NEW FRAMEWORKS FOR SECURE IMAGE COMMUNICATION IN THE INTERNET OF THINGS (IoT)

Umar Abdalah A Albalawi

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

August 2016

APPROVED:

Saraju P. Mohanty, Major Professor
Elias Kougianos, Co-Major Professor
Robert Akl, Committee Member
Cornelia Caragea, Committee Member
Barrett Bryant, Chair of the Department of Computer Science and Engineering
Costas Tsatsoulis, Dean of the College of Engineering
Victor Prybutok, Vice Provost of the Toulouse Graduate School

Albalawi, Umar Abdalah A. *New Frameworks for Secure Image Communication in the Internet of Things (IoT)*. Doctor of Philosophy (Computer Science and Engineering), August 2016, 134 pp., 9 tables, 119 numbered references.

The continuous expansion of technology, broadband connectivity and the wide range of new devices in the IoT cause serious concerns regarding privacy and security. In addition, in the IoT a key challenge is the storage and management of massive data streams. For example, there is always the demand for acceptable size with the highest quality possible for images to meet the rapidly increasing number of multimedia applications. The effort in this dissertation contributes to the resolution of concerns related to the security and compression functions in image communications in the Internet of Thing (IoT), due to the fast of evolution of IoT. This dissertation proposes frameworks for a secure digital camera in the IoT. The objectives of this dissertation are twofold. On the one hand, the proposed framework architecture offers a double-layer of protection: encryption and watermarking that will address all issues related to security, privacy, and digital rights management (DRM) by applying a hardware architecture of the state-of-the-art image compression technique Better Portable Graphics (BPG), which achieves high compression ratio with small size. On the other hand, the proposed framework of SBPG is integrated with the Digital Camera. Thus, the proposed framework of SBPG integrated with SDC is suitable for high performance imaging in the IoT, such as Intelligent Traffic Surveillance (ITS) and Telemedicine. Due to power consumption, which has become a major concern in any portable application, a low-power design of SBPG is proposed to achieve an energy- efficient SBPG design. As the visual quality of the watermarked and compressed images improves with larger values of

PSNR, the results show that the proposed SBPG substantially increases the quality of the watermarked compressed images. Higher value of PSNR also shows how robust the algorithm is to different types of attack. From the results obtained for the energy-efficient SBPG design, it can be observed that the power consumption is substantially reduced, up to 19%.

ACKNOWLEDGMENTS

I would like to take this opportunity to thank God for being my strength and guide in the writing of this dissertation. First and foremost, my utmost gratitude goes to my major adviser Prof. Saraju Mohanty whose guidance and advice have been supporting me. His constant supervision and technical feedback have made this work possible. He has taught me the methodology, such as the divide-and-conquer method, that helps me to carry out the research and present it as clearly as possible. Also, it is with immense gratitude that I acknowledge my co-major advisor Prof. Elias Kougianos who also supported and motivated me through the completion of this work. I would also like to thank my committee members: Prof. Robert Akl and Prof. Cornelia Caragea for agreeing to review this work.

I would like to dedicate this dissertation to my late mother Maheilah. It was her wish to see me as a doctor, but without being able to see this beautiful day she passed away. So with this dissertation, I would like to remember her for all the dreams she had for me and would be thankful for her unconditional love and support throughout my life. I would then like to remember my father, who stood by me in all my difficulties and supported me as a pillar when I needed him the most. Without him by my side, I would not have made this day. I also take this opportunity to extend my heartfelt thanks to my wife and siblings, especially my brother Ali whose continued support and motivation never stopped.

I will forever be grateful to Prof. Wafi Albalawi, my former undergraduate advisor. He guided me all through my undergraduate school and my graduate career and gave me his valuable advice all along. He is and will be one of my role models as a teacher and a scientist. Last, but not least, my gratitude also goes to the University of Tabuk for their financial support of my PhD study. I also wish to thank the staff of the Department of Computer Science and Engineering at UNT for their support and encouragement during this entire period.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In recent years, the Internet and technology have involved at an incredibly fast pace, bringing new challenges and innovations into the modern world. Many aspects of life have been reshaped and re-organized through the continuous expansion of the technology and the Internet. Broadband connectivity and the wide range of new devices with great capabilities have made the Internet easily accessible for many people worldwide.

Since more and more devices become connected each day, a new paradigm is born: The Internet of Things (IoT). The IoT can be described as an integration of physical objects into the expansion of the Internet that use data to deliver intelligent services to the environment and from which data is collected. Every object that is part of the IoT has a unique identity accessible to the network, including information such as position or status [70, 84]. To better understand what the IoT stands for, the semantic analysis of the words reveals a relevant definition. While the word "thing" refers to a things information, where a thing can be anything from a device to a physical object, the word Internet refers to an Internet application. Combining the two meanings, the IoT can be described as possessing two main attributes:

(1) Handling the information that a "thing" generates.

(2) Working as an Internet application.

The IoT makes it possible for the information generated by a thing to be shared without any boundaries between global participants in the network. So far the graphical models that describe the IoT suggest that to build an IoT architecture, it is mandatory to preprocess the information generated by a thing before uploading it online. Research has proven through the set expression models that all IoT applications share a common feature in the sense that every IoT application is a set or an exchange of information. This led to the conclusion that the process of development and the technical methods involved in the execution of an IoT application can be used as a reference system and reused for the

development of more IoT applications.

While the IoT is just starting to be utilized, there are already various applications in the fields of Green-IT, energy efficiency, and logistics which benefit from the new concepts. The IoT unites both digital and physical dimensions, and its applications can change the social, professional and personal areas that comprise the modern life. However, as any new concept, the IoT raises different challenges that need to be overcome before full integration into everyday life. The areas of concern are trust and security, but also governance and standardization that are vital in making the IoT fair, open, and accessible to society. At the moment, the IoT is an essential part of the research agenda of many multinational companies and governmental institutions such as the European Commission [88].

1.1. The Development of the Internet of Things

The "Internet of Things" term appeared for the first time in 1999, when the exponential evolution of the Internet made it possible to predict its further developments and to explore, first theoretically, a wide range of opportunities that could arise [44]. The simplest definition of the IoT describes it as a network that connects physical items through Radio Frequency Identification (RFID) [105] to the digital world. The collaboration between physical and digital is able to provide innovative intelligent services that are yet to be researched. By uniting different types of sensors with the Internet, the IoT will allow the monitoring and control of real time events and objects through an Internet connection.

1.1.1. The Transition from the Internet to the Internet of Things

The Internet can be considered a living organism that grows constantly. Its importance in peoples lives becomes more significant as time goes. From its first definition as the Internet of Computers, which was basically a global network of services that had the World Wide Web as a unifying platform, the Internet changed in recent years in the Internet of People, where the Social Web or Web 2.0 is the main concept that determines how the Internet expands. All the people who are connected create, share and consume content, each having full access to any data. The Internet of People led to the growth of social net-

works that allow unlimited connections among people worldwide, through services such as Facebook, Hotmail, Gmail, and many others. Mobile access has made the social networks become a massive trend worldwide. Moreover, broadband connectivity has become cheap and accessible in most parts of the world. Figure 1.1 presents a simplified view of the IoT.

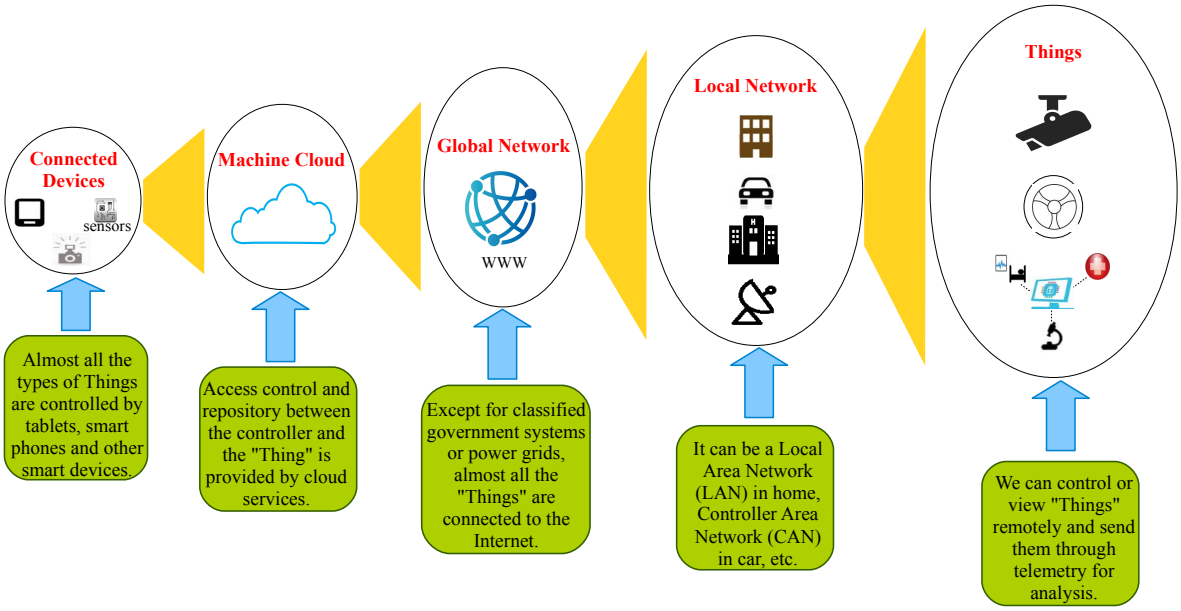


FIGURE 1.1. Simplified View of the IoT. After [43]

Technology has facilitated the expansion of the Internet through hardware implementations such as power and storage capacity, and small-sized devices. The new innovations have made PCs obsolete while increasing significantly the use of mobile devices such as smart phones, tablet computers, or notebooks. These devices contain actuators and sensors which can connect and work together, forming an intelligent environment. The new network of devices is able to compute, act, gather and distribute data, becoming thus an active part of the Internet.

Moreover, physical objects have started to assimilate an identity and a status, through tags such as RFID and Quick Response (QR) codes. The new generations of smart phones have integrated GPS (Global Positioning System) and an RFID scanner/QR-code reader, thus being able to scan any tag that belongs to a physical object [30]. Any smart device can

become a link between the physical and the digital world, transforming the Internet from its current status into the Internet of Things.

The IoT implies a very wide definition of the term "things". There is a massive variety of physical objects that the IoT can operate with, including smart phones, digital cameras, tablets, different elements common in peoples homes, cars, or work places, and also all the things that have a tag attached. Since the IoT is able to connect such an immense number of things and devices to the Internet, the amount of data available will increase tremendously since each thing or device will be able to provide new information and in some cases, services. When things, as envisioned by the IoT, become part of the same network, many smart services and processes will become easily possible and will be able to change how people understand and deal with the economy and environmental issues.

The IoT can be better understood as an ecosystem. Through the scan and identification of tagged things, the network can receive location information which can be transmitted further. At the same time, hardware innovations will make devices with sensors much smaller and easier to integrate into daily life, thus able to act on the local environment by establishing status and transmitting any event to higher levels services. Any activity and change of status would be communicated through the IoT. The data received from or about integrated things would be available in the cloud and would be accessible to all middleware and frameworks that enable applications and provide services. This attains a new level of intelligence which translates into better services with a greater impact on the whole environment. Predictions suggest that the IoT will connect almost every individual object, being able to track its identity, condition, and location, and communicate it to services of superior level. The IoT can unite billions of things, each containing its own data and each being able to act upon its environment.

The huge accumulation of data will have to go through smart processing, which will later make possible the existence of smart services with the ability of making decisions and taking actions. The evolution from the Internet in its current form to the IoT is already possible through certain available technologies. However, these technologies need serious

optimization. Applications are the path to accelerate the transition to the IoT and a way to unleash its potential of having a real impact on society, economy, or the environment.

So far, the implementation and acceptance of the IoT depends on fundamental concerns such as security, privacy, and governance. Even though it is still on the research stage, the IoT has the ability to challenge our entire perspective on technology and communication. There are wide areas uncovered yet by research that can impose more challenges and present even more opportunities. For many research facilities and academic institutions, the IoT is a priority of research among current affairs.

1.1.2. Applications of the IoT

Up to this moment, the concepts that make the IoT have been incorporated in a wide range of fields including transportation, logistics, energy, agriculture, defense, and smart environments such as personal residences, offices, buildings, or infrastructure. However, the true potential of the IoT is unlimited and it can include any other aspect of peoples lives. Figure 1.2 illustrates applications of the IoT.

In the world of technology and communication, the IoT has rapidly become of utmost importance, not just for research facilities or academia, but also for governments and industry players. Many multinational corporations are aware of the commercial benefits that the IoT can bring into their business. At this moment, IBMs Smarter Planet is working on adding intelligence to all the systems and processes that interact directly with the world [1]. To achieve real results and make an impact on the areas of banking, energy, health care, or city transportation, it will have to collect data from several types of things such as clothes, environmental elements, road infrastructure, and many more. Another company that is interested in the IoT is Microsoft and its Eye-on-Earth platform is able to determine the air and water quality in different European countries and thus, to provide essential data to climate change researchers [21]. Hewlett-Packard is also interested in the IoT, especially for their Central Nervous System for the Earth initiative, which aims to plant billions of small sensors on extensive areas of the Earth with the purpose of detecting motion [20]. The IoT is a subject of research for the Cluster of European Research Projects from the

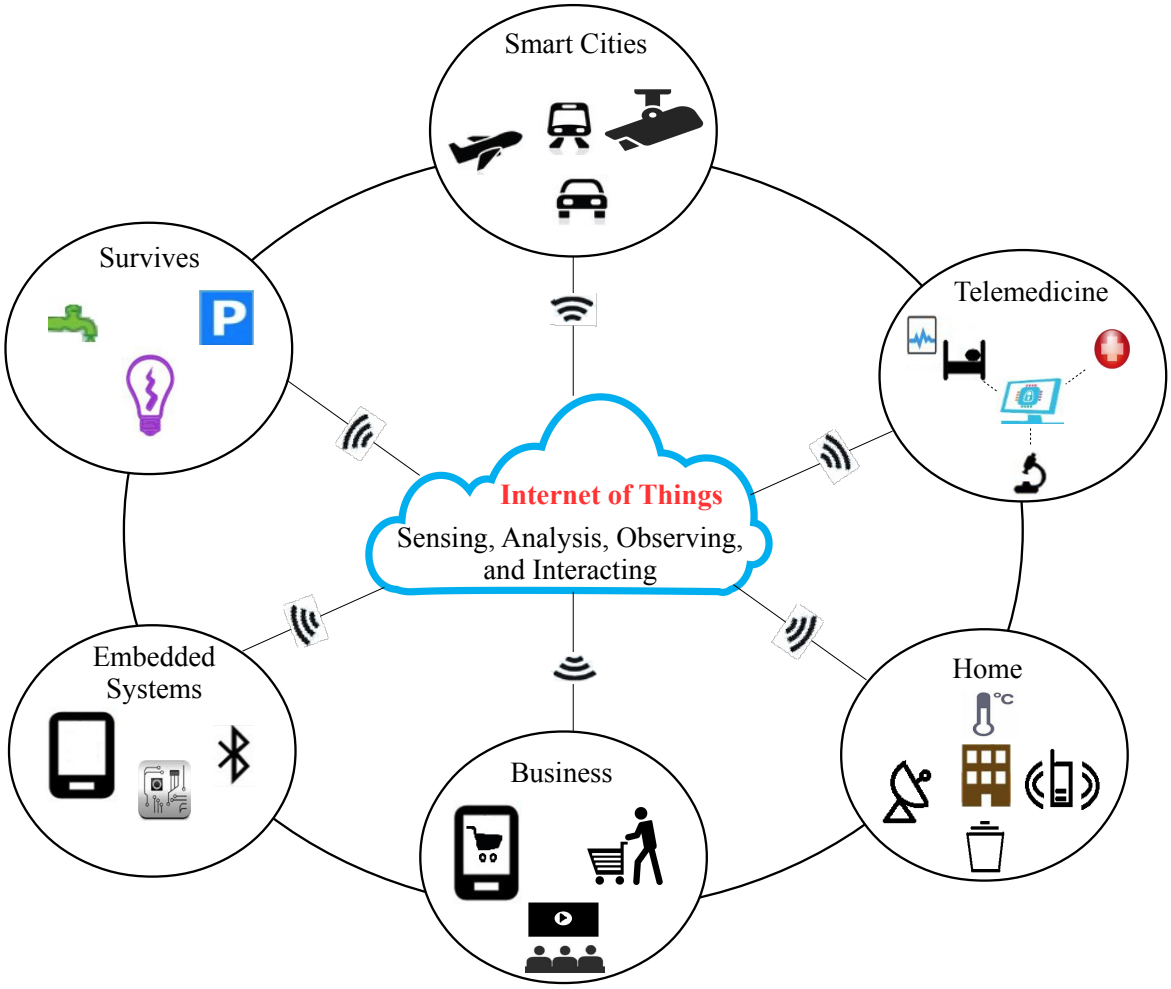


FIGURE 1.2. Applications of the IoT.

European Commission, which is developing platforms and running activities related to the relation between the Internet and the world of physical objects [100]. Some governments are interested in the IoT as well, especially for its potential to fuel economic development.

Worldwide, many research groups and academic institutions are developing projects to help in the implementation of the IoT, especially the MIT Auto-ID Laboratory, who is one of the pioneers that adopted the IoT [67]. These research groups and institutions have identified through their work a large number of domains where IoT applications will have a great impact. CERP-IoT, for example, believes that the IoT will have a tremendous influence on societal, environmental, and industrial fields. Some of the applications researched so

far are environmental monitoring, retail, logistics and supply chain management, energy and utilities optimization, medicine and health care, and independent living for the aging population through increased mobility, constant monitoring and greater diversity of wellness services. Since the IoT is in the starting phase, not all its applications have been yet foreseen. However, as the technologies will have time to mature, new innovations and needs for services and applications will arise.

The expansion of the Internet infrastructure in all the regions of the world and easy access to Internet connectivity can lead the IoT to have a tremendous impact worldwide. While for many years there has been a large inequity in terms of Internet access in some areas of the world, the gaps have been progressively diminished, making the IoT a possibility for many developing countries. The benefits of the IoT do not stop only at first-world applications. It is possible to use the IoT to solve real, imminent problems that can advance the state of society, economy, health, and many more domains by providing intelligent solutions that are feasible and easy to implement.

Some of the proposed applications of the IoT in developing countries refer, for example, to food security, by foreseeing droughts, localizing pests, or even exploring farming methods. The interventions in agriculture can be minor, such as information via text message to farmers, but they can have a huge impact on the overall agricultural activity. The IoT can also be used in the prediction of natural disasters. Using sensors, simulation, and in-situ monitoring, people can be alerted forehand. Many developing countries struggle with the water supply and in this case, an application through the IoT that uses networks of sensors can detect and notify people of catchment area management, presence of a stream or any incidents that affects the quality of water.

Fleisch [36] has been exploring, together with his team, the possibilities of the IoT to improve current world state, through its numerous applications. According to his studies, the IoT has a prominent relevance in every value chain and all corresponding steps. Fleisch has identified these chains and has split them in two categories: machine-to-machine communication, and inclusion of users. Simplified manual proximity trigger refers to the idea

that things are able to transmit their identity when they are located within the sensing area of a sensor, and when their identity is recognized, a certain action and event can be set in motion. On the other side, automatic proximity trigger means that when the physical distance between two different identified things reaches a threshold, an action is triggered, after taking into account the known identity and location of two things. The other value chain is automatic sensor triggering which is described as an intelligent thing that is able to gather data via different types of sensors, tracking orientation, temperature, vibration, humidity and many more parameters. After collecting all the required data, the intelligent thing can communicate the information further and determine decision making. Automatic product security is another important chain that is defined as allowing each thing to provide information by analyzing the relation between the thing and its digital representation in the form of a QR-code with a relevant URL link. Fleisch [36] separated the value chains that refer to users integration. He identifies three different chains:

(1) Simple and direct user feedback is realized through a simple mechanism integrated into each thing with the capability to allow feedback in the form of a signal, either audio or visual. Any individual located in a certain environment can provide this type of feedback.
(2) Extensive user feedback is correlated to all the services in the digital world performed by an intelligent device that is able to provide many types of services to a human, such as a smart phone or tablet.
(3) One of the most complex chains of value is mind changing feedback, which refers to the possibility that the applications of the IoT can influence and change human behavior.

One such example is the opportunity to change the driving behavior according to sensors integrated in the vehicle. Together or separate, all these seven value drivers discovered and defined by Prof. Fleisch have a real impact on the applications of the Internet of Things.

A team of other researchers [26] have come up with a different classification of IoT applications, separating them in two general categories. One category refers to information

and analysis, while the other one to automation and control. The category of information and analysis includes decision making services improved by access to large amounts of updated information received from each object part of the network from a certain environment. Analysis becomes thus more accurate and able to determine with greater precision the current status. This category of application is valuable in tracking, especially in logistics and transportation, and environmental status by offering information such as temperature, humidity, or vibration through the use of real time data and feedback. These applications are also relevant for decision making based on sensor-driven analytics and for determining behavioral patterns such as shopping or entertainment preferences.

The category of automation and control refers to the applications that act according to information taken from data that has been already processed and analyzed. At the same time, these applications can sense and transmit information such as energy consumption and utility usage in homes and offices and transmit then to a central service that informs owners how to adapt to a better usage for lowering costs. Automation and analysis is thus one of the most remarkable and promising areas of applications that come with the IoT. Because of their capacity to display human capabilities such as detecting objects, and measuring parameters, these applications raise many challenges in implementation and research, but they also represent the peak of development for the IoT. While it is difficult to foresee how the IoT will grow, since technology advances so quickly, it is obvious that the IoT will create a massively populated network with the potential to generate highly intelligent services through its unlimited accumulation of data. In the short term, services will become more sophisticated and innovative, while in the long term the network of connected things will become omnipresent and its services universal.

1.2. The Challenges of the IoT

To become a reality, the IoT must overcome a series of challenges that have slowed down the process of development and societal acceptance. The challenges discovered so far range from applications, context and policy, to technical development. When a central location gathers data from every object and environment, it is challenging to ensure the

protection of each persons right to privacy. The second highest concern is a technological challenge that refers to large amounts of data which need reliable storage, interpretation and analysis. Figure 1.3 presented an overview of the IoT challenges.

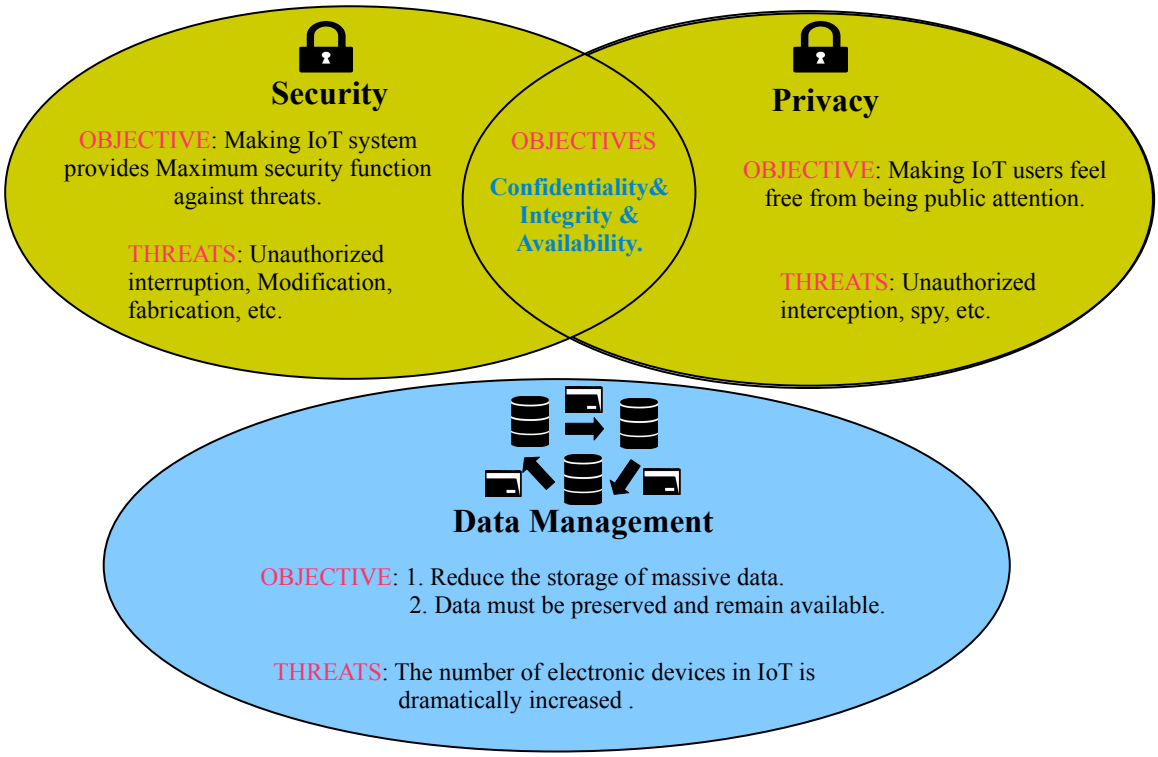


FIGURE 1.3. IoT Challenges.

1.2.1. Privacy and Security Challenge

The fast evolution of the IoT requires societal acceptance before implementation in peoples lives. However, one of the things that slow down the process of acceptance are the concerns regarding privacy and security. The IoT is already a key element of the Future Internet and it is an infrastructure that reaches national and international levels, soon being able to connect the entire world and billions of users worldwide. The need for ensuring privacy and security has thus become a priority.

Most applications and services that rely on the IoT are using large scale information management systems which makes them defenseless when fighting against information theft

and other kinds of attacks. Security threats include DoS (Denial of Service), Man in the Middle attacks, Replay and many other attacks common to networks. So far, the DoS/DDOS attacks are easy to fight on the current Internet [19]. However, the IoT is much more exposed to such types of attacks, which means it will require special defense mechanisms to guarantee safety. It is essential that important infrastructures such as transportation, energy, and city services could not get manipulated by subversive attacks. Another threat is represented by nodes and malicious code hacks which require IoT applications to execute immediate detection and recovery. The IoT requires the development of cyber status awareness tools or methods that will provide continuous monitoring of all its infrastructures. Protection during the lifecycle of a system and prevention against all attacks need to be guaranteed. Moreover, the IoT needs to allow different control and access schemes according to the profile of the user. Authorization and procedure models are difficult to implement because of the variety of devices and gateways that request access. One of the challenges of developing protection schemes is caused by the need to allow all modes of operation to act without human control. The IoT will require in its mature stages a self-management technology, such as machine learning.

For the IoT to reach its full potential, people have to trust it completely. Individual users and contributors must trust that the information they share or use will not be exploited by third parties to negatively impact any other person or society as a whole. The needs for data confidentiality and informed consent are essential in the development of IoT. At the same time, trust brings to light the other technological issue since it is difficult to establish who will be in control of the sensors. So far, there have not been any proposals in concerns to governance and standardization. However, these issues must be addressed as the IoT grows. Most of the information used by an IoT application is personal data which needs protection and prevention against attacks and handling by unauthorized trespassers. Some of the most common methods of protecting data are available for the IoT as well. Through cryptographic techniques, data is stored, interpreted, and shared without giving access to foreign entities. There are also some techniques that safeguard data by using specific design

concepts, such as data minimization, ambiguity, identification, or authentication. Another protection method is self-configuring access control that uses the real world as a model. Some of the privacy implications that result from the development of the IoT refer to the preservation of location isolation, which means that location is indirectly established from things related to an individual, allowing thus the prevention of personal information for individuals who prefer to keep all their data confidential through all the IoT data exchanges. In the structure of the IoT each integrated object has a unique identity and it is provided with the ability to transfer data without requiring permission from a human since most of the interactions in the network are source-to-destination or human-to-computer. In the IoT objects are free to share information about their identity and status and all things can connect at any moment and anywhere. However, all the future opportunities that the IoT can bring are endangered by the lack of appropriate security options. Security is the primal aspect that slows down the growth of IoT applications. Since the magnitude of the IoT is remarkable, so are the risks because when an object from a network is affected, the entire network encounters high levels of insecurity. Moreover, the IoT has the potential to develop in areas where a compromise on security is not possible, for example, health care. One of the problems of security is that it is impossible to associate one device with one individual since most people own multiple devices such as smartphones, tablets, laptops, and others. This raises a critical challenge in terms of identity management. The possibility of identity theft makes it more adequate to detect threats by location, and not by the identity of the user. Privacy concerns also recommend maintaining the level of required information for each application to a minimum and decentralize the computing process, using several soft identities for each specific application to not disclose the real identity of the user.

In general, security of the IoT architecture is mostly focused on the end-to-end interaction links among the integrated nodes. The International Telecommunication Union has found that to ensure the security of the IoT, it is necessary to focus on middleware level, because at this level is where connections between various nodes happens. This discovery, however, is based on the idea that all integrated nodes in the IoT go through a virtual mid-

dleware that allows them to function with great efficiency. This idea has not yet been fully verified by a reality check, which means it is possible that other scenarios that havent been envisioned yet will happen, especially since the nodes connect with each other mostly on a machine-to-machine structure, without requiring human participation. This situation leads to the need of designing a security pattern for the IoT that is embedded into the nodes, where it cannot be threatened. However, there are several limitations on the physical and technological level that require a proper optimization of parameters such as size, storage capacity, memory, and others, otherwise any effort to introduce security algorithms will not give the expected results. The security requirements for the IoT lead to the conclusion that security designs need to be very complex and are thus, complicated to develop. Most of the current security architectures are focused on Wireless Sensor Networks (WSN) and the Internet as it appears today. IoT applications require their own, specific standardized Intrusion Detection Systems (IDS). At the moment, the SVELTE design [86] is a reasonable security design that can prevent the alteration of information or selective forwarding, but this is a fragmentary solution that does not deal with the major security concerns raised by the IoT. Another security solution for a trustworthy IoT includes cryptographic modules which have limited power and can only protect very few IoT objects or hosting domains. Moreover, cryptographic modules only work if the IoT applications are trustworthy by default, which is difficult to establish. Using existing security designs for meeting the requirements of the IoT remains thus an open issue.

Other topics for research in the privacy and security of the IoT are authentication and access control, which must be integrated in the communication architecture of the IoT while maintaining attack resistant features. Both authentication and access control have paramount importance in security designs, and there is a pressuring need to ensure that the authentication and access control schemes are developed enough to cover the needs of the IoT. So far, research on these topics has not reached a mature phase, yet it continues with plenty of room for growing. The current protocols will be most certainly developed further. However, at the moment, it can be concluded that there are three types of attacks:

(1) Application based.

(2) Connection based.

(3) Platform based.

Discovering the perfect security solution is a journey of multiple steps and a process in itself, which opens numerous possibilities. As the opportunity for new solutions arises, the threats also evolve and become more complex. Before designing solutions it is also important to assess the potential of the devices integrated in the IoT and their computational capabilities. For solutions to work properly they must fit the technological potential and capacity of the IoT, and be able to work within its limitations. The need of powerful authentication and access control schemes seems to be correlated with the need to surpass certain technological challenges identified in the architecture of the IoT.

To sum up, the IoT is a heterogeneous environment that requires a flexible and resourceful framework that can deal with its legal status, global reach, ethics, and security. The devices and objects that interact in an IoT system must be protected both in their horizontal and vertical interactions. So far, the predictions suggest that a holistic strategy for security raises many challenges, but once discovered it can be extended to include all kinds of IoT implementations.

1.2.2. Data Management Challenge

As many other large scale data projects, the IoT imposes a key challenge regarding the storage and management of the massive data stream that will include billions of data suppliers from all over the world. Moreover, the data must be preserved and remain available for future generations. At the same time, it needs to be interpreted and analyzed to give actual results. According to research conducted so far, data deluge is one of the greatest challenges that the IoT needs to overpower. When the IoT matures, an entire world of objects will have to be organized. Between these objects, there will be a constant flow of information, which requires the functioning of many simultaneous processes and generates significant amounts of additional data [19].

A series of key concepts have been employed to identify all the challenges and possibilities of development in data management. Some of these concepts are data collection and analysis, virtual sensors, semantic sensor networking, big data, and complex event processing. Saving data in a secure environment is one of the essential aspects that can dictate the success of the IoT, since it deals with sensitive data within a distributed system. A secure storage comprises of three fundamental components that build its architecture [83]:

(1) The first component is the data processor which processes the data before transmitting it further to the cloud.

(2) The second component is a data verifier which checks if the data already in the cloud has suffered any damage.

(3) The third component is a token generator which supports the cloud storage provider in reclaiming fragments of customer data.

1.3. Principal Applications of Image Communication in the IoT

The IoT offers broad opportunities for development in many areas, such as economy, health care, and environment. Through advanced technologies such as RFID [105], the IoT can improve how people manage their entire lives, from daily transportation to medical treatments.

1.3.1. Smart City

The IoT is known to provide numerous opportunities for applications that can impact the environment in a positive way, making life easier for people. The ability to process real-time data, and to use information from a vast number of devices makes it possible to sense and share important data among a huge number of users. The smart city is one of the eco-systems that emerge from the relation between the digital and the physical world. On the path to offer advanced infrastructure and environment information, smart city comes as a solution to provide intelligent services about transportation, roads, power grid, and much more, while optimizing the physical resources through smart sharing of data. The services of a smart city present an extensive variety of solutions in different areas that influence the

life of the city, ranging from transportation, public administration, entertainment options, utilities, and health.

The best definition of a smart city is an application of the IoT through Augmented Reality (AR) technology that focuses on improving public transport by offering to the citizens the possibility to access information about bus arrival and departure times, bus routes, and popular touristic landmarks just by using smartphones and AR technology [83]. Over 50% of the world population lives in cities and this number will increase in the following years. To become easy to navigate, cities would have to adopt an accommodating approach to make life easier for the citizens. The best way to provide quality services of information is using automation that can collect data from different places at the same time and reuse the information without restrictions. Cities are complex systems comprising numerous businesses, communities, services, and a large number of people. Therefore, the smart city becomes a reliable and intelligent help which can introduce new services while also upgrading old ones.

Augmented Reality is the main technology of a smart city application because it adds to a real view of the world supplementary computer generated content, including GPS data, images, sound, video, and others [10] and [15]. When an AR marker is detected, a process of augmentation begins and the user receives all the corresponding AR content based on the detected marker [51]. A marker can be a pre-defined image or a GPS location. Its innovative characteristics make AR one of the top strategic IT technologies available today [38]. Any smartphone possesses AR technology and is capable of supporting AR based applications. However, when it comes to smart city services, AR technology has not been yet fully integrated. A successful example is SmartSantander, an application which allows the citizens of Santander to access information such as real-time view of traffic and beach cameras, bike rental services, bus schedules, and weather forecasts. The application contains information about almost 3000 places in the city, separated into categories. Other applications similar to SmartSantander are StreetMuseum in the UK that offers museum tours and an application based on AR markers in Madison Square, New York that provides

information about the smart city services in use. The advantages of AR technology are numerous, yet the possibility of dynamic information that changes according to location, time and date, user profile, or other parameters is the most important.

One challenge in the development of smart city services is data privacy. To obtain information, citizens must give access to private data such as GPS location and travel itinerary. Since this data will travel through the cloud infrastructure it is important to establish privacy and to not allow public display. Moreover, any unauthorized fleet management devices that are also part of IoT should not be allowed to connect to the system. Both IoT devices and end users must be protected. Role-based techniques already integrated in standard network infrastructure such as LDAP, RADIUS, SSH and others can help establish the identity of each user and associate a series of privileges that correspond to the users profile and the role in the system [48]. This operation uses HTTP cookies stored in the browsers history, but many IoT devices do not disclose their identities. In such cases, control of access is established through other data such as proximity, location, and other essential parameters.

As a conclusion, a smart city cannot be completely safe and trustworthy until the security concerns are fully addressed. However, once these concerns disappear, the smart city can be further developed, as it is already presenting a wide range of opportunities. In the future, the smart city will include the possibility to purchase a bus ticket directly from the application and to use the same ticketing system for all modes of transportation available in a city. The application will cover bicycle rental locations and tickets, tram tickets and timetables, and much more. Moreover, the application will also include an algorithm able to determine the duration of routes depending on the mode of transportation, thus allowing citizens to choose the fastest and cheapest transport according to proximity and many other criteria.

1.3.2. Telemedicine and mobile Health Care

Considering its role in extraction, transmission, and use of information, the IoT has broad application opportunities in the fields of medicine and health care. In the progress of civilization, health has always been a priority since it is the fundamental condition that

must be met before considering economical or societal goals. In the past decades, medical approaches have transitioned from biomedical to biological-psychological-social medical. The development of medicine means integrating personalized treatments and a wide variety of services and interventions.

The IoT is able to ease access to top medical assistance, minimal medical costs, short treatments, and excellent medical services for any patient. The IoT can control medical data such as sample identification or medical records. The IoT can build remote consultation systems centered on the patient, provide an easy way to monitor critical cases, and build a management platform for health care using all the data captured by the equipment which monitors, measures and transmits information on the human body. Some of the most important applications of the IoT refer to medication control and medical equipment, management of medical data, mobile medical care and telemedicine, and personal health management [44].

