Deep Learning and DNA Cryptography based Image Encryption Scheme

Session: BSc. Spring 2023

Project Supervisor: Engr Muhammad Shahzad

Submitted By

[Saba Akhtar]
[Sawaira Iqbal]

Department of Electrical Engineering

HITEC University Taxila Cantt, Pakistan

Declaration

We, hereby declare that this project neither as a whole nor as a part there of has been copied out from any source. It is further declared that we have developed this project and the accompanied report entirely on the basis of our personal efforts made under the sincere guidance of our supervisor. No portion of the work presented in this report has been submitted in the support of any other degree or qualification of this or any other University or Institute of learning, if found we shall stand responsible.

Signature: _____

Name: Saba Akhtar

Signature: _____

Name: Sawaira Iqbal

HITEC University Taxila Cantt, Pakistan

Spring 2023

Certification

This is to certify that Saba Akhtar 19-EE(P)-003 and Sawaira Iqbal 19-EE(P)-081 have successfully completed the final project **Deep Learning and DNA Cryptography based Image Encryption Scheme,** at the HITEC University Taxila Cantt, Pakistan, to fulfill the partial requirement of the degree **B.S. Electrical Engineering.**

_____

(Engr. Muhammad Shahbaz Khan)

Lecturer

_____

(Dr. Muhammad Ali Mughal)

Chairperson-EED

HITEC University Taxila

Sustainable Development Goals

SDG No	Description of SDG	SDG No	Description of SDG
SDG 1	No Poverty	**SDG 9**	Industry, Innovation, and Infrastructure
SDG 2	Zero Hunger	SDG 10	Reduced Inequalities
SDG 3	Good Health and Well Being	SDG 11	Sustainable Cities and Communities
SDG 4	Quality Education	SDG 12	Responsible Consumption and Production
SDG 5	Gender Equality	SDG 13	Climate Change
SDG 6	Clean Water and Sanitation	SDG 14	Life Below Water
SDG 7	Affordable and Clean Energy	SDG 15	Life on Land
SDG 8	Decent Work and Economic Growth	SDG 16	Peace, Justice and Strong Institutions
		SDG 17	Partnerships for the Goals

Range of Complex Problem Solving			
	Attribute	**Complex Problem**	
1	Range of conflicting requirements	Involve wide-ranging or conflicting technical, engineering and other issues.	
2	Depth of analysis required	Have no obvious solution and require abstract thinking, originality in analysis to formulate suitable models.	
3	Depth of knowledge required	Require research-based knowledge much of which is at, or informed by, the forefront of the professional discipline and which allows a fundamentals-based, first principles analytical approach.	
4	Familiarity of issues	Involve infrequently encountered issues	
5	Extent of applicable codes	Are outside problems encompassed by standards and codes of practice for professional engineering	
6	Extent of stakeholder involvement and level of conflicting requirements	Involve diverse groups of stakeholders with widely varying needs.	
7	Consequences	Have significant consequences in a range of contexts.	
8	Interdependence	Are high level problems including many component parts or sub-problems	
Range of Complex Problem Activities			
	Attribute	**Complex Activities**	
1	Range of resources	Involve the use of diverse resources (and for this purpose, resources include people, money, equipment, materials, information and technologies).	
2	Level of interaction	Require resolution of significant problems arising from interactions between wide ranging and conflicting technical, engineering or other issues.	
3	Innovation	Involve creative use of engineering principles and research-based knowledge in novel ways.	
4	Consequences to society and the environment	Have significant consequences in a range of contexts, characterized by difficulty of prediction and mitigation.	
5	Familiarity	Can extend beyond previous experiences by applying principles-based approaches.	

Abstract

In the period of digital communication, securing sensitive data has become a critical concern. As the volume and importance of digital images continue to nurture, the need for robust and efficient image encryption schemes has become necessary. This project proposes a novel image encryption scheme that combines the power of deep learning and DNA cryptography to provide boosted security and confidentiality.

The proposed scheme influences the advancements in deep learning algorithms, specifically convolutional neural networks (CNNs), to extract convoluted features from the input image. This project presents an image encryption scheme combining deep learning, DNA cryptography, and various techniques like logistic map, bit XOR, S-box substitution, and DNA encoding to achieve sequence confusion and diffusion. The scheme utilizes chaotic sequences generated by the logistic map for encryption keys, employs bit XOR and S-box substitution for confusion, and DNA encoding for data conversion.

To assess the proposed scheme's performance, extensive experiments were conducted on a diverse set of digital images. The results validate that the scheme achieves more security and robustness against common cryptographic attacks, including statistical analysis etc. Additionally, the scheme exhibits excellent confrontation to image quality degradation and noise interference.

The combination of deep learning and DNA cryptography presents a unique and effective approach to image encryption, offering enhanced security, complexity, and performance.

This research contributes to the field of information security by introducing an inventive image encryption scheme that addresses the challenges impersonated by the increasing demand for secure image communication in various domains, including military, healthcare, and financial sectors.

Keywords: Deep learning, DNA cryptography, image encryption, convolutional neural networks, security, confidentiality.

Undertaking

I certify that the project **Deep Learning and DNA Cryptography based Image Encryption Scheme** is our own work. The work has not, in whole or in part, been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged/ referred.

[Saba Akhtar]

[19-EE-003]

[Sawaira Iqbal]

[19-EE-081]

TABLE OF CONTENTS

List of Figures

List of Tables

List of Acronyms

DNA	Deoxyribonucleic Acid
CNN	Convolutional Neural Network
XOR	Exclusive OR
S-BOX	Substitution Box
2D-RT	Two-Dimensional Rectangular Transform
SHA	Secure Hash Algorithm
PSNR	Peak Signal-to-Noise Ratio
NCC	Noncommutative Cryptography
PWLCM	Piecewise Linear Chaotic Map
mt DNA	Mitochondrial Deoxyribonucleic Acid
DNASLS	Deoxyribonucleic Acid Strands Level Scrambling
ILM	Intertwining Logistic Map
MSB	Most Significant Bit
LSB	Least significant Bit
DE	Differential Evolution
GA	Genetic Algorithm
CC	Correlation Coefficient
MD5	Message Direct Algorithm
LLSS	Logistic Logistic Sine Sine
LFI	Light Field Image
UACI	Unified Averaged Changed Intensity

IOT	Internet Of Things
MATLAB	Matrix Laboratory

Chapter One

1 INTRODUCTION

1.1 Background

Image encoding references to the process of transforming a digital image into a coded or scrambled form to defend its content from unlawful access. It encompasses applying mathematical algorithms and techniques to alter the pixel values of an image in such a way that it becomes incomprehensible and unintelligible without the rigorous decryption key. The key goal of image encryption is to certify the privacy and integrity of sensitive images during storage, transmission, or sharing. By encrypting an image, only authorized individuals with the correct decryption key can inverse the encryption process and access the original image [1].

Image encryption is an acute requirement in today's digital age for various reasons. Firstly, it makes sure the confidentiality of sensitive images, shielding them from unauthorized access. By scrambling the image data, it becomes unreadable to anyone without the appropriate decryption key. Secondly, image encryption maintains privacy by preventing unauthorized individuals or entities from observing personal or sensitive images, mainly when they are stored in the cloud or transmitted over networks. Besides, image encryption plays a vital role in protecting logical property rights, preventing unauthorized copying or modification of copyrighted images. Moreover, it ensures safe communication by preventing intervention or overhearing on transmitted images. Lastly, image encryption helps preserve data integrity by detecting and preventing unauthorized modifications or interfering. Overall, image encryption is essential for preserving confidentiality, privacy, intellectual property, and ensuring the secure transmission and integrity of digital images [1]-[2].

Securing images involves implementing various measures to guard them from unauthorized access and ensure their reliability. Firstly, encryption techniques can be employed to

scramble the image data, making it unreadable without the exact decryption key. Additionally, access controls such as tough passwords or biometric authentication can be applied to limit access to images. Regular backups and data redundancy help protect against data loss. Water marking and digital initials can be used to verify the validity and integrity of images. Using secure communication rules and storing images on encrypted storage media are also essential. Finally, keeping software and devices up to date with the latest security patches helps avoid susceptibilities that can be exploited.
Image encryption offers numerous advantages. It safeguards the confidentiality of sensitive images, guards' privacy by restricting unofficial access, safeguards cerebral property rights, prevents unauthorized copying or alteration, and sustains data integrity. It offers a secure means of transmitting and keeping images, ensuring they stay protected from interference and damaging [3].

Image encryption techniques incorporate various methods for securing digital imageries. Symmetrical encoding consumes a single key aimed at both encoding and decoding, while asymmetric encryption employs a pair of keys. Chaotic encryption utilizes chaotic systems to produce encryption keys for introducing arbitrariness. Visual cryptography divides images into shares, enlightening partial information. Transform domain encryption performs encryption in transformed domains such as frequency or wavelet domains. DNA image encryption is a cryptographic technique that employs the properties of DNA molecules, such as parallelism and storage capacity, to encrypt and guard the privacy of digital images [4].

Chaos-based image encryption is a technique that exploits chaotic systems, such as logistic maps or Lorenz systems, to create encryption keys and introduce haphazardness and misperception in the encryption process for securing digital images. Chaotic maps are mathematical functions that reveal chaotic behavior, described by sensitivity to initial conditions and the generation of seemingly random and unpredictable sequences. Examples include the logistic map, Hénon map, and Lorenz system. Chaotic maps are used in various solicitations, including encryption, data compression, and random number generation [3]-[4].

Conjoining chaos encryption with DNA encryption offers higher security and toughness. Chaos encryption familiarizes randomness and confusion, while DNA encryption uses the

parallelism and storage capacity of DNA molecules, providing a unique and powerful approach to image encryption [4].

DNA cryptography has appeared as a mesmerizing field that discovers the use of DNA molecules for protected image encryption. This advanced approach takes benefit of the exceptional properties of DNA to deliver robust encryption schemes. The digital image is encoded into an equivalent DNA sequence using a definite algorithm. Each pixel value in the image is plotted to a specific combination of DNA bases (adenine, cytosine, guanine, and thymine). This mapping creates a DNA sequence that signifies the image data [5].

To encrypt the image, various cryptographic operations are applied to the DNA sequence. These operations include substitution, permutation, and diffusion, which are performed based on an encryption key. Substitution involves replacing DNA bases or subsequences with other bases or subsequences according to the encryption key. Permutation rearranges the order of the DNA bases or subsequences, while diffusion ensures that changes in the input DNA sequence propagate throughout, making it difficult to extract meaningful information from localized portions [4]-[5].

The encrypted DNA sequence can then be securely transmitted or stored. To decrypt the image, the reverse operations are applied using a decryption key. This allows the original image to be recovered from the encrypted DNA sequence.

DNA-based image encryption schemes offer several advantages. Firstly, DNA has an incredibly high information density, enabling large amounts of data to be stored in a compact form. Additionally, DNA possesses inherent error correction mechanisms, which enhance the reliability and robustness of the encryption scheme. Furthermore, DNA-based encryption is resistant to various types of attacks, including brute force and statistical attacks, due to the complexity of the encryption algorithms and the vast search space of DNA sequences [6].

However, there are challenges associated with DNA-based image encryption schemes. Implementing the complex encryption and decryption algorithms can be computationally demanding. Moreover, the synthesis and sequencing processes involved in working with DNA introduce errors and noise, which can affect the accuracy of the encryption scheme. Additionally, the cost associated with DNA synthesis and sequencing is currently high, limiting the widespread practical adoption of this technology.

In conclusion, DNA-based image encryption schemes leverage the unique properties of DNA molecules to provide secure encryption for images. Despite challenges in implementation and cost, ongoing research and advancements in DNA synthesis and sequencing technologies hold promise for further development and practical applications of DNA cryptography in image encryption. Such advancements have the potential to revolutionize the field of secure data transmission and storage.

