Ph. D. Thesis on

A Study of Multilevel DNA Cryptosystem for Medical Images

Submitted to

Visvesvaraya Technological University, Belagavi – 590 018

For the award of the degree of

Doctor of Philosophy

Submitted by

Mrs. Sumangala Biradar
USN: 2BL17PEA03

Under the Guidance of

Dr. Prema T. Akkasaligar
Professor

NOVEMBER - 2022

Department of Computer Science and Engineering

BLDEA's V. P. Dr. P. G. Halakatti

College of Engineering & Technology,

Vijayapur-586 103

VISHVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI-590018

B.L.D.E.A 'S
BIJAPUR

B. L. D. E. A's V.P. DR. P. G. HALAKATTI COLLEGE OF ENGINEERING AND TECHNOLOGY, VIJAYAPUR – 586 103

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the thesis entitled "***A Study of Multilevel DNA Cryptosystem for Medical Images***" submitted by Sumangala Biradar, Research Scholar (**2BL17PEA03**), to Visvesvaraya Technological University, Belagavi, for the award of Doctor of Philosophy degree in Computer Science and Engineering, is an original bonafide research work carried out by her during the period 2017-2022. The results embodied in this thesis have not been submitted fully or in part to any Degree or Diploma of this or any other University or Institute.

Research Guide	Head of the Department	Principal
(Dr.Prema T. Akkasaligar)	(Dr.Pushpa B.Patil)	(Dr.V.G.Sangam)
Dr. PREMA T. AKKASALIGAR Professor, Dept. of Computer Science & Engineering, BLDEA's. V.P. Dr. P.G.Halakatti College of Engineering & Technology	Head of Department, Computer Science & Engg B.L.D.E.A's. V.P.Dr. P.G.H.C.E.T VIJAYAPUR	Principal, B.L.D.E.A's. V.P. Dr. P.G.H College of Engg. & Tech VIJAYAPUR-586103.

DECLARATION

I hereby declare that the entire work embodied in this doctoral thesis entitled *'A Study of Multilevel DNA Cryptosystem for Medical Images"* has been carried out by me at BLDEA's V. P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, under the supervision of Dr. Prema T. Akkasaligar. The work presented in the dissertation does not contain the outcome of any work, previously carried out by others/ submitted by the candidate herself for the award of any degree anywhere.

Sumangala Biradar (2BL17PEA03)
Research Scholar,
Department of Computer Science and Engineering,
BLDEA's V. P. Dr. P. G. Halakatti College of
Engineering and Technology, Vijayapur,
Karnataka, India.

Place: Vijayapur
Date: 29|10|2022

ACKNOWLEDGEMENT

With blessings of God, I am in a position to acknowledge the people who are with me through this journey of research. I am certainly the recipient of the dedication, devotion, insight, and hard work of the people around me. My heartfelt gratitude to all those for what I have received over this period.

First of all, I would like to express my deepest sense of gratitude and thanks to my research supervisor, Dr. (Smt.) Prema T. Akkasaligar, for her exceptional patience, tenderhearted supervision and encouragement all through.

I would like to express my sincere gratitude to the Vice-Chancellor, the Registrar, the Registrar (Evaluation), and all officials of Visvesvaraya Technological University (VTU), Belagavi, for their research related timely decisions, cooperation and encouragement during my research work.

Wholehearted thanks to Dr. P. S. Hiremath, Professor, Department of Computer Applications, KLE Technological University, BVB CET, Hubli, who is the true source of inspiration for the researchers of our generation. I took a lot from his scrupulous knowledge and meticulous experience during my entire research phase.

I extend my thanks to the management and the authorities of the BLDE Association, for providing me an opportunity to pursue Ph.D.

I sincerely thank my beloved principal, Dr. V. G. Sangam, and ex-principal Dr. V.P. Huggi whose multidimensional support and unparalleled cooperation kept me active throughout.

I would like to express my sincere gratitude to my doctoral committee experts Dr. (Smt.) Bharati M. Reshmi, Basveshwar Engineering College, Bagalkot, and Dr. Prakash H Unki, BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur for their valuable suggestions and guidance throughout my research phase.

Sincere thanks to the authorities, faculty, and staff of BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, for their untiring support and the pleasant working atmosphere. Special thanks to my fellow researcher, Mrs. Sunanda Biradar for her concern and intellectual support. It would have been impossible without the intellectual support of Dr. R. S. Malladi.

Special thanks to Dr. Rohini Bhusnurmath, Akkamahadevi Women's University, Vijayapura, who shared their valuable time and knowledge with me.

Finally, I share this success with my husband, Mr. Arunkumar G Madagi for his invaluable companionship, warmth support, understanding, and encouragement throughout. My daughter Anushka A Madagi deserve special thanks, who sacrificed so many things of their childhood for me and made this journey a pleasant one.

Sumangala Biradar

CONTENTS

LIST OF FIGURES

Figure No.	Figure Caption

LIST OF TABLES

Table No.	Table Caption

Table No.	Table Caption
Table AI.1	Medical image datasets
Table AII.1	Correlation coefficient of proposed medical image en/decryption using SHA-256
Table AII.2	Performance analysis of proposed medical image en/decryption using SHA-256
Table AII.3	Comparative analysis of proposed medical image en/decryption using SHA-256

LIST OF SYMBOLS

Symbol	Meaning
O(r,c)	Original medical image
E(r,c)	Cipher image
A	Adenine
T	Thymine
G	Guanine
C	Cytosine
x_0, y_0, z_0, w_0	Positional variables of Chen's chaotic map
a_1, b_1, c_1, d_1	Control parameters of Chen's chaotic map
x, y, z, w	Chen's chaotic sequence
p_0, q_0, u_0, v_0	Parameters of Lorenz chaotic map
$\sigma, \alpha,$ t, $\sigma, \beta,$ $\delta, \mu,$ k, ε ρ	Optimistic coefficients of Lorenz chaotic map
p, q, u, v	Lorenz chaotic sequence
s_n	Angular position of the stick
θ_n	Angular momentum after the n^{th} kick
f	Intensity of the kicks on the kicked rotator
Coeff	Correlation coefficient
N	Size of a medical image
r	Width of the medical image
c	Height of the medical image
$P(O_i)$	Probability of scattering of intensity-levels of the medical image
Entropy(O)	Entropy value
K (r, c)	Key image
B (r, c×8)	Binary image
D (r, 4×c)	DNA encoded matrix
Odd(r,c)	Odd image
Even (r,c)	Even image

Symbol	Meaning
M	DNA sequence
IV	Initial vector
H,Hk_1,Hk_2,Hk_3,Hk_4	Hash keys
OC(r,c)	Compressed medical image
A[t]	Message schedule array
$\psi(t)$	Wavelet function
$\varphi(t)$	Scaling function

LIST OF ABBREVIATIONS

Acronym	Expansion
DNA	Deoxyribonucleic Acid
MRI	Magnetic Resonance Imaging
CT	Computed Tomography
PCR	Polymerase Chain Reaction
PRNG	Pseudorandom Number Generator
DRBG	Deterministic Random Bit Generator
PWLCM	Piecewise Linear Chaotic Map
CML	Coupled Map Lattice
LTS	Logistic-Tent system
LSS	Logistic-Sine system
TSS	Tent-Sine system
2D-HSM	Two-Dimensional Henon-Sine Map
2D-SLMM	Two-Dimensional Sine Logistic Modulation Map
NSA	National Security Agency
CNT	Cosine Number Transform
RSA	Rivest, Adi Shamir and Leonard Adleman
LSB	Least Significant Bit
LBG	Linde, Buzo and Gray
AES	Advanced Encryption Standard
ECB	Electronic Code Book
ROI	Region of Interest
RONI	Region of Noninterest
DWT	Discrete Wavelet Transforms
IDWT	Inverse Discrete Wavelet Transform
DHWT	Discrete Haar Wavelet Transform
GA	Genetic Algorithm
DICOM	Digital Imaging and Communications in Medicine
SRM	Structurally Random Matrix

Acronym	Expansion
CS	Compressed Sensing
AES-GCM	Advanced Encryption Standard-Galois Counter Mode
SNR	Signal to Noise Ratio
GDH	Generalized Double Humped
CPU	Central Processing Unit
GPU	Graphics Processing Unit
UACI	Unified Average Changed Intensity
NPCR	Number of Pixel Changing Rate
MSE	Mean Square Error
PSNR	Peak Signal Noise Ratio
CR	Compression Ratio
RLE	Run Length Encoding
DCT	Discrete Cosine Transform
CALIC	Context-Based Adaptive Lossless Image Codec
SPIHT	Set Partitioning in Hierarchical Trees
SDMIE	Selective Digitized Medical Image Encryption
SDMID	Selective Digitized Medical Image Decryption
GUI	Graphical User Interface

ABSTRACT

The advancement in wireless communication networks like 5G and enhancement in bandwidth, leads to rapid development in telemedicine and e-Health services. These services are increasingly being exploited in geographically expanded areas. Where accessibility of the health services are tremendously diminished or even non-existent. The practitioner or medical experts and patient are not physically in communication and their interactions are medicated through electronic forms in a consolidated remote location.

In medical imaging, image types like MRI, CT or ultrasound are used by medical experts for quick and accurate diagnosis of various diseases. The medical images are very important for disease diagnosis, treatments and research. They act as key component of patient records in electronic form. The communication of these medical images is carried out through an insecure opensource network i.e. internet. The digital broadcast of medical image is continuously prone to malwares, cyber criminals and other infringements of security. The communication of medical image across vulnerable channel adds potential risk of undesirable effect and causes important disease related information in the medical image being lost or corrupted. Then, it becomes problematic for medical experts to diagnose the specific disease from corrupted or lost part of medical image. Therefore, security for medical image has become more essential and must fulfil the requirements like integrity, reliability and confidentiality.

Several state-of-art encryption techniques are available. Due to intrinsic properties of medical images such as mass data volume, high pixel correlation among adjacent pixels and high redundancy, these encryption algorithms are not appropriate for medical image encryption. Nowadays a main research challenge is about providing the security, integrity and confidentiality for medical images.

Deoxyribonucleic Acid (DNA) cryptography is an advanced evolving technology in cryptography. It is depending on DNA operations and DNA sequences. In DNA cryptography, data is hidden in terms of DNA sequences by performing biological process. The uniqueness of DNA is appropriate to offer security for medical images.

The main aim of the research study is to develop an efficient and effective system to provide the enhanced higher-level security, integrity and confidentiality for medical images. The

system helps for secure transmission of medical images in real-time applications like telemedicine, e-health services etc.

The workflow consists of, enhancement in security of medical images, enforcing integrity for tamperproof medical images and confidentiality of patient information to prevent from eavesdropper. Along with improvement of security, reduction in computation time is also essential for transmission of medical image through network in less time.

The research work starts with generation of key image using pseudorandom generator. The key image and original medical image are renovated into encoded DNA structures using fixed DNA encoding rules. The pixels of matrices are permuted using Chen's chaotic sequences and diffused using DNA XOR operation. The diffused encoded DNA structures is renovated into cipher image using fixed DNA decoding rules. The performance parameters number of pixels changing rate (NPCR), unified average change intensity (UACI), Chi-square, correlation coefficient, entropy, mean square error (MSE), and peak signal to noise rate (PSNR) are used for security analysis. The key space is sufficient to endure against brute force attack. The time and space efficiency of this method is burden.

To offer superior security for medical image, the original medical image is segmented into ODD and EVEN images based on intensity levels. The fixed DNA encoding rules are applied to construct ODD and EVEN encoded DNA structures. The multiple hyper chaotic sequences are used for permutation process. Encoded DNA structures are diffused by DNA ADD operation. The fixed DNA decoding rule is applied to get the cipher image. The key space is increased due to multiple chaotic sequences. The integrity and confidentiality are not verified. The hash function SHA-256 and SHA-512 generates a hash key for the specific DNA sequence. This hash key is useful to enforce integrity, and specific DNA sequence is useful for confidentiality. For the enhancement of security level of medical image, multilevel security has been developed. The original medical image is bifurcated into two sub images. These sub images are transformed into encoded DNA structures using dynamic DNA encoding rules. The multiple chaotic sequences are utilized for the permutation of encoded DNA structures in permutation process. In diffusion process, DNA ADD operation is applied for the diffusion of structures. The dynamic DNA complementary rules are used to gain a cipher image. The time efficiency of this crypto method is high.

To reduce the time required for encryption algorithm, selective medical image encryption using dual hyper chaos map, dynamic DNA encoding, DNA XOR operation and dynamic complementary rules are proposed. These techniques help to reduce the time required with compromising in security. To provide significant security with reduced time, discreet Haar wavelet transform is proposed to compress the medical image. The dual hyper maps are employed for permutation process and DNA XOR operation for diffusion purpose. The dynamic complementary rules are used to get a cipher image. This leads to enhancement in security with compromising in image quality.

These en/decryption methods are implemented sequentially. In sequential computation, these multilevel approaches take more times to accomplish enhanced security for medical images. For providing the significant security for medical image with less time, the parallel approach is proposed. The original medical image is fragmented into four sub images. These sub images are renovated into DNA sequence matrices using dynamic DNA encoding rules. The pixels of DNA sequence matrices are permuted using four-dimensional multiple chaotic sequences. The DNA XOR operation is applied for diffusion of the DNA sequence matrices. The hash function SHA-512 generates four hash keys, for four different DNA sequences. These keys are used to enforce integrity and four different DNA sequences are used for confidentiality. In parallel approach, multiple threads are created to run encryption process for four sub images parallelly, which reduces the computation time with enhanced security.

The performance of the developed cryptosystems are analyzed using security analysis and time taken for execution. The security analysis depends on resistant of proposed cryptosystems against statistical attacks, differential attacks, and exhaustive attacks. The performance parameters namely, correlation coefficient, histogram analysis, NPCR, UACI, key space, and key sensitivity are utilized to prove the resistant against various attacks. The quality of cryptosystems is measured using MSE, PSNR and entropy. The parallel approach for encryption method is better for providing enhanced higher-level security for medical images with reduced time and resistant to crypto attacks. The work carried out is useful for real-time applications like, virtual consultancy, telemedicine and e-health systems.

Chapter 1

Introduction

An advancement in digital communication leads to online virtual consultancy, telemedicine, and e-Health services. These services are significant in the medical field of electronic world. In medical field, medical imaging types such as MRI, X-rays, CT scans, and ultrasound are important tools used by medical experts for quick and accurate diagnosis of various diseases. Magnetic resonance imaging (MRI) is a non-intrusive medical imaging technique, that perceives strong magnetic field gradients and computer-produced radio waves to produce comprehensive images of the organs and tissues of our body. X-rays are the cheapest and painless medical imaging technique, used to create an image of structures and tissues of our body. Computed Tomography (CT) is a non-intrusive diagnostic imaging technique used in radiology to produce a cross-sectional comprehensive image of the body organs and tissues. Ultrasound also called sonography is a medical imaging technique, that perceives high-frequency sound waves to get an image of inside body organs. These medical images of inside organs are essential for disease diagnosis, treatments, and research. Hence, medical images act as the vital element of patient records in electronic form.

In digital communication, we need to transfer electronic records of patients through a wireless network i.e. Internet. Internet is an insecure network; hence intruders, hackers, and eavesdroppers can access these medical images and alter or manipulate the medical images. Then, it becomes incredible to diagnose the exact diseases from tampered or altered medical images for practitioners and doctors. Thus, security is essential for medical images while transferring through open-source communication networks. The three techniques namely, steganography, watermarking, and cryptography are available to provide security as shown in Fig .1.1.

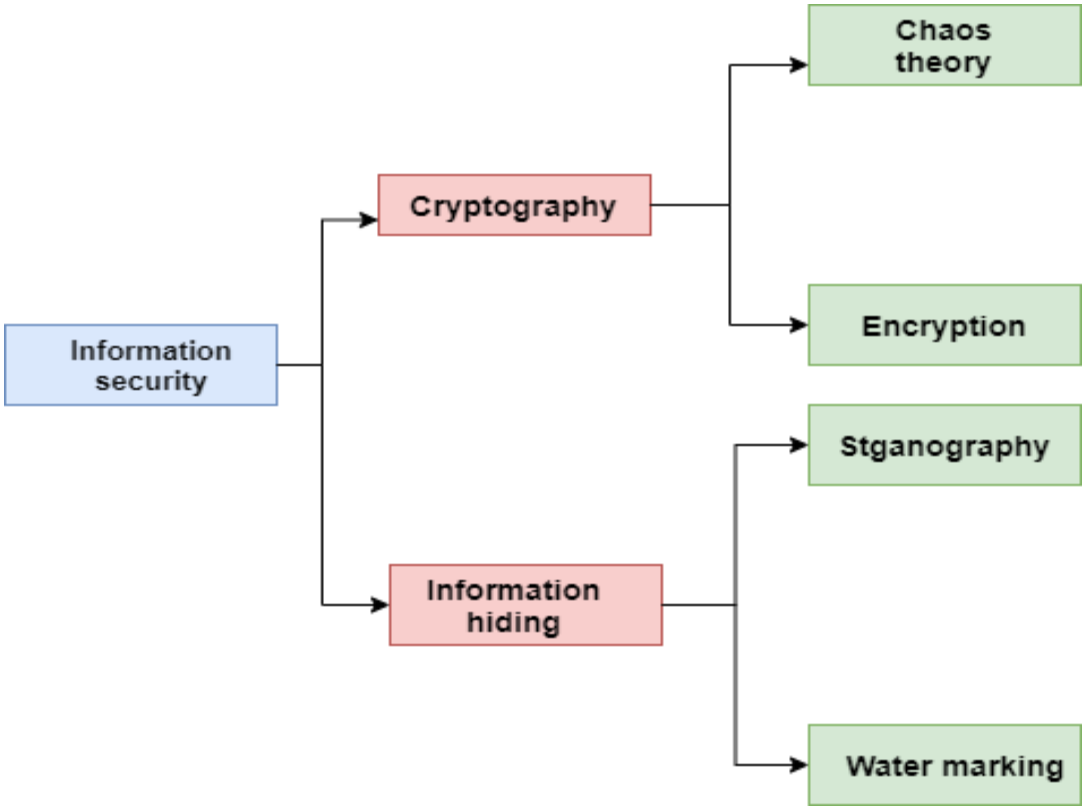


Fig.1.1 Information security systems

Steganography is the art of hiding multimedia information within other multimedia information for secure communication. To conceal secret information, the information is embedded into other cover media. In steganography, information has been hidden in a way that doesn't arouse suspicion. This method is suitable to provide security for information with a limited size. The increase in size of the information degrades the quality of information. It is susceptible to eavesdropping that information is hidden. The eavesdropper can easily reveal concealed information. Medical images contain a very massive data volume. Hence, steganography method is not adequate to stipulate security for medical images.

Watermarking is the process of concealing the piece of data related to identification or authentication in digital information such as images, audio, or video. Watermarking is a marker to prove ownership and prevent copy infringement. The markers are embedded in the information. The categories of watermarking are visible watermarking and invisible watermarking. In visible watermarking the markers are visible. The examples are text or logos. The markers are invisible in invisible watermarking.

Cryptography is the sculpture of science and makes the conversion of readable information into unintelligible information. Only the sender and receiver or intended user will get it in a readable form. The unintended or third-party such as hackers, or intruders are unable to read it, even if they access the information. In cryptography, the term plaintext is used for information of any form like text or image, etc. The term ciphertext is used for unintelligible information. The practice of converting plaintext to ciphertext is called encryption. Similarly, the inverse process of conversion from ciphertext to plain text is known as decryption. Cryptography is more suitable and famous to provide security than steganography and watermarking.

1.1 Cryptography

Cryptography is the Greek word from kryptós, "hidden", and gráphein, "to write". Cryptography is the preparation and learning of principles and methods for secure transmission in the occurrence of adversarial behaviour from malicious third-entities like hackers, intruders, or adversaries (Rivest & Ronald L, 1990). Cryptography entices numerous fields of mathematics including algebra, number theory, statistics, and probability for conversion of plaintext into ciphertext in encryption algorithms (Jeffrey Hoffstein, Jill Pipher & Joseph H. Silverman, 2014).

1.1.1 Goals of Cryptography

The main goals of cryptography for the secure transmission of sensitive and secret information through insecure channels (internet) are:

i) **Authentication:** It is the method of proving or validating the identity of a user's.

ii) **Privacy/confidentiality:** It will give assurance that only intended users have the authority to access the sensitive data**.**

iii) **Integrity:** It is the process of verifying whether unauthorized users altered or modified the sensitive information before it is accessed by intended/authorized users. It gives assurance that only authorized users will modify or alter the sensitive information.

iv) **Non-repudiation:** It is a process to provide the proof of origin of information sent by identified sender. Both sender and recipients later cannot deny the processed information.

Medical image carries a disease related sensitive information. The main requirements for medical image transmission are security, confidentiality, integrity, and non-repudiation. Cryptography is suitable for medical image transmission.

1.1.2 Three Dimensions of Cryptographic System

The three dimensions of cryptographic system are explained below:

a. Type of procedures utilized for converting plaintext into ciphertext

All encryption techniques are generally depending on two principles.

i) **Substitution:** All pixels of the plaintext are replaced with another pixels.

ii) **Transposition:** All pixels of the plaintext are reorganized.

The most important requirement for these techniques is that all operations must be reversible without information loss. The multi-stage substitutions and transpositions are preferable for productive cryptographic systems.

b. Number of keys used

The secret key has a significant role in en/decryption techniques. The sender and receiver use these keys for converting plain text to ciphertext and vice versa. If both encryption and decryption depend on a single key, then encryption is called a secret key conventional encryption. If both encryption and decryption depend on two keys, then encryption is called public key encryption.

c. How the plaintext is processed

The processing of a block of input element i.e. plaintext at a time is called block-cipher. The processing of input elements continuously is called a stream cipher.

The terms encryption and decryption techniques or cryptosystems are used interchangeably in this thesis. The plaintext refers to the medical image in this thesis. The output of encryption refers to encipher/encrypt/cipher text and recovering of plaintext refers to decipher/decrypt.

1.1.3 Types of Cryptosystem

The cryptosystem is categorized into two types namely.

i. Symmetric key or private key or secret key cryptosystem

ii. Asymmetric key or public key cryptosystem

1.1.3.1 Symmetric Key Cryptosystem

Symmetric key cryptosystem is an encryption technique, wherein for encryption and decryption a single key is used. This secret key must be shared among sender and receiver very securely. Hence, the secret key must be transferred through secured communication channels.

In a symmetric key cryptosystem, first, the secret key is circulated among sender and receiver. The sender will encrypt the plain image using a secret key and transfer the encrypted plain image i.e. cipher image through an open-source network. The receiver will decrypt the cipher image using the same secret key to obtain the plain image as exhibited in Fig. 1.2.

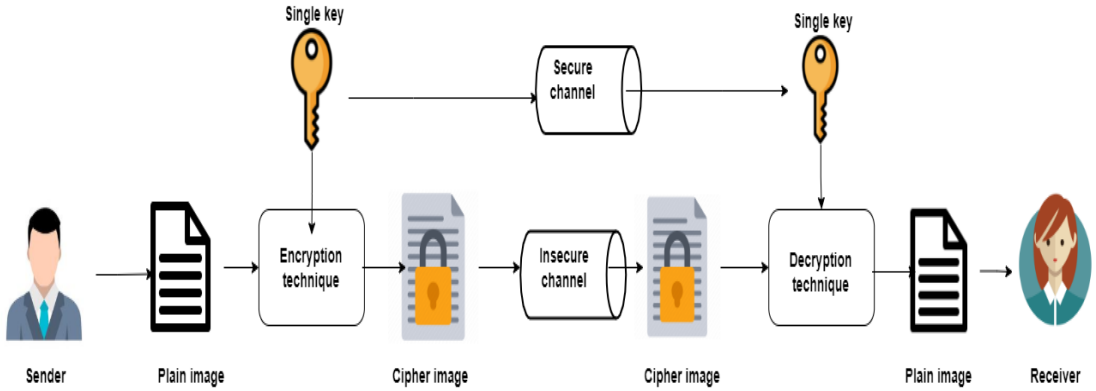


Fig. 1.2 Symmetric key cryptosystem

The pros and cons of a symmetric cryptosystem are specified below:

Pros:

a) A symmetric cryptosystem is fast and efficient for huge data.

b) It utilizes fewer resources of computers for encryption and decryption, compared to a public key cryptosystem.

c) The unintended users know encryption method but are unable to recover the plaintext because the secret key is essential.

d) Different entities use different keys for communication.

Cons:

a) Sharing the secret key among sender and receiver is a big challenge.

b) Generation of different keys for different communication, managing and storing the secret keys are major problems.

c) Due to same key, the origin and authority of the messages are not assured. If sender or receiver denies that message is not sent, then it is a big issue.

d) For communicating the same message with multiple entities, all entities must have the same secret key. Among all these entities if any one entity compromises the secret key then it becomes easy to decrypt the ciphertext.

1.1.3.2 Asymmetric Key Cryptosystem

The asymmetric key cryptosystem is an encryption technique, wherein for encryption and decryption two different secret keys are required. The sender will use an encryption key or public key to encode plain image. The receiver will use a decryption key or private key to decrypt the cipher image. The encryption key is shared among different entities, it is public and hence also called a public key. The decryption key is with owner or receiver, it is private and hence called a private key. The encryption key is shared among different entities using digital certificates or public key servers.

In an asymmetric cryptosystem, the sender will get the public key from the receiver digital certificate or public key server. The sender will encrypt the plain image using a public key to get a cipher image. The cipher image is communicated across an unreliable channel. The receiver will decrypt the cipher image into a plain image with the help of private key as presented in Fig. 1.3. The combination of private key and a public key is known as key pair.

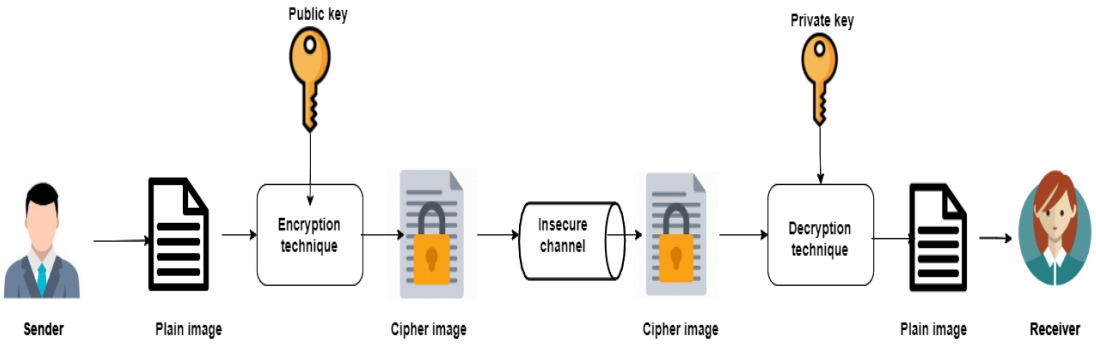


Fig. 1.3 Asymmetric key cryptosystem

The pros and cons of asymmetric cryptosystem are specified below:

Pros:

a) The key distribution problem is solved in an asymmetric cryptosystem. All entities' public keys are available on a public server. So, sender can access it easily and security is necessary for public keys.

b) The origin and authentication are assured using a digital signature. The recipients can validate that, the message is sent from an intended sender.

c) The digital signature also assures that message does not tamper during transit.

d) The security is increased because the private key is kept secret and not necessary to exchange the private key and never expected to disclose the private key.

Cons:

a) The authentication of public key is very important. All entities must verify that the public key belongs to an intended user.

b) It is infeasible for bulk data and slow as compared to a symmetric cryptosystem.

c) Recovering a private key is not possible if it is lost. Then, decrypting messages is impossible.

d) It utilizes more resources of computers for encryption and decryption compared to a single key cryptosystem.

The asymmetric cryptosystem is suitable to stipulate security for small information. The symmetric cryptosystem is a traditional system and appropriate to stipulate security for large information. The medical images are large in data volume. Hence, a symmetric cryptosystem is appropriate to stipulate security for medical images.

1.2 Chaos Theory

The chaos theory is a part of mathematics, converging on the performance of randomness and irregularities of a dynamic system that depends on initial conditions. These theories are extremely sensitive to primary conditions. Slight modifications in initial conditions, for example, because of faults in measurements or due to roundoff mistakes in mathematical calculation, can produce extensively deviating consequences for dynamic systems. In general, interpreting an elongated period forecast of the behavior of a chaotic system is incredible (Kellert & Stephen H, 1993). The deterministic behavior of chaotic systems makes them unpredictable (Bishop & Robert,2017). This behavior is recognized as deterministic chaos, or simply chaos. The ″chaos" means "a state of disorder". The butterfly effect of chaos as shown in Fig.1.4, explains how a minor variation in one state of

Fig. 1.4 Butterfly effect of chaos theory

Image credit: en.wikipedia.org/wiki/Chaos_theory

a deterministic nonlinear system can result in larger variances in upcoming states. The main features of chaos theory are confusion and diffusion. These two properties play an important role in cryptography.

The chaos theory is an irregular, pseudorandom, and nonlinear dynamic system. These systems depend on preliminary conditions. The preliminary conditions of system parameters are secret keys, but size of the key is small. Hence, attackers can guess the key by exhaustive search methods. To resolve this problem, DNA cryptography is evolved.

1.3 DNA Cryptography

Deoxyribonucleic Acid (DNA) cryptography is an advanced evolving technology in cryptography. It depends on DNA operations and DNA sequences. In DNA cryptography, data is hidden in terms of DNA sequences by performing a biological process. DNA cryptography is featured based on DNA of human beings. DNA is a complex hereditary unit made of two long polynucleotide strands. These strands spiral together to build a double helix structure. The double helix carries the genetic information for growth, reproduction, and working of all human beings or living creatures. The double helix structure resemblance like a ladder and each side of ladder is formed of molecules of sugar, phosphate, and base form of molecule rungs as represented in Fig. 1.5.

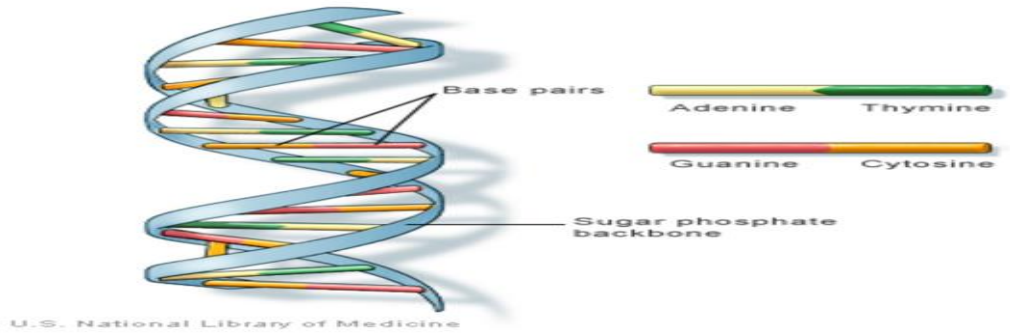


Fig. 1.5 DNA structure

Image credit: www.healio.com/hematology-oncology/learn-genomics/genomics-primer/dna-definition

Each polynucleotide strand is composed of a unit called nucleotides. The nucleotide contains a phosphate group, a nitrogenous base, and a sugar group. The nitrogenous bases are also known as nucleobases as shown in Fig. 1.6. The four bases of nucleobases are adenine (A), thymine (T), guanine (G), and cytosine (C). The nucleotides are connected in

a chain by intramolecular force. The links are between one nucleotide sugar with phosphate next to build a sugar-phosphate backbone. To make double-stranded DNA with hydrogen bonds, nitrogenous bases of two separate polynucleotide strands are joined together, according to base pairing rules (A with T and C with G). The complementary nitrogenous bases are decomposed into two sets namely, pyrimidines and purines. In DNA, the pyrimidines are a combination of thymine and cytosine, known as pyrimidines. The combination of adenine and guanine is called purines as described in Fig 1.6.

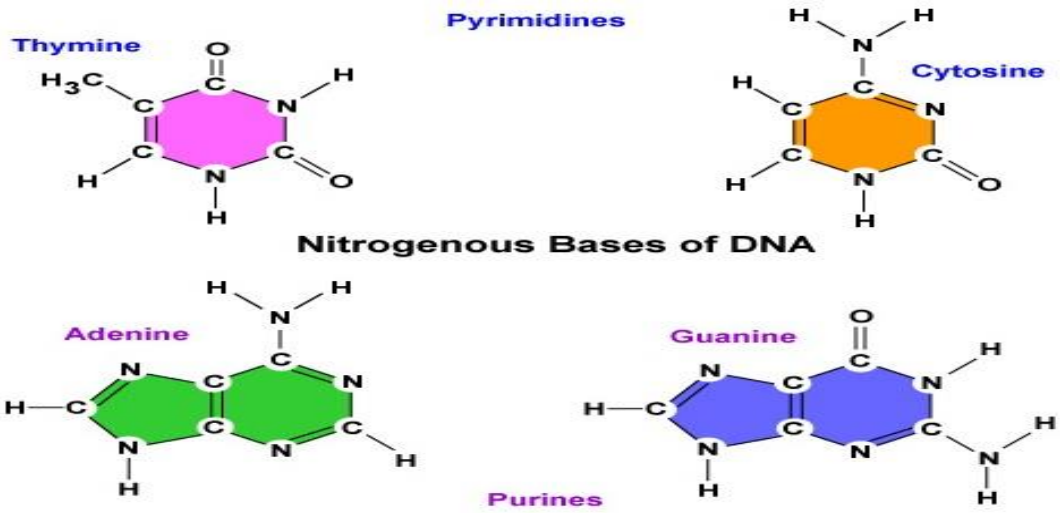


Fig. 1.6 Nitrogenous bases of DNA

Image credit: https://qr.ae/pvOFWK

Due to advancements in information security, the traditional encryption methods based on mathematical and logical operations are breakable. DNA cryptography rely on DNA computation. DNA computation is performed using biological operations. In 1994, DNA computing is used to find a solution for the combinatorial problem "Hamiltonian path" using molecular computation (Adleman,1994). In 1995, DNA computation is extended to find a solution for an NP-complete problem called "satisfaction" using DNA molecules (Lipton. 1995). DNA computation is utilized to achieve a higher-level security mechanism for data and image. Hence, DNA computation is useful to develop unbreakable encryption algorithms. DNA cryptography is based on the combination of both biological and logical operations, which are appropriate to offer security for medical images. The medical image carries disease related sensitive information. If the intruder's tamper or modify medical images during transmission then for practitioners, diagnosing exact diseases from the

tampered medical images is extremely not possible. Hence providing integrity for medical images is also very essential.

1.4 Hash Function

The hash function is appropriate to verify the integrity of medical images. A hash function is one-way and versatile cryptographic algorithm. It takes the input of varying length and produces a compressed unique output of fixed length as depicted in Fig 1.7. The output of a hash function is called as a hash code, or hash key, or hash value, or hash digest. The hash function is a logical process, which is employed to:

i) To store passwords securely in database.

ii) Ensure integrity while transmitting information through insecure channels.

iii) Used as a digital signature to prove authentication.

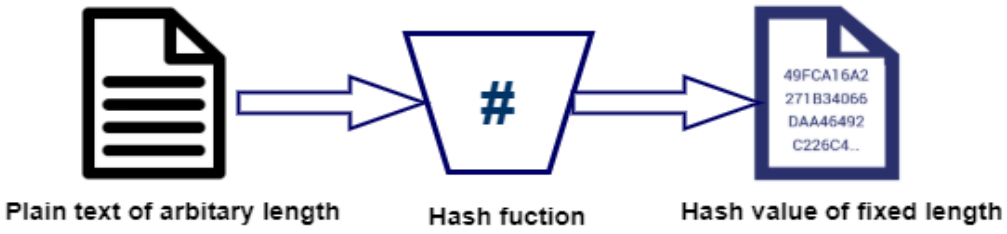


Fig. 1.7 Hashing function

Properties of Hash function

The main properties of hash function are given below:

a. **Determinism** — The hash function is deterministic. The hash function always produces a fixed size output and is independent of input image size.

b. **Pre-image resistance** — The hash function is preimage resistance, which means recovering the original input medical image from hash value is highly infeasible. Hence, hash functions are one-way and irrevocable functions.

c. **Collision resistance** — A collision occurs when two objects collide. If two unique input medical images produce the same output, then a collision occurs. The hash function is collision resistant. Thus, for each input medical image a unique hash key is generated as an output. The main concern is if intruders

could create a malicious medical image with a reproduction hash value that matches with a genuine (safe) medical image then such hash values are passed as pretend genuine because the hash value would match. So, to prevent such attacks a good and trustworthy hashing algorithm is required to resist to these collisions.

d. **Avalanche Effect** — The small changes made to an original medical image, cause a massive modification in output medical image.

e. **Efficiency** — Hash functions are easy to compute a fixed size hash value for given varying size input medical image and computation of hash value is quick.

The desirable property of a hash function is a scientific mechanism to provide integrity for medical images.

1.5 Chaotic Map Based Encryption Methods

The main aim of study is to develop encryption methods to accomplish the requirements of medical images like high-level security, confidentiality, and integrity. The chaotic maps have good confusion properties, hence appropriate to offer higher-level security for medical images. Several encryption methods using chaotic maps are available for the enhancement of medical image security.

1.5.1 Chen's Chaotic Map

The Chen's hyper chaotic map has comprehensive density and blended property because of the optimistic Lyapunov exponent. Chen's hyper chaotic sequences are enormously composite, hard to envisage and discover. In medical image encryption methods for security purpose, the hyperchaotic system is utilized. The pseudo randomness of chaotic maps is depending on permutation and diffusion process. In permutation method, a chaotic sequence is useful to rearrange the pixels of original medical image based on index of the pixels. In diffusion method, a chaotic sequence is useful for alteration of the original medical image pixel values.

Chen's hyper-chaotic map is depicted in Eqs. (1.5.1) - (1.5.4):

$$x_{i+1} = a_1(y_i - x_i) \tag{1.5.1}$$

$$y_{i+1} = x_i z_i + d_1 x_i + c_2 y_i - w_i \quad (1.5.2)$$

$$z_{i+1} = x_i y_i - b_1 z_i \quad (1.5.3)$$

$$w_{i+1} = x_i + k \quad (1.5.4)$$

where x_0, y_0, z_0, and w_0 are positional variables and a_1, b_1, c_1 and d_1 are control factors. The value of k must be in the range of -0.7 to 0.7. The three-dimensional Chen's chaotic map attractor is exposed in Fig 1.8.

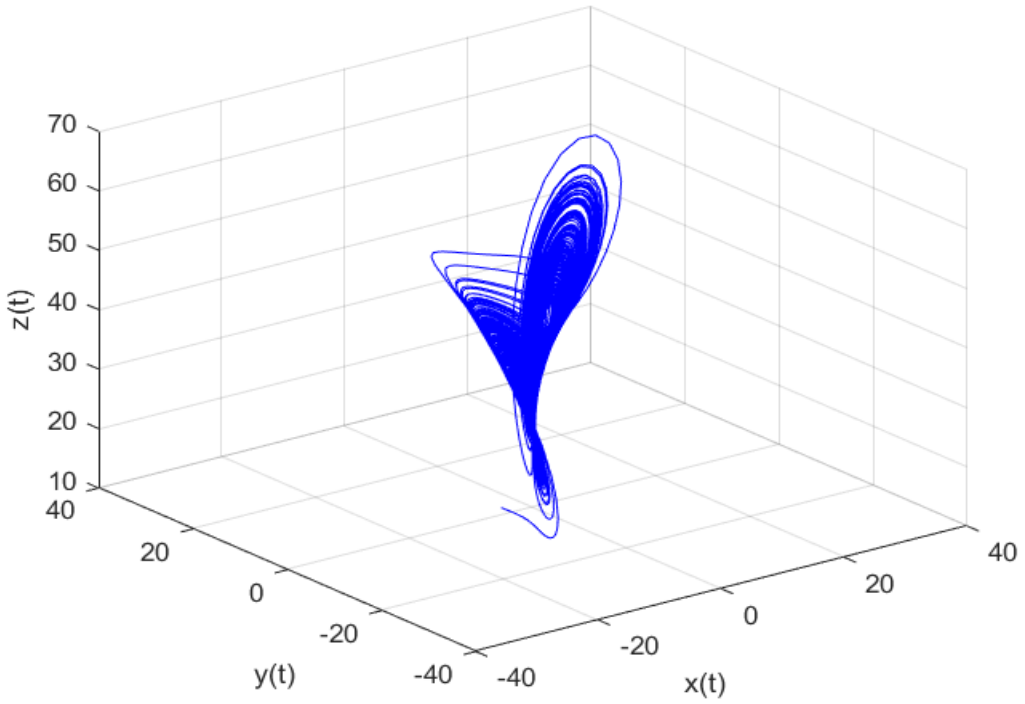


Fig. 1.8 3D Chen's chaotic map attractor

1.5.2 Lorenz Chaotic Map

The Lorenz chaos system is a multifaceted high dimensional chaotic map. The chaotic sequences of Lorenz's chaotic mar are more unpredictable. Lorenz chaotic map has complex pseudo randomness, impulsive permutation, and diffusion process. Thus, suitable to stipulate enhanced security for medical images. The 3D Lorenz chaotic map is elucidated in Eqs. (1.5.5) - (1.5.7).

$$p_{i+1} = \sigma(q_i - p_i) \tag{1.5.5}$$

$$q_{i+1} = \alpha p_i - q_i - p_i u_i \tag{1.5.6}$$

$$u_{i+1} = p_i q_i - t u_i \tag{1.5.7}$$

where p_0, q_0, and u_0 are positional variables and σ =10, α = 28, t = 8/3 are optimistic coefficients. The three-dimensional Lorenz chaotic map attractor is exhibited in Fig.1.9.

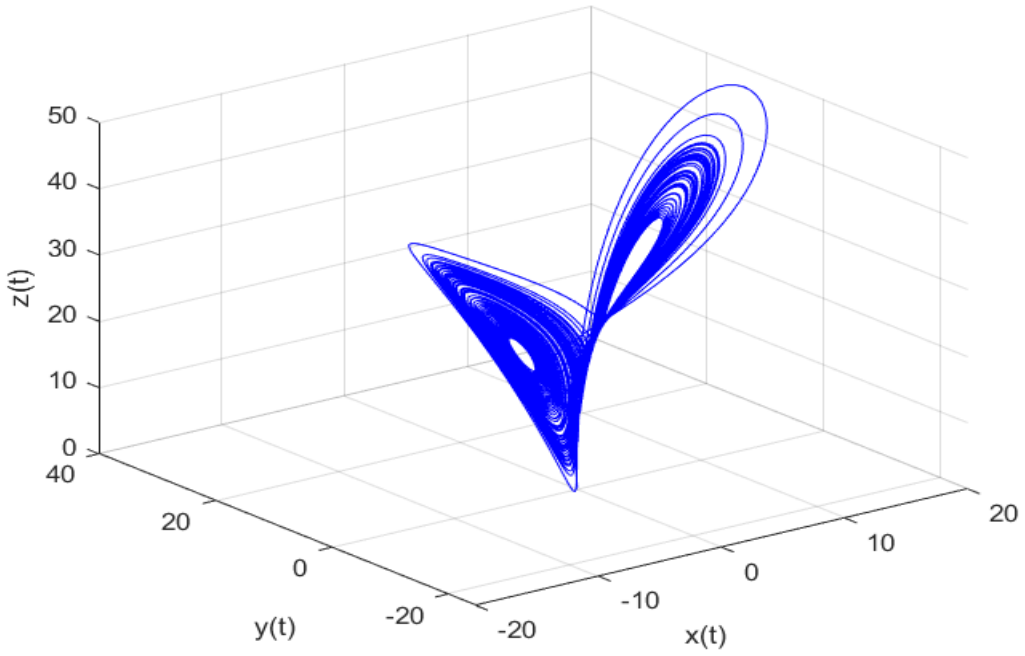


Fig. 1.9 3D Lorenz chaotic map attractor

The 3D Lorenz chaotic system is extended by adding a linear feedback controller '*v*' and a first-order nonlinear differential state equation concerning '*v*'. The extension of 3D Lorenz chaotic system is called a 4D Lorenz chaotic system. The 4D Lorenz chaotic system is described using Eqns. (1.5.8) -(1.5.11).

$$p_{i+1} = \sigma(q_i - p_i) - \varepsilon v_i \tag{1.5.8}$$

$$q_{i+1} = p_i u_i - \rho q_i \tag{1.5.9}$$

$$u_{i+1} = \alpha - p_i q_i - \delta u_i \tag{1.5.10}$$

$$v_{i+1} = \beta p_i - \mu v_i \quad (1.5.11)$$

where p_0, q_0, u_0 and v_0 are positional variables and σ =10, $\alpha = 28, \delta = 1, \mu = 0.1, \beta = 0.1$, $\varepsilon = 20.6$ and $\rho = 1$ are optimistic coefficients.

1.5.3 Taylor Chirikov Map

The Taylor Chirikov Map is a discrete map. This map describes Poincare plane of the faction of a direct reflex approach and is characterized as kicked rotator. The kicked rotator is made of a gravitational force and a free stick. It pivots frictionless over the axis of a plane on one tip and kicked periodically on further tip. The chaotic sequences of the Taylor Chirikov map are enormously complicated and ridiculous to speculate and explore. The standard hyper chaos map is exemplified by Eqs. (1.5.12-1.5.13).

$$s_{n+1} = s_n + f sin(\theta_n) \quad (1.5.12)$$

$$\theta_{n+1} = \theta_n + s_{n+1} \quad (1.5.13)$$

where the variable s_n is the angular position of the stick and θ_n is its angular momentum after the n^{th} kick. The constant f is the intensity of the kicks on the kicked rotator. The value of f controls the degree of chaos.

1.6 DNA Operations

In the early 1990s, mathematician and biologist Leonard Adelman, is the father of DNA computing, became captivated by the analogues between DNA and computing method (Adelman L, 1994). DNA computation uses DNA sequences and base pairing of double helix structure. The DNA sequences contain four basic nucleotide elements i.e. adenine (A), thymine (T), guanine (G), and cytosine (C). In double helix structure, A and T are complements and correspondingly G and C are complements. In binary form 0 and 1 are complements, hence 00 and 11 are complements and 01 and 10 are complement. So, the four basic nucleotide elements A, T, G, and C are coded as 00,11,01 and 10. Based on this perception, 4! = 24 various encoding forms are attainable. Due to complementary base paring, only eight encoding forms meet the complementary base pairing. The eight DNA encoding rules are specified in Table 1.1.

Table 1.1 DNA encoding rules

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

The DNA encoding rules are used for converting medical images into DNA structures. The DNA structure of a medical image is unique like DNA of a human being. The DNA diffusion operations DNA ADD, DNA SUB, and DNA XOR are applied to change the pixel values as specified in Table 1.2, Table 1.3, and Table 1.4 respectively. Hence, DNA encryption method is appropriate to offer a higher-level security for medical images.

Table 1.2 DNA ADD operation

ADD	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

Table 1.3 DNA SUB operation

SUB	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C

Table 1.4 DNA XOR operation

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

During encryption, for diffusion of medical images, if DNA ADD operation is used then during decryption DNA SUB operation is used as an alternative for DNA ADD.

The combination of chaotic map and DNA cryptography is invulnerable to different types of attacks. This combination works for medical images to provide security. Medical images contain a very huge data volume. The computation time is very high. Reducing the computation time of encryption methods is a critical issue for medical images. The compression and parallel computation can reduce computation time.

1.7 Lossless Compression Method

The medical images are highly correlated and contain the bulk of disease-related very sensitive data volumes. Thus, storing medical images require more space and transmission and computation time of encryption techniques requires more time.

For reduction of time and space requirements, compression of medical image is suitable. Medical images contain diseases related very sensitive information. Hence, lossless compression is essential to revert the original medical image after decompression. The discrete Haar wavelet transform based compression is an efficient method for lossless compression.

The Haar wavelet transform was first invented by mathematician Alfred Haar. The Haar defined the Haar wavelet theory in 1909, and this was the easiest of all wavelets. Mathematical interpretation of the Haar technique is characterized as Haar wavelet transform (HWT). In HWT, for compression of medical image, the medical image is converted into signals. These signals are fragmented into a sequence of wavelet

coefficients. The transformed medical image is divided into two bands namely L and H. These bands are passed through a series of low-pass filters (LPF) and high-pass filters (HPF). In low pass filtering, coarse coefficients are extracted by calculating mean between neighboring pixels. In high pass filtering, detail coefficients are extracted by calculating the difference between neighboring pixels. The resultant of these filters is reduced by two. Further, the output is once again divided into four sub bands namely, LL, HL, LH, and HH as shown in Fig.1.10. This process is repeated for entire medical image.

