جـــامـعـة الـــشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

Lightweight Cryptosystem for IoT Image Encryption Using DNA

نظام لتشفير صور إنترنت الأشياء باستخدام الحمض النووي

Prepared by:
Ra'ed Fatihy Abu-Shehab

Supervisor:
Dr. Bassam Al-Shargabi

A Thesis Submitted in Partial Fulfillment of the Requirement for the Degree of Master in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

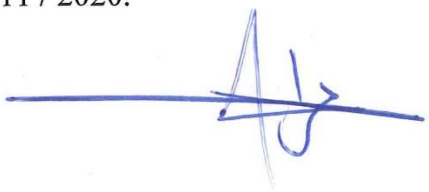
Sep. 2020

Authorization

I, **Ra'ed Fatihy Abu-Shehab**, authorize Middle East University to provide Libraries, Organizations, and Individuals with copies of my thesis when required.

Name: Ra'ed Fatihy Abu-Shehab.

Date: 09 / 11 / 2020.

Signature: 

Thesis Committee Decision

This is to certify that the thesis entitled " Lightweight Cryptosystem for IoT Image Encryption Using DNA " was successfully defended and approved on 7-9-2020 .

Examination Committee Members	Signature

Dr .Bassam Al-Shargabi *(Supervisor / Chairman)*.....

Associate Professor , department of computer science

Middle East University

Dr. Sharefa Murad *(Internal Member)* .....

Associate Professor , department of computer science

Middle East University

(External Committee Member)

Prof. shadi Aljawarneh *(External Member)* .....

Professor , department of computer science

University of science and Technology

Acknowledgement

"Praise be to God who is fulfilled by His righteous grace", this thesis constituted an appreciated stage of my life, which was not easy, but it gave me the opportunity to achieve a decisive goal of my goals in life. I dedicate it to my dear parents and mother, to my wife and children, to my dear brothers, to everyone who has supported me and helped me strongly. Great thanks to Dr. Supervisor Bassam Al-Shargabi. I thank him for his patience. I thank him for the continuous support, knowledge and understanding.

Table of Contents

List of Tables

List of Figures

Table of Abbreviations:

Abbreviation	Meaning
DNA	Deoxyribose Nucleic Acid
XOR	exclusive orj
IOT	internet of thing
(D-GET)	DNA-Genetic Encryption Technique
BDEA	Bi-directional DNA Encryption Algorithm
PCR	Polymerase Chain Reaction
MSE	mean-square error
PSNR	peak signal-to-noise ratio

Lightweight Cryptosystem for IoT Image Encryption Using DNA

Prepared by:

Ra'ed Fatihy Abu-Shehab

Supervisor:

Dr. Bassam Al-Shargabi

Abstract

Given the importance of data security generated from the Internet of things (IoT) applications such as smart building, healthcare monitoring, smart home and, smart city. One of the issues in IoT is to handle and protect the huge amount of data generated from IoT heterogeneous devices. The classical encryption algorithms Data Encryption Standard (DES) and Advanced Encryption Standard (AES) were not suitable for IOT constraint devices, as they have limited memory and processing capabilities. Therefore, there is a need for encryption model that fits the limited computation resources of IoT devices. The proposed DNA based encryption algorithm in this thesis, which is a lightweight encryption algorithm for the (IoT) generated data such as images. The proposed DNA encryption algorithm relies on utilizing the DNA tape for generating strong and completely random key for the data encryption. This algorithm characterized by its high encryption robustness and strength, due to the randomness in creating the encryption key, logical substitution and set of rules for transposition. The DNA based encryption algorithm is implemented and experiments were constructed on different sizes and types of images and compared to DES and AES encryption algorithms under the same environmental conditions to evaluate the efficiency of the proposed algorithm regarding, key size, time, and proportion of distortion. The experimental results reveled that proposed DNA algorithm has lowest encryption time, where it records about 62.5 MSc compared to the other algorithms. In addition, the proportion of distortion shows a value of 8.687 db. For the proposed DNA based encryption algorithm, which is comparable to the DES, and AES algorithms.

Keywords: Data Encryption, Internet of Things (IoT), Deoxyribose Nucleic Acid (DNA).

نظام لتشفير صور إنترنت الأشياء باستخدام الحمض النووي

إعداد: رائد فتحي أبو شهاب

إشراف: د. بسام الشرجبي

المخلص

نظرًا لأهمية أمن البيانات الناتجة من تطبيقات إنترنت الأشياء في جميع جوانب الحياة، حيث تغطي تطبيقات إنترنت الأشياء جوانب كثيرة من حياتنا، مثل المباني الذكية، ومراقبة الرعاية الصحية، والمنزل الذكي، والمدينة الذكية. تتمثل إحدى المشكلات في إنترنت الأشياء في التعامل مع الكم الهائل من البيانات الناتجة عن أجهزة إنترنت الأشياء غير المتجانسة وحمايتها. لم تكن خوارزميات التشفير الكلاسيكية (معيار تشفير البيانات (DES)) و(معيار التشفير المتقدم (AES)) مناسبة لأجهزة انترنت الاشياء المقيدة نظرًا لمحدودية ذاكرة الوصول العشوائي وإمكانيات المعالجة البسيطة. لذلك، هناك حاجة لأنظمة تشفير قوية تناسب أجهزة إنترنت الأشياء. تم اقتراح خوارزمية التشفير المعتمدة على الحمض النووي في هذه الاطروحة، حيث تم اقتراح نظام تشفير فعال لتشفير البيانات الخاصة بإنترنت الأشياء مثل الصور. تعتمد خوارزمية التشفير المقترحة في هذه الاطروحة على استخدام تسلسل الحمض النووي لتوليد مفاتيح تشفير عشوائية وقويه لتعقيد فك تشفير هذه البيانات. تميزت هذه الخوارزمية بقوتها العالية في التشفير، بسبب العشوائية في إنشاء مفتاح التشفير، والاستبدال البسيط، والتبديل المنطقي. تم تطبيق واجراء التجارب العملية للخوارزمية المقترحة في هذه الاطروحة مع بعض الخوارزميات التقليدية مثل **(DES** و**AES)**. من اجل التحقق من فعالية الخوارزمية المقترحة وتم إجراء التجارب على أحجام وأنواع مختلفة من الصور ومقارنتها بخوارزميات تشفير **(DES** و**AES)**، كانت المقارنة ايضا من حيث حجم مفتاح التشفير والوقت المستغرق في التشفير وايضا نسبة **(Proportion of Distortion)**. أظهرت النتائج التجريبية أن أقل وقت تشفيره لخوارزمية التشفير المعتمدة على الحمض النووي المقترحة في هذه الاطروحة، حيث سجلت حوالي 62.5 جزء من الثانية مقارنة بالخوارزميات الأخرى. وكانت قيمة في نسبة **(proportion of distortion)** للصور المشفرة هي **8**.687db لخوارزمية التشفير المعتمدة على الحمض النووي المقترحة في هذه الاطروحة حيث كانت النسبة متقاربة مع بقية الخوارزميات الأخرى.

الكلمات المفتاحية: تشفير، إنترنت الأشياء، الحمض النووي.

Chapter One
Study Background and Motivation

1.1 Introduction

The evolution in the scope of information security have been ever raising. Whole the efforts in the improvement of major strategies for information security directed towards three essential outcomes; information confidentiality, integrity and availability (Kelsi, Kaur & Chang. 2018). Due to the rapid development of information technologies and the huge spread of the Internet with its different applications, the security of multimedia data like image, audio and video, such data generated from IOT devices, has become critical issue, which attracted high attention.

IoT (Internet of Things) devices have been inserted widely in the market drastically, where connected devices about 15 billion. This trend is supposed to continue, with a rating of 26 billion network-connected devices through the year 2020, the plurality of which being IoT and wearable devices. Many as the established systems they deduce from, IoT devices are equipped with sensors but as well offer some type of connectivity functionality. Like, those devices could convey the data they collect to a distant collection point. The different nature of IoT devices is to collect, process, pass data via a communications channel, and periodically control many larger units. The information in question could domain from a heartbeat to the temperature of a room, to living practice and even the site of the user.

IoT devices are open for attack and become an attractive objective to gain the data they hold. Moreover, given the always-on network connectivity, some of those devices

hold and their various usage patterns, these devices could be targeted by malware, raising he potential for harmful usage (Wurm, Hoang, etc, 2016).

Cryptographic methods are used to provide security for valuable data such that just authorized person could decode the data. A cryptographic technology perform encryption to generate encrypted data and allow the secured transmission which could be meaningless to an intruder who doesn't has any knowledge about the key. (Pushpa, 2017).

classical Cryptographic methods and techniques varied, where became not appropriate for multimedia application related to the IOT devices, like Triple DES (The Data Encryption Standard which is a symmetric-key algorithm for the encryption of digital data) DES which designed to substitute the original Data Encryption Standard, and **RSA** algorithm (Rivest, Shamir, and Adelman, the inventors of the technique). Which is based on the fact that there is no efficient method to factor very large numbers, the (RSA) is a public-key encryption methodology. So, DES and RSA are not appropriate for IOT constrained devices because they have limitation in RAM and PCU (Al-gohany & Almotairi, 2019).

The effort in this study will develop a security algorithm constructed for constrained devices that taking advantage of combining the features given by the latest appearing security mechanisms in order to provide sufficiently robust data confidentiality, through adapting simply to emerging and converging technologies such as DNA tape.

