Secure and Power Proficient Design for Trusted Image Transmission in IoT

Dissertation submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Hanisha Verma

(801533006)

Under the supervision of:

Ashish Aggarwal

Assistant Professor, CSED

Rajanpreet Kaur Chahal

Lecturer, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Secure and Power Proficient Design for Trusted Image Transmission in IoT"**, in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Mr. Ashish Aggarwal and Ms. Rajanpreet Kaur Chahal* and refers other researchers' work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Hanisha Verma)
801533006
ME (IS)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Mr. Ashish Aggarwal)
Assistant Professor, CSED

(Ms. Rajanpreet Kaur Chahal)
Lecturer, CSED

ACKNOWLEDGEMENT

First of all, I would like to express my heartfelt appreciation to my supervisor Mr. Ashish Aggarwal and Ms. Rajanpreet Kaur Chahal for their constant guidance, great support, immense patience and valuable advice throughout my research at the Thapar University, Patiala. They helped me in finding research topics, proposing solutions and verifying results. Without their cooperative attitude, endless efforts and advices, this research would have never been possible. It has been a great honor and pleasure for me to do research under their supervision. I sincerely would like to thank Dr. Maninder Singh, Head of the Department, Computer Science Engineering, Thapar University, Patiala for his support during my work.

Last but not the least I would like to thank my family, my colleagues and friends for their encouragement and love.

Hanisha Verma
(801533006)

ABSTRACT

Power consumption has turned into a noteworthy worry in portable applications. A power proficient design of Secure Better Portable Graphic (SBPG) compression architecture is proposed by our thesis for real time intelligent traffic surveillance (ITS) in IoT. Secure Digital Camera (SDC) integrated with SBPG is used to capture the unwanted traffic and transfer image to administration to take some action. To protect the image from tampering, encryption and watermarking is offered by the SBPG module which provides dual layer protection. Without trading off security, aggregation of SBPG and SDC gives the best quality imaging in a power proficient way. A pattern-independent strategy has been embraced to evaluate the power where numerous simulations keep running in the outline with various inputs and moderate of power scattered is considered.

In order to calculate the power from the output of design, voltage and current esteems are considered. Simulink® is used to achieve this by using power blocks and sensors available. In the revised scheme, Discrete Cosine Transform (DCT) based watermarking embedding algorithm is proposed. Proposed scheme is able to tackle the collusion attack by making use of Pseudo Random Number (PRN) along with permutation vector. To make the scheme resistant against rotation attack, square blocks present in the center of channel are embedded for watermark. It is observed from the outcome that the power utilization is considerably reduced with large peak signal to noise ratio.

Keywords— Internet of Things, Security, SBPG, Image Communication, Power Proficiency.

TABLE OF CONTENTS

LIST OF FIGURES

Figure No. **Page No.**

LIST OF TABLES

Table No. **Page No.**

ABBREVIATIONS

IoT	Internet of Things
RFID	Radio Frequency Identification
GPS	Global Position Systems
WSN	Wireless Sensor Network
ITS	Intelligent Traffic Surveillance
SDC	Secure Digital Camera
SBPG	Secure Better Portable Graphic
DCT	Discrete Cosine Transformation
QoS	Quality of Service
VQ	Vector Quantisation
AES	Advance Encryption Standard
HEVC	High Efficiency Video Coding
AVC	Advance Video Coding
CSD	Canonical Signed Digit
CSE	Common Sub-expression Elimination
PTZ	Pan-Tilt-Zoom
DWT	Discrete Wavelet Transformation
DFT	Discrete Fourier Transform
DC	Digital Camera
FSM	Finite State Machine

PSNR	Peak Signal to Noise Ratio
PRN	Pseudo Random Number
AC	Alternating Component
GUI	Graphical User Interface
MSE	Mean Squared Error

CHAPTER 1

INTRODUCTION

1.1 Internet of Things

The Internet of Things (IoT) alludes to an organized interconnection of everyday objects (including users), so empowering objects to associate and coordinate with each other anytime. It broadens the Internet into the physical world with the end goal that objects can be overseen remotely. To internet service, IoT acts as a physical access point. IoT changes the way we perform ordinary exercises by real time tracking of physical objects. To get an uplifted attention of real time occasions, it makes use of sensors in framework (e.g., rooms and structures). To accomplish an improved situational mindfulness, it utilizes RFID (Radio Frequency IDentification) to capture contexts of object (e.g., location). To ensure safe driving and green travel, it utilizes bits to track transportation frameworks. Readings from substantive sensors for objects are various and to a great degree dynamic. We will have many billions of RFID-tagged things by, creating billions of sensor readings each minute. This shows we have a large working space containing small things. Given that trillions of sensors installed or deployed into frameworks and items – are regularly getting readings, IoT works in a substantially bigger data space than that of the Internet. In addition, sensor readings are profoundly dynamic. Readings change with objects and conditions of environment [1]. For instance, IoT may procure a guest's area by GPS (Global Position Systems).The Internet of things alludes to different data detecting gadgets and innovations, for example, sensors, RFID (Radio Frequency Identification Devices), GPS (Global Position System), infrared sensor, laser scanner, and gas inductor, and so forth.

It gathers in real time, an object or process which should be checked, connected and associated. It gathers different request data, including sound, light, warmth, power, mechanics, science, area, and so on. The extent of IoT is to interface machine to machine, machine to man, and man to man. Integration and unification of

all the systems that surround us, is the main objective of IoT. By doing so, one system can get control of or can communicate with other system to provide a new generation of assistive service. A lot of applications are being developed and connected to internet day by day so it is important to assure information security. To accomplish certain tasks, smart technologies are employed with the use of priori knowledge. By teaching smart technologies, the objects get intelligent enough and can interact with users also.

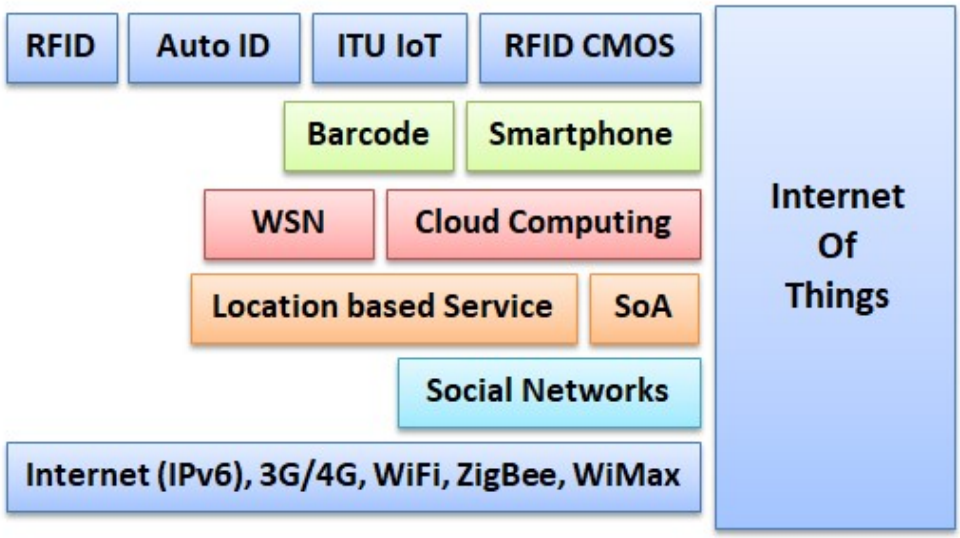

Figure 1.1: Technologies associated with IoT

Artificial intelligence, intelligent signal processing, advance machine- human interaction etc. are some researches which adapt smart technology. In addition, many other technologies are associated with IoT as shown in Fig. 1.1 cloud computing, smart phones, wireless sensor network (WSN), social networks and barcodes are collectively form a network which supports IoT.

1.2 Architecture of Internet of Things

Internet of Things can be isolated into 3 layers: perception layer, network layer, and application layer. The perception layer comprises of GPS, two-dimension code tag along with code reader, sensor network, RFID tag and reader, camera, sensor gateway, all kinds of sensors, M2M terminal etc. The fundamental motive of this

layer is observation and identification of things, and gathering and getting data [2]. The network layer is formed by various types of communication networks and converged networks. It has been generally acknowledged that this is developing part of network architecture. In addition, the IoT administration center and data center are the parts of network layer. In other words, the network layer has the capacity of network operation, as well as ought to enhance the capacity of data operation. The network layer which is mainly answerable for transforming the information work consists of wireless and wired networks, communication channels, network interface and intelligent processing. The application layer is the Internet of Things innovation joined with industry ability to accomplish an expansive arrangement of smart application solutions. Through the application layer, IoT can accomplish the task of reconciliation of data innovation with the business which can be used for long period of time. It will have an great impact on financial and social improvement. The main issue of the application layer is sharing and security of data. Fig 1.2 explains the layered architecture of IoT and work associated with each layer. Internet of Things (IoT) comprises of a several tiny gadgets associated together to frame a shared processing framework. IoT forces particular imperatives as far as connectivity, computational power and vitality spending plan, which make it unique in relation to those mulled over by the standard convention of security in distributed system.

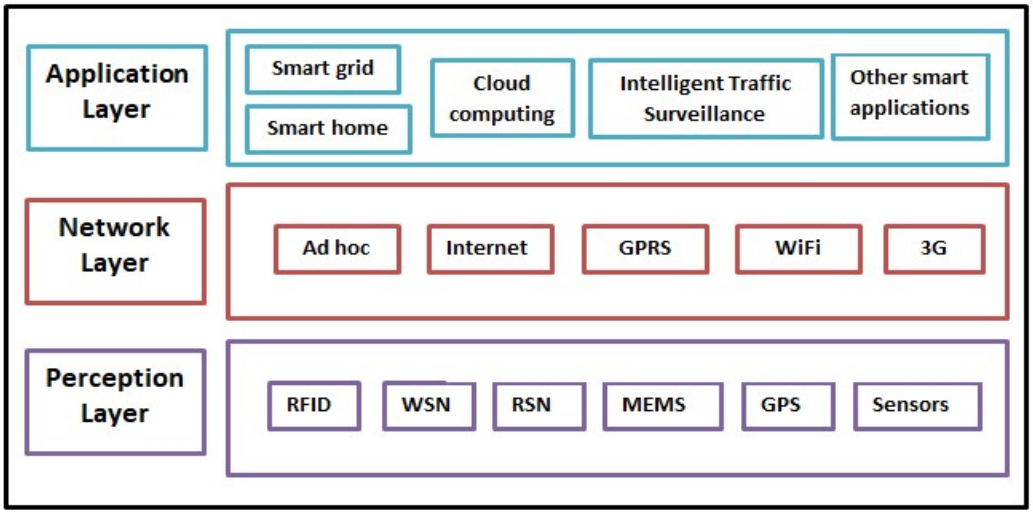

Figure 1.2: Layered Architecture of IoT

IoT applications can convey comfort to individuals, yet in the event that it can't guarantee the security of individual protection, private data might be spilled at any time. So the security of IoT can't be overlooked [3]. Once the signal is stolen or interfered with, it will specifically influence the security of the whole data of IoT. With the general spreading of IoT, it will give more broad knowledge of data, the danger of leakage of such data will increment. On the off chance that IoT can't have a decent answer for security issues, it will to a great extent limit its advancement. In this manner, over every one of the issues of IoT, security issue is especially vital. IoT, as a combination of heterogeneous systems, not just includes a similar security issues with sensor arrangement, mobile communication network and the internet, additionally more specific ones, for example, security assurance issue, heterogeneous system confirmation and access control issues, data store and administration, and so on [4]. The exploration of IoT security is not quite the same as that of internet security, for it is much more entangled.

1.3 Characteristics of Internet of Things

Internet of thing includes three major characteristics [2].

- Extensive sense:

  Collect information of objects anytime, anywhere, with use of RFID, two dimension code and sensors to accomplish an improved situational mindfulness. Deploy sensors in infrastructure for uplifted consciousness of constant occasions. IoT appoints objects of daily life with unique identification and associate with internet, by using RFID and sensors. In this way all the objects are mapped with internet and can be dealt anytime. As sensors are sensing continuously, so the readings keep changing as the information is changing rapidly.

- Credible transmission:

  The information is transmitted over the web where number of networks are connected with each other and massive amount of data is transmitted by this heterogeneous network. So it is important to maintain the security to protect the information from leakage. IoT deliver explicit real-time information of things through intermixed telecommunication networks and internet, reliably.

- Inventive processing:

  For implementation of inventive control of objects, it analyses and process massive amount of data and information by using intelligent computing such as fuzzy identification and cloud computing. As information of users and environmental features is captured by the sensors, however these readings are just information about objects. As individuals move regularly and same object may be monitored by multiple sensors. So it is essential for IoT to identify the objects to accommodate smart space and lightweight representation. IoT should handle the interaction in proper manner so that the system must be organised properly, irrespective of number of objects connected and their interaction.