Using visualization technologies in material management, it is possible to keep track of the entire process of medical production to ensure a high level of medical safety and security for the public. The IoT is able to monitor and manage medication and medical equipment in two different ways:

(1) By ensuring the anti-counterfeit of medication and medical equipment.

(2) By providing steady real time monitoring.

Since the RFID tag attached to each product establishes its identity, and the tags are too complex to replicate, any product can be checked for identity, thus making it easy to discover counterfeit products. Both patients and hospitals can scan the tags and compare them to a public database of all medication information, and determine if the product is genuine or not, according to the record from the database. At the same time, RFID tags offer the possibility for stable and constant monitoring of the entire process of production, distribution, and consumption of medication. During the process of packaging, readers attached to the production line can scan automatically each medicine, establishing its identity and communicating it to the medication database. Moreover, during distribution, readers can access any information about the process at any time and monitor its every step. By moni-

toring delivery and storage of medicine, it is possible to ensure a high standard of medication quality. Another benefit is that in case of quality issues, it is possible to follow the process backwards and check for the causes of any malfunction. Information such as name, category, origin, distribution, sale, and any other, will be available for tracing the source of problems. The collaboration between hospitals and shipping companies, aided by RFID technology, can ensure that the medical refuse information is available and can be traced, preventing thus any illegal utilization.

The IoT can bring multiple advantages in the management of medical information by developing applications for the management of patient information, medical emergency, medication storage, blood information, medicine traceability, information sharing, and many more. Having access to a complete health profile makes it easier to prevent any misappropriate treatment that could harm the patient. RFID technology can be a great aid in cases of medical emergency when critically wounded patients are not able to offer their identity. RFID allows quick access to the patients name, blood type, medical history, age, and contact information for getting in touch with relatives and saving a lot of valuable time in providing emergency treatment. Another application of RFID technology refers to medication storage. With no need for paper and manual recording, it will become easier to prevent misunderstandings about medication names, dosages, expiration dates and much more. The ability to detect identity of patients and blood type makes RFID technology a great help in blood information management, since it can prevent blood contamination and increase overall efficiency.

The fact that RFID technology can keep track of the entire medication process and pharmaceutical preparations, including details such as prescription, distribution, dosage, medicine taking, effects, purchases, and storage conditions, doctors can easily check which medication a patient has taken and what the effects of the treatment are. At the same time, patients can keep track of their treatment history and make sure they have followed every step correctly. RFID can also track the identity and origins of each medication and medical equipment and the identity of patients who used certain medication, ensuring that in cases

of quality problems, suspect medication can be removed from public access and utilization.

RFID technology also allows the formation of a wide and advanced network of doctors, hospitals, and private clinics that share medical information and records for the benefit of the patient. Patients will be able to change easily both their doctors and their hospitals while doctors will be assured they have access to the complete medical history of each patient. RFID technology can also work as an alarm system, helping patients to easily send emergency signals, preventing them from leaving hospitals or quitting vital treatments.

The Internet of Things also deals with two new concepts such as telemedicine and mobile health care [44]:

(1) Telemedicine is a series of innovative services based on a combination of different technologies such as computer science, communication, and multimedia that is able to provide diagnoses, reduce the costs for health care, and offer the possibility of remote assistance and constant monitoring of patients.

(2) Mobile medical care means the creation of a database for each patient, able to monitor health dynamic information such as weight, fat content, cholesterol level, and many more. The information can be transmitted to related medical facilities that can provide assistance and advice for improving the health state.

Overall, the applications of the IoT in the field of medicine and health care are remarkable and can provide intelligent services and make the medical world easier to navigate for both doctors and patients alike.

CHAPTER 2

RELATED PRIOR RESEARCH

Acceptable size with highest quality of the image has been the demand of the rapidly increasing number of multimedia applications. Undoubtedly with that extension, the concerns of privacy and security in the multimedia field have been also increased, and the secure network communication to transfer multimedia over the Internet, cloud, or Ethernet becomes a critical aspect. The privacy and security concerns include man-in-middle attack, data tampering, and unauthorized access. The major threats depend on the application domain that a digital camera is used for, since a digital camera is used as an emerging technology for various applications and systems such as surveillance, entertainment, and smart environment. The Secure Digital Camera (SDC) offers new trends for scrutiny and inspection of road traffic at different route points including critical intersection points. In this chapter, related prior research in secure image communication is described. In addition, related studies in SDC design and image compression are discussed. Significant research has been conducted in the last decade towards the usage of SDC in image communication in IoT applications.

2.1. Secure Digital Camera (SDC)

Photography might seem like a modern invention, but the reality is that its history goes as back as the 12th century, when simple glass lenses were invented. The first photograph ever taken dates from 1787 and was taken with the use of an in-house camera. One century later, George Eastman built the worlds first camera and named it “Kodak”. Eastmans invention went through another century of development and in 1975 the Kodak Company introduced the first digital camera in history. In 1990 digital cameras with a CCD image sensor, able to store images and make them available for download through a computer, became commercially accessible. One year later, Kodak DCS-100 was released, becoming the first of a wide production of Kodak DCS DSL cameras.

Today, digital cameras come in an incredible range of sizes, quality, prices, or capabilities. Figure 2.1 illustrates various types of digital camera. The simplest version of a digital

camera is the webcam. A compact CMOS sensor-based camera, the webcam is usually integrated within computing appliances, such as PCs or PDAs. For casual use, compact cameras have portable designs that make them very user-friendly. Another type of camera available on the market is the bridge digital cameras, which are usually mid-end digital cameras that combine the portability of the compact camera with the classical single-lens reflex (SLR) of the professional cameras. DSLRs, or digital SLR cameras, are professional cameras built on the classic model of SLR cameras while mirrorless interchangeable-lens cameras are a type of camera that feature the large sensors and interchangeable lenses typical of DSLRs and the live-preview option typical of compact cameras [69].

With the rise of the Internet, multimedia information can be transferred easily. However, the flexibility in sharing multimedia data raises the concerns of copyright protection and intellectual property rights. To solve this issue and enforce real-time DRM, the SDC has been developed.

SDC or Secure Digital Cameras are a type of camera that includes built-in feature that ensure the protection of all images that the camera produces. In the architecture of an SDC, every module such as image sensor, watermarking, and encryption is independent from each other, but they collaborate in the system-on-a-chip (SoC) design of the SDC. Every secure image sensor is composed of several units that include: APS array, ADC, LFSR or linear feedback shift register, and watermark adder. The secure image sensor, as shown in figure 2.2, works by taking the output signal from the APS and changing it to a digital signal by ADCs, with every column of pixels in the APS array corresponding to one ADC. Afterwards, the watermark creation unit represented by the LFSR circuit produces a unique bit stream. The LFSR is built to take as input a sensor characteristic aware key. Each input key is unique for the APS, and it remains private to allow the watermarking process to go through a false verification. The final step belongs to the watermark adder which has the task of adding together the digital signal captured by the ADC and the unique watermark produced by the LFSR in order to generate the watermarked and protected output signal with the use of the secure image sensor.

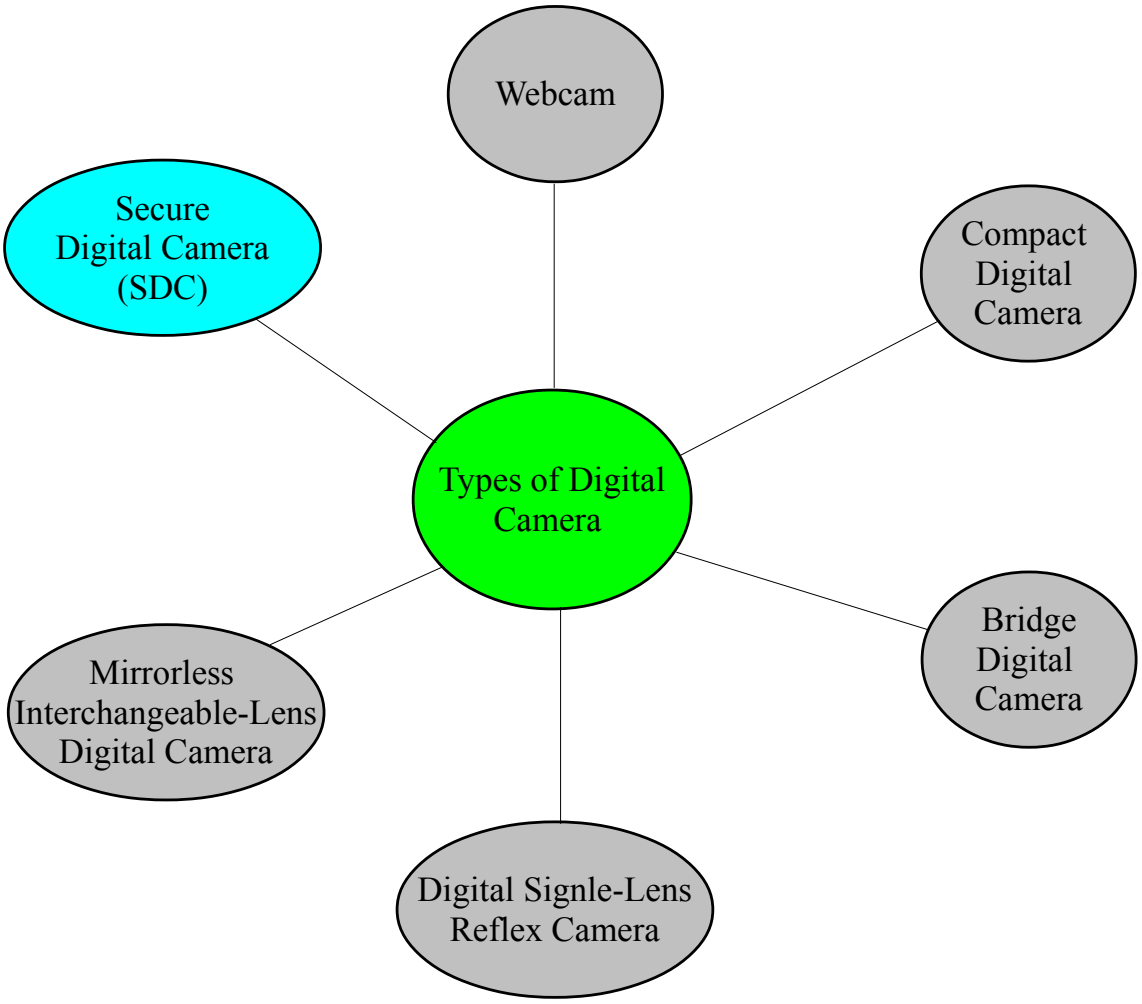


FIGURE 2.1. Types of Digital Cameras. After [69]

A unique approach of SDC integrated with two-layer protection, encryption capability and watermarking is presented by Mohanty [71]. The proposed architecture considers hiding binary images and their secure authentication. A method for Field Programmable Gate Array (FPGA) implementation is also presented. Compatibility of the proposed methodology with SoC technology and different multimedia constructing electrical devices was also presented. Darji *et al.* [31] shows development of hardware capable of entrenching an invisible watermark using LeGall 5/3 (Discrete Wavelet Transform) DWT. The limitations of the digital camera were considered by the authors in the suggested structural design. A

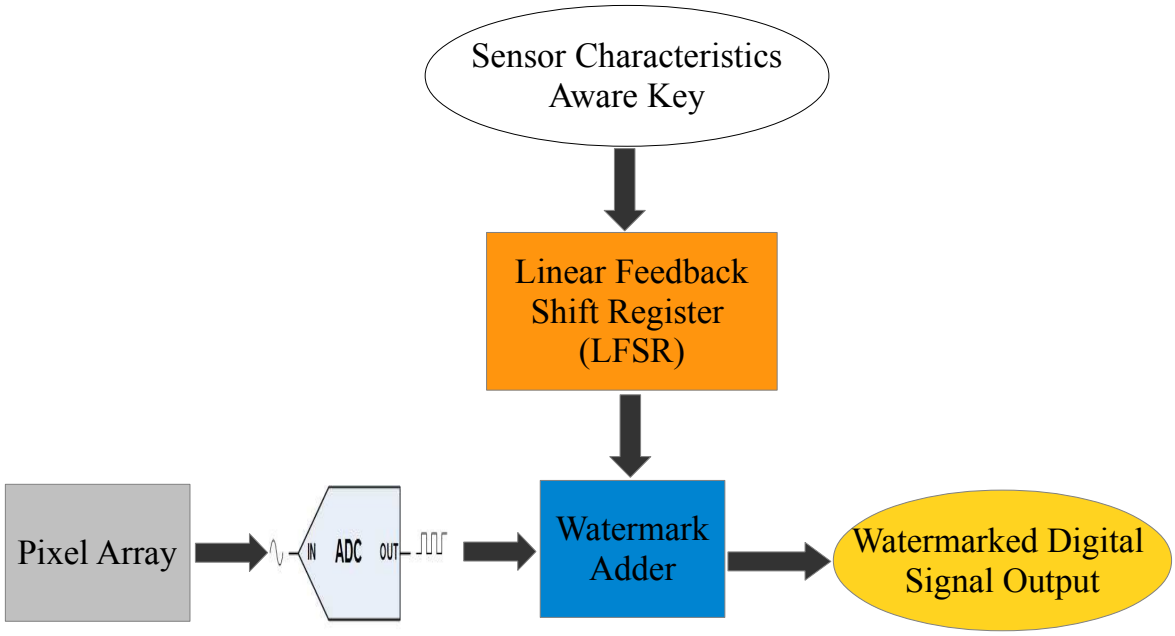


FIGURE 2.2. Schematic Diagram of Secure Image Sensor. After [69]

0.18-μm technology UMC standard processor was used with Verilog HDL to implement in VLSI design. The algorithm was assessed with the JPEG compression.

To attain support for pictures and illustrations captured by digital cameras, a novel scheme is used in [104]. The two-fold techniques proposed employed a combination of semi-brittle and vigorous blind type watermarks. The proprietors biometric records and rate of recurrence of information are used by the authors for the development of watermarks. It is worthy to mention that the projected plan is capable of meeting the requirements needed for image verification and patent protection.

An innovative approach for implementing the two observable digital image-watermarking methods was provided by the study in [91]. These methods are principally based on the very large scale integration construction approach, which is capable of being incorporated into any other available digital camera structure. A series of steps for dealing out pixel-by-pixel watermarking based on signal-to-noise ratio were also presented.

2.2. Image Compression Algorithm

The JPEG-2000, a successor to JPEG, intends to overcome several of present drawbacks such as better compression scalability, resolution accuracy and compression ratios. Ghodhbani *et al.* [90] suggested that the JPEG-2000 compression is very efficient and optimized when implemented using hardware compared to the present software implementations and demonstrated an optimized EBCOT algorithm architecture which is implemented on an FPGA platform. An improved efficiency of operation is observed which is implemented in VHDL for a pipelined BPC encoder.

HEVC which implements methods of compression based on minimum recursive block partitions of 4×4 and 64×64 blocks were studied by Liu *et al.* [64]. The efficiency of HEVC coding is improved by tree-structures and prediction modes. A fully pipelined parallel HEVC implementation with negligible Peak Signal-to-Noise-Ratio (PSNR) was demonstrated that allows real-time encoding, such as 1080p at 30fp with minimal hardware at 600 MHz.

Resolution of 7680×4320 and 3840×2160 at a frame rate of 120fps is the expected support by the Ultra High Definition Television (UHDTV) format. This requires a data throughput that is 100 times higher than the current 1080p HDTV. Zhou *et al.* [118] proposed optimizations such as binarization components, lookahead rLPS, hybrid path coverage, context modeling and pre-normalization to reduce the path delay of BAE. These optimizations are possible by exploiting the incompleteness of data dependencies in rLPS updating, which yields a Context-Adaptive Binary Arithmetic Coding (CABAC) encoder at 4.37 bins/s, i.e. a 45.3% optimization costing 4.8% BPCC performance degradation and 62.5% better performance than current architectures.

HEVC with high performance SAO encoding is allowed by an optimized VLSI architecture. Mody *et al.* [68] demonstrated 4K resolution at 60 fps at 200 MHZ using 0.15 mm^2 of silicon area in a 28 nm CMOS process with artifact avoidance algorithms, which provide 4.3% savings in SAO encoding.

Recent research has produced a new high performance lossless color image encoder and decoder architecture capable of functioning with minimal memory and bandwidth re-

quirements. The proposed system [55] is composed of Golomb-Rice coding and DDPCM (Differential-Differential Pulse Coded Modulation). The processing starts with organizing the host image frame as $m \times n$ arrays. These arrays go through DDPCM and generate 1 seed and $(m \times n) - 1$ individual sections. The algorithm compresses the data and generates lossless compressed data. An analysis on performance conducted on real benchmark images proved that the presented architecture provides high compression rate and throughput, and it is able to execute an enhanced number of real-time lossless compression and decompression operations within a moderate hardware area and with reasonable power consumption. This is possible because the new architecture exploits the possibility of carrying out parallel operations at the same time.

Image compression can be defined as a process of encoding data by using a shorter number of bits. Compression is mostly helpful in lowering the size and transmission bandwidth. Image compression can be categorized as [95]:

(1) Lossless image compression, that facilitates the reconstruction of the original data from the compressed data.

(2) Lossy image compression, which generates an approximate reconstruction of the original data while maintaining a better compression rate.

To make lossless compression more efficient by increasing the accuracy and reducing the resource-dependency, recent research on the topic has proposed [95] the building of an integer to integer multiwaveletet unit which would be applied on the lossless image compression. The results of the tests show that integer to integer multiwavelets can reduce image entropy by integer transform, and it can achieve better processing speed.

Most of the time, practical scenarios require that image encryption should be executed before the image compression. The challenge of designing a pair of algorithms for encryption and compression that would generate an efficient encryption of the images before their compression has raised many problems. To solve these problems, a new Encryption-then-Compression (ETC) system has been designed [119]. ETC is highly efficient and can be applied to both lossless and lossy types of compression. ETC achieves image encryption

by using random permutation and prediction error clustering. To compress the encrypted data, the system employs a context-adaptive arithmetic coding approach. After extensive testing, it has been proven that ETC provides a high security level. Furthermore, the ETCs compression efficiency is similar to state-of-the-art image codecs, both lossless and lossy, even though the latter work with original images as inputs, and not encrypted versions. So far, most of the current ETC solutions come with certain disadvantages in terms of compression efficiency.

One of the concerns in the design of a wireless sensor network is that when the networks are integrated in cameras, the image size suffers limitations. Therefore, transform-based image compression techniques have become popular, usually built either on Discrete Cosine Transform (DCT) like JPEG or on Discrete Wavelet Transform (DWT)like JPEG2000 [40]. While DCT algorithms combine high speed, with low memory and low complexity, they can also cause malfunctions in low bit rate transmissions. DWT algorithms, on the other side, have also low complexity but are able to produce a bitstream with the possibility to decode it at multiple transmission bit rates, maintaining a reasonable quality of the reconstructed image. A short analysis on the DWT achievements when associated with Set Partitioning in Hierarchical Trees (SPIHT) has been conducted in [40]. A quality-scalable wavelet based image coder, SPIHT can be used in image compression with lifting based DWT techniques. SPIHT makes the new architecture suitable for platforms with limited resources and restricted memory.

A comparative study of image compression methods has been conducted in [24]. These techniques are useful in cases of need for high speed communication. The study analyzed different compression methods such as JPEG-2000, Fractal image compression, Tri-DCT, SADCT, and DCT integrated in encoding and encoding methods such as Embedded Zero Tree Block Coder (EZBC), and Set Partition Embedded Block (SPECK). It is also important to underline that images present distinctive features in comparison to natural images. After running several tests, the results demonstrate that, JPEG-2000 with SPECK coding provide the most outstanding results in comparison to all the other techniques and combinations.

2.2.1. High-performance Design of Image Compression

A new SIFS (searchless iterative function system) fractal compression method has been developed in [81]. The new method is able to encode image range blocks centered on fixed location domain blocks. One of the benefits that this method brings is the possibility to maintain an impressive image quality and a compression rate even for range blocks as small as 2×2 pixels. This is possible because the fractal code does not include the typical coordinates (x, y) of the domain-range pairs. The method has been incorporated in a fractal image compression device. After various tests, the experimental results suggest that the highest PSNR and the compression rate of the recomposed image maintain the same level of quality as the typical domain block search techniques. The conclusion is that real-time fractal image encoding is possible. The method proves to be highly efficient and fit for hardware integration. Since the encoding process can be performed without iterative operations, the computation will not require great effort from the hardware.

A new high-performance system for real-time video compression applications has been developed in [114]. The system consists of a motion-estimation processor (PC-486), a DCT/IDCT processor, a camera, and an image grabber. The two processors perform at 12.5 MHz as back-end. While the motion-estimation requires around 100 μs to complete computing, the DCT/IDCT processor only requires 10 μs to compute the bidimensional DCT-IDCT for a single 8×8 block. Its performance is very suitable for a real-time video image encoding application. Considering these results, a real-time H.261 working on a MPEG image encoding system integrated in a personal computer can be easily developed.

A new image compression method has been proposed in [103]. Built on the independent EBCOT, the method is capable of an outstanding compression performance. It can generate a bit-stream with a wide and complex range of features, among which are the "random access" feature, resolution scalability, and SNR scalability. All these remarkable features cooperate within each bit-stream without compromising the efficiency of the compression. Even though it performs extremely well, the algorithm remains modest in regards to complexity. It is easy to integrate in applications revolving around remote browsing

of sizeable compressed files. Since the algorithm can produce independent, well-embedded bit-streams for a small block of sub-band samples, the optimization of the rate-distortion after compression is easily enabled. The EBCOT algorithm allows impressive flexibility for each bit-stream, because the encoder can use any number of layers from a combination of code-block inputs, thanks to the abstract quality layers that do not correspond directly to a specific structural property of the entropy encoder.

Real-time image compression can be also realized with a new method and VSLI architecture that is built on the Vector Quantization of DWT parameters. The architecture in [41] can generate real-time image compression of a 1024×1024 resolution, as a result of combining efficiently the hardware of VQ and DWT. The algorithm also features a high speed encoder since it uses a 2D DWT and a binary tree search based on VQ (BTSVQ) that does not require high hardware performance in VSLI integration. The real-time Wavelet Vector Quantization architecture brings together two types of VQ. While the MSVQ can encode the lowest frequency sub-bands of wavelet parameters, the CVQ can encode sub-bands of higher frequency, thus leading to a higher overall coding efficiency. The proposed architecture can be integrated in VHDL.

A new compound image compression architecture for real-time applications of image transmission has been proposed [63]. For an efficient real-time image transmission it is necessary to have a compression algorithm able to encode at a high compression ratio, while employing low complexity and having the ability to generate first-rate visual quality. The experimental results show that SPEC is remarkably suited for such a performance. Usually, for each image, SPEC performs two main tasks:

(1) Generating an accurate division algorithm that can separate graphics/text from pictures.

(2) Generating a lossless coding algorithm for graphics/text compression.

Future research will focus on raising the precision of the segmentation and the efficiency of the lossless coding. Another addition for the future could be modifying SPEC to perform compression of scanned document images.

Most digital cameras are able to perform demosaicing and compression. Recent research has proved that compression-first scheme provides better image quality and complexity than the typical demosaicing-first scheme. A new scheme [27] for efficient lossless compression of Bayer images has been developed. The scheme for the difference estimation of adaptive color has been created to eliminate spectral redundancy. It employs a context matching technique that ranks the adjacent pixels of a pixel to predict its sample value. The next step is encoding separately the prediction remainders of the two sub-images using Rice code. The results of the experiments prove that the algorithm is capable of performing a high quality compression.

The research in [45] proposes real-time image compression, which is built on the JPEG-2000 standard. The system performs image segmentation together with parallel compression. After segmenting high resolution pictures, the system compresses them tile by tile through the help of various image codecs such as ADV212. The results of the experimental tests suggest that the system is able to provide real-time lossless compression with high resolution images. As a result of parallel processing, the processing speed is increased and the system works at an upgraded capacity compared to previous versions. The image processing becomes highly convenient to implement. With its powerful processing ability and the remarkable capacities of ADV212, the proposed architecture can perform successfully image and video encoding or decoding of JPEG-2000 standard, requiring only minimal adjustments in the FPGA.

A new innovative hardware architecture of JPEG-LS in FPGA based on low complexity lossless compression for the image compression method is presented in [109]. This recent design combines a significantly lower complexity with significantly higher data, all through an advanced prediction pattern, by interrupting the feedback loop of context coefficients in the process of update. The design can reach a processing speed of up to 75MP/s while generating a lower compression ratio compared to the standard JPEG-LS compression. The parallel processing means that the system does not waste any clock cycles during the encoding route. The system is able thus to achieve full pipelined processing. This architecture is

perfectly optimized to support a good performance/cost tradeoff. The performance analysis suggests that it is possible to achieve satisfying results with a low complexity design and proper compression efficiency. This hardware implementation could be also utilized in the high-speed compression of remote sensing images on board a satellite.

A new parallel lossless image compression engine (PICE) has been developed in [110]. The new algorithm is built on context update and Golomb coding and is meant to improve high performance embedded systems. It functions by achieving n-way parallelism by a column-wise tiling. It starts by taking n parallel codeword streams and adds them to a corresponding multiplexer tree which is also added to a buffer for fixed-length output. Mostly, PICE has been modified to surpass the JPEG-LS in the area of memory and processing efficiency. The JPEG-LS algorithm combines low complexity with high performance, being thus suitable for integration in embedded systems. Various tests prove that the proposed architecture provides compression performance very similar to the original JPEG-LS algorithm. However, PICE requires 25% less resources for each single EPU than the JPEG-LS when it comes to hardware implementation. PICE performs online memoryless compression which means it does not require memory bandwitdth, using thus less hardware resources and avoiding any implementation difficulties.

The availability of real-time imagery is crucial especially in military operations. One of the most essential problems in image compression operations is the struggle between large amounts of image data and low memory bandwidth of tactical data link. A new efficient real-time transmission and image compression scheme [116] is introduced. The new method for CCSDS image compression is perfectly suitable for hardware integration since it has lower complexity and improved parallel architecture, able to provide great recomposed image quality while working at a great coding speed. The experimental tests suggest that the new method provides an increased feasibility and precision. Since the peak signal-to noise ratio is higher than 35dB and the processing time is decreased, the method fulfills the requirements for real-time compression. The conclusion is that the new scheme can satisfy the need for handling a high-quality flow of data and low bit-stream image in the real-time compression

of data link. The scheme can be thus utilized in target recognition, damage assessment, or threat identification.

A new innovative and precise eye tracking method [8] is proposed. The method includes an embedded system attached to a CCD sensor inserted in glasses. An image compression algorithm has been developed along with the eye tracking method. The algorithm is capable of combining power consumption optimization with reasonable cost. The purpose behind it is to be able of transmitting high resolution images while maintaining an accurate definition of the pupil edge to help in the post-processing pupil localization. Several experimental tests have been conducted to check and compare the performance of different processors and FPGAs and to show that FPGAS facilitate the achievement of the goals using less power. The tests showed that the system of algorithm and architecture is capable of reaching all its purposes, and that the FPGA consumes less power than any dedicated microcontroller in data flow operations. The next step will be implementing a full Iris localization algorithm on the same architecture.

2.2.2. Low-power Design of Image Compression

The High Efficiency Video Coding (HEVC) standard is a newly designed video compressor. To evaluate its performance, the Joint Collaborative Team [102] has conducted a verification test, comparing HEVC with its most recent predecessor, the Advanced Video Coding (AVC). The results of the test have shown that the HEVC standard distinguishes itself significantly from the AVC, being able to work at only half of the bit rate, while providing the same subjective quality.

The development of a low-power HEVC standard requires a detailed analysis of characteristics such as power consumption, temperature, or computational complexity. The study in [92] demonstrated the next-generation HEVC that maintains the right balance between power efficiency and quality of output brings many challenges in terms of architectural techniques. The presented low-power HEVC system is able to surpass these challenges through an interplay of software and hardware optimization, which makes it highly efficient in power saving.

The research in [89] partially studied motion compensation that refers to the process of using blocks of pixels from a Reference Picture in the formation of the newly processed image. The complexity of its function makes motion compensation difficult to implement in hardware. However, the presented motion compensation architecture is able to overcome several hardware implementation challenges by integrating key elements like a 2D reference pixel data caching scheme, a pixel interpolation engine, and a DMA engine.

Energy consumption is an important aspect in the development of limited and embedded devices that process images. After running several experiments, the study in [85] has discovered that image encoding and decoding algorithms consume different levels of energy. The study concluded that JPEG compression is the most energy efficient algorithm. Portable devices that use JPEG instead of PNG for image rendering and compression may increase by more than half the duration of their batteries.

A new low-power and high-speed Discrete Cosine Transform (DCT) for image compression is proposed in [49]. The DCT has been designed for implementation on FPGAs. The DCT optimization requires less computations and less material complexity, which makes it highly power-efficient. While the power consumption is reduced, the techniques based on Canonical Signed Digit encoding and Common Subexpression Elimination allow the compression to be performed at high operating frequency.

Rizzo *et al.* [87] presented Lossless coding of AVIRIS data, which can be performed by two new methods. The two algorithms for hyperspectral image compression are low-complexity, yet outperform any other existent technique. The first algorithm is based on a linear predictor, while the second one is based on a least-squares optimized linear predictor. The algorithms have been designed to perform on limited hardware and low-power, which makes them perfectly suitable for spacecraft on-board implementation.

The performance of a video compression algorithm is dependent upon the implementation on power-efficient systems. The implementation of an H. 264/AVC encoder, the latest standard for video compression, on an Analog Devices Blackfin processor is presented in [60]. After running several optimization techniques and verification tests to check improvement

and overall performance, it has been demonstrated that the low-power Blackfin processor is a great choice for next-generation embedded multimedia applications.

Designing VSLI for mobile devices [106] involves two main requirements, which are area minimization and power optimization. To fix these issues, the 8-point Discrete Cosine Transform, or DCT, can now benefit from a new efficient approximation algorithm. The new 8×8 transformation matrix does not require multiplication or bit shift operations because it is composed of 0s and 1s which only need adders. With a requirement for only 16 additions, the processing complexity is decreased largely, with a minor degradation in PSNR. The results suggest that the presented algorithm has a superior efficiency to any other current approximation methods in use. The algorithm can reduce power consumption with 25.39% and optimize the area with 15.43%, in comparison to BAS-2009 and BAS-2011 versions. The algorithm also reduces the operating frequency.

A new method of motion vector estimation is introduced in [52], firstly for MVE built around the implementation of a CMOS image sensor and secondly, MVE based on chip integration. A CMOS image sensor employs two different sensing modes:

(1) Normal, destructive video rate image sensing mode.

(2) Non-destructive high speed interpolated image sensing mode.

A new algorithm for iterative block matching has been thus developed [52]. The algorithm facilitates the estimation of the video-rate (30 frames/s) MVs with precision by using MVs taken from high-speed interpolated images. The algorithm is capable of significantly reducing the complexity of the computation in comparison with the other conventional full search block matching schemes. At the same time, it enables low power design for video encoders.

Recently, there has been an increase in applications in the field of a wireless video sensor and in the field of medical care where most applications are ultra-low-power [96]. Most of these new applications require extensive research because of the challenges they present. For example, these applications need to capture large amounts of data and do complex processing in real time. At the same time, hardware implementation must meet the criteria for little physical space and low-power consumption. Therefore, a new adaptive scheme is

proposed. Based on boundary adaptation processing, the scheme [96] is able to work on low-power consumption, implemented in a digital CMOS image sensor. Experimental tests on 0.35 μm CMOS technology are favorable, with promising compression rate, PSNR, and minimal power use.

The research in [50] proposes a user-friendly scheme and FPGA hardware architecture for low-power wireless sensor of camera networks for image compression. The FPGA circuit is necessary for taking the task of image compression from the main microcontroller in the camera sensor node. Moreover, the FPGA can facilitate high speed processing while maintaining low power consumption. The presented hardware solution includes two different schemes:

(1) The number of DCT parameters that have to be processed, quantized, and encoded in each block of image is decreased by a fast zonal DCT algorithm.

(2) The dynamic adjustment between energy consumption and image degradation becomes possible because the compression settings can be changed during run-time.

Several experimental tests run through the FPGA platform prove that the image compression scheme is highly efficient.

A new low power image compression algorithm for endoscopic application is proposed in [77]. The algorithm is based on simple integer-based DCT with efficient sub-sampling. The algorithm exploits the properties of endoscopic images, converted from RGB and captured in the YCgCo plane and it is meant to be integrated in the wireless capsule endoscope system that the YCgCo utilizes. By sub-sampling non-important color compounds from the color plane to improve the compression ratio, the algorithm can still achieve a high image quality for the reconstructed image. An analysis through experimental tests has shown that the new scheme is effective for both narrow band images (NBI) and wide band images (WBI), while requiring low cost implementation. Thus, the scheme can be the desired solution able to fix the problems of power and cost that conflict in WCE applications. The use of the proposed algorithm can result in a better battery life.

Two new schemes of architecture for image and video compression based on bi-

dimensional Discrete Cosine Transform are presented in [3]. Considering the high level of accuracy and complexity that the 2-D DCT computation requires, the two schemes are built with the goal to optimize power consumption, accuracy, and speed. Integrated through Xilinx system generator on the Virtex5 platform, two systems have been tested on six different standard images. The systems divide the original image into blocks of 8×8 pixels which are then computed individually through 2-D DCT. The tests involved different word lengths and different levels of accuracy and showed that the systems are able to generate outstanding image quality. Moreover, the architecture operates at high speed while keeping a low power consumption. Comparing with the other similar architectures, the new proposed architectures provide significantly better performance in the area of output accuracy, energy consumption, and the cost of hardware resources.

Using image compression technologies for increasing the performance of low power devices is a concept similar to the typical concept of the image compression system. Most image compression technologies used for communication have high complexity and work with high power consumption. Following a systematic approach, a Vertically Differential Encoding (VDE) has been developed for a low-power LCD interface [80]. VDE works by cutting to half the clock frequency while avoiding image degradation. The probability of bit transient is reduced thus to a minimum. By integrating FPGA with the VDE, the new prototype architecture consumes 14-15% less power in LCD with a resolution of SXGA+ than any other known conventional method.

2.3. Secure Image Communication in Internet of Things IoT

The IoT introduces four essential components for application systems: sensors, computation, communications, and services [23]. These four components include large amounts of data which need ultra-large analysis before being able to provide context information and to extract the knowledge behind the simple signals. Developments in silicon technology have reduced significantly the costs of computation, making it possible to allocate computation on each node in the IoT, especially sensors and aggregators. Distributed computing for the IoT can reduce transmission bandwidth and take on the overload of computations from the cloud

servers. It is also highly beneficial for ultra-big data analysis in a video sensing network. A new adaptable smart-camera stream processor is presented [23]. Combining a system-on-a-chip solution for distributed smart cameras with a coarse-grained reconfigurable image stream processing design, a subword-level parallelism, and heterogeneous stream processing, the new architecture proved in several tests that it can provide power efficiency.

A new and improved hardware design of the HEVC slim model for intra prediction is presented in [98]. The new design can be implemented through the use of HDL (hardware description language). The design eliminates techniques such as TSM or RQT used in HM and omits some blocks. At the same time, the design simplifies other techniques such as RMD or RDO, and simplifies some blocks as well. The simplification reduces the compression performance, but it facilitates the hardware integration of a real-time encoder. In the IoT, a real-time encoder can be a great asset because of its small size and high speed. The intra prediction design has been analyzed through a series of tests run via FPGA. The results show that the presented architecture can achieve reasonable throughput for encoding the target images. At the moment Full-HD (1920×1080) is the encoding target. In the future, the remains of HEVC hardware block (inter prediction, de-blocking filter) will be further tested.

2.3.1. IoT Image Communication in a Smart City

A new smart city service application based on Augmented Reality (AR) will be developed [83] for the public transportation in Novi Sad, Serbia. The presented application is able to function as a highly effective method for citizens to access information regarding bus arrival and departure times, bus routes, and typical touristic landmarks, all through AR technology integrated on a smartphone. AR information is gathered by the use of image and geo-location markers set throughout the city, which are able to transmit the data further using the IoT secure infrastructure. Using bus-mounted IoT devices able to access secure CoAp software for communicating the data to the corresponding cloud servers, the application can handle large amounts of data between users. The research on the application included an emphasis on security concerns that need to be addressed before the system is

in use. Future developments will include the possibility to purchase tickets for all modes of transportation from the city, or payments for bicycles rental. Moreover, the application will make it possible to calculate routes according to the mode of transportation.

In the smart traffic surveillance domain, the authors in [66] have considered the effectiveness of an embedded smart front-end camera for implementing complex algorithms. The camera could reach approximately seventeen frames in one second. The proposed system has taken into account major issues faced in traffic networks like the need to reduce system bandwidth for video streaming. It is unique due to its feature of recording the unanticipated traffic events autonomously. The essence of the research in [34] lies within the proposed Scale Adaptive Object Tracking (SAOT) algorithm used for real-time trailing of the traffic from a motionless camera. The model initially allows decentralization of the vehicles and then scales their inferences and projections. It also offers data connection for ongoing correlation of past and new information coming in continuously resolving the drift issues.

