

**A New Symmetric Lightweight Encryption
Algorithm Based on DNA for Internet of Things
Devices**

نظام تشفير جديد متماثل خاص بأجهزة إنترنت الأشياء باستخدام
خاصية الحمض النووي

Prepared By

Rame Jamil Al-Dwairi

Supervisor

Dr. Bassam Al-Shargabi

**A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master's in Cyber Security & Cloud
Computing**

Department of Computer Science

Faculty of Information Technology

Middle East University

June, 2021

Authorization

I, **Rame Jamil Al-Dwairi**, authorize Middle East University to provide libraries, organizations, and individuals with copies of my thesis on request.

Name: Rame Jamil Al-Dwairi

Date: 07/06/2021

Signature: 


Thesis Committee Decision

This is to certify that the thesis entitled " A New Symmetric Lightweight Encryption Algorithm Based on DNA for Internet of Things Devices " was successfully defended and approved on 07/06/2021.

Examination Committee Members:

Dr. Bassam Al-Shargabi (Supervisor)

Middle East University



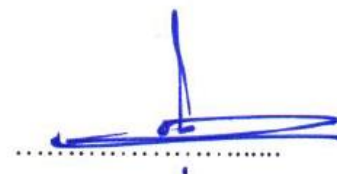
Dr. Hesham Abusaimh (Internal Examiner/Chairman)

Middle East University



Dr. Abdelrahman Abuarqoub (Internal Examiner)

Middle East University



Prof. Nidal Mahmmoud Turab (External Examiner)

Al Ahliyya Amman University



Acknowledgment

Firstly, I would send my gratitude to the almighty Allah for his grace to pass my Master thesis successfully.

I would also extend my gratitude to my extraordinary supervisor Dr. Bassam Al-Shargabi for his tremendous support, recommendations, and encouragement to complete this thesis and all its stages successfully. Definitely, the gratitude extends even more to reach the master's thesis discussion committee, those who were supportive till the last second of my discussion.

My sincerest appreciation also goes to Professors Mohammad Al-Husainy and my friend Haitham Amirah who supported me to complete my thesis. I would also thank all doctors who supported me during all my master's years.

Finally, many appreciations to all those who helped me to finish my master's degree.

Rame Al-Dwairi

The Researcher

Dedication

{وَقُلْ رَبِّ زِدْنِي عِلْمًا} [طه] 111

I dedicate this thesis to My Beloved Father and Mother who have tirelessly supported and encourage me to achieve all my dreams, to my cherished wife who strived with me in every and each single step in our fruitful life and fortunately never gave up on me, to my angels, to My Daughters, Naya and Amaya who enlightened my way and were the reason why I endeavor to achieve my dreams no matter how vigorous the ways is.

Finally, I dedicate my thesis to My Brother, My Sisters, All My Friends, and everybody who played a role to help me complete this thesis.

Rame Al-Dwairi

Table of Contents

Authorization.....	II
Thesis Committee Decision.....	III
Acknowledgment.....	IV
Dedication.....	V
List of Tables.....	VIII
List of Figures.....	IX
Table of Abbreviations.....	X
Abstract.....	XI
المخلص.....	XIII
Chapter One: Study Background and Motivation.....	1
1-1 Introduction.....	1
1-2 Motivation.....	3
1-3 Problem Statement.....	4
1-2 Research Questions.....	4
1-3 Research Objectives.....	5
1-4 Limitations of the Study.....	5
1-5 Delimitations of the Study.....	5
Chapter Two: Background and literature review.....	6
2-1 Introduction.....	6
2-2 Background of IoT and Security.....	6
2-2.1 IoT Devices.....	6
2-2.2 Cryptography.....	8
2-2.2.1 Symmetric Cryptography.....	9
2-2.2.2 Asymmetric Cryptography.....	9
2-2.3 Lightweight Cryptography (LWC).....	10
2-2.4 DNA.....	11
2-3 Related work.....	12
Chapter Three: Methodology and Proposed Model.....	18
3-1 Introduction.....	18
3-2 The Proposed LWC based on DNA.....	18

3-2.1	Key Generation.....	20
3-2.2	Encryption algorithm.....	23
3-2.3	Decryption algorithm.....	27
3-3	Exchange DNA Key.....	30
Chapter four: Experimental Result and Discussion		32
4-1	Introduction.....	32
4-2	Experiments Setup	32
4-3	Evaluation metrics and parameters	34
4-4	Performance and evaluation of the LWCD algorithm.....	36
4-4.1	The Compared Result with the classical encryption algorithm.....	36
4-4.1.1	Encrypted Images	36
4-4.1.2	Images Histogram	37
4-4.1.3	Images correlation.....	39
4-4.1.4	Encryption Time.....	39
4-4.1.5	PSNR Comparison	40
4-4.1.6	Information Entropy.....	41
4-4.2	Avalanche effects.....	42
4-4.3	Evaluation of Variable Number of Rounds	44
4-4.4	Different Block Size.....	48
4-4.5	The keyspace size.....	52
Chapter Five: Conclusion and Future Work.....		56
5-1	Conclusion.....	56
5-2	Future Work.....	57
References		58

List of Tables

Table No.	Table Name	Page
Table 2.1	Research Gap	14
Table 3.1	Example of Fix-Table for generation key	23
Table 3.2	Partitions of key used	31
Table 4.1	Encrypted images	36
Table 4.2	Histogram of original images and the encrypted images	38
Table 4.3	Correlation between original images and encrypted images	39
Table 4.4	Encryption time in second	40
Table 4.5	PSNR in the decibels comparison	41
Table 4.6	Information entropy comparison	41
Table 4.7	The Avalanche effects results	42
Table 4.8	Encrypted images based on Avalanche effect	43
Table 4.9	Encrypted images based on the number of rounds	44
Table 4.10	Correlation between Original and Encrypted Image based on the number of rounds	46
Table 4.11	The encryption Time when changing the number of encryption rounds	46
Table 4.12	The PSNR result when changing the number of encryption rounds	47
Table 4.13	The Entropy result when changing the number of encryption rounds	47
Table 4.14	Encrypted images based on block size	48
Table 4.15	Correlation between encrypted images based on block size	49
Table 4.16	The result of encryption time when changing the block size	50
Table 4.17	The PSNR result when changing the block size	51
Table 4.18	The Information entropy result when changing the block size	51
Table 4.19	Encrypted images with different key space	52
Table 4.20	Correlation between the original image and encrypted images with different key space	53
Table 4.21	Encrypted time with different key space	54
Table 4.22	The PSNR result with different key space	54
Table 4.22	The information entropy result with different key space	55

List of Figures

Figure No.	Figure Name	Page
Figure 3.1	The proposed encryption algorithm (LWCD)	20
Figure 3.2	The proposed generation key operations	21
Figure 3.3	3X3 matrix of k Sequence	22
Figure 3.4	the proposed function for key generation	22
Figure 3.5	LWCD encryption operations into blocks	24
Figure 3.6	3X3 matrix of s Sequence	25
Figure 3.7	Example of S-Box	25
Figure 3.8	Example of 3X3 matrix T-Box	26
Figure 3.9	The LWCD algorithm when the data less than 72-bits	26
Figure 3.10	The LWCD decryption algorithm	27
Figure 3.11	Decryption process for remaining data with of size less than 72-bits	28
Figure 3.12	The LWCD decryption cipher block operations	29
Figure 3.13	Inverse S-box	30
Figure 4.1	Images for evaluation	33
Figure 4.2	Correlation between original images and encrypted images	39
Figure 4.3	Encryption time in second	40
Figure 4.4	PSNR in the decibels comparison	41
Figure 4.5	Entropy comparison	42

Table of Abbreviations

Abbreviations	Meaning
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
CIA Triad	Confidentiality Integrity Availability
CPU	Central Processing Unit
DES	Data Encryption Standard
DNA	Deoxy Ribo Nucleic Acid
ECC	Elliptic-curve cryptography
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability
IoT	Internet of Things
LWC	Lightweight Cryptography
MQTT	Message Queuing Telemetry Transport
NAME	Normalized Mean Absolute Error
NIST	National Institute of Standards and Technology
OTP	One Time Pad
PSNR	Peak Signal to Noise Ratio
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
TEA	Teny Encryption Algorithm
WSN	Wireless Sensor Network

A New Symmetric Lightweight Encryption Algorithm Based on DNA for Internet of Things Devices

Prepared By: Rame Jamil Al-Dwairi

Supervised by: Dr. Bassam Al-Shargabi

Abstract

IoT devices play a pivotal role in making our lives easier, smarter, and more luxurious; therefore, it is applied in many areas such as smart cities, healthcare, military, and more others. These devices assemble important information including personal information, important data, and others. This data should be protected to maintain the confidentiality and integrity of the data in rest or transit by using encryption; nevertheless, the IoT devices have limited resources and need specialized encryption that performs light operations named Lightweight Cryptography (LWC) to suit IoT devices and ensure security and protection of that data.

This thesis aims to propose a new Lightweight Cryptography based on DNA (LWCD). LWCD uses the DNA tape as a key with some operations to generate keys for multi-encryption rounds. The multi-encryption rounds are changeable with the block size to be suitable for IoT devices and get high encryption robustness and strength based on the importance of the data collected. LWCD is performed in two main operations, substitution, and transposition.

The LWCD is implemented and tested using different images, and then, some results are compared with Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Furthermore, the efficiency of multi-encryption rounds of the LWCD

achieved the best proportion of distortion when using four rounds. On the other hand, the efficiency of using variable block size on the LWCD has achieved the best results for encryption times and entropy when using 128-bits block size while the best results of the proportion of distortion when using 72-bits block size.

All these results confirm that the LWCD is effective and can be altered to match IoT devices resources and the importance of the collected data.

Keywords: LWC, Symmetric Encryption, DNA, Lightweight Encryption, IoT Security

نظام تشفير جديد متماثل خاص بأجهزة إنترنت الأشياء باستخدام خاصية الحمض النووي

إعداد: رامي الدويري

إشراف: الدكتور بسام الشرجبي

الملخص

تعتبر إنترنت الأشياء من أبرز المصطلحات الحالية التي تشمل مجموعه من المستشعرات والأدوات المتصلة معاً من خلال شبكة الإنترنت وتقوم بجمع المعلومات والبيانات حيث أن بعض هذه الأدوات يمكنها تحليل هذه المعلومات ومن ثم إتخاذ القرار بالاعتماد على الذكاء الاصطناعي بدون أي تدخل بشري. وتستخدم إنترنت الأشياء في العديد من مجالات الحياة كالمجالات الطبية، والعسكرية، والمدن الذكية، وغيرها وذلك لجعل الحياة أكثر سهولةً وذكاءً.

ونظراً لأهمية إنترنت الأشياء وأهمية المعلومات التي يتم جمعها حيث أنها من المحتمل أن تحتوي على معلومات مهمة، أو شخصية، أو عسكرية، أو غيرها ومن ثم يتم إرسالها عبر شبكة الإنترنت، وبالتالي يمكن قراءة هذه المعلومات وتحليلها بسهولة من خلال أشخاص غير مصرح لهم بالأطلاع عليها أو من خلال مخترقين. ومن هنا يجب أن يتم تشفير هذه المعلومات عند النقل أو التخزين باستخدام وسائل تشفير، ولكن تعتبر أجهزة إنترنت الأشياء من الأجهزة المحدودة الخصائص مثل الذاكرة العشوائية البسيطة والمعالج البسيط مما يؤدي إلى صعوبة استخدام خوارزميات التشفير الحالية على هذه الأجهزة.

في هذه الرسالة تم إقتراح خوارزمية جديدة سميت (LWCD) اعتمدت على استخدام تسلسل الحمض النووي كمفتاح للتشفير حيث أنه يتميز بعشوائيته العالية. ويمكن من خلال هذه الخوارزمية التحكم بعدد دورات التشفير وإمكانية التحكم بحجم تقطيع المعلومات قبل التشفير لتناسب أجهزة إنترنت الأشياء وحسب أهمية المعلومات التي يتم جمعها. حيث تم استخدام عمليتين رئيسيتين للتشفير وهما: عملية التبديل وعملية تبديل المواقع. أما بالنسبة لمفتاح التشفير فيتم عليه مجموعة من العمليات وذلك لإستخدام مفتاح مختلف لكل دورة تشفير وكل مقطع من المعلومات يشفر بمفتاح مختلف.

تم تطبيق وإجراء مجموعة من التجارب على الخوارزمية المقترحة بنجاح حيث تم إستخدام خمس صور بحجمين مختلفين وملون وغير ملون وتم مقارنتها بخوارزميتان مشهورتان وهما معيار تشفير البيانات الثلاثي (3DES) ومعيار التشفير المتقدم (AES) وحصلت الخوارزمية المقترحة على أفضل النتائج بثلاث صور من حيث سرعة التشفير، ونسبة التشويش بالصورة ومقدار العشوائية في الصورة المشفرة وبالنسبة لباقي الصور فكانت النتائج متقاربة جداً

تم إجراء عدة تجارب أخرى لفحص تأثير عدد دورات التشفير حيث تبين أن أفضل نتيجة من حيث نسبة التشويش كانت بإستخدام أربع دورات تشفير. أما بالنسبة للوقت المستغرق للتشفير ومقدار العشوائية في الصورة المشفرة فكانت أفضل النتائج بإستخدام دورتين. ومن التجارب الأخرى فحص تأثير حجم المعلومات المقطعة حيث أظهرت النتائج أن أفضل وقت للتشفير ومقدار العشوائية في الصورة المشفرة كانت عند استخدام حجم 128-bits وفيما يتعلق بنسبة التشويش بالصورة كانت أفضل نتيجة عند استخدام حجم 72-bits.

أثبتت النتائج كفاءة الخوارزمية المقترحة وإمكانية إستخدامها والتحكم بها والتغير بحيث تصبح مناسبة لأجهزة إنترنت الأشياء وحسب أهمية المعلومات التي تم تجميعها.

الكلمات المفتاحية: أمن المعلومات، إنترنت الأشياء، تشفير إنترنت الأشياء، تسلسل الحمض النووي، حماية إنترنت الأشياء.

Chapter One: Study Background and Motivation

1-1 Introduction

Internet of Things (IoT) is one of the important aspects in the world that aids people to make their life easier and smarter. IoT is a physical object that includes sensors to collect data and forward it to applications, systems, or other programs over the Internet. The huge spread of IoT devices connected to the Internet increased dramatically in smart homes, smart farms, medical care, cars... etc (Boakye-Boateng et al., 2019). By 2025, the IoT connected devices will break the limit of 26 billion devices (Al-Shargabi & Al-Husainy, 2021).

The IoT devices are considered as resources constrained devices because they have limited resources (CPU, Memory, and Storage) with limited power especially when they use a battery (Thakor et al., 2021). The huge number of IoT devices with huge data generated and transmitted over the Internet to reach the application server in the cloud or on-premise data center will contain some personal, medical, or other important information.

These collected data can be easily hacked and exposed by an unauthorized user or can be modified during storing or transmitting. Consequently, the confidentiality and integrity of the data need to be secured by an encryption algorithm (Dhanda et al., 2020).

The encryption algorithms are methods to convert the data into secret code to hide the true meaning of them by converting the plaintext to a ciphertext to maintain the confidentiality and integrity of the data. There are two main types of cryptography symmetric and asymmetric encryption.

Symmetric encryption (Secret or Private Key) always uses the same key to encrypt and decrypt the data as the name suggests. It is faster and simpler than asymmetric encryption but it has a problem of how to securely share the encryption key between the sender and receiver (Dutta et al., 2020). The other type of encryption is asymmetric (Public key) where a pair of keys are used. One of these two keys is private and the other is public. This type of cryptography is complex and slower than symmetric cryptography (Dutta et al., 2019).

The growth in the scope of information security has been consistently boosting and there are international laws to protect personal information like General Data Protection Regulation (GDPR) in Europe, medical information like the Health Insurance Portability, and Accountability (HIPAA), and other laws (R. Singh & Sharma, 2020).