The encryption algorithm based on DNA tape have been proposed in this study, as we suggested working in key generation Depending on the sequence of bits randomly. DNA is robust and can encode digital data with top density, making it a granular area for key

generation and using it for image encryption, where image source related to IOT devices. However, data security on multimedia application actually demands all the DNA in a pool to be sequenced, even if just a subset of the information requires to be extracted (Organick, Chen & others .2018).

The major purpose for choosing DNA techniques is to gained benefit of DNA encoding and DNA computing , which contained some biological functions and algebra operations on DNA sequence, like the complementary principle of DNA bases, DNA addition and DNA exclusive OR functions in subsequent research, also , the -features of DNA computing, huge parallelism, massive storage and ultra-low power consumption had been setup and explored for cryptographic objectives like ,signature, encryption and authentication **(**Guesmi, Farah & others .2016).

The contribution within this study related to providing improved DNA cryptography algorithm which will gains high data integrity and security. as we had been used the DNA tape to generated encryption key (Skey). The proposed algorithm created robust encryption algorithm which offered a strong encryption method that fit the limited CPU and RAM for constrained devices. Algorithm strength derived from DNA randomness that provides a robust encryption algorithm which is difficult to break easily.

1.2 Definitions

DNA: Deoxyribose Nucleic Acid (DNA) is a molecule which represents the genetic material for whole living organisms. It is the data carrier of all life styles, and deem as the genetic blue print of every living or located creatures. DNA molecules includes of two long chains grasp with other by complementary base pairs, which twisted around each other to

form a double-stranded helix with the bases on the inside, as shown in table [1,1]. (AlWattar, Zukerman Others, 2015).

Table [1.1]: DNA letters coding

DNA BASE	**CODE**
A	00
C	10
G	01
T	11

A DNA tape include of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), as A and T are complementary (0011), and C and G are complementary (0110). The base pairing technique is the basis for DNA replication. One of the major attributes of the DNA strand series is that it contained various orientations and everyone is different from the other, like, TCCGAATGC is distinct from ATCGATCGC. Another main attribute is the reverse complement, which is implement in two stages: firstly is to reverse the order of the DNA strand bases, and secondly is to take the complements of the reversed strands, where the complement of the base A is T and C is G and vice versa. For example, the reverse complement of AGCTAACC is GGTTAGCT (Raj and Panchami, 2014).

Cryptographic: is a technique of protecting data and communications by using codes so that just those for whom the data is intended could read and handle it. then "crypt"

means "hidden" or "vault" while "graphy" stands for "writing." Cryptography present secure communication in the existence of malicious third parties, called adversaries. Encryption utilizes an algorithm and a key to convert an input (plaintext) into an encrypted output (cipher text). A given methodology will usually transform the same plaintext into the identical cipher text if they used the same key (Krüger, Nadi, et al, 2017).

In computer science, cryptography related to secure information and communication mechanism obtained from mathematical notation and a set of rule depend calculations named algorithms to transform messages in a method that are difficult to decipher. These deterministic algorithms are utilized for cryptographic key generation and digital indicating and verification to safeguard data privacy, web browsing over the internet and confidential communications like email and credit card transactions. Algorithms are being secure if an attacker cannot detect any attributes of the plaintext or the key (Al-gohany & Almotairi, 2019).

Encryption: is the process of transforming the data into cryptographic encoding which can't be read without a key. Encrypted information views meaningless and is highly complex for unauthorized side to decrypt without the valid key (Liu, 2018).

Decryption: is the procedure of takeover encoded or encrypted text or any other information and transforming it back into text which any person or the computer can simply read and understand. This idiom may be utilized to describe the algorithm of unencrypting the information manually or unencrypting the information utilizing the convenient codes or keys (Feng, 2019).

IoT or constraint devices: The constrained devices defined as end nodes with sensors/actuators which could handle a particular application purpose. They are originally linked to gateway-like devices, which need least power, least network management, and in-turn contacted with the IoT cloud stands (Elvstam & Nordahl, 2016).

1.3 Research context

Due to increasing demand for using surveillance cameras which needed for high security environment has surely raised, many different algorithms and methodology have been proposed to develop more security options (Ashby, 2017). So, due to the DNA advantages that have been proven in latest research's on DNA computing which has focused on DNA for key generation to be used in encryption image algorithm related to IOT devices. This study provided adequate encryption algorithm based on DNA for data or images generated from IOT devices like surveillance cameras, which has powerful features that lead to acquiring robust encryption and decryption technique. Therefore, we here put our effort in order to develop strong DNA algorithm which gained the benefit of DNA encoding and DNA computing, which contained some biological functions and algebra operations on DNA tape, like the complementary principle of DNA bases and DNA exclusive OR functions in encryption.

1.4 Problem statement

IoT constraints devices have been widely used in all aspects of our lives , where IoT devices are used to convey sensitive data, as this data need high protection, appropriate to the limited RAM with low and weak CPU just like sensors and cameras. where they are not compatible with traditional cryptographic algorithms such as: (DES), (RSA), where DES is

a symmetric-key algorithm for the encryption of digital data, while the RSA is based on the use of public-key. Such conventional methods are not suitable for constrained devices due to the high computing resources needed by such methods. For the IOT devices, the need to have encryption and decryption algorithm that fit the capabilities of constraints devices with regarding RAM and processing.

From this standpoint, this thesis came to direct its efforts in employing DNA technology to formulate an encryption algorithm which will generate an encryption key that offers perfect encryption method that fit the CPU power and RAM size for IOT constrained devices. This algorithm derives its strength from the DNA randomness that provides a robust encryption algorithm which is difficult to break easily.

Therefore, in this thesis we proposed a DNA encryption algorithm that suits the resources of IoT devices, where the algorithm is based on DNA to generate completely random key and provides a simple encryption stages utilizing substitutions and transposition operations for that fit IoT devices resources.

1.5 Questions of the study

This thesis raises important questions, where this research followed a theoretical and practical approach to providing accurate answers to the following, question:

Q1- How can we employ the DNA sequence for the key generation to provide an encryption algorithm that meets the requirements of IOT constrained devices

Q2- What are the most notable performance aspects differences between proposed DNA based encryption algorithm and the other traditional encryption methods regarding the encryption time, key size and proportion of distortion?

1.6 Objectives of the study

The main objectives for this thesis constructed as follow:

1. Utilizing the DNA sequence to provide a new cryptographic algorithm to meet the limited computation resources of IOT devices
2. Studying the effects of using DNA sequence to provide simple and strong substitution and transportation as key operations for the encryption process
3. Assessing the proposed algorithm in terms of encryption and decryption time, key size, and proposition of distortions for encrypting the images generated from IOT devices.

1.7 Motivation

The numerous security threats in transition data over networks and huge growth in the number and kind of attacks which should be handle with by data security expert in order to safeguard sensitive data, or data vulnerable to unauthorized disclosure or undetected amendment have demanded employ of defense mechanisms in order to provide: Authenticity, Availability, Confidentiality in best level. So this study motivation focus in Providing an efficient and lightweight encryption algorithm for constraints devices, proportional to limited RAM and CPU.

1.8 Contribution

This study will employ DNA technology to create an encryption algorithm that based on DNA tape in order to generate completely random encryption key. The key is then used to for a robust and simple substitution and transposition as the two main phases on the encryption process create to fit the CPU limited Size and small RAM for constrained

devices. The algorithm strength derived from DNA randomness that provides a robust encryption algorithm which is difficult to break easily and hardly to attacked.

1.9 Scope of the study

Several studies were carried out in the evolution of cryptographic techniques, however present improvement in this scope is DNA Cryptography which is developed by depending on the computational strength of DNA (Deoxyribose Nucleic Acid). This thesis proposes algorithm in order to confirm complicated data encryption utilizing DNA sequence. within this work, the notation of binary coding with random values are utilized and sample DNA tape is proposed to encrypt the data. The receiver will acquire both DNA sequence which will be used to obtain the original message. In this technique the sender and the receiver will utilize a common DNA tape through encryption and decryption procedure.

Chapter Two
Related Work

2.1 Introduction

Cryptography is a specified domain of science which compact with the encoding of data for the goal of concealing messages. It plays a vital function in the infrastructure of communication security. The latest work had been done in the domain of cryptography had shown the capability of molecular computation. This opens the way for DNA Computing as the DNA technique consolidates the advance cryptology. Chapter two will provide an overview through Theoretical Literature which is concentrated on the DNA cryptography domain and how it used within IOT devices to generated encryption key, and then we go through Previous Studies to acquire a clear idea about DNA encryption and decryption algorithms that have been constructed in different researches

2.2 Cryptography Methods

The science of protecting information by converting it into a secure format called Cryptography. This procedure called encryption, were it used for centuries to deny handwritten messages from being violated and hacked by unauthorized recipients. Recently, cryptography utilized to protect digital data. It is a branch of computer science which focuses on converting data into texture which couldn’t be identify by unintended users. There are essentially two techniques of cryptography- Symmetric and Asymmetric (Al-Shabi, 2019).

Symmetric Encryption: Within symmetric Cryptography, method the key used for encryption is the same to the key utilized in decryption. therefore, the key distribution has

to be made before the transmission of information. The key applies a very significant role in symmetric cryptography as their security directly based on the nature of key i.e. the key length. There are several symmetric algorithms such as (Aishwarya & Sreerangaraju, 2019**):**

- AES (Advanced Encryption Standard)
- Blowfish (Drop-in replacement for DES or IDEA).
- IDEA (International Data Encryption Algorithm)
- DES (Data Encryption Standard).

