T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Information Technologies

DESIGN AND EVALUATION OF IMAGE ENCRYPTION ALGORITHM BASED ON DNA COMPUTING AND S-BOX OF AES

Ali ABDULRIDHA SALMAN

Master of Science

Supervisor

Asst.Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2021

DESIGN AND EVALUATION OF IMAGE ENCRYPTION ALGORITHM BASED ON DNA COMPUTING AND S-BOX OF AES

by

Ali Abdulridha Salman

Information Technologies

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ali Abdulridha Salman

Signature

ACKNOWLEDGEMENTS

I might want to thank my administrators: Asst.Prof. Dr. ABDULLAHI ABDU IBRAHIM Please let me express my profound feeling of appreciation and gratefulness to both of you for the information: direction and unrestricted help you have given me. I want you to enjoy all that life has to offer and further achievement and accomplishments throughout your life.

ABSTRACT

DESIGN AND EVALUATION OF IMAGE ENCRYPTION ALGORITHM BASED ON DNA COMPUTING AND S-BOX OF AES

Ali Abdulridha Salman,

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst.Prof. Dr. Abdullahi Abdu IBRAHIM

Date: 2021

Pages: 81

Traditional cryptographic schemes are founded on strong theoretical and mathematical concepts. It is thus crucial to establish an important understanding that DNA encryption does not only negate tradition, but also develop further connections between current and new technologies. The proposed Advanced Encryption Standard (AES) architecture for DNA Sequence is introduced and implemented. With all its features (data, algorithms and functions), the proposed algorithm is being implemented with the DNA sequence rather than bits in column steps. The technology proposed shows the possibility to create such a complex DNA sequence system in a method to make it a suitable contestant for biological use or on DNA computers. We have created three secret keys to prevent plain-text attacks. (1) The main key for the AES algorithm is the principal key. (2) The key is the DNA base with the number of key odds and DNA Rule 1 is named. (3) key indicates the number of binding possibilities between the helical DNA structures which increase the key length. This is done to hit a higher degree of security, and DNA Rule 2 is named. MATLAB 2016b is used to implement and assess the proposed algorithm. The findings demonstrated improved protection against brute attacks and required more time to crack compared to other techniques. Security checks, performance analysis and comparison of other methods suggest a higher security and complexity of the proposed algorithm. For images encryption-based applications, the proposed algorithm is safe and efficient. The standard images were used for testing and evaluating the algorithm proposed.

Keywords: DNA sequence; key generation; encryption; AES Algorithm; S-box

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

AES : Advanced Encryption Standard

DNA : Deoxyribonucleic Acid

DSA : Digital Signature Algorithm

NPCR : Number of Pixel Change Rate

S-Box : Substitution-Box

UACI : Unified Average Changing Intensity

1. INTRODUCTION

With the advent of the Internet, the computer network, the computer scenario entered the landmark age. The internet has become all-embracing, faster and easier for anyone on earth to handle. Social networking helps people of all ages and communities in the entire world to connect with sites like Facebook, Twitter, Linked-In, YouTube, Blogs and wikis. The current information era provides information to individuals, corporations and countries and can be obtained at anytime, anywhere. information on request. The global economy is influenced by the Internet and without e-mail or social networking it is difficult to imagine a day.

In science and technology, data storage and transmission from one device to another are essential problems and are often linked to risk. The data accessible in the computer network or cloud facilitates practices such as unauthorized access, unlawful use, intrusion and modification of transmitted and stored data. It is more vulnerable than if paper and cabinet security contain the same information. Intruders and hackers can publish and conceal the confirmation of their unauthorized activities without touching a paper. As the availability of information and data sharing often poses considerable danger, ISOs must concentrate their attention on mitigating risk while upholding the three core CIA trinity principles: confidentiality, honesty and availability [1]. Confidentiality ensures that only those allowed to access this information are available. The concept of confidentiality allows information only to be accessed by individuals with reasonable rights of access.

This chapter provides an overview of the concepts related to cryptography, Advanced Encryption Standard (AES) and DNA computing. It also introduces the aim of the work as well as the motivation keys that lead to this research. It also describes the contents and organization of the thesis.

1.1 CRYPTOGRAPHY

Cryptography and cryptology are the practice and studies of secure communication strategies (called adversaries). Before the modern era, cryptography meant simply the transformation of data from an apparent impossibility into encryption. Modern encryption is focused largely on mathematical theory and computer science; cryptographical algorithms are based on assumptions of computational complexity which make it difficult for any adversary to break such algorithms. In principle, such a mechanism can be broken, but by any known practical means it is unlikely. Therefore, theoretical advancement e.g., improvement in integrated factorization algorithms and faster computational technology requires constant adaptation of these solutions. These systems are called computationally safe systems. There are information-safe structures that cannot even be breached with unlimited computer power but that are harder to enforce than the best technically breaches able but reliable mechanisms. In other words, decryption is the opposite, going back to the plaintext of the unintelligible cipher. A cipher (or cipher) is an algorithm in cryptography for encryption or decryption, which can be followed by a sequence of well-defined steps. The detailed functioning of a chip is regulated by the algorithm as well as a "key" [1].

In general, different cryptography techniques such as substitution (replacements of one alphabet with the other) and transposition (replaces alphabets and permutations) have been developed.,

For privacy security, DES, IDEA, RSA, and others in previous years [2]. As we know, Internet use is growing and most users and organizations use a large number of new technologies and services, which means that data loads on networks are also increasing, whereas unauthorized users or intruders also have greater chances of information being stole, altered or read. Of course, a new technology is required that can meet the high storage demand from the modern age of information and protect this huge amount of information [3].

DNA computing is one of the latest areas that are now rising. The development of DNA computing began the DNA Cryptography journey. The complex machine problem was solved by DNA computing [4]. DNA Cryptography has come out of DNA computing research as a new instinctual

cryptographic area. Some DNA cryptography algorithms have limitations in that in some steps they still use modular arithmetic cryptography, or biological lab experiments, that are not suitable in the digital computer world. [5]. DNA can generally not only be used for storing and transmitting information, it can also be used for calculating. The vast parallelism and extraordinary density of information found in this molecule can be used for encryption, authentication, and so forth, using various DNA-based algorithms [6] [9] [7].

DNA's high storage capacity, comprehensive parallelism and high energy efficiency are the reason behind its consideration as a computing medium. Due to this power, the DNA can be a processor that can process large quantities of data and calculate many possible solutions. One gram of DNA comprises 1021 DNA bases, approximately equivalent to 108 tera-bytes of data so the capacity of the conventional storage media such as electronic, optical or magnet media can be clearly seen to far surpass, for example. [4]. DNA's strong storage ability and extensive parallelism demonstrated that it was a modern information medium and its processing power sought new solutions to complex mathematical challenges. DNA computing resolved a new direction in the field of cryptography. Currently, the study on DNA-based cryptography is in the first stage and several research studies need to investigate DNA computing [4].

Women scientists have accepted few DNA technologies for DNA encryption, such as PCR, DNA and digital DNA codification. The PCR is a quick-amplifying method for encrypting a document with two primers. If the right primary pair is not found, encoded message sequence will be very difficult to amplify. Formally speaking, digital DNA coding is a system based on 0 or 1 binary digital encoding. There are four coded nuclear bases of DNA A, C, T, and G. This coding pattern consists of a compatible DNA coding platform for both standard and conventional cryptosystems. Digital data can be mapped to biological DNA sequence and backward. [8].

However, the US government decided to standardize a cryptographic algorithm, which it has used to the full as Advanced Encryption Standards (AES)[1], the National Institute of Technology (NIST) announced a program for designing and opting for an Advanced Encrypting Standard (AIS). The study is progressing and it gained appreciation in various fields of its usage (DES). In

order to select a single norm, they requested algorithms from the cryptographic community. Therefore, a lot of NIST algorithms have been presented. The AES algorithm was then chosen for Rijndael by the most votes. Protection, efficiency and versatility were three of the selection criteria for NIST. Another important criterion was the performance of algorithms. The AES selection has defined two characteristics as critical: safety and performance. [2].

Generally speaking, cryptography is generally called the 'Secret Analysis.' There are also some main concepts which need to be grasped. The terms plaintext and cipher text are first and foremost. Plaintext refers to unencrypted data and cipher text refers to encrypted data. Encryption is the mechanism by which ordinary text is translated into unreadable form. The method of decryption in the legible form is to turn encrypted text into normal text [1]. Although encryption systems are distributed in two forms, in accordance with the character of their secret keys: asylum key and symmetrical key encryption, also known as private key cryptography. The asymmetric key algorithms are those in which two separate keys are encrypted and decrypted, and the same key is used in both encryption and decryption for symmetric key algorithms. [1].

Examples of symmetric data encryption and Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Diffie Hellman, the Digital signature, Elliptic Curve Cryptography (ECC), and ElGamal Encryption Method (EES) include the asymmetric key encryption examples, such as the three data encryption standard (T-DEA or 3-DES), the Educational Data Encryption Standard (E-DES), AES, BLOWFISH, the DC 6, the RC4, the RC2, the TWOFISH, the Serpent and the CAST. On the basis of input data, encryption algorithms are known as block chips where the block size of the encryption block and stream chips are transmitted for encryption and decipherment by means of a continuous stream. Some of the examples of block cipher [1][2][3] are RC2, AES, DES, RC6 and BLOWFISH. Illustration 1.1. It shows a separate Cryptographic algorithm of Symmetric and Asymmetric. A main objective of cryptography is to approach both theory and practice correctly in the following five areas [1]. Table 1.1. Table 1. Explain the key objectives that any cryptographic scheme can achieve.

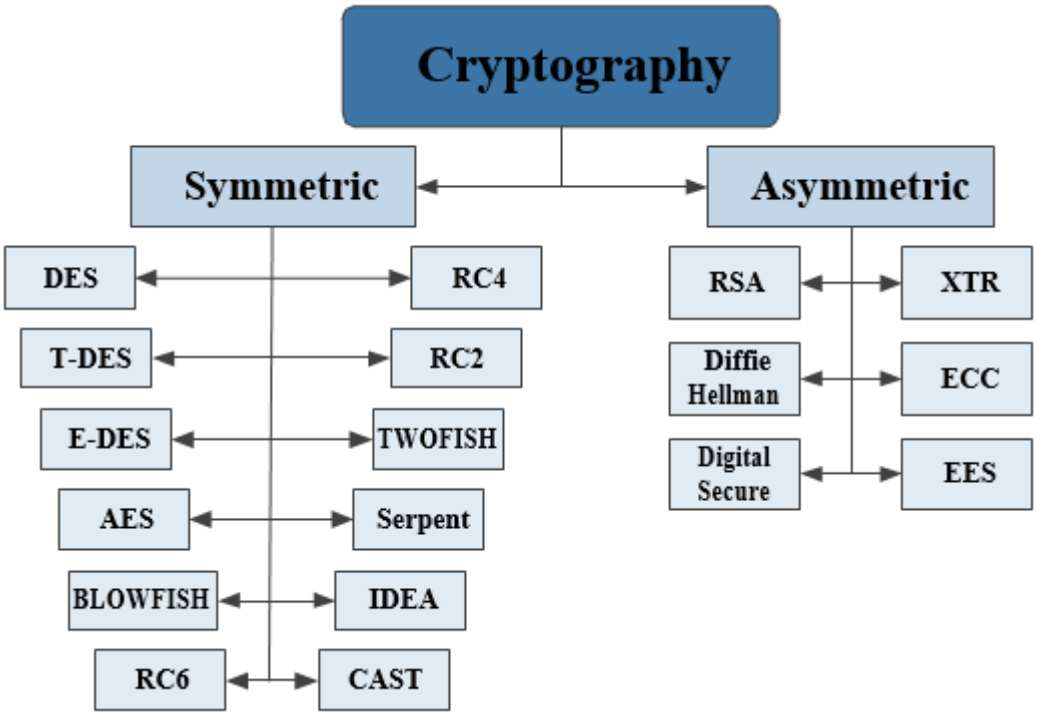


Figure 1.1: Different Symmetric and Asymmetric Cryptographic Algorithm

Table 1.1: Cryptography Goals

Cryptographic System	Definition
Confidentiality	Service used to hold information content from everyone, except those who are allowed to have it. Many confidential approaches range from physical security to mathematical algorithms Unintelligibility of data.
Data integrity	Service that deals with unauthorized data modification. In order to ensure the safety of data, unauthorized parties need to be able to detect data handling. The manipulation of data involves things like insert, erase and replace.
Authentication	Channel information should be authenticated according to source, date of origin, data quality, time transmitted, etc. This aspect of cryptography is therefore generally divided into two key classes: authentication of entities and authentication of data origin. Authentication of data source supplies data integrity indirectly (for if a message is modified, the source has changed).
Non-repudiation	This service does not dispute prior obligations or acts to an individual. When problems occur when an individual rejects such steps, it is important for the situation to be resolved.
Access Control	Service confirms that only the community with correct authentication can log into the message provided.

1.2 ADVANCED ENCRYPTION STANDARD (AES)

In both crypting and decryption, AES is one of the most popular algorithms that uses a symmetrical key. It can be one of three, 128-, 192- or 256-bits options. The speed of the AES algorithm for encryption and decryption is fast and secret according to the key length [9]. This makes it one of the most popular symmetrical key algorithms used. For the original 16-byte text, the AES algorithm uses 128 bits to combine the 4*4 matrix. The algorithm depends largely on the key length, as is the case with a 128-bit key in the 10 rounds and a 192-bit key in the 12 rounds, and so on. The original 128-bit key has likely 2128 keys = 3.4*1038 The main 192-bit key has likely 2192 keys = 6.2*1057 likely and the original 256-bit key has likely keys 2256 = 1.1*1077 likely keys. Each round uses different 128-bit key. [10].

Otherwise, the benefits of AES are executed quicker for both hardware and software, the latest in usage and the safer in line with U.S. and International Requirements, and eventually promoting a greater key size than other algorithms. AES then has a disadvantage in knowing the specifics of the procedure as too patent encryption and when the hidden (private) keys are lost, it would be difficult to decrypt data (chip text) [9]. There are four stages in each processing round in this algorithm [10]:

(1) SubBytes: On the encryption site, the first transformation, SubBytes, is used. We understand the byte as two hexadecimal digits to replace one byte.

(2) ShiftRows: In the encryption, the transformation is called ShiftRows.

(3) Mix Columns: At column level the transformation of the mix columns works; each column is transformed into a new column.

(4) AddRoundKey: AddRoundKey proceeds one column at a time. AddRoundKey adds a round key word with each state column matrix; the operation in AddRoundKey is matrix addition.

1.3 DNA COMPUTING

Deoxyribonucleic acid (DNA), a biological supermolecule produced by nucleotides, is a source plasm in all existence. The deoxyribonucleotides is a monomer unit of DNA. There are four kinds of DNA or DNA-based bases or nucleotides, which are four bases [11]. Adenine (A), Cytosine (C), Thymine (T), and Guanine are the foundations or nucleotides (G). DNA contains two essential nitrogen: purines and pyrimidines where A and G are two-ring molecules known as purines and C and T are one ring molecules known as pyrimidines. DNA contains [12].

DNA has a double helical structure, which is rendered by two single-strands of DNA that runs in the opposite direction each other in Figure 1.2 [13]. In helical structure, A joins with T by double hydrogen bonds and C joins with G by triple hydrogen bonds, where A-T pair weaker about 30 percent than C-G pair. DNA nucleotide mixture of hydrogen is known as the Watson and Crick complementary combination. [14]. Pairing of bases forms base units of DNA. Structure of DNA's strand consists of a backbone that is built from sugar molecules. These sugar molecules are attached together by phosphate group. Sugar and phosphate group has ratio of 3 carbons of sugar attached with 5 carbons of the phosphate group connected with next sugar molecule.

A DNA structure reads in terms of carbon ratio of sugar molecules and the phosphate group. For example, a DNA is read as 5 carbons to 3 carbons, where 5 carbons terminations represent phosphate group, and 3 carbons terminations represent sugar molecules. Sugar molecules are attached with one of the four bases i.e. (T, A, C, G) [15]. The backbone of nucleotide is two units negative charged for per base-pair and one-unit negative charge for per phosphate group. There will be a strong repulsion occur between two strands and split up, if there is no salt present in the medium.

