Arab American University

Faculty of Graduate Studies

An Enhanced Encryption Scheme for Wireless Visual Sensor Networks

By

Kefaya Tayseer Sabaneh

Supervisor

Prof. Adwan Yasin

This thesis was submitted in partial fulfillment of the requirements for the Master's degree in Computer Science

July/ 2018

An Enhanced Encryption Scheme For Wireless Visual Sensor Networks

By

Kefaya Tayseer Sabaneh

This thesis was defended successfully on ……and approved by:

Committee members	Signature
1. Supervisor Name: Prof. Adwan Yasin	.....
2. Internal Examiner Name: Dr. Muath Sabha	.....
3. External Examiner Name: Dr. Rushdi Hamamreh	.....

Declaration

This is to declare that the thesis entitled “An Enhanced Encryption Scheme for Wireless Visual Sensor Networks" under the supervision of Prof. Adwan Yasin is my own work and does not contain any unacknowledged work or material previously published or written by another person, except where due reference is made in the text of the document.

Date: 7/7/2018

Name: Kefaya Tayseer Sabaneh Signature:

Dedication

This thesis is wholeheartedly dedicated to my husband (Mutaz), who has been a constant source of support and encouragement during this challenge.

To my little kids (Jood and Ahmed), whom I am truly grateful for having in my life.

To my family and friends who have always loved me unconditionally.

Acknowledgments

Firstly, I would like to express my sincere gratitude to my supervisor Prof. Adwan Yasin for his continuous support and engagement.

Besides, I would like to express my love, appreciation and profound gratitude to my family: my parents, my husband, my mother-in-law and my father-in-law for providing me with unfailing support and continuous encouragement through the process of researching and writing this thesis.

Huge thanks, to my special friends: Shafaq Abulhof, Dhua Shebani, Ansar Kmail, Najla Alshayeb, Wafaa Zakarneh and Abeer Zaroor for their unconditional support and love.

Thanks for all your encouragement

Abstract

Wireless Sensor Networks (WSNs) are increasingly gaining attention. Recent improvements in WSN that are represented by the incorporation of camera sensor nodes in Wireless Visual Sensor Network (WVSN) has attracted the employment of the technology in a broad range of new monitoring and tracking systems. The diversity in these systems demands various and variable security requirements. Accordingly, several approaches have been presented to address the issue of image security in WVSN.

To assure the main security requirements in the constrained WVSN nodes, conventional cryptographic algorithms have been studied deeply to investigate their applicability and performance implications, including their computational overhead, required storage and energy consumption. Moreover, to overcome the inability of these algorithms to provide real time image encryption, and due to the bulky data size in WVSN compared with scalar data, new approaches in image encryption have been proposed, including discretized chaotic based image crypto-systems and modified conventional crypto-systems. In addition to that, to address the problem and reduce the required resources, other approaches have employed partial (selective) image encryption to reduce the amount of the encrypted content, and prolong the network lifetime as a whole .

In this work, we tackle the issue of image encryption in WVSN using an enhanced image encryption scheme (EIES) in which a modified AES algorithm is employed to encrypt images within WVSN adaptively, according to the application requirements. In the first version of EIES we have employed a modified AES in CBC mode of operation using a chaotic based bit-level permutation step. We have evaluated the security of the our scheme using several security analysis including the key space analysis, key

sensitivity analysis, statistical and differential analysis. In addition to that, we have calculated the encryption algorithm's runtime, and compared it with other recent schemes to show the superior enhancement incorporated by our scheme. Accordingly, the obtained security analysis provided comparable results with respect to other works from the state-of-the-art with a reduced execution time. Most of the available works in the domain of image encryption in WVSN including the EIES in its first version suffer from the unstable resistance against differential attack. Based on that, in the second version of our scheme the combination between bidirectional partial image encryption, chaotic-based bit level permutation, and AES in CBC mode of operation guarantees the security of the transmitted images, with a reduced resource consumption, and minimized encryption time. Based on the conducted security analysis, EIES in its second version has proven its ability to provide an enhanced diffusion property, and resist against several statistical and differential attacks, in addition to brute force attacks. Also, our scheme provides a significant reduction in the encryption time to 14% of the time required for the original AES-128 encryption algorithm.

Table of Contents

List of Figures

List of Tables

List of Equations

List of Abbreviations

ADC – Analog to Digital Convertor

AES – Advanced Encryption Standard

CBC – Cipher Block Chaining

CFB – Cipher Feedback

CPU – Central Processing Unit

DCT – Discrete Cosine Transformation

DoS – Denial of Service

DWT – Discrete Wavelet Transformation

ECB – Electronic Codebook

EBCOT – Embedded Block Coding with Optimized Truncation of the Embedded Bit-Stream

EZW – Embedded Zerotree Wavelet

FoV – Field of View

HD – High Definition

JPEG – Joint Photographic Expert Group

LAN – Local Area Network

MAD – Mean Absolute Difference

MATLAB – Matrix Laboratory

NIST – National Institution of Standards and Technology

NPCR – Number of Changing Pixel Rate

NSA – National Security Agency

OFB – Output Feedback

PDA – Personal Digital Assistant

PRNG – Pseudo Random Number Generator

PWLCM – Piecewise Linear Chaotic Map

QoS – Quality of Service

RC5 – Rivest Cipher 5

RC6 – Rivest Cipher 6

RF – Radio Frequency

SPECK – Set Partitioned Embedded Block

SPIHT – Set Partitioning in Hierarchical Trees

UACI – Unified Averaged Changed Intensity

WMSN – Wireless Multimedia Sensor Network

WSN – Wireless Sensor Network

WVSN – Wireless Visual Sensor Network

XXTEA – Corrected Block Tiny Encryption Algorithm

1. Introduction

In the recent years, various surveillance and monitoring systems tended to use WVSN to enhance their operations. Assuring image security within WVSN is a broad research domain that remains one of the most important and challenging tasks, because of the different security requirements that need to be satisfied, and the limited available resources within the sensor nodes.

To address this challenge, cryptography is the most used security mechanism to guarantee the authenticity, integrity and data confidentiality. According to WVSN, the scenario of image data encryption is more complicated than in the scalar WSN. This is related to the inherited features from WSN which are represented by the limited available power, memory and processing capabilities. Moreover, compared with scalar data; image is characterized by its bulky data size, high correlation between adjacent pixels and high pattern redundancy property [1, 2].

In order to provide a trustworthy security level for the transmitted images in WVSN with a reduced resources consumption, several researches studied the applicability of the conventional cryptographic algorithms for image encryption. On the other hand, other works shifted to develop new lightweight algorithms, to address the tradeoff between image security and resource consumption [3].

Starting from this point, we propose developing a comprehensive crypto-system that can provide secure image transmission with a reduced resources consumption. This is accomplished by the adoption of an adaptive encryption scheme, that has the ability to encrypt image content fully or partially according to the sensing relevance of the visual

sensor. Besides, we present a robust hybrid encryption algorithm that integrates the strengths of AES-128 algorithm, chaotic bit level permutation and bidirectional encryption to guarantee robust confusion and diffusion properties, while reducing the algorithm's execution time effectively.

The remainder of this chapter is ordered as follows. The background and motivations behind our proposed security scheme are presented in Section 1.1. In Section 1.2, we present the problems and constraints that are associated with the existing image cryptographic schemes in WVSN. Section 1.3 provides our research methodology. Section 1.4 outlines our contributions and clarifies the shortcomings that we attempt to overcome through the proposed scheme. At last, we present the structure of our thesis in section 1.5.

1.1. Background and Motivations

The capabilities of WVSN in image capturing and transmission have made it a reliable candidate to replace the traditional monitoring systems. Various applications have different security necessities that are determined by the sensitivity of the captured scenes. Because of that, three main approaches were followed to achieve the main security requirements in WVSN: In the first approach, they employed conventional encryption algorithms to hide image content [4]. The main drawback of such works is related to its high computational complexity, and long execution time. As a consequent, in the second approach the modification of the available standard encryption algorithms was exploited to provide a suitable balance between the provided security level in one hand, and resource consumption in the other hand [1, 5, 6]. In the third approach several

efforts were exerted to prolong the network lifetime and propose new lightweight encryption algorithms [7-9]. Even the second and third approaches have proven its ability to reduce the resource consumption and decrease the encryption time, but a reduced security level is obtained. Not far from that, new approaches have utilized the combination between image compression and encryption, to reduce the amount of the encrypted data and accordingly, reduce the required resources for image encryption [10, 11].

Motivated by these works, we develop a new security scheme for image encryption in WVSN, that has the ability to be adapted to the application requirements based on the node's sensing relevance. Different from previous works in the scope of image encryption in WVSN, the proposed algorithm outperforms conventional encryption algorithms such as AES while reducing the algorithm's execution time and related resources draining. Moreover, the application of the original AES for image encryption presents new obstacles including the high pattern redundancy property in the encrypted image and weak defense against some differential attacks. To meet these problems, we propose to execute a modified AES encryption algorithm with an enhanced diffusion property and reduced execution time using: Cipher Block Chaining (CBC) mode of operation, chaotic based bit-level permutation and bidirectional encryption order.

1.2. Problem Statement and Research Questions

As we explained in the previous section, various encryption algorithms have been employed to guarantee the security of the captured images in WVSN considering the computational complexity of those algorithms in addition to their operation cost and memory requirements. Available algorithms were categorized to either security aware

algorithms, or resource aware algorithms. Little approaches tried to achieve the tradeoff between resources consumption and security requirements in the constrained visual sensor nodes .

In this section, we introduce the research questions that we try to investigate and address throughout our research.

- What are the obstacles that encounter the application of an encryption algorithm to encrypt images in visual sensors?

To answer this question, we presented an overview about the components, applications, requirements and challenges that distinguish WVSN.

- What are the shortcomings and strengths in the available algorithms that are used for image encryption in WVSN?

To answer this question, we provided a comparative study for the available encryption algorithms in both WSN and WVSN considering both; its security evaluations and performance implications.

- How to provide a robust encryption algorithm while prolonging the network lifetime as much as we can?

To tackle this issue, we propose an adaptive security scheme based on the bidirectional modified CBC-AES algorithm, using Chirikov standard chaotic map bit level permutation. Our research work aims to provide an adaptive security level according to the visual node sensing relevance, while reducing the encryption time, and prolonging the network lifetime as a whole.

- How to evaluate the performance and security of the proposed security scheme, and how to prove its reliability compared with other schemes that have been presented for image encryption in WVSN?

In order to answer this question, first we have employed MATLAB_R2016a to encrypt a set of standard test images using the proposed algorithm and other recent algorithms. After that, we state and clarify the different security and performance analysis that we will use to evaluate the proposed scheme, and compare its results with other algorithms in the state-of-the-art. Results for statistical analysis, differential analysis, key space, sensitivity analysis and encryption time are presented to indicate the strengths of our scheme.

1.3. Research Methodology

In the following, we state the main phases that we followed in our research work:

- **Image significant part selection**

At this phase, the amount of the image details that will be encrypted later in the encryption phase is selected using Discrete Wavelet Transform (DWT) based compression for partial encryption. On the other hand, full image size is kept for high security necessities. Visual nodes are prioritized dynamically or statically according to their sensing relevance within the monitored field. Consequently, the size of the encrypted image has a proportional relationship with the node's sensing relevance.

- **Reduce the computational complexity and execution time of the diffusion step**

One of the main obstacles that prevent the use of the original AES algorithm for image encryption in WVSN is related to the MixColumns transformation which requires high

computational overhead and consumes considerable runtime. To provide a comparable diffusion step with a reduced computations and execution time, we replace the MixColumns transformation with a chaotic based bit level permutation step that shuffles the block bits in the most significant four bit-planes chaotically.

- **Pattern redundancy removal**

Images are featured by their high redundancy property. For an input image that contains identical gray scale regions, some patterns will occur within the ciphered image in the same areas. To tackle this issue, we apply the modified AES algorithm in CBC mode. Such that redundant pixels are affected by other pixels in the previous ciphered block and hence different pattern will appear in the ciphered image.

- **Diffusion property enhancement**

In version 1 of our work the previous modifications are applied on the original AES-128 while keeping other parameters unchanged. It provides robust confusion and diffusion properties, with a minimized execution time compared with the original AES. However, according to the evaluation results, applying the conventional one-directional block encryption provides unstable resistance against differential attacks. To meet this problem, we apply the encryption algorithm in a bidirectional manner to provide a stable defense against differential attacks.

1.3.1. Cryptographic Scheme Evaluation

To evaluate the proposed encryption scheme, we use a set of well known analysis that are used for security and execution time evaluation. For security analysis, we provide the key space analysis, key sensitivity analysis, differential and statistical analysis. Mean Absolute Difference (MAD) is used to show that changing one bit in the secret

key should produce a completely different cipher image. For the differential analysis; Number of Changing Pixel Rate (NPCR), and Unified Averaged Changed Intensity (UACI) are the main two examined parameters. Finally for the statistical analysis, several metrics are tested including the image entropy, image histogram, correlation analysis and scene visibility. To evaluate the performance of our scheme, the algorithm's execution time is calculated and compared with other recent algorithms [4-6]. Obtained results indicate the ability of the encryption algorithm to resist against various attacks and provide completely hidden image content, with a minimized execution time.

1.4. Contribution

The main contribution of our research work lies in the followings:

- **Proposing an adaptive security scheme that is based on the sensing relevance of the visual nodes in WVSN**

The incorporation of different image quality/security levels within the proposed scheme, allows to prioritize different sensing nodes, with several image quality and security requirements. Usually, more critical data are observed in specific spatial area within the monitored field. Additionally, high quality reconstructed image is required in this area. To tackle these challenges, we provide four main security levels that can be attached to the visual nodes according to its sensing relevance. Most of the sensor nodes are likely to adopt moderate security level and so, a reduced execution time is required to encrypt observed scenes due to the partial encryption. Other sensor nodes have either high security requirements or low security requirements. Accordingly, a proper security level

is applied. Our scheme has the ability to provide several security levels, prolong the network lifetime and encrypt images with a reduced execution time.

- **Enhance the operation of the original AES-128 algorithm for image encryption in WVSN**

The followings are the modifications we conduct to enable an efficient application of the original AES-128 encryption algorithm:

1. To tackle the image's pattern redundancy issue and the weak diffusion property using the AES in Electronic Codebook mode of operation (ECB), we use CBC cipher mode to spread the pixel values within each ciphered block to other blocks.
2. To reduce the execution time of the Mix columns transformation, we replace it by another chaotic-based bit level permutation step that shuffles bits in the four most significant bit-planes chaotically based on Chirikov standard map. In addition to the execution time reduction, the use of the secret chaotic parameters extends the obtained key space and hence provides additional complexity for the execution of brute force attack.
3. To afford a stable diffusion property and resist against differential attacks, we apply the modified AES algorithm (modified using the previous steps 1 and 2) in a bidirectional way, keeping the number of the algorithm's rounds unchanged.

1.5. Structure of the Thesis

The rest of our thesis is organized as follows. Chapter 2 presents a background about the Wireless Multimedia Sensor Network (WMSN) and WVSN, including their components, applications and challenges. In addition to that, we introduce a comprehensive comparative study for the existing image encryption algorithms in the

context of WSN and WVSN from both performance and security views. The proposed security scheme is presented in chapter 3. In chapter 4, we present the security analysis and evaluate the performance of the proposed security scheme with respect to its operation cost. We also compare between the results produced by our algorithm and another three recent works from the state-of-the-art image encryption algorithms in WVSN. At last, in Chapter 5, we provide the conclusions and present the future enhancements and extensions of our research.

2. Background and Literature Review

The aim of this chapter is to present a survey that covers several topics in the scope of WSN. First, we provide a background about WMSN, its components, architectures and applications. Then we move to a special part of the multimedia networks which is WVSN. We discus its challenges and requirements. After that we clarify the issue of image security in WVSN, focusing on the image encryption approach. Finally, a comprehensive comparative study about the security and performance analysis of the existing image encryption algorithms in WVSN is presented.

2.1. Background

WSN is a rising technology, due to its beneficial characteristics, and wide range applications in different domains. Using WSN, various environmental conditions are monitored, recorded and collected to be organized at a central location [12]. Actually, WSN has played an essential role in smart city owing to its low cost and wide coverage capabilities, while providing useful readings that help supervisors to analyze the collected data and make appropriate decisions [13].

2.1.1. Wireless Multimedia Sensor Networks

The emergence of WMSNs is an evolutionary step for WSN. In addition to scalar sensors; audio and visual sensors are integrated into wireless sensor nodes (also called motes). As a result, the applications of WSN has been extended to additional areas in which visual and audio data reveals more information than scalar data [2].

2.1.2. Wireless Multimedia Sensor Network Components

The general structure of the WMSN is shown in Figure 1 It includes the following main components; wireless multimedia sensor node, wireless cluster head, wireless network

node and a base station. Similar to scalar WSN, WMSN nodes form the endpoints of the network. Each sensing node in the network contains four main units; a sensing unit, a processing unit, a power unit and a transmission unit. Each unit within the node is responsible for a specific duty to facilitate data gathering and transmission within the network [14, 15].

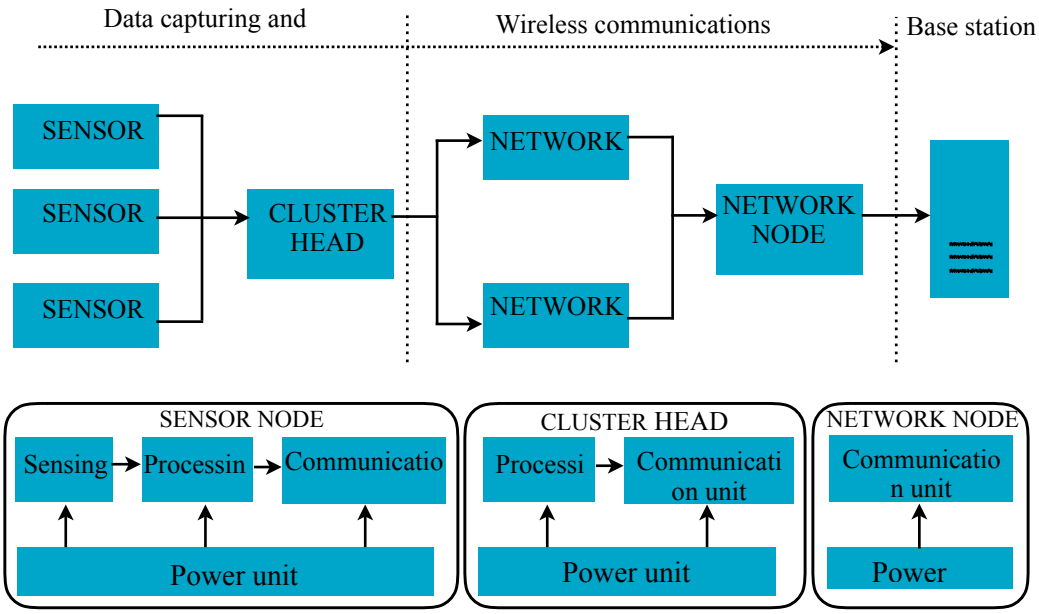


Figure 1. General structure of WMSN

- **Sensing unit**

It has one sensor or more to capture the environmental measurements. The sensor is equipped with a visual or audio capturing unit and is responsible for gathering a specific type of data. In the scope of WVSN, each camera sensor has a Field of View (FOV) of the scene, and the captured scene is called an image frame. Since the captured data is analog, an analog to digital convertor (ADC) is necessary to convert the gathered measurements to digital signals. These signals are the input to the node's processing unit [15].

- **Processing unit**

It contains a microprocessor to process obtained digital signals gathered by the sensing units and produce valuable information. The processing unit is responsible for performing the visual data processing to reduce the high amount of the captured scene data. Two approaches can be employed here; the first approach uses an event driven detector to identify useful events in the scene. If no event is detected then the image frame is discarded and not transmitted through the network. Furthermore, the second approach utilizes event compressors to reduce the amount of data in the captured image frames; hence, less amount of data is transmitted through the network. In addition to the microprocessor, there is a memory unit included in the processing unit that is used to store the processed data locally to be transmitted later [14].

- **Power unit**

This unit is responsible for the regulation of the power to and from a portable energy storage unit such as a battery.

- **Communication unit**

It contains a short range transceiver that is responsible for the transmission of data to and from the sensing node. Radio frequency (RF) based protocols are the most common communication methods in WMSN because they take into account the limited power supply, and the need for a short range transmission requirements. IEEE 802.11 wireless Local Area Network (LAN) Wi-Fi, Bluetooth and IEEE 802.15.4 (ZigBee) standards satisfy the previous requirements [15].

The second component in the WMSN is the wireless cluster head. It is composed of a processing unit, communication unit and power unit. Each cluster head is responsible for the aggregation of data gathered by several sensor nodes. Since the FOV for

different camera sensors in the network may overlap, cluster head can perform additional processing to consolidate redundant data.

Finally, the destination of all gathered data is the base station. It is equipped with powerful processing capabilities, and a main power supply to perform its operation [14, 16].

2.1.3. Wireless Multimedia Sensor Network Architectures

WMSN has various architectures and classifications. As illustrated in Figure 2 in terms of its composition, it can be homogeneous or heterogeneous. In terms of its tier architecture, it can be single-tier or multi-tier. Finally, in terms of its mote platform architectures, it is classified to lightweight-class, intermediate-class or Personal Digital Assistant (PDA)-class [14, 15].

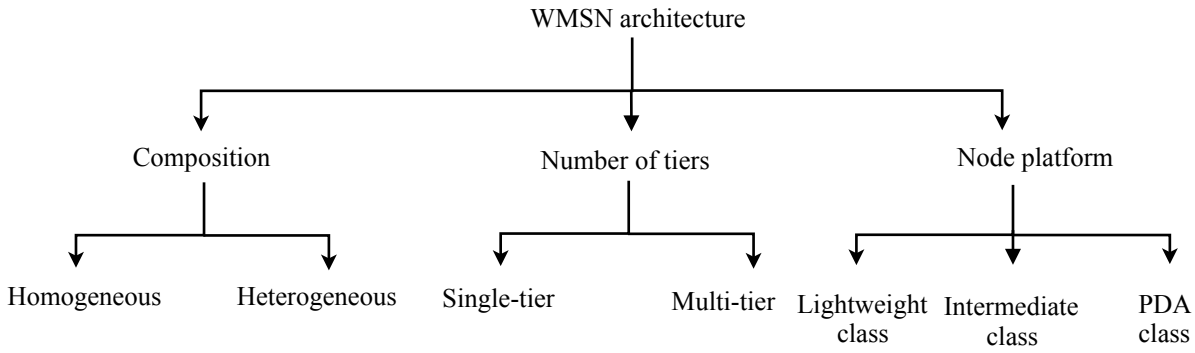


Figure 2. WMSN architecture classification

Homogeneous WMSN contains a collection of nodes with the same capabilities in terms of energy, storage and computation. On the other hand, heterogeneous architecture includes nodes with different capabilities [17]. Nodes that have better capabilities can be used for the cluster head nodes in order to improve its energy efficiency, and thus prolong the network lifetime.

According to the tier architecture, a single-tier architecture is based on flat network topology with either homogeneous or heterogeneous nodes. Differently, multi-tier architecture uses the nodes with higher processing, power and communication capabilities as high-end nodes to form a hierarchal network [18]. Compared with the flat architecture, Hierarchal network architecture is more commonly used in WMSN since it can balance the traffic load through the clustering concept and data aggregation, optimize the energy consumption within the network and improve scalability when the network grows .

Wireless node platform architectures are categorized into three main categories depending on the available resources (processing power and storage) in the node. Lightweight class platforms have low processing power capabilities, small storage and basic communications [19]. An example of the lightweight class platform is FireFly node. Intermediate-class platforms have better computational processing power and more storage size, but they are usually equipped with basic communications. An example of the intermediate class node platform is the TelosB. Finally, PDA-class platforms such as Stargate node have more powerful processing capability and larger storage. Table 1 provides a detailed comparison between different node architectures in terms of processing power and available storage [14].

Table 1. Comparison of node platforms in WMSN

Platform	Node	Microcontroller	RAM	Flash memory
Lightweight	FireFly	8-bit ATmega128L	8 kB	128 kB
Intermediate	TelosB	16-bit TI MSP430	10 kB	1MB
PDA-class	Stargate	32-bit PXA255 XScale	64 MB	32 MB

Usually, WMSNs are designed with heterogeneous multitiered architecture using the proper mote class according to the application requirements. Due to the large size of the multimedia content, intermediate mote class and PDA-class are more commonly used [14].

2.1.4. Wireless Multimedia Sensor Network Applications

WSNs can be employed in various monitoring systems; systems that need to capture content in the surrounding environment such as temperature, humidity, motion or even the voice and images of the monitored objects. Several surveillance applications including those which already use the traditional WSN tended to use WMSN to provide an enhanced system, that has the ability to sense, process and deliver multimedia date to reinforce the observation of unusual behaviors and changes [20, 21].

The followings are some approaches in which WMSN can be employed:

- **Environmental and habit monitoring**

Due to the wide coverage capability of WMSN, it is suitable for habits and environmental monitoring applications. For example, visual sensors can be deployed to study the pattern of wildlife in their natural environment.

- **Traffic control, avoidance and enforcement systems**

WMSNs assist to monitor the average traveling time on roads and highways, such gathered data can be used in the traffic routing services to avoid congestion and reduce driver traveling time [14]. WMSNs can also be deployed in intelligent parking systems to guide drivers where to park their vehicles (at which parking facility), and directing them to the available parking bays .

- **Home, personal and healthcare monitoring**

In the home monitoring and healthcare fields, WMSN provides more precious information compared with scalar WSN [21]. Visual information helps in theft detection, medical emergencies detection and taking care of elderly people and those who are physically or mentally impaired. Studying the behavior of elderly people helps to identify the causes of illnesses that affect them. Additionally, WMSN can be connected to emergency or remote assistance services to provide the required help [2].

- **Industrial process control**

WMSN can be used for industrial quality control and plant monitoring. Compared with the scalar WSN the use of visual sensors allows more flexibility for its placement to provide more accurate monitoring on the manufacturing process. Emergency situations also can be detected, to allow the proper service provisioning [14].

2.1.5. Wireless Visual Sensor Networks

In this research, we concern about image security in WMSN, so we focus on WVSN; a special type of WMSN, in which sensing nodes are equipped with cameras.

Compared with scalar information, captured scenes within WVSN reveal more precious information. As a result, researches became more interested with the additional applications in which WVSN can be useful. Moreover, the additional flow of data included within the images caused additional challenges and security requirements, that need to be satisfied to guarantee the operation of the network [22].