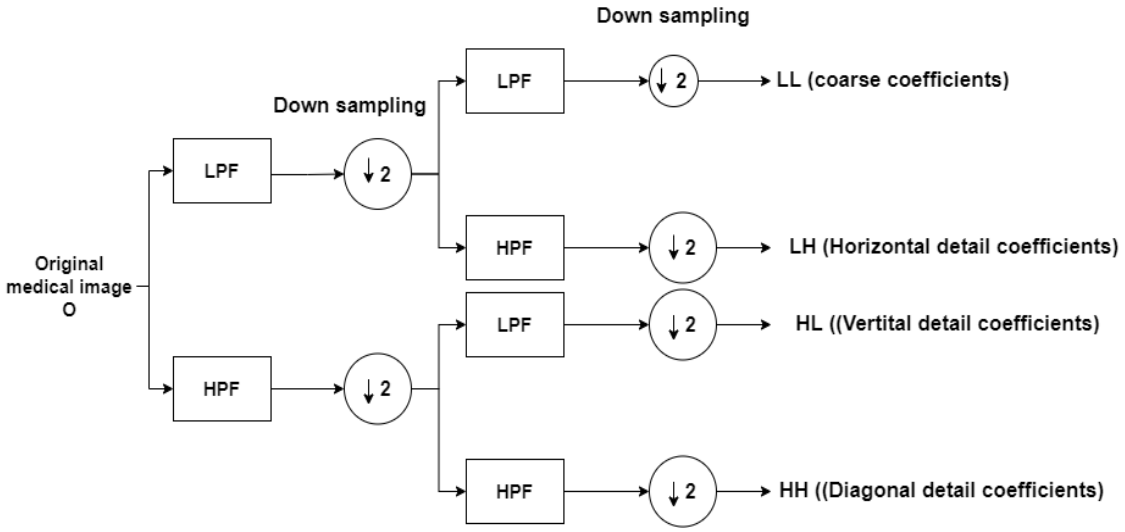


Fig. 1.10 DHWT compression

The LL subbands contain coarse coefficients and remaining subbands contain detail coefficients. These wavelet coefficients near to zero or zero are altered with a level-dependent threshold to get a sparse matrix. In this manner, the medical image is compressed and for decompression, same compression method is performed in reverse order.

1.8 Parallel Computation

Generally, system problems are divided into discrete sets of instructions. These instructions are processed, one by one in central processing unit (CPU) of the computer as shown in Fig 1.11. The processing of instructions one after another in a sequence is known as serial computation. In serial computation, only one instruction is executed at a time. Only 25 % of the CPU is utilized for the execution of an instruction. Hence, the execution time required to solve the problem in serial computation is high.

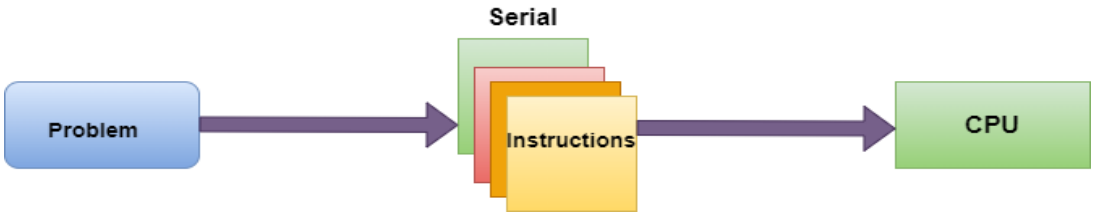


Fig. 1.11 Serial computation of instructions

Instead of executing the discrete instructions in serial, we can run instructions parallelly in parallel computation. In parallel computation, a set of independent instructions will run simultaneously by multiple processors as shown in Fig 1.12. At a time, a set of instructions are executed concurrently. The 100% of the CPU is utilized for the execution of instructions. Hence, the execution time required to solve problem in parallel computation is reduced.

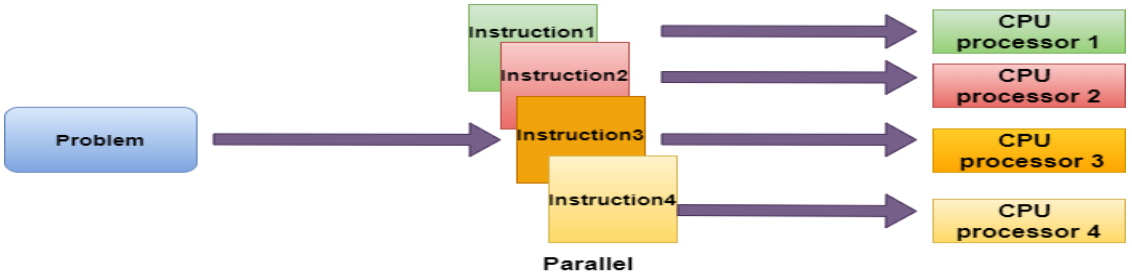


Fig. 1.12 Parallel computation of instructions

The four categories of parallelism are as follows:

i. ***Bit-level parallelism:*** Computation depends on increasing size of the processors. To operate on large size word, which is greater than the variable, the processor reduces the number of instructions.

ii. ***Instruction-level parallelism:*** Based on dynamic and static parallelism, hardware and software approaches are used. The hardware approach is used for dynamic parallelism; the processor dynamically selects an instruction to execute parallelly at runtime. In software approach for static parallelism, the compiler will dynamically select an instruction to execute in parallel.

iii. ***Task parallelism:*** Task parallelism divides the main task into subtasks and allocates each subtask for execution. The processor will perform the execution

of subtasks concurrently. The multiple processors execute multiple subtasks at a time on same data.

iv. ***Data-level parallelism:*** The vectorization technique exploits the parallelism of inline code.

1.9 Performance and Security Analysis

The performance of encryption methods relies on how much it is secure against various attacks. The security analysis is accomplished by cryptanalysis to substantiate the invulnerable to several attacks namely, statistical attacks, differential attacks, and exhaustive attacks.

1.9.1 Statistical Attack

In this attack, crypto analyst tries to exploit the weakness of cryptosystem by analyzing the dissemination of pixels of the cipher image. Crypto analyst verifies whether based on frequency analysis, is it possible to crack the encryption method. The correlation coefficient and histogram metrics are utilized to check the resistant for statistical attack.

1.9.1.1 Correlation Coefficient Analysis

The correlation coefficient measures the statistical association between neighboring pixels of medical images are analyzed. The degree of linear correlation specifies the strength of association among the pixels. The smaller degree means association among pixels is less, means encryption method has good pseudo randomness. The correlation coefficient is defined in Eq. (1.9.1).

$$\text{Coeff} = \frac{N\sum OE - (\sum O)(\sum E)}{\sqrt{N(\sum O^2) + (\sum O)^2}\sqrt{N(\sum E^2) + (\sum E)^2}} \qquad (1.9.1)$$

where ‘O’ is original medical image and ‘E’ is cipher image. The size of a medical image is ‘N’. The scale of coefficient is in the range of +1 and -1. If the coefficient value is +1 then pixels are associated positively. If the coefficient value is -1 then pixels are associated negatively. In positive association, the adjacent pixels move alongside. In negative association, the adjacent pixels move in reverse direction. The correlation coefficient equal to zero designates no correlation.

1.9.1.2 Histogram Analysis

The histogram is pictorial interpretation of frequency distribution of pixels. If the histogram bins are more persistently disseminated in encrypted image, it demonstrates that most of the medical image pixels are reformed, and encryption method enforces the good confusing property.

To evaluate the histogram analysis mathematically chi-square test is accomplished. The chi-square is a statistical hypothesis test used to significantly substantiate the uniform dissemination of pixels of cipher images. It is defined in Eqs. (1.9.2-1.9.3)

$$\chi^2 = \sum_{i}^{256} \frac{(\mathbb{O}_i - \mathbb{E}_i)^2}{\mathbb{E}_i} \tag{1.9.2}$$

$$\mathbb{E}_i = \frac{r \times c}{256} \tag{1.9.3}$$

Where $\mathbb{O}_i$ is the observed frequency distribution bin count of intensity levels and $\mathbb{E}_i$ is the expected frequency distribution bin count of intensity levels. The ideal value of $\chi^2_{(0.05,255)}$ for significance level 5% is 293.2478 (S. T. Kamal et al.,2021).

1.9.2 Differential Attack

In differential attack, crypto analyst verifies chosen cipher text attack and chosen plain text attack. The Unified Average Changed Intensity (UACI) and Number of Pixel Changing Rate (NPCR) metrics are exploited to analyse differential attack.

In differential attacks, significant metrics NPCR and UACI are utilized to validate the strength of encryption methods for medical image against various attacks. The NPCR is elucidated in Eq. (1.9.4)

$$\mathrm{NPCR} = \frac{\sum_i^r \sum_j^c G(i,j)}{r \times c} \times 100\% \tag{1.9.4}$$

where r×c is the dimension of medical image and G(i, j) is specified in Eq.(1.9.5).

$$G(i,j) = \begin{cases} 0, & \text{if } E_{11}(i,j) = E(i,j) \\ 1, & \text{if } E_{11}(i,j) \neq E(i,j) \end{cases} \tag{1.9.5}$$

The UACI is defined in Eq. (1.9.6)

$$\mathrm{UACI} = \frac{1}{r \times c}\left[\sum_{i}^{r}\sum_{j}^{c}\frac{|E_{11}(i,j) - E(i,j)|}{255}\right] \times 100\% \qquad (1.9.6)$$

where 'E' is a cipher image conquered from an original medical image. The selected 1000 pixels of an original medical image are altered and encrypted using the encryption method to get a cipher image 'E_{11}'. The ideal values of NPCR and UACI are 100 and between 33-40 respectively for resistance of chosen cipher-text, known plaintext, and known cipher-text attacks.

1.9.3 Exhaustive Attack

In exhaustive attack, a crypto analyst verifies the feasibility of guessing secret keys by trying all possible combination of keys. The key space and key sensitive analysis validate the resistance of an exhaustive attack.

1.9.3.1 Key Space Analysis

The main security in encryption method rely on length of the key space. The length of key space is dependent on the number of secret keys. If the length of key space is small, then it is vulnerable to brute force attack. Hence, a very large key space is significant to endure from exhaustive attack. According to standard format of IEEE floating point numbers, the precision of 10^{-15} unit is used for each secret key. This precision is used, in this thesis to measure the key space.

1.9.3.2 Key Sensitivity Analysis

In encryption methods, secret keys should be very susceptible to slight changes. It is highly impossible to decrypt an original medical image, with very minor changes in the secret key.

1.10 Encryption Algorithm Quality Measurements

The encryption algorithm quality measurement is also very essential in a cryptosystem. The parameter Entropy is applied to quantify the quality of encryption techniques. The

error rate of medical images is evaluated using indicators Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

1.10.1 Mean Square Error

The MSE and PSNR are used for quality assessment of a medical image against the glitches during transmission over insecure channels. The 'MSE' find outs the error rate between original medical image and cipher image. The larger value signifies a good cryptosystem. The MSE computes nearly the average of squared errors between original digital medical image 'O', encrypted image 'E' and N is size [r, c]. The MSE is elucidated in Eq. (1.10.1).

$$\mathrm{MSE} = \frac{\sum_{\mathrm{N}}[\mathrm{O}(\mathrm{r},\mathrm{c})-\mathrm{E}(\mathrm{r},\mathrm{c})]^2}{\mathrm{N}} \qquad (1.10.1)$$

where ‘N’ is the dimension (r×c) of medical image. The ideal value for MSE to resist against glitches during transmission of a medical image is '0'.

1.10.2 Peak Signal-to-Noise Ration

The PSNR is applied for verification of resistance against additional noise during transmission of medical images. The PSNR is elucidated in Eq. (1.10.2).

$$\mathrm{PSNR} = 10\log_{10}\frac{(256-1)}{\mathrm{MSE}} \qquad (1.10.2)$$

The ideal value for PSNR ranges between 45-60 dB.

1.10.3 Entropy

The entropy is contingency of dispersal of pixels in a medical image. The larger entropy value reveals a more pseudo randomness of dispersal of pixels in a medical image. The entropy is elucidated by Eq. (1.10.3).

$$\mathrm{Entropy}(\mathrm{O}) = \sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{P}(\mathrm{O_i})\log(\mathrm{P}(\mathrm{O_i})) \qquad (1.10.3)$$

where ‘$P(O_i)$’ signifies the contingency of dispersal of pixels in a medical image and 'N' signifies the dimension of medical image. The ideal value for entropy to prove the quality of encryption method is ‘8’.

1.11 Literature Review

An insignificant work is accomplished on chaos theory and DNA cryptography for communication of images securely. Some encryption methods for plain images had been suggested by many authors using DNA-based cryptographic methods.

1.11.1 Digital Image Encryption using DNA Cryptography Technique

DNA cryptography is presently exploited for encryption and decryption of normal digital images. The pixels of DNA sequence matrix blocks are permuted using 1D and 2D chaotic maps and blocks are added using DNA ADD to gain a cipher image (Wang Qian, Qiang Zhang & Changjun Zhou, 2009; Quang et al., 2009; Soni et al., 2013; Gupta, Shreya, & Anchal Jain, 2015). The external key is applied to get the primary value for a chaotic map to produce a chaotic sequence and these sequences are mapped with DNA encoded matrix blocks in permutation process. The encrypted image is attained by adding blocks using XOR operation (Saranya M. R, Arun K. Mohan & K. Anusudha, 2015; Abhishek Jain & Navin Rajpal, 2013). Several DNA masks are produced by chaos logistic map and DNA sequences. The genetic algorithm recognizes best DNA mask for encryption (Saranya et al., 2015; Enayatifar et al., 2014). The pseudo-random number generator (PRNG) is employed to choose DNA code rules to attain the DNA matrix. The 1D chaotic sequences are referred for the permutation of DNA matrix. The encrypted image is obtained using DNA operations (Sukalyan Som, Ayantika Chatterjee & Atanu Kotal, 2013; Mondal Bhaskar, & Tarni Mandal, 2016).

The above literature review shows that 1D and 2D chaotic map methods have limited and discontinuous chaotic ranges. The preliminary values of parameters are used as keys and keys are very small in size, so easily attacked by brute force attacks.

The authors (Zhou Shihua, Qiang Zhang & Xiaopeng Wei, 2010) have presented a DNA self-assembly technology for image encryption. The DNA structure is constructed by mapping the original image using DNA encode rules. Then five DNA tiles i.e. plaintext DNA, DNA tiles of encryption, cipher text DNA tiles, DNA tiles of t key, and DNA tiles of decryption are used to get a cipher image. The authors (Wang Qian, Qiang Zhang & Xiaopeng Wei, 2010) used DNA code rules to generate DNA structure of the original image and anti-complement DNA to get polymerase chain reaction (PCR) DNA sequence.

The fusion of DNA matrix and PCR DNA matrix is performed by using XOR operation. Further, 1D chaotic map sequences are mapped for the permutation of fusion matrix to get cipher image.

The authors (Zhou Shihua, Qiang Zhang & Xiaopeng Wei, 2010) have presented DNA templates to attain encoded DNA matrices and XOR operation is applied to DNA encoded templates to get a cipher image. The authors (Jain Sonal &Vishal Bhatnagar, 2014) have presented DNA complementary rules to renovate input images into DNA sequences and an external key to attain a cipher image. The authors (Anchal Jain, Pooja Agarwal, Rashi Jain &Vyomesh Singh, 2014) have presened image encryption techniques using S-box and DNA approaches. The image is translated into a binary image to conquer a DNA encoded matrix. The static DNA S-box is generated with help of gene sequence from the gene bank. The DNA encoded matrix is substituted from S-box values. Then rows and columns are permuted to get an encrypted image.

The authors (Zhang Linlin, Tiegang Gao & Rui Yang, 2014) have presented DNA coding, vigenere cipher, and chaos map for central dogma-based image encryption. The original image is mapped into a DNA encoded matrix. An amino acid matrix is obtained by executing transcript and interpretation corresponding to central dogma, after randomly removing a base from each pixel. The 3D vigenere cipher is employed to obtain a new codon matrix. The nucleotide base matrix obtained by the new codon matrix is decoded to get an intermediate cipher image. The encrypted image is attained by scrambling pixels of the intermediate cipher image with the help of a chaotic sequence.

The authors (Kuldeep Singh & Komalpreet Kaur, 2011) presented three chaotic map types: duffing map, tinkerbell map, and ginger breadman map to permute the subblocks of DNA encoded matrices. DNA ADD operation is applied to combine these subblocks to generate cipher image. The key image is constructed using PRNG method. The key image and original image are renovated into DNA-encoded matrices. Chen's hyper chaotic sequences are referred for the permutation of DNA encoded matrices. The permuted DNA encoded matrices are diffused using XOR to produce a cipher image (Ozkaynak Fatih & Sirma Yavuz, 2014).

The results of above literature review show that low dimensional chaos cannot withstand the degradations of dynamics under predictable precision calculations in modern computers. Thus, some high dimensional chaotic map is essential for encryption of medical images. The Chen's hyper chaotic map is a high dimensional chaotic map method hence decided to use it in the proposed method.

The authors (Abraham Lini & Neenu Daniel, 2013; Wang Xingyuan & Chuanming Liu, 2016) have presented a piecewise linear chaotic map (PWLCM) and Rubik's cube for permutation of original image. The pixels are scrambled using a DNA complementary rule to generate a cipher image. The authors (Mokhtar M, Amr Sameh N. Gobran & El-Sayed A-M. El-Badawy, 2014) used three DNA chains from National Center for Biotechnology Information (NCBI) site and color image is separated into RGB components. The XOR operation is used between DNA chains and scrambled pixels of RGB components using a 1D logistic map to obtain an encrypted image. The authors (Rakesh Kumar Jangid, Noor Mohmmad, Abhishek Didel & Swapnesh Taterh, 2014) have developed the DNA cryptography and TF hill cipher algorithm for color image encryption. The authors (Belazi et al.,2014; Jain Anchal & Navin Rajpal, 2015; Wang Xing-Yuan, Ying-Qian Zhang & Yuan-Yuan Zhao, 2015) presented 1D and 2D chaotic sequences for the permutation of toriginal image and mask image. The DNA coding rule is used to generate DNA sequences for mask images and original images. The DNA ADD operation combines the DNA encoded matrices. DNA decode rules are utilized to get a cipher image.

The authors (Wang Xing-Yuan, Ying-Qian Zhang & Xue-Mei Bao, 2015) have presented coupled map lattice (CML) to produce a random sequence. The XOR is used between the random sequence and original image. The pixels of e DNA encoded sequences are shuffled using CML to generate a cipher image. The authors (Xiangjun Wu, Haibin Kan & Jurgen Kurths, 2015) have developed three 1D chaotic systems for color images, i.e., Logistic-Tent system (LTS), Logistic-Sine system (LSS), and Tent-Sine system (TSS) to scramble the pixels of DNA encoded R, G, B elements using three improved 1D chaotic maps, one for each component. The XOR operation diffuses the scrambled RGB components to get a cipher image.

The authors (Kalpana J &P. Murali, 2015) have presented Lorenz system, Chen's hyper-chaotic system, sine map, and cubic map for permutation of DNA encoded RGB elements.

These elements are merged to get a cipher image. The authors (Rasul Enayatifar, et al.,2015) presented hamming distance to calculate the preliminary values for 2D tinkerbell chaotic map. The original image pixels are scrambled using CML (coupled map lattice). The scrambled pixels are coded by DNA coding rules to get encoded DNA matrices. The DNA XOR is applied between chaotic sequence and DNA matrices to obtain an encrypted image. The authors (R. Guesmi, M. A. B. Farah, A. Kachouri & M. Samet, 2016) have presented a secure hash algorithm (SHA-2) to generate key sequences and a color image is split up into RGB elements. For fusion, XOR operation is used between key sequences and RGB components. The Lorenz system generates a chaotic sequence. These chaotic sequences are mapped with DNA fusion matrices to generate a cipher image.

In (Li T, Shi J, Li X, Wu J & Pan F,2019), the 5D hyperchaotic map is applied for permutation of normal image. Dynamic filtering and DNA encoding are performed to modify the pixels of image. The diffused image is converted into various 3D DNA-level. The Latin cubes are applied to 3D DNA-level cubes and integrated to get a cipher image. The 4D hyperchaotic map generates the chaotic sequences and these sequences are referred for multiple bit permutation and diffusion. The diffused image is transformed into a cipher image (Taiyong Li & Duzhong Zhang, 2021). In (Lone, Singh & Mir,2021), the modified 3D Arnold cat map chaotic sequence are utilized for permutation of plain image. The permuted image is renovated into a DNA matrix using DNA coding rules. DNA XOR operation is applied to get the DNA diffusion matrix. The inverse of DNA encode rules are applied to attain an encrypted image.

The Secure Hash Algorithm-512 (SHA-512) is utilized to yield a 512-bit hash key. The hash key is employed to determine the primary values of chaotic systems. The four-wing chaotic systems and Lorenz systems produces a chaotic sequence. These sequences are applied for two-round diffusion and permutation processes. The DNA coding and DNA shifting are used dynamically to get a cipher images (Zhou S, He P, Kasabov N, 2020). The author (Samiullah et al., 2020) presented a symmetric encryption method using PWLCM, Lorenz, and 4D Lorenz-type chaotic systems, a SHA, and a DNA sequence-based Linear Feedback Shift Register to enhance the degree of permutation and diffusion to provide multilevel security. The author (Liu M & Ye G.,2021) developed an asymmetric encryption method using DNA coding and hyperchaos theory. The embedded message is separated from the plain image by calculating a sum of odd and even rows and columns

respectively. The extracted message is taken as input for RSA algorithm and output of the algorithm is transformed as an preliminary value of hyperchaotic maps. The hyperchaotic sequences are used to get permuted plain image. Dynamic encode and decode rules are used to get a cipher image.

The above literature review shows that the Lorenz system has good confusion properties, which are suitable for providing high-level security to digital medical image. Therefore, decided to use it in proposed methodology. DNA cryptography depends on biological operations, which use DNA word logic instead of classical bit logic. Hence, decided to use DNA biological operations in the proposed methodology.

The survey reveals that most of the work is carried out for the encryption of plain images using DNA cryptography.

1.11.2 Digital Medical Image Encryption using Watermarking and Cryptography

The digital medical image encryption using watermarking and traditional cryptography techniques are studied in different papers and highlights are specified below:

The authors (Lima J. B, F. Madeiro & F. J. R. Sales, 2015) have suggested cosine number transform (CNT) approach to get an encrypted image. The medical image is segmented into sub-images and CNT technique is employed multiple times to acquire a cipher image. The CNT is substantial in accomplishing the low-frequency feature of medical images. The high-frequency coefficients are coarsely quantized. The authors (Kanso A & M. Ghebleh, 2015) have suggested a 2D logistic map to permute the pixel of medical image. The medical image is alienated into sub-images, the penetrating portion of sub-images is recognized and concealed with a synthetic image. The selected concealed image is encoded to gain a cipher image.

The authors (Kester et al.,2015) have presented a digital watermarking algorithm, entropy and mean of the medical image are calculated to get an encrypted image. The authors (Arya Sebastian & Delson T R, 2016) have suggested Rivest, Adi Shamir, and Leonard Adleman (RSA) process for encrypting and decrypting of MR images. Further, for extraction of the

tumour details, K-means and watershed segmentations are utilized. The RSA takes a very long period for a large database and reliability is depends on third party.

The authors (Vallathan G, G. Gayathri Devi & A. Vinoth Kannan, 2016) presented least significant bit (LSB) embedding algorithm to conceal patient confidential data in the high-frequency elements of a renovated image. The Linde, Buzo, and Gray (LBG) method is applied to get a cipher image. The electronic code book (ECB) mode of advanced encryption standard (AES) is employed to encrypt the patient records (Al-Haj, Ali Noor Hussein & Gheith Abandah, 2016). The medical image is decomposed into a region of interest (ROI) and a region of noninterest (RONI). The discrete wavelet transforms (DWT) and inverse discrete wavelet transform (IDWT) are utilized to conceal encrypted patient information in RONI region. The limitation of AES algorithm is, that it uses simplified algebraic concepts and the size of the key is small i.e.56 bits.

The patient health information is embedded in a medical image using a digital watermarking algorithm. Several DNA masks are built using chaotic sequences and DNA coding rules. The genetic algorithm (GA) is applied iteratively to acquire best DNA mask. The best DNA mask and watermarked images are encrypted to gain an encrypted image (K. Anusudha, N. Venkateswaran & J. Valarmathi, 2017). Fuzzy-logic method is employed to get diffused medical image. The diffused medical image pixels are confused using a logistic map to attain a cipher image (Lakshmi C et al.,2018). The Digital Imaging and Communications in Medicine (DICOM) image is transformed into a wavelet frequency domain. The wavelet frequency domain pixels are embedded with encrypted patient records to generate a watermarking image. The DWT method is used to ensure data integrity. The wavelet filters are separable and real. Thus, DWT has inadequate directional discrimination for diagonal elements. In t transform domain, there is a deficiency in shift-invariance of frequency.

The Advanced Encryption Standard-Galois Counter Mode (AES-GCM) technique is utilized for encryption along with authentication (Brindha M, 2018). This method produces an authentication tag for enforcing the integrity and authenticity of an image. The whirlpool hash function generates a 512-bit hash value. The 128 bits of a hash key are utilized for encryption and the remaining 384 bits are used as an initial vector. The initial vector is

encrypted using AES-GCM. The DICOM image is bifurcated into 128-bit blocks. The output of the initial vector is XORed with the image blocks to gain the cipher image.

In medical image encryption system, pseudo-random number key generation (PRNG) depends on the generalized double humped (GDH) method is used. The chaotic map range is more complex due to traditional generalized parameters (Ismail et al., 2018). The 1D logistic map and lightweight operations are presented for encrypting images (Siva et al., 2018). An inward spiral scanning pattern (round-robbin fashion) is employed to permute the pixels. The control parameters of Arnold mapping depend on Kent mapping. The Arnold mapping and wavelet transform are utilized to rearrange pixels of image. The permuted image is diffused using XOR operation to get a cipher image (Chen, Xiao, & Chun-Jie Hu, 2017). The bitwise XOR and modulo arithmetic processes are used to execute the pixel adaptive diffusion (Hua, Zhongyun, Shuang Yi, & Yicong Zhou, 2018). First, the boundaries of image are extended by adding some random data. Two-level permutation and adaptive diffusion are accomplished to spread the added random data over the complete image. The adaptive diffusion is applied to get a cipher image.

The literature review emphasizes ancient cryptographic techniques, digital watermark, and steganography for medical images. These methods failed in ensuring the necessary security and enforcing integrity for medical images.

The digital images are highly correlated and large in volume and reductant. Thus, t run-time of encryption techniques is very high. To reduce the computational run-time two approaches are available namely, compression technique and parallel approach.

1.11.3 Digital Image Encryption Methods with Reduced Computational Complexity

Several encryption techniques to compressed images, for the reduction of computation time are studied and depicted below.

The authors (X.-J. Tong, M. Zhang, Z. Wang, and J. M,2016), have presented a discrete cosine transformation dictionary for compression and a hyperchaotic map for encryption. In (L Gong, C Deng, S Pan, N Zhou, 2018), discrete cosine transform spectrum cutting technique is applied to compress the input image. The hyperchaotic map creates a random

matrix. Discrete fractional random transform is used to get a cipher image. In (N Zhou, S Pan, S Cheng, Z Zhou,2016), two-dimensional compressive sensing technique is employed to compress the plain image. Further, the pixels of compressed images are rearranged repetitively utilizing chaotic sequences to gain a cipher image. The author (Chen et al.,2018) presented both encryption and compression methods simultaneously. The chaos-based structurally random matrix (SRM) is created using a 3-D cat map. The secret compressed sensing (CS) is developed for SRM, which is utilized for compression. The key stream is produced using a 3D cat map. This key stream is used as permutation vector and diffusion mask in encryption process.

In (Xie, Yaqin, Jiayin Yu, Shiyu Guo, Qun Ding, and Erfu Wang, 2019), the 3D chaotic map creates a measurement matrix and this matrix is utilized for compressed sensing. The Arnold map sequences are utilized for the permutation of compressed image and to obtain a cipher image. In (Ghaffari A,2021), the image is expanded in transform domain to obtain a two-dimensional sparse matrix. The Lorenz chaotic map is utilized to confuse the pixels of a two-dimensional sparse matrix and singular value decomposition is used to compress the confusion matrix. The XOR operation is employed to get a cipher image.

This review shows that several methods are available for the reduction of time and space requirements. The above discussed methods are vulnerable to dictionary attacks and chosen plain text attacks as a result of limited key space.

To reduce the computation time, the parallel approach is used instead of sequential approach. Several encryption methods using a parallel approach are studied and specified below.

In (Zhou, Qing, et at., 2008), authors presented a parallel encryption algorithm for images using discretized Kolmogorov flow map. The cipher image is obtained using four transformations namely, M, A, S, and K transformation (M A S K). In (Hussein, Khalid Ali, Sadiq A. Mehdi, and Salam Ayad Hussein,2019), the authors presented a parallel environment for encrypting images using a 3-D hyperchaotic map and zig-zag ordering transformation. In (Kumar, P. Kranthi, et al.,), the author presented fast image encryption using Lorenz attractor (FIELA) to utilize parallel computing resources of GPU and multicores. The image is considered as a cube and the Lorenz attractor is applied for all

coordinates of cubes to generate a confusion matrix. This process is repeated multiple times based on keys to get a cipher image. In (You, Lin, Ersong Yang, and Guangyi Wang,2020), the author presented a parallel encryption algorithm for images using hybrid chaotic map (HCMO). A combination of 2D logistic dynamic system and OpenCL are presented for the encryption of image.

In (RaghuM, E. and K. Ravishankar, 2018), the image is divided into slices and each slice is encrypted utilizing Advanced Encryption Standard (AES) method. The chunks of the image are encrypted simultaneously using multi threads. In (Abbas, Alaa M., Ayman A. Alharbi, and Saleh Ibrahim, 2021), pixel-level parallelism is performed to generate chaotic sequences swiftly. The discrete chaotic sequence is generated based on defined elliptic curve (EC) points and logical add operation. These sequences are referred to gain a cipher image. The encryption process is parallelized using parallel processing toolboxes such as GPU acceleration, multi-core CPUs, and DSPs. In (Yu, Jiayin, Chao Li, Xiaomeng Song, Shiyu Guo, and Erfu Wang, 2021), the author presented a parallel encryption method using a compressed sensing framework and chaotic encryption theory. The chaotic sequences and compressed sensing concepts are presented to compress the image. The compressed image is united with sample image to get a mixed image. The mixed image is divided into eight samplings and these image pixels are shuffled by a 3D chaotic map to get a cipher image.

The limitation of key size is a major flaw in chaos theory. In t encryption technique, the size of the key is a prime factor. If the length of the key is large, it is invulnerable to crypto attacks. Hence, the above specified methods are not appropriate to offer security for medical images. For the reduction of computational run-time, a parallel approach is suitable. Hence, decided to use parallel approach to reduce the computation time.

1.12 Motivation

From the literature survey, it is perceived that most of the work is conducted using watermarking and traditional cryptographic methods. These methods are not enough in providing security to digital medical image and mainly focus on providing security for normal images.

The medical images are very large in volume, highly correlated, and contain disease-related sensitive information. Medical images are main tools in diagnosing the exact diseases. Hence, broadcasting of medical images through an open-source network is a big challenge. The intruders can alter or modify medical images during transmission through an open source network. For normal images, recovering the tampered or modified part is possible. In medical images, if disease related information is tampered or modified then recovering is not possible. Diagnosing the specific disease from altered image is extremely impossible. The security requirement for a medical image is different from normal mages.

Existing methods are inadequate in providing security for medical images and time consuming. The main motivation of the study is to design efficient en/decryption methods to contribute to high-level security for medical images in less time.

1.13 Problem Statement and Objectives of the Study

In information security, mathematical operation-based techniques like RSA, DSA, AES, etc. are used for encryption. DSA and AES methods are suitable for encryption of text only. The RSA is very slow for large datasets and for verification of reliability a third party is essential. Nowadays, a new technique called DNA cryptography based on biological operation has evolved in information security and it is in premature stage. Hence, motivated us to use DNA cryptography for enhancing the security level of medical images. This challenging task will lead to helpful application in the field of telemedicine. Hence, the problem statement is formulated as following:

"*To develop novel efficient cryptography algorithms based on multilevel DNA cryptosystem to enhance security, enforce integrity and confidentiality for medical images*"

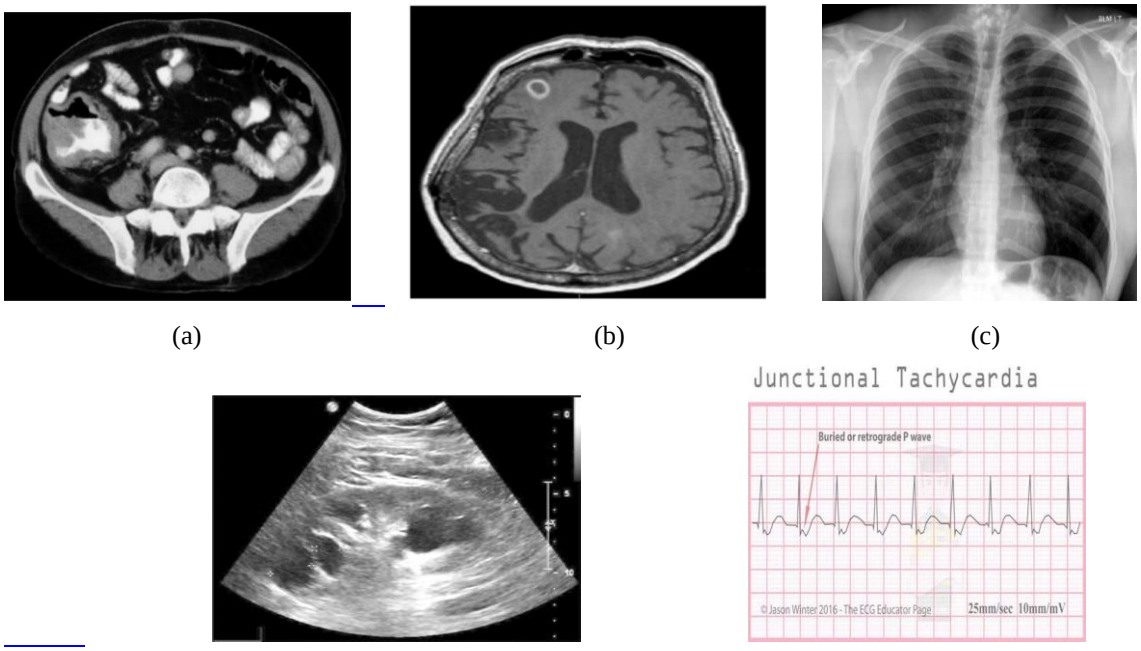
The main objectives of proposed research work are as follows:

- Development of multilevel cryptosystem for digital medical images to offer high-level security. Generation of multiple secret keys for multiple levels of DNA cryptosystem to increase the size of the secret keys.
- Design of robust DNA cryptosystem to secure e-health system with integrity and confidentiality. Applying optimal performance parameters to DNA cryptosystem for analysis of resistance of cryptosystem against different types of crypto attacks.

- Development of compressed medical image encryption method to reduce the space requirement.
- Implementation of efficient parallel DNA cryptography method to reduce computation time.
- Experimentation of the proposed methods based on DNA cryptography using benchmark medical image datasets and comparison of performance with other methods.

1.14 Medical Image Datasets

The medical imaging techniques such as MRI, CT, or ultrasound are important tools used by medical experts for quick and accurate diagnosis of various diseases. Medical images act as a main tool for disease diagnosis, treatments, and research. A total of 500 medical images of five different kinds are used for the study is shown in Appendix I. The five different kinds of medical images are CT, Ultrasound, X-Ray, MRI, and ECG images. For



(a) (b) (c)

(d) (e)

Fig.1.12 Medical image samples (a) CT image (b) MR image (c) X-ray image (d) Ultrasound image (e) ECG image

each type 100 medical images of size 512×512 are collected. The Ultrasound, MRI, X-Ray, and CT images are gathered from the National Library of Medicine's Open Access Biomedical Images Search Engine, from web source https://openi.nlm.nih.gov. The ECG

images are accumulated from web source http://ecg-educator.blogspot.com and stored in the dataset. The sample medical images of each category are presented in Fig. 1.12.

1.15 Organization of the Thesis

The thesis is structured into eight chapters.

Chapter 1- Introduction to DNA cryptography, literature review, motivation and research objectives of the present research are presented.

Chapter 2- Medical image encryption and decryption method with key image generation using a pseudorandom generator, biological and logical operations based cryptosystem is discussed in this chapter.

Chapter 3- In this chapter, medical image encryption and decryption algorithm based on the pixel value of a medical image is discussed.

Chapter 4- Medical image encryption and decryption techniques along with verification of integrity using a hash function and providing confidentiality are discussed in this chapter.

Chapter 5- Selective medical image cryptosystem based on a dual hyperchaotic map is discussed.

Chapter 6- In this chapter, encryption and decryption method for compressed medical image is discussed and analyzed.

Chapter 7- Importance of parallel computation and illustration of parallel approach for medical image encryption and decryption scheme using DNA cryptography are illustrated.

Chapter 8- This chapter includes overall concluding remarks on thesis. The contribution and limitations of the developed medical image encryption and decryption methods are discussed. The scopes for further research are outlined at the end.

Chapter 2

DNA Cryptosystem for Medical Images Based on Biological and Logical Operations

2.1 Introduction

The medical images carry a disease related sensitive information. High-level security is vital for medical images during online communication. The encryption method using both logical and biological operations is proposed in this chapter. Includes discussion of the key image generation technique. Also, highlights the performance evaluation of proposed cryptosystem depending on resistance against several types of attacks.

The ancient encryption methods are depending on mathematical and logical operations. It is suitable for plain images. The author (Safwan El, 2016) have presented 2D cat map for encryption of image. The 2D cat map sequences are utilized to permute image. The author (X. Zhang, Z. Zhao & J. Wang, 2014) have proposed an encryption method using a circular substitution box and key stream buffer. The substitution and diffusion of pixels of the image are accomplished using an encryption key. The encryption key is derived from the plain image. The image is disintegrated into sub images and each sub image pixels are permuted and diffused using Arnold cat transformation. The diffused and permuted blocks are united to obtain an encrypted image (Rakesh, S., Kaller, A.A., Shadakshari, B.C. & Annappa, B., 2012). The Chen's chaotic map is employed for encryption of plain image. The primary values of state parameters are derived from the given image. Thus, dynamic initial values are generated for state parameters of Chen's chaotic map to get a cipher image (Chen, J.X., Zhu, Z.L., Fu, C., Yu, H. & Zhang, L.B., 2015).

Prema T. Akkasaligar, Sumangala Biradar, "***Multiphase Image Encryption using Chen's hyper chaotic map, Biological and Logical operator***", UGC Sponsored National Conference on Recent Trends in Image Processing and Pattern Recognition-2016, Karnataka Arts, Science and Commerce College, Bidar, Karnataka, India, 2-3 April 2016, pp.103-113.

These encryption methods are suitable to provide security for plain images and not safeguard for chosen plaintext and chosen ciphertext attacks due to limited key space. To overcome these loopholes and to provide security for medical images, a new cryptosystem using logical operations and biological operations is proposed. The mathematical and logical operations like key image generation method, and Chen's chaotic map are utilized in proposed en/decryption method. The biological operations like DNA cryptography is utilized to provide high-level security for medical images.

2.2 Generation of Key Image

The key image is utilized as a secret image to stipulate security for medical images. The pseudo-random number generator (PRNG) is used to create a key image. The PRNG is also called a deterministic random bit generator (DRBG). The PRNG generates a sequence of random numbers using mathematical functions. The generation of random numbers depending on the primary value of PRNG called a seed. This seed is important to generate a deterministic and efficient random number. The key image generated using PRNG is a matrix of discrete uniformly distributed random integers. Sample key image matrix of size 4×4 is given below.

Key image matrix =

8	10	11	14
4	9	7	5
21	40	20	13
2	1	3	6

2.3 Proposed Method for Medical Image Encryption and Decryption

The proposed medical image encryption method using logical and biological operations is presented in Fig. 2.1. The key image is created using logical operation PRNG. Chen's chaotic map discussed in section 1.5.1 of Chapter 1 is utilized for permutation and diffusion of medical image and key image. DNA cryptography discussed in Section 1.3 of Chapter 1 is utilized to yield a distinctive encoded DNA matrix for individual medical image.

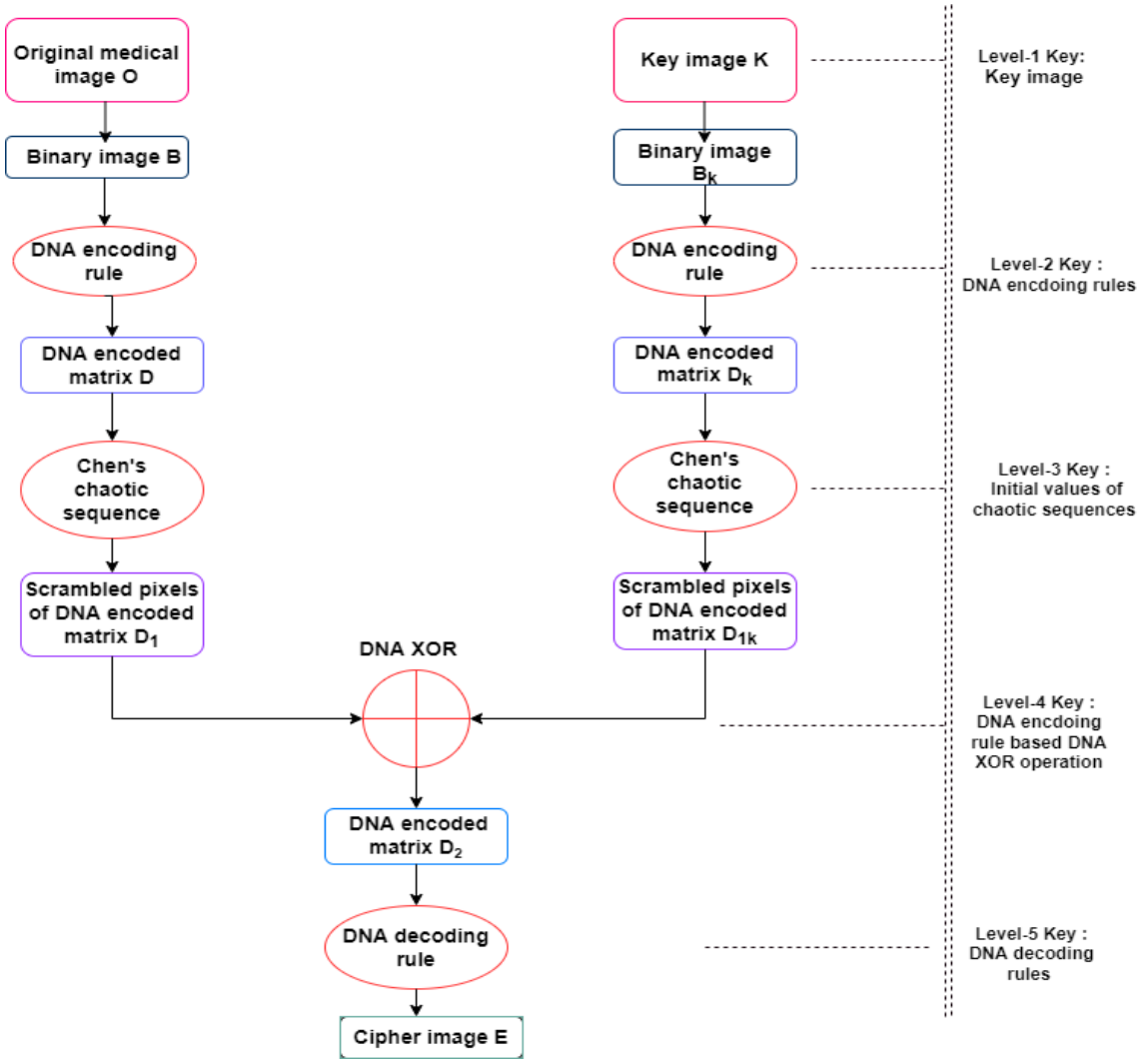


Fig. 2.1 Block diagram of proposed medical image encryption method

The multistate encryption is performed to anticipate multi-level security for medical images. In first state, original medical image and key image are renewed into eight-bit binary image respectively. The binary images are mapped into DNA sequence structure using DNA encoding rules as specified in Section 1.6 of Chapter 1 in second state. In third state, chaotic sequences are produced using Chen's chaotic system. These sequences are utilized to get permuted DNA structures. In fourth state, DNA XOR process is exploited to combine DNA structure of input image and DNA structure of a key image. DNA decode rules are used to get a cipher image in fifth state. The expansive steps of proposed encryption method are illustrated in Algorithm 2.1.

Algorithm 2.1: Medical Image Encryption

//Input: Original medical image O (r, c) of size r rows and c columns

//**Output**: Cipher image E (r, c) of size r rows and c columns

Step 1: Start

Step 2: Original medical image O (r, c) and key image K (r, c) are renovated into eight bit binary image B (r, c×8) of size r rows and c×8 columns and B_k (r, c×8) of size r rows and c×8 columns respectively.

Step 3: Binary images are renovated into encoded DNA matrices as D (r, 4×c) of size r rows and 4×c columns and D_k (r, 4×c) of size r rows and 4×c columns sequentially.

Step 4: Chen's chaotic map generates chaotic sequences *x* and y. These sequences are arranged in ascending order.

Step 5: A position of arranged chaotic sequences are referred to permute the pixels of D (r, 4×c) and D_K (r, 4×c) distinctly. These rearranged pixels of encoded DNA matrices are signified as D_1(r, 4×c) and DK_1 (r, 4×c) respectively.

Step 6: DNA XOR operation is employed for the association of D_1(r, 4×c) and D_{K1} (r, 4×c). A result of the combination is denoted as D_2(r, 4×c).

Step 7: The inverse of DNA encode rules are used to transform matrix D_2(r, 4×c) into a binary image to obtain a cipher image E (r, c).

Step 8: Stop

To get an original medical image, cipher image is decrypted using decryption method. The decryption method is the converse of encryption method. Expansive steps of proposed decryption method are illustrated in Algorithm 2.2.

Algorithm 2.2: Medical Image Decryption

//Input: Cipher image E (r, c) of size r rows and c columns

//Output: Decipher image i.e. original medical image O (r, c) of size r rows and c columns

Step 1: Start

Step 2: The cipher image E (r, c) is renewed into a binary image. The DNA encoding rules are used to transform the binary matrix into encoded DNA matrix D_2(r, 4×c).

Step 3: DNA XOR process is applied for the diffusion of pixels of D_2(r, 4×c) to get D_1(r, 4×c) and D_{K1} (r, 4×c).

Step 4: Chen's chaotic map generates chaotic sequences x and y. These sequences are arranged in descending order.

Step 5: A position of arranged chaotic sequences are utilized to reshuffle the pixels of $D_1(r, 4\times c)$ and D_{K1} $(r, 4\times c)$ respectively. These reshuffled pixels of encoded DNA matrices are denoted as D $(r, 4\times c)$ and D_K $(r, 4\times c)$ respectively.

Step 6: The inverse of DNA encode rules are applied to convert the matrices as D $(r, 4\times c)$ and D_k $(r, 4\times c)$ into binary image matrices B $(r, c\times 8)$ of size r rows and $c\times 8$ columns and B_k $(r, c\times 8)$ of size r rows and $c\times 8$ columns sequentially.

Step 7: Binary image matrices B $(r, c\times 8)$ and B_k $(r, c\times 8)$ are converted into decipher image O (r, c) and key image K (r, c) respectively.

Step 8: Stop

In this proposed method, encryption is performed in five states to deepen the security of medical image. In each state, different keys are used to generate multiple secret keys.

In first state, a secret key is the generation of a key image and DNA encoding rules used to construct an encoded DNA matrix are a secret key in second state. In third state, initial values of chaotic sequence are secret keys. DNA decoding rules are secret keys of fifth state. The uniqueness of DNA cryptography and pseudo randomness of Chen's chaotic system are appropriate to fulfil the security requirements for medical images during transmission.