1.4 Security in IoT

1.4.1 Sources of Threat

It is feasible now to understand the sources of threat by studying different layers of IoT system. Sources of threats are basically attackers which pose danger to the system to breach the data or infect the data by doing malicious activities without leaving any footprints behind [5]. Attacker could be part of the system or may be an outsider who has link to inside activities. There are three primary users that pose dangers to the security and protection in IoT:

- Malicious User:

  Malicious user is the holder of the IoT appliance with potential to perform intrusion to understand the secrets of maker, and access confined services. By revealing the flaws in the framework the noxious user can get information, share confidential data to outsiders, or even assault comparative frameworks.

- Bad Manufacturer:

  Bad manufacturer is the maker of the appliance with the capacity to exploit the technology to breach data about the clients, or other IoT gadgets. Such a producer can purposely present security gaps in its outline to be exploited later on for getting client's information and presenting it to outsiders. Similarly, the generation of inadequately secured products results in trading off the clients protection. What's more, in IoT where distinctive items associate with each other, a producer can assault other contenders' gadgets to damage their reputation.

- External Adversary:

  External adversary is an outside individual who is not member of the framework and has no approved access to it. Adversary would attempt to breach information about the client of the framework for malignant purposes, for example, causing financial harm and undermining the client's validity. Likewise, by changing the sensing information, adversary will try to defect the system, for example, transmitting electromagnetic signals to infuse bogus information.

1.4.2 Classes of Attacks Impact

Analysing the assaults on a framework is mandatory for understanding the dangers. Different categories are addressed for identification of threats [5]. These threats pose different impacts on the system like:

- Device Tampering:

  IoT gadgets are tiny gadgets integrated in different frameworks, for example, oven, light switches, TVs, cars, and others. Some of IoT gadgets do not come online for long time hence can be effortlessly stolen without being taken note. Once a gadget falls into the wrong hands, different sets of assaults can be performed, for example, stealing, manipulation of software, and equipment altering. An adversary can mess with the gadget and utilize it to embed impostor to the framework, utilize the gadget maliciouly or out of its proposed usefulness.

- Side-Channel:

  Private and confidential information established on, for example, timing examination of the execution, power utilization, traffic investigation, analysis of fault, and electromagnetic investigation of the gadget, can be breached.

- Privacy Breach:

  It is not at all like information disclosure. An adversary does not really need access to confidential data to find out about the client. The adversary can deduce private data from different sources, for example, meta information and by traffic examination.

- Elevation of Privilege:

  It is a condition in which an unprivileged client gets advantaged access to a gadget/benefit. This can be accomplished by introducing an impostor in the

framework that puts on a show to be another gadget, which has special access in the framework.

- Denial-of-Service:

  Denial of service alludes to the property of being blocked off when requested by an approved client. The framework must be able to keep functioning even when some undesired activity is being performed by malevolent clients. This class of assaults can be performed by appliance piracy, controlling its product, or disrupting the correspondence channel.

- Signal Injection:

  It is the point at which an attacker infuses fake information into the framework to change the detected information, for example, electromagnetic signals are transmitted to sensor.

- Information Disclosure:

  Information disclosure is the uncovering of information to an individual who does not have consent to see it. This incorporates unplanned presentation, directed assault, and derivation or connection. An assailant can get data by listening stealthily on the system channel, physical access to the gadget, or through getting to the gadget over the system.

- Spoofing:

  Spoofing alludes to gaining access to inaccessible service by making use of others accreditations. The accreditations can be acquired straightforwardly from a gadget, using eavesdropping on the correspondence channel, or by phishing attack.

1.4.3 Secure Architecture Development

The IoT structure is isolated into three layers generally, including perception layer, network layer and application layer. Processing layer is taken by some systems for network backing technology (for example, computing technology, network processing, and middleware innovation). The perception layer includes RFID tag, sensor networks, smart cards, WSN sensors which ensure the uprightness and secrecy of data. The network layer which is mainly answerable for transforming the information task consists of wireless and wired networks, communication channels, network interface and intelligent processing. The application layer is responsible for the examination of

data and furthermore controls basic leadership to accomplish altered smart applications and administrations, and eventually accomplish the control\connection\identification among personals and materials. This layer also export functionality for particular applications and provide embedded interface. This chain of importance present that the construction of security components of things ought depends on specialized attributes of each layer and manage security dangers [3] .

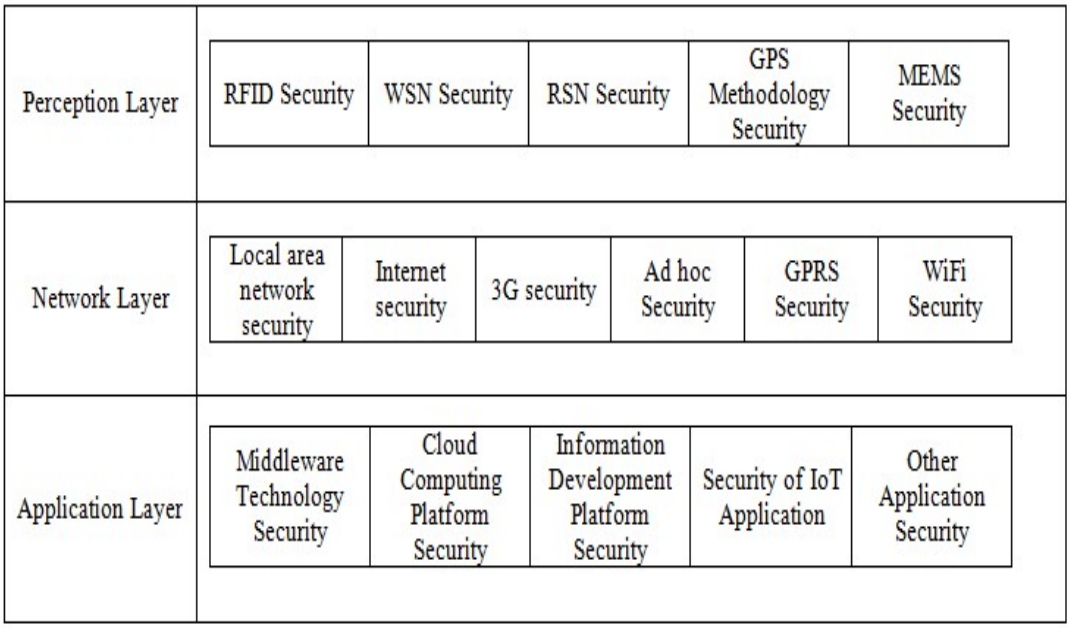

Figure 1.3: Secure Architecture Development

IoT security can be explained as: handling information securely, reliable transmission of data, and awareness of information security [6]. IoT must insure security at all layers and additionally incorporate the security of entire framework crossing the perception layer, network layer and application layer as shown in Fig 1.3. Perception layer consists of RFID security, RSN security, WSNs security etc. Transportation layer incorporates core system security, access network security, security of local network. The sub-layer includes WiFi security, security of Ad-Hoc network, 3G access network security and others. Distinct network transmission has distinct technology. Application layer consists of particular IoT applications and application support layer. The security at this layer includes cloud computing platform security, service support platform security, information development platform security in application support layer and

IoT application includes smart home security, smart grid security and other application security. IoT applications in different businesses have distinct necessities.

1.5 Applications of Internet of Things

As application layer consists of integrated application business, for example, smart home, brilliant security, smart grid and so on. Application with number of smart feature are developing and making the world smart. These applications are easy to use and do excellent work for humans. Some of these applications are wearable devices, connected cars, home automation, and smart city like projects. Intelligent traffic surveillance (ITS) is application of IoT which monitor the roads for traffic congestion, accidents and other unexpected situation [2]. So that appropriate actions could be taken by the authorities.

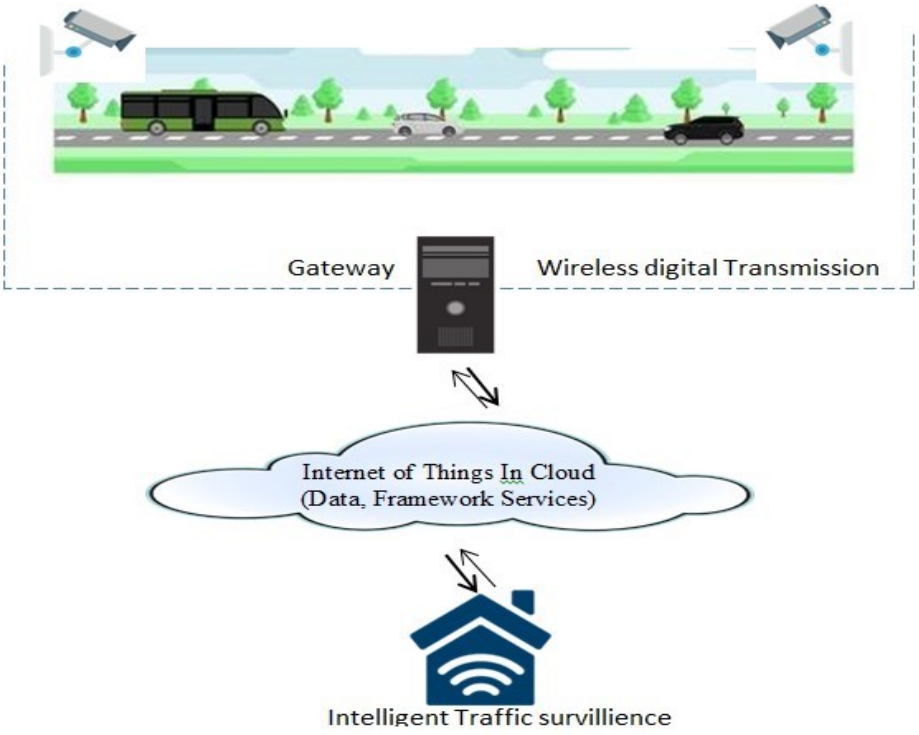

Figure 1.4: Components of ITS in IOT

ITS system through IoT which incorporates the secure digital camera (SDC) integrated with secure better portable graphic (SBPG). The main role of this system is to keep track the situations and monitor all the paths to address all the problems such

as unwanted accidents, traffic jam and other conditions affecting normal situations as shown in Fig 1.4. This led to formation of large chain of connection which covers the entire city and makes the system intelligent. Further other cities can connect their system and communicate with each other to make the system more intelligent. Breaking down information from one end of the framework to comprehend its effect on the flip side of the framework should be possible easily. For instance, a mishap on a roadway can be identified by the smart camera which will send the data to the city wide transportation framework, where the data will be investigated and the effect of the mischance will be computed, to see how it will influence traffic on different sections of the street. In the event that the mishap happens, for instance, close to an air terminal or almost a school, at that point the frameworks could speak with each other to modify flights or change school plan. The frameworks could likewise tell drivers through the city computerized sign framework about option courses and give them directions on the best way to dodge the mischance. While this is only a straightforward illustration, the presentation of the IoT in ITS could bring innumerable preferences and benefits.

1.6 Need of Study

IoT emerges a lot of applications in its infrastructure in which a lot of things are connecting to each other and communicating to each other. Information can be private information or may contain some credentials of user so it is important to maintain the security of multimedia information transmitted over the network. As to do the task a lot of power is consumed by application to accomplish their task so it is important to utilize power in IoT system to make the system more smart and intelligent. As in our IoT application, we are dealing with image so it is important to protect the image from tempering and other malicious activities by securing it with appropriate security mechanism. As image captured by secure digital camera (SDC) is of high resolution so it is important to make the design power proficient so less energy could be consumed. By using security mechanism we will secure the application without compromising with the quality of image and will also work on making the design power proficient.

1.7 Structure of Dissertation

This dissertation is basically divided into five main chapters. Chapter 1 contains the introduction of the IoT. It gives a brief description about IoT and security of IoT. Chapter 2 presents the background of our work and a brief vision on prior related work done by researchers. Problem statement and research questions are presented in chapter 3. Chapter 4 describes the proposed work done to overcome the problem stated in chapter 3. In chapter 5, results obtained by testing and analyzing revised scheme are shown. Chapter 6 describes the conclusion and future scope.

1.8 Summary

This chapter summarizes necessary basic characteristics and reliable information of IoT. Architecture of IoT containing the all layers is explained briefly. Various security attacks, impact of attack and secure architecture of IoT are discussed in this chapter. In addition it also describes application of IoT on which we are working on.

CHAPTER 2

REVIEW OF STATE OF ART

In this chapter, the work of researchers has been surveyed for enhancement in secure better portable graphic module integrated with secure digital camera in IoT. In this review the performance and design goals of distinct watermarking techniques are presented and various issues which affect the performance during embedding of watermarking technique are also mentioned. Different researches are studied in this review to find the appropriate solution to the problem.