1.1.1 AI Tools

DNA-based image encryption involves converting digital images into DNA sequences for secure storage and transmission. MATLAB, a popular programming environment, can be utilized alongside AI techniques to facilitate various aspects of this process, from image preprocessing to DNA sequence generation and error correction.

Image Preprocessing: MATLAB offers a range of image processing functions that can be used to preprocess images before encryption. AI tools like convolutional neural networks (CNNs) can aid in tasks such as image denoising, enhancing contrast, and edge detection. These preprocessing steps can help improve the quality of the encrypted image and enhance the accuracy of subsequent DNA sequence generation.

Feature Extraction: AI algorithms, including CNNs and autoencoders, can be employed to extract relevant features from images. These features can be encoded into DNA sequences more efficiently, optimizing storage capacity and encryption quality. MATLAB's deep learning toolbox facilitates the design and training of such AI models for feature extraction.

DNA Sequence Generation: AI-driven algorithms can determine the most suitable DNA sequences for encoding image data. Genetic algorithms, for instance, can optimize DNA sequence selection based on properties such as GC content, codon usage, and minimizing potential hybridization. MATLAB's optimization toolbox can be utilized to implement and fine-tune these algorithms.

Data Encoding: MATLAB's ability to manipulate strings and perform complex computations is instrumental in converting extracted image features into DNA sequences. AI can aid in developing encoding strategies by mapping digital values to nucleotide bases in a way that preserves essential information while accommodating DNA's constraints.

Error Correction: DNA sequences are susceptible to errors during reading and synthesis due to factors like noise and experimental variations. AI models like recurrent neural networks (RNNs) can predict and correct errors, enhancing the reliability of DNA data retrieval. MATLAB's machine learning and deep learning capabilities enable the training and deployment of error-correction models.

Hybridization Analysis: AI can help predict the potential hybridization between DNA sequences, which is essential for ensuring accurate and efficient data retrieval. MATLAB can simulate DNA hybridization reactions, aiding in the design of encoding schemes that minimize cross-hybridization and improve overall security.

Decoding and Reconstruction: AI techniques, including pattern recognition and neural networks, can be employed to convert retrieved DNA sequences back into image data. These models can learn the mapping between DNA sequences and image features, allowing for accurate image reconstruction. MATLAB's machine learning tools enable the development and training of such models.

Security Analysis: AI-driven simulations and analyses can assess the security of the DNA-based image encryption scheme. MATLAB can assist in modeling potential attacks and evaluating the robustness of the encryption method against various threats, enhancing overall security.

In conclusion, MATLAB, coupled with AI tools, provides a comprehensive environment for developing DNA-based image encryption solutions. The combination of image preprocessing, feature extraction, DNA sequence generation, error correction, hybridization analysis, and decoding using AI models within MATLAB enables the creation of robust, efficient, and secure DNA-based image encryption techniques. This interdisciplinary approach merges biotechnology, cryptography, and AI to open up new possibilities for secure data storage and transmission.

1.2 Problem Statement

Due to advancements in network communication, the Internet of Things (IoT), telemedicine, online biometric systems, and social media, a large number of digital images are transmitted over the Internet. Transmission of digital, multimedia images and image encryption in IOT network is not secure. To secure them, we need enhanced image encryption scheme.

1.3 Proposed Solution

Recently, DNA encryption is considered most preferable and cyber-attack proof technique.

1.4 Aims

The main aim of DNA-based image encryption is to harness the unique properties of DNA molecules to develop a highly secure and efficient method for encrypting digital images. By encoding image data into DNA sequences, leveraging the vast information storage capacity and inherent biochemical stability of DNA, researchers aim to create a novel encryption technique that offers enhanced security against modern cryptographic attacks.

1.5 Objectives

The main objective was to develop a DNA-based image encryption scheme, specifically for HD-colored images that should not only be highly secure but should also address the latency issues faced during the encryption and transmission processes.

1.6 Report Organization

The description is dispersed in the subsequent means.

Chapter 1: This section demonstrates the introduction of DNA Cryptography, AI tools, Problem statement, Proposed solution, Aims, and objectives.

Chapter 2: This section grants the literature review, which comprises the impression from dissimilar periodicals on Deep Learning and DNA Cryptography based Image Encryption Scheme. Research gap is also discussed.

Chapter 3: In this chapter we have established the methodology, the flow scheme for the work.

Chapter 4: This chapter presents results of the scheme and from the outcomes it is concluded that the proposed scheme is very good.

Chapter 5: This chapter represents the conclusion and future work of proposed scheme.

Chapter 6: This chapter illustrates the impact of proposed scheme (Deep Learning and DNA Cryptography based Image Encryption Scheme) on society.

Chapter Two

2 LITERATURE SURVEY

The sanctuary of an image encoding system by Hénon-Sine map and DNA arbitrary coding is assessed in [7]. Moreover, Substitution boxes are primarily presented in [7], to homogenously combine the encryption properties of DNA arbitrary coding and XOR procedures. Specifics of the substitution boxes and permutation vector are stared as corresponding encryption components. Inclusive cryptanalysis is directed, built on which a selected-plaintext attack is step-by-step defined and experimentally confirmed in [7].

An image encryption scheme constructed on the hyper chaotic coordination and creation of a 5D continuous hyper chaotic system is proposed in [8], which accepts DNA dynamic coding contrivance and conventional encrypting dispersal encoding assembly. The anticipated algorithm in [8] contains two phases: scrambling phase and two rounds of diffusion phase. The presented scheme not only has the returns of "scrambling substitution" structure procedure but also overwhelms the trouble of key organization in "one time pad" scrambling order and can outbreak selected-plaintext attack. The presented image encoding procedure has the subsequent three benefits:

(1) In the dispersion phase, the vibrant directions of DNA encryption (decryption) are assumed, so the key tributaries used to encode diverse images are altered and the processes can fight the attack of selected plaintext (ciphertext).

(2) The procedure has the outcome of "one time pad" but the decipher key is only the preliminary value of the chaotic scheme, which overwhelms the trouble of key organization in the "one time pad" scrambling scheme (the key used to encode changed plaintexts is altered).

(3) Due to the two round dispersal contrivance, the procedure is extremely subtle to basic image. Tentative outcomes and speculative study in [8] have shown that this system can

fight distinction attack, brute-force attack, arithmetic attack and selected-plaintext attack. Thus, the presented procedure in [8] has unusually great sanctuary.

An image encoding scheme built on Secure Hash Algorithm-512 (SHA-512) having the assembly of two sequences of variation and dispersal is estimated in [9], by using two chaotic schemes, vibrant DNA encoding, DNA sequencing processes, and provisional shifting. Also, a 2D rectangular transform (2D-RT) on the transformation is employed in [9]. Moreover, four-wing chaotic systems and Lorentz systems is proposed in [9], to cause chaotic orders and reconnect three channel milieus and chaotic milieus with irregular constraints. Furthermore, the initial standards are employed in [9], to make the chaotic orders and the chaotic matrices for the building of the DNA coding rule matrices. Also, the novel chaotic matrices were created, and the recurrent constraints were used in [9], to build the DNA deciphering rule matrices, assembly all the DNA deciphering rules found by the plain image. Besides, the eighth alternating constraints were used to decay the coded images and encoded chaotic matrices, and in the second round of transformation–dispersion, conditional shifting on the decayed images and execution of the XOR calculation with the disintegrated chaotic matrices is projected in [9], to get the ultimate encrypted image. Incentive results and security analysis demonstrated that the proposed scheme in [9], was safe and adept of counterattacking several kinds of attacks, and formed suitable stimulus consequences on image encoding and image decoding.

An innovative highly competent image encryption and steganography procedure are accessible in [10]. The anticipated technique in [10], practices hybrid DNA encoding and Choquet's Fuzzy Integral arrangements. Firstly, a jumbled kind of the image, consuming a simple chaotic map, is programmed by DNA's bases. Four programmed images are engendered by the DNA bases, namely AT, CG, GC, and TA. Then, the resultant four DNA orders are used to verbose the four DNA encoded images using the matching DNA XOR rule, according to firm control code. Also, the wavelet fusion procedure is then used to rage the resulting four fuzzy-DNA encoded images, to get the scrambled image. A new method is used in [10], for security. The outcomes evidence the strength of the procedure in contrast to many kinds of attacks. Also, the steganography test showed that invisible scrambled images are almost unseen at high PSNR and have upright NCC values under altered sorts of attacks. The toughness of the projected process in [10] and the capable results of its altered safety assessments make it apt for ordinal image encryption for upcoming interactive program communication classifications.

DNA cryptography and duple hyper chaotic map procedures are proposed in [11], to deliver high-level safety for an ordinal medical image. The ordinal medical images are very big in dimensions and necessitate extra arithmetic time. To lessen arithmetic time, the discerning ordinal medical image scrambling procedure is presented in [11]. Also, the transformation and dispersal process are executed on designated pixels of ordinal medical pictures. The inventive medical digitized image is renewed into designated pixel DNA-coded matrix C1 and residual pixel DNA coded matrix C2 using all DNA rules created on the pixel index value. The chaotic arrangements are formed using constraints and system factors of the dual hyper chaotic map. The dual hyper chaotic map is hired to mix-up the designated pixels of coded DNA matrix C1. The DNA XOR scheme is engaged to combine the jumbled DNA-encoded matrix C1 and DNA-encoded matrix C2. The collective DNA-encoded matrix is transformed into binary image using all DNA decoding rules and is transformed into grayscale image to get cipher image. The enactment analysis demonstrates that a presented algorithm in [11] develops the safety level and also hinders differential, in-depth and statistical attacks. The presented method takes less computational time (i.e., 0.236 s) and is appropriate for telemedicine, smart health, and e-health solicitations.

To discourse latency issues of encoding/decoding procedures for outsized size-colored images, a new deep learning-based encoding system using DNA, chaos and multiple s-boxes is projected and assessed in [12]. The presented scheme consists of two segments; 1) a deep learning-based convolutional autoencoder to wrapping the large-size three-dimensional colored images into a pointedly lower size two-dimensional gray-scale image, and 2) a novel DNA-based image encryption and decryption module using multiple chaotic series and substitution boxes to make the cipher image random as obvious from the results described in [12]. A symmetric key technique is projected in [12] for encrypting digital images. The proposed scheme in [12] can efficiently be employed for secure and fast broadcast of large size-colored images over a low bandwidth broadcast network.

To certify the safety and secrecy of ordinal image when it's communicating online or stowing in the cloud, a chaos-based image encryption scheme by using arbitrarily DNA encode and plaintext related variation is planned in [13]. In this scheme, plain image is arbitrarily encoded into a nucleotide sequence under the control by the piecewise linear chaotic map (PWLCM). Under the control order produced by hyper-chaotic Lorenz system, the plaintext associated variation is done, which can upsurge the plaintext compassion and increase confrontation to differential attack. Moreover, key DNA sequence is used in [13]

to variety diffusion processing, which can powerfully resist statistical attack. The assessment results exposed that projected image cryptosystem in [13] has exceptional safety performance in ordinal image communication. The image encryption based on chaos and DNA computing are still under continuous research, and there are still many complications that need to be more deliberate and resolved.

A new bijective algorithm which is devoted to secure image transmission over the data communication systems is introduced in [14]. An innovative symmetric cryptosystem is existing in [14] that hang on the fusion chaotic Lorenz dispersion phase and DNA confusion phase. It contains two alike scrambling and decipher algorithms that streamlines the application of spreading and reception patterns of images strongly as a bijective system. The scheme was discovered to be much subtle against negligible alteration in the produced undisclosed key. The examination verifies that the structure has larger arithmetic possessions, huger key space, improved plain text compassion, and enhanced key compassion associated with prior systems.