2.4 Experimental Results and Discussion

The proposed cryptosystem is accomplished using Intel Core i7, 9th Gen processor with software tool MATLAB R2016b. The 500 samples from five different categories namely, CT, MRI, ECG, Ultrasound, and X-Ray images are taken from benchmark datasets and details of these samples are given in the Appendix-I. From each category 100 image samples of size 512×512 are collected. In proposed multistate encryption method, original medical image as depicted in Fig. 2.2(a), and key image of size 512×512 are renewed into binary matrices. These binary matrices are renovated into a DNA

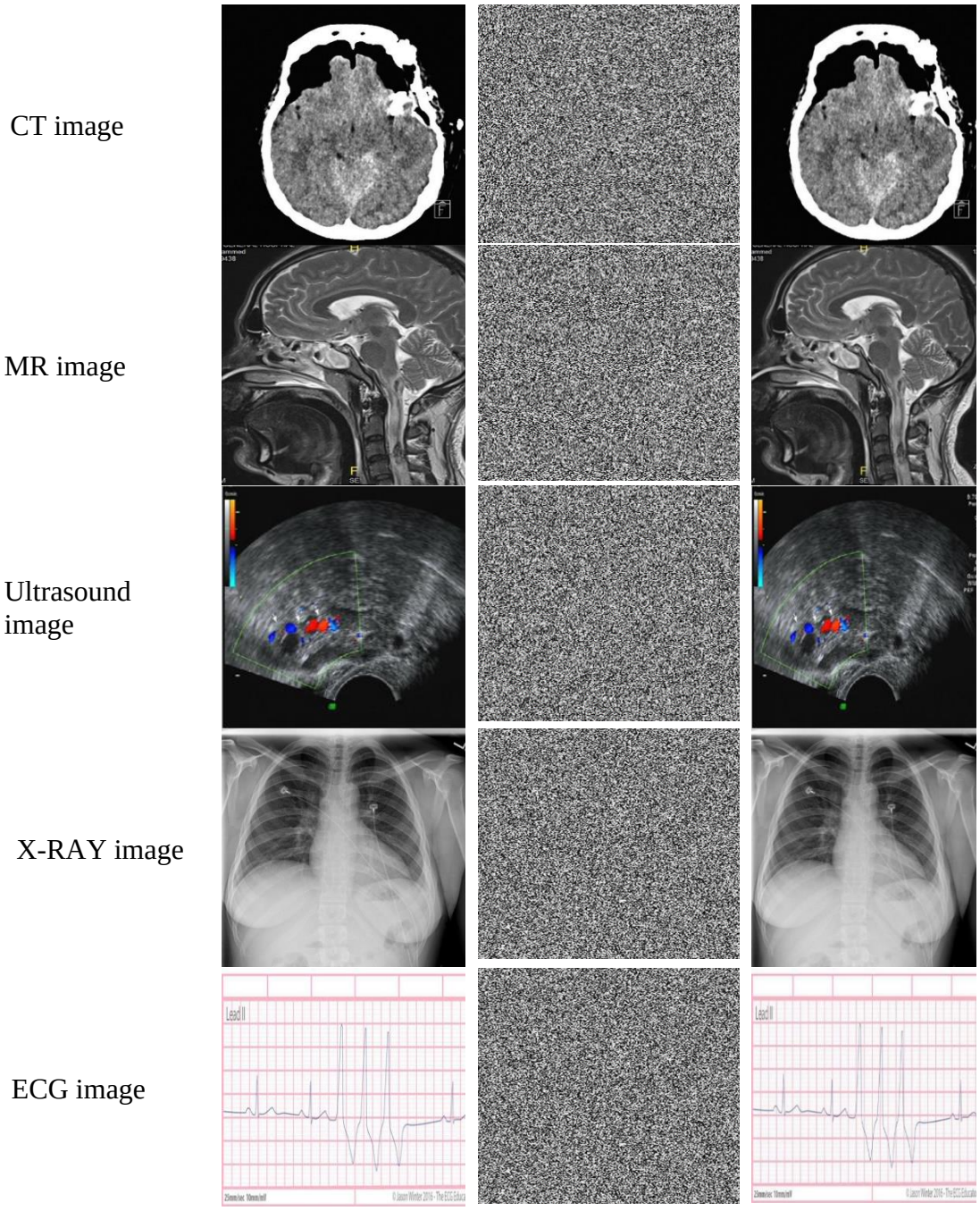


Fig. 2.2 Medical image samples: (a) Original medical images (b) Cipher images (c) Decipher images

sequence matrices using DNA encoding rule 6 as specified in Table 1.1 of section 1.6. Initial values of position parameters are x_0=0.3, y_0=-0.4, z_0=1.2, and w_0=1 and control factors a_1=36, b_1=3, c_1=28, d_1=-16, and k=0.2 are empirically found to generate a Chen's chaotic sequence using Eqns. (1.5.1) - (1.5.4) of Chapter 1. These chaotic sequences are placed in ascending order and position of arranged sequences is utilized to permute DNA sequence matrices. DNA sequence matrices, pixels are diffused with help of DNA XOR operation as tabulated in Table 1.4 of Section 1.6 of Chapter 1. The modified DNA

sequence matrix is renewed into a cipher image as presented in Fig 2.2(b), using DNA decoding rule 4 i.e. inverse of DNA encoding rule.

In proposed decryption method, a cipher image is rendered into a binary matrix through DNA decoding rule 4. DNA XOR is operated for diffusion of encoded DNA matrices. Diffused matrices pixels are reshuffled using Chen's chaotic map sequences. These reshuffled pixels of encoded DNA matrices are renovated into binary matrices by applying DNA decoding rule 6. The binary matrices are transformed into an original medical image as depicted in Fig 2.2(c) and key image respectively.

The working procedure of Algorithm 2.1 is illustrated with one suitable example. Consider original medical image matrix of size 4×4 and key image matrix of size 4×4.

Step 1: Construction of key image

O =

4	2	8	3
1	6	10	9
7	3	4	5
12	11	33	20

K=

8	10	11	14
4	9	7	5
21	40	20	13
2	1	3	6

Step 2: Conversion of O and K into binary matrix B and B_k

B =

00000100	00000010	00001000	00000011
00000001	00000110	00001010	00001001
00000111	00000011	00000100	00000101
00001100	00001011	00100001	00010100

B_k =

00001000	00001010	00001011	00001110
00000100	00001001	00000111	00000101
00010101	00101000	00010100	00001101
00000010	00000001	00000011	00000110

Step 3: Transform binary matrices into encoded DNA matrices D and D_k using DNA encoding rule 6.

D =				
	CCTC	CCCA	CCAC	CCCG
	CCCT	CCTA	CCAA	CCAT
	CCTG	CCCG	CCTC	CCTT
	CCGC	CCAG	CACT	CTTC

D_k =				
	CCAC	CCAA	CCAG	CCGA
	CCTC	CCAT	CCTG	CCTT
	CTTT	CAAC	CTTC	CCGT
	CCCA	CCCT	CCCG	CCTA

Step 4: The Chen's chaotic sequence *x* and *y* generation

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	0.285039	0.270294	0.255755	0.241413	0.172348	0.106952	0.044253	-0.01668

x	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
	-0.09861	-0.18097	-0.26584	-0.35531	-0.46712	-0.59131	-0.73158	-0.89213

y	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	-0.40475	-0.40971	-0.41488	-0.42027	-0.45053	-0.48654	-0.52865	-0.5773

y	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
	-0.65519	-0.74778	-0.85696	-0.98496	-1.15955	-1.36756	-1.6148	-1.90819

Step 5: Sort the chaotic sequence

$\bar{x}$	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**
	-0.89213	-0.73158	-0.59131	-0.46712	-0.35531	-0.26584	-0.18097	-0.09861

$\bar{x}$	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
	-0.01668	0.044253	0.106952	0.172348	0.241413	0.255755	0.270294	0.285039
$\bar{y}$	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**
	-1.90819	-1.6148	-1.36756	-1.15955	-0.98496	-0.85696	-0.74778	-0.65519

$\bar{y}$	**8**	7	6	5	4	3	2	1
	-0.5773	-0.52865	-0.48654	-0.45053	-0.42027	-0.41488	-0.40971	-0.40475

Step 6: Depending on index of sorted chaotic sequence, D_1 and D_k pixels are permuted row-wise and column-wise respectively.

D_1= (row-wise)				
	CTTC	CACT	CCAG	CCGC
	CCTT	CCTC	CCCG	CCTG
	CCAT	CCAA	CCTA	CCCT
	CCCG	CCAC	CCCA	CCTC

D_1= (column-wise)				
	CCTC	CCCT	CCTG	CCGC
	CCCA	CCTA	CCCG	CCAG
	CCAC	CCAA	CCTC	CACT
	CCCG	CCAT	CCTT	CTTC

D_{k1}= (row-wise)				
	CCTA	CCCG	CCCT	CCCA
	CCGT	CTTC	CAAC	CTTT
	CCTT	CCTG	CCAT	CCTC
	CCGA	CCAG	CCAA	CCAC

D_{k1}= (column-wise)				
	CCAC	CCTC	CTTT	CCCA
	CCAA	CCAT	CAAC	CCCT
	CCAG	CCTG	CTTC	CCCG
	CCGA	CCTT	CCGT	CCTA

Step 7: Fusion of column-wise D_1 and D_{k1} using DNA XOR

D_2 =				
	AATA	AAGG	AGAC	AATC
	AACA	AATT	ACCT	AACC
	AAAT	AATG	AGAA	ACAC
	AATG	AATA	AACA	AGAC

Step 8: DNA decoding rule 4 is applied to decode DNA sequences into binary form.

B =				
	01011001	01010000	01000111	01011011
	01011101	01011010	01111110	01011111
	01010110	01011000	01000101	01110111
	01011000	01011001	01011101	01000111

Step 9: The binary matrix is renovated into a cipher image matrix.

E =				
	89	80	71	91
	93	90	126	95
	86	88	69	119
	88	89	93	71

The cipher image is decrypted into an original medical image using decryption method.

2.4.1 Performance and Security Analysis

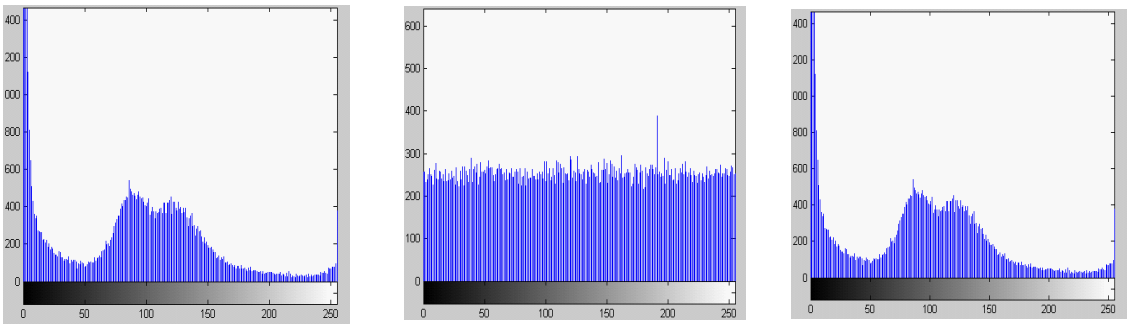
The performance of proposed multistate en/decryption method depends on how much it resists numerous types of attacks. Security analysis is to analyze the sustainability of multistate en/decryption method against statistical, differential, and exhaustive attacks.

A. Statistical Attack

The cryptanalyst performed, a histogram analysis and correlation coefficient analysis to verify resistant to statistical attack. Main aim of cryptanalyst is to retrieve original medical image and guess the secret keys from given cipher image.

Histogram Analysis

The pixels spreading frequencies are studied by intruders to predict the original medical image. Hence, pixels of cipher images must be scattered in a manner, that it must be highly unfeasible to envisage the original image. The pixels are disseminated randomly in original medical image and decipher image as exhibited in Fig. 2.3 ((a) and (c)). The pixels are disseminated consistently in cipher image as exhibited in Fig 2.3 (b). From Fig 2.3, it is proved that the pixels are rearranged in cipher image. Therefore, predicting original medical image by observing dissemination of pixels of cipher image is highly impossible.



(a) (b) (c)

Fig. 2.3 Histogram analysis: (a) CT image (b) Cipher image (c) Decipher image

Chi-test is used for statistical interference of uniform dissemination of pixels in cipher image. Outcomes of hypothesis test are presented in Table 2.1, which proves that pixels of cipher image are scattered uniformly.

Table 2.1 Chi-square test for proposed medical image encryption method

Medical image type	Cipher image	Hypothesis test
MR	286.8589	pass
CT	288.4922	pass
X-ray	291.9531	pass
Ultrasound	289.7500	pass
ECG	288.7422	pass

Correlation Coefficient Analysis

The pixels of original medical images are highly correlated. Intruders try to guess the original medical image by studying correlation among pixels of cipher image. If there is no

Table 2.2 Correlation coefficient of proposed DNA cryptosystem

Medical image type	Direction	Cipher image	Decipher image
MR	*Horizontal*	0.008	0.992
	Vertical	0.029	0.993
	Diagonal	0.032	0.994
CT	*Horizontal*	0.026	0.993
	Vertical	0.017	0.992
	Diagonal	0.042	0.991
X-ray	*Horizontal*	0.011	0.992
	Vertical	0.021	0.993
	Diagonal	0.029	0.994
Ultrasound	*Horizontal*	0.009	0.991
	Vertical	0.032	0.992
	Diagonal	0.019	0.995
ECG	*Horizontal*	0.025	0.992
	Vertical	0.042	0.994
	Diagonal	0.014	0.993
Average:		**0.024**	**0.993**

correlation among neighboring pixels or negatively correlated, then guessing original medical image is highly impossible. The correlation among pixels of original medical image and cipher image are depicted in Table 2.2. The correlation among pixels of original medical image and decipher image are also tabulated in Table 2.2. Correlation coefficient analysis proves that pixels are extremely interrelated in original medical image and decipher image. There is no relationship among neighboring pixels of cipher image. For intruders guessing original medical image by studying correlation between neighboring pixels is not possible.

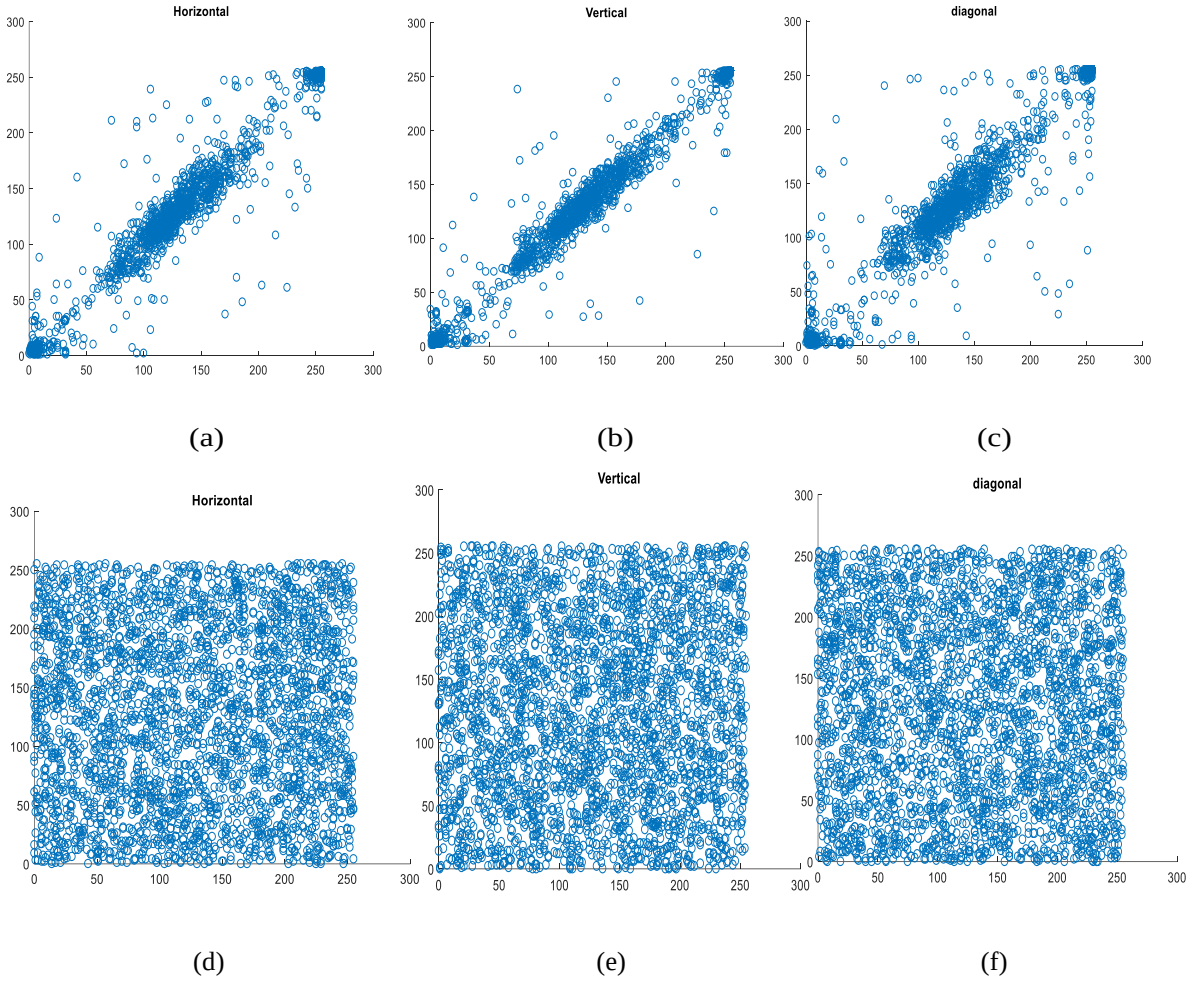


Fig. 2.4 Scatter plot of original CT image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

The 3000 pixels of original medical image and cipher image are chosen horizontally, diagonally, and vertically to interpret the correlation coefficient of contiguous pixels. Scatter plot for correlation coefficient of original medical image and cipher image in three

directions namely, horizontal, vertical, and diagonal are exhibited in Fig.2.4. From Fig.2.4 (a and b and c), it is perceived that all pixels are concentrated towards same direction. This means pixels are correlated in an original medical image. All pixels are scattered in cipher image as exhibited in Fig.2.4 (d and e and f), proves that there is no correlation among pixels. This demonstrates that pixels of original medical image are entirely diverse from cipher image.

B. Exhaustive Attack

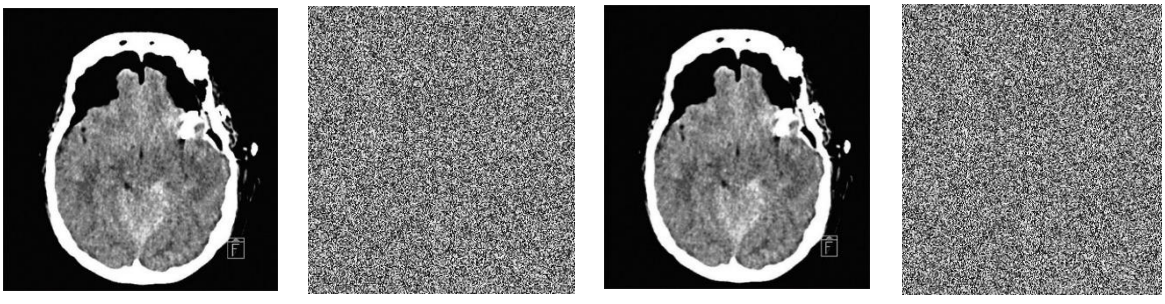
Intruders try to guess secret keys. The secret keys must be very large so that it becomes impossible to guess. The key space and key sensitivity analyses are performed by cryptanalyst to verify invulnerable to exhaustive attack also known as brute force attack.

Key space Analysis

Secret keys of proposed multistate encryption method are preliminary conditions of positional variables and control factors of Chen's chaotic map. A total of five secret keys (x_0, y_0, z_0, w_0, and k) are available. The size of five secret keys is $(10^{15})^5 \approx 2^{250}$ and key image is of $512\times512=2^{18}$. Key space is adequate to survive against exhaustive attack.

Key sensitivity Analysis

Chen's chaotic map is very sensitive to preliminary conditions. Among five secret keys, if we change any one key initial value during decryption, then retaining original medical image is highly impossible. For example, original medical image and cipher image are exhibited in Fig. 2.5((a) and (b)). The decipher image, decrypted using correct $x_0=0.3$ is



(a) (b) (c) (d)

Fig. 2.5 Key sensitivity analysis: (a) Original CT image (b) Cipher image (c) Decipher image decrypted using correct key $x_0=0.3$ (d) Decipher image decrypted using incorrect key $x_0=0.0000003$

exhibited in Fig.2.5(c). Decrypted cipher image using x_0=0.0000003 instead of x_0=0.3 is shown in Fig 2.5(d). Decrypting original image with a very minor variance in initial condition is not possible.

C. Differential attack

The parameters NPCR and UACI discussed in Section 1.8.2 of Chapter 1 are used by cryptanalysts to check endurance against differential attacks. The NPCR average value is 99.64 and UACI average value is 33.61 are exhibited in Table 2.3. The NPCR and UACI value of proposed multistate encryption method is almost equal to ideal values as specified in Section 1.8.2.1 of Chapter 1.

Table 2.3 Performance analysis of proposed DNA cryptosystem

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.65	33.28	7.9907	2.7242e+02	7.4786
CT	99.65	33.56	7.9929	3.3470e+02	6.0810
X-ray	99.64	33.43	7.9918	3.9247e+03	7.1201
Ultrasound	99.67	33.87	7.9939	3.6320e+02	6.4852
ECG	99.59	33.93	7.9914	3.7528e+03	7.0537
Average:	**99.64**	**33.61**	**7.99214**	**1.753e+03**	**6.8437**

The quality of proposed multistate encryption scheme is measured using parameters MSE, PSNR, and entropy discussed in Section 1.10 of Chapter 1. The values of MSE, PSNR, and entropy between original medical image and cipher image are tabularized in Table 2.3. From Table 2.3, it is proved that the proposed multistate en/decryption scheme is

invulnerable to different types of attacks and suitable to provide security for medical images.

2.4.2 Computation Time of Proposed En/Decryption Algorithm

The computation time and space efficiency of proposed en/decryption scheme based on logical and biological operations for original medical image of size (m×n) is calculated as follows:

Step 1: Key image generation process: (m×n)

Step 2: Binary conversion of original medical image and key: 2(m×n)

Step 3: Construction of encoded DNA matrices for original medical image and key image: 2(m×n)

Step 4: Permutation process: 2(m×n)

Step 5: Diffusion process: 2(m×n)

Step 6: DNA decoding: 2(m×n)

Step 7: Generating cipher image: (m×n)

Total time complexity of the proposed method is given below:

$$T(n)= (m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ (m\times n)= 12(m\times n)$$

If m=n then time complexity $T(n)=12(n^2)\in O(n^2)$.

The space complexity of proposed method for original medical image of size (m×n) and key image of size (m×n) is $2(n^2) \in O(n^2)$ assuming m=n.

2.4.3 Comparative Analysis

The proposed multistate en/decryption system is compared with existing encryption schemes is depicted in Table 2.4. From Table 2.4, it is anticipated that the proposed DNA cryptosystem is invincible to various types of crypto attacks.

Table 2.4 Comparative analysis of proposed DNA cryptosystem

Method	Lena image			Pepper image		
	NPCR (%)	UACI (%)	Entropy	NPCR (%)	UACI (%)	Entropy
Safwan El, et al., 2016	99.645	33.57	7.9993	99.639	33.600	7.9994
Chen, J.X., et al., 2015	99.62	33.48	7.9993	99.60	33.54	----
Proposed encryption method	**99.66**	**33.67**	**7.99923**	**99.67**	**33.79**	**7.99935**

The length of secret keys plays a vital role in offering security for medical images. Comparison analysis of key space is exhibited in Table 2.5. From Table 2.5, it proves that key space of proposed en/decryption method is bigger than other methods specified in literature survey. Comparative analysis reveals that proposed multistate cryptosystem is effective to offer security for medical images during transmission through internet.

Table 2.5 Comparison of proposed DNA cryptosystem key space with existing methods

Method	Rakesh, S., et al., 2012	Chen, J.X., et al., 2015	**Proposed encryption method**
Key Space	2^{256}	2^{199}	$\mathbf{2^{268}}$

2.5 Summary

The present chapter discusses a multistate medical image en/decryption scheme based on logical and biological operations. The logical operations namely, PRNG is used to generate key image and Chen's chaotic sequences are applied to get the permuted medical images. The biological operations like DNA encoding rules and DNA XOR are applied for diffusion of medical images. The performance and security analysis manifested that proposed method is exempted to statistical, differential, and exhaustive attacks. A key space is adequate to provide security for medical images during transmission through an open-source network. The five-state encryptions are performed, and an additional key image is generated to offer security for medical images. The secret key image requires

additional memory space. However, it is essential to design en/decryption methods having the virtues of reduced memory requirement and enhanced security. The methods discussed in subsequent chapters concentrate on these virtues.

Chapter 3

DNA Cryptosystem Based on Intensity Levels of Medical Image

3.1 Introduction

The medical images carry information related to diseases. The digital broadcasting of medical images through wireless network is not secure. Providing security for medical images is a prime concern. Several encryption techniques based on chaos theory are available. Due to limitation of key space, these techniques are vulnerable to brute force attacks. A novel method called DNA cryptography is emerged for security purpose. In (Jangid, 2014), the color images are reformed as a binary image and based on nibbles of binary bits, pixels of binary image are rotated. The rotated binary image is redeemed into a DNA structure and DNA structure into amino acids. TF Hill cipher is employed to amino acid to attain a cipher image. DNA structures are generated for original color image by applying DNA encoding rules. DNA structures are separated into Red, Green, and Blue channels. Each channel's pixels are scrambled using Chen's chaotic sequences. DNA ADD method combines RGB channels and a cipher image is obtained (Xiaopeng, 2012). The image is converted into an encoded DNA matrix. The logistic map sequences permuted the encoded DNA matrix. DNA ADD method diffuses the pixels of encoded DNA matrix. The entropy is calculated for encoded DNA matrix. These values are exercised to get the primary values for a spatiotemporal chaotic system. The chaotic sequences of spatiotemporal are referred to permute encoded DNA matrix. Inverse of DNA encoding rules are applied to gain an encrypted image (Zhen,2016).

---

[1] Prema T. Akkasaligar, Sumangala Biradar, "***Secure Medical Image Encryption based on Intensity level using Chao's theory and DNA Cryptography***", 2016 IEEE International Conference on Computational Intelligence and Computing Research, 15-17 December 2016, pp. 958-963.

These encryption approaches are used for providing the security to normal images. Due to limited computation time and key space, these approaches are not appropriate for medical images. The novel encryption method for medical images based on high-dimensional chaotic maps and DNA cryptography is discussed in this Chapter. The main objective of the proposed en/decryption method is to increase key space for the enhancement of security for medical images.

3.2 Proposed DNA Cryptosystem Based on Intensity Levels of Medical Image

The cryptosystem using Chen's chaotic map and Lorenz system and DNA cryptography is proposed to strengthen the security of medical images. The block diagram of proposed encryption method is represented in Fig.3.1.

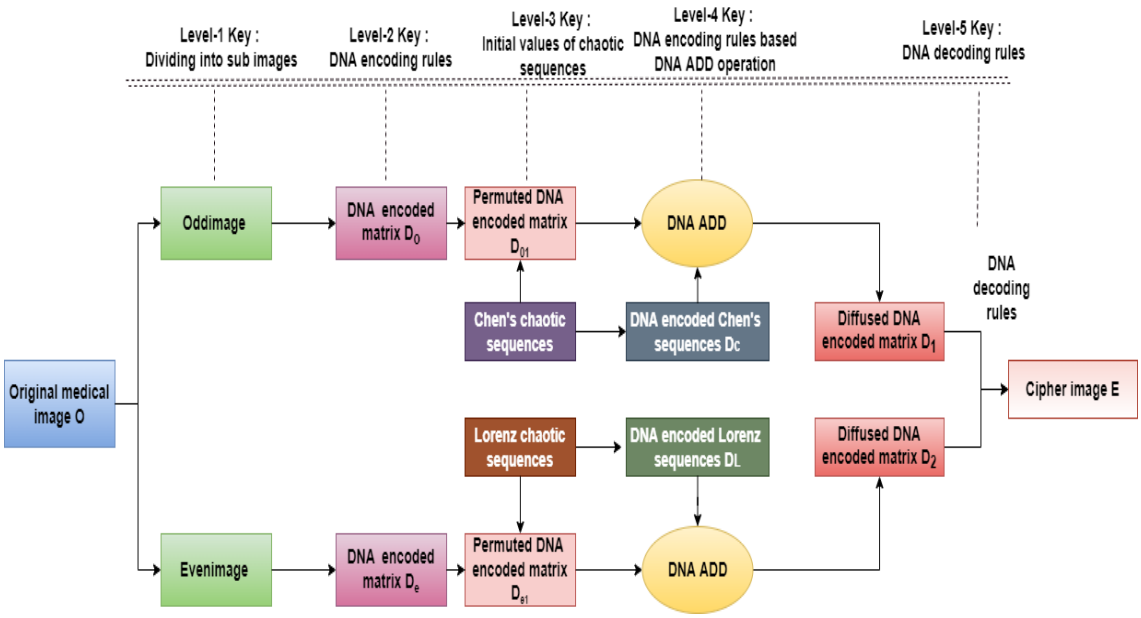


Fig. 3.1 Block diagram of proposed encryption scheme based on intensity levels of medical image

In proposed cryptosystem, on basis of intensity levels the original medical image is bifurcated into two sub images namely, an odd intensity level medical image and an even intensity level medical image.

The intensity level means, the pixel values of medical images. These sub images are renewed into binary images. These images are transformed into odd DNA sequence matrix

and even DNA sequence matrix by DNA encode rules. The pixels of odd DNA sequence matrix are permuted by chaotic sequences of Chen's chaotic map. The pixels of even DNA sequence matrix are permuted by chaotic sequences of Lorenz chaotic system. The shuffled pixels of both DNA sequence matrices are modified by DNA diffusion operation namely, DNA ADD method. Further, diffused matrices are interpreted using inverse of DNA encoding rules to get a cipher image.

The expansive steps of the proposed method are illustrated in medical image encryption and decryption algorithm based on pixel value.

3.2.1 Encryption Algorithm

In proposed medical image encryption algorithm, medical image is split into two sub images based on pixel values of original medical image. The division process is illustrated in Algorithm 3.1.

Algorithm 3.1: Division Process

//Input: Original medical image O (r, c)

//Output: Divided image Odd (r, c), Even(r, c) and Idx

```
  for i=1 to r do
       for j=1 to c do
            if (O (i, j) %2 ==0)
               then Even (i, j) =O (i, j);
            else {
                 Odd (i, j) =O(i, j);
                 Idx(i, j)=j;
                  }
           end
      end
end
```

The output of Algorithm 3.1 is used in the proposed encryption algorithm. The expansive steps of proposed encryption algorithm based on pixel values of medical image are represented in Algorithm 3.2.

Algorithm 3.2: Encryption Algorithm Based on Pixel Values

//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1 : Start

Step 2 : Original medical image O (r, c) is divided into two sub images Odd (r, c) and Even (r, c) by means of the division process as depicted in Algorithm 3.1.

Step 3 : The Odd (r, c) and Even (r, c) are converted into 8-bit binary images B_o (r, c×8) and B_e (r, c×8) respectively.

Step 4 : DNA encoding rules are used to transform binary images into DNA sequence matrices as D_o (r, 4×c) and D_e (r, 4×c) sequentially.

Step 5 : Chen's chaotic sequences *x* and *y* are rearranged in ascending order.

Step 6 : A position of ordered Chen's chaotic sequences is utilized to permute the pixels of D_o (r, 4×c). The permuted DNA sequence matrices are represented as D_{o1} (r, 4×c).

Step 7 : Lorenz chaotic sequences *p* and *q* are rearranged in ascending order.

Step 8 : A position of ordered Lorenz chaotic sequences is utilized to permute the pixels of D_e (r, 4×c). The permuted DNA sequence matrix is represented as De_1 (r, 4×c).

Step 9 : The chaotic sequences *x*, *y*, *p*, and *q* are renovated into encoded DNA matrices namely D_c (r, 4×c) and D_L (r, 4×c) using DNA encoding rules.

Step 10 : DNA ADD operation is applied between D_c (r, 4×c) and D_{o1} (r, 4×c) for the diffusion of DNA sequence matrices. The result of diffusion process is denoted as D_1 (r, 4×c).

Step 11 : DNA ADD operation is also applied between D_L (r, 4×c) and D_{e1} (r, 4×c) for the diffusion of DNA sequence matrices. The result of the diffusion process is denoted as D_2(r, 4×c).

Step 12 : Inverse of DNA encoding rules are used to transform diffused matrices D_1(r, 4×c) and D_2(r, 4×c) are converted into 8-bit binary images B_1(r, c×8) and B_2(r, c×8).

Step 13 : Binary images are converted into grayscale images G_1(r, c) and G_2(r, c) to acquire a cipher image E (r, c).

Step 14 : Stop

The cipher image is decrypted into original medical image in decryption technique. The proposed decryption technique is the converse of encryption technique.

3.2.2 Decryption Algorithm

In proposed decryption process, the cipher is bifurcated into sub images using bifurcation method. The cipher image is divided into sub images with help of index matrix. This matrix contains index of ODD image. The Odd (r, c) and Even (r, c) matrices are initialized with zeros. The Chen's chaotic sequences are referred to permute the index matrix. Later, sub images are assigned to Odd (r, c) and Even (r, c) based on permuted index matrix. The expansive steps of bifurcation are illustrated in detail in Algorithm 3.3.

Algorithm 3.3: Bifurcation Method

//**Input:** Cipher image E (r, c) and matrix Idx

//**Output:** Bifurcated images G_1(r, c) and G_2(r, c)

//Initialize both images G_1 (r, c) andG_2 (r, c) with zeros and permute the matrix Idx using

//Chen' chaotic sequences

```
for i=1 to r do
    for j=1 to c do
                if (Idx (i, j)==0)
                        then G1 (i, j) =E (i, j);
                else
                        G2 (i, j) =E (i, j);
                end
            end
     end
```

The decryption process is the converse of encryption process and DNA ADD method is replaced with DNA SUB operation. The output of Algorithm 3.3 is used in decryption algorithm. The expansive steps of proposed decryption algorithm based on pixel values of medical image is represented in Algorithm 3.4.

Algorithm 3.4: Decryption Algorithm Based on Pixel Values

//Input: Cipher image E (r, c)

//Output: Decipher medical image O (r, c)

Step 1: Start

Step 2: The cipher image E (r, c) is divided into sub images namely, G_1 (r, c) and G_2 (r, c)

using the bifurcation method specified in Algorithm 3. Both sub images are converted into 8-bit binary images B_1 (r, c×8) and B_2(r, c×8) respectively.

Step 3: DNA encoding rules are used to transform binary images into DNA sequence matrices as D_1 (r, 4×c) and D_2(r, 4×c) sequentially.

Step 4: Chen's chaotic map chaotic sequences *x* and *y* are arranged in descending order.

Step 5: Lorenz chaotic map chaotic sequences *p* and *q* are arranged in descending order.

Step 6: The chaotic sequences *x*, *y*, *p*, and *q* are renovated into DNA sequence matrices namely D_c (r, 4×c) and D_L (r, 4×c) using DNA encoding rules.

Step 7: DNA SUB operation is applied between D_c (r, 4×c) and D_{0c} (r, 4×c) for diffusion of DNA sequence matrices. The result of the diffusion process is denoted as Do_1(r, 4×c).

Step 8: DNA SUB operation is also applied between D_L (r, 4×c) and D_{eL} (r, 4×c) for the diffusion of DNA sequence matrices. The result of the diffusion process is denoted as D_{e1}(r, 4×c).

Step 9: A position of sorted chaotic sequences *p* and *q* are mapped for permutation of De_1(r, 4×c). Permuted DNA sequence matrix is signified as De (r, 4×c).

Step 10: A position of ordered chaotic sequences *x* and *y* are mapped for permutation of D_{o1} (r, 4×c). Permuted DNA sequence matrix is signified as D_o (r, 4×c).

Step 11: Inverse of DNA encoding rules are used to transform DNA sequence matrices D_o and D_e into 8-bit binary images as B_o (r, c×8) and B_e (r, c×8) sequentially.

Step 12: Binary images are converted into grayscale images as Odd (r, c) and nEven (r, c).

Step 13: Grayscale images are merged to get decipher image O (r, c).

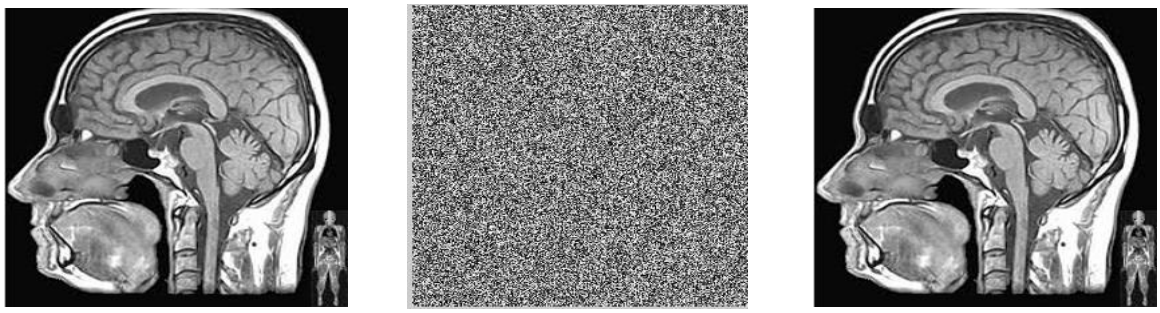
Step 14: Stop

In proposed intensity-based cryptosystem, multiple level security is provided by division of original medical image into Odd image and Even image based on intensity levels is secret key in level 1. The DNA encoding rules (as a secret key) are applied to construct Odd DNA structure and Even DNA structure in level 2. The Odd DNA structure is permuted by Chen's chaotic sequences and Even DNA structure is permuted by Lorenz's chaotic sequences. The preliminary values of chaotic sequences are secret keys in level 3. The permuted image pixels are modified using DNA encoding rule-based DNA ADD operation is a secret key in level 4. In level 5, the secret keys are inverse of DNA encoding

rules. These rules are referred to get a cipher. The use of multiple chaotic map strength key space and enhanced the security of medical images.

3.3 Experimental Results and Discussion

The Intel Core i7, 9th Gen processor with software tool MATLAB R2016b is used for implementation. The different types of medical images namely, MRI, CT, Ultrasound, ECG, and X-Ray images are used to carry out the experiment. From each category 100 samples are collected. Total 500 medical image samples of size 512×512 are utilized. In this proposed cryptosystem, based on intensity level the original medical image as exhibited in Fig.3.2. (a), is segmented into two sub images specifically Odd image and Even image using Algorithm 3.1. Both sub images are renewed into binary images. These images are transformed into DNA structures using DNA encoding rule 7 specified in Table 1.1 of Section 1.6 of Chapter 1. Chen's hyper chaotic map specified in Eqns.(1.5.1) - (1.5.4) of Chapter 1, the primary values of position variables x_0=0.3, y_0=-0.4, z_0=1.2 and w_0=1 and control factors a_1=36, b_1=3, c_1=28, d_1=-16 and k=0.2 are empirically determined to generate Chen's chaotic sequences. The chaotic sequences are sorted in ascending order and position of sorted sequences is referred for the permutation of Odd DNA structure. In Lorenz chaotic map specified in Eqns. (1.5.5) - (1.5.7) of Chapter 1, the primary values of arbitrary parameters are taken as p_0=1.2, $q_{0=}$1.2, and u_0 =3.7 to create Lorenz chaotic sequences. The Lorenz chaotic sequences are arranged in increasing order, and position of ordered sequences is mapped for permutation of Even DNA structure. DNA ADD operation specified in Table 1.2 of Section 1.6 of Chapter 1, is utilized for diffusion of



(a) (b) (c)

Fig. 3.2 MR image samples: **(**a) original MRI medical image (b) Cipher image (c) Decipher MR image

DNA structures. The diffused structures are decoded into binary images using an inverse of DNA encoding rule 6 specified in Table 1.1 of Section 1.6 of Chapter 1. These images are renovated into cipher image as exhibited in Fig.3.2 (b).

In proposed decryption method, the cipher image is bifurcated into two sub images using bifurcation process specified in Algorithm 3.3. Both sub images are renovated into Odd and Even DNA matrices using DNA encoding rule 6. DNA SUB operation specified in Table 1.3 of Section 1.6 of Chapter 1, is employed for diffusion of DNA structures. Chen's chaotic sequences and Lorenz's chaotic sequences are used for permutation of Odd and Even DNA structures. The binary images are obtained using DNA decoding rule 7. The binary images are converted into decipher image as exhibited in Fig.3.2 (c).

The working procedure of Algorithm 3.2 is illustrated with one suitable example. Consider the original medical image matrix of size 4×4.

Step 1: The original medical image O is bifurcated into Odd image and Even image based on intensity levels.

O =				
	4	2	8	3
	1	6	10	9
	7	3	4	5
	12	11	33	20

Oddimage =				
	0	0	0	3
	1	0	0	9
	7	3	0	5
	0	11	33	0

Evenimage				
	4	2	8	0
	0	6	10	0
	0	0	4	0
	12	0	0	20

Step 2: Conversion into binary images

B_o =				
	0	0	0	00000011
	00000001	0	0	00001001
	00000111	00000011	0	00000101
	0	00001011	00100001	0

B_e=	00000100	00000010	00001000	0
	0	00000110	00001010	0
	0	0	00000100	0
	00001100	0	0	00010100

Step 3: Chen's chaotic sequence *x* and *y* generation and conversion into binary form

Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
x	0.2850394	0.270294	0.255755	0.241413	0.172348	0.106952	0.044253	-0.01668
$\bar{x}$	-0.89213	-0.73158	-0.59131	-0.46712	-0.35531	-0.26584	-0.18097	-0.0986
Integer form	87	149	231	77	82	199	73	123
Binary Form	'1010111'	'10010101'	'11100111'	'1001101'	'1010010'	'11000111'	'1001001'	'1111011'

Index	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
x	-0.0986	-0.18097	-0.26584	-0.35531	-0.46712	-0.59131	-0.731578	-0.89213
$\bar{x}$	-0.01668	0.044253	0.106952	0.172348	0.241413	0.255755	0.270294	0.2850394
Integer form	123	78	40	52	135	5	58	130
Binary Form	'1111011'	'1001110'	'101000'	'110100'	'10000111'	'0000101'	'111010'	'10000010'

Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
y	-0.404746	-0.40971	-0.41488	-0.42027	-0.45053	-0.48654	-0.52865	-0.5773
$\bar{y}$	-1.90819	-1.6148	-1.36756	-1.15955	-0.98496	-0.85696	-0.74778	-0.65519
Integer form	229	245	240	213	2	242	126	125
Binary Form	'11100101'	'11110101'	'11110000'	'11010101'	'10'	'11110010'	'1111110'	'1111101'

Index	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
y	-0.6552	-0.74778	-0.85696	-0.98496	-1.15955	-1.36756	-1.6148	-1.90819
$\bar{y}$	-0.5773	-0.52865	-0.48654	-0.45053	-0.42027	-0.41488	-0.40971	-0.40476
Integer form	16	229	64	63	12	203	56	157
Binary Form	10000	11100101	1000000	111111	1100	11001011	111000	10011101

Step 4: The Lorenz chaotic sequence *p* and *q* generation and conversion into binary form

Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
p	1.2135248	1.252562	1.315411	1.401076	1.509175	1.639867	1.793797	1.972059
$\bar{p}$	4.534352	4.07593	3.664014	3.29473	2.964470	2.669898	2.408013	2.176162
Integer form	8	72	213	75	133	146	179	85
Binary Form	00001000	01001000	11010101	01001011	10000101	10010010	10110011	01010101

Index	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
p	2.176162	2.408013	2.669898	2.964470	3.29473	3.664014	4.07593	4.534352
$\bar{p}$	1.972059	1.793797	1.639867	1.509175	1.401076	1.315411	1.252562	1.2135248
Integer form	16	161	237	255	1	65	41	59
Binary Form	00010000'	10100001	11101101	11111111	00000001	01000001	00101001	00111011

Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
q	1.479801	1.764195	2.059093	2.370055	2.702438	3.061515	3.452578	3.881027
$\bar{q}$	9.364305	8.421036	7.563769	6.786644	6.083361	5.447470	4.872573	4.352431
Integer form	12	35	85	205	163	231	169	6
Binary Form	00001100	00100011	01010101	11001101	10100011	11100111	10101001	00000110

Index	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
q	4.352431	4.872573	5.447470	6.083361	6.78664314	7.563769	8.421036	9.364305
$\bar{q}$	3.881027	3.452578	3.061515	2.702438	2.370055	2.059093	1.764195	1.479801
Integer form	43	89	235	80	8	152	119	238
Binary Form	00101011	01011001	11101011	01010000	00001000	10011000	01110111	11101110

Step 5: Construction of DNA structures (D_o and $D_{e)}$ using DNA rule-7 from binary images B_o and B_e. The DNA structure D_o is shuffled row-wise and column-wise using the index of sorted sequences $\bar{x}$ and $\bar{y}$.

D_o Row-wise =				
	0	TGTC	TTGA	0
	TTCC	0	TTTA	TTCA
	TTGC	0	0	TTTC
	TTTA	0	0	0

D_{o1} Column-wise =				
	0	TTTC	TTCA	0
	0	0	TTTA	TTGA
	0	0	0	TGTC
	TTTA	TTGC	TTCC	0

Step 6: The DNA structure D_e is shuffled row-wise and column-wise using the index of sorted sequences $\bar{p}$ and $\bar{q}$.

D_e Row-wise =				
	TCCT	0	0	TTAT
	0	TTCT	0	0
	0	TTGG	TTCG	0
	0	TTGT	TTTG	TTCT

D_{e1} Column-wise =				
	TTCT	0	0	TTAT
	TTTG	TTCG	0	0
	TTGT	TTGG	TTCT	0
	0	0	0	TCCT

Step 7: The DNA structures are constructed for chaotic sequences.

D_{cx} =				
	CCCA	GCCC	AGCA	CTAC
	CCTG	ATCA	CTGC	CAGA
	CAGA	CTAG	TGGT	TACT
	GTCA	TTCC	TAGG	GTTG

D_{cy} =				
	AGCC	TTTG	TGTT	TTAT
	AACC	AATG	AGCC	ATGA
	AATT	CAAG	CTTT	TAGT
	ACCC	CAAC	TAAA	GCAC

D_{Lp} =				
	TTGT	CTGT	ACCC	CTGA
	GTCC	GCTG	GATA	CCCC
	TCTT	GGTC	AGAC	AAAA
	TTTC	CTTC	TGGC	TAGA

D_{Lq} =				
	TTAT	GGTA	TGGA	TTGT
	TGTA	AGCA	CCGC	GCCT
	CCCC	GGGC	AGGA	CACA
	ATTC	TTCG	CCTT	AGAG

Step 8: The DNA structures are diffused row-wise and column-wise using DNA ADD operations respectively.

D_{oc} = (row-wise)				
	0	ATTC	GACC	0
	0	0	TCAA	TGCC
	0	0	0	CTTT
	ACTC	CCGC	CGGG	0

D_{oc} = (column-wise)				
	0	GCCG	ATTT	0
	0	0	GGAA	GAGA
	0	0	0	TGAC
	CCTC	CATC	TTTT	0

D_{eL}= (row-wise)				
	CCGC	0	0	TCTG
	ACTG	ATTC	0	0
	CTAC	AAAG	GAAT	0
	0	0	0	CAGG

D_{eL}= (column-wise)				
	TTTT	0	0	CTAA
	GGCT	CATA	0	0
	CTAC	TTTG	TTTG	0
	0	0	0	ATTC

Step 9: The diffused column-wise DNA structures are decoded into binary images using DNA rule 6.

Bo =				
	0	00111100	10010101	0
	0	0	00001010	00100010
	0	0	0	01001011
	11110101	11100111	01010101	0

B_e =				
	01010101	0	0	11011010
	00001101	11100110	0	0
	11011011	01010100	01010100	0
	0	0	0	11011010

Step 10: Generation of grey-scale images G_1 and G_2.

G_1 =				
	0	60	149	0
	0	0	10	34
	0	0	0	75
	245	231	85	0

G_2=	85	0	0	218
	13	230	0	0
	219	84	84	0
	0	0	0	218

Step 11: Generation of cipher image E.

E =	85	60	149	218
	13	230	10	34
	219	84	84	75
	245	231	85	218

3.3.1 Performance and Security Analysis

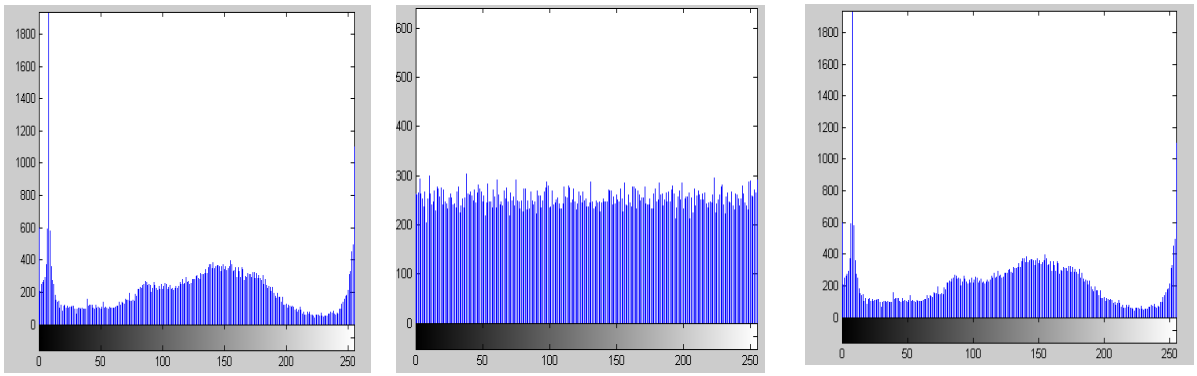
The performance of proposed cryptosystem depends on invulnerable to various kinds of attacks. The security analysis verifies the resistant of intensity-based cryptosystem against various kinds of attacks namely, statistical, exhaustive, and differential attacks.

A. Statistical Attack

The histogram and correlation coefficient parameters are exploited to prove resistant against statistical attacks. The intruders study the pixels of cipher and try to predict original medical image and secret key.