2.2.1 Symmetric Encryption

Symmetric encryption use the same cryptographic keys for both encryptions of plaintext and decryption of cipher text. They are faster than asymmetric ciphers and allow encrypting large sets of data. However, they require sophisticated mechanisms to securely distribute the secret keys to both parties. There are five main components of a symmetric encryption system: plaintext, encryption algorithm, secret key, cipher text, and the decryption algorithm (Wen, Wei & others, 2020).).

symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information (Wen, Wei & others, 2020).

One of the most significant property that Symmetric Encryption Algorithm works faster as compared to Asymmetric key algorithms. Another propority is the memory

requirement of Symmetric algorithm where it's lesser as compared to asymmetric (Al-Shabi, 2019).

2.2.1.1 Advanced Encryption Standard

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. The features of AES are as follows:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

Operation of AES: AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix (Rahaman, Corraya, et al, 2020).

2.2.1.2 Data Encryption Standard

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.

DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

DES is based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition (Ratnadewi , Adhie, et al, 2018).

2.2.2 Asymmetric Encryption

Within Asymmetric Key encryption, two various keys the public and the private key are utilized for encryption and decryption. The public key is intended for general use so it is obtainable to anyone on the network. Anyone who going to encrypt the plaintext must know the Public Key of receiver. The authorized person has the ability to decrypt the cipher text via his own private key, below are list of asymmetric encryption algorithms

- Diffie–Hellman key exchange protocol.
- Elliptic-curve cryptography.
- DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm.
- Elliptic-curve cryptography (Al-Shabi, 2019).

2.2.3 Key difference between encryption and cipher text

The key difference between encryption and cipher is that encrypted strings can be reversed back into their original decrypted form if you have the right key. The major difference between a cipher and a cipher is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time.

Encryption is the process, of encrypting something, with a cipher or ciphering methods. Cipher or the Ciphering methods, are the tools unto which you use to encode/decode the data (Al-Farraji, 2020).

2.3. IoT and Encryption

Internet of Things (IoT) is an uprising innovative technology which is gaining popularity day by day. In an IoT network, devices are connected with each other at any time anywhere in the world.

The “Thing” in the IoT is the starting point for an IoT solution. It is typically the originator of the data, and it interacts with the physical world. Things are often very constrained in terms of size or power supply; therefore, they are often programmed using microcontrollers (MCU) that have very limited capabilities. The microcontrollers powering IoT devices are specialized for a specific task and are designed for mass production and low cost (Sehgal, Perelman, etc, 2012).

Latest advances sensors technologies, embedded processors and wireless communication have facilitated the design of small-size low-cost and low-power devices which could be networked or linked to the Internet. Those are the major components of the

emerging model of Internet-of-things (IoT). IoT coverage an ever-increasing level of applications, like smart building, healthcare monitoring, smart home, smart city, and more, one of the issues in IoT is to handle and analyze a large amount of information from heterogeneous devices. The huge number of IoT devices will direct to a fast explosion of the scale of gathered data which produce Security concerns associated with IoT devices such surveillance cameras that create potential risks in our life (Samie & others ,2016).

This issue has two sides: Big Data and diverse application requirements of IoT. Treating all these gathered data with central cloud servers is inactive, and unfeasible, due to: limitation of communication, computing, and storage resources, overall energy and cost and unreliable latency (Samie & others, 2016).

The IoT devices generates a massive amounts of data were transferred through these IOT network to be stored in Cloud. Considering the sensibility of applications in the IoT network. The growing number of intruders and hackers has made that mission very complex. Through time, several cryptographic algorithms have been utilized to ensure the security of transmitted data through IoT networks (Khan & Salah, 2018). The robust of the cryptographic algorithms based on the techniques utilized for managing, producing and distributing the secret keys. Secret keys which are weakly maintained make the cryptographic algorithm useless, even if the algorithm was theoretically and also, practically perfect. Cryptographic algorithms introduced in the literature for IoT constrained devices could be categorized into the symmetric and asymmetric algorithms. Symmetric algorithms utilize the same key for both encryption and decryption. The strength of the symmetric algorithms actually based on how the key was securely exchanged between the sender and receiver (Vermesano & Friess, 2014).

Asymmetric algorithms actually avail two various keys involving the public and private keys. The private key is never transmitted via the network and then it is secure. The public key is sent via the network to the receiver. Through encryption, the sender encrypts the plaintext utilizing the public key of the receiver and sends the resultant cipher text to the receiver utilizing the network. Even if the public key was known to the hacker, he cannot read the scrambled message because secret key was not recognized for him. Through decryption, the receiver will utilize the private key to decrypt the cipher text. Asymmetric algorithms were more complex to implement and utilize more resources than symmetric algorithms. Therefore, most of the applications of IoT utilize symmetric algorithms in order to provide security to the transmitted data (Rajesh, Paul, et al, 2019). Further, they are simple to execute, utilize less resources with low overhead and are secure as long as the key is save secret (Khan & Salah, 2018).

With massive use of IoT devices a security issue was raised regarding security of transmitted data. One of the main requirements for an effective security protocol in IoT devices was that it must be lightweight with regarding processing and storage capabilities. The processing time taken must be at minimal range for better implementation. Also, the security algorithm demanded to be less complex with minimal overhead. Because of these reasons several protocols utilized with normal computer networks didn’t give good performance in IoT devices and are not preferred (Rajesh, et al, 2019).

2.3.1 Types of IOT Encryption

Latest advancements in wireless technology have generated an exponential increasing in the number of connected devices leading to revolution in the internet of things (IoT).

Big amounts of data are attained, handled and transmitted via the network by these embedded devices. Security of the transmitted data was a major area of concern in IoT networks. Numerous encryption algorithms have been proposed recently to ensure security of transmitted data through the IoT network, such as:

- Tiny encryption algorithm (TEA): which is the most attractive among all, due to its lower memory utilization and ease of implementation on both hardware and software scales (Rajesh,et al , 2019).
- Secure IoT (SIT): which has a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of festal and a uniform substitution-permutation network (Usman, Ahmed, et al, 2017).

2.4 DNA Cryptography

The domain of biology and cryptography have begun integrated to work together. DNA computing permits a new method for cryptography. The nucleotide bases own the ability for generating self-assembly structures which have perfect means of performing computations. Recently, many DNA computing methodologies are adopted in key generation, encryption, steganography and cryptanalysis, from the cryptographic point of view, DNA is fully powerful (Tornea, 2013).

DNA encryption preferred instead of digital encryption because most of the cryptographic techniques have been cracked at least partially, if not entirely or might likely to be a cracked in the future by the new computers generation. So, threats raise exponentially with technology development, the data communication and storage have

become defenseless more and more. The major portion of breaking any encryption algorithm is brute force attacks (Vijayakumar, et al, 2011).

Sharma et al. explained how can cracking the Simplified DES (SDES) technique at little cost and in an acceptable time (Shamra, Bhupendra, et al, 2012). While Bhatejaand Kumar present that with the support of genetic algorithms and without the key utilizing elitism with a novel fitness task he can break the Vigenere cypher (Bhateja & Kumar, 2014). Other more, about key generation issue, any key is generated in the format of binary code set the exponential power to be two, while the DNA code exponential power is 4, creating a single bit key eight times powerful. The randomness and complexity of DNA structure attached an additional layer of security by the cryptography mean, DNA biological capability in high data capacity and parallel processing also added. Upon that, the concept of joining DNA in the domain of cryptography has been defined as possible algorithms that get forward a new hope for acquiring more robust algorithms **(**El-Moursy, et al, 2018).

2.4.1 DNA Technologies

Different DNA technologies have been created and adopted to improved DNA computing in the security domain such as:

- Polymerase Chain Reaction: PCR is significant in DNA computing as it is the mechanism which utilized to elicited the obstacles solution. moreover, it is a prescription to expand a pattern of DNA through multiple orders of size and primers. From a cryptographic perspective, PCR may be useful as it needs two primers to achieve the amplification procedures. For an opponent, it should be extremely

complex to amplify the message encoded series with PCR without these right primers selected from about 21023 types of sequences.

- DNA Fragment Assembly: related to the aligning and integrating portions of DNA tape to retrieve the original sequence. The technology is utilized in the DNA tape system and cannot realize all genomes at a time. There are many other DNA methodology as Gel electrophoresis that utilized to break mixed DNA portions and DNA chip technology, a technology used for gene expression and DNA profiling, in this research we just focus on technologies which could be adopted in cryptography (El-Moursy, et al ,2018).

2.4.2 DNA Limitations and Challenges

DNA characteristics re-appointed for various sciences and cryptographic objectives. Biological difficulties and computing complexity present two-fold security protection and make it complicated to penetrate. Therefore, a development in cryptography is required not to negate the tradition algorithms but to make it applicable to recent technologies. (Grati & Gross, 2019).

The more improvements in information technology the more obstacles it will attain by the mean of integrity, insurance, and security, as all of the presently utilized cryptographic schemes are depending on computational difficulty proposition which cannot keep up with the more progress on the information technology improvement environment. Cryptography challenges based on multiple operators, one of them depend on existing method restrictions and another is on the cryptanalysis effort to them (Vijayakumar, et al, 2011).

The study of DNA cryptography still at its foremost phase and several aspects still uncovered. Furthermore, it matched with some obstacles the same matched to DNA computing studies (Thachuk & Liu, 2019). Which can be outlined as follows:

1. Theoretical problems: a robust tool for keys generating in encryption algorithms must utilize the complicated mathematical operations, DNA cryptography does not have any ripe mathematical background to assist Shannon`s related theory (Thachuk & Liu, 2019).