2.1 Background

The explosive development of the need of the communication for data between machines raised concerns, for example, the enhancement of the human condition, the administration of urban security, the change of living quality, and the successful administration of generation, the "Internet of Things" (IoT) is in incredible request. As innovation propels in the advancement of gadgets, for example, Wi-Fi able tablets, cell phones and other convenient gadgets, IoT are progressively getting to be noticeably well known. Research has been conducted on transmission of real time multimedia data like image, video and audio in different IoT application. As security is main concern in IoT because numbers of things are connecting to internet everyday so different attacks on the data are also studied.

Research has been conducted on distinct watermarking techniques to make the secure better portable graphic (SBPG) module power proficient without compromising the quality of image. Distinctive strategies and diverse reproduction conditions give diverse outcomes and there is along these lines need to widen the range to represent impacts not contemplated in a specific domain. In this we evaluate the performance of image quality and power by studying different watermarking techniques in discrete cosine transformation (DCT) domain. In this, we use image to study the effects of watermarking on power and quality of service (QoS). Various attacks and solution to those attacks are also studied that attack the watermarked image while transmission

over the network. Our schematic design does provide implementation of theoretical concepts in practical implementation. At first it was difficult to analyse which technique is better and in which way we should go but the prior research done helped a lot to understand the problem and finding solution to that problem.

2.2 Relevant Work

Lin, Shie et al. [7] provides a DCT-based image watermarking based on the idea of mathematical remainder. This technique used the low-frequency coefficients in frequency domain and modifies the coefficients on basis of the mathematical remainder concept. Even after attacked by distinct image processing operations, the watermark embedded by this scheme can survive strongly for JPEG compressed images. This technique works well with highly compressed images with JPEG format and transmitted over the internet.

A watermarking approach is proposed by researchers Huang and Fang [8], for copyright protection of images. This scheme generally modifies the chosen coefficients of the content of image to accomplish the embedding. Algorithm and application integrate the EXIF metadata of image and error control codes in it. For better protection and high performance channel coding is employed. Technique can be applied on the ordinary images captured by the normal camera also. The idea of using EXIF metadata is basically that if the information of marked image is modified, from channel decoding process the metadata can be recovered easily.

Procedures for advanced picture altering are winding up noticeably more complex and far reaching. Copy-move fraud is one of the altering systems that are often utilized. In this research, Huang, Lu, Wei Lu, et al. [9] made an effort to make an enhanced DCT-based technique is created to distinguish this particular artefact. The picture is isolated into fix size overlapping blocks firstly and, DCT is activated to each block to speak to its elements. Truncating is utilized to decrease the measurement of the components. At that point the component vectors are lexicographically arranged and, copied picture blocks will be neighboring in the arranged list. In matching step the duplicate blocks of image are compared.

Lu and Sun [10] provide a novel advanced picture watermarking method in view of vector quantisation (VQ) has been exhibited. It is mystery and productive. The water-stamped picture is hearty to VQ pressure with a similar code-book. This strategy utilizes code-word files to convey the watermark data. At first the image in VQ is decomposed into vectors and then best match if founded for each vector in codebook. Research is presented basically a compression scheme with low bit rate.

In study [11], MACQ and DITTMANN et al. discusses various issues related to scenario on digital rights management demand and related to image watermarking. There are many categories of attack presented by research like removal attacks, protocol attacks, cryptographic attacks, and geometrical attacks. Algorithm proposed by author which uses web based approach, evaluate the quality of image under geometrical transforms. Research addresses some issues like finding the strength of attack and combinations of attack depending upon the image characteristics. Mostly benchmark systems consider the collusion attacks and cryptographic attacks, while other attacks like protocol attack are not taken under consideration.

Blind video watermarking technique is proposed by Karmakar, Phadikar et al. [12] which is based on DCT and is resistant to rotation attack. To accomplish the goal, complex Zernike moments and permutation vectors are used. The research has designed the scheme in such a way that for successive frames of video, embedding blocks will very. The rotation invariance property is used to reach the goal. The Zernike moment of blocks which are computed for embedding is calculated and to predict the rotation angle of video invariance property is exploited.

Albalawi, P.Mohanty et al. [13] proposes a technique in which secure digital camera (SDC) is integrated with secure better portable graphic compression algorithm. This research gave two basic advantages of this technique, one is this technique is efficient enough for real time applications in IoT and other is it provide two layer protection. BPG compression module uses inter and intra prediction in this approach and watermarking is done in frequency domain. By doing so this method reduces the temporal and spatial redundancy.

An exclusive approach of integrating watermarking chip with a digital camera for getting watermarking images is introduced. The chip can also be integrated in JPEG encoder. The algorithm presented by Ramesh and Majeed [14], follows pixel by pixel processing and is capable of doing two different type of watermarking in spatial domain. Tian and Tai in study [15] explained how image captured by digital camera can be secured using robust and semi-fragile watermarks. Watermarks are generated using biometric data of owner and frequency contents of image. This scheme provides both protection and authentication.

For advance encryption standard (AES) algorithm that performs both encryption and decryption, VLSI architecture is presented by Mohanty et al. [16]. Round keys are required for each round and keys of length 192 and 256 can be implemented easily. For implementation of multiplicative inverse, S-boxes are used and shared. Both reverse and forward key scheduling can be implemented which allow efficient area minimization.

The High Efficiency Video Coding (HEVC) standard is used over Advanced Video Coding (AVC), as is newly designed compressor and provide improved video compression. Distinct verification tests were directed by the joint collaborative team [17] to figure out its performance. The outcomes of the tests prove that HEVC work at only half of bit rate as compared to AVC, while giving same quality. For compression of image a new design is presented by Jridi and Alfalou [18], in which high speed and low power Discrete Cosine Transform (DCT) is implemented. To implement the constant multiplication, it uses constant multipliers which are based on Canonical Signed Digit (CSD) encoding. This minimizes the number of registers, adders and subtracts. A new approach also examined by the author which reduces the number of operators, based on Common Sub expression Elimination (CSE). With the implementation of CSE, the computations and material complexity reduces which results is power saving. Power consumption relay on the algorithm used to do the computational work as the processing type and algorithm may influence the usage of power.

Wu and Abouzeid [19] in case of sensor networks, it is not always necessary that maximum compression done before the transmission always lead to minimal consumption of energy, with composite signal processing algorithms. A heuristic

algorithm is given to satisfy quality constraints of image while transmission of image in a multi-hop wireless network by selecting optimal image parameters. If compared for both encoding and decoding, images with PNG format consumes more power than the images having format JPEG from the viewpoint of portable devices. Experiments prove that JPEG is perfect choice for both encoding and decoding of images. Digital cameras are used to capture the image to detect, track and classify the vehicles for traffic analysis. In urban area to increase the safety the analysis of behaviour of individual vehicle is carried out using 3D models to detect the unsafe situation and accidents [20], [21]. This permits the arrangement of appropriate locations for grouping and confinements to lanes.

A system is employed by the researchers Khoshabeh et al. [22] that uses an omnidirectional camera along with a pan-tilt-zoom (PTZ) camera in order to capture, analyse traffic flow. While actively moving scene, PTZ is able to achieve refined arrangement by taking advantage of broad viewing area of omnidirectional camera. Scene captured can be analysed in detail due to high resolution even with a simple calibration. Using such a system will also help the drivers choose the right path to overcome the traffic and accident prone area and finding the optimal path [23].

2.3 Secure Better Portable Graphic (SBPG)

The SBPG module is assembled with three units: AES encryption part, watermarking unit and BPG compression unit [13]. The architectural design shown in Fig 2.1 uses the central quarter of the host image captured by the secure digital camera as the center part constitutes the essential information about the image. As encryption and watermarking is done at center quarter portion this will result in best quality, robustness and optimized computational load. Images can be dealt in spatial domain as well as in frequency domain. Spatial domain processes the image directly and analyse image with time but in frequency domain, image is analysed with respect to frequency and processing of image includes distribution and transformation. The watermarking imbedding speed is boosted by doing watermarking in frequency domain using Discrete Cosine Transformation (DCT). To boost the robustness the mid frequency blocks are choose for insertion of watermark. As elimination of any high or low frequency component does not influence the watermark [24]. Then image

is compressed in the BPG encoder phase then the image is transmitted to ITS.

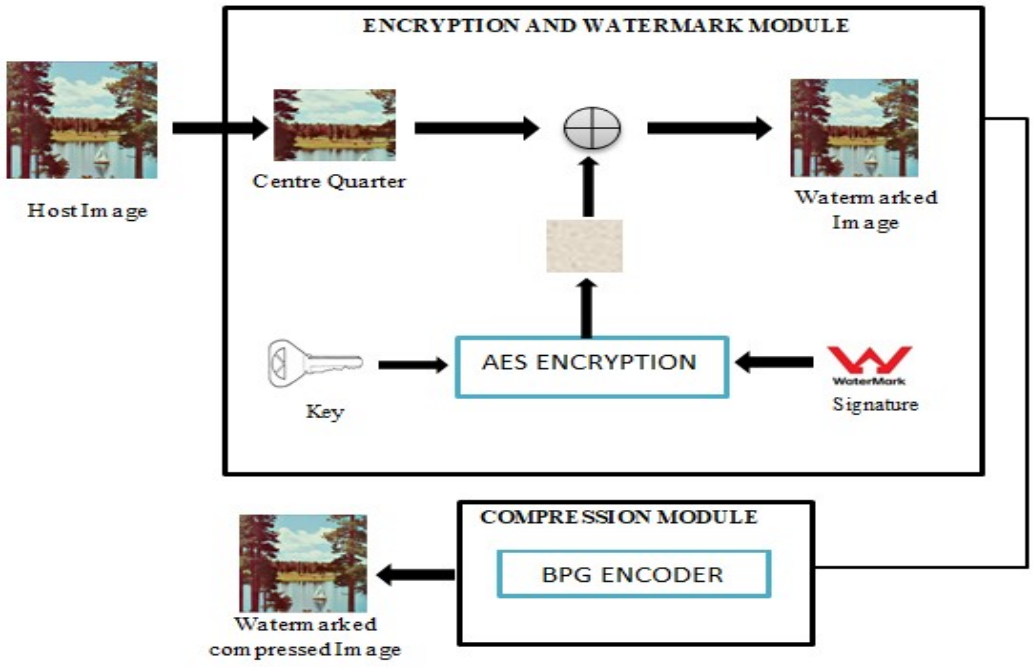

Figure 2.1: Overview of SBPG module

2.3.1 Phases of SBPG module

There are three phases of Secure BPG module: encryption, watermarking and BPG encoder. Now we will discuss each phase of the SBPG module in detail.

- Encryption and Watermarking Phase:

  Center portion of the image is used for insertion of encryption and watermark as by doing so robustness, and quality of image increases. Watermarking can be done in spatial domain or in frequency domain using transformation technique. There are three transformation techniques are present for obtaining the result, discrete cousin transform (DCT), discrete wavelet transform (DWT) and discrete fourier transform (DFT) [25]. From these three DFT is complex transformation from other two so DCT and DWT are used mostly for watermarking process. DWT provide both spatial and frequency representation of image at the same time and work on high frequency components. DCT have high recognition rate and work on low frequency components for global details. DCT provide better energy

compaction then other two and also increase the speed of insertion so mainly DCT domain is used for watermark embedding. The insertion of watermark in image block is done in middle frequency as change in any high or low frequency components will not affect the watermark and robustness will increase. This phase assure the authentication and reliability of communicated data.

- BPG Encoder Phase:

This phase compress the image for reducing the size of the image so that less power is consumed by design for processing the image. BPG image encoder is divided into two phases: Initialisation phase and HEVC encoding phase as shown in Fig 2.2. In the initialisation phase, the encoder read the color space, meta data , bit depth, etc. In HEVC encoding phase [26], the block of basic coding unit is used and is transformed with DCT in frequency domain. HEVC encoding is implemented in three stages. In first stage, motion vector prediction is used for predicting the current motion vector, to ensure from group best candidate is selected. Rate distortion optimization process is used by the encoder. The reconstruction of the blocks is done in second stage. The compressed watermarked image is constructed after passing the blocks from third stage called the bitstream core which includes context adaptive binary arithmetic coding. Controller unit is liable for controlling the process with appropriate sequence.