As mentioned before, the IoT devices can't rely on the traditional encryption algorithm and need a special encryption algorithm that requires low resources without complex operations such as Lightweight Cryptography (LWC).

The LWC is designed to minimize resource utilization and support the balance between security and efficiency in the IoT devices by reducing the number of encryption rounds, key size, block size, encryption complexity operation, and others (Al-Husainy et al., 2018). Numerous LWC algorithms are proposed to modify a classical encryption algorithm or design a new algorithm to be compatible with the constrained devices (Dhanda et al., 2020).

The simple encryption operations need a secure method to increase the complexity and security of the LWC. As a result, the Deoxy Ribo Nucleic Acid (DNA) tape in the information technology inspired by the idea of the DNA of humans that is the genetic

material. It is a sequence containing four parts: A (Adenine), C (Cytosine), G (Guanine), and T (Thymine) and can generate around 55 million random public sequences (Barman & Saha, 2018; Indrasena Reddy et al., 2020). This huge number of random DNA tape sequences is used as a key for LWC to increase the encryption complexity, efficacy, and security (Aditya et al., 2020).

Recently, researchers studied and designed an encryption algorithm and used the DNA tape by adding it as a layer of encryption operation (Kubba & Hoomod, 2020). Another way of using a DNA tape is by converting the ciphertext to a DNA sequence before transmitting (Ibraheem et al., 2018).

This thesis proposes a new lightweight encryption algorithm (LWCD) based on DNA tape with a variable number of encryption rounds and variable block sizes depending on the IoT device's resource specifications and the importance of the data collected.

1-2 Motivation

In the 21st century, people are excessively relying on IoT devices in order to live a more luxurious life especially with the current prestige many people are living, which is definitely going to replace the traditional lifestyle. The abnormal usage of IoT technology and connected IoT devices to the Internet are increasing promptly with information security. Correspondingly, the breach of the data increased. Moreover, personal information became very important worldwide. The IoT devices collect huge data and transmit it to the cloud; in addition, bear in mind the limited resources of IoT devices. From these points, the motivation of this thesis is to maintain the confidentiality and integrity of the data collected from IoT devices.

1-3 Problem Statement

Cybersecurity is an extremely important term nowadays because of the huge reliance on the Internet including IoT devices which collect a huge amount of confidential data that should be secured from any external, malicious breach. This collected data needs a high-security method appropriate to the constrained devices that have limited CPU with low RAM. These limitations of IoT devices and their connections are attractive targets to acquire and violate the collected data to be misused by the attackers. The IoT devices are not compatible with traditional encryption like AES and 3DES due to the fact that they need high computing resources. IoT devices require an encryption algorithm that is compatible with constrained devices.

Based on the aforementioned, this thesis intends to create a symmetric encryption algorithm to provide simple encryption operations utilizing substitution and transposition to fit the resources of IoT devices and the randomness of the DNA tape as a key to increasing the difficulty to break the encryption and provide robust encryption. It is flexible to change the encryption block size and the number of encryption rounds depending on the importance of the data collected and the IoT device specifications.

1-2 Research Questions

This thesis attempts to answer the following research questions:

1. What is the effect of using a variable number of encryption rounds in the LWCD algorithm?

2. What are the most pivotal performance differences between LWCD and other traditional encryption algorithms based on encryption time, key size, Peak Signal to Noise Ratio (PSNR), and information entropy?

1-3 Research Objectives

The main objectives of this thesis can be summarized as follows:

1. Design an encryption algorithm to meet the limitation of IoT device resources.
2. Conduct experimental tests to evaluate the LWCD based on encryption time, key size, PSNR, information entropy, and the avalanche effect.
3. Study the effects of variable multi-operation rounds and variable block size in the LWCD.

1-4 Limitations of the Study

The LWCD is limited to design an encryption algorithm to be suitable with IoT devices and changeable block sizes (32-bits, 72-bits, and 128-bits) and changeable multi-encryption rounds.

1-5 Delimitations of the Study

The main delimitation of this thesis is the limitation of IoT device resources and the possibility of changing and increasing these resources.

Chapter Two: Background and literature review

2-1 Introduction

Chapter two provides a brief background of IoT devices in addition to their challenges. The best method to secure collected data by encryption, and the DNA technique. Section 2-2.1 discusses the IoT devices and specifications; section 2-2.2 discusses cryptography, especially symmetric and asymmetric cryptography; section 2-2.3 discusses the LWC to be suitable with constrained devices. Section 2-2.4 discusses the benefits of using DNA in cryptography. Finally, section 2-3 discusses the related work within the last five years including the gaps table.

2-2 Background of IoT and Security

IoT created tremendous changes in the world and people's daily lives through eHealth, manufacturing, knowledge sharing, smart machines, and more. Thus, the importance of security increased due to the confidentiality of the information. Moreover, the Cybersecurity of IoT takes a very important domain around the globe which led some countries to legislate laws including the implementing a standard of Cybersecurity in the United States in addition to activating a Cybersecurity Law in China (Lu & Da Xu, 2018).

2-2.1 IoT Devices

IoT is a concept that describes physical objects (things) that are connected together to collect data and transmit it to the Internet, other devices, servers, or cloud without human interference. This includes intelligent objects, smart homes, smart cities, machines, and others to digitalize life to be smarter. Furthermore, human bodies can be easily connected to

these devices to read their biological signs or even their current or past locations (A. Biswas et al., 2020). The IoT initially used radio frequency identification (RFID), and then later wireless sensor network (WSN) has been developed (Dhanda et al., 2020).

Some IoT devices have the ability to analyze and store data with the main object of detecting, collecting, and conveying data between IoT devices and the cloud (Al-Husainy & Al-Shargabi, 2020).

The IoT is a heterogeneous device, so there are different IoT architectures. Firstly, some researchers divided the IoT architecture into three layers: physical layer which contains physical sensors to collect the data, network layer which transfers the data and responsible for communication and routing protocol, and on the top of these layers comes the application layer which transmits the data to the destination. (Kotha & Gupta, 2018). Secondly, other researchers describe four layers: perception layer which is identical to the physical layer previously discussed, network access layer which is also previously discussed, data management layer which manages the data, and finally intelligent service layer. The third architecture includes five layers: business layer to define the application and management, application layer to determine the type of application, processing layer, network layer using IPV6, and perception layer (Bhardwaj et al., 2017).

The IoT devices have special specifications that are challenges which need to be taken into consideration when designing the IoT. The major issue of IoT devices is constrained devices which means that there are limited resources including a low central processing unit (CPU), low random access memory (RAM), low storage, low read-only memory (ROM),

low data transmit rate, little physical security, and limited battery capacity (Barman & Saha, 2018).

These challenges allow hackers to easily breach and manipulate data. One of the main attacks on IoT communication is the man-in-the-middle attack which aims to monitor the traffic and obtain important data or even modify it during the communication. Nevertheless, cryptography can mitigate this attack by encrypting the data in transit or at rest and make it unreadable (Abusaimh & Al-dwairi, 2020). Another attack is the denial of service attack by flooding a huge packet to stop the services (Bhardwaj et al., 2017).

Steganography is another way to protect the data by hiding the information in the multimedia like image, audio, video, and other, some researcher used it for IoT devices (Hashim et al., 2020; Jiang et al., 2020).

2-2.2 Cryptography

Securing data is a very attractive topic in the world due to the huge number of devices connected to the Internet and the weakness of security which definitely causes loss of privacy and economy. Consequently, international laws control and maintain security to ensure a security triad which contains three principles: confidentiality which allows only authorized users to access the data, integrity which ensures the data accuracy and reliability, and availability which ensures accessibility to the data (R. Singh & Sharma, 2020).

Cryptography is a vital and paramount part of information security; it is an indispensable tool to protect the data by converting the readable information to unintelligible information by using complex operations, and only authorized users can read it. The main

cryptography types are symmetric and asymmetric cryptography depending on the encryption key (Dhanda et al., 2020).

2-2.2.1 Symmetric Cryptography

Symmetric cryptography (Secret or Private Key) uses only one key for both encryption and decryption with the advantage of higher security and faster operation compared to asymmetric, but it is difficult to share a key between the partners (Bhardwaj et al., 2017).

The most famous symmetric cryptography is Data Encryption Standard (DES). DES is a 64-bits of cipher block with a 56-bits key, but it is no longer considered secure due to that fact that it is easily hacked; therefore, it is replaced with Triple DES (3DES) which works as the exact operation of DES, but it repeats the DES operations three times with the same block size and different key size of 112-bits for two rounds or 168-bits for three rounds. The other important encryption algorithm is the Advanced Encryption Standard (AES). AES uses block size 128-bits with key size of 128-bits for ten rounds, 192-bits for 12 rounds, and 256-bits for 14 rounds with four main operations: static S-box, mix columns by multiplying, shift rows, and adding a complex key that is generated (Renuka et al., 2018). The 3DES and AES are still secured and recommended to be used (Al-Husainy et al., 2018; M. R. Biswas et al., 2019; A. Singh et al., 2017)

2-2.2.2 Asymmetric Cryptography

Asymmetric cryptography (Public key) uses two pairing keys. The first one is a private key which is never transmitted in the network, and the other is a public key shared with other

users. This type of cryptography is a complex operation and slower than symmetric cryptography (Dutta et al., 2020). Some of the important types of asymmetric cryptography include Rivest-Shamir-Adleman (RSA) which gains its security from the complexity of operations to generate a private key from the public key working with key size 1024-bits to 4096-bits. Another type is Diffie-Hellman which is used for sharing the symmetric key with a very short key which leads to faster operation and less security compared to others (Dutta et al., 2019). The last type to be discussed is the Elliptical Curve Cryptography (ECC) which is very complex and difficult to implement; nevertheless, it is stronger than (RSA); for instance, when the RSA uses a 1024-bits key size, ECC can get the same level of security with the key size of 160-bits and uses low power for exchanging the key (Barman & Saha, 2018).

2-2.3 Lightweight Cryptography (LWC)

The cryptography algorithm requires high resources and complex operations. As a result, the constrained devices cannot support conventional cryptography due to their limitation; therefore, the constrained devices need a LWC for more compatibility by a simple and low computational process. Accordingly, the block size, key size, number of encryption rounds, and algorithm structured are the main parameters that should be considered in the LWC to be suitable for IoT devices (Kubba & Hoomod, 2020).

The main idea of the LWC is to define a simple encryption operation with the best security by modifying a secure complex algorithm like AES (Bhavani et al., 2019) or modify a weak encryption algorithm like DES to be DESL with some modification (Dhanda et al., 2020).

Most LWC algorithms used to secure IoT devices are based on the symmetric approach to provide secured data transmission due to the easy implementation and low utilization of resources in case the key is securely shared with authorized users. Most LWC used in IoT devices are Tiny Symmetric Encryption Algorithm (TEA). TEA is a symmetric encryption with a block size of 64-bits, a key size of 128-bits, and 64 or 32 rounds. The main operation of TEA is XOR and AND, alternatively with one key for all rounds. Therefore, the implementation of TEA to secure data is used to facilitate relying on minimal memory and utilization. Hence, the security is reduced with a high period of encryption and decryption (Rajesh et al., 2019).

ECC in the LWC provides non-repudiation and authentication. Moreover, symmetric and asymmetric are used to provide confidentiality and integrity. PRESENT is another example of LWC; it is a symmetric LWC with a key of 80-bits and blocks size 64-bits (Dhanda et al., 2020).

2-2.4 DNA

DNA is a genetic information sequence for information technology inspired by human DNA which contains nucleotide. Nucleotide is one of the four nucleobases that are combined together to produce a DNA tape. It is presented into two binary digits: 00 = A (Adenine), 01 = T (Thymine), 10 = G (Guanine), and 11 = C (Cytosine) to generate around 50 million public sequences (Barman & Saha, 2019; Bhavani et al., 2019). The randomness of the DNA improves the security and the complexity of encryption to protect the value of the information from hackers. The other advantage of DNA computing is the fast processing with minimal power and storage requires. (Aishwarya & Sreerangaraju, 2019), that is clear

when encoding plain data with DNA sequence (AL-Wattar, 2020; El-Moursy et al., 2018; Liu et al., 2019).

The researchers implement DNA directly in their algorithm or indirectly by using DNA properties. Hybrid cryptography mixed the two implementations to provides and increase the strength of security for classical cryptography (Sajisha & Mathew, 2017).

Most of the researchers used the DNA by converting the ciphertext to DNA tape, like encrypting the data by using AES and convert it to hexadecimal format, and then to binary, and finally to DNA tape to provide more security of data (Bhavani et al., 2019). Some other researchers used the DNA to increase the security of the classical encryption like AES (Pradeeksha & Sathyapriya, 2020).

2-3 Related work

Al-Shargabi & Al-Husainy, (2021) proposed a new LWC algorithm based on a random key generated from a DNA sequence to make it difficult to break. It is a block symmetric encryption algorithm that divides the image and key into one-byte block and then uses substitution by XORing each block of the image with a DNA block key, and then transposition with special rules. They found a simple LWC with a strong randomized DNA tape as a key to be difficult to breach.

Kolate & Joshi, (2021) used 128-bits of DNA tape as a key in the AES encryption after converting the data to DNA tape before encryption. It improved the performance of encryption of operations and provided multi-levels of security.

Kubba & Hoomod, (2020) proposed and developed a symmetric algorithm by adding a DNA layer to PRESENT cryptography and named it DPPRESENT. It uses a 64-bits block algorithm with optional key size of 80-bits or 128-bits through 21 rounds operation. Each round contains XOR with the round key, and then substituted by using PRESENT S-box and processed by using permutation table in the P-layer. After that, the packet moved to DNA layer and permuted by using DNA sequence. Finally, XOR with a round key again. These operations looped 20 rounds, and then the last stage of operation by XORing the ciphertext with a new key. They found the DNA is an efficient algorithm for IoT communication and increased the complexity of the ciphertext with a minimum time of execution.

Hussein & Shujaa, (2020) proposed simple streaming encrypt algorithm by using XOR operation with generating a key from One Time Pad (OTP) and used once for each message with the same message length. Generating the key is the strongest point by using the OTP in linear feedback operation, and then encoding the key with DNA. This operation depends on Message Queuing Telemetry Transport (MQTT) protocol. MQTT uses the publish/subscribe model between devices.

Al-Husainy & Al-Shargabi, (2020) developed a streaming symmetric LWC algorithm with a changeable 80-bits key generated randomly in the central server depending on the current time. The main operations of the LWC are substitution three times and transposition.

Liu et al., (2019) designed symmetric Novel encryption for remote sensing images based on the DNA with special rules and DNA addition, substitution, and masking as main operations. All these operations work only one time.

Ibraheem et al., (2018) proposed an encryption algorithm based on RSA and DNA to encrypt messages in MQTT protocol. The algorithm encrypts the data by using RSA, and then converts the ciphertext to DNA tape and sends it to the cloud. It uses asymmetric encryption with 2048-bits, and then encodes it to 64-bits by converting it to DNA tape with key size of 178-bits.

Tiwari & Kim, (2018) Proposed an algorithm for IoT devices that uses ECC with DNA as a key. DNA key is selected and divided by the sender, and then the sequence is sorted to be ready as a key for ECC encryption to generate a ciphertext.

M. Al-Husainy et al., (2018) studied and suggested a lightweight block cryptosystem by using an auto-generated key from 16x16 exchange table and keyspace of 2048-bits. The block size is 32-bits with any key size in the space. They compared the result with AES and DES.

To summarize the related work and pinpoint the research gap between this thesis and the other related works are shown in table 2.1.