2.1.6. Challenges and Requirements in Wireless Visual Sensor Network

Compared with the previous wired networks and wireless scalar networks, WVSN faces additional challenges. Compared with wired networks, WVSN incorporates [3] challenges due to its wireless inherent nature and the sensor nodes constraints. On the other hand, WVSN differs from scalar WSN in the following aspects [19]:

- The nature of the data flow in WVSN is pixel based visual flow, which has larger size compared with the simple scalar data flow. Because of that, additional resources including memory, processing and communication power are required for WVSN.

- In contrary to scalar WSN, energy aware compression methods are essential in WVSN to reduce the required resources for image sensing and transmission as much as possible. Accordingly, data correlation and redundancy are used to compress the transmitted images.

- To ensure the transmitted data security, the adopted security approach should take in to account the additional resources required to protect the image content, in addition to the need to prolong the sensor node lifetime, as much as possible.

Due to the various applications in which WVSN may be used, in addition to the previously mentioned network challenges, it is important to guarantee the following requirements [2, 21]:

1. **High processing power, memory and communication bandwidth:** Since the number of pixels included in an image is large, image acquisition, processing and transmission require more power and processing than scalar data. Additionally,

image transmission requires more power than image processing. To solve this problem, image compression and partial image analysis is needed to transmit only the meaningful (important) part of the image to the base station [10]. Even the compression process requires a significant amount of storage and processing resources, it still less resource demanding than transmitting the original image entirely.

2. **Real-time transmission and Quality of Service (QoS):** In most cases, monitoring application require fast image processing and transmission, to detect dangers or intruders in real-time [23]. The transmission of Real-time multimedia data such as images requires a certain bandwidth with minimum delay.
3. **Secure image transmission:** Since images reveal critical and detailed information, image security in WVSN became a main research direction. Several security schemes may be used taking in to account the required security level in one hand, and the resources limitation in the other hand. The required security level of the transmitted information in WVSN varies depending on the sensitivity of the observed entities, the application in which it is employed and the environment in which it is deployed [21] .

2.2. Security in Wireless Visual Sensor Network

Usually, sensors are spread in large and hard-to-access environments, and this make them vulnerable to other parties access. Additionally, the type of sensed and transmitted data varies in its secrecy and importance in different applications. Visual sensor which is equipped with camera reveals precious information including people identities, habits, preferences and social links. Therefore, it is important to protect information against outsiders and even insiders such as system operators [14].

2.2.1. Security Requirements in Wireless Visual Sensor Network

The components of the WVSN should be protected to grantee the security of the system as a whole. Sensing nodes, sensed data, users and the network itself are the main actors

in WVSN. The main security requirements in WVSN are confidentiality, availability, integrity, authenticity, freshness and localization. From [19, 21], security requirements in WVSN based on the main actors' security necessities are:

- **Data centric security:** this includes the protection of raw sensed data, in addition to all types of derived data such as processed data, and data transmitted between different nodes. For all derived data, non-repudiation and data confidentiality should be achieved to guarantee the security of data within the WVSN.

    1. Non-repudiation: preventing both the sender and the receiver from denying a transmitted image is a main security requirement. Accordingly, non-repudiation emphasizes the answer to by whom, when and where image was produced, and detects any manipulation upon its data.

        a. Authenticity: to answer by whom data is produced, authenticity guarantees the ability to assure the origin of the transmitted image.

        b. Location: for many applications it is important to determine the location of the origin node that captured data.

        c. Time stamping and freshness: preventing an attacker from exploiting old messages is essential to preserve the security of its contained data, especially when the captured data is critical. Data freshness guarantees the inability of the attacker to know old generated data.

        d. Integrity: To prevent the modification of captured data during the transmission within the network, or even during data storing in database. Data integrity is

not limited to the captured data; attached data such as location and timestamps should be protected from any change.

2. Confidentiality: To assure that private or confidential data is not made available to unauthorized individuals, confidentiality need to be guaranteed through:

    a. Access authorization: Access to confidential data within the WVSN should be limited to a set of legitimated users. An access authorization scheme should be used to ensure that only persons with a specific security clearance have the ability to access secure data.

    b. Privacy: while confidentiality attempts to protect data within the WVSN from unauthorized foreign parties, privacy attempts to protect sensitive data from being misused by legitimated parties.

- **User centric security:** this aspect is essential to protect the security of the users within the monitored environment [3]. It is important to notify that users should be aware about the existence of a monitoring system within the area they exist in, a user walking within a surveillance system has the right to be notified either by active or passive means about the cameras and sensing nodes that exist in the area.

- **Node centric security:** The importance of the node security either at the physical or software level comes from the implication of its role as an underlying base for the data at the application level. An attacker who is capable of node permeation has the ability to get and modify data within the node before it could be secured [24].

1. Availability: often WVSN is used for several critical systems, so it is important to assure that the system works promptly and service is not denied to authorized users.

2. Physical security: WVSN nodes may be deployed in open environment in which they are easily accessed, so it is important to protect nodes within the network from several attacks, varying from simple thefts and disruption, to nodes manipulation and modification.

3. Code security: as any embedded system, WVSN implements a lot of system as software. Software attacks forms a serious danger in the system.

- **Network centric security:** networking components such as the communication channel and the routing protocol need to be secured [24]. Also, the communication channel used to transmit image data between the network nodes need to be protected.

2.2.2. Threats and Attacks in Wireless Visual Sensor Network

As in traditional scalar WSN, attacks are viewed from the WVSN perspective as any undesirable behavior or intervention by an unauthorized party, which in turn threatens the system defense line. Security threat can be classified based on different categories, such as its nature, origin, level at which it works and its goals [16, 25].

- **Passive vs. active attack:** passive attacker is interested in transmitted information eavesdropping, so it aims to make use of the captured information only without any modification. In contrast, active attacks provide the attacker with a degree of partial control upon the system.

- **Mote class vs. laptop class attack:** In mote class attack an adversary uses a node or a set of nodes with the same capabilities of the WSN nodes to accomplish his attack. While in laptop class, attack the attacker uses powerful devices that exceeds the capabilities of WVSN nodes in terms of energy, transmission range and processing power.
- **Software vs. hardware attack:** in software attacks, the attacker aims to manipulate the software stack of the WVSN node. It includes software modification, new software installation and attacks on routing protocols. On the other hand, hardware dependent attack targets the physical hardware components, such as obtaining the network end nodes.
- **Attack Context:** in this categorization attacks are classified according to the targeted element within the system based on the purpose of the attacker. It could be either node centric, network centric, data centric or even user centric attack that targets the monitored user's security.
- **Attack nature:** It can be an interruption, interception, modification or fabrication attack. The first aims to compromise the availability of the network by launching a Denial of Service (DoS) attack, while in the second attacker aims to compromise the network confidentiality, allowing unauthorized access to the sensor nodes and data within the network. The third attack aims to compromise the integrity of the network, allowing data modification. Finally, fabrication is an attack on authentication, by injecting false data and compromise the trustworthiness of the information within the WVSN.

2.2.3. Defense Mechanisms to Ensure Security in Wireless Visual Sensor Network

The adoption of a security scheme in WSN requires additional energy , memory space and computational complexity, which are not available in our scenario. Securing the WVSN is more challenging because of the bulky data size in the captured image, so the adoption of a security scheme should be studied carefully to achieve the tradeoff between security strength in one hand, and resource consumption in the other hand [21].

The main defense mechanism that guarantees the authenticity, confidentiality and integrity requirements is cryptography. This mechanism depends on hiding the content of the image transmitted through the network. The use of cryptographic keys to encrypt image content allows to authenticate the source nodes, because they should have the proper key to encrypt its data. Confidentially is also guaranteed since security keys are also required to recover the encrypted data. Finally, since a robust cryptographic algorithm prevents original data access, integrity property is also achieved [2].

Watermarking is another defense mechanism that is used to guarantee the source node authentication. It is based on embedding secrecy information into the transmitted image to allow the detection of malicious nodes within the network [26].

WSN consists of distributed sensor nodes, which are cooperative and trustworthy in essence, but this is not the real case because nodes may be dynamically inserted and discarded in WVSN. Accordingly, trust modeling is essential in WVSN to authenticate the interacted network nodes [27].

DoS attacks are primarily designed to compromise the availability of the WVSN. This is performed by draining sensor nodes resources and prejudicing the sensing and transmission of the gathered information as a result. DoS attacks may be performed in

different ways, and at different layers of the network stack. Specialized counter-measures need to be adopted for DoS attacks. For example for jamming attack which works at the physical layer, frequency hopping is used as a defense mechanism [28].

In this research, we are concerning about the investigation of different image encryption algorithms as a defense line, to guarantee the security of the transmitted images within WVSNs.

2.3. Image Encryption in Wireless Visual Sensor Network

Digital images encryption has become a major concern in the domain of WVSN information security. Due to the numerous domains in which secure image processing and transmission are required, the adoption of a proper cryptographic algorithm that can protect the transmitted image from any undesirable access and meet the main security requirements is essential [7].

2.3.1. Image Encryption Techniques in Wireless Visual Sensor Network

Cryptographic approaches for image encryption are classified to either full image encryption, or partial image encryption [11]. The computational overhead and processing time required to execute full image encryption are considered limiting factors that prevent its usage for real time and resource constrained applications [4]. To overcome this problem, many recent works benefited from the image's spatial and visual redundancy property, and use partial encryption approach to encrypt the most significant parts of image, and consequently, reduce the encryption overhead [10, 29].

A. Full Image Encryption

The application of WVSN is critical surveillance systems like healthcare monitoring, traffic monitoring and theft detection need to retrieve images with high quality to allow the post processing of the captured image; such as face detection and recognition in theft detection. At the same time, image security is a major concern to protect the transmitted image from illegal parties' access. Based on that, full image encryption is required in some applications which are not tolerant for data loss [2].

B. Partial Image Encryption

The main constraints in WVSN, including the limited available power and processing capabilities, in addition to the fact that images in WVSN require large memory space, and suitable bandwidth to be transmitted. These constraints make the task of full image encryption in sensor nodes more difficult. Especially, in surveillance systems where real time image compression and transmission is required [1, 6]. This observation has drawn researchers attention to benefit from the data redundancy property within the transmitted images and propose the use of partial image encryption instead of full encryption [11].

In partial encryption, only representative data is encrypted instead of encrypting the whole image. Leading to improve the image encryption process efficiently. Partial image encryption can achieve the tradeoff between limited resources in WVSN in one hand, and the need to use a satisfactory security level in the other hand. In [30] they studied the use of both full image encryption, and partial encryption based on edge detection and face detection. Experiment results showed that the partial encryption has

the ability to significantly reduce the required time and resources for the process of image encryption, while maintaining adequate quality and security compared to full image encryption. Consequently, this approach can be considered a good alternative for real-time applications that need sufficient security level, or for resource constrained systems such as visual nodes in WVSN.

Since the operation of partial encryption depends on two main components, Image compression, and image encryption, by finding a suitable compression algorithm that provides the required image quality, while presenting a robust and light encryption scheme, we can provide an encryption algorithm that suites the WVSN requirements [29].

2.4. Image Compression in Wireless Visual Sensor Network

In applications that are based on image compression and transmission such as WVSN, intermediate nodes consume more energy for image transmission process compared with data collection and forwarding process, this is because transceiver is one of the most energy greedy components in WSN node [14, 31]. Depending on that, it is important to reduce the amount of transmitted data in the network, and this is done through image compression.

2.4.1.Theory Behind Image Compression in Wireless Visual Sensor Network

In the context of WVSN, Image compression has vital benefits including:

- **Extending the lifetime of the source node:** this is true when the complexity of the adopted compression algorithm is reasonable, because such algorithm would reduce

the amount of data that represents an image with a reduced power and storage requirements, while maintaining a satisfactory image quality [32].

- **Extending the lifetime of the intermediate nodes:** reducing the amount of data at the source leads to fewer packets received by intermediate nodes that are responsible for relaying packets between the source and the destination node [33].

- **Decrease the risk of congestion:** The amount of transmitted data is reduced because of the compression process. This leads to reduce the risk of network congestion, and thus decrease packets loss and transmission delays [33].

Neighboring pixels in an image are highly correlated, so finding another less correlated representation of the image by discarding redundant and irrelevant data is the idea of image compression. When the image is reconstructed, it looks similar (or exact) to the original data. In case that the reconstructed image is an exact replica of the original one, the algorithm used in compression and decompression is lossless [34]. Furthermore if the reconstructed image provides good perceptual quality (but not an exact replica of the original one). Then, the compression algorithm is lossy. Owing to the limited processing power, storage and small battery of a sensor node, lossy compression methods are more investigated in WVSN [35].

Compression is based on two main components; Redundancy reduction and relevance reduction. Redundancy reduction is related to the removal of redundant information within the image. It is the core of lossless compression but also used in lossy compression . Moreover, relevance reduction is related to the removal of parts of the

signal that will not be noticed by the receiver, owing to the properties of the human visual system, since the human eye is insensitive to certain spatial frequencies. Lossy compression uses this technique but lossless doesn't [35].

Image compression schemes are categorized to first generation, and second generation schemes. First generation image coding concerns about how to efficiently encode information in a transformed image. Furthermore, second generation image coding concerns about how to extract useful information from an image. The second generation image coding schemes make use of available techniques developed in the entropy coding stage which is computationally intensive, and consumes long time. Based on that, second generation compression schemes are not the ideal choice for WVSN [31].

As shown in Figure 3, second generation image compression schemes follow three main steps to obtain a reduced image size as an output. In the first step, a mapper is used to transform the original input image that has correlated pixels into another domain where it becomes highly de-correlated, and suitable for the compressor to reduce spatial redundancy in the input image. Two main transforms are used here; Discrete Cosine Transform (DCT), and DWT [31, 36]. In the second step a quantizer is used to reduce the accuracy of the mapper's output in accordance with some pre-established criterion. This step reduces the psycho-visual redundancy of the input image by discarding irrelevant data, a good quantizer is the one which represents the original signal with minimum distortion. Finally, an entropy coder is used to reduce the quantizer's output bits. The coder creates a fixed or variable-length code to represent the quantizer output,

and map the output in accordance with the code. This process removes the redundancy in the form of repetitive bit patterns at the output of the quantizer [32].

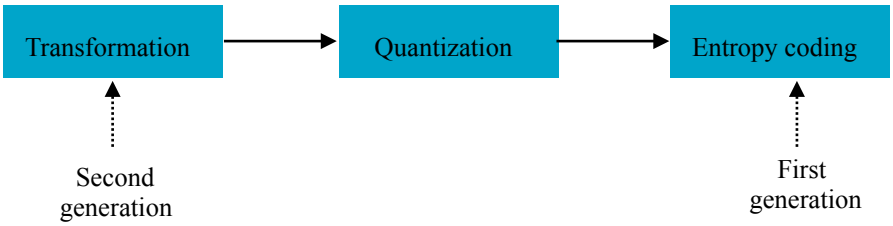


Figure 3. Process of image compression

2.4.2. Image Compression Algorithms in Wireless Visual Sensor Network

The choice of the suitable compression technique in WVSN depends on a set of parameters including simplicity in coding, low memory requirements, low computational overhead and fast compression [32]. A compression algorithm needs to be evaluated to ensure that it will not dissipate more energy compared to the amount of energy consumed while transmitting uncompressed images. In the context of WVSN, several transform based image coding schemes were used and adapted to meet the node requirements, including DCT based algorithms, and DWT based algorithms [33, 36-38].

A. Discrete Cosine Transform-Based Image Compression

DCT converts the image blocks to its elementary frequency components. It is widely used for image compression purposes due to its power compaction property. For example, Joint Photographic Expert Group (JPEG) which was released in 1992, is a well-known image compression scheme that depends on DCT [39].

DCT based image compression standards works as following:

1. The input image is broken in to fixed size 8x8 pixel blocks and two dimensional DCT is applied on each block to transform the image from spatial domain in to frequency domain. Two dimensional DCT is given by [40]:

$$D(i,j) = \frac{1}{4}C(i)C(j)\sum_{x=0}^{7}\sum_{y=0}^{7} p(x,y)cos(\frac{(2x+1)i\pi}{16})cos(\frac{(2y+1)j\pi}{16}) \quad (1)$$

Where $C(i) = \frac{1}{\sqrt{2}}$ if i=0 and 1 otherwise.

Entries within the output block D represent the frequency of intensity changes for each component of the image. Coefficients at the top left of the matrix represents low frequency intensity changes, while coefficients at the button right represents high frequency intensity changes.

2. A 8x8 size Quantization matrix (Q) is used to compress Each block in the quantization stage. The JPEG quantization matrix is obtained through numerous experiments on human vision, high entries values at the right bottom are related to the fact that human eye is poor at detecting high variation (frequency changes) in the color over a short distance. The JPEG standard quantization matrix renders both high compression and excellent decompressed image quality. A 8x8 C matrix is obtained by the dividing D/Q and result rounding; high frequency changes are likely to become zeroes. The C matrix will have lot of zeroes, related to more compression rate while perceiving less degradation in the image quality. To adjust JPEG compression degree, the quantization matrix can be multiplied by a positive constant q, if q is less than one then the output values of M/Q will be larger and this leads to less values rounded to zero, and high quality image is obtained.

3. The array of compressed blocks is stored in a reduced amount of space in the entropy coding stage. All coefficients produced by the quantization stage are encoded in a zig-zag sequence via an encoder in to a stream of binary data , Instead of recording each zero entry, the number of C matrix zero entries in succession is recorded, this will reduce the amount of required storage for a specific image [32].

DCT-based image compression gives acceptable compression results and low memory implementation, this is because the encoding is done on small individual 8x8 blocks. Moreover, splitting the original image into several blocks causes blocking artifacts at blocks boundaries. This happens because neighboring blocks quantize frequency coefficients differently. Therefore, the quantization process leads to discontinuities at the block boundaries and degrades the compression performance as a result. To overcome DCT limitations, DWT transform is performed on the entire image [31].

B. Discrete Wavelet Transform-Based Image Compression

DWT was introduced to overcome weaknesses in DCT, by the decomposition of the image in to a discrete wavelet representation (a set of basic functions called wavelets). DWT is adopted by the JPEG2000 image compression standard, which is the most used standard for image coding nowadays. Wavelet-based coding has several benefits including image progressive transmission and its inherent multi-resolution nature, so it is suitable for applications where scalability and tolerable degradation are essential [41].

DWT decomposes an image into spatial sub bands. These sub-bands facilitates the design of efficient quantization algorithms and allows to exploit the human visual system characteristics. Wavelet decomposition of an image can be interpreted as a

filtering process. To decompose an input image to one level, first a low pass filter and high pass filter are applied on the rows of the image. Low pass filter gives the low frequency information or the background of the image (L sub-band), while high pass filter gives the high frequency information of the image or the edges (H sub-band). A subsequent down sampling by a factor of 2 for each filtered image provides both L and H sub bands. In the same way we apply the low pass filter and high pass filter on the image columns, this includes applying them on the images L and H to obtain 4 sub bands; LL (low resolution-sub band), HL (horizontal orientation sub-band), LH (vertical orientation sub-band), and HH (diagonal orientation sub-band). The low resolution sub-band contains low frequency components that implies the smooth information and background intensity of the image. On the other hand, other sub-bands contain high frequency components that represent edges and detailed information [31].

In the second level, each of these four sub-bands is decomposed into another four sub-bands. As we know low frequencies contain more image energy compared with high frequencies, so we need to decompose the LL sub-band usually. The operation of DWT is illustrated in Figure 4.

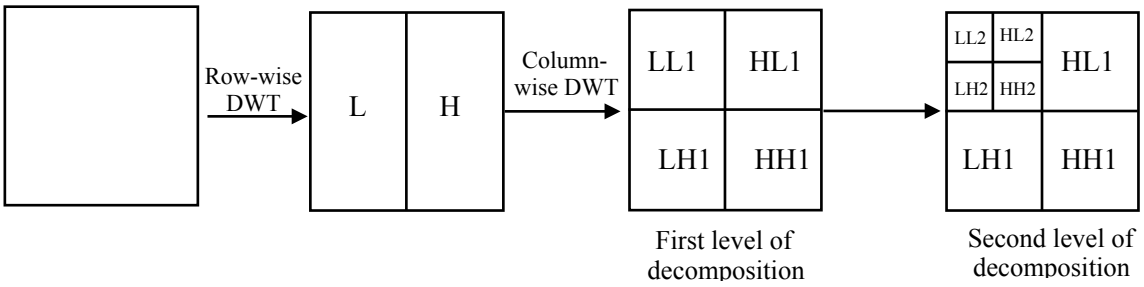


Figure 4. Two levels of decomposition for two dimensional DWT

In [31] they evaluated both DWT and DCT in the context of WVSN. Evaluation results concluded that in terms of compression performance and execution time, and Compared with DCT and other transforms, DWT give better results. Additionally, there is no big difference in the energy consumption and battery lifetime using both of them. As a result, DWT image compression is preferred for the following reasons. First, it is a non-block-based transform, so it allows to avoid the annoying blocking artifacts incorporated by the DCT transform within the reconstructed image. Second, it has a good localization in both time (space) and frequency domains, so not only we know what frequencies are in the image, but also where these frequencies are. And finally the multi-resolution characteristic which leads to superior energy compaction, while providing high quality reconstructed images [37].

Several DWT based compression schemes for images have been developed in the literature due to their usefulness for image energy compaction and each one of them has its unique characteristic that make it suitable for specific applications. In the context of WVSN, several well-known algorithms such as Embedded Zerotree Wavelet (EZW), Set Partitioning in Hierarchical Trees (SPIHT), Embedded Block Coding with Optimized Truncation of the embedded bit-streams (EBCOT), and Set Partitioned Embedded Block (SPECK) were employed and adapted to meet specific requirements. The advantages and shortcomings of using them in the scope of WVSN was discussed in [33].

2.5. Image Encryption Algorithms in Wireless Visual Sensor Network

Image encryption algorithms have been used to assure the main security requirements. Encryption algorithms used for WVSN are categorized to either conventional ciphers, or lightweight ciphers that were developed to meet the node capabilities [3]. Since real time image encryption was proved to be a serious problem while employing traditional image cryptographic algorithms in WVSN, new algorithms including modified versions of the conventional ciphers, and chaotic based ciphers has proven its ability to provide a comparable image security and performance results [2, 4, 5, 9].

2.5.1. Conventional Image Encryption Algorithms

To assure the authenticity, confidentiality and integrity of the transmitted images in WVSN, the use of traditional symmetric and asymmetric cryptographic algorithms was studied carefully in [2], indicating that every encryption algorithm has its benefits and drawbacks in terms of the required storage, time, key size and power consumption.

Results obtained in [42] claimed that asymmetric encryption is not feasible for WVSN owing to the high computing overhead and processing power incorporated in this method. This is related to the use of two different keys; public key and private key for the encryption and decryption steps. Additionally, compared with symmetric encryption algorithms, long cryptographic key sizes are used for asymmetric algorithms to guarantee a robust security level. As a result; Unless the use of energy efficient techniques such as elliptic curve cryptography or dedicated cryptographic coprocessors, the use of public key cryptography is not the proper choice in the context of WVSN. Other works such as [3] concluded that the feasibility of the encryption technique

depends mainly on the key size. Smaller key size requires less memory usage and computing overhead, and incorporates more bandwidth saving. Based on that, with the proper selection of the key size, a suitable asymmetric or symmetric cryptographic technique can be used.

Since symmetric encryption algorithms usually use smaller key size than asymmetric encryption, researches in WVSN security shifted to the symmetric image cryptographic approach. The shared key used in symmetric encryption facilitates and simplifies the cryptography process, but secure key distribution methodology is required to protect it from any unauthorized access [2]. Symmetric cryptographic algorithms are categorized to either stream ciphers, or block ciphers. Stream ciphers are distinguished by its low latency and low error propagation. This is related to the concept which it depends on, i.e., the transformation of a single symbol of plaintext in to a corresponding symbol of cipher-text. On the other hand, because the plaintext block information is contained entirely in a single cipher-text block, stream ciphers has low diffusion property, making the cipher more prone to differential attacks. Although block ciphers are slower than stream ciphers and incorporate more error propagation, they present stronger diffusion such that a simple change in one input bit propagates to the other ciphered bits [43].

2.5.2. Chaotic-Based Image Encryption Algorithms

Images are characterized by their bulk data capacity property, high spatial redundancy and strong correlation among adjacent pixels. Therefore, conventional block ciphers were found not suitable for practical image encryption due to its low level efficiency and security in such scenarios [29]. Accordingly, researchers in the field of image

encryption shifted their attention toward new cryptographic schemes that have the ability to provide the following advantages:

- Large key space to resist brute force attack.
- Mixing property, and sensitive dependence on the initial conditions.
- High security, and the ability to resist statistical and differential attacks.
- No relationship between adjacent pixels.
- Less time complexity and computational overhead compared with the traditional encryption algorithms.

In recent years, chaotic based cryptographic algorithms where found as new applicable field for chaos theory. Compared with conventional block ciphers, chaotic based cryptographic algorithms showed their superior performance in aspect of complexity, speed, and security [44].

The ease of mapping chaos theory properties to cryptographic properties played a key role in the employment of chaotic maps for image encryption. For example, the sensitive dependence of chaotic systems on its initial conditions is relevant to diffusion property in cryptography. Two relatively close initial conditions will begin to diverge over time, becoming very different after a short number of iterations. At the same time, diffusion property is defined as the process by which the influence of a single bit of the plaintext will spread out over many cipher-text bits (at least half of the cipher text bits will be changed). The second similarity between chaotic system and cryptographic

algorithms is the relationship between discrete time-based system iterations and encryption rounds.

Since both chaotic systems and cryptographic primitives are deterministic, the third similarity between them is the relationship between the system parameters and the cryptographic keys, both system parameters and cryptographic keys are used to determine the functional output of the system or the cipher. As a result, without the knowledge of such values an attacker cannot guess the output of the system or the cipher [45] .

Several one-dimensional and high-dimensional chaotic maps where found and incorporated in image encryption. One-dimensional chaotic system such as logistic map has the advantages of high-level efficiency and simplicity, but its small key space leads to weak security level. On the contrary, complex high-dimensional chaotic systems provide an improved security level with additional low-level efficiency. Accordingly, the selection of the proper chaotic system depends on the proper tradeoff between the required security level and efficiency [46].

Figure 5 illustrates the encryption process in chaotic based crypto-system, in which [47], Fridrich suggested that the encryption process is composed of two stages: pixel confusion and pixel diffusion. At the confusion stage, pixels in the input image are scrambled using a chaotic map, without disturbing the pixel's value. Subsequently, the value of each pixel is altered to ensure the diffusion property of the cryptographic algorithm using the same chaotic map or another one. Confusion and diffusion stages are iterated for n and m times respectively, to provide a satisfactory security level.