The research in [18] offers a prototype for a new smart camera that can be used for smart surveillance of traffic. The camera was based on a CMOS sensor, digital signal routing and a complex system CPU. The uniqueness of the approach lies in its ability to detect motionless vehicles mechanically. Further, by using the proposed model, jamming cargo traffic in real time could become possible. Wafi *et al.* [107] investigated the camera-video-surveillance abilities that could be used for distinguishing moving vehicles in diverse and variable street settings. The authors have considered functional encoding of OpenCV by integrating several operating systems to assess the outcomes, mainly GNU Linux. The study in [54] proposed an original approach in the form of camera capable of transmitting and receiving ways in multitude of dimensions when used along with a pan-tilt-zoom (PTZ). Due to the distinct ability, it would be easier for the tracker to follow irregular activities. The attributes of omni cameras identified included coarse categorization, refined classifications and generation of long-term statistics.

2.3.2. IoT Image Communication in Telemedicine

Ultrasound imaging is already extensively used to determine preliminary diagnosis. However, the ultrasound imaging diagnosis is very time-consuming and demands intensive training for sonographers [58]. An automatic detection system that can detect abnormality in kidneys through the ultrasound imaging can present incredible advantages. Therefore, a new fully-automated kidney malfunction detection system has been developed [58]. The system is built on wavelet based noise removal, supervised classification, and automated feature selection. Several experimental tests reached the conclusion that the designed classifier is capable of validating the malfunction without errors. Having such information available, the sonographers can recommend immediate precaution while also monitoring the advancement of the disease. For the first tests, kidney images have been classified as normal or abnormal. Medical conditions such as cysts, kidney stones, or bacterial infections are classified as abnormal, and any deviation from the standard is observed. A Support Vector Machine (SVM) implemented on FPGA and verification with large amounts of data will be researched further.

Another research in ultrasound imaging is proposed in [2]. Ultrasound imaging generates echo signals with a high dynamic range of 12 bits which cannot be visualized on CRT or LCD monitors that are present in the ultrasound machine. Log compression is required to compress the data from 12 bits to 8 bits. However, log compression is non-linear which means it does not allow tracking of all the original features of the signal. Several global and local compression methods have been analyzed to find a suitable replacement for log compression that can retrieve the dynamic range when the physician finds access to better monitors, and that can ensure minimal errors in the reconstructed image [2]. The results of studies suggested that Gamma compression provides promising image quality in comparison to other tested techniques, but it is not capable of retrieving statistical properties which doctors need for analysis. Therefore, the best compression method for IoT ultrasound remote diagnosis systems is wavelet based compression.

A home based Telehealth system, CogSense, has been developed [4]. Through a

combination of imaging, sensing, and human-computer communications technologies able to diagnose, treat, and monitor patients without interfering on their life quality, the new device system offers remarkable services in medical care. CogSense operates at great speed and involves low cost data analysis, being thus able to bring efficient services to home Tele-Health users. Through the IoT network, CogSense is capable of connecting patients, doctors, hospitals, and caretakers, creating a collaborative environment which lowers the need for computational limitations. Another important aspect in the development of CogSense is maintaining a low cost in development and production by using COTS products. The system will also offer the possibility for users to receive feedback on their medical condition or questions, through the analytics engine that will engage a wide network of health care providers.

CHAPTER 3

SECURE DIGITAL CAMERA IN THE IOT ERA

Acceptable size with highest quality of the image has been the demand of the rapidly increasing number of multimedia applications. Undoubtedly, with the IoT becoming reality, it is necessary to improve the information management and transmission scheme. This is due to the fact that IoT involves interaction of huge numbers of small objects and this increases the amount of data produced in the system by an exponential level. The situation is even more worsen by the fact that IoT involves a variety of devices and for variety of applications which produce a vast variety of datasets. In order to handle these large datasets, compression plays a key rule in IoT where the data needs to be compressed by an order of magnitude while keeping the signal distortion within the acceptable bound. So, the aspect of reducing the computational complexity in IoT is very important for power and speed contained devices. This chapter proposes frameworks for secure digital camera in the IoT. The objectives of this chapter are twofold. On the one hand, the proposed framework architecture offers double-layer of protection: encryption and watermarking that will address all issues related to security, privacy , and digital rights management (DRM). On the other hand, the chapter introduces a new hardware architecture of Better Portable Graphics (BPG) Compression, which is integrated with SDC. Thus, the proposed framework of SBPG integrated with SDC address all issues related to security, privacy and provides acceptable size with highest quality of the image. The proposed framework is suitable for high performance imaging in the IoT, such as Intelligent Traffic Surveillance (ITS) and Telemedicine, which are illustrated in this chapter. The demonstration of the proposed framework with experimental results follows a top-down approach. First in this chapter, the block diagram and the overview architecture of secure digital camera in the IoT is discussed. In Chapter 4, the hardware architecture of BPG is presented. The high-performance of secure BPG integrated with SDC is proposed in Chapter 5. In Chapter 6, the energy-efficient design of SBPG is presented.

3.1. Secure Digital Camera SDC

Secure Digital Camera (SDC) is a novel approach in capturing digital images. A comparative analysis of Secure Digital Camera with Digital Camera can provide a better understanding. A simple digital camera can capture images in digital format, store them and maintain the visual records of events. But to track the source, check the authenticity and possession of custody for these digital images is not possible in this camera. The authenticity of the image cannot be proven completely even with digital image watermarking techniques. Images captured with a digital camera are also susceptible to data loss. A scope for eavesdropping on the multimedia file is also available with the DC. On the other hand, a Secure Digital Camera by the help of its unique components, is able to track the identity of the original photographer, corroborate image veracity and maintain detailed records of the chain of custody to the point of time, day, year and other significant information [71]. Figure 3.1 shows an architectural overview of the SDC. It is a digital camera but with significant capabilities like encryption and digital image watermarking for the protection of the images that it captures. It consists of an Analog-to-digital converter, compression unit, liquid crystal display, encryption unit, active pixel sensor unit and watermarking unit. The entire sequence of events is controlled by the controller unit. Compression module, encryption module and watermarking module are working together in SoC architecture of secure digital camera. It is evident from the above discussion that the Secure Digital Camera is arguably one of the best proven appliance of capturing multimedia. Security and privacy concerns are eliminated by using SDC. This is a device that has all the standard features of a DC along with additional features like working in real-time consuming low-power and available at low cost [69].

3.2. Proposed SDC Integrated with Secure BPG Compression

A novel concept of a Secure Better Portable Graphics (SBPG) with built-in encryption and watermarking facility is presented in this chapter. BPG compression is very suitable for real time and bandwidth application due to its low size and high quality of image which are the drawbacks of JPEG compression. Secure BPG is integrated into the Secure Digital

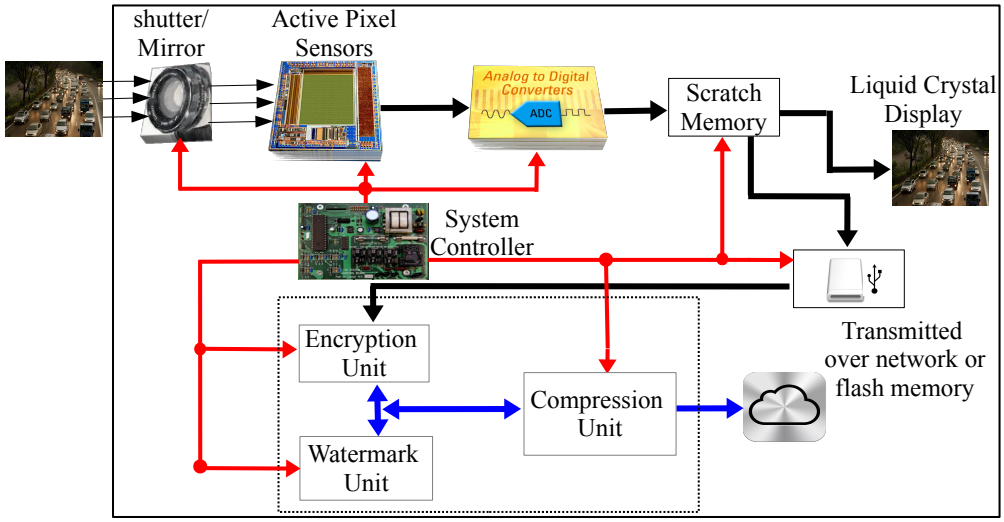


FIGURE 3.1. System-level Block Diagram of the SDC. After [69]

Camera and is typically designed as System On Chip (SoC). SDC addresses many Data Rights Management related tasks like extent of tampering, facilitating content authentication, ownership rights and tracking usage using double layer of protections, encryption and watermarking. In this chapter, IoT in highway surveillance system is introduced for which SDC is arguably the best way to manage real-time rights and considered to be suitable.

The outline stages of the SBPG integrated with SDC are represented in Fig. 3.3. We argue that starting with watermarking and encryption process then preforming the BPG compression is more secure than starting with the compression process because information is again changed during the compression process. If we do the opposite, the original data in a host image is changed by the compression process before applying the watermarking, which means the watermark is altered since it is based on changed information of the host image.

3.3. Framework Overview of Secure Image Communication in IoT

Recently, the IoT has drown much attention in both industrial and academic settings. It is very rapidly turning out to be an important part of any business due to an exponential increase in the volume of data traffic transferred across the network. Hence, security becomes extremely important while transferring this information across the Internet. Users

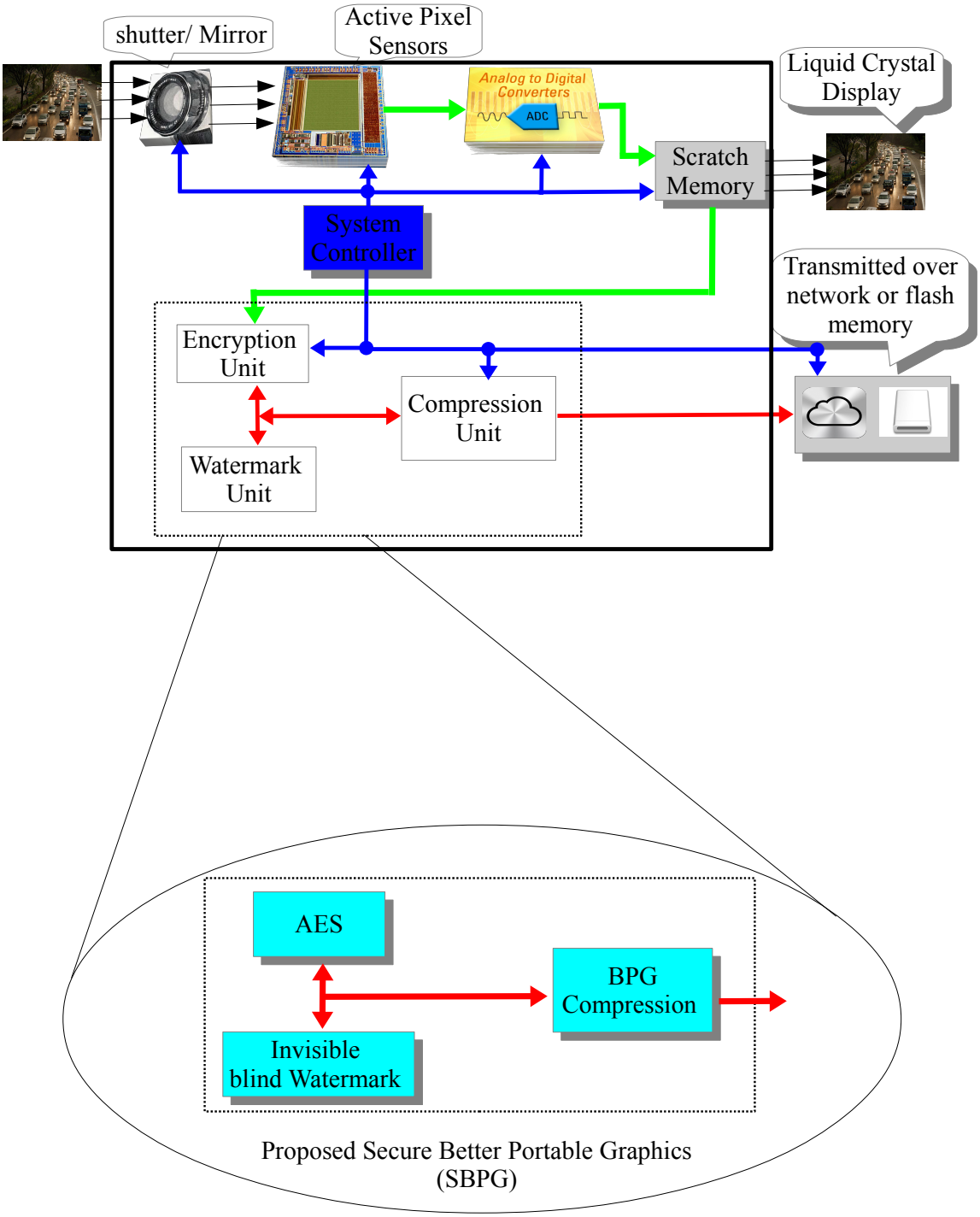


FIGURE 3.2. Block Diagram of Secure BPG.

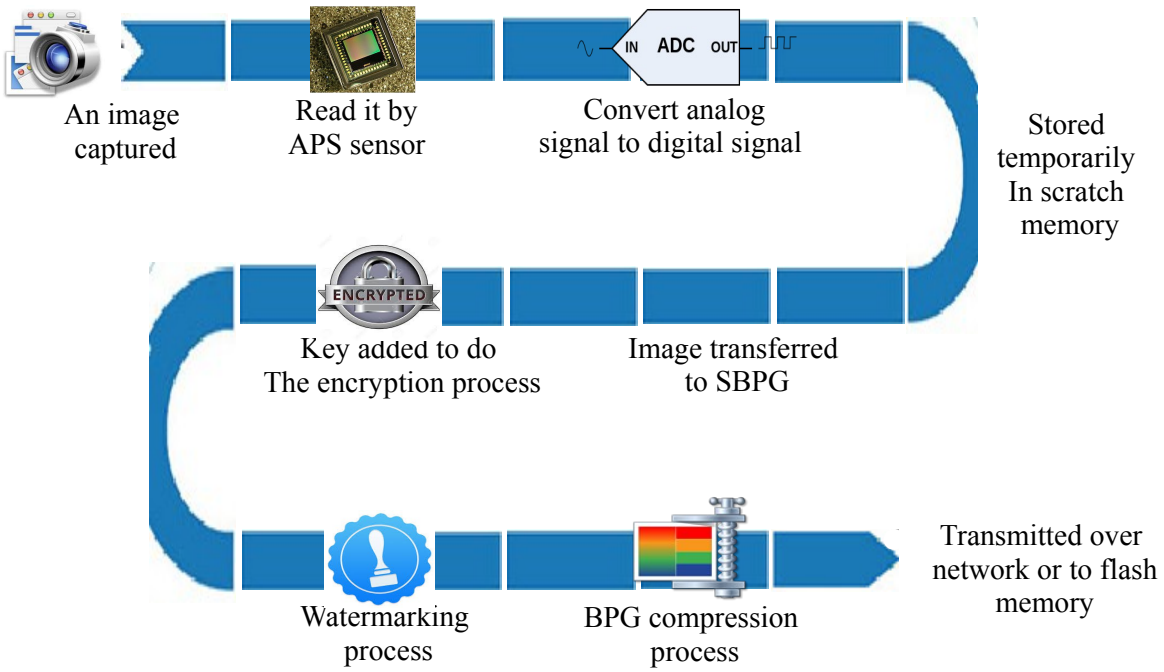


FIGURE 3.3. Outline stages of the SBPG Integrated with SDC.

information can be in any form like images, audios, and videos. Here security implies that the data are only accessible or delivered to the Intended person, while unintended users have no access to it. In the case of information being an image, there have been many schemes already proposed to secure these images like encryption, image hiding, visual cryptography, and watermarking [12].

Since the amount of traffic involved in the IoT is exponentially huge, there is a need to make the security algorithm as simple as possible. This needs the ability to be implemented across various devices with varying capability. Let us consider an image signal. An image signal is very important for multimedia services. Hence, it has a wide range of values to take from. When the images are used in different systems, some of these images may have out-of-range color [97]. It has thus to be mapped to in-range colors. This type of situation can occur very often, hence there is a need of image code to compare the image data efficiently so that the devices can access it. For this purpose, HEVC has been developed with several

new coding techniques so as to give high coding performance. However, these new technique have significantly increased the computational complexity. For example, the intra prediction in HEVC requires very high computation [98].

There are several application domains of IoT based on the type of networking, availability, and user involvement and impact. This can be broadly categorized into mainly application domains [39]:

(1) Personal and home: a scale of an individual or home

(2) Enterprise: a larger scale like communities.

(3) Utilities: a national or regional scale.

(4) Mobile: spread across other domains.

Overall, security and privacy are important concerns in image communication in the IoT. From the above discussions, it is evident that compression technique potentially aims to reduce the image's size with acceptable quality, which is also an important aspect in any image communication system.

3.3.1. Intelligent Traffic Surveillance ITS

In the past few decades, there has been an exponential increase in automobile traffic, leading to heavy congestion. This rate of increment in traffic has surpassed the road capacity, hence it has become necessary for better traffic management strategy. Since transportation is the backbone of any economic department and any kind of disruption has severe impact on the economy, there is a need of smart transportation. Smart transportation refers to intelligent systems in the transportation domain [61]. It can be enhanced to a new level by incorporating IoT technique with it. For this, it is necessary to collect and analyze numerous data, as IoT for transportation combines wireless communication, distributed system, data mining, and machine learning techniques. The key idea is to create a variety of objects like cameras, sensors, embedded systems, which surround the environment and are able to interact each other to cooperate with each other which aims to accomplish certain task and improve the outcomes and performance. Recently, the Intelligent Transportation System

has evolved as an effective solution to improve transportation safety and mobility. ITS is composed of different types of technology based systems which are divided into intelligent infrastructure Systems and intelligent vehicle system [9].

The IoT is an evolutionary step in the world of technology. Home and mobile devices, or embedded applications connect to the Internet and extract information by using analytics. At any moment, the number of devices connected to the Internet is in the range of billions. Moreover, as time goes by, more and more devices will connect, until hundreds of billions of devices will be online. Devices from the same class also connect with each other, forming an intelligent network of systems. Making these systems of systems to communicate with each other, and share or analyze data through the cloud, can transform our relationship with technology forever. The new technology can add improvements in many important fields and can contribute significantly to our lives. It can develop medical outcomes, optimize energy consumption, or offer advanced products with low development. Thus, IoT is an elastic technology that raises high expectations regarding its potential network capabilities, but which raises, at the same time, security concerns that threaten its future capabilities. Some of these security concerns are connected to the common attacks conducted upon networked environments, such as Replay or Man in the middle attack [28]. Without a good protection system that could address these security issues and reduce the risks to a minimum, the technology is compromised. It is mandatory to ensure efficient protection for IoT data processing, as well for high-source heterogeneous data, by keeping them private through hiding methods. For example, digital cameras are able, with the help of a proper positioning strategy, to ensure maximum coverage of the area which is under surveillance. While the data of interest might be connected with the anti-malicious protection, the rest of the bits and details cannot be excluded, or isolated.

In this chapter, an intelligent traffic surveillance system is proposed that uses the SDC device integrated with SBPG through IoT. Basically, the role of this smart traffic camera would be to monitor roads and keep track of all possible issues such as accidents, congestion, or severe weather conditions. The system communicates the status of the road to a main

gateway which analyzes data from all cameras. This way, a large chain of communications forms, and this wide chain leads to the creation of an intelligent traffic system which can cover a whole city. Moreover, more cities can connect their traffic systems and make them communicate to form an even wider and more intelligent system of systems. The possibilities to use such a system are endless. Analyzing data from one end of the system to understand its impact on the other end of the system could be done effortlessly. For example, an accident on the highway can be detected by the smart camera which will send the information to the city wide transportation system, where the information will be analyzed and the impact of the accident will be calculated, to understand how it will influence traffic on other segments of the road. If the accident takes place near an airport or near a school, then the systems could communicate to each other to adjust flights or change school schedules. The systems could also notify drivers through the city digital sign systems about alternative routes and give them instructions on how to avoid the accident. While this is just a simple example, the introduction of the IoT in ITS could bring countless advantages and benefits. Figure 3.4 illustrates the components of Intelligent Traffic Surveillance in IoT; also, figure 3.5 shows one scenario of the potential benefit of introducing the IoT in ITS system.

3.3.2. Telemedicine

Medical imaging is evolving in the direction of digital data acquisition. There are several technologies such as magnetic resonance imaging able to generate digital images directly. Moreover, there are digital X-ray systems used in chest or breast imaging. The traditional X-ray films can easily be converted into digital images by using film digitizers. Digital format is highly valuable and convenient because it allows image compression, transfer, and archival. Digital images also present the opportunity for manipulation and enhancement of medical information, especially concerning diagnostics [62]. Digital medical imaging systems such as X-ray, Ultrasound, MRI, and CT are already widely in use, but their extensive use leads to some major challenges in terms of storage and transmission. The medical information datasets are constantly growing, which requires an increase in both storage space and transmission bandwidth. In this situation, the development of efficient image compres-

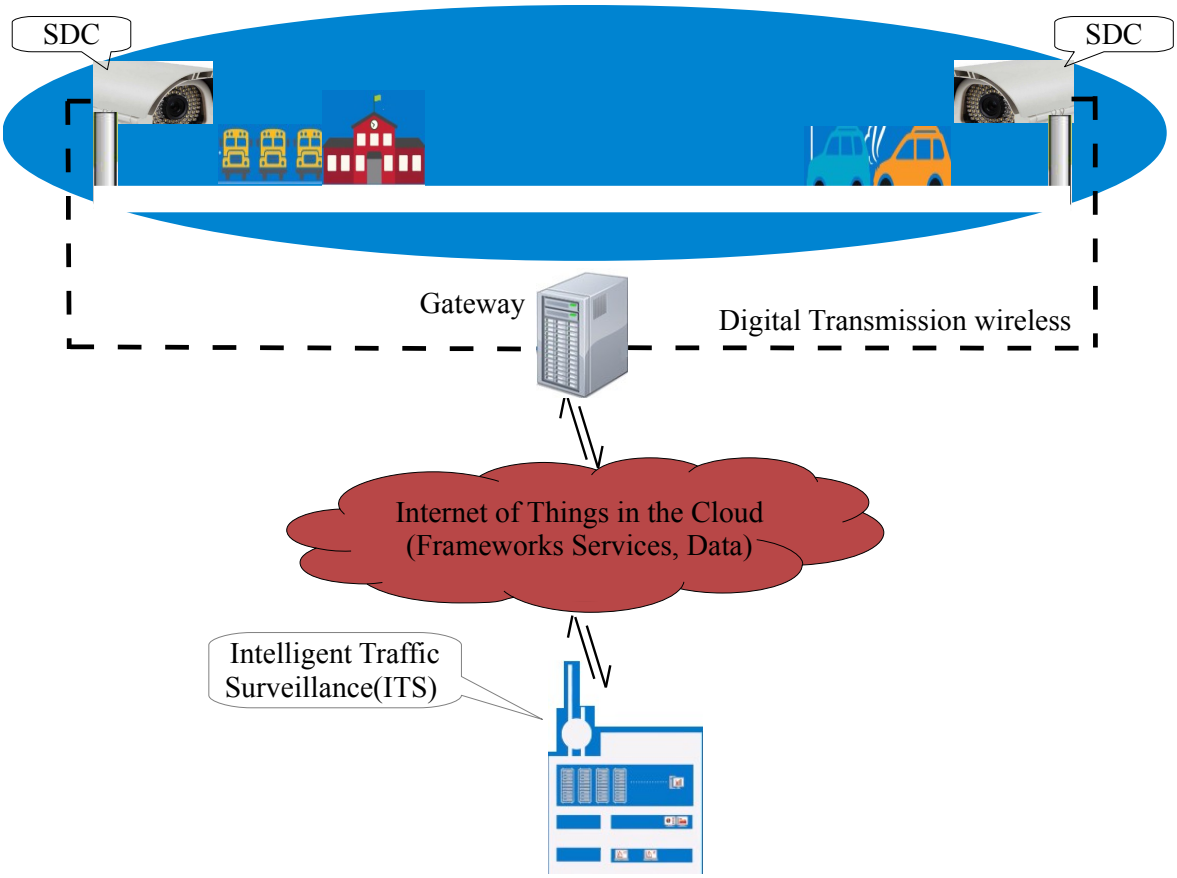


FIGURE 3.4. Components of Intelligent Traffic Surveillance in IoT.

sion techniques is essential, because it can simplify the storage and transmission of all digital medical data between patients, doctors, and hospitals. Image compression can easily achieve a reduction in storage requirements, together with fast and reliable transmission [65].

Digital medical images require special compression methods because the area that is relevant for diagnosis occupies a very small part in the full capture. Besides the patients clinical reports and diagnosis, health care records contain other types of information, such as video streams or image scans. Most image scans come from research work and practical studies within medical science and its professionals. The quality of health care services is dictated by the qualifications of the doctors and all the health personnel. Specialists find it difficult to stay updated on their field because of large amounts of information, studies, and developments in the medical fields. It is thus imperative that important medical data

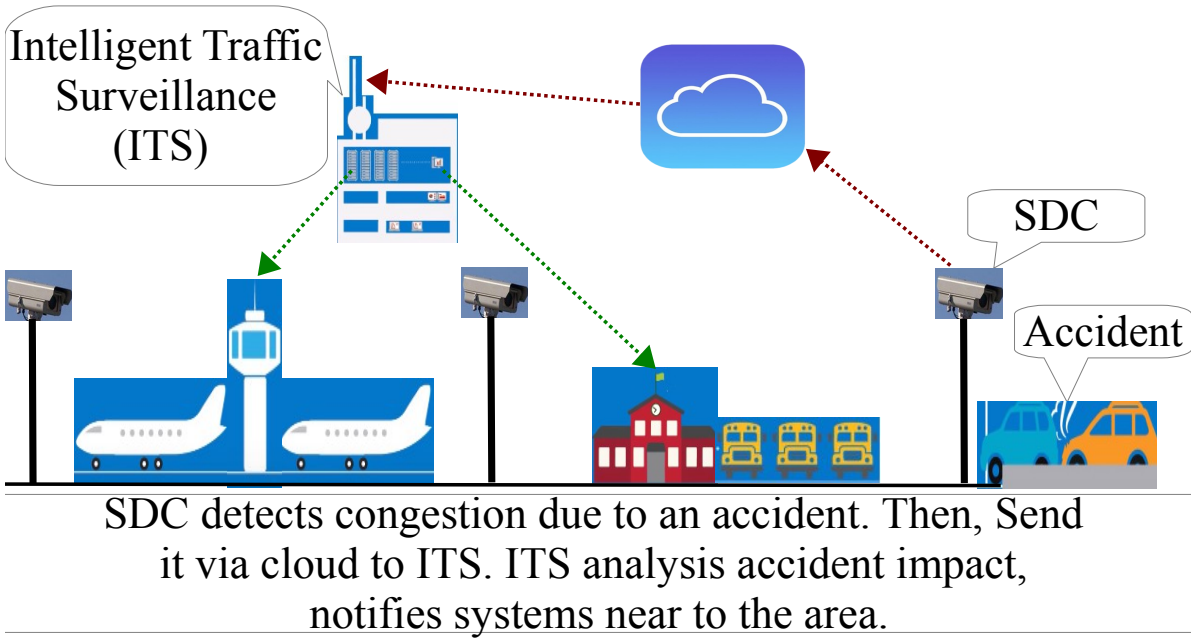


FIGURE 3.5. Scenario of the Potential Benefit of Introducing the IoT in ITS system.

reaches key medical specialists. In this case, the medical data should be easy to transmit and share with key professionals who know how to interpret it. Figure 3.6 illustrates the potential benefit of telemedicine in the IoT.

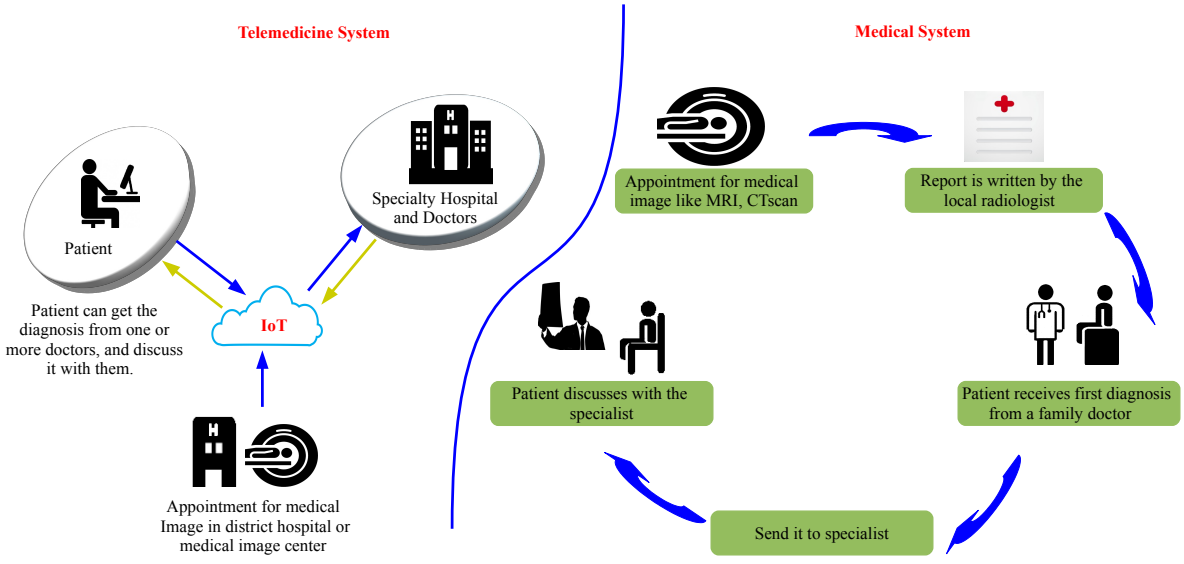


FIGURE 3.6. The Potential Benefit of Introducing Telemedicine in the IoT.

The broadest definition of telemedicine describes it as a transfer of digital medical

data, including patient records, images of high resolution, sounds, or live video, by using a wide range of technologies able to deliver and improve health care services. By being able to access a variety of off-site datasets, to ease the communication between clinics, doctors, and central hospitals, and to transmit medical data between different locations, these technologies can change the entire world of health care. Currently, telemedicine is employed in several main medical fields such as telesurgery, teleradiology, telepathology, and also medical education. The vital criterion that determines how successful telemedicine services are is ensuring that medical data is accessible by external parties in a timely manner. Moreover, medical information must be protected efficiently with high degree security systems that will not allow the information to leak into the outside world. The security systems must ensure protection of confidential data, but most importantly an efficient security method must not allow the infiltration of malware or mischievous parties that could enter, undermine the order of the system and make it unreliable [59].

3.3.2.1. Telemedicine in the IoT

Estimations conducted by the World Health Organization [82] suggest the population of the world is in a fast stage of aging. Together with aging, there is a corresponding growth of health problems which the current health care systems have difficulties in handling. The aging of the population is a phenomenon that affects the entire world. Not only that proportion of elders has become more significant in the total population, but the trend that has led to this situation will become more powerful in the future. While aging is one of the main elements that brings a pressing need for the development of new health care technologies, there are also many other factors which suggest that adopting the Internet of Things in health care might significantly simplify health care services. Large proportions of the active population do not consider health monitoring a priority. Constantly distracted by a career, social activities, and hobbies, most people only go to a doctor when the symptoms of a health condition become very prominent. When their diagnostic is settled, their diseases are usually already developed or in the final stages, which makes treatment very challenging and expensive. To change this unfortunate situation, it is highly important to keep regular track

of a persons health state and to raise awareness about the importance of a healthy lifestyle. Even though in developed countries there are well-established governmental programs that promote healthy habits, including health monitoring, a visit to a doctor is still the most popular way of keeping track of a persons health. However, his method of providing diagnostics is expensive and raises many concerns, because the medical records of a patient can only offer fragmented information, usually referring to short periods of time [11].

To increase the effectiveness of diagnosis and treatment, there is a pressing need for continuous health monitoring, which could allow tracking of essential health parameters. This situation has led to the need for developing a new health care system, eHealth, which has been given a thorough description in [35].

3.3.2.2. Importance of Compression Techniques in Telemedicine

Both the relevance and the usage of digitized medical information are growing constantly, bringing new technological challenges with regards to the storage and the transmission of huge amounts of data. These challenges can be overcome using compression techniques. Medical data includes large amounts of images that require a different compression method than raw binary data. While current compression methods can be used for images as well, they provide unsatisfactory results. Images require a compression method able to sacrifice unnecessary details from the image to decrease the requirements for storage space or bandwidth. In this case, lossy compression methods are very effective. Applications for medical image compression must be able to preserve any relevant image information that might be necessary in establishing the diagnosis, which can be done through lossless compression methods. While lossy compression methods provide efficiency for storage and transmission, they do not guarantee that vital information will not be lost during the processing. Lossy compression ensures that all the characteristics of an image will be saved in the parameters of the domain space where the image is processed [17].

All compression methods are either lossless, or lossy:

- Lossless compression techniques encode images by preserving their full quality and characteristics, meaning that the image can be reproduced accordingly, without

changing the intensity of pixels.

- Lossy compression techniques offer a high compression ratio while sacrificing from quality by determining a slight deterioration of the reconstructed image.

Lossless compression methods are popular for applications where data loss leads to unreliability and where incorrect prediction is useless, for example in the compression of medical images or satellite images. Lossy compression methods are valuable in situations where a minor loss of data does not represent an inconvenience, for example, in handling photographic images [65].

3.3.2.3. Importance of security in Telemedicine

Telemonitoring includes handling large amounts of personal private information which must be provided with reliable security mechanisms and strategies. In a network where everything is connected, the need for confidentiality, privacy, and authenticity increases significantly. The security requirements for adequate protection must include resistance against attacks, the possibility for data authentication and access control, and also client privacy. A system that is resilient to attacks can easily adjust itself in case of node failures and can also identify and avoid any point of failure. Access control on the data provided by information sources must include access control and data authentication so every retrieved address can be identified. It is also vital the client privacy is protected with powerful measures that can ensure the information provided will not leak out of the system.

Any digital data such as images, videos, audio sequence, or texts can have an integrated identification code, known as a watermark or digital signature. The watermark is necessary for identifying the owner or the document and for impeding unauthorized distribution or copying which goes against copyrights.

CHAPTER 4

BPG FOR DIGITAL CAMERA

A hardware architecture for newly introduced Better Portable Graphics (BPG) Compression is proposed in this chapter [5]. Since its introduction in 1987, the Joint Photographic Experts Group (JPEG) graphics format has been the *de facto* choice for image compression. But JPEG is outperformed by the new compression technique, BPG in terms of the size of compressed file and compression quality of the image. The image enhanced compression in real-time is implemented in hardware, which is the main objective of this chapter. The complexity introduced by the software compression in BPG encoder library can be reduced using hardware compression wherever possible to match the real-time requirements and possibly low latency embedded systems. BPG compression [16] is based on the High Efficiency Video Coding (HEVC), which is considered a major advance in compression techniques. In this chapter, only image compression is considered. MATLAB®/Simulink® is used to design the prototype of the proposed architecture. The higher and improved visual quality of BPG compression than that of the JPEG compression with equal or reduced file size can be observed from the experimental results. To the best of the authors' knowledge, this is the first ever proposed hardware architecture for BPG compression.

The main objective of this chapter is to describe a hardware architecture of the BPG compression encoder. To the best of the author's knowledge, this is the first ever proposed hardware architecture of BPG compression encoder. On a subset of complete BPG specifications, hardware compression is used to reduce the complexity of the BPG encoder library and is presented in this chapter. The novel contributions of this research include the following:

- The first-ever architecture for hardware BPG compression.
- Prototype implementation of the algorithm based on Simulink®.
- Experimental comparison and analysis of JPEG versus the proposed architecture.

Advantages of hardware implementation over the software implementation include the fol-

lowing:

- Minimal hardware is used to encode the real-time image.
- Power usage is reduced significantly compared to a general purpose processor.
- The host is not slowed down by the dedicated circuitry.
- Hardware implementation is not affected by malicious software such as worms, Trojans etc.