Encryption and decryption algorithm is presented in [15] for the drive of confirming portrait broadcast over information correspondence backgrounds. Color image encryption in [15] employments a confusion method based on a hybrid chaotic map, initially to split each channel of color images into n-clusters; then to generate global shuffling over the entire image; and lastly, to apply interpixel shuffling in each cluster, which fallouts in very muddled pixels in the encoded image. Then, it utilizes the rationale of human mitochondrial genome mtDNA to diffuse the earlier confused pixel values. Theoretical examination and trial results validate that the anticipated scheme displays outstanding encryption, as well as positively compete with chosen/known plaintext, statistical, and differential attacks.

A new-fangled system for the encoding of color images built on the DNA strands level scrambling (DNASLS) has been anticipated in [16]. Next a color picture is insert, it is disintegrated into the red, green and blue constituents. Later these mechanisms are combined to create a large solitary image. Interlinking logistic map (ILM) has been used for the arbitrary data which produces three tributaries of arbitrary numbers. These tributaries have been extra operated in such mode that nine tributaries are reproduced out of them. To generate the dispersal possessions, an XOR process has been done among the DNA coded image after the exchange of elements and the DNA encrypted key image. The possessions of plaintext compassion have been attained through the integration of Secure

Hash Algorithm-256 or SHA-256 hash codes. At last, the experiment and the safety investigation have been accomplished. The outcomes of the validation metrics like data entropy (7.9973), average key sensitivity (99.61%) and mean absolute error (84.7158) validate the security, boldness to the number of attacks and a potential for real world solicitation of the anticipated image encryption.

Image encoding has been seen as an exciting study area by various professionals and numerous procedures to encode imageries have arisen, presently, the emphasis is on gaining improved imageries. An innovative image encoding outline that practices intertwining logistic map (ILM), DNA encrypting and DE optimization is presented in [17]. The anticipated method is built on trio chapters: transformation including ILM dispersal appealing DNA and optimization via DE. The main involvement of [17] is too contemporary the efficacy of DE in duplicate optimization and show by what means DE is well than GA. The optimization acting a vital part provided that an effective encoding. High randomness standards and little CC standards straight gather restored outcomes for an enhanced encoding. The consequences of DE enhancement are too correlated with that of GA optimization in [17]. Hypothetical examination and investigational fallouts in [17] support that the set of rules by DE determines improved encoding efficacy than GA. The outcomes as well validate the datum that encoding via DE is quicker than encoding with GA. Henceforth, DE can be cast-off to attain a faster and additional safe encoding method.

In [18], A different image encoding system created on an amalgam typical of DNA computation, chaotic schemes and hash purposes is familiarized. The vital gain of the anticipated outline is from top to bottom competence. A miscellaneous SHA256/MD5 hash from the basic duplicate and the top-secret key to certify the primary state and switch constraints of chaotic systems variation by flicking individual bit of the unadorned copy or the undisclosed key is shown in [18]. The investigational results in [18] exposed that the projected image encoding outline can not only attain decent safety product than five further illustrative image encoding structures, nevertheless as well adequately wild for hands-on claims.

Combine DNA computation with double-chaos schemes is proposed in [19] and advises a procedure for color copy encoding at the minute close. Initial, Arnold procedure is used in [19] to clamber the trio mechanisms of the color copy, and the quantity of repetitions was strong-minded by the normal of the tierce apparatuses, which amended the shambling

consequence of Arnold procedure. Also, later a proportion of experimentations, a double-chaos scheme collected of Lorenz chaotic plotting with inconstant limitations and then Rossler hyperchaotic drawing in [19] to produce trio groups of chaotic orders for dispersion process. The tentative outcomes in [19] illustrate that the procedure has upright protection presentation and can efficiently counterattack countless outbreaks.

In demand to acquire chaos with a broader chaotic possibility and improved chaotic performance, [20] associate the numerous standing simplistic chaos and arrange a new basic chaotic plot by means of an integrated procedure which is called by LLS structure and abridged as LLSS. To become an improved encoding result, an original copy encoding technique founded on double chaos and DNA ciphering expertise is probable in [20]. Tentative imitation and safety investigation in [20] express that this procedure rises the key space, has from top to bottom compassion, and can counterattack numerous public outbreaks. At the similar period, the procedure in [20] can lessen the connection between together picture element, produce it close to 0, and rise the data randomness, constructing it adjacent to the model worth and accomplishing a virtuous encoding consequence.

In [21], a copy encoding procedure founded on hash table construction shambling and DNA replacement is introduced. The procedure in [21] practices the standard 'scrambling-diffusion' method, and the pseudo-random arrangement cast-off to each method is engendered by the hyper-chaotic Chen scheme. Primarily, in the method of motocross, dual orders with no repetitive standards are made by means of the locked hash technique in the hash board building for chaotic classifications, and the basic copy is jumbled two times rendering to the dual orders. The haphazardness of the chaotic arrangements in [21] is cast-off in in cooperation procedures of encoding, which efficiently advances the safety and consistency of the system. Over the encoding and decoding trial and sanctuary study of various imageries in [21], and evaluation with supplementary writings, our encoding process can complete the resolution of defending image safety and can be cast-off for image scrambled spread.

Visual careful image encoding can together advance the proficiency of the image encoding procedure and lessen the occurrence and strictness of outbreaks in contrast to facts. In [22], an original system of encoding is projected built on keys resulting from Deoxyribonucleic Acid (DNA) and plaintext copy. The planned arrangement in [22] results in chaotic graphic careful encoding of image information. In command to style and certify that this innovative

arrangement is vigorous and protected compared to countless types of outbreaks, the preliminary situations of the chaotic plots employed are produced from an arbitrary DNA arrangement as well as plaintext image via an SHA-512 hash function. To rise the key space, trio changed solo measurement chaotic maps are cast-off. In [22], these maps present dispersion in a simple image by picking a chunk that have better relationship and then it is bitwise XORed with the casual matrix. The additional dual chaotic maps disrupt the connection between next to picture element through muddle (row and column shuffling). The key benefit of the anticipated system in [22] is that scrambled image is not casual alike clamor and later enemy might not distinguish that image comprise particular material.

An image encoding procedure recognized on 3-D DNA level version and replacement arrangement is offered in [23]. SHA 256 hash rate of simple image is cast-off to compute the preliminary standards of the 6-D hyperchaotic scheme and the organization limitations of the 3-D cat plot. Investigational outcomes and safety study in [23] have established that the planned image encoding process has virtuous safekeeping and forcefulness, and can also counterattack nearly identified outbreaks.

[24] suggests a chaotic paint image encoding system built on DNA-coding designs and mathematics over the Galois field. Initially, trio revised simple-minded (1D) chaotic charts with bigger key planetary and well chaotic features are accessible in [24]. The investigational grades in [24] display that their chaotic pauses are non-only prolonged to (0, 15], but then their usual major Lyapunov Proponent ranges 10. They stay used as primary keys. Furthermore, DNA ciphering and intentions are pragmatic in demand to enhance extra variation of the cryptosystem. Eventually, the enumeration over the Galois field certifies the result for the dispersion of picture element. The recreation examination in [24] demonstrates that the encoding arrangement planned in [24] has respectable encoding consequence, and the mathematical outcomes confirm that it has advanced safety than nearly of the up-to-date cryptosystems.

An image encoding structure by means of the mixture of chaos, hyper-chaos, and DNA classification process is acquaint within [25]. The projected structure executes trio phases of encoding processes. Individuals are selection-level hyper-chaotic order-based DNA shambling process, key-image created DNA-diffusion action, and hyper-chaotic arrangement constructed DNA scuffling procedure. The rewards of the arrangement in [25] are advanced key planetary, advanced confusion or casualness of picture element,

sophisticated compassion to the keys and plaintext picture element, tougher resistivity to the clatters, and lossless encoding and decipherment. Furthermore, collection side by side hyper-chaotic order created DNA shambling process creates extra complications in the misperception method which growths the strong point of encodings and decoding. The computer replication and safety examine in [25] authorize the decent encoding outcomes of the anticipated system and solid resistivity to the frequently cast-off outbreaks. The contrast results in [25] demonstrate that the projected procedure is extra protected as associated to the additional described arrangements. Completely these structures illustrate that the anticipated procedure is sheltered and appropriate for image encoding.

[26] offered the light field image (LFI) material contains the strength of the composed article and the way of the light over videorecording. An LFI through a 4-D act illustration consist of a 2-D longitudinal field and a 2-D sharp area, which is totally changed than overall ordinary images. In adding, DNA encrypting and Chen's chaotic structure are cast-off in [26] to hike and verbose the picture element of the sub-block images after chunk dealing out. Lastly, all the scrambled sub-blocks in [26] stay combined to gain the encryption image. The Arnold convert was pragmatic to the built multi-view image medium, and the last secret message image was found. The tentative replication in [26] illustrates that the outline is full-bodied and has no clear impact on the unique LFI superiority. Trial fallouts in [26] reveal that the anticipated structure can counterattack discrepancy outbreak and validate from top to bottom safety.

In [27] a novel chaos-based encoding scheme is projected for medical images. It is built on a grouping of chaos and DNA computing below the state of two encryption series, headed by a key generation layer, and trails the permutation-substitution-diffusion structure. In [27] SHA-256 hash function together with the preliminary secret keys is engaged to yield the secret keys of the chaotic systems. Security studies and processer mockups together endorse that the planned order in [27] is strong beside all types of outbreaks. Its little difficulty specifies its great prospective for present and safe image solicitations.

[28] takes a general attitude to suggest an inclusive outline for color image encoding with some new sorts. In [28] a color image is encrypted into a DNA sequence using arbitrarily nominated row-level encoding rules. A novel 4D-Hyperchaotic system is used in [28] to produce pseudo-random orders to permutate image information at bit-level and block-level. The multidimensional Hyperchaotic system rises non-periodicity, randomness, and

unpredictability than a modest chaotic system. Changed subkeys have been engaged near rise the key cosmos and implant encoding and decipher into the anticipated order. Consequences and examination indicate that the projected agenda in [28] is arithmetically effective and vigorous to altered kinds of outbreaks and cryptanalysis passed over the pictures.

In [29] a novel ordinal image encoding technique is projected built on bit swapping procedure, chaotic schemes and DNA encoding procedure. Initially, in this technique each pixel of the picture is transformed to its equivalent binary order encompassing of 0's and 1's bits. After that, the 0 bit is exchanged by (1 and 0) bits and the 1 bit is exchanged by (0 and 1) bits. Then, the created images are scrambled using large dimensional chaotic schemes built on the standard of transformation and dispersion practices in detached to differ the locations and standards of the ordinal image pixels. Then, the subsequent scrambled pictures are encrypted by embracing DNA procedure rules and at that time these pictures are combined by manipulating DNA addition process. Lastly, the encoded DNA pictures are deciphered to gain the output scrambled picture. To sum up, the projected method in [29] formed huge secret key space of (2747), an equivalent differential examination enactment NPCR (99.61%) and UACI (34.61%) and conceded all safety and haphazardness examinations.

In [30] a new encryption patterns that chains hyperchaotic maps patterns, SHA-2, and a pixel-shifting built on the Zaslavskii map is projected. The plain image is initially jumbled based on standards gained from a 2-D hyperchaotic map. A cover picture is then created using the mutual logistic-tent map. A mask image is formed after that, built on a unique bit indexing pattern built on the SHA-2 value of the cover picture. In [30] DNA encryption is conceded out on both images, using an animatedly chosen logistic-tent map. Then dispersal using the exclusive-OR technique was implemented. Finally, multiple dispersion processes are conceded out to yield the coded image. Through simulation examination, this projected system in [30] has been firm to yield great security. The projected technique surpasses the formerly established technique by the biographers.

A novel image encoding pattern is proposed in [31] built on the chaotic scheme and the substitution actions of the pixels equally at the fraction and DNA levels. Through arbitrarily selecting two arrays of the specified input picture for a number of spells, casually selected pixels of these two ranges are exchanged. In [31] similar process is executed on the two

arbitrarily selected columns to acquire the jumbled duplicate. Then, an XOR process is executed among the jumbled image and the key tributary of arbitrary statistics specified by the chaotic scheme. Finally, the DNA-encoded statistics are deciphered back into its fraction corresponding. SHA-256 hash ciphers for the specified input image have been cast off in the projected code in command to attain the plaintext compassion. The imitation and the presentation examination depict the good safety possessions, insolence to the diverse intimidations and the positive projections for the practical solicitation of the presented code in [31].