Table 2.1: Research Gap

Previous Studies (Purpose)	Variables of Previous Studies	Gaps
Al-Shargabi & Al-Husainy, (2021) Developed an LWC algorithm based on DNA as a key for substitution	Symmetric, each one-byte of image block encrypted with one byte of DNA as key. Single encryption round.	The study used simple operations that used any key size of DNA tape with fixed block size and single encryption round, while the

and used transposition operations.		LWCD had variable block size with multi-encryption operations and multi-encryption rounds.
Kolate & Joshi, (2021) used a DNA tape as a key for AES encryption after converting the data to DNA tape	AES Symmetric used 128-bits of DNA tape as a key	Used classical encryption algorithm with DNA key size 128-bits and fixed block size, while LWCD developed a new LWC with variable block size and used the DNA tape as a key.
Kubba & Hoomod, (2020) developed LWC with normal operations substitution, permutation, and DNA layer.	Symmetric, 64-bits block used 80-bits or 128-bits key. The number of Rounds 21. Using DNA as a layer in the operation	The study used a fixed block size and a fixed number of rounds. while the LWCD used the DNA tape as a key with changeable block size and changeable multi-rounds.
Hussein & Shujaa, (2020) proposed a streaming symmetric encryption algorithm with the key	Symmetric encryption Key generated from OTP and DNA with the key size	Simple operation XOR used variable key size from OTP and DNA, without any round operation. While LWCD is a

generated from OTP and DNA		block encryption algorithm with changeable block size and multi-encryption rounds.
Al-Husainy & Al-Shargabi, (2020) developed symmetric LWC for streaming data, with a strong random key changed periodically depending on the current time by using a central server.	Symmetric encryption. 80-bits Key generated from the central server depending on the current time. Streaming encryption.	LWC without using DNA. They used steaming encryption. While LWCD is a block encryption algorithm and used DNA tape as a key with changeable block size and multi-encryption rounds.
Liu et al., (2019) proposed novel encryption based on DNA	Symmetric encryption. Streaming encryption.	LWC with only one round. While LWCD is a block encryption algorithm and used DNA tape as a key with changeable block size and multi-encryption rounds.
Ibraheem et al., (2018) using RSA then encrypt it with DNA	Asymmetric encryption and DNA encryption 64-bits block 178-bits key	Asymmetric and classic algorithm with large key size. While LWCD is a symmetric encryption algorithm and the

		DNA tape is used as a key with changeable block size and multi-encryption rounds.
Tiwari & Kim, (2018) Using DNA as a key for ECC encryption with streaming data in IoT devices	Asymmetric Using ECC with DNA key	They used an asymmetric classical algorithm. While LWCD is a symmetric encryption algorithm and changeable block size and multi-encryption rounds.
M. Al-Husainy et al., (2018) proposed an LWC used substitution table and transposition	Symmetric encryption 32-bits block size with any key size and keyspace 2048 bits	They didn't use DNA. While LWCD used the DNA tape as a key with changeable block size and multi-encryption rounds.

The proposed LWCD is designed to be appropriate for the IoT devices by the simplest operation with the randomizing of DNA tape as a key to add extra security to the algorithm. Most of the previous related works used symmetric block encryption with DNA or traditional encryption with DNA but without any flexibility to change the block size or the number of encryption rounds. Al-Husainy & Al-Shargabi, (2020) proposed an LWC algorithm with a very small block size of one-byte, single and simple encryption operation, encryption while the LWCD has flexible block size and flexible encryption rounds with extra encryption operations depending on the first byte of DNA key as seed to generate S-Box matrix for substitution and T-Box roles for transposition.

Chapter Three: Methodology and Proposed Model

3-1 Introduction

Encryption is the most important domain in information security to maintain the confidentiality of the data, especially in the IoT devices during the vast usage of IoT in our life with security demand that directed the researcher to find a secure LWC. Most researchers design an LWC for IoT devices without using the DNA tape. Nevertheless, a few researchers design and suggest LWC based on DNA with or without repeating the encryption operations. Interestingly, personal efforts did not meet any suggested LWC based on DNA with a variable number of encryption rounds and with variable block sizes depending on the vitality of the data collected or the IoT device specifications.

The proposed LWCD algorithm described in section 3-2 is a symmetric encryption algorithm that uses the DNA tape as a key with some operation to generate a unique key for each round which is described in section 3-2.1. The LWCD operation is discussed in details in section 3-2.2. Section 3-2.3 describes the LWCD decryption algorithm. Finally, section 3-3 describes the suggested exchange key.

3-2 The Proposed LWC based on DNA

This thesis proposes a new LWC based on DNA as a key with a variable number of encryption operations rounds and variable block size named LWCD. LWCD is a symmetric block encryption algorithm shown in figure 3.1. The phases of the LWCD depend on the substitution and transposition with multi-operation rounds and adding a different key in each round.

The main aim of using DNA tape is to exploit the huge randomness features of DNA to increase the security and reduce the power consumption of the LWCD algorithm; therefore, get a convenient cipher compatible with IoT resources as illustrated in figure 3.2. The key generation and the key size are the strongest aspects of any encryption algorithm. As a result, LWCD proposed some operations such as shift and XOR to generate a random DNA tape as a key for each round.

The flexibility of changing the number of encryption rounds should add a value to the LWCD algorithm to increase the security of that algorithm depending on the value and the sensitivity of the collected data. Therefore, when the encryption rounds are increased, the encryption operations are repeated multi times with multi different keys to gain a robust cipher or decreased the number of rounds to fit IoT devices computation resources.

The LWCD has the ability to change the block size where it is considered as another variable parameter that can be changed depending on the IoT device specifications. It is variable depending on the matrix selected: 2X2 (32-bits), 3X3 (72-bits), or 4X4 (128-bits). It is important to mention that the encryption key depends on the block size. From this point, the DNA tape will be divided into the exact size of the data block and encrypt each block with a different key.

S-Box, T-Box and Fix-table are used to increase the complexity of the LWCD. S-Box, T-Box and Fix-table are generated randomly by using pseudo-random generator algorithm which relies on built-in function supported by the language used (C-Sharp) to make the generated value more random, and the LWCD more secure, the seed value that is fed by the pseudo-random generated algorithm is selected randomly from the DNA tape used as the

key. This provides each user or device with different S-Box and T-Box which are used in the encryption operations, and different Fix-Table which is used in the key generation.

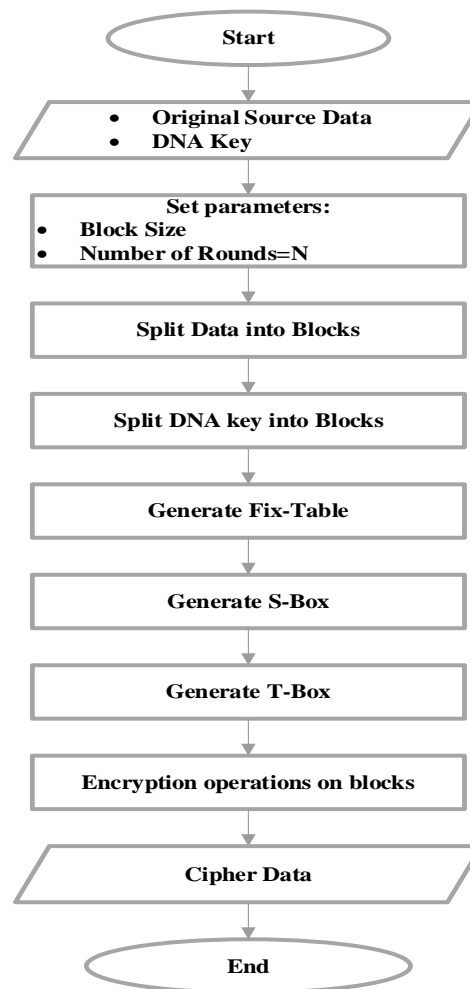


Figure 3.1: The proposed LWCD

3-2.1 Key Generation

The LWCD uses a DNA tape for the encryption and decryption algorithm. The DNA tape is divided into blocks size similar to the size of the data block (32-bits or 72-bits or 128-bits). Then, each data block is encrypted with a different DNA key such as the first data block

uses the first DNA tape block for encryption, and then the second data block uses the second DNA tape block and so on.

The LWCD used transposition and substitution operations to generate a different key for each round after converting the DNA key into the matrix as a row-major order. Figure 3.2 illustrates the operations used to generate the keys applied in multi-round encryption. Therefore, the encryption rounds should be equal to or larger than one. For example, we used a DNA tape key with a size block of 72-bits. The process of generating the encryption keys is described as follows:

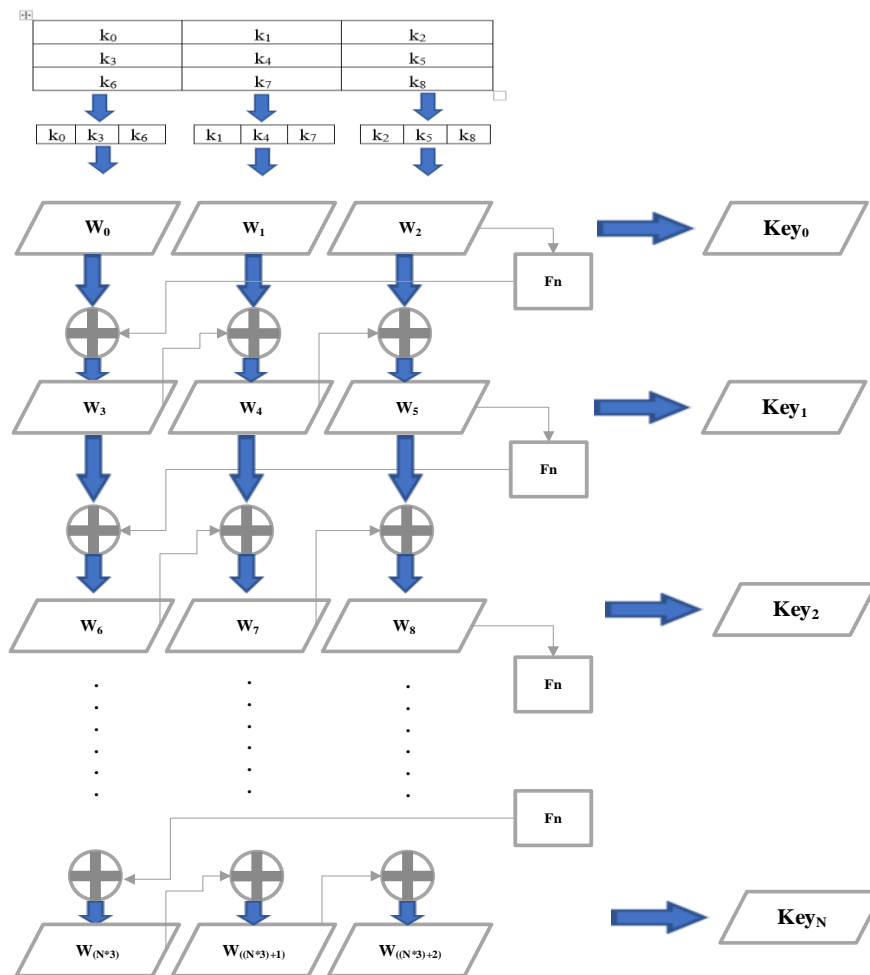


Figure 3.2 The proposed generation key operations of LWCD

1. The 72-bits block from the DNA sequence tape key is divided into nine bytes and each byte named k to generate k sequence ($k_0, k_1, k_3, \dots, k_8$).
2. Store k sequence into 3X3 matrix as row-major order as shown in figure 3.3.

k_0	k_1	k_2
k_3	k_4	k_5
k_6	k_7	k_8

Figure 3.3: 3X3 matrix of k Sequence

3. Each column of the matrix generated a word (W) with a size of 24-bits, then every three words generate the key (Key_N) (where N is the number of encryption rounds).
4. In each round of generation key, the third word ($W_{((N*3)+2)}$) inserted in the operation function (F_n) as figure 3.4

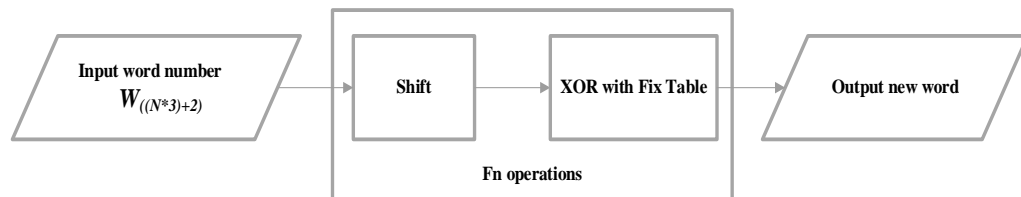


Figure 3.4 the proposed function for key generation

5. The function (F_n) operation started with transposition operation by shifting the input word ($W_{((N*3)+2)}$) one byte to the right, then substitution operation by XOR result with the value from the Fix-table depending on the round number. The Fix-table generated a hexadecimal value randomly based on the first byte

from DNA as a seed. An example of the Fix-Table value is shown in table 3.1.

Table 3.1: Example of Fix-Table for generation key

Round Number	Fixed Number
1	26AF11
2	231AA0
3	BCA11A
.	.
.	.
.	.
N	A00114

6. The output of the operation function \mathbf{Fn} XORed with the word ($\mathbf{W}_{(N*3)}$) to generate the first word in the next round.
7. Then the output from the previous step will be XORed with $\mathbf{w}_{((N*3)+1)}$.
8. And finally, the output XORed with $\mathbf{W}_{((N*3)+2)}$.
9. Then $\mathbf{key}_N = \mathbf{W}_{(N*3)} \mathbf{W}_{((N*3)+1)} \mathbf{W}_{((N*3)+2)}$
10. This operation is repeated until generated all keys that needed.

3-2.2 Encryption algorithm

The LWCD is symmetric block encryption with the changeable block size and a variable number of rounds as shown in figure 3.1. It divides the input data and DNA key into blocks, and then generates a random S-Boxes, T-Box, and Fix-table based on the first byte of DNA tape as a seed. Each block data encrypted is separated with different DNA keys based on the block size as shown in figure 3.5. For example, the block size is set as a 3X3 matrix (72-bits) and the number of rounds equals N to explain the main operations, substitution and transposition, of the proposed algorithm. The encryption processes for the proposed LWCD are as follows:

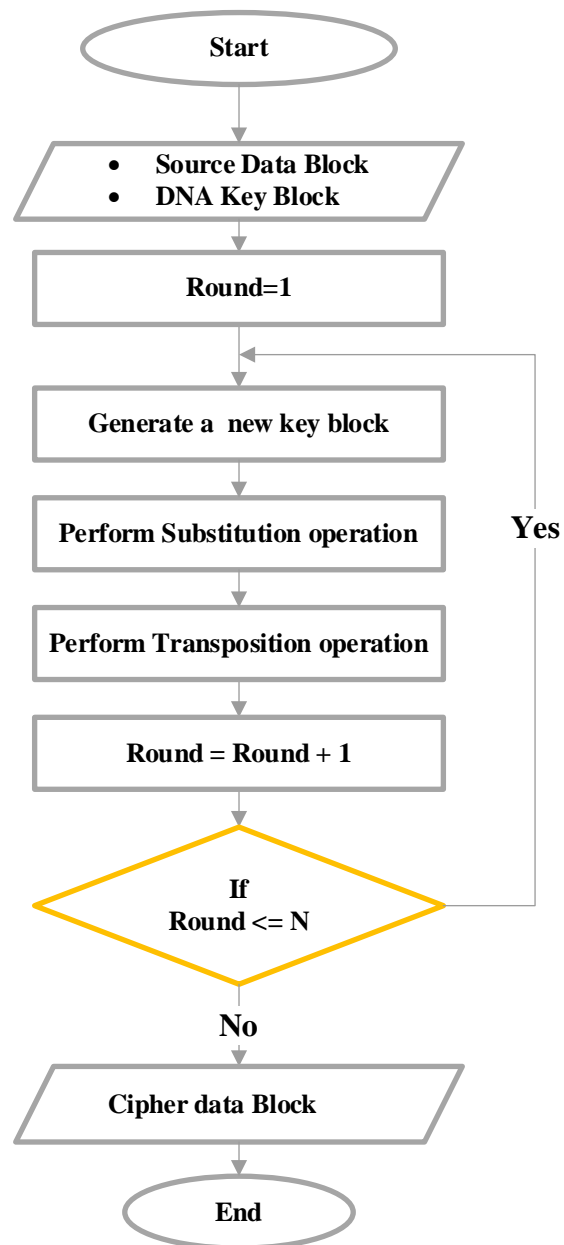


Figure 3.5: LWCD Encryption operations into blocks

1. Each data block with a size of 72-bits is divided into a sequence of 9 bytes named s to generate s sequence $(s_0, s_1, s_3, \dots, s_8)$.
2. Store data (s sequence) into 3X3 matrix as column-major order shown in figure 3.6.