Histogram Analysis

Intruders monitor the frequency of distribution of pixels and based on frequency distribution, try to predict the original medical image. Thus, pixels of cipher images must be distributed very randomly. So that, the speculation of original image must be impossible. The pixels are distributed very inconsistently in original medical image and decipher image as exhibited in Fig 3.3 (a) and Fig 3.3 (c) respectively. The pixels are distributed very uniformly in cipher image as exhibited in Fig 3.3 (b). It proves that, proposed medical image en/decryption method based on intensity of the pixels has good confusion properties.



(a) (b) (c)

Fig. 3.3 Histogram analysis: (a) Original MR medical image (b) Cipher image (c) Decipher MR image

The consistency of spreading is statistically proved using chi-square hypothesis test as exhibited in Table 3.1. From Table 3.1, it is proved that pixels of cipher image are disseminated consistently.

Table 3.1 Chi-square test results of proposed intensity level-based DNA cryptosystem

Medical image type	Cipher image	Hypothesis test
MR	251.2489	pass
CT	253.7632	pass
X-ray	255.7344	pass
Ultrasound	254.2075	pass
ECG	250.5625	pass

Correlation Coefficient Analysis

The correlation coefficient analysis is to verifies the linear relation amid adjoining pixels of original medical images and cipher images. The contiguous pixels are extremely correlated in original medical images. If contiguous pixels are either correlated negatively or do not correlate in cipher image then, it is appropriate to offer security. The correlation among pixels of cipher image and decipher image are exhibited in Table 3.2. The contiguous pixels of cipher image are negatively correlated, indicating that pixels are altered in cipher image.

Table 3.2 Correlation coefficient of proposed intensity level-based DNA cryptosystem

Medical image type	Direction	Cipher image	Decipher image
MR	*Horizontal*	-0.0020	0.997
	Vertical	-0.0029	0.999
	Diagonal	-0.0021	0.995
CT	*Horizontal*	-0.0019	0.996
	Vertical	-0.0018	0.993
	Diagonal	-0.0017	0.995
X-ray	*Horizontal*	-0.0030	0.995
	Vertical	-0.0032	0.994
	Diagonal	-0.0034	0.995
Ultrasound	*Horizontal*	-0.0024	0.993
	Vertical	-0.0022	0.996
	Diagonal	-0.0023	0.997
ECG	*Horizontal*	-0.0028	0.994
	Vertical	-0.0023	0.998
	Diagonal	-0.0021	0.996
	Average:	**-0.0024**	**0.995**

The scatter plot for the correlation coefficient of contiguous pixels of an original medical image in horizontal, vertical, and diagonal directions are shown in Fig. 3.4 (a and b and c). The correlation coefficient of contiguous pixels of the cipher image in three directions are shown in Fig.3.4 (d and e and f). From Fig. 3.4, it is observed that there is a linear relation among pixels of origin al image and no linear relation among pixels of cipher image.

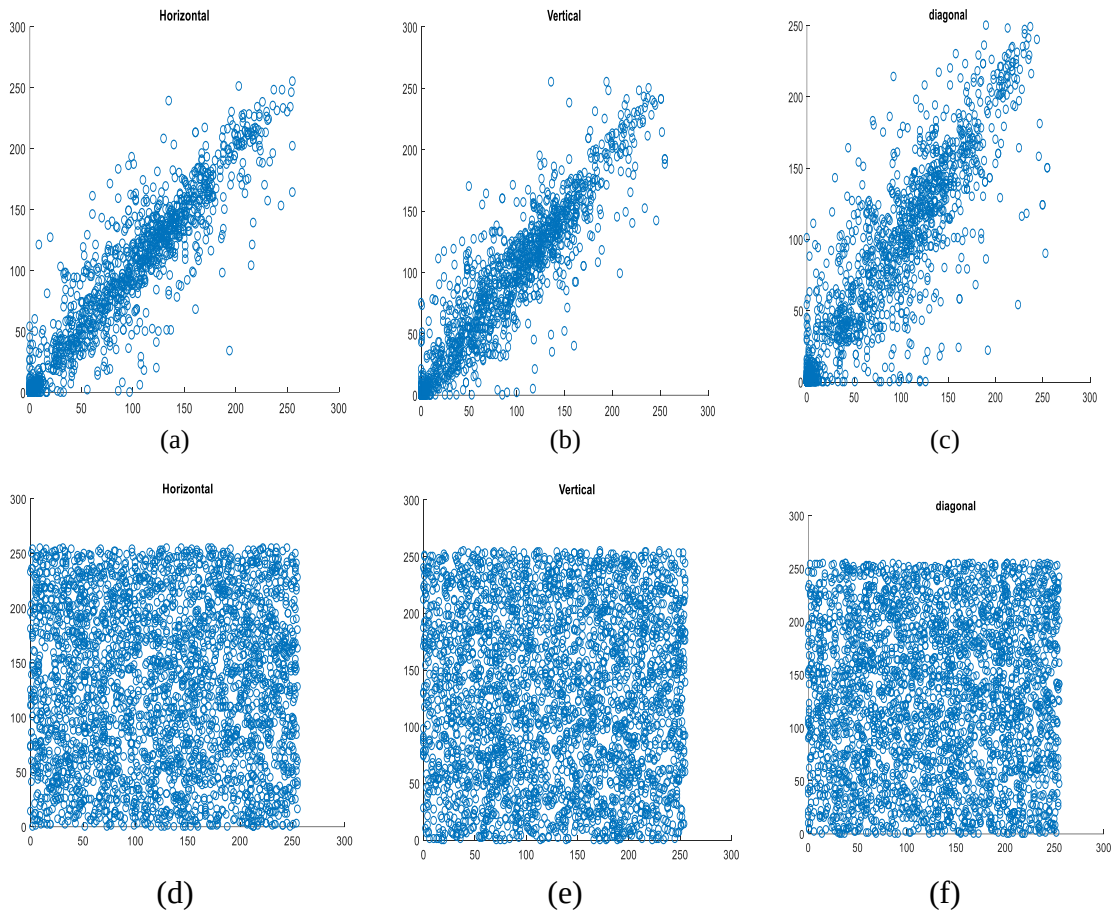


Fig. 3.4 Scatter plot of original MR image in horizontal, vertical and diagonal directions (a)-(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

B. Exhaustive Attack

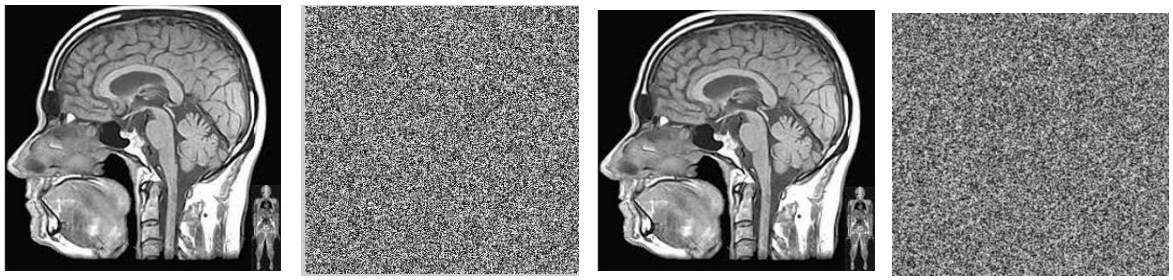
Intruders try to get the decipher image with all possible keys. The secret keys are very crucial in DNA cryptosystem. The key space and key sensitivity analyses are accomplished to validate against exhaustive attack.

Key Space Analysis

In proposed en/decryption based on intensity method, secrete keys are the preliminary values of positional variables and control factors of Chen's chaotic map and Lorenz's chaotic map. A total of eight secret keys (x_0, y_0, z_0, w_0, k, p_0, q_0, *and* u_0) are available. Then, the length of key space is $(10^{15})^8 \approx 2^{400}$. The key space is high enough to endure exhaustive attack.

Key Sensitivity Analysis

The high-dimensional Chen's chaotic map and Lorenz's chaotic map are very sensitive to initial conditions. Hence, decrypting the original medical image with a very small variance in preliminary condition is highly impossible. In en/decryption based on intensity method, among eight secret keys if we vary any one secret key preliminary value, then it is highly incredible to decrypt the original image. The cipher image as exhibited in Fig. 3.5(b), is decrypted using the correct secret key q_0=1 as exhibited in Fig.3.5(c). The deciphered image is the same as the original medical image as exhibited in Fig.3.5(a). The decipher image decrypted with modified secret key value q_0=1.0000001 instead of q_0=1 is exhibited in Fig 3.5(d). the deciphered image is unlike from the original medical image. This proves that the proposed cryptosystem is very sensitive to initial conditions.



(a) (b) (c) (d)

Fig. 3.5 Key sensitivity analysis: **(**a) Original MR image (b) Cipher image (c) Decipher image decrypted using q_0=1 (d) Decipher image decrypted using wrong key q_0=1.0000001

C. Differential Attack

The parameters NPCR and UACI discussed in Section 1.9.2 of Chapter 1. are used by cryptanalysts to verify invulnerable to differential attacks. The NPCR average value is 99.64974 and UACI average value is 33.56 almost equal to the ideal value shown in Table 3.3. Therefore, the proposed cryptosystem resists differential attacks.

The quality assessment is measured using metrics MSE, PSNR, and entropy discussed in Section 1.10 of Chapter 1. The values of MSE, PSNR, and entropy for cipher image are exhibited in Table 3.3. From table 3.3, it is perceived that MSE is very high and PSNR value is very low. The proposed intensity-based cryptosystem is very much robust and

efficient. The entropy average value is 7.99738 is almost equal to ideal value. It demonstrates that the proposed method provides good randomness.

Table 3.3 Performance analysis of proposed intensity level-based DNA cryptosystem

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.6554	33.45	7.9991	5.6068e+03	6.6345
CT	99.6552	33.62	7.9990	4.5684e+03	5.1507
X-ray	99.6501	33.48	7.9945	5.9979e+03	6.0934
Ultrasound	99.6637	33.69	7.9978	4.7841e+03	5.6387
ECG	99.6243	33.56	7.9965	5.0825e+03	6.1437
Average	**99.6497**	**33.56**	**7.9973**	**5.21e+03**	**5.9322**

3.3.2 Computation Time of Proposed En/Decryption Algorithm Based on Pixel Values

The computation time of proposed encryption algorithm based on pixel value for original medical image of size (m×n) is calculated as follows:

Step 1: Fragmentation process: (m×n)

Step 2: Binary conversion of sub images: 2(m×n)

Step 3: construction ODD and EVEN DNA structure: 2(m×n)

Step 4: Permutation process: 2(m×n)

Step 5: Diffusion process: 2(m×n)

Step 6: DNA decoding: 2(m×n)

Step 7: Generating cipher image: (m×n)

Total time complexity of the proposed method is given below:

$$T(n)= (m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ 2(m\times n)+ (m\times n)= 12(m\times n)$$

If m=n then $T(n)=12(n^2)\in O(n^2)$.

The space efficiency of medical image encryption system based on intensity of the pixels for a given original medical image of size (m×n) and a temporary array of size ((m×n) to process ODD and EVEN images. It is $O(2n^2)$ assuming m=n.

3.3.3 Comparative Analysis

The proposed intensity-based cryptosystem is compared with existing methods is depicted in Table 3.4. From Table 3.4, it is perceived that the performance parameter values of the proposed intensity-based cryptosystem are approximately equivalent or larger than existing methods. The key space is also larger.

Table 3.4 Comparative analysis of proposed intensity level-based DNA cryptosystem

Method	Entropy	NPCR (%)	UACI (%)	Key Space
Xiaopeng, et al., 2012	7.9971	99.57	33.48	2^{233}
Zhen, et al., 2016	7.9993	99.60	33.45	2^{295}
multistate en/decryption (Chapter 2)	7.9921	99.64	33.61	2^{268}
Proposed en/decryption method	**7.9973**	**99.65**	**33.56**	**2^{400}**

The comparative analysis as exhibited in Fig. 3.6 evidences that the proposed cryptosystem is invulnerable to crypto attacks and size of the secret keys is very large. Hence, proposed cryptosystem ensures secured broadcast of medical images through an open-source network.

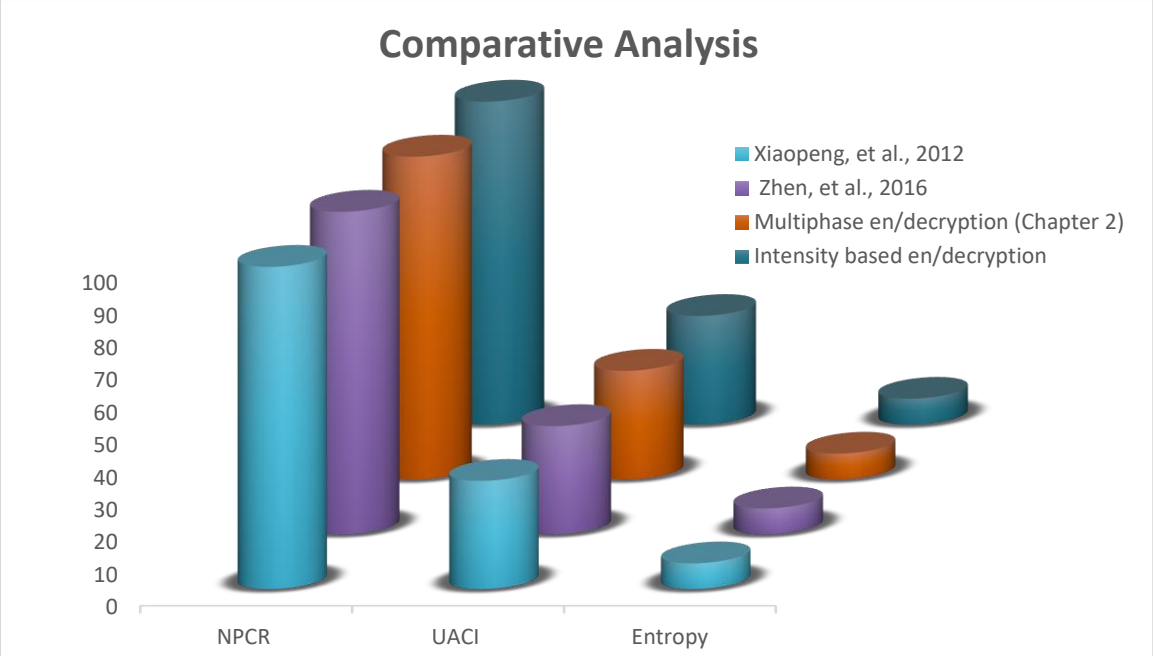


Fig. 3.6 Comparative analysis of proposed DNA cryptosystem based on intensity levels of medical image

The proposed medical image en/decryption based on intensity level is efficient to offer security for medical images compared to method specified in Chapter 2. The size of the secret key is also higher than technique specified in the Chapter 2. Thus, proposed cryptosystem based on intensity level is more efficient than the en/decryption method specified in Chapter 2.

3.4 Summary

This Chapter describes medical image en\decryption method based on intensity level of the pixels. The medical image is bifurcated into Odd image and Even image depending on intensity level of pixel. DNA coding rules are used for the conversion of DNA structures. The Odd DNA structure is permuted by Chen's chaotic sequence and Even DNA structure is permuted by Lorenz's chaotic sequences. DNA ADD method is used between DNA encoded Chen's chaotic sequences and Odd DNA structure for diffusion of Odd DNA structure. The DNA ADD method is used between DNA encoded Lorenz chaotic sequences and Even DNA structure for diffusion of Even DNA structure. The DNA decoding rule is used to get a cipher image. The performance analysis demonstrates that proposed en/decryption technique based on intensity level is endure to statistical, differential, and exhaustive attacks. The medical images carry a sensitive information related to diseases.

During transmission through insecure channels, intruders can add noise or tamper the medical images. Then, diagnosing the specific disease from a tampered medical image is extremely not possible. Hence, ensuring the integrity of medical image is also very significant like security. The proposed en/decryption technique based on intensity level is adequate to provide security, but integrity is not verified. The new encryption method concentrating on providing security and enforcing integrity, is proposed in consequent Chapters.

Chapter 4

DNA Cryptosystem with Integrity and Confidentiality

4.1 Introduction

Telemedicine and e-Health services are growing rapidly, due to advancement in digital communication and enhancement in wireless transmission. These services are time efficient and easily accessible in remote areas where medical services are limited. These services are not in potential use, due to a lack of security issues. Several encryption techniques based on chaos theory are available. In (Tanveer et al.,2021), the SHA-256 function calculates the 256-bit hash digest of original medical image. These hash values are employed to get the initial values for logistic map and Lorenz attractor. The chaotic sequence of the logistic map is applied to confuse the pixels of the medical image in the first stage. The confused medical image pixels are again confused using Lorenz attractor and single circular shift in second stage. The pixels of a multistage confused medical image are diffused using logical XOR to gain a cipher image.

In (Kamal et al.,2021), the medical image is bifurcated into sub parts and each sub part's pixels are confused using a zigzag pattern, rotation, and random permutation. These pixels are diffused to gain a cipher image. In (Massod et al.,2021), the medical image is divided into sub parts. The henon map chaotic sequences are utilized to shuffle the pixels of each sub part separately in first phase. All sub parts are shuffled in the second phase. The three-dimensional Brownian motion and Chen's chaotic sequences are utilized for the diffusion of confused medical images to attain a cipher image. In (Shanshan et al.,2021), the

---

[1] Prema T. Akkasaligar and Sumangala Biradar, "***Medical Image Encryption with Integrity using DNA and Chaotic Map*** ", Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2018. Communications in Computer and Information Science, vol. 1036, part 2, Springer Nature Singapore Ple. Ltd. 2019, pp. 143-153.

[2] Prema T. Akkasaligar and Sumangala Biradar, "***Multilevel security for medical image using heterogeneous chaotic map and deoxyribonucleic acid sequence operations",*** Concurrency Computat Pract Exper. 2022; e7222, vol.34,issue 20/10, pp.1-21.

combination of two-dimensional sine logistic modulation map (2D-SLMM) and two-dimensional henon- sine map (2D-HSM) are employed to produce the chaotic sequences. These sequences are mapped for permutation of even rows and odd rows pixels separately. These pixels are scrambled one more time using zigzag transform. The modified cat map sequences are applied for the diffusion of a scrambled image to attain a cipher image. In (Yasser et al.,2022), the given medical image is bifurcated into two sub images. The sub image pixels are diffused by logical XOR. The permutation and diffusion operations are performed on two sub images separately using modified 2D chaotic maps. These confused intermediate cipher images are merged to get a final cipher image.

These encryption methods are suitable to offer security for medical images, but integrity is not verified. For plain images, if any part of the image is tampered or discarded during transmission, it can be recovered at the receiver end. The main tool for diagnosis of the disease in smart-health service is a medical image. The medical images carry a sensitive and confidential information about patient. Small variance in medical images creates a very significant problem. So, high-level security, integrity, and confidentiality, are fundamental for medical images while transmitted through insecure channels. Confidentiality means only authorized users can view sensitive information. Integrity means maintaining the consistency, accuracy, and trustworthiness of medical images. A new encryption method with multilevel security, confidentiality and integrity is discussed in this chapter.

4.2 Importance of Integrity

Medical images are major tool in the diagnosis of potential disease, treatment, and research. Transmission of medical images through insecure channel may lead to irrevocable harm, substantially, ethically, and generally to the patient, and hypothetically disturb the trustworthiness of healthcare institution. Thus, it is important to take measures to prevent tampering and verify the patient provenance. This issue challenges to implementation of security techniques to ensure the integrity of medical images.

Hash function described in Section 1.4 of Chapter 1 is suitable to endorse the integrity of medical images. Most used hash function is Secure Hash Algorithm (SHA-2) family. The SHA-2 is a significant variant of antecedent SHA-1. SHA-1 is broken down by brute force attack. Hence, the SHA-2 family is premeditated by United States National Security

Agency (NSA) and first published by National Institute of Standards and Technology (NIST) in 2001. The SHA-2 family consists of six variants of hash functions namely, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 based on the size of hash values. The SHA-256 and SHA-512 are innovative hash functions worked out with eight 32-bit and 64-bit words, respectively. Details of hash function SHA-256 are shown in Appendix II.

4.2.1 SHA-512

In emerging advancements in computation, on a 64-bit processor computing hash value is faster for hash function SHA-512 than hash function SHA-256. The SHA-512 gives a fixed-size hash output of 512-bit. Whereas, the SHA-256 produces a fixed size hash output of 256-bit. The hash output of 512- bit hash key is larger than the 256-bit hash key. The greater number of bits in the hash output is more secure and collision resistance is also high. Hence, for more security purposes SHA-512 is used in proposed method.

The SHA-512 give a fixed 512-bit hash value for varying input up to 2^{128} bits. The input DNA sequence M of varying length $L < 2^{128}$ bits is processed into 1024-bit blocks depicted in Eq. (4.2.1).

$$M = M_1 + M_2 + M_3 + \ \ldots. \ + \ M_{128} \qquad (4.2.1)$$

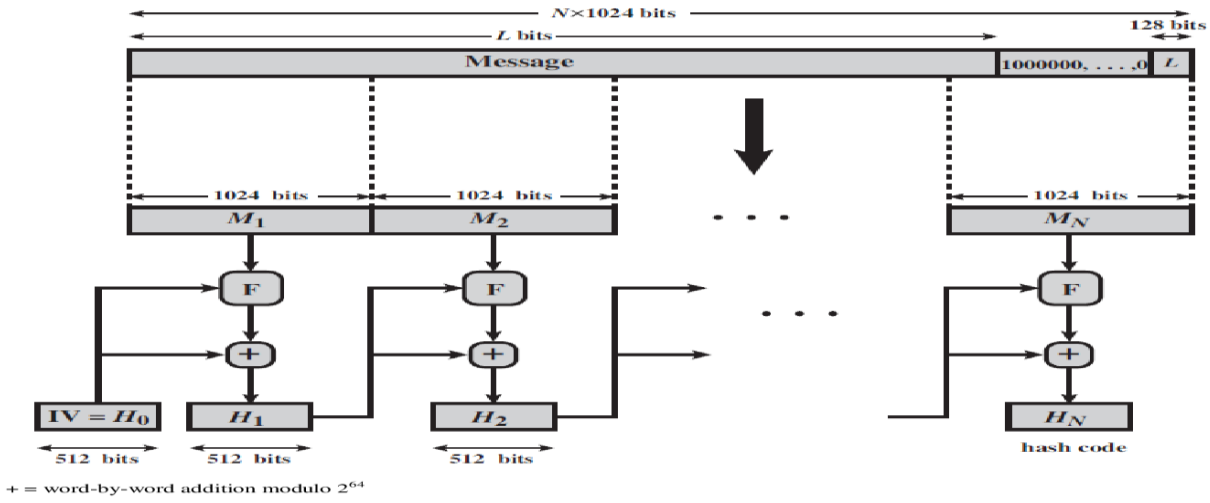


Fig.4.1 Block diagram for hash function SHA-512

Image credit: https://en.bitcoinwiki.org/wiki/SHA-512

The DNA sequence is padded with a '1' bit followed by '0' bits to get the desired length block. In last block, the last 128 bits are used to specify the size of DNA sequence and it is appended at the end of DNA sequence i.e. message as presented in Fig.4.1.

Each block of size 1024-bits is processed to get the intermediate hash value of size 512-bits. The output of each block is stored in hash buffer H of size 512-bits. Each buffer is represented as eight registers and each register is initialized with 64-bit hexadecimal values. The initial vector (IV) value is the initial block buffer H_0. The initial block buffer H_0 is further divided into eight blocks. The eight blocks are considered as eight registers and are initialized with the following constant values.

H_0^1= 0x6A09E667F3BCC908 H_0^5 = 0x510E527FADE682D1

H_0^2 = 0xBB67AE8584CAA73B H_0^6= 0x9B05688C2B3E6C1F

H_0^3 = 0x3C6EF372FE94F82B H_0^7=0x1F83D9ABFB41BD6B

H_0^4 = 0xA54FF53A5F1D36F1 H_0^8= 0x5BE0CDI9137E2179

Each DNA sequence block of size 1024-bits is further subdivided into 16 parts of size 64-bits word each, specified in Eq. (4.2.2).

$$M^1 = M_1^1 + M_1^2 + M_1^3 + \ldots\ldots\ldots + M_1^{16} \quad (4.2.2)$$

The message schedule array A [0….79] is created. The values of 16 parts of the DNA sequence block are assigned to array A [0…15]. Remaining values of array A [16…79] are derived from 16 parts of DNA sequence using Eqs. (4.2.3 - 4.2.6).

$$A[t] = M_t^1 \quad \text{for } 1 <= t <= 16 \quad (4.2.3)$$

$$A[t] = \text{Sigma1}(A[t-2]) + A[t-7] + \text{Sigma0}(A[t-1\ 5]) + A[t-16] \quad \text{for } 16 <= t <= 79 \quad (4.2.4)$$

$$\text{Sigma0} = (A[t-15] \text{ rightrotate } 1) \oplus (A[t-15] \text{ rightrotate } 8) \oplus (A[t-15] \text{ rightshift } 7) \quad (4.2.5)$$

$$\text{Sigma1} = (A[t-2] \text{ rightrotate } 19) \oplus (A[t-2] \text{ rightrotate } 61) \oplus (A[t-2] \text{ rightshift } 6) \quad (4.2.6)$$

This process is repeated, in 80 rounds for each DNA sequence part to get the intermediate hash value of fixed size 512-bits. This intermediate output is used as input for the next part

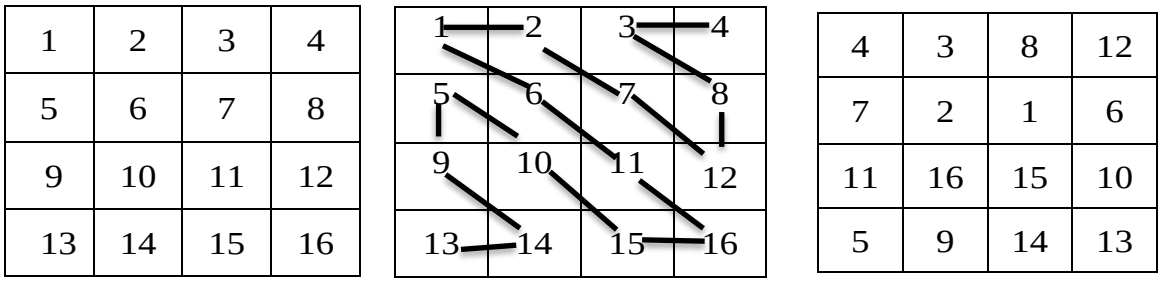
of DNA sequence. This procedure is iterative until it reaches the big-endian of DNA sequence. The output of last part is the final value for the given DNA sequence. The hash value of SHA-512 is utilized to ensure the integrity of medical images.

The en/decryption methods proposed in previous chapters are suitable to provide security and entail additional memory space. Hence, it is very essential to develop a new en/decryption method with reduced memory space and with significant security, confidentiality, and integrity.

The method based on SHA-256 is proposed to provide integrity and confidentiality respectively is presented in Appendix II. Chen's chaotic map and DNA cryptography are proposed to offer significant security for medical images. The description of the method is available in Appendix II. To improve the performance of the DNA cryptosystem and to enhance the security of medical images with longer hash keys, a SHA-512 is used instead of SHA-256. The zigzag transform is utilized to provide multilevel security.

4.3 Zigzag Transform

Zigzag transform is applied to transform the pixels in zigzag pattern. In this pattern, position of pixels considered from left-side corner. In new zigzag transform, instead of left-side corner a right-side corner is considered to get a new zigzag pattern. For example, consider a matrix of size 4×4 and new zigzag pattern for the given matrix is depicted in Fig.4.2.



(a) (b) (c)

Fig.4.2 Zigzag transform: (a) Sample matrix (b) Zigzag Process (c) Zigzag pattern

4.4 Proposed DNA Cryptosystem with Integrity and Confidentiality

To enhance security along with confidentiality and integrity, a cryptosystem using SHA-512 is proposed. In proposed cryptosystem to enhance security, the heterogeneous chaotic maps, zigzag transform and DNA cryptography are used. To provide confidentiality and integrity for medical images, DNA sequence and SHA-512 are used. In first level, the SHA-512 function produces a 512-bit hash key for Canis lupus DNA sequence (ID MW549038 in GenBank). The original medical image is renewed as a binary image and a 512-bit hash value is embedded in the LSB of a binary image. In the second level, DNA structure is constructed for an embedded binary image using dynamic DNA encoding rules. DNA structure is bifurcated into two sub DNA structures. In third level, chaotic sequences are generated using heterogenous chaotic maps namely, Chen's chaotic map and Lorenz's chaotic map. Chen's chaotic sequences permutes the first sub-image DNA structure. Lorenz chaotic sequence permutes the second sub-image DNA structure. In fourth level, the scrambled pixels are one more time scrambled by zigzag transform. In fifth level, DNA ADD operation diffuses the pixels of scrambled DNA structures. In sixth level, with the help of dynamic DNA decoding rules the cipher image is obtained.

4.4.1 Medical Image Encryption Algorithm using SHA-512

The proposed medical image encryption method is aimed for fulfilling the integrity, confidentiality, and security necessities of medical images as exhibited in Fig. 4.3. The multilevel medical image encryption is proposed using SHA-512, Chen's hyperchaotic system, Lorenz's chaotic system, and DNA operations. An expansive description of the proposed medical image encryption using SHA-512 is represented in Algorithm 4.1.

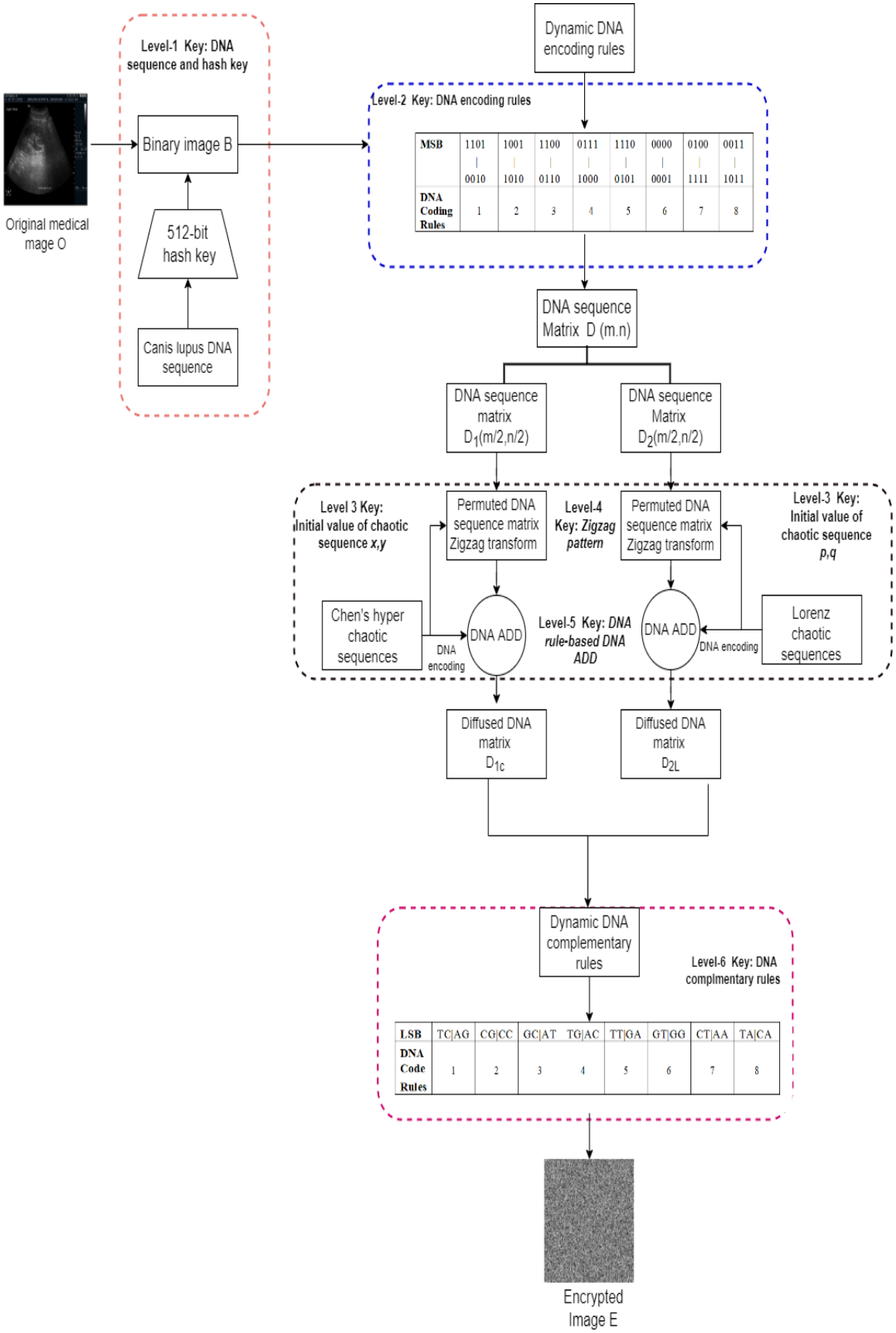


Fig. 4.3 Block diagram of proposed medical image encryption method using SHA-512

Algorithm 4.1: Medical Image Encryption using SHA-512
//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1: Start

Step 2: The original medical image is renewed as a binary image

B (r, c×8) = dec2bin (O (r, c));

Step 3: For arbitrary length input Canis lupus DNA sequence, a SHA-512 function produces a fixed size 512-bit hash value 'H'. It is embedded into the LSB of binary image B.

Step 4: Embedded binary image is reformed into a DNA structure using all eight DNA encoding rules. Depending on 4-bit MSB of the pixel of a binary image, DNA encoding rules are selected dynamically. The dynamic selection of DNA encoding rules is depicted in Table 4.1.

Table 4.1 Selection of dynamic DNA encoding rules

MSB	1101 | 0010	1001 | 1010	1100 | 0110	0111 | 1000	1110 | 0101	0000 | 0001	0100 | 1111	0011 | 1011
DNA encoding rules	1	2	3	4	5	6	7	8

D (r, 4×c) = DNA sequence matrix for B (r, c×8);

Step 5: DNA structure is bifurcated into two equal DNA submatrices

D_1 (m×n) = DNA sequence matrix D_{12} (0…(r/2)-1, 0…(4c/2)-1);

D_2 (m×n) = DNA sequence matrix D_{12} ((r/2) …4c-1, (4c/2) …. 4c-1);

Step 6: Chen's hyperchaotic sequences x and y are arranged in increasing order.

$$x = [x_0, x_1, x_2, \ldots\ldots x_n];$$

$$y = [y_0, y_1, y_2, \ldots\ldots y_n];$$

$$\bar{x} = sort(x);$$

$$\bar{y} = sort(y);$$

Step 7: Index of sorted sequences $\bar{x}$ and $\bar{y}$ are mapped to permute the pixels of D_1, row-wise and column-wise respectively.

Step 8: Lorenz chaotic sequences p and q are arranged in increasing order.

$p = [p_0, p_1, p_2, \ldots\ldots p_n];$

$q = [q_0, q_1, q_2, \ldots\ldots q_n];$

$\bar{p} = sort(p);$

$\bar{q} = sort(q);$

Step 9: Index of sorted sequences $\bar{p}$ and $\bar{q}$ are mapped to permute the pixels of D_2, row-wise and column-wise respectively.

Step 10: The chaotic sequences *x, y, p,* and *q* are transformed into DNA sequences D_c and D_L using DNA encoding rules. The dynamic selection of DNA encoding rules depends on the 4-bit MSB of the pixel of a binary image. Dynamic selection of DNA encoding rules is depicted in Table 4.1.

Step 11: Zigzag pattern is applied to transform the pixels of D_1 and D_2.

Step12: Diffusion operation DNA ADD is employed to diffuse the pixels of D_1 and D_2 respectively.

D_{1c} (m×n) = D_1 (m×n) DNA ADD D_c (m×n);

D_{2L} (m×n) = D_2 (m×n) DNA ADD D_L (m×n);

Step 13: Diffused matrices D_{1c} and D_{2L} are concatenated.

$D_{12}(r, 4\times c) = D_{1c} \,||\, D_{2L}$

Step14: The diffused matrix is renovated into a binary image using DNA complementary rules. Depending on 2-bit LSB of the DNA sequence matrix, DNA complementary rules are chosen dynamically, as shown in Table 4.2.

Table 4.2 Selection of dynamic DNA complementary rules

LSB	TC|AG	CG|CC	GC|AT	TG|AC	TT|GA	GT|GG	CT|AA	TA|CA
DNA encode rules	1	2	3	4	5	6	7	8

B (r, c×8) = DNA complementary rules D_{12} (r, 4×c);

Step 15: Binary image is reformed into cipher image

E (r, c) = bin2dec (B (r, c×8));

Step 16: Stop

The cipher image is decrypted into a decipher image using the decryption method.

4.4.2 Medical Image Decryption Algorithm using SHA-512

The medical image decryption method is utilized to decrypt the original medical image from the cipher image. The decryption method is the converse of encryption method. The expansive steps of the proposed decryption method are demonstrated in Algorithm 4.2.

Algorithm 4.2: Medical Image Decryption using SHA-512

//**Input:** Cipher image E (r, c)

//**Output:** Original medical Image O (r, c)

Step 1: Start

Step 2: Conversion of cipher image into a binary image

B (r, c×8) = bin2dec (E (r, c));

Step3: Transform binary image into a DNA structure using DNA inverse complementary rules. Depending on 4-bit LSB of a binary image, e DNA inverse complementary rules are chosen dynamically as depicted in Table 4.3.

Table 4.3 Selection of dynamic DNA inverse complementary rules

LSB	1101 | 0010	1001 | 1010	1100 | 0110	0111 | 1000	1110 | 0101	0000 | 0001	0100 | 1111	0011 | 1011
DNA encoding rules	1	2	3	4	5	6	7	8

D_{12} (r, 4×c) = DNA inverse complementary rules B (r,8c);

Step 4: Diffused matrices D_{1c} and D_{2L} are separated.

$D_{1c}(m \times n)$ = Split (D_{12}(r, 4×c))

$D_{2L}(m \times n)$ = Split (D_{12}(r, 4×c))

Step 5: Diffusion operation DNA SUB is employed to diffuse the pixels of D_{1c} and D_{2L} respectively.

D_1 (m×n) = D_{1c}(m×n) DNA SUB D_c (m×n);

D_2 (m×n) = D_{2L}(m×n) DNA SUB D_L (m×n);

Step 6: The pixels of D_1 and D_2 are retransformed using inverse of zigzag pattern

Step 7: Lorenz chaotic sequences *p* and *q* are arranged in decreasing order.

$$p = [p_0, p_1, p_2, \ldots\ldots p_n];$$

$$q = [q_0, q_1, q_2, \ldots\ldots q_n];$$

$$\bar{p} = sort(p);$$

$$\bar{q} = sort(q);$$

Step 8: Index of sorted sequences $\bar{p}$ and $\bar{q}$ are mapped to reshuffle the pixels of D_2.

Step 9: Chen's hyperchaotic sequences *x* and *y* are arranged in decreasing order.

$$x = [x_0, x_1, x_2, \ldots\ldots x_n];$$

$$y = [y_0, y_1, y_2, \ldots\ldots y_n];$$

$$\bar{x} = sort(x);$$

$$\bar{y} = sort(y);$$

Step 10: Index of sorted sequences $\bar{x}$ and $\bar{y}$ are mapped to reshuffle the pixels of D_1.

Step 11: The chaotic sequences *x*, *y*, *p*, and *q* are renewed into DNA sequences D_c and D_L using DNA coding rules. The dynamic selection of DNA encoding rules depends on the 4-bit MSB of the pixel of a binary image. The dynamic selection of DNA encoding rules is depicted in Table 4.1.

Step 12: Diffused matrices D_1 and D_2 are concatenated.

$$D_{12}(r, 4\times c) = D_1 \,||\, D_2$$

Step 13: The concatenated DNA matrix is renovated into a binary image using DNA complementary rules. DNA inverse coding rules are chosen dynamically based on 2-bits MSB of the DNA sequence matrix, as shown in Table 4.4.

Table 4.4 Selection of dynamic DNA inverse coding rules

MSB	TC|AG	CG|CC	GC|AT	TG|AC	TT|GA	GT|GG	CT|AA	TA|CA
DNA encode rules	1	2	3	4	5	6	7	8

B (r, c×8) = DNA inverse coding rules D_{12} (r, 4×c);

Step 14: The 512-bit hash key Hk is extracted from an embedded binary matrix. The SHA-512 function is executed to get the hash value 'Hk_1' for Canis lupus and compared with the extracted hash key. If both are

equal, then integrity is preserved otherwise the medical image is altered by attackers during transmission.

Step 15: Binary image is reformed into decipher image i.e. original medical image.

O (r, c) = bin2dec (B (r, c×8));

Step 16: Stop

The hash key and DNA sequence are secret keys in first level. In second level, DNA encoding rules are secret keys used to get a DNA sequence matrix. The primary values of state parameters of heterogeneous chaotic maps are secret keys in third level. The zigzag pattern is secret key in fourth level. Further, the DNA ADD operation is applied for the diffusion of a medical image in fifth level. In sixth level, DNA complementary rules are secret keys, used to translate the DNA sequence matrix into a cipher image. Therefore, the multiple keys in multiple levels are used for the enhancement of security level of medical images in this methodology. The SHA-512 is used to enforce integrity and DNA sequences for confidentiality of medical images in a proposed cryptosystem. All eight DNA encoding and complementary rules are utilized for the construction of unique DNA structures.

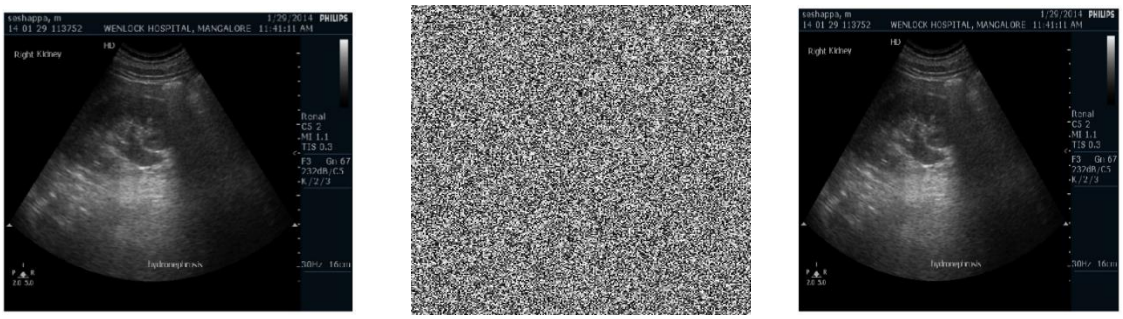
4.5 Experimental Results and Discussion

The proposed cryptosystem is exemplified using on 9^{th} generation Intel CoreTM i7 7500U CPU @ 2.70GHz, 2901 MHz, 2 Core(s), 4 Logical Processor(s). The software tool MATLAB 2016b is used for implementing the multilevel en/decryption technique using SHA-512. Total 500 medical image samples of five different categories namely CT, MRI, Ultrasound, X-ray, and ECG images are utilized for the experiment.

In proposed encryption method, the original medical image as exhibited in Fig.4.4(a) is transformed into a binary image. In first level, the SHA-512 is executed for the selected 512-bits of Canis lupus DNA sequence to get a 512-bits hash key. This hash key is embedded in the LSB of a binary image. At second level, DNA coding rules are chosen depending on bit-level value of medical image for the construction of DNA structure matrix. DNA structure matrix D is partitioned into two equal parts D_1 and D_2. The heterogeneous chaotic maps, namely Chen's hyperchaotic map and Lorenz chaotic

maps, are mapped for the permutation of DNA structure matrices D_1 and D_2, in the third level. The primary values of state parameters x_0 =0.3, y_0=- 0.4, z_0=1.2, and w_0=1 are empirically determined. The preliminary values of control parameters a_1=36, b_1=3, c_1=28, d_1=-16, and k=0.2 are empirically determined for the generation of a chaotic sequence using Eqns. (1.5.1) - (1.5.4) of Chapter 1.

In Lorenz chaos system, p_0=1.2, q_0=1.2, and u_0=3.7 are used as preliminary values. The chaotic sequences are generated using the Eqns. (1.5.5) - (1.5.7) of Chapter 1. These chaotic sequences are mapped for permutation of matrices (D_1, D_2). The zigzag pattern is utilized to transform the pixels of D_1 and D_2. The DNA ADD operation specified in Table 1.2 of Section 1.6 of Chapter 1 is applied for diffusion of DNA structures (D_1, D_2) in the fourth level. In the fifth level, the DNA complementary rules are employed to get the cipher image as depicted in Fig.4.4(b).



(a) (b) (c)

Fig. 4.4 Ultrasound image samples: (a) Original ultrasound image (b) Cipher image (c) Decipher image

In proposed decryption process, the cipher image is transformed into a binary image. The binary image renewed into a DNA structure matrix using DNA inverse complementary rules at the sixth level. The DNA structure matrix is bifurcated into the DNA submatrices D_1 and D_2. The inverse of zigzag pattern is applied to retransform the pixels of D_1 and D_2 in fifth level. The heterogeneous chaotic maps, namely Chen's hyperchaotic map and Lorenz chaotic maps, are mapped for the permutation of DNA matrices D_1 and D_2, respectively, in fourth level. The DNA SUB operation is applied to regain the DNA structure matrix D in the third level. In second level, DNA inverse complementary rules are applied to reform the binary image. Hash key is extricated

from the binary image. As depicted in Fig.4.4(c), the decrypted medical image is conquered in first level. At the receiver end once again hash key is calculated for Canis lupus DNA sequence (ID MW549038 in GenBank) using SHA-512. The extricated hash value is compared with the calculated hash. If both hash values are similar means integrity of the medical image is maintained.

The working procedure of Algorithm 4.1 is illustrated with one suitable example. Consider the original medical image matrix of size 4×4.

Step 1: The original medical image O is converted into a binary image.

O=				
	4	2	8	3
	1	6	10	9
	7	3	4	5
	12	11	33	20

B =				
	00000100	00000010	00001000	00000011
	00000001	00000110	00001010	00001001
	00000111	00000011	00000100	00000101
	00001100	00001011	00100001	00010100

Step 2: The hash digest is embedded into the LSB of a binary image.

Hash key = 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0

Embedded B =				
	00000101	00000010	00001001	00000011
	00000000	00000110	00001011	00001001
	00000110	00000011	00000101	00000101
	00001101	00001011	00100000	00010100

Step 3: The DNA structure matrix is constructed using all eight DNA encoding rules depending on dynamic bit-level selection.

D =				
	GGTT	GGGA	GGAT	GGGC
	GGGG	GGTA	GGAC	GGAT
	GGTA	GGGC	GGTT	GGTT
	GGCT	GGAC	AGAA	GTTG

Step 4: The DNA structure matrix is bifurcated into two equal DNA sub matrices.

D_1 =	GGTT	GGGA
	GGGG	GGTA
	GGTA	GGGC
	GGCT	GGAC

D_2 =	GGAT	GGGC
	GGAC	GGAT
	GGTT	GGTT
	AGAA	GTTG

Step 5: The Encoded DNA matrices D_1 and D_2 are permuted using heterogeneous chaotic sequences.

$D_{1\ \text{Row-wise}}$ =	GGAC	GGCT
	GGGC	GGTA
	GGTA	GGGG
	GGGA	GGTT

D_{1} Column-wise =	GGTT	GGTA
	GGGA	GGGC
	GGGG	GGCT
	GGTA	GGAC

$D_{2\ \text{Row-wise}}$ =	GTTG	AGAA
	GGTT	GGTT
	GGAT	GGAC
	GGGC	GGAT

D_2 Column-wise =	GGAT	GGTT
	GGGC	GGTT
	GGAC	AGAA
	GGAT	GTTG

Step 6: The DNA encoded chaotic sequences.

$D_c x$=	TTTG	CGGG
	GATG	CTAC
	TTCA	GCAG
	CTGC	ACTC

D_cy=	GATT	GGGA
	AACC	AATG
	AATT	ACCT
	TCCC	ACCA

$D_L p$=	GGAG	CTGT
	TCCC	CTGA
	TGAA	CGAC
	CATA	TTTT

$D_L q$=	GGCG	CCAT
	AGAT	GATG
	TTTT	CCCG
	GCGA	GGTA

Step 7: The zigzag transform of permuted DNA encoded sequences.

D_1 Column-wise =	GGTA	GGTT
	GGGC	GGCT
	GGGA	GGGG
	GGAC	GGTA

D_2 Column-wise =	GGTT	GGAT
	GGTT	AGAA
	GGGC	GGAC
	GTTG	GGAT

Step 8: The permuted Encoded DNA matrices pixels are diffused using DNA ADD.

Diffusion D_{1c} Row-wise =		
	AACT	GCAA
	CTAG	GAAT
	AAGC	CGTC
	GATC	TGCA

Diffusion D_{1c} Column-wise =		
	TCTC	CGTC
	AGAG	TCGA
	CCAT	AGTT
	AATC	GGCC

Diffusion D_{2L} Row-wise =		
	CCGA	GATC
	AGTT	AATC
	ACTA	GCCC
	GGCT	AAGC

Diffusion D_{2L} Column-wise =		
	GGGT	GAGT
	CCGC	TCCG
	GTCG	GCCG
	CGGG	TTAA

Step 9: Concatenation of diffused column-wise DNA encoded matrices.