4.1. A Simplified BPG Compression Algorithm

Acceptable size with highest quality of the image has been the demand of the rapidly increasing number of multimedia applications. BPG compression [16] is a novel step in the field of image compression that aims to supersede the decades-old *de facto* JPEG format [108] with its unique attributes, meeting the requirements of modern display with higher quality of image at much lower sizes, developer and programmer requirements and graphic businesses. HEVC (High Efficiency Video Coding) [99] and compatibility considerations are accommodated in the form of a small JavaScript (56 KB) decoder which is a key composing elements of new format. New supplementary browser plugins are not required to display the image compressed by BPG unlike the JPEG. Some of the attributes which show the difference between the JPEG and BPG and make BPG an excellent choice are:

- Users need not be concerned with any legal issues because BPG compression is a patent-free, open source and royalty free algorithm which justifies it as a more appropriate choice for the users.
- BPG can offer lossless compression and is in close spirit to JPEG.
- BPG offers, with advanced quality features, different chroma formats, which makes it compatible with multiple video encoding schemes such as JPEG, digital and analog encoding schemes.
- Different chroma formats like YCgCo, RGB, Premultiplied Alpha, Non-premultiplied alpha and YCbCr are supported.
- A range of meta data which includes XMP, ICC profile and EXIF is used by BPG

for efficient conversion.

- Using Java, cross platform support can be achieved.

Similar quality of image like JPEG can be achieved by using BPG with higher compression ratio and smaller size. Chroma formats, animation, various color spaces (YCbCr, YCqCo, grayscale, RGB) and lossless compression is supported in BPG format. The reference BPG image library and utilities (libbpg) can be divided into four functions: Javascript decoder, BPG decoder, BPG encoder and BPG decoding. JPEG or PNG images are given to the BPG encoder as inputs and the encoder provides the corresponding BPG image as the output. The decoder takes the BPG image as input and gives the JPEG or PNG image as the output. BPG is supported by most web browsers with a small Javascript decoder. This BPG decoder allows most of the applications to decode and get the original image from BPG compressed image. The BPG encoder is based on HEVC encoding [99]. H.264 is primarily replaced by the HEVC due to its efficiency of compression [53]. Reduction of bitrate compared to the H.264/AVC is the main aim of the HEVC project because it is more parallel friendly [22][93].

Image compression, when used in a proper way, can make a significant difference in terms of quality of the image and its size so as to meet modern display requirements (high quality images at lower sizes) of programmers, developers and graphic businesses. BPG is considered as the newest technique in image compression. BPG depends on HEVC, which is considered as top line (latest) standard of video compression. Better Portable Graphics is substantially an I-frame of HEVC unlike the other compression technique, JPEG. Efficiency of I-frame encoding is increased by using the HEVC. Each block is encoded separately in JPEG. But in HEVC, the differences between the blocks are encoded rather than deal with the full block information that can be done by reducing the redundancy between different block in the HEVC I-frames. BPG image encoder compression is the main focus in the proposed architecture. The BPG encoder is based on the HEVC encoding [99]. Compression efficiency [53] is the main advantage of HEVC which makes it a replacement to H.264 encoders. Initial steps of BPG encoder algorithm are shown in Figure 4.1. From the figure,

it is clear that at some point, the input of the encoder is checked whether it is a static image or a video (dynamic image). If the image is static, the algorithm proceeds to image encoder as shown in figure 4.3; or it will proceed to a video encoder as illustrated in figure 4.2.

After the image is read, an initialization processes is performed by the encoder to read color space, meta data and bit depth etc., Two conditions are checked by the algorithm: color space and bit depth which is an essential step. Bit (color) depth refers to the amount of data that can be used to indicate the color of each pixel [71]. Different numbers are used to represent it, 8, 10, 12, $\cdots$. It describes the number of bits used to represent colors per pixel. Data storage is the main concern for the images that are having high bit depth which in turn require high transmission bandwidths. Besides this, all the colors are not reproduced by some of the displays. Undoubtedly, there must be a tradeoff between quality and bit depth. Strictly, images with a bot depth of 8 is considered by the BPG compression encoder.

4.2. Proposed Hardware Architecture for the BPG Encoder

This section presents the hardware architecture of Better Portable Graphics encoder compression. Figure 4.4 shows the two phases into which the BPG encoding can be divided into : HEVC encoding phase and the pre-encoding (initialization) phase. In general, compression can be classified into two categories, lossless and lossy. When original data can be recovered without any errors, it is called lossless compression. But in the case of lossy compression, an approximation of the original data can only be recovered. Both lossy and lossless are available through BPG.

4.2.1. Initialization Phase

Images can have different pixel depth, color spaces, and alpha channel. Many initializations should be completed before performing the compression encoding. Image details are obtained in the first step: alpha, color space, pixel depth and meta data. Images with grayscale or true color and bit depth of 8 are required for the BPG compression encoder algorithm. If these essential requirements are not met, the encoder will give out an error message indicating that the color space or bit depth are not supported. The initialization

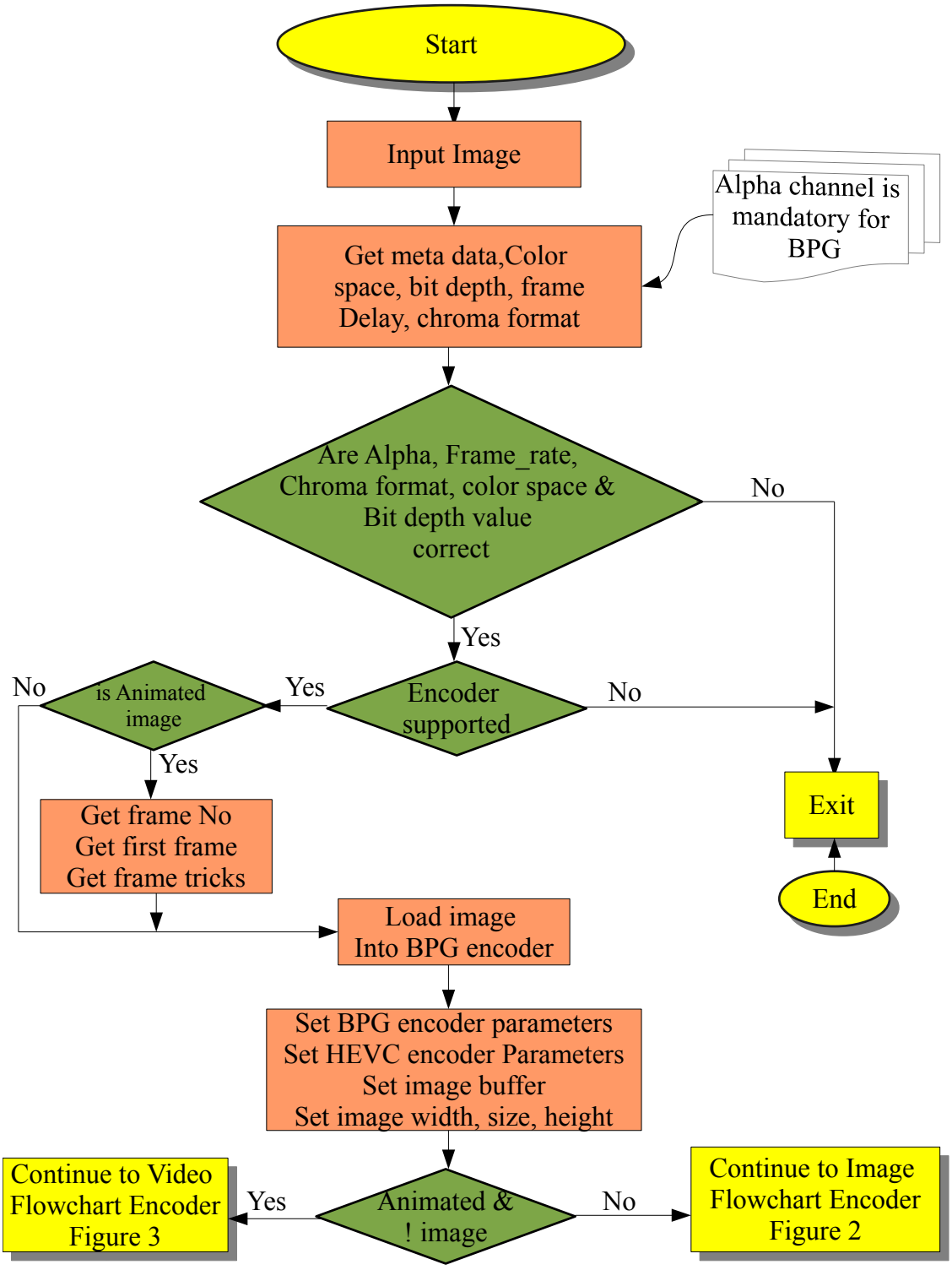


FIGURE 4.1. BPG Encoder Algorithm.

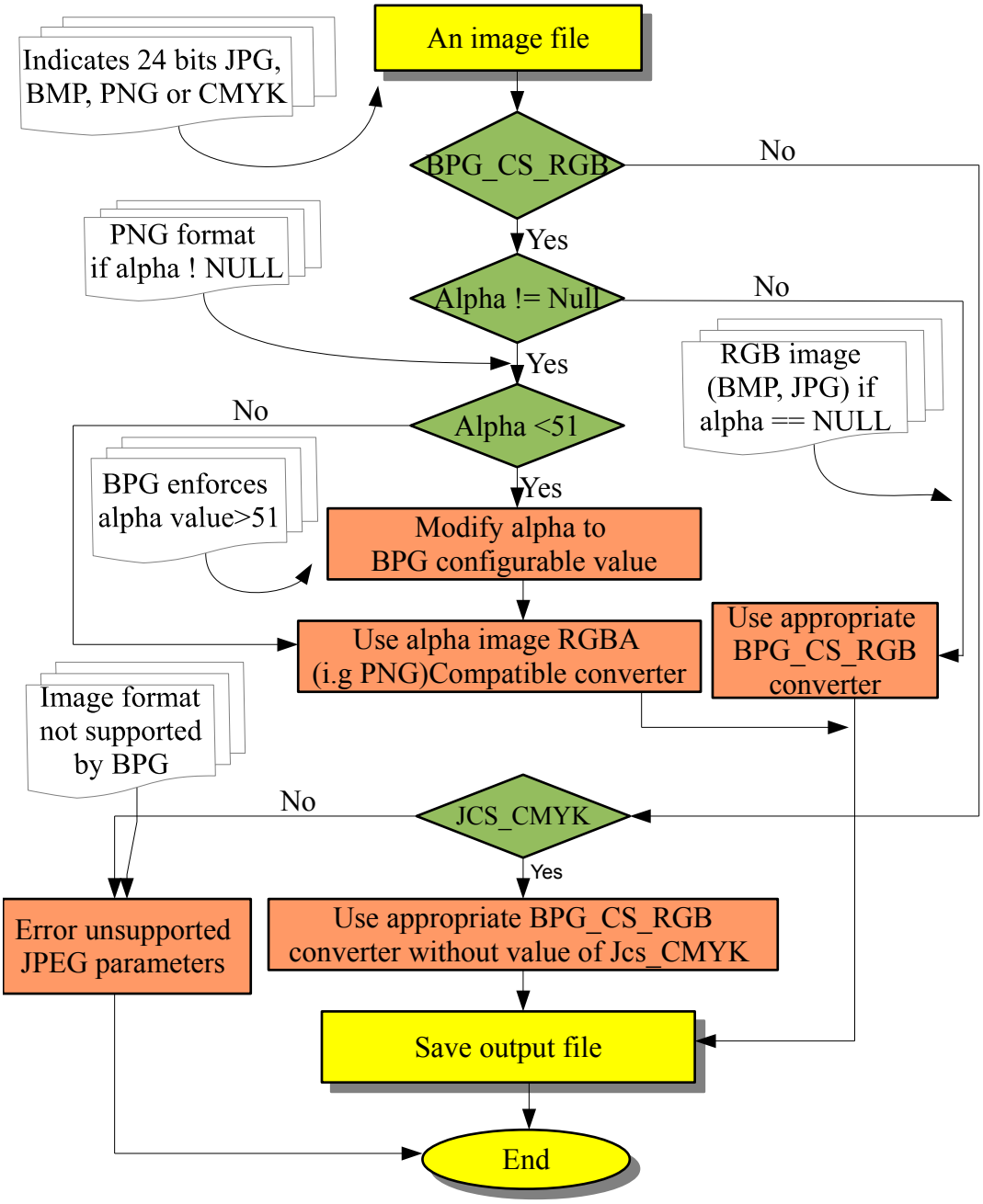


FIGURE 4.2. BPG Image Encoder Algorithm.

phase steps are illustrated in Algorithm 1.

4.2.2. HEVC Encoder Phase

BPG encoding is based on the HEVC encoder, which is considered a major advance in compression techniques. HEVC uses an intelligent approach where the encoded area

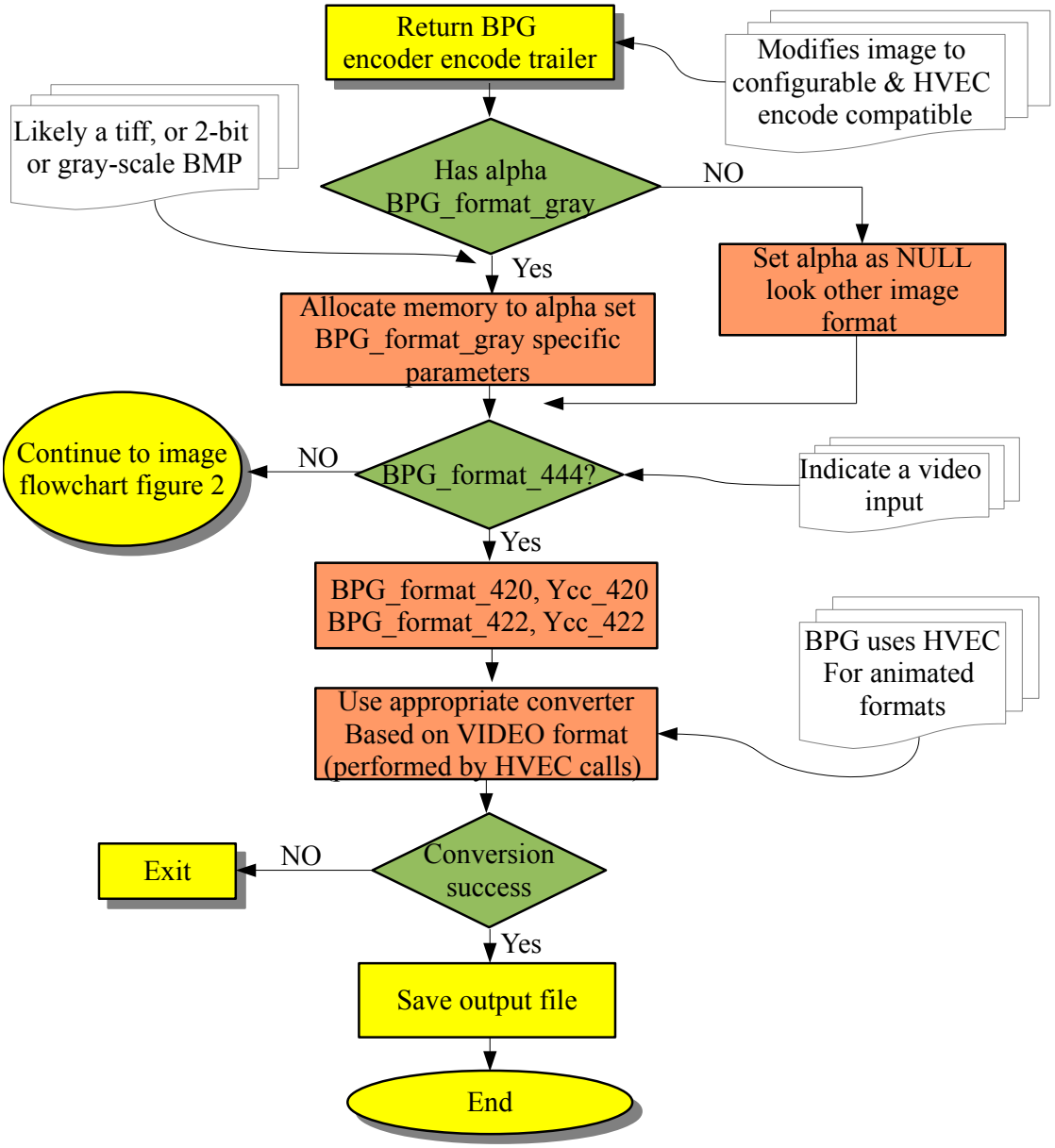


FIGURE 4.3. BPG Video Encoder Algorithm.

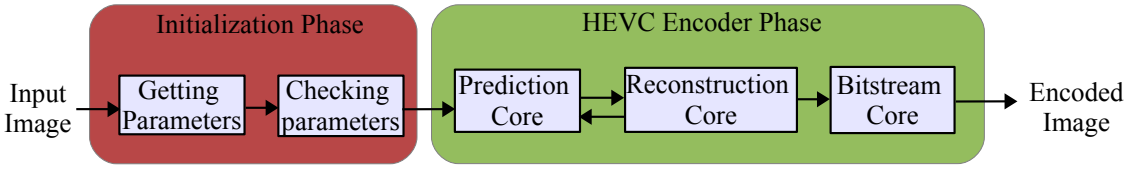


FIGURE 4.4. BPG Encoder Block Diagram.

Algorithm 1 BPG Encoder Algorithm.

input $imageX$
get $Parameters \leftarrow \{PixelDpth, ColorSpace, Alpha\}$
calculate $Resolution \leftarrow \{pixels/inch\}$
calculate $ColorType \leftarrow \{TrueColor, GrayScale\}$
if $Length > 2$ **then**
    $Bitdepth \leftarrow \{MateData/numChannel\}$
    if $Bitdepth \neq 8$ **then**
        $AlphaChannel \leftarrow \emptyset$
        print "ERROR: while opening bitdepth encoder"
else
if $Bitdepth \neq 8$ **then**
    $AlphaChannel \leftarrow \emptyset$
    print "ERROR: while opening bitdepth encoder"
if $ColorType < 1$ **then**
    print "ERROR: Color space is not supported"
end
print "Bit Depth and color space is supported"
print "Image accepted for BPG compression"
if $AlphaChannel \neq Null$ **then**
    use appropriate BPG CS RGB converter
else
if $AlphaChannel < 51$ **then**
    modify alpha to BPG configurable
end
use alpha image RGBA compatible HEVC
save output file BPG image
end

(pixels) is reduced [112] and hence the efficiency of the encoding is high. The basic coding unit of the HEVC is an 8×8 block and Discrete Sine Transform (DST) or Discrete Cosine Transform (DCT) is used to transform into frequency domain. In HEVC context-adaptive binary arithmetic coding (CABAC) entropy is used which is much efficient compared to the JPEG where hauffman entropy coding is used [115]. In the HEVC encoder, the pictures are encoded into bitstreams. These bitstreams contain a sequence of data known as a Network Abstraction Layer (NAL). The encoder stores pictures in the Decoder Picture Buffer (DPB) as illustrated in figure 4.5. In HEVC, a single picture is divided into one or more slices where each slice contains one or more slice segment.

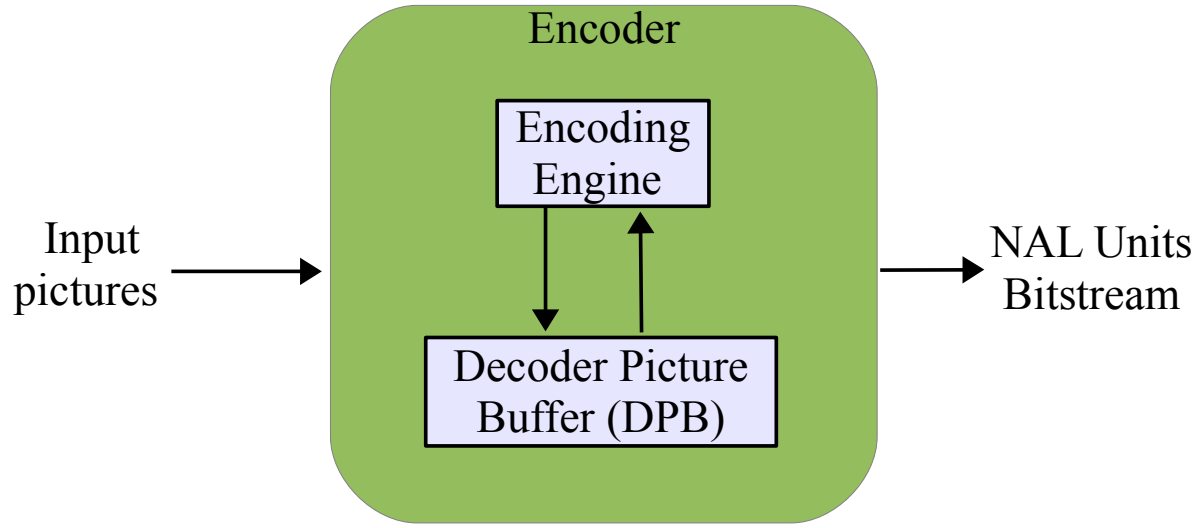


FIGURE 4.5. HEVC Encoding Block Diagram. After [101]

The encoding process in HEVC is divided into three stages: prediction, reconstruction, and bit-stream core. The essential stage is the prediction core where it handles the inter prediction and intra prediction in parallel. Then the reference frames are reconstructed by the reconstruction code at each time of encoded frame. CABAC is performed by the bitstream core. Following are the four core stages of the HEVC encoder:

- **Inter Prediction:** The main function of this block is to reduce the temporal redundancy. This can be achieved by comparing a current prediction unit with neighboring prediction units. Motion estimation is used for this comparison. In the

motion pictures, the Inter-picture is performed to make prediction in which motion vectors specify the movement of suggested image in the direction existing image. In order to perform Inter prediction on block basis, the suggested picture is chosen from the interpreted image buffer. According to prediction block and selected picture this indicates the displacement location.

- **Intra Prediction:** is the process of disconnecting the link surrounded by the regions of the picture, on the basis if prediction block process is carried out. In order to reduce the spatial redundancy, intra prediction is applied. To attain more efficiency while performing intra prediction, it is essential to get a signal from the intra prediction mode.
- **Transform and Quantization:** The next step after reducing the spatial redundancy and temporal redundancy is the transform. Size of transform can be 32×32, 16×16, 8×8 or 4×4. Here, two transforms, Discrete Sine Transform (DST) and Discrete Cosine Transform (DCT) are used to divide the work into categories according to cosine and sine functions. Sinusoidal transform is considered appropriate for decorrelation. After the transform in complete, the sample is transformed into entropy coding using the quantization. Quantization is the process that exemplifies signals to an assembly of denoted values; however, scalar quantization process involves the quantization of individual value.
- **Entropy Coding:** In entropy coding, the syntax elements are plotted into the bitstream. Syntax elements are the transformed quantized elements. These syntax elements also include motion vectors, intra prediction modes etc. However, according to the design criteria, there are different coding stages of entropy. There are two categories of syntax elements: Fixed length codes are applied when syntax elements identify eminent characteristics of bitstream is code by using symbolized value, while Variable length codes (VLCS) are known for coding information on the images. The elimination of the redundancy which is not removed in the prediction stage is the main objective.

Encoding of images of series of shots of videos are encoded into a bitstream is the responsibility of the encoder control as required by the function. It also makes sure that the encoding of video is according to the required videos coding specification. It also makes sure that the decoder buffer of receiving bittstream is runoff with the amount of bits. The decisions that encoder control takes depends on the division of code blocks and division of image.

4.3. Simulink® Implementation of the Proposed BPG Encoder Architecture

Figure 4.6 shows the system-level architecture of proposed BPG compressed encoder. HEVC encoder and initialization phase are shown in the dotted lines in the block. The initialization phase preprocesses the input image and obtains image details: bit depth, alpha, chroma format, and a code for color space. Postprocessing verifies color space and bit depth. After the image is received at the HEVC encoder, intra frame prediction, IDCT, DCT, splitting and quantization processes are performed.

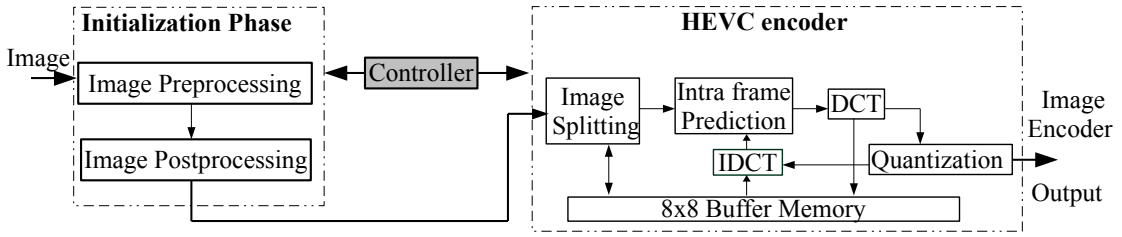


FIGURE 4.6. System Level Architecture of the Proposed Algorithm.

4.3.1. Simulink® Based Modeling

MATLAB® /Simulink® Version 8.3 (R2014a), was used to prototype the proposed algorithm with the Computer Vision System Toolbox Version 9.7 [72]. Figure 4.7 shows the HEVC encoder model. Bottom-up methodology is used to represent the high level system modeling. Initially the function units are built and then these units are integrated into sub-systems and finally, overall system functionality is tested and verified. Fast prototyping of the image processing functions and modules are facilitated by MATLAB® /Simulink® offers. The availability of DCT/IDCT, block processing and other functions is another main

advantage of MATLAB®/Simulink®. Different modules, DCT domain compression and color conversion are used in addition to accomplish the system-level modeling.

4.3.2. Validation of the BPG Encoder

Four standard test images were selected: IceClimb, Bear, Lena and Wallpaper with different frequency and spatial characteristics. The proposed BPG compression encoder encodes the test images. The major concern while evaluating the quality of the picture in the image compression systems is describing the amount and type of degradation in reconstructed and compressed images. It has been proven [78] that some measures of image quality correlate well for a given compression algorithm but they are not reliable for an evaluation across different algorithms. Thus, the most common measures of image quality were used in this work: Root Mean Squared Error (RMSE) [25] given in Eqn. 1 and Peak Signal to Noise Ratio (PSNR) [46] given in Eqn. 2:

$$(1) \qquad RMSE = \frac{1}{\sqrt{MN}} \sum_{j=1}^{m-1} \sum_{n=1}^{N} ||(I_O(i,j) - I_{O'}(i,j)||^2.$$

$$(2) \qquad PSNR = 10 \log \left(\frac{(2^n - 1)^2}{MSE} \right) = 10 \log \left(\frac{255^2}{MSE} \right).$$

The need of resulting values that do correlate well with human perception of quality justifies introduce additional quality assessments: Multi-scale MSSIM, Structural SIMilarity (SSIM) and Visual Information Fidelity (VIF). MSSIM and SSIM aim to measure the viewing condition and image resolution. Reference images are the uncompressed images which are then used to measure the similarity between the compressed images and reference images [111], given in Eqn. 3, and 4:

$$(3) \qquad SSIM(i,j) = L_{I,J}(i,j) C_{I,J}(i,j) S_{I,J}(i,j).$$

$$(4) \qquad MSSIM(i,j) = m_k(I,J)^{\alpha k} \prod_{k=1}^{K} v_k(I,J)^{\beta k} c_k(I,J)^{\gamma k}.$$

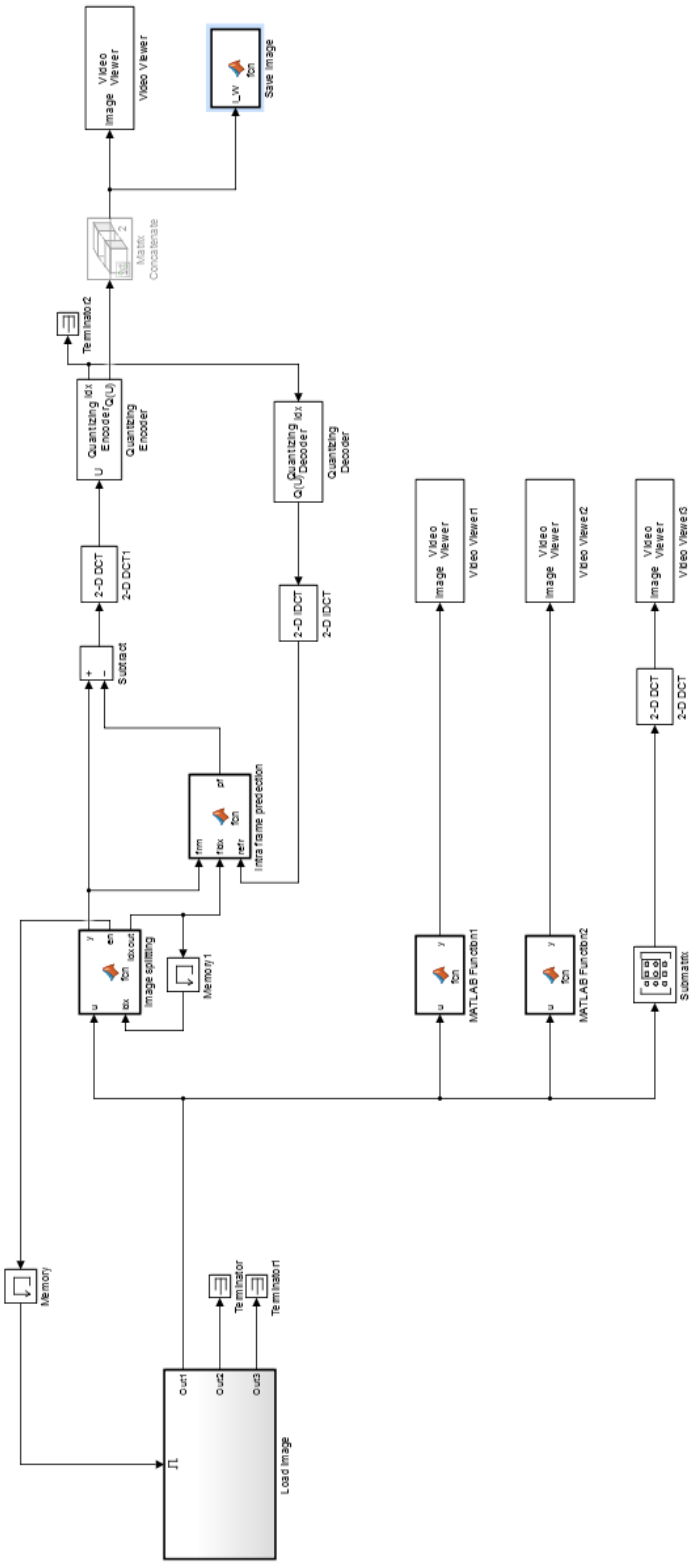


FIGURE 4.7. BPG Compression Encoder in Simulink®.

The mutual information between the compressed and reference images is utilized by the VIF to assess the quality [94], given in Eqn. 5. The image quality assessments used in this chapter are summarized in Table 4.1

$$VIF = \frac{\sum I(C^{N,j}; F^{N,j}|S^{N,j})}{\sum I(C^{N,j}; E^{F,j}|S^{N,j})}. \tag{5}$$

The test images and the corresponding BPG images format are shown in figure 4.8, figure 5.11, figure 5.12, and figure 6.5. Related metrics for each test image and compression technique is illustrated in Table 5.1. It can be observed that the size of the BPG image, for the same PSNR, is substantially reduced. According to experimental results, it can be inferred that better quality can be achieved using the hardware architecture confirming quality assessments, shown in table 5.1. Figures (12(a)), (12(b)), (12(c), 13(a)), (13(b)), (13(c)), 14(a)), (14(b)), (14(c)), 15(a)), (15(b)), and (15(c)) analyze and illustrate the related metrics for Bear, IceClimb, Lena, and Wallpaper image respectively.

Quality Metric	Remarks
RMSE	The average squared difference, pixel-by-pixel.
PSNR	Luminance Component.
SSIM	Correlates with human perception: luminance, contrast, and structure.
MSSIM	Variance and cross-correlation.
VIF	Mutual information.

TABLE 4.1. Quality Metrics used for the Compression Technique and Test Image

A hardware architecture for BPG compression encoder in images is presented in this chapter. There are two phases of encoding. In the first stage, the initialization stage, the image is read and details like color space, alpha and bit depth are extracted and verified. The second phase is HEVC encoding, which is considered a major advance in compression

(a) JPEG Image. (b) BPG Image

FIGURE 4.8. Compression of Bear Image (256×256).

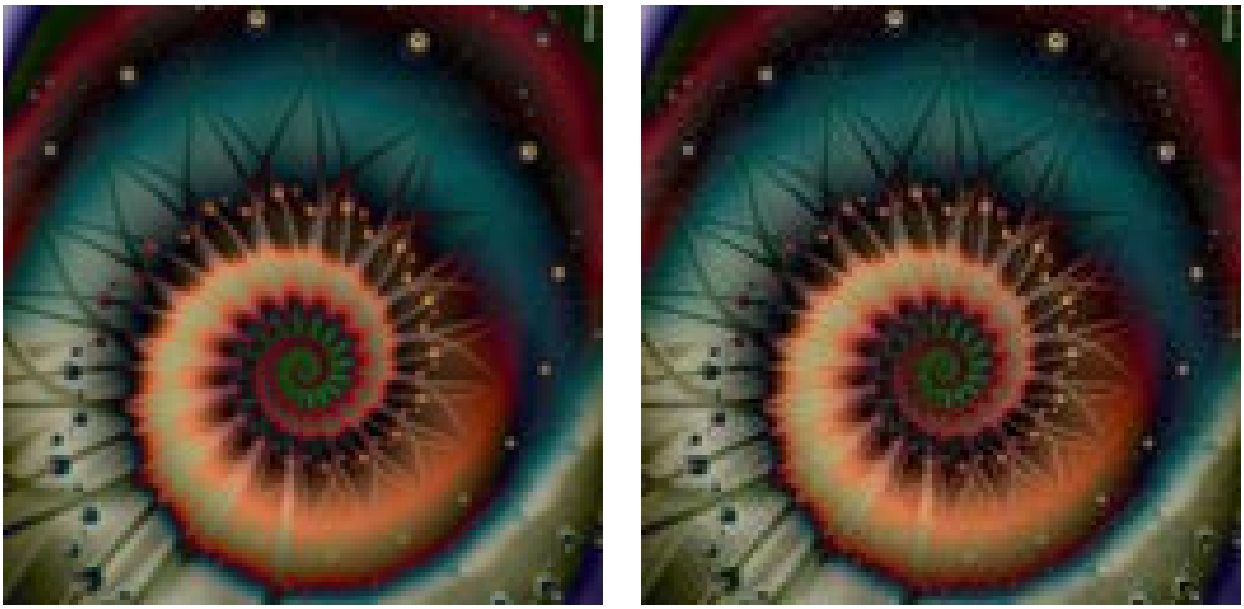
(a) JPEG Image. (b) BPG Image

FIGURE 4.9. Compression of IceClimb Image (512×512).

techniques. Simulink®is used to prototype the proposed architecture. JPEG techniques are compared with the existing experimental results in terms of size and quality and indicate

(a) JPEG Image. (b) BPG Image

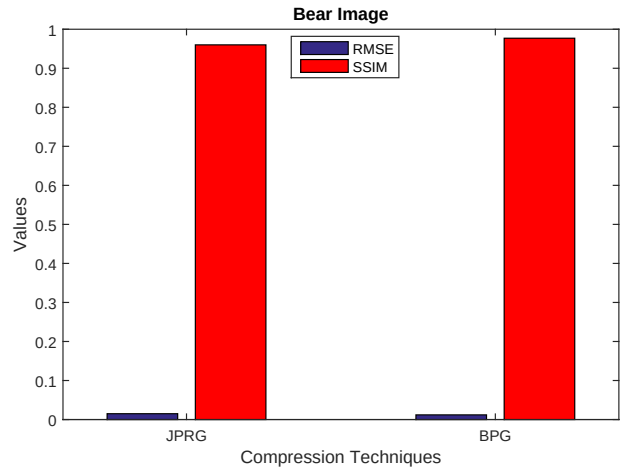
FIGURE 4.10. Compression of Lena Image (512×512).



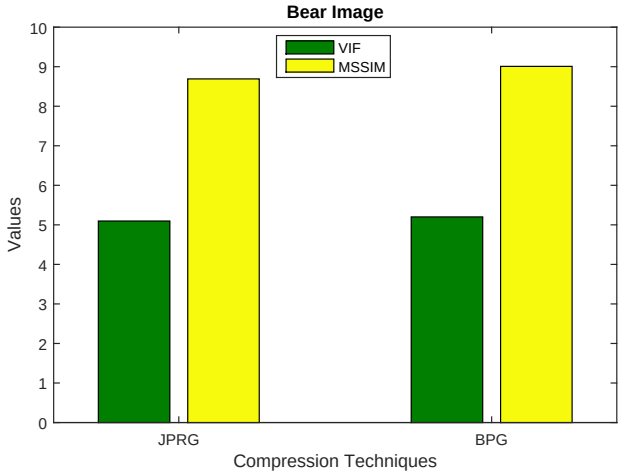
(a) JPEG Image. (b) BPG Image

FIGURE 4.11. Compression of Wallpaper Image (128×128).