S_0	S_3	S_6
S_1	S_4	S_7
S_2	S_5	S_8

Figure 3.6: 3X3 matrix of s Sequence

3. The encryption of each block started as shown in figure 3.5 as follows:
 - a. First, setting the round equal 1.
 - b. Then the generating encryption key for rounds started.
 - c. The first encryption operation in this loop is the substitution. The substitution operation started with XORed the data block with a round key (key_N). Then replace the data with the value from random S-Box generated based on the first byte of DNA key as a seed, the value represented as a hexadecimal value between 00 to FF without repetition of 256 elements in the 16X16 table. figure 3.7 shows an example of an S-Box.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3.7: Example of S-Box

- d. The transposition is the second operation in the loop by changing the position of the s sequence data as a T-Box generated randomly based on the first byte of DNA tape as a seed. As an example of T-Box shown in figure 3.8:

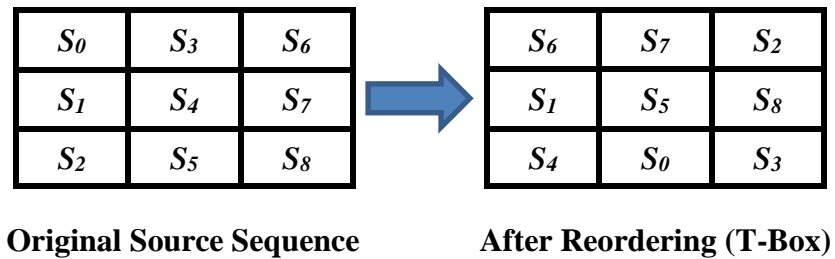


Figure 3.8: Example of 3X3 matrix T-Box

- e. This looped repeated until the round value be larger than the number of encryption rounds (N).

Eventually, the output of the encryption process is cipher block data ready to be stored or transmitted. All above operations are repeated for all blocks until all data blocks are completed. In case of the data remaining with a size less than 72-bits, it will be encrypted directly with a DNA key that had the exact size of the remaining data as illustrated in figure 3.9.

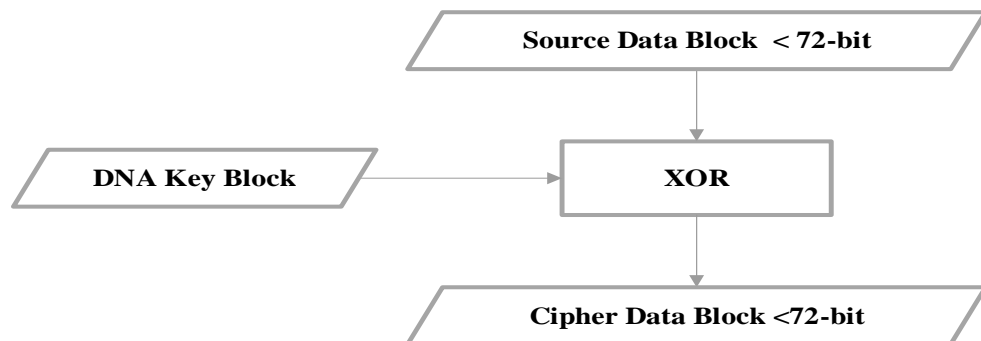


Figure 3.9: The LWCD algorithm when the data less than 72-bits

3-2.3 Decryption algorithm

The LWCD decryption operation is a reversed operation of the LWCD encryption algorithm and uses the same DNA tape key; therefore, it starts by generating the Fix-table, inverse S-Box, inverse T-Box, and all keys needed from DNA tape. as shown in figure 3.10.

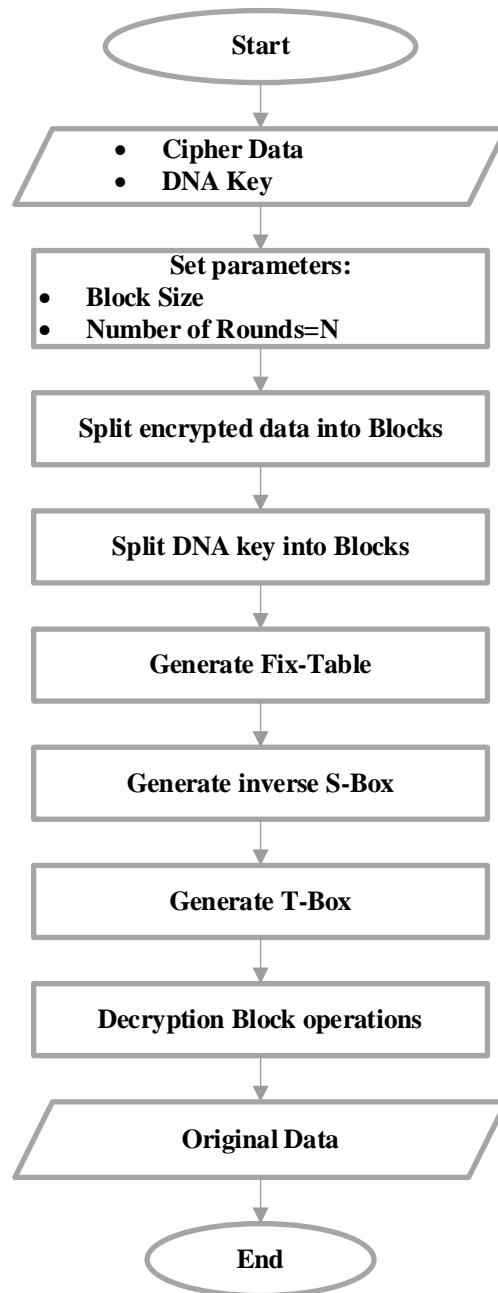


Figure 3.10: The LWCD decryption algorithm

Each cipher data block is decrypted separately, the decryption operation starting with XOR the remaining data with DNA tape that had the same size, as an example, a 3X3 matrix with block size 72-bit is suggested as illustrated in figure 3.11.

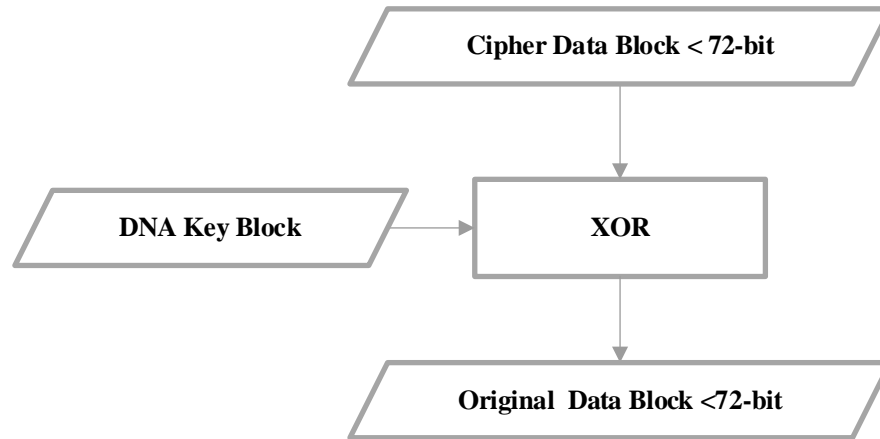


Figure 3.11: Decryption process for remaining data with of size less than 72-bits

Accordingly, the decryption operations for each cipher block, as shown in figure 3.12, started by setting the round value for the looped equal to the number of encryption rounds (N), and then the looped operation starts first by inversing transposition operation. After that, the inversed substitution starts by using the inverse S-box generated randomly based on the first byte of DNA tape. An example of this inverse process, S-Box is shown in figure 3.13. After that, the round value decreased by one, and then the loop continues and repeats the operations until the round value reaches a value less than one to restore the original data.

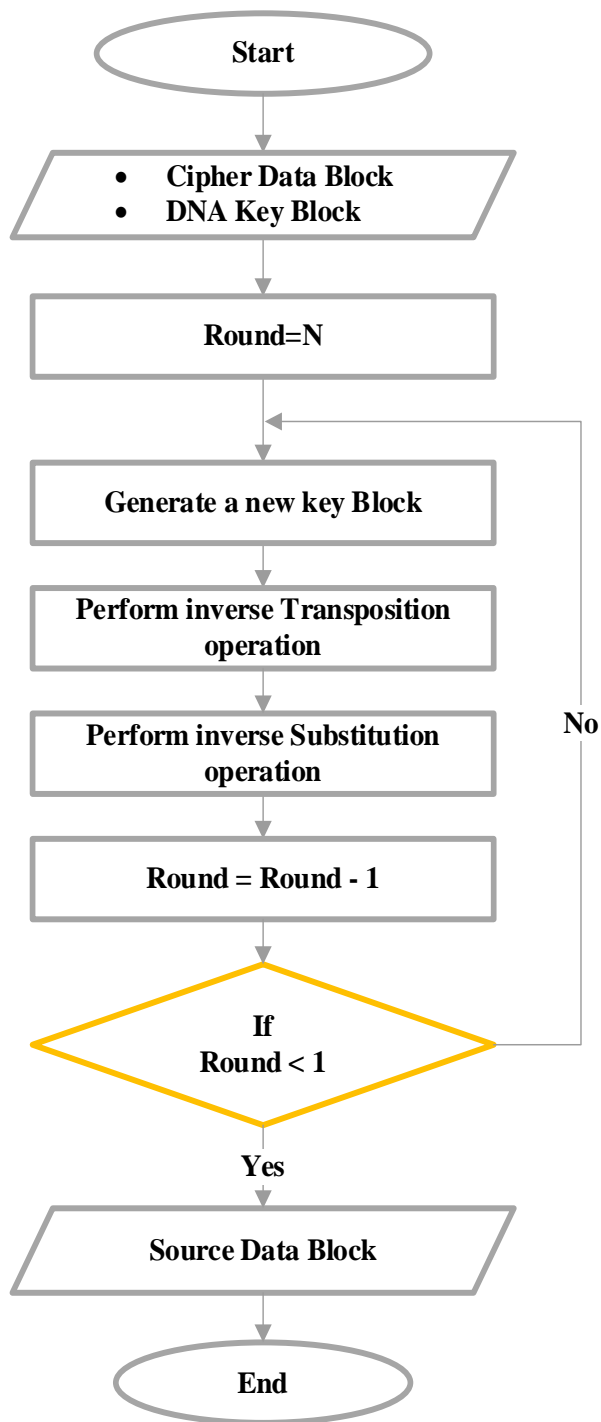


Figure 3.12: The LWCD decryption cipher block operations

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure 3.13: Inverse S-box

3-3 Exchange DNA Key

The encryption key is very important to secure any symmetric encryption algorithm and should be exchanged securely between the sender and the receiver to ensure that only authorized users are able to recover the cipher data that has been transferred.

The DNA datasets can be stored when implementing the encryption and decryption algorithm or used online DNA datasets. In the LWCD encryption, small size of information should be exchanged to restore the cipher data. This amount of information contains three important partitions: the block size, the number of encryption rounds, and the starting point of the DNA tape which are shown in table 3.2.

Table 3.2: Partitions of key used.

Block size	Number of encryption rounds	Starting point on the DNA tape
------------	-----------------------------	--------------------------------

This thesis suggested exchanging the encryption key by using one of two methods first any secure methods such as using a classical asymmetric algorithm or secured by hiding the key using steganography.

Chapter four: Experimental Result and Discussion

4-1 Introduction

The LWCD algorithm is implemented successfully by using images. In addition, it can be implemented to different media data set like audio, video, and others. The images were selected rather than the other data media to demonstrate the effectiveness of the LWCD algorithm because the images can clearly show the results by using some measurements like the histogram of the image and encrypted images. Regarding the DNA tape, there is a lot of online DNA datasets to share and export a huge DNA data that can be accessible from both the sender and receiver which allow choosing any part of the online data to be robust against hackers. In this thesis, the online Fasta datasets (Genomatix, 2021) were selected to generate the encryption DNA key.

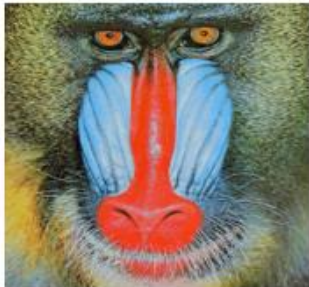
The conducted experiments and the obtained results are discussed in this chapter. Section 4-2 proposes and describes the setup of the experiment, and then section 4-3 evaluates metrics and parameters that are used to evaluate the LWCD algorithm. Section 4-4 compares the result of the proposed LWCD algorithm with AES and 3DES results, and then analyzes the effects of changing the encryption rounds, the effect of the block size, the avalanche effect, and finally the effect of the key size in the LWCD algorithm.

4-2 Experiments Setup

The proposed LWCD algorithm presented in this thesis is implemented by using the c-sharp programming language over the test environment running on windows 7 ultimate SP1 64-bits with a System Processor Intel(R) Core (TM) i3-3110M CPU @2.4GHz processor and 4 GB System Memory.

Different images were used to investigate and evaluate the LWCD algorithm as shown in figure 4.1. These images are selected because most of the research papers used and tested it (Babaei et al., 2020; Wan et al., 2020), and they are called as follows:

- 1) Baboon.bmp colored image with 512x512 original resolution and size 786432 bytes.
- 2) Lake.bmp gray image with 256x256 original resolution and size 196608 bytes.
- 3) Lena.bmp colored image with 256x256 original resolution and size 196608 bytes.
- 4) Pepper.bmp colored image with 512X512 original resolution and size 786432 bytes.
- 5) Photographer.bmp gray image with 512X512 original resolution and size 786432 bytes.



A: Baboon



B: Lake



C: Lena



D: Pepper



E: Photographer

Figure 4.1: Images for evaluation.

4-3 Evaluation metrics and parameters

This section introduces the evaluation metrics that are used to test and evaluate the LWCD algorithm and compares some of the results with other classical cryptography algorithms like AES and 3DES. Most researchers used these two encryption algorithms to evaluate because The National Institute of Standards and Technology (NIST) recommends comparing with AES (Almuhammadi & Al-Hejri, 2017); it is one of the strongest symmetric encryptions; and 3DES is a classical and a strong encryption (Al-Omari, 2019; Gupta et al., 2020; Priyatham, 2020), these two encryption algorithms are very strong due to the large key size. For evaluation, the AES selected with key size 256-bits and 3DES with key size 192-bits. The five popular criteria metrics listed below are used in the evaluation (AL-Wattar, 2020; Wan et al., 2020):

1. Encryption time: the encryption time is one of the main parameters used to evaluate any encryption algorithm by calculating the required time to complete all operations of the encryption algorithm.
2. Key size: the effect of the key size.
3. Peak Signal to Noise Ratio (PSNR):. Peak signal-to-noise ratio (PSNR) is one of the most quality evaluation methods to measure the distortion of the data after the encryption. PSNR is calculated using equations 1, and 2 used for encrypted images, and measured in decibels, it is defined as the ratio between the original image and the encrypted image. The higher value of PSNR means the encrypted image is near to the original image so the PSNR must be as a low value as possible (Nasution & Wibisono, 2020; Wan et al., 2020)

$$NMAE = \frac{1}{w*h*p} (\sum_{k=0}^{(w*h*p)^{-1}} |I(k) - E(k)|) * 100 \quad (1)$$

Where the NMAE is a normalized mean absolute error, w is the width, h is the height, p is the palette, I is a source image, and E is an encrypted image (Al-Husainy & Uliyan, 2017).

$$PSNR = 10. \log_{10} \left(\frac{MAX_I^2}{NMAE} \right) \quad (2)$$

Where the MAX_I is the maximum byte value in the image (Al-Husainy & Uliyan, 2017).