Concatenation =				
	TCTC	CGTC	GGGT	GAGT
	AGAG	TCGA	CCGC	TCCG
	CCAT	AGTT	GTCG	GCCG
	AATC	GGCC	CGGG	TTAA

Step 10: The concatenated matrix is translated into binary image

B =				
	11011101	01101101	00000001	00100001
	00100010	01001110	00001100	11101001
	00000110	10110101	01111001	01101001
	00001101	01011010	11000000	00001111

Step 11: Generation of cipher image.

E =				
	221	109	1	33
	34	78	12	233
	6	181	121	105
	13	90	192	15

4.5.1 Performance and Security Analysis

The performance analysis of proposed medical image en/decryption method depends on invulnerable to various attacks such as statistical attacks, differential attacks, and exhaustive attacks. The correlation coefficient and histogram analysis for statistical attack. The key security and key space analysis for exhaustive attack. The entropy

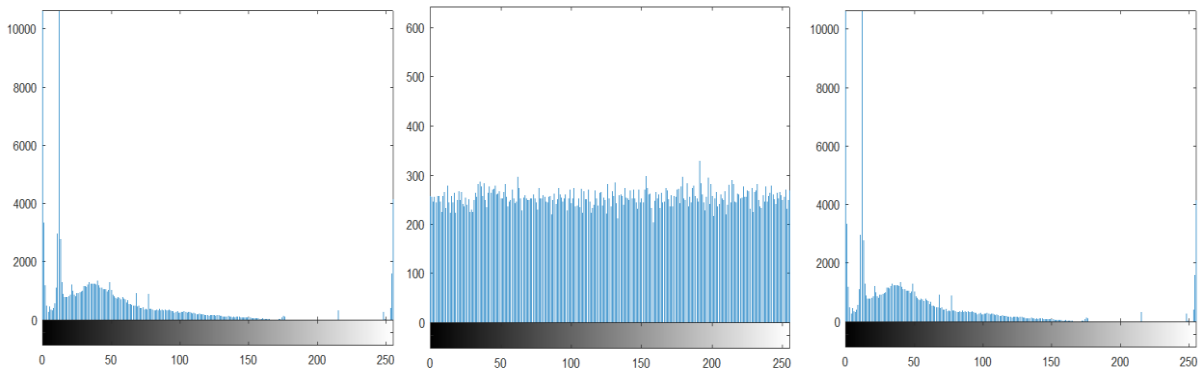
analysis to quantify the quality of medical image. The MSE and PSNR are employed to ascertain the superiority of medical image.

A. Statistical attack

A crypto analyst performs the statistical analysis to check is it possible to decrypt the original medical image from examining the scattered pixels in cipher image. The correlation coefficient analysis and histogram analysis are performed to prove the anti-attack proof against statistical attack.

Histogram Analysis

The histogram of ultrasound image is shown in Fig.4.5(a) and in Fig.4.5(b) histogram of cipher image, and in Fig.4.5(c) histogram of decipher image is shown. From Fig.4.5, we noticed that the pixels are dispersed more constantly in cipher image and uneven in decipher image and original medical image. Distribution of pixels proves that most image pixel values are modified in cipher image. Hence, proposed multilevel medical image encryption algorithm maintains the suitable confusing property.



(a) (b) (c)

Fig.4.5 Histogram analysis: (a) Original ultrasound image (b) Cipher image (c) Decipher image

The chi-square test results are exhibited in Table 4.5. From Table 4.5 it is proved statistically that, pixels are distributed uniformly.

Table 4.5 Chi-square hypothesis test for proposed DNA cryptosystem using SHA-512

Medical image type	Cipher image	Hypothesis test
MR	244.9609	Pass
CT	245.6016	Pass
X-ray	249.8125	Pass
Ultrasound	247.5547	Pass
ECG	245.6351	Pass

Correlation Coefficient Analysis

The correlation coefficient specifies the association with adjacent pixels of medical images. The lesser degree of correlation indicates that adjacent pixels are poorly correlated. The higher degree of correlation indicates that adjacent pixels are strongly correlated. The ideal value for a higher degree is '1' and for a lower degree '0' and '-1'

Table 4.6 Correlation coefficient of proposed DNA cryptosystem using SHA-512

Medical image type	Direction	Cipher image	Decipher image
MR	*Horizontal*	0.0012	0.999
	Vertical	-0.0016	0.996
	Diagonal	-0.0014	0.994
CT	*Horizontal*	0.0016	0.998
	Vertical	-0.0017	0.996
	Diagonal	0.0002	0.991
X-ray	*Horizontal*	0.0013	0.998
	Vertical	-0.0014	0.996
	Diagonal	-0.0012	0.998
Ultrasound	*Horizontal*	0.0012	0.998
	Vertical	-0.0013	0.992
	Diagonal	-0.0013	0.995
ECG	*Horizontal*	0.0012	0.992
	Vertical	-0.0023	0.996
	Diagonal	-0.0014	0.993
Average:		**-0.00046**	**0.9954**

indicates negatively correlated. From Table 4.6, it is observed that adjacent pixels are strongly correlated in decipher image. The average coefficient value is 0.99 almost equal to the ideal value of a higher degree. The adjacent pixels are poorly correlated in cipher image. Average coefficient value is -0.00046 almost equal to ideal value of a lower degree. From Table 4.6, we can conclude that pixels of cipher image are shuffled pseudo randomly. Therefore, prediction of original medical image is impractical for eavesdroppers during transmission through an open-source network.

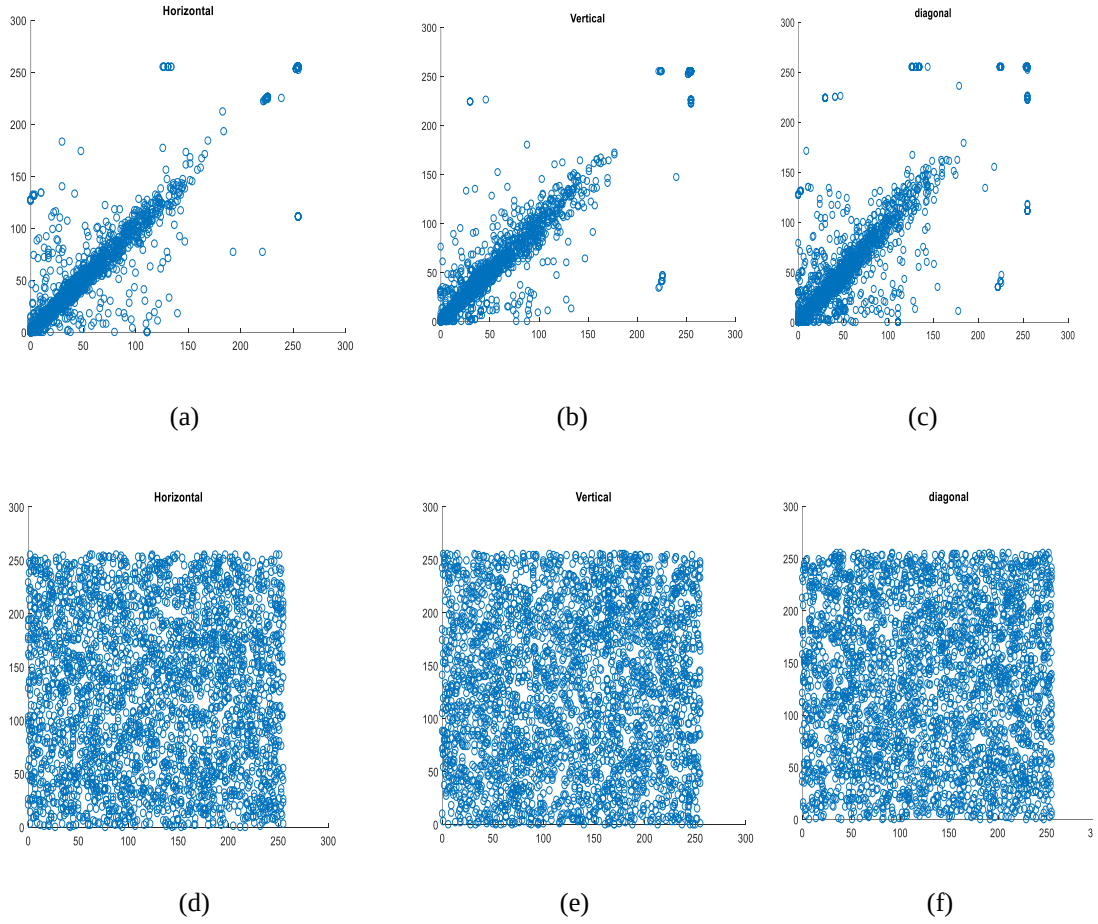


Fig. 4.6 Scatter plot of original ultrasound image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

The pictorial representation of correlation coefficient of contiguous pixels of original medical image and cipher image in horizontal, vertical, and diagonal directions are exhibited in Fig. 4.6. The pixels are highly correlated in original medical image as exhibited in Fig.4.6(a and b and c). The pixels are dispersed uniformly in cipher image as exhibited in Fig. 4.6(d and e and f). This proves that pixels are not correlated in

cipher image.

B. Exhaustive Attack

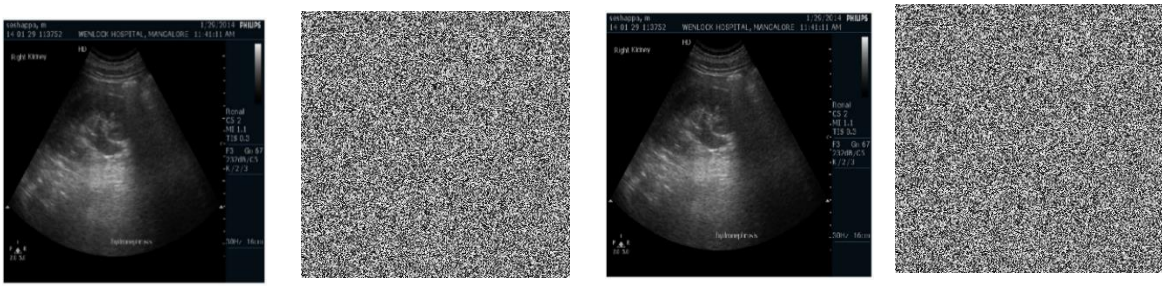
A crypto analyst performs an exhaustive attack to verify whether guessing the secret keys by brute force search is possible or not. The key space analysis and key sensitive analysis parameters are exploited to validate an exhaustive attack.

Key Space Analysis

In proposed cryptosystem, secret keys are the preliminary values of positional variables of Chen's hyperchaotic map and Lorenz chaotic system. A total of eight secret keys (x_0, y_0, z_0, w_0, k, p_0, q_0, and u_0) are available. Then, the size of eight secret keys is $(10^{15})^8 \approx 2^{400}$ and the hash key of size 512 (2^9) bits and the DNA sequence of size 512 (2^9). The total key space is 2^{418}. The increase in the number of secret keys is significant to withstand exhaustive attacks.

Key Sensitivity Analysis

The generation of Chen's chaotic map and Lorenz's chaotic map sequences are very sensitive to initial conditions. Decrypting the original medical image with small deviations in any one secret keys among a total of eight secret keys is highly impossible. The original medical image, cipher image and decipher image decrypted cipher image is decrypted using a secret key value as u_0=3.69999 instead of correct



(a) (b) (c) (d)

Fig.4.7 Key sensitivity analysis: (a) Original ultrasound image (b) Cipher image (c) Decipher image decrypted using correct secret key value u_0=3.7 (d) Decipher image decrypted using incorrect secret key value u_0 =3.69999

value, then obtained decipher image is diverse from original medical image as shown Fig.4.7(d).

C. Differential attack

A crypto analyst performs the differential attack to check the resistant against the chosen ciphertext attack and chosen plain text attack. Cryptanalyst used UACI and NPCR metrics to prove refrain from differential attacks. The metrics NPCR and UACI are utilised to verify the original medical image sensitivity. The average NPCR value is 99.662 and UACI value is 33.90 as exhibited in Table 4.7. The metrics values are almost equal to ideal values as specified in Section 1.9.2 of Chapter 1. This demonstrates the sensitivity of the original medical image. A slight variation in the original medical image yields a new distinct cipher image. Thus, the proposed en/decryption method using SHA-512 is resistant against chosen plain text attacks and known plain text attacks.

Table 4.7 Performance analysis of proposed DNA cryptosystem using SHA-512

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.658	33.92	7.9992	4.9034e+04	5.3354
CT	99.669	33.65	7.9994	5.5409e+04	6.0810
X-ray	99.659	34.15	7.9993	4.8953e+04	5.0031
Ultrasound	99.665	33.95	7.9997	5.2004e+04	5.2363
ECG	99.662	33.86	7.9992	5.3519e+04	5.8212
Average	**99.662**	**33.90**	**7.9993**	**5.18e+04**	**5.4954**

The quality assessment of the proposed cryptosystem is measured using metrics MSE, PSNR, and entropy as discussed in Section 1.10 of Chapter 1. The values of MSE, PSNR, and entropy for original medical image and cipher image are shown in Table

4.7. From table 4.7, it is revealed that MSE is very high and PSNR value is very low and entropy value is 7.99. The graphical representation of performance analysis is shown in Fig. 4.8.

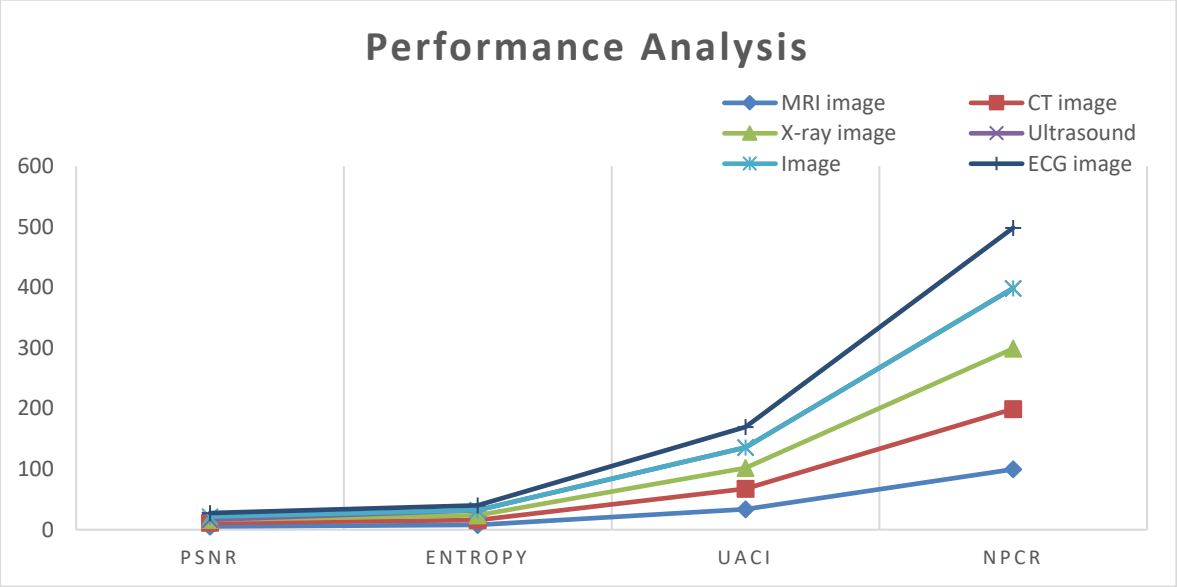


Fig. 4.8 Performance analysis of proposed DNA cryptosystem with integrity

The performance analysis exhibits that the proposed DNA cryptosystem is appropriate to convey multilevel security, confidentiality, and integrity for medical images.

4.5.2 Computation Time of Proposed En/Decryption Algorithm using SHA-512

The computation time of proposed en/decryption using SHA-512 for original medical image of size (m×n) is calculated as follows:

Step 1: Generating hash key: m

Step 2: Binary conversion of original medical image: (m×n)

Step 3: Embedding hash key LSB: m

Step 4: Construction of DNA structure: (m×n)

Step 5: Permutation process: (m×n)

Step 6: Diffusion process: (m×n)

Step 7: DNA decoding: (m×n)

Step 8: Generating cipher image: (m×n)

Total time complexity of proposed method is given below:

$T(n) = 2m + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n)$

$= 7(m\times n) + 2m$

If m=n then $T(n)=7(n^2) \in O(n^2)$. The space efficiency is $O(n^2)$.

4.5.3 Comparative Analysis

The proposed medical image en/decryption method using SHA-512 is compared with existing methods. The pictorial representation of comparative analysis is exhibited in Fig.4.9.

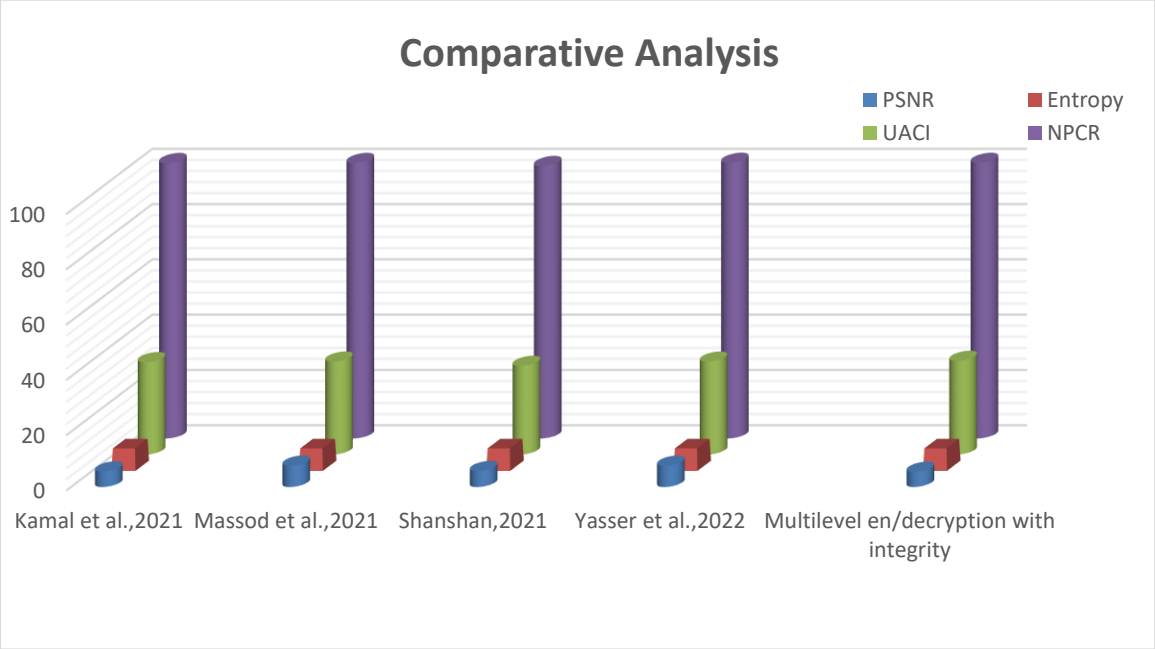


Fig. 4.9 Comparative analysis of proposed DNA cryptosystem with integrity

The comparative analysis is depicted in Table 4.8. From Table 4.8, it is observed that performance metrics of the proposed method are equivalent or bigger than the existing methods. The key space of proposed cryptosystem is very large and is substantial in providing security. The comparative analysis validates that the proposed en/decryption method for medical image using SHA-512 is suitable to provide high-level security, confidentiality, and integrity.

Table 4.8 Comparative analysis of proposed DNA cryptosystem using SHA-512

Method	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	Key Space
Kamal et al.,2021	7.9993	99.60	33.44	5.63	10^{45}
Massod et al.,2021	7.9995	99.62	33.63	7.74	10^{90}
Shanshan,2021	7.9993	98.536	32.10	5.79	10^{120}
Yasser et al.,2022	7.9991	99.69	33.63	7.72	10^{75}
Intensity based en/decryption (Chapter 3)	7.9973	99.65	33.56	5.93	10^{120}
Proposed en/decryption method	**7.9993**	**99.662**	**33.90**	**5.49**	**10^{126}**

4.6 Summary

This chapter describes medical image en/decryption using hash function SHA-512. Main aim of this cryptosystem is to provide security, confidentiality, and integrity. In this method, the original medical image is transferred into a binary image. The 512-bit hash value is calculated for Canis lupus DNA sequence. This hash key is embedded in the LSB of a binary image. Embedded binary image is renovated into a DNA sequence matrix using DNA encoding rules. All eight DNA encoding rules are applied dynamically based on binary bit values of medical image. DNA sequence matrix is bifurcated into two equal sub matrices. dual hyper chaos method namely, Chen's chaos map and Lorenz's chaotic system are used to generate the chaotic sequences. Chen's chaotic sequence shuffles the pixels of first DNA sequence matrix and Lorenz's chaotic sequence shuffles the pixels of second DNA sequence matrix. The permuted DNA

sequence matrices are transformed using zigzag pattern. DNA ADD is operated for the diffusion of transformed matrices. The diffused DNA sequence matrices are combined. Finally, all eight DNA complementary rules are applied dynamically to attain a cipher image. This proposed en/decryption method ensures high-level security, confidentiality, and integrity. The computation time of this method is high. The methods discussed in succeeding chapters are concentrating on reducing computation time.

Chapter 5

DNA Cryptosystem using Dual Hyperchaos Map for Selective Process

5.1 Introduction

The medical images carry very sensitive disease specific information. High-level security is essential while communicating online. For the enchantment in security of medical images, the multistate encryption techniques are adequate. The medical images contain a heavy information volume and pixels are highly correlated. Hence, the computation time of multistate encryption techniques for medical images are very high. In current era, providing enhanced security with reduced computation time is a big challenge. Hence in this chapter, we are concentrating on reducing the computation time of multistate encryption techniques.

In (Li T, Shi J, Li X, Wu J & Pan F,2019), the 5D hyperchaotic map is applied for permutation of a plain image. Dynamic filtering and DNA encoding are performed to diffuse the pixels. The diffused image is converted into various 3D DNA-level. Latin cubes are applied to 3D DNA-level cubes and integrated to get a cipher image. The 4D hyperchaotic map generates the chaotic sequences and these sequences are referred to perform multiple bit permutation and diffusion. The diffused image is transformed into a cipher image (Taiyong Li & Duzhong Zhang, 2021). In (Lone, Singh & Mir,2021), the modified 3D Arnold cat map chaotic sequence are mapped for the permutation of plain image. The permuted image is renovated into a DNA matrix using DNA coding rules. DNA XOR is operated for the diffusion of DNA matrix. DNA decoding rules are applied to attain a cipher image.

---

[1] Prema T Akkasaligar, Sumangala Biradar, "***Selective Medical Image Encryption Using DNA Cryptography***" Information Security Journal: A Global Perspective Volume 29(2), 2020, pp. 91-101.

Multilevel medical image encryption systems are suitable to offer enriched security for medical images. The computation time is very high. Main aim of the proposed en/decryption method is to deliver efficient security with less time. To reduce the execution time, the selective medical image en/decryption method using a dual hyper chaos map is proposed in this chapter.

5.2 Dual Hyper Chaos Map

In dual hyperchaos map, Taylor Chirikov's map and Chen's hyperchaotic map are merged. Taylor Chirikov map and Chen's hyperchaotic map are high-dimensional discrete maps. The dual hyperchaos map is depicted in Eqs. (5.2.1-5.2.6).

$$x_{i+1} = \frac{(x_i + K sin(y_i))}{2} \quad (5.2.1)$$

$$y_{i+1} = (y_i + x_{i+1} (\text{mod } 2\pi)) - 0.4 \quad (5.2.2)$$

$$x_{i+1} = a_1 (y_{i+1} - x_{i+1}) \quad (5.2.3)$$

$$y_{i+1} = -x_{i+1} z_i + d_1 x_{i+1} + c_2 y_{n+1} - w_i \quad (5.2.4)$$

$$z_{i+1} = x_{i+1} y_{i+1} - b z_i \quad (5.2.5)$$

$$w_{i+1} = x_{i+1} + k \quad (5.2.6)$$

where x_0, y_0, z_0, and w_0 are positional variables and a_1, b_1, c_1 and d_1 are control parameters. The value of k is in a range from -0.7 to 0.7. Outcomes of Taylor Chirikov map are the primary values for state parameters of Chen's hyper chaotic map. Gradation of dual hyper chaos produces extremely complicated confusion properties and is extremely sensitive to the primary condition of state parameters. Thus, it is appropriate to offer security for original medical images. To provide multistate security for medical images, the dual hyper chaos map with DNA cryptography is anticipated. For reduction of the computation time, a selective medical image encryption method is proposed.

5.3 Proposed DNA Cryptosystem for Selective Process

In proposed selective DNA cryptosystem, selective medical image encryption is performed using a dual hyper chaos map and DNA cryptography. The original medical image is bifurcated into two sub images depending on a selection of pixels. The pixel selection depends on the pixel value. The selected pixels are considered as selective pixel region and the remaining pixels of the medical image are considered as non-selective pixel region. The permutation is performed on a selective pixel region using a dual hyper chaos sequence. The diffusion is performed on non-selective pixel region using DNA XOR operation. Both regions are merged to attain a final cipher image as exhibited in Fig.5.1.

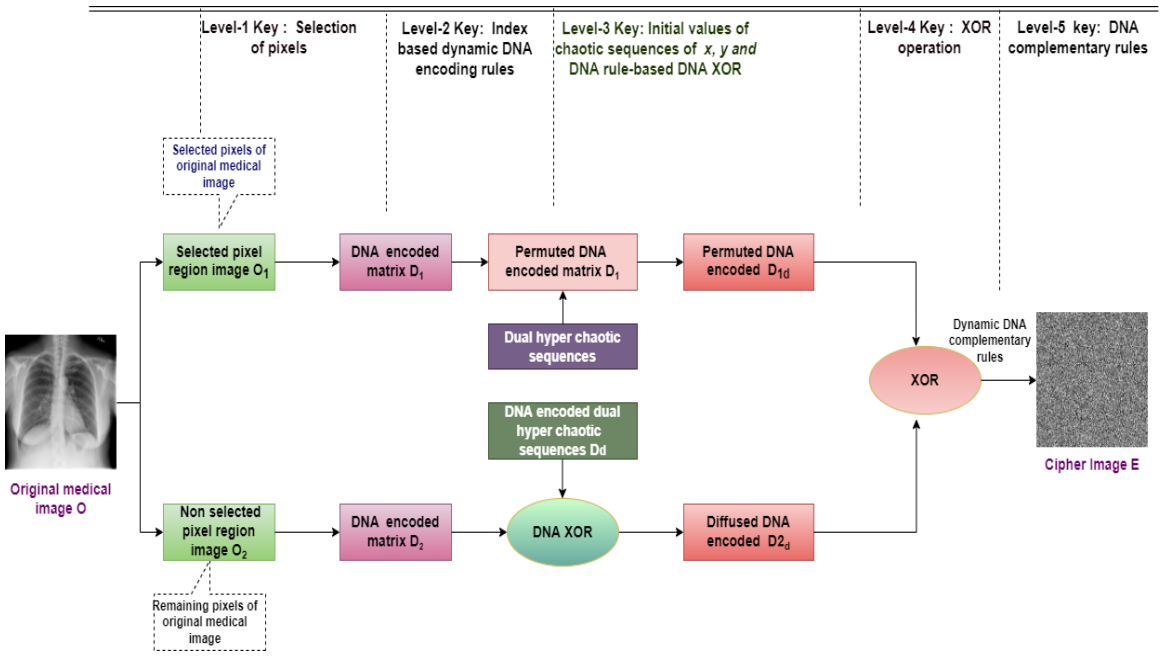


Fig.5.1 Block diagram of proposed selective medical image encryption method

5.3.1 Encryption Method

In proposed selective medical image encryption method, dual hyperchaos and DNA operations are used to deliver security with reduced in computation time. First, the original medical image is bifurcated into two regions using the Pixel_selection method as illustrated in Algorithm 5.1.

Algorithm 5.1: Pixel_selection

// **Input:** The original medical image O (r, c)

// **Output:** Selected pixels are stored in matrix O_1 and remaining in matrix O_2 and matrix //Idx

```
for i=0 to r do
    for j=0 to c do
    Sel= O (i, j) / 3;
    Sel1= floor (Sel);
    Sel2=Sel-Sel1;
    if (Sel2≤0) then
        O1(i,j) = O(i,j);
        Idx(i.j)=j;
    else
        O2(i,j) =O(i,j);

    end
end
end
```

The original medical image is bifurcated into two sections O1 and O2 using the Pixel_selection method. In the Pixel_selection method, the selection of pixels depends on the pixel value. The selected pixels of original medical image are considered as a selective pixel region O1 and the remaining pixels of the medical image are considered as a non-selective pixel region O2. The index of O1 are stored in matrix Idx. These two regions are converted into 8-bit binary images B1 and B2. All eight DNA encoding rules are utilized to construct the 4-bit DNA encoded sequences D1 and D2 respectively. The DNA encoding rules are chosen dynamically.

I. Dynamic Selection of DNA Encoding Rules

The DNA encoding rules are selected dynamically depending on the index value of original medical image pixels. Instead of using specific rule, all eight DNA encoding rules are exploited to enhance the security of medical images. Dynamic selection of DNA encoding rules is depicted in Eq.(5.3.1).

$$Rule\_n = (Index\ (O\ (i, j)) \bmod 8) + 1 \qquad (5.3.1)$$

where Index O (i, j)) is an index of medical image pixel. For each pixel, a different rule is employed to construct a unique DNA encoded sequence. A dual hyper chaos map sequences are referred for permutation and diffusion of DNA encoded sequences.

II.Dual Hyper Chaos Map Processes

The dual hyper chaotic map contains two processes namely, permutation and diffusion. In permutation process, the pixels of DNA encoded sequence are rearranged. To rearrange the pixels of DNA encoded sequence, chaotic sequences of dual hyper chaos map are arranged in sorted order. A position of the sorted sequences is considered to shuffle the pixels of DNA encoded sequence D_1.

In diffusion process, the pixel values of DNA encoded sequences are modified. The chaotic sequences of dual hyper chaos map are converted into DNA encoded sequence D_d. The DNA XOR is applied for D_2 and $D_{d,}$ to change the pixel value of DNA encoded sequence D_2. The permuted D_{1d} and diffused D_{2d} are merged using XOR operation to get an intermediate cipher matrix. The intermediate cipher matrix is renovated into a final cipher image using DNA complementary rules.

III. Dynamic Selection of DNA Complementary Rules

The DNA complementary rules are converse of DNA encoding rules. These rules are selected dynamically based on 2-bit LSB of a pixel value of the intermediate cipher matrix. The selection of dynamic DNA complementary rules is specified in Table 4.2 of Section 4.3.1 of Chapter 4.

The intermediate cipher image is reformed into an 8-bit binary image. The binary image is renovated into a final cipher image. The expansive steps of proposed selective encryption technique are exhibited in Algorithm 5.2.

Algorithm 5.2: Selective_Digitized_Medical_Image_Encryption (SDMIE)

//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1: Start

Step 2: Split the original medical image O (r, c) into two regions.

$O_1(r, c)$ = Selected pixels of O (r, c)

using Pixel_selection Algorithm 5.1;

$O_2(r, c)$ = Remaining pixels of O (r, c);

Step 3: Conversion of regions into binary images B_1 and B_2

$B_1(r, c\times8)$ = dec2bin ($O_1(r, c)$);

$B_2(r, c\times8)$ = dec2bin ($O_2(r, c)$);

Step 4: Transformed binary images into encoded DNA matrices D_1 and D_2 using DNA base encoding rules using Eq. (5.3.1).

$D_1(r, 4\times c)$ = DNA sequence matrix of $B_1(r, c\times8)$

$D_2(r, 4\times c)$ = DNA sequence matrix of $B_2(r, c\times8)$

Step 5: The chaotic sequences *x* and *y* of dual hyper chaos map are sorted in ascending order.

Step 6: A position of sorted chaotic sequences $\bar{x}$ and $\bar{y}$ are referred to permute the pixels of $D_1(r, 4\times c)$ to get jumbled DNA encoded matrix D_{1d} (r, 4×c).

Step 7: Chaotic sequences *x* and *y* are renovated into DNA encoded matrix D_d (r, 4×c) using dynamic DNA coding rules using Eq. (5.3.1).

Step 8: The pixels of D_2 (r, 4×c) are diffused using DNA XOR operation

D_{2d} (r, 4×c) = $D_2(r, 4\times c)$ DNA XOR D_d (r, 4×c)

Step 9: Transform $D_{1d}(r, 4\times c)$ and D_{2d} (r, 4×c) into a binary image using DNA complementary rules as specified in Table 4.2 of Section 4.3.1 of Chapter 4.

$B_{1d}(r, c\times8)$ = reshape (D_{1d} (r, 4×c))

$B_{2d}(r, c\times8)$ = reshape (D_{2d} (r, 4×c))

Step 10: Combine the permuted and diffused matrices using logical XOR operation.

$B_{12}(r, 4\times c)$ = B_{1d} (r, 4×c) XOR B_{2d} (r, 4×c)

Step 11: The binary image is reformed to attain a cipher image

E (r, c) = bin2dec($B_{12}(r, c\times8)$)

Step 12: Stop

In proposed SDMIE algorithm, as an alternative for permuting all pixels, only selected pixels of the original medical image are permuted. Similarly, instead of diffusing all pixels, only the remaining pixels of an original medical image are diffused to decrease the computation time of SDMIE algorithm. The decryption technique is the converse of SDMIE algorithm.

5.3.2 Decryption Method

In proposed decryption method, dual hyper chaos sequences are referred to permute the index matrix Idx. Depending on permuted index matrix the cipher image E pixels are selected and stored in matrix E_{1d}. The expansive steps of division are depicted in Algorithm 5.3.

Algorithm 5.3: Pixel_selection for decryption
// Input: Cipher image E (r, c)
// Output: Selected pixels are stored in matrix E_{1d}
//The matrices E_{1d} is initialized with zeros and Idx pixels are permuted by dual hyper //chaos

```
for i=0 to r do
    for j=0 to c do
    if(Idx!=0)
        E1d(i,j)= E(r,c);
      end
end
end
```

The cipher image is decrypted into an original medical image using the decryption method. To better understand the method, the expansive steps of proposed decryption are illustrated in Algorithm 5.4.

Algorithm 5.4: Selective_Digitized_Medical_Image_Decryption (SDMID)
//Input: Cipher image E (r, c)
//Output: Original medical Image O (r, c)

Step 1: Start

Step 2: The selected pixel matrix E_{1d} obtained using Pixel_selection Algorithm 5.3 is converted into a binary image. The cipher image is also converted into binary image.

$$B_{1d}(r, c\times8) = \text{bin2dec}\,(E_{1d}(r, c));$$

$$B_{12}(r, c\times8) = \text{bin2dec}\,(E(r, c));$$

Step 3: Split the binary image into two sub images using a logical XOR operation.

$$B_{2d}(r, c\times8) = B_{12}(r, c\times8)\ \text{XOR}\ B_{1d}(r, c\times8)$$

Step 4: Transform $B_{1d}(r, 8\times c)$ and $B_{2d}(r, 8\times c)$ into DNA sequence matrix using the inverse of DNA inverse complementary rules as stated in Table 4.2 of Section 4.3.1 of Chapter 4.

$$D_{1d}(r, 4\times c) = \text{reshape}\,(B_{1d}(r, c\times8))$$

$$D_{2d}(r, 4\times c) = \text{reshape}\,(B_{2d}(r, c\times8))$$

Step 5: The chaotic sequences *x* and *y* of dual hyper chaos map are sorted in descending order.

Step 6: A position of sorted chaotic sequences $\bar{x}$ and $\bar{y}$ are used to rejumble the pixels of $D_{1d}(r, 4\times c)$ to get DNA encoded matrix $D_1(r, 4\times c)$.

Step 7: The chaotic sequences *x* and *y* are renovated into DNA encoded matrix $D_d(r, 4\times c)$ using dynamic DNA coding rules using Eq. (5.3.1).

Step 8: The pixels of $D_2(r, 4\times c)$ are diffused using DNA XOR operation.

$$D_2(r, 4\times c) = D_{2d}(r, 4\times c)\ \text{DNA XOR}\ D_d(r, 4\times c)$$

Step 9: Transform $D_1(r, 4\times c)$ and $D_2(r, 4\times c)$ into an eight-bit binary image using the dynamic inverse of DNA coding rules using Eq. (5.3.1).

$$B_1(r, c\times8) = \text{reshape}\,(D_1(r, 4\times c))$$

$$B_2(r, c\times8) = \text{reshape}\,(D_2(r, 4\times c))$$

Step 10: Merge permuted and diffused binary matrices.

$$B_{12}(r, 4\times c) = B_1(r, 4\times c)\ ||\ B_2(r, 4\times c)$$

Step 11: The binary image is reformed to attain a decipher image

$$O(r, c) = \text{bin2dec}\,(B_{12}(r, c\times8))$$

Step 12: Stop

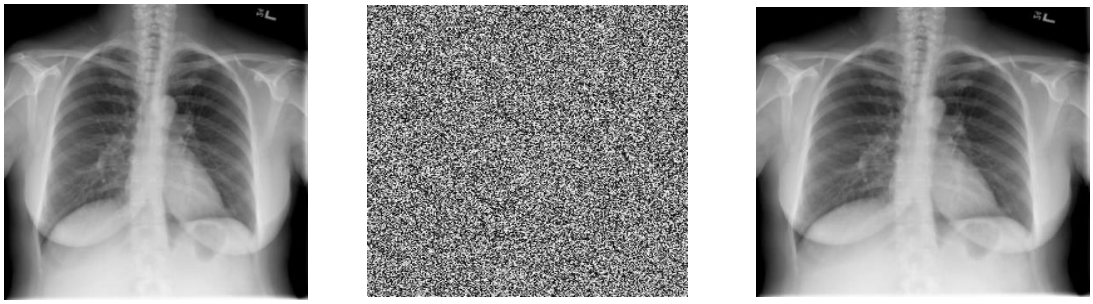
In proposed SDMIE/D methodology, all DNA encoding rules depending on index and all DNA complementary rules depending on bit-level values of medical image are used for the

enhancement of security. The time complexity of DNA computation is major issue. To overcome from this issue, only selected pixels of a medical image are permute using a dual hyper chaos sequence. Also, only remaining pixels of a medical image are diffused instead of all pixels. The dual hyper chaos map has good confusion and diffusion property. So, the selective DNA system is suitable to provide security with reduced execution time of encryption algorithm.

5.4 Experimental Results and Discussion

The proposed SDMIE/D methodology is executed using system 9th generation Intel CoreTM i7 7500U CPU @ 2.70GHz, 2901 MHz, 2 Core(s), 4 Logical Processor(s) and MATLAB 2016b. Total 500 medical image samples of size 512×512, from five different categories namely CT, MRI, Ultrasound, X-ray, and ECG images are used for the experiment. From each category, 100 medical images are collected. The original X-ray image sample is exhibited in Fig.5.2 (a).

In proposed SDMIE algorithm, Pixel_selection Algorithm 5.1 is used for the bifurcation of original medical image O. The selected pixels matrix is denoted as O_1 and the remaining pixels matrix is denoted as O_2. These matrices are renovated into binary matrix. DNA encoding rules specified in Table 1.1 of Section 1.6 of Chapter 1 are mapped to binary matrix to attain a DNA sequence matrices D_1 and D_2. The primary values of system parameters x_0=1, y_o=0.5, K=0.8, z_0=1.2, w_0=1 and control factors a_1=36, b_1=3, c_1=28, d_1=16, and k=0.2 are empirically determined to produce a chaotic sequences. These sequences are arranged in ascending order. A position of ordered sequences is referred for the permutation of D_1. The diffusion procedure DNA XOR depicted in Table 1.4 of Section 1.6 of Chapter 1, is operated for the diffusion of D2. All DNA complementary rules exhibited in Table 5.1 are mapped with diffused matrix to attain a cipher image as exhibited in Fig.5.2(b).



(a) (b) (c)

Fig. 5.2 X-ray image samples: (a) Original X-ray image (b) Cipher image (c) Decipher image

In proposed SDMID algorithm, the cipher image is reformed as an eight-bit binary image and selected pixel image using Pixel_selection for decryption Algorithm 5.3. The first sub image contains the selected pixels of the original medical image and the remaining pixels are stored in the second sub image. The sub images are transformed into encoded DNA matrices D_1 and D_2. The dual hyperchaotic sequences are referred to reshuffle the pixels of D_1. DNA XOR is applied for the diffusion of D_2. The DNA encoding rules are mapped to get a decipher image as exhibited in Fig.5.2(c).

The working procedure of Algorithm 5.2 is illustrated with one suitable example. Consider the original medical image matrix of size 4×4.

Step 1: The original medical image O is divided into two sub images O_1 and O_2 using Algorithm 5.1.

O =	4	2	8	3
	1	6	10	9
	7	3	4	5
	12	11	33	20

O_1=	0	0	0	3
	0	6	0	9
	0	3	0	0
	12	0	33	0

O_2 =	4	2	8	0
	1	0	10	0
	7	0	4	5
	0	11	0	20

Step 2: Conversion of two sub images O_1 and O_2 into binary images B_1 and B_2

B_1 =	0	0	0	00000011
	0	00000110	0	00001001
	0	00000011	0	0
	00001100	0	00100001	0

B_2 =	00000100	00000010	00001000	0
	00000001	0	00001010	0
	00000111	0	00000100	00000101
	0	00001011	0	00010100

Step 3: Construction of DNA structures D_1 and D_2.

D_1 =	0	0	0	GGGC
	0	AAGC	0	GGTA
	0	AAAT	0	0
	AATA	0	CTCA	0

D_2 =	AACA	AAAC	CCTC	0
	AAAC	0	CCTT	0
	AACT	0	CCAC	GGAA
	0	AACT	0	GAAG

Step 4: The permutation process is performed for DNA structure D_1

D_{1d} Row-wise =	0	CTCA	0	AATA
	0	0	AAAT	0
	GGTA	0	AAGC	0
	GGGC	0	0	0

D_{1d} Column-wise =	0	0	0	AATA
	0	AAGC	AAAT	0
	0	0	0	CTCA
	GGGC	GGTA	0	0

Step 5: The diffusion process is performed for DNA structure D_2 using DNA XOR operation.

D_{2d} Row-wise =	GGTT	TAAC	AGTA	0
	TTGC	0	TGGC	0
	GTAA	0	TGTT	TATC
	0	TTAG	0	AAAA

D_{2d} Column-wise =	AGCC	ATTA	CGGC	0
	AAAA	0	AATA	0
	GTTT	0	GCAA	CCTT
	0	TCGG	0	TAGA

Step 6: The permuted DNA structures D_{1d} and diffused DNA structure D_{2d} are converted into binary images.

B_1 =	0	0	0	01011001
	0	00000110	01010110	0
	0	0	0	11101101
	10101001	01011100	0	0

B_2 =	00100101	00111100	00111100	0
	00000000	0	01011001	0
	10111111	0	11000101	11111010
	0	11100101	0	10010001

Step 7: Binary images are combined using a logical XOR operation to get a cipher image.

B_{12} =	00100101	00111100	00111100	01011001
	00000000	00000110	00001111	00000000
	10111111	00000000	11000101	00010111
	10101001	10111001	00000000	10010001

E =	37	60	60	89
	0	6	15	0
	191	0	197	23
	169	185	0	145

5.4.1 Performance and Security Analysis

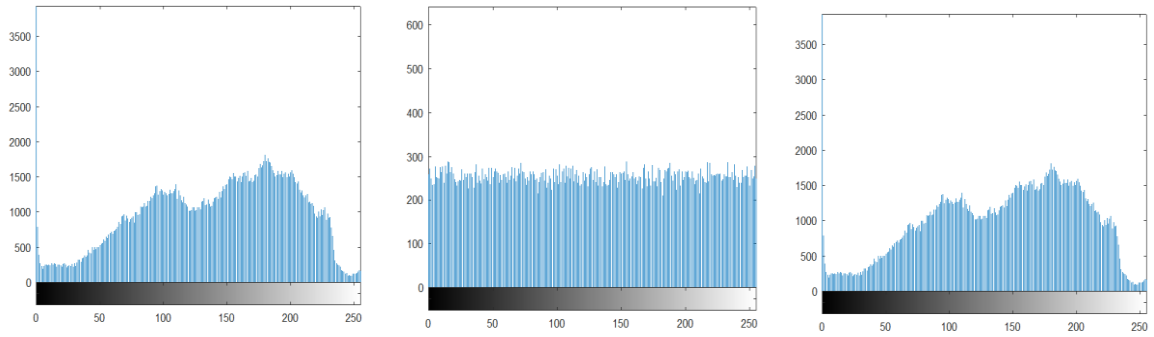
The performance of proposed SDMIE/D depends on defying capacity against different kinds of attacks such as statistical attacks, differential attacks, and exhaustive attacks. The quality is measured using metrics like entropy, MSE, and PSNR.

A. Statistical attack

In statistical attacks, cyber punks study the dissemination of pixels in the cipher image. Based on frequency distribution, they try to predict the original medical image and secret keys. The correlation coefficient and histogram analysis are performed to substantiate the statistical attack.

Histogram analysis

The histogram is the pictorial representation of dissemination of pixels. The pixels are disseminated randomly in original medical image and decipher imageas exhibited in Fig. 5.3((a) and (c)). The pixels are disseminated consistently in cipher image as exhibited in Fig. 5.3(b). From Fig. 5.3, it is observed that pictorial representation for the distribution of pixels in cipher image are different from original medical image and decipher medical image. Thus, it proves that proposed SDMIE/D has good confusion properties.



(a) (b) (c)

Fig.5.3 Histogram analysis: (a) Original X-ray image (b) Cipher image (c) Decipher image

The chi-square hypothesis test results are illustrated in Table 5.1. In Table 5.1, the hypothesis test pass means, uniformity of distribution of pixels in cipher image are proven mathematically.

Table 5.1 Chi-square test for proposed SDMIE method

Medical image type	Cipher image	Hypothesis test
MR	270.9844	pass
CT	274.5703	pass
X-ray	280.1641	pass
Ultrasound	279.6094	pass
ECG	278.8672	pass

Correlation Coefficient Analysis

The linear relationship among pixels of cipher images are analysed. The pixels of original medical images are highly correlated. If the pixels are not correlated, then the encryption method has good pseudo randomness property.

Table 5.2 Correlation Coefficient for proposed SDMIE/D method

Medical image type	Direction	Cipher image	Decipher image
CT	*Horizontal*	0.0196	0.996
	Vertical	0.0178	0.999
	Diagonal	0.0169	0.997
MR	*Horizontal*	0.0159	0.995
	Vertical	0.0162	0.992
	Diagonal	0.0168	0.996
Ultrasound	*Horizontal*	0.0153	0.994
	Vertical	0.0153	0.992
	Diagonal	0.0146	0.992
X-ray	*Horizontal*	0.0194	0.995
	Vertical	0.0195	0.995
	Diagonal	0.0195	0.996
ECG	*Horizontal*	0.0121	0.993
	Vertical	0.0135	0.996
	Diagonal	0.0181	0.991
Average :		**0.00154**	**0.9946**

The correlation coefficient average values from each category are tabulated in Table 5.2. The correlation coefficient average value for the cipher image is 0.00154 and decipher image is 0.9946 by considering all 500 images in the data set. From Table 5.2, it is

demonstrated that in cipher images the pixels are not correlated and in decipher image the pixels are highly correlated. This proves that proposed SDMIE/D technique has good confusion and diffusion property. So, it provides security for medical images while transmitting through insecure channels.