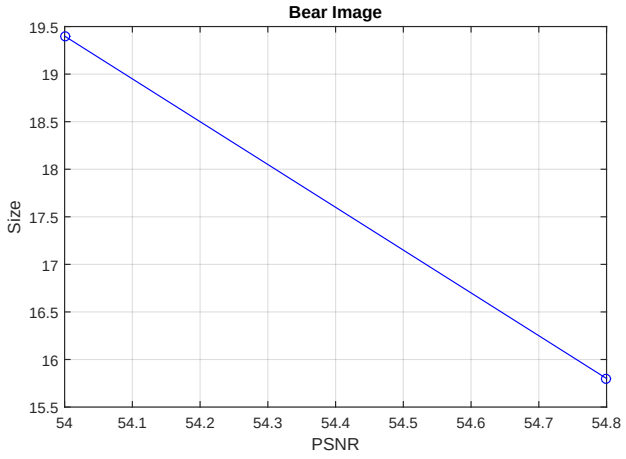
that the BPG compression has superior characteristics. The BPG architecture will be soon be integrated with encryption and or digital watermarking capabilities [72, 56].



(a) RMSE & SSIM

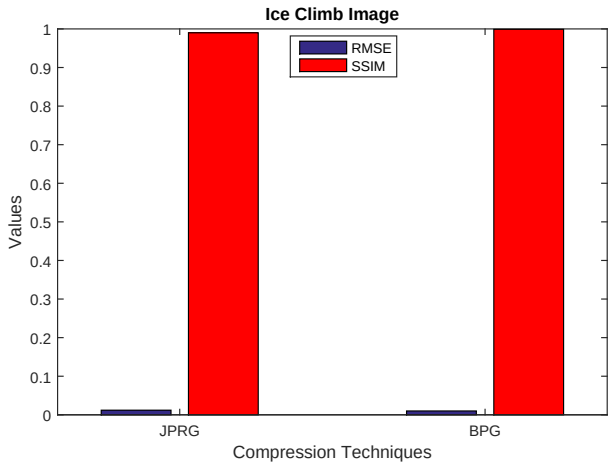


(b) VIF & MSSIM

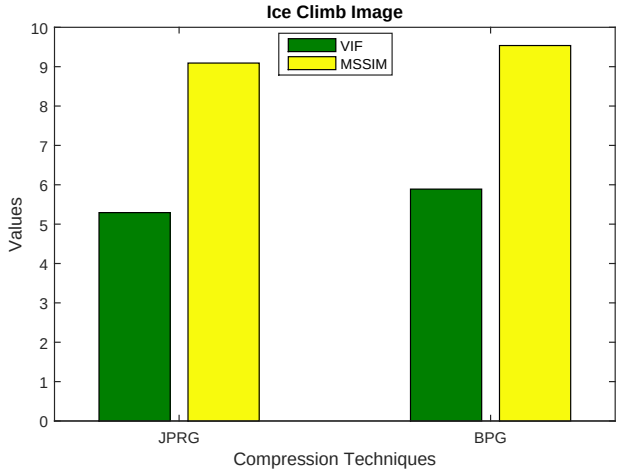


(c) Size versus PSNR

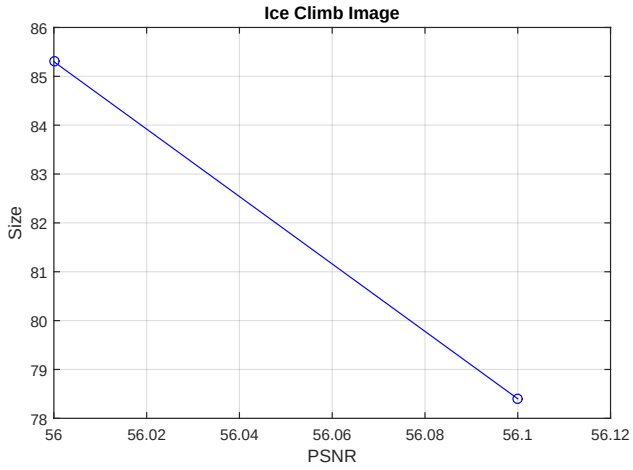
FIGURE 4.12. Bear Image



(a) RMSE & SSIM

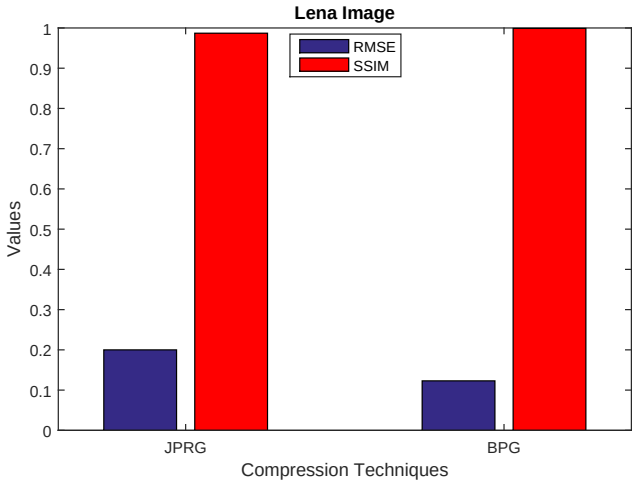


(b) VIF & MSSIM

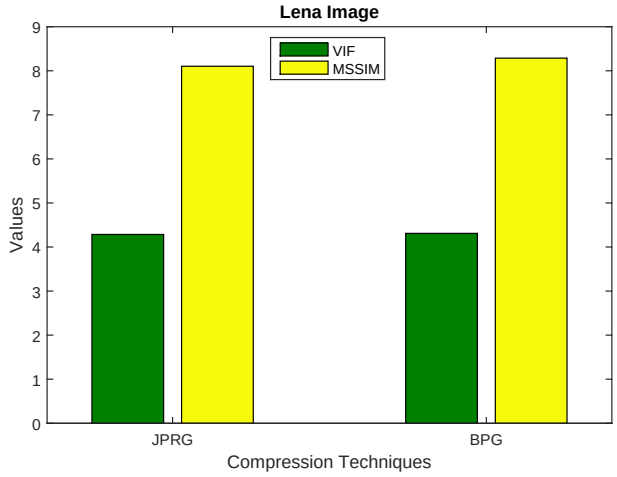


(c) Size versus PSNR

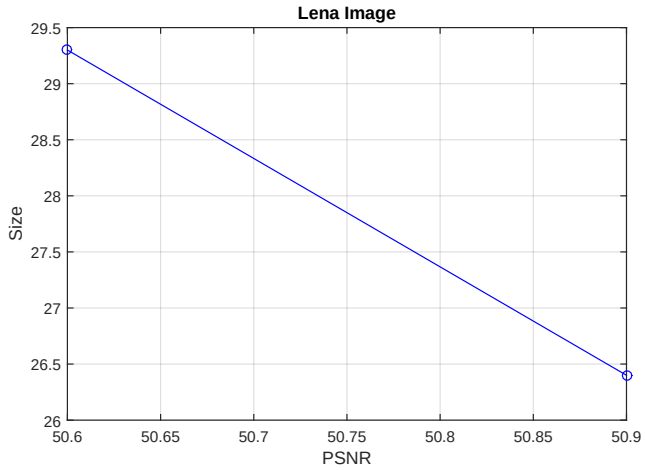
FIGURE 4.13. ICeClimb Image



(a) RMSE & SSIM

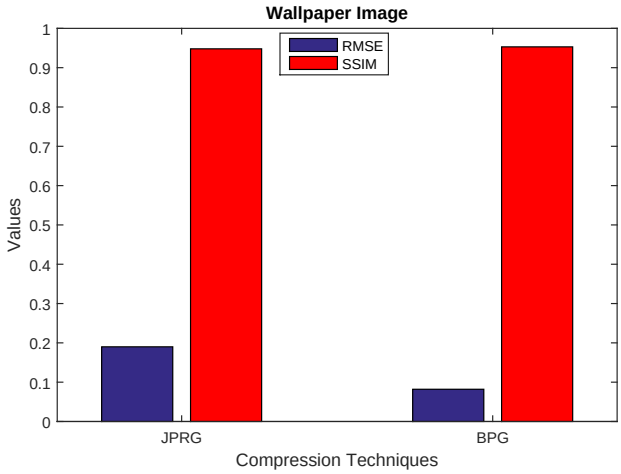


(b) VIF & MSSIM

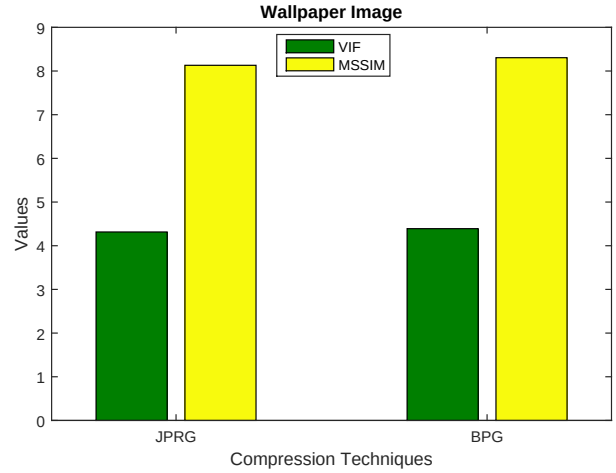


(c) Size versus PSNR

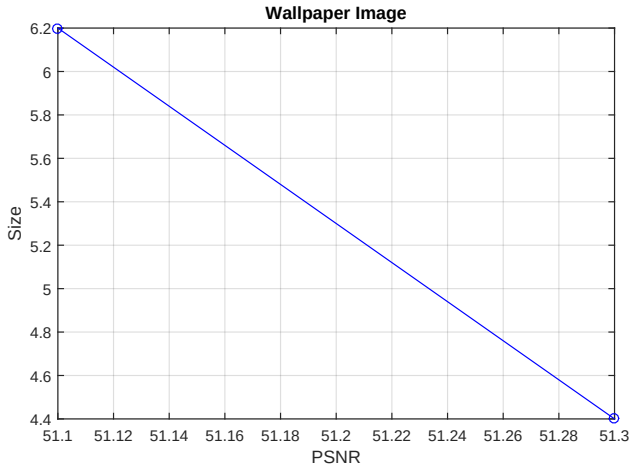
FIGURE 4.14. Lena Image



(a) RMSE & SSIM



(b) VIF & MSSIM



(c) Size versus PSNR

FIGURE 4.15. wallpaper Image

Test Image	Compression	Size (KB)	RMSE	SSIM	VIF	MSSIM	PSNR
Bear Image	JPEG (input image)	19.4	0.015	0.960	5.097	8.691	54.0
	BPG image	15.8	0.012	0.977	5.201	9.008	54.8
IceClimb Image	JPEG (input image)	85.3	0.012	0.990	5.293	9.092	56.0
	BPG image	78.4	0.010	0.999	5.890	9.537	56.1
Lena Image	JPEG (input image)	29.3	0.200	0.987	4.285	8.103	50.6
	BPG image	26.4	0.123	0.999	4.310	8.287	50.9
Wallpaper Image	JPEG (input image)	06.2	0.190	0.948	4.315	8.131	51.1
	BPG image	04.4	0.082	0.953	4.391	8.305	51.3

TABLE 4.2. Quality Metrics for the BPG Compression for Test Images.

CHAPTER 5

HIGH-PERFORMANCE DESIGN OF SECURE BPG FOR TRUSTED IMAGE COMMUNICATION IN THE IOT

This chapter proposes a prototyping development of a hardware architecture for Secure Digital Camera (SDC) integrated with Secure Better Portable Graphics (SBPG) compression algorithm. The proposed architecture is suitable for high performance imaging in the IoT [7]. The objectives of this chapter are twofold. On the one hand, the proposed SBPG architecture offers double-layer of protection: encryption and watermarking that will address all issues related to security, privacy , and digital rights management (DRM). On the other hand, the chapter proposes SDC integrated with secure BPG compression for real time intelligent traffic surveillance (ITS). The experimental results prove that the new compression technique BPG outperforms JPEG in terms of compression quality and size of the compression file. As the visual quality of the watermarked and compressed images improves with the larger value of PSNR, the results show that the proposed SBPG substantially increases the quality of the watermarked compressed images. To achieve a high performance architecture the author considers three techniques; first, using the center portion of the image to insert the encrypted signature. Second, watermarking is done in the frequency domain using block-wise DCT size 8×8. Third, in BPG encoder, the proposed architecture uses inter and intra prediction to reduce the temporal and spatial redundancy. All of the above techniques optimize the proposed architecture by decreasing the computing complexity , which lead to increase the speed of watermarking and compression process. The proposed architecture is prototyped in Simulink®. To the best of the author's knowledge, this is the first ever proposed hardware architecture for SBPG compression integrated with SDC.

The main objective of this chapter is to describe a hardware architecture of the secure better portable graphics (SBPG) compression encoder that is integrated with SDC. The proposed architecture meets modern technology requirements: high quality and smaller size because of using BPG compression. To the best of the author's knowledge, this is the

first ever proposed hardware architecture of SDC that is integrated with SBPG compression encoder. The novel contributions of this work include:

- The first-ever architecture for hardware SBPG compression integrated with SDC.
- The concept of SBPG that is integrated with SDC, which is suitable for real time intelligent traffic surveillance (ITS).
- A Simulink®-based prototype of the algorithm implementation.
- Experimental analysis and comparison of the proposed architecture.

5.1. Motivation of High-Performance Design

High compression of images is useful in a wide range of applications, even when it provides only approximate results. However, it is almost essential for real-time applications where any information transmission involves a time-consuming and expensive process. Using wireless transmission channels to transfer images is a growing technology that has many challenges and limitations to overcome. Efficient high compression is mandatory for wireless image communication because it can eliminate the problem of limited bandwidth. Traditional image compression standards sometimes include transmission errors and need correction codes. An efficient image coding method, with a reasonable image quality over an unstable channel and high compression ratio needs to be designed. The number of computer and digital devices that are connected throughout the world grows constantly so the need of transmitting real-time screen image seems a critical need in the future technological development.

5.2. Secure Better Portable Graphics: Algorithm and Architecture

The schematic overview of the proposed SBPG module showing the order of operations is illustrated in figure 5.1.

5.2.1. Algorithm and Architecture of Encryption and Watermark Unit

AES is considered the most common block cipher, it supports a variable data block and a variable key length. The block sizes and key sizes could be any multiple of 32 bits between 128 and 256 bits. The reasons behind choice of AES algorithm is due to the fact

that there are no practical attacks known against AES. In addition, AES can be optimized in VLSI architecture to achieve high-performance and high throughput with area efficient architecture [56]. AES consists of four fundamental algebraic function transformations: byte substitution, shift row, mix column, and round key for each standard round except the last standard round does not perform mix column. Based on the block and key size, 128, 192, or 256, the number of standard round will be 10, 12, or 14, respectively.

Digital watermarking is a method where information about the image or owner is embedded in the images in such a way that an unauthorized user cannot recover an original copy of the image whereas the authorized user can, after necessary processing of the image. Depending upon the application requirement, such as speed, cost, and reliability, one can employ different types of watermarking. A schematic overview of the proposed encryption and watermarking is shown in figure 5.1. The motivation behind the use of the center quarter of the host image for watermark placement is due to reduced computation load and increased robustness. The invisible-robust-blind watermarking algorithm is summarized as follows:

(1) Optimization of robustness, quality, and computational load because of using the center portion of the image, which contains the main information about the image. Also, encryption and watermarking insertion at this center quarter increases robustness.

(2) Watermarking is done in the frequency domain using the Discrete Cosine Transform (DCT) that will increase watermarking insertion speed.

(3) The insertion of the watermark is done in the midfrequency of the image block so that will increase the robustness since any removal of high or low frequency components of the watermarked image by operations does not significantly affect the watermark.

5.2.1.1. Insertion Algorithm

Watermarking insertion is done on the color image of size $N \times N$ based on the procedure proposed by Mohanty *et al.* in [73]. As a first step of insertion, the color image is transformed from RBG component to YCbCr color component. Y-color component is

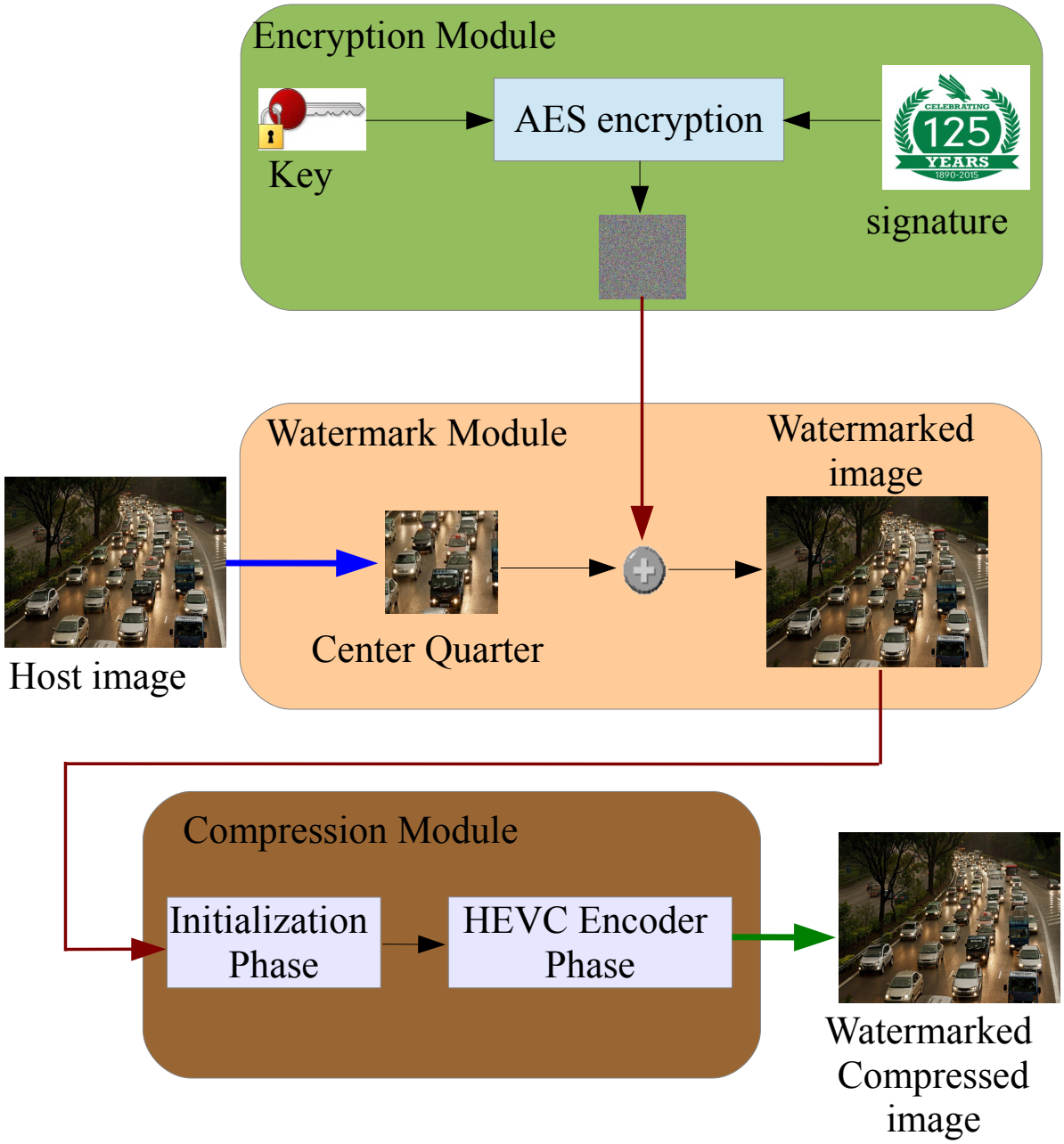


FIGURE 5.1. Schematic overview of the proposed SBPG module.

considered for further processing. The Y image component is divided into equal number of 8×8 blocks and DCT is performed on each block. Since the center portion of the image is the center of attention from viewers' point of view, the watermark will be embedded in the center quarter of the image. Since this 25% of the image area is used for watermarking, it increases the computational efficiency as well as the overall image quality. Furthermore,

if attackers try to remove or destroy the watermark for this center portion, then it will degrade the image quality. The selection of suitable DCT coefficients for watermarking is very important, selecting the low frequency leads to degreed quality. On the other hand, insert in high frequency domain makes the watermarking easy to remove by using filters. Hence, it is the best to select mid frequency for watermark. Four mid frequency coefficients are chosen from each block in the center quarter of the image. From these coefficients, a vector R of size K is generated where K is the number of blocks in the center quarter of the image given in Eqn. 6, where $r_{x,y}$ is the coefficient of the selected block y. A pseudo random sequence is chosen from bits in the encrypted signature, which will be used as the watermark represented shown in Eqn. 7. The watermark A is to be inserted into the DCT coefficients of the image of vector R according to Eqn. 8.

$$R = \{r_{1,i}, r_{2,i}, r_{3,i}, r_{4,i}, ..., r_{1,K}, r_{2,K}, r_{3,K}, ..., r_{4,K}\} \tag{6}$$

$$A = \{a_1, a_2, a_3, ..., a_{4\times K}\} \tag{7}$$

$$r_i^{'} = r_i + \alpha \mid r_i \mid a_i, \tag{8}$$

for $i = 1, 2, \cdots, 4 \times K$ and α is a scaling constant, which is used to determine the watermark strength. Small values of α can make the watermark vulnerable to modification and also make it difficult to extract and detect during the detection and extraction stage. Similarly, large values of α can make the watermark visible. So an optimum choice of this scaling constant is necessary [25]. In this chapter, we are focusing in high performance with promising quality because of that we decide to have mid value of $\alpha = 0.5$. The complete insertion process is shown in figure 5.2. The extraction process is the reverse process of the insertion algorithm; therefore, for brevity, only the insertion process is discussed.

The system-level architecture of the proposed watermarking algorithm is illustrated in Fig. (5.3). The block shown in the dotted line finds the region where the watermarking needs to be done. Thus, the five important aspects of (1) the center quarter, (2) edginess, (3) texture, (4) contrast, and (5) intensity, are analyzed to find the important region.

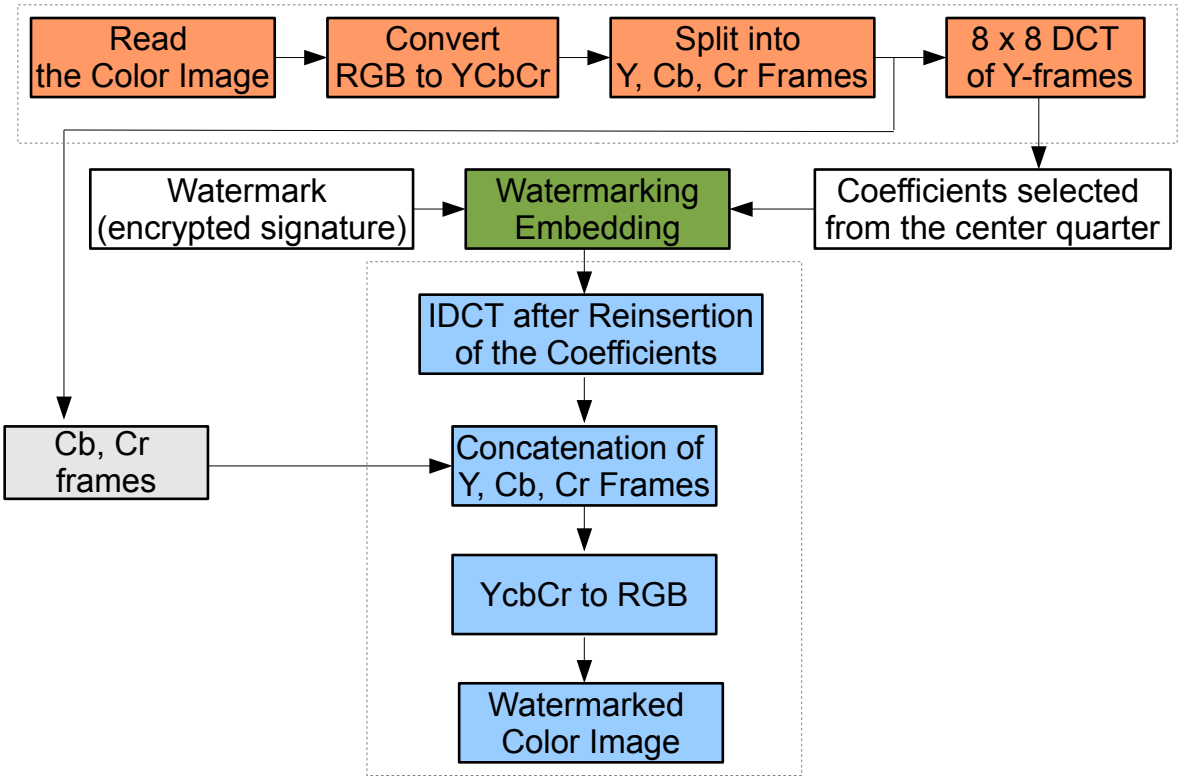


FIGURE 5.2. Watermark Insertion Algorithm.

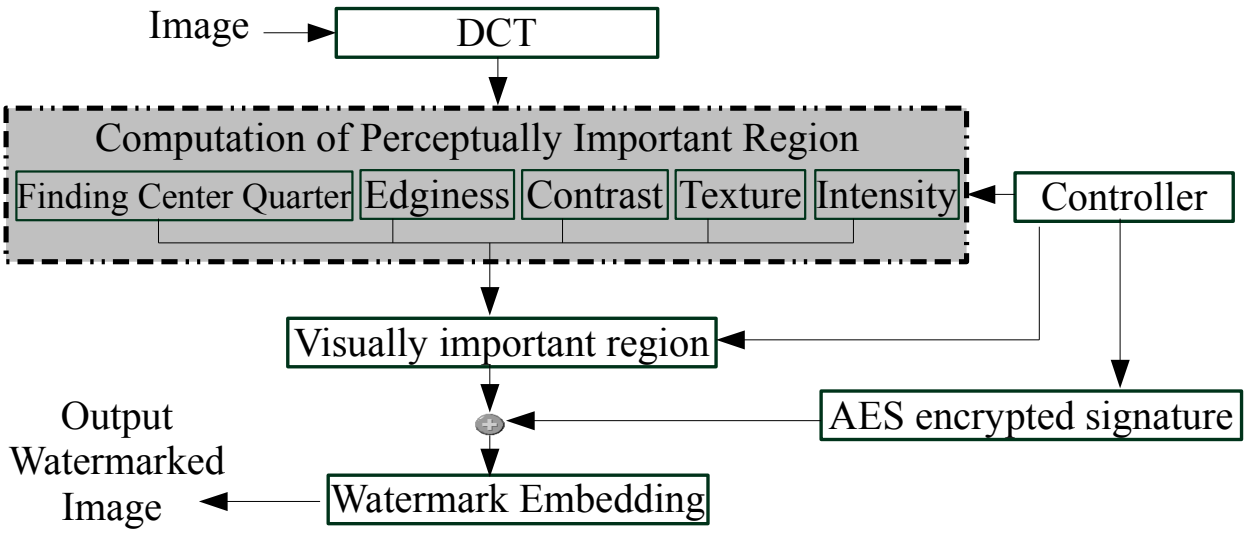


FIGURE 5.3. System Level Architecture of the Proposed Watermarking Algorithm.

The insertion unit is composed of several sub-modules: a DCT module, a perceptual analyzer, a scale factor, and the insertion module. The DCT module calculates the DCT coefficients of the host image. The controller manages the operation schedules of all other modules and the data flow of the unit. Figure (5.4) illustrates the watermark insertion unit.

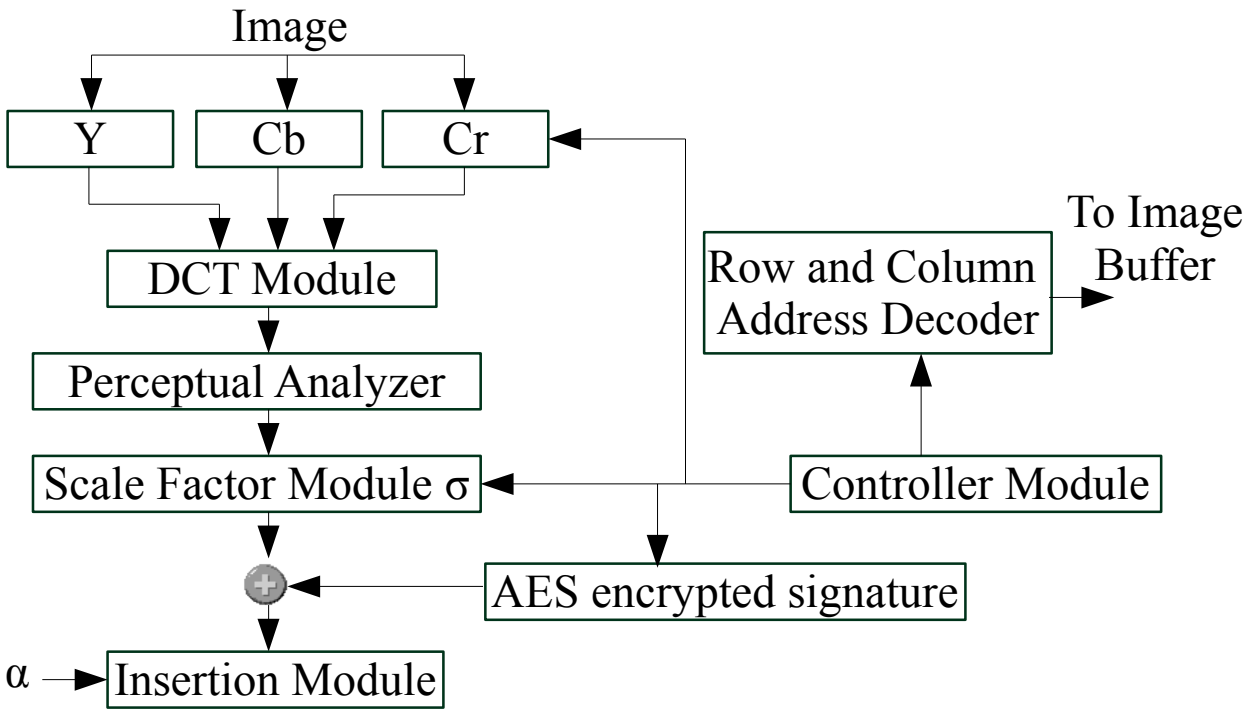


FIGURE 5.4. Watermark Insertion Unit.

The DCT module calculates the DCT coefficients of the image, as shown in figure 5.5. The algorithm splits the image into Y, Cb, and Cr frames, then considers just the Y frame in blocks of size 8×8. A buffer is used to assist in finding the transpose of the 1D row DCT [72].

5.2.1.2. Detection Algorithm

The main advantage of using the blind algorithm is original image information at the detector non-availability, which means that when detecting for watermark, no information about the original image is compromised [79]. In the insertion of the watermark, the original

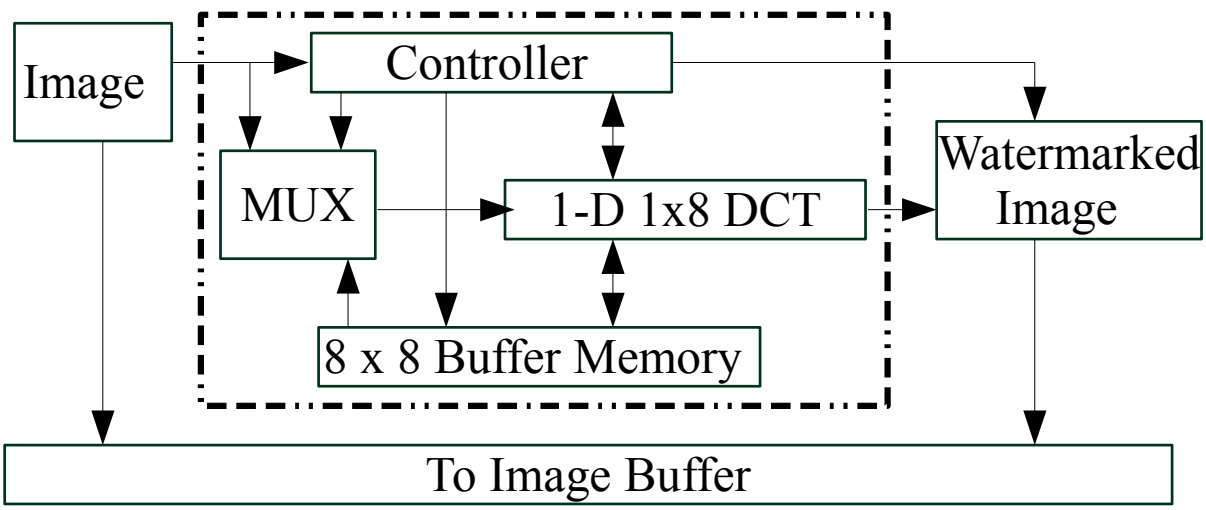


FIGURE 5.5. Discrete Cosine Transformation (DCT) Unit. [72]

$Y^{'}$CbCr is converted to Y^{*}CbCr. In order to extract the coefficients the central quarter of the image is identified from which the watermark will be extracted. From the selected coefficients, a vector R^{*} of size $4 \times K$ is generated in order to provide information:

$$R^{*} = \{r_1^{*}, r_2^{*}, r_3^{*}, \cdots, r_{4\times K}^{*}\}. \tag{9}$$

To determine the presence of a watermark in image O^{*}, a correlation coefficient σ is driven according to the watermark A, which is inserted into the DCT coefficient of the image of vector R in Eqn. 8. The correlation coefficient σ is defined that computes the correlation between the extracted coefficients R^{*} and the watermark itself using the formula:

$$\sigma = \frac{AR^{*}}{K} = \sum_{i=1}^{K} a_i r_i^{*}. \tag{10}$$

From Eqn 10, which provides the correlated between R^{*} and a generic watermark A, and with considering of ideal situation where the watermark is not corrupted:

$$r_i^{*} = r_i^{'} = r_i + \alpha \mid r_i \mid x_i. \tag{11}$$

Where X is DCT coefficient; then, the the correlation σ will be:

$$\sigma = \frac{1}{K} = \sum_{i=1}^{K} r_i a_i + \alpha \mid r_i \mid x_i a_i. \tag{12}$$

When A and X are matched the correlation σ will be:

$$\sigma = \frac{1}{K} = \sum_{i=1}^{K} r_i a_i + \alpha \mid r_i \mid a_i^2. \tag{13}$$

With the following assumptions: Zero means of r_i's and x_i's, μ equals $\alpha\mu_{|r|}$ when $A = X$; otherwise, μ equals 0. A threshold Th_σ is defined so that by comparing the calculated σ with this threshold Th_σ, it is possible to determine the presence or absence of watermark. In order to test the robustness of our algorithm and increase the threshold, different values of threshold are selected. Starting from the label in [14], which was 2.0, we used a trial and error method by trying with 1.8, 1.6, 1.4, 1.2, 1.0, and 0.8. The value 1.2 gives the best results considering all our test images. Thus, we have correspondingly increased the threshold label, that makes our algorithm more immune to noise and at the same time less probability of making wrong decision than the algorithm in [14]. This threshold is determined using the formula in 14. The threshold helps to make the decision: if $\sigma > Th_\sigma$ then a watermark is present, where if $\sigma < Th_\sigma$ then a watermark is absent.

$$Th_\sigma = \frac{\alpha}{1.2K} \sum_{i=1}^{K} \mid r_i^* \mid . \tag{14}$$

5.2.2. Algorithm and Architecture of BPG Compression Unit

the BPG image encoder algorithm is documented in details in chapter 4. It is divided into two phases: the pre-encoding (initialization) phase and HEVC encoding, as shown in figure 5.6.

The controller units is responsible for controlling the entire sequence of processes. The SBPG controller is modeled as finite state machine (FSM) with fifteen states (init, and S0 to S13) as presented in figure 5.7. The init state checks the watermark signal, if it is 0 that means the watermarking process has not been performed, in this situation the transition occurs from the initial state to S0. The first process is to read pixels in order to calculate DCT coefficients. The DCT operation is carried as a pipelined operation. If the

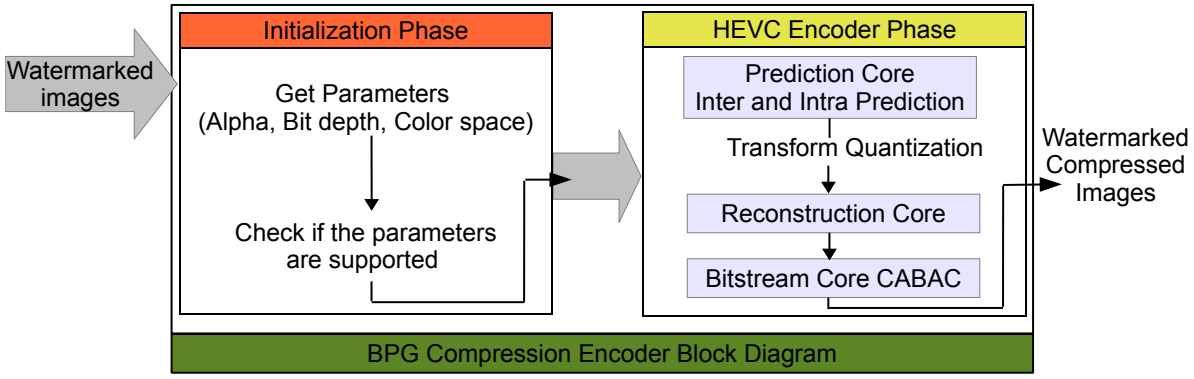


FIGURE 5.6. BPG Compression Encoder Block Diagram.