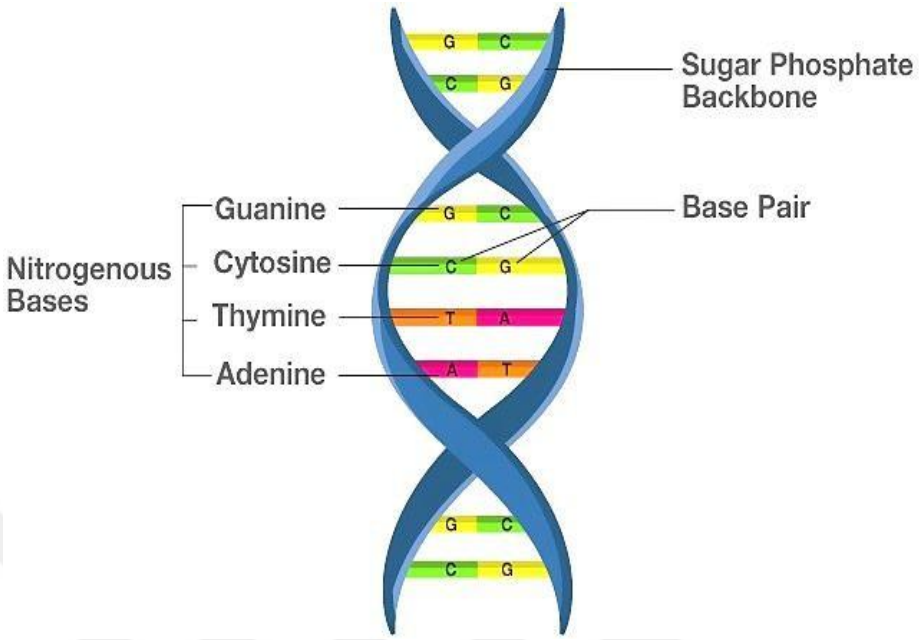


Figure 1.2: DNA Structure [13]

1.4 RESEARCH MOTIVATION

Cryptography is a perspective which uses cryptographic algorithms to transform plaintext into an incomprehensible format (cipher text). Conventional cryptographical algorithms cannot guarantee the protection of the vast quantity of data on the increasing internet and can be easily disrupted for malicious purposes by intruders. A new cryptographic algorithm has arisen to ensure the protection of information that provides powerful cipher text and safeguards unauthorized access. Consequently, the 'Dependent cryptography DNA computing' area is developed with two key roles:

(1) There are practically no variations between the actual DNA sequence and the false DNA sequence, and it is therefore 163 million publicly accessible DNA sequences worldwide; it is therefore an integrally important median for encryption keys., cipher text of these algorithms is more complex than the cipher text of normal keys [16].

(2) DNA has some interesting features, such as high-capacity storage, broad parallels, and a high energy efficiency. [17].

1.5 RESEARCH PROBLEM

The conception of cryptographic algorithms is based on complex problems to ensure algorithm security for at least some time. On the other hand, the cryptography algorithms can be broken using attack against so, cryptography algorithms should be kept secure by increasing complexity. The most common and widely accepted symmetric encryption algorithm today is the Advanced Encryption Standard (AES).

From almost two decades onwards, AES is commonly used to protect confidential information. While no assault has basically been able to crack all 10 AES rounds, it remains susceptible to countless assaults. AES is vulnerable to algebraic attacks and 7 rounds of AES with a collision attack may be potentially destroyed. In addition, an AES meeting was suggested in the middle attack, consisting of 8 rounds cited in [18] Theoretical breaking of the AES. However, the AES 'safety margin.' The security expert Bruce Schneider found in a blog post that continues to erode. He wrote, citing an expert from the United States: "Attacks will always be better; they will never be worse. Agency for National Security [18] [19].

1.6 RESEARCH OBJECTIVES

DNA encryption is a promising new area for cryptography that has arisen as DNA machine progress has been made. This thesis adopts DNA computing techniques to enhance AES algorithm so that it becomes more immune to most cryptanalytic attacks. This research proposes DNA computing hybridization in Advanced Encryption Standard (AES) algorithm and making use of the strength of the two fields in developing the proposed cryptographic algorithm.

1.7 CONTRIBUTION AND METHODOLOGY

The suggested model relies on the concept of DNA computing to enhance the traditional AES algorithm, increases the breaking time. In general, the contributions in this thesis are presented as follows:

•The proposed algorithm was built on the basis of DNA, and not bits, with all its functions (data, algorithms and functions used) in a mixed column step. The proposed technique shows that such an elaborate DNA system can be built using a method to make it a suitable contestant for use in biological environments or DNA computers.

•The proposed algorithm produces a longer key. The aim of increasing the key length is to disable the attackers from breaking into the system while maintaining a decreased time delay for the encryption and decryption.

1.8 ORGANIZATION OF THE THESIS

The next chapters of this thesis are organized as follows:

Chapter 2 provides a background and a survey of the cryptography algorithms and DNA computing. Chapter 3 describes in details the proposed algorithm and its hybridization DNA computing in the AES algorithm. In Chapter 4 the performed security analysis reveals the efficiency of the proposed algorithm. Finally, Chapter 5 gives a general summary of the thesis, the research conclusions, and suggestions for future research.

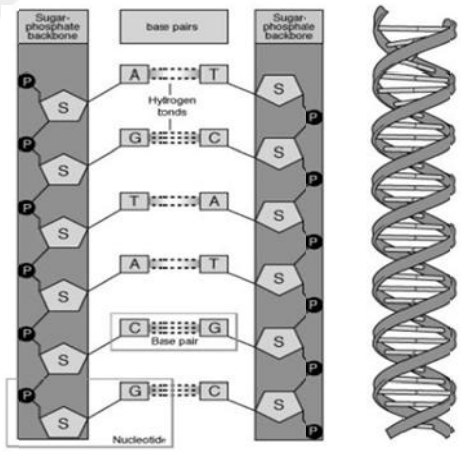
2. BACKGROUND AND RELATED WORK

This chapter presents related concepts to cryptography. It also reviews previous related work to the objectives and scope of the thesis. It discusses the Advanced Encryption Standard (AES) and DNA computing. It also introduces classification of cryptographic and covers a literature review on data encryption.

2.1 STRUCTURE OF DNA

Adenine (A), Guanine (G), Cytosine (C), and Thymine were stored in a code consisting of four basic chemical products (T). The base pairs are DNA-based, A with T and C with G. Every base is attached to the molecule of sugar and phosphate [21].

Figure 2.1: Structure of DNA



A significant feature of DNA is that it can either reproduce or produce copies. As a motive for duplicating the sequence of bases, each DNA strand in the double helix will help. This is important for the division of cells because any new cell requires a precise copy of the DNA in the old cell. DNA includes the biological guidelines which distinguish each species. DNA is passed on to adult species during reproduction, along with the guidance it contains. [22].

Although the practical advantages of DNA-based computing systems are not fully explored and the majority of work performed up till now has been theoretical, the potential use of this computational model has been suggested several times.

It can be classified as one of three overall classes to develop DNE computing techniques and finally to develop DNA computers:

i. Applications using 'classic' DNA computers, which have an advantage over conventional computation systems via significant parallelism, including possible time polynomial solutions for computation problems;

ii. Applications that make use of DNA's 'natural' capabilities, including information storage and engaging with established and emerging biotechnology;

iii. Contributions to basic research in both computer science and physics, in particular the study of computer limitations and the understanding and manipulation of biomolecular chemistry.

2.2 DNA INSTRUCTIONS

DNA is released during DNA replication and protein development. However, DNA is in its compact chromosome shape during cell division, which enables translation to new cells. The base sequence specifies the biological instructions in a DNA strand. For eg, the ATCGTT sequence could initiate blue eyes, and brown could be activated by ATCGCT. Any DNA sequence containing protein-building instructions is called a gene. The full manual DNA instruction book, or genome, has about three billion bases on 23 pairs of chromosomes and some 20,000 genes. DNA provides guidelines for creating, living and reproducing an organism. The instructions of DNA are used in a two-stage method for the processing of proteins. In the first position, enzymes read and transcribe the information into an intermediate molar called ribonucleic acid messenger or mRRNA in a DNA molecule. Next the data in the mRNA molecule are passed to the "language" of the amino acids that are the protein building blocks [23].

2.3 BACKGROUND

This section discusses the cryptography algorithms and DNA computing.

2.3.1 Cryptography Overview

Data hiding or cryptography protects personal or sensitive data with the use of a range of symmetric and asymmetrical key cryptographies, such as: Advanced Encryption Standard, (DES, Advanced Encryption Standard) (T-DEA or 3-DES), Educational Data Encryption Standard (E-DES), BLOWFISH, TWOFISH, SEAL, CAST, RC2, RC4, RC6, Adi Shamir and Leonard Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie Hellman (DH), ElGamal Encryption System (EES), and Digital Signature Algorithm (DSA) [20][24]. The cryptanalysis is, by way of analysis, the reverse encryption methods used to decode the ciphertext. Cryptanalysis offers a strong text chipboard with the application of encrypted data to enhance chipboards. Cryptanalysis mainly used for the illicit use of data by hackers to crack ciphertext. Cryptography and cryptography are required to develop a powerful cryptographic algorithm [25]. Figure 2.2 displays the encryption method comprising both encryption processes and decryption processes. Cryptanalysis destroys the initial message ciphertext, thus cryptography strengthens ciphertext. Recently, various tools such as frequency analysis, Morse code, substitution are available to crack the ciphertext [20].

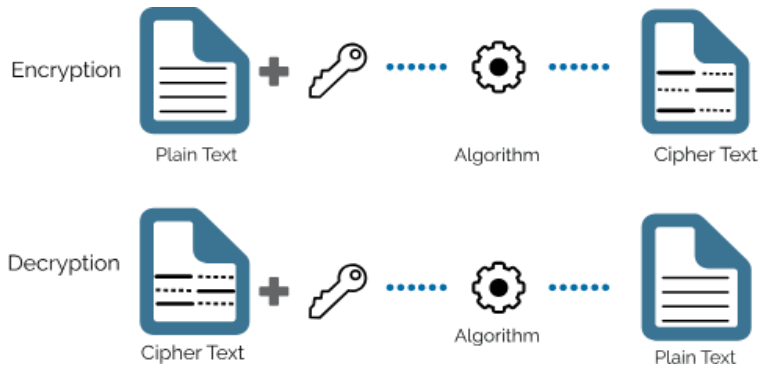


Figure 2.2: Process of Cryptography [20].

2.3.2 Classification of Cryptographic Procedures

Cryptographic procedures are based upon various cryptographic algorithms. Symmetric key algorithm uses identical key for encryption and decryption at both sender and receiver end whereas, asymmetric key algorithm uses distinct keys for encryption and decryption processes [26]. On the other hand, cryptography algorithm uses hash procedure where no key required. The following is a review of the main cryptographic procedures:

2.3.2.1 Symmetric Key Algorithm

Symmetric key algorithm referred as private key algorithm. In this algorithm, plaintext gets convert into ciphertext that is non-understandable for human by using an encryption process at sender end. After that, ciphertext is shared to receiver with symmetric key using the communication channel. Receiver applies inverse encryption process to ciphertext with the same key and gets the original plaintext. Figure 2.3 shows process of symmetric key algorithm [27].

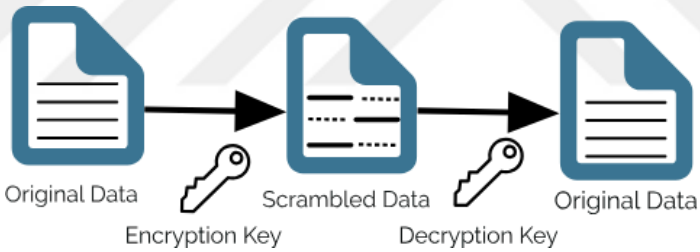


Figure 2.3: Symmetric Key Cryptography [24].

2.3.2.2 Asymmetric Key Algorithm

Asymmetric key algorithm or public key algorithm is proposed in 1975. It uses a combination of two keys for encryption and decryption processes at both ends. One is a private key or secret key and second one is a public key. Secret key used by receiver to decipher the encrypted data for obtaining plaintext whereas, public key used by sender to convert plaintext into ciphertext. Both ends try to make private key confidential to the outside world whereas, public key available for the outside world. Figure 2.4 shows asymmetric key algorithm [24]

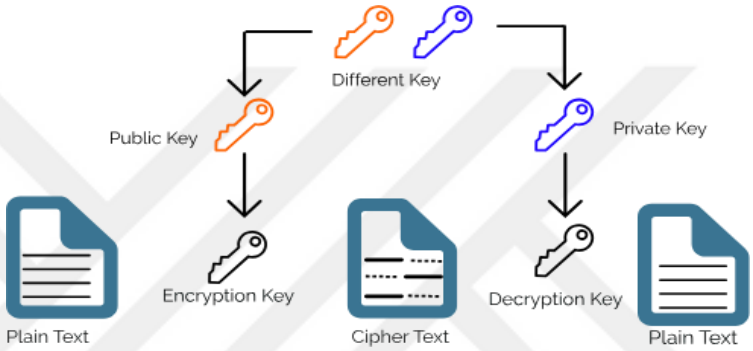


Figure 2.4: Asymmetric Key Cryptography [24]

Table 2.1. presents a comparison between symmetric and asymmetric cryptographic procedures [25].

Table 2.1: A Comparison Between Symmetric and Asymmetric Cryptographic [28]

Term	Symmetric	Asymmetric
Keys	One key is shared between two or more entitles	One entity has a public key, and the other entity has a private key
NIST recommended key length	128-bits	2048-bits
Number of keys	Grows exponentially as users grow	Grows linearly as users grow
key management / Sharing	Big issue	Easy and Secure

Speed of Encryption and Decryption	Algorithm is less complex and faster	Algorithm is more complex and 1000 times slower because they require more computational processing power.
USE	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys like PIN of ATM
Confidentiality	Yes	Yes
Integrity	Yes	-
Authenticity	Yes	Yes
Complexity	Medium	High
Examples	AES, and DES	RSA, and Diffie-Hellman

2.3.3 Cryptographic Algorithms

Bilateral encoding algorithms are symmetric and asymmetric algorithms: AES, DES, 3DES, EDES, BLOW FISH, RC2, RC4, RC6 etc. In comparison to the unilateral algorithms RSA, ECC, DH, EES and DSA [29].

2.3.3.1 Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) introduced an up-to-date chip-holding strategy to replace DES [30]. The AES method codes for the last coded message 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for the 256-bit key. Figure 2.6 illustrates the Flowchart of the AES Algorithm [28]. These steps can be defined as follow:

(1) Transformation of Subbytes: AES consists of a data block of 128 bits, i.e. every database object consists of 16 bytes. Each bit of the data element will be modified in another part by adding the 8-bit replacement box called the S-box Rijndael in SubBytes transformation.

(2) Transformation ShiftRows: The transformation is easy; the bytes in the remaining three row lines are moved in cycle ways, depending on the row location. In the second section, a round

left shift of 1 byte is carried out. During the third and fourth line, the circular changes are two bytes and three bytes left.

(3) Mix Columns: This transposition applies to each column's matrix multiplication. A fixed matrix is multiplied for every column vector. Instead of numbers in his service, bytes are called polynomials.

(4) Transformation of RoundKey: it's a clear XOR between the current condition and the round key. It is its own inverse transformation. There are several steps to the encryption process. The AddRoundKey operation will be performed initially, and a round function will be implemented on the SubBytes, ShiftRows, Mix Columns and AddDoundKey processing data block). This round operation (Nr times) is carried out iteratively depending on the duration of the key. The decryption operation has the same transformation sequence as the one in the encryption. The Inv-Subsubbytes, Inv-ShiftRows, Inv-Mix columns and AddRoundkey transformations make it possible to create and decrypt key schedules in the same way.

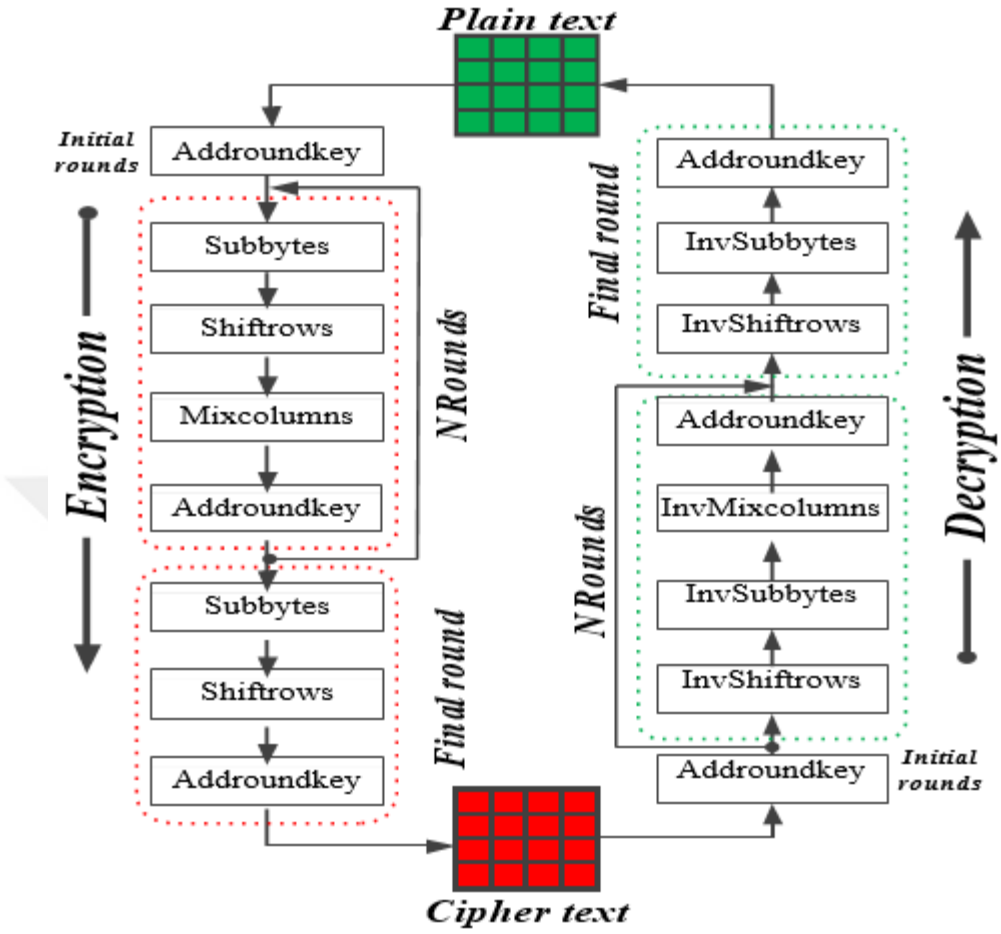


Figure 2.5: Flowchart of AES Algorithm [31].