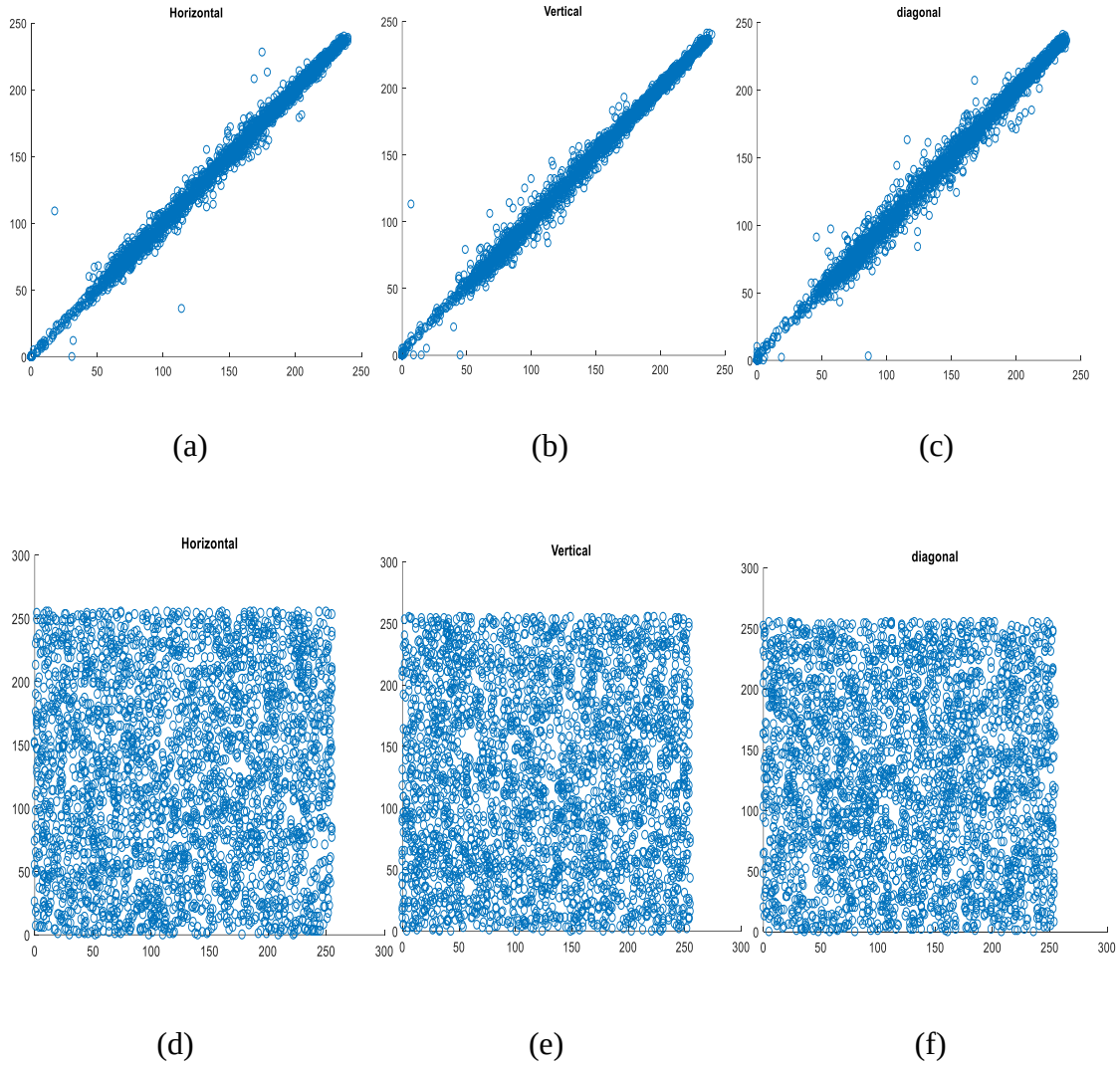


Fig. 5.4 Scatter plot of original X-ray image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions(d) -(f)

The correlation coefficient of neighboring pixels of original medical image and cipher image are exhibited in Fig. 5.4. From Fig. 5.4. (a and b and c) it is proved that the pixels

are linearly related in an original medical image. From Fig. 5.4. (d and e and f) it is proved that, no linear relationship among pixels in cipher image.

B. Exhaustive Attack

The key space analysis and key sensitivity analysis are performed to validate the exhaustive attack.

Key Space Analysis

In proposed SDMIE/D algorithm, secret keys are the primary values of control factors and system parameters of dual hyper chaos map. The five secret keys (K, x_0, y_0, w_0, l) are available. The key space of proposed SDMIE/D algorithm is $(10^{15})^5 = 10^{75} \approx .2^{250}$. The length of key space is huge enough to substantiate the exhaustive attack.

Key Sensitivity Analysis

The dual hyper chaos map is very sensitive to primary values of control factors and system parameters. Decrypting the original medical image as exhibited in Fig.5.5(a), with small variation in initial values is highly impossible. To analysis the key sensitivity, the cipher image as exhibited in Fig.5.5(b) is deciphered with the correct key x_0=1. The decipher image as shown in Fig.5.5(c) is the same as the original X-ray image. The cipher image

(a) (b) (c) (d)

Fig. 5.5 Key sensitivity analysis: (a) Original X-ray image (b) Cipher image (c) Decipher image decrypted with correct key x_0=1 (d) Decipher image decrypted with wrong key x_0=0.99999

was deciphered with the incorrect key x_0=0.99999. The deciphered image as exhibited in Fig.5.5(d) is not the original medical image. The remaining parameters of secret keys are also extremely sensitive.

C. Differential attack

In differential attack, invaders verify the sensitivity of original medical image. The UACI and NPCR metrics are utilized to substantiate the resistance of differential attacks. The average value of NPCR is 99.468% and UACI is 33.55% as tabulated in Table 5.3. Ooutcomes of NPCR and UACI prove that proposed selective cryptosystem is very sensitive to original medical image.

Table 5.3 Performance analysis of proposed SDMIE/D method

Medical image type	NPCR (%)	UACI (%)	MSE	PSNR (dB)	Entropy
CT	99.47	33.70	730.10	5.8	7.50
MR	99.47	33.55	767.07	5.9	7.51
Ultrasound	99.46	33.57	710.07	5.9	7.48
X-ray	99.48	33.29	780.12	5.7	7.53
ECG	99.46	33.63	708.30	5.3	7.69
Average:	**99.468**	**33.548**	**739.13**	**5.7**	**7.54**

The PSNR, MSE, and entropy metrics quantify the quality of the encryption methods. The value of MSE is near 739.132 and PSNR value is near 5.72dB. The entropy value for ciphered image is 7.54 closely equal to ideal entropy value. The outcomes represented in

Table 5.4, reveal that the quality of the proposed SDMIE/D is invulnerable to statistical, differential, and exhaustive attacks.

5.4.2 Computation Time of Proposed En/Decryption Algorithm

The time efficiency of proposed SDMIE for original medical image of size (m×n) is calculated as follows:

Step 1: Division of the original medical image into two regions: (m×n)

Step 2: Binary conversion of two regions: (m×n)

Step 3: Construction DNA structure: (m×n)

Step 4: Permutation process: (m×n)/2

Step 6: Diffusion process: (m×n)/2

Step 7: DNA decoding: (m×n)

Step 8: Generating cipher image: (m×n)

Total time complexity of the proposed method is given below:

$$T(n)= (m\times n) + (m\times n) + (m\times n) + (m\times n)/2 + (m\times n)/2 + (m\times n) + (m\times n) =6(m\times n)$$

If m=n then $T(n)=6(n^2) \in O(n^2)$.

The size of medical image n^2 and index value of selected and non-selected regions are n^2. Thus, space efficiency of SDMIE is $O(2n^2)$.

In proposed SDMIE/D method, to reduce the computation time the original medical image is bifurcated into two selected and non-selected pixel regions. The selected regions are permuted. The non-selected regions are diffused to reduce the computation time. The computation time is exhibited in Table 5.4, demonstrated that time complexity of proposed SDMIE/D is very less compared to en\decryption method specified in Chapter 4.

Table 5.4 Computation time of proposed SDMIE/D method

Medical image type	**SDMIE**		Multilevel DNA Cryptosystem with integrity (Chapter 4)	
	Encryption Time (seconds)	Decryption Time (seconds)	Encryption Time (seconds)	Decryption Time (seconds)
CT	2.24	2.27	36.7	36.00
MR	3.43	3.44	35.9	35.00
Ultrasound	2.25	2.29	33.4	32.39
X-ray	2.59	2.62	30.9	29.21
ECG	2.98	3.11	38.0	38.04
Average :	**2.698**	**2.746**	**34.98**	**34.128**

5.4.3 Comparative Analysis

The proposed SDMIE/D method is compared with the methods specified in section 5.1. The pictorial illustration of comparative analysis of proposed SDMIE/D is shown in Fig. 5.6. From Fig.5.6. it is proved that; the proposed SDMIE/D is appropriate to offer security for medical images.

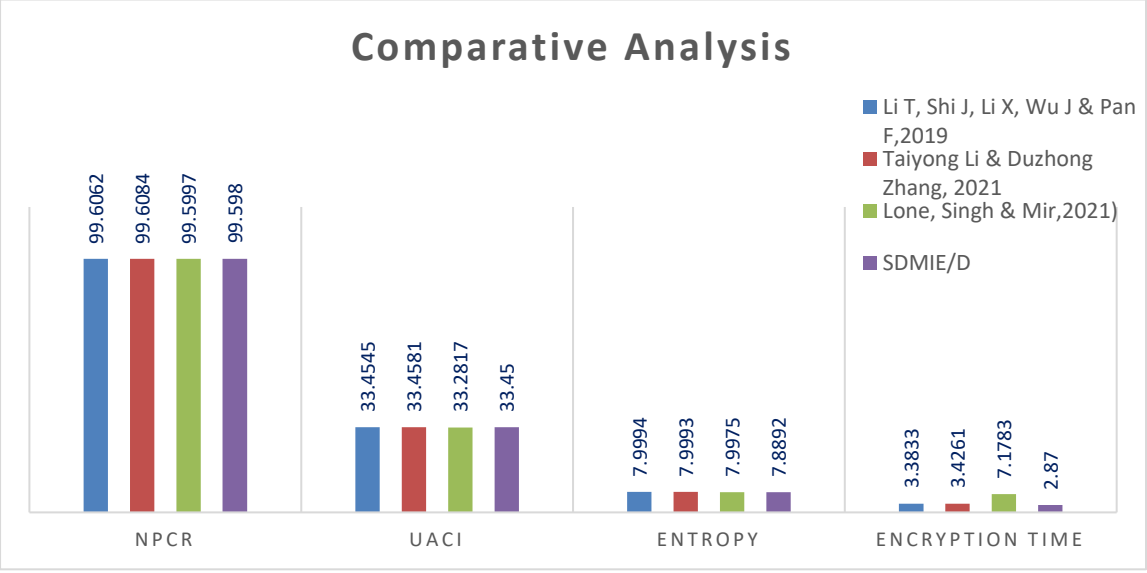


Fig. 5.6 Comparative analysis of proposed SDMIE/D

The comparative analysis is tabulated in Table 5.5, showing that proposed SDMIE/D performance indicators values are almost near to the other methods discussed in section 5.1, and time complexity is lesser than these methods. This demonstrates that proposed SDMIE/D is adequate for securely transferring medical images with less computation time.

Table 5.5 Comparative analysis of proposed SDMIE/D method

Methods	Entropy	NPCR (%)	UACI (%)	Encryption Time (seconds)	Key Space
Li T, Shi J, Li X, Wu J & Pan F,2019	7.9994	99.6062	33.4545	3.3833	2^{249}
Taiyong Li & Duzhong Zhang, 202)	7.9993	99.6084	33.4581	3.4261	2^{199}
Lone, Singh & Mir,2021	7.9975	99.5997	33.2817	7.1783	2^{390}
Multilevel DNA cryptosystem with integrity (Chapter 4)	7.99936	99.6626	33.906	36.01	2^{409}
Proposed SDMIE/D	**7.8892**	**99.598**	**33.4500**	**2.8700**	**2^{250}**

The security is deficient due to selective method. The length of key space plays a vital role in providing security for medical images. The key space is comparatively less than the method discussed in Chapter 4.

5.5 Summary

The method discussed in this chapter is concentrated on reducing computation time with suitable security for medical images. The selective medical image en/decryption process is proposed to reduce the computation time. The original medical image is bifurcated into selected pixel region and non-selected pixel region. Instead of shuffling all pixels, selected pixel region pixels are shuffled using dual hyperchaotic sequences. The non-selected pixel region is diffused using DNA XOR operation. All DNA encoding rules are utilized dynamically to construct encoded DNA matrices for both regions. All DNA

complementary rules are applied dynamically to produce ta cipher image. In subsequent chapters, will concentrate on reducing the computation time with security enhancement.

Chapter 6

DNA Cryptosystem for Compressed Medical Image

6.1 Introduction

The broadcast of medical images through a wireless open-source network is very vital in online virtual consultancy and electronic health services. The malicious attacks, eavesdropping, and adversarial attacks on medical images are very threatening. Security and confidentiality for medical images are necessary while communicating through insecure networks. For plain images, several encryption methods are available, these methods are not enough for medical images. Medical images are a major tool for practitioners to diagnose diseases. The minor discrepancy in disease related information causes a major critical problem. Hence, highly secured encryption methods are required to deliver security for medical images. The computation time for developing highly secured encryption techniques is high. The major challenge is the development of a highly secured encryption method with reduced computation time.

For reduction in time efficiency, a combination of compression and encryption methods are available. In (Tong et al.,2017), the SPIHT (Set Partitioning in Hierarchical Trees) encoding method based on integer wavelet transform is used for lossless compression. The wavelet coefficients are shuffled using chaotic maps in multiple rounds to encrypt the image. In (Zhang H et al.,2020), the author presented lossless image compression and encryption based on set partitioning in hierarchical trees (SPIHT) and cellular automata. The key stream is generated using cellular automata. The image is divided into three channels and these channels are further divided into low range frequency coefficients and high range frequency coefficients using a four-level wavelet transform. The low frequency

[1] Prema T. Akkasaligar, Sumangala Biradar, "Medical Image Compression and Encryption using Chaos based DNA Cryptography," 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC), 2020, pp. 261-265.

coefficients are scrambled using the Arnold cat map, Henon map, and Lorenz map. The encrypted low frequency coefficients are combined with frequency coefficients to compress the image. In (Gong L et al.,2020), authors have represented a combination of encryption method and lossless image compression using context-based adaptive lossless image codec (CALIC) and hyperchaotic system. These methods are not resisting known ciphertext attacks, known plain text attacks, and exhaustive attacks.

In SDMIE/D, the computation time is reduced but security is compromised. The multilayer encryption method using DNA cryptography and a high-dimensional chaotic map is proposed in this chapter to enrich the security of medical images. The main aim of the proposed cryptosystem is the reduction of computation time and enhancement of the security level of medical images. For reducing the time efficiency of the proposed system, the medical image is compressed using the compression technique.

6.2 Lossless Compression Method using DHWT

The compression represents a shrinking the size of images. The reduction in size leads to a reduction in redundancy of pixels and blur in the visual quality of an image. The compression is categorized as lossless compression and lossy compression. The lossy compression means with information loss and lossless compression means without information loss. For medical images, lossless compression is suitable because, if disease related information is lost then diagnosing the exact disease is highly impossible. The lossless compression method with a high compression ratio (CR) is good. The discrete Haar wavelet transform (DHWT) method is a simple, fast, and more efficient method than the state-of-art methods namely, run length encoding (RLE) and discrete cosine transform (DCT) (Khan S et al.,2019).

In DHWT, first medical image is transformed from the spatial domain into a frequency domain. In frequency domain, the medical image signals are decomposed into two subbands. In t first subband, the pairwise pixel average is calculated to lower the resolution of medical image. This process is called averaging or approximation or coarse coefficient. In second sub band, the pairwise pixel difference is calculated to recover the lossless medical image. This process is called differencing or detail coefficients. The Haar wavelet transform produces the sparse matrix for input images based on coarse and detail

coefficients. A sparse matrix contains many zeros, hence can be stored effectively. This leads to lesser image dimensions. The Haar wavelet's mother wavelet function $\psi(t)$ is defined in Eq. (6.2.1)

$$\psi(t) = \begin{cases} 1 & 0 \le t < \frac{1}{2} \\ -1 & \frac{1}{2} \le t < 1 \\ 0 & otherwise \end{cases} \qquad (6.2.1)$$

The scaling function $\varphi(t)$ is defined in Eq. (6.2.2)

$$\varphi(t) = \begin{cases} 1 & 0 \le t < 1 \\ 0 & otherwise \end{cases} \qquad (6.2.2)$$

The scaling function is Haar wavelet function. In proposed system, the original medical image is compressed to moderate the computation time during encryption. The compression algorithm reduces the number of bits used for representation of digital medical image. The expansive steps of compression algorithm are depicted in Algorithm 6.1.

Algorithm 6.1: Compression of medical image

//**Input:** Original medical image O (r, c)

//**Output:** Compressed medical image OC(r, c)

Step 1: Start

Step 2: Transform original medical image O(r,c) into signals in wavelet domain.

Step 3: Transformed medical image is divided into two sub-bands namely, L and H respectively.

Step 4: The L subbands are transformed through a low pass filter. In a low pass filter, mean operation is accomplished to get the coarse coefficients as shown in Eq.6.2.3.

$$\text{Coarse coefficients} = \frac{O(i,j)+O(i+1,j+1)}{2} \qquad (6.2.3)$$

Step 5: The H subbands are transformed through a high pass filter. In a high pass filter, difference operation is accomplished to get detail coefficients as shown in Eq.6.2.4.

$$\text{Detail coefficients} = \frac{O(i,j)-O(i+1,j+1)}{2} \quad (6.2.4)$$

Step 6: The level-dependent threshold matrix 't' is generated. The hard thresholding is used to set pixel values less than 't' to zero.

Step 7: The sparse matrix is obtained. In this way, the compressed OC(r, c) medical image is generated.

Step 8: Stop

The Haar wavelet is an orthogonal function and reversible function. Hence, during decompression, the transpose of Haar wavelet function is employed to get an original medical image.

6.3 Proposed DNA Cryptosystem for Compressed Medical Image

In proposed DNA cryptosystem with compression, the original medical image is compressed using DHWT to reduce the computation time. DNA cryptography and high-dimensional chaotic maps are utilized to offer high-level security for medical images as presented in Fig.6.1.

In proposed DNA cryptosystem, for compression of original medical image, the image is interpreted into frequency domain and divided into two subbands. In one subband, an average operation is used between neighboring pixels to extract coarse coefficient values. In another subband, difference operation is used between neighboring pixels to extract the details coefficient values in horizontal, diagonal, and vertical directions respectively. The level-set thresholding matrix is enforced to get the compressed medical image. The compressed medical image is segmented into four sub images in first level. The sub images are renovated into binary images. In second level, these binary images are converted into DNA encoded structures by applying all DNA encoding rules. In third level, 4D hyperchaotic sequences are referred for permutation of encoded DNA structures. The permuted DNA encoded structure pixels are diffused by DNA diffusion operation namely, DNA XOR in fourth level. The diffused DNA structures are merged to attain an

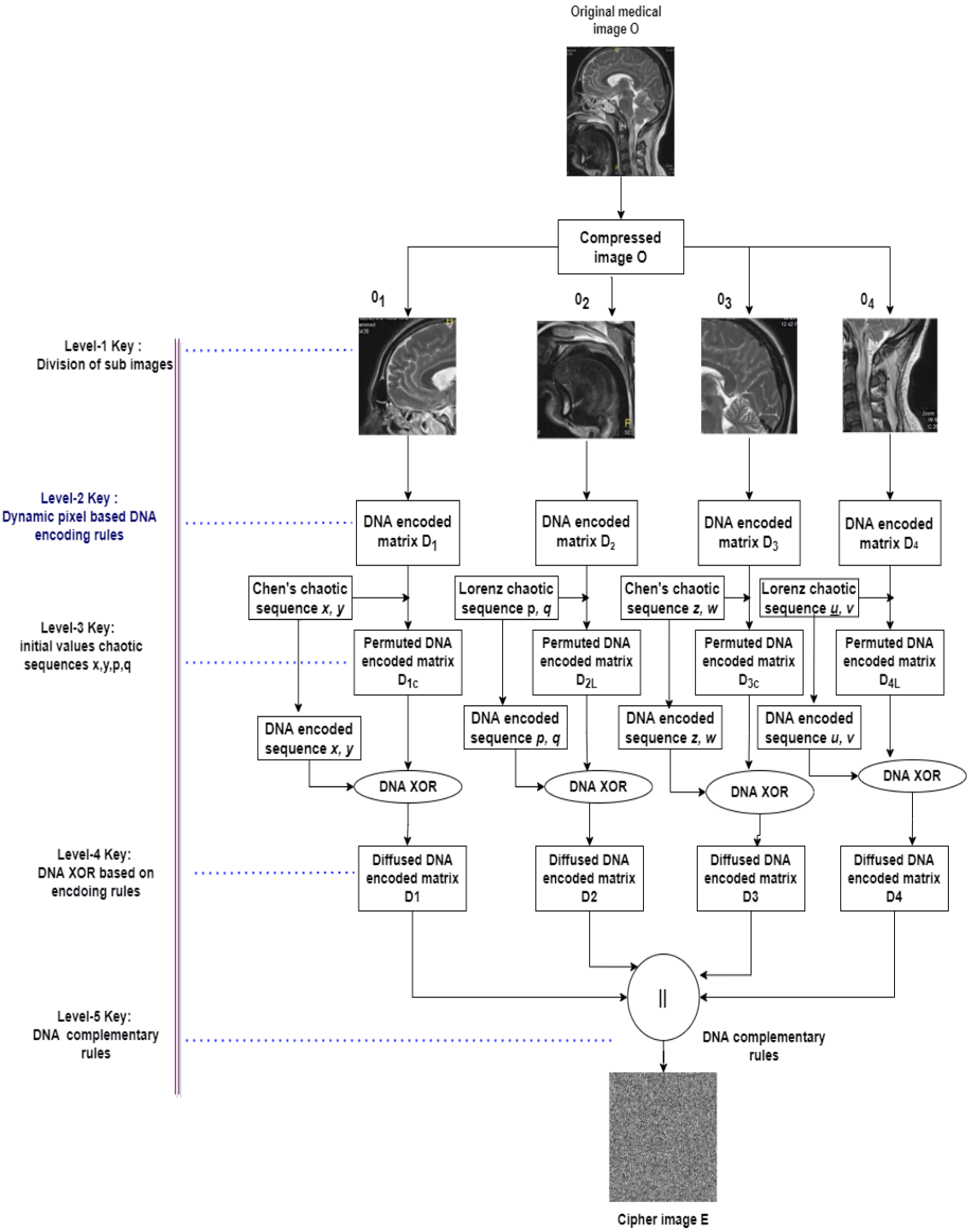


Fig .6.1 Block diagram of proposed encryption method for compressed medical image

intermediate cipher image. In fifth level, DNA complementary rules are mapped to convert the intermediate image into a cipher image. The details of the proposed DNA cryptosystem with compression are portrayed in en/decryption algorithm for compressed medical images.

6.3.1 Encryption Algorithm

The main objective of proposed encryption method is to offer high-level security for medical images with less time. The proposed encryption technique is demonstrated in Algorithm 6.2.

Algorithm 6.2: Encryption algorithm for compressed medical image

//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1: Start

Step 2: Original medical image is compressed using lossless DHWT as specified in compression Algorithm 6.1. The compressed medical image is bifurcated into four sub images of equal size.

$$O_1 = OC(1: r/2, 1: c/2);$$

$$O_2 = OC((r/2) +1: r,1: c/2);$$

$$O_3 = OC(1: r/2, (c)/2+1: c);$$

$$O_4= OC((r)/2) +1: r, (c/2) +1: c);$$

Step 3: The sub images are converted into a binary image.

$$B_1 (r, c\times8) = dec2bin (O_1 (r, c));$$

$$B_2 (r, c\times8) = dec2bin (O_2 (r, c));$$

$$B_3 (r, c\times8) = dec2bin (O_3 (r, c));$$

$$B_4 (r, c\times8) = dec2bin (O_4 (r, c));$$

Step 4: Binary images are converted into DNA encoded structures using all DNA encoding rules. The DNA encoding rules are chosen dynamically. Selection of dynamic DNA encoding rules is tabulated in Table 4.1 of Section 4.3.1 of Chapter 4.

$$D_1 (r, 4\times c) = reshape\ B_1 (r, c\times8);$$

$$D_2 (r, 4\times c) = reshape\ B_2 (r, c\times8);$$

$$D_3 (r, 4\times c) = reshape\ B_3 (r, c\times8);$$

$$D_4\ (r, 4\times c) = \text{reshape}\ B_4\ (r, c\times 8);$$

Step 5: The 4D hyperchaotic sequences *x, y, z, and w* are arranged in ascending order.

$$x = [x_0, x_1, x_2, \ldots\ldots\ldots x_n];$$

$$y = [y_0, y_1, y_2, \ldots\ldots\ldots y_n];$$

$$z = [z_0, z_1, z_2, \ldots\ldots\ldots z_n];$$

$$w = [w_0, w_1, w_2, \ldots\ldots\ldots w_n];$$

$$\bar{x} = sort(x);$$

$$\bar{y} = sort(y);$$

$$\bar{z} = sort(z);$$

$$\bar{w} = sort(w);$$

Step 6: Depending on position of sorted sequences $\bar{x}$ and $\bar{y}$, the pixels of D_1 are shuffled row-wise and column-wise respectively. Index values of ordered sequences $\bar{z}$ and $\bar{w}$ are utilized to shuffle the pixels of D_3, row-wise and column-wise respectively.

Step 7: The chaotic sequences *p, q, u, and v* are arranged in ascending order.

$$p = [p_0, p_1, p_2, \ldots\ldots\ldots p_n];$$

$$q = [q_0, q_1, q_2, \ldots\ldots\ldots q_n];$$

$$u = [u_0, u_1, u_2, \ldots\ldots\ldots u_n];$$

$$v = [v_0, v_1, v_2, \ldots\ldots\ldots v_n];$$

$$\bar{p} = sort(p);$$

$$\bar{q} = sort(q);$$

$$\bar{u} = sort(u);$$

$$\bar{v} = sort(v);$$

Step 8: Depending on position of sorted sequences $\bar{p}$ and $\bar{q}$, the pixels of D_2 are shuffled row-wise and column-wise respectively. Index values of ordered sequences $\bar{u}$ and $\bar{v}$ are utilized to shuffle the pixels of D_4, row-wise and column-wise respectively.

Step 9: The chaotic sequences *x, y, z, w, p, q, u, and v* are converted into DNA sequences D_{xy}, D_{zw}, D_{pq}, and D_{uv} using DNA encoding coding rules. The 4-

bit MSB of chaotic sequences are utilized to choose DNA encoding rules dynamically as tabulated in Table 4.1 of Section 4.3.1 of Chapter 4.

Step 10: Diffusion operation DNA XOR is utilized to diffuse the pixels of $D_{1,}$ $D_{2,}$ $D_{3,}$ and D_4 respectively.

$$D1\ (r, 4\times c) = D_1(r, 4\times c)\ \text{DNA XOR}\ D_{xy}\ (r, 4\times c);$$

$$D2\ (r, 4\times c) = D_2\ (r, 4\times c)\ \text{DNA XOR}\ D_{pq}\ (r, 4\times c);$$

$$D3\ (r, 4\times c) = D_1(r, 4\times c)\ \text{DNA XOR}\ D_{zw}\ (r, 4\times c);$$

$$D4\ (r, 4\times c) = D_2\ (r, 4\times c)\ \text{DNA XOR}\ D_{uv}\ (r, 4\times c);$$

Step 11: Diffused matrices D1, D2, D3, and D4 are concatenated.

$$D\ (r, 4\times c) = D1 \parallel D2 \parallel D3 \parallel D4;$$

Step 12: DNA encoded structure is renovated as a binary image using DNA complementary rules. As tabulated in Table 4.2 of Section 4.3.1 of Chapter 4, the 2-bit LSB of DNA encoded structure is utilized to choose DNA complementary rules dynamically.

$$B\ (r, c\times 8) = \text{reshape}\ D\ (r, 4\times c);$$

Step 13: Binary image is renewed into a cipher image

$$E\ (r, c) = \text{bin2dec}\ (B\ (r, c\times 8));$$

Step 14: Stop

In state-of-art encryption techniques, only two chaotic sequences are utilized for the permutation and diffusion process. In this encryption method, all four Chen's chaotic sequences x, *y*, *z*, and *w* are utilized in permutation and diffusion process of first and third sub-images. Similarly, all four Lorenz chaotic sequences *p*, *q*, *u*, and *v* are utilized in permutation and diffusion process of the second and fourth sub images. The cipher image is decrypted using a decryption algorithm.

6.3.2 Decryption Algorithm

The cipher image is decoded into an original medical image using a decryption technique. The decryption technique contains the reverse steps of an encryption technique. The expansive phases of proposed decryption technique are demonstrated in Algorithm 6.3.

Algorithm 6.3: Decryption algorithm for compressed medical image

//**Input:** Cipher image E (r, c)

//**Output:** Original medical Image O (r, c)

Step 1: Start

Step 2: The cipher image is renovated as a binary image.

$$B(r, c\times 8) = \text{dec2bin}(E(r, c));$$

Step 3: All DNA inverse complementary rules are mapped to convert the binary form of cipher image into a DNA encoded structure. The dynamic selection of DNA inverse complementary rules is depicted in Table 4.3 of Section 4.3.2 of Chapter 4.

$$D(r, 4\times c) = \text{reshape } B(r, c\times 8);$$

Step 4: Split the diffused D into D_1, D_2, D_3, and D_4 matrices.

Step 5: The chaotic sequences *p, q, u,* and *v* are arranged in descending order.

$$p = [p_0, p_1, p_2, \ldots\ldots p_n];$$

$$q = [q_0, q_1, q_2, \ldots\ldots q_n];$$

$$u = [u_0, u_1, u_2, \ldots\ldots u_n];$$

$$v = [v_0, v_1, v_2, \ldots\ldots v_n];$$

$$\bar{p} = sort(p);$$

$$\bar{q} = sort(q);$$

$$\bar{u} = sort(u);$$

$$\bar{v} = sort(v);$$

Step 6: The 4D hyperchaotic sequences *x, y, z,* and *w* are arranged in descending order.

$$x = [x_0, x_1, x_2, \ldots\ldots ..x_n];$$

$$y = [y_0, y_1, y_2, \ldots\ldots ..y_n];$$

$$z = [z_0, z_1, z_2, \ldots\ldots\ldots z_n];$$

$$w = [w_0, w_1, w_2, \ldots\ldots w_n];$$

$$\bar{x} = sort(x);$$

$$\bar{y} = sort(y);$$

$$\bar{z} = sort(z);$$

$$\overline{w} = sort(w);$$

Step 7: The chaotic map sequences *p, q, u, x, y, z, w,* and *v* are converted into DNA sequences D_{xy}, $D_{zw,}$ $D_{pq,}$ and D_{uv} using DNA encoding rules. Dynamic selection of DNA encoding rules is tabulated in Table 4.3 of Section 4.3.2 of Chapter 4.

Step 8: Diffusion operation DNA XOR is utilized to diffuse the pixels of D_1, D_2, D_3, and D_4 respectively.

$$D_1\,(r, 4\times c) = D1(r, 4\times c)\ \text{DNA XOR}\ D_{xy}\,(r, 4\times c);$$

$$D_2\,(r, 4\times c) = D2(r, 4\times c)\ \text{DNA XOR}\ D_{pq}\,(r, 4\times c);$$

$$D_3\,(r, 4\times c) = D3(r, 4\times c)\ \text{DNA XOR}\ D_{zw}\,(r, 4\times c);$$

$$D_4\,(r, 4\times c) = D4(r, 4\times c)\ \text{DNA XOR}\ D_{uv}\,(r, 4\times c);$$

Step 9: A position of sorted sequences $\bar{x}$ and $\bar{y}$ are referred to permute D_1 row-wise and column-wise respectively. A position of sorted sequences $\bar{z}$ and $\overline{w}$ are referred to reshuffle the pixels of $D_{3,}$ row-wise and column-wise respectively.

Step 10: A position of sorted sequences $\bar{p}$ and $\bar{q}$ are referred to permute D_2 row-wise and column-wise respectively. A position of sorted sequences $\bar{u}$ and $\bar{v}$ are referred to permute D_4, row-wise and column-wise respectively.

Step 11: Diffused matrices D_1, D_2, D_3, and D_4 are concatenated.

$$D\,(r, 4\times c) = D_1 \,||\, D_2 \,||\, D_3 \,||\, D_4;$$

Step 12: DNA encoding rules are utilized to renew the encoded DNA matrix as a binary image. As tabulated in Table 4.4 of Section 4.3.2 of Chapter 4, the 2-bit MSB of a pixel of DNA encoded structure is utilized to choose the DNA inverse encoding rules dynamically.

$$B\,(r, c\times 8) = \text{reshape}\ D\,(r, 4\times c);$$

Step13: Binary image is transformed into decipher image. The decipher image is decompressed using a converse of Algorithm 6.2 to obtain an original medical image.

$$O\,(r, c) = \text{bin2dec}\,(B\,(r, c\times 8));$$

Step 14: Stop

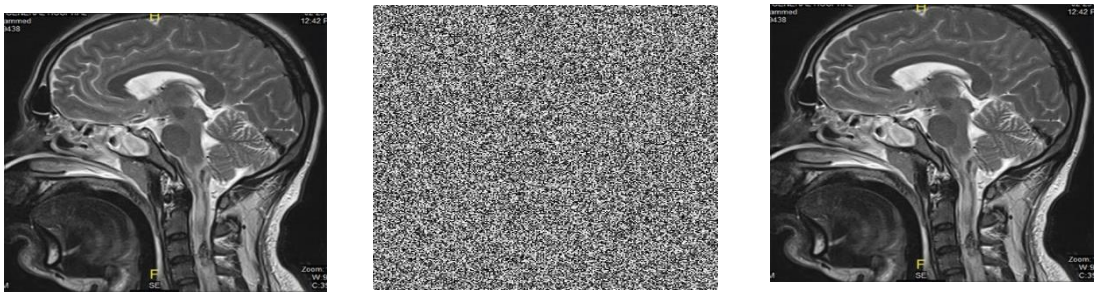
In this proposed cryptosystem, the original medical image is compressed for the reduction of computation time. The compressed image is bifurcated into four sub images of equal size. All eight DNA encoding rules are utilized to create a DNA matrix. The 4D Chen's chaotic sequences and 4D Lorenz sequences are utilized for permutation and diffusion process. The dynamic selection of DNA encoding and DNA complementary rules and high-dimensional chaotic sequences are useful for enhancement of security level of medical images.

6.4 Experimental Results and Discussion

The experimentation is conducted using MATLAB R2016b tool on system 9th generation Intel CoreTM i7 7500U CPU @ 2.70GHz, 2901 MHz, 2 Core(s), 4 Logical Processor(s). The developed crypto method is implemented on a dataset of five hundred medical images. The five different categories of medical images namely, MRI, Ultrasound, X-ray, ECG, and CT are gathered. From each category, 100 images are collected for implementation of the DNA cryptosystem with compression.

The original medical image as exhibited in Fig.6.2(a), is compressed using DHWT. Compressing the original medical image relies on average and difference operations. These operations are used to extract coarse and detail coefficients. The level-set thresholding is used to get the final compressed medical image. The compressed medical image is segmented into four sub images. These sub images are transformed into binary images. All eight DNA encoding rules as specified in Table 1.1 of Section 1.6 of Chapter 1, are selected dynamically based on bit-level values of binary images to construct DNA encoded structures. The Chen's chaotic map specified in Eqns. (1.5.1) - (1.5.4) of Chapter 1 are utilized to generate the chaotic sequences. The analytically determined primary values of state variables x_0=0.3, y_0=-0.4, z_0=1.2 and w_0=1 and control factors a_1=36, b_1=3, $c_{1=}$28, d_1=-16 and k=0.2 are employed to produce chaotic sequences. The 4D Lorenz chaotic system specified in Eqns. (1.5.8) – (1.5.11) of Chapter 1 are applied to generate chaotic sequences. The primary values of state variables p_0=3.2, q_0=8.5, u_0=3.6, and v_0= 2.2 are empirically determined. The chaotic sequences are sorted in increasing order and position of tsorted sequences are referred for the permutation of DNA structures. The confused DNA encoded structure pixels are diffused using DNA XOR operation. All eight chaotic sequences of both Chen's and Lorenz are utilized for confusing and diffusing the pixels of DNA

structures. The diffused DNA structures are merged and transformed as a binary image by all DNA complementary rules. The binary image is renovated into a cipher image as exhibited in Fig.6.2(b).



(a) (b) (c)

Fig.6.2 MR image samples: (a) Original MR image (b) Cipher image (c) Decipher image

In propose decryption algorithm, the cipher image is transformed into a binary image. The binary image is segmented into four sub images. DNA encoded structures are constructed for sub images using DNA inverse complementary rules. DNA XOR is applied for the diffusion of DNA encoded structures. The Chen's and Lorenz chaotic sequences are used for reshuffling the pixels of DNA structures. The DNA encoded structures are merged to get an intermediate decipher image. Further, DNA complementary rules are mapped to obtain a final compressed decipher image. The converse of DHWT is used to decompress the decipher image. The decompressed image is the original medical image as exhibited in Fig.6.2(c).

The working procedure of Algorithm 6.2 is illustrated with one suitable example. Consider original medical image matrix of size 4×4.

Step 1: The original medical image O is compressed using compression of the medical image algorithm i.e. Algorithm 6.1.

O =	4	2	8	3
	1	6	10	9
	7	3	4	5
	12	11	33	20

OC=	3	3	8	8
	3	3	8	8
	8	8	16	16
	8	8	16	16

Step 2: The compressed medical image OC is divided into four equal sub parts O_1, O_2, O_3, and O_4.

O_1=	3	3
	3	3

O_2=	8	8
	8	8

O_3=	8	8
	8	8

O_4=	16	16
	16	16

Step 3: The sub images are converted into binary sub images.

B_1 =	000000011	000000011
	000000011	000000011

B_2 =	00001000	00001000
	00001000	00001000

B_3 =	00001000	00001000
	00001000	00001000

B_4 =	00010000	00010000
	00010000	00010000

Step 4: DNA structures are constructed.

D_1 =	GGGC	GGGC
	GGGC	GGGC

D_2 =	GGAG	GGAG
	GGAG	GGAG

D_3 Row-wise =	GGAG	GGAG
	GGAG	GGAG

D_4 =	GTGG	GTGG
	GTGG	GTGG

Step 5: The DNA structure D_1 pixels are scrambled using *x* and *y* sequences.

D_1 Row-wise =	GGGC	GGGC
	GGGC	GGGC

D_1 Column-wise =	GGGC	GGGC
	GGGC	GGGC

Step 6: The DNA structure D_2 pixels are scrambled using *p* and *q* sequences.

D_2 Row-wise =	GGAG	GGAG
	GGAG	GGAG

D_2 Column-wise =	GGAG	GGAG
	GGAG	GGAG

Step 7: The DNA structure D_3 pixels are scrambled using *z* and *w* sequences.

D_3 =		
	GGAG	GGAG
	GGAG	GGAG

D_3 Column-wise =		
	GGAG	GGAG
	GGAG	GGAG

Step 8: The DNA structure D_4 pixels are scrambled using *u* and *v* sequences.

D_4 Row-wise =		
	GTGG	GTGG
	GTGG	GTGG

D_4 Column-wise =		
	GTGG	GTGG
	GTGG	GTGG

Step 9: The permuted pixels of D_1 are diffused by employing DNA XOR operation between D_1 and encoded DNA Chen's chaotic sequence D_{xy}.

D_x=		
	TTTG	CGGG
	GATG	CTAC

D_1 Row-wise =		
	CCCT	TAAT
	AGCT	TCGA

D_Y=		
	GATT	GGGA
	AACC	AATG

D_1 Column-wise =		
	TCGA	CGGT
	AGAG	TCCG

Step 10: The permuted pixels of D_2 are diffused by employing DNA XOR operation between D_2 and encoded DNA Lorenz chaotic sequence D_{pq}.

Dp=		
	GGAG	CTGT
	TCCC	CTGA

D_2 Row-wise =		
	AAAA	TCGC
	CTCA	TCGG

Dq=		
	GGCG	CCAT
	AGAT	GATG

D_2 Column-wise =		
	GGCG	GAGG
	CCCT	CCCA

Step 11: The permuted pixels of D_3 are diffused by employing DNA XOR operation between D_3 and encoded DNA Chen's chaotic sequence D_{zw}.

Dz =		
	GACT	GGTG
	AGCT	CTGA

D_3 Row-wise =		
	AGCC	AATA
	GACC	TCGG

Dw=	CAAG	AACC
	TCGG	GTGG

D_3 Column-wise =	CGCT	AAGC
	CCTT	CGAA

Step 12: The permuted DNA structure D_4 pixels are diffused using DNA XOR operation between D_4 and encoded DNA Lorenz chaotic sequence D_{uv}.

Du=	TGGA	GGGA
	GGAA	GAAA

D_4 Row-wise =	CCAG	ACAG
	ACGG	ATGG

Dv=	TTTC	GTGT
	AACG	GGGG

D4 Column-wise =	GGTT	GGGA
	ACTA	GCAA

Step 13: The concatenation of diffused encoded DNA matrices

D =	TCGA	CGGT	CGCT	AAGC
	AGAG	TCCG	CCTT	CGAA
	GGCG	GAGG	GGTT	GGGA
	CCCT	CCCA	ACTA	GCAA

Step 14: The encoded DNA matrix is transformed into a binary image to get a cipher image.

B =	01001110	11000001	01100100	01011100
	00100010	11101001	00000101	01101111
	01011001	00100000	11110101	11111110
	01010100	10101011	11100011	10011111

E =	78	193	100	92
	34	233	5	111
	89	32	245	254
	84	171	227	159

6.4.1 Performance and Security Analysis

In performance analysis, the quality of decompressed medical image depends on the compression ratio. The compression ratio (CR) is calculated using Eq. (6.3.1).

$$\text{CR} = \frac{\text{Image size before compression}}{\text{Image size after compression}} \qquad (6.3.1)$$

The average CR of this cryptosystem is 7.7 almost equal to ideal value 8 for lossless compression. This demonstrates that compression method DHWT is lossless. Hence, the proposed cryptosystem is adequate for medical images.

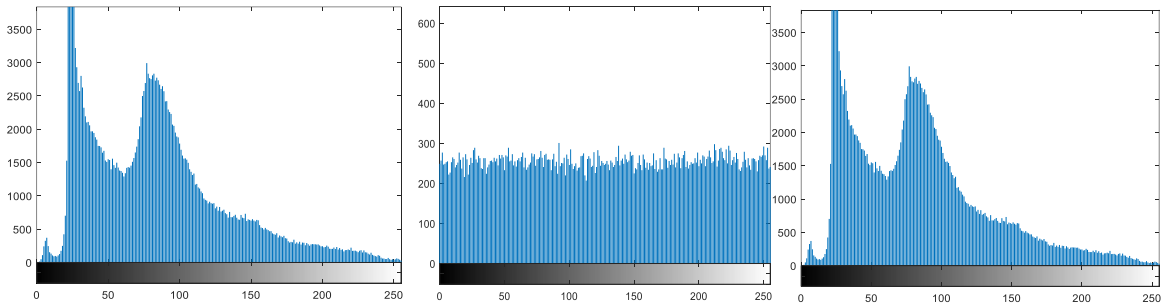
The performance of proposed cryptosystem is dependent on the resistance power of system against a variety of attacks such as statistical attacks, differential attacks, and exhaustive attacks. The quality of proposed en/decryption method is measured using metrics MSE, PSNR, and entropy.

A. Statistical Attacks

The crypto analyst substantiates the resistant of proposed DNA cryptosystem with compression against statistical attack using indicators such as histogram and correlation coefficient analysis. These analyses are based on frequency distribution and correlation between neighboring pixels.

Histogram Analysis

The histogram is depending on the distribution of intensity levels of medical images. Consistent distribution of pixels is preferable for good encryption techniques. In the



(a) (b) (c)

Fig.6.3 Histogram analysis: (a) Original MR image (b) Cipher image (c) Decipher image

histogram of original medical image and decipher image, pixels are scattered inconsistently as exhibited in Fig. 6.3((a) and (c)). In the histogram of cipher image, pixels are scattered consistently as exhibited in Fig. 6.3 (b). This demonstrates that developed encryption method has good pseudo-randomness.

The outcomes of chi-square are tabularized in Table 6.1. The hypothesis test evidences statistically, that pixels are scattered evenly in cipher image.

Table 6.1 Chi-square test for proposed DNA cryptosystem for compressed medical image

Medical image type	Cipher image	Hypothesis test
MR	257.6016	pass
CT	259.6953	pass
X-ray	261.5078	pass
Ultrasound	262.1641	pass
ECG	259.4844	pass

Correlation Coefficient Analysis

The pixels of medical images are highly correlated, and intruders will take the advantage of correlation to predict the original medical image. The correlation coefficient analysis is

Table 6.2 Correlation coefficient for proposed DNA cryptosystem for compressed medical image

Medical image type	Direction	Cipher image	Decipher image
CT	*Horizontal*	0.00182	0.9995
	Vertical	-0.00108	0.9999
	Diagonal	-0.00147	0.9997
MR	*Horizontal*	0.00126	0.9996
	Vertical	-0.00189	0.9994
	Diagonal	0.00175	0.9998
Ultrasound	*Horizontal*	-0.00169	0.9993
	Vertical	0.00191	0.9993
	Diagonal	-0.00106	0.9993
X-ray	*Horizontal*	-0.00108	0.9996
	Vertical	0.00169	0.9997
	Diagonal	-0.00157	0.9998
ECG	*Horizontal*	0.00165	0.9995
	Vertical	0.00129	0.9998
	Diagonal	0.00106	0.9994
Average :		**0.000172**	**0.9995**

carried out to analyze the association between neighboring pixels of original medical image, cipher image, and decipher image. The result of correlation coefficient analysis is depicted in Table 6.2. The average correlation value of cipher image is 0.000172 and decipher image is 0.9995. The correlation value of the cipher is almost equal to '0' proves that neighboring pixels are not correlated. The correlation value of decipher image is almost equal to '1' means adjacent pixels are highly correlated.

The correlation coefficient among neighboring pixels of original medical image and cipher image in three different directions namely, horizontal, vertical, and diagonal are depicted in Fig.6.4. The pixels are correlated in original medical images as exhibited in Fig.6.4 (a and b and c). The pixels are not correlated in cipher image as exhibited in Fig.6.4 (d and e and f). Thus, DNA cryptosystem with compression is highly secure for medical images.

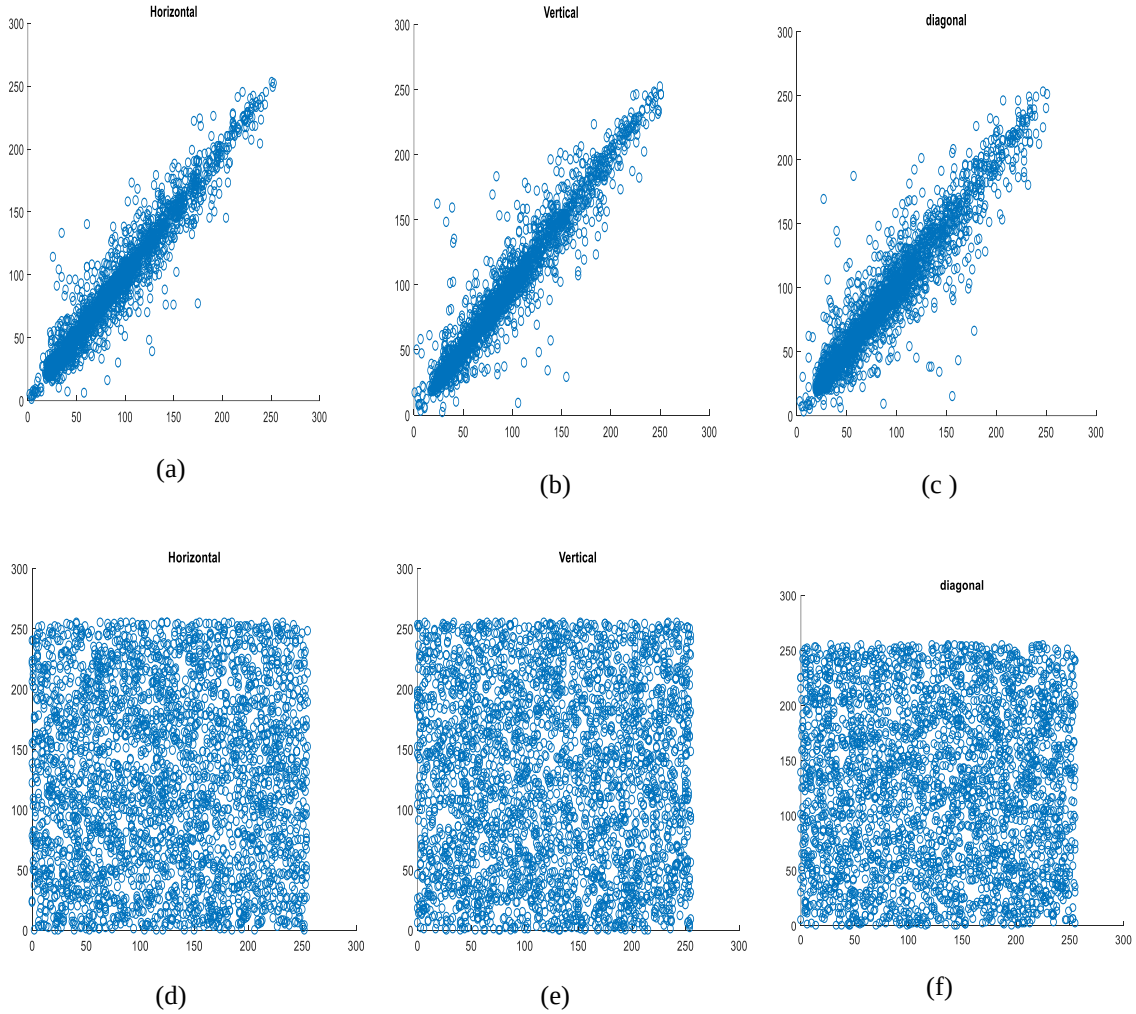


Fig. 6.4 Scatter plot of original MR image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

B. Exhaustive Attacks

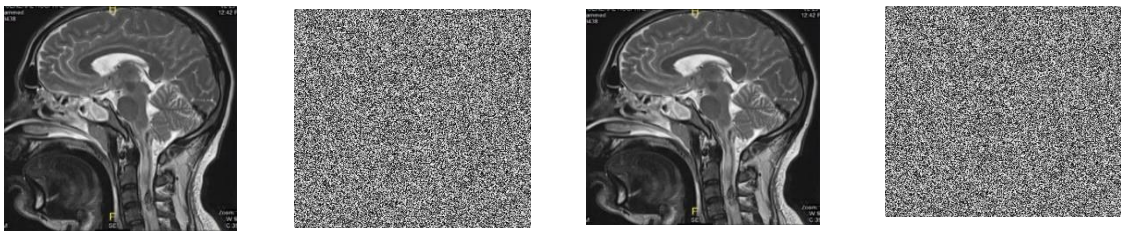
In encryption method secret keys are the main provisions in providing security for medical images. Attackers struggle to get an encryption keys in exhaustive attacks. The key space and key sensitivity indicators are employed to validate invulnerable to exhaustive attacks.