As there are abundant users and muggers over the internet, IoT data face several safety matters. Presently, DNA cryptography is a front-line area, which is used to improve data safety. In [32], a new cryptosystem is presented using DNA cryptography and DNA steganography for the cloud-based IoT substructure. Here, the private data is encoded by using an extended secret key. Then, it is concealed in an image. Therefore, the presented cryptosystem in [32] not only hides the data, but also encodes the private data prior to loading it on the cloud server, and it fights many safety outbreaks in the cloud-based IoT substructure. To assess the working of the presented scheme in [32], numerous tryouts are executed. The outcomes show the efficiency of the presented scheme.

In [33], a novel encryption process is proposed based on DNA cryptography, a hyperchaotic system and a Moore machine. The hyperchaotic system produces four pseudo-random number sequences used in DNA-based processes. The Moore machine executes replacements in the DNA sequence that makes the system more protected. The presented technique in [33] can defend a system from many attacks, namely man-in-the-middle attacks, ciphertext-only attacks, known-plaintext attacks, brute force attacks and differential cryptanalysis attacks. The presented scheme in [33] gives an average avalanche effect of 54.75%, which assures a high level of robustness. Furthermore, tentative outcomes show that the presented scheme in [33] is safer and more effective than the current schemes.

Most state-of-the-art solicitations demands nominal network latency in the network so that the reply can reach the user within segment of seconds. To meet this necessity, fog computing came into survival. In [34], a new encoding technique is presented, which is built on genetic science and works in two phases. In the initial phase, the plaintext is transformed to a complex cipher text by making use of a complex key. The key is arbitrarily nominated from the DNA population and is made extra complex by using logical operators.

The cipher text acquired in the first phase is made much impassable in the second phase, by using genetic science principles of crossover and alteration. The mockup and outcomes of the presented technique in [34] specify that it offers much safety to the data as equated to the current encoding techniques.

[35] Presents a protected data encoding and hiding process built on DNA cryptography and steganography. Approach in [35] uses DNA for encoding and data hiding procedures due to its great capability and plainness in fortifying many types of data. Presented method in [35] has two phases. In the initial phase, it encodes the data using DNA bases along with Huffman coding, In the next phase, it pelts the encoded data into a DNA sequence using a exchange algorithm. Presented method in [35] is unsighted and conserves biological functionality. The outcome displays an attired cracking chance with moderately improved dimensions. Presented method in [35] has removed many boundaries recognized in the associated works. Presented hybrid technique in [35] can offer a double layer of refuge to subtle data.

In [36] a new scheme is presented for image encoding by raising the well-known DNA technique and the three-dimensional chaos maps. The 3D Arnold map makes a key order which is altered by DNA rule and XORed with a DNA tributary to achieve a complicated dispersal, and instantaneously get through to shuffle all the pixel positions. The destruction level is altered by asset of three key producing sequences attained by 3D logistic map with subtle limitations and primary values. The effectiveness of the presented procedure in [36] is proved via a succession of trials conceded on some test images. The arithmetical consequences validate that the presented procedure accomplishes remarkably well and delivers improved encoding outcomes abreast the higher key compassion as associated to the preceding current schemes. However, the presented scheme in [36] also shows an improved confrontation to the recognized arithmetical, differential, and comprehensive outbreaks.

2.1 Research Gap

In spite of the developments in image encryption techniques using DNA, chaos, and hybrid approaches, there are numerous research gaps that are essentials to be addressed:

Comparative Analysis: The literature reviews present several image encryption schemes but lack an inclusive comparative analysis. A relative study that estimates the strengths,

faintness, performance, and security of different encryption schemes would be esteemed in recognizing the most effective and competent techniques for different application situations.

Robustness against Advanced Attacks: While the reread encryption schemes demonstrate flexibility against public attacks, such as chosen-plaintext and statistical occurrences, there is a need to inspect their robustness against more advanced attacks, including machine learning-based attacks and cryptanalysis techniques. Supplementary research should focus on evaluating the liabilities and potential weaknesses of these schemes in the face of developing attack methods.

Practical Implementation and Performance Estimation: The literature reviews primarily focus on hypothetical analysis and simulation results. However, practical implementation and performance evaluation of the proposed encryption schemes in real-world scenarios are inadequate. Future research should consider implementing these techniques in practical environments, considering factors such as computational competence, resource requirements, and scalability, to validate their viability and effectiveness.

Standardization and Interoperability: The reviewed encryption schemes lack standardized protocols and frameworks, which can delay their interoperability and integration into current systems. Forthcoming research should highlight standardization efforts to ensure compatibility and whole integration of image encryption techniques across different platforms and systems.

Security Evaluation in Multimedia Communication Systems: While the literature reviews remark the suitability of certain encryption schemes for multimedia communication systems, there is a research gap in assessing their security performance in real-world multimedia applications. Upcoming research should focus on assessing the security and robustness of these schemes in hands-on multimedia communication systems, considering factors such as network limitations, transmission quality, and resistance to attacks specific to multimedia data.

Addressing these research gaps would contribute to the advancement of image encryption techniques, ensuring their effectiveness and security in various application fields. Additionally, it would ease the development of standardized encryption protocols, improve

interoperability, and help the practical implementation of secure image encryption in real-world set-ups.

Chapter Three

3 METHODOLOGY

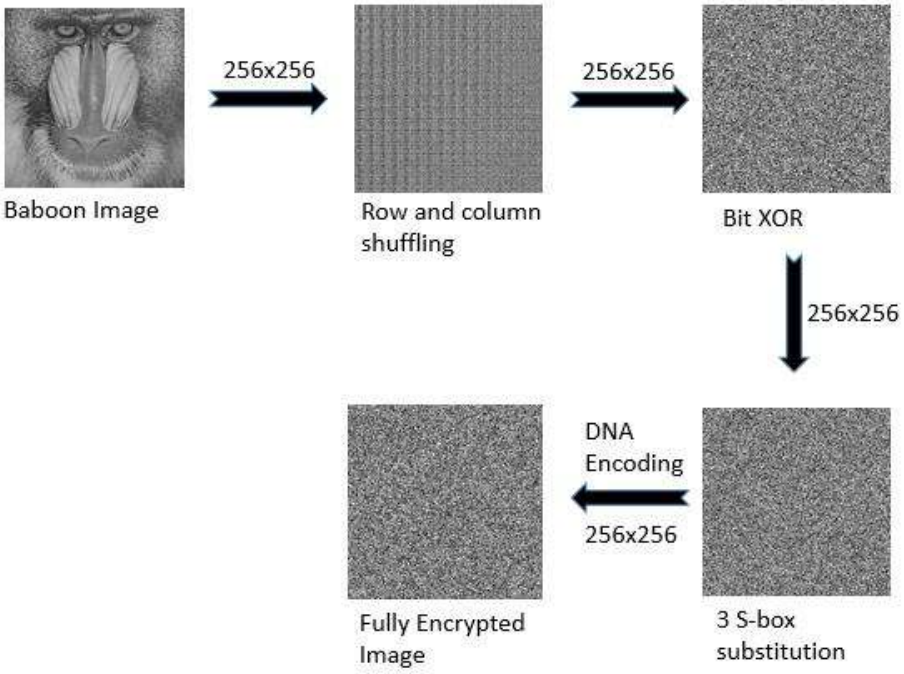


Figure 3-1: Flow chart of proposed scheme

As in Figure 3-1, the first step of the encryption process includes choosing an appropriate original image, in this case, a Baboon image. To present spatial confusion and modify the pixel arrangement, the logistic map algorithm is engaged. The logistic map algorithm produces a sequence of pseudorandom numbers, which are then conditioned to shamble the rows and columns of the original image. This shuffling process objects to disrupt the spatial consistency of the image, making it more challenging to decipher. The logistic map algorithm is employed once again to create another sequence of pseudorandom numbers. By performing a bitwise XOR operation among the shuffled image and the pseudorandom numbers, the encryption process adds a supplementary layer of difficulty and diffusion. The XOR operation varies the pixel values in the image, making it more stimulating for

unauthorized persons to understand the encrypted data. Then three rounds of S-Box substitution are applied to the XOR-ed image. To provide an exceptional representation for the encrypted data, DNA encoding is employed. A specific DNA sequence mapping scheme is established to map the pixel values or bit sequences of the encrypted image to equivalent DNA sequences. This encoding process adds a further layer of complexity and distinctiveness to the encrypted data, making it more challenging to decipher without the right decoding algorithm. S-Boxes are predefined substitution tables that map input values to specific output values. Each S-Box substitution presents nonlinear transformations to the encrypted image, further improving its safety and opposition to cryptographic attacks.

After completing the previous steps, the result is an encrypted image. The encrypted image embodies the original Baboon image transformed through row and column shuffling, bit XOR operations, S-Box substitutions, and DNA encoding. The encrypted image contains greatly scrambled and encoded information, safeguarding the original content against unlicensed access.

3.1 Logistic map

The logistic map is a mathematical function used to model population growth or other dynamic systems that show non-linear behavior. It was first introduced by the biologist Robert May in 1976 as a simple iterative equation.

The equation for the logistic map is expressed as:

$$X(n+1) = r * X(n) * (1 - X(n)) \quad (3.1)$$

In equation 3.1, X(n) characterizes the value of the logistic map at time step "n." The value of "r" is a parameter that defines the growth rate or the bifurcation behavior of the map. It is characteristically within the range of 0 to 4, where different values of "r" lead to distinct dynamic behaviors. The logistic map is an iterative equation, which means that the value at each time step rest on the value at the earlier time step. By iterating this equation multiple times, the logistic map creates a sequence of values that can exhibit intricate behavior, including steadiness, periodicity, divergence, and disorder, depending on the value of "r."

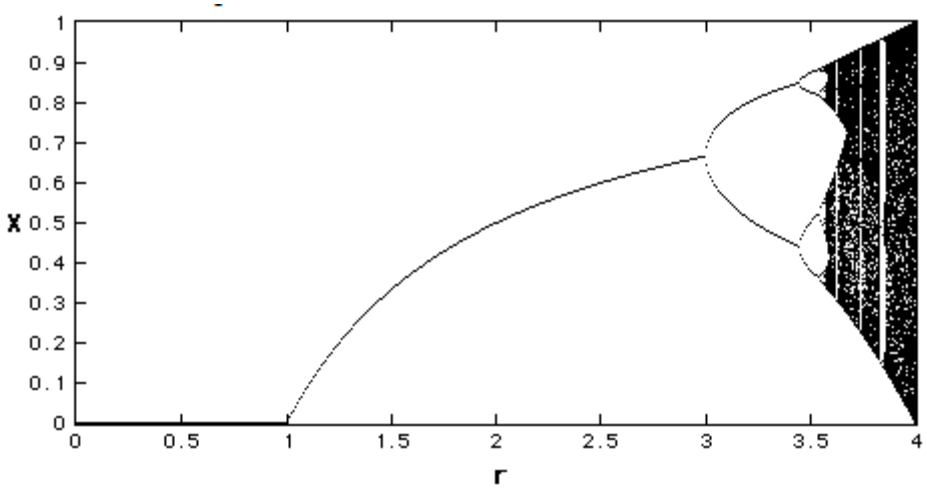


Figure 3-2: Bifurcation Diagram r between 0 and 4 [1],[20]

The logistic map produces a bifurcation diagram as shown in Figure 3-2 [1],[20], which illustrates the behavior of the system as the parameter r varies. To create this diagram, one starts with an initial value X_0 and applies the logistic map equation repeatedly, discarding some initial iterations to allow the system to settle into its long-term behavior. The resulting values of X_n is then plotted against the parameter r.