4. Information entropy: The most important indicator for information randomness is the information entropy and it is described and used to measure the randomness of the data and it is the average scale of information expected from the data after the encryption (Babaei et al., 2020). Equation 3 is used to calculate the entropy.

$$Entropy = - \sum_{i=1}^n p_i \log_2(p_i) \quad (3)$$

Where p_i the probability of occurring the data i and n is the difference value of the data (Al-Husainy & Uliyan, 2017).

5. Avalanche effect: the Avalanche effect means that any bits change or minor change of the original image or in the encryption key should affect the encrypted image. The avalanche effect evaluates the strongest of the encryption algorithm from hacking threats such as Brute force attack and calculated by using equation 4 (Aljawarneh & Yassein, 2017) and the result should be above 50% (Verma & Sharma, 2020).

$$Avalanche\ effect = \frac{No:\ of\ flipping\ bits\ in\ the\ ciphertext}{No:\ of\ bits\ in\ the\ ciphertext} X 100\% \quad (4)$$

4-4 Performance and evaluation of the LWCD algorithm

This section analyzes and evaluates the proposed LWCD algorithm to answer the research questions of this thesis. Several images have been used in different situations and some images have been encrypted by using AES and 3DES under the same implementation conditions.

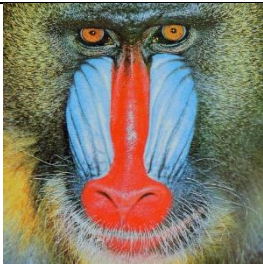

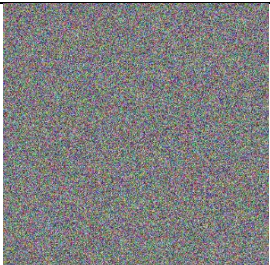
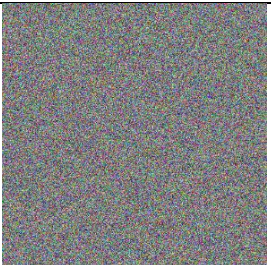
4-4.1 The Compared Result with the classical encryption algorithm

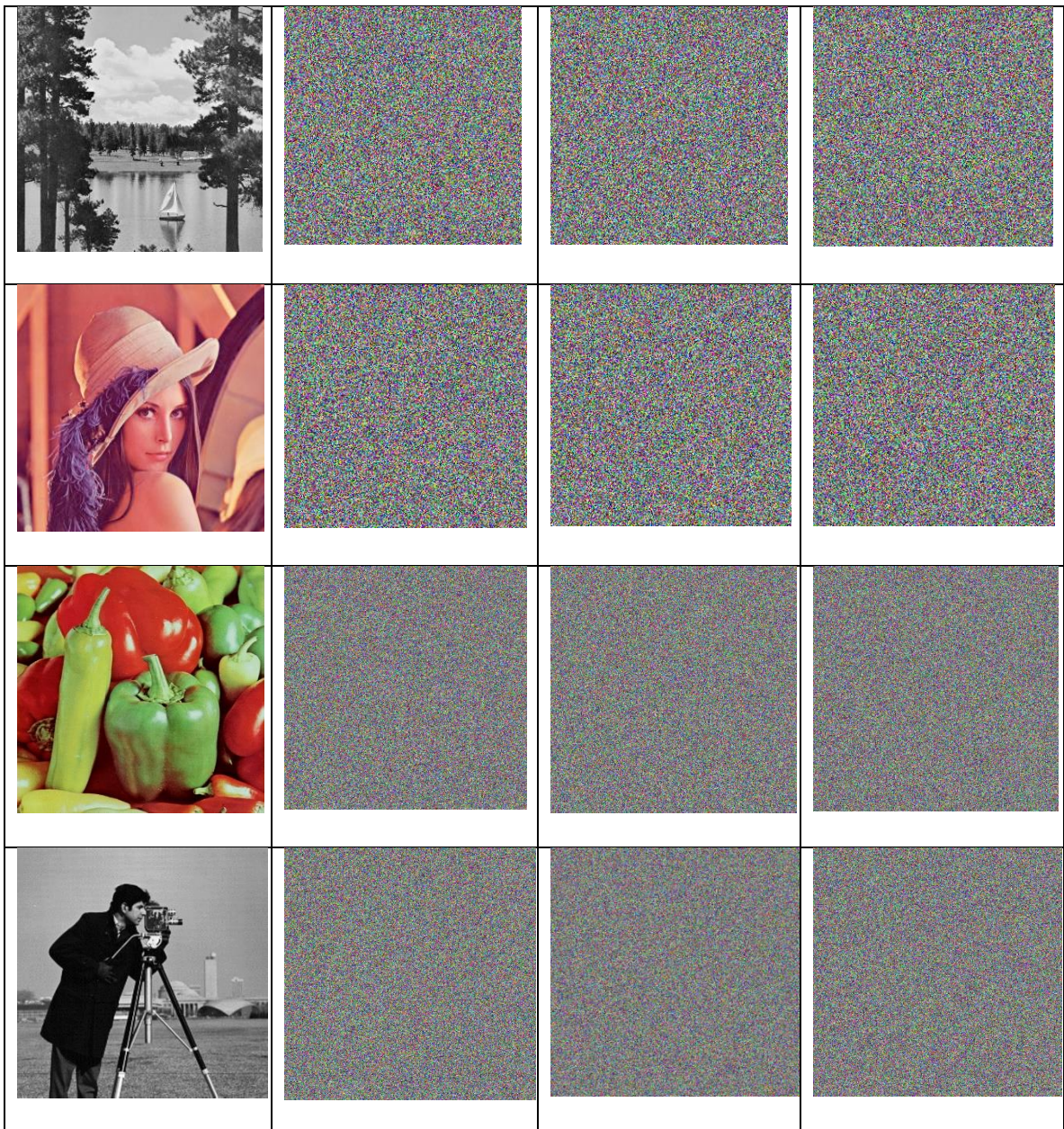
This section analyzes the LWCD algorithm and compares the result with AES and 3DES. In this evaluation, the LWCD algorithm is configured with block size 72-bits and uses a DNA tape with size 21272-bits divided to 72-bits. The encryption rounds are set as three rounds for each block. The five images as in figure 4.1 are used to analyze the LWCD algorithm.

4-4.1.1 Encrypted Images

The five testing images are encrypted and decrypted successfully by using the LWCD algorithm, AES, and 3DES. As table 4.1. The encrypted images display the effect of encryption in the three methods where from noticing the LWCD algorithm got competitive encrypted images compared with other algorithms.

Table 4.1. Encrypted Images

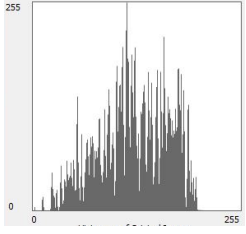
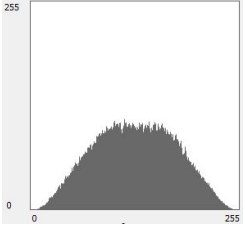
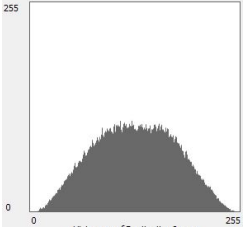
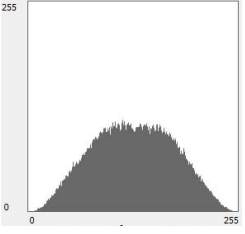
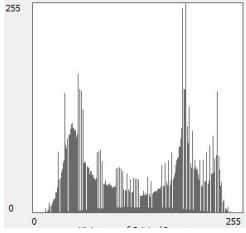
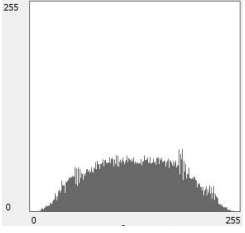
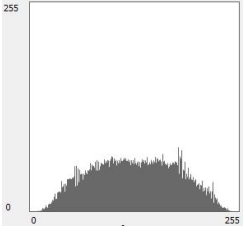
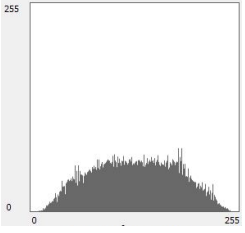
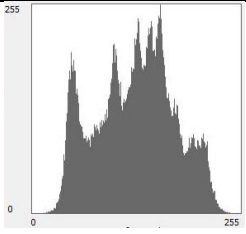
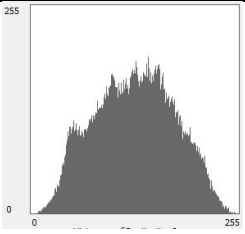
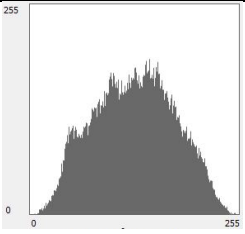
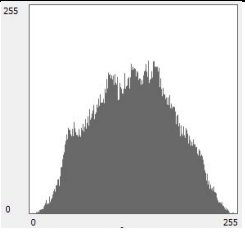
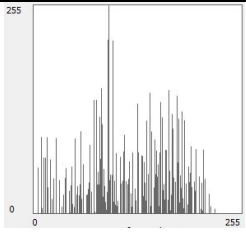
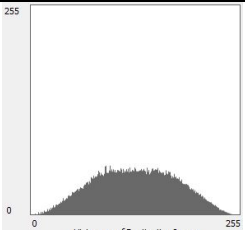
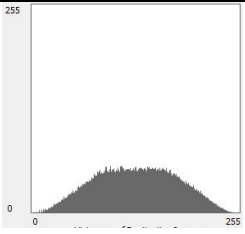
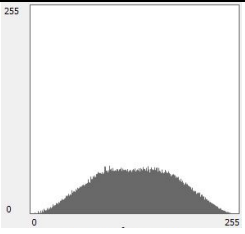
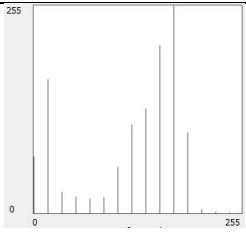
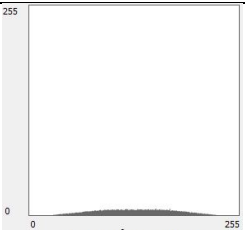
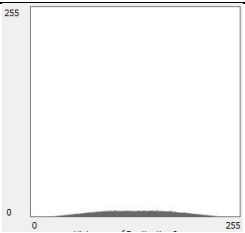
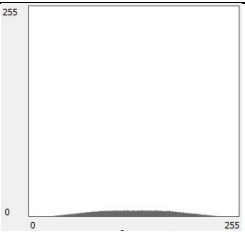
Image	LWCD	AES	3DES
			



4-4.1.2 Images Histogram

The image histogram is graphical of the pixel intensity distribution as shown in table 4.2. The pixels of the original images fluctuate and not uniform while the pixels of encrypted images are uniform and flat which means the statistical hackers are not able to extract information from the encrypted images. That indicates that the LWCD algorithm is efficient.

Table 4.2 Histogram of original images and the encrypted images

Image	Image	LWCD	AES	3DES
Baboon				
Lake				
Lena				
Pepper				
Photographer				

4-4.1.3 Images correlation

The correlation between the original images and the encrypted images as shown in table 4.3 and figure 4.2 closed to 0.1 with most of the lower results by the LWCD algorithm.

Table 4.3 Correlation between original images and encrypted images

Encryption Algorithm	key size bits	Baboon	Lake	Lena	Pepper	Photographer
LWCD	72	0.099	0.088	0.097	0.098	0.123
AES	256	0.101	0.089	0.102	0.096	0.122
DES	192	0.1	0.085	0.101	0.097	0.123

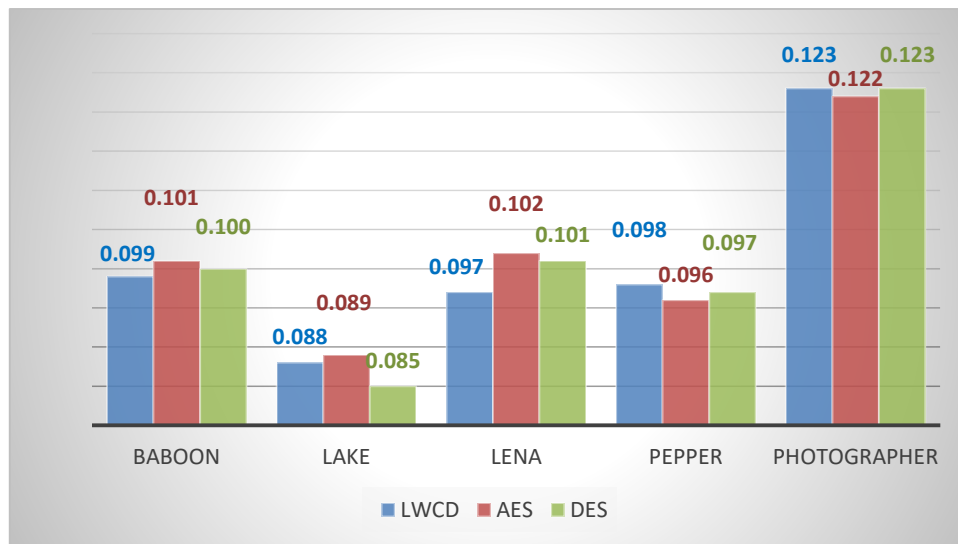


Figure 4.2: Correlation between original images and encrypted images

4-4.1.4 Encryption Time

One of the main parameters that should be tested to evaluate the LWCD algorithm is the encryption time, especially for IoT devices. Table 4.4 clearly displays that the LWCD algorithm has the shortest encryption time for four images except the Lake image which is close enough to the AES and 3DES. The LWCD algorithm uses a small encryption key size

compared to other encryption algorithms and gets the best encryption time that is clearly displayed in figure 4.3.