DCT coefficient of all the coefficients of a block is not completed, there is a transition from state S2 to S0. After the completion of all blocks, transition from the S2 to S3 occurrs in order to encrypt the signature. The computation of the center quarter of the original image is obtained in state S4. In states S4 and S5 the process of watermarking is performed and it is then written to RAM. When all the coefficients of the blocks are watermarked, a transition occurs to the init state and changes the watermark signal to 1. Then, the init state again checks the watermark signal since it is 1, the transition from init to state S8 occurres in order to check the image parameters. If the image parameters are compatible for BPG encoder, image splitting is performed in state S9, otherwise the transition occurs back to init state. After reducing the temporal and spatial redundancy in state S10, quantization is performed in state S11, then the reference frames are constructed. In state S13, context-adaptive binary arithmetic code (CABAC) is performed, which provides the BPG compression of the watermarked image.

5.3. Experimental Results

The main objective of this chapter is to implement secure BPG compression. For this, the SBPG architecture is implemented in MATLAB® /Simulink® Version 8.3 (R2014a), with the computer vision System Toolbox Version 9.7 [72]. Implementing the algorithm in MATLAB® gives a better understanding of the low-level implementation while Simulink® model provides a top-level functional and dataflow visualization. The HEVC encoder model

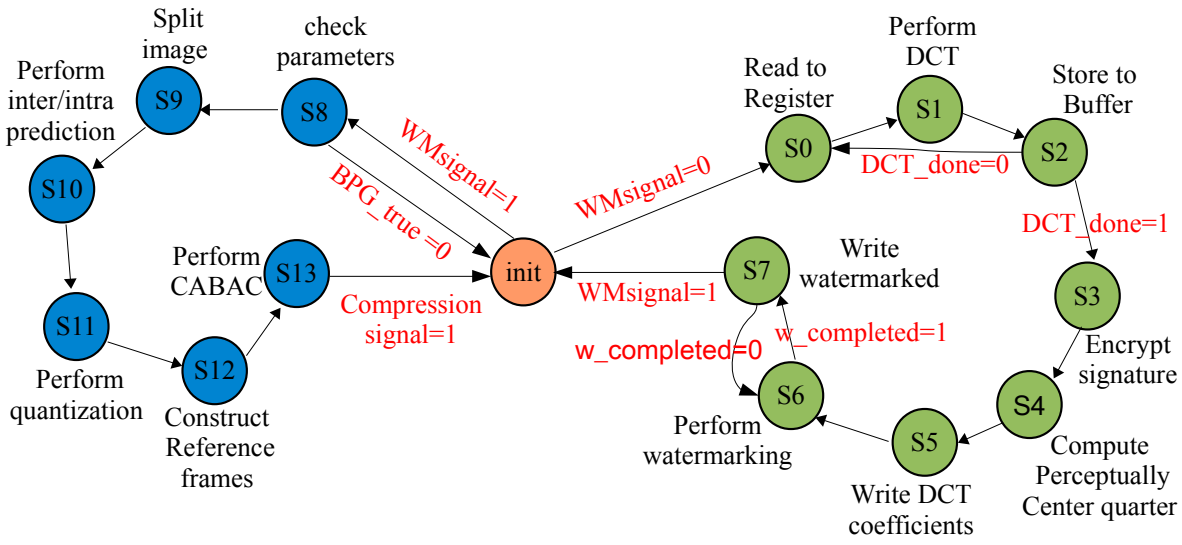


FIGURE 5.7. Finite State Machine Presenting the Controller of SBPG Architecture.

is shown in Fig. 5.8. The methodology that is used to represent the high level system modeling is bottom-up. The first step focuses on building the functions of encryption, watermark, and BPG units; the next step is to integrate these units into sub-system; and finally, verifying and testing overall system functionality. Extensive testing of the proposed architecture for several test images is done and the details are shown in this section.

5.3.1. Watermarking Insertion and Image Compression using SBPG Encoder

Five standard images are selected randomly from a large scale of images of Joint Picture Expert Graphics (.jpg) with different spatial and frequency characteristics. The cover images, watermarked images, and corresponding BPG images are presented in figure 5.9, figure 5.10, figure 5.11, figure 5.12, and figure 5.13. It can be seen from the result that the visual quality of the image is maintained. So the change in the image quality before and after watermarking and BPG compression encoder cannot be perceived by the human eye.

5.3.2. Graphs of RMSE and PSNR and Quality Assurance

In order to measure the robustness and the strength of the watermarked images and the corresponding BPG images, two performance measures are consider: the Root Mean

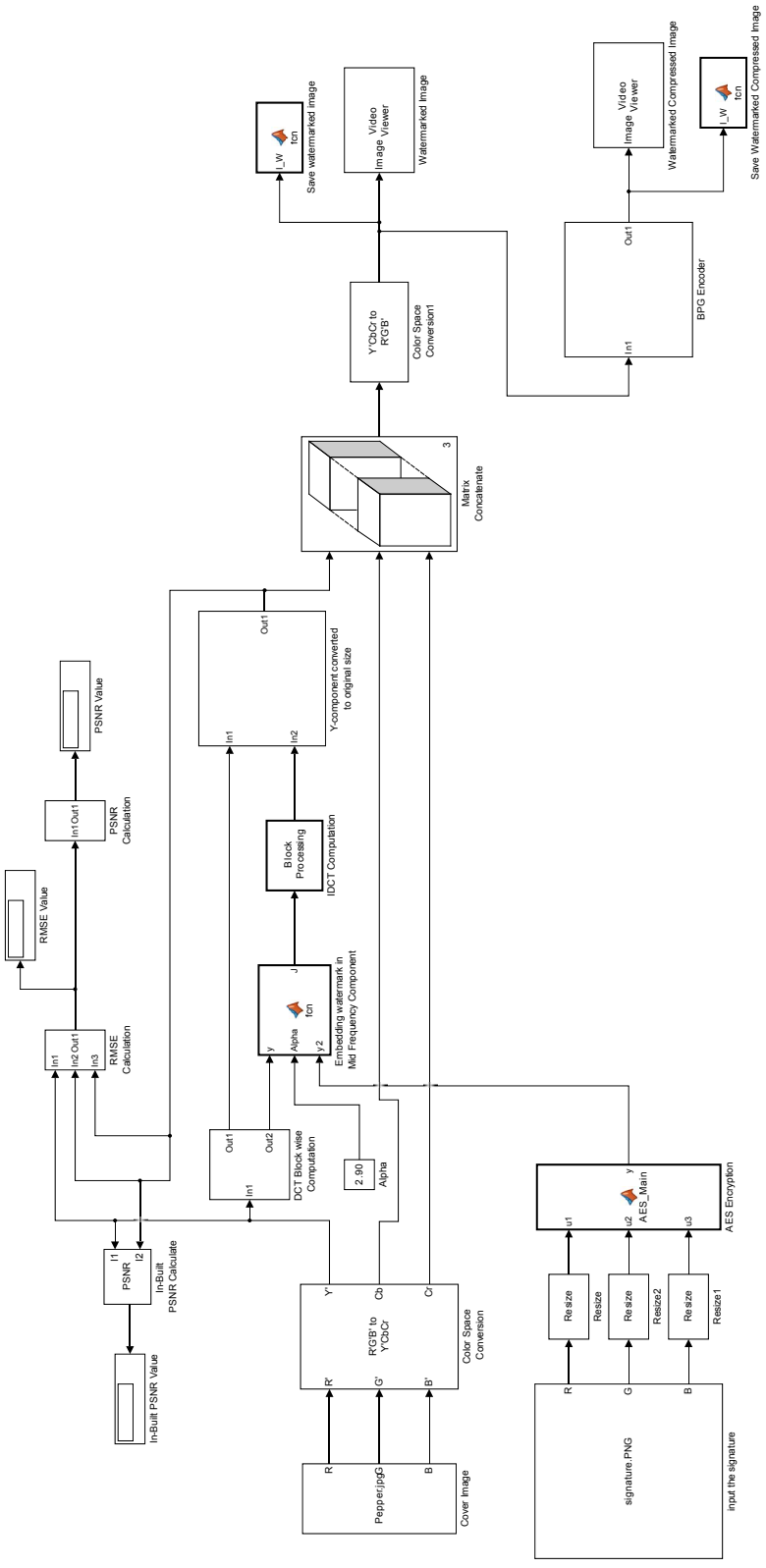


FIGURE 5.8. SBPG Compression Encoder in Simulink®.

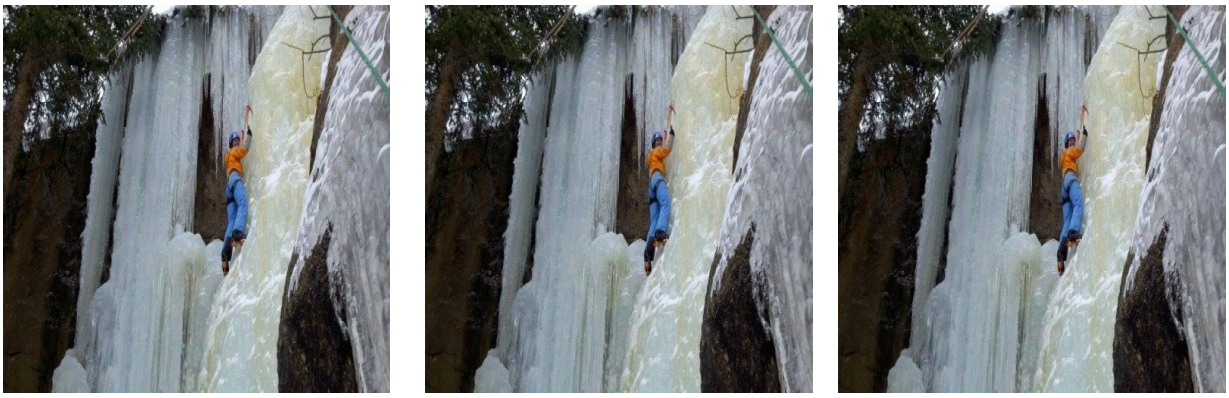
(a) cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 5.9. Secure BPG Compression of Baboon Image (256×256).

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 5.10. Secure BPG Compression of Forest Image (256×256).

Square Error (RMSE) [113] given in Eqn. 1, and the Peak Signal-to-Noise Ratio (PSNR) [46] given in Eqn. 20. RMSE is used twice; first, it compares the watermarked image $O^{'}$ to original image O of size $m \times n$. Second, RMSE compares the watermarked compressed image $O^{'}$ to watermarked image O. This process applies to PSNR as well. Table 5.1 illustrates the related metrics for each watermarking and BPG compression technique and test image. It can be seen that the value for PSNR is maintained above 47.9 dB for all cases. As the visual quality of the watermarked and compressed images improves with larger values of



(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 5.11. Secure BPG Compression of IceClimb Image (512×512).

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 5.12. Secure BPG Compression of Lena Image (512×512).

PSNR, this result shows that the proposed SBPG maintains the quality of the watermarked images so that it is impossible for the human eye to detected the signature of any watermark in it. Higher value of PSNR also shows how robust the algorithm is to different types of attack. In addition, it substantially increases the quality of the compressed images. The graphs of PSNR and RMSE versus size of the watermarked and watermarked compressed images for all tested images are shown in figure 5.14 and figure 5.15. From Table 5.1, the PSNR value for the "Pepper" image is maximum 55.4 dB, where for the "Forest" image

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 5.13. Secure BPG Compression of PepperImage (512×512).

the minimum. The RMSE is reversed as presented in figure 5.16 and figure 5.17. Figure 5.18 and figure 5.19 compare the PSNR and RMSE between the watermarked images and watermarked compressed images for all the standard images.

The comparative perspective of this architecture with respect to existing secure digital camera schemes is presented in table 6.1. It may be noted that the proposed SBPG in the first proposed hardware architecture for BPG compression encoder integrated with SDC.

5.3.3. Estimation of the Embedding Capacity

The estimation of embedding capacity is the process of finding the size of the largest watermark capacity that can be embedded into images. It is one of the most important issues in invisible watermarking. There are potentially many different techniques to estimate the embedding capacity such as multi-pass embedding capacity and Human visual system (HVS). Because the multi-pass embedding capacity requires additional memory [47], we use HVS to quantify the embedding capacity by calculating the perceptual metric in CIELAB [33] to find the color difference between host images and watermarked images. From the definition of CIE $L^*a^*b^*$ or CIELAB, let us consider that L^*_c, a^*_c, b^*_c refers to the host image and L^*_w,a^*_w,b^*_w the corresponding watermarked images. The total difference of color, which is considered as

TABLE 5.1. Quality Metrics for the Watermarking and Compression Techniques and Test Image

Test Image	Code	Size (KB)	RMSE	PSNR
Cover Baboon Image (16.7KB)	Watermarked Image	20.0	0.76	50.4
	Watermarked Compressed Image	16.1	0.50	52.1
Cover Forset Image (25.1KB)	Watermarked Image	28.2	0.92	47.9
	Watermarked Compressed Image	24.0	0.89	50.3
Cover IceClimb Image (85.3KB)	Watermarked Image	88.1	0.58	52.7
	Watermarked Compressed Image	84.7	0.42	53.0
Cover Lena Image (29.3KB)	Watermarked Image	34.2	0.89	49.8
	Watermarked Compressed Image	30.8	0.85	51.0
Cover Pepper Image (39.3KB)	Watermarked Image	40.0	0.52	53.6
	Watermarked Compressed Image	39.0	0.41	54.4

the tolerance of a color [32], is determined by the following:

$$\Delta total^* = \sqrt{\Delta L^{*2} + \Delta a^{*2} + \Delta b^{*2}}, \tag{15}$$

where ΔL^*, Δa^*, and Δb^* are the color differences for each color channel R, G, and B respectively. By separating those channels of the host image O, and transforming them into ΔL^*,Δa^*, and Δb^*, the algorithm separately calculates the color difference of each channel

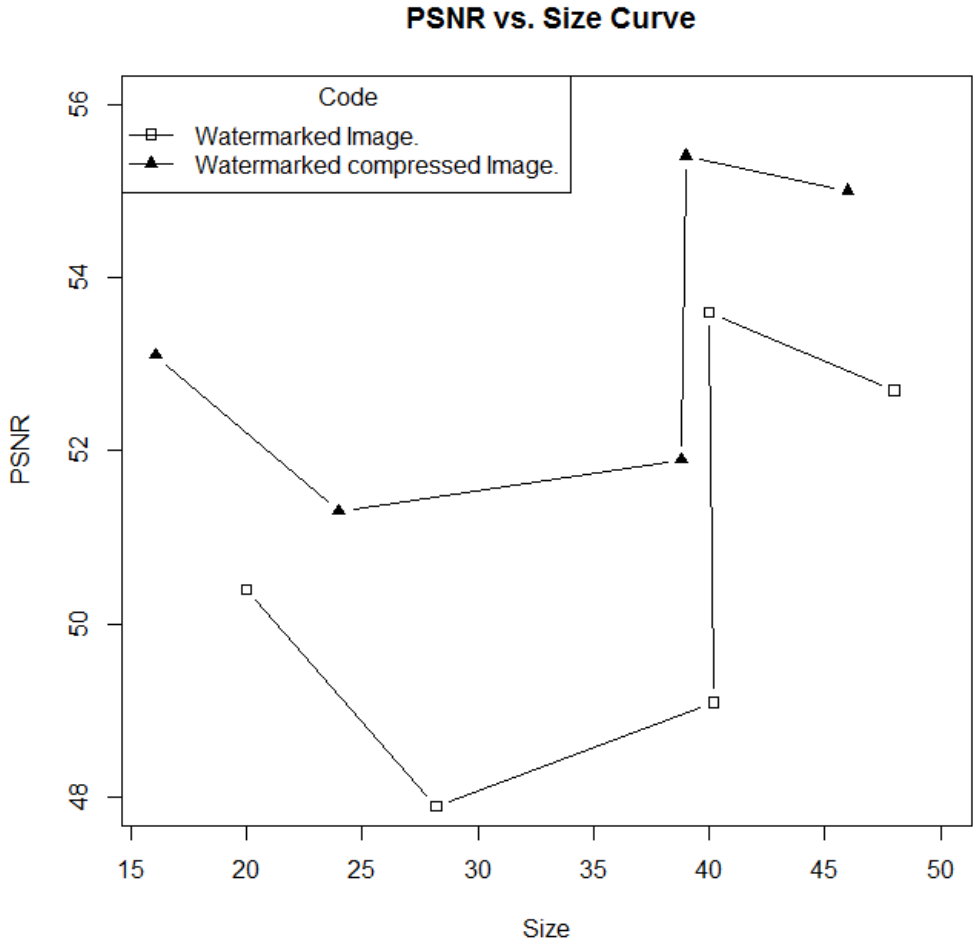


FIGURE 5.14. PSNR vs Size Curve.

as following:

$$\Delta L^* = L_w^* - L_c^* \tag{16}$$

$$\Delta a^* = a_w^* - a_c^* \tag{17}$$

$$\Delta b^* = b_w^* - b_c^* \tag{18}$$

From Eqn. 15, the estimation of the watermark embedding capacity will be the total capacity of colors of an image. For brevity, we select three different sizes of host images and their corresponding watermarked images with value of $\alpha = 0.45$ to estimate the embedding capacity. Since our proposed scheme considers just the center quarter of a host image, which

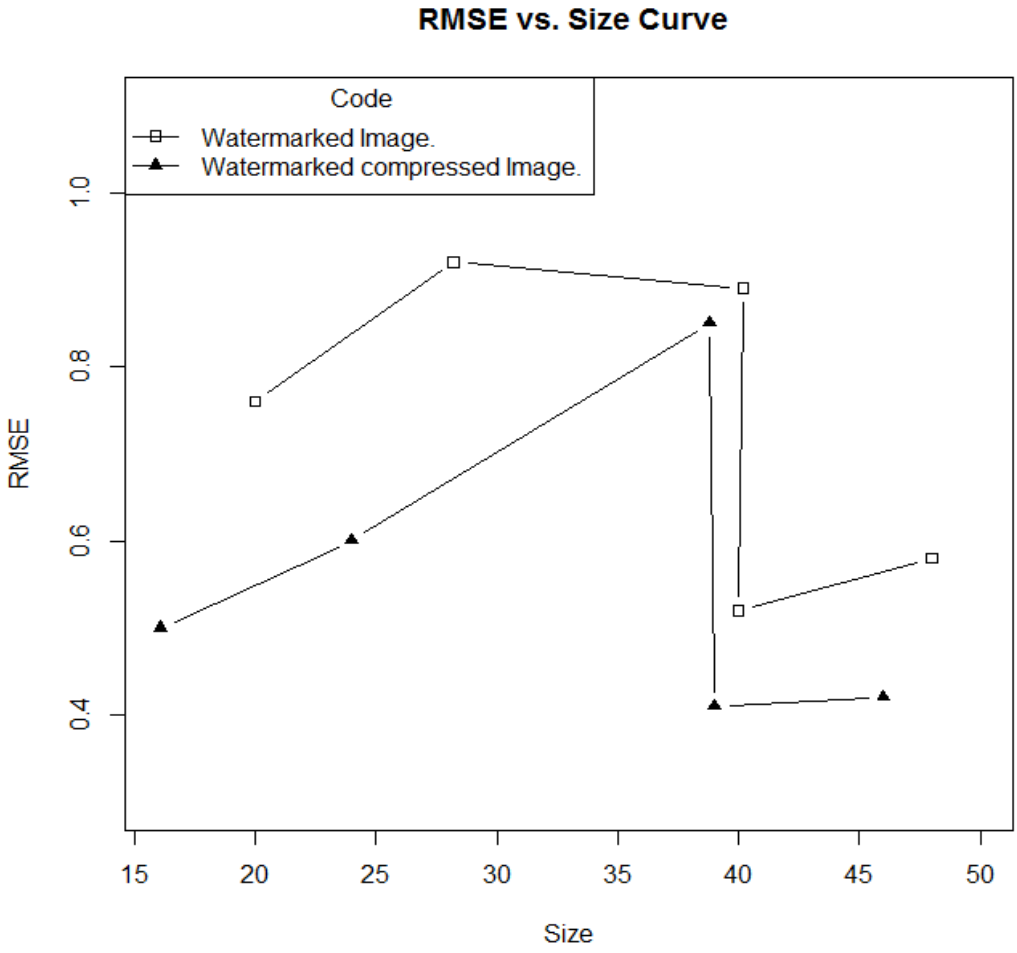


FIGURE 5.15. RMSE vs Size Curve.

is chosen based on computation process of perceptually important region, we focus in the center quarter of the image to estimate the embedding capacity. Table 5.3 demonstrates the estimation of embedding capacity. The proposed scheme potentially considers the center quarter of a host image, which provides several advantages in term of robustness and high performance, but at the same time the embedding capacity will be reduced because focusing just in the important region will degrade the image quality and some information will be lost.

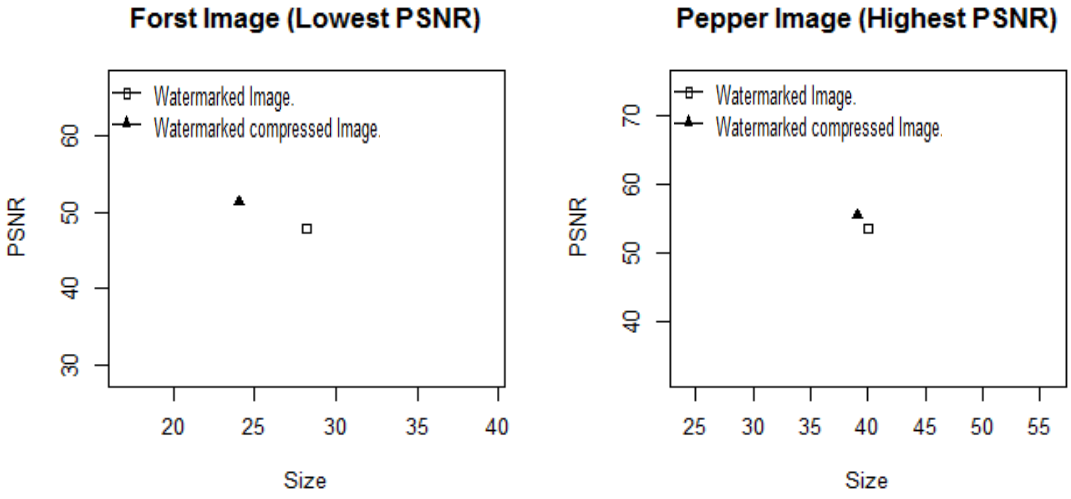


FIGURE 5.16. Highest and Lowest value of PSNR.

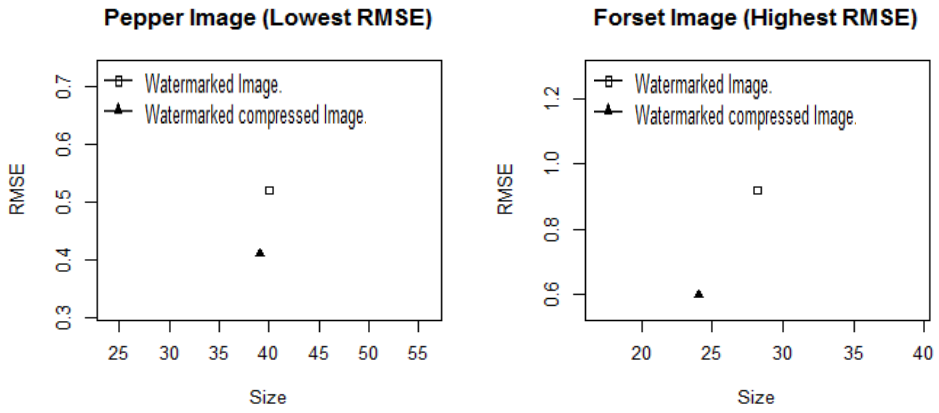


FIGURE 5.17. Highest and Lowest value of RMSE.

5.3.4. Testing for High performance

It is imperative to consider watermark and compression quality and performance trade-offs. From table 5.1, we can argue that the proposed SBPG architecture gives high quality since the value of PSNR is maintained above 47.9 dB for all cases. To achieve a high performance architecture we consider:

(1) Optimization of robustness, quality, and computational load because of considering just the center portion of the image, which contains the main information about the

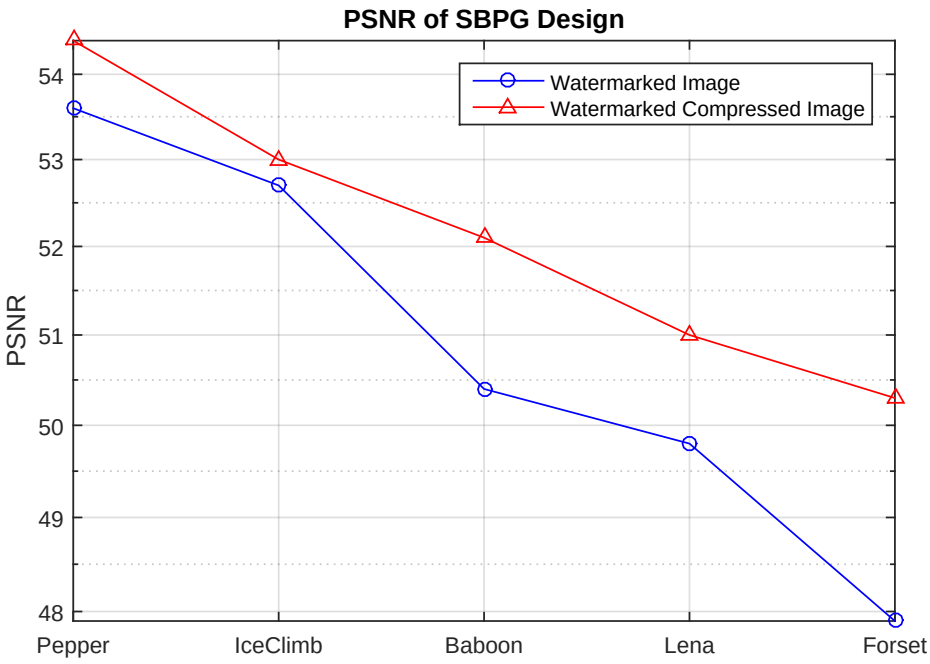


FIGURE 5.18. PSNR of SBPG Design.

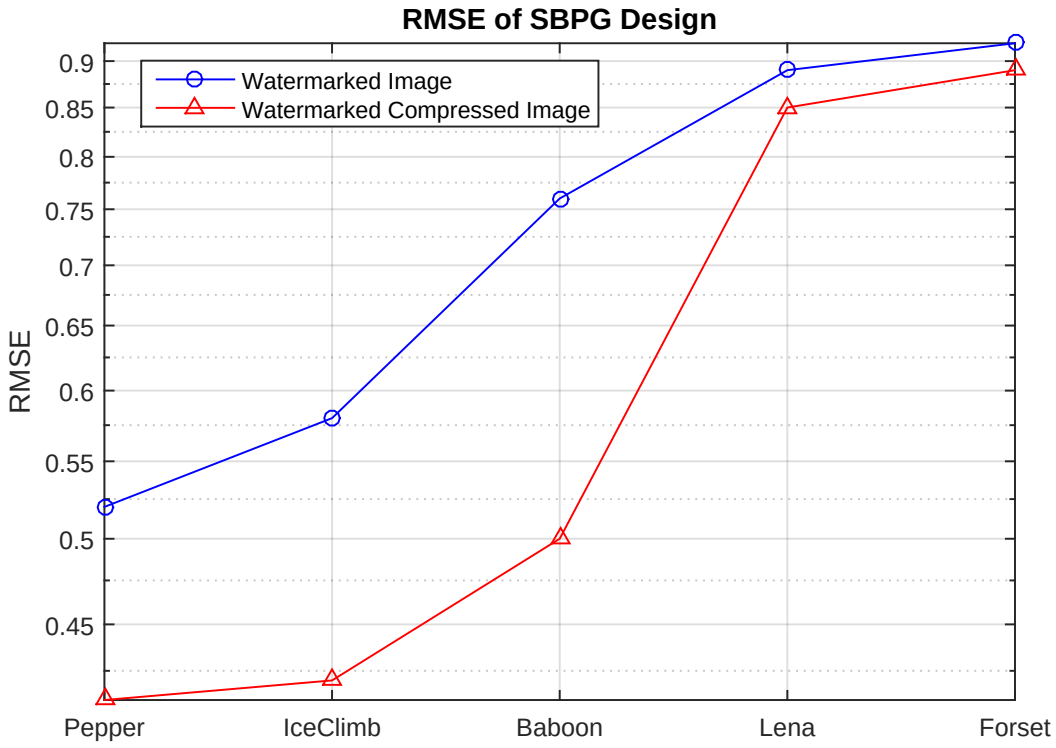


FIGURE 5.19. RMSE of SBPG Design.

TABLE 5.2. Comparative Perspective with Existing Secure Digital Camera Architecture.

Prior Research	Built-in Security Function		Domain	Built-in Compression	object
	Watermarking	Encryption			
Mohanty *et al.* [71]	Invisible Robust	AES	DCT	None	Image
Darji *et al.* [31]	Invisible Feasible	None	DWT	None	Image
Mohanty *et al.* [76]	Visible	None	DCT	JPEG Encoder	Image
Lei *et al.* [104]	Semi-Fragile and Robust	None	DWT	None	Image
Mohanty *et al.* [72]	Visible	None	DCT	MPEG-4 Compression	Video
The proposed SBPG	Invisible Robust Blind	AES	DCT	BPG Encoder	Image

TABLE 5.3. Estimation of the embedding capacity

Host Image	**Dimensions of Important Region**	**Embedding Capacity of the Center Quarter (bits)**
Baboon (256 × 256)	64× 64	308265
Forest (256 × 256)	64× 64	312031
IceClimb (512 × 512)	128 × 128	432926
Lena (512 × 512)	128 × 128	401817
Pepper (512 × 512)	128 × 128	429417

image. Thus, the speed is increased when the algorithm consider the portion of the image not the whole image. Also, the watermarking insertion at this center quarter increases the robustness because any attempt to remove the watermark will result in degradation of image quality.

(2) Watermarking is done in the frequency domain using block-wise Discrete Cosine

Transform (DCT) size 8×8 that will increase watermarking insertion speed.

(3) In BPG encoder, the proposed architecture uses inter and intra prediction to reduce the temporal and spatial redundancy, which improves the computational speed.

To calculate the frame-rate, we feed the Simulink®file with 30 random images as inputs. The time taken to get the outputs (30 watermarked compressed images) is 1.27s. Thus, the maximum throughput of the proposed SBPG is 25 frames/sec at a clock speed of 2400 MHz. We can argue that the frame rate is acceptable due to the fact that modules in the proposed SBPG must run sequentially because the output of the watermarking module is considered as an input for BPG compression encoder. Overall the proposed SBPG offers a double-layer of protection: watermarking and encryption, with applying state-of-the-art image compression technique (BPG), which achieves high compression ratio with small size. With all the above security and compression features it is acceptable that the frame rate is 25 frames pre second (fps).

5.4. Testing the Watermark Algorithm with Different Attacks

This section analyzes the detector's response when the watermarked images are subjected to different types of attacks. This reveals how robust the watermarking algorithm is. If the watermark can be extracted from the attacked, corrupted, and/or modified watermarked image then the watermark is said to have survived, otherwise it has not survived. The attacks that have been tested for this experiment are the following: compression attack, geometric distortions, and collage attack.

5.4.1. Compression Attack

The proposed SBPG is robust since it applies the watermarking first then the BPG compression. It can be argued that starting with watermarking and encryption process then preforming the BPG compression is more secure than starting with compression process because information is again changed during the compression process. If we do the opposite, the original data in a host image is changed by the compression process before applying the watermarking, which means the watermark is altered since it is based on changed informa-

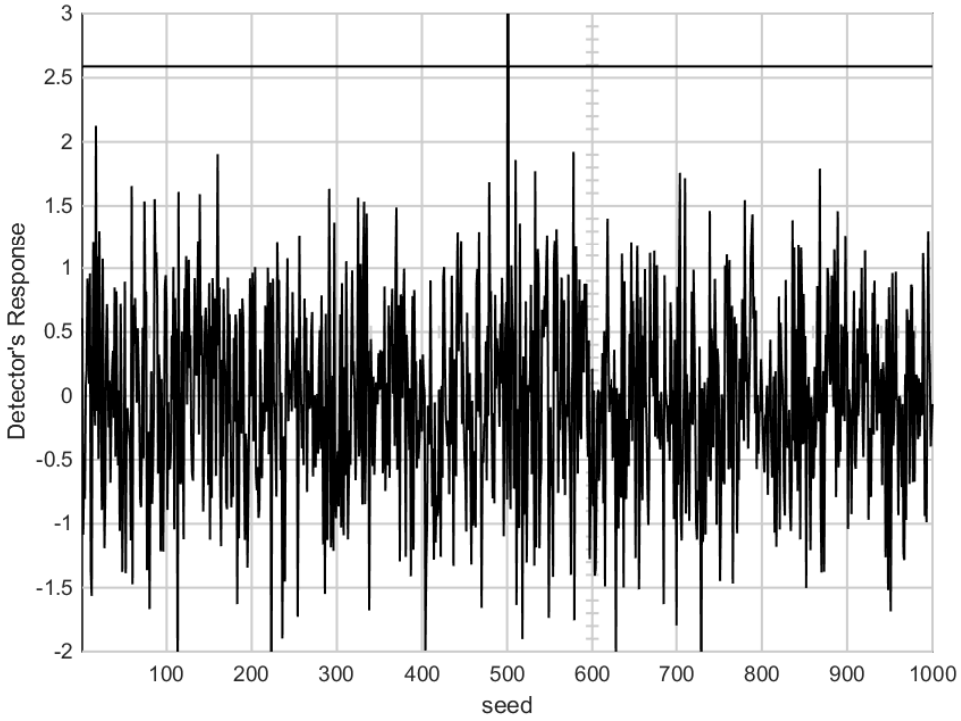


FIGURE 5.20. Detector's Response of Watermarked Compressed Baboon.

tion of the host image. Thus the output of SBPG (watermarked compressed images) can be used to test again the compression attack. The detector's responses of all the watermarked compressed images are shown in Figures (5.20), (5.21), (5.22),(5.23), and (5.24) which illustrate that all of them are survived the compression attack. Thus, the proposed watermark prove to resist the compression attack.

5.4.2. Noise Attack

Gaussian noise is inserted into the image in different amounts and then the image is compressed. Figures (25(b)), and (25(c)) show the watermarked image affected by noise and the corresponding detector's response. The effect of noise on the images is given in Table (5.4). From the table it is inferred that larger size images are more resistant to noise.

5.4.3. Geometric Distortion Attack

Geometric distortion is an important concern in testing the robustness of the watermarking algorithm for copyright protection of digital images. Resizing, rotation, and

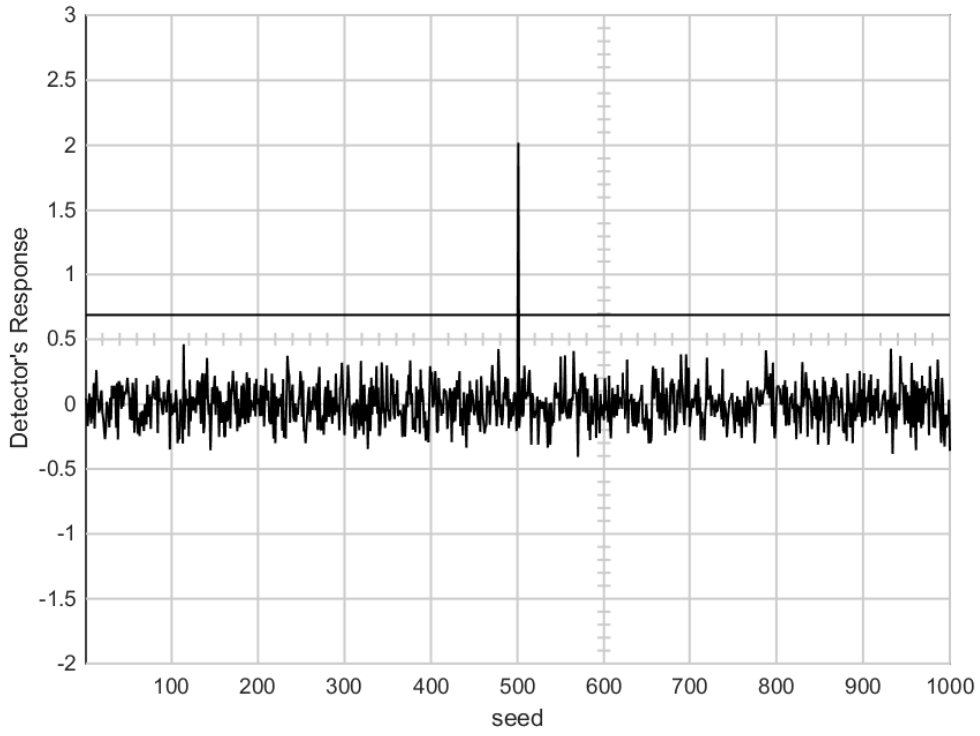


FIGURE 5.21. Detector's Response of Watermarked Compressed Forest.