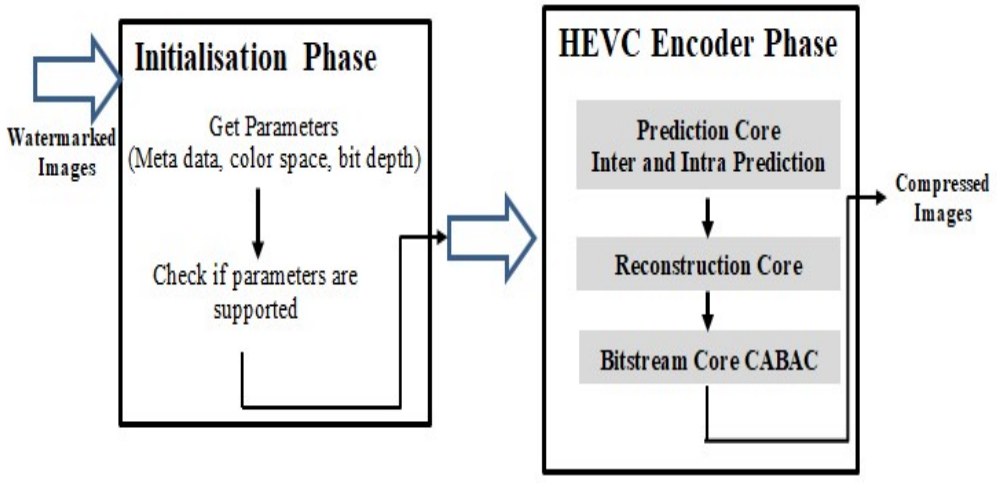

Figure 2.2: Block diagram of BPG encoder

2.4 Secure Digital Camera integrated with SBPG

The Secure Digital Camera (SDC) is a novel approach in taking digital images. As images taken by normal Digital Camera (DC) provide only digital images and maintain record of an event visually. SDC not only capture digital images but also capable of tracking the identity, image veracity and also preserve chain of custody [27]. It also maintain record of year, day, time and other information in detail. In short SDC have many high standard function which are not provided by the normal digital camera. The integrated design typically designed as SoC, has inherent facilities like watermarking and encryption, with digital camera. The architecture shown in Fig 2.3 consists of SBPG module, scratch memory, liquid crystal display, active pixel sensor unit, and converter.

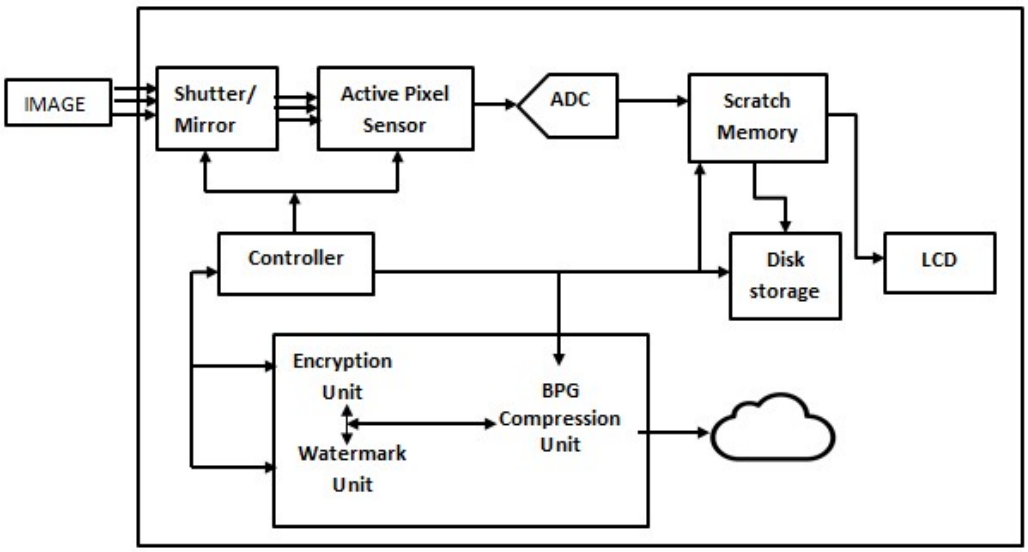

Figure 2.3: System level block diagram of SDC integrated with SBPG

SBPG module consists of three units, watermarking, encryption and BPG compression, to secure the image. After capturing the image it is transformed to digital signal and momentary stored in scratch memory then transformed to SBPG. This double layer protection addresses many functions related to DRM including tempering, ownership rights, authentication of content, and tracking usage. For real time applications in IoT and to simplify real time rights management, SDC is considered as best choice. Controller is responsible for handling this whole sequence

and is modelled as FSM (finite state machine) with 15 states. The compressed image is then transmitted over network or saved in flash memory for further processing.

2.5 Problem Formulation

SBPG integrating SDC provide a unique design for advance IoT application and can be used in many applications of IoT. As there are number of functions performed by the SBPG module so it is important to make the design good enough by enhancing its features. The main concern in of this module is to provide double layer protection against the malicious activities. Watermarking is done to achieve imperceptibility and robustness. On the other hand encryption is done to protect the image against authentication. After watermarking process the quality of image is affected so it is important to maintain the quality of image after embedding watermark in it. Also number of attacks can be perused against the watermarked image [28]. So it is important to design a powerful algorithm for embedding watermark in image so that quality of image can be maintained by protecting it from different possible attacks. Power utilization is another concern of this module, as mage taken by the SDC is of high resolution image which will take more power for processing so algorithm should be designed in such a way that minimum amount of power should be utilised while processing the image.

2.6 Summary

This history of SBPG and all work related to watermarking techniques done by researches is discussed in this chapter. This review helped in implementation of ideas into practical work. SBPG module is viewed by studying its phases and work. During this chapter we have discussed various modules of SDC integrated with SBPG with its architecture. Problem formulation is also discussed in this chapter. SDC integrated with SBPG have many unique features and can be emerged in many application of IoT which include the image processing.

CHAPTER 3

PROBLEM STATEMENT

In past few years, a lot of image watermarking techniques were proposed by many researchers in both frequency and spatial domain. The main motive of researchers is to make an algorithm which is strong enough to counter distinct type of image attacks. Attackers are attacking the system with a lot of new attacks by analysing the vulnerabilities of system. In IoT number of attacks are implemented by attackers during transmission of data [28]. So it is important to hide or protect the data against those attacks. As discussed in chapter 1, we are using secure digital camera integrated with SBPG in which the image is first encrypted with AES encryption [33] and then watermarking is done on the image. After embedding watermark, the image is compressed in the BPG encoder and then the image is transmitted to intelligent traffic surveillance (ITS) for taking appropriate actions. Still there are number of attacks that could be implemented on the designed system. Our main object is to develop a design which is power proficient and gives better quality image after compression along with security. While developing this kind of algorithm a lot of difficulties arise as there are already numbers of watermarking algorithm are present. But none of the previous work provides the power proficiency along with secure and better quality image.

3.1 Possible Difficulties

There are a lot of difficulties that arise in the present system. So while development of the proposed algorithm the problems listed below were kept in mind.

3.1.1 Possible Security Attacks:

Basically while development of watermarking algorithm certain type of temporal attacks are kept in mind. There are many categories of attacks like removal attacks, protocol attacks, cryptographic attacks, and geometrical attacks [29]. Watermark is removed from the watermarked data in case of removal attacks. This approach estimates the original data from the watermarked data as this approach considers the

watermark as noise. Protocol attacks develop protocol ambiguities in watermark mechanism. Copy attack is a kind of protocol attack which copies the watermark from one image to other image without knowing the secret key. Cryptographic attacks try to find the key or position of modified pixels used for embedding. Watermark can be overwritten if key is found. Geometric attacks alter the watermarked data for distortion, but do not remove the embedded watermark [30]. The attack is applied in such a way that with embedding information, the watermark detector loses its synchronization. The process of verification is fooled by the attacker but watermark is there. Rotation attack is another type of attack which destroys the synchronization by changing the pixel position of watermarked image. As in our case we are using encryption and watermarking both so it was difficult to decide which kind of attack attacker can do on our system. Beside these attacks, there is another kind of attack called collusion attack for watermarked images. In some conditions it is feasible for attacker to make multiple watermarked copies. Attacker, without understanding the algorithm can remove the watermark for exploitation. So collusion attack is basically an attack in which attacker needs many watermarked copies [12]. There are two types of collusion attacks.

Type-1: In this type, attacker obtains copies of same work but with distinct watermarks. The attacker tries to detect the image which is similar in nature. As image have high degree of correlation belonging to the same scene, the different scenes of image are separated by attacker. Then average of distinct blocks is done to mix distinct marks and by doing so new unmarked frame is computed. If successive image frames are different enough only then attack can be successful.

Type-2: In this type, attacker studies the watermarked image by obtaining several copies of watermarked image to learn about algorithm used. Attacker then computes the average of these copies. If same pattern is added to all the copies then the average is returned and subtracted from the image to generate unmarked image.

In our algorithm, we mainly concentrated on rotation and collusion attack. Research was done to make the proposed algorithm feasible against these attacks. Research done till now has mainly concentrated on temporal attacks so it was difficult to find a way to implement this idea as there is no proper solution against these attacks.

3.1.2 Watermarking Phase:

Watermarking is the main phase of our thesis. Digital watermarking is basically a method to protect the copyright and intellectual property of image containing information. While transferring the information through the internet, it also maintains the integrity. Watermark is embedded in such a fashion that the quality of image is not affected perceptually. There are a lot of algorithms provided by the researchers for embedding of watermark in DCT domain [31]. Image data is de-correlated by DCT. For highly correlated images, DCT has magnificent energy compaction property. Even DCT exhibits lack in deconstruction of image and can be conveyed in separable format [32]. Some techniques give robustness and some provide imperceptibility but only few can provide both. Our main motive is to improve the quality of image by increasing the Peak Signal to Noise Ratio (PSNR) value of watermarked image. Higher the value of PSNR means an increase in robustness. The main problem which we tackle is how to achieve both the robustness and imperceptibility while maintaining the quality of image.

3.1.3 Power Estimation:

As IoT devices are used in real time, so speed and power are intervened. Power estimation can be comprehensively arranged into pattern dependent and pattern independent methodologies. In pattern dependent methodology, a large number of patterns is simulated to estimate the power but in other methodology only single probabilistic analysis of design is done instead of large number of simulations. The consumption of power depends upon so many factors like size of the image to be processed, algorithm chosen for the watermarking and time taken for completing the whole process. As IoT deal with real time processing of data so consumption of energy is also high, hence it is a really big challenge to utilize the energy as input data is varying in size. On the basis of hardware and software also, consumption of power can be estimated [34]. Good software is capable enough to handle the requirements by utilizing the power. In proposed scheme, efficient usage of power is taken without compromising the quality of image. So algorithm should be designed in such a way that it will take less time for processing of image without losing quality. To achieve this, the factors on which power depends are analysed. By keeping these factors in

mind, algorithm is designed so that the optimal design should be proficient in terms of power. The factors on which power depend while doing watermarking are intensity of coloured image and time taken by algorithm for embedding. After analysing these factors, next difficulty that arises was how to simulate the design to estimate power.

3.2 Summary

This chapter explains each problem we tackle while designing of proposed scheme. The factors which affect the results of thesis are highlighted in this chapter with their definition. Distinct types of attacks that can be simulated against the watermarked image are also listed in this chapter. After analysing the problems it is easy to find what we have to do and which factors should be kept in mind while developing the algorithm.

CHAPTER 4

PROPOSED WATERMARKING SCHEME

4.1 Watermarking Process

Digital watermarking is a method to protect the copyright and intellectual property of image containing information. While transferring the information through the internet it also maintains the integrity. Watermark is embedded in such a fashion that the quality of image is not affected perceptually [32]. The discussion is mainly done on temporal attacks if robustness is main concern, only few schemes are robust against the geometrical attacks specially rotation attack. Rotation attack change the position of pixels of watermark frames and disturb the synchronization. Collusion attack is another type of attack which can be performed by the attacker. In this type of attack, multiple watermarked data is obtained by the attacker and without understanding the algorithm attacker can do the exploitation. In our thesis, in DCT domain a watermarking algorithm is proposed by which robustness is increased and individual frames can also be checked against the integrity. Proposed scheme is able to tackle against the collision attack by making use of pseudo random number (PRN) along with permutation vector and to make the scheme resistant against rotation attack, square blocks present in the center of channel are embedded for watermark. Only few algorithms are able to provide protection against both rotation and collusion attack. The alternating components (AC) of each DCT frame are selected randomly and then watermark is embedded. The main reason of this research was to make the system power proficient and secure against the attacks while maintaining the quality of embedded image in less time taken by the baseline scheme.

The algorithm is implemented in images of JPEG format. If compared for both encoding and decoding, images with PNG format consume more power than the images having format JPEG from the viewpoint of portable devices. Experiments prove that JPEG is perfect choice for both encoding and decoding of images [35]. As embedding adds some noisy pixels in the image by which the quality of the image decreases, to overcome this we proposed a new algorithm for embedding of

watermark. In revised scheme, to make the algorithm powerful against dropping of frames, embedding is done in every frame of the image. Frames are chosen pseudo-randomly. By doing so it is difficult for attacker to analyze in which frame embedding is done. Below are listed some important steps and parameters taken to accomplish the process.