Table 4.4 Encryption time in second

Encryption Algorithm	key size bits	Baboon	Lake	Lena	Pepper	Photographer
LWCD	72	1.144	0.319	0.313	1.109	1.17
AES	256	1.84	0.308	0.334	1.128	1.193
DES	192	1.383	0.369	0.312	1.269	1.408

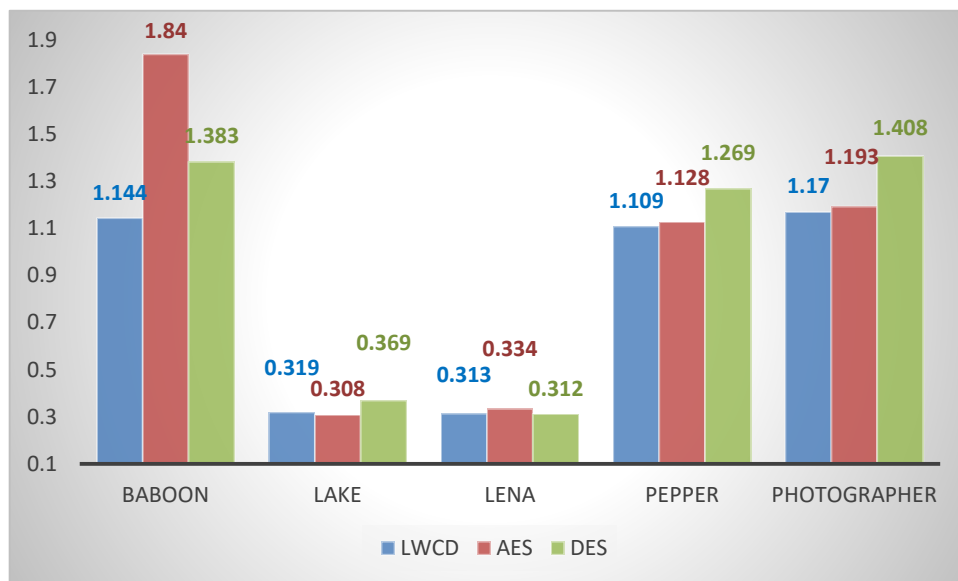


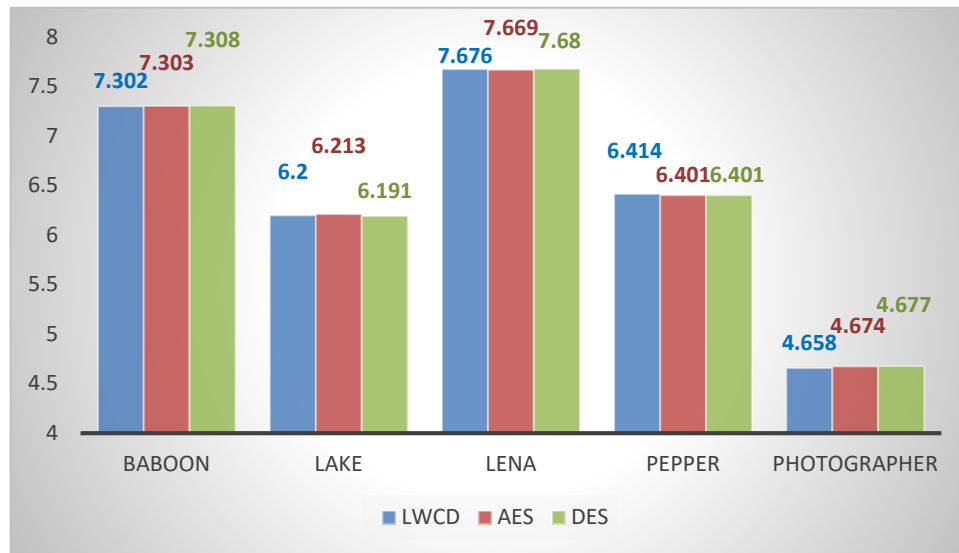
Figure 4.3: Encryption time in the second

4-4.1.5 PSNR Comparison

PSNR is a numerical test used to calculate the distortion of the data after the encryption. The high noise ratio means a good encryption technique (Al-Husainy & Uliyan, 2017). Whereas, the higher PSNR value means that the encrypted image is near to the original image, so the PSNR must be as low value as possible (Nasution & Wibisono, 2020; Wan et al., 2020). As table 4.5 and figure 4.4 show, most of the results of the LWCD algorithm are the lowest value or nearest to the other result of the AES and the 3DES algorithm.

Table 4.5 PSNR in the decibels comparison

Encryption Algorithm	key size bit	Baboon	Lake	Lena	Pepper	Photographer
LWCD	72	7.302	6.2	7.676	6.414	4.658
AES	256	7.303	6.213	7.669	6.401	4.674
DES	192	7.308	6.191	7.68	6.401	4.677

**Figure 4.4: PSNR in the decibels comparison**

4-4.1.6 Information Entropy

Information entropy measures the randomness of the image gray value. It is a scalar value that should be close to eight (Babaei et al., 2020). As in table 4.6 and figure 4.5, the LWCD algorithm achieves a comparable result of entropy and nearest to the results of the AES and 3DES encryption which indicates that the likelihood of information leakage is very small.

Table 4.6 Information entropy comparison

Encryption Algorithm	key size bits	Baboon	Lake	Lena	Pepper	Photographer
LWCD	72	7.999728	7.998927	7.998951	7.999669	7.99899
AES	256	7.999748	7.998981	7.999102	7.999791	7.999771
DES	192	7.999758	7.998958	7.998998	7.999793	7.999746

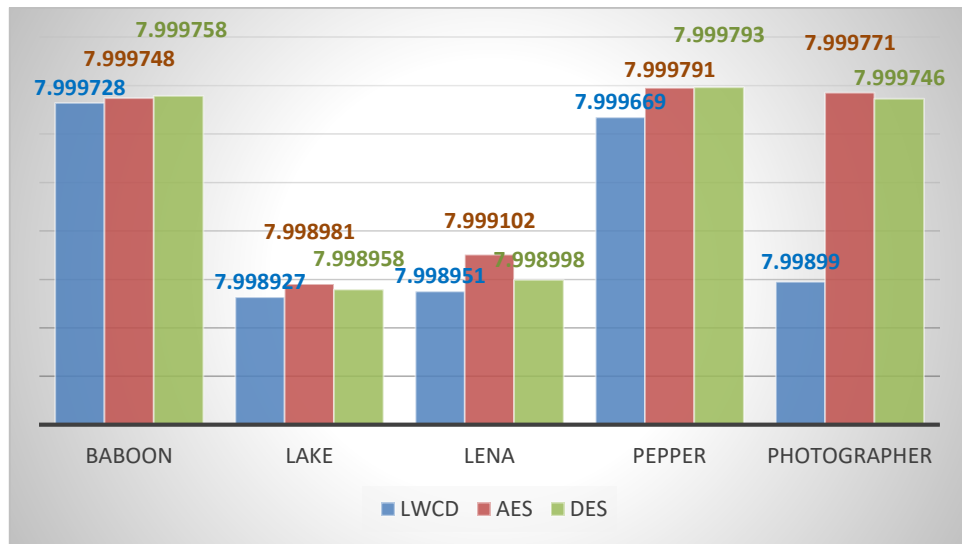


Figure 4.5: Entropy comparison

4-4.2 Avalanche effects

The Avalanche describes the probability of changing the encrypted data if the source data or the key changed slightly (Aljawarneh & Yassein, 2017)




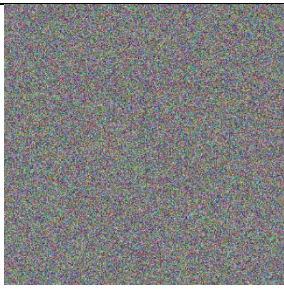
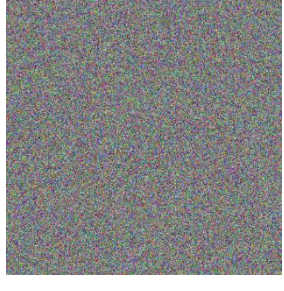
Table 4.7 shows the percentage of the avalanche effects with a result larger than 50% when changing one-bit and close to 50% when changed to 3-bits and 5-bits. Table 4.8 shows the difference between the original encrypted images and other encrypted images when changed 1-bit, 3-bits, and 5-bits.

Table 4.7: The Avalanche effects results

Number of bits changed	Avalanche Effects %
1-bit	50.0122%
3-bits	49.9710%
5-bits	49.9936%

Number of bits changed	Avalanche Effects %
1-bit	50.0122%
3-bits	49.9710%
5-bits	49.9936%

Table 4.8: Encrypted images based on Avalanche effect.


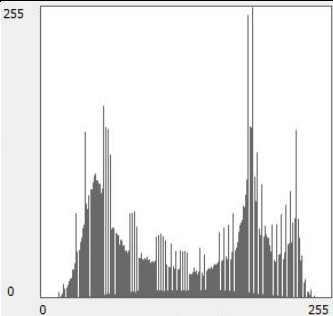
Original Image	
0 bit changed	
1 bit changed	
3 bits changed	
5 bits changed	

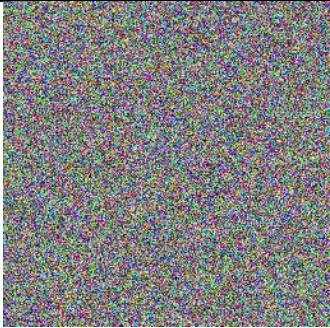
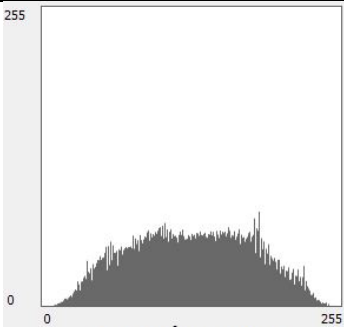

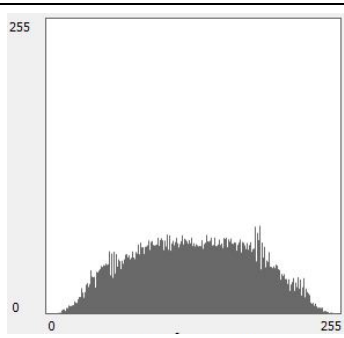
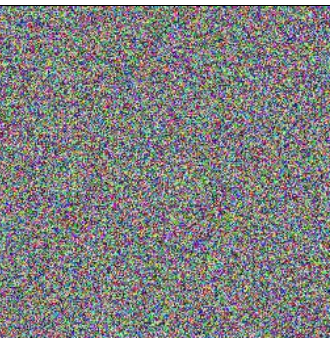
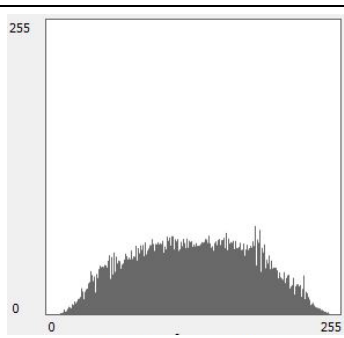
4-4.3 Evaluation of Variable Number of Rounds

This section answers the first question of this thesis. The Lake image size of 1572864 bits (256x256) is used with block size 72bits, and DNA tape space is 21272 bits used by the LWCD algorithm and successfully decrypted and get the original Lake image. The multi-encryption rounds changed three times from 2 to 4 rounds and then evaluated the encryption time, PSNR, the correlation between the original image and encrypted image, and information entropy.

Table 4.9 displays the original image, the encrypted images, and the histogram of the original image with the encrypted images based on the number of encryption rounds. The result in table 4.9 shows that one encrypted image is visually unmeaningful image and the histogram explains the encrypted images are uniformed with flatness rather than the histogram of the original image.

Table 4.9 Encrypted images based on the number of rounds

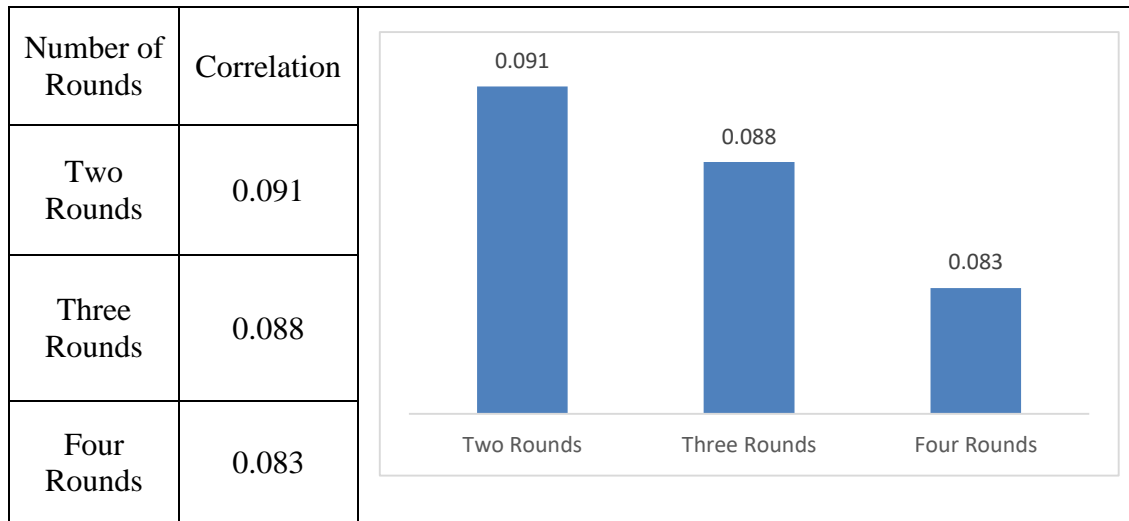
	Image	Histogram of the image
Original image		

<p>Encrypted image with Two Rounds</p>		
<p>Encrypted image with Three rounds</p>		
<p>Encrypted image with Four rounds</p>		

The correlation between the original image and the encrypted images is based on the number of encryption rounds shown in table 4.10, and it is less than 0.1 in all number of rounds. Thus, the best result shown is when four rounds are used while the largest correlation when two rounds are used.

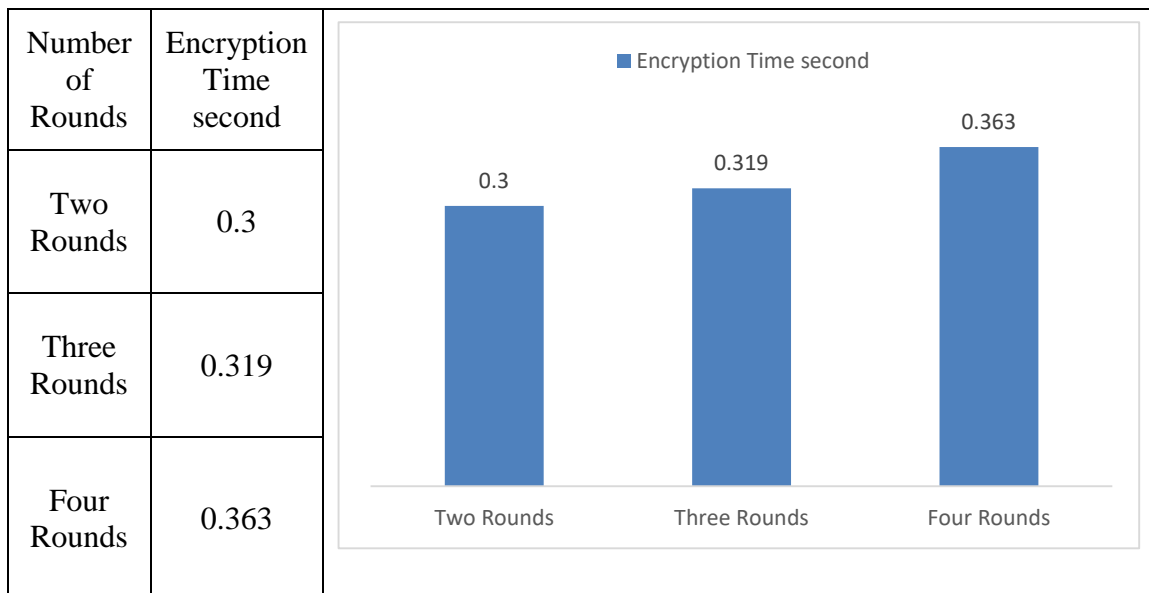
Table 4.10 Correlation between original and encrypted images based on the number of rounds

Table 4.11 displays the execution time when changing the number of rounds and it is



clear that the encryption and decryption time is a little bit increased when the number of rounds increased because the LWCD algorithm needs more encryption operations and the shortest time when using two rounds and the largest encryption time when using four rounds.