Decryption process reverses the encryption steps to reconstruct the original image from the ciphered image.

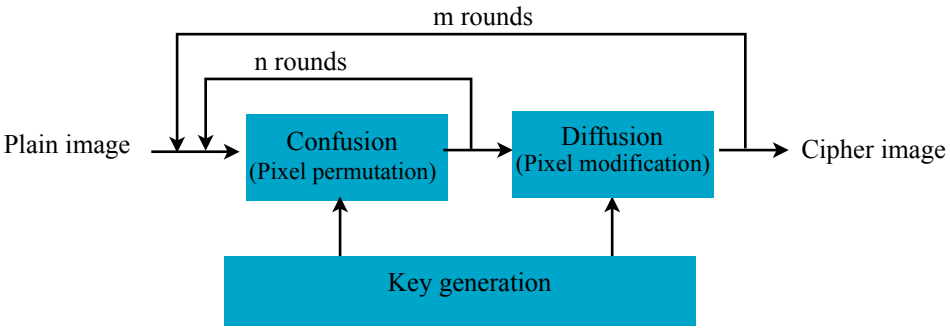


Figure 5. The architecture of chaotic-based image encryption

Digital chaotic cryptographic algorithms are classified with respect to the structure of the encryption algorithm in to stream ciphers and block ciphers. Stream ciphers encrypt the image content bit by bit with an XOR operation at the output of a pseudo-random number generator (PRNG), which is based on a specific chaotic map. However, decryption would be impossible, unless the whole key stream, with the same length as the plain image is transmitted to the legitimate receiver via a safe channel. This procedure is often impractical especially in the wireless networks because it is prone to network targeted attacks. In contrast, block based crypto-system treats the input image as a set of blocks, and each block is encrypted separately [44]. Although the previous common characteristics between chaotic maps and cryptographic primitives make them convenient to work together, there is one important different property that should be considered while determining the use of chaotic map in the symmetric key crypto-system. It is related to the encryption transformations which operate on finite sets of integers, while chaotic map behavior exists on subsets of real numbers. Therefore, the

level of chaotic behavior is closely limited to the precision with which those real numbers are represented.

Complex chaotic systems involve the use of floating point arithmetics. Compared with fixed point arithmetics and because of the constrained visual nodes in WVSN, floating point arithmetics decrease the speed of the encryption algorithm and harden its applicability. Moreover, the use of floating point arithmetics in WVSN requires dedicated processors, since the numerical precision of the main processor in the node is limited even in the advanced PDA-class mote processor which only supports fixed point arithmetics. Based on the previous observations, chaotic map discretization is required . Even the discretized chaotic encryption algorithm provides a reduced precision, the main chaotic properties including the pseudorandom behavior ,and its dependence on the initial conditions are still guaranteed [7, 45] .

2.5.3. Encryption Algorithms Evaluation in the Scope of WVSN

As we mentioned in the previous sections, researcher have followed two main approaches to encrypt images in WVSN. The first one concentrated on the use of traditional symmetric and asymmetric encryption algorithms which were also employed in scalar WSN [2]. Comparisons between various traditional algorithms in scalar WSN were conducted according to the performance analysis and resources required to encrypt the sensed data. On the other hand, the second approach concentrated on the feasibility of using new encryption algorithms and modified conventional algorithms that were developed to cope with the constrained nodes in WVSN [1, 7, 8, 11]. Analysis in the second approaches have focused on the algorithm's security strength and its ability to resist known attacks.

A. Performance Evaluation for the Encryption Algorithms in WVSN

The selection of a suitable cryptographic algorithm that meets the limited capabilities within the sensor node in WVSN is not a straightforward process. Performance evaluation of different cryptographic algorithms is necessary to test their feasibility in terms of resource consumption [48], so in the following we survey the main performance metrics and recent comparative studies that discussed the feasibility of different cryptographic algorithms in WSN.

1. Performance Metrics for the Encryption Algorithms in WVSN

To cope with the tradeoff between security and performance within the WVSN nodes, the cryptographic algorithm design must have low power consumption, reduced storage requirements and satisfactory speed [48, 49]. To compare the performance of different encryption algorithms in WSN nodes and facilitate the process of selecting the proper candidates for WVSN, the following are the main crucial parameters that should be considered:

- **Computational cost (Energy efficiency):** The computational complexity is used to calculate the energy efficiency of an algorithm. Assuming the energy consumption per a Central Processing Unit (CPU) cycle is fixed, the energy consumption per byte is computed by measuring the number of CPU cycles required to process one byte of plaintext [50].

- **Memory efficiency:** According to WVSN, memory is limited due to the small size of sensor node. Additionally, more memory usage entails more energy consumption to

store and retain data in memory [49]. For the previous reasons, efficient usage of memory is essential.

- **Operation cost:** To estimate the average operation time of a cryptographic algorithm, the encryption and decryption process should be executed repeatedly. The execution time of the key setup, encryption process, and decryption process are influenced by the key size. The longer the key is, the longer it takes for those phases to be executed [50].

2. Performance Analysis for the Encryption Algorithms in WVSN

Previous works compared the performance of the encryption algorithms according to the various constraints in WSN. The followings are the main conventional ciphers used in WSN, that can be employed and adapted for image encryption in WVSN:

- **Skipjack:** It is a block cipher that was developed by the U.S National Security Agency (NSA). Skipjack uses a 80 bit key, 64 bit data block and implements an unbalanced Feistel network with 32 rounds. Since it uses a short key size (80-bit), Skipjack is vulnerable to exhaustive key search attack, so National Institute of Standards and Technology (NIST) recommended not to use Skipjack after 2010 [50].

- **Corrected Block Tiny Encryption Algorithm (XXTEA):** It operates on variable-length blocks that are multiple of 32 bits in size (minimum 64 bits) and 128-bit key length. XXTEA implements an unbalanced Fiestel network with variable number of rounds (6 to 32 full cycles). Based on differential cryptanalysis, E. Yarrkov presented a chosen plaintext attack against full-round XXTEA using 2^{59} queries in 2010 [51].

- **Rivest Cipher 5 (RC5):** It was introduced by Ron Rivest in 1994 as a symmetric cipher. RC5 is a flexible cipher with variable parameters including block size (32, 64, or 128-bits), key length (0 to 2040-bits) and number of encryption rounds (0 to 255). This algorithm is widely used in WSNs due to its distinguished features including low storage space, fast speed and variable parameters. The algorithm's simplicity is another property for RC5, because it depends only on the general operation on common microprocessors such as XOR, modular addition and cyclic shift. From the security perspective, RC5 has some security risks due to its weak diffusion. As a result, 12-round RC5 with 64-bit blocks and 128 bit key is vulnerable to a differential attack using 2^{44} chosen plaintext. Additionally, breaking RC5 with 128 bit blocks,128 bit key size and 16 rounds requires 2^{66} chosen plaintext. Since the security of RC5 cipher depends on both key size and number of rounds, 18-20 rounds are suggested to provide sufficient protection [50].

- **Rivest Cipher 6 (RC6):** RC6 is derived from RC5 cipher to meet the requirements of AES cipher and enhance the diffusion of RC5. RC6 has a 128 bit block size, with variable key size and number of rounds. Similar to RC5, RC6 uses data dependent operations, modular addition and XOR operations. Moreover, RC6 encryption can be viewed as two interweaving parallel RC5 encryption processes. The key difference between RC5 and RC6 is related to the use of an extra multiplication operation in RC6. According to [50], RC6 with 32 word length and 20 rounds can provide sufficient security level.

- **Advanced Encryption Standard (AES):** AES uses keys of 128,192 and 256 bit to encrypt and decrypt a 128 bit block. The number of rounds varies according to the key size, so it could be 10,12 or 14 round. AES is an iterative algorithm, which is made to apply consecutive four different transformations on a 4x4 bytes matrix (called state) in each encryption round.

  The main transformations in AES encryption algorithm are: SubBytes, ShiftRows, MixColumns and AddRoundKey. In subByte transformation, a substitution table (S-box) is used to replace each byte in the state. After that, a permutation function that shifts each row in the state to the left is used in the ShiftRows step. In the next MixColumns transformation step, the MixColumns function multiplies a constant matrix with the state. Finally, the AddRoundKey transformation includes an XOR function that performs an XOR operation between the round sub-key and the state matrix. Confusion property is guaranteed in AES through the SubByte and AddRoundKey steps, while the ShiftRows and MixColumns transformations were carefully selected to work in tandem ensuring the diffusion property within just two rounds [5].

  From the security perspective, Cheon et al. in [52] presented an impossible differential cryptanalysis that require 291.5 chosen cipher-texts to attack 6-round of AES-128 bit key size. In addition to that, Gilbert and Minier [53] presented an attack of 7-round AES 128, AES-196 and AES-256 with 232 chosen plaintext and computational complexity that is slightly less than the complexity for exhaustive

search. Based on the previous explanation, Rijindae with 128 bit key and more than 7 rounds is considered secure [54] .

The performance of four conventional block ciphers was studied in [50]. The selected ciphers are Skipjack, XXTEA, RC5 and AES. The performance was evaluated on Arduino pro and Mica2 sensor nodes according to the computational cost, operation time and memory usage. With regard to the memory usage, they found that ciphers with big S-box of 256 byte such as AES and Skipjack, require more memory space compared with other ciphers which don't use S-box including RC5, XXTEA and CGEA. Results showed that RC5 with 128 bit key size and 14 round is the lightest, while Skipjack and AES-256 require more memory space compared with all other algorithms. Besides, the memory required to execute AES-128 is slightly less than that required for AES-256 due to the additional encryption rounds in the later. According to the computational complexity; they found that the computational complexity is affected by both the key size and the number of rounds, so Skipjack was found the most energy efficient cipher, while AES-128 consumes half of the energy consumed by AES-256. Accordingly, RC5 with 14 rounds and 128 key size consumes more energy compared with AES-128 even both have the same key size, this is related to the additional two rounds in RC5. Operation speed also was evaluated for all above ciphers, and results in terms of encryption time is obtained, indicating that ciphers with longer key size require more encryption time. Skipjack is the faster cipher since it has the shortest expanded key. Also, AES-128 is faster than AES-256. XXTEA has the same key size as AES-128, but

a reduced encryption time is obtained since it is structured with simple XOR and shift operations.

In [49] and [48] the performance of AES, RC5 and RC6 cryptographic algorithms with (128, 192 and 256 key size) in WSN was evaluated according to three parameters: power consumption, required storage and operation time. Because simulation platforms are fault tolerated, ciphers performance was experimentally evaluated in this work and real measurements using Mica2 nodes where obtained. The key size in all ciphers was set to 128,192 and 256 bit. Additionally, 16 rounds are used for RC5 to enhance the obtained security level. In terms of memory efficiency; RC5 requires a little memory in both Random Access Memory (RAM) and Read Only Memory (ROM). The memory efficiency of RC6 is worse than RC5, but AES has the worst memory efficiency due to its S-box. The execution times of key setup, encryption, and decryption for the three cryptographic algorithm is evaluated, and obtained results concluded that the execution time of all of them is affected by the key size; i.e longer key requires more execution time in the three phases. According to the energy efficiency which is directly affected by the algorithm's computational complexity, obtained results in [49] showed that AES-128 is the most energy efficient algorithm compared with RC5 and RC6 with the same key size.

Based on the previous explanation and compared with RC5 and RC6 encryption algorithms; AES-128 with more than 7 rounds guarantees an enhanced security level with a minimized encryption time and reduced power consumption. This is related to

the additional number of rounds needed in RC5 and RC6 to provide a comparable security level.

B. Security Evaluation for the Encryption Algorithms in WVSN

As we mentioned before, Image security in WVSN has received more attention due to the various critical applications in which visual sensors are employed. In this part we are surveying the security analysis of previous research works which studied the use of conventional ciphers, modified conventional ciphers and chaotic based ciphers in WVSN [2].

1. Security Metrics for the Encryption Algorithms in WVSN

The main concern of crypto-analysis is to discover the shortcomings of a crypto-system and recover the original image partially or fully without having the decryption key. Conventional encryption algorithms, in addition to the new ones need to be secure against various types of attacks such as brute force attack, statistical and differential attacks. Several image security metrics are used to determine the suitability of an encryption algorithm for image encryption [5, 45, 55]. The followings are the most widely recognized assaults on an encrypted image:

- **Key space analysis:** Brute-force attack attempts to discover the decryption key by checking all possible keys. The total number of possible attempts is related to the key space of the crypto-system which is affected directly by the key size; key space increases exponentially with the key size. A crypto-system with key size of 128 bit gives 2^128 possible combinations which looks powerful, because brute force attack will be computationally impossible [56].

- **Key sensitivity analysis:** Robust crypto-system not only requires large key space, but also it ought to be sensitive to any change in the secret key. In order to study the sensitivity to different keys, the key sensitivity test is applied such that two slightly different secret keys should produce entirely different encrypted images [29].

- **Statistical analysis:** The relationship between original and ciphered image can be determined by analyzing its data statistically. Because of Shannon's hypothesis; image after encryption should be totally different from the original image. There are a set of approaches to check if the ciphered image reveals any data about the original one [11, 55].

    1. **Image entropy:** Entropy is the most significant feature of the non-predictability in an image. It measures the randomness in the image data, the more the data content is random the harder it is to be recognized after the encryption process. For a ciphered image with 256 gray scale levels, the ideal entropy should be 8. Entropy value less than 8 means there is a certain degree of predictability, which threatens the cipher's security [5].

    2. **Image histogram:** Image histogram illustrates the distribution of the image pixels by plotting the number of pixels at each grayscale level. A robust cipher should provide totally different ciphered image histogram, and hence; does not provide any clue to employ statistical attack. A flat distribution of the grayscale level's redundancies is considered the optimal distribution [1].

3. **Correlation analysis:** Statistical analysis for both natural and computer-graphical images indicates that on average 8 to 16 pixels are correlative in horizontal, vertical and diagonal direction. Correlation analysis represent the correlation between adjacent elements in the image. Consequently, two neighboring pixels in the cipher image with high relevance indicate more information about the corresponding pixels in the original image. A good cipher should provide the minimum correlation between adjacent pixels within the ciphered image [55, 57].

- **Differential analysis:** Differential analysis concern about how differences in the plain image affect the resulting difference at the ciphered image output. A set of techniques are used to discover where the cipher shows a non-random behavior, through tracing the differences in the cipher transformations. NPCR and UACI are the two most common criteria that are used to evaluate strength of an image encryption algorithm against differential attacks [58]. UACI calculates the averaged difference between two paired ciphered images, while NPCR calculates the absolute number of pixels which change its value.

2. Security Analysis for the Encryption Algorithms in WVSN

In the following we present the recent works that have analyzed the security capabilities of different cryptographic algorithms used for image encryption in WVSN.

•The application of the original AES for image encryption has incorporated several propagating drawbacks, including high computation cost, pattern appearance and high hardware requirements. Accordingly, a modified AES version is shown in [1] to encrypt

high definition (HD) images in WVSN. Three main modifications were proposed to enhance the security of AES-128, and reduce its computational power and execution time. First, Mix-columns transformation is performed only in 4 rounds instead of 9. Second, to enhance the cipher security, the key schedule operation is improved by adding MixColumns transformation to this operation. Finally to decrease the hardware and memory requirements, the substitution box in the standard AES is replaced by another simple S-box. To deal with the pattern redundancy problem they tested the proposed algorithm using several modes of operation including ECB,CBC, Cipher Feedback (CFB) and Output Feedback (OFB).

MATLAB 2010b was used to simulate the proposed algorithm, and encrypt both gray and colored HD images.They evaluated the security of the new modified AES version statistically using scene visibility, image histogram, entropy and correlation of adjacent pixels analysis. Additionally, the execution time for the encryption and decryption algorithms is calculated, and compared with the corresponding execution time required for the original AES. Simulation results using MATLAB confirmed the feasibility of the proposed approach to provide good statistical results in the CBC and CFB modes. In addition to that, The encryption time of the proposed algorithm in different cipher modes has been examined, and results showed that the cipher's encryption time in CBC mode provide a significant reduction to about 35% of the original AES.

Even they enhanced the key schedule algorithm, but the reduction of the MixColumns transformation rounds from 9 to 4 rounds may degrade the diffusion property in the cipher. Based on that, NPCR and UACI measurements are required to assure the strength of the diffusion steps and hence investigate the robustness of the proposed

work against differential attacks. Moreover, even they reduced the encryption time effectively, but the key schedule algorithm will demand more execution time compared with the original AES key schedule due to the additional MixColumns transformation.

- In [57] the application of the standard RC5 and RC6 for digital image encryption in WVSN was investigated and corresponding security analysis where conducted according to different statistical and differential analysis. RC5 parameters were set to 16 round, 128 bit key size and 128 bit input block size, while RC6 with the same key size and block size, but with 20 round is used. Results for Correlation analysis, key sensitivity analysis and differential analysis proved that RC6 outperforms RC5 for image encryption. On the other hand, NPCR and UACI results indicated the high vulnerability of both RC5 and RC6 to differential attacks.

  Employing conventional cryptographic algorithms in image encryption within their original versions is not compatible with the nature of digital images. As we discussed in the previous sections, images are distinguished by its pattern redundancy property which allows to provide redundant ciphered blocks in the output image. This leads to weak confusion and diffusion results. Besides, recent studies which we surveyed in the previous section emphasized the inappropriateness of RC5 and RC6 in the scope of WSN due to their high power consumption and execution time, this problem will propagate in WVSN because of the huge image size compared with scalar data.
- In [5] Msolli, Helali, and Maaref proposed a modified lightweight AES-128 encryption algorithm to encrypt captured images within WVSN fully in real time, with a reduced energy consumption compared with the original AES. Authors proposed to use AES with a reduced number of rounds (5 rounds) instead of 10

rounds. MATLAB was used to implement the simulation of the test images, and results of a set of security analysis including image histogram, entropy and encryption execution time where obtained. The histogram of the encrypted image indicated a random flat pixel distribution compared with the original image histogram. Additionally, the execution time was reduced significantly for both encryption and decryption phases.

Although a reduced execution time and resource consumption were obtained, from security perspective; According to [54] AES with 7 rounds is reported insecure because it is vulnerable to differential attack using 232 chosen plaintext. Moreover, the evaluated security metrics didn't include any parameter related to differential analysis. In addition, the proposed work doesn't explain the used mode of cipher operation, which has a significant impact on the cipher strength, especially in the NPCR and UACI metrics.

- Gonçalves and Costa in [4] presented a new energy-efficient partial encryption paradigm to assure the confidentiality, authenticity and integrity of image data in WVSN adaptively according to the application requirements. Doing so, a suitable level of security is provided for each node according to its importance for the whole application, while saving the network resources. Three main definitions are utilized to govern the operation of the proposed security model including confidential area, confidentiality level and security scheme. Confidential area (CA) defines an area of influence and an expected level of confidentiality for that area, it can be dynamically created over the monitored field. Based on the confidential area, a Confidentiality level is assigned to each node depending on its location, and to which confidential

area it belongs. Accordingly, four main confidentiality levels are defined here arranged from low to high security requirements. Finally, a specific security scheme is assigned to each node depending on the confidentiality level of the area it belongs to. Several security schemes could be obtained based on the different combinations between compression and encryption techniques for in the partial encryption scheme.AES-128 with three level DWT, AES-192 with two levels DWT and AES-256 without compression are suggested to provide low, medium and high security levels.

Results of the scheme's energy consumption indicated that the consumed energy depends on the adopted security scheme, i.e nodes in a high CA consumes more energy to encrypt its data compared with others in less confidential areas. As a result, the consumed energy for the whole network is less compared with a WVSN that ensures a full protection for all sensor nodes.

Encryption time is not considered in this work although it is a main performance metric, especially when real time encryption is a major concern. AES cryptographic algorithm is distinguished by its robust diffusion which implicates complex mathematical operations, that require considerable execution time. In addition, the use of AES with 192 and 256 key size will consume more resources due to its additional rounds and maximized key size, so it will deplete the nodes resources quickly.

- In [6] a new security approach for real-time full image encryption in WVSN was presented using a modified AES-128 cipher called Shift-AES. Since the MixColumns transformation in the original AES includes complex multiplication operations, the

algorithm requires a significant time to perform the encryption and decryption processes properly. In applications where real-time image transmission is as important as image security, the standard AES will not be a proper choice, so authors here replaced the high time consuming MixColumns transformation with a simple ShiftCols transformation. Moreover, they rearranged the algorithm's transformations to improve the entropy and execution time parameters by moving the ShiftCols step to the beginning of the round transformations. As in the previous work, different cipher modes were examined to provide an enhanced security level.

To perform the security analysis of Shift-AES approach, and compare it with other previous works. MATLAB R2015b was used in the simulations. According to statistical attacks; visibility scene, histogram, entropy, the correlation of adjacent pixels and key sensitivity are considered. Furthermore, a comparison according to the cipher's execution time between Shift-AES and previous works was presented. Security results show that Shift-AES provides a comparative results in all the modes of encryption, especially CBC and CFB for all security tests. In addition to that, the execution time was reduced to about 1/6 of the standard AES execution time. Even the proposed algorithm provided high reduction in the execution time, but to provide a robust diffusion step that is comparable to the robust MixColumns in the original AES, the cipher need to guarantee that after the execution of the ShiftRows and Shift-cols transformations, the values in each word within the input block is affected by all other words in the state. This cannot be guaranteed with a simple shift process.

All of the previous cryptographic algorithms encrypted image blocks sequentially from left to right, top to down. Accordingly, the NPCR and UACI will degrade while the changed pixel is located at lower level in the image. So, a differential attack can be accomplished if the attacker has the same image with one pixel difference at the end of the input image. Chaos based cryptographic algorithms treated with this problem using the iterated permutation step.

- To benefit from chaotic based image cryptography robustness, and reduce the power consumption of the standard cryptographic algorithms, a discretized chaotic based image encryption scheme was proposed in [7]. The proposed cipher takes 3 bytes of the input image as an input block, and operates in CBC mode ,ensuring the required confusion and diffusion properties. A simple left cyclic permutation of pixels is used to achieve diffusion, while confusion is ensured using a discretized Lorenze chaotic map which take in to account the limited power and accuracy in the sensor node. Statistical and differential analysis including image histogram, correlation analysis, NPCR and UACI were obtained using Wsim/Wsnet simulators, indicating good confusion and diffusion properties compared with other ciphers including the original AES. To measure the power consumption of the proposed algorithm, authors implemented the proposed security scheme in a real sensor nodes platform (SensLab), which is equipped with Ti MSP430f1611 micro-controller. Results for energy consumption (simulation and experimental results) were better than that for the original AES. In addition to that, the execution time of the simulated ciphers indicated a reduced execution time for the proposed approach by 1/6 of the AES

execution time. The proposed work didn’t provide details about the key space and key sensitivity analysis.

- In [11] an efficient and secure partial image encryption scheme for WMSN using DWT, chaotic maps and a substitution box was presented. DWT was applied to get the LL sub-band that have 1/4 of the image details, then discretized Piece-wise linear chaotic map(PWLCM) and discretized Nonlinear chaotic map were used to shuffle image columns and image rows respectively. In the diffusion step, they used discretized Intertwining logistic chaotic map to XOR the output of the permutation step. Finally, to enhance the confusion property they substituted image pixels with corresponding values in the substitution box. The proposed scheme was verified via MATLAB2015 using a system with 3.0 GHZ CPU, 4 GB memory, and standard security parameters indicated that the scheme can resist various statistical and differential attacks, while providing a reduced power consumption and execution time due to the incorporation of DWT.

  The calculated NPCR value (less than 99%), indicates the cipher's vulnerability to some types of differential attacks. In addition to that, the test is conducted using only one standard test image (Baboon 128x128), which is not sufficient to generalize the calculated results. From the performance perspective, using three different chaotic maps with different dimensions and large key space (10^135) may lead to more power consumption.

2.6. Summary

In this chapter we have presented a background about the WVSN, followed by its security requirements and the available defense mechanisms. To guarantee the security

of the captured images, we have provided a comprehensive study about the different encryption algorithms that have been used in the scope of WVSN, including a comparative study about their security and performance analysis. At last, we have reviewed the last research works that concerned about the investigation of new encryption schemes for WVSN.

3. Proposed Security Scheme

3.1. Introduction

In this chapter, we present our proposed work to protect the transmitted image content in WVSN. First, we discuss the proposed security scheme and its components. After that, we clarify the theory behind the proposed encryption algorithm. Finally, we discuss the function of the encryption and decryption algorithms that we employed to provide a comprehensive image crypto-system.

3.2. The Proposed Scheme for Image Compression and Encryption

Visual sensors capture much information that varies in its importance and sensitivity. Moreover, the required security level in a specific node is affected by both the application in which it is employed, and its spatial location within that application. To achieve the main security requirements within the constrained visual nodes in WVSN, EIES provides an adaptive image cryptographic scheme that is based on the combination between DWT image compression and an enhanced encryption algorithm. The included encryption algorithm provides fast and robust image encryption through the application of bidirectional AES-128 algorithm in CBC mode and modifying it using a chaotic-based bit level permutation step.

EIES aims to provide an adaptive compression/protection mechanism for the transmitted images within WVSN. To do so, the captured image is encrypted fully or partially using the proposed algorithm at the sensor node and transmitted to the sink node through a set of intermediate nodes. Conversely, the original image is reconstructed at the sink node via the decryption algorithm. A key expansion algorithm is used to expand the round keys that are used in both encryption and decryption

algorithms. The encryption, decryption and key expansion algorithms form the crypto-system within the EIES.

Partial image encryption is used to provide the different levels for the image compression/encryption in EIES. Accordingly, two main factors influence the use of partial image encryption in EIES; First, we aim to provide secure and fast image encryption and transmission, with a reduced power consumption. Second, the variable sensing relevance property in WVSN, which prioritizes sensor nodes according to their spatial location within the monitored field, motivated us to provide a corresponding prioritized compression/encryption scheme. Compared with other encryption schemes, EIES has the ability to support both partial and full image encryption adaptively and prolong the network lifetime as a whole.

Two complimentary phases are included in partial image encryption; image compression phase, followed by the encryption phase.

