systems
B. Image processing-based IoT safety applications
C. Image processing-based IoT Privacy applications
V. Analysis
A. What is role of image processing techniques aiming to enhance security issue of IoT applications?
B. What are tools which image processing have benefitted from in order to enhance security of IoT applications?
VI. Discussion
VII. Future trends
A. Image processing as a bridge to the IoT platform and environment
B. Future trends – concerns and DIP techniques
C. Future trends – a comprehensive framework
VIII. Conclusion
A. Overview
B. Concluded remarks
C. Examples of image processing techniques in real-world IoT security
D. Limitations of image processing associated with IoT applications
E. Gaps and challenges in the literature
F. Linkage to Sustainable Development Goals 7 and 13

FIGURE 1. Article's organization.

TABLE 1. A number of current review papers, focus, scope, field, and other issues.

Ref.	Focus and scope	Field covered	Other issues included
[51]	The review considers multimedia such as images and video that shifted the IoT to Multimedia Internet of Things (MIoT).	M-IoT applications related to road traffic management, security, industry, and health	Storage memory, and data size
[52]	It covers the machine learning methods and algorithms assigned to Healthcare Internet of Things (H-IoT).	H-IoT	Smart health, machine learning for H-IoT applications, security related to H-IoT applications
[53]	The review has mainly surveyed computer vision methods applied to network security.	Image processing for security purposes applied to IoT devices	Biometrics security with image processing techniques e.g., face, iris, and fingerprint recognition
[47]	The survey paper has introduced a number of types of attacks and privacy-preserving techniques in deep learning.	Attack and defense methods associated with deep learning privacy and security.	adversarial attacks under the physical condition have been reviewed.
This review	It 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 devices safety, contents security, location detection applications in the era of IoT.	Image processing techniques applied for IoT applications applied to perform security related to internet-based digital contents, monitoring of certain objects, remotely-detected location, and few others.	monitoring, privacy, safety, and security- related IoT applications for multi elements in our environment such as human, products, and few others.

RQ1. What is role of image processing techniques aiming to enhance security issue of IoT applications?

RQ2. What are tools which image processing have benefitted from in order to enhance security of IoT applications?

This article makes an effort to respond to each of these research questions by providing a detailed discussion on the primary topic. This is accomplished by trying to analyze and investigating tens of related research articles that have been published within the past few years. This is done to cover a broader variety of research studies and applications in the age of the IoT.

C. RESEARCH OBJECTIVES

Objectives of this review article can be described as follows:

1. This article tries to analyze and investigate a number of related research articles covering a broader variety of research studies and applications in the IoT age.
2. It also aims to review proposed methods in which image processing techniques are applied to enhance the security, privacy, and safety of IoT applications.
3. It aims to highlight what role(s) of image processing techniques to enhancing security of IoT applications are.
4. It aims to highlight what those techniques applied to enhance security of IoT applications are.

III. METHOD

This part is broken up into three sub-sections, each of which focuses on a different aspect of the primary technique that was used throughout the selection process of the articles that were evaluated. The primary strategy is broken down into three subsections, the first of which explains the keywords that were used to extract papers and articles from a number of DLs, the second of which discusses the criteria that were applied to the age of papers that were reviewed, and the third of which lists a number of publishers along with the relative DLs from which papers were extracted.

A. KEYWORDS APPLIED TO EXTRACT RESEARCH STUDIES

''Image processing'', ''Internet of things'', ''image processing based IoT security applications'', ''image processing'', ''image-processed safety IoT'', and ''image processing-based private IoT applications'' are some of the keywords that have been used to extract research studies and publications from the DLs.

B. PRISMA 2020

PRISMA 2020, a methodology designed specifically for systematic reviews, has been used in this particular study. Figure 2 depicts the method in all of its granularity.

C. DIGITAL LIBRARIES (DLs)

The following is a list of some of the publications that were taken into consideration for this review: In addition, the indexing services of the associated journals that all of the reviewed articles in this publication are a part of have been brought to your attention here. Figure 3 illustrates the distribution of papers according to the DLs from which the papers are taken.

IV. LITERATURE REVIEW

We take a look at a variety of apps that have been put into use in an IoT and smart city setting and have used image processing methods. There are three main topics are considered in this review paper which are security, safety, and privacy issues for image-related IoT applications.

A. IMAGE PROCESSING-BASED IoT SECURITY APPLICATIONS AND SYSTEMS

Images have been exploited to secure and protect other related data while, for example, transferring data via IoT platforms utilizing cloud storage and communication networks. Through this transferring, data is in a non-secure medium, images have been used in such a way they should have protected data through this journey until it arrives to

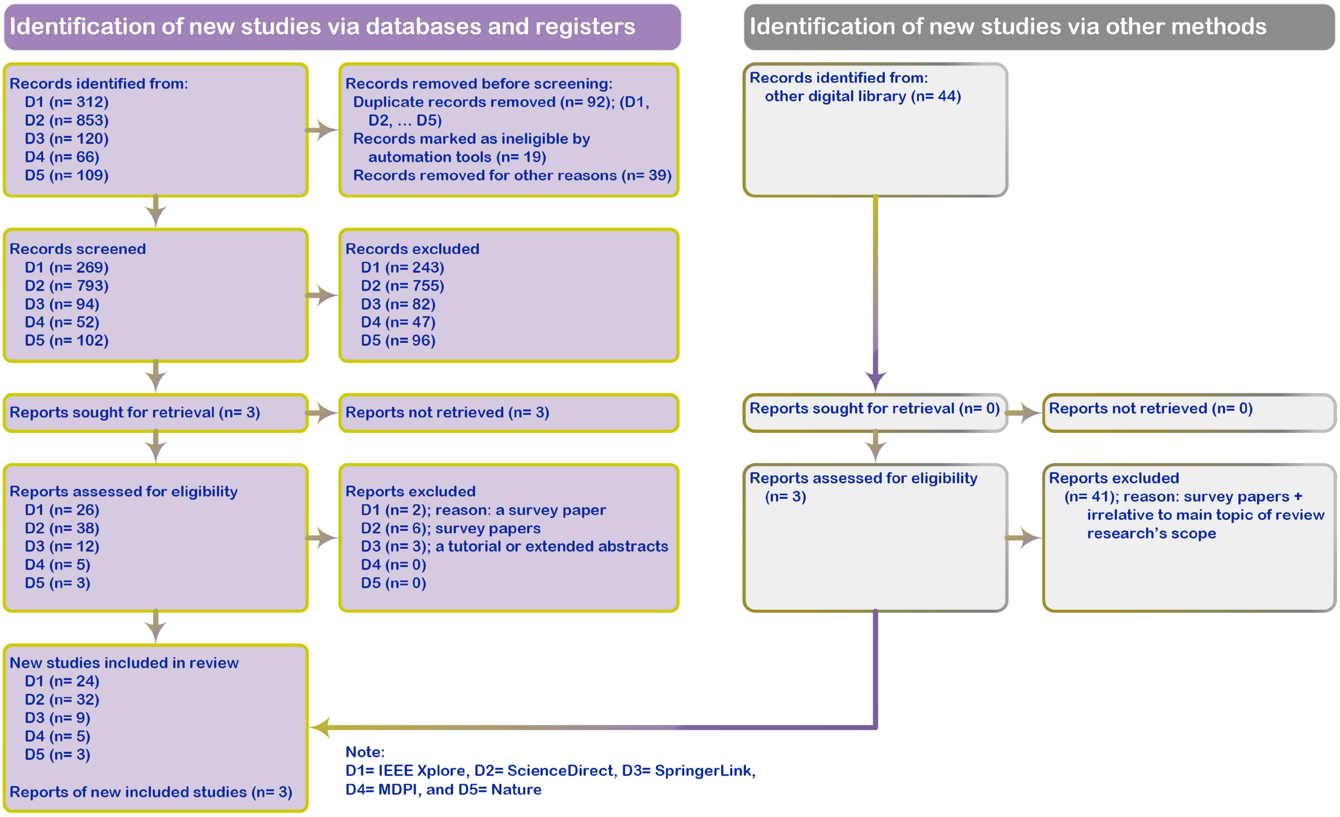

Identification of new studies via databases and registers
Identification of new studies via other methods
Records identified from:
D1 (n= 312)
D2 (n= 853)
D3 (n= 120)
D4 (n= 66)
D5 (n= 109)
Records removed before screening:
Duplicate records removed (n= 92); (D1, D2, … D5)
Records marked as ineligible by automation tools (n= 19)
Records removed for other reasons (n= 39)
Records identified from:
other digital library (n= 44)
Records screened
D1 (n= 269)
D2 (n= 793)
D3 (n= 94)
D4 (n= 52)
D5 (n= 102)
Records excluded
D1 (n= 243)
D2 (n= 755)
D3 (n= 82)
D4 (n= 47)
D5 (n= 96)
Reports sought for retrieval (n= 3)
Reports not retrieved (n= 3)
Reports sought for retrieval (n= 0)
Reports not retrieved (n= 0)
Reports assessed for eligibility
D1 (n= 26)
D2 (n= 38)
D3 (n= 12)
D4 (n= 5)
D5 (n= 3)
Reports excluded
D1 (n= 2); reason: a survey paper
D2 (n= 6); survey papers
D3 (n= 3); a tutorial or extended abstracts
D4 (n= 0)
D5 (n= 0)
Reports assessed for eligibility
(n= 3)
Reports excluded
(n= 41); reason: survey papers + irrelative to main topic of review research's scope
New studies included in review
D1 (n= 24)
D2 (n= 32)
D3 (n= 9)
D4 (n= 5)
D5 (n= 3)
Reports of new included studies (n= 3)
Note:
D1= IEEE Xplore, D2= ScienceDirect, D3= SpringerLink, D4= MDPI, and D5= Nature

FIGURE 2. Statistics related to the PRISMA 2020 methodology for systematic reviews.

destination safely. What digital image processing techniques have contributed to IoT applications for security purposes will be highlighted.

In this subsection, we survey a number of researches reviewed in literature in which image processing techniques are contributing to secure data and other digital contents while being transferred between IoT parties. The general architecture for IoT security applications is depicted and shown in Figure 4.

The proposed system in [54] has replaced the currently being used techniques for securing transferred data between IoT applications and parties including communication networks and devices, by proposing a biometrics- and pairing-based encryption solution. It is said that this technique is stronger against vulnerabilities than other techniques such as password-based authentication due to the unique features the biometrics-based techniques have.

The proposed solution is supported with case study performing face recognition process utilizing relevant biometrics' features. Prior to the face recognition process, the face image has been captured by a certain sensor installed on an IoT-connected device such as a smartphone. The proposed system will transmit the captured image via communication network to the destination utilizing IoT platform. An end-to-end encryption with the help of image processing techniques might be achieved.

Image processing techniques have been used in order to perform a security task for an IoT-based home control system [55]. The main aim of the proposed system is to perform a security task to the home via IoT platform by capturing an image at the location the camera-embedded system is installed in. The role of image processing is to perform a number of image processes such as image preprocessing, analysis, and matching between the captured image and the database-stored image. The system alerts the owner of the home if there is a mismatch by sending an IoT-based message.

Image processing has been used to carry out an image encryption with the help of Cellular Automata (CA). Values representing pixel intensities (elements of an image) are converted into a group of 8-bit string series. These values are mixed with CA rules. The authors in [56], have highlighted that the camera, firstly, captures an image to be encrypted at the perception layer, it is supposed that these images contain sensitive contents.

Therefore, they are encrypted at this layer. Secondly, those images will be sent to network layers. They will be decrypted at this stage. This security scheme has been applied on sensitive images to ensure a secure path between the network and perception layers. Since, the fog nodes are deployed at the network layer. At this stage, fog nodes are responsible to, send received images to the cloud for other processing upon necessity.