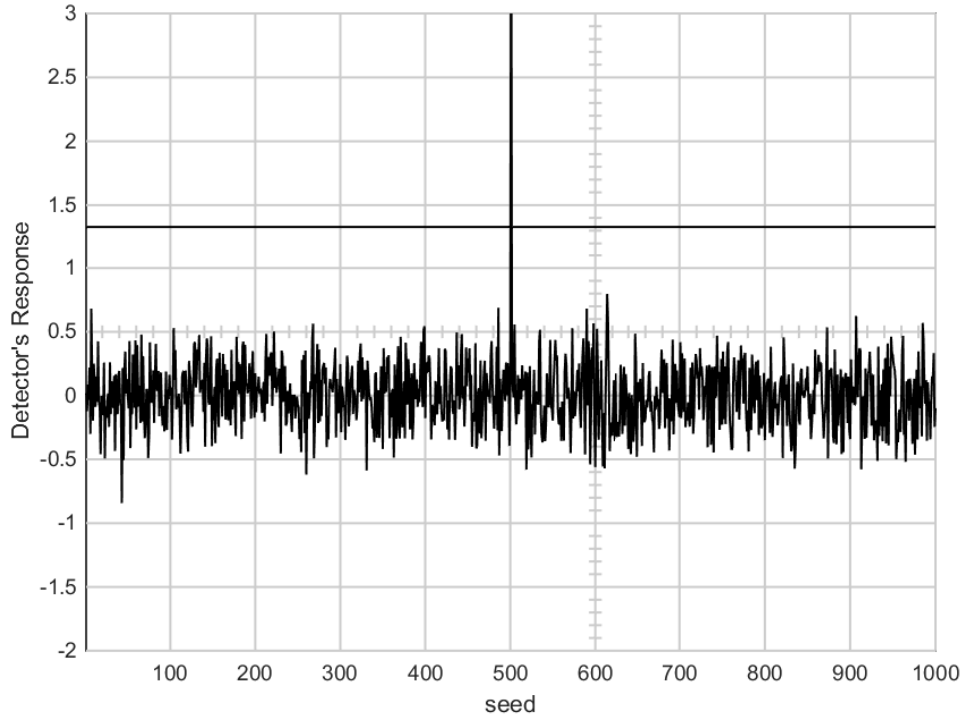


FIGURE 5.22. Detector's Response of Watermarked Compressed IceClimb.

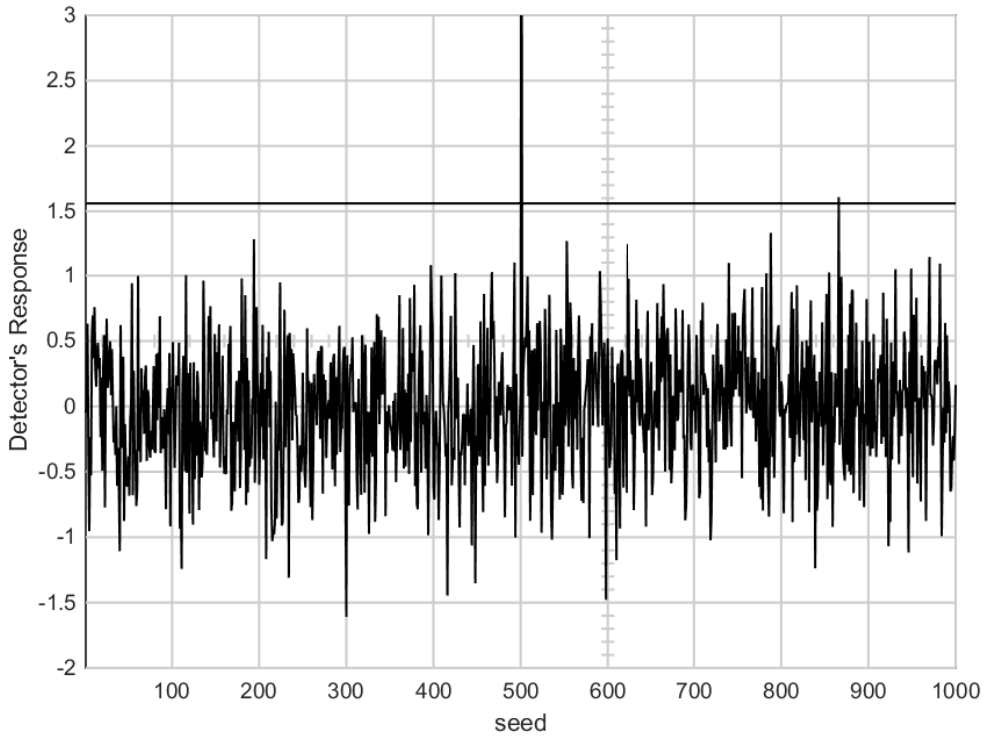


FIGURE 5.23. Detector's Response of Watermarked Compressed Lena.

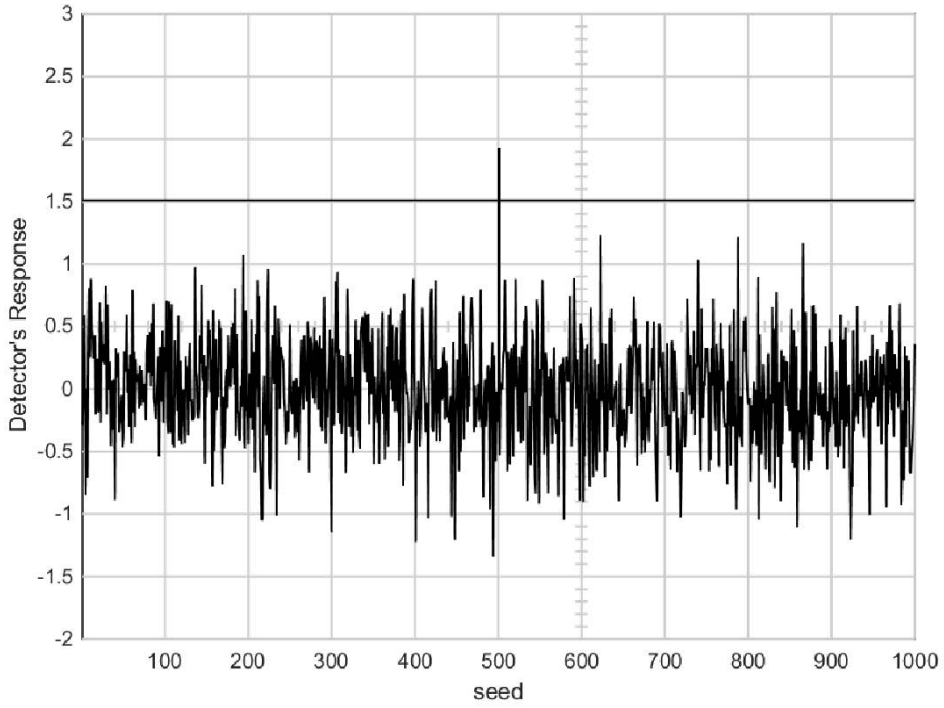
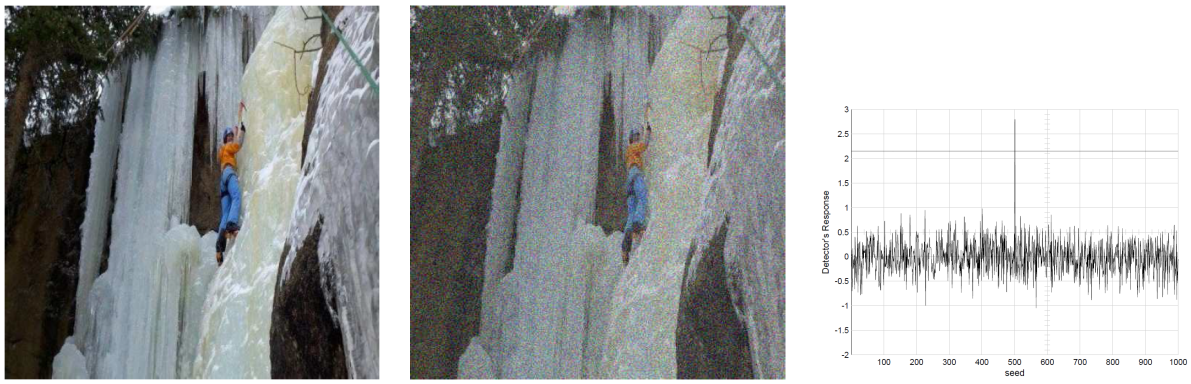


FIGURE 5.24. Detector's Response of Watermarked Compressed Pepper.



(a) Wallpaper image (b) 40% noise added (QF=25) (c) Detector's Response (QF=25, 40% Noise)

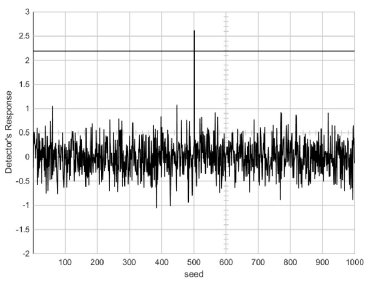
FIGURE 5.25. Noise added to Watermarked Image.

TABLE 5.4. Noise on Different Images.

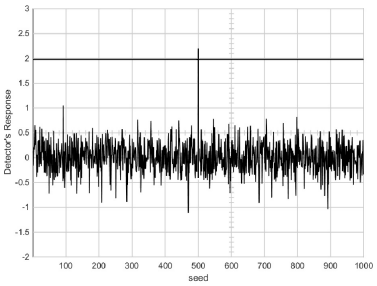
Tampering Operation	**Wallpaper Image** (128×128)	**Bear Image** (256×256)	**Ice Climb Image** (512×512)
25% Noise	Survived	Survived	Survived
35% Noise	Too noisy	Survived	Survived
40% Noise	Too noisy	Noisy	Survived

cropping are considered to be the common attacks in this class. We experimentally investigated the robustness of our algorithm against the resize attack. We consider the standard test image (Lena of size 512×512), then we resized the watermarked image to new size of 500×500, 490×490, and 480×480, and compressed them with different QF. Figures (26(a)), (26(b)), and (26(c)) show the resized watermarked images along with the detector's responded. Table (5.5) shows the result. The results prove that the algorithm is robust with respect to higher values of α. A combination of rotation and cropping attack is used to test the robustness of our algorithm against geometric distortions. Applying different angles in the rotational process then cropping the images, the detector is able to detect the presence of the watermark in images with larger size, which are more resistant to rotation and cropping, as demonstrated in table (5.6) and figures (27(a)), (27(b)), (27(c),(28(a),(28(b)and (28(c)).

(a) Watermarked compressed image, rezied to 480×480



(b) Detector's Response (α=0.65, QF=25, 480×480 resizing)



(c) Detector's Response (α=0.65, QF=25, 480×480 resizing)

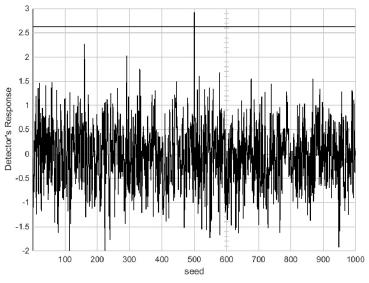
FIGURE 5.26. Resizing Watermarked Compressed "Lean" Image.

TABLE 5.5. Resizing Watermarked "Lena" Images with 25% QF.

Tampering Operation **Lena 512X512**	α	**Detector's Response**
Resize to 500×500, BPG Compression	0.65	Survived
Resize to 490×490, BPG Compression	0.65	Survived
Resize to 480×480, BPG Compression	0.65	Survived

(a) Watermarked image with 90° rotation

(b) Watermarked image with 90° rotation, cropping)



(c) Detector's Response (α=0.65, 90° rotation, cropping)

FIGURE 5.27. Rotation and Cropping Watermarked "Bear" Image.

(a) Watermarked image with 30° rotation (b) Watermarked image with 30° rotation, cropping) (c) Detector's Response (α=0.65, 30° rotation, cropping)

FIGURE 5.28. Rotation and Cropping Watermarked "Ice Climb" Image.

TABLE 5.6. Rotation and cropping on different Images with different angles.

Tampering Operation	**Wallpaper Image** (128×128)	**Bear Image** (256×256)	**Ice Climb Image** (512×512)
30° rotation, with cropping	Not recognized	Not recognized	Survived
90° rotation, with cropping	Not recognized	Survived	Survived

5.4.4. Collage Attack

Collage attack is considered to be a substitution or counterfeiting attack. It takes advantage of the vulnerability of embedding the watermark independently into a local region of the image with the same mark. An attacker forges a falsified image using parts of a group of images protected by the same authenticator using the same mark. The study in [37] proves the possibility of collage attack even when a logo is not known by using a larger number of images watermarked with the same key and logo to create a new image while preserving their relative spatial location within the image. However the proposed scheme independently embeds the watermark in each block, our algorithm effectively resists collage attack due to the following:

(1) Pseudo random noise is used as mark, which is changed for every image. So, no logo is used to figure out the relative spatial location within large number of images.

(2) The proposed watermarking algorithm analyzes five important aspects for computation of perceptually important region. Thus, this partial region is selected based on the image; that means it is changed from image to image.

CHAPTER 6

ENERGY-EFFICIENT DESIGN OF SECURE BPG FOR TRUSTED IMAGE COMMUNICATION IN THE IOT

Power consumption has become a major concern in any portable application. This chapter proposes an energy-efficient design of the Secure Better Portable Graphics Compression (SBPG) Architecture [6]. The aim of this chapter is to optimize the SBPG baseline design, which is presented in the chapter 5, to achieve an energy-efficient SBPG design. To estimate the power in the proposed architecture we have adopted a pattern-independent method where many simulations run in the design with different inputs and the average of the power dissipated was considered. The current and voltage values are considered from the output of the design, in order to calculate power. This is achieved with the help of sensors and power block available in Simulink®. This is the first attempt to propose an energy efficient hardware architecture of Secure Digital Camera integrated with Secure Better Portable Graphics Compression encoder to the best of author's knowledge. From the results presented in the chapter, it can be observed that with the same peak signal to noise ratio, the power consumption is substantially reduced up to 19%.

The novel contributions of this chapter include:

- The first-ever architecture for an energy efficient hardware of SBPG compression integrated with SDC.
- The concept of SBPG that is integrated with SDC, which is suitable for low power intelligent traffic surveillance (ITS).
- A Simulink®-based prototype of the algorithm implementation.
- An experimental analysis and comparison of the proposed architecture.

6.1. The motivation of Low-power Design

One of the most important aspects of any portable application is power consumption [74, 75]. Low power consumption means extended battery life, which increases the portability. Moreover, low power consumption determines a decrease of the packaging cost, and it is

beneficial for cooling in both portable and non-portable applications. Technology develops with impressive speed, and most products go through a progressive change. The constant innovations have made most products to require a low level of energy and a reduced material density. It is highly important for consumers to adapt their behaviors to the requirements of the devices, yet few people are aware of how they use and spend energy. The lack of knowledge regarding this topic makes it difficult for people to change and adapt their behavior in order to increase efficiency. The term of energy-awareness has gained utmost importance over time. Any battery-powered system is dependent on its energy consumption level, thus understanding how a device uses energy is crucial in optimizing energy consumption. Energy consumption can be studied in accordance to both software and hardware optimization. Innovators of the hardware industry investigate the levels of energy consumption for every new device and technique in order to optimize it. On the other hand, researchers from the software field investigate how the software itself and its different uses can influence energy consumption. An efficient software is capable of adapting to the requirements of everyday usage while saving as much energy as possible. Software engineers contribute to improving energy consumption by designing frameworks and tools used in the process of energy metering and profiling [13].

In our modern times, the visual richness of the world has become easily accessible to anyone. Images form the basis of our cultures. Every transient moment of life can be captured and saved through an image, allowing us to return to it whenever we want. As a specific type of data, images can have a long life if stored properly. However, images require a large storage space. The process of storing an image starts with its compression. Through compression, the data volume is reduced, which facilitates both storage and transmission. A compression algorithm can easily manage this task, BPG [16] is the novel step in the field of image compression that is highly effective because it is based on the High Efficiency Video Coding (HEVC) [99], released in the beginning of 2013. HEVC/H.265 uses innovative tools and efficient methods for coding. The real-time compression and decompression of high-resolution videos in HEVC come with specific requirements that only multicore platforms or

application-specific solutions can meet. These types of applications perform a reduction of bandwidth for transmission and storage by using video coding and real-time image.

Multimedia data such as images, video, or audio consumes many resources and requires complex computational operations that might be difficult to handle by the system. A limited memory for storage or limited energy supply might become challenges which decrease the possibility of maximizing the capacities of the application. VLSI technology is highly concerned, nowadays, with low power design, in an attempt to optimize battery-powered portable systems or PDAs. These multimedia devices process large amounts of data [42]. When it comes to digital cameras, the operations done by the device are highly complex and include capturing real-time images, compressing and storing them.

6.2. Digital System-on-Chip (SoC) energy Optimization

Different levels of abstractions for various energy-efficient or low-power techniques for a digital SoC are shown in figure 6.1. In digital circuit abstractions, at each of the levels, building blocks or basic elements are different. Various levels of granularity are present for the design engineers at different levels. The higher the level of abstraction, the higher is the possibility of optimization and bigger is the granularity as the large building blocks or basic elements are used. At the same time, more time is required for design iterations for low-power optimization. The higher the abstraction level, the lower is the accuracy and vice versa. The lower the level of abstraction, the lower is the optimization possibility. Granularity of building blocks or basic elements is finer. However, iteration of design optimization takes more time. Use of analog/SPICE simulator in the iteration loop can make it infeasible for the optimization of power at physical level in case of large digital circuits. [69].

6.3. The Proposed Low Power of Secure Better Portable Graphics: Optimization Perspective

The optimized architecture of HEVC encoding is shown in Fig. 6.2. First, advanced motion vector prediction is used for the prediction of the current motion vector, which uses a specific scheme belonging to a candidate group that includes temporal motion vectors. To ensure that the best candidate is selected from the group, the encoder uses a rate distortion

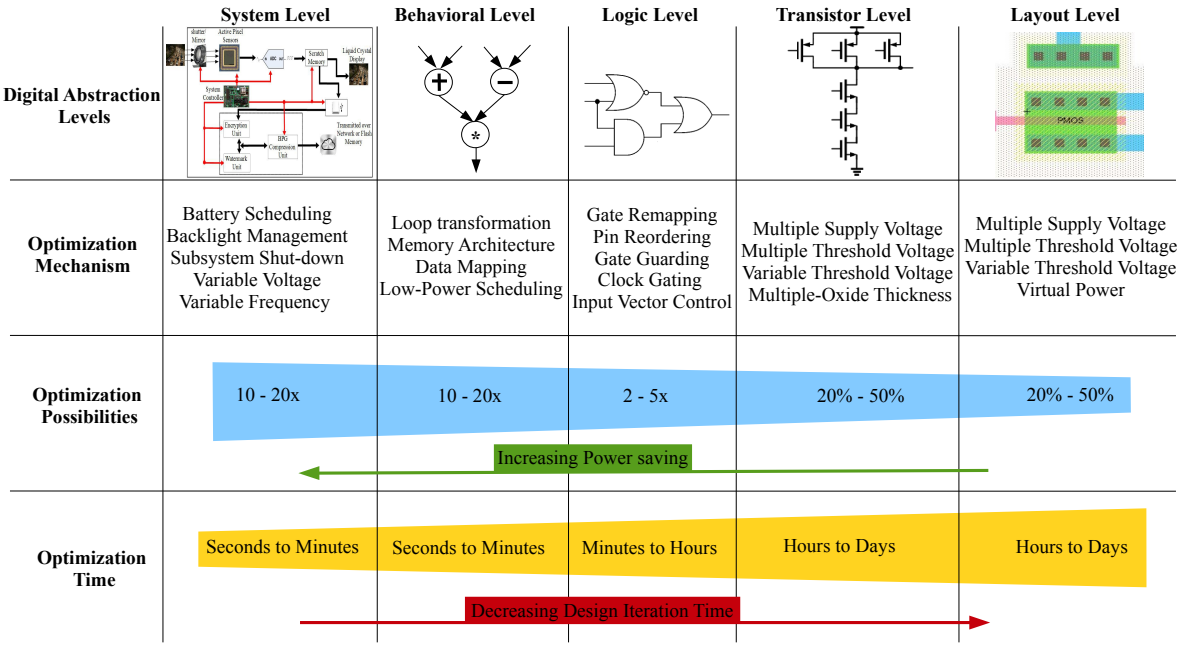


FIGURE 6.1. Power Reduction at Different Abstractions of a Digital SoC. After [69]

.

optimization process. The decoder is thus able to indicate and extract the best motion vector predictor by knowing the index. The proposed architecture includes in the competitive group of candidates two neighboring candidates and one candidate from a co-located temporal area. After the derivation of the candidates, they go through a scanning process that checks for redundancy and eliminates duplicates from the existing list of candidates. If the numbers of the candidates on the list is lower than two, the list will receive an additional zero motion vector, which is useful for increasing the efficiency of partitioning representation. To make the prediction possible, the motion information of the reference pictures requires proper storage and must be made easily accessible. To keep the storage requirements to a minimum, the resolution of the motion information is kept at 16×16 for each block. The second key factor in the proposed architecture is DCT optimization and quantization, which is used to drive interpolation filter to achieve the low-power design.

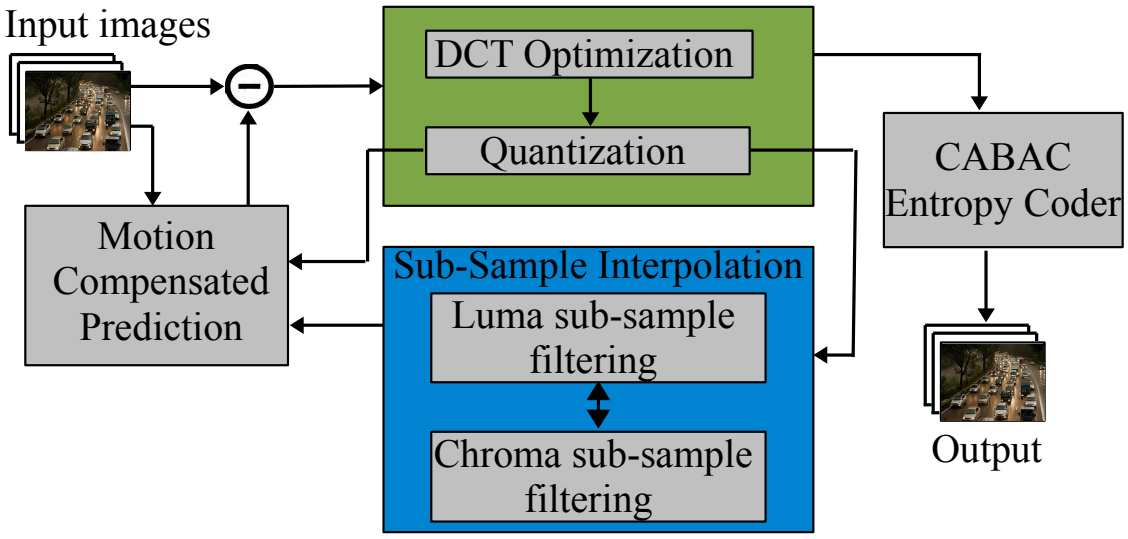


FIGURE 6.2. Overview of the Optimized HEVC encoding System.

6.3.1. Motion Compensated Prediction

HEVC encoding standard uses inter-prediction for the prediction block (PB) level [102]. Inter-prediction is best described as a motion compensated prediction, understood as the interchange and manipulation of areas from the reference picture in the construction of the current PB. Because of the distortion rate, the motion vectors are capable of representing a solid approximation of the motion, even though they cannot represent the true motion of the area involved. The results showed that bi-prediction is the best choice because it provided a balance between compression performance and implementation complexity [112]. The only concern regards the high amount of required memory, which can only be fixed by hardware optimization. To limit the number of maximum possible motion compensation operations, inter-prediction is done only with smallest block sizes, 4×8 or 8×4.

The possibility to merge motion information is useful in efficiently encoding motion in cases of randomly shaped areas in a picture. Merge mode extracts the applicable motion information from a configurable group of candidates. The PB syntax can indicate which candidate motion information should be utilized by adding a merge index to the list of candidates.

Figure 6.3 shows the advanced motion vector prediction. The process starts with

selecting one candidate, then removing the duplicated candidates. The algorithm adds a zero motion vector if the remaining candidate is smaller than 1. Otherwise, it removes the candidate with index larger than 1. Accordingly, the final number of candidates is 2, which is AM_1 and AM_2, the final motion vector AM_f is calculated by [117]:

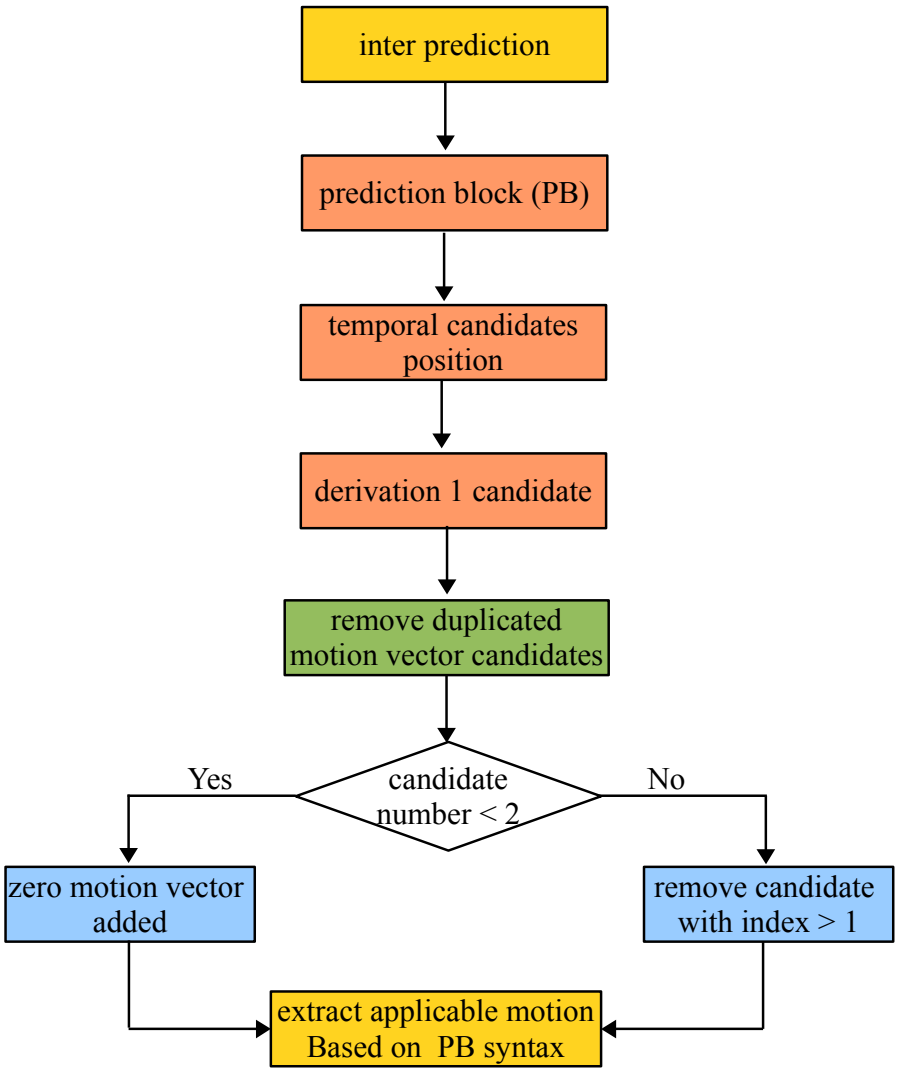


FIGURE 6.3. Advanced Motion Vector Prediction. After [117]

$$MV_f = Mean(MV_1 + MV_2). \tag{19}$$

Every reference picture can have a weighting factor and an offset value attached to

the prediction of P or B slices [112]. The two parameters are applied if the reference picture generates a motion compensated prediction. In case of partition slices, weighted prediction has the role of fading in or out the amount of color compounds while in case of block slices, weighted prediction has the additional role of mixing over the prediction generated from two reference pictures.

6.3.2. DCT Optimization

The aim of DCT optimization is to minimize the number of arithmetic operations. Once DCT is performed on the image block, there is a clear distinction of higher and lower frequency coefficients of the image. Lower frequency coefficients contain most of the visual information. The first row and first column in the block represent the DC component while the remaining blocks represent AC components. Since it is possible to reconstruct the image just with the DC component along with few AC component of lower frequencies, this method results in a very computationally efficient circuit without compromising the quality of the image. By discarding the high frequency coefficients, high image compression can be achieved as well.

For DCT-based interpolation, initially, Forward DCT is performed over N neighboring samples. Then DCT coefficients are reconstructed from the shifted center location with a shift δ [112]. The above two steps are merged to derive the filter coefficients. The transform coefficients $c = [c0, c1..cN - 1]$ when $p = [c0, c1, ..cN - 1]$ are derived as:

$$c = T_{DCT} \times P. \tag{20}$$

6.3.3. Sub-Sample Interpolation

In dealing with the luma and chroma components, High Efficiency Video Coding uses the same motion vectors. To reduce these effects and raise the level of precision, HEVC uses an increased dynamic range. In motion compensated prediction, a series of steps including filtering, dynamic range change, and horizontal or vertical shifting are performed in order to generate the prediction signal. Sub-sample locations are extracted using corresponding fixed

interpolation filters from the full-sample luma values in the case of luma sub-sample interpolation. The sub-sample location on the corresponding motion vector is determined using a modulo operation. A similar process is executed for the chroma sub-sample interpolation as for the luma sub-sample interpolation.

6.3.4. Mechanism of Power Measurement

Power spectrum is a representation of frequency components of a 2-D image. Hence for isolating the periodical structural features of an image or for decorrelating noise in the image, power spectrum estimation is critically important. It should be noted that the power spectrum is represented in log scale due to the fact that the power varies greatly in an image, by orders of magnitude. So, it becomes very easy to interpret and analyze the results in log scale. Since the power spectrum is represented with respect to frequency components, the image has to be converted to the frequency domain. Thus the first step in calculating the power spectrum of a 2-D image is to convert the image into the frequency domain which is done by the Fast Fourier Transform (FFT), which splits the signal into frequency bins. The frequency components which are farther away from the origin represent the higher frequency components. Different orientations of the features of image are represented by the different direction of the frequency components from the origin.

Steps involved in measuring the power spectrum of any image are:

(1) Load the image in MATLAB using the command imread.
(2) Since it is easier to analyze square images, if the image is not square then it is converted to square by truncating the largest dimension.
(3) The FFT is then taken for the squared image which converts the image from the spatial domain into the frequency domain.
(4) Taking the square of the modulus of the Fourier transform obtained from previous step.
(5) It is necessary to define some frequency coordinates to display the power spectrum.
(6) The log power spectrum can then be displayed using the function imagesc.

Power estimation is a very crucial task for advancements in designs. Speed and power is a trade off when the devices are used in real-time. Power estimation can be broadly categorized into pattern-dependent and pattern-independent. In the pattern-dependent method, the simulation results are considered for estimating the power dissipation. In this design we have adopted pattern-independent method i.e. many simulations were run in the design with different inputs and the average of the power dissipated was considered. The design is considered as a black box and the current and voltage values are considered from the design, in order to calculate power. This was achieved with the help of sensors and power blocks available in Simulink®. The design is simulated using the ode45 solver configuration, as shown in fig. 6.4.

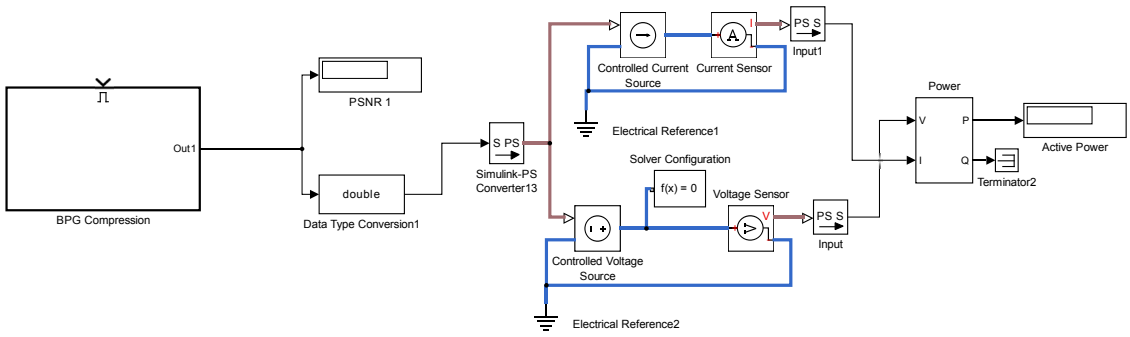


FIGURE 6.4. Mechanism of Power Measurement.

6.4. Experimental Results

The low-power architecture of SBPG implemented in MATLAB® /Simulink® Version 8.3 (R2014a), with the computer vision System Toolbox Version 9.7 [72]. The reason behind using MATLAB® is due to the fact that it provides a better understanding of the low-level implementation while Simulink® model provides a top-level functional like sensors and power blocks as well as dataflow visualization. With different spatial and frequency characteristics, five standard image are selected randomly from a set of Joint Picture Expert Graphics (JPG) images. For a sample image, the cover image and corresponding BPG image are shown in Fig. 6.6. Table 6.1 illustrates the related metrics for the baseline design, which presented

(a) cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 6.5. Secure BPG Compression of Wallpaper Image (128×128).

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 6.6. Secure BPG Compression of Resort Image (256×256).

in the chapter 5 and the proposed optimal design. The experimental results prove that the proposed-SBPG architecture is considered to be energy-efficient design with no significant effect on the quality comparing with the baseline design. It is observed that for almost the same PSNR, the power consumption of the optimal SBPG design is substantially reduced. Figures 6.10, 6.11, and 6.12 analyze and illustrate the related metrics for Wallpaper, Resort, Squirrel, Googlemap, and F16 images.

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 6.7. Secure BPG Compression of Squirrel Image (256×256).

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 6.8. Secure BPG Compression of GoogleMap Image (256×256).

(a) Cover Image. (b) Watermarked Image (c) Watermarked Compressed Image

FIGURE 6.9. Secure BPG Compression of F16 (512×512).

TABLE 6.1. Quality Metrics for the proposed architecture and Comparative Perspective with Baseline Design.

Test Image	SBPG Baseline Design		SBPG Optimal Design		Power Reduction
	PSNR	Power (nW)	PSNR	Power (nW)	
Wallpaper 128×128	50.2	8.09	49.31	6.63	18%
Resort 256×156	47.14	8.2	46.82	6.89	16%
Squirrel 256×256	50.37	8.22	50.19	6.85	17%
GoogleMap 256×256	48.09	8.3	47.5	6.90	17%
F16 512×512	51.9	8.55	50.03	6.94	19%

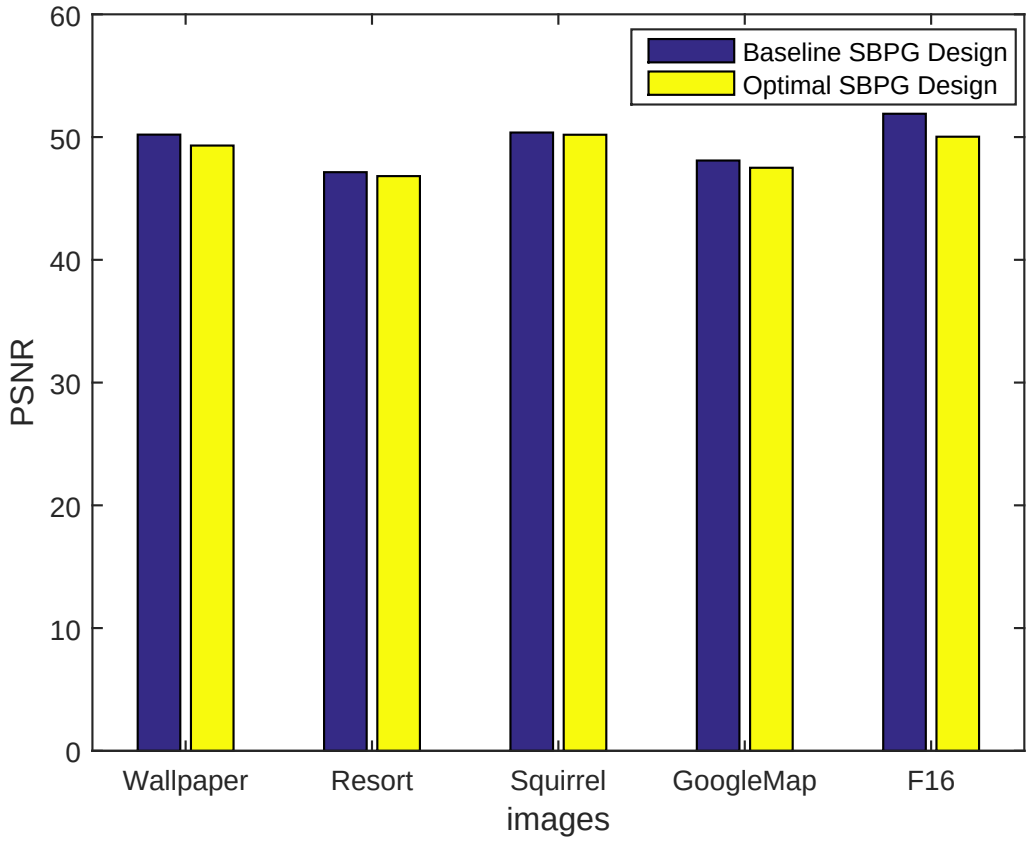


FIGURE 6.10. Comparison of Baseline SBPG with Final Optimal Design in Term of PSNR.