2. Implementation difficulty much comprehensive material and much biological and lab experience must be implemented to generate a DNA-based cryptosystem; this could be one of the causes why just little examples of effective DNA cryptography technique were presented. A constant foundation among the biological construction and computer science are necessary to be the standard to improve efficient and constant algorithms for DNA computing. Furthermore, its low computing velocity and supposed solution analysis in a molecular computer is harder than the digital one. Thus, there is a necessity to produce a bridge between actual and advanced technologies and to open the chance for hybrid cryptographic mechanisms that provide higher confidentiality and stronger authentication methods (El-Moursy, 2018).

2.5 Related work

Al-Husainy and others ,2018, have developed in their paper a new lightweight cryptographic (LWC) algorithm to improve application security, their study proposed block cipher light weight image cryptosystem, which used digital file of any type (text, image, audio and video) as a seed in order to generating secret key. Their method works on a 32-bit block size and a key of any length and type of digital data. It created a 16×16

exchange table of bytes, thus, a key space of 2048 was utilized, in addition part of the key was embedded into the encrypted image (Al-Husainy & others, 2018).

This study tries to follow their research methodology in general, based on the results of the proposed algorithm (LWC), which made a clear improvement in the level of security and the necessary time for the encryption and decryption process. instead of (LWC), this study will employee the DNA method in the process of key generation, choosing DNA algorithm regarding to its strength in encryption, also, random selection of the key generation is determining, because it is strong and hard to reveal (providing high randomness cryptographic key). DNA encryption and decryption process will have adopted as LWC, with the difference in some operations, where this study will use (DNA) key instead of four (LWC) keys extracted from prepared table.

Pasupuleti and Varma, 2020, showed in their study that IoT devices have fixed memory, storage, and bandwidth, which makes it complex for them to handle large and complicated data. So, much of this data should be outsourced to the cloud. This outsourcing, generate privacy problems and permits for unauthorized access to the data. Ciphertext-policy attribute-based encryption (CP-ABE) schemes were the best solution for providing privacy and access control to the data in the cloud. So, CP-ABE schemes were not appropriate for lightweight IoT devices because they produced more computation overhead while implementing encryption and decryption operations. Their study proposed a lightweight CP-ABE scheme with a Walsh-Hadamard transform access structure for providing data privacy with access control in cloud-assisted IoT (Pasupuleti & Varma, 2020).

Marin, Pawlowski & Jara, 2015**,** were explained in their study that (IOT)The Internet of Things is merging information systems, places, users and billions of constrained devices into one global network. This network needs a secure and private method of communications. The building blocks of the Internet of Things are devices manufactured via different producers and are designed to fulfil many needs. There would be no common hardware platform which could be used in every scenario. In such a heterogeneous environment, there is a strong need for the optimization of interoperable security. They present optimized elliptic curve Cryptography algorithms, which address the security issues in the heterogeneous IoT networks. They have combined cryptographic algorithms for the NXP/Jennic 5148- and MSP430-based IoT devices and used them to created new key negotiation protocol (Marin, Pawlowski & Jara, 2015).

Mujumdar and others, 2015, proposed in their study a method that utilizing integrated technologies of cryptography and steganography via following the notation of genetic engineering depend on the DNA. This method going to support message security, which is the major concern in data transmission security. Their technique proposed a long and robust key, which was, used for encryption with a strong new algorithm of encryption, producing of DNA sequence, and a novel method to hidden the encrypted DNA sequence to a cover image (Majumdar, et al, 2015).

Najaftorkaman and Kazazi, 2015**,** in their paper were primarily focused on new cryptography, which depends on quantum and DNA cryptography. Then, a novel algorithm to encrypt data via utilizing DNA-based cryptography was discussed. In their study, DNA coding method was utilized to changed binary data to DNA strings. Then, the suggested

DNA cryptography algorithm's strength was evaluated depending on the features of DNA strands and possibility theories (Najaftorkaman & Kazazi, 2015).

Anwar and others, 2015, provided in their study another cryptography algorithm was suggested utilizing one-time pad scheme, Symmetric Key Exchange and DNA hybridization to decrease time complexity. XOR operation with OTP DNA sequence was utilized as an encryption method depend on DNA cryptography. Symmetric Key Exchange was introducing a secure key generation scheme. Their algorithm was very efficient in encrypting, transmitting, hiding and preventing sturdy attacks (Anwar, et al, 2015).

Akasaligar and Biradar, 2016**,** proposed in their paper a novel technique using Chao's theories and DNA encoding to supply the security for digital medical images. the input medical image was revamped into two DNA encoded matrices depend on intensity levels. the results proved that the proposed algorithm supports the security level, integrity, robustness and efficiency of digital medical image encryption. (Akkasaligar & Biradar, 2016).

Mousa, 2016**,** proposed DNA-Genetic Encryption Technique (D-GET) which make the technique more secure and less predictable. So, the technique, binaries any kind of digital data and changed it to DNA tape, encrypt, reshape, crossover, mutate and reshape. The important stages of D-GET were repeated three times or more. Results show that the suggested technique has multilayer protection stages against different attacks and a higher level of security based on the multi-stages and genetic operations (Mousa, 2016).

Barkha, 2016**,** was addressing cloud services utilization regarding to data security matters as the data set on the cloud services provider's servers. thus, such data security

techniques were The Bi-directional DNA Encryption Algorithm (BDEA), it's focused only on the ASCII character set, neglect the non-English user of the cloud computing. so, this study focused on supporting the BDEA to use with the Unicode characters (Barkha, 2016).

Kalsi and others,2018**,** have been introduced in their study firstly, a method with its implementation for key generation depend on the theory of natural selection utilizing Genetic Algorithm with Needleman-Wunch (NW) algorithm and then, a method for execution of encryption and decryption depend on DNA computing by utilizing biological procedures translation, Transcription, DNA Sequencing and Deep Learning (Kalsi, et al, 2018).

Tiwari and Kim, 2018, proposed a novel hybrid DNA-encoded ECC (Elliptic curve cryptography) scheme, which extends multi-level security. The DNA tape was chosen, and utilizing a sorting algorithm, a unique set of nucleotide sets was assigned. These were instantly converted to binary sequence and then encrypted utilizing the ECC; so, granting double-fold security. Algorithm analysis proved that DNA added with ECC could provide better security compared to ECC alone. Results showed good performance for upcoming **IoT** technologies which need a smaller but operative security system (Tiwari & Kim, 2018).

Aishwarya and Sreerangaraju, 2019**,** proposed a lightweight and secure compressive sensing of stream cypher depends on DNA encoding and decoding approach. Their method encrypts text and data produced by image sensors. it integrated the compressive sensing algorithm with DNA encoding and decoding based stream cypher to perform the secure compressive sensing. To attain the security, aim, the overhead must be minimal which is done through utilizing the stream cypher for creating the measurement matrix. The

proposed system was executed by using Verilog HDL and simulated by using Modalism 6.4 c and synthesized using Xilinx tools (Aishwarya & Sreerangaraju, 2019).

finally, Table [2.1] summarizes the related work based on DNA generated key related to IOT constraints devices encryption methods.

Table [2.1] : Summery of related work.

Authors	**Algorithm**	**Difference between our thesis and related study**
(Al-Husainy & others, 2018).	(LWC) algorithm 32-bit block size	They used digital file of any type as a seed in order to generating secret key, while we used DNA for key generation.
(Pasupuleti & Varma, 2020).	NXP/Jennic 5148- and MSP430-based IoT devices	Providing secure and private method of communications between IOT devices, while we provide method based DNA for key generation to provide complicated cryptography algorithm..
(Pasupuleti & Varma, 2020).	Cipher text -policy attribute-based encryption (CP-ABE) schemes	Gained best solution for providing privacy and access control to the data in the cloud utilizing IOT applications. While we used DNA for constraint devices.
(Aishwarya & Sreerangaraju, 2019)	DNA encoding and decoding approach executed by using Verilog HDL, simulated by using Modalism 6.4 c, and synthesized using Xilinx tools.	CP-ABE not appropriate for lightweight IoT devices because they produced more computation overhead while our proposed algorithm suitable for lightweight IoT.
(Tiwari & Kim, 2018)	hybrid DNA-encoded ECC (Elliptic curve cryptography	It is suitable and provide good performance for upcoming IoT technologies which need a smaller security system, which in somehow similar to our proposed method.
(Majumdar, et al, 2015)	DNA sequence	Support message security and providing hidden to the encrypted DNA tape image (suitable for IOT devices), its share our methodology in its main objective.

Chapter Three
Methodology and the Proposed Algorithm

3.1 Introduction

DNA cryptography is rapid and promising emerging domain in data security, so, in this thesis we provide new DNA-based encryption model. The DNA tape randomness nature was exploited to generate strong encryption and decryption key, which could be used application using the symmetric ciphering applications.

DNA has been adopted in this algorithm, due to its strength features such as: The strength of the encryption process, which is strong and difficult to hack, as it depends on high randomness, also, it is suitable for IOT constraint devices, in terms of RAM and CPU. In addition to the key generation process, that employs the DNA bar according to the sequence binary string representation.

3.2 Methodology

The algorithm presented in this thesis is a new DNA block cipher symmetric system, which include the next main operations:

- Select DNA tape for secret key generation.
- Divided source image that will be handled through encryption method each byte by each byte consequently; where each part of the picture will represent one byte, (Pool, Aqsa and mosque images were selected).
- Perform sequence of segmenting input DNA tape.
- Extract secret key from the DNA tape letters with one-byte size for each secret key.