- In the compression phase, we have reduced the amount of the transmitted data using wavelet-based image compression. The selection of the DWT based compression is related to its distinguished features including the multi-resolution characteristic and high quality reconstructed images. The ability to decompose an image to several resolution sub-bands allows controlling the amount of image details that will be encrypted and transmitted, leading to superior energy compaction and reduced resources consumption, facilitating real-time image transmission.
- In the encryption phase, we have encrypted the compressed image using a modified version of the AES-128 algorithm. The new algorithm overcomes the original AES shortcomings in image encryption including its long execution time, unstable

diffusion property and pattern appearance problem. To reduce the execution time of the exhaustive MixColumns transformation in the original AES-128, we have replaced it with a light and robust bit-level permutation step based on Chirikiv standard map. Additionally, to overcome the pattern appearance property, we have applied the encryption algorithm in CBC mode, such that redundant input blocks will not provide redundant ciphered blocks. Moreover, applying the encryption algorithm within EIES in CBC mode guarantees its diffusion property. Finally, to enhance the diffusion of the image, we have applied the 10 rounds of the algorithm in a bidirectional way, such that no degradation occurs for the diffusion metrics, and thus differential attacks become infeasible.

3.2.1. Levels of the Proposed Security Scheme

Benefiting from the sensing relevance approach, sensor nodes with high sensing relevance monitor more critical observations and preferred to have higher image quality and security level compared with other less relevant nodes. As a result, the amount of the encrypted and transmitted data in each node depends on its sensing relevance. The adopted security level at each node can be determined either dynamically by the sink node, or it may be statically predefined at the network deployment stage.

As illustrated in Figure 6, four main security levels are defined to form EIES.

1. **Level-1 (high image quality and security):** The priority is given to the image quality and security necessities here, so the entire image is encrypted using the proposed encryption algorithm, while the compression phase is discarded.

2. **Level-2 (Moderate image quality and security):** We apply one-level DWT image compression to obtain 1/4 of the image size, and encrypt the compressed image using the proposed algorithm.
3. **Level-3 (low image quality and security):** We apply two-level DWT image compression to obtain 1/16 of the image size and encrypt the compressed image using the proposed algorithm.
4. **Level-4 (No security):** image is compressed using Three-levels wavelet transformation and transmitted directly without performing the encryption step.

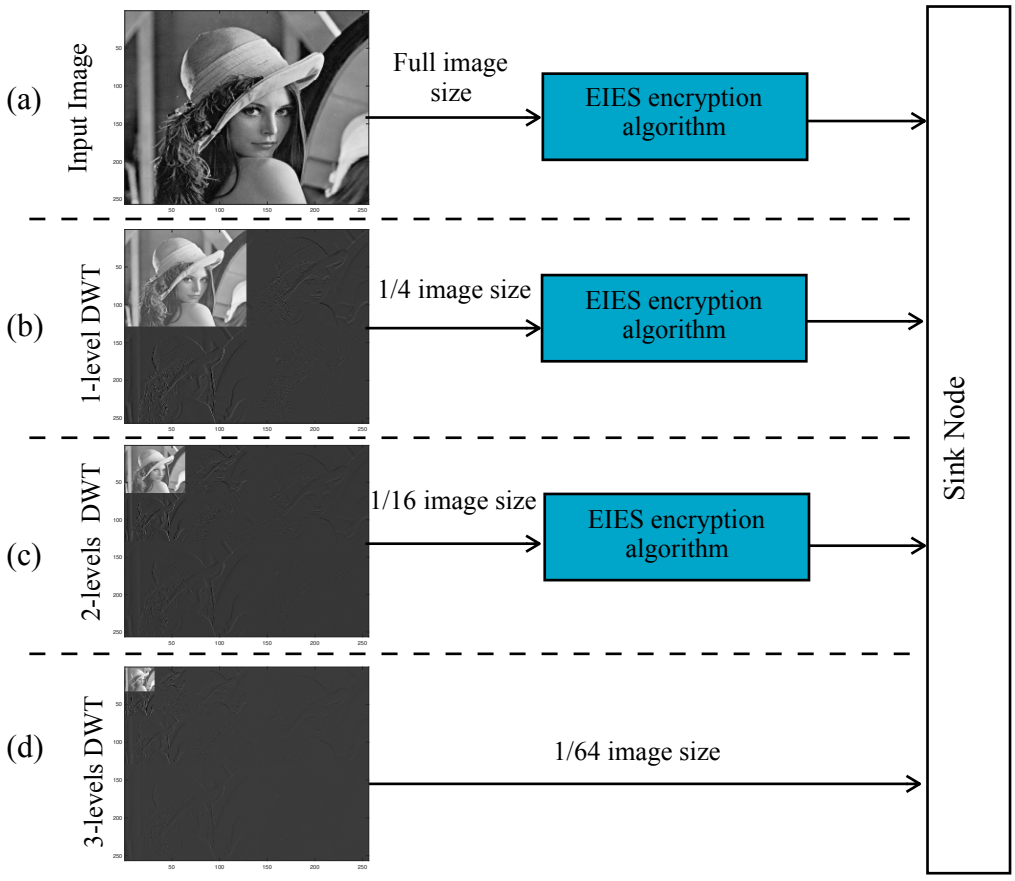


Figure 6. Levels of the proposed security scheme: (a) Level-1 (b) Level-2 (c) Level-3 (d) Level-4

In the first level of the EIES we encrypt the captured image fully to guarantee high reconstructed image quality with high security priority. Such robust security level is

recommended for a selected small group of nodes, where the FoV of their cameras covers critical areas that contain the top secret data. Next, two scales are defined to provide two various moderate and low image quality/security levels, including Level-2 and Level-3. In Level-2, one level wavelet decomposition is performed to encrypt and transmit a reduced amount of the image information. Most of the network nodes adopt this level since it provides a satisfactory balance between security and image quality. In the third level of the EIES image compression is combined with LL2 sub-band image encryption, providing a reduced image quality and security. Since LL1 and LL2 sub-bands contain the most important 1/4 and 1/16 of the image details respectively, the required resources to encrypt the image and its subsequent transmutation is significantly reduced, satisfying both acceptable reconstructed image quality and good encryption strength. Finally, for no security necessity, 3-levels wavelet decomposition is used to transmit the LL3 sub-band image details without any security overhead. Such no security level may be attached to the newly entered nodes to be modified later based on it's sensing relevance, which will be determined according to it's FoV. Furthermore, sensor nodes which have no sufficient residual resources may adopt this level to provide monitoring services only.

3.3. The Proposed Encryption Algorithm Components

In this work, we have proposed a modified AES cryptographic algorithm to provide a fast and robust image encryption, with reduced resources consumption. The proposed algorithm enhances the AES using three main modifications; incorporating CBC mode of operation, replacing the MixColumns with a chaotic-based bit level permutation step and finally applying the encryption in a bidirectional manner. In the following section

we illustrate the theory behind the employment of each component in the cryptographic algorithm.

3.3.1. Modified Advanced Encryption Algorithm

As a first step, the employed partial image encryption provides significant resources usage reduction and hence extends the node's lifetime. In the second step; we need to select a proper encryption algorithm that has the ability to resist against several known attacks, with a reduced encryption time.

The selection of Rijndael among other standard cryptographic algorithms in our work was studied carefully from both security and resource consumption perspectives.

As mentioned in chapter 2, and based on results obtained from the comparative studies conducted in previous works, which compared the standard ciphers applicability in traditional WSN and its resource requirements, AES with 128 bit key size and 10 rounds has a reduced energy consumption and operation time compared with other ciphers with the same key size such as RC5 and RC6. On the other hand, the use the 256 byte S-box in AES demands more memory requirements. To meet such requirements, WVSN is equipped with nodes that have more processing capabilities and larger storage.

From a security perspective, the selection of AES-128 with the full 10 rounds is related to its robustness against several statistical and differential attacks, in addition to its wide key space which proved its strength against brute-force attack. Compared with other ciphers; using RC5 or RC6 with the same parameters(128 bit key and 10 rounds), RC5 and RC6 were found vulnerable to several differential attacks.

Generally, traditional encryption algorithms including AES still have some drawbacks that prevent its applicability for image encryption in WVSN.

- First, the bulky data size within images increases the computational cost, hardware requirements and execution time of the encryption process dramatically. Moreover, the complex MixColumns transformation in the standard AES that uses matrix multiplication requires a considerable computational overhead and execution time, so image real-time encryption and transmission will not be achieved. To solve this problem, a new robust diffusion step with minimized computations and execution time is required.

  From another perspective, and since the captured image contains large number of input blocks, the application of the AES-128 in the basic EBC mode will degrade the cipher's diffusion property. This is because changing one pixel can affect only the block which it belongs to, while other blocks will not be affected. As a result, the algorithm will be more vulnerable to differential attacks. To tackle this issue, a suitable cipher mode that has the ability to propagate the effect of any change in the input image to all ciphered blocks is required.

- Second, images are characterized by their pattern redundancy property. More clearly, if an input image contains identical gray scale regions, some patterns will occur within the ciphered image in the same regions. As a result, a corresponding degradation in its statistical analysis will happen. To solve this problem, a suitable cipher mode needs to be used.
- Third, adjacent pixels are highly correlated in digital images compared with scalar data. Consequently, a robust confusion mechanism is required to redistribute the pixel values effectively within the encrypted image.

To overcome the previous three shortcomings, We have improved the standard AES-128 algorithm using the following modifications:

A. Instead of MixColumns transformation, we have employed chaotic based bit level permutation to reduce the MixColumns complexity, and enhance the confusion property.

B. CBC mode of operation has been utilized to reduce the image pattern redundancy and enhance the diffusion property.

3.3.1.1.Chaotic-Based Bit Level Permutation

Because discretized chaotic based image encryption has proven its superior role in real-time image encryption while providing robust confusion and diffusion properties, we have replaced the complex MixColumns transformation in the original AES with another simpler bit level permutation step based on the standard chaotic map.

Usually, applying the permutation process at the pixel level is used to enhance the confusion property of the encrypted image and reduce the correlation between adjacent pixels. The proposed bit-level permutation aims to change the pixel values and positions at the same time, based on a permutation process in which bits within the input block exchange their positions using a specific chaotic equation.

Two-dimensional chaotic map provides a mapping rule from the original position in the plain image to another pseudorandom position in the ciphered image. Several area preserving chaotic maps are used for pixel permutation. However, all chaotic systems can be used to encrypt digital images, but the performance and efficiency of such crypto-systems, in terms of security, depend mainly on the technique and how to use the chaotic equations. We choose to use Chirikov standard map for the bits permutation step

due to its efficiency in the domain of pixel shuffling, in addition to its simple mathematical operations.

Chirikov standard map is an invertible area preserving chaotic map from a square with side 2π on to itself, it generates its values in the space of two dimensions x and y. The mathematical representation of Chirikov map is defined as follows [55]:

$$(x_i, y_i) \longmapsto (x_{i+1}, y_{i+1}), \begin{cases} x_{i+1} = (x_i + y_i) mod(2\pi) \\ y_{i+1} = (y_i + k sin(x_i + y_i)) mod(2\pi) \end{cases} \quad (2)$$

Where k is the control parameter that satisfies($k > 0$), and the ith states (x_i and y_i) both take real values in the range $0, 2\pi$) for all i.

To incorporate Chirikov standard map into image encryption that operates on finite set, it needs to be discretized. Although the properties of the discretized chaotic maps are not good as in the continuous ones, the most useful features of the continuous Chirikov map, including the mixing property and sensitivity to initial condition are inherited in its discretized version.

Discretized Chirikov standard map is obtained by changing the map range from the square $[0,2\pi)\times[0,2\pi)$ to the discrete range NxN. It is defined as follows [55]

$$(x_i, y_i) \longmapsto (x_{i+1}, y_{i+1}), \begin{cases} x_{i+1} = (x_i + y_i) mod(N) \\ y_{i+1} = (y_i + k sin \frac{2\pi x_{i+1}}{N}) mod(N) \end{cases} \quad (3)$$

Where *k* is a positive integer that represents the control parameter and N represents the image height or width.

- **The application of the Standard chaotic map for bit-planes permutation**

In digital images, each pixel in an image with 256 gray levels is represented by 8-bit format, given by [59]:

$$B(x, y) = b(7)b(6)b(5)\ldots b(0) \tag{4}$$

Where $B(x, y)$ refers to the value of the pixel at coordinate (x, y) and the number in parentheses indicates the bit index from highest bit 7 to the lowest bit 0.

We can deal an image with 256 gray levels as 8 independent bit-planes ordered from the most significant bit-plane to the least significant bit-plane, and each bit-plane is a binary image since only two possible values (0 or 1) exist for each pixel.

The bit-level based permutation is achieved by applying the chaotic map based bit shuffling at each bit-plane independently. After that, the image is reconstructed by combining the 8 permuted bit-planes together. The permuted image is given by [59]:

$$B'(x, y) = b'(7)b'(6)b'(5)\ldots b'(0) \tag{5}$$

Where $b'(i)$ is the shuffled bit-plane and $(i \in [1:8])$.

Figure 7 shows the test image (Lenna 256x256), followed by its 8 bit-planes that are combined to reconstruct it again. In the same way, Figure 8 shows the permuted bit-planes using Chirikov standard map with different control parameters, ordered from the lowest to the most important bit-plane, followed by the reconstructed permuted image.

One bit may carry different amount of information depending on its position within the image pixel. For instance, one bit at the 8th position in the pixel represents the value 128, while in the first position of the same pixel it represents the value 1.

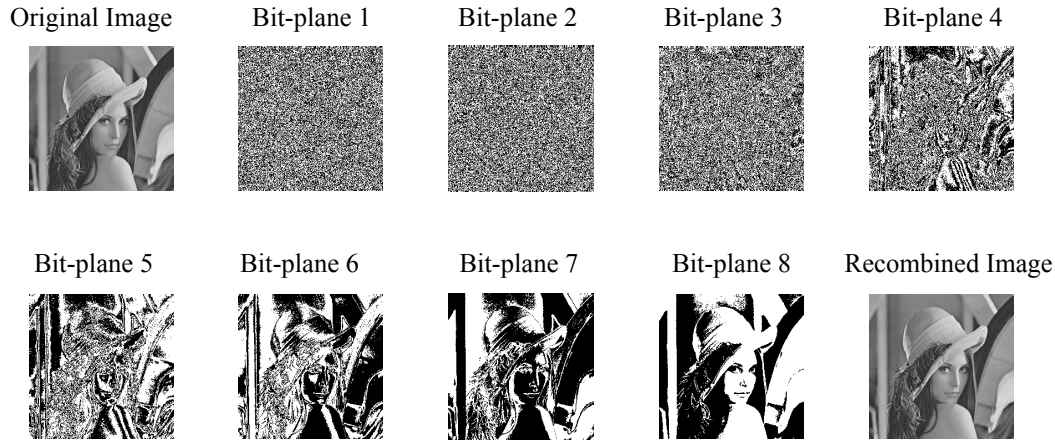


Figure 7. The original image (Lenna), followed by its bit-planes from the lowest bit-plane to the highest, and the recombined image

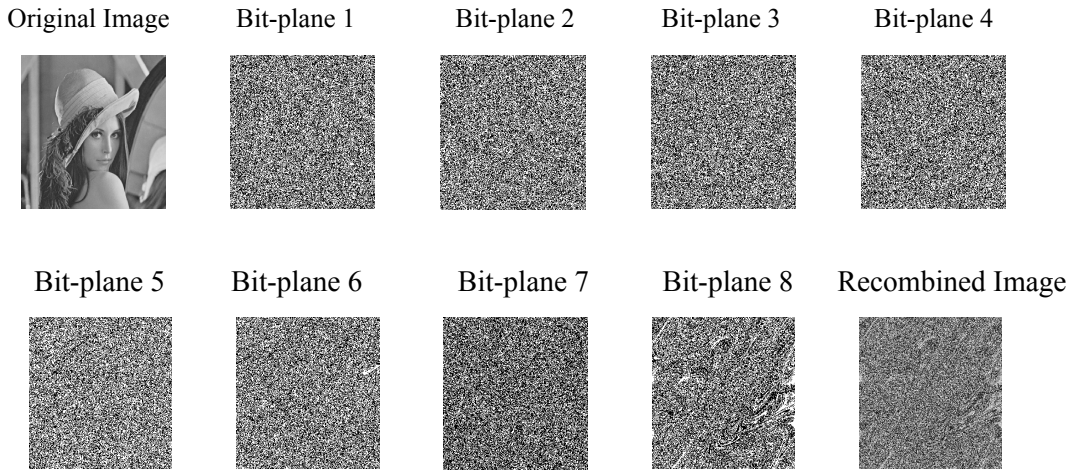


Figure 8. The original image (Lenna), followed by its permuted bit-planes from the lowest bit-plane to the highest, and the recombined permuted image

Table 2 clarifies the percentage of the image information carried by different bit positions (i) within a pixel, which is calculated using the following formula [59]:

$$P(i) = \frac{2^i}{\sum_{i=0}^{7} 2^i} \tag{6}$$

Table 2. Percentage of pixel information contributed by different bits

Bit position	Contribution Percentage
1	0.39
2	0.78
3	1.57
4	3.14
5	6.27
6	12.55
7	25.10
8	50.20

As we can see, the higher 4 positions (8,7,6,5) contribute by 94.12 of the pixel value, while the lower 4 positions affect the pixel value only by 5.88%. Based on this observation and to reduce the resource requirements to perform this step within the constrained WVSN nodes, we shuffled the pixel bits that have the higher contribution in the pixel value, so only the bit-planes (8,7,6,5) are shuffled using different control parameters, while the lower bit-planes are lifted unchanged. Figure 9 provides the

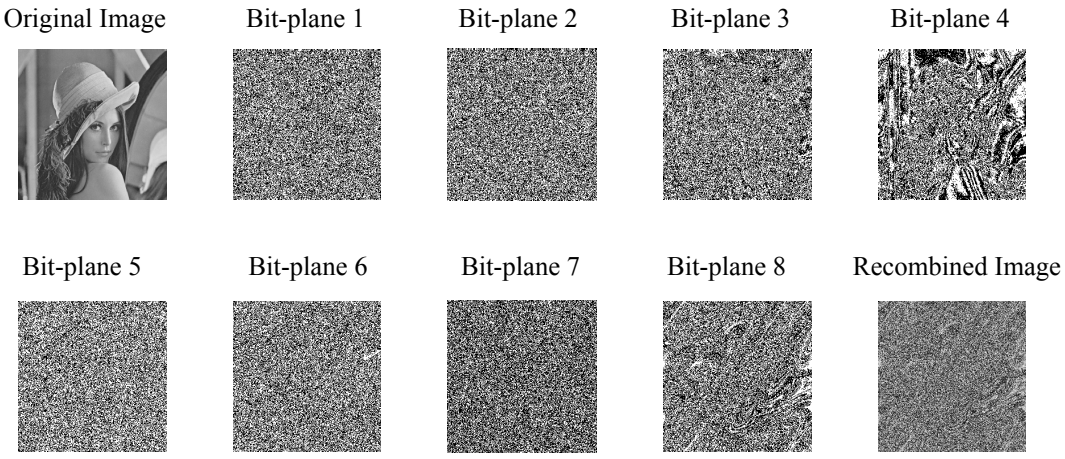


Figure 9. The original image (Lenna), followed by the bit-planes (1,2,3,4) and the permuted bit-planes (5,6,7,8). Finally the recombined image using the 8 bit-planes

result of shuffling only the bit-planes (5,6,7 and 8), while keeping the other bit-planes unchanged.

3.3.1.2. CBC Mode of Operation

Image encryption using the AES-128 with ECB mode is not feasible because it will be prone to differential attacks. Moreover, due to the image's redundancy property, we need to use a specific mode that has the ability to hide any correlated redundancy in the ciphered image, because it may reveal a clue that the original image has identical grayscale value in the related area, making the algorithm more vulnerable to statistical attacks.

Through the process of selecting a proper mode of operation, we take in to account the need to use a mode that provides confidentiality, with a reduced power consumption. Depending on [43] and compared with other cipher modes, the power consumed by AES-128-CBC and AES-128-CFB in MicaZ and TelosB sensor nodes is the least. Moreover, results in [1] showed that the entropy values of the AES algorithm executed using the CBC and CFB modes are near the ideal value of 8. Depending on the previous explanation, both of CBC and CFB modes are close to each other, so we employed the most commonly used mode of operation; CBC mode. The operation of CBC is defined as follows:

CBC encryption:
$$C_1=\text{CIPHER}(P_1 \oplus IV)$$
$$C_i=\text{CIPHER}(P_i \oplus C_{i-1}) \quad (7)$$

CBC decryption:
$$P_1=\text{INVCIPHER}(C_1) \oplus IV$$
$$P_i=\text{INVCIPHER}(C_i) \oplus C_{i-1} \quad (8)$$

Where Pi and Ci are the input block and ciphered block respectively, IV is an initialization vector used for the first block encryption and decryption steps.

- **CBC mode to guarantee the diffusion property**

Since the strength of the diffusion property depends on the ability of the cipher to provide a totally different image when making a slight change in the input image, we have calculated the resultant NPCR and UACI of changing the first pixel value within the input image (Cameraman 512x512), which was encrypted using the AES-128 with ECB and CBC mode of operation. As we observe from the differential analysis results in Figure 10, the importance of the CBC mode lies in its ability to spread the effect of the slight change in the first input block not only within the same block, but also to the whole image.

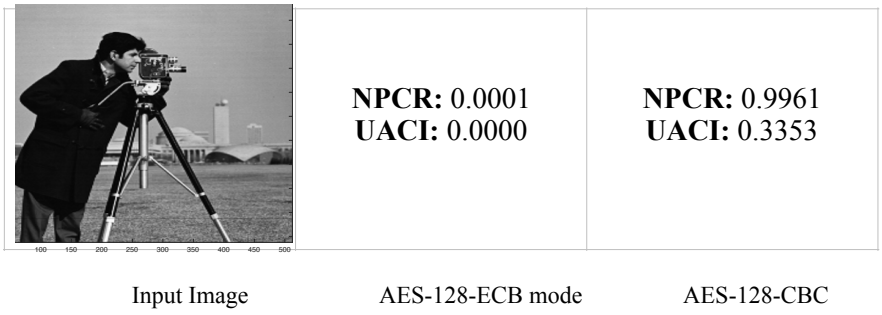
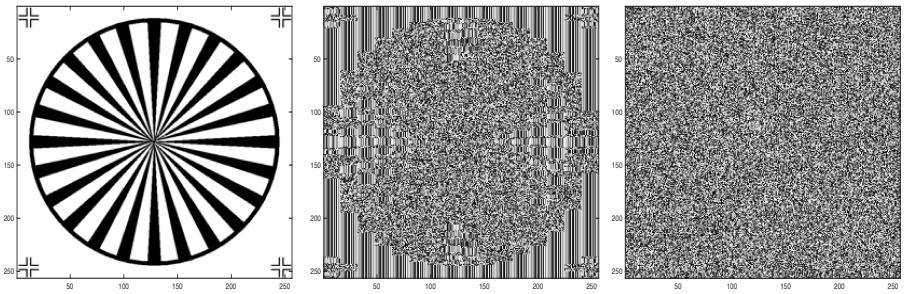


Figure 10. NPCR and UACI results obtained after encrypting the test image (Cameraman) twice with one bit difference using AES-128 algorithm in EBC mode and CBC mode.

- **CBC mode to reduce the pattern redundancy property**

To clarify the effect of pattern redundancy property, we encrypted the input image(Testpat 256x256) in Figure 11 using the original AES-128 in ECB mode. Since the original image has some pattern redundancy, the encrypted image shows a related redundancy in the same region and hence the scene visibility of the ciphered image and other statistical analysis will indicate some relationship between redundant pixels. On

the other hand, encrypting the image with AES-128-CBC mode hides the redundancy effect in the ciphered image.



Input Image AES-128-ECB mode AES-128-CBC mode

Figure 11. The effect of different cipher modes on the encrypted image pattern redundancy

3.3.1.3.Bidirectional Based Image Encryption

The previous one-directional standard and modified encryption algorithms deal with the image content sequentially. As illustrated in Figure 12, pixels are encrypted and decrypted in order from the top left corner to the bottom right one.

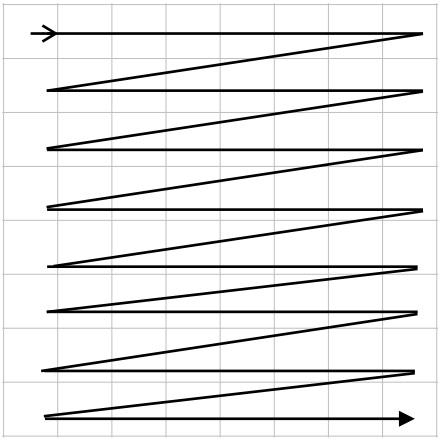


Figure 12. Scanning order of the conventional encryption and decryption algorithms

In the first version of the EIES we have applied the previous two modifications (modified AES-128 using bit-level permutation and CBC mode), while keeping other AES parameters unchanged. Figure 13 shows the corresponding encryption and decryption process.