- Color model RGB (red, green, blue) is chosen and luminance area of image is targeted as the embedding part. RGB components are most correlated components which mean the color quality of image frame relies on all components [36].
- For watermark logo, an image is chosen of size (M x M). Every bit of the logo image is either "0" or "1" and embedded with the input image.
- To make the plan strong against rotation attack, center of the block is chosen for processing. At the time of computation the square area of size (P x P) is chosen where the unit circle is placed for embedding. The size of (P x P) must be multiple of (8 x 8) as the scheme uses block size of (8 x 8) for embedding process. After completion of the embedding process the extracted center block is fit again to make the image of same size. In this way the image is watermarked only in center portion as center of image contains the actual information.
- To make the plan strong against the collusion attack, for selection of embedding blocks of size (8 x 8) pseudo random number (PRN) is used. It guarantees that embedding squares will differ for progressive frames [12]. To produce seed estimation of PRN generator a permutation vector is utilized and conserved as a secret key (k). The permutation vector act as secret key defined by user which is given as input to PRN generator. In case watermark extraction is needed then same vector is used for choosing the embedding blocks and to produce the seed.
- It depends upon the size of watermark logo, that in a group how many frames are required. Within a group of frames the whole watermark is embedded and a single bit is embedded into a square block (8 x 8), for adjustment between reliability and robustness.

4.2 Revised Scenario

Fig 4.1 represents blocks of each step of embedding scheme and the process of embedding goes as follows:

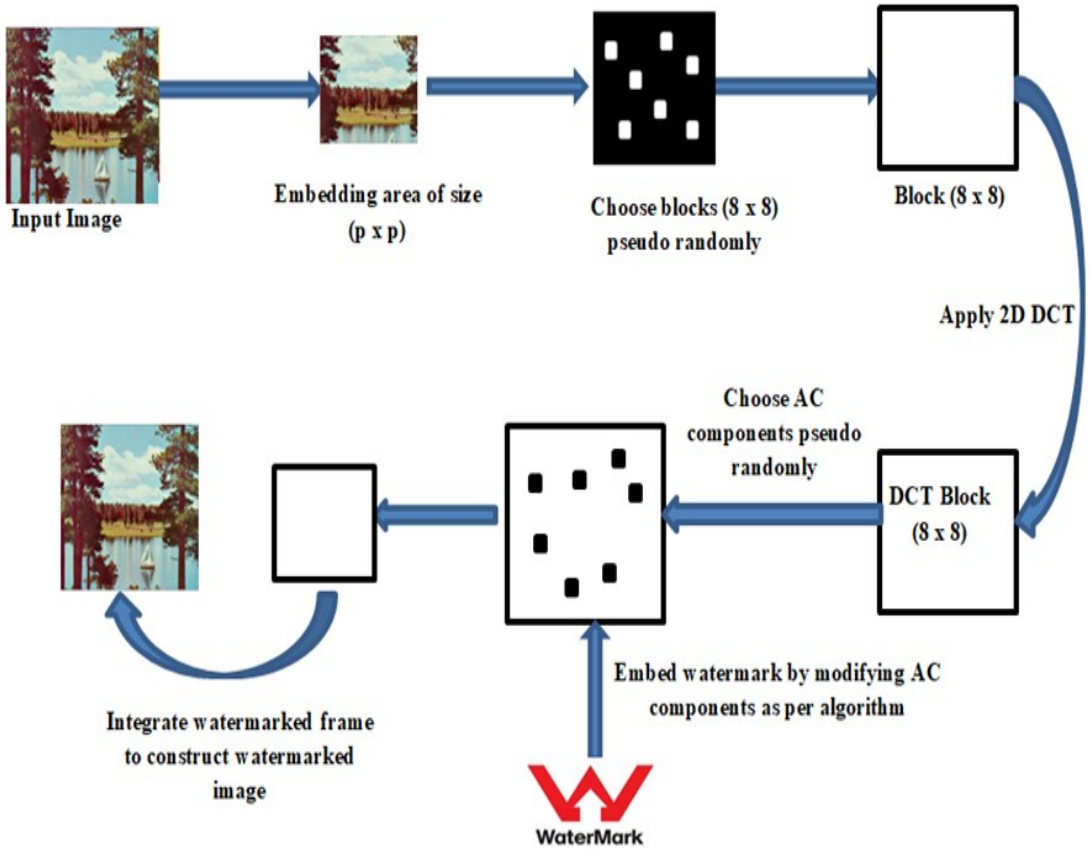

Figure 4.1: Proposed watermark embedding scheme

Step 1: A square piece of size (P x P) is picked in every luminance part's center which is considered as the objective embedding zone. Information embedding into the focal region of the frame makes the scheme safe against cropping. The square block (P x P) is separated into non-overlapping sub-pieces of size (8 x 8). It is seen that the watermark is inserted in the focal region of frame to make the scheme powerful against cropping. Additionally, the plan is secured because of the resulting reasons, (1) the squares (8 x 8) which are utilized for information embedding are chosen pseudo randomly (key dependent), (2) the "n" number of AC coefficients which are modulated

amid information installing are likewise chosen pseudo arbitrarily (key ward). Without the above data, it is difficult to extricate the watermark by unapproved user into its exact shape which makes the plan secure.

Step 2: Then to embed the watermark information, N number of different (8 x 8) blocks are chosen pseudo-randomly.

Step 3: On each selected block (8 x 8), 2D DCT is applied.

Step 4: For each DCT block (8 x 8), „n" number of AC components are selected pseudo randomly. One bit of watermark is embedded in selected „n" number of AC components of block size (8 x 8). In PRN generator for managing the secret key, the same mechanism discussed in Step-2 is used. Rules shown in Fig 4.2 are used for modification of AC components.

```
if (W(k) = = 1)
  do {
   if (mod(D(i, j), d) ≤ a)
     Dw(i, j) = D(i,  j) – mod(D(i, j), d) – a
   else
     Dw(i, j) = D(i , j) – mod(D(i , j), d) + c
   endif
  } until 'n' number of AC coefficients are considered.
elseif (W(k) = = -1)
   do{
     if (mod(D(i , j), d) ≥ c)
       Dw(i , j) = D(i , j) – mod(D( i, j), d) + e
     else
       Dw(i, j) = D(i , j) – mod(D(i , j), d) + a
    endif
   } until 'n' number of AC coefficients are considered.
endif
```

Figure 4.2: Rules for modification of AC components

In above rules W(k) is watermarked embedded bit, D(i, j) is original AC component and $D_w(i, j)$ is watermarked AC component. For embedding strength, a, b, c, d and e are taken as global constants. These global constants are related to each other as: b=2a, c=3a, d=4a and e=5a. in order to maintain the acceptable range of robustness and

reliability. The values are taken on the basis of large number of experimentation. For more optimum result the values can be generated by using the genetic algorithm (GA). The function mod(D(i, j), d) is remainder of D(i, j) and d.

Step 5: The watermarked image is then passed to BPG encoder for compression and then the compressed image is transmitted to the ITS through cloud. Fig 4.3 shows the secure BPG encoding compression implementation on sails image by using revised watermarking scheme. For selection of AC components "n" is taken as 5 in our experiment. Peak Signal to Noise Ratio (PSNR) is used in this study to measure the distortion for watermarked image. Increase in the value of PSNR is indication of better imperceptibility and preservation of hidden information [37]. If the gadgets are used in real-time, speed and power are main concerns. In our design we adopted the pattern independent method for which distinct inputs and mean of power dispersed is considered by running many simulations. The outline is considered as a black box and the current and voltage esteems are considered from the plan, in order to measure power. This was accomplished with the assistance of sensors and power blocks.

Cover Image | Watermarked Image | Watermarked Compressed Image

Figure 4.3: Secure BPG compression of Sails image (512 x 512)

4.3 Solution to problem

In this section, solution to the problems discussed in chapter 3 is provided with the development of proposed algorithm.

4.3.1 Resistant Against Attack:

To make the plan strong against rotation attack, center of the block is chosen for processing by proposed algorithm. At the time of computation the square area of size

(P x P) is chosen where the unit circle is placed for embedding. In this way the image is watermarked only in center portion as center of image contains the actual information. To make the plan strong against the collusion attack, for selection of embedding blocks of size (8 x 8) pseudo random number (PRN) is used. It guarantees that embedding squares will differ for progressive frames. To produce seed estimation of PRN generator a permutation vector is utilized and conserved as a secret key (k). In this way watermarking scheme is resistant against both the attacks.

4.3.2 Improved Quality:

For each DCT block, numbers of AC components are selected pseudo randomly. Rules discussed in section 4.1 are used for modification of AC components. By adoption of these rules, there occurs an increase in Peak Signal to Noise Ratio (PSNR) which is used in this study to measure the distortion for watermarked image. Increase in the value of PSNR is indication of better imperceptibility and preservation of hidden information. As the quality of watermarked image is improved so it is impossible for human eye to read the embedded watermark.

4.3.3 Power Proficiency:

For evaluation of power dispersal, only simulation results are considered. In our design we adopted the pattern independent method for which distinct inputs and mean of power dispersed is considered by running many simulations. The outline is considered as a black box and the current and voltage esteems are considered from the plan, in order to measure power. The design is prototyped in Simulink to estimate the power with assistance of sensors and power blocks. The calculated power from the Simulink design proves that the proposed system takes less power as compares to baseline design. As with decrease in time taken to process the image, according to algorithm there is decrease in power utilization even with better quality image.

4.4 Research Objectives

- The main objective of this research is to develop an optimal algorithm for Secure Better Portable Graphic (SBPG) module to improve the quality of image after encryption and watermarking phase
- Another objective is to make the design power proficient against the baseline design. To accomplish this objective, we proposed an algorithm based on

DCT. For each DCT blocks, AC components are chosen pseudo-randomly for embedding of watermark.

- As security is main concern in IoT, the proposed algorithm is able to tackle the collision attack and rotation attack by making use of pseudo random number (PRN) along with permutation vector and choosing square blocks present in the center of channel for embedded of watermark.

4.5 Scope of Work

One of the applications where this approach can be adapted is ITS i.e. Intelligent Traffic Surveillance where the Secure digital camera capture the image of any unexpected accident or traffic and send this image to ITS through gateway so that appropriate action could be taken to control the traffic. In this way multiple cities can connect to the same gateway and can share their data with each other to make the system more intelligent. This approach can be implemented in medical field also to transmit the medical reports to other specialist for better advice or to share the analysis reports with each other as the method is secure and reliable. A lot of IoT applications are present where this approach can be implemented. Further advancement can also be done in the design to make the SBPG more secure and efficient against different attacks.

4.6 Summary

The proposed work of watermark embedding is discussed in this chapter. Algorithm designed for better results is discussed in this chapter in detail. Solution to problems listed in chapter 3 is also given in this chapter. Further the objectives of research done are also presented to have a clear view of research work. Scope of work is also given in this chapter. As the proposed method provides authentication and reliability of data, as well as security against the collusion attack and rotation attack, so this approach can be used in many applications of IoT.

CHAPTER 5

TESTING AND RESULTS

From the review of state of art, we concluded that in IoT the main concern is consumption of energy as whole system is power dependent and is all about internet. As a lot of things are connected to the network, it is important to maintain the security of information circulated between the nodes over the internet. Due to infrastructure less network and presence of vulnerabilities, system suffers from number of attacks and these attacks breach the information, alter the data, add fake nodes in the network and hide the informative data. So to make the system strong against these attacks it is important to adapt effective algorithm for secure communication between two ends by utilizing low power. This chapter describes the experimental procedures followed and processing parameters. In this chapter the Secure Better Portable Graphic module is implemented in MATLAB / Simulink® version 9.0 (R2016a) for transmission of image taken by secure digital camera and check the performance of the proposed scheme according to parameters like PSNR, Elapsed Time and Power. To measure the power proposed scheme is prototyped in Simulink®, as it gives best data flow perception using functional blocks. Standard JPEG images (512 x 512) are used for transmission in our simulation for all kind of possibilities. Then the results of proposed scheme and baseline scheme are compared to see which schematic design approach is better.

5.1 Tool Used

MATLAB stands for MATrix LABoratory and the product is developed around vectors and matrix. MATLAB is a multi-worldview numerical registering framework and programming dialect of fourth generation. An exclusive programming language created by MathWorks, MATLAB permits manipulation of matrix, function and information plotting, execution of calculations, creation of user interface, and interfacing with programs written in different languages, including C, C#, Java, C++, Python and Fortran. It has an extra package, Simulink which includes graphical multi-area simulation and model-based outline for dynamic and embedded framework. With

features of graphical user interface (GUI), MATLAB support development of application. MATLAB incorporates GUIDE (GUI advancement condition) for graphically planning GUIs. It has firmly coordinated features of chart plotting. To return and pass the data types, a wrapper function is created in MATLAB. The progressively loadable object files made by incorporating such capacities are named "MEX-records". A MATLAB program can deliver three-dimensional illustrations utilizing the functions surf, plot3. The framework is isolated into three functional ranges.