2.3.3.2 Data Encryption Standard (DES)

A symmetric key-based block cipher is the Data Encryption Standard (DES). DES is based on Feistel block cipher and only runs on 64-bit blocks of data at a time. It was initially used in International Business Machines (IBM). This block is divided into a half right and a half left each with an initial permutation with a length of 32 bits. In 16 related operations, the data is combined with the 56-bit key length. Everywhere you transfer the key bits and 48 bits are picked from the 56 bits of the key. By means of the expansion permutation, the right half of the data is extended to 48 bits, with the combination of 48 bits of a shifted and permuted key through an XOR. The output is combined with the left half via another XOR after these four operations. From the above

operations, the new right half is created and the old right half the new left one. These operations are repeated for 16 DES rounds. Following sixteenth round there are joined the right and the left halves, and the final permutation ends the DES algorithm [31], which is the other way round. Illustration 2.7. Explains DES algorithm steps.

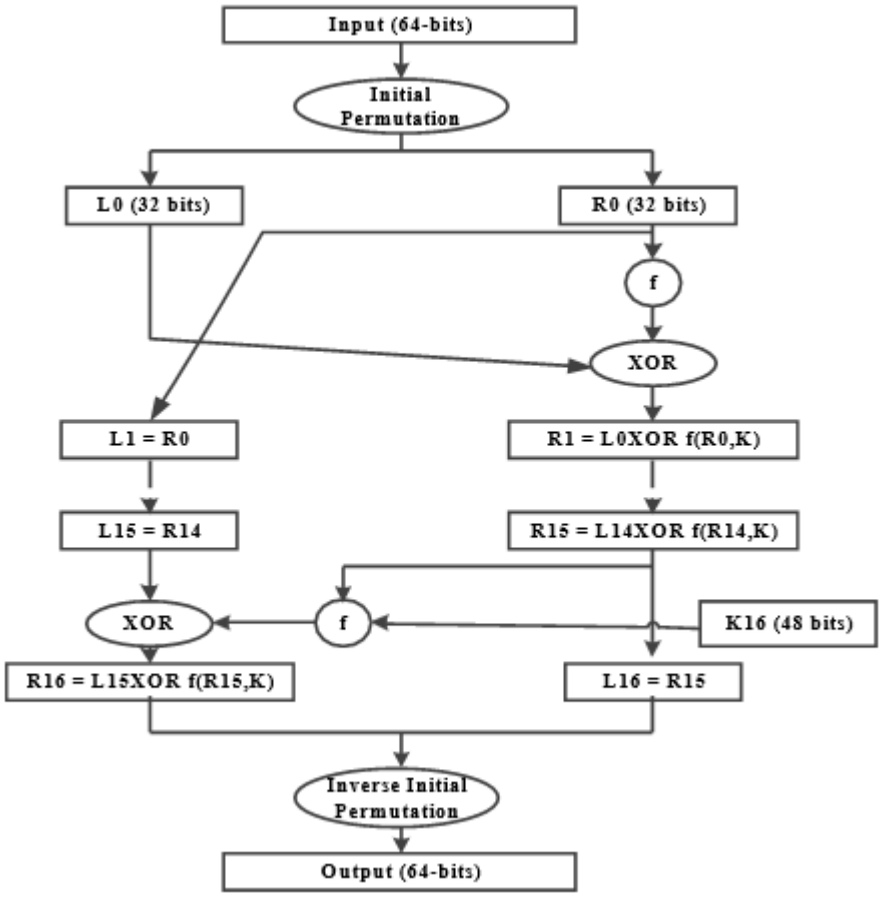


Figure 2.6: A Flowchart of DES Algorithm [31].

2.4 LITERATURE STUDY

This section reviews and discusses previous studies and techniques related to data encryption and DNA computing.

In 1999, Taylor et al. [32] proposed plaintext replacement encode cipher where alphabet, number and special character letters were allocated with base triplets, and demonstrated steganographic approach by hiding hidden messages encoded with DNA strands between multiple random DNA strands. Taylor et al. The use of subcloning, sequencing and a further triple coding table were difficult to decode.

In 2000 the first DNA-based cryptography trials were presented by Gehani et al. [33] and two methods were put forward: I a method of substitution using libraries with different single time pads, each one specifying a specific, pair-specific randomly generated mapping system, and (ii) an XOR system using molecular calculation. Such tests could only be performed in a well-stocked laboratory using modern technology.

In 2003, Chen [35] implemented the modern DNA cryptography method, using the huge parallel computer processing capabilities. A library was constructed of once pads in the shape of a DNA strand. The addition method modulo-2 was then used to encrypt a large number of short messages with a single pad to encrypt. Kazuo et al. [36] built a new public-key scheme with DNA in 2005 based on one-way.

Cui et al. [37] developed an encryption scheme in 2008. Data were first preprocessed to obtain entirely different ciphertexts to avoid attacks as PCR primers. A ciphertext was subsequently used using the optical DNA encoding technique. When the data entered the receiver side in encrypted form it was deciphered by reverse procedure. Dual security for the scheme was provided by biologically difficult problems and computer cryptography difficulties. The two primers used for the PCR key of this system were designed to boost the security of this encryption scheme thanks to the complete cooperation between sender and recipient.

In 2009, Monica et al. [39] suggested a one-time pad method for hidden writing using DNA. The message has been encrypted with XOR OTP tiles and chromosomes. Method of cleavage and limitation enzymes.

Sadeg et al. proposed in 2010 a symmetrical main block chip algorithm, Require a simulation stage of ideas from transcriptions and translation processes (DNA transfer to mRNA) (from mRNA into amino acids). The technically unbreakable encryption algorithm (OTP) has been suggested, the algorithm suffered some drawbacks. These inconveniences have discouraged its widespread usage in modern crypto-systems.

In 2010, Qinghai [41] put forward a protection process. Alice and Bob share a secret sequence codebook for DNA in this protocol. Alice has the power to construct a sequence that matches one sequence in the codebook to Bob via a public channel and sends the planned sequence to. When the sequence is obtained by Bob, the private sequence uses the non-matching letters as an encryption key. An opponent cannot decrypt the information given with public knowledge alone.

2010 was the year of L. In conjunction with GM technology and cryptology, Xuejia et al. [42] have proposed an asymmetrical encoding and signature encoding system. This was a biological cryptology exploratory study. For encryption and signature purposes, DNA-PKC uses two pairs of keys. Everybody is able to send an encrypted message to a specific user using public encryption keys. The ciphertext can only be decrypted and the message retrieved by the owners of the private decryption key.

In [44] The addition of these blocks was using DNA complementarity and DNA sequence adding. To get the encrypted image, the DNA sequence matrix has been decoded. The experimental results and safety review have shown that the algorithm proposed has a bigger reach and failed to attack widely, statistically and differently.

In 2010 Qiang et al. [43] introduced a new image encoding algorithm, which uses a logistic map to scrape the position and value of the pixels from the image using the concept of DNA subsequent operations (e.g., elongation, truncation, removal operation, etc.). The experimental results and the

security review have shown the simple implementation of the proposed algorithm and the highly efficient encryption and large space of the key, the good sensitivity to a hidden key and the ability to withstand an extensive attack and statistical attack.

The three levels of DNA encryption suggested by Soni et al. in 2013 were the automate theory, standard encryption and DNA. In 2013, Tripathi et al. [108] introduced a cryptographic solution incorporating public key encryption into the traditional algorithm of DNA security. DNA is symmetrically encrypted and the key used to symmetrically encrypt the data is asymmetrically encrypted through changed RSA. This study shows very clearly that windows consume more time compared with Linux, particularly when it comes to the algorithm test.

2014 saw the implementation of DNA Cryptography in the Multicloud by Ranalkar and Phulpagar[46] in which data is broken down into sections and DNA dependent encryption applied to every component and then uploaded to several clouds.

A combination of DNA computing and round-reduced AES block cipher was proposed [47], in the existing method, images of dimensions use n×m = 256 x 256 pixels. However, it has not been applied to any application of smart network applications [48]. Another papier suggested an algorithm based on AES [49] for high-definition imaging. You spoke about the well known AES block cipher algorithm, which is safer. This scheme has mostly been limited by the length of crypting/decrypting time and by the cryptography algorithm's attacks. For the same reason, the Cloud implements a hybrid encryption algorithm that uses RSA and AES algorithms to ensure that the user has data safety [50]. The choice to use an RSA and AES encryption algorithm comes with three keys: a public encryption key and private decryption key.

In the existing research, an AES algorithm for data security is designed to provide more security using Polybius square matrix and thus increased number of rounds [51]. Key stores and reads in the same clock cycle from the key RAM. In addition, AES-based digital imaging technology is introduced and demonstrates that the technique can better explain the effect of encryption and decryption [53].

In order to provide a high degree of safety and necessary high-performance application an updated AES algorithm is implemented with a 512-bit length [54]. Increase the strength of the AES algorithm to 512-bit and increase the number of rounds to provide a better encryption method for safe communication. Another study suggested a combination of AES encryption and base 64 encoder compression capabilities, so that a powerful encryption system would encrypt the data and save time and increase the efficiency. [55]. Basis 64 first encodes or translates the string value into text or complete data, and then encrypts the ciphertext with an AES algorithm. The file size is reduced after encoding and then submitted to encryption, minimizing further the processing time.

Similarly, it is proposed to give faith and trust through the use of enhanced two-key AES algorithm and steganography to boost safety aspects through combining AES with Steganography. [56]. Later, a work on message encryption and authentication at MAC level is introduced based on AES forward cipher function with 128-bit key and cipher block chaining modes in order to save power [57]. Another work is proposed to combine cryptography with image steganography in order to determine data protection. For cryptography and steganography respectively, the study used AES and Least Significant Bit (LSB) to boost data security. They concluded that LSB is an outstanding technique for incorporating critical data into a media carrier [58].

A high efficiency device on chip (DBUS) for (AES) is used with DBUS and the data sequence for AES encryption and decryption can also be pre-selected, thus reducing the overhead for state buffering and rescheduling. DBUS based design results show that the dynamic energy is reduced to 66.93% and the performance is 1.30 times higher compared to Advanced extensible Interface (AXI), which is based on the implementation. [59]. An additional RFID tags mutual authentication protocol is developed based on Elliptic Curve Cryptography and AES [60]. The new protocol can also submit useful information saved in the tag in encrypted pattern, in comparison to existing authentication protocols. The protocol is a theoretical structure not only; an RFID experimental tag has coded and checked it. With the same target, a new updated DNA mechanism approach is

proposed with the AES algorithm, where the cipher and key are combined and transmitted in protein form along a channel. [61].

An Enhanced AES (EAES) algorithm for secured fiber optic communication is introduced using dynamic key and S-box generation makes the data transmission more secure by adding more complexity in AES by increasing the Confusion and Diffusion in Ciphertext. The proposed EAES algorithm is simulated and the results are analyzed in terms of throughput and conversion time [62] [63].

With identical goals, a dual-implemented first research and hardware evaluation is carried out on a separate type of S-boxes. According to the style of architecture they are categorized in many categories. In addition, the S-Box in AES cipher based Linear Feedback Shift Register (LFSR) is used for benchmarking analysis of implementation. Second, the S-box, chosen from every group, is implemented on FPGA's platform with complete AES encryption. The AES cipher with different S-box designs is assessed for hardware size and speed. [64].

In addition to the Modified AES encryption algorithm for the image data file, the encryption method used by JEX encoding-decoding was implemented and did not apply to smart grid applications[65]. "The concept of DNA deep learning cryptography to hide ciphertext using deeper learned and DNA cryptography technologies," proposes "the DNA Cryptography and Deep Learning using Genetic Algorithm for Key Generated NW algorithm." The method of producing keys using natural selection has also been suggested [66].

2.5 CONCLUSION

This chapter reviewed the background and related concepts to cryptography. This chapter also reviewed and discussed the recent efforts related to cryptography algorithms. It is clear that AES is the most commonly used algorithm. Recently, some related work enhanced the AES using a hybrid AES and DNA computing algorithms. The following chapter introduces the proposed algorithm.

3. PROPOSED SYSTEM

The objective of this research work is to employ the properties of DNA computing in the cryptography algorithms to get "Better Secure, Authentication, Confidentiality and Data Integrity". This chapter explains the Advanced Encryption Standard (AES) based on a design principle known as a substitution-permutation network. This chapter also introduces and presents the proposed algorithm for enhancing the AES with DNA computing. It introduces and explains the proposed algorithm steps and operations: SubBytes operation, ShiftRow operation, DNA Encryption operation and AddRoundKey operation.

3.1 INTRODUCTION

There is an extended history of conventional cryptographic schemes. They are based on a strong theoretical and mathematical basis. A significant idea must therefore be established that DNA cryptography is often a bridge between current and new technologies, to avoid the tradition. This chapter describes in detail the proposed algorithm based on data encryption that integrates both AES and DNA computing. The objective of the proposed algorithm is to be higher in security by increasing the key length size using the DNA which is incorporated in the AES algorithm and results in preventing the piracy of the unauthorized users.

3.2 INTRODUCTION TO THE ADVANCED ENCRYPTION STANDARD

AED is a design principle known as a substitute-permutation network that has been substituted and permutated and has been easily introduced both in software and hardware. AES comprises 128 bits and 128, 192, and 256 bits of fixed block size. In comparison, AES is characterized with a number of blocks and key sizes, both 128 and a maximum of 256 bits, which can be multiple 32 bit. AES functions in the following matrix as a 4x4 column ordering matrix of bytes:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

The main size used for the AES cipher shows how many times transformation rounds the input is translated into the final output, called the plaintext, called the cypher text. The cipher, the cipher and the state of the output block are 128 bits in length. The representation is Nb = 4, showing the amount of 32-bit words (column number) in the State. K, 128, 192, or 256 bits of the Cipher Key. Nk = 4, 6, or 8 represents a number of words of 32 bits (number of columns) on the keyboard key. During the execution of the algorithm the number of rounds is based on the key size. No is the number of rounds, where No=10 is Nk=4, No=12 is Nk=6, and No=14 is Nc=8. Nk=14 is the number of rounds. Table 3.1 offers the only key-block-round combinations that comply with this requirement. For the implementation of the main length, block size and round number. The round number is determined as:

$$N_r = \frac{K}{32} + 6 \qquad (3.1)$$

Table 3.1: Key-Block-Round Combinations

Key Length	**Number of Key Length *(Nk words)***	**Number of block size *(Nb words)***	**Number of Rounds *(Nr)***
128-bit	4	4	10
192-bit	6	4	12
256-bit	8	4	14

3.3 THE PROPOSED ALGORITHM

DNA encryption is a promising new area for cryptography that has arisen as DNA machine progress has been made. This thesis adopts DNA computing techniques to enhance AES algorithm so that it becomes more immune to most cryptanalytic attacks. This research proposes DNA computing hybridization in Advanced Encryption Standard (AES)algorithm and making use of the strength of the two fields in developing the proposed cryptographic algorithm for image encryption.

The suggested model relies on the concept of DNA computing to enhance the traditional AES algorithm, increases the breaking time. In general, the contributions in this thesis are presented as follows:

•The proposed algorithm was built on the basis of DNA, and not bits, with all its functions (data, algorithms and functions used) in a mixed column step. The technique suggested shows the possibility of constructing such a complex DNA device in a method to make it suitable for biological use or on computers with DNA.

•The proposed algorithm produces a longer key. The aim of increasing the key length is to disable the attackers from breaking into the system while maintaining a decreased time delay for the encryption and decryption.

The proposed algorithm adopts of the DNA computing techniques to enhance AES algorithm. The four different transformations of the encryption process are sequentially applied on the state. These transformations are AddRoundKey; SubBytes; ShiftRows; and DNA encryption as illustrated in Figure 3.1. It represents a block diagram for the encryption/decryption processes using the proposed DNA-enhanced AES algorithm. The proposed algorithm aims to strengthen AES algorithm to reach the highest level of security which depends on the key length in AES algorithm. The proposed algorithm is an iterated block cipher that uses a fixed number of bytes to perform the same operations several times. A round is called an iteration of the steps above. The number of rounds depends on the size of the key. The proposed algorithm is using

block cipher size 128-bits and N of rounds. Figure 3.2 illustrate the flowchart of the proposed algorithm.

Using DNA Encryption to increase the key length, which gives more complexity to the AES so becomes immune in away that adapts the technological development. The key length of the proposed algorithm is calculated as follows:

•First key: The standard AES main key size is 2^128.