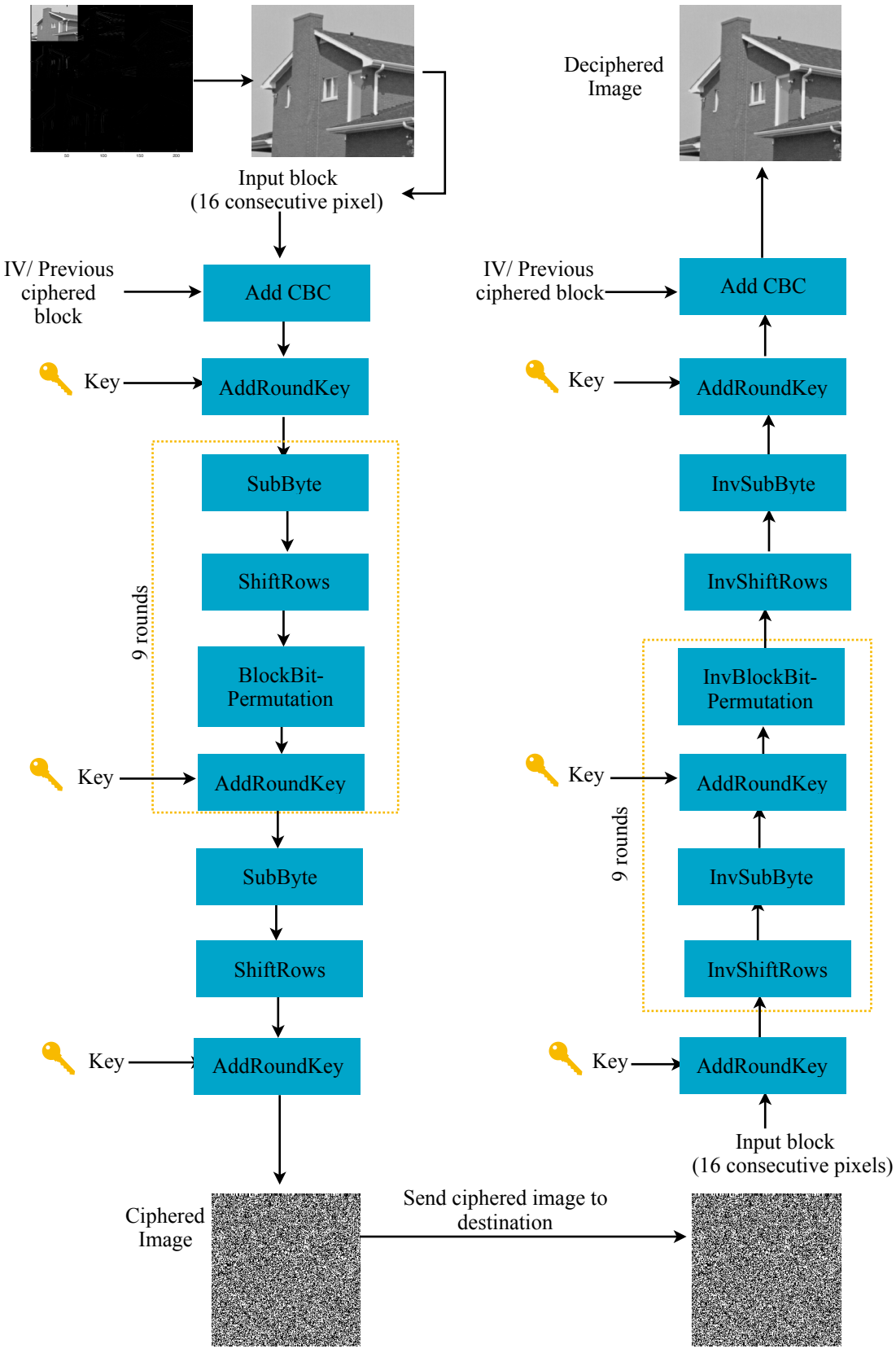


Figure 13. Encryption and decryption algorithms within the proposed security scheme (version 1)

The obtained results (refer to chapter 4 to view the statistical and differential analysis) showed a significant reduction in the encryption time and satisfactory statistical and differential analysis results. Accordingly, the strength of the encryption algorithm is as good as other recent works in the domain of image encryption within WVSN.

The use of CBC mode enhances the cipher resistance against differential attacks, and provides comparable NPCR and UACI results. Actually, to find the resistance of the encryption algorithm against differential attacks, encrypting two images with only one bit difference should provide a totally different ciphered image. This is achieved in the previous works and version 1 of EIES if the pixel having the changed bit is at the beginning of the image. Nevertheless, while moving to the image's bottom right corner, the effect of changing a pixel value on the NPCR and UACI metrics will be reduced dramatically.

Chaotic encryption performs the confusion and diffusion steps for several rounds to spread the effect of the changed pixel to the entire image (forward and backward). Moreover, new approach have been suggested to reduce the number of required permutation/diffusion steps, while keeping the cipher's properties using an enhanced bidirectional diffusion process. To overcome the inability of the traditional AES and other block based encryption algorithms to provide stable resistance against differential attacks, we have proposed to use a bidirectional encryption approach, in which instead of applying the 10 rounds of AES-128 in one direction, we use 5 rounds for the forward encryption phase, while the other 5 rounds are used to encrypt the image in a backward order. Doing so, the effect of changing one bit at any position within the image would spread to the whole image, and hence a robust defense against differential attacks will

be guaranteed. Figure 14 illustrates the new bidirectional image encryption. Clearly, using bidirectional encryption will enhance the cipher's features and distribute the changed pixel effect quickly.

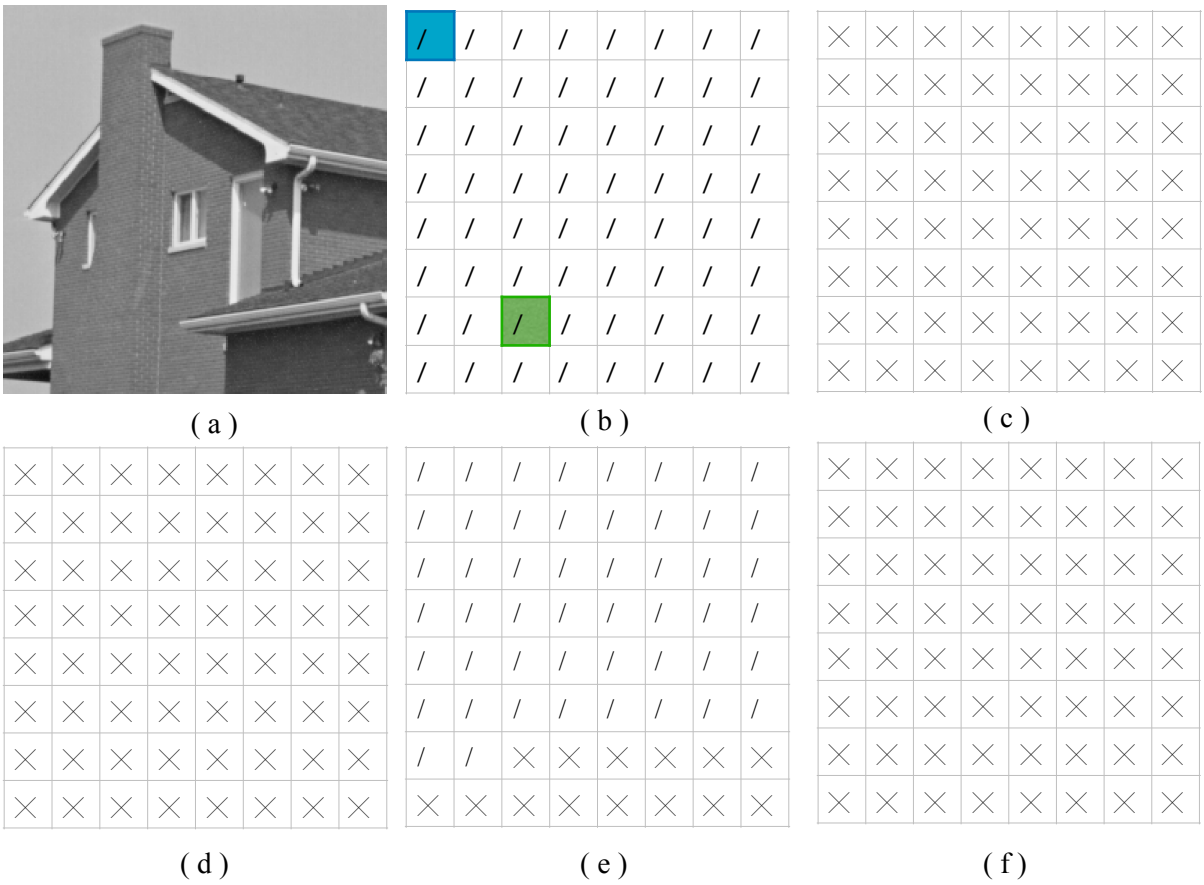


Figure 14. The effect of encrypting the same image with a slight change in one pixel, using 1 directional and bidirectional encryption (a) The original image (b) the ciphered image (c, d) 1-directional and bidirectional encryption after changing the blue pixel value in the original image (e, f) 1-directional and bidirectional encryption after changing the green pixel value in the original image.

3.4. The Proposed Crypto-System Algorithms

The crypto-system within EIES includes the following three algorithms:

- An encryption algorithm which is a modified version of the conventional AES-128.
- A key expansion algorithm used to provide the encryption and decryption algorithm with the required secret keys (identical to the key schedule in the AES-128).

- A decryption algorithm used to inverse the encryption process, and reconstruct the original image at the destination.

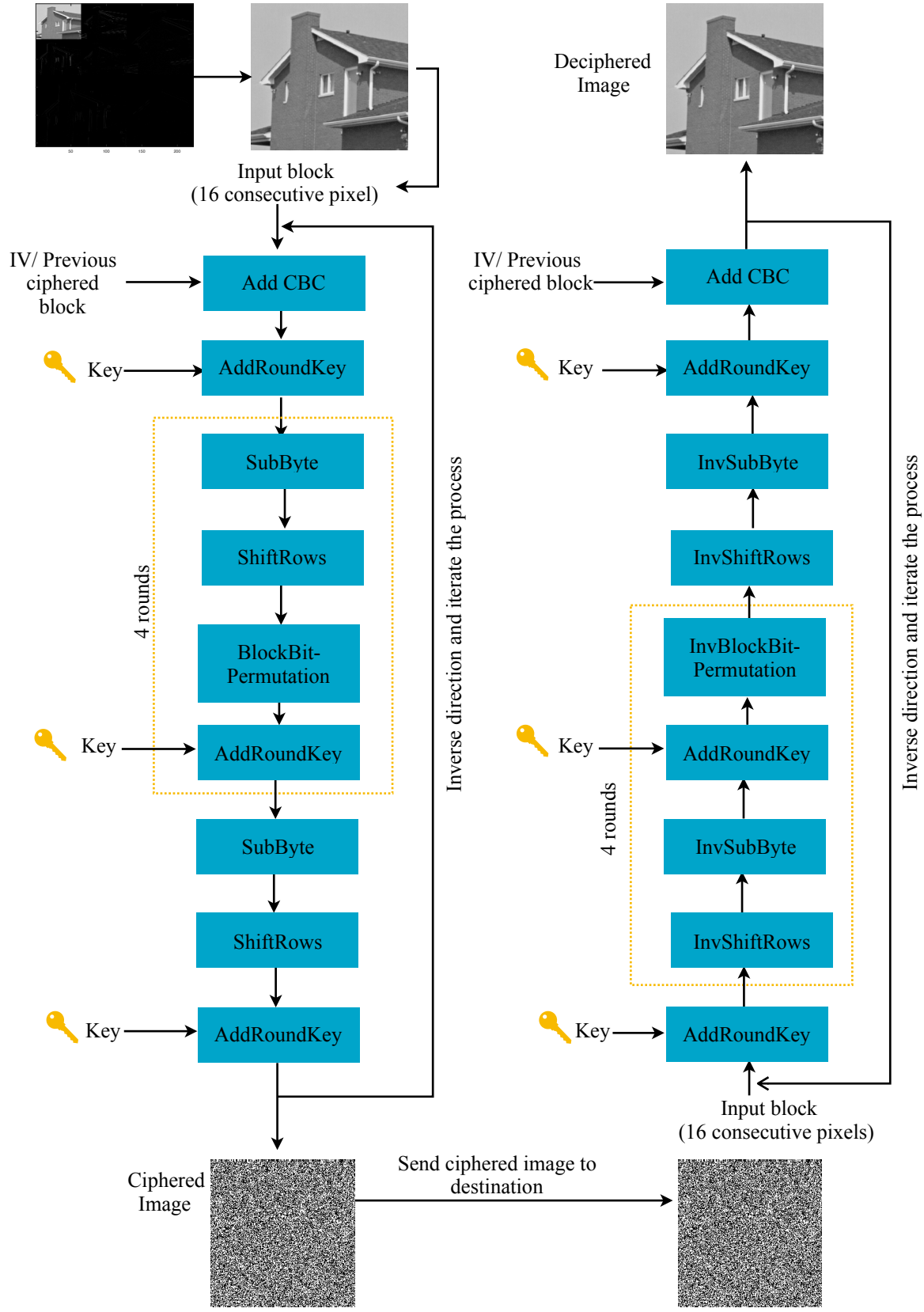


Figure 15. Encryption and decryption algorithms within the proposed security scheme (version 2)

A. Image Encryption Algorithm

To encrypt a captured image locally in a sensor node within the WVSN, the following procedure is executed:

1. The input image is determined according to the adopted image quality/security level, which is influenced by the node sensing relevance. For partial encryption, the most significant part of the image is obtained using the 2-D DWT.
2. The input to the encryption algorithm is a block, also called a state of 16 consecutive image pixels, Scanning order starts from the top left corner to the bottom right one.
3. AddCBC: To enhance the cipher's resistance against the common differential attacks and overcome the image pattern redundancy property, we defined an AddCBC transformation, in which the CBC mode of operation is used to XOR the output of the previously encrypted block with the current input block. To involve CBC mode an initial vector (IV) with 128 bit size is used to be XORed with the first input block.
4. Instead of iterating the 10 rounds in one direction, bidirectional encryption is employed such that the first 5 rounds are applied in the regular scanning order, while the last 5 rounds are applied in the reverse direction. i.e we will encrypt the image in two phases. In the first phase, we will encrypt the input image blocks using 5 rounds. While in the second phase, another 5 rounds are performed on the inverted version of the obtained image. Accordingly, each block will be encrypted using 10 rounds, but with different execution order. To incorporate the bidirectional block based image encryption, we replaced the 5th round in the original AES-128 with

another round that is similar to the last round, such that the cipher remains invertible. As shown in Figure 14, the first 4 rounds in both phases are identical, consisting of the following transformations:

a. Substitution transformation (SubByte)

Similar to original AES, in this step each byte in the state matrix is substituted with a corresponding byte in the AES S-box which serves as a lookup table. SubByte transformation works as shown in Figure 16 [5].

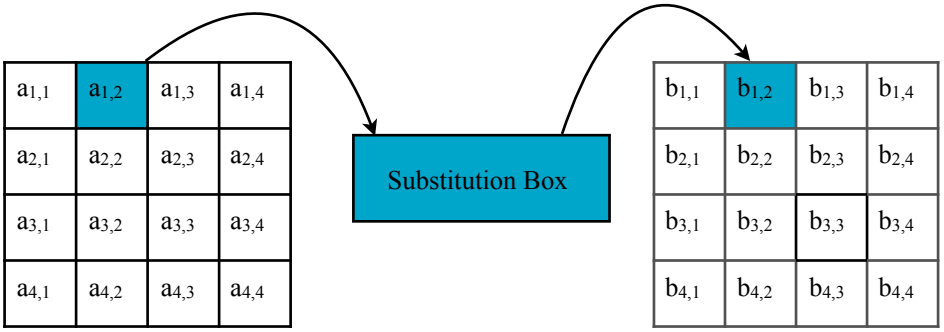


Figure 16. SubByte transformation

b. Shift rows transformation (ShiftRows)

It is a permutation process that operates on the state rows; such that each row is cyclically shifted to the left by a certain offset. As illustrated in Figure 17, the first row remains unchanged, while the bytes within the second, third and fourth rows are shifted by one, two and three bytes respectively [1].

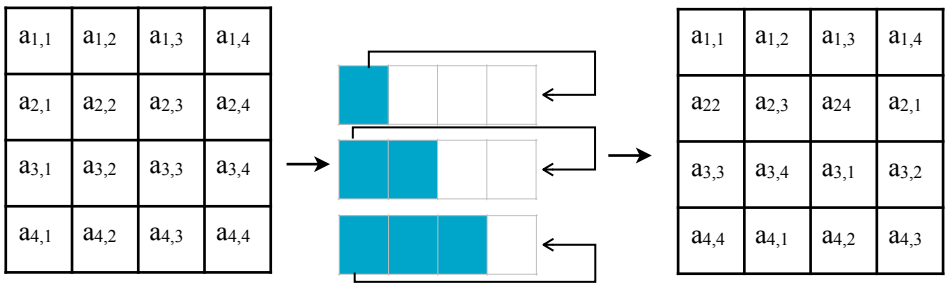


Figure 17. ShiftRows transformation

c. Chaotic-based bit permutation transformation (BlockBitPermutation)

In this step the state is treated as a 4x4 image that can be represented by 8 bit-planes. Bits that belong to (8,7,6,5) bit-planes are chaotically permuted using the Chirikov standard map, with 4 unique control parameters. Since discretized chaotic map proved its compatibility in the domain of image encryption, moving the bit-plane elements chaotically make the value of any byte in the state dependent on 4 other different bytes and thus enhance the cipher's diffusion property. Additionally, since the control parameters work as the mystery key, the key length of the encryption algorithm will be extended. In Table 3 bits at position (A) in the 16 pixel input block will be permuted chaotically, also bits at position (B, C, D) also will be permuted using the standard chaotic map. Depending on that, each pixel is affected by another four pixels selected in a random manner.

Table 3. BlockBitPermutation transformation

A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H
A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H
A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H
A B C D E F G H	A B C D E F G H	A B C D E F G H	A B C D E F G H

d. Add the round key transformation (AddRoundKey)

In this step, the round key obtained from the key expansion algorithm is XORed with the state. To make the two encryption phases dependent on each other, we have used the last key used in the first phase to initialize the second phase.

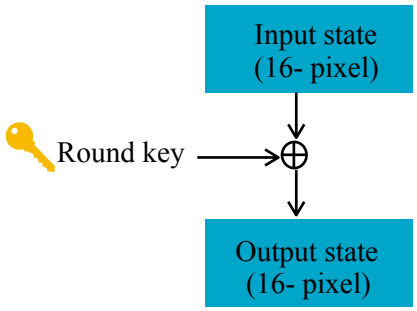


Figure 18. AddRoundKey transformation

5. The last round in the two phases of the EIES bidirectional encryption algorithm is similar to the last round in the original AES algorithm. A SubByte step, followed by ShiftRows and AddRoundKey transformations are applied sequentially.

The activity diagram in Figure 19 illustrates a detailed sequence of the included activities within the encryption algorithm in EIES.

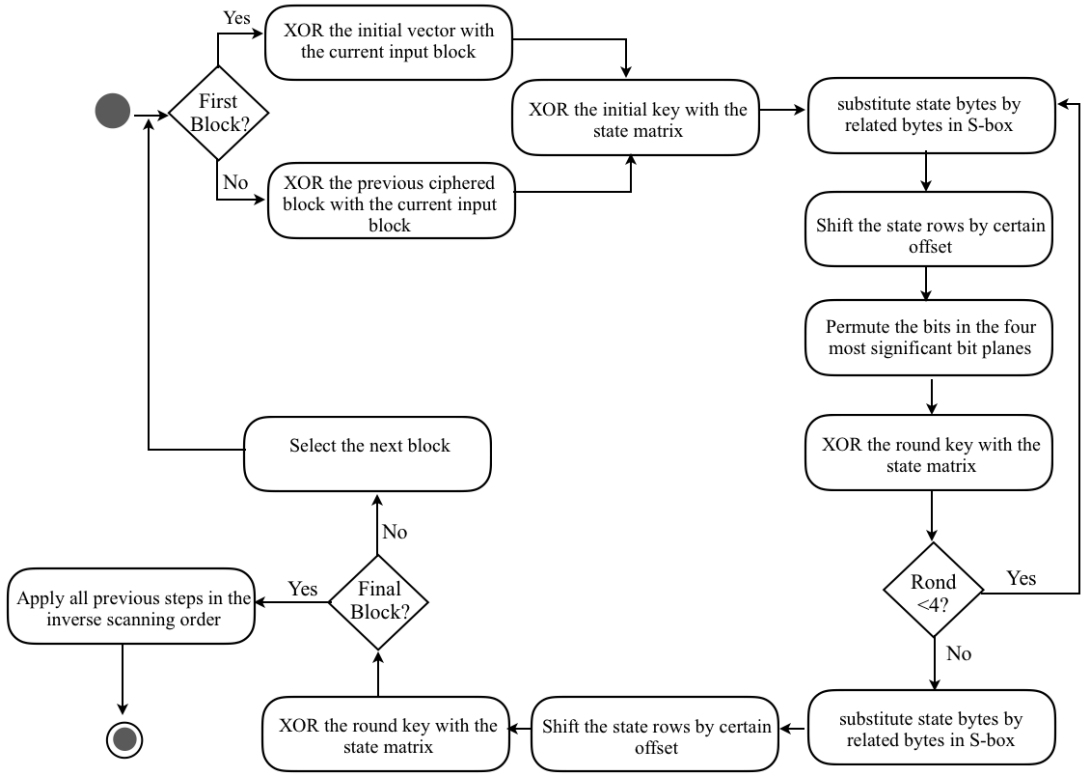


Figure 19. Activity diagram of the encryption algorithm in EIES

B. Image Decryption Algorithm

The encryption algorithm in EIES is an invertible algorithm. The decryption algorithm allows the image reconstruction at the sink node, to be analyzed and used for several purposes. As shown in Figure 14, the decryption algorithm reverses the process of the encryption algorithm using a set of transformations that flips the process of the corresponding transformations in the encryption algorithm. First, the encrypted image is decrypted in the inverse direction of the regular cipher's scanning order and an intermediate version of the decrypted image is obtained. After that, the intermediate image is decrypted in the regular scanning direction. Five rounds are used in each step to retrieve the original image.

The followings are the main transformations within the decryption algorithm:

- Inverse the shift rows transformation (InvShiftRows)

In this step each row is cyclically shifted to the right by a certain offset; the first row remains unchanged, while the bytes within the second, third and fourth rows are shifted by one, two and three bytes respectively.

- Inverse the substitution transformation (InvSubByte)

This is a substitution operation in which each byte in the state is substituted by a corresponding one from the inverse S-box; which is simply an S-box runs in reverse.

- Add the round key transformation (AddRoundKey)

As in the encryption algorithm, a 128-bit round key is used to be XORed with the state bytes.

- Inverse the chaotic-based bit permutation transformation (InvBlockBitPermutation)

Chirikov standard chaotic map is used in this step to inverse the effect of the BlockBitPermutation transformation. Accordingly, bits in the four bit-planes that have

the highest contribution in the image are re-permuted chaotically using the same four control parameters, which we have employed in the encryption process.

C. Key expansion algorithm

To expand the rounds sub-keys from an input 128-bit key, we employed the original Rijndael key schedule to obtain 10 different round keys. The operation of the key expansion algorithm works as follows:

1. The input key (K_0) is represented by 4x4 bytes, where bytes within the same column are related to the same word. Words are ordered from W_0 to W_3.
2. To obtain the first word of the key K_i, the following rule is used:

   Rule 1: $K_n : W_0 = K_{n-1} : W_0 \oplus SubByte(K_{n-1} : W_3 << 8) \oplus Rcon_i$

   Where K_n is the current sub-key, W_i is the word i within the key K_n ,(<<8) is a circular left shift operation by 8 bits and $Rcon_i$ is the round constant.
3. To obtain the second, third and fourth words of the round key K_i , rule 2 is employed:

   Rule 2: $K_n : W_i = K_{n-1} : W_i \oplus K_n : W_{i-1}$

The process is iterated until the required 10 keys are calculated. Figure 20 shows the 44 words which are obtained from the key expansion algorithm.

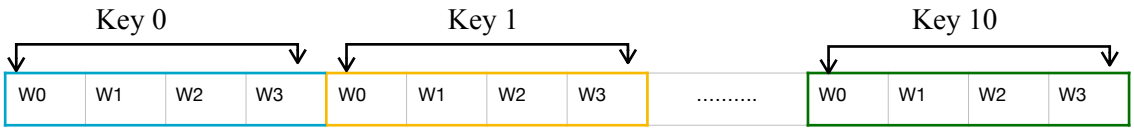


Figure 20. Round keys obtained from the Key expansion algorithm

3.5. Summary

In this chapter, we have presented the theoretical basis behind our work including the several components that we used to modify the original AES-128 and enhance its operation for image encryption in WVSN. In addition to that, we have illustrated the two versions of the proposed cryptographic algorithm. The first version depends on the use of AES-128 with CBC mode and chaotic a bit level permutation step instead of the exhaustive MixColumns transformation. Although we obtained satisfactory performance and security results, we have demonstrated the reason behind the incorporation of bidirectional image encryption in the second version. Finally, we have discussed the proposed crypto-system algorithms, including the encryption, decryption and key expansion algorithms.

4. Performance Evaluation and Security Analysis

In this chapter, we describe the analysis that have been carried out to evaluate the strength of the proposed cryptographic algorithm and the encryption execution time. Additionally, we present a comparative analysis between our algorithm including its two versions, and another three recent works that we have implemented beside the implementation of the proposed encryption algorithm.

Robust crypto-systems can resist several kinds of attacks, including brute-force attack, statistical attacks and differential attacks. In order to demonstrate the effectiveness of the EIES, we have analyzed a set of security parameters to ensure that the captured image in WVSN can't be reconstructed by illegal parties. Accordingly, MAD is used as a key sensitivity metric, while for the statistical analysis we have analyzed the image histogram, entropy, scene visibility and correlation coefficients. Finally for the differential analysis we have calculated the NPCR and UACI values.

We have encrypted a set of standard test images, using MATLAB_R2016a, installed on MacBook Pro with 2.2 GHz Intel Core i7 processor and 16 GB memory. Depending on the encrypted images, we have compared the strength of the proposed cryptographic algorithm with other recent works in [4-6]. In addition to that, we have calculated the execution time of the encryption process in EIES, and compared the obtained results with the other works. To simplify the illustration we have named the compared algorithms. AES-5 round refers to the work in [5], AES-128 refers to one of the security schemes that were proposed in [4] and Shift-AES is the proposed algorithm in [6]. In addition to that, we have evaluated the security of the first version of our work to clarify

the strengths of the bidirectional image encryption compared with one directional algorithms.

The reminder of this chapter is organized as follows. Section 4.1 presents the key space analysis of the proposed algorithm. In section 4.2 the key sensitivity analysis are conducted, while section 4.3 provides the statistical analysis. In section 4.4 we present results for the NPCR and UACI parameters, which are mainly used to indicate the robustness of the diffusion step in the algorithm and its ability to resist differential attacks. Results of the algorithm's execution time are shown in section 4.5. Finally, in section 4.6 we provide a concluding discussion about the obtained results.

4.1. Key Space Analysis

The key space in reliable encryption algorithms has to be large enough to make brute-force attack infeasible. Consequently, the key space need to be more than 2^{100} [29] to make the brute-force attack computationally insufficient. The original AES-128 algorithm is considered secure since it provides a key space of 2^{128}. Moreover, the proposed encryption algorithm provides an enlarged key space due to the use of Chirikov standard map for the bit-level permutation step. The standard map has a control parameter (k) that acts as a part of the whole secret key. Assuming that the length of the secret key is K, then $K= (k_{AES}+k_{BLP})$, where $k_{AES}=128$ is the size of the AES-128 key, and k_{BLP} is the size of the chaotic control parameter which $\in N^{+}$, where N is a natural number.