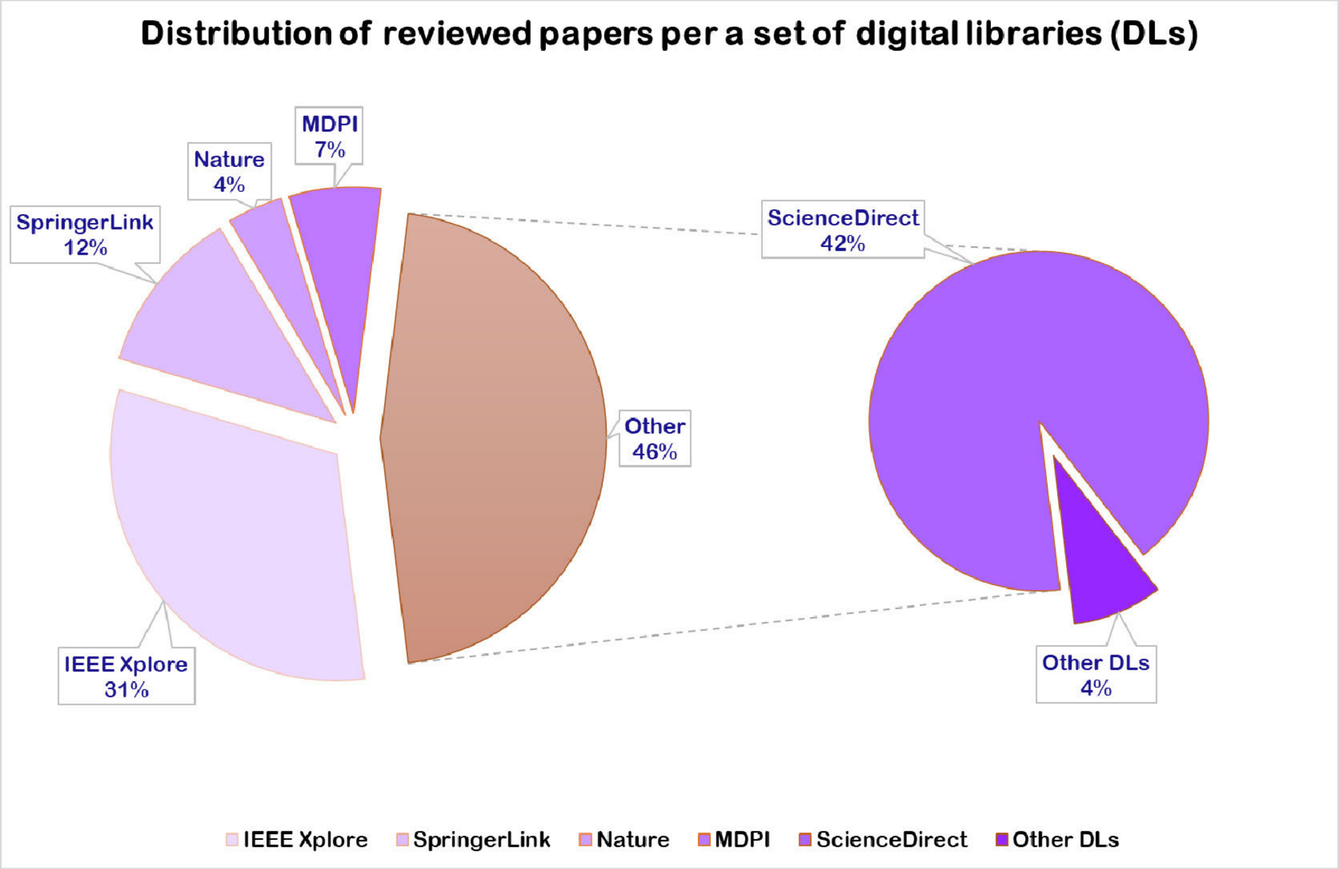


FIGURE 3. Distribution, [%], of reviewed papers per DLs.

Image encryption has been used widely and increasingly in recent times due to the huge amount of information as images sent via cloud whereby a lot of IoT applications perform this transmission. Therefore, image-based encryption is still of improvement to serve better and contribute towards this direction [57]. The image needs to be encrypted to ensure a secure public channel between the image capturing source through which image is sent to the other destination which is the fog node. An interesting encryption scheme is that both pixels' intensities and CA-generated values are combined together.

Security of IoT devices has utilized the image processing by classifying a distributed denial of service (DDoS) malware attacks. Gray-scale images can be classified according to the families, firstly. Secondly, DDoS malware attacks can be detected. Additional security scheme can be achieved then with the help of image processing techniques [58].

For security purposes, face recognition process is needed. Many IoT applications have utilized this feature for varied uses. Face recognition can be used with smart home for many purposes such as control and security. Other applications are dedicated to perform face recognition for the purpose of crowd monitoring in certain areas and zones such as airports [59].

Another security IoT application utilizing image processing can be reviewed in [10]. An indistinguishable plaintext attack-protected image classification framework for IoT applications is proposed and implemented in [10]. An IoT device is not required to constantly communicate with the cloud-based image categorization system. Using DNNs, a mechanism for the safe evaluation of linear functions has been proposed, such as divide-and-conquer and a set of unified ideal protocols, as well as for the secure evaluation of non-linear functions.

The lattice-based homomorphic approach and 2-PC secure computation algorithms ensure that the image contents, the private DNNs model parameters, and the intermediate outputs are kept secret. Visual Geometry Group (VGG-16) pre-trained deep convolutional neural network model is used to extract deep features from an image. The proposed framework has been shown to be accurate and efficient in a wide range of experiments. The white-box membership inference attack, often considered the most powerful attack against DNN models, is another way that the framework's security is

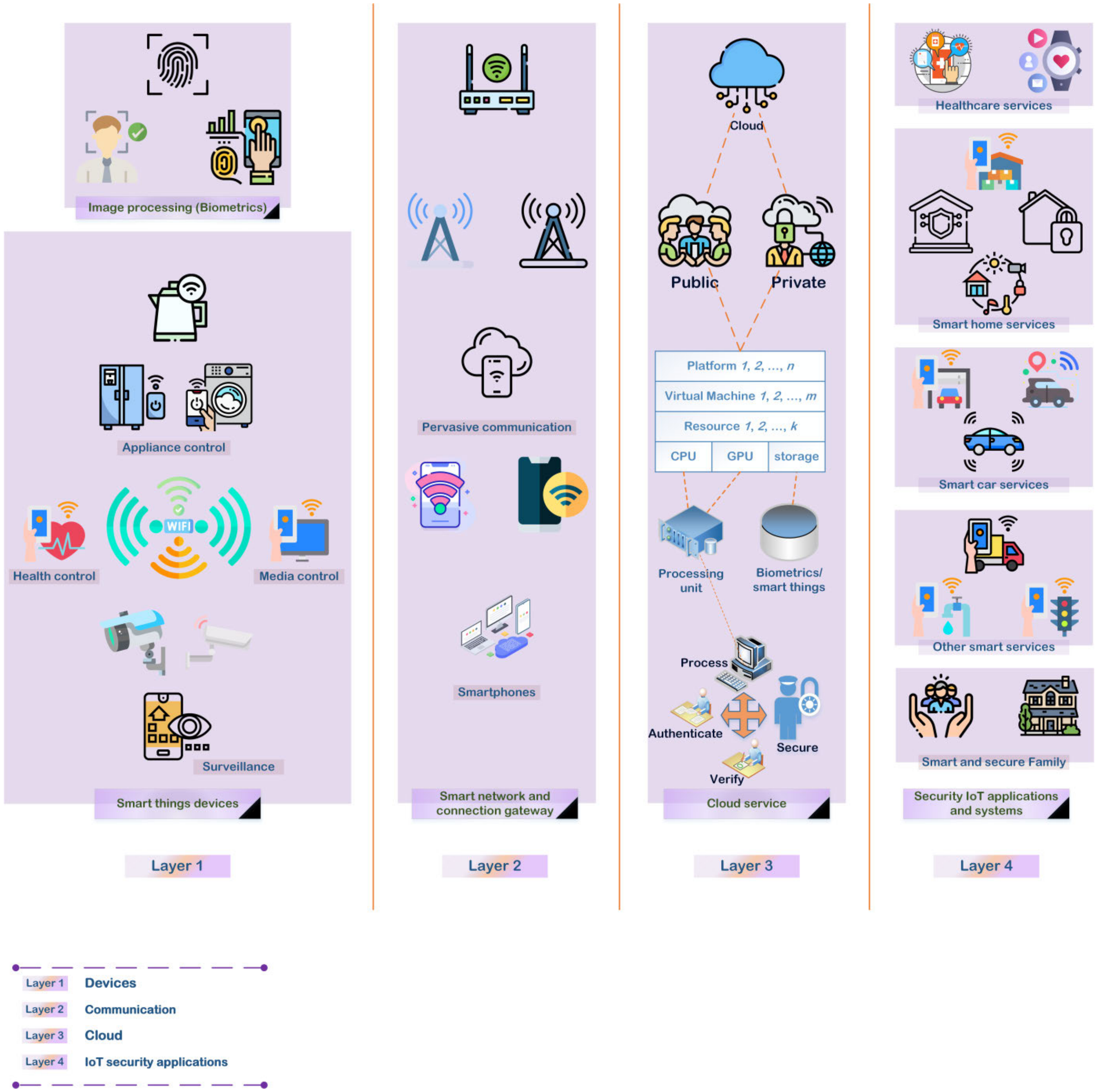


FIGURE 4. Image processing-based IoT security applications and systems: A graphical conception. Images are licensed. Design done by authors. A number of parts of this illustration has been derived from [54].

tested. The failure of the attack demonstrates that this system is practical secure [10].

B. IMAGE PROCESSING-BASED IoT SAFETY APPLICATIONS

Different needs have come out with purposes from using image processing in the field of smart city and IoT applications. One interesting application has exploited image processing with the purpose of safety of people on roads by applying detection and recognition of road target(s). Meaning, the proposed algorithm presented in [60] has applied a fusion-based recognition process of interested objects placed on roads such as harm and harmless objects.

Once the object recognition has been applied and successfully been performed, an artificial intelligence (AI)-based reinforcement learning (RL) algorithm is used to transfer this information to a robot or wearable device so that the user can understand and/ or interact with that device in order to make a decision based on.

Safety is a real matter to human being and therefore it has been assigned a big quota for vision-impaired people. A graphical representation highlighting a generalized conception of IoT safety and privacy applications and systems and how they interact with image processing is illustrated in Figure 5.

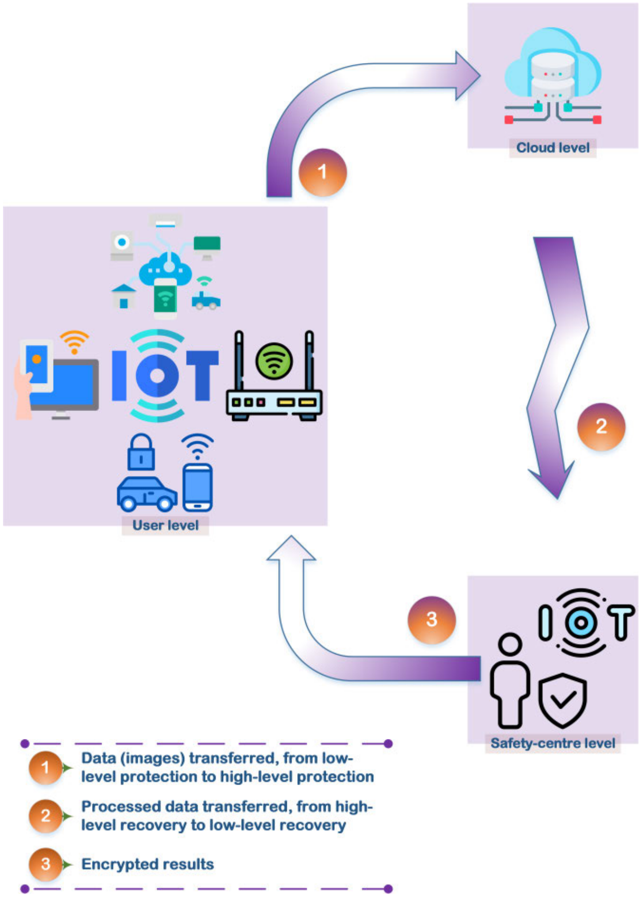

Cloud level
1
IOT
User level
2
3
Safety-centre level
IOT
1 Data (images) transferred, from low-level protection to high-level protection
2 Processed data transferred, from high-level recovery to low-level recovery
3 Encrypted results

FIGURE 5. Image processing-based encryption for IoT safety applications and systems: A graphical representation. Images are licensed. Design done by authors. Selected parts in this figure have been derived from [48].

For example, an Optical Character Recognition (OCR)-based smart assistance system using face detection is proposed [61]. The proposed system mainly depends on captured images and recorded video for objects detected and recognized by the system so that the visually-challenged person will be supported and guided once objects have been identified without the need for a real supporter.

The proposed system has ability to share locations, listen to audio received from the system after translation a text during the pre-defined read mode, and capture multi frame images.

Additionally, using the OCR, the built-in camera captures a book's page, translates it, and then recognizes its writings so that the user will be able to listen to translated texts as an audio format by auto reading. This is a feature allowing visually-impaired humans virtually read books.

Safety of valuable and digital assets such as workplace are considered to have sensitive data. By protecting them, more privacy of the relevant contents should have achieved. Protecting these places requires, for example, a security scheme for the door by locking and unlocking it via an IoT application [62]. Therefore, to allow a securely authorized access to that workplace, there should be a verification of the identification (ID) of the person who is aiming to access. A face-based matching process will be required to achieve such a security goal. The proposed IoT application, will apply an image analysis process to the captured image of a person's face and then it applies a matching process with the prestored images in the database. If the face is recognized correctly, an authorized access can be allowed. Then, a privacy purpose in regard to the digital assets and contents will be achieved. For more security, an email is sent to notify the person who is allowing such an access to happen.

Recent years have seen a rise in interest in the IoT. IoT terminal devices, on the other hand, collect images that are intimately linked to users' personal information, which is sensitive and has to be secured. Homomorphic encryption primitives, for example, may facilitate privacy-preserving outsourced computing, but they take a lot of CPU and storage resources. Because of this, IoT terminals with limited resources are put to the test. An edge-assisted privacy-preserving outsourced computing architecture for image processing is proposed, including image retrieval and classification, in order to decrease the resource consumption of the terminal device.

A semi-trusted cloud server is supported by edge nodes that work with the terminal device to secure data and provide privacy-preserving computing in the cloud. Using [48], image retrieval and classification methods that use edge-assisted privacy preservation are proposed. IoT terminal devices' computing, communication, and storage burdens may be significantly reduced by the suggested approaches, according to the security analysis and performance assessment.