•Second key: The DNA key size is 24. This key presents the DNA sequence where the probability of the key could be:

A= 11, 10, 01, 00,

T= 11, 10, 01, 00,

C= 11, 10, 01, 00,

G= 11, 10, 01, 00.

•Third Key: The key size is 3 according to three different DNA bases which can be represented as one of the following:

(A=C, G=T)

or (A=G, T=C)

or (A=T, G=C)

In the proposed algorithm, the key size is (2^128* 24* 3) bits.

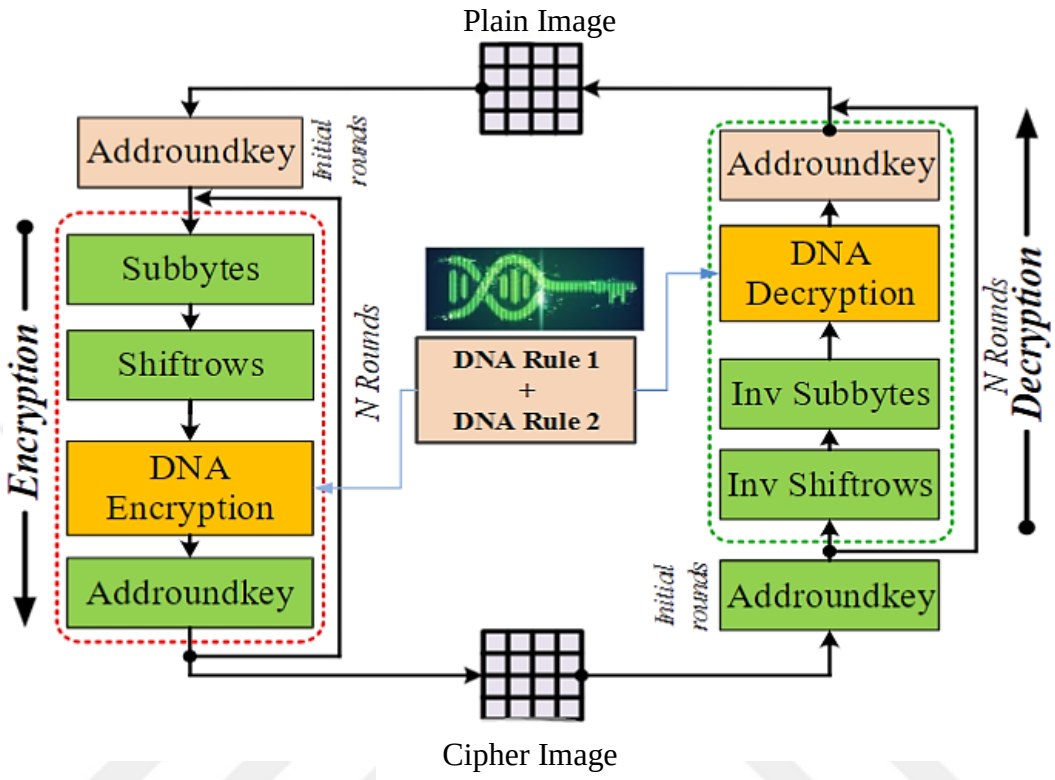


Figure 3.1: Hybridization AES and DNA Computing

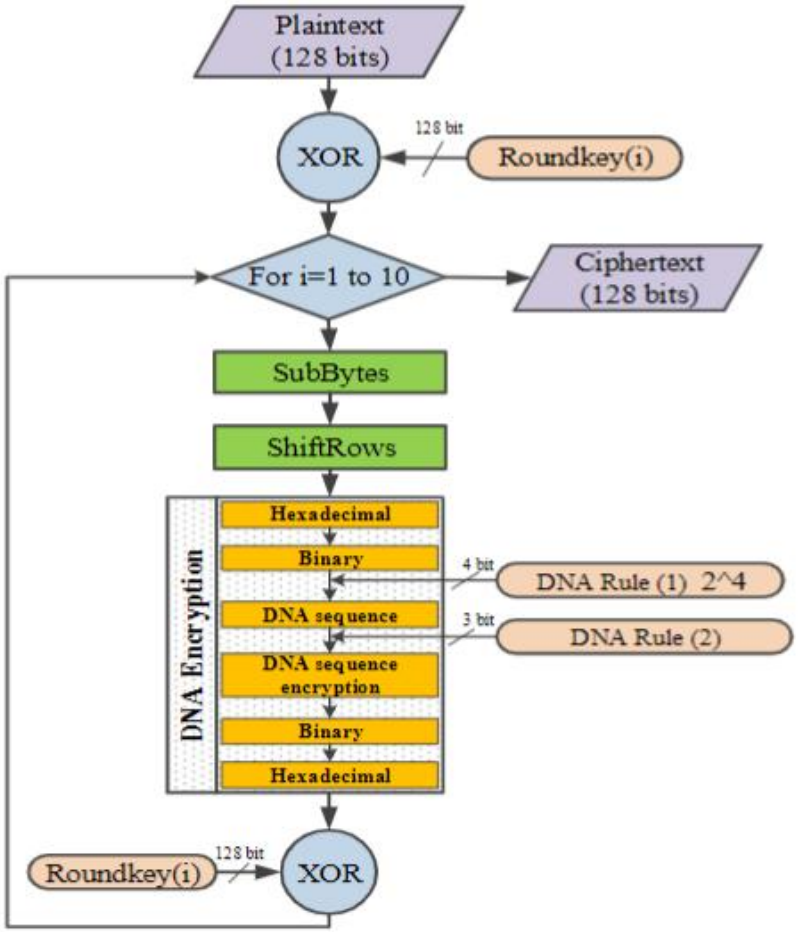


Figure 3.2: Flowchart of the Encryption of Data using the Proposed Algorithm

3.4 THE PROPOSED ALGORITHM STEPS

Aside from the key expansions that are round keys, each byte of the state "plaintext" is combined with a block of the round key using the bit-wise XOR by the Rijndael key calendar and the initial round. In the state, four separate encryption method transformations are implemented. The following paragraphs define the key steps.

3.4.1 SubBytes operation

SubBytes is a non-linear octet replacement working independently on each byte of the state as shown in Figure 3.3. The replacement table (S-Box) is invertible and uses precalculated forms irrespective of any data. The value in an s-box, the index of which corresponds to the value in the state, replaces each byte of the state:

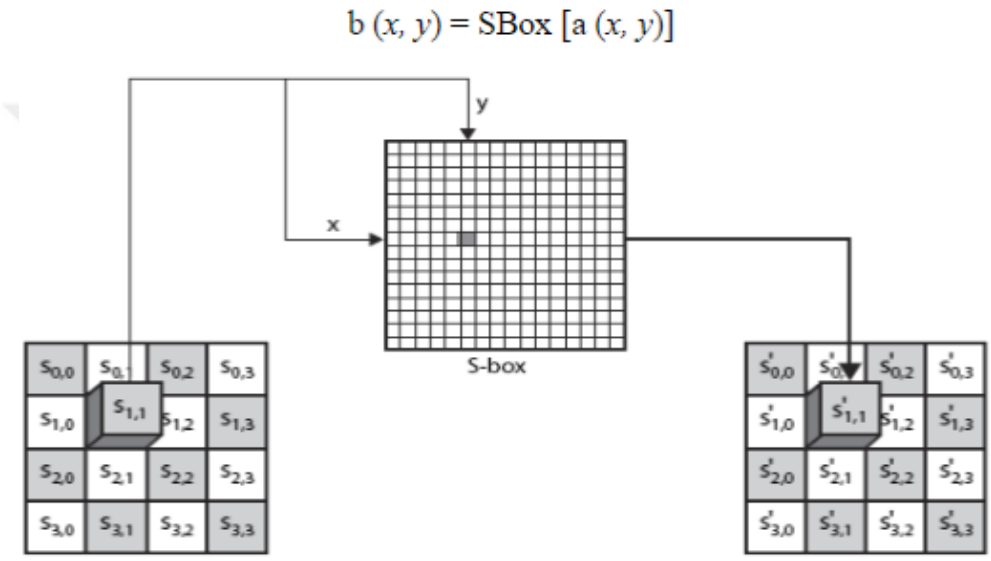


Figure 3.3: SubBytes Operation Representation

The inverse of SubBytes is the same operation, using the inversed S-Box, which is also pre-calculated as shown in Figure 3.4.is a SubBytes step:

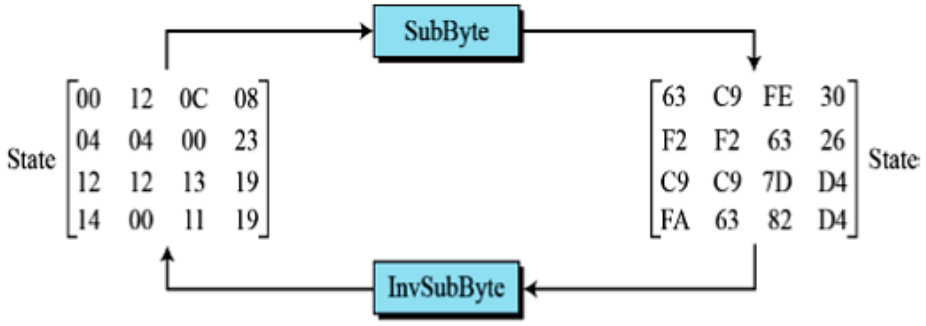


Figure 3.4: SubBytes and Inverse of SubBytes Transformations

Every byte is replaced with an entry in the Subbytes step, in a fixed 8-bit search table, S; b I j) = S. (i, j). Figure 3.5 and 3.6 illustrates S-Box and Inverse S-Box table. The SubBytes transformation and InvSubBytes transformation is the inverse of each other.

	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 3.5: S-Box Table

	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 3.6: Inverse S-Box Table

3.4.2 ShiftRow operation

Each row of the state, depending on the row index, is cyclically moved to the left.

•The 1strow is shifted 0 positions to the left.

•The 2ndrow is shifted 1 position to the left.

•The 3rdrow is shifted 2 positions to the left.

•The 4throw is shifted 3 positions to the left

The inverse is the same cyclic to the right of ShiftRows. Later, decoding is necessary. Bytes in each row of the state are shifted cyclically to the left. Each byte is modified according to the number of locations. Table 3.7.and Table 3.8. ShiftRows and ShiftRows and InvShiftRows examples are.

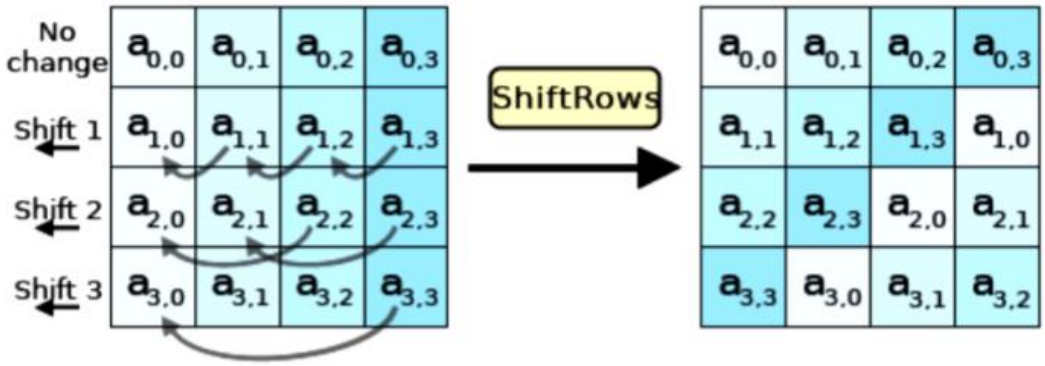


Figure 3.7: ShiftRows Schema

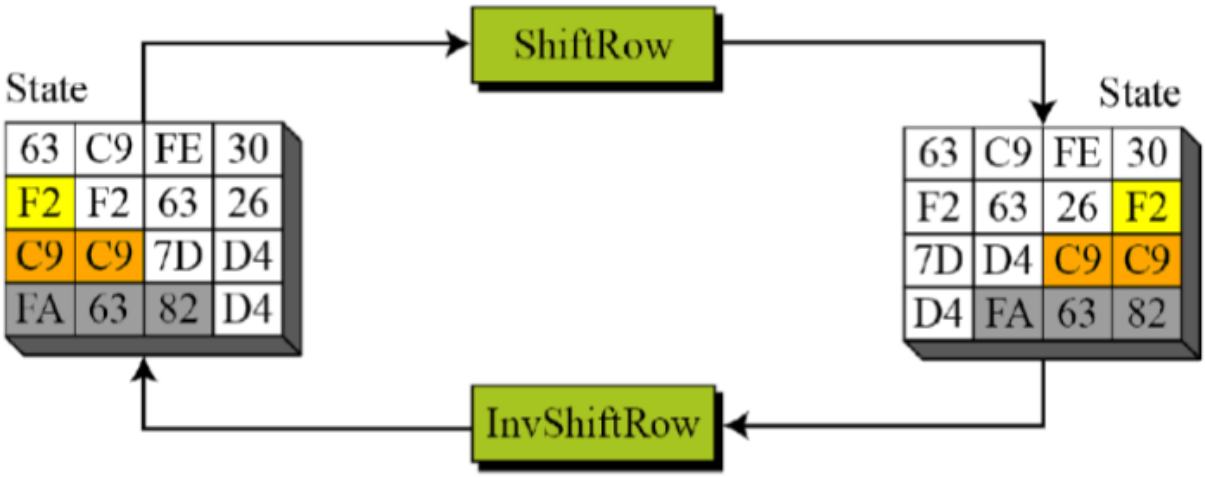


Figure 3.8: ShiftRows and InvShiftRows Operations

3.4.3 DNA Encryption Operation

The process of the DNA Encryption starts with turning the Hexadecimal message obtained from the ShiftRows step into a binary message. This message is transformed through the variable DNA bases into a DNA helix. Then it is ciphered through the DNA bases to present a wholly different outcome which is returned into binary text. Once again, the message is transformed into a Hexadecimal message handed to the AddRoundKey step. Table 3.2 and 3.3 illustrates DNA Rule (1) "key size is 24"and DNA Rule (2) "key size is 3". Figure 3.9 illustrate the sequence of DNA encryption operation.

Table 3.2: DNA Rule (1)

No. of Rule	A	T		
Rule 1.1	1	0	1	0
Rule 1.2	1	0	1	0
Rule 1.3	1	0	1	0
Rule 1.4	1	0	1	0

Rule 1.5	0	1	0	1
Rule 1.6	0	1	0	1
Rule 1.7	0	1	0	1
Rule 1.8	0	1	0	1
Rule 1.9	1	0	1	0
Rule 1.10	1	0	1	0
Rule 1.11	1	0	1	0
Rule 1.12	1	0	1	0
Rule 1.13	0	1	0	1
Rule 1.14	0	1	0	1
Rule 1.15	0	1	0	1

Table 3.3: DNA Rule (2)

No. of Rule	**DNA sequence**
Rule 2.1	A=T, C=G
Rule 2.2	A=C, T=G
Rule 2.3	A=G, T=C

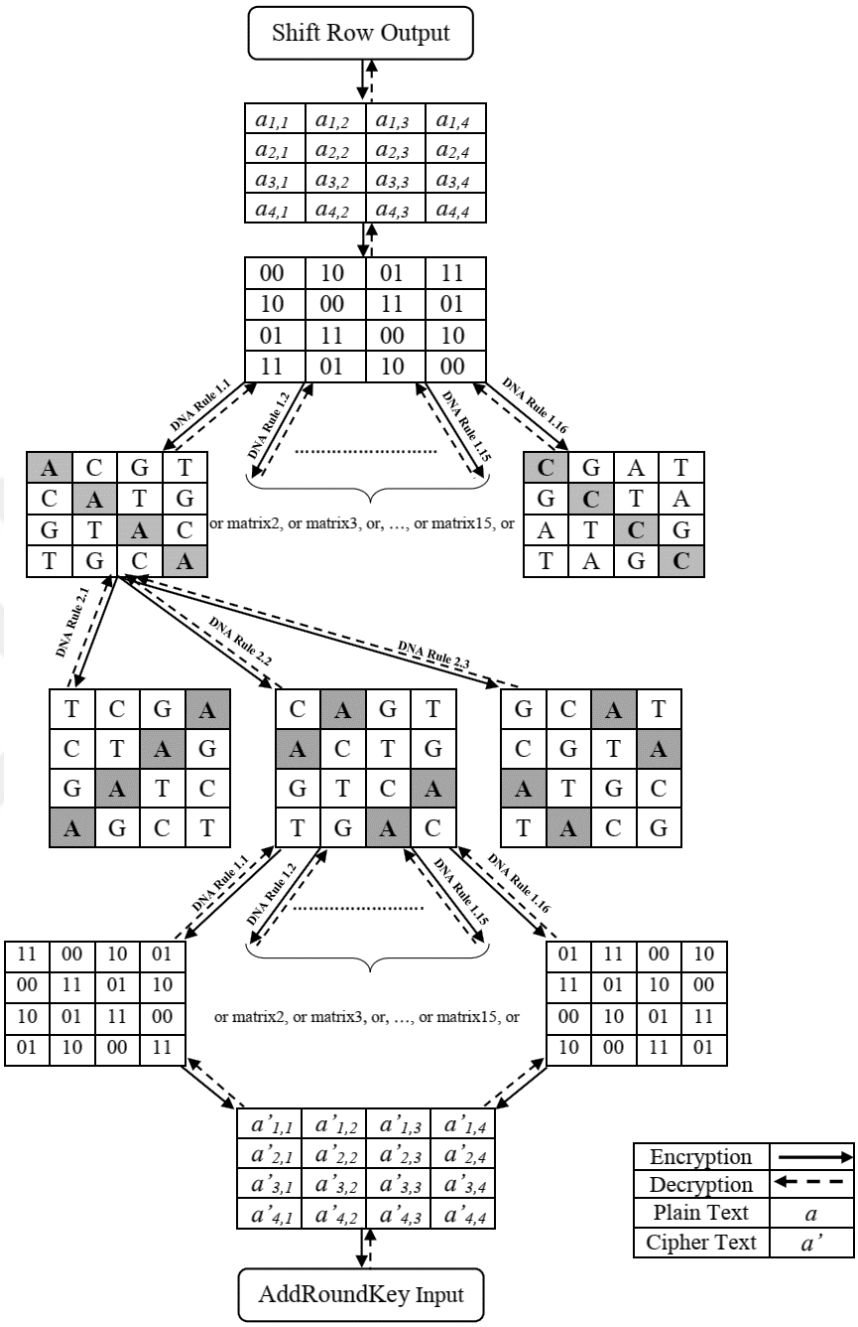


Figure 3.9: Sequence of DNA Encryption Operation

3.4.4 AddRoundKey Operation

In this operation, a simple bit-wise XOR applies a round key to the state. The Round Key from the chip Key shows the process by which key rounds are produced for each round by means of the key schedule in Figure 3.10. The length of the round key is equivalent to 128-bit block key. Figure 3.11 shows the procedure AddRoundKey where the subkey and the state are joined together. A subkey is taken from the main key with the key schedule of Rijndael for every round; each subkey is the same size as the state. By means of a bit-wise XOR, each byte of the state is combined with the corresponding byte of the subkey. Each byte of the state, with the XOR operation, is associated with a byte of the round subkey.