- Performed substitution process using XOR operation between each image segment and DNA secret key.
- Perform transposition on the XOR operations results based on set of rules based on DNA tape.
- Continue performing the whole procedures until the end of DNA tape and when the image become completely encrypted.
- Measure PSNR for each image.
- Measure encryption time for each image.
- Measure key size for each method.
- Compare the constructed results for each three methods (DNA, DES AND AES)

These operations are performed in both, encryption and decryption, but they differ in their orders of executions.

3.3 Proposed Algorithm

The proposed encryption and decryption algorithm employed the DNA tape for in the secret key generation, the proposed algorithm is lightweight cryptosystem which was appropriate for IoT devices, so the main procedures had performed key generation, encryption process that depend in substitution and transposition as two main phases, with sequence orders for decryption procedures from the last step until the first one in the sequence to retrieve the original source image.

3.3.1 Encryption algorithm:

Encryption procedures will start with key generation using DNA tape as input seed, then the substitution process will be implemented, and next the transposition operation will execute sequentially. Bellow set of definition to be used in the proposed algorithm as follows:

Definitions:

- **SImage:** the source image or the input image to be encrypted, it is bitmap color image.
- **EImage:** the encrypted image generated by proposed cryptographic algorithm.
- **Skey:** the generated secret key, produced randomly from DNA tape, which will be used for encryption and decryption process.
- **XOR**: the simple XOR cipher is a kind of collective cipher, an encryption algorithm, where a string of text could be encrypted by performing the bitwise XOR operator to each character utilizing a given key. XOR consider as a binary operation, it stands for "exclusive or", that is mean that the resulting bit evaluates to one if just exactly one of the bits is specified. This is its function stream: a | b | a ^ b --|---|------ 0 | 0 | 0 0 | 1 | 1 1 | 0 | 1 1 | 1 | 0. This operation is executed between every two corresponding bits of a number XOR which permit easily encrypt and decrypt a string, the other logic operations don't. XOR cipher does not leak information about the original plaintext. XOR is a significant criterion in the design of lightweight cryptographic primitives, generally to estimate the effectiveness of the diffusion layer within a block cipher. (Sarkar& Sim, 2016).

The proposed algorithm in this thesis is lightweight cryptosystem for Image Encryption Using DNA is block cipher that fit IOT constraint devices, which it performs two main operations on the bytes of source image Simage, they called substitution, and transposition as shown in next flowchart figure [3.1]. Described below:

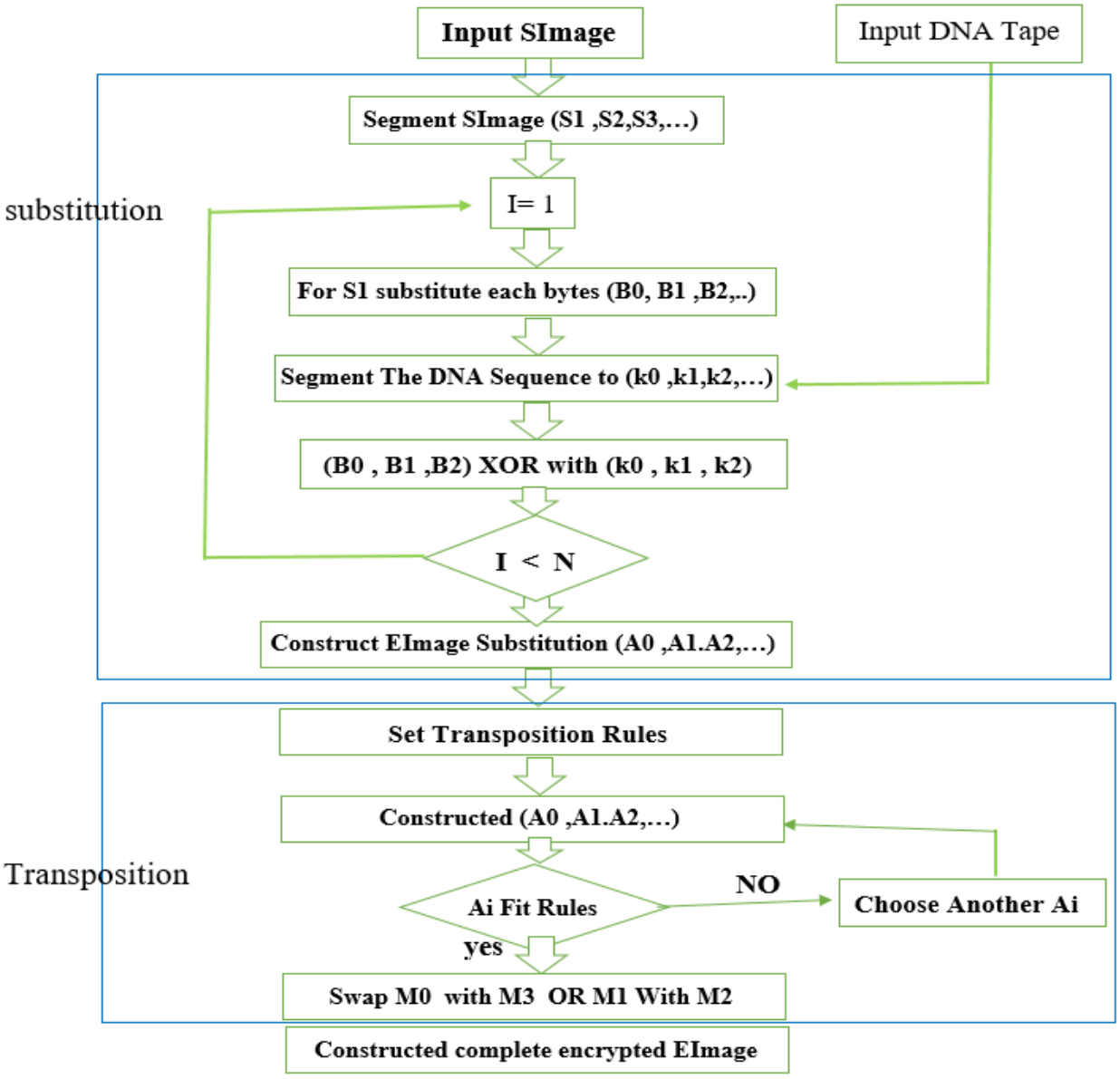


Figure [3.1]: Flowchart summarizing the encryption process of based on DNA

Where:

S0, S1, S2, represent each segment constructed from source image.

B0, B1, B2, represent size of each segment where its size is 1 byte for each segment.

K0, K1, K2, represent DNA generated key

A0. A1, A2 represent the constructed parts for EImage after performing substitution and transposition.

M0, M1, M2, M3: Represent two bits.

N: Length OF Image in Bytes

Key generation:

The key generation is based on DNA series, where DNA strand series has various orientations, everyone is different from the other, like, TCCGAATGC is distinct from ATCGATCGC. This is one attribute, another main attribute is the reverse complement, which is done in two phase:

The first: reverse the order of the DNA strand bases. The second: take the complements of the reversed strands (the complement of the base A is T and C is G and vice versa). DNA tape {A, C, G, and T} is presented into binary code utilizing the simplest coding pattern of four digits (0, 1, 2, 3,) consequently. "every digit is given into 2-bit, pattern will be: 0 as A→00, 1 as C→01, 2 as G→10, and3 as T→11, The DNA tape ACGT has different numeric encoding format, like (0123 for ACGT, 0132 for ACTG, 0213 for AGCT, etc.)", and consequently every encoding form will have another binary representation (Hussain & Al-Bahadili, 2016).

In our methodology, instead of using digital file (text, image, video, audio) as input image (source image) as many encryption algorithms done, we will use DNA tape as input source in order to generate strong and completely random key, figure [3.2].

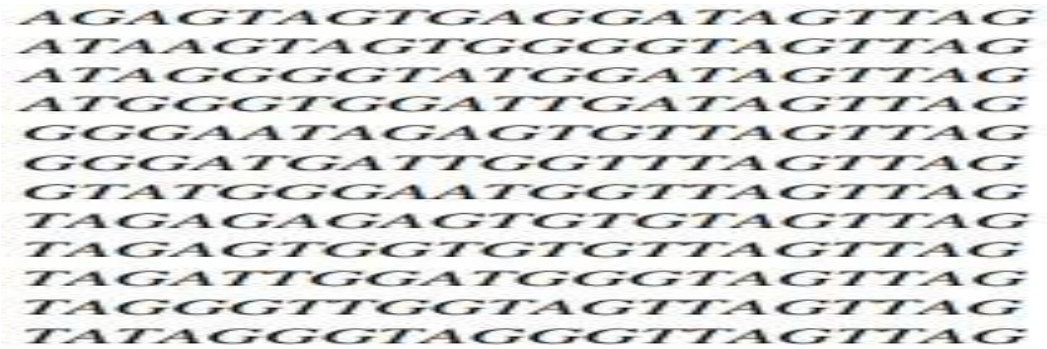


Figure [3.2]: Set of unique DNA letters.

In the proposed algorithm in this thesis, DNA tape is taken within any size, where it contains a series of letters, and each four consecutive letters represent a series of randomly arranged bits, as each letter representing two bits as it showed in table [3.1]. the DNA key generation procedures were described as follows:

Table [3.1]: DNA letters Binary representation

Letter	**Binary representation**
A	00
T	01
C	10
G	11

a) Use DNA sequence as input for key generation

b) Execute sequence of step that include segmenting the input DNA tape into segments from each four DNA letters (A, C, G, T)

c) Construct 1 bytes from each four DNA letters to form encryption (as we need more than on key).