Another image processing based contents safety has been proposed by [63]. In this proposed IoT system, once the image has been captured, a cryptographic scheme has been applied. Then, it was sent to another server. Then, another security scheme has also been applied to the cryptographic image; that is a cover image security scheme. The cryptographic image then will be embedded in a cover image. Finally, the cover image is sent via the IoT platform to be stored in the cloud.

Other examples that utilized image processing techniques for the IoT applications and platform can help in industrial monitoring for the purpose of machine safety and industries' environment monitoring [18], help in agriculture industry for the purpose of plants growth monitoring for better safety of such a process [64], or help to detect a location of the illness on plants [65].

In [18], the input image has been gone through the feature extraction in order to apply the objects' detection process later on. The original image will be re-presented in order to verify its consistency the image's scale space and scale invariance. Then, spatial filters are applied such as Difference of Gaussians in order to detect edges as well as to find interested points from the original image. After that, by computing the maximum and minimum values from the previous step related to the Difference of Gaussians, interested points will then be identified. Interested points that have edges or low contrast regions will then be recognized and removed. After that, orientation of the interested points will be calculated and then the rotation for those points will be invariant. Finally, the use of scale and rotation invariance in place will allow for the generation of another representation for the feature generation based on the scale-invariant feature transform (SIFT). This will allow to identify the features in the image in a unique way.

In [64], images have been acquired; then it has been converted to a gray-scale image; after that, it has been binarized by converting its values to only white and black correspondences by applying a thresholding technique; next, small objects that don not belong to the Region of interest (ROI) have been removed. The ROI has been identified from the binarized image. The last step applied was to compute the ROI's area.

In [65], there will be a camera that is connected to a PC, then captured images will be gathered in order to be processed. Then, illness location existed in a very small area on the plants will be detected by increasing the lucidity of the captured processed image where the *k*-implies grouping is highlighted.

C. IMAGE PROCESSING-BASED IoT PRIVACY APPLICATIONS

The issue of privacy leakage caused by deep learning in robot systems has been addressed by the presentation of a unique privacy-preserving image classification deep learning model. This will help to fill the vacuum in research on the privacy implications of deep learning in robotics. To enhance the effectiveness of the training process and make use of deep learning, two methodologies have been proposed. These methodologies use encrypted activation and cost functions, along with secure calculation protocols. These methodologies are then implemented in a fog control center with an honest server using homomorphic encryption. This might also assist address the encryption computation concerns and preserve the privacy of data and models in robot systems. The results of the performance assessment and security analysis show that the suggested methods provide the desired levels of security, accuracy, and efficiency while maintaining minimal levels of both communication and computing overhead [40].

In the IIoT age, enterprises are driven to store data on cloud servers for cost savings and efficient application. IIoT data are always valuable. Direct outsourcing might leak crucial company data and create economic losses. Before outsourcing, it is a good idea to encrypt the data using one of the basic encryption techniques. This is an easy approach. Despite this, the consumption of data will become extremely cumbersome as a result of this. The safe storage of image data on cloud servers is the primary subject of this research article. images are saved in an encrypted format on cloud servers, and the local binary pattern feature may be immediately retrieved from encrypted images for use in programs. The encrypted images are also kept in the cloud. Both the security analysis and the experimental results reveal that our approach is both secure and effective [41]. A graphical conception of privacy for image-related IoT applications has been shown in Figure 6.

A blockchain-based system for the recovery of medical images that also provides protection for users' privacy has been presented in this article. In the first part of [42], the common circumstances surrounding the recovery of medical images are discussed. After that, a synopsis of the appropriate requirements for the system design is presented. In this section, researchers show the layered architecture and threat model of the proposed system by making use of the upcoming blockchain methods. A carefully picked feature vector is extracted from each medical image, and a bespoke transaction structure is built, in order to make room for large-sized image with storage-constrained blocks. This is done in order to accommodate the images. This ensures that the privacy of medical images and image characteristics is maintained [42].

An edge-assisted privacy-preserving outsourced computing architecture for image processing has been proposed as a means of cutting down on the amount of resources that terminal devices are required to use. Image retrieval and categorization have been components of this process. Together with the terminal device, the edge nodes work to provide data protection and support for computing that is sensitive to the user's privacy on the nearly fully trusted cloud server. In [48], researchers offer edge-assisted privacy-preserving image classification algorithms that function inside this context. Specifically, they focus on image retrieval. The security analysis and performance assessment both reveal that the proposed schemes significantly decrease the load placed on IoT terminal devices in the areas of computing, communication, and storage while simultaneously maintaining the safety of data of image.

V. ANALYSIS

In this section, there are two types of analysis. They both consider to provide an analysis of the reviewed papers according to the said research questions.

A. WHAT IS ROLE OF IMAGE PROCESSING TECHNIQUES AIMING TO ENHANCE SECURITY ISSUE OF IoT APPLICATIONS?

1) COMMUNICATION CHANNELS SECURITY

Image processing has considered the security of the communication channel between the source of image processing and the destination by proposing different techniques. Mentioned are roles of image processing techniques to improving communications channels security:

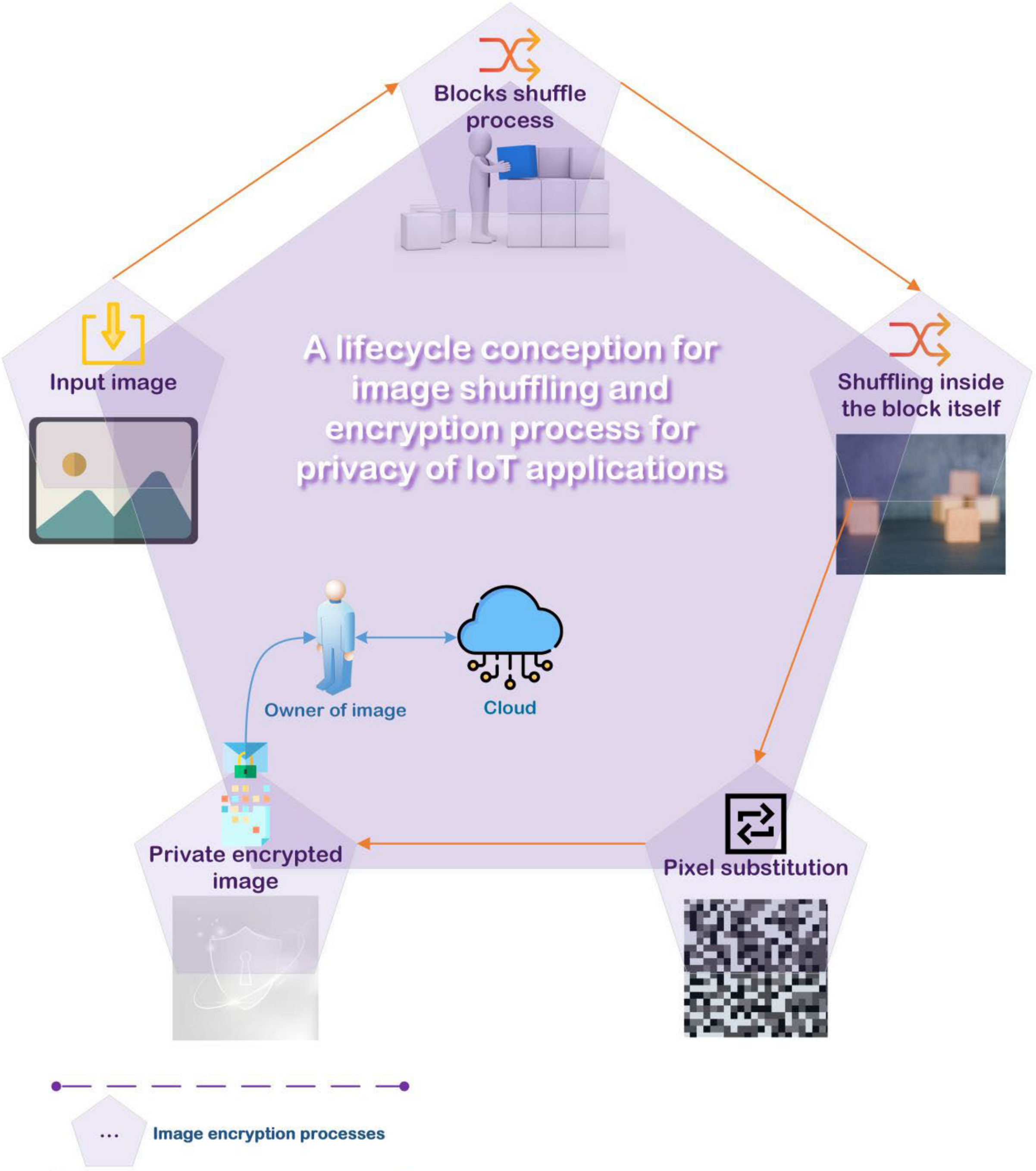

Blocks shuffle process
Input image
A lifecycle conception for image shuffling and encryption process for privacy of IoT applications
Shuffling inside the block itself
Owner of image
Cloud
Private encrypted image
Pixel substitution
...
Image encryption processes

FIGURE 6. Privacy conception for image-related IoT applications. Images are licensed. Design done by authors. Conception highlighted in this illustration is partially retrieved from [41].

1. Images matching process has been used with in-cloud-stored images where it has shown success with security of data storage and communication networks. It has contributed to the safety and privacy of the recalled in-cloud-stored image. Matching process has contributed to security of communication [55].
2. Image encryption has been associated with image transferring to cloud storage by several IoT applications. communication channel's security have been enhanced in term of security [57].

2) CONTENT's SECURITY

Image processing techniques have contributed much to increase the security of contents and channels needed for transmission. We review a number of mechanisms that image

TABLE 2. A summary of roles of image processing techniques towards addressing privacy, safety, and security issues.

No.	Role of image processing towards addressing privacy, safety, and security issues			Ref.
1.	**Privacy issue**	To allow the privacy of image's contents, there must be an authentication and verification procedure by another party, it could be, for example, the owner of the digital asset.		[62]
2.	**Safety issue**	For the safety of visually challenged persons, captured images and recorded video for objects detected and recognized by an IoT application will be a helpful tool to the visually-challenged person – to be supported and guided once objects have been identified. Safety of valuable and digital assets e.g., workplace is considered to have sensitive data. By protecting them, more privacy of the relevant contents should have achieved. Protecting these places requires, for example, a security scheme for the door by locking and unlocking it via an IoT application.		[61, 62]
3.	**Security issue**	**Communication channels security**	Images matching process and image encryption have been applied.	[55, 57]
		Content's security	Zigzag image encryption approach, biometric-based encryption system, a division process of an image into blocks, image encryption, and matching process have been utilized.	[54, 55, 57, 66, 67]

processing techniques have helped to produce in order to increase the security of the IoT applications.

1. Zigzag image encryption approach can be more resistant to data threats [66].
2. IoT devices and networks may now safely transport data because of advances in image processing techniques. A biometric encryption system utilizing image processing has been proposed to replace the present conventional security strategy, notably the two-step authentication process [54].
3. A division process of an image into blocks contributes to security achievement specifically for those IoT applications that might be vulnerable to attacks at the server level once they are stored. By dividing the secret image into blocks, the safety of the contents will be increased the attacking probability is being reduced [67].
4. Image encryption could lead to enhance security of image contents safety. However, this process is still in improvement to increase the performance of privacy of images' contents related to the IoT applications [57].
5. Matching process has contributed to safety of image contents related to the IoT applications [55].

In Table 2, a list of issues that image processing techniques have played an indispensable role to enhance security, privacy, and safety of IoT applications.

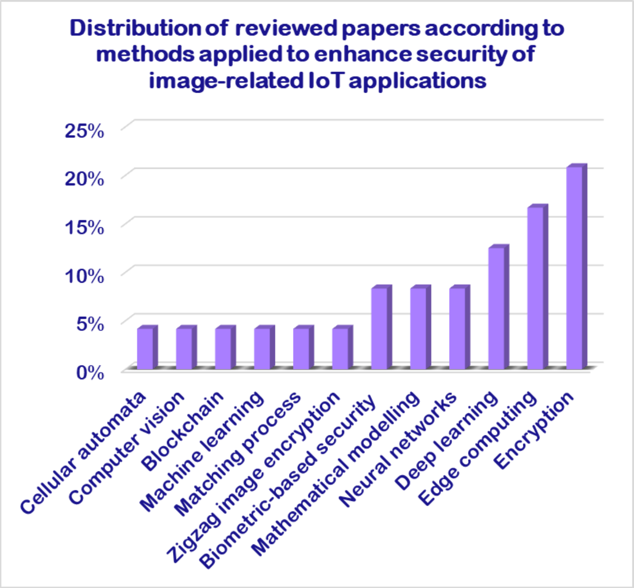


FIGURE 7. Distribution, [%], of analyzed papers according to techniques and methods applied to enhance security of image-related IoT applications.