To calculate the total secret key size, we set the size of different control parameters which are used for the chaotic bit permutation to 8 bits. Accordingly, k_{BLP} size will be

32 bit because we use 4 different control parameters to permute bits in the four most significant bit-planes. The obtained K has (128+32) bit size, which equals 160 bit. Based on that, the encryption algorithm within EIES provides 2^{160} key space. The most powerful supercomputer can perform up to nearly hundred quadrillion Floating Point Operation Per Second (FLOPS). Accordingly, we have calculate the number of the required years to crack EIES encryption algorithm using the following formulas [56] :

$$\text{Number of years to crack encryption algorithm} = \frac{s}{c \times t} \tag{9}$$

$$c = \frac{nFlops}{nc} \tag{10}$$

Where s is the key space, c is the number of the combination checks per second and t is the number of seconds in one year. We calculated c using formula 10 where nFlops is the number of the Flops that can be processed using the latest super computer and nc is the number of Flops that are required per combination check.

The obtained result indicated that EIES has the ability to resist brute-force attacks because it require more than 10^{22} years to be cracked.

4.2. key Sensitivity Analysis

This test is used to emphasize the strength of the confusion property in the proposed encryption algorithm and its sensitivity to different keys. An intruder may guess parts of the encryption key and try to reconstruct the plain image from its corresponding ciphered image using this key. To confirm the key sensitivity of the proposed

cryptographic algorithm, we have conducted a key sensitivity test to show that two slightly different secret keys lead to an entirely different encrypted image.

As we mentioned in the previous section, the secret key in this work depends on both the original AES key and the chaotic map control parameter. Based on that, a tiny modification in any part of the encryption key should change the encrypted image entirely. To study the algorithm's key sensitivity property, we have encrypted the input image with the following keys:

K0=k_{AES}+k_{BLP}

Kb=$k\acute{}_{AES}$+k_{BLP}

Kc=k_{AES}+$k\acute{}_{BLP}$

Where K0 is the original encryption key, Kb and Kc are another two keys obtained by changing only one bit in the AES-128 key and the control parameter respectively.

We have conducted the key sensitivity test by calculating the Mean of the Absolute Difference (MAD) between a pair of two ciphered images (C,Ć). C and C´ were obtained by encrypting the same input image with a two slightly different keys (K0,Kb) and (K0,Kc). MAD is defined as follows [29] :

$$MAD(C, C') = \frac{1}{W \times H} \sum_{i,j} | C(i, j) - C'(i, j) | \tag{11}$$

Where W and H are the image width and image heigh.

Based on [60], the ideal value of MAD equals $\frac{l}{3}$, where l is the number of the possible states for each image element (pixel). Since each pixel is represented by 8 bits, l equals

2^8; representing 256 different states. If the encrypted images C and C´ are independent then MAD will be close to the ideal value which equals 256/3 or 85.3333.

To calculate MAD first we encrypted the input image to obtain (C,C´) using the pair of keys (K0,Kb), where the slight difference occurs in the K_{AES} part. The value of K0 and Kb in hexadecimal was set to:

K0=((ab 7e e9 e6 28 ad dd a6 bb f7 f5 d8 09 cf 4f 3c), (73, 2D, 62, 75))

Kb=((ab 6e e9 e6 28 ad dd a6 bb f7 f5 d8 09 cf 4f 3c), (73, 2D, 62, 75))

In the same way, we made a tiny change in the control parameter part to show that even if the attacker tried to check the validity of a specific key and by chance he entered the right AES part of the secret key, then the chaotic part of the encryption key will controvert the feasibility of the entered key. K0 and Kc values were set to the following values:

K0=((ab 7e e9 e6 28 ad dd a6 bb f7 f5 d8 09 cf 4f 3c), (73, 2D, 62, 75))

Kc=((ab 7e e9 e6 28 ad dd a6 bb f7 f5 d8 09 cf 4f 3c), (73, 2D, 60, 75))

We encrypted a set of grayscale standard test images using the proposed encryption algorithm (version 1 and version 2) and the other three algorithms. Several test conditions were set to track the change in MAD value, so images are encrypted fully or partially using DWT to obtain the image from LL1 sub-band and LL2 sub-band. Table 4 shows that the retrieved results for all of the of the algorithms provided MAD values that are very close to the ideal one, indicating high sensitivity to any slight change in the secret key.

Table 4. Mean Absolute Difference (MAD) for different test images

Input Image		EIES **version 2**		EIES **version1**		AES-128	AES-5 rounds	Shift-AES
		MAD $(C_{(K0)},C'_{(Kb)})$	MAD $(C_{(K0)},C'_{(Kc)})$	MAD $(C_{(K0)},C'_{(Kb)})$	MAD $(C_{(K0)},C'_{(Kc)})$	MAD $(C_{(K0)},C'_{(Kb)})$	MAD $(C_{(K0)},C'_{(Kb)})$	MAD $(C_{(K0)},C'_{(Kb)})$
Cameraman 512x512	Full encryption	85.3003	85.2960	85.2549	85.2630	85.3060	85.2414	85.2359
	LL1 band	85.6082	85.6856	85.3695	85.6710	85.1533	85.1751	85.1199
	LL2 band	85.6491	84.7018	86.4485	86.6653	85.16565	85.7599	84.5734
House 256x256	Full encryption	85.5485	85.3401	85.4342	85.4132	85.3449	85.8529	84.9458
	LL1 band	85.0853	84.8047	85.3052	84.9122	85.6774	84.9672	84.4078
	LL2 band	85.9282	85.2124	85.1826	84.0342	85.6726	85.9419	84.0715
Lenna 256x256	Full encryption	85.0744	85.0491	85.516	85.1519	85.3667	85.3605	85.2714
	LL1 band	84.7686	85.3359	86.4456	84.9902	84.9736	86.07568	85.3070
	LL2 band	85.0811	86.2263	83.9893	86.6272	87.0015	86.1240	84.5823

As we can see, AES variants proved its reliability against the key modification targeted attacks. In Table 5 we provide DIS1 and DIS2 values, which refer to the distance between the obtained MAD values and the ideal value DIS((MAD $(C_{(K0)},C'_{(Kb)})$, ideal MAD), DIS(MAD $(C_{(K0)},C'_{(Kc)})$, ideal MAD) respectively. Also, we calculated the average distance for each encryption algorithm.

Compared with other ciphers, the proposed algorithm in version 2 provides more uniform MAD results for different $(C_{(K0)},C'_{(Kb)})$ pairs. Additionally, the average change in the calculated MAD values with respect to the ideal value indicates that the proposed algorithm in its second version is more sensitive to a simple change in the secret key. Besides, changing one bit in the control parameter provides MAD values that are very close to the ideal value, so even with the same K_{AES} the ciphered image will be totally different with a slight change in the K_{BLP} part of the secret key.

Table 5. Distance between the calculated MAD value and the ideal MAD value

Input Image		EIES **version 2**		EIES **version 1**		AES-128	AES-5 rounds	Shift-AES
		DIS1	DIS2	DIS1	DIS2	DIS1	DIS1	DIS1
Cameraman 512x512	Full encryption	0.0330	0.0373	0.0784	0.0703	0.0273	0.0919	0.0974
	LL1 band	0.2749	0.3523	0.0362	0.3377	0.1800	0.1582	0.2134
	LL2 band	0.3158	0.6315	1.1152	1.3320	0.1676	0.4266	0.7599
House 256x256	Full encryption	0.2152	0.0068	0.1009	0.0799	0.0116	0.5196	0.3875
	LL1 band	0.2480	0.5286	0.0281	0.4211	0.3441	0.3661	0.9255
	LL2 band	0.5949	0.1209	0.1507	1.2991	0.3393	0.6086	1.2618
Lenna 256x256	Full encryption	0.2589	0.2842	0.1827	0.1814	0.0334	0.0272	0.0619
	LL1 band	0.5647	0.0026	1.1123	0.3432	0.3597	0.7424	0.0263
	LL2 band	0.2522	0.8930	1.3440	1.2939	1.6682	0.7907	0.7510
Average distance		0.3064	0.3175	0.4609	0.5954	0.3479	0.4146	0.4983

4.3. Statistical Analysis

Statistical attacks are common in cryptanalysis. Based on that, we have performed corresponding statistical analysis to prove the robustness of the encryption algorithm within the proposed EIES. The obtained results including the visibility analysis, image histogram, entropy and the correlation between adjacent pixels demonstrated the effectiveness of EIES against statistical attacks.

4.3.1. Visibility Analysis

The main purpose of image encryption is to hide the critical information within the input image. Consequently, Figures 21 and 22 clarify the perfect invisibility of the image content through the application of EIES (version2). The grayscale tested images are (House 256x256) and (Baboon 512x512). Also, Figure 23 shows the complete invisibility of the encrypted image (House 256x256) for various tested algorithms.

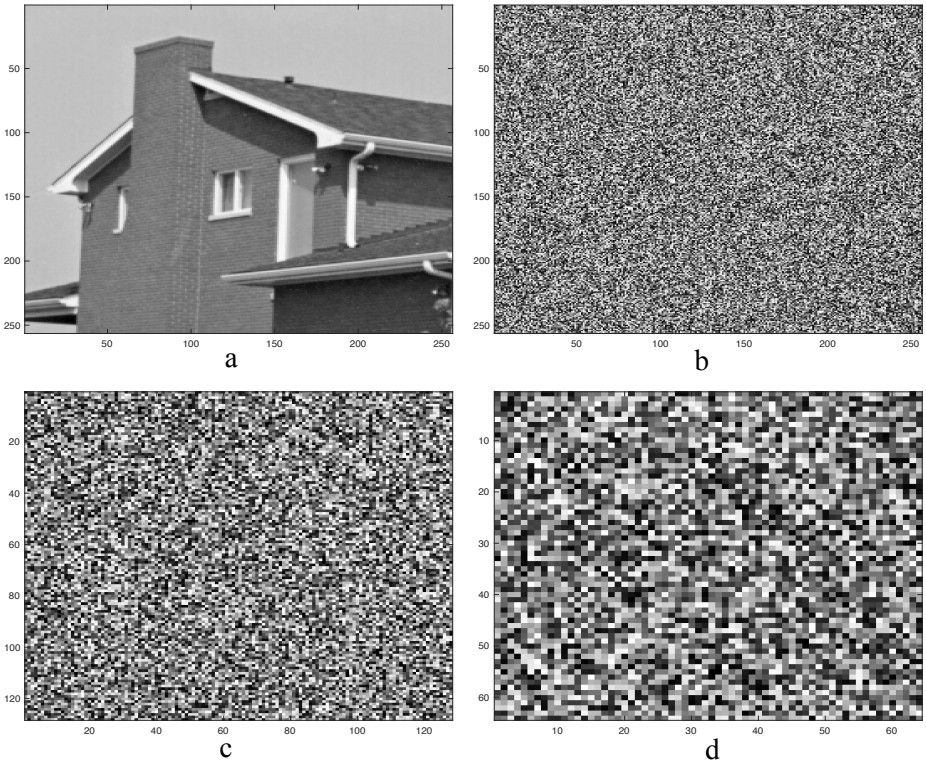


Figure 21. visibility analysis of the proposed algorithm (version2) for the image (House 256x256): (a) original image (b) Full image encryption (c) LL1 band encryption (d) LL2 band encryption

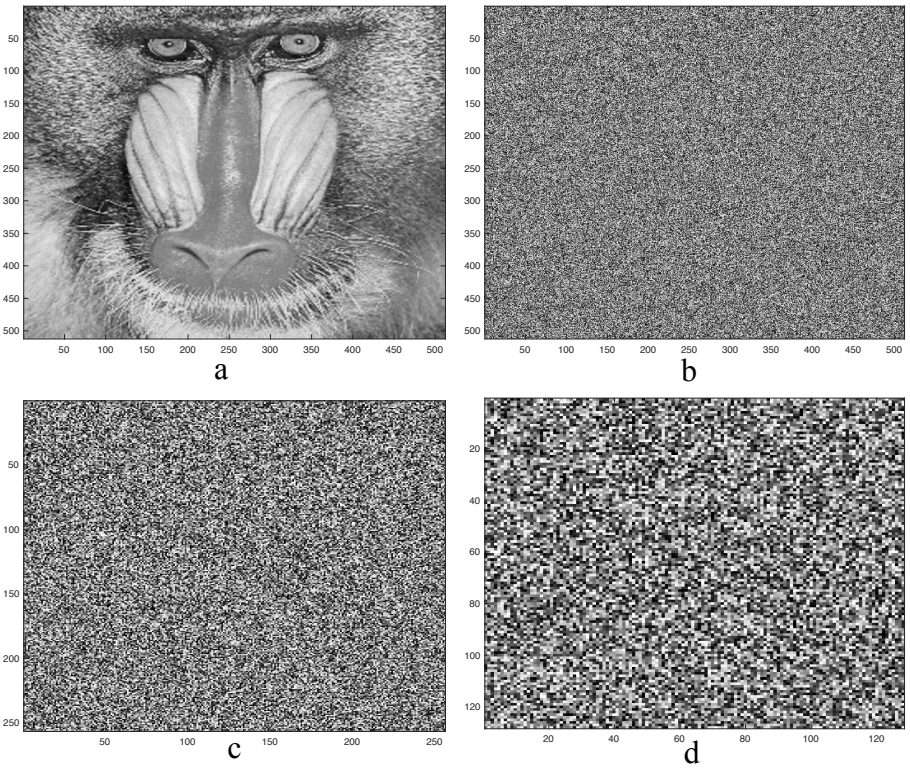


Figure 22. visibility analysis of the proposed algorithm (version2) for the image (Baboon 256x256): (a) original image (b) Full image encryption (c) LL1 band encryption (d) LL2 band encryption

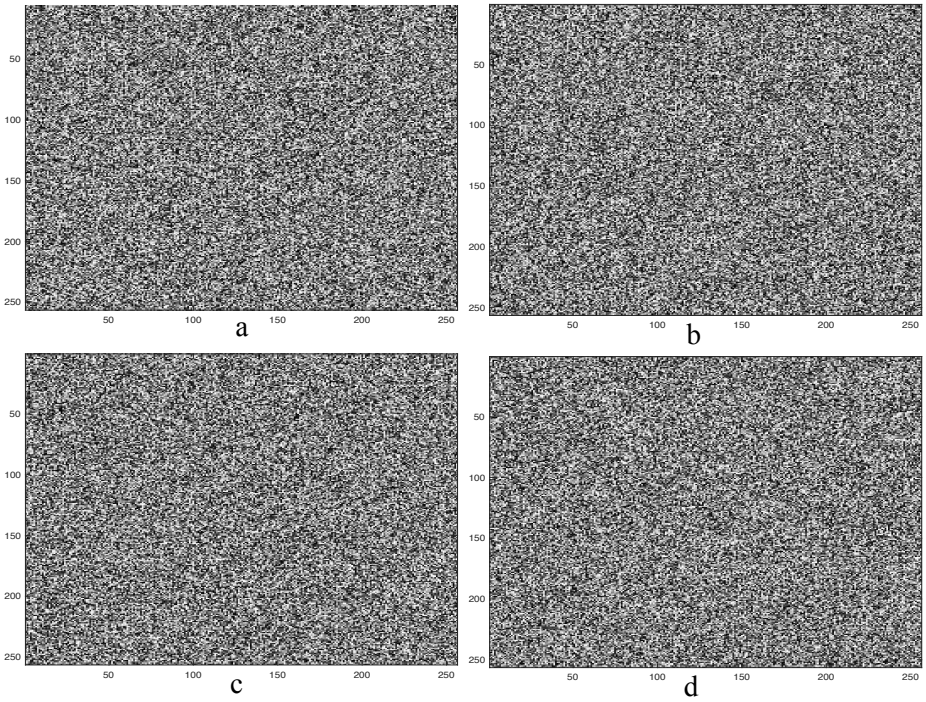


Figure 23. visibility analysis for the image (House 256x256) encrypted using various algorithms: (a) proposed algorithm (version1) (b) AES-128 (c) AES-5 rounds (d) Shift-AES

Colored Red,Green and Blue (RGB) image contains three main channels including red, green and blue channel. To encrypt a colored image, each channel is encrypted independently and ciphered image is obtained by recombining the three channels again.

Figure 24 provides the same content invisibility property which we obtained for the encrypted grayscale images. As we observe the RGB colored image which was encrypted using the second version of the encryption algorithm within EIES is completely different from the original image.

a b

Figure 24. Visibility analysis for the RGB image (Baboon 512x512): (a) original image (b) encrypted image

4.3.2.Histogram

The original image histogram should be totally different from the histogram of the corresponding ciphered image. The histogram of a 8-bit grayscale image has 256 gray intensity values at the x axis, while the y axis represents the number of the pixels that have a specific intensity value. The distribution of the image pixel's intensity values need to be flat to ensure its security.

To explore the distribution of the grayscale levels within the plain image and its cipher image, Figure 25 shows the histogram of the original grayscale test image (House 256x256) and its corresponding encrypted image which is ciphered fully using various algorithms. The proposed encryption algorithm results (version1 and version2) show that the histogram of the encrypted image has no relation with the original image histogram. In the same manner, the histogram of each channel within the encrypted RGB image (Baboon 512x512) in Figure 26 provides a uniform distribution for the different intensity levels. As a result, EIES histogram distribution for the encrypted images is comparable with the robust resource demanding AES-128 algorithm and other recent algorithms in the domain of image encryption within WVSN.

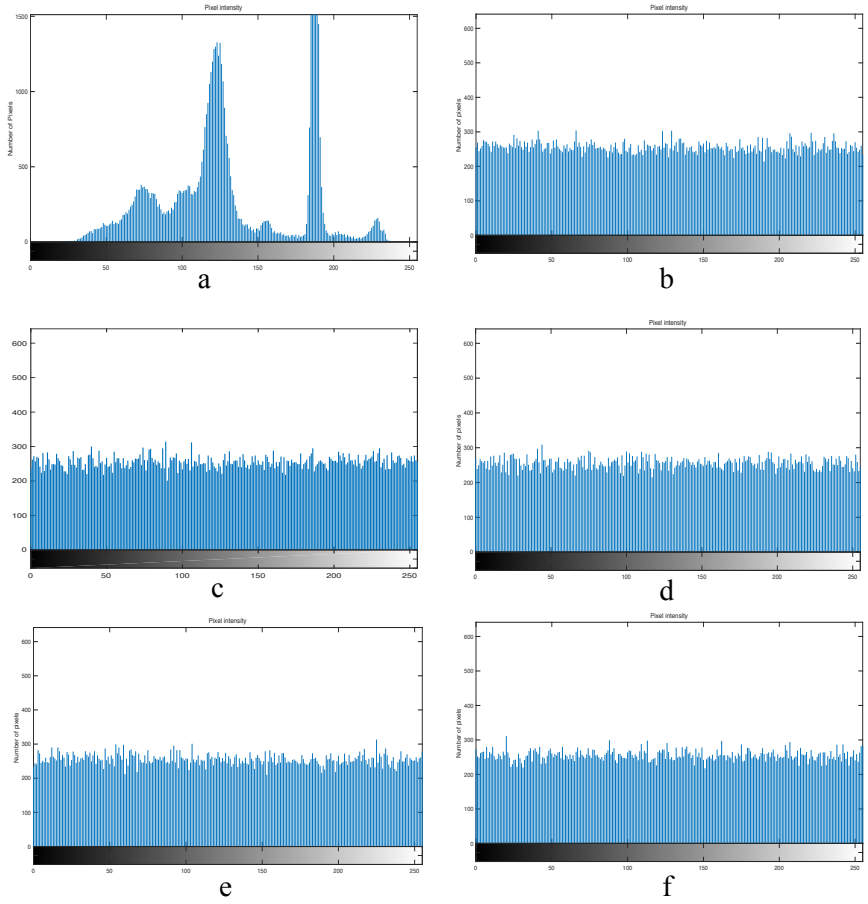


Figure 25. Histogram of the original image (House 256x256) and its ciphered images using different encryption algorithms: (a) The original image (b) The proposed algorithm (version1) (c) The proposed algorithm (version2) (d) AES-128 (e) AES-128 with 5 rounds (f) Shift-AES

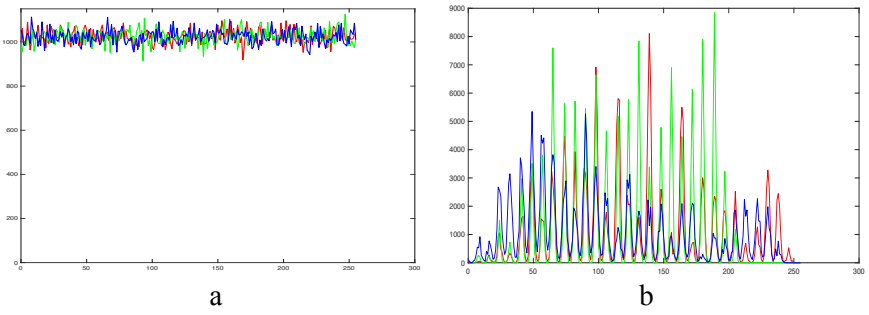


Figure 26. Histogram of the RGB image (Baboon 512x512): (a) Original image histogram (b) Ciphered image histogram

To find the distribution of the gray level values within the output image while using partial encryption, we have encrypted only the LL1 and LL2 sub-bands, which are

obtained by applying one level and two levels DWT based compression. Results are shown in Figures 27 and 28 respectively.

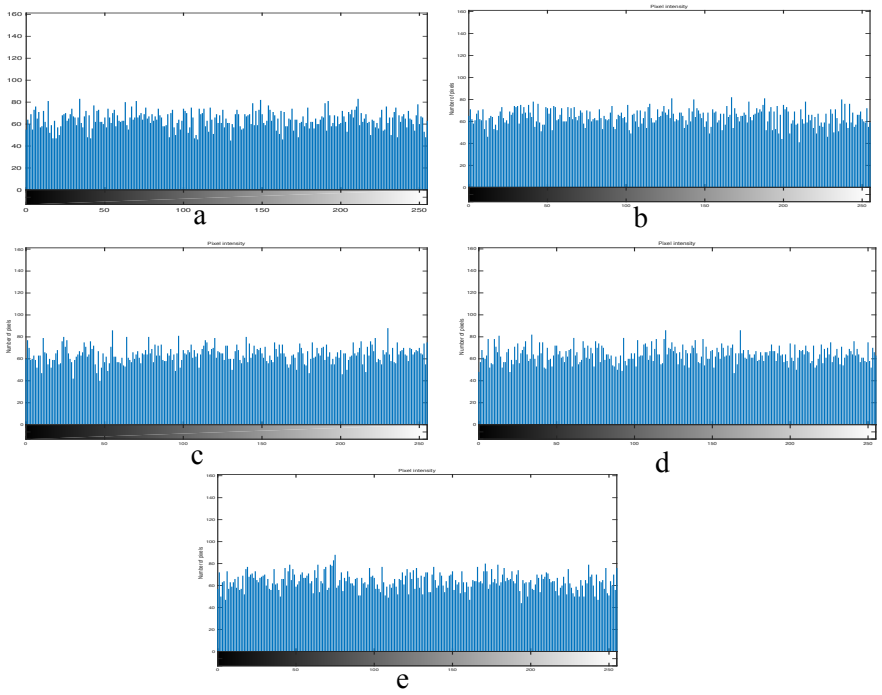


Figure 27. Histogram of the ciphered image related to the LL1 sub-band of the image (House) using different ciphers: (a) Proposed algorithm (version1) (b) Proposed algorithm (version2) (c) AES-128 (d) AES-128 with 5 rounds (e) Shift-AES-128

The histogram of the partially encrypted image is fairly uniform and does not reveal any clue about the plain image in all ciphers. Meanwhile, compared with the full image encryption, applying partial image encryption degrades the histogram of the obtained images. This appears slightly in Figure 27 and more obviously in Figure 28.

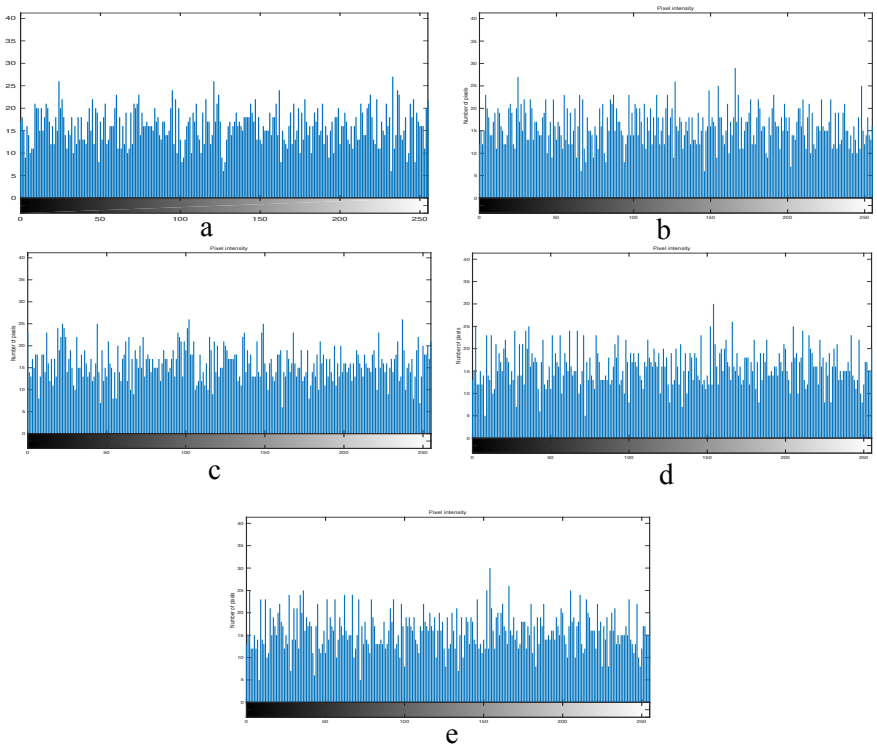


Figure 28. Histogram of the ciphered image related to the LL2 sub-band of the image (House) using different ciphers: (a) Proposed algorithm (version1) (b) Proposed algorithm (version2) (c) AES-128 (d) AES-128 with 5 rounds (e) Shift-AES

To investigate the reason of the degradation in the histogram for partial encryption, we have encrypted additional images with various sizes using the proposed algorithm (version2). Results in Figure 29 indicate that the distribution of the intensity values within the ciphered image histogram is proportional to the plane image size, because larger images candidate more number of pixels at each grayscale level and so, more uniform distribution in the ciphered image histogram.