Each one byte is made of four letters, which represent 8 bits (one byte), where it constitutes the encryption Skey as in figure [3.3]. Then the complete DNA will be generated completely as it appears in Figure [3.4].

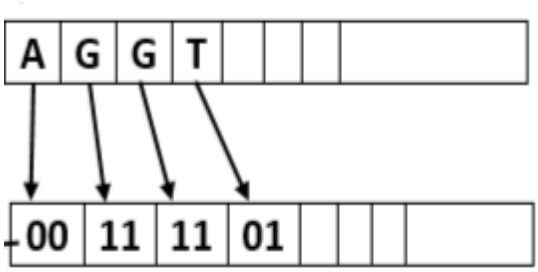


Figure [3.3]: DNA key bits representation

K0: 00111101	**K1:00011101**	**K2:11010100**	**K3:11001010**

Figure [3.4]: key generation example

The tape is taken within any size, the main encryption procedures related to DNA algorithms depend on two phases, substitution and transposition operations presented below.

Substitution:

In substitution phase each one DNA byte is made of four letters, which represent 8 bits (one byte), where it constitutes the encryption Skey as presented above in figure [3.3]. The generated Skye will be used in XOR operations with each image segment of size one byte. each constructed encryption key with size 1 byte with one image segments with size on

byte and perform encryption on the whole image segments until finished the segments. As shown in figure [3.5], the substitution process described below:

- XOR will be executed between K0 of DNA SKey and Byte 0 of Simage, to constructed partial A1 of Eimage, and the process continues till the last byte of image.

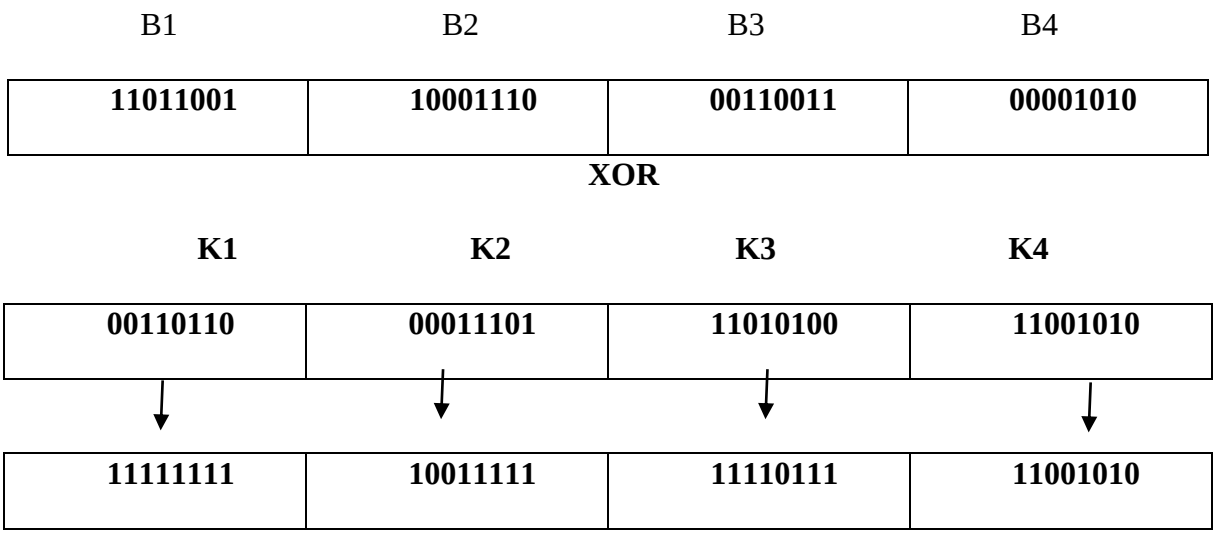


figure [3.5]: XOR implementation results

Transposition:

After the completion of the substitution phase, the transposition will be executed on the results of the XOR process between the encryption keys and the image bytes, which produced A1, An bytes as we showed in substitution phase. As we perform the transposition process in order to further complicate the encryption algorithm.

In the transposition process, we swap between the bits that represent the index number zero with the bits in the index number two, and swap the bits in the index number one

with the bits in the index number three, according to specified rules that were assumed as follows:

- transposition will be executed on the results of the substitution operations A1, An segments of EImage.
- Set of swapping rules between bits of Ai according which allow swapping or prevent swapping, as table [3.2] showed.

Table [3.2]: Transposition rules

index letter [M0or M2]	**index letter [M0 or M2]**	**operation**
A	A	Swap
A	C	Swap
C	C	Swap
T	T	Swap
T	G	Swap
G	G	Swap
T	A	Don’t Swap
C	G	Don’t Swap

- swap between the bits that represent the index number zero with the bits in the index number three if they match the above rules in table[3.2].
- swap the bits in the index number one with the bits in the index number three.

As example of the trasnposition rules is illsutrated in figure [3.6], we can see in the next example , M1 will be replaced with M2, because It conforms to the rules that have been assumed, While the M0 was not replaced with M3 because it did not conform to the rules that were assumed, as displayed.

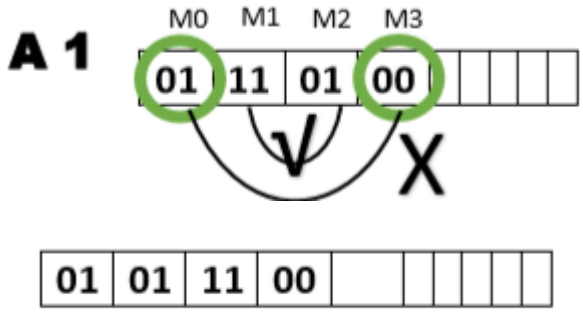


Figure [3.6] : transposition procedures

- Continue the transposition until the DNA key file is completed and the whole image encrypted.

3.3.2 Decryption Algorithm:

The Decryption process begins in a reverse way, as it begins with transposition then substitution, the Decryption process starts from the last byte in the image, in which we finished the transposition process, returning the swapped bits to its original position, before making the swapping, and we start from the last byte gradually until we reach the first byte. When the transposition ends at the first index, we take the byte for the last four letters, then we execute the XOR with the resulted byte from the transposition process, and we restore the original part of the previously encoded image

3.4 Data Set

FASTA DNA dataset: In biological computing, dealing with DNA tape data is common domain. DNA tape data frequently are included in a file structure called "Fasta" format. Fasta format is clearly a single line prefixed by the utmost than symbol, which contains annotations and another line that involves the sequence:

ATGTTTCGCATCACCAACATTGAGTTTCTTCCCGAATACCGACAAAAGG

The file may contain one or multiple DNA sequences. There are many of other formats, but Fasta is the most widespread (Albalawi, Chahid, et al, 2018).

3. 5 Performance Evaluation:

The proposed algorithm in this thesis is evaluated and assessed regarding the encryption and decryption time, size of key, PSNR, and compare the results with DES and AES.

Chapter Four
Experiments Design and Evaluation

4.1. Introduction

The proposed Lightweight Cryptosystem for Image Encryption Using DNA tape as presented presented and explained in Chapter Three, is implemented by using Visual Basic version 2019 which is a third-generation event-driven programming language from Microsoft implemented on System Processor : Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 3600 Mhz System Total Memory : 16 GB, as it enables the rapid application development of graphical user interface applications and , access to dataset (FASTA DNA dataset) using Data Access Objects, and creation of Active programming language, also we have connected it with visual studio in order to gain analysis evaluation. The implementation stages, concentrate on obtaining and comparing the results, are presented in this chapter. Besides the proposed Lightweight Cryptosystem for Image Encryption Using DNA tape, other encryption algorithms like AES and DES were presented and examined in this chapter; they were evaluated and compared with the proposed DNA encryption algorithm based on DNA tape. The performance evaluation compared, key size, encryption time for performance rating and compares outcomes.

4.2. Parameter and evaluation metrics setting

In this section we are introducing the evaluation metrics and lists some statistics about the DNA based algorithm, and other properties and compare it with other algorithms such as AES and DES. Metrics are listed below:

1. key type impact on the encrypted image

2. key size used in encryption algorithm (Determine (x) as key size and Generate (Key x) depending on desired key size)

3. PSNR comparison for proposed algorithm, AES and DES algorithm in order to prove the efficiency of the DNA algorithm among traditional algorithms.

4. Encryption execution time comparison (compute execution time for each algorithm).

4.3. Experiments design and setup

In order to investigate the proposed algorithm impact and effectiveness, that have been described in the methodology chapter, different images were presented and passed through the main cryptography procedures encryption and decryption by using several types of files as a key for each cases, so we presented three images of various size, color and contents as display on figure [4.1] where they called as follow:

a- POOL jpg image with (424*283) original resolution.

b- PETRA jpg image with (256* 256) original resolution.

c- AQSA jpg image with (381*254) original resolution.