When the parameter r is small, the population size converges to a stable equilibrium value. However, as r increases, the system undergoes period-doubling bifurcations, leading to the emergence of periodic oscillations. Eventually, at a critical value of r (around 3.57), the system transitions to chaotic behavior, where the population size exhibits irregular, unpredictable fluctuations.

The graph of the logistic map's bifurcation diagram showcases the complex behavior of the system as the parameter r increases. It displays a cascade of bifurcations, with period-doubling leading to the emergence of a fractal pattern. The graph is characterized by a series of branches that correspond to stable points, periodic orbits, and regions of chaotic behavior.

The logistic map provides insights into the dynamics of nonlinear systems and is widely used in various fields, including biology, physics, and economics. Simple equation and the rich complexity make it a valuable tool for studying chaotic phenomena and understanding the behavior of nonlinear dynamical systems.

3.2 Confusion

Confusion is an essential concept in cryptography that mentions to the process of disguising the association among the plaintext and the ciphertext. It includes converting the input data in such a way that the resulting encrypted data seems random and barren of any apparent patterns or correlations. The motive of familiarizing confusion in a cryptographic scheme is to make it problematic for an attacker to take out any evocative information from the ciphertext without retaining the suitable decryption key. Confusion techniques classically involve operations such as substitution, permutation, or bitwise manipulation, which modify the values or positions of the data elements. By introducing confusion, the encoded data becomes statistically vague from random noise, thereby increasing the security of the encryption scheme. Confusion, along with diffusion, is a central element in attaining robust and protected encryption, as it certifies that even small changes in the input result in major changes in the output, baffle attempts at cryptanalysis and increasing the total strength of the encryption.

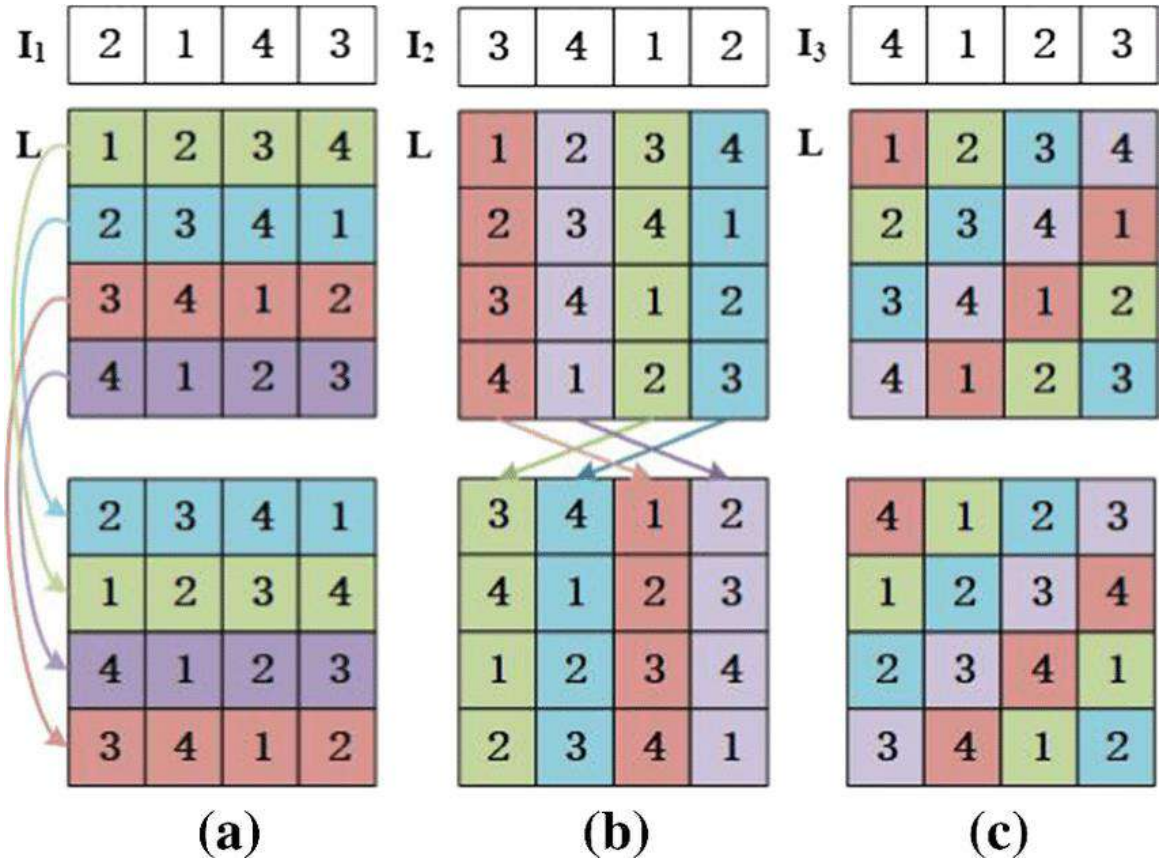


Figure 3-3: Process of Matrix Scrambling. (a) Row Scrambling; (b) Column Scrambling; (c) Entity.

Balancing the level of confusion is crucial, and it often requires careful consideration of various factors such as the encryption algorithm's strength, computational efficiency, and the specific requirements of the application. The choice of confusion operations and their parameters must be designed to provide a sufficient level of complexity while preserving the integrity and visual quality of the encrypted image as shown in Figure 3-3.

Furthermore, the choice of encryption key plays a significant role in achieving confusion. The key determines the specific transformations applied during encryption and decryption. A strong and secure key is essential to ensure the effectiveness of the confusion process and maintain the confidentiality of the encrypted image.

In conclusion, confusion is a critical aspect of image encryption, aiming to disrupt patterns and correlations in the image to make it resistant to attacks. Achieving an appropriate level of confusion while maintaining image integrity and security is a complex task that requires careful consideration of various factors, including the choice of operations, parameters, and encryption key.

3.3 Bit XOR (Diffusion)

Bit XOR, or exclusive OR, is an important operation in cryptography used for diffusion, which is the procedure of spreading the effect of individual bits across the whole ciphertext. In a bit XOR operation, two bits are equated, and the result is a new bit that is set to 1 if the two input bits are dissimilar, and 0 if they are the similar. This process presents arbitrariness and intricacy into the scrambled data by changing the individual bit values. By applying bit XOR to the ciphertext, the impact of each bit spreads through succeeding rounds of encryption, making it difficult to distinguish any patterns or links between the original plaintext and the encrypted output. Bit XOR, as a diffusion technique, ensures that variations in a single bit of the plaintext lead to substantial changes throughout the ciphertext, firming up the security of the encryption scheme. It is a modest yet powerful operation that, when combined with other cryptographic techniques, helps attain robust and secure encryption.

The key used in the bitxor operation is crucial for ensuring the security of the encryption scheme. It adds randomness and complexity to the encryption process, making it more difficult for an attacker to decipher the original image from the encrypted version. The key should be sufficiently long and securely generated to resist cryptographic attacks.

Table 3-1: Bit XOR Operation

A	B	C= A^B
0	0	0
0	1	1
1	0	1
1	1	0

The bitxor operation is reversible, meaning that applying the same key again to the encrypted pixel value will yield the original pixel value as shown in Table 3-1. This property allows for decryption by performing the bitxor operation between the encrypted pixel value and the decryption key.

Bitxor is often used in conjunction with other encryption techniques, such as substitution and permutation, to provide a more robust and secure image encryption scheme. It helps introduce confusion into the encrypted image and prevents statistical analysis or simple correlations between the original and encrypted pixel values.

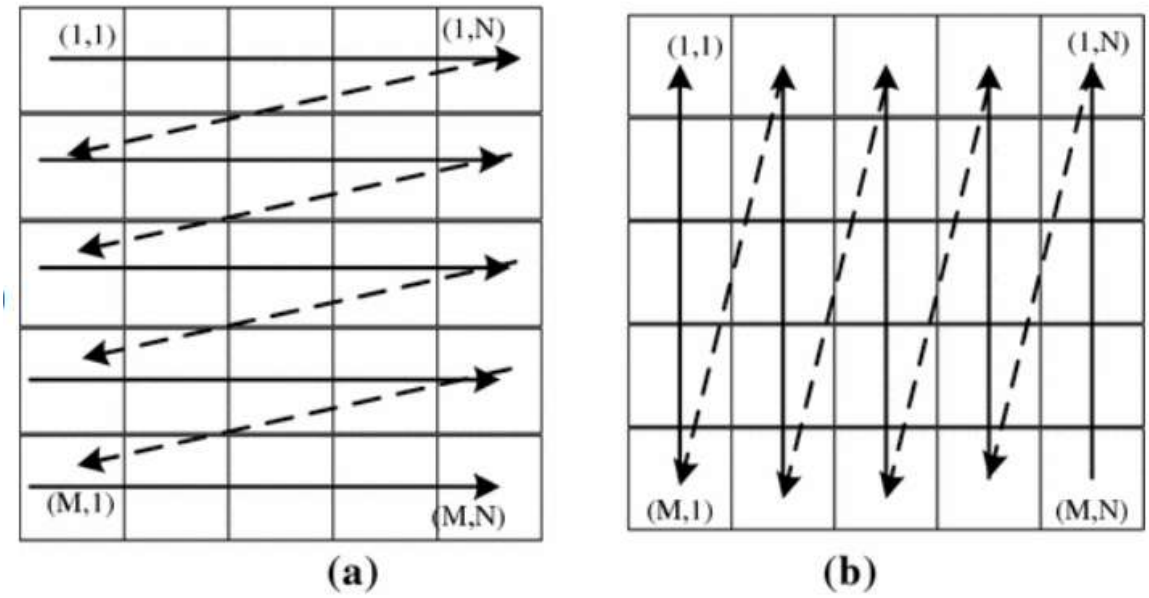


Figure 3-4: The Diffusion Process of Encryption. (a) the diffusion process of row-major and (b) the diffusion process of column major.

In Figure 3-4, the diffusion process of encryption by row major and column major is illustrated.

In summary, the bitxor operation (Diffusion) plays a crucial role in image encryption by introducing confusion and enhancing the security of the encrypted image. It combines the pixel values of the image with an encryption key through bitwise XOR, creating a new pixel value that is difficult to decipher without the correct decryption key. Bitxor is an important component of many image encryption algorithms and contributes to protecting the confidentiality and integrity of sensitive image data.

3.4 S-box substitution

S-box substitution, also recognized as substitution box, is a vital factor in many encryption algorithms, mainly symmetric key ciphers. It aids as a nonlinear substitution mechanism that improves the muddle and dispersal properties of the encoding method. A S-box operates by changing input bit patterns with corresponding output bit patterns based on a predefined lookup table. This substitution table presents composite and nonlinear relationships between the input and output values, making it tough to separate any statistical patterns or regularities. By smearing S-box substitution, the encryption algorithm presents confusion into the data, confirming that small variations in the input result in weighty changes in the output. This nonlinearity and difficulty provide confrontation against many outbreaks, including differential cryptanalysis and brute-force attacks. S-box substitution is often iteratively smeared across multiple rounds in encryption schemes, further strengthening the sanctuary and certifying the privacy and reliability of the scrambled data.

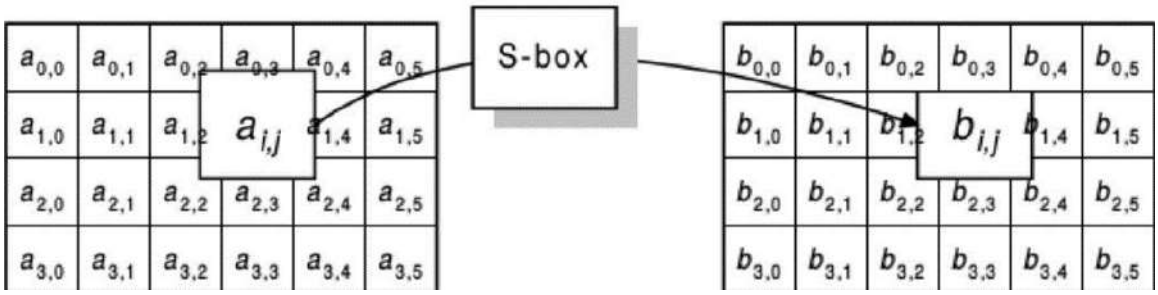


Figure 3-5: S-Box Substitution

The primary purpose of S-box substitution as shown in Figure 3-5, is to disrupt any statistical patterns or correlations in the pixel values, making it difficult for an attacker to decipher the original image from the encrypted version. By introducing non-linearity, the

S-box strengthens the confusion aspect of the encryption process and prevents simple algebraic relationships between the input and output values.