Key Space Analysis

In proposed DNA cryptosystem with compression, secret keys are the preliminary values of state factors of 4D Chen's chaotic sequence and 4D Lorenz chaotic sequences. A total of eight secret keys (x_0, y_0, z_0, w_0, p_0, q_0, u_0, and v_0) are available. Then, the length of eight secret keys is $(10^{15})^8 \approx 2^{400}$. The proposed cryptosystem key space is huge. Hence, this method is suitable to boost the security of medical images.

Key Sensitivity Analysis

The proposed cryptosystem is extremely sensitive to preliminary conditions of state parameters of high dimensional chaotic maps. A small modification in initial value of any one of the secret keys will create a major issue. For example, the encryption of an original medical image as exhibited in Fig.6.5(a) is dependent on initial values of eight secret keys to obtain a cipher image as exhibited in Fig. 6.5(b). During decryption, the same initial values of eight secret keys are utilized to get a decipher image as exhibited in Fig. 6.5(c). If we decrypt the same cipher image with a minor difference in one of the secret keys as v_0= 2.199999 instead of v_0= 2.2 then decrypted image is exhibited in Fig.6.5(d). The decrypted medical image with incorrect secret key is not same as the original medical



(a) (b) (c) (d)

Fig.6.5 Key sensitivity analysis: (a) Original MR image (b) Cipher image (c) Decipher image with correct initial values of secret key *v0*= 2.2 (d) Decipher image with an incorrect secret key as v_0= 2.199999

image. Hence, proposed DNA cryptosystem with compression is very sensitive to the preliminary conditions of secret keys.

C. Differential Attacks

The differential attacks are carried out by crypt analysts to verify the plain image sensitivity. The metrics NPCR and UACI as specified in Section 1.9.2 of Chapter 1 are used to check the resistant of differential attacks. The NPCR and UACI value for the average of 500 medical images is 99.6628% and 33.10% as tabularized in Table 6.3. The NPCR and UACI value is equal to ideal value. Hence, proposed DNA cryptosystem with compression is sensitive to original medical image. The slight variation in original medical image generates a varied cipher image.

Table 6.3 Performance analysis of proposed DNA cryptosystem for compressed medical images

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.662	33.06	7.9998	6.2567e+03	4.0982
CT	99.664	33.00	7.9996	6.8546e+03	4.0675
X-ray	99.660	33.08	7.9994	6.3958e+03	4.3476
Ultrasound	99.668	33.17	7.9999	7.0012e+03	4.6879
ECG	99.660	33.19	7.9997	6.9871e+04	4.5031
Average	**99.663**	**33.10**	**7.99968**	**1.93E+04**	**4.3408**

The entropy value is 7.99968 and MSE value is very high and PSNR value is very less as shown in Table 6.3. The visual representation of performance analysis is shown in Fig.6.6.

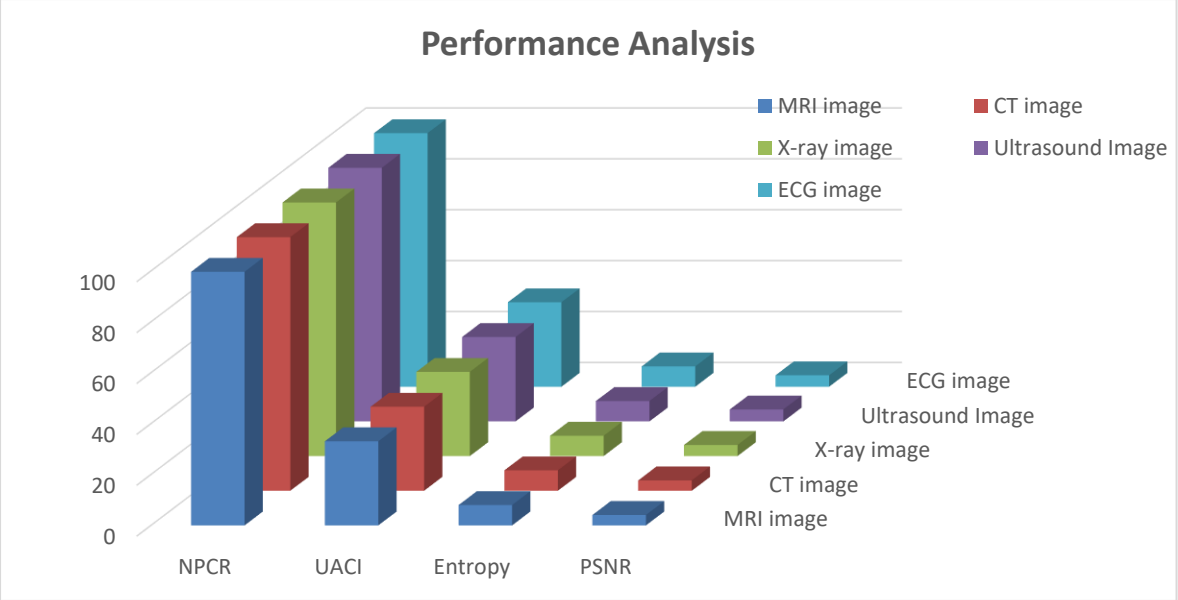


Fig. 6.6 Performance analysis of proposed DNA cryptosystem for compressed medical image

From the Fig.6.6, it is proved that the proposed en/decryption technique for compressed medical image is resistant to all attacks. Hence, it is appropriate to offer enhanced security to medical images.

6.4.2 Computation Time of Proposed En/Decryption Algorithm for Compressed Medical Image

The computation time of proposed en/decryption algorithm for a compressed original medical image of size (m×n) calculated as follows:

Step 1: Medical image compression: (m×n)

Step 2: Binary conversion of compressed original medical image: (m×n)

Step 3: Construction of DNA structure: (m×n)

Step 5: Permutation process: (m×n)

Step 6: Diffusion process: (m×n)

Step 7: DNA decoding: (m×n)

Step 8: Generating cipher image: (m×n)

Total time complexity of proposed encryption algorithm is given below:

$T(n)= (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) = 7(m\times n)$

If $m=n$ then $T(n)=7(n^2) \in O(n^2)$.

In proposed en/decryption method, DHWT method is utilized to attain a compressed medical image for the original medical image. The compression algorithm DHWT makes the medical image with smallest possible bits for a reduction in the computation time. The high dimensional chaotic systems, dynamic selection of all eight DNA encoding and complementary rules, and DNA XOR operations are employed to offer high-level security to medical images. The computation time is reduced by the compression of medical image as shown in Table 6.4.

Table 6.4 Computation time of proposed DNA cryptosystem for compressed medical image

Medical image type	Encryption time for original medical image (seconds)	Encryption time for compressed medical image
CT	38.14	28.72
MR	37.09	27.65
Ultrasound	37.16	28.57
X-ray	38.41	27.23
ECG	39.98	23.78
Average :	**38.156**	**27.19**

From Fig. 6.7, the reduction of computation time for the compressed medical image is proven.

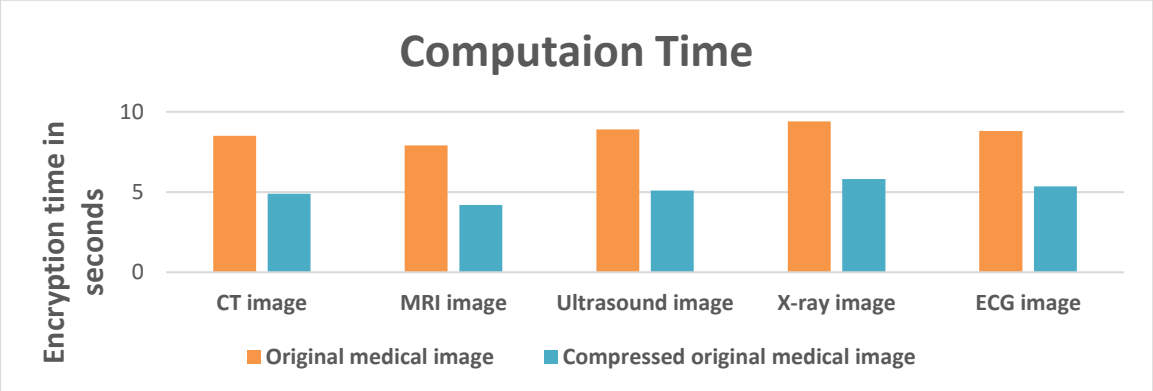


Fig. 6.7 Computation time of proposed DNA cryptosystem for compressed medical image

6.4.3 Comparative Analysis

The en/decryption for compressed medical image method is compared with methods discussed in section 6.1. From comparative analysis, as shown in Table 6.5, it is proved that proposed cryptosystem is a lossless compressed method and Key space is also large.

Table 6.5 Comparative analysis of proposed DNA cryptosystem for compressed medical images

Methods	Entropy	Compression ratio	Key Space
Tong et al.,2017	7.5802	6.4449	------
Zhang H et al.,2020	7.9887	5.6843	------
Gong L et al.,2020	7.9989	4.7186	2^{384}
Proposed DNA cryptosystem for compressed medical image	**7.9992**	**7.7000**	**2^{400}**

The graphical representation of comparative analysis is exhibited in Fig.6.8. The proposed DNA cryptosystem for compressed medical image is appropriate to offer a highest-level security with reduced computation time.

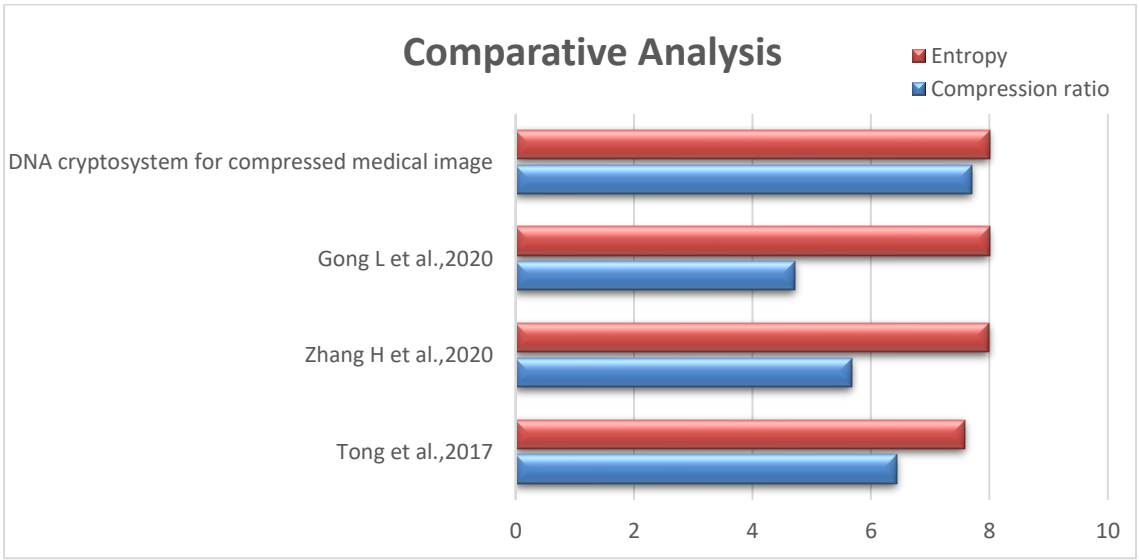


Fig. 6.8. Comparative analysis of proposed DNA cryptosystem for compressed medical image

The proposed en/decryption method compressed medical image is also compared with the methods discussed in previous Chapters. The comparative analysis as depicted in Table 6.6 illustrated that the proposed encryption method computation time is reduced compared to encryption method of Chapter 4. Also, proves that computational cost and key space are high enough than the encryption method specified in Chapter 5 and almost equal to encryption method specified in Chapter 4. Hence,proposed DNA cryptosystem with compression is appropriate to offer enough security for medical images during digital communication with reduced computation time.

Table 6.6 Comparative analysis of proposed DNA cryptosystem for compressed medical image with previous methods

Performance Metrics	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	MSE	Key Space	Encryption Time (Seconds)
DNA cryptosystem with integrity (Chapter 4)	7.99936	99.6626	33.906	5.4954	5.18E+04	2^{409}	34.98
SDMIE/D (Chapter 5)	7.542	99.468	33.5	5.72	7.39E+02	2^{250}	2.698
Proposed DNA cryptosystem for compressed medical image	**7.999**	**99.662**	**33.1**	**4.34**	**6.70E+04**	$\mathbf{2^{400}}$	**27.19**

6.5 Summary

The en/decryption technique for compressed medical image is discussed in this chapter. The original medical is transformed into wavelet signals in frequency domain. These signals are divided into sub bands. The coarse coefficients of one sub bands and detail coefficients of other sub bands are utilized to compress the original medical image. The compressed medical image is decomposed into four sub images of equal size. The sub images are transformed into DNA encoded structures using all eight DNA encoding rules. The 4D Chen's chaotic map and 4D Lorenz's chaotic map sequences are referred for the permutation of encoded DNA structures row-wise and column-wise respectively. These chaotic sequences along with DNA XOR operation diffuse the pixels of DNA structures. The DNA encoded structures are combined and renovated into binary image using all eight DNA complementary rules. The binary image is transformed into a cipher image. The

security is enhanced in this proposed en/decryption technique with a dynamic selection of DNA coding rules, complementary rules and high dimensional eight chaotic sequences. To reduce the computation time, the medical image is compressed. The selective medical en/decryption method is compromised in security and this encryption method is significantly compromised in quality. Hence, the main challenge is to reduce the computation time without compromising in security and quality of medical image. All en/decryption methods discussed are computed sequentially. In sequential computation, for achieving enhanced high-level security to medical images requires more execution time. The en/decryption technique discussed in subsequent chapter is concentrating on parallel approach to resolve this problem.

Chapter 7

Parallel Approach for DNA Cryptosystem

7.1 Introduction

The recent COVID-19 pandemic has introduced a medical emergency everywhere. The practitioners or doctors are inclining toward online virtual consultation. In online virtual communication, diagnosis is based on symptoms and images of implicit body parts. This information is communicated through wireless communication channels. These channels are open-source networks; hence cyberpunks can breach the information. For practitioner, diagnosing the specific diseases from breached information is extremely not possible. Hence, significant security, integrity, and confidentiality of medical images are very important for wireless communication. Several encryption techniques based on chaotic maps and DNA cryptography are available. The computation time of these encryption techniques are very high. So, the main research challenge is to embellish the security of medical images, with less time. Selective part encryption and compressed medical image encryption methods are available. However, these encryption techniques are either sacrificed in security or quality. In this chapter, we developed a new approach for medical image encryption with reduced computation time and without compromising quality and security.

In (Abbas, Alaa M., Ayman A. Alharbi, and Saleh Ibrahim, 2021), pixel-level parallelism is performed to generate chaotic sequences swiftly. The discrete chaotic sequence is generated based on defined elliptic curve (EC) points and logical add operation. These sequences are referred to construct a cipher image. The encryption process is parallelized using parallel processing toolboxes such as GPU acceleration, multi-core CPUs, and DSPs.

---

[1] Prema T. Akkasaligar, Sumangala Biradar, "***A Parallel Algorithm Approach for Medical Image using DNA Cryptography***", Journal of The Institution of Engineers (India)-Series B.(communicated)

In (Yu, Jiayin, Chao Li, Xiaomeng Song, Shiyu Guo, and Erfu Wang, 2021), the author presented a parallel encryption technique using a compressed sensing framework and chaotic encryption theory. The chaotic signals with compressed sensing theory are applied to compress the image. The compressed image is united with sample image to get a mixed image. The mixed image is divided into eight samplings and these image pixels are rearranged by a 3D chaotic map to get a cipher image. These encryption techniques are focused on reducing computation time but, security is compromised as a result of limited key space. Hence, not adequate to rescue medical images from intruders.

The main aim of parallel DNA cryptosystem is to enforce integrity and provide enhanced security and confidentiality for medical images with reduced run-time.

7.2 Proposed Parallel DNA Cryptosystem for Medical Image

The previous encryption methods depend on serial execution. In serial execution, the set of instructions of encryption methods runs in sequential and it requires more execution time. To stipulate intensify prominent level security with reduced execution time, the parallel approach is proposed to run a set of encryption instructions concurrently.

The parallel encryption algorithm reduces the computation time with the help of multiple processors. These multiple processors will run simultaneously to condense the execution time of encryption algorithm.

The parallel encryption algorithms are classified into Central Processing Unit (CPU) and Graphics Processing Unit (GPU). In GPU based algorithms, additional hardware configuration and similar expensive configuration must exist on both sides i.e. sender and receiver. One more apprehension about compatibility is to need a different programming frameworks and manufacturers, such as CUDA and OpenCL. The CPU based encryption algorithm is cost-effective and adapts the same programming framework. Hence, the proposed parallel encryption algorithm is implemented using CPU based method.

In proposed parallel DNA cryptosystem, the high dimensional chaotic maps and DNA sequence processes are utilized to offer significant security for medical images. To reduce the computation time a parallel encryption algorithm is proposed as shown in Fig.7.1.

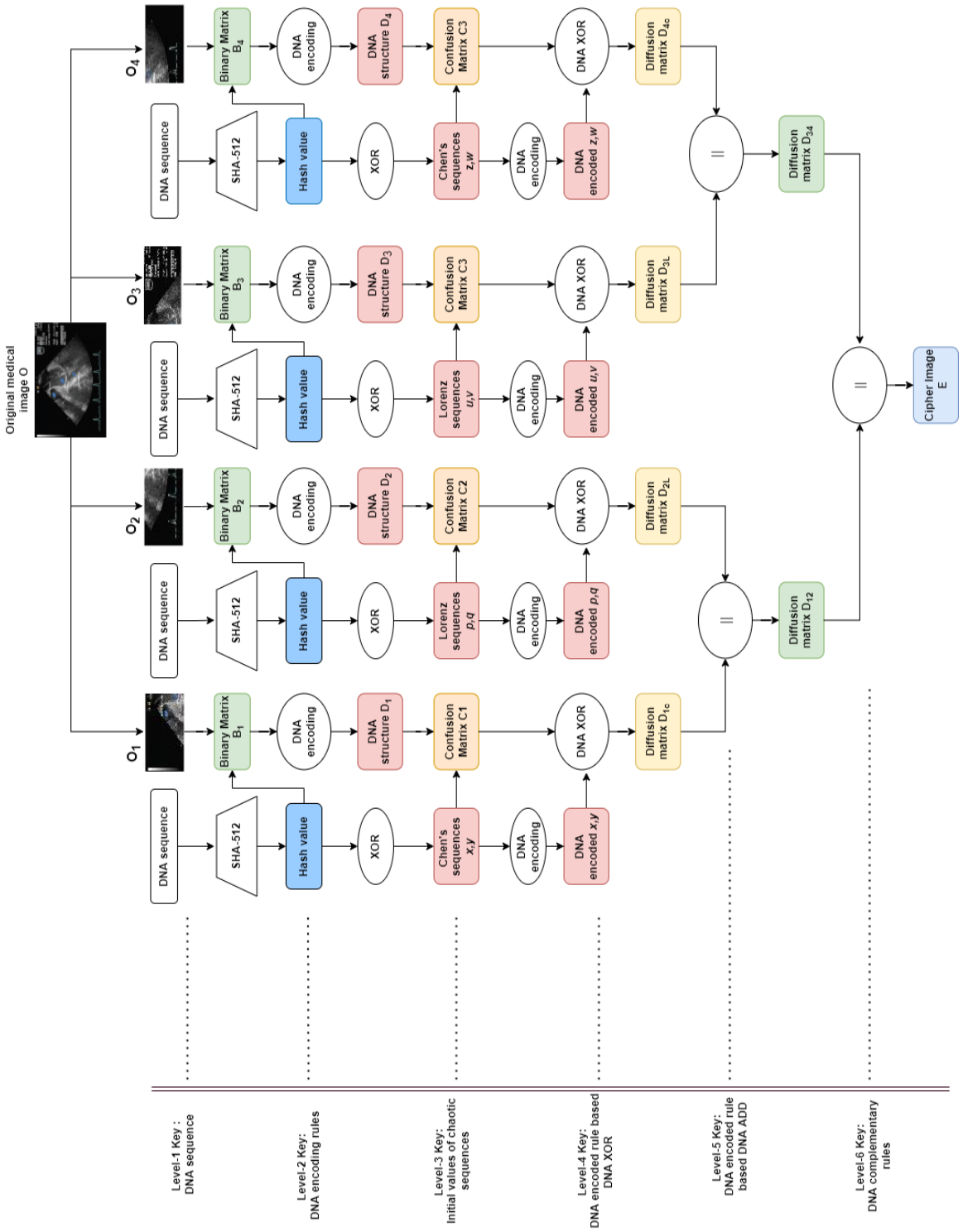


Fig.7.1 Block diagram of proposed parallel encryption method

The process of instruction-level parallelism of parallel DNA cryptosystem is exhibited in Fig.7.2. In proposed parallel DNA cryptosystem, the hash function SHA-512 is used to calculate hash keys for four different DNA sequences namely, Canis lupus (ID

MW549038.1 in GenBank), Homo sapiens (ID AJ276502.1 in GenBank), Erythrocebus patas (ID D85291.1 in GenBank) and Oryctolagus cuniculus (ID NW_001082024.1). The medical image is bifurcated into four sub parts. Each subpart of a medical image is transformed into binary image form. For each matrix, row-wise threads are created and assigned to workers of local clusters to run parallel. Each thread performs computation concurrently in a nondeterministic order. The hash keys are embedded into 2-bit LSB of binary images concurrently. The multiple chaotic system sequences are used to confuse the pixels row-wise using multiple threads. The DNA sequence structure is composed by all eight DNA encoding rules. Chen's chaotic sequences and Lorenz's chaotic sequences are embedded with hash values. The embedded chaotic sequences are referred for the permutation of DNA structures row-wise. The permuted rows are diffused using DNA XOR operations. The diffused rows are decoded by DNA complementary rules. The decoded binary image is renewed into a cipher image. This process is repeated to remaining all sub parts of the medical image successively.

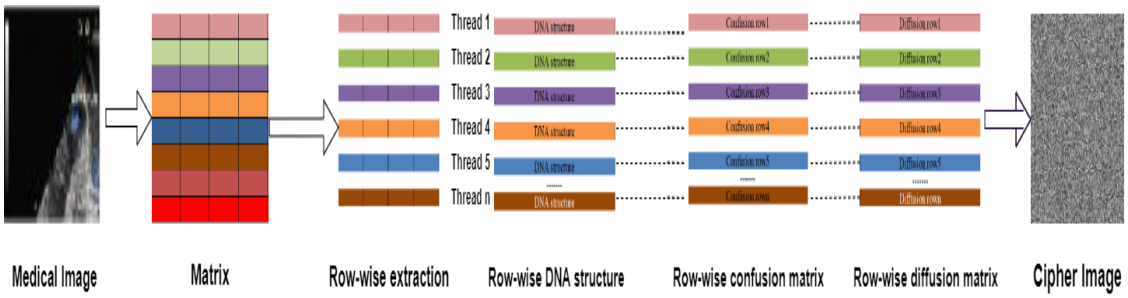


Fig.7.2 Parallel computation of proposed encryption algorithm

The expansive steps are demonstrated in a parallel DNA encryption algorithm.

7.2.1 Parallel Encryption Algorithm

In proposed parallel DNA cryptosystem, the integrity is enforced using SHA-512 and confidentiality using four different DNA sequences. For enhancement of the security of medical images, multilevel encryption is performed using high dimensional chaotic sequences namely, 4D Chen's hyperchaotic system and 4D Lorenz chaotic system. The eight DNA encoding and complementary rules are applied to produce a distinctive DNA encoded sequence. To reduce the computation time instruction-level parallelism is implemented. The proposed parallel encryption method for medical image is illustrated in Algorithm 7.1.

Algorithm 7.1: A parallel encryption method for medical images

//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1: Start

Step 2: The original medical image is segmented into four sub images of equal size.

$O_1 = O(1: r/2, 1: c/2);$

$O_2 = O((r/2) +1: r, 1: c/2);$

$O_3 = O(1: r/2, (c)/2+1: c);$

$O_4 = O((r)/2) +1: r, (c/2) +1: c);$

Step 3: Multiple threads are utilized to boost the execution time. For each row-wise iteration, one thread is created. The medical image 'O' of size 'r' uses 'r' threads and these threads run simultaneously with the help of workers available in the local cluster.

Step 4: The sub images are converted into four binary images, row-wise using multiple threads.

$B_1 (r, c\times8) = dec2bin (O_1 (r, c));$

$B_2 (r, c\times8) = dec2bin (O_2 (r, c));$

$B_3 (r, c\times8) = dec2bin (O_3 (r, c));$

$B_4 (r, c\times8) = dec2bin (O_4 (r, c));$

Step 5: The SHA-512 is applied for four different DNA sequences namely, Canis lupus (ID MW549038.1 in GenBank), Homo sapiens (ID AJ276502.1 in GenBank), Erythrocebus patas (ID D85291.1 in GenBank) and Oryctolagus cuniculus (ID NW_001082024.1) to obtain four different hash values Hk_1, Hk_2, Hk_3, and Hk_4.

Step 6: The Hk_1, Hk_2, Hk_3, and Hk_4 are embedded into 2-bit LSB of four binary images B_1, B_2, B_3, and B_4 respectively.

Step 7: Binary images are transformed into a DNA encoded structures using all DNA encoding rules concurrently. The DNA encoding rules are selected dynamically. Selection of dynamic DNA encoding rules is depicted in Table 4.1 of Section 4.3.1 of Chapter 4.

$D_1 (r, 4\times c) = reshape\ B_1 (r, c\times8);$

$D_2 (r, 4\times c) = reshape\ B_2 (r, c\times8);$

D_3 (r, 4×c) = reshape B_3 (r, c×8);

D_4 (r, 4×c) = reshape B_4 (r, c×8);

Step 8: The 4D Chen's sequences *x, y, z,* and *w* are arranged in ascending order.

$$x = [x_0, x_1, x_2, \ldots\ldots .. x_n];$$

$$y = [y_0, y_1, y_2, \ldots\ldots .. y_n];$$

$$z = [z_0, z_1, z_2, \ldots\ldots\ldots\ldots z_n];$$

$$w = [w_0, w_1, w_2, \ldots\ldots w_n];$$

$$\bar{x} = sort(x);$$

$$\bar{y} = sort(y);$$

$$\bar{z} = sort(z);$$

$$\bar{w} = sort(w);$$

Step 9: The chaotic sequences *x, y, z,* and *w* are embedded with HK_1 and HK_4 using logical XOR respectively.

$$x = x \oplus HK_1$$

$$y = y \oplus HK_1$$

$$z = z \oplus HK_4$$

$$w = w \oplus HK_4$$

Step 10: The position of sorted chaotic sequences $\bar{x}$ and $\bar{y}$ are referred for the permutation of D_1, row-wise and column-wise respectively. The index values of ordered sequences $\bar{z}$ and $\bar{w}$ are utilized to shuffle the pixels of D_4, row-wise and column-wise respectively with the help of multithreads.

Step 11: The Lorenz chaotic sequences p, q, *u*, and *v* are arranged in ascending order.

$$p = [p_0, p_1, p_2, \ldots\ldots p_n];$$

$$q = [q_0, q_1, q_2, \ldots\ldots q_n];$$

$$u = [u_0, u_1, u_2, \ldots\ldots u_n];$$

$$v = [v_0, v_1, v_2, \ldots\ldots v_n];$$

$$\bar{p} = sort(p);$$

$$\bar{q} = sort(q);$$

$$\bar{u} = sort(u);$$

$$\bar{v} = sort(v);$$

Step 12: The 4D Lorenz chaotic sequences *p, q, u,* and *v* are embedded with HK_2 and HK_3 using logical XOR respectively.

$$p = p \oplus HK_2$$
$$q = q \oplus HK_2$$
$$u = u \oplus HK_3$$
$$v = v \oplus HK_3$$

Step 13: The position of sorted chaotic sequences $\bar{p}$ and $\bar{q}$ are referred for the permutation of D_2, row-wise and column-wise respectively. Index values of ordered sequences $\bar{u}$ and $\bar{v}$ are utilized to shuffle the pixels of D_3, row-wise and column-wise respectively with the help of multi threads.

Step 14: The chaotic sequences *x, y, z, w, p, q, u,* and *v* are converted into DNA sequences D_{xy}, D_{zw}, D_{pq}, and D_{uv} by DNA encoding rules. DNA encoding rules are chosen dynamically based on a 4-bit MSB of chaotic sequence using a dynamic selection of DNA encoding rules as depicted in Table 4.1 of Section 4.3.1 of Chapter 4.

Step 15: Diffusion operation DNA XOR is employed to diffuse the pixels of D_1, D_2, D_3, and D_4 respectively.

$$D_{1c}(r, 4\times c) = D_1(r, 4\times c) \text{ DNA XOR } D_{xy}(r, 4\times c);$$
$$D_{2L}(r, 4\times c) = D_2(r, 4\times c) \text{ DNA XOR } D_{pq}(r, 4\times c);$$
$$D_{3L}(r, 4\times c) = D_3(r, 4\times c) \text{ DNA XOR } D_{uv}(r, 4\times c);$$
$$D_{4c}(r, 4\times c) = D_4(r, 4\times c) \text{ DNA XOR } D_{zw}(r, 4\times c);$$

Step 16: Diffused matrices D_{1c}, D_{2L}, D_{3L}, and D_{4c} are merged.

$$D_{12}(r, 4\times c) = D_{1c}(r, 4\times c) \,||\, D_{2L}(r, 4\times c);$$
$$D_{34}(r, 4\times c) = D_{3L}(r, 4\times c) \,||\, D_{4c}(r, 4\times c);$$

Step 17: Diffused matrices D_{12} and D_{34} are concatenated.

$$D(r, 4\times c) = D_{12} \,||\, D_{34};$$

Step 18: Row-wise threads are used to renovate DNA encoded sequences as a binary image using DNA complementary rules parallelly. The DNA complementary rules are chosen dynamically with help of 2-bit LSB of the

DNA encoded sequences, as depicted in Table 4.2 of Section 4.3.1 of Chapter 4.

B (r, c×8) = reshape D (r, 4×c);

Step 19: The binary image is reformed as a cipher image parallelly using multiple threads.

E (r, c) = bin2dec (B (r, c×8));

Step 20: Stop

7.2.2 Parallel Decryption Algorithm

In proposed parallel decryption technique, cipher image is reverted into an original medical image. The expansive process of proposed decryption method is depicted in Algorithm 7.2.

Algorithm 7.2: A parallel encryption method for medical images

//Input: Cipher image E (r, c)

//Output: Original medical Image O (r, c)

Step 1: Start

Step 2: Conversion of a cipher image into binary image concurrently using multiple threads.

B (r, c×8) = bin2dec (E (r, c));

Step 3: Multiple threads are utilized to boost the execution time. For each row-wise iteration one thread is created. The medical image 'O' of size 'r' uses 'r' threads and these threads run simultaneously with the help of workers available in the local cluster.

Step 4: Row-wise threads are used to renovate a binary image into DNA encoded sequences by DNA complementary rules parallelly. The DNA inverse complementary rules are chosen dynamically with help of the 4-bit LSB of the DNA encoded sequences, as depicted in Table 4.3 of Section 4.3.2 of Chapter 4.

D (r, 4×c) = reshape B (r, c×8);

Step 5: Split the diffused matrix D into D_{12} and D_{34}.

Step 6: Split the diffused matrix D_{12} and D_{34} into D_{1c}, D_{2L}, D_{3L}, and D_{4c}.

Step 7: The 4D Lorenz chaotic sequences *p, q, u,* and *v* are arranged in descending order.

$$p = [p_0, p_1, p_2, \ldots\ldots p_n];$$
$$q = [q_0, q_1, q_2, \ldots\ldots q_n];$$
$$u = [u_0, u_1, u_2, \ldots\ldots u_n];$$
$$v = [v_0, v_1, v_2, \ldots\ldots v_n];$$
$$\bar{p} = sort(p);$$
$$\bar{q} = sort(q);$$
$$\bar{u} = sort(u);$$
$$\bar{v} = sort(v);$$

Step 8: The 4D hyperchaotic sequences *x, y, z,* and *w* arranged in descending order.

$$x = [x_0, x_1, x_2, \ldots\ldots ..x_n];$$
$$y = [y_0, y_1, y_2, \ldots\ldots ..y_n];$$
$$z = [z_0, z_1, z_2, \ldots\ldots\ldots z_n];$$
$$w = [w_0, w_1, w_2, \ldots\ldots w_n];$$
$$\bar{x} = sort(x);$$
$$\bar{y} = sort(y);$$
$$\bar{z} = sort(z);$$
$$\bar{w} = sort(w);$$

Step 9: The SHA-512 is applied for four different DNA sequences namely, Canis lupus (ID MW549038.1 in GenBank), Homo sapiens (ID AJ276502.1 in GenBank), Erythrocebus patas (ID D85291.1 in GenBank) and Oryctolagus cuniculus (ID NW_001082024.1) to obtain four different hash values Hk_{d1}, Hk_{d2}, Hk_{d3}, and Hk_{d4}.

Step 10: The 4D hyperchaotic sequences *x, y, z,* and *w* are embedded with HK_1 and HK_4 using logical XOR respectively.

$$x = x \oplus HK_{d1}$$
$$y = y \oplus HK_{d1}$$
$$z = z \oplus HK_{d4}$$
$$w = w \oplus HK_{d4}$$

Step11: The position of sorted chaotic sequences $\bar{x}$ and $\bar{y}$ are referred for permutation of D_1, row-wise and column-wise respectively. Index values of

ordered sequences $\bar{z}$ and $\bar{w}$ are utilized to reshuffle the pixels of D_4, row-wise and column-wise respectively with the help of multi threads.

Step 12: The 4D Lorenz chaotic sequences *p, q, u,* and *v* are embedded with HK_{d2} and HK_{d3} using logical XOR respectively.

$$p = p \oplus HK_{d2}$$

$$q = q \oplus HK_{d2}$$

$$u = u \oplus HK_{d3}$$

$$v = v \oplus HK_{d3}$$

Step 13: The position of sorted chaotic sequences $\bar{p}$ and $\bar{q}$ are referred for permutation of D_2, row-wise and column-wise respectively. Index of ordered sequences $\bar{u}$ and $\bar{v}$ are utilized to reshuffle the pixels of D_3, row-wise and column-wise respectively with the help of multi threads.

Step 14: The chaotic sequences *x, y, z, w, p, q, u,* and *v* are converted into DNA sequences D_{xy}, D_{zw}, D_{pq}, and D_{uv} using DNA encoding rules. Dynamic selection of DNA encoding rules depends on 4-bit MSB of the chaotic sequence as depicted in Table 4.1 of Section 4.3.1 of Chapter 4.

Step 15: Diffusion operation DNA XOR is applied to diffuse the pixels of D_{1c}, D_{2L}, D_{3L}, and D_{4c} respectively.

$$D_1(r, 4\times c) = D_{1c}(r, 4\times c) \text{ DNA XOR } D_{xy}(r, 4\times c);$$

$$D_2(r, 4\times c) = D_{2L}(r, 4\times c) \text{ DNA XOR } D_{pq}(r, 4\times c);$$

$$D_3(r, 4\times c) = D_{3L}(r, 4\times c) \text{ DNA XOR } D_{uv}(r, 4\times c);$$

$$D_4(r, 4\times c) = D_{4c}(r, 4\times c) \text{ DNA XOR } D_{zw}(r, 4\times c);$$

Step 16: The DNA encoded structures are renovated as a binary image using all DNA complementary rules concurrently. The inverse of DNA encoding rules is chosen dynamically based on 2-bit MSB of the pixel of binary images. Dynamic selection of DNA inverse encoding rules is depicted in Table 4.4 of Section 4.3.2 of Chapter 4.

$$B_1(r, c\times 8) = \text{reshape } D_1(r, 4\times c);$$

$$B_2(r, c\times 8) = \text{reshape } D_2(r, 4\times c);$$

$$B_3(r, c\times 8) = \text{reshape } D_3(r, 4\times c);$$

$$B_4(r, c\times 8) = \text{reshape } D_4(r, 4\times c);$$

Step 17: The four hash keys Hk_1, Hk_2, Hk_3, and Hk_4 are extracted from four binary images. The extracted hash keys are compared with calculated hash keys Hk_{d1}, Hk_{d2}, Hk_{d3}, and Hk_{d4}. If both are same means integrity is preserved else medical image is modified during transmission.

Step 18: The four binary images are converted into sub images, row-wise using multiple threads.

$$O_1 (r, c) = \text{bin2dec} (B_1 (r, c\times 8));$$

$$O_2 (r, c) = \text{bin2dec} (B_2 (r, c\times 8));$$

$$O_3 (r, c) = \text{bin2dec} (B_3 (r, c\times 8));$$

$$O_4 (r, c) = \text{bin2dec} (B_4 (r, c\times 8));$$

Step 19: The sub images are merged and converted into decipher images concurrently using multiple threads.

Step 20: Stop

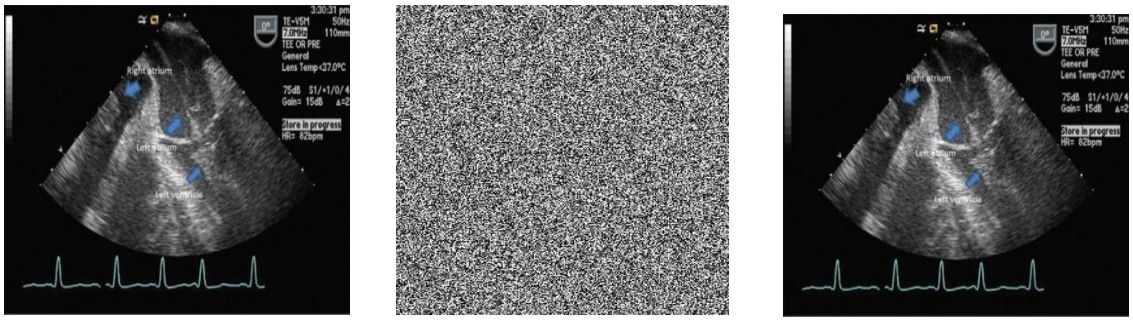
In proposed parallel DNA cryptosystem, instruction based parallel computing is used to run a set of instructions of en/decryption methods concurrently. The SHA-512 produces a fixed 512-bit hash keys for four different DNA sequences. The hash keys and DNA sequences are secret keys of first level. The original medical image is bifurcated into four sub images. The sub images are reformed as a binary image. The four hash keys are embedded into binary images. These binary images are renovated into DNA structures using all eight DNA encoded rules. DNA encoding rules are secret keys of second level. The Chen's chaotic sequences and Lorenz's chaotic sequences are used for shuffling the pixels of DNA encoded structures. These chaotic sequences are embedded with hash values. The primary values of chaotic sequences are secret keys of third level. DNA XOR (DNA rule based as a secret key in the fourth level) is used between embedded chaotic sequences and shuffled DNA encoded structures for diffusion. The diffused DNA encoded structures are renovated into cipher image using DNA complementary rules. The DNA complementary rules are secret keys of fifth level. All these instructions are run concurrently with the help of multithreads. Thus, the computation time is reduced.

7.3 Experimental Results and Discussion

The experimentation is implemented on 9th gen Intel CoreTM i7 7500U CPU using Matlab (R2020b). The inputs for parallel encryption algorithm are medical images, considered from five different categories namely, Ultrasound, MRI, X-Ray, CT, and ECG. From each category 100 medical images are collected.

In proposed parallel en/decryption method, the original medical image of size 512×512 presented in Fig.7.3(a) is divided into four equal sub images of size 256×256 namely O_1, O_2, O_3, and O_4. For each subpart parallel computation is performed by creating row-wise multiple threads. For each sub image, 256 row-wise threads are created. These multiple threads process the task simultaneously with the help of workers available in local clusters. These sub images are converted into binary images B_1, B_2, B_3, and B_4. The SHA-512 is used to obtain the four different hash keys Hk_1, Hk_2, Hk_3, and Hk_4 for four different DNA sequences of size 512 namely, Canis lupus (ID MW549038.1 in GenBank), Homo sapiens (ID AJ276502.1 in GenBank), Erythrocebus patas (ID D85291.1 in GenBank) and Oryctolagus cuniculus (ID NW_001082024.1). These hash keys are embedded into 2-bit LSB of four binary images respectively. The embedded binary images are transformed into row-wise DNA structures namely, D_1, D_2, D_3, and D_4 simultaneously using all DNA encoding rules as specified in Table 1.1 of Section 1.6 of Chapter 1. The row-wise confusion matrices D_1 and D_4, are framed using Chen's chaotic sequences specified in Eqns. (1.5.1) - (1.5.4) of Chapter 1 concurrently with the help of multithreads. We have considered x_0 =0.3, y_0=- 0.4, z_0=1.2, and w_0=1 as preliminary conditions of system factors in Chen's hyperchaotic system. The preliminary values of control factors a_1=0.3, b_1=-0.4, c_1=1.2, and d_1=1 are determined through empirical examination to generate a Chen's chaotic sequences. The confusion matrices D_2 and D_3, are formed using Lorenz chaotic sequences specified in Eqns. (1.5.8) – (1.5.11) of Chapter 1 concurrently with the help of multithreads. The initial values of state variables p_0=3.2, q_0=8.5, u_0=3.6, and v_0= 2.2 are empirically determined. The four hash keys are embedded into chaotic sequences using XOR operation. The diffusion matrix is obtained by applying DNA XOR operation between embedded chaotic sequences and confused DNA matrices. DNA decoding is performed to decode diffusion matrices into

binary images using DNA complementary rules. Further, binary images are renovated into cipher image as exhibited in Fig.7.3(b).



(a) (b) (c)

Fig.7.3 Ultrasound image samples: (a) Original ultrasound image (b) Cipher image and (c) Decipher image

In proposed parallel decryption method, the cipher image is converted as a binary form image and split into four sub images. These sub images are renovated into encoded DNA matrices with row-wise multithreads. The hashing algorithm SHA-512 is utilized for four different DNA sequences to get hash keys Hkd_1, Hkd_2, Hkd_3, and Hkd_4. These keys are embedded into Chen's chaotic sequences and Lorenz's chaotic sequences using XOR operation. The embedded sequences are renovated into DNA chaotic sequences. The diffusion matrix is obtained by applying DNA XOR between encoded DNA matrices and DNA chaotic sequences. The Chen's and Lorenz's chaotic sequences are referred for reshuffling the pixels of diffused matrices concurrently. The reshuffled encoded DNA matrices are converted into binary images using an inverse of all DNA encoding rules. The hash keys are extracted from binary image i.e., Hk_1, Hk_2, Hk_3, and Hk_4. The extracted hash values are compared with calculated hash values namely, Hkd_1, Hkd_2, Hkd_3, and Hkd_4. If both are similar, then integrity is preserved otherwise the medical image is modified during transmission. Further, the binary images are combined to get decipher image as shown in Fig.7.3(c).

7.3.1 Performance and Security Analysis

The performance of proposed parallel medical image encryption algorithm depends on resistant against various types of crypto attacks such as statistical attacks, exhaustive attacks, and differential attacks. The correlation coefficient analysis and histogram analysis are performed for attack proof against the statistical attacks. The key security and key space

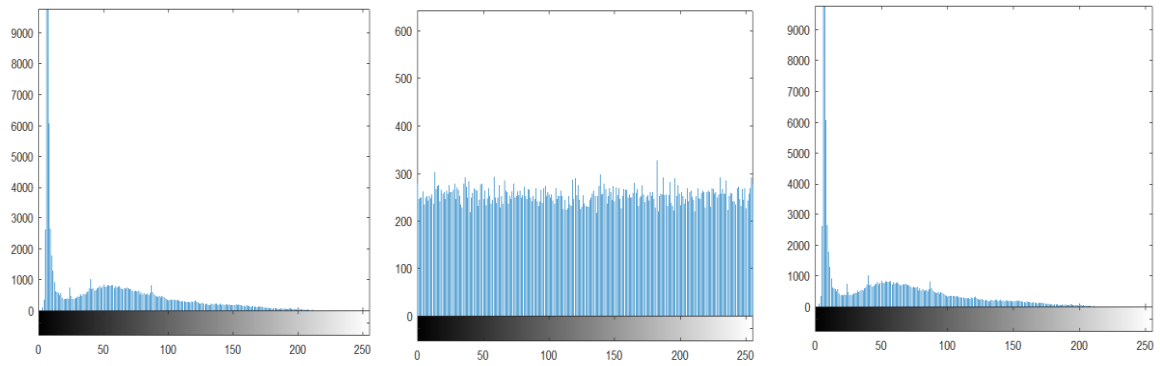
analysis are performed to verify the attack proof against exhaustive attack. The entropy, MSE, and PSNR are employed to verify the error rate of medical image.

A. Statistical Attacks

The statistical attack is accomplished to verify, whether it is possible to speculate the original medical image and secret keys by observing the encrypted image. The cryptanalysts used histogram and correlation coefficient parameters to verify statistical attacks.

Histogram Analysis

The histogram is the visual depiction of spreading of pixels intensity-level. The histogram analysis of original ultrasound image is exhibited in Fig. 7.4(a) and in Fig. 7.4(b) histogram analysis of cipher image and in Fig.7.4(c) histogram analysis of decoded ultrasound image are exhibited. From Fig. 7.4, it is observed that histogram bins are scattered uniformly in cipher image and randomly in original ultrasound image and decipher image. It proves that the parallel cryptosystem has good pseudorandom properties.



(a) (b) (c)

Fig.7.4 Histogram analysis: (a) Original ultrasound image (b) Cipher image (c) Decipher image

The uniformity of dispersal of histogram bins of cipher image is proven using chi-square test. The results of hypothesis test are exhibited in Table 7.1. From Table 7.1 it is examined that, test results are very low compared to ideal value as specified in Section 1.9.1.2 of Chapter 1. This proves the uniformity of dispersal of pixels in cipher image.

Table 7.1 Chi-square test for proposed parallel DNA cryptosystem

Medical image type	Cipher image	Hypothesis test
MR	235.0078	pass
CT	237.9219	pass
X-ray	255.7344	pass
Ultrasound	248.1016	pass
ECG	239.2813	pass

Correlation Coefficient Analysis

The correlation coefficient analysis is performed to verify the correlation among adjacent pixels of the original input medical image, encrypted image, and decipher image. The correlation coefficient of proposed parallel DNA cryptosystem is tabulated in Table 7.2.

Table 7.2 Correlation coefficient analysis of proposed parallel DNA cryptosystem

Medical image type	Direction	Cipher image	Decipher image
MR	*Horizontal*	0.0098	0.9998
	Vertical	-0.0011	0.9999
	Diagonal	-0.0015	0.9996
CT	*Horizontal*	0.0013	0.9998
	Vertical	-0.0018	0.9995
	Diagonal	0.0009	0.9994
X-ray	*Horizontal*	0.0008	0.9999
	Vertical	-0.0005	0.9998
	Diagonal	-0.0008	0.9999
Ultrasound	*Horizontal*	0.0009	0.9998
	Vertical	-0.0001	0.9995
	Diagonal	-0.0007	0.9996
ECG	*Horizontal*	0.0008	0.9994
	Vertical	-0.0006	0.9998
	Diagonal	-0.0007	0.9995
Average :		**0.00005**	**0.99962**

The visual representation of correlation coefficient among contiguous pixels of original medical image and cipher images in three different directions namely, horizontal, vertical, and diagonal are depicted in Fig. 7.5. From Fig.7.5 (a and b and c), it is observed that pixels are linearly related in an original medical image, and pixels are not linearly related in cipher image as exhibited in Fig. 7.5 (d and e and f). This proves that pixels are totally modified in cipher image.