They were presented as examples to examined and then evaluated in order to demonstrated the acquired results, and held comparison with other algorithms to support proposed algorithm effectiveness within this thesis.

a) Pool b) Petra c) Aqsa

Figure 4.1: Images Examples

proposed system have been implemented coding in VP.NET where it's a multi-paradigm, object-oriented programming language, implemented on the NET Framework. here we had started created our program for initiated the first implementation procedures:

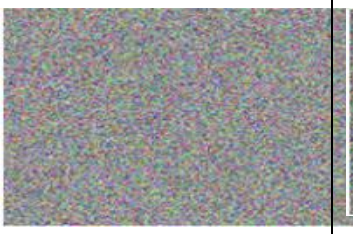
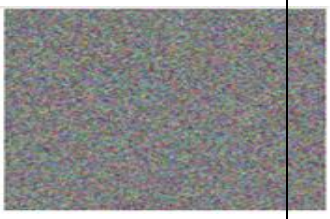
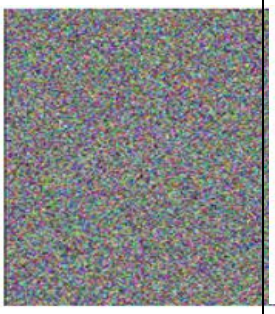
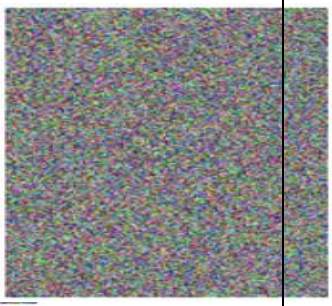
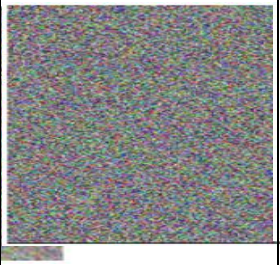
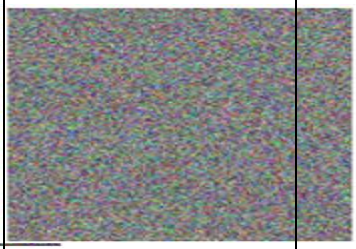
4.4. Performance and Evaluation of the proposed Algorithm.

In order to evaluate the performance effect for the proposed algorithm, several images were encrypted with proposed DNA based encryption algorithm, AES and DES methods under the same implementation condition, and then the results were evaluated, measured and compared in order to prove accuracy rate for DNA key generation algorithm.

4.4.1 Pixel's intensity distribution

three selected files images were encrypted, Table [4.1] shows the original selected images and the output encrypted images after processing by encryption procedures related to the DNA, DES and AES techniques

Table [4.1]: images pixels' intensity distribution produced by DNA, DES and AES algorithm.

Image	DNA	DES	AES
			
			
			

The selected encrypted images files are clearly displayed encryption effect similarities for each image in table [4.1], they reflect the influence of the encryption process by noticing the pixel's intensity distribution.

Where those distributions indicate that the pixel's distribution for the encrypted image by proposed DNA based encryption algorithm displayed improvement and gets better and comparable with AES and DES, where the image become more natural and clear as it

clears in AQSA image. As it is worth noting that the encryption process was done for the three algorithms with the same key type (Text) for the three encrypted images.

4.4.2 PSNR comparison for the encryption methods

Peak Signal-to-Noise Ratio defined as the ratio between the original image and the encrypted image. where it calculated in decibels. when PSNR is higher, the nearer the encrypted image is to the original. in common, a higher PSNR value must correlate to a higher quality image. For best encryption scheme the PSNR must be as low as possible.

To calculate the PSNR, the block first computes the mean-squared error by utilizing the next equation 1:

$$MSE = \sum_{M\ .\ N} \frac{[I_1(m.n) - I_2(m.n)]^2}{M * N} \quad (1)$$

where M and N represented the number of rows and columns in the input images. next, the PSNR computed using the following equation 2 (Nasution, & Wibisono, 2020).

$$PSNR = 10\ \log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

As table [4.2] display the values for PSNR due implementing the with the proposed DNA based encryption algorithm compared with DES and AES encryption methods under the same environment and condition. The results show that the PSNR value for proposed DNA based encryption algorithm. on the three images is considerable comparable to the DES and AES algorithms. Moreover, figure [4. 2], shows that the PSNR value for PETRA and AQSA images of DNA based encryption algorithm has proportion of distortion close enough to the DES and AES.

Table [4.2]: PSNR comparison utilizing DNA, DES and AES

Image	DNA	DES	AES
POOL	8.528	8.369	8.355
PETRA	7.786	7.648	7.667
AQSA	8.687	8.594	8.587

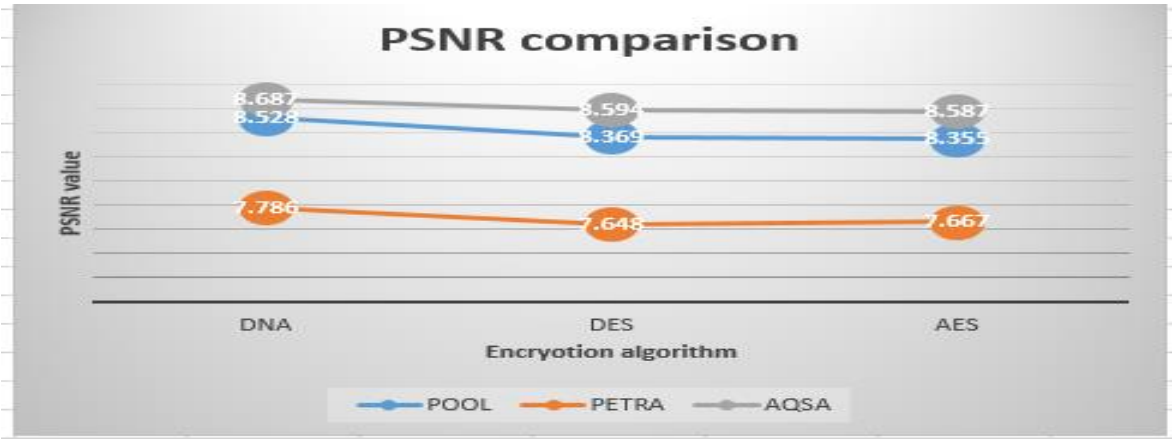


Figure [4.2]: PSNR values

4.4.3 Encryption Time for each image through the three methods:

Time has usually played a significant role in different communication application and its related encryption algorithms especially for IoT devices and its application. Information could become useless after a pointed time, sensitive data might not be released before a specific time, or it may need to enable access to data for just a limited period. In our results analysis, the Time for executed specific encryption algorithm has major role in specifying the impact of time in algorithm performance.

As table [4.3], showed clearly that DNA algorithm has the shortest encryption time among all the three types of images under consideration within this study. As it showed that PETRA image has record the lowest time for encryption with value 62.5 MSEC under DNA encryption algorithm implementation, while the PETRA image has the highest encryption time with value 2625 MSc under DES encryption method. DNA encryption algorithm has counted a range of time execution from 1 to 2.6 times DNA was faster than AES and DES algorithms as figure [4.3] can display

Table [4.3]: Encryption time comparison in MSEC

Image	**DNA**	**DES**	**AES**
POOL	203.125	2625	2609.375
PETRA	62.5	1421.85	1421.875
AQSA	109.375	2093.75	2125

.

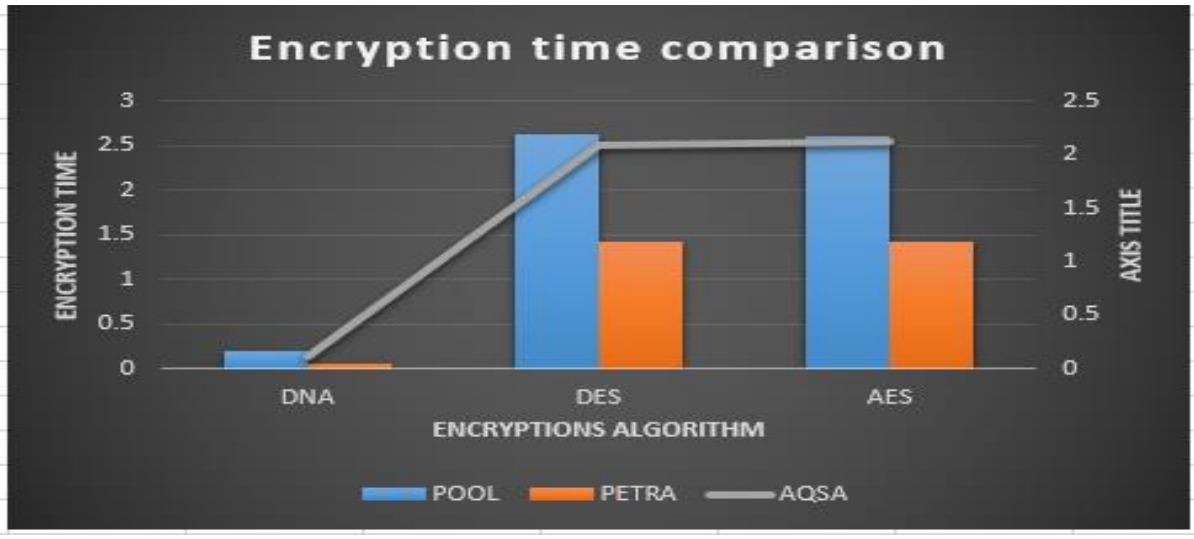


Figure [4.3]: Encryption Time Representation in seconds

4.3.4 The size of the key used in the encryption algorithm

Within this study, The Encryption key for the proposed algorithm was generated from DNA tape as we explained previously, the key type was defined as text (TTCCGTTTGTCGCGATAAAATA) as it sequences of letters, while the total number of DNA letters that have been used in key generation were 1162308 letters during the encryption process.