The design and properties of the S-box are critical for the overall security of the encryption algorithm. S-boxes should possess desirable cryptographic properties such as resistance to differential and linear attacks, and they should be resistant to reverse engineering. Extensive research and analysis are conducted to create S-boxes that exhibit strong cryptographic properties and satisfy specific security requirements.

In summary, S-box substitution is a vital component of image encryption algorithms that introduces confusion and non-linearity to enhance the security of the encrypted image. By replacing pixel values based on complex substitution rules, the S-box disrupts statistical patterns and correlations, making it challenging to decrypt the original image without the proper decryption key. Proper design and selection of S-boxes are crucial to ensure the overall strength and security of the image encryption scheme.

3.4.1 MSB (Most Significant Bit)

S-box substitution with MSB (Most Significant Bit) is a cryptographic technique that includes substituting input bit patterns with equivalent output bit patterns based on a predefined lookup table. In this method, only the most significant bit of each input byte is reflected for the substitution process. By concentrating on the MSB, the S-box introduces supplementary complication and non-linearity to the encryption scheme, improving the safety of the cryptographic algorithm. The substitution table used in MSB S-box substitution is cautiously projected to ensure that the substitution patterns are vastly nonlinear and resistant to several cryptanalysis techniques. This technique offers a form of confusion and diffusion in the encryption process, making it more tough for attackers to examine the affiliation between the plaintext and ciphertext. S-box substitution with MSB is usually employed in symmetric key algorithms such as block ciphers.

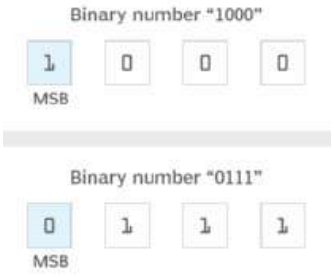


Figure 3-6: Most Significant Bit concept

Furthermore, as shown in Figure 3-6, the MSB can also be used for further cryptographic operations, such as key generation or expansion. The MSB of keys can be used to determine the sequence or selection of specific S-boxes, introducing additional variations and randomness in the encryption process.

Overall, the utilization of the MSB in S-box substitution adds an extra level of complexity and enhances the security of image encryption algorithms. By considering the most significant bit, the encryption scheme gains improved resistance against attacks and ensures the confidentiality and integrity of the encrypted image data.

3.4.2 LSB (Least Significant Bit)

S-box substitution with LSB (Least Significant Bit) is a cryptographic technique that contains changing input bit patterns with corresponding output bit patterns built on a predefined lookup table. Unlike the MSB S-box substitution, which emphases on the most significant bit, LSB S-box substitution deliberates only the least significant bit of each input byte. This approach adds an extra layer of difficulty and non-linearity to the encryption process, improving the safety of the cryptographic algorithm. The substitution table used in LSB S-box substitution is wisely intended to confirm that the substitution patterns exhibit strong diffusion properties, making it thought-provoking for attackers to detect any patterns or relationships between the plaintext and ciphertext. By integrating LSB S-box substitution, the encryption scheme presents confusion and diffusion, making it more resistant to many kinds of cryptanalysis attacks. LSB S-box substitution is normally employed in symmetric key algorithms, such as block ciphers, to ensure the concealment and veracity of delicate data during communication or storage.

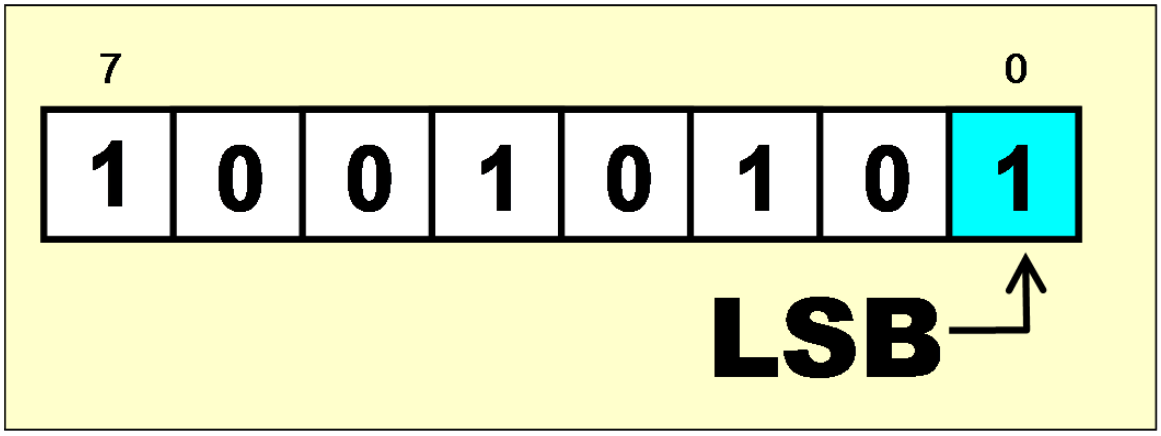


Figure 3-7: Least Significant Bit Concept

In image encryption, as shown in Figure 3-7, the LSB of pixel values can be manipulated using bitwise operations or Boolean functions. By modifying the LSB, the encryption algorithm can hide or distort lower-order bits, making it challenging for an attacker to decipher the original image from the encrypted version. This helps to preserve the confidentiality and integrity of the image data.

Furthermore, the LSB can also be used for data hiding purposes. By selectively embedding secret information into the LSBs of pixel values, it is possible to hide messages within the encrypted image. This technique, known as steganography, enables the combination of encryption and data hiding for enhanced security.

Overall, the LSB in S-box substitution provides an additional layer of complexity and non-linearity to the encryption process. By considering and manipulating the LSB, image encryption algorithms can achieve increased security and resistance against attacks while facilitating data hiding capabilities.

3.5 DNA Encoding

DNA encoding is a captivating technique used in cryptography to improve the safety of data encryption algorithms. Encouraged by the structure and properties of DNA molecules, this encoding method influences the tetrad nucleotide bases (adenine, cytosine, guanine, and thymine) as symbols to represent binary data. In DNA encoding, binary data is transformed into a corresponding DNA sequence using a predefined mapping scheme. Each binary bit or a group of bits is mapped to a precise nucleotide base, making a unique DNA sequence that signifies the original data. The compensations of DNA encoding lie in its potential for huge parallelism, error correction, and its capability to imitate biological processes. Furthermore, DNA encoding presents a level of complication and arbitrariness to the scrambled data, making it more unaffected to cryptographic attacks. This technique finds solicitations in many fields, including secure communication, image encryption, and DNA-based computing. DNA encoding adds an advanced dimension to cryptography, binding the power of nature's building blocks for secure information exchange and storage.

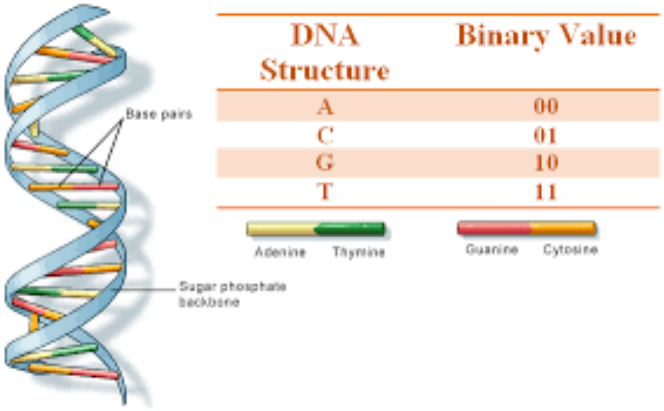


Figure 3-8: DNA Cryptography System [6]

The encoding process as shown in Figure 3-8 [6], involves mapping the binary or digital information into a DNA sequence using a specific encoding scheme. For example, the ASCII encoding scheme can be used to map each character of the text into a binary code, which is then converted into a corresponding DNA base sequence. The resulting DNA sequence represents the encoded information.

To decode the information stored in DNA, the reverse process is applied. The DNA sequence is sequenced using advanced DNA sequencing technologies, which determine the order of the DNA bases. The decoded DNA bases are then converted back into the original digital information using the appropriate decoding scheme.

DNA encoding offers several advantages over traditional data storage methods. One significant advantage is the tremendous information storage capacity of DNA. DNA molecules can store an extraordinary amount of data in a very compact form. It has been estimated that a single gram of DNA can store several exabytes (1 exabyte = 1 billion gigabytes) of digital information.

Additionally, DNA encoding provides long-term data storage potential. DNA molecules have been found preserved in ancient specimens for thousands of years. When properly stored, DNA can withstand extreme conditions and remains stable over extended periods, making it suitable for archival purposes.

Furthermore, DNA encoding offers the potential for data encryption and security. By combining DNA encoding with encryption algorithms, sensitive information can be encoded and stored securely in DNA sequences. DNA has natural error-correcting mechanisms, which enhance the reliability and integrity of the encoded data.

Table 3-2: Eight encoding rules for DNA sequences

Rules	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00	A	A	C	G	C	G	T	T
11	T	T	G	C	G	C	A	A
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C

However, DNA encoding as shown in Table 3-2 also comes with challenges. The process of DNA synthesis, sequencing, and decoding is currently time-consuming and expensive. DNA synthesis technologies are improving rapidly, but the cost and throughput still present limitations for large-scale adoption of DNA encoding.

Moreover, the encoding and decoding process require specialized laboratory equipment and expertise. Advanced DNA sequencing technologies, such as next-generation sequencing platforms, are utilized for efficient and accurate decoding of the DNA sequences.

Despite these challenges, DNA encoding holds tremendous potential for long-term, high-density data storage. Ongoing research and advancements in DNA synthesis, sequencing technologies, and encoding algorithms are expected to further optimize the process, reduce costs, and improve the practicality of DNA encoding as a viable data storage solution.

In conclusion, DNA encoding is an innovative approach to store digital information using the unique properties of DNA molecules. It offers high information storage capacity, long-term stability, and potential for data security. While challenges remain, DNA encoding holds great promise for revolutionizing the field of data storage and preservation, opening new possibilities for long-term archival and secure information storage applications.

Chapter Four

4 RESULTS

The result of the following steps, applied sequentially to an original image 256x256 (such as the baboon image), would be an encrypted version of the image:

Original Image: The starting point is the original image, which serves as the input for the encryption process.

Row and Column Shuffling: This step involves rearranging the rows and columns of the image to introduce confusion and disrupt the spatial relationships within the image. This shuffling operation alters the order of the pixels, making it more difficult to discern patterns or extract meaningful information.

Bitxor: Bitwise XOR (bitxor) is applied to the shuffled image. Each pixel value of the image is combined with a corresponding value from an encryption key using the XOR operation. This process introduces additional complexity and further obscures the relationship between the original image and the encrypted version.

S-Box Substitution: 3 S-box are used to substitute on the bitxor result. S-boxes are lookup tables that map input values to corresponding output values based on a substitution rule. This step introduces non-linearity and confusion into the encryption process, further scrambling the pixel values and preventing easy analysis or extraction of the original image.

DNA Encoding: Finally, the output from the previous step is encoded into a DNA sequence using a specific encoding scheme. The digital information of the image is translated into a sequence of DNA bases (A, C, G, and T) based on predefined mapping rules. This encoding process leverages the properties of DNA, such as its high information density and long-term stability, for secure data storage.