B. WHAT ARE TOOLS WHICH IMAGE PROCESSING HAVE BENEFITTED FROM IN ORDER TO ENHANCE SECURITY OF IoT APPLICATIONS?

According to the reviewed papers, the analysis performed in this phase has surveyed and deeply focused on the other technologies and methods applied alongside image processing techniques to enhance the security of image-related IoT applications. This analysis does not concern the image being encrypted as a whole piece but instead it concerns how such an image processing technique has been applied to serve to the security of the image itself. For example, using a zigzag method by an IoT application applied to an image in order to increase the ambiguity of images details to increase the protection of image is that the concern of this analysis. Statistics extracted from the analyzed papers have shown a number of methods and techniques that image processing has utilized to increase the security of processed image such as deep learning, edge computing, block-chain, encryption schemes and few others. In Figure 7, results obtained after the analysis has been applied where the distribution of papers according to the techniques and methods applied to enhance the security of image-related IoT applications.

VI. DISCUSSION

On the basis of the nature of the use of image processing by IoT applications, which has been reviewed in the literature, there is a primary consideration that is the purpose of using image processing techniques exploited by IoT applications in order to potentially produce secure and safe IoT applications. This purpose of using image processing techniques exploited by IoT applications is to produce secure and safe IoT applications.

As a result of this, there are many different reasons why IoT applications and systems have been making use of image processing techniques. A number of the reasons that have been reported and mentioned have been chosen. The aims of various IoT applications are outlined in Table 3.

TABLE 3. What are the image processing techniques that have been used for, and what is their purpose? in this review paper, the presented values are calculated in accordance with the total number of articles that were reviewed.

Image processing is used for:	Percentage (%)
IoT safety applications	28
IoT security applications	35.1
IoT privacy applications	21.05
Other IoT applications	15.85
Total	100.00

Table 3 shows that the computed percentage numbers vary depending on the context in which techniques are applied. As can be seen, the most common uses for image processing are for security applications that run via the IoT and the Cloud. There is a pressing need for researchers working in the field of privacy of IoT applications to pay a greater amount of attention to the widespread utilization of image processing techniques. This would allow for an improvement in the related performance in terms of reliability and security of data and information. That is important and crucial with, for instance, medical IoT applications specifically the patient's medical history and record(s). Fortunately, the relevant information that needs to be transferred to another IoT-dependent party or to the Cloud will be securely protected by a number of different security schemes. These schemes, in a number of cases, depend primarily on the utilization of image processing techniques in order to function properly.

VII. FUTURE TRENDS

In this section, we will examine future trends and highlight a number of crucial possibly increased developments that may be made in the era of the IoT via the use of image processing techniques. There are three further subsections, the first of which discusses the function that enables image processing to play as a bridge linking us to a safe environment for IoT devices in an effective and seamless manner. The second of these is a list of several areas related to the IoT to which image processing techniques have contributed. In addition, this area is backed by a stated menu of associated methods that image processing has included. In the third subsection, we present and suggest a comprehensive framework that circulates essential points that could help interested IoT-related researchers and designers from a variety of fields and areas to propose and design an IoT environment that is supported by image processing techniques. This framework circulates these points in a way that could help researchers and designers from other fields and areas.

A. IMAGE PROCESSING AS A BRIDGE TO THE IoT PLATFORM AND ENVIRONMENT

Applications of the IoT have been primarily reliant on a variety of technologies that are evolving and expanding. The digital image processing technique is only one of these technologies. How did the various image processing algorithms contribute to the improvement of the IoT platform, the related devices, and the many additional communication networks? Image processing techniques have been responsible for the development of a great deal of functionality and progress in the IoT. The following is a list of upcoming developments in image processing that are related to the IoT:

1. Image processing aims to enable IoT be more secure whereby all things associated with its infrastructure are involved. Thus, image processing techniques are day-by-day improved and therefore researches dedicated to enhance image processing techniques would also aim to reflect this enhancement towards development of IoT in terms of several considerations such as security and safety of data either transferred through IoT medium and stored in IoT storage devices [54].
2. Images matching process considering both captured and previously in-cloud-stored images is a very sensitive task due to that the success of this process mainly depends on the highly secure data storage and communication networks. Hence, the security of communication between cloud and image-matching processing part, from the one hand, and the safety and privacy of the recalled in-cloud-stored image, on the other hand, is a huge matter and is a future trend of interaction between and integration of IoT and image processing. Any issue, with or without knowledge, in regard to security of communication and/ or safety of image contents will make the whole system fails to achieve a potential image matching processing for IoT applications. Hence, researches should have concerned this issue and could either enhance security of communication between IoT parties including the image processing part or enhance image processing techniques to perform further complicated security schemes applied to in-cloud-stored image while they continuously and repeatedly recalled once a matching process and image-based analysis is required [55].
3. Image processing can contribute to IoT by shortening the distance between two far and remote workplaces. How? In the so near future, several applications will be used for the aim of accessing digital and sensitive workplaces. To allow both an authorized access and safety and privacy of contents, there must be an authentication and verification procedure by another party, it could be, for example, the owner of the digital asset. So, firstly, the first party will ask for an authorized access to the workplace. Secondly, a captured image of the person is sent to the other party for verification purpose, however, a matching process might be used to support the decision making. Thirdly, the other party

could allow for such an authorized access to maintain contents safe. The role of image processing is essential in such a scenario. The focus will also be on, for example, security enhancement and computation time needed to process either a single image or multi-frame images. From any place in the world, the access request made by the first person at the location of workplace might be approved or rejected via a smartphone-based application [62].

4. Recently, the topic of image encryption has been widely and increasingly considered by numerous IoT applications to perform an image transferring to cloud storage. To enhance security during this process, both image contents safety and communication channel's security are essential. One research direction in the near future is to efficiently perform image encryption. Therefore, image-based encryption is still of improvement to serve better and contribute towards this direction. There is a need to enhance performance of the IoT application that aims to transfer images to cloud storages or to a remote part such as between two users. The most important and critical issue to be considered regarding IoT application performance is the security and privacy of images' contents [57].
5. Even though security of IoT devices by enabling them be always protected against DDoS malware attacks utilizing the image processing has achieved a good and promising level of highly detected rate, there is a need to enhance this way of security by reducing potential vulnerabilities caused by complex code obfuscation that is usually associated with image-based detectors. One of the proposed solutions by [58] is to consider more complex static features.
6. Another big challenge to image processing in the environment of IoT-implemented systems is related to the security of the communication channel between the source of image processing and the destination. This issue is still challenging because of the necessity of the safety of transferred digital contents and security of the communication channel during the time those contents are sent. Hence, currently proposed works are focusing and addressing this issue with noticing that the security scheme is required to achieve a high level of lightweight. The concern about security achievement before transfer is due to the necessity of protecting sensitive digital contents before it can be lost due to the unsecure communication channel through which the images are transmitted to the Cloud [68].
7. Another vital safety is ensuring the well-being of individuals, particularly youngsters. In order to address this worry, a system that makes use of FPGA was suggested. Researchers designed a fog-based system that can accept numerous Kinect sensors near each other, such as at a school or hospital, by reproducing violent activities against children IP and according to number of Kinect sensors and running in parallel with only one FPGA device [69]. The testing with violent actions against children IP yielded promising results, which prompted the researchers to build the fog-based system [69].
8. According to [63], the more secure the image being transferred via IoT-cloud is, the less image size is. That is, as a result, going to indirectly contribute to energy consumption issue (energy-reduced consumption) by reducing the size needed to be transmitted though IoT communication channels. This finally will contribute to shift energy-friendly IoT aiming to achieve the conception of development of sustainable energy. One of the future trends towards sustainable energy in the IoT environment is to apply effective security schemes that, besides, help largely reduce the size of image in order to reduce both the time of transmission and size. That would reduce the related and resulted heat as well as reduce the CO2 caused by the processes of transmitted contents at the IoT cloud server or at the destination location.
9. An effective and useful solution to increase the security for those digital contents specifically images being stored at the IoT cloud and/ or other servers is to divide the image into blocks of images to constitute a double-phase security scheme applied to images. A suggested scenario implemented by [67] is described as follows:
   a. The first security scheme constitutes the encrypted images.
   b. These encrypted images can be transmitted to the IoT cloud or server for storage purposes.
      i. But, what will it be happening if the server itself has been attacked?
      ii. There are many possibilities able to occur.
   c. Then, before sending these encrypted images to the IoT cloud or servers, it is better to store these images in a secure server.
      i. How was that be happening?
      ii. Answer of this question is provided in the following point (i.e., d).
   d. By increasing the security of both images and the IoT cloud or server. How?
      i. That can be done by performing a process that divides encrypted images into block of other sub-images.
      ii. These blocks are by a decentralized mechanism stored in many other servers.
   e. This scenario of a double-phase security guarantees a better scheme for protecting highly sensitive images than other single-layer security schemes.
   f. This security scheme might be one of the future trends to secure stored images in the IoT cloud. It would be useful to very important images to have such a double-phase security scheme.

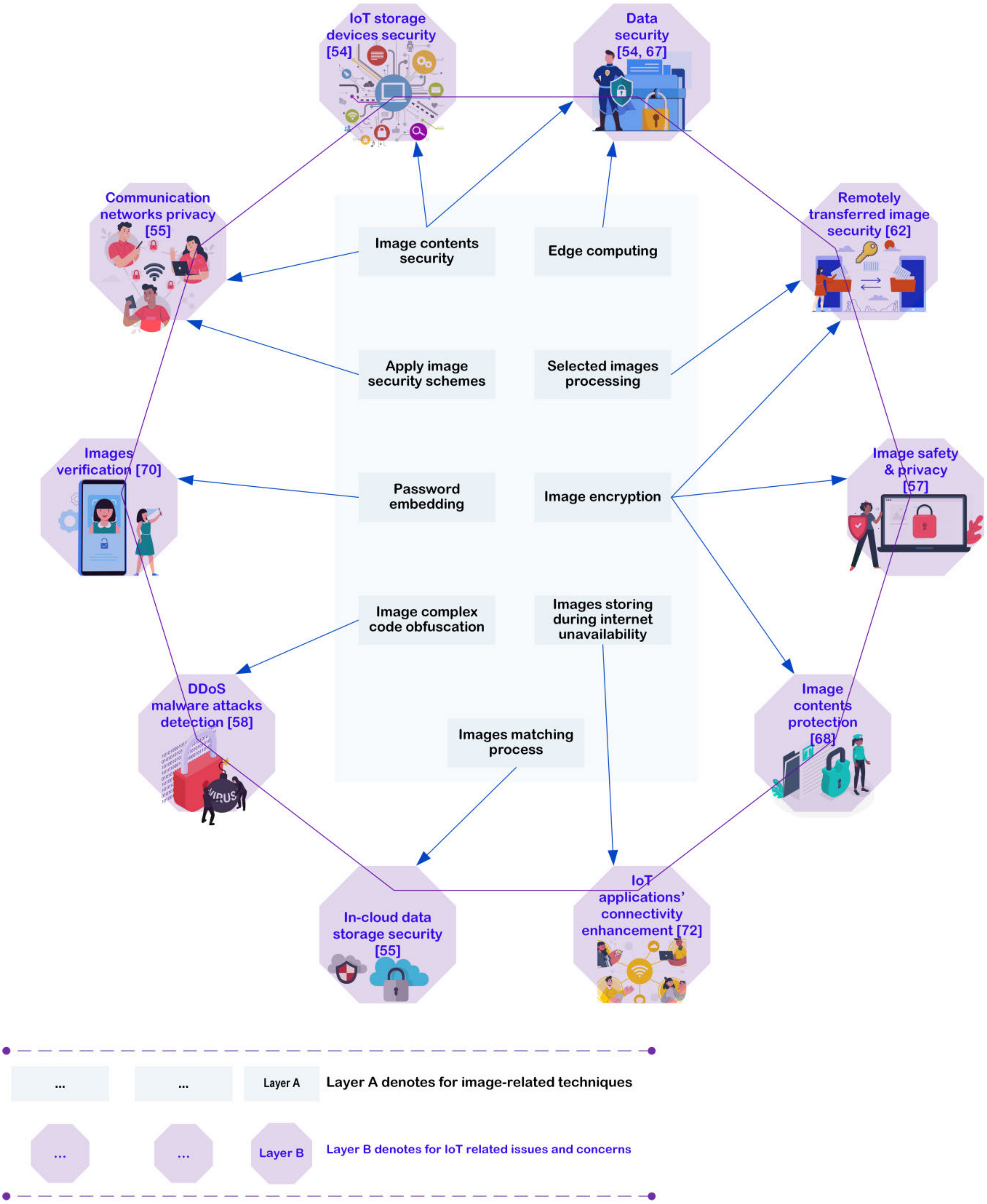

IoT storage devices security [54]
Data security [54, 67]
Communication networks privacy [55]
Remotely transferred image security [62]
Images verification [70]
Image safety & privacy [57]
DDoS malware attacks detection [58]
Image contents protection [68]
In-cloud data storage security [55]
IoT applications' connectivity enhancement [72]
Image contents security
Edge computing
Apply image security schemes
Selected images processing
Password embedding
Image encryption
Image complex code obfuscation
Images storing during internet unavailability
Images matching process
VIRUS
...
...
Layer A
Layer A denotes for image-related techniques
...
...
Layer B
Layer B denotes for IoT related issues and concerns

FIGURE 8. Future trends. To read what has been conceptualized and illustrated in this figure, it is useful to have a look at the two main layers illustrated – Layer A and Layer B. The rectangle-shaped layer is Layer A and the decagon-shaped layer is Layer B. Each layer consists of a number of elements. Layers A and B encompass 9 and 10 elements, respectively. This figure can be read as: role of image processing via an element belongs to Layer A can enhance a relevant element belongs to B. Highlighted relationships between elements from layers A and B through the blue-colored arrows represent the future trends of suitability of applying a technique (an element from Layer A) to the aim of enhancing an issue (an element from Layer B). Meaning, if there is a need to enhance, for example, "image contents protection" (an element from B), one of the proposed solutions is to utilize "image encryption" (an element from A). Numbers between brackets represent cited research studies being analyzed. Images and photos shown in this figure are licensed. Design is done by authors.