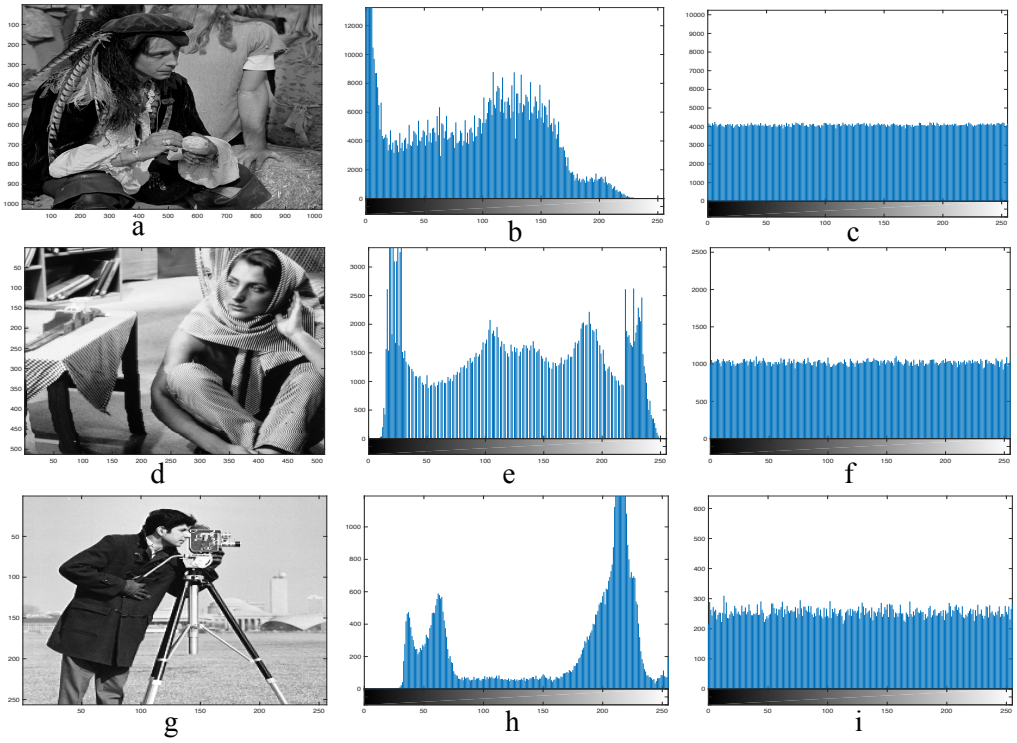


Figure 29. The histogram of the original and ciphered images using the proposed encryption algorithm (version2): (a, d, g) plain image (man 1024x1024), (Barbara 512x512), (Cameraman 256x256) (b, e, h) plain image histogram (c, f, i) ciphered image histogram

4.3.3. Entropy

Image entropy measures the disorder of the image data; the more the image content is random the harder it will be to recognize the encrypted image. The entropy (E) of an image (I) is expressed as follows [59]:

$$E = -\sum_{i=0}^{N} X_i log_2 X_i \tag{12}$$

Where X is the probability of the level of intensity i, and N is the total number of the intensity levels.

Usually, a grayscale image has 2^8 gray levels. Consequently, if the probabilities of the different 2^8 or 256 gray levels are equally, then the ideal entropy value must be equal to

eight. We calculated the entropy for a set of the pairs (E(I), E(C)) , where I is an input image, and C is the corresponding cipher image respectively. Since the image entropy depends on the probability of the intensity levels, its value has high correlation with the image histogram. Based on that, larger cipher images with well permuted pixels has better histogram. Moreover, their entropy values are closer to the optimal value 8 .

Tables 6 and 7 provide the entropy values and the entropy change rate for different pairs of the grayscale test images and the corresponding encrypted images. Higher entropy change rate indicates more randomness in the cipher image. Compared with other algorithms, the proposed encryption algorithm provides an average intensity change rate that is very close to the AES-128. Additionally, other algorithms provide entropy values that are very close to the ideal value 8, emphasizing their pseudorandom behavior.

Table 6. Entropy value of grayscale input image and corresponding encrypted image

Input Image		E(I)	E(C)				
			EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	7.0480	7.9992	7.9992	7.9993	7.9992	7.9993
	LL1 band	7.0515	7.9970	7.9974	7.9976	7.9967	7.9974
	LL2 band	7.0476	7.9884	7.9886	7.9893	7.9898	7.9871
Baboon 512x512	Full encryption	7.2925	7.9993	7.9993	7.9993	7.9993	7.9993
	LL1 band	7.4910	7.9978	7.9973	7.9968	7.9971	7.9974
	LL2 band	7.5393	7.9879	7.9890	7.9893	7.9877	7.9887
House 256x256	Full encryption	6.4971	7.9974	7.9966	7.9969	7.9970	7.9974
	LL1 band	6.5213	7.9903	7.9889	7.9896	7.9895	7.9893
	LL2 band	6.4700	7.9526	7.9548	7.9572	7.9521	7.9489

Table 7. Percent change of the entropy values for the input image and encrypted image

Input Image		Percent change				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	13.4960	13.4960	13.4974	13.4960	13.4974
	LL1 band	13.4085	13.4142	13.4170	13.4042	13.4142
	LL2 band	13.3492	13.3521	13.3620	13.3691	13.3308
Baboon 512x512	Full encryption	9.6921	9.6921	9.6921	9.6921	9.6921
	LL1 band	6.7655	6.7588	6.7521	6.7561	6.7601
	LL2 band	5.9502	5.9647	5.9687	5.9475	5.9608
House 256x256	Full encryption	23.0918	23.0795	23.0841	23.0857	23.0918
	LL1 band	22.5262	22.5047	22.5154	22.5139	22.5108
	LL2 band	22.9150	22.9490	22.9861	22.9073	22.8578
Average percent change		14.5772	14.5790	14.5861	14.5747	14.5684

Since RGB image channels are encrypted independently, image entropy is calculated by averaging the entropy values of the red, green and blue channels. Figure 30 provides the entropy values for the input image (Baboon 512x512) and its related encrypted image. The obtained average entropy result for the encrypted image (7.9993) is very close to the ideal value 8, indicating high randomness within the image content after encryption.

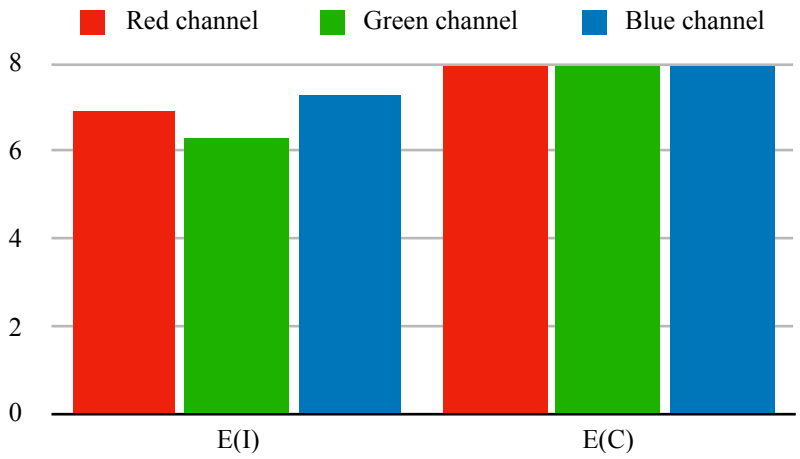


Figure 30. Entropy value for different channels in the RGB image (Baboon 512x512) and its ciphered image using EIES version 2

4.3.4. Correlation Analysis

Generally, the most extreme estimation of relationship coefficient in an image is 1 and it corresponds to high correlation, and the base is 0 corresponding to low correlation. Since Adjacent pixels in the plane image are highly correlated horizontally, vertically and diagonally, the relationship coefficient between two contiguous pixels is close to 1. On the other hand, a strong cipher ought to produce an encrypted image with relationship coefficient close to 0. By plotting the distribution of the contiguous pixels in the plain image and its related cipher image, we can test the correlation analysis visually.

To compare the correlation of the contiguous pixels in the original image and the cipher image, first we randomly selected 1000 pairs of the contiguous pixels in each direction from the plain image and the cipher image. After that, the correlation coefficient $r_{x,y}$ for each selected pair is calculated for both images using the following formulas [55]:

$$r_{x,y} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - D(x))^2)(\frac{1}{N}\sum_{i=1}^{N}(y_i - D(y))^2)}} \tag{13}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{14}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{15}$$

Where x_i and y_i are the grayscale values of the two adjacent pixels pair. N is the total number of the randomly selected samples.

We encrypted a set of test images to calculate the correlation coefficients in the plain images and cipher images. Accordingly, the results of the correlation between adjacent pixels in the horizontal, vertical and diagonal direction are listed in Table 8.

Table 8. Correlation coefficients of adjacent pixels for grayscale input image and its ciphered image

Input image		Correlation coefficients of the input image			Correlation coefficients of the encrypted image		
		Horizontal correlation	Vertical correlation	Diagonal correlation	Horizontal correlation	Vertical correlation	Diagonal correlation
Cameraman 512x512	Full image	0.9837	0.9897	0.9717	0.0409	0.0204	0.0349
	LL1 band	0.9454	0.9667	0.9355	-0.0391	0.0119	-0.0322
	LL2 band	0.9057	0.9625	0.8861	-0.0454	0.0191	-0.0576
House 256x256	Full image	0.9818	0.9670	0.9525	0.0270	0.0209	0.0158
	LL1 band	0.9494	0.9337	0.8908	-0.0137	-0.0216	-0.0085
	LL2 band	0.9025	0.8808	0.8509	-0.0076	-0.0226	0.0039
Lenna 256x256	Full image	0.9347	0.9728	0.9119	-0.0137	0.0215	0.0382
	LL1 band	0.9005	0.9529	0.8526	0.0139	-0.0113	-0.0273
	LL2 band	0.8081	0.9138	0.7395	0.0183	-0.0098	0.0140

In Table 9 we provided the correlation coefficients which were calculated after encrypting the grayscale input image (Baboon 128x128) using various encryption algorithms. The value of the correlation coefficient for all ciphers is close to zero.

Table 9. Correlation coefficients of adjacent pixels for different encryption algorithms

Encryption algorithm	Correlation coefficients of the input image			Correlation coefficients of the cipher image		
	Horizontal correlation	Vertical correlation	Diagonal correlation	Horizontal correlation	Vertical correlation	Diagonal correlation
EIES (**version2**)	0.8726	0.8428	0.7811	-0.0414	-0.0055	0.0282
EIES (**version1**)	0.8726	0.8428	0.7811	-0.0368	0.0037	0.0458
AES-128	0.8726	0.8428	0.7811	0.0094	-0.0389	-0.0165
AES-5 rounds	0.8726	0.8428	0.7811	-0.0558	0.0132	0.0086
Shift-AES	0.8726	0.8428	0.7811	-0.0181	0.0456	0.0400

In Figure 31 we plotted the correlation distribution of two adjacent pixels in the plain image and the cipher image. Generally, the correlation between adjacent pixels in all directions for the input image approaches to 1, while it is close to zero for the cipher image. The obtained results indicate the strength of the confusion step in the cipher.

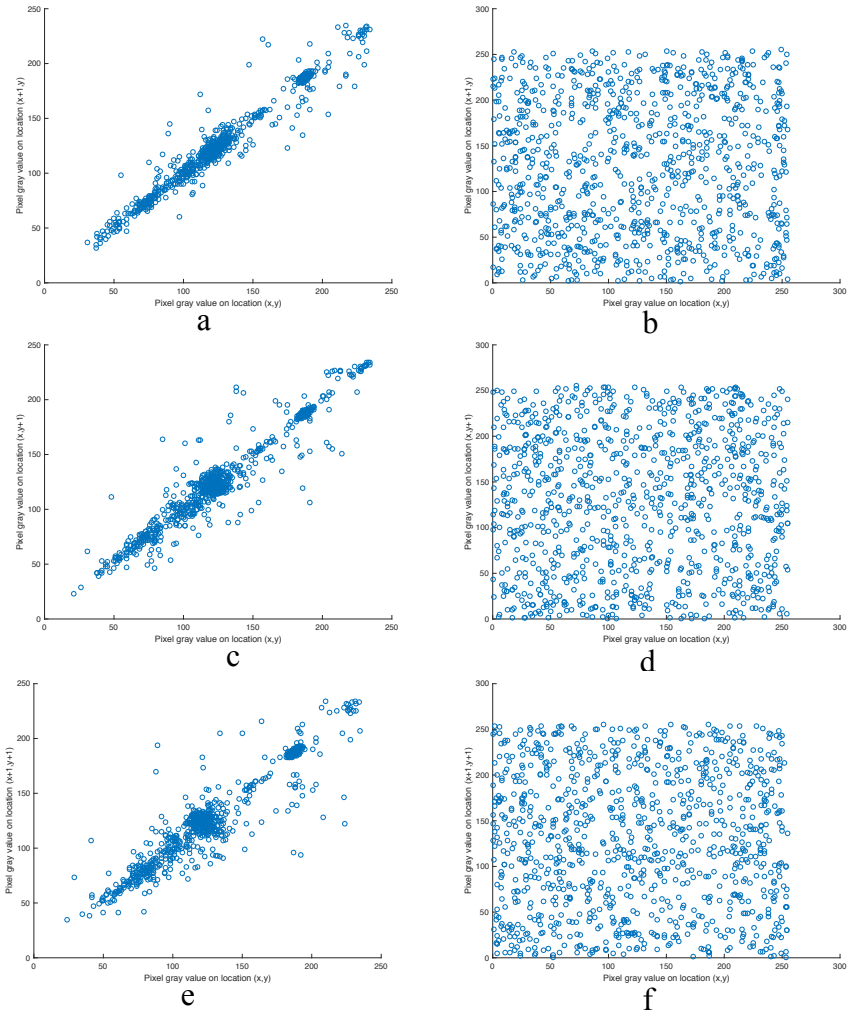


Figure 31. Correlation of adjacent pixels in the plain image and its corresponding cipher image (House 256x256): (a, b) horizontal correlation (c, d) vertical correlation(e, f) diagonal correlation.

The correlation coefficients of adjacent pixels within the RGB image (baboon 512x512) is shown in Table 10 and Figure 32, using EIES the correlation coefficients within the

encrypted image in all directions is close to zero, indicating a low correlation between adjacent pixels for the red, green and blue channels.

Table 10. Correlation coefficients of adjacent pixels for RGB input image and its ciphered

Input image	Channel	Correlation coefficients of the encrypted image		
		Horizontal correlation	Vertical correlation	Diagonal correlation
RGB Baboon 512x512	Red	0.0055	0.0112	0.0404
	Green	-0.0536	0.0357	-0.0451
	Blue	0.0090	-0.0302	0.0203

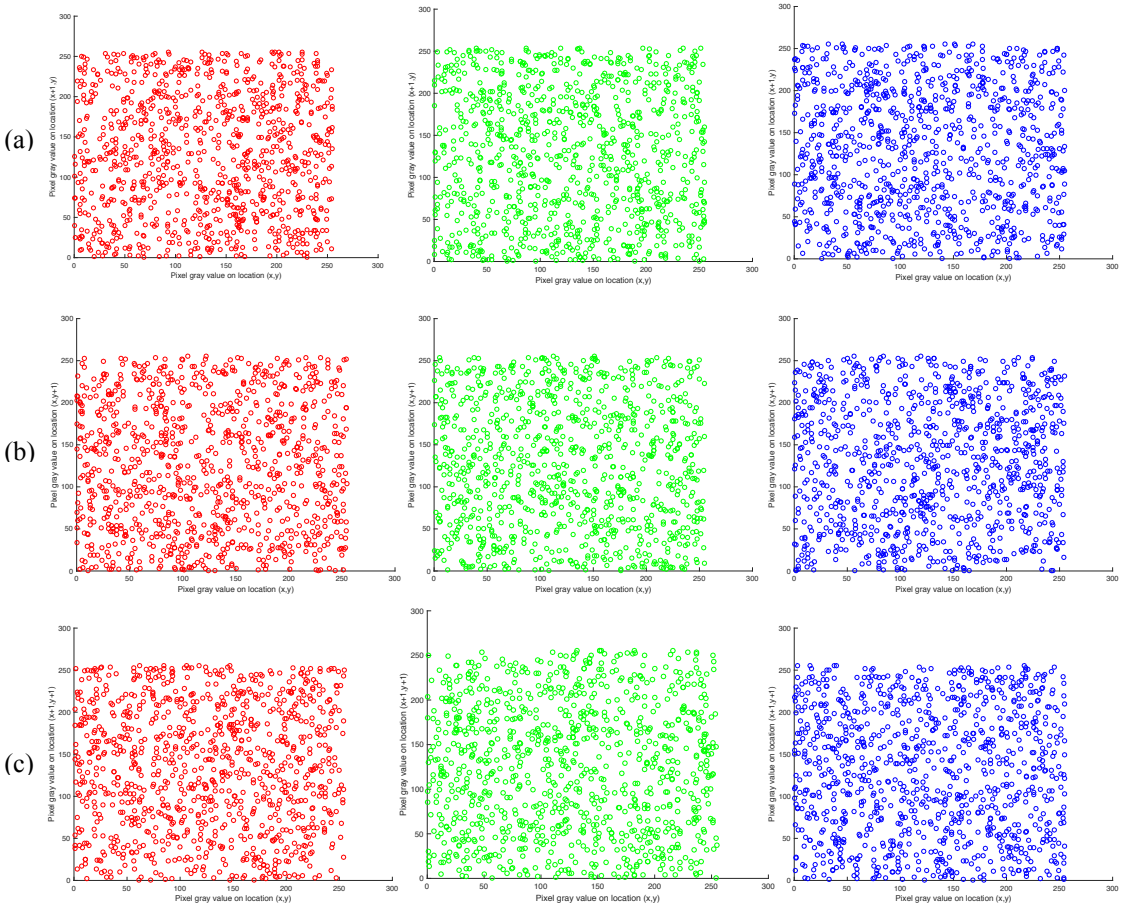


Figure 32. Correlation of adjacent pixels in the channels of the ciphered RGB image (Baboon 512x512): (a) horizontal correlation (b) vertical correlation (c) diagonal correlation.

4.4. Differential Analysis

To perform a differential attack, an opponent makes a slight change in the plain image to perceive the related variations in the corresponding cipher image. Depending on these variations the attacker try to extract some expressive information that can assist to discover the secret key. If a slight difference in the plain image can be efficiently diffused to the entire cipher image, then the differential attacks will be practically insufficient. NPCR and UACI are the two main criteria that are used to measure the diffusion property of the image encryption algorithms.

From equations (16 and 17), It is clear that NPCR focuses on the absolute number of pixels which changes its value in differential attack, while the UACI concerns with the averaged difference between two paired ciphered images [58].

$$NPCR(C_1, C_2) = \frac{1}{W \times H}\left(\sum_{i,j} D(i,j)\right) \times 100\,\% \tag{16}$$

$$UACI(C1,C2) = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|\,C_1(i,j) - C_2(i,j)\,|}{255}\right) \times 100\,\% \tag{17}$$

Where C_1 and C_2 are two ciphered image whose related plain images are identical with only one pixel difference. $C_1(i,j)$ and $C_2(i,j)$ are the pixel values in the cipher images, while W and H are the image dimensions.

D(i,j) in NPCR is calculated as follows:

$$D(i,j) = \begin{cases} 0 & \textbf{\textit{if}}\ C_1(i,j) = C_2(i,j) \\ 1 & \textbf{\textit{if}}\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

NPCR and UACI optimal values should be greater than 99.6% and 33.4%, respectively [11].

To test the robustness of the EIES against differential attacks, we computed the NPCR and UACI values for a set of ciphered image pairs (C_1,C_2), which were obtained by encrypting two input images with a slight change (1 bit difference only).

Three scenarios for the one bit difference between the identical input image pairs (I, I´) are examined in our work. First, we assumed that the slight change between (I, I´) occurred in the first block within I´, such that the value of one bit in the first pixel within the block is changed. Tables 11 and 12 provide the NPCR and UACI values which we have obtained through the application of the proposed encryption algorithm and the other recent works). Due to the robust bit-level permutation step and the use of CBC cipher mode the received results for NPCR and UACI provide values that are very close to the ideal values. Moreover, in many cases the obtained results are greater than (99.6% and 33.4%). Results for other encryption algorithms including the original AES-128 with 10 rounds, and the modified AES using 5 rounds also provide high resistance against differential attacks. This is related to the use of the robust MixColumns transformation that has high computational complexity. Since AES algorithm is designed such that it can achieve the avalanche criteria from the second round, we observe a high convergence between the NPCR and UACI results in both AES-128 and AES-5

rounds. The Shift-AES failed in the differential analysis test, because of its weak ShiftCols transformation, which was not able to replace the MixColumns diffusion step in the original AES.

Table 11. Scenario (1): NPCR performance results for different encryption algorithms

Input image		NPCR				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	0.9962	0.9962	0.9961	0.9962	0.0625
	LL1 band	0.9956	0.9961	0.9960	0.9959	0.0625
	LL2 band	0.9960	0.9957	0.9965	0.9961	0.0625
House 256x256	Full image	0.9959	0.9964	0.9966	0.9962	0.0625
	LL1 band	0.9965	0.9967	0.9962	0.9958	0.0625
	LL2 band	0.9956	0.9968	0.9963	0.9966	0.0625
Lenna 256x256	Full image	0.9959	0.9958	0.9959	0.9960	0.0625
	LL1 band	0.9957	0.9970	0.9958	0.9963	0.0625
	LL2 band	0.9980	0.9951	0.9956	0.9966	0.0625

Table 12. Scenario (1): UACI performance results for different encryption algorithms

Input image		UACI				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	0.3340	0.3344	0.3348	0.3337	0.0210
	LL1 band	0.3364	0.3333	0.3344	0.3353	0.0214
	LL2 band	0.3353	0.3353	0.3360	0.3309	0.0208
House 256x256	Full image	0.3357	0.3361	0.3354	0.3343	0.0212
	LL1 band	0.3330	0.3351	0.3371	0.3334	0.0216
	LL2 band	0.3331	0.3344	0.3344	0.3304	0.0218
Lenna 256x256	Full image	0.3336	0.3330	0.3354	0.3347	0.0206
	LL1 band	0.3326	0.3367	0.3353	0.3364	0.0212
	LL2 band	0.3385	0.3335	0.3330	0.3317	0.0206

In the second scenario, We conducted the change in the input image pair ((I,Í) , by the modification of one bit at the (H/2,W/2) pixel within the input image Í, where H and W are the height and the width of Í. Tables 13 and 14 show the NPCR and UACI results, as in the first scenario; the obtained NPCR and UACI values for EIES are very close to the ideal ones. The proposed cipher preserved a robust diffusion property, due to the use of bidirectional encryption in addition to the CBC mode of operation, such that each block affects its contiguous pixels (b_{i-1}) and (b_{i+1}). On the other hand, the first version of the proposed algorithm, and other encryption algorithms including AES-128, AES-5 rounds and Shift-AES showed a high degradation in both NPCR and UACI values (approximately by half). These results are related to the one directional encryption in AES, in which the diffusion effect spreads forward from the encrypted block (b_i) to the next block (b_{i+1}) through the CBC mode of operation.

Table 13. Scenario (2): NPCR performance results for different encryption algorithms

Input image		NPCR				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512xX512	Full image	0.9961	0.4992	0.4990	0.4990	0.0313
	LL1 band	0.9961	0.5002	0.5001	0.5000	0.0314
	LL2 band	0.9965	0.5033	0.5032	0.5031	0.0316
House 256x256	Full image	0.9962	0.5003	0.5004	0.5001	0.0314
	LL1 band	0.9945	0.5028	0.5026	0.5027	0.0316
	LL2 band	0.9958	0.5107	0.5095	0.5105	0.0320
Lenna 256x256	Full image	0.9963	0.5001	0.5002	0.5004	0.0314
	LL1 band	0.9962	0.5028	0.5027	0.5032	0.0316
	LL2 band	0.9985	0.5102	0.5103	0.5090	0.0320

Table 14. Scenario (2): UACI performance results for different encryption algorithms

Input image		UACI				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	0.3344	0.1671	0.1673	0.1676	0.0105
	LL1 band	0.3356	0.2524	0.1686	0.1677	0.0108
	LL2 band	0.3331	0.1693	0.1691	0.1694	0.0101
House 256x256	Full image	0.3350	0.1694	0.1689	0.1692	0.0104
	LL1 band	0.3333	0.1700	0.1680	0.1712	0.0106
	LL2 band	0.3345	0.1748	0.1713	0.1704	0.0094
Lenna 256x256	Full image	0.3341	0.1670	0.1689	0.1674	0.0103
	LL1 band	0.3377	0.1682	0.1685	0.1697	0.0104
	LL2 band	0.3320	0.1689	0.1665	0.1708	0.0107

In the third scenario, additional degradation in the NPCR and UACI values is observed for all one directional encryption algorithms, leading to very similar ciphered images and weaker diffusion property as a result. In opposite to that, EIES has maintained a stable robust defense against differential attacks.Tables 15 and 16 illustrate the obtained results for changing only one bit in the last block within the image Í.

Table 15. Scenario (3): NPCR performance results for different encryption algorithms

Input image		NPCR				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	0.9962	0.0001	0.0001	0.0001	0.0000
	LL1 band	0.9962	0.0002	0.0002	0.0002	0.0000
	LL2 band	0.9970	0.0010	0.0001	0.0010	0.0001
House 256x256	Full image	0.9960	0.0002	0.0002	0.0002	0.0000
	LL1 band	0.9968	0.0010	0.0010	0.0010	0.0001
	LL2 band	0.9963	0.0039	0.0039	0.0039	0.0002
Lenna 256x256	Full image	0.9962	0.0002	0.0002	0.0002	0.0000
	LL1 band	0.9960	0.0010	0.0010	0.0009	0.0001
	LL2 band	0.9966	0.0039	0.0039	0.0039	0.0002

Table 16. Scenario (3): UACI performance results for different encryption algorithms

Input image		UACI				
		EIES **version2**	EIES **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	Full image	0.3347	0.0000	0.0000	0.0000	0.0000
	LL1 band	0.3341	0.0001	0.0001	0.0001	0.0000
	LL2 band	0.3332	0.0004	0.0003	0.0004	0.0000
House 256x256	Full image	0.3344	0.0001	0.0001	0.0001	0.0000
	LL1 band	0.3347	0.0002	0.0003	0.0003	0.0000
	LL2 band	0.3296	0.0013	0.0010	0.0011	0.0001
Lenna 256x256	Full image	0.3331	0.0001	0.0001	0.0001	0.0000
	LL1 band	0.3328	0.0003	0.0005	0.0003	0.0000
	LL2 band	0.3332	0.0013	0.0016	0.0011	0.0000

4.5. Runtime Analysis

Many WVSN applications are very sensitive to real-time image encryption and transmission. Table (17) provides the runtime (execution time) that is required to encrypt a set of test images using the proposed encryption algorithm, and compare it with other recent works. The results show the proportional relation between the image size and the required time for both of the encryption and decryption steps.