The result of these steps would be an encrypted version of the original image, with its pixel values shuffled, XORed with a key, subjected to S-box substitution, and finally represented

as a DNA sequence. This encryption process enhances the security of the image, making it more resistant to attacks and protecting the confidentiality of the image data.

A plaintext image and its corresponding cipher images with same resolution of 256x256 pixels are shown in Figures.

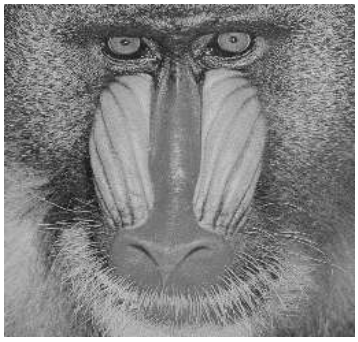
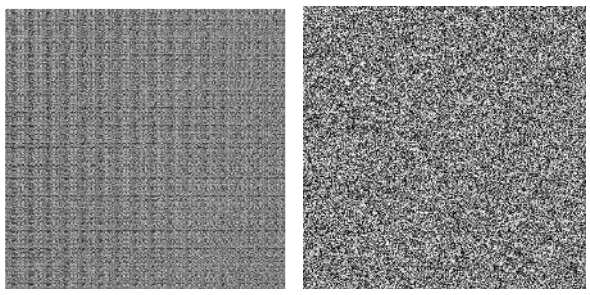
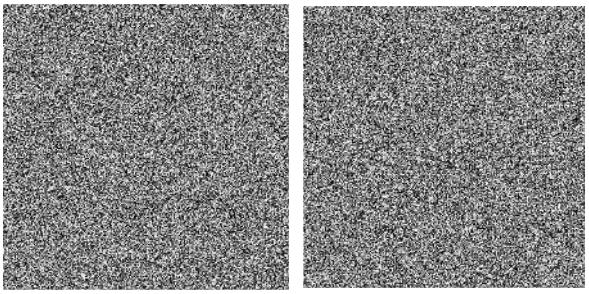


Figure 4-1: Original Image (Baboon) [2]



(a) (b)



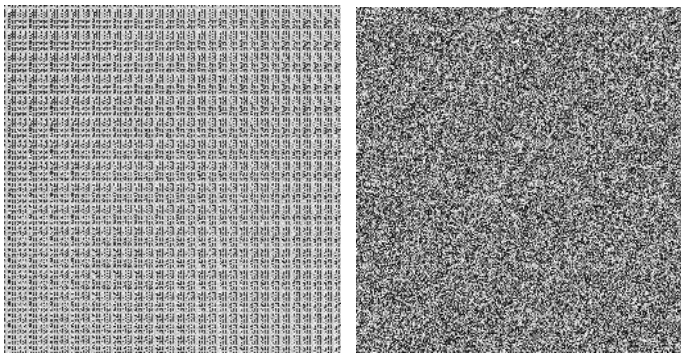
(c) (d)

Figure 4-2: (a) Row and Column Shuffling; (b) Bit XOR; (c) S-Box substitution; (d) DNA Encoding (Encrypted image).

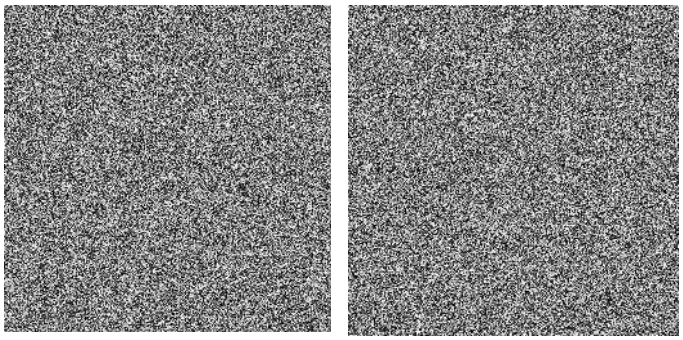
Figure 4-1 [2] illustrate that the original image is Baboon image of 256x256. And after applying confusion (row and column shuffling) on original image we got row and column shuffled image as shown in Figure 4-2(a). After applying diffusion (bitxor operation) on scrambled image we got more scrambled image as shown in Figure 4-2(b). After applying

S-Box substitution we got further scrambled image as shown in Figure 4-2(c). At last, we applied DNA Encoding and got fully encrypted image of 256x256 as shown in Figure 4-2(d).

Figure 4-3: Original Image (Cameraman) [18]



(a) (b)

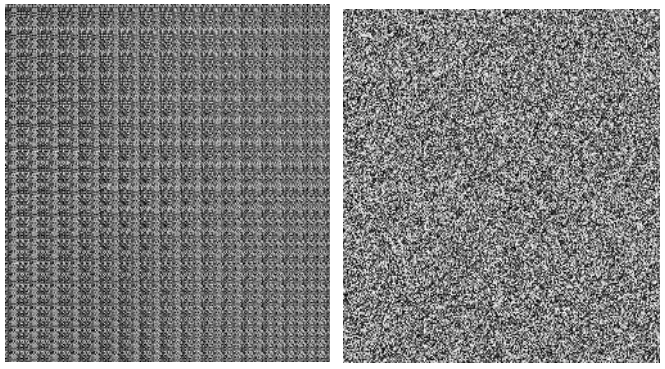


(c) (d)

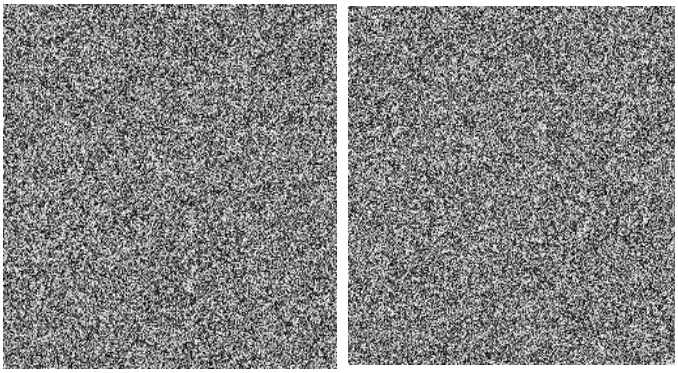
Figure 4-4: (a) Row and Column Shuffling; (b) Bit XOR; (c) S-Box substitution; (d) DNA Encoding (Encrypted image).

Figure 4-3 [18] illustrate that the original image is cameraman image of 256x256. And after applying confusion (row and column shuffling) on original image we got row and column shuffled image as shown in Figure 4-4(a). After applying diffusion (bitxor operation) on scrambled image we got more scrambled image as shown in Figure 4-4(b). After applying S-Box substitution we got further scrambled image as shown in Figure 4-4(c). At last, we applied DNA Encoding and got fully encrypted image as shown in Figure 4-4(d).

Figure 4-5: Original Image (Peppers) [5]



(a) (b)



(c) (d)

Figure 4-6: (a) Row and Column Shuffling; (b) Bit XOR; (c) S-Box substitution; (d) DNA Encoding (Encrypted image).

Figure 4-5 [5] illustrate that the original image is peppers image of 256x256. And after applying confusion (row and column shuffling) on original image we got row and column shuffled image as shown in Figure 4-6(a). After applying diffusion (bitxor operation) on scrambled image we got more scrambled image as shown in Figure 4-6(b). After applying S-Box substitution we got further scrambled image as shown in Figure 4-6(c). At last, we applied DNA Encoding and got fully encrypted image of 256x256 as shown in Figure 4-6(d).

Chapter Five

5 IMPACT OF PROJECT ON ENVIRONMENT AND SOCIETY

The influence of deep learning and DNA cryptography-based image encryption schemes on the environment and society is multidimensional, with both encouraging and damaging consequences. On one hand, these innovative encryption techniques offer better security and concealment for digital images, certifying that complex information remains secured during broadcast and storage. This can have a affirmative societal impact by safeguarding personal data, logical property, and subtle government information, thereby improving trust in digital communication systems.

From an environmental outlook, the approval of deep learning and DNA cryptography-based encryption schemes can contribute to reducing energy feasting. Deep learning procedures, such as convolutional neural networks (CNNs), have shown significant developments in image recognition and processing tasks, allowing more effective and precise encryption processes.

Moreover, DNA cryptography-based encryption schemes influence the characteristic properties of DNA molecules for data storage and encryption. DNA has the potential to store vast amounts of information in a compressed and energy-efficient manner. By consuming DNA as a medium for encryption, these schemes have the potential to curtail the dependence on traditional electronic storage devices, which often consume significant amounts of energy during process and need frequent upgrades.

However, it is significant to consider the potential drawbacks and challenges accompanying with these technologies. Deep learning algorithms, though highly effective in image processing tasks, want significant computational possessions, with high-performance computation systems and significant data centers. The act of such structure can have a

substantial environmental impact, including amplified energy consumption and carbon emissions.

Moreover, the employment of DNA cryptography-based encryption schemes presents its own set of contests. DNA synthesis and sequencing processes, which are integral to these schemes, involve specialized laboratory equipment and materials. The manufacture and disposal of these materials can have environmental consequences, mainly if not managed properly. Additionally, the scalability and cost-effectiveness of DNA-based encryption methods are immobile areas of active research, which may limit their widespread acceptance in the near future.

From a societal viewpoint, the adoption of these advanced encryption techniques can also have inferences for accessibility and inclusivity. The computational requirements and specialized knowledge necessary for implementing and utilizing deep learning algorithms and DNA-based encryption schemes may posture barriers to entry for individuals and societies with limited resources or technological knowledge. Certifying equal access and helping digital literacy will be crucial to lessen any potential societal differences that may arise from these advancements.

The impact of a DNA Cryptography based image encryption scheme on the environment and society is a crucial aspect that needs to be carefully considered. Here are some potential impacts of a DNA cryptography-based image encryption scheme:

Environmental Impact: DNA-based image encryption schemes have the potential to contribute positively to the environment. Since DNA has an incredibly high information density, it allows for the storage of large amounts of data in a compact form. This can significantly reduce the physical storage requirements, leading to a smaller carbon footprint associated with data centers and storage facilities. By utilizing DNA as a storage medium, the need for traditional electronic storage devices, which require raw materials and energy for production, can be reduced.

Data Security and Privacy: DNA-based encryption schemes have a significant impact on data security and privacy. With the increasing threat of cyberattacks and data breaches, robust encryption methods are essential. DNA-based encryption provides a high level of security, making it extremely difficult for unauthorized individuals to decrypt the encrypted

data. By ensuring the security and privacy of sensitive information, these encryption schemes contribute to building trust and protecting individuals' rights in the digital world.

Long-Term Data Preservation: DNA has exceptional properties that make it suitable for long-term data preservation. Unlike traditional storage media, DNA can withstand extreme environmental conditions and has demonstrated stability over thousands of years. DNA-based encryption schemes enable the preservation of valuable information for future generations. This can be particularly significant for preserving cultural heritage, scientific data, and historical records, ensuring their availability and accessibility over extended periods.

Challenges and Limitations: While DNA-based encryption schemes offer numerous benefits, there are challenges and limitations that need to be addressed. The process of DNA synthesis and sequencing requires specialized laboratory equipment and expertise, which may have associated environmental impacts in terms of energy consumption and waste generation. Additionally, the cost of DNA synthesis and sequencing is currently high, which may limit the widespread adoption of these encryption schemes.

Ethical Considerations: The use of DNA, a fundamental component of life, for data storage and encryption raises ethical considerations. Researchers and practitioners must adhere to strict ethical guidelines and regulations to ensure the responsible use of DNA-based encryption technologies. This includes obtaining informed consent for the use of DNA samples, respecting privacy rights, and considering the potential consequences and implications of manipulating genetic material.

Accessibility and Inclusion: The adoption of DNA-based encryption schemes should consider accessibility and inclusion to ensure that individuals and communities from diverse backgrounds can benefit from the technology. Efforts should be made to overcome barriers such as cost, technical expertise, and infrastructure limitations, ensuring that the benefits of secure data encryption and preservation are available to all segments of society.