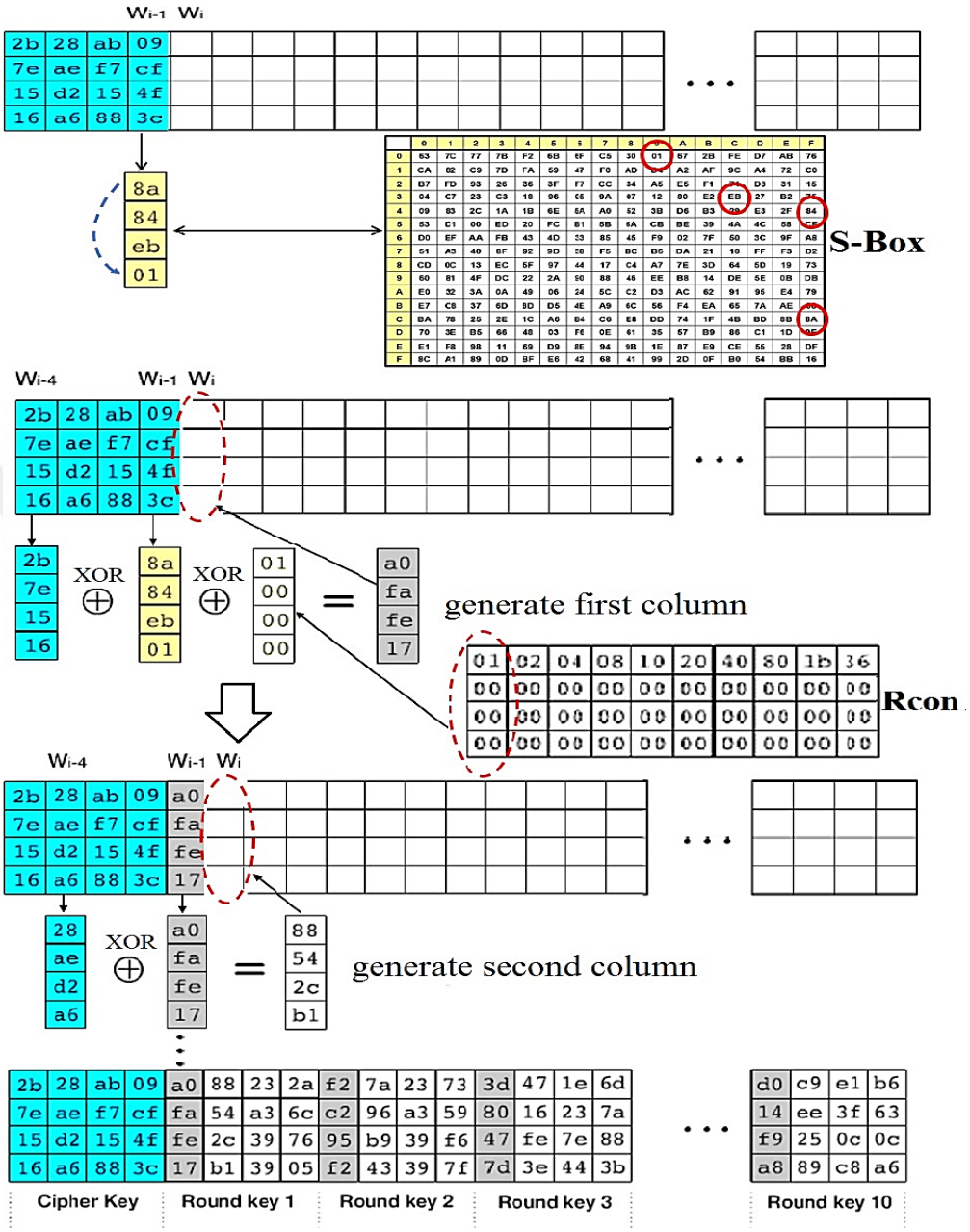


Figure 3.10: Process to Generate Key Round

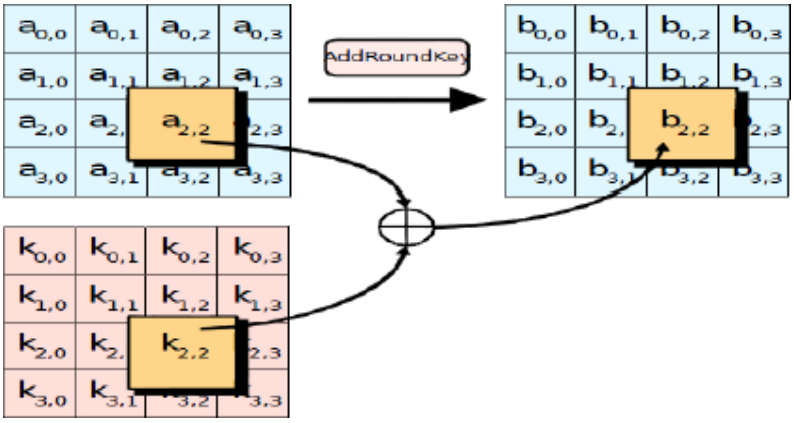


Figure 3.11: AddRoundKey Operation

3.4.5 Case Study

The case study used the four transformation steps of the proposed algorithm to explain how the plain text is ciphered in every transformation step. The plain text is first transformed into decimal, then the XOR operation is applied to the decimal and the initial key to obtain the state. The state goes through the four-step process to get the ciphered text. The process is repeated N number of times, resulting a more secure and complex encryption. Figure 3.12 illustrates the real case study of all steps of the proposed algorithm.

- Plain text 128 bit “OMARGHAZIABBOODD”.
- First key 128 bit “DATAENCRYPTION11”.
- DNA Rule 1.1 = 4 bit “11,10,01,00”.
- DNA Rule 2.1 = 3 bit “A=T, C=G”.

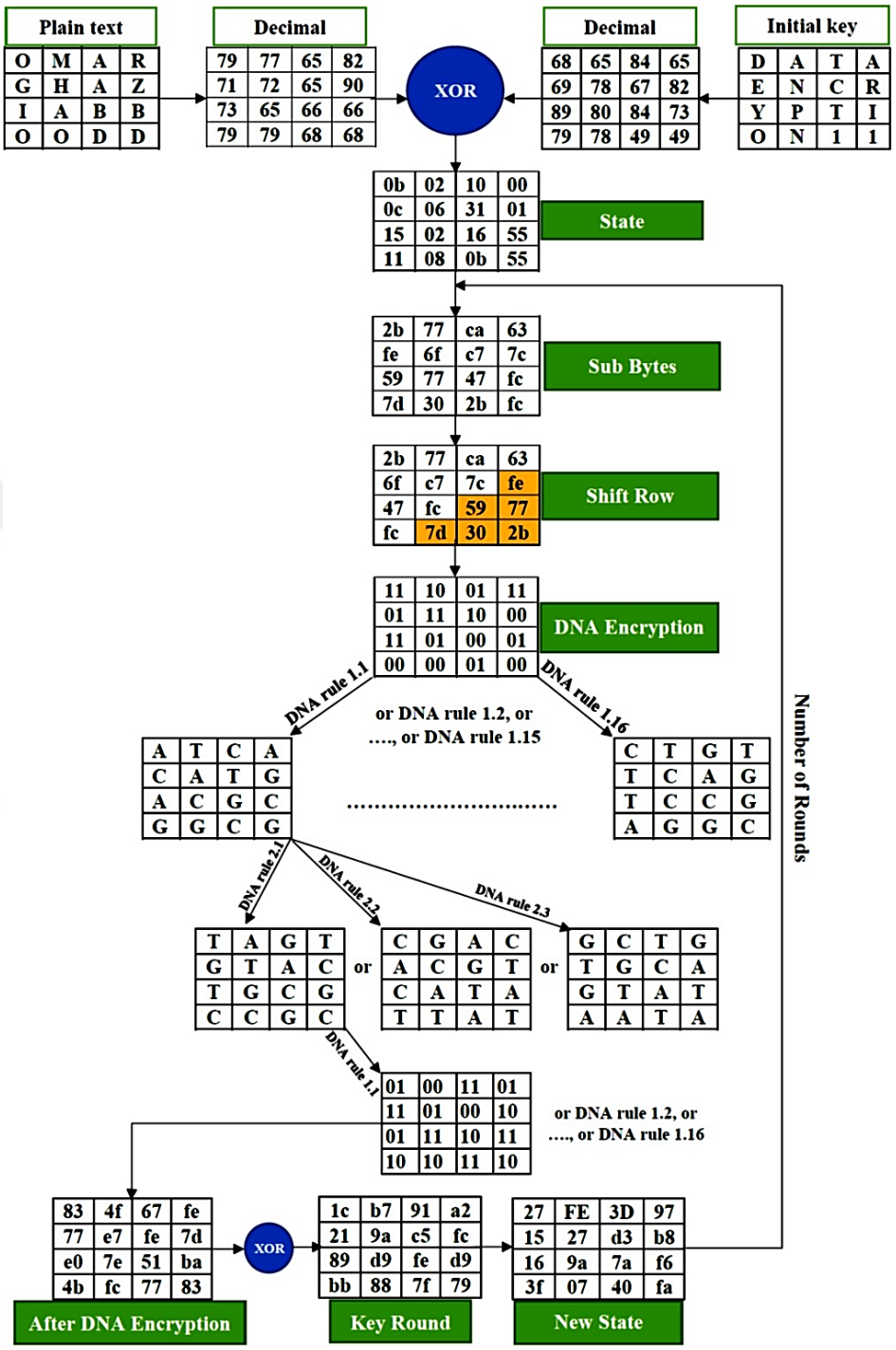


Figure 3.12: A Case Study of Proposed Algorithm

3.4.6 Pseudo Code

Figure 3.13 illustrates the summarize pseudo-code descriptions for the algorithms utilized in the experiments.

Require: Plain-image [n * m], key [Nr] [4 * 4],
and DNA-key [4 * m] bytes.
Ensure: Cipher-image [n * m] bytes.
1: Suppose that the plain-image size is n * m pixels and the state size is [4 * 4] bytes.
2: **for** i = 1 step 1 to n/4 **do**
3: **for** j = 1 step 1 to m/4 **do**
4: Add-Round-Key (state [i, j], key [0] [4 * 4]);
5: **for** r = 1 step 1 to Nr - 1 **do**
6: Sub-Bytes (state [i, j]),
7: Shift-Rows (state [i, j]),
8: DNA-Columns (state [i, j]),
9: Add-Round-Key (state [i, j], key [Nr] [4 * 4]);
14: **end for**
15: **end for**
16: //Note that: The DNA-key size is 4 * m bytes, consequently,
the state size will be changed to 4 * m bytes.
17: **for** i = 1 step 1 to n/4 **do**
19: **end for**

Figure 3.13: The Pseudo Code for Proposed Algorithm

3.5 CONCLUSION

This chapter discussed the details of the proposed DNA inspired AES algorithm based on the DNA computing concept. It also demonstrated how the four transformation steps are used to increase

complexity of the text. It also explains how the key length is increased by applying DNA Rules. In our case, the best developed model gives more security than the pre-specified models optimized by both original AES algorithm and other techniques. By combining the AES and DNA concept, the key length of the proposed algorithm is successfully enhanced. Using DNA is considered one of the important features of the proposed algorithm. It gives positive results in exhaustive attack, encryption quality, statistical analysis and differential analysis.

4. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this Chapter, the efficiency of the proposed algorithm is analyzed. Many different sets of experiments are carried out to determine the variation in the robustness of the proposed algorithm explained in chapter 3.

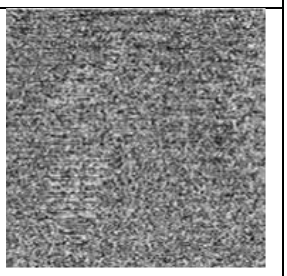
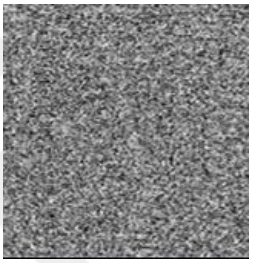
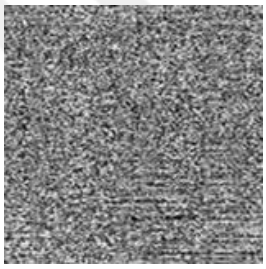
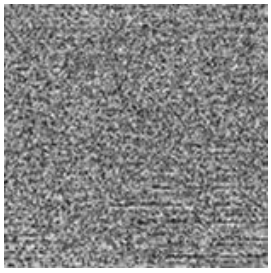
4.1 TEST CONDITIONS

This section presents the simulation results and the security analysis. Many analysis methods are used such as statistical analysis, numerical analysis, differential analysis, encryption quality, and Keyspace analysis, to measure the resistance to brute force attack. For a single image, the difference between different cipher images is used to calculate the resistance to a single text attack. In order to fully determine the efficacy of the proposed algorithm, this number of different tests are performed. In the following subsections, the experimental study is discussed in detail. The experimental findings are also discussed.

4.1.1 Dataset Description

This sub-section describes the dataset of images that are used for the experimental purposes. Database of gray-scale images are downloaded from the SIPI database [67]. The 6 gray-scale images chosen from 50 gray-scale images in the SIPI database are used for the comparative analysis of the proposed algorithm with other state-of-the-art methods. The dataset contains different edgy and smooth standard gray-scale images of dimensions (256×256). This standard image dataset includes Cameraman; Lena; Mona Lisa; Mandrill; Peppers; Plane respectively. Table 4.1. shows the attributes of the images used by thumbnails.

Table 4.1: Dataset Description

Name	Size	Original Images	Cipher Images
Cameraman	**256*256**		
Lena	**256*256**		
Mona Lisa	**256*256**		
Peppers	**256*256**		

4.1.2 Image Quality Assessment Metrics (IQAMs)

This sub-section highlights different IQAMs that are used for comparison of existing ten prominent image encryption schemes with the proposed algorithm. In this work full- reference image-quality assessment method has been used were original images, encrypted and decrypted images are compared with one another different number of rounds. Table 4.2. illustrates the ten objective image quality measures and their parameter based on that, the quality of images depends on the lower and higher score value. Full-reference IQAMs include Histogram Analysis, Correlation Analysis of the Adjacent Pixels, Correlation Coefficients, Entropy Analysis, NPCR, UACI, SC, NAE, PSNR, and MSE. These metrics are discussed in the following sections. The performance of these techniques is also evaluated.

The techniques are coded using MATLAB (R2016b) platform on a Laptop running Windows 10 Pro 64-bit, System Model: HP 15 Notebook PC, BIOS: InsydeH2O Version 03.73.06F.31, Processor: Intel(R) Core (TM) i5-4210U CPU @ 1.70GHz (4 CPUs) ~2.4GHz, Memory: 4096 MB RAM, Card name: Intel(R) HD Graphics Family, Display Memory: 1189 MB.