- Specification environment: The MATLAB environment consists of menus, buttons and a writing area similar to an ordinary word processor called command window.
- Simulation: MATLAB is also a key part of model-based design, which is used for multi-domain simulation, physical and discrete-event simulation, and verification and code generation.
- Analysis: The analysis area processes and graphically presents simulation results, and the integrated editing and debugging tools let you quickly explore multiple options, refine your analysis, and iterate to an optimal solution.

The reason for using this software is because of its highly rich features. It has a leading atmosphere for design and modeling simulation. It combines a high-level language with a desktop environment tuned for iterative engineering and scientific workflows.

5.1.1 Simulation workflow

Simulation is a process in which you validate and verify a model by comparing simulation results. The simulation workflow is performed as shown in Fig 5.1 after you've finished building your model and a simulation completes without errors. Before simulating a model, you need to understand your goals and requirements. The steps in a typical simulation workflow include:

- Determine Simulation Goals

  Before simulating a model, you need to understand your goals and requirements.

  - Understand input to output causality

- Verify model
- Optimize parameters
- Visualize results

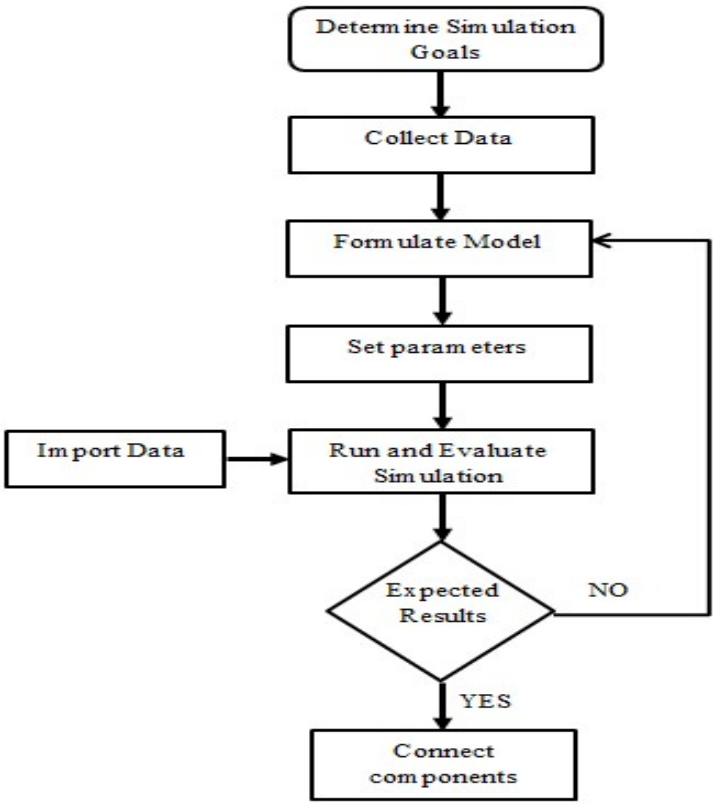

Figure 5.1: Simulation Workflow

- Collect Data

  Gather input information and yield output information from a genuine framework. Utilize the deliberate information to drive the simulation. Contrast measured yield information and the model simulation results to check the exactness of your model.

- Formulate Model

  Setting up a model for simulation incorporates characterizing the external interfaces for input information and control flags, and yield signals for survey and recording results of simulation.

- Set Parameters

  For the primary simulation, utilize model parameters from the approved model. After contrasting the simulation outcomes and measured output information, alter model parameters to more accurately represent modelled framework.

- Run Simulation and Evaluate Result

  Utilizing measured input information, run a simulation and save outcomes. Evaluate the contrasts between simulated output and measured output information. Utilize the assessment to confirm the exactness of your model and how well it speaks to the framework conduct. Choose if the precision of your model sufficiently speaks to the dynamic framework you are modelling.

5.1.2 Application Areas of MATLAB

There are some application areas where MATLAB is very useful and can give better results. These include-

- Toolboxes for specialized applications such as image processing, computer vision, generic algorithms and many more.
- SimuLink graphical simulation tool
- Mathematical computations and visualizing data through graphs
- Algorithms for numerical methods

5.2 Design Parameters

The design parameters/performance metrics described in this section are used for the evaluation of image quality after watermarking process and power utilization for communicating the image. These parameters have great impact on overall performance of SBPG integrated with Secure Digital Camer (SDC) architecture. We dealt with three performance metrics of SBPG module i.e. PSNR, elapsed time and power. These metrics are evaluated with respect to baseline design to see the performance. The description of the design parameter is as follows:

- PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power

of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. It is most easily defined via the mean squared error (MSE). It is mostly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression) [38]. The signal in this case is the original data, and the noise is the error introduced by compression. Although a higher PSNR generally indicates that the reconstruction is of higher quality.

- Elapsed Time: Elapsed time is the amount of time that passes from the start of an event to its finish. In simplest terms, elapsed time is how much time goes by from one time to another [39]. Tic command starts a stopwatch timer to measure performance. The function records the internal time at execution of the tic command. Display of elapsed time is done with the toc function. Toc reads the elapsed time from the stopwatch timer started by the tic function. The function reads the internal time at the execution of the toc command, and displays the elapsed time since the most recent call to the tic function that had no output, in seconds.

- Power: Power factor demonstrates the measure of dynamic power out of aggregate power expended in the framework. In control framework, reactive power is additionally required alongside active power for charging inductive and capacitive parts. Dissimilar to active power, receptive power is not used by the framework. Rather it is given to the framework [40]. However this power is required for smooth power exchange. Since the reactive power is not used in this way it is prescribed to keep its incentive beneath certain limit. To discover reactive and active power in a framework, an amount is characterized called power factor which demonstrates the rate of active and reactive power. Power factor is the proportion of the active energy to the aggregate energy of the framework. Current (I) and voltage (V) test is taken from the framework utilizing sensors (Current Transformer and Potential Transformer). The power block processes the active power (P), in watts, and the reactive power (Q), in volt-ampere responsive (var), of a voltage-current match at principal recurrence. To perform this calculation, the square initially decides the central esteems

(magnitude and phase) of the two information signals V and I.

5.3 Results and Discussions

In this section, we described the results of proposed design with metrics PSNR, elapsed time and power. In this section total six images are processed through the design to evaluate the performance of revised scheme. In the following sub sections, we will compare the performance of proposed SBPG design with the baseline SBPG design on the basis of different parameters. The results are converted into the form of tables and specially taken for the sake of comparison and for making the statistical calculation more easy and precise. Results are compared with standard JPEG images of size (512 x 512). Each image is processed with the proposed algorithm and then the results are compared with the baseline approach.

5.3.1 Comparison on the basis of PSNR value

Table 5.1 shows the comparison of both baseline and proposed optimal design on the basis of value of PSNR parameter. As discussed above in section 5.2, increase in PSNR value leads to increase in quality of image. This proves that quality of image improved after embedding the watermark in the image by modifying each AC component as per rule of proposed algorithm. As shown in Table 5.1 the PSNR value of optimal design is higher than the baseline design which means the revised design provides better reliability of image along with better quality image.

Table 5.1: Comparison on basis of PSNR value

TEST IMAGE	SBPG Baseline PSNR	SBPG Optimal Design PSNR
Sails	54.48	68.45
Tulip	54.59	68.27
Papper	54.50	68.25
Lenna	54.49	68.42
Baboon	54.48	68.22
Fruits	54.57	68.58

Fig 5.2 shows the comparative analysis of both the designs with the help of bar graph. Bar with the color red indicates the performance of proposed method and bar with blue color indicate the performance of base method. From the graph it is clearly demonstrated that the performance of proposed design is much better then the performance of base design.

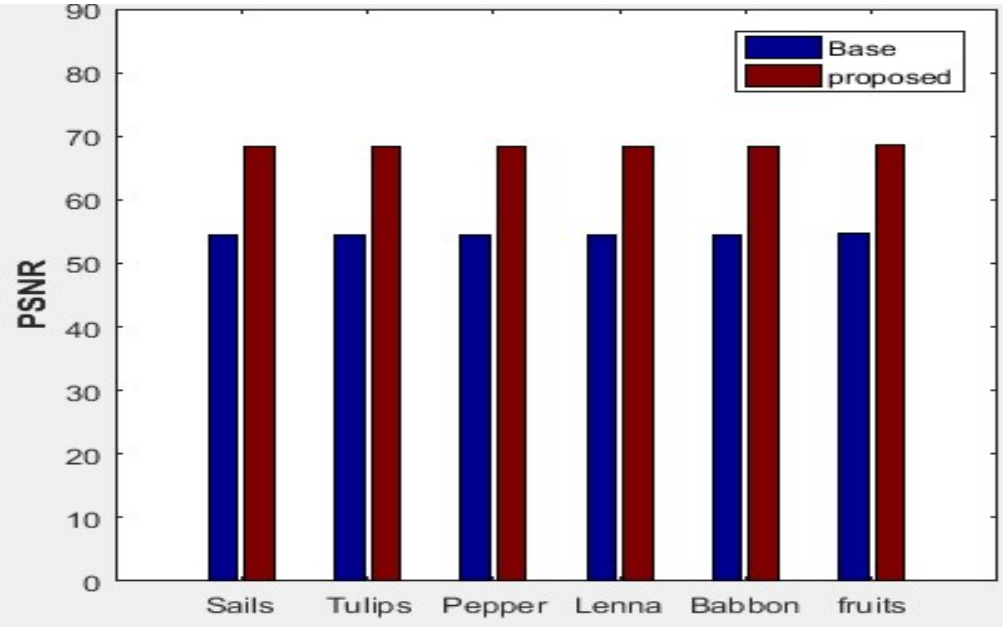

Figure 5.2: Bar graph showing comparison of baseline and proposed optimal design in terms of PSNR

Fig 5.3 shows the line graph, red line with circle indicates the value of proposed scheme and black line with star indicates the results of base approach. The value for each image is calculated and then each value is plotted on the graph with the help of MATLAB. The x-axis of graph indicates the six standard images taken to test the design and the y-axis indicates the output value of each image by processing through the design.

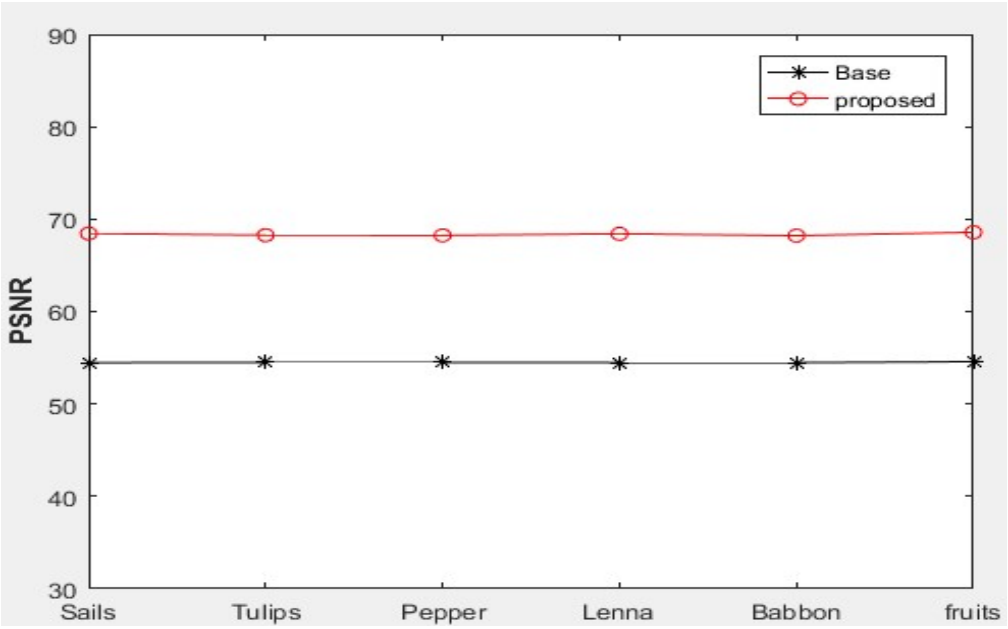

Figure 5.3: Line graph showing comparison of baseline and proposed optimal design in terms of PSNR

5.3.2 Comparison on the basis of Elapsed Time

Table 5.2 shows the comparison of both baseline and proposed optimal design on the basis of elapsed time. As discussed above in section 5.2, elapsed time is how much time goes by from one time to another. Our results prove that time taken to process the image according to the algorithmic rules is less than the time taken by the baseline scheme. As shown in table, the value of elapsed time of optimal design is much lower than the baseline design which means the revised design takes less computation time which implies to fast processing of image.

Table 5.2: Comparison on basis of parameter Elapsed Time

TEST IMAGE	SBPG Baseline TIME	SBPG Optimal Design TIME
Sails	7.2	2.7
Tulip	4.5	3.0
Papper	5.1	2.9
Lenna	5.0	3.0
Baboon	5.3	3.0
Fruits	4.5	3.4

Fig 5.4 shows the comparative analysis, on the basis of time, of both the designs with the help of bar graph. Representative graph clearly demonstrates that proposed method take less time for computation.