In conclusion, DNA cryptography-based image encryption schemes have the potential to make a positive impact on the environment and society. They offer high-level data security and privacy, contribute to long-term data preservation, and reduce the physical storage requirements associated with traditional storage methods. However, challenges such as cost, technical complexity, and ethical considerations must be addressed to ensure

responsible implementation and maximize the benefits for society while minimizing potential drawbacks.

Chapter Six

6 CONCLUSION AND FUTURE WORK

In conclusion, the thesis discovers the integration of deep learning and DNA cryptography in the background of image encryption. The proposed encryption scheme validates promising results in terms of security, efficiency, and robustness. By leveraging the competences of deep learning algorithms, such as convolutional neural networks, the scheme achieves actual transformation of input images into cipher images, making them resistant to several cryptographic attacks. Furthermore, the integration of DNA cryptography techniques boosts the overall security and robustness of the encryption system, using the unique properties of DNA molecules for secure information transmission.

The experimental assessments directed throughout the research provide valuable insights into the performance and effectiveness of the anticipated scheme. The results reveal its potential as a reliable and efficient image encryption solution. However, additional research and improvements are obligatory to fully explore and address the challenges and limitations acknowledged during the study.

DNA-based image encryption schemes offer several advantages. They provide high information density, allowing large amounts of data to be stored in a compact form. DNA's inherent error correction mechanisms enhance the reliability and robustness of the encryption scheme. Furthermore, the physical properties of DNA make it suitable for long-term data storage applications.

These encryption schemes exhibit resistance to various types of attacks, including brute force and statistical attacks, due to the complexity of the encryption algorithms and the vast search space of DNA sequences. The use of DNA as the medium for encryption adds an additional layer of security, as DNA sequencing and decoding require specialized laboratory equipment and expertise.

However, challenges remain, including the complexity and computational requirements of the encryption and decryption algorithms, as well as the cost associated with DNA synthesis and sequencing. Ongoing research and advancements in DNA synthesis and sequencing technologies are necessary to address these challenges and further refine DNA cryptography-based image encryption schemes.

The potential applications of DNA cryptography-based image encryption are vast, ranging from secure cloud storage and data transmission to preserving cultural heritage and scientific data. These encryption schemes hold the potential to revolutionize the field of secure information exchange, enabling individuals and organizations to protect their data in an increasingly interconnected and digital world.

However, challenges such as the cost of DNA synthesis and sequencing, technical complexities, and ethical considerations must be addressed to facilitate the widespread adoption of DNA-based encryption schemes. Continued research and development in optimizing encryption algorithms, error correction mechanisms, and scalability are necessary to enhance the practicality and efficiency of these schemes.

Moreover, efforts should be made to ensure inclusivity and accessibility, making the benefits of DNA cryptography-based image encryption available to all segments of society. This entails addressing barriers such as cost, technical expertise, and infrastructure limitations to promote equitable access to secure data storage and transmission.

In summary, DNA cryptography-based image encryption schemes provide a promising solution for secure information transmission and storage. With their unique advantages and potential for enhancing data security, these schemes have the potential to revolutionize the field of secure data encryption and storage in the future.

6.1 Future Work

While the thesis creates a solid foundation for the integration of deep learning and DNA cryptography in image encryption, future work should focus on improving the proposed scheme, conducting thorough security analyses, discovering hybrid approaches, inspecting real-world applications, and leading extensive performance evaluations. Addressing these areas of research will contribute to the advancement and practical implementation of deep learning and DNA cryptography-based image encryption schemes, confirming their viability and effectiveness in secure information transmission.

The field of DNA cryptography-based image encryption schemes holds immense potential for future research and development. Here are some directions for future work in this area:

Optimization of Encryption Algorithms: Further research can focus on optimizing the encryption algorithms used in DNA-based image encryption schemes. This includes exploring more efficient and secure substitution, permutation, and diffusion techniques to enhance the encryption process. Developing novel algorithms that strike a balance between security and computational efficiency is crucial for practical implementation.

Error Correction and Noise Reduction: Improving error correction mechanisms and minimizing noise in DNA synthesis and sequencing processes is a key area of future work. Enhancing the reliability and accuracy of the encoded DNA sequences will result in higher fidelity decryption and better preservation of the original image during encryption and decryption processes.

Scalability and Cost Reduction: DNA synthesis and sequencing technologies have made significant progress, but further advancements are needed to address scalability and cost limitations. Exploring new synthesis methods and sequencing techniques that can reduce the overall cost and increase throughput will make DNA-based image encryption more practical for widespread adoption.

Security Analysis and Vulnerability Assessment: Conducting comprehensive security analyses and vulnerability assessments of DNA-based encryption schemes is crucial. This includes evaluating the resistance against various cryptographic attacks, such as differential and linear attacks, and identifying potential weaknesses or vulnerabilities. Such assessments will lead to the development of more robust encryption schemes.

Integration with Other Technologies: Exploring the integration of DNA cryptography-based image encryption with other emerging technologies, such as artificial intelligence, machine learning, or blockchain, can further enhance the security and applicability of the encryption schemes. These integrations can enable advanced encryption methods, automated key generation, and secure data sharing mechanisms.

Practical Applications and Real-World Implementations: Future work should focus on developing practical applications and real-world implementations of DNA-based image encryption schemes. Exploring use cases in areas such as secure cloud storage, data

transmission over untrusted networks, and secure image sharing platforms can demonstrate the practicality and effectiveness of the technology.

In summary, the future work in DNA cryptography-based image encryption schemes should address optimization of encryption algorithms, error correction, scalability, security analysis, integration with other technologies, and practical applications. Continued research and development in these areas will drive the advancement and adoption of DNA-based encryption schemes in secure image transmission and storage domains.

7 REFERENCES

[1] Rahul, B, K. Kuppusamy, and A. Senthilrajan. "Dynamic DNA cryptography-based Image Encryption Scheme using Multiple Chaotic Maps and SHA-256 hash function." Optik (2023): 171253.

[2] Fetteha, Marwan A., et al. "Chaos-Based Image Encryption Using DNA Manipulation and a Modified Arnold Transform." International Conference on Model and Data Engineering. Cham: Springer Nature Switzerland, 2022.

[3] Hasan, Mohammad Kamrul, et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.

[4] Arthi, G., V. Thanikaiselvan, and Rengarajan Amirtharajan. "4D Hyperchaotic map and DNA encoding combined image encryption for secure communication." Multimedia Tools and Applications 81.11 (2022): 15859-15878.

[5] Yousif, Sura F., Ali J. Abboud, and Raad S. Alhumaima. "A new image encryption based on bit replacing, chaos and DNA coding techniques." Multimedia Tools and Applications 81.19 (2022): 27453-27493.

[6] Alrubaie, Asmaa Hasan, Maisa'A. Abid Ali Khodher, and Ahmed Talib Abdulameer. "Image encryption based on 2 DNA encoding and chaotic 2D logistic map." Journal of Engineering and Applied Science 70.1 (2023): 1-21.

[7] Chen, Junxin, Lei Chen, and Yicong Zhou. "Cryptanalysis of a DNA-based image encryption scheme." Information Sciences 520 (2020): 130-141.

[8] Zhu, Shuqin, and Congxu Zhu. "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," Entropy 22.7 (2020): 772.

[9] Zhou, Shihua, Pinyan He, and Nikola Kasabov. "A dynamic DNA color image encryption method based on SHA-512." Entropy 22.10 (2020): 1091.

[10] El-Khamy, Said E., Noha O. Korany, and Amira G. Mohamed. "A new fuzzy-DNA image encryption and steganography technique." IEEE Access 8 (2020): 148935-148951.

[11] Akkasaligar, Prema T., and Sumangala Biradar. "Selective medical image encryption using DNA cryptography." Information Security Journal: A Global Perspective 29.2 (2020): 91-101.

[12] Ahmed, Fawad, et al. "A DNA Based Color Image Encryption Scheme Using A Convolutional Autoencoder." ACM Transactions on Multimedia Computing, Communications and Applications (2022).

[13] Li, Zhen, et al. "A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation." Applied Sciences 10.21 (2020): 7469.

[14] El Kamchouchi, Dalia H, Heba G Mohamed, and Karim H Moussa. "A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion." Entropy 22.2 (2020): 180.

[15] Mohamed, Heba G, Dalia H El Kamchouchi, and Karim H Moussa. "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences." Entropy 22.2 (2020): 158.

[16] Iqbal, Nadeem, et al. "DNA strands level scrambling-based color image encryption scheme." IEEE Access 8 (2020): 178167-178182.

[17] Dua, Mohit, et al. "Differential evolution optimization of intertwining logistic map-DNA based image encryption technique." *Journal of Ambient Intelligence and Humanized Computing* 11 (2020): 3771-3786.

[18] Zefreh, Ebrahim Zarei. "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions." *Multimedia Tools and Applications* 79.33-34 (2020): 24993-25022.

[19] Liu, Qian, and Lingfeng Liu. "Color image encryption algorithm based on DNA coding and double chaos system." *IEEE Access* 8 (2020): 83596-83610.

[20] Wan, Yujie, Shuangquan Gu, and Baoxiang Du. "A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding," *Entropy* 22.2 (2020): 171.

[21] Wang, Xingyuan, and Lin Liu. "Image encryption based on hash table scrambling and DNA substitution." *IEEE Access* 8 (2020): 68533-68547.

[22] Khan, Jan Sher, et al. "DNA and plaintext dependent chaotic visual selective image encryption." *IEEE Access* 8 (2020): 159732-159744.

[23] Zhu, Changjiang, et al. "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme." *Multimedia Tools and Applications* 79 (2020): 7227-7258.

[24] Huang, Lilian, et al. "Chaotic color image encryption scheme using Deoxyribonucleic Acid (DNA) coding calculations and arithmetic over the galois field." *Mathematical Problems in Engineering* 2020 (2020): 1-22.

[25] Patro, K. Abhimanyu Kumar, Bibhudendra Acharya, and Vijay Nath. "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation." *IETE Technical Review* 37.3 (2020): 223-245.

[26] Wen, Wenying, et al. "Colour light field image encryption based on DNA sequences and chaotic systems." *Nonlinear Dynamics* 99 (2020): 1587-1600.

[27] Belazi, Akram, et al. "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE access* 7 (2019): 36667-36681.

[28] Jasra, Bhat, and Ayaz Hassan Moon. "Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system" *Expert Systems with Applications* 206 (2022): 117861.

[29] Yousif, Sura F., Ali J. Abboud, and Raad S. Alhumaima. "A new image encryption based on bit replacing, chaos and DNA coding techniques." *Multimedia Tools and Applications* 81.19 (2022): 27453-27493.

[30] Paul, L. Shane John, et al. "A novel color image encryption scheme using dynamic DNA coding, chaotic maps, and SHA-2." *Multimedia Tools and Applications* 81.26 (2022): 37873-37894.

[31] Iqbal, Nadeem, et al. "On the novel image encryption based on chaotic system and DNA computing," *Multimedia Tools and Applications* 81.6 (2022): 8107-8137.

[32] Namasudra, Suyel. "A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure." Computers and Electrical Engineering 104 (2022): 108426.

[33] Pavithran, Pramod, et al. "A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems." Computer Communications 188 (2022): 1-12.

[34] Garg, Disha, Komal Kumar Bhatia, and Sonali Gupta. "A novel genetic algorithm-based encryption technique for securing data on fog network using DNA cryptography." 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). Vol. 2. IEEE, 2022.

[35] Hassan, Shahriar, et al. "A Hybrid Encryption Technique based on DNA Cryptography and Steganography." 2022 IEEE 13th Annual Information

Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2022.

[36] Lone, Parveiz Nazir, Deep Singh, and Umar Hussain Mir. "Image encryption using DNA coding and three-dimensional chaotic systems." Multimedia tools and Applications 81.4 (2022): 5669-5693.