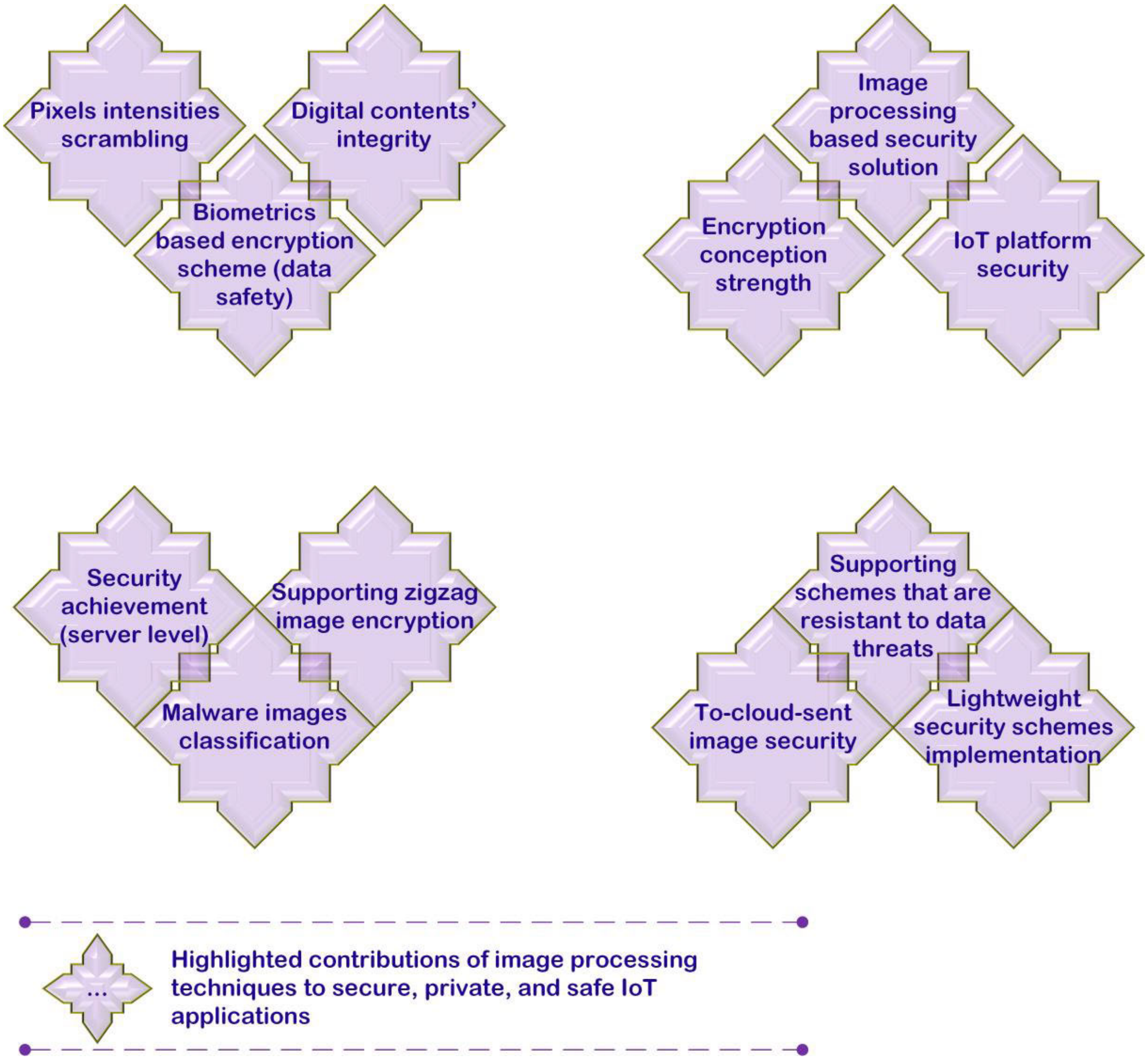

Pixels intensities scrambling
Digital contents' integrity
Biometrics based encryption scheme (data safety)
Image processing based security solution
Encryption conception strength
IoT platform security
Security achievement (server level)
Supporting zigzag image encryption
Malware images classification
Supporting schemes that are resistant to data threats
To-cloud-sent image security
Lightweight security schemes implementation
...
Highlighted contributions of image processing techniques to secure, private, and safe IoT applications

FIGURE 9. A combination of selected contributions of image processing towards various IoT applications and systems as concluded from the reviewed papers.

10. Embedding a password technique in an encrypted medical image is one of the effective methods enabling a verification procedure to be carried out so that authentication of images' contents can be verified. Embedding a password technique should have contributed to the achievement of the integrity objective of encrypted medical images [70]. That can be achieved by embedding a One-time password (OTP) within the encrypted medical image where the OTP can be verified by the authorized person by comparing the embedded OTP to another OTP sent via a secure channel to the authorized person's mobile. It is preferable for certain cases to implement such a technique so that a contribution to the healthcare and medical images could be achieved.
11. Passive infrared sensor (PIR sensor) can be used by different IoT applications to perform a remote monitoring to maintain certain areas secure [71]. The image processing role can be summarized in the following steps:
    a. A PIR sensor is to be mounted in areas-of-interest (AOI).
    b. A camera is also mounted in certain areas. More than a camera can be used.
    c. Suppose, an object has moved and entered the AOI.
    d. The PIR sensor would be able to sense the movement.
    e. The PIR will be able to send a notification to the camera via a pre-set mechanism.
    f. The camera is enabled to capture the object.
        i. The camera could capture the face of the person.
        ii. The camera is able to capture the whole object.

  g. The image can be sent utilizing the IoT platform to a server for a further processing in a remote processing unit. It is sent before any process.
    i. The image is processed locally.
    ii. Then, it will be sent after it has been processed.
    iii. Usually, the object detection process is needed in such cases.
  h. A decision can be made depending on the nature of the security of that area, i.e., AOI.

12. There is an issue associated with the security IoT systems specifically those which require a real-time Internet connection. The availability of processed images or digital contents [72].
    a. This issue has been partially solved by storing the captured images (with monitoring IoT applications) in the system until the internet connection is available.
    b. However, this procedure that postpones to send the image to the IoT cloud to a postponed time, will face another issue which is the size of the images especially if it is required to send multi-frame images.

TABLE 4. IoT future trends based on the roles of image processing techniques: applications and fields served by these techniques.

Concerns and issues	DIP techniques
• Data security [54, 67] • Data safety [54] • IoT storage devices security [54] • In-Cloud data storage security [55] • Communication networks security [55] • Communication channels privacy [55] • Remotely transferred data security [62] • Transferred image security [57] • Image contents safety and privacy [57] • DDoS malware attacks detection [58] • Sensitive image contents protection [68] • Images' contents authentication and verification [70]	• Image contents security [55] • Image analysis • Image encryption [57] • Image complex code obfuscation [58] • Effective implementation of image's security schemes [63] • Embedding a password technique for encrypted images [70] • Ease-of-connection with sensor devices [71] • Edge computing [73-75]

B. FUTURE TRENDS – CONCERNS AND DIP TECHNIQUES

Image processing has made significant contributions to a variety of sectors that are relevant to the IoT, as shown in Table 4 below. Table 4 contains image processing techniques that are relevant to the aforementioned domains and elements of study.

C. FUTURE TRENDS – A COMPREHENSIVE FRAMEWORK

An extensive summary of vital and critical aspects that should be taken into consideration by interested academics working in a variety of relevant domains that are connected to both image processing and the IoT. In the not-too-distant future, it will be essential for highlighted points relating to fields to be applied by techniques. These techniques are graphically represented in Figure 8. In spite of this, the articles that were read and analyzed for this work revealed that image processing has been beneficial to a variety of domains and facets within the IoT industry as well as its associated applications. In addition, it has been demonstrated that the image processing techniques presented in Table 4 and Figure 8 have been used for a variety of IoT applications; however, it is necessary that related researchers make significant efforts to improve those techniques, with the goal of achieving high levels of performance(s) in the direction of optimizing the IoT platform and environment through the efficient utilization of image processing techniques that can meaningfully assist in this direction.

VIII. CONCLUSION

A. OVERVIEW

This analysis will focus on three of the most common challenges that are associated with IoT applications. In this context, both the problems that may be solved and the contributions that can be made by image processing techniques have been extensively discussed. The roles that various image processing approaches have in improving the performance of these three difficulties have been analyzed and discussed. The primary advantage that the possibly interested academics and engineers in the relevant domains can probably obtain from this review article is the ability to design a private, safe, and secure application that makes use of the IoT.

This article reviewed 76 research studies that concerns the field of image-processed IoT applications in terms of security, privacy, and safety issues. For the review process, related studies have been extracted from a number of DLs including IEEE Xplore, ScienceDirect, Nature, and SpringerLink.

The remainder of the conclusion consists of detailed observations and conclusions on the papers that were examined, in which the benefits and drawbacks of systems as well as research studies have been evaluated alongside one another.

B. CONCLUDED REMARKS

1. Image processing techniques contributed to IoT regarding to safety of data transferred through communication networks. It replaced conventional security schemes specifically two-step authentication procedure by proposing a biometrics-based encryption scheme. Image processing increased data encryption by introducing multi-processing solutions. Image processing-based security solutions lessen vulnerabilities compared to other methods [54].
2. According to [55], image processing techniques could contribute to enhance home safety and security by using sensors and camera for sensing any change in movement and capturing images. Then, easily and effectively, an alert as a message could be sent to another remote part (receiver) utilizing IoT links.

Additionally, the role that image processing has played is by performing analysis of captured images and matching comparative analysis based on details and features of the analyzed image to that one in-cloud-stored, safety and security in home sector should be enhanced.

3. Digital and precious assets are becoming more accessible thanks to image processing. Images of a person's face can be captured using image processing in the proposed system application, which can then be shared with a person who is providing access to a digital asset. This person has the ability to grant remote access to someone who has been authorized, and that person can then unlock the door on their behalf. IoT platform has run smoothly and safely thanks to the ability to ensure safety and security from a distance [62].
4. Image processing has contributed to securely sent delivery of sensitive contents at perception layer to the network layer. Images will be then sent to the Cloud. Hence, a variety of IoT applications that need to encrypt images using random and complex patterns with the help of CA might benefit from using the proposed security scheme and that could be applied for, specifically, cloud-enabled IoT [56], [57].
5. The classification of dangerous image families is one of the ways that image processing contributes to the detection of malware. Images are created from the malicious binaries. Because the classification of malware images is being handled, IoT devices that have been compromised by an assault will be safer. Malware that causes DDoS assaults is one of the attacks that has been linked to IoT devices [58].
6. The application of lightweight security techniques to images before the step of transmitting them to the IoT cloud will prevent the need for a significant amount of processing and computing capacity. Therefore, achieving energy sustainability would be within the realm of possible [63].
7. It is suggested that a division process of an image into blocks of sub-images contributes to security achievement specifically for those IoT applications that might be vulnerable to attacks at the server level after a storage procedure has been done at the IoT cloud. It is mentioned by [67] that it is not enough to maintain communication channels secure while an image's transmission but it is needed to maintain the IoT servers dedicated for images storage to be also highly secure. Hence, by dividing the secret image (or even other IoT data) into blocks, the safety of its contents will be increased and the probabilities of images being attacked will be reduced.
8. According to [70], a password can be embedded in a medically-encrypted image. This approach increases the security of an image's contents by verifying the embedded password and sending it to an authorized individual. The comparison will be used to verify the encrypted image's integrity and authenticity.
9. Image processing is utilized to monitor and secure IoT-enabled areas. Image processing has improved security, therefore smart systems have integrated image processing-based and non-image processing-based security techniques [71], [72], [76], [77], [78], [79], [80].
10. In order to accomplish the goal of maintaining privacy, FPGA-based solutions have been deployed. An intellectual property solution based on FPGAs has been made available for detecting instances of child abuse. The proposed device safeguards individuals' privacy at home or at school by collecting information only on their skeletal joints. The recommended hardware achieved an over 98 percent detection rate. The FPGA-based intellectual property for recognizing frequent child maltreatment without invading a kid's privacy by using just skeleton joint data, and the IP identifies both violence and kindness [69], [81], [82], [83].
11. Cloud computing security has become vital in healthcare, especially for storing medical data and images and predicting sickness. The healthcare business creates a lot of data due to medical device advancements. Cloud computing stores and handles these vast volumes of data securely. Enhanced zigzag image encryption is utilized in a secure cloud computing environment to identify illnesses [66], [80], [84], [85], [86].
12. Edge computing is a promising approach that, if implemented correctly, has the potential to significantly improve the data security offered by IoT applications and systems [63], [73], [74], [87], [88], [89], [90].