Table 4.2: Image Quality Metrics

No.	Image Quality Measure	Quality of Image
1	**Histogram Analysis**	The cipher image is very uniform and significantly different from the plain image [68] [69].
2	**Correlation Analysis of the Adjacent Pixels**	The value of a pixel and its neighboring pixel are identical in the simple picture (high correlation). Conversely, the cipher pixels, which cover the whole range of data, are randomly distributed (low correlation) [70].
3	**Correlation Coefficients**	The range between from -1 to +1, where value one higher quality [70].

4	**Entropy Analysis**	The ideal entropy value is close to 8 [69] [71].
5	**NPCR**	The value of NPCR should be close to 100% [70].
6	**UACI**	The value of UACI should be close to 33% [70].
7	**SC**	Lower SC value provides higher quality [72].
8	**NAE**	Large value of NAE means that image is poor quality [72].
9	**PSNR**	Higher PSNR value provides higher Quality [73] [74].
10	**MSE**	Lower MSE Value provides Lower Quality [73] [74].

4.2 PERFORMANCE EVALUATION METRICS

Various metrics are used for calculating the algorithm's effectiveness. These security performances can be split up into two groups, namely time and safety efficiency initiatives.

4.2.1 Execution Time Encryption

Encryption time is known as the time taken to convert the plaintext by the algorithm. into something that seems to be random and unmeaning (ciphertext). The decryption computational time is the time taken of converting ciphertext back to plaintext.

4.2.2 Security Performance Metrics

Some security analyzes are employed to measure the resistance of a cipher to various types of attacks. For example, statistical analysis Histogram and correlation used to measure statistical attack resistance. The measure of randomness, for example, is entropy. Numerical analysis. Numerical analysis. For example, the difference analysis used to calculate resistance to differential attacks, the number of pixels (NPCR) and the unified mean intensity change value for example

(UACI). Performance of encryption, such as Structural Material (SC), NAE, PSNR, and Median Square Errors (MSE). Keyspace analyzes are used to test brute force attack resistance.

4.2.2.1 Keyspace Analysis

Keyspace analysis is used to measure resistance to brute force attack. Keyspace is the mixture of all potentially useable keys in the cryptosystem. In a strong cryptographic scheme, the key should be big[75] in order to render the brute force attack impossible. The main space size should be K > 2100 [77] to ensure adequate protection from brute force attacks. Therefore, we use complex secret keys, which are long enough to withstand brute attacks. DNA sequences with the AES are used as stated below to establish the key of the proposed algorithm:

AES key size = **128 (2^{128}):** this key presents the main key for the AES standard algorithm.

DNA sequence size = **4 (2^4)** bits: this key presents the DNA sequence where the probability of the key could be one of the following:

A = 11, 10, 01, 00
T = 11, 10, 01, 00
C = 11, 10, 01, 00
G = 11, 10, 01, 00

Three different DNA bases = 3 bits: this base is presented as one of the following:

(A = C, G = T)
(A = G, T = C)
(A = T, G = C)

The Key space = $2^{128} * 2^4 * 3 = 1.633350*10^{40}$ keys

If a malicious user produces 1 million keys per second **(10^6),** then the time required for breakage multiplied by **(365)** number of days of the year and **(86400)** number of seconds per day [79] is:

$$\frac{2^{128}*2^4*3}{10^6*365*86400} = 5.179340 * 10^{26}\ year \quad (4.1)$$

4.2.2.2 Histogram Analysis

The pixel values are represented in a picture histogram. For a cipher image, it is necessary for a cipher image to be distributed uniformly, and without statistical comparison to the originals, making statistical attacks difficult to recover the original image. In this way, the attacker cannot recover meaningful information from a fluctuating histogram. [68] [69].

4.2.2.3 Correlation Analysis of the Adjacent Pixels

The correlation test is one of the frequently used methods for testing an encryption system, where the correlation r ij is calculated as [71] [80]:

$$r = \frac{cov_{(i,j)}}{\sqrt{D_{(i)}}\sqrt{D_{(j)}}}, where \tag{4.2}$$

$$cov_{(i,j)} = \frac{1}{n}\sum_{m=1}^{n}\left(i_m - E_{(i)}\right)\left(j_m - E_{(j)}\right) \tag{4.3}$$

$$E_{(x)} = \frac{1}{n}\sum_{m=1}^{n}(i_m) \tag{4.4}$$

$$D_{(i)} = \frac{1}{n}\sum_{m=1}^{n}\left(\left(i_m - E_{(i)}\right)\right)^2 \tag{4.5}$$

In the case where I and j are gray-scale figures of two neighboring pixels, E I is a variance of I and D I N shows the total number of pixels and CoV I j), a covariance of I and j is determined. Since pixels for images are closely interrelated, a decrease in image correlation coefficients is an indicator of the encryption System strength of (horizontal, vertical and diagonal) pixels. [69] [80].

4.2.2.4 Correlation Analysis of Original and Encrypted Image

You can measure the correlation of the original and encrypted images as:

$$\rho = \frac{\sum_{i=1}^{n}\sum_{i=1}^{m}\left(X_{(i,j)} - E_{(x)}\right)\left(Y_{(i,j)} - E_{(y)}\right)}{\sqrt{\sum_{i=1}^{n}\sum_{i=1}^{m}\left(X_{(i,j)} - E_{(x)}\right)^2 \sum_{i=1}^{n}\sum_{i=1}^{m}\left(Y_{(i,j)} - E_{(y)}\right)^2}} \tag{4.6}$$

Where, X I j), Y I j) are the pixel values of the ith row and of the jth column of the image and cipher. Average images of the single image and of the chip images are represented by E (x), E (y). (n, m) the dimension of the image [71] [80].

4.2.2.5 Information Entropy Analysis

Information entropy is one of the most important aspects of randomness and measuring the system complexity. Higher entropy means more complexity of the system. Information entropy is calculated as [69] [71]:

$$H(s) = \sum_t p(s_i) log2 \frac{1}{p(s_i)} \quad (4.7)$$

Where si indicates the gray level and p(si) indicates whether the event is probable. For gray pictures with image pixels called random events the ideal entropy value is 8. So the picture with a closet value of 8 displays the best degree of uncertainties [69] [71].

4.2.2.6 Differential Analysis Metrics

Differential analysis is a method used for the resistance to differential attack of the encryption algorithm[76]. In order to test the sensitivity of the algorithm to a slight change in the plain image, the NPCR is used for measuring and calculating the percent of different pixel numbers between two pictures: pixel rate of changing (NPCR) numbers and unified mean rate of change (UACI):

$$NPCR = \frac{\sum_{i=1}^{w} \sum_{i=1}^{h} D_{(i,j)}}{w*h} * 100\% \quad (4.8)$$

UACI is used to assess the average intensity of various images. The UACI is calculated as follows:

$$UACI = \frac{1}{w*h} * \frac{\sum_{i=1}^{w} \sum_{i=1}^{h} |C_{1(i,j)} - C_{2(i,j)}|}{255} * 100\% \quad (4.9)$$

The gray pixel values at position I j), C 1 and C 2 are referred to as C 1 I j) and C 2 I j); W and H are the width and height of the C 1 or C 2; D(i, j) is calculated by C 1(i, j, j) and C 2(i, j); in this

case, C 1(i, j) is the same as those for the corresponding single image; in the case of C 1(i, j), j(i). In that case, C 1(i, j) are referred to the two images with only one pixel difference.

4.2.2.7 Structural Content (SC)

It is defined as the sum of the original value for the image pixels, divided by the sum of the decrypted value for the image pixels. The connection between images is also found. In decrypted images, the Lower SC Value provides better quality, so that SC is 1 [72] if there is no distortion. The SC is determined as:

$$sc = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} f_{(i,j)^2}}{\sum_{i=1}^{m}\sum_{i=1}^{n} \bar{f}_{(i,j)^2}} \tag{4.10}$$

4.2.2.8 Normalized Absolute Error (NAE)

In summing up the original pixel square pixel[72], the description of the discrepancies between the original f(i,j) and the decrypted f'(i,j) image is defined. The NAE is founded:

$$NAE = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n}\left\| f_{(i,j)^2} - f'_{(i,j)^2} \right\|}{\sum_{i=1}^{m}\sum_{i=1}^{n} f_{(i,j)^2}} \tag{4.11}$$

4.2.2.9 Peak Signal-to-Noise Ratio (PSNR)

It is defined as takes the square of the peak value in the image and divide it by the Mean Square Error. The PSNR is used to measure the quality of a grayscale image after the reconstruction, PSNR is measured in decibels (dB) [73] [74]. The PSNR and MSE are calculated as:

$$PSNR = 10 * log_{10}\left(\frac{255*255}{MSE}\right)(bB) \tag{4.12}$$

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left\| I_{1(i,j)} - I_{2(i,j)} \right\|^2 \tag{4.13}$$

Here MSE is the mean error square between I2 I j) and original I1 decrypted picture (i, j). m and n represent the original picture width and height, respectively [73] [74].

4.3 EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The experimental research consists of a number of safety checks and effects, such as space analytics, mathematical analysis, numerical analysis and differential analysis. These tests are the most critical tests to prove that the proposed algorithm is secure.

4.3.1 Encryption and Decryption Time Analysis

This time for encryption and decryption can be used to measure the algorithms by way of encryption and decryption. Parameters of performance include the time taken to encode and decode input images by the algorithm. For the reason of preventing discrimination, the research has been carried out 50 times an average of the findings. Table 4.3 indicates how long and picture is machine encrypted and decrypted with different rounds.

Table 4.3: The Encryption and Decryption Execution Time with Different Rounds.

Image Name	AES only		2-rounds AES&DNA		5-rounds AES&DNA		10-rounds AES&DNA	
	ET (s.)	DT (s.)	ET (s.)	DT (s.)	ET (s.)	DT (s.)	ET (s.)	DT (s.)
Cameraman	52.029	61.8915	27.698	37.304	41.351	48.281	102.841	111.251
Lena	49.777	61.2352	26.973	39.636	42.141	50.412	99.312	112.545
Mona Lisa	49.730	62.9285	27.249	42.699	41.844	51.254	102.141	116.012
Mandrill	49.849	61.6671	25.175	37.683	43.842	51.842	99.899	109.991
Peppers	51.638	60.2609	28.234	41.344	45.221	52.332	101.916	112.225
Plane	50.412	67.7599	26.938	40.449	46.103	54.381	103.884	116.015
AVERAGE	***50.6***	***62.6***	***27***	***39.9***	***43.4***	***51.4***	***101.7***	***113***

** ET (s.) =Encryptions Time (second), DT (s.) =Decryption Time (second).*

4.3.2 Security analysis

Protection is the main challenge in any technique of encryption. All sorts of known attacks can occur under a strong encryption scheme. These attacks are built on the view, that the deterioration of the encrypted image is decreased with a mathematical model, which attempts to decrypt the cipher image without knowing the encryption key by studying the relationship between the simple image and the cypher image. Therefore, the cipher must require random properties to avoid the attacker obtaining image characteristics by the pixel [81] [82].

The protection of the proposed encryption technique is thoroughly investigated in this section. Security analyzes have been used to measure the resistance of a chiper against various types of attacks. Keyspace analyzes are used to test brute force attack resistance. Histogram, Adjacent Pixel correlation Analysis and Original and Encrypted Image Correlation Analysis are used to detect statistical attack resistance. A randomness calculation is a numerical analysis, for example entropy. Pixel Change Rate Number (NPCR) and UACI for the measure of differential attack resistance. UACI values. PSNR, MSE, SC and NAE were used to assess the achievement of the focused image quality measures implemented.

4.3.2.1 Key space Analysis

Protection is the main challenge in any technique of encryption. Most types of known attacks can occur in a good encryption framework. An analysis of main spaces is used to calculate brute-force resistance. In the proposed algorithm, the key space is equal to (2128 * 24 * 3), this exceeds the effective key size necessary to ensure computational security that expected to be secure against future brute force attacks. As well as, the DNA sequence of the key is utilized to generate the 2-extra key. This means that the adversary has to deviate from direct DNA key, instead of all the possible combinations of the hexadecimal key and the binary key. The proposed algorithm was compared with other works and the results suggest that the proposed algorithm needs (51.79340*1025) years to be broken or to be hacked. Table 4.4 shows that the proposed algorithm

is better security against brute-force- attack and needs a long time for breaking when compared with other work.

Table 4.4: Results of Decryption Breaking Time.

Technique Name	**(15) Key Length (bits)**	**Keyspace**	**Amount of Time for Breaking (years)**
AES Original	128	2^{128}	$1.078950 * 10^{25}$
H. Hennawy [93]	128	2^{128}	$1.078950 * 10^{25}$
Proposed Algorithm	132*3	$2^{128} * 2^4 * 3$	**$51.79340*10^{25}$**

4.3.2.2 Histogram Analysis

An algorithm implementation is performed to represent the encryption and decryption performance. Various images of the same dimension 256 x 256 are provided with the proposed algorithm. Illustration 4.1. Shows that cipher photo histograms are very even and substantially different from plain picture histograms, which makes it very difficult for statistical analyzes to attack an encrypted picture.

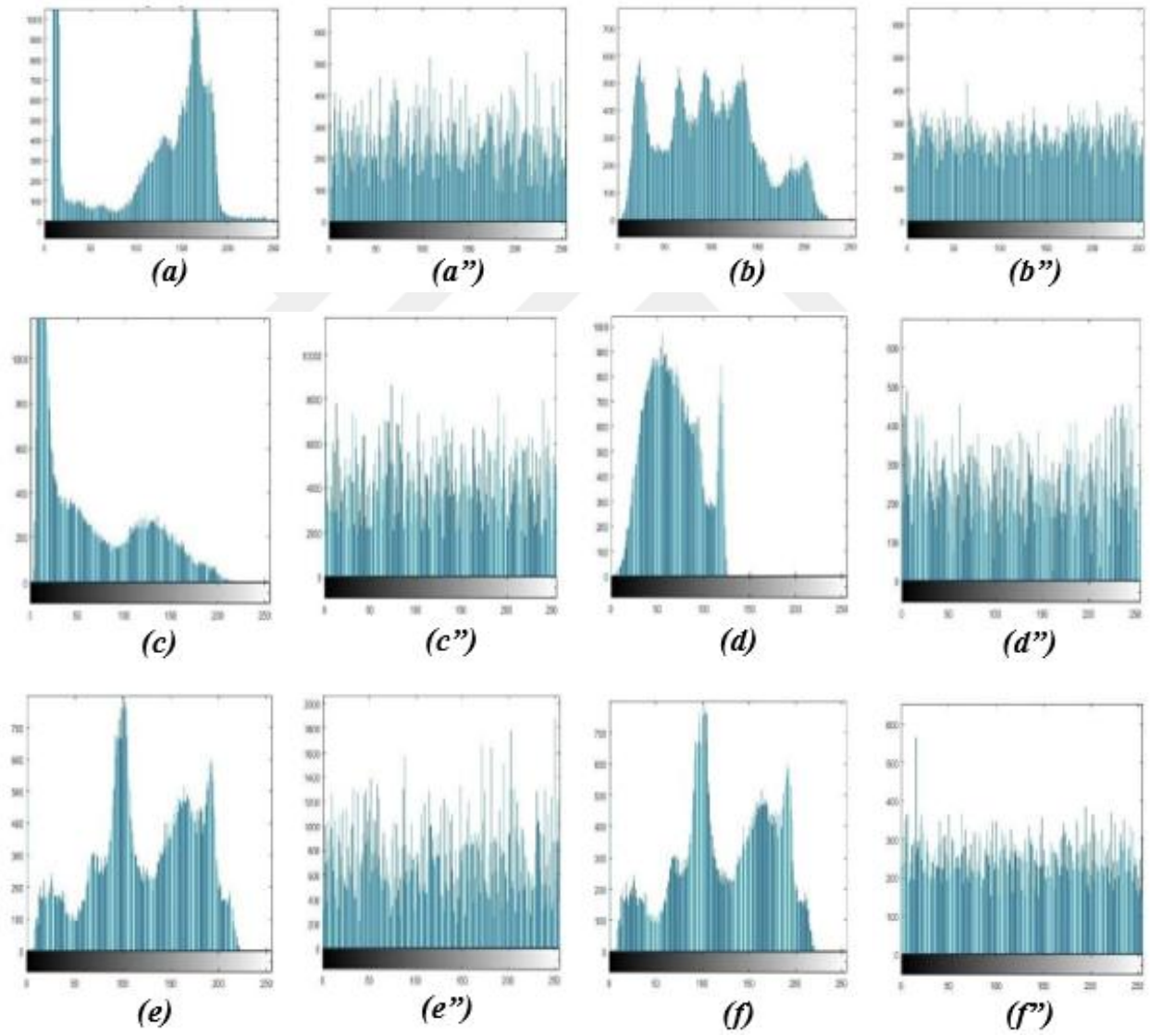


Figure 4.1: Histograms of Original and Encrypted Images Used in The Simulations

4.3.2.3 Correlation Analysis of the Adjacent Pixels

The original picture is generally considered to have a good association with its neighboring pixels. In order to resist statistical attack, it is necessary to reduce this connection in the encrypted image[84]. An powerful image cryptosystem produces a chip image with a slight association of adjacent pixels. The similarity between two contiguous pixels on the single image and the chip image is tested in order to assess the efficacy of the cryptosystem. The procedure below is performed. Second, select 5000 pairs of adjacent pixels from the original image (horizontal, vertical and diagonal) randomly. Then each pair is determined with a correlation coefficient [57]. Figure 4.2 shows a horizontal, vertical and diagonal distribution of the neighboring pixel-pairs of the single image and its chip image. Mainly near the diagonal line of the diagram are the pixel-pair of single images. Everyone is similar or has the same beliefs. Whereas pixels are altered randomly in the case of a cipher image covering the entire data range indicate that they are not interrelated. The low correlation between the pixels only renders the attacker unaffected, if the adjacent information is given by pixel pairs. The proposed algorithm can also withstand a statistical assault.