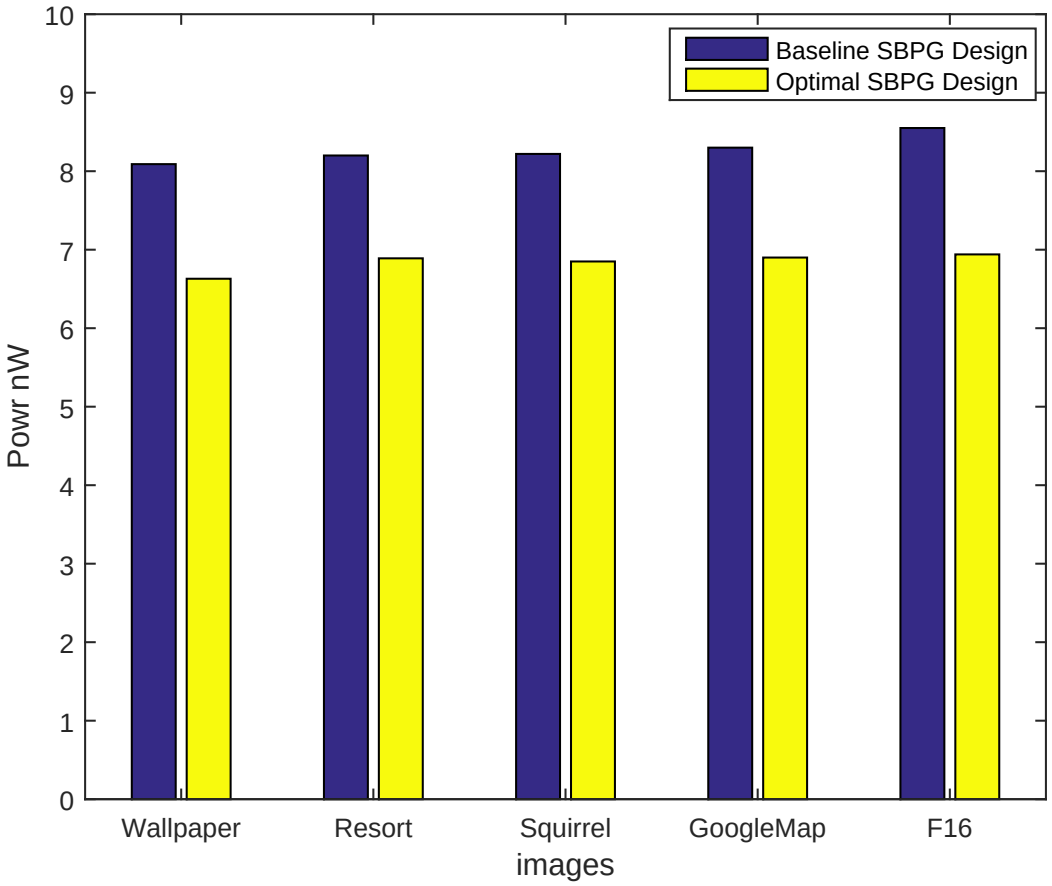


FIGURE 6.11. Comparison of Baseline SBPG with Final Optimal Design in Term of Power Consumption.

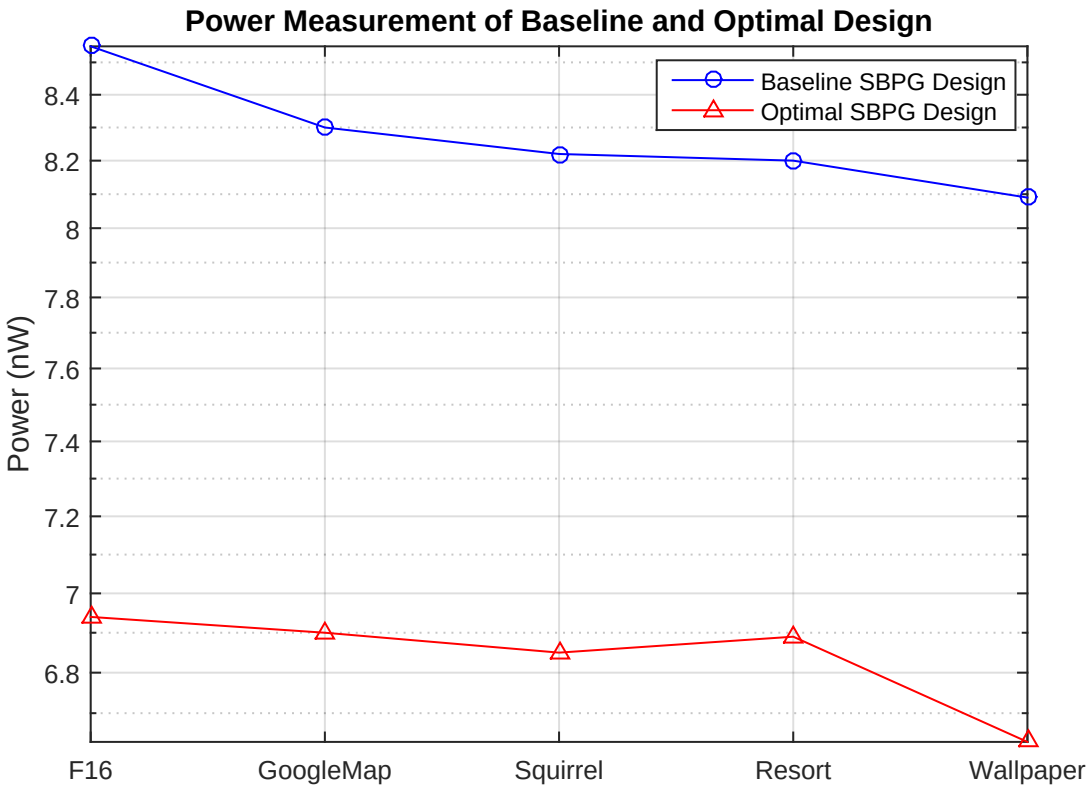


FIGURE 6.12. Comparison of Baseline SBPG with Final Optimal Design in Term of Power Consumption.

CHAPTER 7

CONCLUSIONS AND FUTURE RESEARCH

The effort in this dissertation contributes to the resolution of concerns related to the security and compression functions in image communication in the Internet of Things (IoT) due to the fast of evolution of IoT. The continuous expansion of the technology, broadband connectivity and the wide range of new devices in the IoT cause more concerns regarding privacy and security. In addition, in the IoT a key challenge regards the storage and the management of the massive data stream. For example, there is always a demand of acceptable size with highest quality of images to meet the rapidly increasing number of multimedia applications.

7.1. Summary and Conclusion

This research proposes new frameworks for secure image communication in the Internet of Things (IoT). The design flow of the proposed framework with experimental results is a top-down approach.

First in Chapter 3, the block diagram and the overview architecture of the secure digital camera in the IoT are highlighted. The objectives of the chapter are twofold. On the one hand, the proposed framework architecture offers double-layer of protection: encryption and watermarking that will address all issues related to security, privacy, and digital rights management (DRM). On the other hand, the chapter introduces a hardware architecture of the newly developed Better Portable Graphics (BPG) Compression, which is integrated with SDC. Thus, the proposed framework of SBPG integrated with SDC address all issues related to security, privacy and provides acceptable size with highest quality of the image. The above functions make the proposed SBPG suitable for high performance imaging in the IoT, such as Intelligent Traffic Surveillance (ITS) and Telemedicine, which are illustrated in the chapter.

The hardware architecture of BPG is presented in Chapter 4. The main objective of the chapter is to describe a hardware architecture of the BPG compression encoder. To

the best of the author's knowledge, this is the first ever proposed hardware architecture of BPG compression encoder. Prototype implementation of the algorithm based on Simulink® is implemented. The experimental results show experimental comparison and analysis of JPEG versus proposed architecture.

In Chapter 5, a prototyping development of a hardware architecture for secure BPG integrated with SDC, which is introduced in Chapter 3, is proposed and prototyped in Simulink®. To achieve a high performance architecture three techniques are considered; first, using the center portion of the image to insert the encrypted signature. Second, watermarking is done in the frequency domain using block-wise DCT of size 8×8. Third, in the BPG encoder, the proposed architecture uses inter and intra prediction to reduce the temporal and spatial redundancy.

The aim of chapter 6 is to optimize the SBPG baseline design, which is presented in chapter 5, to achieve an energy-efficient SBPG design. From the results presented in the chapter, it can be observed that with the same peak signal to noise ratio, the power consumption is substantially reduced, up to 19%.

7.2. Future Research

The secure BPG integrated with digital camera is proposed in this research. High efficiency, being the main target achieved in this research, could be achieved with low power consumption and smaller sizes with the implementation of this architecture. For future research, the proposed methodology could be extended to energy-efficient design of secure image sensors in the IoT communication that could be as wireless sensor framework. Further work could include designing the proposed SBPG in a hardware description language such as Verilog, then implementing it using Field Programmable gate Array (FPGA). Exploring mechanisms to integrate these SBPG and SDC in diverse Internet of Things (IoT) and smart cities applications is also future research [57, 29].

BIBLIOGRAPHY

[1] *Smarter Planet - United States*, http://www.ibm.com/smarterplanet/us/en/, 2016.

[2] Vivek Akkala, R. Bharath, P. Rajalakshmi, and Punit Kumar, *Compression techniques for IoT enabled handheld ultrasound imaging system*, Proceedings IEEE Conference on Biomedical Engineering and Sciences (IECBES), 2014, pp. 648–652.

[3] Saad Al-Azawi, Said Boussakta, and Alex Yakovlev, *High precision and low power DCT architectures for image compression applications*, Proceedings IET Conference on Image Processing, 2012, pp. 1–6.

[4] Salah S. Al-Majeed, Intisar S. Al-Mejibli, and Jalal Karam, *Home Telehealth by Internet of Things (IoT)*, Proceedings IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), 2015, pp. 609–613.

[5] U. Albalawi, S. P. Mohanty, and E. Kougianos, *A Hardware Architecture for Better Portable Graphics (BPG) Compression Encoder*, Proceedings of the 1st IEEE International Symposium on Nanoelectronic and Information Systems, 2015, pp. 291–296.

[6] 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*, Proceedings of the 15th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016.

[7] ———, *SBPG: A Secure Better Portable Graphics Compression Architecture for High Speed Trusted Image Communication in IoT*, Proceedings of the 17th IEEE International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE), 2016.

[8] Frdric Amiel, Boubacar Barry, Maria Trocan, and Marc Swynghedauw, *Real Time Image Compression for Eye Tracking Applications*, Proceedings 6th Latin American Symposium on Circuits & Systems (LASCAS), 2015, pp. 1–4.

[9] C. Anagnostopoulos, T. Alexandropoulos, V. Loumos, and E. Kayafas, *Intelligent traf-*

fic management through MPEG-7 vehicle flow surveillance, Proceedings IEEE International Symposium on Modern Computing, 2006, pp. 202–207.

[10] Pedram Azad, Tamim Asfour, and Rudiger Dillmann, *Combining Harris interest points and the SIFT descriptor for fast scale-invariant object recognition*, Proceedings IEEE/RSJ International Conference on Intelligent Robots and Systems, 2009, pp. 4275 – 4280.

[11] Ekaterina Balandina, Sergey Balandin, Yevgeni Koucheryavy, and Dmitry Mouromtsev, *IoT Use Cases in Healthcare and Tourism*, Proceedings IEEE 17th Conference on Business Informatics (CBI), 2015, pp. 37–44.

[12] Akanksha Bandil and K.V. Arya, *Multiple image sharing scheme for secure communication*, Proceedings 9th International Conference on Industrial and Information Systems (ICIIS), 2014, pp. 1–5.

[13] Alessandro Bardine, Pierfrancesco Foglia, Giacomo Gabrielli, and Cosimo Antonio Prete, *Analysis of Static and Dynamic Energy Consumption in NUCA Caches: Initial Results*, Proceedings the 2007 workshop on MEmory performance: DEaling with Applications, systems and architecture, 2007, p. 105112.

[14] Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva, *A DCT-domain system for robust image watermarking*, Elsevier the Single Processing 66 (1998), 357–372.

[15] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool, *SURF: Speeded Up Robust Features*, Computer Vision and Image Understanding 3 (2008), 346–359.

[16] F. Bellard, *The BPG Image Format*, `http://bellard.org/bpg/`, Last Accessed on 09/20/2015.

[17] Puja Bharti, Savita Gupta, and Rajkumari Bhatia, *Comparative Analysis of Image Compression Techniques: A Case Study on Medical Images*, Proceedings International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 820–822.

[18] Michael Bramberger, Josef Brunner, Bernhard Rinner, and Helmut Schwabach, *Real-*

time video analysis on an embedded smart camera for traffic surveillance, Proceedings 10th IEEE Real-Time and Embedded Technology and Applications Symposium, 2004, pp. 174 – 181.

[19] Anup W. Burange and Harshal D. Misalkar, *Review of Internet of Things in development of smart cities with data management & privacy*, Proceedings International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015, pp. 189–195.

[20] CeNSE, *HP Central Nervous System for the Earth (CeNSE)*, http://www8.hp.com/us/en/hp-information/environment/cense.html, 2013.

[21] Microsoft News Center, *Eye on Earth Enables Cloud-Based Environmental Data Sharing*, http://news.microsoft.com/2011/11/30/eye-on-earth-enables-cloud-based-environmental-data-sharing/, November 2011.

[22] Chi Ching Chi, Mauricio Alvarez-Mesa, Ben Juurlink, Gordon Clare, Felix Henry, Stephane Pateux, and Thomas Schierl, *Parallel Scalability and Efficiency of HEVC Parallelization Approaches*, IEEE Transactions on Circuits and Systems for Video Technology. 22 (2012), no. 12, 1827 – 1838.

[23] Shao-Yi Chien, Wei-Kai Chan, Yu-Hsiang Tseng, and Chia-Han Lee, *Distributed computing in IoT: System-on-a-chip for smart cameras as an example*, Proceedings 20th Asia and South Pacific Design Automation Conference (ASP-DAC), 2015, pp. 130–135.

[24] Karri Chiranjeevi, Dr.U.R Jena, Ch.Babji Prasad, and akulaTrinadh, *Comparative study of Image compression*, Proceedings International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015, pp. 1–6.

[25] Byeong C. Choi and Dong I. Seo, *A statistical approach for optimal watermark coefficients extraction in HVS-based blind watermarking system*, Proceding The 7th International Conference on Advanced Communication Technology, vol. 2, 2005, pp. 1085 – 1088.

[26] Michael Chui, Markus Loffler, and Roger Roberts, *The Internet of Things*,

http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things, March 2010.

[27] King-Hong Chung, Yuk-Hee Chan, Chang-Hong Fu, and Yui-Lam Chan, *A High Performance Lossless Bayer Image Compression Scheme*, Proceedings IEEE International Conference on Image Processing, vol. 2, 2007, pp. 353–356.

[28] DU Chunquan and ZHU Shunbing, *Research on Urban Public Safety Emergency Management Early Warning System based on Technologies for the Internet of Things*, International symposium on safety science and technology, Procedia Engineering 45 (2012), 748–754.

[29] Gavin Coelho, Elias Kougianos, Saraju P Mohanty, Prabha Sundaravadivel, and Umar Albalawi, *An iot-enabled modular quadrotor architecture for real-time aerial object tracking*, 2015 IEEE International Symposium on Nanoelectronic and Information Systems, IEEE, 2015, pp. 197–202.

[30] Louis Coetzee and Johan Eksteen, *The Internet of Things Promise for the Future An Introduction*, Proceedings IST-Africa Conference, 2011, pp. 1–9.

[31] Anand Darji, A.N.Chandorkar, S.N.Merchant, and Vipul Mistry, *VLSI Architecture of DWT Based Watermark Encoder for Secure Still Digital Camera Design*, Proceedings 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 760 – 764.

[32] Nagaraj Dharwadkar and B.B. Amberker, *Estimating the embedding capacity of a color image using Color Difference*, Seventh International Conference on Wireless And Optical Communications Networks (WOCN), 2010, pp. 1 – 5.

[33] Publication Publication (E-1.3.1), *Colorimetry, 2nd edition*, Central Bureau of the CIE, AustriaCIE Publication 15.2, 1986.

[34] Sara ElKerdawy, Ahmed Salaheldin, and Mohamed ElHelw, *Vision-based scale-adaptive vehicle detection and tracking for intelligent traffic monitoring*, Proceedings IEEE International Conference on Robotics and Biomimetics (ROBIO), 2014, pp. 1044 – 1049.

[35] G. Eysenbach, *What is e-health*, Journal of Medical Internet Research 3 (2001), no. 2.

[36] Elgar Fleisch, *What is the Internet of Things An Economic Perspective*, January 2010.

[37] Jessica Fridrich, Miroslav Goljan, and Nasir Memon, *Cryptanalysis of the Yeung-Mintzer fragile watermarking technique*, JOURNAL OF ELECTRONIC IMAGING 11 (2002), 262–274.

[38] Gartner, *Hype Cycles 2015 Research Report*, Tech. report, 2015.

[39] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, and Marimuthu Palaniswami, *Future Generation Computer Systems*, Elsevier the Future Generation Computer Systems 29 (2013), 1645–1660.

[40] Khamees Khalaf Hasan and Umi Kalthum Ngah, *Low complexity image compression architecture based on lifting wavelet transform and embedded hierarchical structures*, Proceedings IEEE International Conference on Control System, Computing and Engineering (ICCSCE), 2013.

[41] Safar Hatami, Shervin Sharifi, Hossein Ahmadi, and Mahmoud Kamarei, *Real-time image compression based on wavelet vector quantization, algorithm and VLSI architecture*, Proceedings IEEE International Symposium on Circuits and Systems, 2005, vol. 3, 2005, pp. 2381–2384.

[42] Jin-Maun Ho and Ching Ming Man, *The design and test of peripheral circuits of image sensor for a digital camera*, Proceedings IEEE International Conference on Industrial Technology, vol. 3, 2004, pp. 1351–356,.

[43] Leslie Horacek, *IoT: Will Ubiquitous Connectivity Mean Less Security?*, https://securityintelligence.com/iot-will-ubiquitous-connectivity-mean-less-security/, November 2014.

[44] Fang Hu, Dan Xie, and Shaowu Shen, *On the Application of the Internet of Things in the Field of Medical and Health Care*, Proveedings IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber Physical and Social Computing, 2013, pp. 2053 – 2058.

[45] Hongping Hu and Zhongyuan Zhao, *A Real-Time High Resolution Image Compression*

System Based on ADV212, Proceedings 2nd International Congress on Image and Signal Processing, 2009, pp. 1–4.

[46] Q. Huynh-Thu and M. Ghanbari, *Scope of Validity of PSNR in Image/Video Quality Assessment*, Electronics Letters, vol. 44, 2008, pp. 800 – 801.

[47] Rishabh Iyer, Rushikesh Borse, and Subhasis Chaudhuri, *Embedding capacity estimation of reversible watewatermark schemes*, Indian Academy of Science 39 (2014), 1357–1385.

[48] Jan Janak, Hyunwoo Nam, and Henning Schulzrinne, *On Access Control in the Internet of Things*, February 2012.

[49] M. Jridi and A. Alfalou, *A low-power, high-speed DCT architecture for image compression: Principle and implementation*, Proceedings IEEE/IFIP VLSI System on Chip Conference (VLSI-SoC), 2010, pp. 304–309.

[50] Med Lassaad KADDACHI, Leila MAKKAOUI, Adel SOUDANI, Vincent LECUIRE, and Jean-Marie MOUREAUX, *FPGA-based image compression for low-power Wireless Camera Sensor Networks*, Proceedings 3rd International Conference on Next Generation Networks and Services (NGNS), 2011, pp. 68–71.

[51] Hirokazu Kato and Marker Billinghurst, *Marker tracking and HMD calibration for a video-based augmented reality conferencing system*, Proceedings 2nd IEEE and ACM International Workshop on Augmented Reality, 1999, pp. 85–94.

[52] Shoji Kawahito, Dwi Haridoko, and Yoshiaki Tadokoro, *A CMOS image sensor with motion vector estimator for low-power image compression*, Proceedings the 16th IEEE Instrumentation and Measurement Technology Conference, vol. 1, 1999, pp. 65–70.

[53] Muhammad Usman Karim Khan, Muhammad Shafique, and Jorg Henkel, *Software Architecture of High Efficiency Video Coding for Many-Core System with Power-Efficient Workload Balancing*, Proceedings Automation and Test Design in Europe Conference and Exhibition (DATE), 2014, pp. 1–6.

[54] Ramsin Khoshabeh, Tarak Gandhi, and Mohan Trivedi, *Multi-camera Based Traffic*

Flow Characterization & Classification, Proceedings IEEE Intelligent Transportation Systems Conference ITSC, 2007, pp. 259 – 264.

[55] Hong-Sik Kim, Joohong Lee, Hyunjin Kim, Sungho Kang, and Woo Chan Park, *A Lossless Color Image Compression Architecture Using a Parallel Golomb-Rice Hardware CODEC*, IEEE Transactions on Circuits and Systems for Video Technology 21 (2011), no. 11, 1581–1587.

[56] N. M. Kosaraju, M. Varanasi, and S. P. Mohanty, *A High-Performance VLSI Architecture For Advanced Encryption Standard (AES) Algorithm*, Proceedings of the 19th International Conference on VLSI Design, 2006, pp. 481–484.

[57] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, *Design of a high-performance system for secure image communication in the internet of things*, IEEE Access 4 (2016), 1222–1242.

[58] K. Divya Krishna, Vivek Akkala, R. Bharath, P. Rajalakshmi, and Abdul Mateen Mohammed, *FPGA based preliminary CAD for kidney on IoT enabled portable ultrasound imaging system*, Proceedings IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), 2014, pp. 257–261.

[59] Phooi Yee Lau and Shinji Ozawa, *A secure distribution method for digitized image scan using a two-step wavelet-based technique: A Telemedicine Case*, Proceeding 27th Annual International Conference of the Engineering in Medicine and Biology Society, 2005, pp. 2228 – 2231.

[60] Shi lei Yan and Jian wei Sun, *Implementation and Optimization of H.264/AVC Encoder on Blackfin (ADSP-BF537) Processor*, Proceedings International Conference on Computational Intelligence for Modelling Control and Automation,and International Conference on Intelligent Agents,Web Technologies and Internet Commerce (CIMCA-IAWTIC), 2006, pp. 109–112.

[61] Benjamin Yee Shing Li, Lam Fat Yeung, and Kim Fung Tsang, *Analysing traffic condition based on IoT technique*, Proceedings IEEE International Conference on Consumer Electronics, 2014, pp. 1–4.

[62] Xiaofeng Li, Yi Shen, and Jiachen Ma, *An Efficient Medical Image Compression Scheme*, Proceedings 27th Annual International Conference of the Engineering in Medicine and Biology Society, 2006, pp. 3437–3439.

[63] Tony Lin and Pengwei Hao, *Compound image compression for real-time computer screen image transmission*, IEEE Transactions on Image Processing 14 (2005), no. 8, 993–1005.

[64] Cong Liu, Weiwei Shen, Tianlong Ma, Yibo Fan, and Xiaoyang Zeng, *A Highly Pipelined VLSI Architecture for All Modes and Block Sizes Intra Prediction in HEVC Encoder*, Proceeedings of IEEE 10th International Conference on ASIC (ASICON), 2013.

[65] R Loganathan and Y.S.Kumaraswamy, *An improved active contour medical image compression technique with lossless region of interest*, proceedings 3rd International Conference on Trendz in Information Sciences and Computing (TISC), 2011, pp. 128 – 132.

[66] Xiuqing Lu, Chen Ye, and Jian Yu andYaying Zhang, *A Real-Time Distributed Intelligent Traffic Video-Surveillance System on Embedded Smart Cameras*, Proceedings Fourth International Conference on Networking and Distributed Computing (ICNDC), 2013, pp. 51 – 55.

[67] MIT, *MIT Auto-ID Labs Laboratory Cloud of Things*, http://news.mit.edu/2012/auto-id-cloud-of-things-big-data, November 2012.

[68] Mihir Mody, Hrushikesh Garud, Soyeb Nagori, and Dipan Kumar Mandal, *High Throughput VLSI Architecture for HEVC SAO Encoding for Ultra HDTV*, Proceedings of IEEE International Symposium on Circuits and Systems, 2014.

[69] S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*, no. 9780071825719, McGraw-Hill Education, 2015.

[70] S. P. Mohanty, U. Choppali, and E. Kougianos, *Everything You wanted to Know about Smart Cities*, IEEE Consumer Electronics Magazine 6 (2016), no. 3.

[71] Saraju P. Mohanty, *A Secure Digital Camera Architecture for Integrated Real-Time*

Digital Rights Management, Elsevier Journal of Systems Architecture (JSA) 55 (2009), 468–480.

[72] Saraju P. Mohanty and Elias Kougianos, *Real-Time Perceptual Watermarking Architectures For Video Broadcasting*, Elsevier Journal of Systems and Software (JSS) 19 (2011), no. 12, 724 – 738.

[73] Saraju P. Mohanty, Nishikanta Pati, and Elias Kougianos, *A Watermarking Co-Processor for New Generation Graphics Processing Units*, Proceedings of the 25th IEEE International Conference on Consumer Electronics (ICCE), 2007, pp. 303–304.

[74] Saraju P Mohanty, N Ranganathan, and Karthikeyan Balakrishnan, *Design of a low power image watermarking encoder using dual voltage and frequency*, VLSI Design, 2005. 18th International Conference on, IEEE, 2005, pp. 153–158.

[75] Saraju P Mohanty, N Ranganathan, and Vamsi Krishna, *Datapath scheduling using dynamic frequency clocking*, VLSI, 2002. Proceedings. IEEE Computer Society Annual Symposium on, IEEE, 2002, pp. 58–63.

[76] Saraju P. Mohanty, Nagarajan Ranganathan, and Ravi K. Namballa, *A VLSI architecture for visible watermarking in a secure still digital camera (S/sup 2/DC) design*, Proceeding IEEE Transactions on Very Large Scale Integration (VLSI) System, vol. 13, 2005, pp. 1002 – 1012.

[77] Atahar Mostafa, Khan Wahid, and Seok-Bum Ko, *A low-power subsample-based image compression algorithm for capsule endoscopy*, Proceedings IEEE International Symposium on Circuits and Systems (ISCAS), 2012, pp. 109–112.

[78] Marta Mrak, Sonja Grgic, and Mislav Grgic, *Picture Quality Measures in Image Compression System*, Proceedings The IEEE Region 8 Computer as a Tool EUROCON, 2003, pp. 233–236.

[79] Sahasan Naraharisetti, *Region Aware Dct Domain Invisibile Robust Blind Watermarking For Color Images*, Master's thesis, Dept. of Computer Science and Engineering, University of North Texas, Denton, TX 76203, December 2008.

[80] H. OKUMURA, *Image compression if technologies for low power FPDs*, Proceedings IEEE International Conference on Consumer Electronics (ICCE, 2014, pp. 75–76.

[81] Songpol Ongwattanakul, Xianwei Wu, and David Jeff Jackson, *A new searchless fractal image encoding method for a real-time image compression device*, Proceedings International Symposium on Circuits and Systems, vol. 3, 2004, pp. 23–26.

[82] World Health Organization, *World Health Statistics 2013*, Tech. report, World Health Organization, 2013.

[83] Boris Pokric, Srdan Krco, and Maja Pokric, *Augmented Reality Based Smart City Services Using Secure IoT Infrastructure*, Proceedings 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2014, pp. 803–808.

[84] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and U. Choppali, *Wireless Sensor Network Simulation Frameworks: A Tutorial Review*, IEEE Consumer Electronics Magazine 6 (2016), no. 2, 63–69.

[85] Mohammad Rashid, Luca Ardito, and Marco Torchiano, *Energy Consumption Analysis of Image Encoding and Decoding Algorithms*, Proceedings IEEE/ACM 4th International Workshop on Green and Sustainable Software (GREENS), 2015, pp. 15–21.

[86] Shahid Raza, Linus Wallgren, and Thiemo Voigt, *SVELTE: Real-time intrusion detection in the Internet of Things*, Elsevier Ad Hoc Networks 11 (2013), no. 8, 26612674.

[87] Francesco Rizzo, Bruno Carpentieri, Giovanni Motta, and James A. Storer, *Low-Complexity Lossless Compression of Hyperspectral Imagery via Linear Prediction*, Proceedings IEEE Signal Processing Letters, vol. 12, 2005, pp. 138–141.

[88] Zenonas Rokus Rudzikas, *Internet of Things - An action plan for Europe*, http://www.eesc.europa.eu/i=portal.en.ten-opinions.18007, December 2009.

[89] Hetul Sanghvi, *Low power architecture for motion compensation in a 4K Ultra-HD AVC and HEVC video codec system*, Proceedings IEEE Second International Conference on Image Information Processing (ICIIP), 2013, pp. 400 – 404.

[90] Kishor Sarawadekar and Swapna Banerjee, *Area Efficient, High-speed VLSI Design*

for Ebcot Block Coder in JPEG 2000, Proceedings of International Conference on Electronics and Information Engineering (ICEIE), vol. 2, 2010, pp. V2–110 – V2–113.

[91] S.C.Ramesh and M. Mohamed Ismail Majeed, *Implementation of a visible watermarking in a secure still digital camera using VLSI design*, Proceedings AFRICON, 2009, pp. 1 – 4.

[92] Muhammad Shafique and Jrg Henkel, *Low power design of the next-generation High Efficiency Video Coding*, Proceedings 19th Asia and South Pacific Design Automation Conference (ASP-DAC), 2014, pp. 274 – 281.

[93] Muhammad Shafiquea, Muhammad Usman Karim Khan, and Jrg Henkel, *Power Efficient and Workload Balanced Tiling For Parallelized High Efficiency Video Coding*, Proceedings IEEE International Conference on Image Processing, 2014, pp. 1253 – 1257.

[94] Hamid Sheikh, Muhammad Sabir, and Alan Bovik, *A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms*, IEEE Transactions on Image Processing 15 (2006), 1057–7149.

[95] Yu Shen, Xieping Gao, Linlang Liu, Caixia Li, and Qiying Cao, *Integer to integer multiwavelets for lossless image compression*, Proceedings 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), 2011, pp. 217–221.

[96] Chen Shoushun, Amine Bermak Wang Yan, and Dominique Martinez, *Adaptive-Quantization Digital Image Sensor for Low-Power Image Compression*, IEEE Transactions on Circuits and Systems 45 (2007), no. 1, 13–25.

[97] Ghanapriya Singh, *A generalized contrast enhancement algorithm for seamless high contrast image across devices in Internet of Things*, Proceedings International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 294–298.

[98] Jaehyuk So, Kyungmook Oh, , and Jaeseok Kim, *Design and verification of intra prediction hardware for video streaming in IoT systems*, Proceedings International SoC Design Conference (ISOCC), 2015, pp. 283–284.

[99] Gary J. Sullivan, Jens-Rainer Ohm, Woo-Jin Han, and Thomas Wiegand, *Overview of the High Efficiency Video Coding (HEVC) Standard*, IEEE Transactions on Circuits and Systems for Video Technology 22 (2012), 1649 – 1668.

[100] Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelffl, *Vision and Challenges for Realising the Internet of Things*, Tech. report, European Commission, 2010.

[101] Vivienne Sze, Madhukar Budagavi, and Gary J Sullivan, *High Efficiency Video Coding (HEVC) : Algorithms and Architectures*, no. 9783319068947, Springer, 2014.

[102] Thiow Keng Tan, Rajitha Weerakkody, Marta Mrak, Naeem Ramzan, Vittorio Baroncini, Jens-Rainer Ohm, and Gary J. Sullivan, *Video Quality Evaluation Methodology and Verification Testing of HEVC Compression Performance*, IEEE Transactions on Circuits and Systems for Video Technology 26 (2016), no. 1, 76–90.

[103] David Taubman, *High Performance Scalable Image Compression with EBCOT*, IEEE Transactions on Image Processing 9 (2000), no. 7, 1158–1170.

[104] Lei Tian and Heng Ming Tai, *Secure Images Captured by Digital Camera*, Proceedings International Conference Consumer Electronics, 2006, pp. 341 – 342.

[105] S.L. Ting, S.K. Kwok, Albert Tsang, and W.B. Lee, *Enhancing the information transmission for pharmaceutical supply chain based on Radio Frequency Identification (RFID) and Internet of Things*, Proceeedings 8th International Conference on Supply Chain Management and Information Systems (SCMIS), 2010, pp. 1–5.

[106] D. Vaithiyanathan and R. Seshasayanan, *Low power DCT architecture for image compression*, Proceedings International Conference on Advanced Computing and Communication Systems (ICACCS), 2013, pp. 1–6.

[107] Zainab Nazar Khalil Wafi, R.Badlishah Ahmad, and Paulraj M.P, *Highways Traffic Surveillance System (HTSS) using OpenCV*, Proceedings IEEE Control and System Graduate Research Colloquium (ICSGRC), 2010, pp. 44 – 48.

[108] G. K. Wallace, *The JPEG Still Picture Compression Standard*, IEEE Transactions on Consumer Electronics 38 (1992), no. 1, xviii–xxxiv.

[109] Ze Wang, Tianxu Zhang, Luxin Yan, and Cheng Gong, *A High Performance Fully Pipelined Architecture for Lossless Compression of Satellite Image*, Proceedings International Conference on Multimedia Technology (ICMT), 2010, pp. 1–4.

[110] Zhe Wang, Anto Y. Michael, Simeon Wahl, Philipp Werner, and Sven Simon, *A memory efficient parallel lossless image compression engine for high performance embedded systems*, Proceedings 7th International Symposium on Image and Signal Processing and Analysis (ISPA), 2011, pp. 390–395.

[111] Zhou Wang, Bovik A.C, Sheikh H.R, and E.P Simoncelli, *Image quality assessment: from error visibility to structural similarity*, IEEE Transactions on Image Processing 13 (2004), 1057–7149.

[112] Mathias Wien (ed.), *High Efficiency Video Coding (HEVC) CCoding Tools and Specification*, Springer International Publishing, 2014.

[113] Cort J. Willmott and Kenji Matsuura, *Advantages of the Mean Absolute Error (MAE) over the Root Mean Square error (RMSE) in assessing average model performance*, Proceedings Climate Research, vol. 30, 2005, p. 79 82.

[114] Chen-Mie Wu, Dah-Jyh Perng, Wen-Tsung Cheng, and Jian-Shing Ho, *A high-performance system for real-time video image compression applications*, Proceedings IEEE Transactions on Consumer Electronics, vol. 41, 1995, pp. 125–131.

[115] Jiangming Wu, Wenrui Dai, and Hongkai Xiong, *Regional context model and dynamic Huffman binarization for adaptive entropy coding of multimedia*, Proceedings IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2014, pp. 1 –6.

[116] Chunlin Xia, Deyun Zhou, and Kun Zhang, *Embedded real time image compression module for data link*, Proceedings International Conference on Automatic Control and Artificial Intelligence (ACAI), 2012.

[117] Li Yu, Guangtao Fu, Aidong Men, Binji Luo, and Huiling Zhao, *A novel motion compensated prediction framework using weighted AMVP prediction for HEVC*, Proceedings Visual Communications and Image Processing (VCIP), 2013, pp. 1–6.

[118] Dajiang Zhou, Jinjia Zhou, Wei Fei, and Goto S., *Ultra-High-Throughput VLSI Architecture of H.265/HEVC CABAC Encoder for UHDTV Applications*, Proceedings of IEEE Transactions on Circuits and Systems for Video Technology, vol. 25, 2014, pp. 497 – 507.

[119] Jiantao Zhou, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, *Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation*, IEEE Transactions on Information Forensics and Security 9 (2013), no. 1, 39–50.