The most widely discussed and concluding observations from evaluated articles that have emphasized the contributions of image processing to IoT applications are shown in Figure 9.

C. EXAMPLES OF IMAGE PROCESSING TECHNIQUES IN REAL-WORLD IoT SECURITY

We conclude by providing a list of examples of image processing techniques in real-world IoT security.

One of these examples is that, imagine a smart office where employees use their smartphones to gain access. Image processing algorithms analyze facial features to allow authorized individuals entry. Even if someone knows the access code, they can't get in without their face matching the system's records. This is particularly useful in ensuring physical security within corporate environments [59].

In a medical setting, IoT devices transmit patient data among various healthcare providers. Image processing comes into play by encrypting patient records into images using visual cryptography techniques. Only when multiple authorized parties collaborate can the original data be decrypted, ensuring the confidentiality of sensitive patient information during transmission [91].

In a smart city scenario, surveillance cameras capture visual data across urban spaces [92]. Image processing algorithms continually monitor these feeds, flagging any instances of tampering or vandalism. If someone tries to disable a camera, the system detects the change and sends an alert, ensuring the integrity of the surveillance network [93].

Another example is that image processing techniques contribute to anomaly detection in industrial IoT. In an industrial setup, IoT sensors monitor machinery and equipment. Image processing analyzes real-time images of these devices and their surroundings. If a machine behaves strangely or there's an unauthorized presence, the system triggers an alert, preventing potential safety hazards and unauthorized access [94].

Smart traffic management is one of the important examples benefiting from image processing techniques. In urban traffic management, IoT-enabled cameras monitor traffic flow. Image processing identifies license plates, allowing for real-time monitoring of vehicle movements. If a stolen vehicle is detected, the system triggers an alert to aid law enforcement in preventing crime [95].

Biometric authentication in smart homes is a real example of utilizing image processing by IoT applications towards security achievement. In a smart home environment, biometric authentication using image processing ensures that only authorized family members can access the premises. Smart doorbells equipped with cameras can recognize familiar faces and allow entry, while alerting homeowners about unfamiliar individuals, enhancing both security and privacy [96].

D. LIMITATIONS OF IMAGE PROCESSING TECHNIQUES ASSOCIATED WITH IoT APPLICATIONS

A number of considerations and limitations of employing image processing in the context of IoT application security have been included.

One significant limitation of image processing techniques is their computational complexity [97]. These methods often involve complicated algorithms that require substantial processing power. In resource-constrained IoT devices, especially those with limited computing capabilities, implementing real-time image analysis might be challenging. This can lead to delays in threat detection and response, potentially compromising the overall security of IoT systems.

Another imitation is that image processing techniques often rely on consistent and favorable environmental conditions for accurate analysis. Factors like lighting changes, weather conditions, and image quality variations can affect the performance of these techniques [98]. In real-world IoT deployments, where devices operate in diverse and uncontrolled environments, ensuring consistent and reliable image data can be challenging.

One more thing is that, while image processing can be effective in detecting known patterns and anomalies, its efficacy can diminish when faced with novel or evolving threats [99]. Adversarial attacks, where malicious actors manipulate visual input to deceive image processing algorithms, can undermine the security of IoT applications. Developing algorithms that are resistant to such attacks is a complex endeavor [100].

The privacy concerns are considered a big limitation. Image processing techniques that involve biometric authentication or visual data analysis can raise privacy concerns. The storage and transmission of sensitive visual information, even when encrypted, can be subject to breaches or unauthorized access. Balancing security and privacy considerations becomes paramount, requiring robust encryption and secure data management practices [101].

E. GAPS AND CHALLENGES IN THE LITERATURE

Since image processing techniques offer substantial potential, it is essential to recognize the frontiers that have yet to be explored and the obstacles that need to be overcome. This section attempts to discuss gaps and challenges within the literature and to highlight the areas in order to warrant further research and development.

A significant gap in the literature pertains to the lack of standardized methodologies for incorporating image processing techniques into diverse IoT applications. The absence of a unified framework hampers comparability across studies and limits the scalability of these techniques. Addressing this gap requires collaborative efforts to establish best practices and guidelines that can be universally adopted across different IoT contexts.

The literature reveals a notable challenge in adapting image processing techniques to resource-constrained IoT devices. Many existing methods are computationally intensive, potentially straining the limited processing power and energy reserves of these devices. Overcoming this challenge necessitates the exploration of techniques that strike a balance between accuracy and computational efficiency, ensuring real-time security without compromising device performance.

The literature presents a gap between theoretical efficacy and real-world application. While studies highlight the potential of image processing techniques, their practical validation in diverse IoT scenarios remains limited. Bridging this gap requires more empirical research that deploys these techniques in real-world settings, comprehensively evaluating their effectiveness, feasibility, and impact.

The literature lacks comprehensive strategies to enhance the resilience of image processing techniques against a number of attacks, demanding research efforts to develop techniques that can maintain their integrity in the face of adversarial manipulations.

Existing literature lacks comprehensive privacy-preserving mechanisms that effectively protect sensitive visual information without compromising the accuracy of security measures. Exploring innovative solutions to strike a balance between security and privacy remains explored in a limited domain.

F. LINKAGE TO SUSTAINABLE DEVELOPMENT GOALS 7 AND 13

Sustainable Development Goal 7 (SDG 7) focuses on ensuring access to affordable, reliable, sustainable, and modern energy for all. While on the surface, the relationship between image processing and energy might not be immediately apparent, the application of image processing techniques in IoT security significantly contributes to the advancement of this goal.

IoT devices play a significant role in managing and monitoring energy distribution networks. By fortifying the security of these devices using image processing techniques, vulnerabilities in energy systems are mitigated, leading to enhanced resilience against cyber threats and potential disruptions.

Besides, a secure IoT ecosystem facilitates the efficient collection and analysis of energy consumption data. Image processing aids in identifying anomalies and patterns that could indicate energy wastage or inefficiencies. This contributes to the promotion of sustainable energy consumption patterns.

Efficient energy utilization directly impacts environmental sustainability. Strengthening the security of IoT applications through image processing indirectly supports environmentally conscious energy practices, aligning with SDG 7's focus on sustainable energy and climate action (SDG 13).

ACKNOWLEDGMENT

The authors would like to thank the team of freepik.com. Licensed images are borrowed from https://www.freepik.com/.

REFERENCES

[1] F. Wen, Z. Zhang, T. He, and C. Lee, "AI enabled sign language recognition and VR space bidirectional communication using triboelectric smart glove," *Nature Commun.*, vol. 12, no. 1, p. 5378, Sep. 2021, doi: 10.1038/s41467-021-25637-w.

[2] C. Li, M. Hu, Y. Li, H. Jiang, N. Ge, E. Montgomery, J. Zhang, W. Song, N. Dávila, C. E. Graves, Z. Li, J. P. Strachan, P. Lin, Z. Wang, M. Barnell, Q. Wu, R. S. Williams, J. J. Yang, and Q. Xia, "Analogue signal and image processing with large memristor crossbars," *Nature Electron.*, vol. 1, no. 1, pp. 52–59, Dec. 2017, doi: 10.1038/s41928-017-0002-z.

[3] K. Li, R. Yuasa, R. Utaki, M. Sun, Y. Tokumoto, D. Suzuki, and Y. Kawano, "Robot-assisted, source-camera-coupled multi-view broadband imagers for ubiquitous sensing platform," *Nature Commun.*, vol. 12, no. 1, p. 3009, May 2021, doi: 10.1038/s41467-021-23089-w.

[4] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, vol. 527, pp. 493–510, Jul. 2020, doi: 10.1016/j.ins.2019.01.070.

[5] S. Rajput, A. Ippili, D. Puraswani, S. Johri, A. Nadathur, and S. Dhar, "Impact of earthquakes based on satellite images using IoT and sensor networks," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 551–554, doi: 10.1109/COMSNETS48256.2020.9027380.

[6] N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Proc. Comput. Sci.*, vol. 132, pp. 109–117, Jan. 2018, doi: 10.1016/j.procs.2018.05.170.

[7] I. J. Jacob and P. E. Darney, "Design of deep learning algorithm for IoT application by image based recognition," *J. ISMAC*, vol. 3, no. 3, pp. 276–290, Aug. 2021.

[8] L. Yao, Q. Z. Sheng, B. Benatallah, S. Dustdar, X. Wang, A. Shemshadi, and S. S. Kanhere, "WITS: An IoT-endowed computational framework for activity recognition in personalized smart homes," *Computing*, vol. 100, no. 4, pp. 369–385, Apr. 2018, doi: 10.1007/s00607-018-0603-z.

[9] M. M. Rathore, H. Son, A. Ahmad, and A. Paul, "Real-time video processing for traffic control in smart city using Hadoop ecosystem with GPUs," *Soft Comput.*, vol. 22, no. 5, pp. 1533–1544, Mar. 2018, doi: 10.1007/s00500-017-2942-7.

[10] A. Hassan, F. Liu, F. Wang, and Y. Wang, "Secure image classification with deep neural networks for IoT applications," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 8, pp. 8319–8337, Aug. 2021, doi: 10.1007/s12652-020-02565-z.

[11] S. Byun, I.-K. Shin, J. Moon, J. Kang, and S.-I. Choi, "Road traffic monitoring from UAV images using deep learning networks," *Remote Sens.*, vol. 13, no. 20, p. 4027, Oct. 2021, doi: 10.3390/rs13204027.

[12] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and secure image communication system based on compressed sensing for IoT monitoring applications," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 82–95, Jan. 2020, doi: 10.1109/TMM.2019.2923111.

[13] H. Gupta and O. P. Verma, "Monitoring and surveillance of urban road traffic using low altitude drone images: A deep learning approach," *Multimedia Tools Appl.*, vol. 81, no. 14, pp. 19683–19703, Jun. 2022, doi: 10.1007/s11042-021-11146-x.

[14] A. Sharma, P. K. Singh, and Y. Kumar, "An integrated fire detection system using IoT and image processing technique for smart cities," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102332, doi: 10.1016/j.scs.2020.102332.

[15] L. Chen, B. Fan, Y. Cai, and Q. Shi, "Application of IoT medical image detection and prenatal genetic testing in obstetric clinic," *Microprocessors Microsyst.*, vol. 81, Mar. 2021, Art. no. 103705, doi: 10.1016/j.micpro.2020.103705.

[16] Y. Wei, D. Sree, C. Yang, and A. W.-K. Law, "Surface wave measurements with IoT image processing," *J. Hydro-Environ. Res.*, vol. 39, pp. 60–70, Nov. 2021, doi: 10.1016/j.jher.2021.07.001.

[17] Z. Mishra and B. Acharya, "High throughput and low area architectures of secure IoT algorithm for medical image encryption," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102533, doi: 10.1016/j.jisa.2020.102533.

[18] P. Rukmani, G. K. Teja, M. S. Vinay, and K. B. P. Reddy, "Industrial monitoring using image processing, IoT and analyzing the sensor values using big data," *Proc. Comput. Sci.*, vol. 133, pp. 991–997, Jan. 2018, doi: 10.1016/j.procs.2018.07.077.

[19] M. Tresanchez, A. Pujol, T. Pallejà, D. Martínez, E. Clotet, and J. Palacín, "A proposal of low-cost and low-power embedded wireless image sensor node for IoT applications," *Proc. Comput. Sci.*, vol. 134, pp. 99–106, Jan. 2018, doi: 10.1016/j.procs.2018.07.149.

[20] Y. Liu, L. Kong, G. Chen, F. Xu, and Z. Wang, "Light-weight AI and IoT collaboration for surveillance video pre-processing," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101934, doi: 10.1016/j.sysarc.2020.101934.

[21] A. Manocha, G. Kumar, M. Bhatia, and A. Sharma, "Video-assisted smart health monitoring for affliction determination based on fog analytics," *J. Biomed. Informat.*, vol. 109, Sep. 2020, Art. no. 103513, doi: 10.1016/j.jbi.2020.103513.

[22] Y. Wu, J. Zhao, N. Yu, and R. Feng, "Indoor surveillance video based feature recognition for pedestrian dead reckoning," *Expert Syst. Appl.*, vol. 173, Jul. 2021, Art. no. 114653, doi: 10.1016/j.eswa.2021.114653.

[23] I. Ahmed, M. Ahmad, A. Ahmad, and G. Jeon, "IoT-based crowd monitoring system: Using SSD with transfer learning," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107226, doi: 10.1016/j.compeleceng.2021.107226.

[24] K. Jung, "Neural network-based text location in color images," *Pattern Recognit. Lett.*, vol. 22, no. 14, pp. 1503–1515, 2001, doi: 10.1016/S0167-8655(01)00096-4.

[25] Wahyono and K. Jo, "LED dot matrix text recognition method in natural scene," *Neurocomputing*, vol. 151, pp. 1033–1041, Mar. 2015, doi: 10.1016/j.neucom.2014.07.079.

[26] C. Shi, C. Wang, B. Xiao, S. Gao, and J. Hu, "End-to-end scene text recognition using tree-structured models," *Pattern Recognit.*, vol. 47, no. 9, pp. 2853–2866, Sep. 2014.