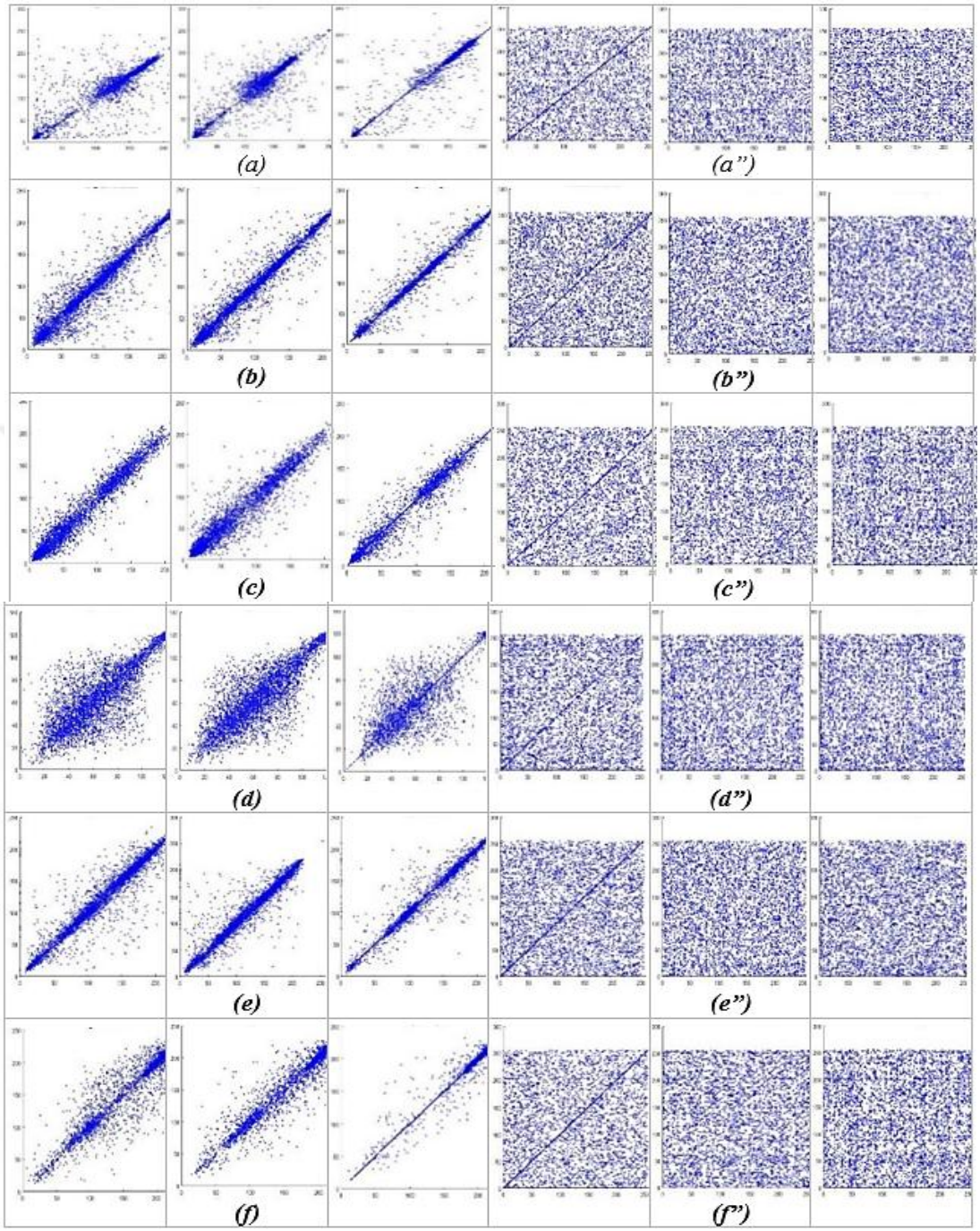


Figure 4.2: Horizontal, Vertical, and Diagonal Correlations of Original and Encrypted Images.

4.3.2.4 Correlation Analysis of Original and Encrypted Image

Table 4.5 shows the correlation distribution of the plain-images and cipher images which represent the entire plain-images and cipher-images and don't represent the selected part. The correlation coefficients values assumed to be in the range from -1 to +1, where +1 indicates the strongest possible correlation and -1 means the strongest negative correlation. However, the value of 0 means de-correlation between the compared values [70]. The images are encrypted using AES only and using 2 - rounds of AES followed results with a DNA sequence and comparison with various schemes. However, in the cipher images a distortion of the correlation among pixels has widely appeared, thus, the pixels information can't be obtained from the adjacent pixels.

Table 4.5: The Correlation of Original and Encrypted Images.

Image Name	AES Original	E. Shehab [57]	Proposed Algorithm
Camera man	0.0088	**-0.0076**	0.00225974
Lena	**-0.0036**	-0.0014	0.0122426
Mona Lisa	-0.0128	0.0046	**-0.0164441**
Mandrill	-0.0060	-0.0019	**-0.0129461**
Peppers	0.00072	**0.00039**	0.00529184
Plane	0.00042	-0.00010	**-0.00381678**
AVERAGE	***-0.002216667***	***-0.001001667***	***-0.002235467***

4.3.2.5 Information Entropy Analysis

Entropy is one of the major characteristics that defines a picture's randomness and uncertainty level and is widely used to compute a uniform pixel gray-level distribution. Entropy is around 8, so the diffusion is fine and induces high performance disorder [69] [80] [71]. Table 4.6 displays

the entropy data of the encrypted files. The results show that the entropy of cipher images closely corresponds to an optimal value that can make it clear that the cipher image of the proposed algorithm is goodly random.

Table 4.6: Results of Information Entropy of Original and Encrypted Images.

Image Name	Plain Image	J. Wu [94]	Proposed Algorithm
Cameraman	7.12563	**7.9975**	7.9973
Lena	7.33018	7.9976	**7.9997**
Mandrill	7.22307	7.9971	**7.9979**
Peppers	7.53269	**7.9974**	7.9959
Plane	6.89796	7.9970	**7.9987**
AVERAGE	***7.221906***	***7.99732***	***7.9979***

The results of the histogram analysis, the correlation among adjacent pixels, and the entropy results demonstrate that the proposed algorithm is resistant to statistical attack. These results are related to the high sensitivity of the three different keys and the high randomization of the DNA computing.

4.3.2.6 Differential Analysis Metrics

A differential attack is one of the most common block iteration cryptanalytical tools [86]. Two standard quantitative measurements are used to determine the sensitivity of the algorithm to a slight change in the plain image: the number of changes in pixel rate (NPCR) and the unified average exchange strength (UACI), which are shown in Table 4.7. Ideally, the value of NPCR in real random chips should be close to 100% and the higher UACI value is calculated to be close to 33%, as cited in [70] [85]. Average strength varies between the picture and the cipher image. The

results suggest that NPCR and UACI values are purely theoretical and thus highly resistant to differential attacks on all test images. These findings are strongly associated with the heavy algorithm confusion and diffusion.

Table 4.7: NPCR and UACI Performance of Different Schemes

Image Name	**NPCR**		**UACI**	
	J. Wu [94]	**Proposed Algorithm**	**J. Wu [94]**	**Proposed Algorithm**
Cameraman	0.9961	**0.996307**	0.3353	**0.31716**
Lena	0.9962	**0.996582**	0.3341	**0.3395**
Mandrill	0.9959	**0.997055**	0.3338	**0.31744**
Peppers	0.9960	**0.996933**	0.3349	**0.31156**
Plane	0.9962	**0.996719**	0.3363	**0.331179**
AVERAGE	***0.99608***	***0.9967192***	***0.33488***	***0.3233678***

4.3.2.7 Structural Content (SC) and Normalized Absolute Error (NAE)

A higher value of SC indicates that images are of low quality and the optimum SC is near 1 is a global measure comparing the total weight of the decryptable frame with the original image. A higher NAE value shows that image is of poor quality. Table 4.8. illustrates the good quality of the proposed algorithm.

Table 4.8: SC and NAE of The Proposed Algorithm.

Image name	SC	NAE
Camera man	1	$4.58772e^{-05}$
Lena	1.00002	0.000112941
Mona Lisa	0.999927	$4.40573e^{-06}$
Mandrill	1.00002	$5.35004e^{-05}$
Peppers	1	0
Plane	1	0
AVERAGE	0.9999945	3.61E-05

4.3.2.8 Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE)

In order to measure the encryption strength of the proposed algorithm, some quantitative metrics as PSNR and MSE are utilized to estimate the variance between the encrypted image and original image. Table 4.9. illustrates the PSNR and MSE statistical metrics result, these metrics are used to evaluate the proposed algorithm. PSNR is one of the metric parameters most commonly used. A higher PSNR value indicates that the image and decryption are of higher quality than the image. Likewise, for MSE it is extremely easy and very common to calculate distortion. The MSE value varies from the original picture to the decryption picture. The less the MSE, the better the result.

Table 4.9: PSNR and MSE of The Proposed Algorithm.

Image Name	PSNR	MSE
Camera man	47.5892	1.13281
Lena	43.4469	2.94032
Mona Lisa	42.9821	3.2724
Mandrill	45.2007	1.96341
Peppers	Inf*	0
Plane	Inf*	0
AVERAGE	***44.80473***	***1.55149***

∗ *Since the definition is PSNR=10log10(peakval^2/MSE) and the MSE is zero if the two images are identical, as we know that one over zero is infinity, and that log of infinity is also infinity.*

4.4 CONCLUSION

Protection is the main challenge in any technique of encryption. Most types of known attacks can occur with a strong encryption algorithm. The key study of space is used for calculating brute force attack resistance. The main space is equivalent to (2128*24*3) in the proposed algorithm. This exceeds the effective key size necessary to ensure computational security expected to be secure against future brute force attacks. The histograms of the cyphered images have proved to be distinctly stable and distinct from the original images, so that statistical cryptanalysis is very difficult to do with the ciphered image. The correlation coefficients values indicate that the pixel's distribution of the cipher images show a widely distortion of the correlation among pixels. Thus, the pixel's information can't be obtained from the adjacent pixels. Therefore, the proposed algorithm is strongly resistant to differential attack. These results are achieved due to the strong process of confusion and diffusion of the proposed algorithm. In order to determine the efficacy

of the focus measures introduced, PSNR, MSE, SC and NAE are used. The proposed algorithm produces substantially better performance. Different statistical tests were experimented to demonstrate resistance to classical types of attacks by the proposed algorithm.

5. CONCLUSIONS AND FUTURE WORKS

This chapter provides a summary of the thesis and results with the general concluding remarks of the findings. This chapter also lists and discusses suggestions for future work.

5.1 CONCLUSIONS

This thesis presented state of the art algorithm incorporating DNA computing in AES algorithm instead of the mix-column stage. DNA computing replaced the mix-column because DNA computing has many advantages over mix-column due to complex mathematical operations that uses more resources and take longer time to process. The proposed algorithm uses three keys offered by DNA Rules. This improves the encryption power and gives higher security and more complexity to the proposed algorithm. The required decryption breaking time is remarkably increased more than 47 times the breaking time using the original algorithm. In this context the opponents need information on hidden keys to make their selection more difficult and the algorithm proposed has enough space to resist attacks by brute forces.

By combining the concept of AES and DNA computing, successfully enhanced the encryption/decryption processes. The results showed that the proposed AES algorithm and other algorithms are obviously better than the original. The following issues are considered:

- Security is the major issue of any encryption techniques. Most types of known attacks can occur in good encryption algorithms. An analysis of main spaces is used to calculate brute-force resistance. In the proposed algorithm, the key space is equal to (2132 * 3), this exceeds the effective key size necessary to ensure computational security that expected to be secure against future brute force attacks.

- The histogram has been shown to be substantially different from the histogram of the original image and to be precisely compatible with the histogram. This means a statistical encrypted image analysis is difficult to perform.

- The correlation value of the pixel distribution of the cipher images means that there is a major distortion between the correlation between pixels. Therefore, information on the pixels of the neighboring pixels cannot be obtained. Moreover, the average correlation coefficient between the original and the encrypted images is similar to (- 0.002235467 percent) which means that the stronger resistance is the correlation.

- The average NPCR is near (0.9967192%), and the average UACI value is near (0.323678%), which means that the image is encrypted with high sensitivity towards the original photo.

- The SC average value is close to (0.9999945 %) and NAE average value is close to (3.61E-05 %), which indicate high of image quality of the proposed algorithm.

- The picture with highest PSNR value and smaller MSE values can be reconstructed in the best degraded form. For the suggested algorithm, the average PSNR and MSE values are similar to (44.80473 db) and (1.55149). These findings indicate the efficacy of the encoding power of the proposed algorithm.

The experiment results suggest that a high standard of protection, honesty, performance, and robustness is given by the proposed algorithm. The algorithm proposed meets the criteria for moving images to unsafe channels.

5.2 FUTURE WORKS

In general, the area of joint encryption is a rich area for research. The following are suggestions for research points and future work.

•To increase the speed of the encryption and decryption execution time by integrating Quantum computing concept with our proposed algorithm.

•Developing a new scheme using Bio-inspired computing that combines both of the compression and encryption.

•Apply parallel processing for the proposed scheme.

•Apply the proposed algorithm on video.

REFERENCES

[1]. S. Li, C. Li and K. Lo, “Cryptanalysis of an Image Scrambling Scheme without Bandwidth Expansion”, IEEE Transactions On Circuits And Systems For Video Technology,18(3): 338–349, 2008.

[2]. K. R. Sandeep, M. Dindayal, and A. K. Danish, "A Survey on Advanced Encryption Standard," International Journal of Science and Research, vol. 6, issue 1, pp.711-724, 2017. (DOI: 10.21275/ART20164149)

[3]. G. Manjula, and H. S. Mohan, "A Survey of Commonly Used Cryptographic Algorithms in Information Security," International Journal of Engineering and Computer Science, vol. 04, issue. 11, pp.15083-15090, 2015. (DOI:10.18535/Ijecs/v4i11.37)

[4]. L. Adleman, “Molecular Computation of Solutions to Combinatorial Problems,” Science, vol. 266, issue 5187, pp. 1021-1025, 1994. (DOI: 10.1126/science.7973651)

[5]. R. Lipton, “DNA Solution of Hard Computational Problems,” Science, vol. 268, no. 5210, pp. 542-545, 1995. (DOI: 10.1126/science.7725098)

[6]. D. Boneh, C. Dunworth, and R. Lipton, “Breaking DES using a Molecular Computer,” DNA Based Computers, pp. 37-65, 1996. (DOI: 10.1090/dimacs/027/04)

[7]. C. Taylor, V. Risca, and C. Bancroft, “Hiding Messages in DNA Microdots,” Nature Magazine, vol. 399, no. 6736, pp. 533-534, 1999. (DOI: org/10.1038/21092)

[8]. N. Chidambaram, K. Thenmozhi, A. Rengarajan, K. Vineela, S. Murali, V. Vandana, and P. Raj, “DNA Coupled Chaos for Unified Color Image Encryption - a Secure Sharing Approach,” Proceedings of the International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 759-763, India, 2018. (DOI: 10.1109/ICICCT.2018.8473288)

[9]. FIPS, PUB. “197, Advanced Encryption Standard (AES),” National Institute of Standards and Technology, U.S. Department of Commerce, 2001. (DOI: 10.6028/nist.fips.197)

[10]. P. Kumar and S. B. Rana, “Development of Modified AES Algorithm for Data Security,” Optik - International Journal for Light and Electron Optics, vol. 127, no. 4, pp. 2341- 2345, 2016. (DOI: org/10.1016/j.ijleo.2015.11.188)

[11]. M. Babaei, “A Novel Text and Image Encryption Method Based on Chaos Theory and DNA Computing,” Natural Computing, vol. 12, no. 1, pp. 101-107, 2012. (DOI: 10.1007/s11047-012-9334-9)

[12]. X. Lai, M. Lu, L. Qin, J. Han, and X. Fang, "Asymmetric Encryption and Signature Method with DNA Technology," Science China Information Sciences, vol. 53, no. 3, pp. 506-514, 2010. (DOI: 10.1007/s11432-010-0063-3)

[13]. M. Borda and O. Tornea, "DNA Secret Writing Techniques," Proceedings of the International Conference on Communications (ICCOMM), Romania, pp. 451-456, 2010. (DOI: 10.1109/iccomm.2010.5509086)

[14]. T. Mandge and V. Choudhary, "A DNA Encryption Technique Based on Matrix Manipulation and Secure Key Generation Scheme," Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES), India, pp. 47-52, 2013. (DOI: 10.1109/icices.2013.6508181)

[15]. S. Kalsi, H. Kaur, and V. Chang, "DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation," Journal of Medical Systems, vol. 42, no. 17, pp. 1-12, 2018. (DOI: 10.1007/s10916-017-0851-z)

[16]. B. Wang, Y. Xie, S. Zhou, C. Zhou, and X. Zheng, "Reversible Data Hiding Based on DNA Computing," Computational Intelligence and Neuroscience, vol. 2017, pp. 1-9, 2017. (DOI: 10.1155/2017/7276084)

[17]. M. S. Rahman, I. Khalil, and X. Yi, "A Lossless DNA Data Hiding Approach for Data Authenticity in Mobile Cloud-Based Healthcare Systems," International Journal of Information Management, 2018. (DOI: 10.1016/j.ijinfomgt.2018.08.011)

[18]. X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A Novel Color Image Encryption Scheme using DNA Permutation Based on the Lorenz System," Multimedia Tools and Applications, vol. 77, no. 5, pp. 6243-6265, 2017. (DOI: 10.1007/s11042-017-4534-z)

[19]. Z. Chen and X. Geng, "Efficient DNA Sticker Algorithms to Data Encryption Standard," Journal of Computational and Theoretical Nanoscience, vol. 7, no. 5, pp. 840-847, 2010. (DOI: 10.1166/jctn.2010.1429)

[20]. B. Wang, Y. Xie, S. Zhou, X. Zheng, and C. Zhou, "Correcting Errors in Image Encryption Based on DNA Coding," Molecules, vol. 23, no. 8, pp. 1-13, 2018. (DOI: 10.3390/molecules23081878)

[21]. J. D Watson and F. H. C. Crick, "Molecular structure of nucleic acids: a structure for De-oxy ribose Nucleic Acid", Nature, 25: 737-738, 1953.