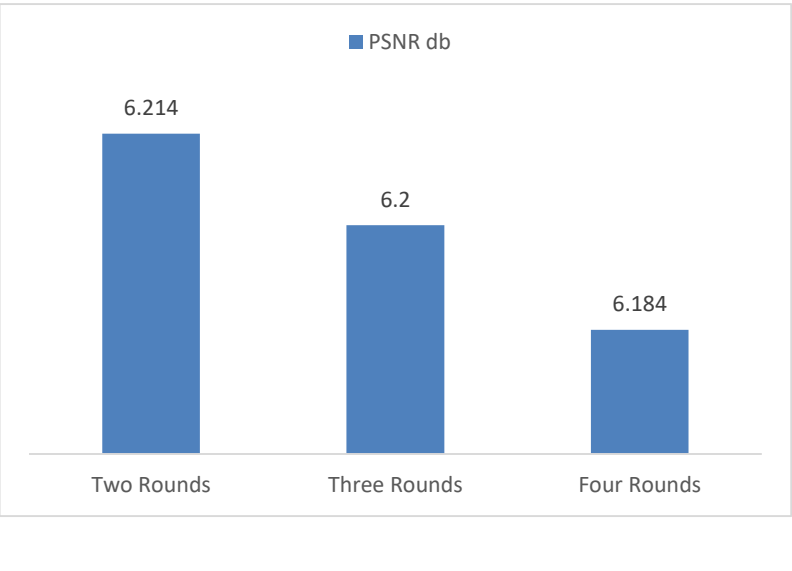
Table 4.11 The encryption time when changing the number of encryption rounds



The best PSNR result when using four rounds, in addition, all results were nearly closed as shown in table 4.12 with the worst result when using two rounds.

Table 4.12 The PSNR result when changing the number of encryption rounds

Number of Rounds	PSNR db
Two Rounds	6.214
Three Rounds	6.2
Four Rounds	6.184

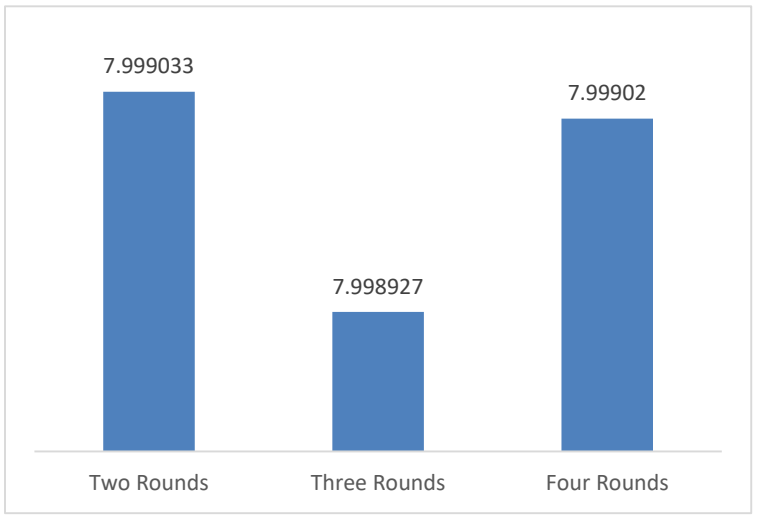


A bar chart titled 'PSNR db' showing the results for three different numbers of encryption rounds. The x-axis is labeled with 'Two Rounds', 'Three Rounds', and 'Four Rounds'. The y-axis represents the PSNR value in decibels. The bars are blue. The values are: Two Rounds: 6.214, Three Rounds: 6.2, and Four Rounds: 6.184.

Table 4.13 displays the result of information entropy when changing the number of encryption rounds and all results are close to 8 and with very few differences.

Table 4.13 The Entropy result when changing the number of encryption rounds

Number of Rounds	Entropy of Encrypted Image
Two Rounds	7.999033
Three Rounds	7.998927
Four Rounds	7.99902




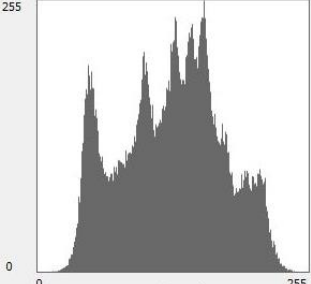
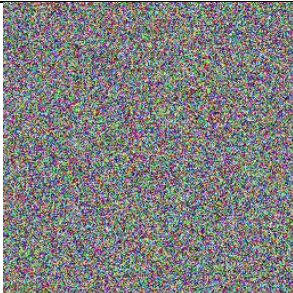
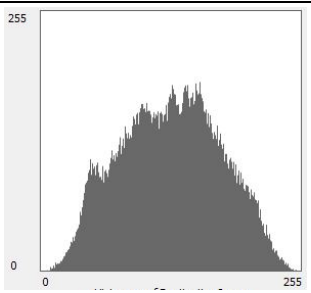
A bar chart showing the entropy of encrypted images for three different numbers of encryption rounds. The x-axis is labeled with 'Two Rounds', 'Three Rounds', and 'Four Rounds'. The y-axis represents the entropy value. The bars are blue. The values are: Two Rounds: 7.999033, Three Rounds: 7.998927, and Four Rounds: 7.99902.

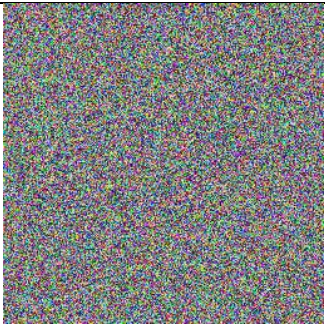
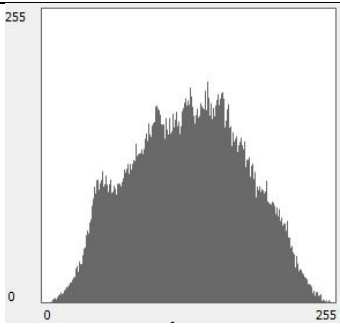
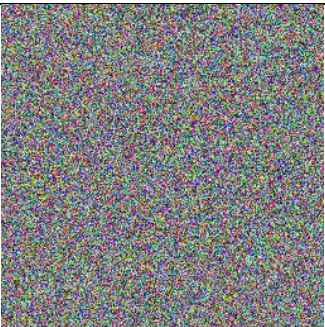
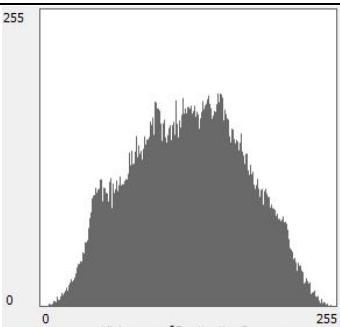
4-4.4 Different Block Size.

The block size is the second variable parameter in the LWCD algorithm. The Lena image with 256x256 original resolution and size 196608 byte is used to test this parameter using a DNA tape keyspace 21272-bits, and three encryption rounds. As the LWCD, the key size depends on the block size and should be the same size; therefore, the block size changed three times: 32-bits, 72-bits, and 128-bits to calculate the encryption time, PSNR, the correlation between the original image and encrypted image, and information entropy.

Table 4.14 displays the original image, the encrypted images, the histogram of the original image, and encrypted images based on the block size. As a result, the change of block size is affective and provides flatness and uniformity of the histogram of the encrypted image.

Table 4.14 Encrypted images based on block size

	Image	Histogram of the image
Original image		
Encrypted image with block size 32-bits		

<p>Encrypted image with block size 72-bits</p>		
<p>Encrypted image with block size 128-bits</p>		

The correlation between the original image and the encrypted images, when changed the block size is shown in table 4.15, displayed the best result when using 72-bits block size.

Table 4.15 Correlation between encrypted images based on block size

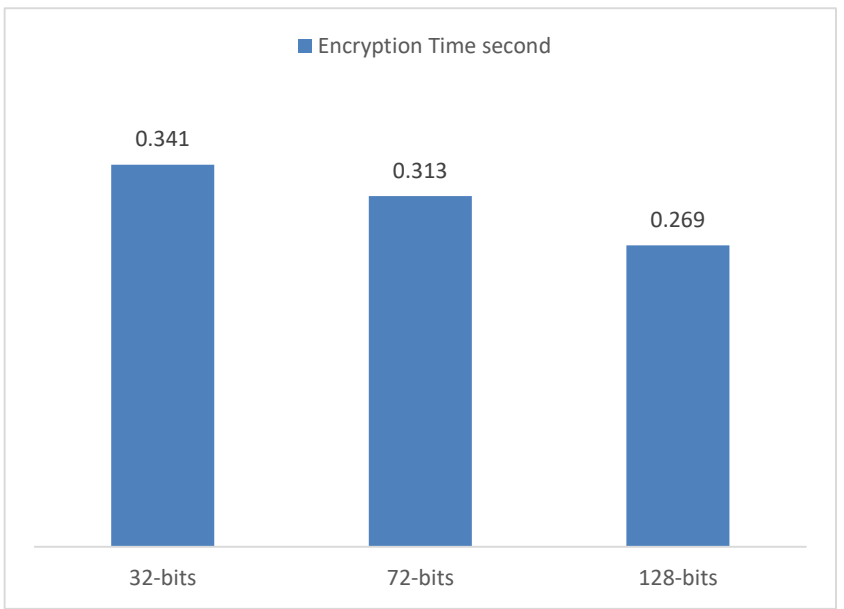
Block size	Correlation between Original and Encrypted Image
32-bits	0.101
72-bits	0.097
128-bits	0.105

Block size	Correlation
32-bits	0.101
72-bits	0.097
128-bits	0.105

Table 4.16 displays the result of encryption time when changing the block size and it is clear that the encryption and decryption time is a little bit decreased when the block size is increased because the big block size means a low total number of the blocks, so it needs a small total operation but needs more resources so the lowest encryption time when using 128-bits block size.

Table 4.16 The result of encryption time when changing the block size

Number of Rounds	Encryption Time second
32-bits	0.341
72-bits	0.313
128-bits	0.269



The bar chart displays the encryption time in seconds for three different block sizes: 32-bits, 72-bits, and 128-bits. The y-axis represents the encryption time in seconds, and the x-axis represents the block size. The values are 0.341 for 32-bits, 0.313 for 72-bits, and 0.269 for 128-bits. The legend indicates that the blue bars represent 'Encryption Time second'.

Block Size	Encryption Time (seconds)
32-bits	0.341
72-bits	0.313
128-bits	0.269

Table 4.17 displays the PSNR result when changing the block size and finds that the 72-bit block size is the best result.

Table 4.17 The PSNR result when changing the block size

Block size	PSNR db
32-bits	7.7
72-bits	7.676
128-bits	7.683

The bar chart displays the PSNR db values for three different block sizes. The x-axis represents the block size (32-bits, 72-bits, 128-bits) and the y-axis represents the PSNR db value. The bars are blue and labeled with their respective values: 7.7 for 32-bits, 7.676 for 72-bits, and 7.683 for 128-bits.

Table 4.18 displays the information entropy result when changing the block size and finds that the 128-bit block size is the best result and close to eight.

Table 4.18 The Information entropy result when changing the block size

Block size	Entropy of Encrypted Image
32-bits	7.999025
72-bits	7.998951
128-bits	7.999088

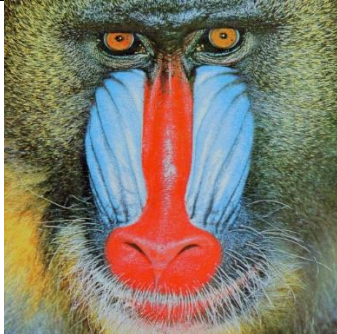
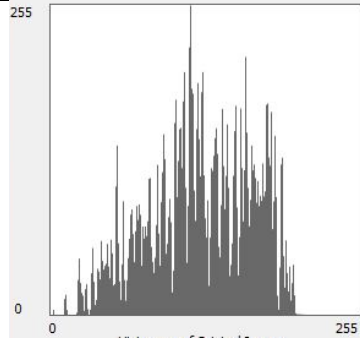
The bar chart displays the Entropy of Encrypted Image values for three different block sizes. The x-axis represents the block size (32-bits, 72-bits, 128-bits) and the y-axis represents the Entropy of Encrypted Image value. The bars are blue and labeled with their respective values: 7.999025 for 32-bits, 7.998951 for 72-bits, and 7.999088 for 128-bits.

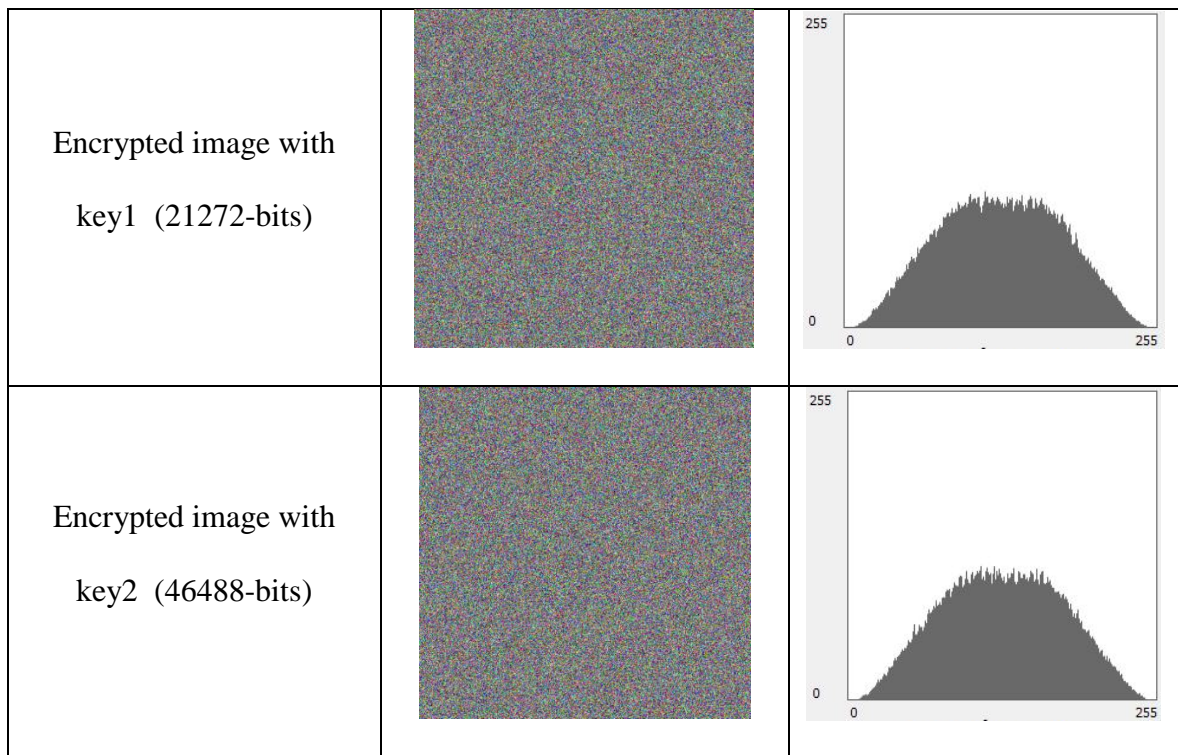
4-4.5 The key space size

The encryption key used in the LWCD algorithm depends on the DNA tape and each data block is encrypted with a different key while AES uses a 256-bits key for whole blocks and 3DES uses a 192-bit key for whole blocks. To evaluate the LWCD encryption based on the key space size, the Baboon image with 512x512 resolution, and size of 786432 bytes used with block size of 72-bits and three encryption rounds. The two DNA key space used are key1 with size of 21272-bits and key2 with size of 46488-bits.

Table 4.19 displays the original image, the encrypted images, the histogram of the original image, and encrypted images based on the different encryption key space sizes used. As a result, the change of encryption key space affects the encryption image and the histogram of the image.