[27] L. Zhang, T. Jung, K. Liu, X.-Y. Li, X. Ding, J. Gu, and Y. Liu, ''PIC: Enable large-scale privacy preserving content-based image search on cloud,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 11, pp. 3258–3271, Nov. 2017, doi: 10.1109/TPDS.2017.2712148.

[28] R. Alonso-Calvo, J. Crespo, M. Garc'ia-Remesal, A. Anguita, and V. Maojo, ''On distributing load in cloud computing: A real application for very-large image datasets,'' *Proc. Comput. Sci.*, vol. 1, no. 1, pp. 2669–2677, May 2010, doi: 10.1016/j.procs.2010.04.300.

[29] C. A. da Costa, C. F. Pasluosta, B. Eskofier, D. B. da Silva, and R. da Rosa Righi, ''Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards,'' *Artif. Intell. Med.*, vol. 89, pp. 61–69, Jul. 2018, doi: 10.1016/j.artmed.2018.05.005.

[30] A. Chopard, Q. Cassar, J. Bou-Sleiman, J. P. Guillet, M. Pan, J. B. Perraud, A. Susset, and P. Mounaix, ''Terahertz waves for contactless control and imaging in aeronautics industry,'' *NDT E Int.*, vol. 122, Sep. 2021, Art. no. 102473, doi: 10.1016/j.ndteint.2021.102473.

[31] K. Zhuang, ''Film and television industry cloud exhibition design based on 3D imaging and virtual reality,'' *Displays*, vol. 70, Dec. 2021, Art. no. 102107, doi: 10.1016/j.displa.2021.102107.

[32] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, ''Access control and surveillance in a smart home,'' *High-Confidence Comput.*, vol. 2, no. 1, Mar. 2022, Art. no. 100036, doi: 10.1016/j.hcc.2021.100036.

[33] Y. R. Serpa and M. A. F. Rodrigues, ''Human and machine collaboration for painting game assets with deep learning,'' *Entertainment Comput.*, vol. 43, Aug. 2022, Art. no. 100497, doi: 10.1016/j.entcom.2022.100497.

[34] Q. Wu, W. Yang, Z. Chen, and P. Zhang, ''Research of semantic understanding on target region of interest for fuzzy image,'' *Eng. Appl. Artif. Intell.*, vol. 37, pp. 135–144, Jan. 2015, doi: 10.1016/j.engappai.2014.09.005.

[35] C. Yang, W. Wang, and X. Feng, ''Joint image restoration and edge detection in cooperative game formulation,'' *Signal Process.*, vol. 191, Feb. 2022, Art. no. 108363, doi: 10.1016/j.sigpro.2021.108363.

[36] T. Mao, H. Tang, and W. Huang, ''Unsupervised classification of multispectral images embedded with a segmentation of panchromatic images using localized clusters,'' *IEEE Trans. Geosci. Remote Sens.*, vol. 57, no. 11, pp. 8732–8744, Nov. 2019.

[37] L. Chen, D. Zhao, and F. Ge, ''Gray images embedded in a color image and encrypted with FRFT and region shift encoding methods,'' *Opt. Commun.*, vol. 283, no. 10, pp. 2043–2049, May 2010.

[38] K. Naik, T. Pandit, N. Naik, and P. Shah, ''Activity recognition in residential spaces with Internet of Things devices and thermal imaging,'' *Sensors*, vol. 21, no. 3, Feb. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/3/988

[39] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, ''RETRACTED ARTICLE: Hybrid optimization with cryptography encryption for medical image security in Internet of Things,'' *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979–10993, Aug. 2020, doi: 10.1007/s00521-018-3801-x.

[40] Y. Chen, Y. Ping, Z. Zhang, B. Wang, and S. He, ''Privacy-preserving image multi-classification deep learning model in robot system of industrial IoT,'' *Neural Comput. Appl.*, vol. 33, no. 10, pp. 4677–4694, May 2021, doi: 10.1007/s00521-020-05426-0.

[41] Z. Xia, L. Jiang, X. Ma, W. Yang, P. Ji, and N. N. Xiong, ''A privacy-preserving outsourcing scheme for image local binary pattern in secure industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 629–638, Jan. 2020, doi: 10.1109/TII.2019.2913217.

[42] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, ''Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach,'' *IEEE Netw.*, vol. 33, no. 5, pp. 27–33, Sep. 2019, doi: 10.1109/MNET.001.1800503.

[43] Y. Wu, X. Zhang, Y. Xiao, and J. Feng, ''Attention neural network for water image classification under IoT environment,'' *Appl. Sci.*, vol. 10, no. 3, p. 909, Jan. 2020, doi: 10.3390/app10030909.

[44] V. M. Lidkea, R. Muresan, and A. Al-Dweik, ''Convolutional neural network framework for encrypted image classification in cloud-based ITS,'' *IEEE Open J. Intell. Transp. Syst.*, vol. 1, pp. 35–50, 2020, doi: 10.1109/OJITS.2020.2996063.

[45] S. B. Park, J. W. Lee, and S. K. Kim, ''Content-based image classification using a neural network,'' *Pattern Recognit. Lett.*, vol. 25, no. 3, pp. 287–300, Feb. 2004, doi: 10.1016/j.patrec.2003.10.015.

[46] H. Kalantarian, K. Jedoui, P. Washington, Q. Tariq, K. Dunlap, J. Schwartz, and D. P. Wall, ''Labeling images with facial emotion and the potential for pediatric healthcare,'' *Artif. Intell. Med.*, vol. 98, pp. 77–86, Jul. 2019, doi: 10.1016/j.artmed.2019.06.004.

[47] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, and A. V. Vasilakos, ''Privacy and security issues in deep learning: A survey,'' *IEEE Access*, vol. 9, pp. 4566–4593, 2021, doi: 10.1109/ACCESS.2020.3045078.

[48] X. Li, J. Li, S. Yiu, C. Gao, and J. Xiong, ''Privacy-preserving edge-assisted image retrieval and classification in IoT,'' *Frontiers Comput. Sci.*, vol. 13, no. 5, pp. 1136–1147, Oct. 2019, doi: 10.1007/s11704-018-8067-z.

[49] S. Almajali, H. B. Salameh, M. Ayyash, and H. Elgala, ''A framework for efficient and secured mobility of IoT devices in mobile edge computing,'' in *Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2018, pp. 58–62, doi: 10.1109/FMEC.2018.8364045.

[50] S. Hamdan, M. Ayyash, and S. Almajali, ''Edge-computing architectures for Internet of Things applications: A survey,'' *Sensors*, vol. 20, no. 22, p. 6441, Nov. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/22/6441

[51] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, ''Multimedia Internet of Things: A comprehensive survey,'' *IEEE Access*, vol. 8, pp. 8202–8250, 2020, doi: 10.1109/ACCESS.2020.2964280.

[52] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, ''A review on the role of machine learning in enabling IoT based healthcare applications,'' *IEEE Access*, vol. 9, pp. 38859–38890, 2021, doi: 10.1109/ACCESS.2021.3059858.

[53] J. Zhao, R. Masood, and S. Seneviratne, ''A review of computer vision methods in network security,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1838–1878, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3086475.

[54] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, ''Toward end-to-end biomet rics-based security for IoT infrastructure,'' *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44–51, Oct. 2016, doi: 10.1109/MWC.2016.7721741.

[55] A. B. Dorothy, S. B. R. Kumar, and J. J. Sharmila, ''IoT based home security through digital image processing algorithms,'' in *Proc. World Congr. Comput. Commun. Technol. (WCCCT)*, Feb. 2017, pp. 20–23, doi: 10.1109/WCCCT.2016.15.

[56] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, ''IECA: An efficient IoT friendly image encryption technique using programmable cellular automata,'' *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5083–5102, Nov. 2020, doi: 10.1007/s12652-020-01813-6.

[57] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, ''IEVCA: An efficient image encryption technique for IoT applications using 2-D von-neumann cellular automata,'' *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 31529–31567, Sep. 2021, doi: 10.1007/s11042-020-09880-9.

[58] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, ''Lightweight classification of IoT malware based on image recognition,'' in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2018, pp. 664–669, doi: 10.1109/COMPSAC.2018.10315.

[59] P. B. Balla and K. T. Jadhao, ''IoT based facial recognition security system,'' in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Jan. 2018, pp. 1–4, doi: 10.1109/ICSCET.2018.8537344.

[60] K. Wang, C.-M. Chen, M. S. Hossain, G. Muhammad, S. Kumar, and S. Kumari, ''Transfer reinforcement learning-based road object detection in next generation IoT domain,'' *Comput. Netw.*, vol. 193, Jul. 2021, Art. no. 108078, doi: 10.1016/j.comnet.2021.108078.

[61] V. Sharmila, N. R. R. Paul, P. Ezhumalai, S. Reetha, and S. N. Kumar, ''WITHDRAWN: IoT enabled smart assistance system using face detection and recognition for visually challenged people,'' *Mater. Today, Proc.*, Dec. 2020, doi: 10.1016/j.matpr.2020.10.198.

[62] A. Nag, J. N. Nikhilendra, and M. Kalmath, ''IoT based door access control using face recognition,'' in *Proc. 3rd Int. Conf. Converg. Technol. (I2CT)*, Apr. 2018, pp. 1–3, doi: 10.1109/I2CT.2018.8529749.

[63] S. Arunkumar, S. Vairavasundaram, K. S. Ravichandran, and L. Ravi, ''RIWT and QR factorization based hybrid robust image steganography using block selection algorithm for IoT devices,'' *J. Intell. Fuzzy Syst.*, vol. 36, no. 5, pp. 4265–4276, May 2019, doi: 10.3233/JIFS-169984.

[64] J. D. Franco, T. A. Ramirez-delReal, D. Villanueva, A. Gárate-García, and D. Armenta-Medina, "Monitoring of ocimum basilicum seeds growth with image processing and fuzzy logic techniques based on cloudino-IoT and FIWARE platforms," *Comput. Electron. Agricult.*, vol. 173, Jun. 2020, Art. no. 105389, doi: 10.1016/j.compag.2020.105389.

[65] N. Mahesh, K. N. Baluprithviraj, L. Anbarasu, B. Balaji, U. S. Kumar, and S. S. Kumar, "WITHDRAWN: Quality inspection system using IoT and image processing," *Mater. Today, Proc.*, Feb. 2021, doi: 10.1016/j.matpr.2021.01.481.

[66] J. Deepika, C. Rajan, and T. Senthil, "Security and privacy of cloud- and IoT-based medical image diagnosis using fuzzy convolutional neural network," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–17, Mar. 2021, doi: 10.1155/2021/6615411.

[67] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the Internet of Things," *Sensors*, vol. 20, no. 3, p. 916, Feb. 2020, doi: 10.3390/s20030916.

[68] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018, doi: 10.1109/TII.2018.2791944.

[69] M. Alhammami and S. M. Hammami, "An FPGA-based IP for recognizing violence against children," *MethodsX*, vol. 8, Jan. 2021, Art. no. 101378, doi: 10.1016/j.mex.2021.101378.

[70] S. Rajagopalan, S. Janakiraman, A. Rengarajan, S. Rethinam, S. Arumugham, and G. Saravanan, "IoT framework for secure medical image transmission," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2018, pp. 1–5, doi: 10.1109/ICCCI.2018.8441284.

[71] I. Aydin and N. A. Othman, "A new IoT combined face detection of people by using computer vision for security application," in *Proc. Int. Artif. Intell. Data Process. Symp. (IDAP)*, Sep. 2017, pp. 1–6, doi: 10.1109/IDAP.2017.8090171.

[72] N. Patil, S. Ambatkar, and S. Kakde, "IoT based smart surveillance security system using raspberry pi," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2017, pp. 344–348, doi: 10.1109/ICCSP.2017.8286374.

[73] K. Casey. *Edge Computing and IoT: How They Fit Together*. The Enterprisers Project. Accessed: Jun. 18, 2022. [Online]. Available: https://enterprisersproject.com/article/2021/3/how-edge-computing-and-iot-fit-together

[74] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, "Edge computing in IoT-based manufacturing," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 103–109, Sep. 2018, doi: 10.1109/MCOM.2018.1701231.

[75] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 110–115, Nov. 2018, doi: 10.1109/MCOM.2018.1700906.

[76] Q. Yao, K. Xu, T. Li, Y. Zhou, and M. Wang, "A secure image evidence management framework using multi-bits watermark and blockchain in IoT environments," *Wireless Netw.*, Jan. 2023, doi: 10.1007/s11276-023-03229-4.

[77] S. Alshathri and E. E.-D. Hemdan, "An efficient audio watermarking scheme with scrambled medical images for secure medical Internet of Things systems," *Multimedia Tools Appl.*, vol. 82, no. 13, pp. 20177–20195, May 2023, doi: 10.1007/s11042-023-14357-6.

[78] A. Sardar, S. Umer, R. K. Rout, S.-H. Wang, and M. Tanveer, "A secure face recognition for IoT-enabled healthcare system," *ACM Trans. Sensor Netw.*, vol. 19, no. 3, pp. 1–23, Aug. 2023, doi: 10.1145/3534122.