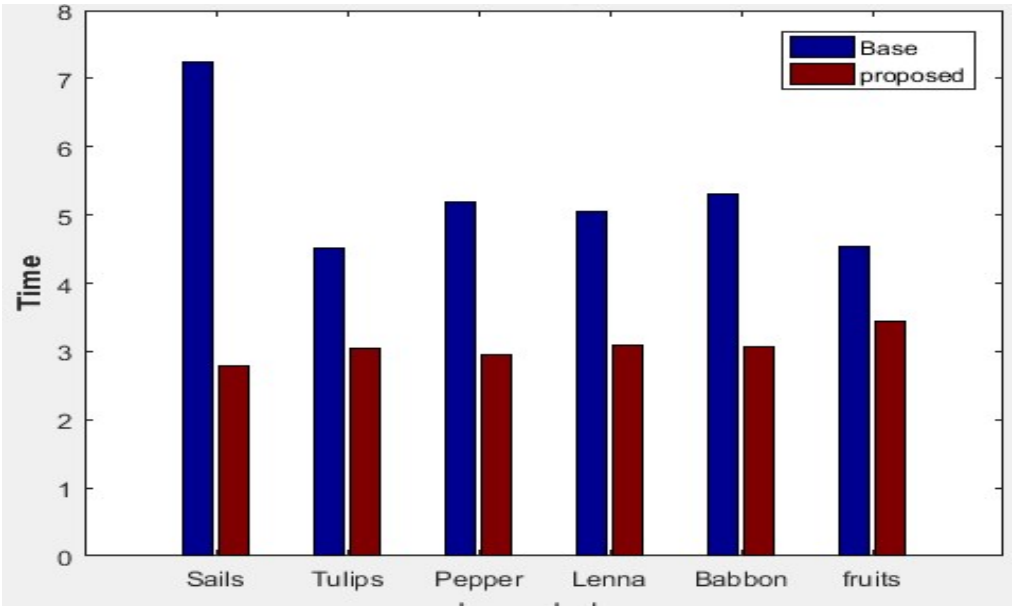

Figure 5.4: Bar graph showing comparison of baseline and proposed optimal design in terms of elapsed time

In line graph shown in Fig 5.5, red line with circle indicates the value of proposed scheme and black line with star indicates the results of base approach. The time taken for processing of each image is calculated and then each value of time is plotted. The x-axis of graph indicates the six standard images taken to test the design for elapsed time and the y-axis indicates the output value of elapsed time calculated by processing image through the design.

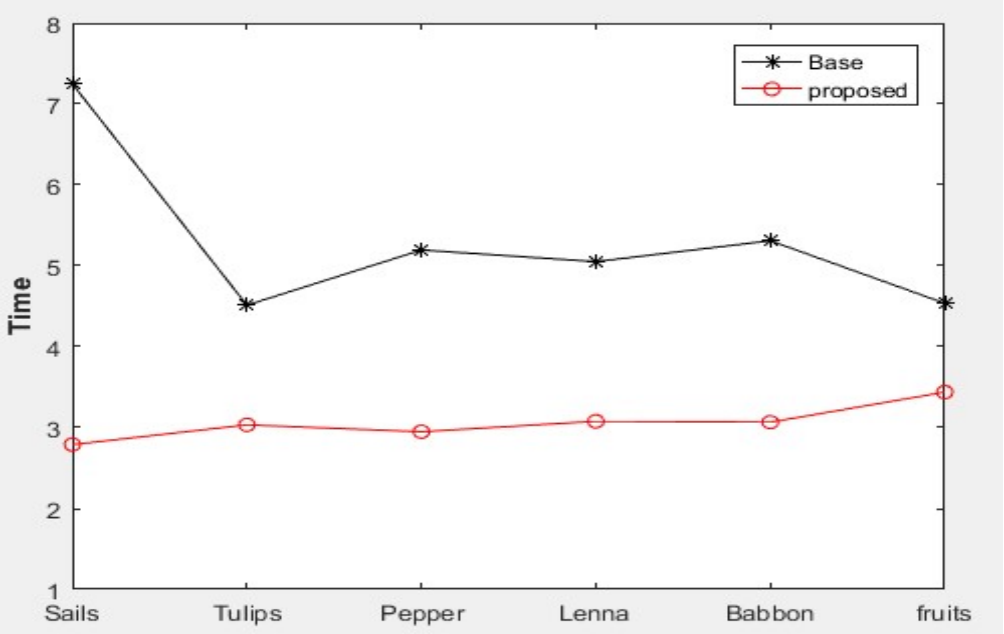

Figure 5.5: Line graph showing comparison of baseline and proposed optimal design in terms of elapsed time

5.3.3 Comparison on the basis of Power

Table 5.3 shows the comparison of both baseline and proposed optimal design on the basis of power consumption. As discussed above in section 5.2, power is calculated with voltage and current values. To calculate value of power the image is given as input to the Simulink model and estimated value is derived from the output. From table it is clear that power consumed by the optimal design is less than the baseline secure BPG encoder module. As revised method take less time to compute as shown in the results in Table 5.3, the value of power automatically decreases as the computation time taken for processing is less.

Table 5.3: Comparison on basis of parameter Power

TEST IMAGE	SBPG Baseline	SBPG Optimal Design
	POWER	POWER
Sails	3.78	3.65
Tulip	6.64	6.25
Papper	3.71	3.65
Lenna	13.85	13.01
Baboon	3.86	3.77
Fruits	15.35	14.77

Bar graph shown in Fig 5.6 shows the difference of consumption of power by both the designs. Power consumption depends upon processing of image. For different images even of the same size, the processing power differs as the intensity of RGB colors of one image is different from another image. Image with low intensity will take less time and power for embedding and image with high intensity take more power. As shown in bar graph, different images take different power even though size of all the images taken is same (512 x 512).

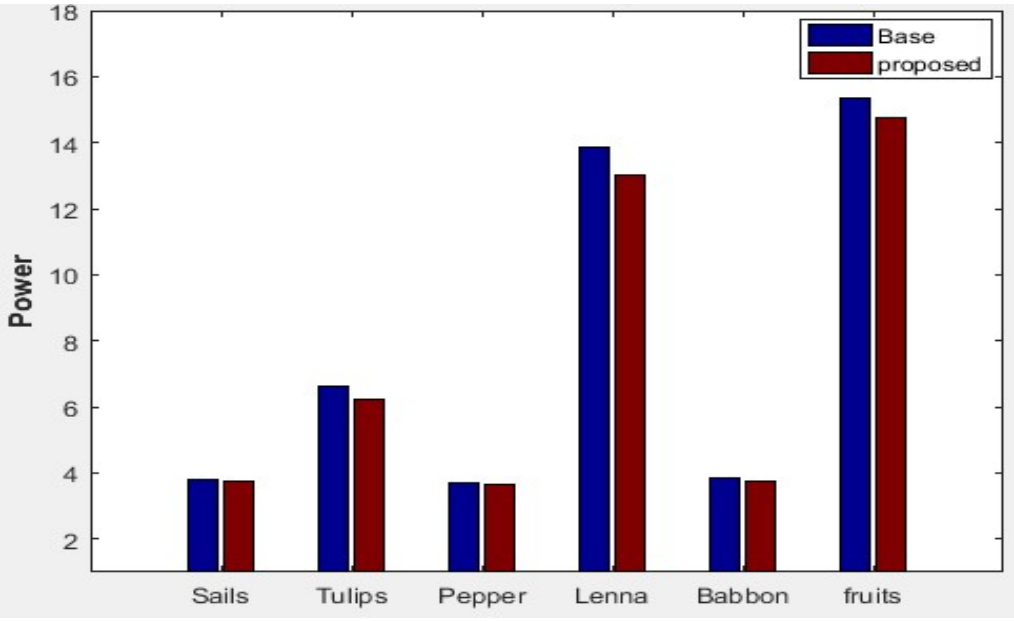

Figure 5.6: Bar graph showing comparison of baseline and proposed optimal design in terms of power

In line graph shown in Fig 5.7, red line shows the values of power consumed by the optimal design and black line shows the values of power consumed by baseline design. Different images take different power for processing depending upon the color intensity of image. From line graph, it is proved that proposed design is power proficient than the baseline design scheme which was our main motive.

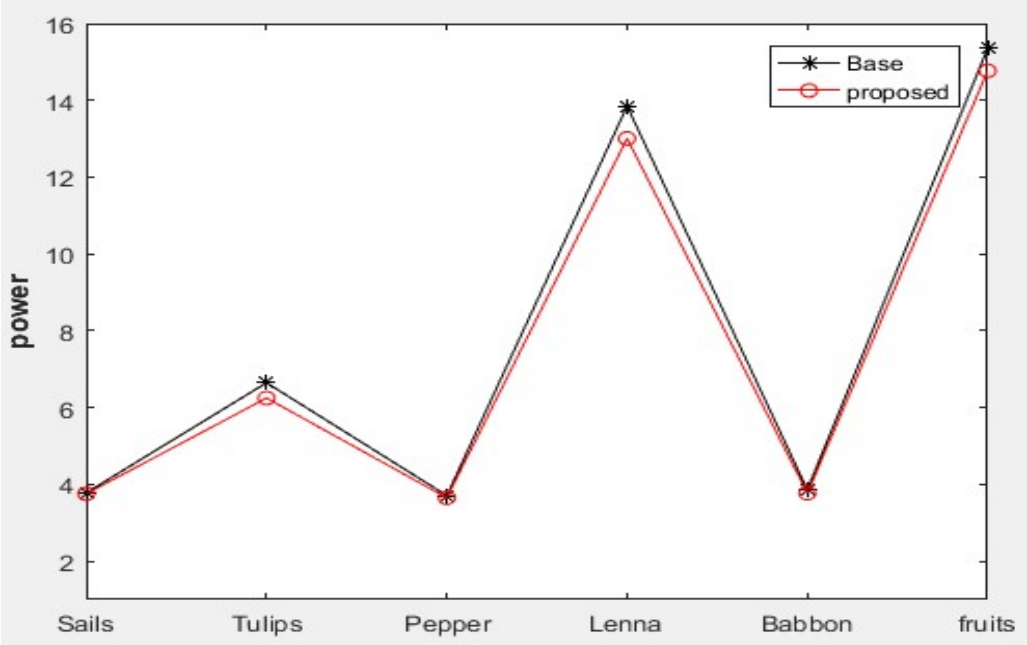

Figure 5.7: Line graph showing comparison of baseline and proposed optimal design in terms of power

5.4 Summary

In this chapter, various comparisons are done between the optimal design and baseline design, which provide information about which schematic design is better than another on the basis of various parameters. Various tables are given from which various results can be withdrawn like comparison between both the schemes on basis of various factors. By doing this analysis, it is concluded that proposed optimal design is power proficient and provides better quality image after embedding in less time.

CHAPTER 6
CONCLUSIONS

6.1 Conclusion

Information security plays an important role in IoT. With the adoption of new applications and design, it is critical to accomplish security objectives. Effectiveness and reliability of secure transmission of data depends on the selection of the security mechanism. In ITS, it is important to maintain the security of data transmitted over the open network by consuming low power. Power consumption depends upon the type and amount of data to be transmitted. In ITS, image taken by secure digital camera is sent to gateway and then to surveillance center. So design chosen for transmission should have the capacity to preserve QoS in terms of distinct parameters such as power consumption, quality of image, delay, authentication, reliability etc. Secure BPG encoder is used to achieve good results in communication as this module consists of three phases: encryption, watermarking and BPG compression. In this thesis, a power proficient design for the application of IoT is proposed which is able to perform the compression using secure BPG encoder, as well as securing the data while transformation by using the proposed DCT based watermarking method. In revised scheme, to make the algorithm powerful against dropping of frames, embedding is done in every frame of the image. For selection of embedding blocks, pseudo random number (PRN) is used as it likewise guarantees that embedding squares will differ for progressive frames.

From this study we can conclude that the proposed algorithm is able to deliver the data with better quality by consuming less power than used by the baseline design. The proposed scheme is implemented in MATLAB and prototyped in Simulink® to calculate PSNR and power. MATLAB is used as it gives a superior comprehension of the low-level execution while Simulink® provides best level functional squares and dataflow perception. The proposed design scheme if compared with baseline design has better performance in terms of power, PSNR and elapsed time. Increase in PSNR is indication of better imperceptibility and preservation of hidden information and

decrease in power and time values indicates that the design is power proficient. In order to calculate the power from the output of design, voltage and current esteems are considered. Simulink® is used to achieve this by using power blocks and sensors available. We concluded that the proposed scheme is able to tackle against the collusion attack by making use of pseudo random number (PRN) along with permutation vector and to make the scheme resistant against rotation attack, square blocks present in the center of channel are embedded for watermark. It is observed from the outcome that the power utilization is considerably reduced with large Peak Signal to Noise Ratio.