Table 17. Runtime results for different encryption algorithms

Input image	Encryption time (seconds)				
	proposed algorithm **version2**	proposed algorithm **version1**	AES-128	AES-5 rounds	Shift-AES
Cameraman 512x512	17.6076	18.0792	108.6382	64.1621	6.5298
Lenna 256x256	3.6304	3.6404	26.1444	15.2761	1.1891
Cameraman 128x128	0.8520	0.9160	6.5389	3.9367	0.2637
Lenna 64x64	0.2156	0.2222	1.8277	1.0161	0.0680

As we observe in Figure 33, Shift-AES have the shortest encryption time. This is because of the simple lightweight ShiftRows step which reduced the computational complexity and runtime significantly. Compared with other image encryption algorithms including (AES-128) and (AES-5 rounds), EIES provides a significant reduction in the encryption time due to the elimination of the MixColumns transformation, which consumes a considerable time in its multiplication operations. The obtained results indicate that the proposed algorithm needs on average (1/7) of the time that is consumed by the original AES with 128 bit key, and 1/4 of the time that is required for the (AES-5 rounds).

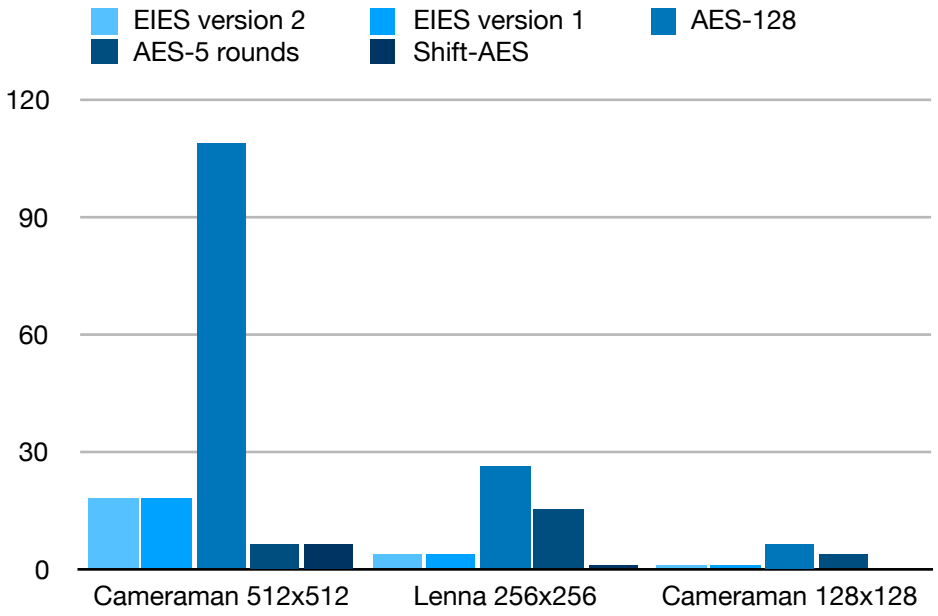


Figure 33. Comparison of encryption algorithms runtime for various images

4.6. Summary

In this chapter, we discussed the analysis that we have conducted to examine the security and efficiency of EIES. Additionally, to investigate the validity of the obtained results within the resource constrained visual nodes in WVSN, we implemented the proposed algorithm, in addition to another three works in the state-of-the-art using MATLAP_R2016a. A set of standard test images with various sizes were encrypted fully and partially to obtain the corresponding results.

Acquired results corresponding to statistical analysis and key space analysis were comparable to that obtained for the other works. Moreover, Our algorithm provided better NPCR and UACI results for various differential attack scenarios, while other algorithms performance degraded in some cases. According to the runtime, our algorithm consumed less runtime compared with other algorithms. It consumed only 1/7 which equals 14% of the original AES-128 in [4] , and 1/4 of the modified AES-128 proposed in [5]. The algorithm in [6] consumed less execution time than our algorithm, but with a weak defense against differential attacks.

In conclusion, EIES can be a promising candidate for image encryption in WVSN.

5. Conclusions and Future Work

In this chapter we provide a short summary about the proposed encryption scheme that we have developed to tackle the issue of image encryption in WVSN. In addition to that, we discuss the possible modifications, enhancements and extensions that we can follow to support our work.

5.1. Conclusions

In the domain of WVSN, image security is one of the main challenging issues. Due to the various monitoring applications in which WVSN can be employed, in addition to the constrained visual nodes and the bulky image nature, a convenient tradeoff between the adopted security level and resources consumption need to be guaranteed.

In this thesis we proposed EIES; an adaptive encryption scheme that has the ability to encrypt images fully or partially, according to the sensing relevance of the visual nodes within the monitored field. Several obstacles impeded the adoption of the conventional encryption algorithms for image encryption in WVSN including the image pattern redundancy, vulnerability to the differential attacks and the increased amount of the required resources which are not available in visual sensor nodes.

To overcome the previous challenges, we provided a modified version of the AES-128 algorithm that uses the Chirikov standard map to provide a robust and lightweight bit-level permutation step instead of the exhaustive MixColumns transformation in the original AES. Moreover, we employed CBC cipher mode to improve the diffusion property, and deal with the pattern redundancy problem. Finally, we proposed to encrypt the image in a bidirectional manner to enhance the algorithm's ability to resist several

differential attacks. The obtained results for statistical analysis, differential analysis, key space and key sensitivity analysis proved the ability of the proposed algorithm to protect and encrypt the captured images with a reduced runtime time to about 1/7 of the time that is required by the original AES.

5.2. Challenges and Future Work

In this work we attempted to guarantee the main security requirements in WVSN nodes, and encrypt images within the network in a reduced time. The aim of the proposed EIES was to prolong the network life time as a whole, while providing fast and robust image encryption.

Although we obtained promising results for the algorithm's security analysis and operational cost, in the following we list the possible enhancements and extensions for EIES:

- Since the performance analysis is not limited to the algorithms runtime, evaluating the proposed scheme according to the power consumption and memory efficiency is required either experimentally, or using a proper simulation environment. We need to conduct a detailed study about the memory efficiency of our algorithm, since as we discussed in chapter 1, the big AES S-box which we also employed, in addition to the large image size are main resources of the high memory requirement.

- Because several compression algorithms have the ability to send image content as a bitstream flow progressively, the next step will be the combination between image compression such as SPECK coding with image encryption by integrating the steps of both of the algorithms together. Such combination can provide a fast encryption

process with high quality reconstructed image which is one of the main properties of SPECK, so instead of encrypting the whole image only representative data is encrypted and sent through the network. Additionally, encrypting images in the transform domain rather than the spatial domain can eliminate the high correlation property between adjacent pixels.

References

1 Wadi, S.M., and Zainal, N.: ‘High definition image encryption algorithm based on AES modification’, Wireless personal communications, 2014, 79, (2), pp. 811-829

2 Gonçalves, D.d.O., and Costa, D.G.: ‘A survey of image security in wireless sensor networks’, Journal of Imaging, 2015, 1, (1), pp. 4-30

3 Costa, D.G., Figuerêdo, S., and Oliveira, G.: ‘Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions’, Cryptography, 2017, 1, (1), pp. 4

4 De Oliveira Gonçalves, D., and Costa, D.G.: ‘Energy-efficient Adaptive Encryption for Wireless Visual Sensor Networks’, in Editor (Ed.)^(Eds.): ‘Book Energy-efficient Adaptive Encryption for Wireless Visual Sensor Networks’ (edn.), pp. 1-14

5 Msolli, A., Helali, A., and Maaref, H.: ‘Image encryption with the aes algorithm in wireless sensor network’, in Editor (Ed.)^(Eds.): ‘Book Image encryption with the aes algorithm in wireless sensor network’ (IEEE, 2016, edn.), pp. 41-45

6 Msolli, A., Helali, A., and Maaref, H.: ‘New security approach in real-time wireless multimedia sensor networks’, Computers & Electrical Engineering, 2018

7 Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., and Samet, M.: ‘A New Encryption Algorithm based on Chaotic Map for Wireless Sensor Network’: ‘Architectures and Protocols for Secure Information Technology Infrastructures’ (IGI Global, 2014), pp. 103-123

8 Qi, J., Hu, X., Ma, Y., and Sun, Y.: ‘A hybrid security and compressive sensing-based sensor data gathering scheme’, IEEE Access, 2015, 3, pp. 718-724

9 Escamilla-Ambrosio, P.J., Salinas-Rosales, M., Aguirre-Anaya, E., and Acosta-Bermejo, R.: ‘Image compressive sensing cryptographic analysis’, in Editor (Ed.)^(Eds.): ‘Book Image compressive sensing cryptographic analysis’ (IEEE, 2016, edn.), pp. 81-86

10 Rachedi, A., Kaddar, L., and Mehaoua, A.: ‘EDES—Efficient dynamic selective encryption framework to secure multimedia traffic in Wireless Sensor Networks’, in Editor (Ed.)^(Eds.): ‘Book EDES—Efficient dynamic selective encryption framework to secure multimedia traffic in Wireless Sensor Networks’ (IEEE, 2012, edn.), pp. 1026-1030

11 Khan, M.A., Ahmad, J., Javaid, Q., and Saqib, N.A.: ‘An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box’, Journal of Modern Optics, 2017, 64, (5), pp. 531-540

12 Fahmy, H.M.A.: ‘WSNs Applications’: ‘Wireless Sensor Networks’ (Springer, 2016), pp. 69-213

13 Hashem, I.A.T., Chang, V., Anuar, N.B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., and Chiroma, H.: ‘The role of big data in smart city’, International Journal of Information Management, 2016, 36, (5), pp. 748-758

14 Ang, L.-m., Seng, K.P., Chew, L.W., Yeong, L.S., and Chia, W.C.: ‘Wireless multimedia sensor networks on reconfigurable hardware: information reduction techniques’ (Springer Science & Business Media, 2013. 2013)

15 Okwor, C., Okomba, N., Okoli, G., Odiase, P., and Adebimpe, E.: ‘A Review of the state-of-the-art Ubiquitous Multimedia Sensor Networks’, FUOYE Journal of Engineering and Technology, 2017, 2, (1)

16 Kumar, V., Jain, A., and Barwal, P.: ‘Wireless sensor networks: security issues, challenges and solutions’, International Journal of Information and Computation Technology (IJICT), 2014, 4, (8), pp. 859-868

17 Guo, J., and Jafarkhani, H.: ‘Sensor deployment with limited communication range in homogeneous and heterogeneous wireless sensor networks’, IEEE Transactions on Wireless Communications, 2016, 15, (10), pp. 6771-6784

18 Porambage, P., Heikkinen, A., Harjula, E., Gurtov, A., and Ylianttila, M.: ‘Quantitative power consumption analysis of a multi-tier wireless multimedia sensor network’, in Editor (Ed.)^(Eds.): ‘Book Quantitative power consumption

analysis of a multi-tier wireless multimedia sensor network' (VDE, 2016, edn.), pp. 1-6

19 Harjito, B., and Han, S.: 'Wireless multimedia sensor networks applications and security challenges', in Editor (Ed.)^(Eds.): 'Book Wireless multimedia sensor networks applications and security challenges' (IEEE, 2010, edn.), pp. 842-846

20 Akyildiz, I.F., Melodia, T., and Chowdhury, K.R.: 'Wireless multimedia sensor networks: Applications and testbeds', Proceedings of the IEEE, 2008, 96, (10), pp. 1588-1605

21 Winkler, T., and Rinner, B.: 'Security and privacy protection in visual sensor networks: A survey', ACM Computing Surveys (CSUR), 2014, 47, (1), pp. 2

22 Costa, D.G., and Guedes, L.A.: 'Exploiting the sensing relevancies of source nodes for optimizations in visual sensor networks', Multimedia tools and applications, 2013, 64, (3), pp. 549-579

23 Khan, S., Pathan, A.-S.K., and Alrajeh, N.A.: 'Wireless sensor networks: Current status and future trends' (CRC press, 2012. 2012)

24 Soro, S., and Heinzelman, W.: 'A survey of visual sensor networks', Advances in multimedia, 2009, 2009

25 Chowdhury, M., and Kader, M.F.: 'Security issues in wireless sensor networks: A survey', International Journal of Future Generation Communication and Networking, 2013, 6, (5), pp. 97-116

26 Harjito, B., Potdar, V., and Singh, J.: 'Watermarking technique for wireless multimedia sensor networks: a state of the art', in Editor (Ed.)^(Eds.): 'Book Watermarking technique for wireless multimedia sensor networks: a state of the art' (ACM, 2012, edn.), pp. 832-840

27 Yasin, A., and Sabaneh, K.: 'Enhancing Wireless Sensor Network Security using Artificial Neural Network based Trust Model', INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2016, 7, (9), pp. 222-228

28 Kaushal, K., and Sahni, V.: 'DoS Attacks on different Layers of WSN: A Review', International Journal of Computer Applications, 2015, 130, (17)

29 Hamdi, M., Rhouma, R., and Belghith, S.: ‘A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map’, Signal Processing, 2017, 131, pp. 514-526

30 Khashan, O.A., Zin, A.M., and Sundararajan, E.A.: ‘Performance study of selective encryption in comparison to full encryption for still visual images’, Journal of Zhejiang University SCIENCE C, 2014, 15, (6), pp. 435-444

31 Ghorbel, O., Ayedi, W., Jmal, M.W., and Abid, M.: ‘DCT & DWT images compression algorithms in wireless sensors networks: Comparative study and performance analysis’, International Journal of Wireless & Mobile Networks, 2012, 4, (6), pp. 45

32 Chew, L.W., Ang, L.-M., and Seng, K.P.: ‘Survey of image compression algorithms in wireless sensor networks’, in Editor (Ed.)^(Eds.): ‘Book Survey of image compression algorithms in wireless sensor networks’ (IEEE, 2008, edn.), pp. 1-9

33 Mammeri, A., Hadjou, B., and Khoumsi, A.: ‘A survey of image compression algorithms for visual sensor networks’, ISRN Sensor Networks, 2012, 2012

34 Shukla, J., Alwani, M., and Tiwari, A.K.: ‘A survey on lossless image compression methods’, in Editor (Ed.)^(Eds.): ‘Book A survey on lossless image compression methods’ (IEEE, 2010, edn.), pp. V6-136-V136-141

35 ZainEldin, H., Elhosseini, M.A., and Ali, H.A.: ‘Image compression algorithms in wireless multimedia sensor networks: A survey’, Ain Shams Engineering Journal, 2015, 6, (2), pp. 481-490

36 Hasan, K.K., Ngah, U.K., and Salleh, M.F.M.: ‘Efficient hardware-based image compression schemes for wireless sensor networks: A survey’, Wireless personal communications, 2014, 77, (2), pp. 1415-1436

37 Nasri, M., Helali, A., Sghaier, H., and Maaref, H.: ‘Energy-efficient wavelet image compression in Wireless Sensor Network’, in Editor (Ed.)^(Eds.): ‘Book Energy-efficient wavelet image compression in Wireless Sensor Network’ (IEEE, 2010, edn.), pp. 1-7

38 Kidwai, N.R., Khan, E., and Reisslein, M.: ‘ZM-SPECK: A fast and memoryless image coder for multimedia sensor networks’, IEEE Sensors Journal, 2016, 16, (8), pp. 2575-2587

39 Wallace, G.K.: ‘The JPEG still picture compression standard’, Communications of the ACM, 1991, 34, (4), pp. 30-44

40 Cabeen, K., and Gent, P.: ‘Image compression and the discrete cosine transform’, College of the Redwoods, 1998

41 Chowdhury, M.M.H., and Khatun, A.: ‘Image compression using discrete wavelet transform’, International Journal of Computer Science Issues (IJCSI), 2012, 9, (4), pp. 327

42 Gaubatz, G., Kaps, J.-P., Ozturk, E., and Sunar, B.: ‘State of the art in ultra-low power public key cryptography for wireless sensor networks’, in Editor (Ed.)^(Eds.): ‘Book State of the art in ultra-low power public key cryptography for wireless sensor networks’ (IEEE, 2005, edn.), pp. 146-150

43 Lee, J., Kapitanova, K., and Son, S.H.: ‘The price of security in wireless sensor networks’, Computer Networks, 2010, 54, (17), pp. 2967-2978

44 Sankpal, P.R., and Vijaya, P.: ‘Image encryption using chaotic maps: a survey’, in Editor (Ed.)^(Eds.): ‘Book Image encryption using chaotic maps: a survey’ (IEEE, 2014, edn.), pp. 102-107

45 Ye, R.: ‘A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism’, Optics Communications, 2011, 284, (22), pp. 5290-5298

46 Bansal, R., Chawla, R., and Gupta, S.: ‘A comparison of image encryption techniques based on chaotic maps’, in Editor (Ed.)^(Eds.): ‘Book A comparison of image encryption techniques based on chaotic maps’ (IEEE, 2016, edn.), pp. 933-938

47 Fridrich, J.: ‘Symmetric ciphers based on two-dimensional chaotic maps’, International Journal of Bifurcation and chaos, 1998, 8, (06), pp. 1259-1284

48 Trad, A., Bahattab, A.A., and Othman, S.B.: ‘Performance trade-offs of encryption algorithms for Wireless Sensor Networks’, in Editor (Ed.)^(Eds.):

‘Book Performance trade-offs of encryption algorithms for Wireless Sensor Networks’ (IEEE, 2014, edn.), pp. 1-6

49 Othman, S.B., Trad, A., and Youssef, H.: ‘Performance evaluation of encryption algorithm for wireless sensor networks’, in Editor (Ed.)^(Eds.): ‘Book Performance evaluation of encryption algorithm for wireless sensor networks’ (IEEE, 2012, edn.), pp. 1-8

50 Biswas, K., Muthukkumarasamy, V., Wu, X.-W., and Singh, K.: ‘Performance evaluation of block ciphers for wireless sensor networks’: ‘Advanced Computing and Communication Technologies’ (Springer, 2016), pp. 443-452

51 Yarrkov, E.: ‘Cryptanalysis of XXTEA’, IACR Cryptology ePrint Archive, 2010, 2010, pp. 254

52 Cheon, J.H., Kim, M., Kim, K., Jung-Yeun, L., and Kang, S.: ‘Improved impossible differential cryptanalysis of Rijndael and Crypton’, in Editor (Ed.)^(Eds.): ‘Book Improved impossible differential cryptanalysis of Rijndael and Crypton’ (Springer, 2001, edn.), pp. 39-49

53 Gilbert, H., and Minier, M.: ‘A collision attack on seven rounds of Rijndael’, in Editor (Ed.)^(Eds.): ‘Book A collision attack on seven rounds of Rijndael’ (edn.), pp. 230-241

54 Law, Y.W., Doumen, J., and Hartel, P.: ‘Survey and benchmark of block ciphers for wireless sensor networks’, ACM Transactions on Sensor Networks (TOSN), 2006, 2, (1), pp. 65-93

55 Fu, C., Chen, J.-j., Zou, H., Meng, W.-h., Zhan, Y.-f., and Yu, Y.-w.: ‘A chaos-based digital image encryption scheme with an improved diffusion strategy’, Optics Express, 2012, 20, (3), pp. 2363-2378

56 Lee, H., Lee, K., and Shin, Y.: ‘Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs’, in Editor (Ed.)^(Eds.): ‘Book Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs’ (2010, edn.), pp. 243-248

57 Mohamed, A.B., Zaibi, G., and Kachouri, A.: ‘Implementation of RC5 and RC6 block ciphers on digital images’, in Editor (Ed.)^(Eds.): ‘Book Implementation of RC5 and RC6 block ciphers on digital images’ (IEEE, 2011, edn.), pp. 1-6

58 Wu, Y., Noonan, J.P., and Agaian, S.: ‘NPCR and UACI randomness tests for image encryption’, Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, 1, (2), pp. 31-38

59 Diaconu, A.-V., Ionescu, V., Iana, G., and Lopez-Guede, J.M.: ‘A new bit-level permutation image encryption algorithm’, in Editor (Ed.)^(Eds.): ‘Book A new bit-level permutation image encryption algorithm’ (IEEE, 2016, edn.), pp. 411-416

60 Hamdi, M., Rhouma, R., and Belghith, S.: ‘An appropriate system for securing real-time voice communication based on ADPCM coding and chaotic maps’, Multimedia Tools and Applications, 2017, 76, (5), pp. 7105-7128

اختياره من الصورة باستخدام خوارزمية تشفير جديدة قمنا باقتراحها. إن ما يميز التشفير الجزئي للصورة، هو قدرة خوارزميات ضغط الصورة على تقليل حجمها، وبالتالي تقليل كمية الطاقة والمعالجة والوقت اللازم لتشفير الجزء المنتقى من الصورة.

تعتمد خوارزمية التشفير التي قمنا باقتراحها على تطوير إحدى أهم خوارميات التشفير التقليديه وهي خوارزمية نظام معيار التشفير المطور، من خلال اجراء بعض التغييرات اللازمة لتقليل الوقت الذي تستغرقه عملية التشفير، وتحسين قدرة الخوارزمية على صد الهجمات الإحصائية والتفاضلية التي يقوم بها الدخلاء. لتحقيق الاهداف السابقه، قمنا في الاصدار الاول من الخوارزميه بتعديل عملية مزج الاعمدة في الخوارزمية الاساسية واستبدالها بعملية أبسط وأقل استهلاكا للوقت تعمل على تبديل الوحدات المكونة للصورة باستخدام الخريطة القياسية العشوائية.

لتقييم الخوارزمية التي قمنا باقتراحها وتحليل قدرتها على مواجة الهجمات الاحصائية والتفاضلية قمنا بتشفير العديد من صور الاختبار المتعارف عليها باستخدام الخوارزمية المقترحه و ثلاث خوارزميات أخرى تم اقتراحها وتطويرها مؤخراً. قدمت نتائج تحليل السريه التي قمنا باجرائها للخوارزمية باصدارها الاول نتائج موازيه لتلك التي تم الحصول عليها في الخوارزميات المستخدمه لتشفير الصور في الشبكات اللاسلكيه وقدرتها على تقليل الوقت اللازم لعملية التشفير بشكل ملحوظ.

إن معظم خوارزميات التشفير التقليديه التي تقوم بتشفير الوحدات المكونه للصوره من خلال مسحها بالترتيب المتعارف عليه تعاني من عدم قدرتها على مقاومة جميع اشكال الهجمات التفاضليه بسبب اعتمادها على اجراء عملية التشفير بترتيب متسلسل بالإعتماد على موقع الوحدات المكونه للصوره ، لذلك قمنا في الاصدار الثاني من الخوارزمية المقترحة بتنفيذ خوارزمية التشفير على مرحلتين باستخدام تسلسل كتلة التشفير. في المرحله الاولى تمت عملية التشفير بنفس إتجاه التشفير التقليدي، أما في المرحله الثانيه فقد تمت عملية التشفير من أسفل الصورة للأعلي.

أثبتت النتائج المختلفه التي تم الحصول عليها ومقارنتها أن الخوارزمية المقترحة باصدارها الثاني قادرة على ضمان مستوى عالٍ من الأمان والسرية للصور التي يتم التقاطها من خلال أجهزة الإستشعار في شبكات الإستشعار المرئية اللاسلكية، بوقت أقل حيث انها تستغرق فقط ١٤٪ من الوقت اللازم لتشفير الصوره باستخدام خوارزمية نظام معيار التشفير المطور.

الملخص باللغة العربية

نظام أمان محسن لشبكات الاستشعار البصرية اللاسلكية

نظرا للإقبال المتزايد على استخدام شبكات الاستشعار البصرية اللاسلكية من قبل العديد من أنظمة المراقبة والتحكم بهدف تحسين أداء هذه الأنظمة، أصبحت عملية المحافظة على أمن الصور التي يتم تناقلها بين أطراف الشبكة ضرورة ملحة. من الجدير بالذكر أن متطلبات الأمن التي تحتاجها الشبكة تعتمد بشكل أساسي على طبيعة النظام و البيئة التي يتم نشر اجهزة الإستشعار فيها، إذ غالبا ما تكون هذه البيئة معرضة للمخاطر والظروف الغير ملائمة.

تعتبر عملية تشفير البيانات من أهم الطرق التي تعمل على توفير متطلبات الأمان الرئيسية في أي نظام حماية. هذه المتطلبات تشمل ضرورة الحفاظ على سرية البيانات التي يتم تناقلها، والتأكد من مصدرها وأصالتها، بالاضافة إلى حماية البياتات من اي تغيير أو تعديل أثناء عملية تناقلها .

إن عملية تشفير الصور في شبكات الاستشعار البصرية اللاسلكية اكثر تعقيدا منها في تشفير البيانات القياسية في شبكات الاستشعار اللاسلكية التقليدية، اذ أنه بالإضافة لصغر حجم وإمكانيات أجهزة الإستشعار، فإن كمية البيانات المحتواة في الصور تعتبر ضخمة مقارنة بتلك المحتواة في الشبكات القياسية، وبالتالي فان استخدام خوارزميات التشفير التقليدية سيستنزف مصادر جهاز الاستشعار بشكل كبير، و سيتطلب وقت تشفير كبير. إضافة لما سبق، فان الصور تتميز باحتوائها على أنماط تكرار، وعلاقات وطيدة بين وحدات المساحة المكونة لها، وبالتالي فان مثل هذه الانماط والعلاقات ستكون ظاهرة في الصورة المشفرة باستخدام خوارزميات التشفير التقليدية.

نظرا لما سبق، ولتحقيق التوازن ما بين مستوى الأمن الذي سيتم توفيره وكمية المصادرالمستهلكة في جهاز الاستشعار البصري، قمنا باقتراح نظام تشفير يعمل على تشفير الصورة بشكل كامل او جزئي، حسب أهمية جهاز الاستشعار بالنسبة للتطبيق الذي يحتويه، إذ ان كل تطبيق يختلف عن التطبيقات الاخرى بالنسبة لمستوى الامان الذي يحتاجه، وكذلك الأمر بالنسبة لجهاز الاستشعار البصري في الشبكة، فبعض الأجهزة تكون موجودة في مناطق حساسة ومن الضروري توفير مستوى عال من الأمن والدقة للصور التي تقوم بالتقاطها نظرا لأهميتها، بينما بقية اجهزة الاستشعار في الشبكة تتفاوت في أهميتها بالنسبة للتطبيق، وبالتالي فإن الصور الملتقطة من خلالها تحتاج لمستويات أمن و ودقة متفاوتة.

تعتمد عملية التشفير الجزئي للصور على تقنية ضغط الصورة في البداية وتحديد الجزء المهم منها باستخدام خوارزمية ضغط ترتكز على تحويل المويجات المنفصلة، ثم نقوم بتشفير الجزء الذي تم