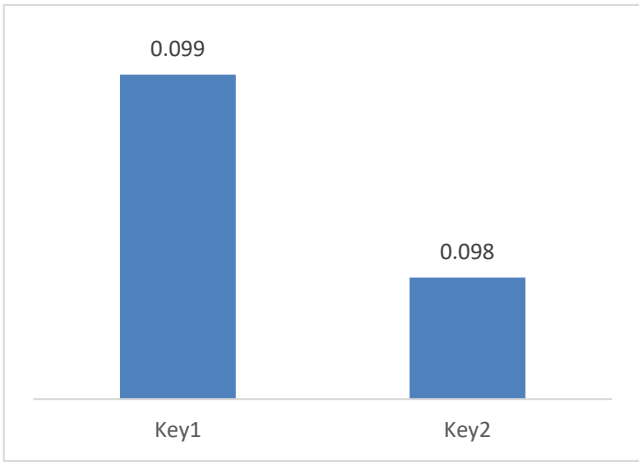
Table 4.19 Encrypted images with different key space

	Image	Histogram of the image
Original image		



The larger DNA keyspace size used in the LWCD algorithm provides a low relation between the original image and the encrypted image as shown in table 4.20

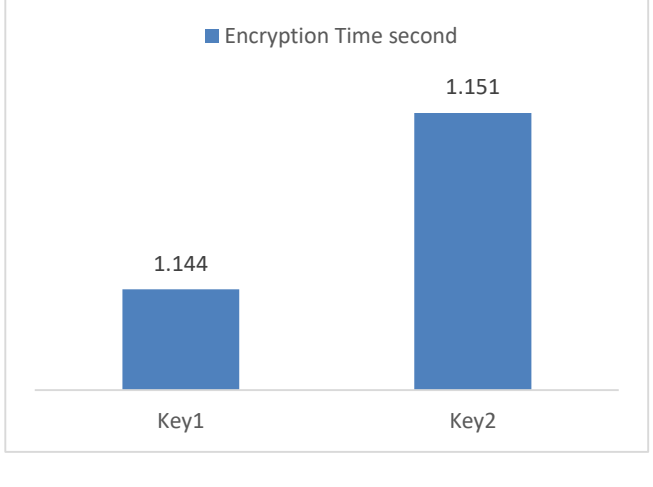
Table 4.20 Correlation between the original image and encrypted images with different keyspace

Encryption Keyspace	keyspace size bits	Correlation between original and encrypted image	
Key1	21272	0.099	
Key2	46488	0.098	

The changing of the encryption keyspace affects the encryption time as in table 4.21. When the size of the encryption block increases, the encryption time also increases because there are operations to generate a key from DNA tape for each round, so the encryption time with the smallest keyspace is less than when using a larger keyspace.

Table 4.21 Encrypted time with different keyspace

Encryption keyspace	keyspace size	Encryption time second
Key1	21272	1.144
Key2	46488	1.151

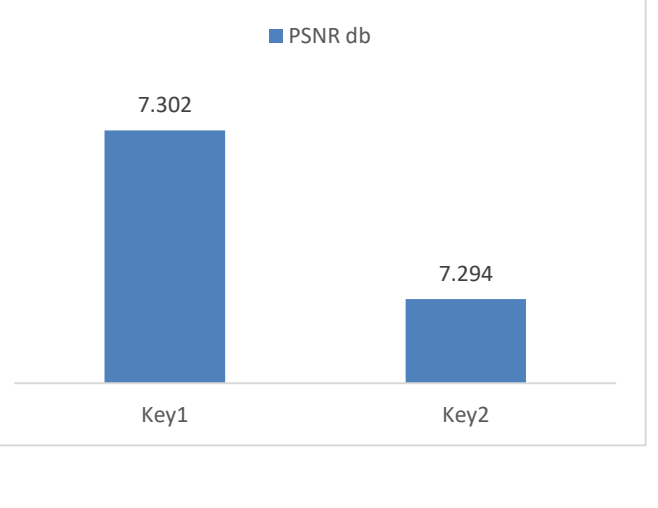


The bar chart displays the encryption time in seconds for two different keys. The x-axis is labeled 'Encryption keyspace' with categories 'Key1' and 'Key2'. The y-axis represents 'Encryption Time second'. For Key1, the time is 1.144 seconds. For Key2, the time is 1.151 seconds. The bars are blue and the values are printed above each bar.

Table 4.22 displays the PSNR result when changing the encryption keyspace, where the best result are obtained when using a large keyspace size.

Table 4.22 the PSNR result with different keyspace

Encryption Keyspace	Keyspace size	PSNR db
Key1	21272	7.302
Key2	46488	7.294

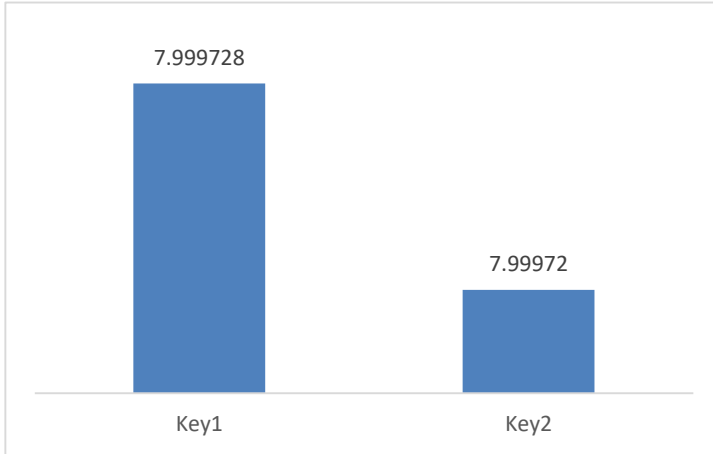


The bar chart displays the PSNR result in decibels (db) for two different keys. The x-axis is labeled 'Encryption Keyspace' with categories 'Key1' and 'Key2'. The y-axis represents 'PSNR db'. For Key1, the PSNR is 7.302 db. For Key2, the PSNR is 7.294 db. The bars are blue and the values are printed above each bar.

The information entropy when using a small key space gives a better result than the large key space but the two results are close to eight as shown in table 4.23.

Table 4.23 The information entropy result with different key space

Encryption Key space	key space size	Entropy of Encrypted Image
Key1	21272	7.999728
Key2	46488	7.99972



The bar chart displays the information entropy values for two different key spaces. The x-axis is labeled 'Key1' and 'Key2', and the y-axis represents the entropy value. The bar for Key1 reaches a value of 7.999728, while the bar for Key2 reaches a value of 7.99972. The bars are blue and set against a white background with a light gray border.

Key	Entropy
Key1	7.999728
Key2	7.99972

Chapter Five: Conclusion and Future Work

5-1 Conclusion

The LWCD proposed in this thesis is a new lightweight cryptography algorithm for IoT devices based on DNA tape as a key with the flexibility to change the block size and encryption rounds to be compatible with IoT devices resources and the importance of the data collected. It uses simple encryption operations and is characterized by using the different DNA keys for each block and round. Consequently, the DNA tape and the randomness of the S-Box, T-Box, and Fix-table increases the security level of the algorithm.

We conducted several experimental results for the LWCD algorithm to clearly answer the two research questions of this thesis. When testing the effect of variable encryption rounds on the LWCD algorithm, the best result of PSNR is achieved by using four rounds, but the encryption time increased because there are extra encryption operations. This means that the security of the algorithm increases by increasing the number of encryption rounds.

The block size is another variable parameter, and the result displays that the 128-bits take the lowest encryption time because the total number of encryption operations is decreased and the best information entropy result is achieved when the 72-bits block size is used to get the best PSNR value.

The pivot evaluation to test the credibility of the LWCD is the comparison with AES and 3DES. The results indicate that the LWCD has proven its efficiency effectiveness in encryption time, PSNR, and closeness to others when testing the information entropy. Regarding the key size, the LWCD algorithm uses the smallest key in addition to variable

key size depending on the data block size while the AES and 3DES use a fixed key to encrypt the data; therefore, the LWCD algorithm achieves the best results or the closest to AES and 3DES.

5-2 Future Work

The LWCD algorithm provides an LWC for IoT devices based on DNA tape with variable encryption rounds, and block size could be improved and investigated in the future by firstly implementing and evaluating a secure way to exchange the DNA key parts as mentioned in section 3-3. Secondly, only images are used to evaluate and test the credibility of LWCD in this thesis. However, other multimedia data such as audio, video, and others will be tested. Finally, the input data of LWCD depends on the byte, so the future work will replace bit with byte and evaluate which one is more secure.

References

- Abusaimh, H., & Al-dwairi, R. (2020). Cloud Computing Authentication Attack and Mitigation. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(4), 5529–5534.
- Aditya, K., Mohanty, A. K., Ragav, G. A., Thanikaiselvan, V., & Amirtharajan, R. (2020). Image encryption using dynamic DNA encoding and pixel scrambling using composite chaotic maps. *IOP Conference Series: Materials Science and Engineering*, 872(1), 12045.
- Aishwarya, R. U., & Sreerangaraju, M. N. (2019). Enhanced Security using DNA Cryptography. *International Research Journal of Engineering and Technology (IRJET)*, 06(06), 3193–3196.
- Al-Husainy, M., Al-Sewadi, H., & Masadeh, S. (2018). Lightweight Cryptosystem for Image Encryption Using Auto-Generated Key. *Journal of Engineering and Applied Sciences*, 13(17), 7418–7425.
- Al-Husainy, M., & Al-Shargabi, B. (2020). Secure and Lightweight Encryption Model for IoT Surveillance Camera. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(2), 1840–1847.
- Al-Husainy, M., & Uliyan, D. (2017). Image encryption technique based on the entropy value of a random block. *Image*, 8(7), 260–266.
- Al-Omari, A. H. (2019). Lightweight dynamic crypto algorithm for next internet generation. *Engineering, Technology & Applied Science Research*, 9(3), 4203–4208.

- Al-Shargabi, B., & Al-Husainy, M. A. F. (2021). A New DNA Based Encryption Algorithm for Internet of Things. *International Conference of Reliable Information and Communication Technology, IRICT 2020*, 786–795.
- AL-Wattar, A. H. (2020). A New Lightweight Proposed Cryptography Method for IoT. *A New Lightweight Proposed Cryptography Method for IoT*, 9(4), 4954–4958.
- Aljawarneh, S., & Yassein, M. B. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, 76(21), 22703–22724.
- Almuhammadi, S., & Al-Hejri, I. (2017). A comparative analysis of AES common modes of operation. *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–4.
- Babaei, A., Motameni, H., & Enayatifar, R. (2020). A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. *Optik*, 203, 164000.
- Barman, P., & Saha, B. (2019). DNA encoded elliptic curve cryptography system for IoT security. *International Journal of Computational Intelligence & IoT*, 2(2), 478–484.
- Barman, P., & Saha, B. (2018). DNA Encoded Elliptic Curve Cryptography System for IoT Security. *Proceedings of International Conference on Computational Intelligence & IoT (ICCIoT)*, 2(1556–5068), 478–484.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355530
- Bhardwaj, I., Kumar, A., & Bansal, M. (2017). A review on lightweight cryptography algorithms for data security and authentication in IoTs. *2017 4th International*

Conference on Signal Processing, Computing and Control (ISPCC), 504–509.

Bhavani, Y., Puppala, S. S., Krishna, B. J., & Madarapu, S. (2019). Modified AES using Dynamic S-Box and DNA Cryptography. *Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 164–168.

Biswas, A., Majumdar, A., Nath, S., Dutta, A., & Baishnab, K. L. (2020). LRBC: a lightweight block cipher design for resource constrained IoT devices. *Journal of Ambient Intelligence and Humanized Computing*, 1–15.

Biswas, M. R., Alam, K. M. R., Tamura, S., & Morimoto, Y. (2019). A technique for DNA cryptography based on dynamic mechanisms. *Journal of Information Security and Applications*, 48, 102363.

Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E., & Djaba, E. (2019). Encryption protocol for resource-constrained devices in fog-based IoT Using one-time pads. *IEEE Internet of Things Journal*, 6(2), 3925–3933.
<https://doi.org/10.1109/JIOT.2019.2893172>

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. *Wireless Personal Communications*, 112(3), 1947–1980.

Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019). Lightweight cryptography for internet of insecure things: A survey. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 475–481.
<https://doi.org/10.1109/CCWC.2019.8666557>

Dutta, I. K., Ghosh, B., Carlson, A. H., & Bayoumi, M. (2020). Lightweight polymorphic

encryption for the data associated with constrained internet of things devices. *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 1–6.

El-Moursy, A. E., Elmogy, M., & Atwan, A. (2018). DNA-based cryptography: motivation, progress, challenges, and future. *JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS*, 3(1), 67–82.

Genomatix. (2021). *DNA Sequence formats*.

https://www.genomatix.de/online_help/help/sequence_formats.html

Gupta, N., Vijay, R., & Gupta, H. K. (2020). Performance Evaluation of Symmetrical Encryption Algorithms with Wavelet Based Compression Technique. *EAI Endorsed Transactions on Scalable Information Systems*, 7(28), e8.

Hashim, M. M., Rhaif, S. H., Abdulrazzaq, A. A., Ali, A. H., & Taha, M. S. (2020). Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography. *IOP Conference Series: Materials Science and Engineering*, 881(1), 1–18.

Hussein, N. A., & Shujaa, M. I. (2020). DNA computing based stream cipher for internet of things using MQTT protocol. *International Journal of Electrical and Computer Engineering*, 10(1), 1035–1042.

Ibraheem, S. S., Hamad, A. H., & Jalal, A. S. A. (2018). A Secure Messaging for Internet of Things Protocol based RSA and DNA Computing for Video Surveillance System. *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, 280–284.

Indrasena Reddy, M., Siva Kumar, A. P., & Subba Reddy, K. (2020). A secured

cryptographic system based on DNA and a hybrid key generation approach.

BioSystems, 197, 104–207. <https://doi.org/10.1016/j.biosystems.2020.104207>

Jiang, S., Ye, D., Huang, J., Shang, Y., & Zheng, Z. (2020). SmartSteganography: Lightweight generative audio steganography model for smart embedding application.

Journal of Network and Computer Applications, 165, 1–7.

Kolate, V., & Joshi, R. B. (2021). An Information Security Using DNA Cryptography

along with AES Algorithm. *Turkish Journal of Computer and Mathematics Education Vol*, 12(1S), 183–192.

Kotha, H. D., & Gupta, V. M. (2018). IoT application: a survey. *International Journal of Engineering & Technology*, 7(2.7), 891–896.

Kubba, Z., & Hoomod, H. (2020). Developing a lightweight cryptographic algorithm based on DNA computing. *AIP Conference Proceedings*, 2290(1), 40013.

Liu, H., Zhao, B., & Huang, L. (2019). A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map. *IEEE Access*, 7, 65450–65459.

Lu, Y., & Da Xu, L. (2018). Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103–2115.

Nasution, A. S., & Wibisono, G. (2020). A comparison of joint reversible data hiding methods in encrypted remote sensing satellite images. *Journal of Physics: Conference Series*, 1528(1), 12038.

- Pradeeksha, A. S., & Sathyapriya, S. S. (2020). Design and Implementation of DNA Based Cryptographic Algorithm. *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 299–302.
- Priyatham, M. (2020). Light Weight Cryptography for Secure Data Transmission. *International Journal of Engineering Trends and Applications (IJETA)*, 7(5), 30–35.
- Rajesh, S., Paul, V., Menon, V. G., & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. *Symmetry*, 11(2), 293.
- Renuka, G., Shree, V. U., & Reddy, P. C. S. (2018). Comparison of AES and DES Algorithms Implemented on Virtex-6 FPGA and Microblaze Soft Core Processor. *International Journal of Electrical and Computer Engineering*, 8(5), 3544.
- Sajisha, K. S., & Mathew, S. (2017). An encryption based on DNA cryptography and steganography. *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, 2, 162–167.
- Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of Development of Dynamic S-Box Generation. *Comput. Sci. Inf. Technol*, 5(5), 154–163.
- Singh, R., & Sharma, T. (2020). An Explication on Data & Information Security in Human Resource Management System. *Vivechan International Journal of Research*, 11(1), 54–62.
- Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research

opportunities. *IEEE Access*, 9, 28177–28193.

Tiwari, H. D., & Kim, J. H. (2018). Novel method for DNA-based elliptic curve cryptography for IoT devices. *ETRI Journal*, 40(3), 396–409.

Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications*, 10(4), 119–125.

Wan, Y., Gu, S., & Du, B. (2020). A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. *Entropy*, 22(2), 171.