[79] A. Altameem, P. P, S. T, R. C. Poonia, and A. K. J. Saudagar, "A hybrid AES with a chaotic map-based biometric authentication framework for IoT and industry 4.0," *Systems*, vol. 11, no. 1, p. 28, Jan. 2023. [Online]. Available: https://www.mdpi.com/2079-8954/11/1/28

[80] S. John and S. N. Kumar, "IoT based medical image encryption using linear feedback shift register—Towards ensuring security for teleradiology applications," *Meas., Sensors*, vol. 25, Feb. 2023, Art. no. 100676, doi: 10.1016/j.measen.2023.100676.

[81] J. Cheng, Q. Feng, C. Li, and W. Yang, "Securing FPGAs in IoT: A new run-time monitoring technique against hardware trojan," *Wireless Netw.*, Mar. 2023, doi: 10.1007/s11276-023-03305-9.

[82] V.-A. Adeyemi, E. Tlelo-Cuautle, Y. Sandoval-Ibarra, and J.-C. Nuñez-Perez, "FPGA implementation of parameter-switching scheme to stabilize chaos in fractional spherical systems and usage in secure image transmission," *Fractal Fractional*, vol. 7, no. 6, p. 440, May 2023. [Online]. Available: https://www.mdpi.com/2504-3110/7/6/440

[83] N. A. Bharadwaj, M. Afsar, K. K. Khaitan, and C. Gururaj, "Efficient FPGA-based implementation of image segmentation algorithms for IoT applications," in *Low Power Architectures for IoT Applications*, D. K. Sharma, R. Sharma, G. Jeon, and Z. Polkowski, Eds. Singapore: Springer, 2023, pp. 25–45.

[84] M. Harun-Ar-Rashid, O. Chowdhury, M. M. Hossain, M. M. Rahman, G. Muhammad, S. A. AlQahtani, M. Alrashoud, A. Yassine, and M. S. Hossain, "IoT-based medical image monitoring system using HL7 in a hospital database," *Healthcare*, vol. 11, no. 1, p. 139, Jan. 2023. [Online]. Available: https://www.mdpi.com/2227-9032/11/1/139

[85] O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, and D. Z. Rodríguez, "Transfer learning approach to IDS on cloud IoT devices using optimized CNN," *IEEE Access*, vol. 11, pp. 1023–1038, 2023, doi: 10.1109/ACCESS.2022.3233775.

[86] G. C. Kagadis, C. Kloukinas, K. Moore, J. Philbin, P. Papadimitroulas, C. Alexakos, P. G. Nagy, D. Visvikis, and W. R. Hendee, "Cloud computing in medical imaging," *Med. Phys.*, vol. 40, no. 7, Jun. 2013, Art. no. 070901.

[87] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," *IEEE Netw.*, vol. 33, no. 2, pp. 111–117, Mar. 2019, doi: 10.1109/MNET.2019.1800254.

[88] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, "Edge computing with artificial intelligence: A machine learning perspective," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–35, Sep. 2023, doi: 10.1145/3555802.

[89] A. K. Nair, J. Sahoo, and E. D. Raj, "Privacy preserving federated learning framework for IoMT based big data analysis using edge computing," *Comput. Standards Interface*, vol. 86, Aug. 2023, Art. no. 103720, doi: 10.1016/j.csi.2023.103720.

[90] H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of blockchain and edge computing in Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 144, pp. 307–326, Jul. 2023, doi: 10.1016/j.future.2022.10.029.

[91] D. Yang, I. Doh, and K. Chae, "Secure medical image-sharing mechanism based on visual cryptography in EHR system," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 463–467, doi: 10.23919/ICACT.2018.8323796.

[92] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," *Sustain. Cities Soc.*, vol. 55, Apr. 2020, Art. no. 102023, doi: 10.1016/j.scs.2020.102023.

[93] G. T. S. Ho, Y. P. Tsang, C. H. Wu, W. H. Wong, and K. L. Choy, "A computer vision-based roadside occupation surveillance system for intelligent transport in smart cities," *Sensors*, vol. 19, no. 8, p. 1796, Apr. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/8/1796

[94] H. Nizam, S. Zafar, Z. Lv, F. Wang, and X. Hu, "Real-time deep anomaly detection framework for multivariate time-series data in industrial IoT," *IEEE Sensors J.*, vol. 22, no. 23, pp. 22836–22849, Dec. 2022, doi: 10.1109/JSEN.2022.3211874.

[95] B. Liu, C. Han, X. Liu, and W. Li, "Vehicle artificial intelligence system based on intelligent image analysis and 5G network," *Int. J. Wireless Inf. Netw.*, pp. 86–102, Sep. 2021, doi: 10.1007/s10776-021-00535-6.

[96] K. Nimmy, S. Sankaran, K. Achuthan, and P. Calyam, "Lightweight and privacy-preserving remote user authentication for smart homes," *IEEE Access*, vol. 10, pp. 176–190, 2022, doi: 10.1109/ACCESS.2021.3137175.

[97] J. Chen, G. Bai, S. Liang, and Z. Li, "Automatic image cropping: A computational complexity study," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 507–515, doi: 10.1109/CVPR.2016.61.

[98] E. Hamuda, M. Glavin, and E. Jones, "A survey of image processing techniques for plant extraction and segmentation in the field," *Comput. Electron. Agricult.*, vol. 125, pp. 184–199, Jul. 2016.

[99] R. Fontugne, T. Hirotsu, and K. Fukuda, "An image processing approach to traffic anomaly detection," in *Proc. 4th Asian Conf. Internet Eng.*, Nov. 2008, pp. 17–26, doi: 10.1145/1503370.1503377.

[100] S. S. Sarikan and A. M. Ozbayoglu, "Anomaly detection in vehicle traffic with image processing and machine learning," *Proc. Comput. Sci.*, vol. 140, pp. 64–69, Jan. 2018, doi: 10.1016/j.procs.2018.10.293.

[101] E. Griffiths, S. Assana, and K. Whitehouse, "Privacy-preserving image processing with binocular thermal cameras," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 1, no. 4, p. 133, 2018, doi: 10.1145/3161198.

ABBAS M. AL-GHAILI received the B.Eng. degree (Hons.) in computer engineering from the University of Science and Technology, Sana'a, Yemen, in 2005, and the M.Sc. and Ph.D. degrees in computer systems engineering from Universiti Putra Malaysia (UPM), Serdang, Malaysia, in 2009 and 2013, respectively. He is currently a Senior Lecturer with the Department of Computing, College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), Malaysia, where he has been a Postdoctoral Researcher with the Institute of Informatics and Computing in Energy (IICE), since February 2018. His research interests include energy informatics, image processing, artificial intelligence, information security, metaverse, and the Internet of Things (IoT). He is a member of the International Association of Computer Science and Information Technology and the Universal Association of Computer and Electronics Engineers.

SARASWATHY SHAMINI GUNASEKARAN received the M.Sc. degree from Universiti Putra Malaysia (UPM), in 2013, and the Ph.D. degree in information and communication technology from Universiti Tenaga Nasional (UNITEN), Malaysia, in 2017. She is currently the Director of the Institute of Informatics and Computing in Energy (IICE), UNITEN. Her research interest includes artificial intelligence. She looks forward for collaboration possibilities in the areas of agent technology, essentially in the field of social commerce and smart sustainable cities.

NORZIANA JAMIL is currently with the Department of Information Systems and Security, College of IT, United Arab Emirates University, United Arab Emirates. She was the Director of the Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional. She is also an Associate Professor with United Arab Emirates University. With an extensive professional journey spanning over two decades, she has garnered a wealth of expertise in the realm of data and cyber security research, and its practical application. Her research interests include cryptography, data security, security for cyber physical systems, security analytics, and intelligent systems. She has published over 100 research manuscripts in esteemed, high-impact journals. Furthermore, she is also a reviewer for numerous international journals, affirming her active involvement and recognition within the scholarly community.

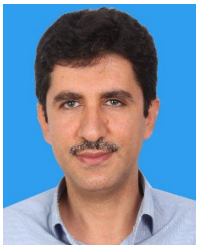
ZAID ABDI ALKAREEM ALYASSERI received the B.Sc. degree in computer science from Babylon University, in 2007, the M.Sc. degree in computer science from University Science Malaysia (USM), in 2013, and the Ph.D. degree in the field of artificial intelligence (brain-inspired computing) from the Computational Intelligence Research Group, School of Computer Sciences, in 2020. He is currently an Assistant Professor with the University of Kufa, Iraq. His research interests include optimization, pattern recognition, EEG, brain–computer interface, signal and image processing, machine learning, and deep learning.

NAIF MOHAMMED AL-HADA received the M.Sc. degree in applied radiation physics and the Ph.D. degree in nanoscience and nanotechnology from Universiti Putra Malaysia (UPM), in 2011 and 2015, respectively. He has been a Lecturer with the Institute of Biophysics, Dezhou University (DZU), China, since October 2019. From 2015 to 2019, he was a Postdoctoral Researcher with the Department of Physics, UPM. From June 2019 to July 2022, he was a Visiting Researcher with Universiti Teknologi Malaysia (UTM), Malaysia. He has been a Visiting Researcher with Istanbul Technical University (ITU), Turkey, since August 2022. His research interests include nanoparticle synthesis and applications; metallic oxide nanostructures and their antibacterial activity, binary oxide nanostructures for solar cell and sensor applications, and renewable energy.

ZUL-AZRI BIN IBRAHIM received the Bachelor of Information Technology degree in computer networking from Universiti Utara Malaysia, in 2002, and the Master of Science degree in information technology from Universiti Teknologi MARA, in 2009. Since 2009, he has been a Lecturer with Universiti Tenaga Nasional, where he is currently a Lecturer. His research interests include cyber security, advanced metering infrastructure, digital forensics, and threat intelligence.

ASMIDAR ABU BAKAR is currently a Senior Lecturer with the College of Computing and Informatics (CCI), Universiti Tenaga Nasional (UNITEN), with nearly 20 years of experience in academia. Over the course of her career, she has contributed significantly to her field, publishing a number of articles in both journals and conferences. Her research interests include access control in mobile networks, information security, privacy, and trust.

HAIROLADENAN KASIM received the bachelor's degree in information technology from Universiti Utara Malaysia, in 1998, and the master's degree and the Ph.D. degree in information management from Universiti Teknologi Mara, in 2007 and 2015, respectively. He is currently with the Department of Informatics, College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN). He is a Certified Information Security Management System Auditor (CISMA) and a Certified HRDF Trainer. He has conducted research on information systems (business informatics), computing in social science, security management, energy management, knowledge management, and computer and society. His research interests include energy informatics and energy and computing.



EGHBAL HOSSEINI received the B.Sc. and M.Sc. degrees in applied mathematics and operations research in Iran, and the Ph.D. degree in optimization from Tehran Payame Noor University in 2015. He is currently working with Institute of Informatics and Computing in Energy (IICE), UNITEN as a Post-Doctoral Researcher. Before that, he was with RoRo Green Project as a researcher with Roskilde University. He was working as a Senior Researcher with Erbil Polytechnic University, and an Assistant Professor at the University of Raparin, from 2017 to 2021. From 2017, he has proposed five new meta-heuristics: Laying Chicken Algorithm (LCA), Big Bang Algorithm (BBA), Volcano Eruption Algorithm (VEA), Multiverse Algorithm (MVA), Covid-19 Optimizer Algorithm (CVA), Gradient-Simplex Algorithm (GSA), and Evolutionary-Gradient Algorithm (EGA). His research interests are meta-heuristic approaches, algorithms, multilevel programming problems and machine learning.

RIDHA OMAR received the master's degree in computer science. He is currently a Senior Lecturer with the Department of Informatics, College of Computing and Informatics. His expertise lies at the intersection of user experience (UX), user interface design (UID), and augmented reality (AR).

RAFIZIANA MD. KASMANI received the Ph.D. degree majoring in vented gas explosion from the University of Leeds, in 2009. She is currently a Senior Academician with the School of Chemical and Energy Engineering, Universiti Teknologi Malaysia. Her research interests include fire engineering, gas and dust explosion, and fire and explosion modeling. She has published more than 70 journals and conference articles to date. Through her experiences and expertise in fire and explosion engineering, she has the opportunity to participate as a speaker in a variety of related courses, conferences, and workshops. She was invited as a keynote speaker on Third Renewable Energy and Green Technology International Conference 2016 in Jakarta, International Symposium on Advanced in Nuclear Engineering, in 2018, and International Symposium on Advanced in Mechanical Engineering in the Pakistan Institute of Engineering and Applied Sciences (PIEAS), Pakistan, in 2019. Besides teaching and research, she served as a technical reviewer to prestige international journals that has allowed for a broad resource base on which to build her career as an educator and a researcher. She was a recipient of AUN-SEED Short-Term Research Program in Japan (SRJP), The University of Tokyo, in 2015, Erasmus + for Staff Mobility Program in Madrid, in 2017, and Fulbright Malaysian Scholar Program for 2017/2018 with the University of Maryland, USA. She continues to build a strong contact network through consultations with local authorities i.e., Malaysia Energy Commission, Department of Occupational Safety and Health (DOSH), and Fire and Rescue Department of Malaysia (BOMBA), among others and private companies.

RINA AZLIN RAZALI received the master's degree in information and technology. She is currently a Lecturer with the Department of Computing, College of Computing and Informatics. Her expertise is in artificial intelligence and renewable energy.