Table [4.4]: Key size effect on DNA, DES and AES

Image	DNA	DES	AES
POOL	8 bits	8 bits	32 bits
PETRA	8 bits	8 bits	32 bits
AQSA	8 bits	8 bits	32 bits

The key size for the proposed DNA based algorithm for encryption process was small with 8 bits' size (block size 8 bits) as table [4.4] display. this because we depend during the

encryption procedure for handling input image just in dividing it into small segments (just one byte), and we handled each image byte with on secret DNA key generated from four letters by using binary representation each time until the end of the DNA tape. We selected short key size because our proposed algorithm related to IOT constraint devices, which need high speed processing without any complicated computations.

4.5 Discussion

In this thesis , the lightweight encryption algorithm have been proposed depend on the power of the DNA sequences in order to enable secure IoT constrained devices communication, as those devices require quick processing in encryption method because of their limited CPU and small memory. Three algorithms have been constructed and compared (DNA, DES and AES) as they were implemented under the same environment conditions, and three images (pool, Petra and Aqsa) were processed within measurement criteria. Verification criteria and their results demonstrate and proved the effectiveness of the proposed DNA based algorithm regarding lowest encryption time, where it also achieved higher pixel's intensity distribution in AQSA image where it becomes more natural and clear, due to PSNR evaluation metric , the results proved that the highest PSNR value was for AQSA image with 8.687 PSNR value through executing the proposed DNA based algorithm, also due to Encryption time comparison in (MSEC), the lowest time for encryption PETRA image with value 62.5 MSEC under DNA encryption condition.

Chapter Five
Conclusion and Future Work

5.1. Conclusion

A DNA algorithm has been proposed and adopted in this thesis, due to its strength features such as: strength of the encryption process, which is strong and difficult to hack, as it depends on high randomness, also, it is suitable for IOT constraint devices, in terms of small RAM and limited CPU size. FASTA data set have been used, the main DNA algorithms was implemented in different images, also implemented other DES and AES encryption algorithms, the main results proved the effectiveness of the DNA algorithm, as it achieved the shortest encryption time with value 62.5 MSEC for the PETRA image compared to other algorithms, and it achieved Peak Signal-to-Noise Ratio value about 08.687 for the AQSA image.

It's clear that the performance of the proposed DNA based encryption algorithm shows comparable outcomes compared to DES and AES, In this thesis, we tried to answer two questions, the first question has been proved that DNA cryptographic technology surely increased the level of security due to the randomness nature of DNA key that is utilized during encryption made it hard to break. Also, the proposed DNA algorithm achieved the lowest encryption time needed that matches the IoT constrained devices computational capabilities. While the most notable performance aspects differences between the proposed DNA algorithm and other traditional encryption methods showed that the DNA algorithm is preferable, and more effective with respect to the key size and proportion of distortion for IoT devices, as it fit small RAM and limited CPU.

5.2. Future Work

Due to the effectiveness of DNA in coding processes, which began to appear in a varied and sophisticated way, this study recommends expanding the use of DNA in smart applications encoding due to the sensitivity of the private information present in them. And due to the large number of social media applications that are widely circulated on smartphones and personal computers.

As a future work, we will study more complex methods for dividing images, and measure their effectiveness in raising the efficiency and speed of the encoding process and study the effects of key size key size in the encryption process in the future.

References

Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. **International Journal on Computer Science and Engineering, 4(5), 877.**

Aishwarya, R. U., & Sreerangaraju, M. N. (2019). **Enhanced Security using DNA Cryptography**.

Akkasaligar, P. T., & Biradar, S. (2016, December). **Secure medical image encryption based on intensity level using Chao's theory and DNA cryptography**. In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-6). IEEE.

Albalawi, F., Chahid, A., Guo, X., Albaradei, S., Magana-Mora, A., Jankovic, B. R., ... & Bajic, V. B. (2018). **Data for: Poly (A) Dataset for PAS sequences and pseudo-PAS sequences Classification** (fasta format).

Al-Farraji, S. M. (2020). **DNA Cryptographic System Utilizing Random Permutation**.

Al-gohany, N. A., & Almotairi, S. (2019). Comparative Study of Database Security in Cloud Computing Using AES and DES Encryption Algorithms. **Journal of Information Security and Cybercrimes Research (JISCR), 2(1).**

Al-Husainy.M, Ali.M & Masadeh.S, (2018). Lightweight cryptosystem for image encryption using auto-generated key. **Journal of Engineering and Applied Sciences 13(17).**

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. **International Journal of Scientific and Research Publications, 9(3).**

Anwar, T., Kumar, A., & Paul, S. (2015). DNA cryptography based on symmetric key exchange. **International Journal of Engineering and Technology, 7(3), 938-950.**

Ashby, M. P. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. **European Journal on Criminal Policy and Research, 23(3), 441-459.**

Barkha, P. (2016, January). **Implementation of DNA cryptography in cloud computing and using socket programming**. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

El-Moursy, A. E., Elmogy, M., & Atwan, A. (2018) **DNA-based cryptography: motivation, progress**, challenges, and future.

Grati, F. R., & Gross, S. J. (2019). **Noninvasive screening by cell**- free DNA for 22q11. 2 deletion: Benefits, limitations, and challenges. Prenatal Diagnosis, 39(2), 70-80.

Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). **A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm** SHA-2. Nonlinear Dynamics, 83(3), 1123-1136.

Hussain, S. M., & Al-Bahadili, H. (2016, July). **A DNA-Based Cryptographic Key Generation Algorithm**. In Proceedings of the International Conference on Security and Management (SAM'16).

Kalsi, S., Kaur, H., & Chang, V. (2018). DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation. **Journal of medical systems, 42(1), 17.**

Khan, M. A., & Salah, K. (2018). **IoT security: Review, blockchain solutions**, and open challenges. Future Generation Computer Systems, 82, 395-411.

klUsman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). **SIT: a lightweight encryption algorithm for secure internet of things**. arXiv preprint arXiv:1704.08688.

Majumdar, A., Podder, T., Majumder, A., Kar, N., & Sharma, M. (2015). **DNA-based cryptographic approach toward information security**. In Intelligent Computing, Communication and Devices (pp. 209-219). Springer, New Delhi.

Marin, L., Pawlowski, M. P., & Jara, A. (2015). **Optimized ECC implementation for secure communication between heterogeneous IoT devices**. Sensors, 15(9), 21478-21499.

Mousa, H. M. (2016). DNA-genetic encryption technique. **International journal of computer network and Information Security, 8(7), 1.**

Najaftorkaman, M., & Kazazi, N. (2015). A method to encrypt information with DNA-based cryptography. **International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4(3), 417426.**

Nasution, A. S., & Wibisono, G. (2020, April). A comparison of joint reversible data hiding methods in encrypted remote sensing satellite images. **Journal of Physics: Conference Series (Vol. 1528, No. 1, p. 012038).** IOP Publishing.

Organick, L., Ang, S. D., Chen, Y. J., Lopez, R., Yekhanin, S., Makarychev, K., ... & Takahashi, C. N. (2018). **Random access in large-scale DNA data storage**. Nature biotechnology, 36(3), 242.

Pasupuleti, S. K., & Varma, D. (2020). **Lightweight ciphertext-policy attribute-based encryption scheme for data privacy and security in cloud-assisted IoT**. In Real-Time Data Analytics for Large Scale Sensor Data (pp. 97-114). Academic Press.g

Rahaman, Z., Corraya, A. D., Sumi, M. A., & Bahar, A. N. (2020). **A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix**. arXiv preprint arXiv:2005.00157.

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.

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.

Ratnadewi, R. P., Adhie, Y. H., Ahmar, A. S., & Setiawan, M. I. (2018, January). **Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). In J. Phys**. Conf. Ser (Vol. 954, No. 1, p. 12009).

Samie, F., Tsoutsouras, V., Bauer, L., Xydis, S., Soudris, D., & Henkel, J. (2016, December). **Computation offloading and resource allocation for low-power IoT edge devices. In 2016 IEEE 3rd World Forum on Internet of Things** (WF-IoT) (pp. 7-12). IEEE.

Sarkar, S., & Sim, S. M. (2016, April). **A deeper understanding of the XOR count distribution in the context of lightweight cryptography**. In International Conference on Cryptology in Africa (pp. 167-182). Springer, Cham.

Sehgal, A., Perelman, V., Kuryla, S., & Schonwalder, J. (2012). **Management of resource constrained devices in the internet of things**. IEEE Communications Magazine, 50(12), 144-149.

Thachuk, C., & Liu, Y. (Eds.). (2019). **DNA Computing and Molecular Programming: 25th International Conference, DNA 25**, Seattle, WA, USA, August 5–9, 2019, Proceedings (Vol. 11648). Springer.

Tiwari, H. D., & Kim, J. H. (2018). **Novel Method for DNA**-Based Elliptic Curve Cryptography for IoT

Tornea, O. (2013). **Contributions to DNA cryptography: applications to text and image secure transmission (Doctoral dissertation).**

Vermesan, O., & Friess, P. (Eds.). (2014**). Internet of things-from research and innovation to market deployment (Vol. 29)**. Aalborg: River publishers.

Vijayakumar, A., & Vijayan, S. S. (2011). **Application of information technology in libraries: an overview**. Library Progress (International), 31(2), 159-168.

Wen, W., Wei, K., Zhang, Y., Fang, Y., & Li, M. (2020). **Colour light field image encryption based on DNA sequences and chaotic systems**. Nonlinear Dynamics, 99(2), 1587-1600.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2016, January). **Security analysis on consumer and industrial IoT devices**. In 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC) (pp. 519-524). IEEE.