6.2 Future Scope

Critical research on information security in IoT has been done so far and is well on the way to grow more and get huge presence in future communication infrastructure. As the utilization of IoT innovation increments and more number of users are interfacing with the system, security turns into a worry as research till now demonstrates sensors and software used are highly vulnerable when it comes to security.

- In this thesis, the work is restricted to processing of image only. In future the work can be extended to video and audio files.
- Different design parameters can be utilised to measure the performance as future work.
- More attack resistance cryptography schemes could be implemented to enhance the security of information.
- We can implement the design in other application fields of IoT.

REFRENCES

1) Daqiang Zhang, Laurence T. Yang and Hongyu Huang, "Searching in Internet of Things: Vision and Challenges," in Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications, 2011.
2) Miao Yun and Bu Yuxin , "Research on the Architecture and Key Technology of Internet of Things (IoT) Applied on Smart Grid ," in IEEE International Conference on Advances in Energy Engineering , 2010.
3) Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, pp. 2481–2501, 2014.
4) Kai Zhao and Lina Ge, "A Survey on the Internet of Things Security," in Ninth International Conference on Computational Intelligence and Security, 2013.
5) Ahmad W. Atamli and Andrew Martin, "Threat-based Security Analysis for the Internet of Things," in International Workshop on Secure Internet of Things, 2014.
6) ShaoXiwen , "Study on Security Issue of Internet of Things based on RFID ," in IEEE Fourth International Conference on Computational and Information Sciences, 2012.
7) Shinfeng D.Lin, Shih-Chieh Shieb and J.Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, pp. 56-60, 2010.
8) Hsiang-Cheh Huang and Wai-Chi Fang, "Metadata-based image watermarking for copyright protection," Simulation Modelling Practice and Theory, vol. 18, no. 4, pp. 436-445, 2010.
9) Yanping Huang, Wei Lu, Wei Sun and Dongyang Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, no. 1-3, pp. 178-184, March 2011.
10) Z.M. Lu and S.H. Sun, "Digital image watermarking technique based on vector quantisation," Electronics Letters, vol. 36, no. 4, pp. 303 - 305, 2000.

11) B. MACQ, J. DITTMANN and E.J. DELP, "Benchmarking of Image Watermarking Algorithms for Digital Rights Management," Proceedings of IEEE, vol. 92, no. 6, pp. 971-984, May 2004.
12) Amit Phadikar, Amlan Karmakar, Baisakhi SurPhadikar and Goutam Kr.Maity, "A blind video watermarking scheme resistant to rotation and collusion attacks," Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 2, pp. 199-210, April 2016.
13) Umar Albalawi, Saraju P. Mohanty and Elias Kougianos, "SBPG: A Secure Better Portable Graphics Compression Architecture for High Speed Trusted Image Communication in the IoT," in 17th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems , 2016.
14) S. C. Ramesh and M. Mohamed Ismail Majeed, "Implementation of a visible watermarking in a secure still digital camera using VLSI design," in IEEE European Conference on Circuit Theory and Design, 2009.
15) Lei Tian and Heng-Ming Tai, "Secure images captured by digital camera," in International Conference on Consumer Electronics (ICCE), 2006.
16) N.M. Kosaraju, M. Varanasi and S.P. Mohanty, "A High-Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm," in Proceedings of the 19th International Conference on VLSI Design (VLSID"06) , 2006.
17) Thiow Keng Tan, Rajitha Weerakkody and Marta Mrak, "Video Quality Evaluation Methodology and Verification Testing of HEVC Compression Performance," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 1, pp. 76-90, 2016.
18) M. Jridi and A. Alfalou, "A low-power, high-speed DCT architecture for image compression: Principle and implementation," in 18th IEEE VLSI System on Chip Conference (VLSI-SoC), 2010.
19) Huaming Wu and A.A. Abouzeid, "Power Aware Image Transmission in Energy Constrained Wireless Networks," in Ninth International Symposium on Computers and Communications , 2004.
20) N. Buch, J. Orwell and S.A. Velastin , "Detection and Classification of Vehicles for Urban Traffic Scenes," in 5th International Conference on Visual

Information Engineering (VIE 2008), 2008, pp. 182 – 187.

21) B. Morris and M. Trivedi, "Robust classification and tracking of vehicles in traffic video streams," in IEEE Intelligent Transportation Systems Conference, ITSC '06, 2006.
22) Ramsin Khoshabeh, Tarak Gandhi and Mohan M. Trivedi, "Multi-camera Based Traffic Flow Characterization & Classification," in IEEE Intelligent Transportation Systems Conference, 2007
23) T. Nadeem, S. Dashtinezhad, Chunyuan Liao and L. Iftode, "TrafficView: A Scalable Traffic Monitoring System," in IEEE International Conference on Mobile Data Management, 2004.
24) Umar Albalawi, Saraju P. Mohanty and Elias Kougianos, "A Hardware Architecture for Better Portable Graphics (BPG) Compression Encoder," in 2015 IEEE International Symposium on Nanoelectronic and Information Systems, 2015.
25) M. Antonini, M. Barlaud, P. Mathieu and I. Daubechies, "Image Coding Using Wavelet Transform ," in IEEE Transactions on Image Processing, 1992, pp. 205-220.
26) Gary J. Sullivan, Jens-Rainer Ohm, Woo-Jin Han and Thomas Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard," in IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, vol. 22, 2012.
27) Umar Albalawi, Saraju P. Mohanty and Elias Kougianos, "Energy-Efficient Design of the Secure Better Portable Graphics Compression Architecture for Trusted Image Communication in the IoT," in IEEE Computer Society Annual Symposium on VLSI, 2016.
28) Jeffrey Voas, Irena Bojanova and Richard Kuhn , "Learning Internet-of-Th ings Security “Hands-On”," in IEEE Computer and Reliability Societies , 2016.
29) Chunlin Song, Sud Sudirman, Madjid Merabti and David Llewellyn-Jones , "Analysis of Digital Image Watermark Attacks," in 7th IEEE Consumer Communications and Networking Conference (CCNC), 2010.
30) V. Licks and R. Jordan, "Geometric Attacks on Image Watermarking Systems," IEEE MultiMedia, vol. 12, no. 3, pp. 68-78, 2005.

31) Vidyasagar M. Potdar, Song Han and Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques," in 3rd IEEE International Conference on Industrial Informatics (INDIN, 2005.
32) Saraju P.Mohanty and Elias Kougianos, "Real-time perceptual watermarking architectures for video broadcasting," Journal of Systems and Software, vol. 84, no. 5, pp. 24-738, May 2011.
33) Henry Kuo and Ingrid Verbauwhede, "Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES Rijndael Algorithm," CHES: International Workshop on Cryptographic Hardware and Embedded Systems, vol. 2162, 2001.
34) F.N. Najm, "A Survey of Power Estimation Techniques in VLSI Circuits," EEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 2, no. 4, pp. 446-455, 1994.
35) A.N.Skodras, C.A.Christopoulos and T.Ebrahimi, "JPEG2000: The upcoming still image compression standard," Pattern Recognition Letters, vol. 22, no. 12, pp. 1337-1345, 2001.
36) Mohammad Rashid, Luca Ardito, and Marco Torchiano, "Energy Consumption Analysis of Image Encoding and Decoding Algorithms," in IEEE/ACM 4th International Workshop on Green and Sustainable Software, 2015.
37) Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," ELECTRONICS LETTERS, vol. 44, no. 13, pp. 800-801, 2008.
38) M. Mrak, S. Grgic and M. Grgic, "Picture quality measures in image compression systems," in The IEEE Region 8 EUROCON 2003, 2003.
39) Osama A. Khashan, Abdullah M. ZIN and Elankovan A, Sundararaj, "Performance study of selective encryption in comparison to full encryption for still visual images," Journal of Zhejiang University SCIENCE C, vol. 15, no. 6, pp. 435-444, 2014.
40) Pablo Acuña, Marco Rivera, Juan Dixon and José Rodriguez, "Improved Active Power Filter Performance for Renewable Power Generation Systems," IEEE Transactions on Power Electronics, vol. 29, no. 2, pp. 687 - 694, 2013.

LIST OF PUBLICATION

[1] H.Verma, R.K.Chahal, "A Review on Security Problems and Measuers of Internet of Things", International Conference on Intelligent Computing and Control Systems (ICICCS), 15-16 June, 2017 (Accepted).

[2] H.Verma, R.K.Chahal, "Power Proficient Design for Communication of Trusted Image in the IoT", International Conference on Research in Computational Intelligence and Communication (ICRCICN), November 03-05, 2017 (Communicated).

https://www.youtube.com/watch?v=vEHGNisRwkQ

Thesis

ORIGINALITY REPORT

%13	%6	%7	%7
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Miao Yun. "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid", 2010 International Conference on Advances in Energy Engineering, 06/2010 Publication	%1
2	Submitted to University of North Texas Student Paper	%1
3	www.help2educate.com Internet Source	%1
4	www.mathworks.co.uk Internet Source	%1
5	Lecture Notes in Electrical Engineering, 2014. Publication	%1
6	Zhang, Daqiang, Laurence T. Yang, and Hongyu Huang. "Searching in Internet of Things: Vision and Challenges", 2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications, 2011. Publication	%1

7	Submitted to University of Babylon Student Paper	%1
8	Albalawi, Umar, Saraju P. Mohanty, and Elias Kougianos. "SBPG: A secure better portable graphics compression architecture for high speed trusted image communication in the IoT", 2016 17th International Conference on Thermal Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE), 2016. Publication	<%1
9	Submitted to University of Bridgeport Student Paper	<%1
10	ijarcce.com Internet Source	<%1
11	uk.mathworks.com Internet Source	<%1
12	Zhao, Kai, and Lina Ge. "A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, 2013. Publication	<%1
13	www.inderscience.com Internet Source	<%1
14	au.mathworks.com Internet Source	<%1

15	www.rroij.com Internet Source	<%1
16	Mohan M. Trivedi. "Multi-camera Based Traffic Flow Characterization & Classification", 2007 IEEE Intelligent Transportation Systems Conference, 09/2007 Publication	<%1
17	Gander, Walter. "Recursion", UNITEXT, 2015. Publication	<%1
18	Submitted to Multimedia University Student Paper	<%1
19	Elias Kougianos, Saraju P. Mohanty, Gavin Coelho, Umar Albalawi, Prabha Sundaravadivel. "Design of a High-Performance System for Secure Image Communication in the Internet of Things", IEEE Access, 2016 Publication	<%1
20	www.slideserve.com Internet Source	<%1
21	Submitted to Brunel University Student Paper	<%1
22	www.coursehero.com Internet Source	<%1

23	Submitted to Auston Institute of Management and Technology Student Paper	<%1
24	Submitted to Lebanese International University Student Paper	<%1
25	Submitted to Institute of Research & Postgraduate Studies, Universiti Kuala Lumpur Student Paper	<%1
26	Submitted to Griffith College Dublin Student Paper	<%1
27	Chang, Han Soo, Naoaki Fujisawa, Tsukasa Tsuchiya, Soichi Oya, and Toru Matsui. "Degenerative Spondylolisthesis Does Not Affect the Outcome of Unilateral Laminotomy With Bilateral Decompression in Patients With Lumbar Stenosis :", Spine, 2014. Publication	<%1
28	Submitted to Malaviya National Institute of Technology Student Paper	<%1
29	Submitted to Visvesvaraya Technological University Student Paper	<%1
30	math.boisestate.edu Internet Source	<%1

31	thescipub.com Internet Source	<%1
32	Jridi, M., and A. Alfalou. "A low-power, high-speed DCT architecture for image compression: Principle and implementation", 2010 18th IEEE/IFIP International Conference on VLSI and System-on-Chip, 2010. Publication	<%1
33	www.tsijournals.com Internet Source	<%1
34	Chaplin, A.. "Studying water uptake effects in resins based on cyanate ester/bismaleimide blends", Polymer, 200005 Publication	<%1
35	ivp.csie.ndhu.edu.tw Internet Source	<%1
36	Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, Hui-Ying Du. "Research on the architecture of Internet of Things", 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010 Publication	<%1
37	Gao Xiaochuan. "Low Luminance Smooth Blocks Based Watermarking Scheme in DCT Domain", 2006 International Conference on Communications Circuits and Systems,	<%1

06/2006
Publication

38	Mastriani, Mario. "Union is strength in lossy image compression.", International Journal of Signal Processi, Spring 2009 Issue Publication	<%1
39	www.jatit.org Internet Source	<%1
40	academicpublishingplatforms.com Internet Source	<%1
41	www.ijecs.in Internet Source	<%1
42	"ADAPTIVE DIGITAL WATERMARK SYSTEM USING SOFT COMPUTATION", International Journal of Computers and Applications, 2010. Publication	<%1
43	globaljournals.org Internet Source	<%1

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON
EXCLUDE MATCHES < 7 WORDS