[22]. Lister Hill National Center for Biomedical Communications, "Genetics Home Reference: Hand book", U.S. National Library of Medicine, 2015

[23]. M. Mandelkern, J.G. Elias, D. Eden and D.M. Crothers, "The Dimensions of DNA in Solution",Journal of Molecular Biology,152(1): 153–61, 1981.

[24]. U. Somani, K. Lakhani, and M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,"Proceedings of the International Conference on Parallel, Distributed and Grid Computing (PDGC), India, pp. 211-216., 2010. (DOI: 10.1109/PDGC.2010.5679895)

[25]. A.P. Thiruthuvadoss, "Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography," M.Sc. Thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology (ICT), Communication Systems (CoS), Sweden, Stockholm, 2013.

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-120103

[26]. B. B. Raj and V. C. Sharmila, "A Survey on DNA Based Cryptography," Proceedings of the International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR), IEEE Conference, India, pp. 1-3, 2018. (DOI: 10.1109/ICETIETR.2018.8529075)

[27]. S. Jain and V. Bhatnagar, "Analogy of Various DNA Based Security Algorithms using Cryptography and Steganography," Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICICT), IEEE Conference, India, pp. 285- 291, 2014. (DOI: 10.1109/icicict.2014.6781294)

[28]. L. Ma and W. Jin, "Symmetric and Asymmetric Hybrid Cryptosystem Based on Compressive Sensing and Computer-Generated Holography," Optics Communications, vol. 407, pp. 51-56, 2018. (DOI: 10.1016/j.optcom.2017.08.047)

[29]. O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, vol. 8, no. 7, pp. 495-516, 2018. (DOI: 10.29322/ijsrp.8.7.2018.p7978)

[30]. D. Suneetha, and, R. Kiran Kumar, "Enhancement of Security for Cloud Data Using Partition-Based Steganography," Proceedings of the 2nd International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing, vol 828, pp. 201-209, 2018. (DOI: 10.1007/978-981-13-1610-4_21)

[31]. S. M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, "Novel Hybrid Encryption Algorithm Based on AES, RSA, and Twofish for Bluetooth Encryption," Journal of Information Security, vol. 09, no. 02, pp. 168-176, 2018. (DOI: 10.4236/jis.2018.92012)

[32]. C. Taylor, V. Risca and C. Bancroft, "Hiding messages in DNA Microdots", Nature, 399: 533-534, 1999.

[33]. A. Gehani, T. LaBean and J. Reif, "DNA Based Cryptography", DIMACS Series in Discrete Mathematics and Theoretical Computer Science. 54: 233-249, 2000.

[34]. A. Leier, C. Richter, W. Banzhaf, H. Rauhe, "Cryptography with DNA Binary Strands",BioSystems, 57(1): 13-22, 2000

[35]. J. Chen, "A DNA-based Biomolecular Cryptography Design", IEEE International Symposium on Circuits and Systems, 822–825, 2003

[36]. T. Kazuo, O. Akimitsu and S. Isao, "Public-key system using DNA as a One - Way Function for Key Distribution", BioSystems, 81(1), 25–29, 2005

[37]. G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology", Computer Engineering and Applications, 42: 29–32, 2006.

[38]. R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt and A. Uhl, "Confidential Storage and Transmission of Medical Image Data", Computers in Biology and Medicine, 33: 273 – 292, 2003.

[39]. E.B. Monica, O. Tornea and T.Hodorogea, "Secret Writing by DNA Hybridization", Acta Technica Napocensis Electronics and Telecommunications, 50(2): 21-24, 2009

[40]. S. Sadeg, "An Encryption Algorithm Inspired from DNA", IEEE International Conference on Machine and Web Intelligence, 344 – 349, 2010.

[41]. G. Qinghai, "Biological Alphabets and DNA based Cryptography", http://www.asee.org/documents/sections/middle-atlantic/spring-2010/Biological-Alphabets-and-DNA-based-cryptography.pdf, 2010.

[42]. L. XueJia, L. MingXin, Q. Lei, H. JunSong and F. XiWen, "Asymmetric Encryption and Signature method with DNA Technology", Information Sciences, 53: 506–514, 2010.

[43]. Z. Qiang, X. Xue and X. Wei, "A Novel Image Encryption Algorithm based on DNA Subsequence Operation", The Scientific World Journal, 2012.

[44]. Z. Qiang, L. Guo and X. Wei, "Image Encryption using DNA addition combining with Chaotic Maps", Mathematical and Computer Modelling, 52: 2028-2035, 2010

[45]. R.Soni, G.Prajapati, A.Khan and D.Kulhare, "Triple Stage DNA Cryptography Using Sequential Machine", International Journal of Advanced Research in Computer Science and Software Engineering. 3(8): 859-867, 2013.

[46]. R.H. Ranalkar and B.D.Phulpagar, "DNA based Cryptography in Multi-Cloud: Security Strategy and Analysis", International Journal of Emerging Trends and Technology in Computer Science, 3(2): 189 – 192, 2014.

[47]. E. Shehab, A. K. Farag, and, A. Keshk, "An Image Encryption Technique Based on DNA Encoding and Round-Reduced AES Block Cipher," International Journal of Computer Applications, vol. 107 no. 20, pp.1-6, 2014. (DOI: 10.5120/18864-0543).

[48]. P. Deshmukh, and, V. Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption," Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES), IEEE Conference, Chennai, India, pp. 1-5, 2014. (DOI: 10.1109/icices.2014.7033928)

[49]. S. M. Wadi, and, N. Zainal, "High Definition Image Encryption Algorithm Based on AES Modification," Wireless Personal Communications, vol. 79, no. 2, pp. 811-829, 2014. (DOI: 10.1007/s11277-014-1888-7)

[50]. V. S. Mahalle, and, A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (RSA &AMP, AES) Encryption Algorithm," Proceedings of the International Conference on Power, Automation and Communication (INPAC), IEEE Conference, Amravati, India, pp. 146-149, 2014. (DOI: 10.1109/inpac.2014.6981152)

[51]. P. Kumar, and, S. B. Rana, "Development of Modified AES Algorithm for Data Security," Optik - International Journal for Light and Electron Optics, vol. 127, no. 4, pp. 2341-2345, 2016. (DOI: 10.1016/j.ijleo.2015.11.188)

[52]. S. S. H. Shah, and, G. Raja, "FPGA Implementation of Chaotic Based AES Image Encryption Algorithm," Proceedings of the International Conference on Signal and Image Processing Applications (ICSIPA), IEEE Conference, Kuala Lumpur, Malaysia, pp. 574-577, 2015. (DOI: 10.1109/icsipa.2015.7412256)

[53]. Q. Zhang, and, Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," Proceedings of the 5th International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), IEEE Conference, China, pp. 1218-1221, 2015. (DOI: 10.1109/imccc.2015.261)

[54]. A. Dandekar, S. Pradhan, and, S. Ghormade, "Design of AES-512 Algorithm for Communication Network," International Research Journal of Engineering and Technology, vol. 3, no. 5, pp. 438-443, 2016.

[55]. M. K. Aery, "String Encryption Technique with Modified AES Encryption," International Journal of Advanced Computing and Electronics Technology, vol. 3, no. 1, pp.13-25, 2016. (http://troindia.in/journal/ijacet/vol3iss1/13-25.pdf)

[56]. G. Yogeswari, and, P. Eswaran, “Enhancing Data Security for Cloud Environment Based on AES Algorithm and Steganography Technique,” International Journal of Advanced Research Trends in Engineering and Technology, vol. 3, no. 20, pp. 233-236, 2016. (https://ijartet.com/1907/v3s20alagappa/conference)

[57]. V. Hoang, T. Phan, V. Dao, and, C. Pham, “A Compact, Ultra-Low Power AES-CCM IP Core for Wireless Body Area Networks,” Proceedings of IFIP/IEEE International Conference on Very Large-Scale Integration (VLSI-SoC), IEEE Conference, Tallinn, Estonia, pp.1-4, 2016. (DOI: 10.1109/vlsi-soc.2016.7753566)

[58]. S. Panghal, S. Kumar, and, N. Kumar, “Enhanced Security of Data using Image Steganography and AES Encryption Technique,” International Journal of Computer Applications, 2016. (https://pdfs.semanticscholar.org/f9ce/755c34e6e933755e2bac0630197ac25ebe0e.p df)

[59]. X. Yang, and, W. Wen, “Design of a Pre-scheduled Data Bus for Advanced Encryption Standard Encrypted System-on-Chips,” Proceedings of the 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE Conference, Chiba, Japan, pp. 506 - 511, 2017. (DOI: 10.1109/aspdac.2017.7858373)

[60]. A. Ibrahim, and, G. Dalkılıç, “An Advanced Encryption Standard Powered Mutual Authentication Protocol Based on Elliptic Curve Cryptography for RFID, Proven on WISP,” Journal of Sensors, vol. 2017, pp. 1-10, 2017. (DOI: 10.1155/2017/2367312)

[61]. B. M. Krishna, G. L. Habibulla, B. Lohitha, E. Bhavitha, P. T. Sri, and, B. A. Kumar, “FPGA Implementation of DNA Based AES Algorithm for Cryptography Applications,” International Journal of Pure and Applied Mathematics, vol. 115, no. 7, pp. 525-530, 2017. (https://acadpubl.eu/jsi/2017-115-6-7/articles/7/81.pdf)

[62]. B. P. Alapatt, “An Enhanced Advanced Encryption Standard (EAES) Algorithm for Secure Fiber Optic Communication,” International Journal of Advanced Research in Computer Science, vol. 9, no. 1, pp. 167-171, 2018. (DOI: 10.26483/ijarcs.v9i1.5285)

[63]. A. Moschos, G. Papadimitriou, and, P. Nicopolitidis, “Proactive Encryption of Personal Area Networks and Small Office-Home Office Networks Under Advanced Encryption Standard Application,” Security and Privacy, vol. 1, no. 1, pp. 1-8, 2018. (DOI: 10.1002/spy2.10)

[64]. M. M. Wong, M. L. Wong, C. Zhang, and, I. Hijazin, “Circuit and System Design for Optimal Lightweight AES Encryption on FPGA,” IAENG International Journal of Computer Science, vol. 45, no. 1, pp. 1-11, 2018. (http://www.iaeng.org/IJCS/issues_v45/issue_1/IJCS_45_1_10.pdf)

[65]. S. Sharma, M. Kantak, and, N. Vernekar, “Novel Approach to Image Encryption: Using a Combination of JEX Encoding-Decoding with the Modified AES Algorithm,” Information and Communication Technology for Sustainable Development. Springer, Singapore, pp.201-210, 2018. (DOI: 10.1007/978-981-10-3932-4_21)

[66]. S. Kalsi, H. Kaur, and, V. Chang, “DNA Cryptography and Deep Learning Using Genetic Algorithm with NW algorithm for Key Generation,” Journal of Medical Systems, vol. 42, no. 17, pp. 1-12, 2018. (DOI: 10.1007/s10916-017-0851-z)

[67]. http://sipi.usc.edu/database/?volume:misc (Last Visit 20 Nov. 2018)

[68]. R. Enayatifar, F. G. Guimarães, and P. Siarry, “Index-based permutation-diffusion in multiple-image encryption using DNA sequence,” Optics and Lasers in Engineering, vol. 115, pp. 131-140, 2019. (DOI: 10.1016/j.optlaseng.2018.11.017)

[69]. X. Tong, M. Zhang, Z. Wang, and, J. MA, “A Joint Color Image Encryption and Compression Scheme Based on Hyper-Chaotic System”, Nonlinear Dynamics, vol. 84, no.4, pp. 2333-2356, 2016. (DOI: 10.1007/s11071-016-2648-x)

[70]. M. Escobar, C. Hernández, F. Abundiz, R. Gutiérrez, and, O. Campo, “A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos,” Signal Processing, vol. 109, pp. 119-131, 2015. (DOI: 10.1016/j.sigpro.2014.10.033)

[71]. R. Enayatifar, A. Abdullah, I. Isnin, A. Altameem, and, M. Lee, “Image Encryption using A Synchronous Permutation - Diffusion Technique”, Optics and Lasers in Engineering, vol. 90, pp. 146-154, 2017. (DOI: 10.1016/j.optlaseng.2016.10.006)

[72]. N. Nandy, D. Banerjee, and, C. Pradhan, “Color Image Encryption Using DNA Based Cryptography,” International Journal of Information Technology, pp. 1-8, 2018. (DOI: 10.1007/s41870-018-0100-9)

[73]. M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, A. N, and, A. Farouk, “Secure Medical Data Transmission Model for IOT - Based Healthcare Systems,” IEEE Access, vol. 6, pp. 20596-20608, 2018. (DOI: 10.1109

/access.2018.2817615)

[74]. N. Taeyoung, and, K. Munchurl, “A Novel No-Reference PSNR Estimation Method with Regard to Deblocking Filtering Effect in H.264/AVC Bitstreams,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 2, pp. 320-330, 2014. (DOI: 10.1109/tcsvt.2013.2255425)

[75]. D. M. Wang, L. S. Wang, Y. Y. Guo, Y. C. Wang, and A. B. Wang, “Key Space Enhancement of Optical Chaos Secure Communication: Chirped FBG Feedback

Semiconductor Laser," Optics Express, vol. 27, no. 3, p. 3065, 2019. (DOI: 10.1364/OE.27.003065)

[76]. M. Hamdi, R. Rhouma, and, S. Belghith, "A Selective Encryption-Encryption of Images Based on SPIHT Coding and Chirikov Standard Map", Signal Processing, vol. 131, pp. 514-526, 2016. (DOI: 10.1016/j.sigpro.2016.09.011)

[77]. G. Alvarez, and, S. Li, "Cryptanalyzing a Nonlinear Chaotic Algorithm (NCA) for Image Encryption", Communications in Nonlinear Science and Numerical Simulation, vol. 14, no. 11, pp. 3743-3749, 2009. (DOI: 10.1016/j.cnsns.2009.02.033)

[78]. M. Zhang, and, X. Tong, "Joint Image Encryption and Compression Scheme Based on IWT and SPIHT", Optics and Lasers in Engineering, vol. 90, pp. 254-274, 2017. (DOI: 10.1016/j.optlaseng.2016.10.025)

[79]. K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and, M. Sajjad, "CISSKA-LSB: Color Image Steganography using Stego Key-Directed Adaptive LSB Substitution Method," Multimedia Tools and Applications, vol. 76, no. 6, pp. 8597-8626, 2016. (DOI: 10.1007/s11042-016-3383-5)

[80]. T. Xiang, K. Wong, and, X. Liao, "Selective Image Encryption using A Spatiotemporal Chaotic System", Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, no. 2, pp. 1-13, 2007. (DOI: 10.1063/1.2728112)

[81]. Q. Zhang, X. Xue, and, X. Wei, "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation," The Scientific World Journal, vol. 2012, pp. 1-10, 2012. (DOI: 10.1100/2012/286741)

[82]. P. Li, and, K. T. Lo, "Joint Image Compression and Encryption Based on Alternating Transforms with Quality Control", Proceedings of the International Conference of Visual Communications and Image Processing (VCIP), IEEE Conference, Singapore, Singapore, pp. 1-4, 2015. (DOI: 10.1109/VCIP.2015.7457867)