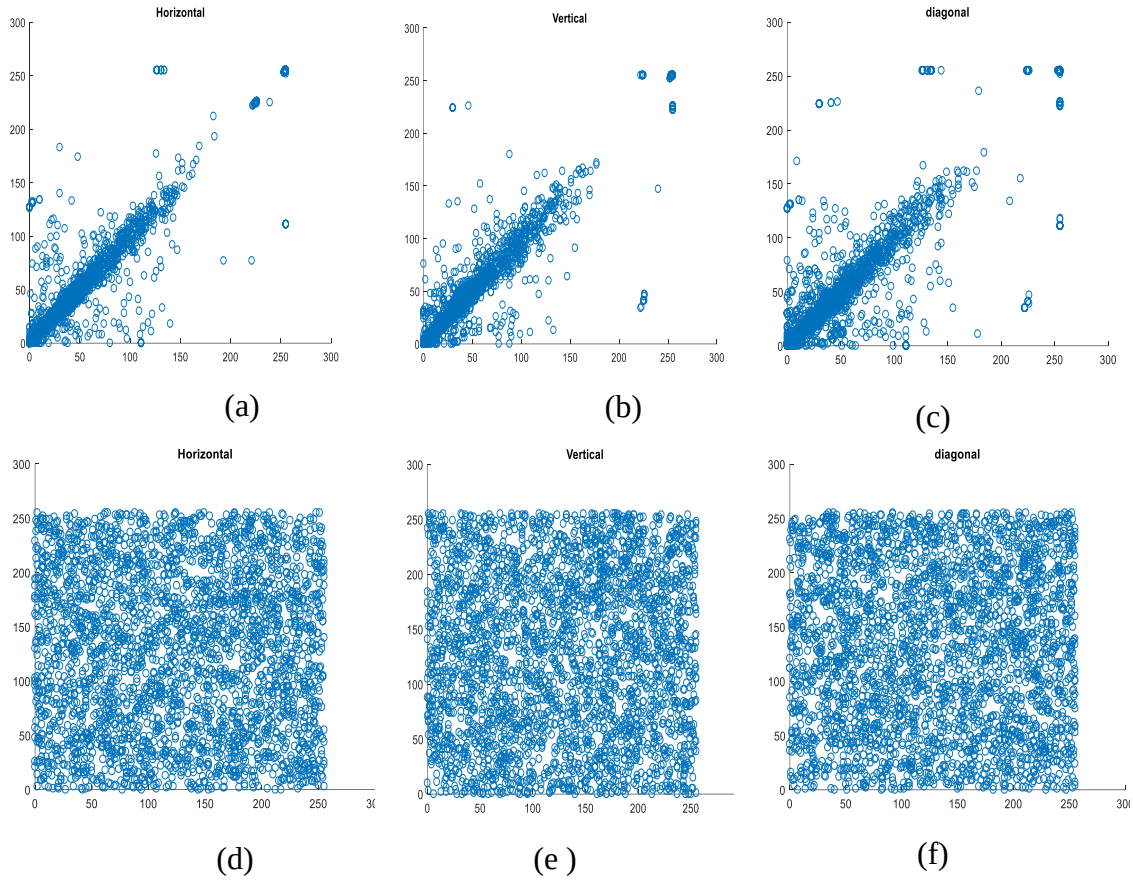


Fig. 7.5 Scatter plot of original ultrasound image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

B. Exhaustive Attacks

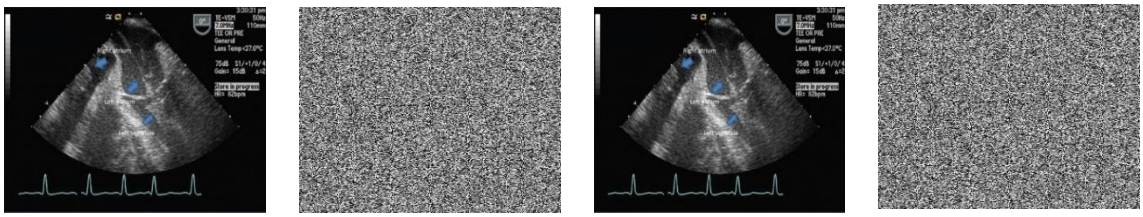
The exhaustive attack is performed to enumerate all possible secret keys and try to get decipher images with these secret keys. The key space and key sensitivity metrics are utilized by the cryptanalyst to prove resistant against exhaustive attack.

Key Space Analysis

In proposed parallel cryptosystem, secret keys are the preliminary values of state factors of 4D Chen's chaotic sequence and 4D Lorenz chaotic sequences. A total of eight secret keys (x_0, y_0, z_0, w_0, p_0, q_0, u_0, and v_0) are utilized. Then, size of eight secret keys is $(10^{15})^8 \approx 2^{400}$. The four DNA sequences and four hash keys, each of size 512 ($(2^9)^8$) are also secret keys. The key space is 2^{472} and it is very huge. Therefore, the proposed method is suitable for the enhancement of security for medical image.

Key Sensitivity Analysis

The decryption of cipher image into original medical image depends on decryption algorithm and secret keys. In parallel cryptosystem, the preliminary values of eight state factors of chaotic sequences and four DNA sequences are secret keys. Among eight secret keys any one keys initial values if modified with very minor variance then decrypting the original medical image is highly impossible. For example, among eight secret keys, if one secret key value z_0=1.2 is modified as z_0=1.200001 then getting decipher image is highly impossible. The original medical image as depicted in Fig.7.6(a), cipher image as depicted in Fig.7.6(b), decipher image decrypted with correct key value z0=1.2 as shown in Fig.7.6(c), and decipher image decrypted with incorrect key value z0=1.200001 as depicted in Fig.7.6(d).



(a) (b) (c) (d)

Fig.7.6 Key sensitivity analysis: (a) Original MR image (b) Cipher image (c) Decipher image with correct initial value of secret key z_0=1.2 (d) Decipher image with an incorrect secret key as z_0=1.200001

From Fig.7.6 ((c) & (d)), it is observed that decrypting the original medical image with a small variance in one secret key is also not possible. Hence, the proposed parallel en/decryption technique is sensitive to the initial values of secret keys.

C. Differential Attacks

The cryptanalyst used UACI and NPCR metrics to analyze the differential attack. The performance analysis of parallel medical image encryption algorithm is tabulated in Table 7.3. The value of NPCR is nearly close to ideal value i.e. 99.997 and UACI is 38.72. It proves that proposed parallel cryptosystem is sensitive to original medical image. The entropy value is 7.9997 close to ideal value of 8.0. This demonstrates that the quality of a multilevel parallel cryptosystem is adequate. The value of MSE is approximately 6.14312e+04 and value of PSNR is 4.07922dB. Which evidences that the superiority of a medical image is preserved. The security analysis revealed that the proposed parallel en/decryption method is appropriate to offer high-level security for medical images.

Table 7.3 Performance analysis of proposed parallel DNA cryptosystem

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.998	39.87	7.9999	5.9987e+04	3.4567
CT	99.997	35.79	7.9998	6.8528e+04	5.0100
X-ray	99.999	39.98	7.9999	5.9678e+04	4.0340
Ultrasound	99.995	39.96	7.9989	5.9987e+04	3.8998
ECG	99.996	37.99	7.9999	5.8976e+04	3.9956
Average :	**99.997**	**38.72**	**7.9997**	**6.14312e+04**	**4.07922**

7.3.2 Computation Time of Proposed Parallel En/Decryption Algorithm

The medical images are very large in volume, pixels are highly correlated and contain very sensitive disease related information. The security requirement for a medical image is different from a plain image. To accomplish this requirement, a high-level security is essential. The computational cost to offer enhanced high-level security is very high. This is one of the drawbacks for online communication. Thus, to overcome from this problem, instead of sequential computation, a parallel computation is performed in a proposed cryptosystem for the reduction of time and to enhance the security of the medical images.

The computation time of proposedparallel medical image en/decryption for a medical image of size (m×n) is calculated as follows:

Step 1: Hash value for DNA sequence: 4m

Step 2: Binary conversion of original medical image: (m×n)/4

Step 3: Construction of DNA structure: (m×n)/4

Step 4: Permutation process: (m×n)/4

Step 5: Diffusion process: (m×n)/4

Step 6: DNA decoding: (m×n)/4

Step 7: Generating cipher image: (m×n)

Total time complexity of the proposed method is given below:

$T(n)= 4m+[(m\times n)/4 + (m\times n)/4 + (m\times n)/4 + (m\times n)/4 + (m\times n)/4+ (m\times n)]$

$= 5(mn) /4+mn+4m$

If m=n then it is $O((5n^2 /4)+n^2+4n)$

Table 7.4 Comparison of time complexity for sequential and parallel approach of proposed parallel DNA cryptosystem

Medical image type	Sequential computation time (Seconds)		Parallel computation time (Seconds)	
	Cipher image	Decipher image	Cipher image	Decipher image
MR	42.68	42.06	0.16	0.17
CT	41.09	40.98	0.12	0.13
X-ray	40.03	39.25	0.15	0.17
Ultrasound	39.48	39.03	0.09	0.14
ECG	43.73	44.15	0.19	0.25
Average :	**41.402**	**41.094**	**0.142**	**0.172**

In parallel computation, the four sub images are encrypted concurrently. Hence, time complexity is O $((5n^2/4)+n^2+4n)$. The proposed parallel encryption offers enhanced high-level security for medical images with reduced time. The comparison of time complexity of sequential and parallel computation of parallel encryption method is shown in Table 7.4.

The graphical representation of computation time for sequential and parallel encryption approaches are shown in Fig.7.7. From Fig.7.7, it is proved that the parallel computation mode for encryption of medical image reduces time complexity drastically as compared to sequential computation mode.

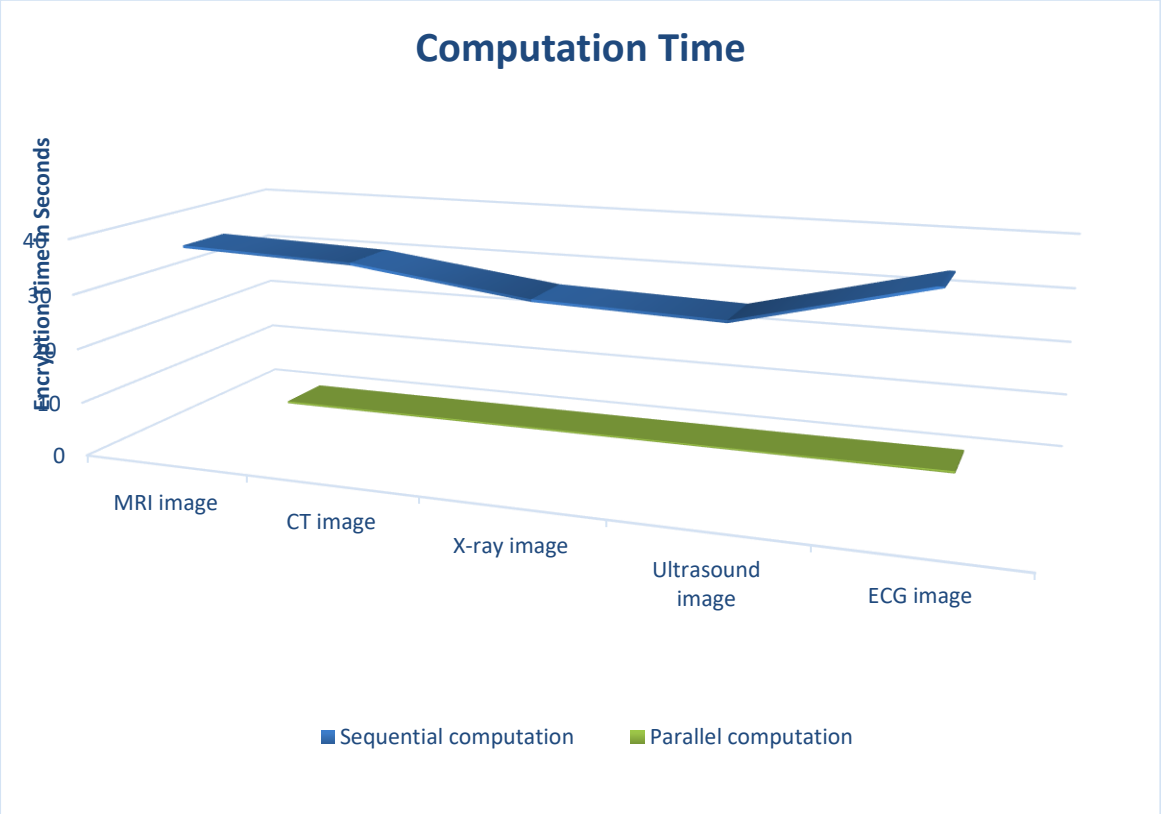


Fig.7.7. Comparison of computation time for sequential and parallel approach of proposed DNA cryptosystem

7.3.3 Comparative Analysis

The proposed parallel cryptosystem is compared with existing methods. From Table 7.5, it is proved that performance parameter values are improved than existing methods, and the time is also reduced.

Table 7.5 Comparative analysis of proposed parallel DNA cryptosystem

Method	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	Key Space	Encryption time (seconds)
Tanveer et al.,2021	7.9973	99.61	33.43	---	---	0.2525
Massod et al.,2021	7.9995	99.62	33.63	7.74	2^{300}	1.53
DNA cryptosystem for compressed medical image (Chapter 6)	7.99968	99.663	33.1	4.34086	2^{400}	27.19
Proposed Parallel en/decryption	**7.9997**	**99.667**	**33.42**	**4.07922**	**2^{472}**	**0.09**

The comparative analysis based on performance metrics proves that proposed parallel DNA cryptosystem is appropriate to offer higher-level security for medical images as shown in Fig.7.8.

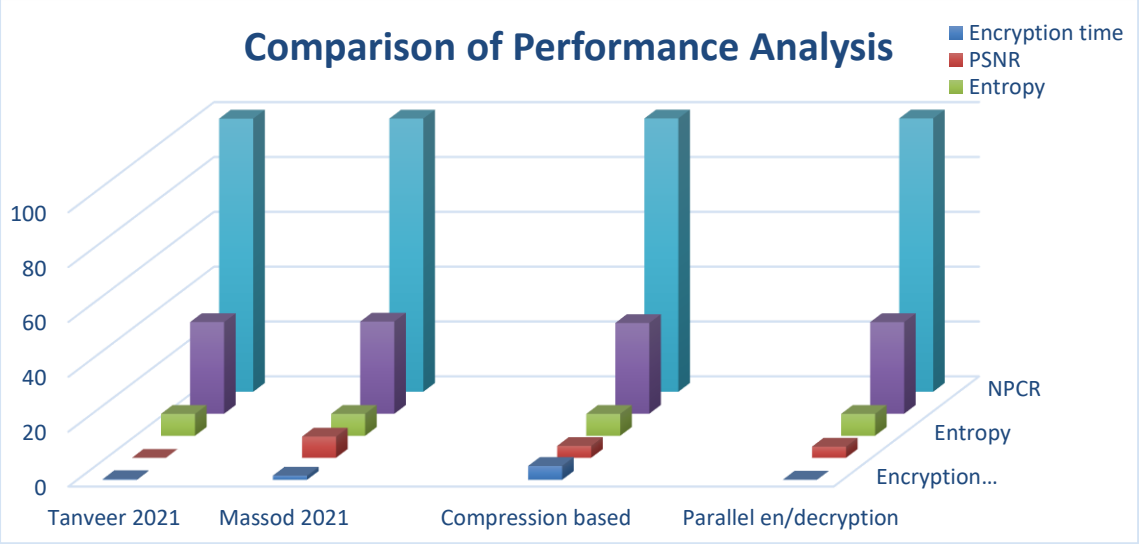


Fig.7.8. Comparison of performance analysis of proposed parallel DNA cryptosystem with existing methods

The comparison of computation time of proposed parallel DNA cryptosystem with method of (Shanshan,2021) is shown in Fig.7.9.

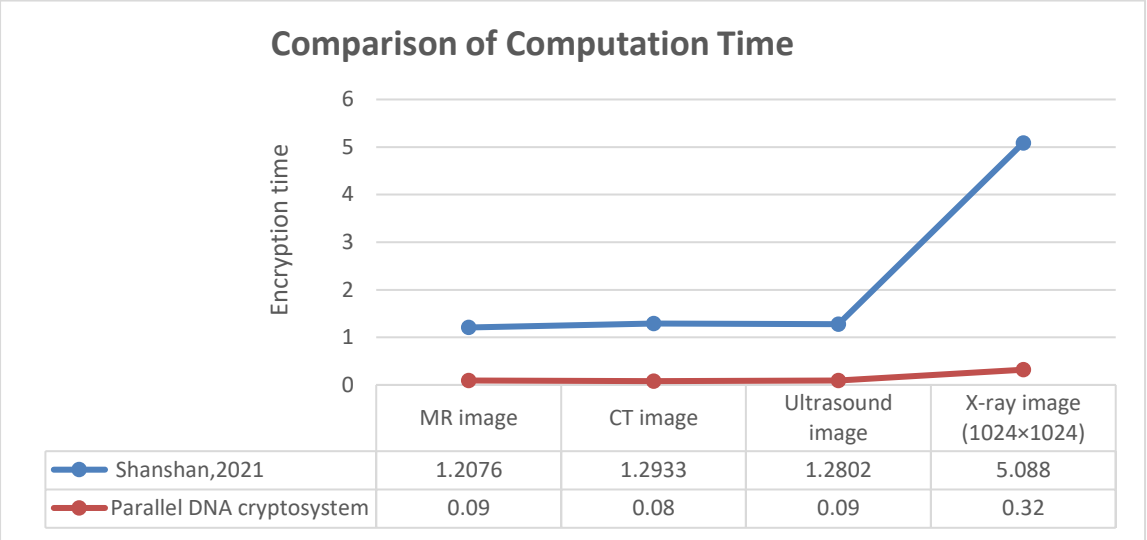


Fig.7.9. Comparison of computation time of proposed parallel DNA cryptosystem with Shanshan method

The comparison results are tabularized in Table 7.6. The comparative analysis demonstrates that proposed parallel DNA cryptosystem is optimal to offer enhanced high-level security for medical image with reduced computation time. The key space is also very huge compared to other methods.

Table 7.6 Comparison of computation time of proposed parallel DNA cryptosystem

Medical image type (512×512)	Shanshan,2021 Computation time (seconds)		**Proposed Parallel DNA cryptosystem Computation time (seconds)**	
	Cipher image	Decipher image	Cipher image	Decipher image
MR	1.2076	1.0865	**0.09**	**0.10**
CT	1.2933	1.1230	**0.08**	**0.10**
X-ray (1024×1024)	5.0880	4.4282	**0.32**	**0.33**
Ultrasound	1.2802	1.1032	**0.09**	**0.08**

The proposed parallel en/decryption technique is compared with previous en/decryption methods discussed in previous chapters as shown in Table 7.7. From Table 7.7, it is proved that performance analysis of proposed parallel method is

improved than previous methods. Hence, proposed parallel DNA cryptosystem is suitable to offer enhanced high-level security with reduced computation time for medical images.

Table 7.7 Comparison of performance analysis of proposed parallel method with previous Chapters methods

Performance Metrics	Biological and Logical (Chapter 2)	Intensity based (Chapter 3)	Integrity and confidentiality (Chapter 4)	Selective (Chapter 5)	Compression (Chapter 6)	**Parallel DNA crypto System**
Entropy	7.99214	7.99738	7.99936	7.542	7.99968	**7.9997**
NPCR (%)	99.64	99.64974	99.6626	99.468	99.6628	**99.667**
UACI (%)	33.61	33.56	33.906	33.548	33.1	**33.42**
PSNR (dB)	6.84372	5.9322	5.4954	5.72	4.34086	**4.07922**
MSE	1.7295e+03	5.2079e+03	5.1783e+04	7.3913e+02	6.6990e+04	**6.14312e+04**
Key Space	2^{268}	2^{400}	2^{418}	2^{250}	2^{400}	**2^{472}**
Encryption Time (Seconds)	26.026	41.39	34.98	2.698	27.19	**0.142**

7.4 Summary

This Chapter describes the parallel en/decryption technique for medical images. The original medical image is split into four sub images. To run each sub image simultaneously multithreads are created and assigned to multi workers available in local clusters. The multi threads are used for row-wise conversion of original medical image into binary images. The SHA-512 is employed to produce four hash keys for four different DNA sequences. Each hash key is embedded into 2-bit LSB of each binary sub image. The binary images are converted into DNA structures using DNA coding rules. DNA structures are converted into a confusion matrix using multiple

high-dimensional chaotic sequences. The hash keys are embedded into chaotic sequences using logical XOR operation. DNA structures are diffused into diffusion matrices in multilayers using diffusion operation DNA XOR. These diffusion matrices are decoded by DNA complementary rules and converted into a binary matrix to acquire a cipher image. The experimental results and cryptanalysis proved that proposed parallel DNA cryptosystem is invulnerable to statistical, exhaustive, and differential attacks. The proposed parallel DNA cryptosystem provides enhanced higher-level security for medical images with reduced computation time, due to parallel computation. The hash keys are used to enforce integrity. The four different DNA sequences are utilized to offer confidentiality for medical images. So, the proposed parallel DNA cryptosystem is suitable for an online virtual consultation, e-health systems, and telemedicine applications without sacrificing the security and quality of medical images and ensures the integrity and confidentiality of patient records.

Chapter 8

Conclusions and Future Scope

Medical images play a vital role in the diagnosis of exact diseases in online virtual consultation, e-health systems, and telemedicine applications. The security of medical images is very significant, and integrity and confidentiality are also incredibly essential. This research work attempts to provide the effective en/decryption methods to secure medical images with integrity and confidentiality using a high dimensional chaos map and DNA cryptography. The contributions made through this research work are concluded and the scope for future work is given in this chapter.

8.1 Conclusions

The advancement in digital communication and effortless accessibility of internet facilities have encouraged remote access to medical services. These services depend on medical images for treatment. These images are communicated through an open source network. The attackers can modify or discard some part of medical images. The minor variation in medical images causes a major problem. Then, diagnosing the exact disease from modified medical images is not possible. Thus, integrity and confidentiality are also necessary for medical images. Several encryption methods are available for plain images, but these methods are not enough for medical images. The medical images carry a disease related sensitive information. The overall process of implementation involves, providing high-level security, confidentiality, and enforcing the integrity for medical images and reducing the computation time.

In the Chapter 1, the introduction to the topic of research is presented. In the Chapter 2, random key generator generates a key image. The key image and medical image are transformed into encoded DNA matrices. These matrix pixels are scrambled with Chen's chaotic sequence. The DNA XOR operation combines both scrambled DNA encoded matrices. The diffused matrix is renovated into a binary image by DNA decoding rules. The binary image is transformed into a cipher image. In this proposed DNA cryptosystem, multilevel security is provided for medical images. The key space

is inadequate due to a single chaotic system and additional memory space is required to store key image and fixed DNA coding and decoding rule are used.

To overcome from these drawbacks in Chapter 3, original medical image is fragmented into odd image and even image based on intensity levels. Both images are converted into encoded DNA matrices using a fixed DNA encoding rule among eight rules. The combination of Chen's chaotic map and Lorenz's chaotic maps are referred for the permutation and diffusion process. DNA ADD operation is applied for the diffusion of encoded DNA matrices. The diffused and confused encoded DNA matrices are combined. Finally, the merged matrix is renovated into a cipher image using DNA decoding rule. In this en/decryption method, multilevel security with multiple keys on each level is proposed to offer high-level security for medical images. Additional memory space is required for odd and even images and fixed DNA coding and decoding rule are used. The DNA ADD operation is irreversible. Hence, in the decryption method DNA SUB operation is used in place of DNA ADD operation. It is time consuming and integrity is not verified.

To enforce integrity for medical images SHA-256 and SHA-512 are used in Chapter 4. The original medical image is segmented into two equal sub images. The encoded DNA matrices are constructed for both sub images using a dynamic selection of all eight DNA encoding rules. The dynamic selection of rules depends on binary bits of sub images. The Chen's and Lorenz chaotic sequences are referred for the permutation of encoded DNA matrices. The pixels of encoded DNA matrices are diffused using DNA ADD. The diffused DNA matrices are merged and transformed into cipher using all eight DNA complementary rules. The dynamic selection of DNA complementary rules depends on the two LSB bits of DNA encoded matrices. In this DNA cryptosystem, multilevel security with multiple keys on each level is proposed to enhance the security of medical images. The hash function SHA-512 is used for integrity and the DNA sequence of Canis lupus is used for confidentiality. The DNA ADD operation is irreversible. Therefore, in decryption method DNA SUB operation is used in place of DNA ADD operation. The computation time of this method is high.

To reduce the computation time of en/decryption method in Chapter 5, the original medical is bifurcated into two regions namely, the selected pixel region and the non-

selected pixel region. Both regions are converted into encoded DNA matrices using index based dynamic selection of DNA encoding rules. The dual hyperchaotic sequences are referred for the permutation of DNA encoded selected pixel region. The DNA XOR operation diffuses the pixels of DNA encoded non-selected pixel region. Both confused and diffused regions are combined and renovated into cipher using a dynamic selection of DNA complementary rules. In this proposed en/decryption method computation time is reduced but compromised in security.

In Chapter 6, original medical image is compressed using DHWT. The compressed medical image is decomposed into four equal sub images. These sub images are converted into encoded DNA matrices by binary bit-based dynamic DNA encoding rules. The 4D Chen's and Lorenz chaotic sequences are referred to shuffle the pixels of DNA encoded matrices. DNA XOR is employed for the diffusion of DNA encoded matrices. The dynamic DNA complementary rules are employed to attain the cipher image. In this en/decryption method the memory space is reduced and multilevel security with multiple keys on each level is proposed. The computation time is reduced but the algorithm is compromised in medical image quality.

All these multilevel en/decryption methods are executed sequential. In sequential computation, to accomplish the enhanced high-level security for medical images requires more time.

To reduce the computation time without compromising security and quality of medical images, parallel computation is proposed in Chapter 7. The instruction level parallel computation is performed with multithreads. The original medical image is bifurcated into four equal sub images. These sub images are renovated into encoded DNA matrices using binary bit-based dynamic DNA encoding rules. The hash function SHA-512 is applied for four different DNA sequences namely Canis lupus, Homo sapiens, Erythrocebus patas, and Oryctolagus cuniculus to get four different hash keys respectively. These keys are embedded in 4D Chen's and Lorenz's chaotic sequences using logical XOR operations. First two sequences of 4D Chen's chaotic sequence are referred for the permutation of first sub image, and the remaining two sequences for the permutation of fourth sub image. First two sequences of 4D Lorenz's chaotic sequence are referred for the permutation of second sub image, and the remaining two

sequences for permutation of third sub image. The encoded DNA matrices are diffused by DNA XOR. The dynamic DNA complementary rules are employed to get a cipher image. In this parallel DNA cryptosystem, multilevel security with multiple keys at each level is proposed to provide enhanced high-level security. The SHA-512 is used to enforce integrity and four different DNA sequences are utilized to prove confidentiality. The instruction level parallel computation helps to reduce computation time.

Overall, significant contributions of the present research study are the following:

- Multilevel medical image encryption methods based on multiple high dimensional chaotic maps namely, 4D Chen's chaotic map,3D Lorenz chaotic map, 4D Lorenz chaotic map, DNA operations namely, DNA encoding rules, DNA complementary rules, DNA ADD, DNA SUB and DNA XOR are implemented to provide high-level security.
- In multiple cryptosystems, for each level different secret keys are used. Namely, the DNA sequences, multiple 4D chaotic map initial values, DNA encoding rules, DNA rule-based DNA XOR, DNA ADD, DNA SUB operations, DNA complementary rules, and division of medical image, are secret keys used to enhance the key strength.
- The robust DNA cryptosystem to offer security, authenticity, integrity and confidentiality for e-health system. To enforce integrity, the hash functions SHA-256 and SHA-512 are used. For confidentiality and authenticity purposes different DNA sequences are utilized. The performance parameters histogram analysis, chi-square test, correlation coefficient, key space analysis, key sensitivity analysis, NPCR, UACI, MSE, PSNR and entropy are used to validate the resistant of cryptosystems against different types of crypto attacks.
- The DNA cryptosystem model is developed for compressed medical images using discrete Haar wavelet transform to reduce the space and time requirement.
- An efficient parallel cryptosystem with high dimensional multiple chaotic maps, dynamic binary bit-based selection of DNA encoding and DNA complementary rules and DNA XOR diffusion operations to provide enhanced

high-level security for medical images. The reduction in computation time is achieved using parallel computation approach.

- For user friendly easy to use purpose a graphical user interface-based DNA cryptosystem is developed. It is useful for secure e-Health services. For example, the GUI for the proposed method based on parallel approach is presented in the Chapter 7. The details are discussed in Appendix III.

It is found that high dimensional multiple chaotic maps have good confusion properties and are very sensitive to initial conditions. Hence, resist exhaustive attack and hash function SHA-512 enhance the security level with integrity. The binary bit-based dynamic DNA encoding rules and DNA complementary rules have a higher degree of uniqueness property. The parallel computation approach is suitable for real-time applications like telemedicine and e-health system for faster communication in a secure manner.

8.2 Future Scope

The research outcomes from this work have unveiled several research directions, which have scope for further studies. For instance, key generators for chaotic map and DNA operations can be accomplished with the help of recently established metaheuristic approaches, deep learning, machine learning, and deep transfer learning. The implementation of encryption techniques for multispectral medical images is still an emergent area. Hence, the development of high-dimensional hyperchaotic systems to support such kinds of multidimensional multispectral images is a future requirement. To enhance further security, the combination of encryption with steganography also has become another research direction.

Future studies would emphasize the use of DNA computing parallelism and large storage in medical image encryption to swiftly encrypt numerous color images and even videos while ensuring security. It also focuses on the development of compressive sensing based medical image encryption techniques to reduce storage space.

Appendix I

Medical Image Datasets

The medical imaging techniques such as MRI, CT, or Ultrasound are important tools used by medical experts for quick and accurate diagnosis of various diseases. Medical images are very important for disease diagnosis, treatments, and research. Hence, medical images act as the key component of patient records in electronic form. Totally, 500 medical images of five different kinds are used for the study. The five different kinds of medical images are CT, Ultrasound, X-Ray, MRI, and ECG images. From each type 100 medical images are collected is tabulated in Table AI.1. The Ultrasound, MRI, X-Ray, and CT images are benchmark dataset gathered from "National Library of Medicine's Open Access Biomedical Images Search Engine", the website link is https://openi.nlm.nih.gov. The ECG images are accumulated from a freely available website such as http://ecg-educator.blogspot.com and stored in the dataset.

Table AI.1 Medical images datasets

Medical image type	Number of images
CT	100
MR	100
Ultrasound	100
X-ray	100
ECG	100
Total number of images	**500**

CT Images:

The 100 sample CT images are shown in the Fig. AI.1.

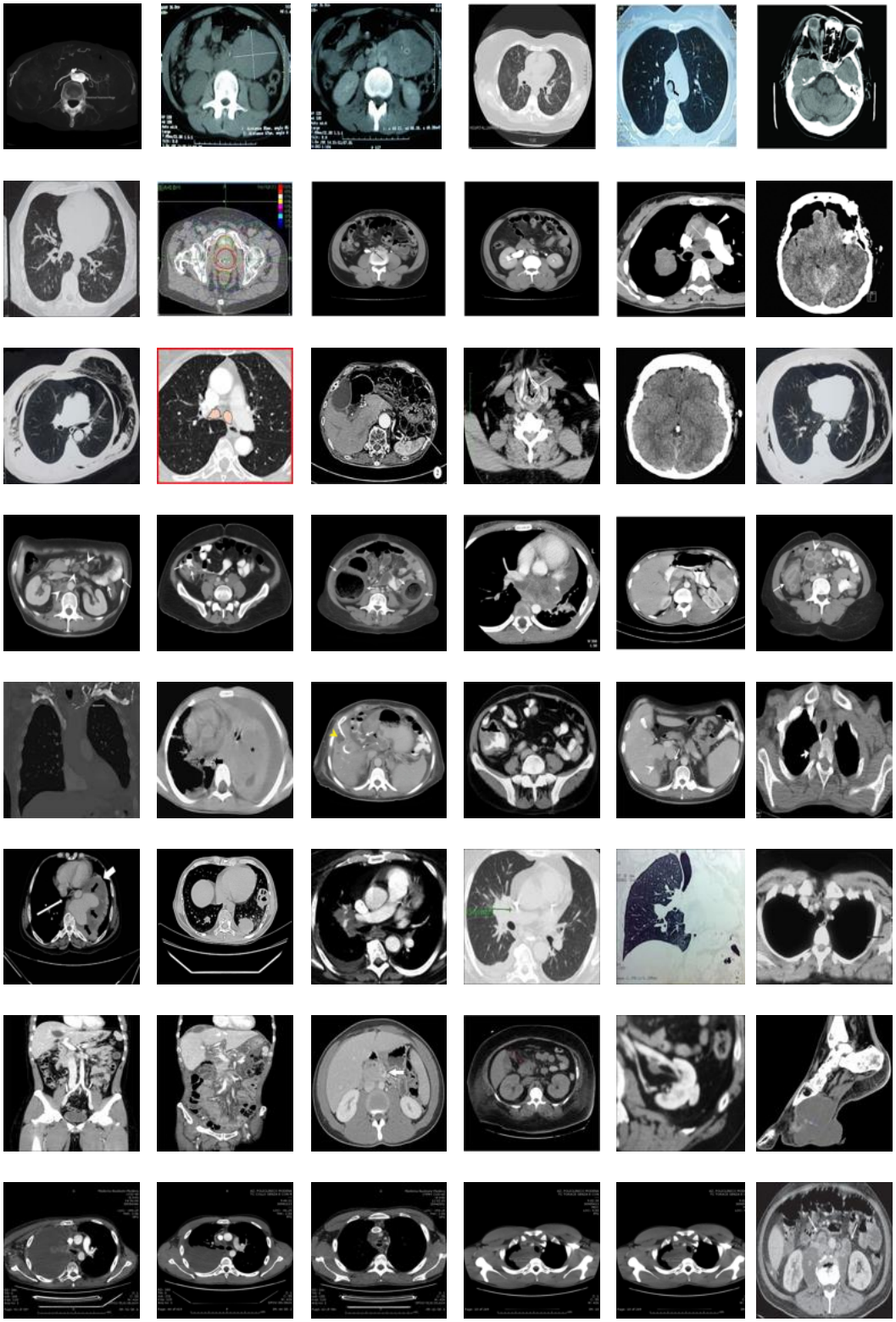
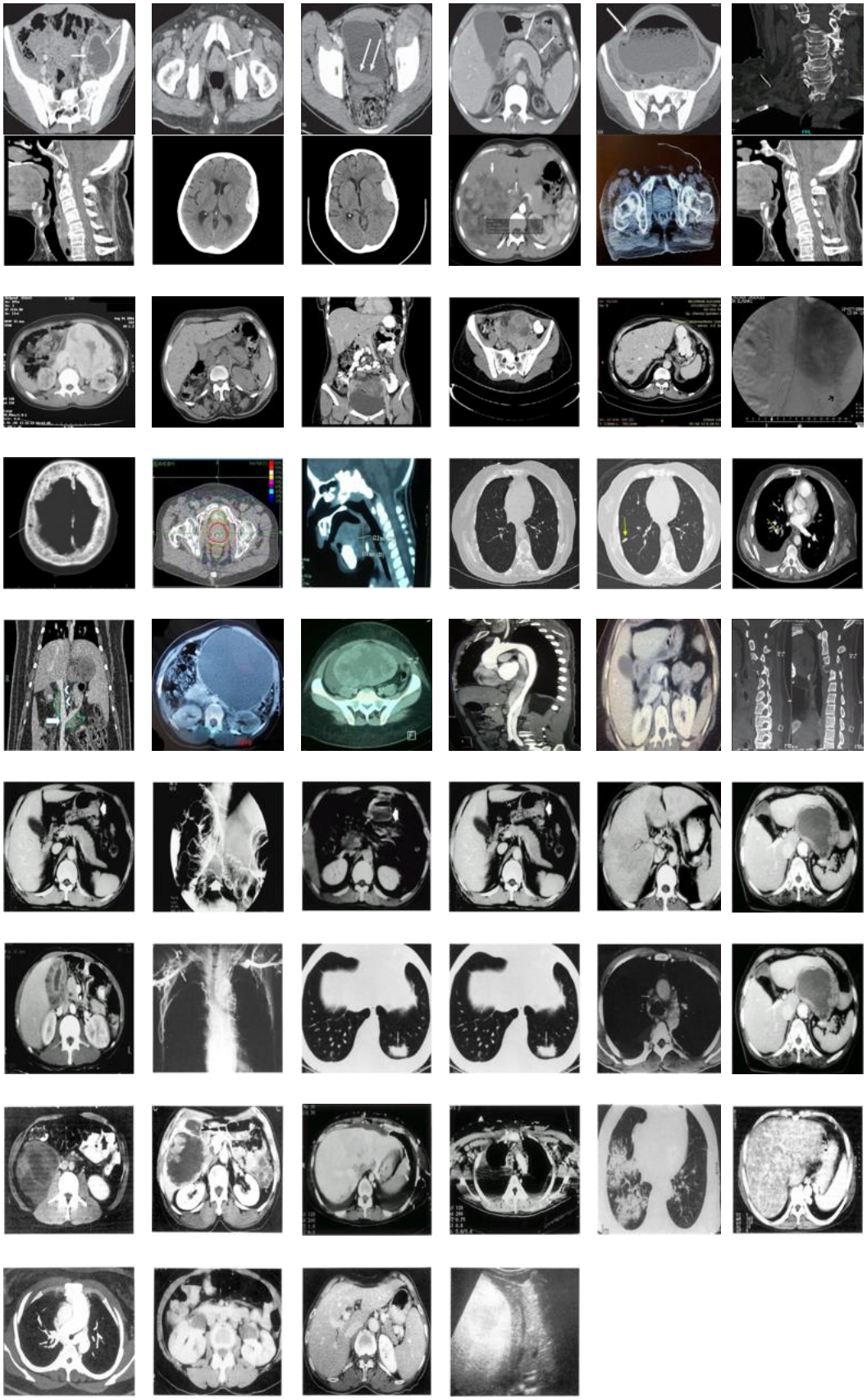


Fig. AI.1 Sample CT Images



Contd.., Fig. AI.1 Sample CT Images

MR Images:

The 100 sample MR images are shown in the Fig. AI.2.

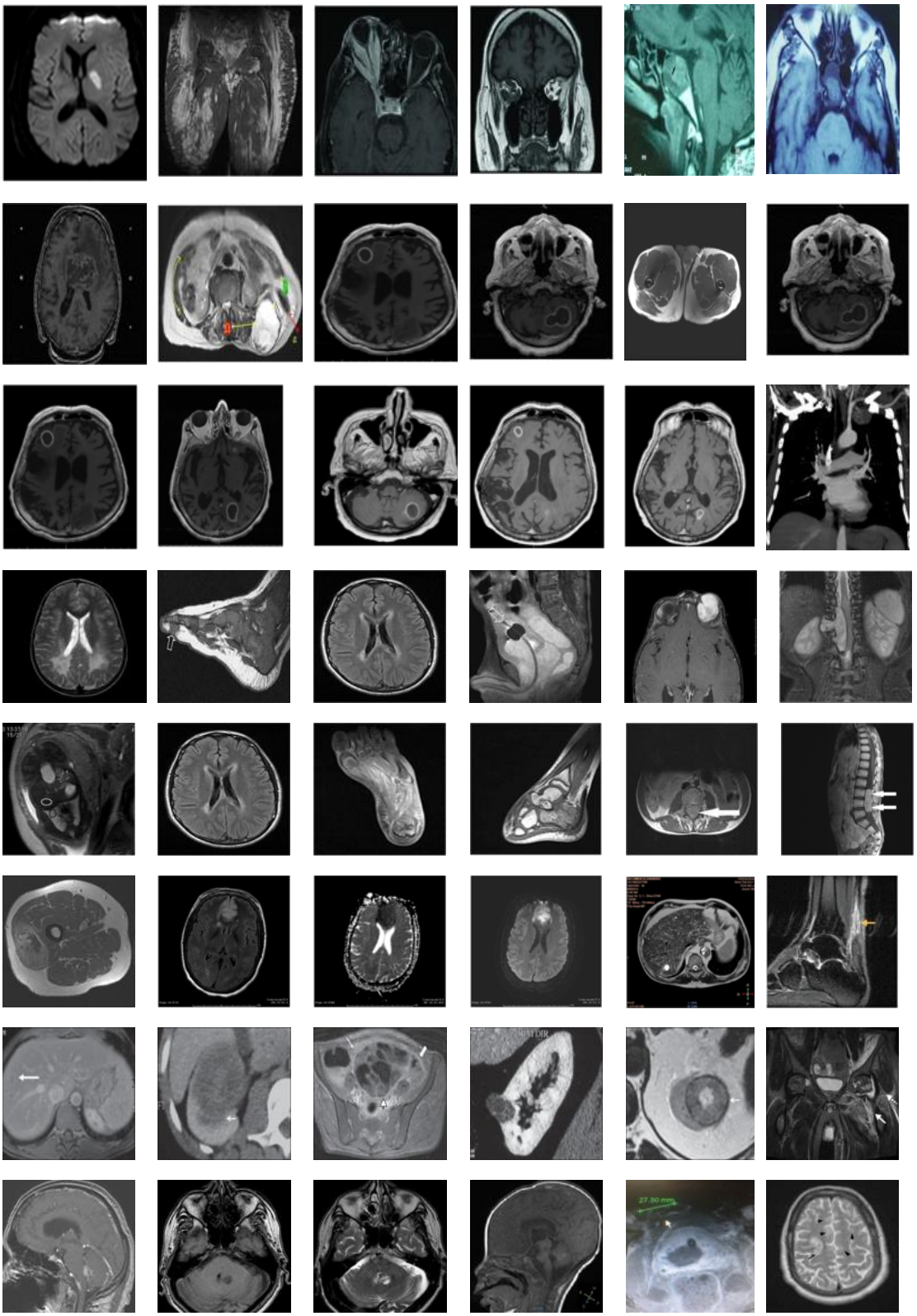
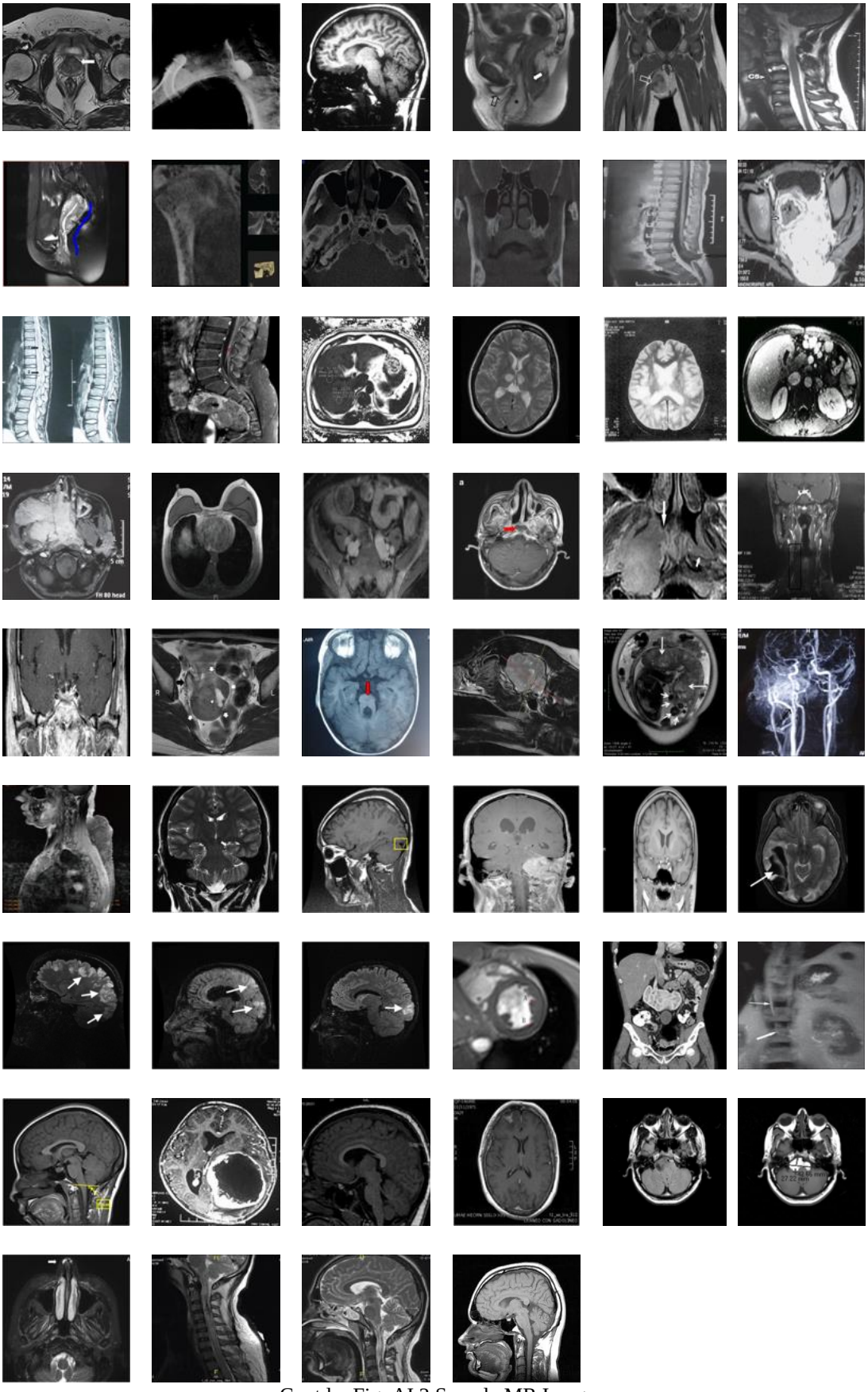


Fig. AI.2 Sample MR Images



Contd.., Fig. AI.2 Sample MR Images

Ultrasound Images:

The 100 sample Ultrasound images are shown in the Fig. AI.3.

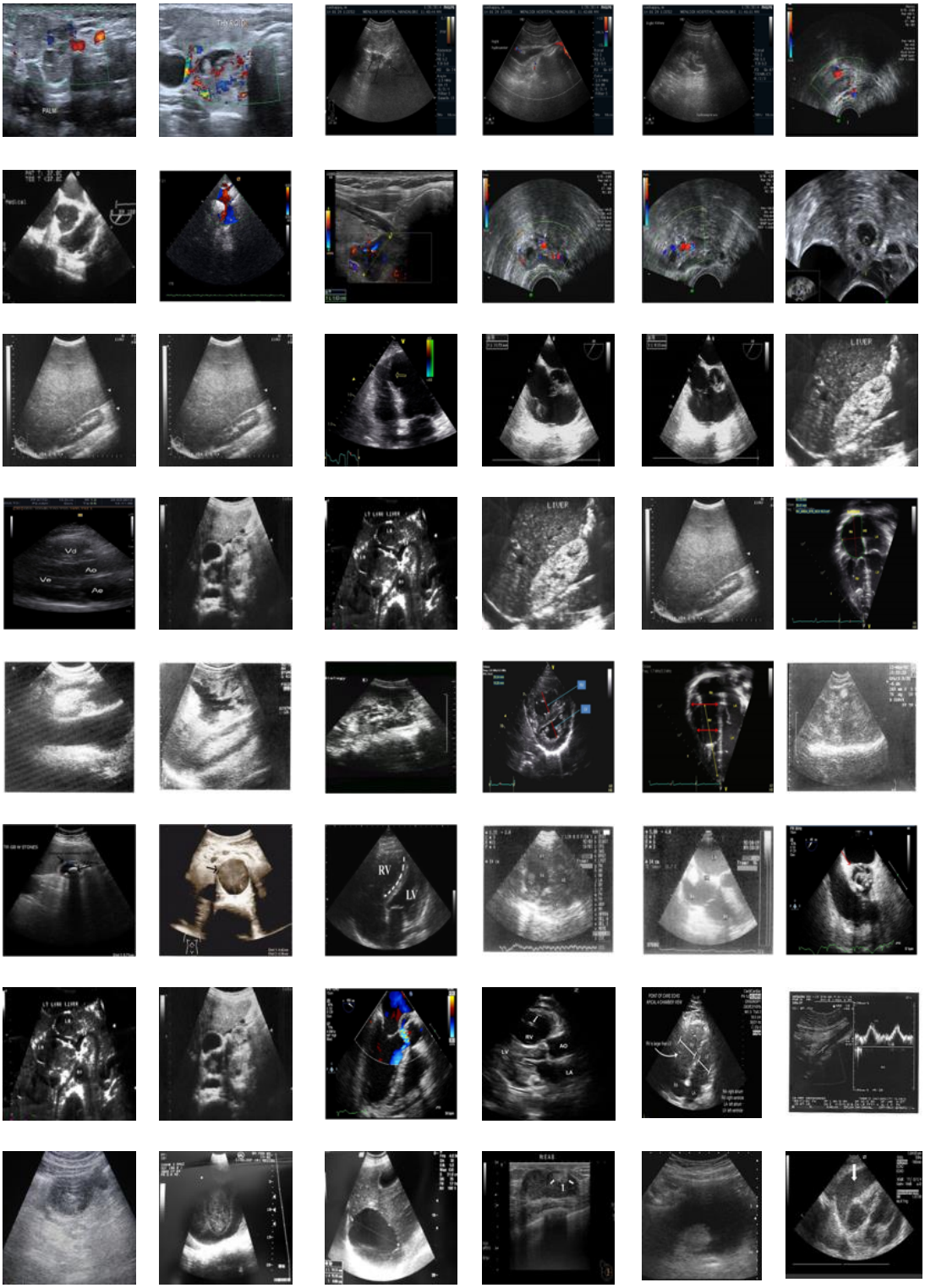
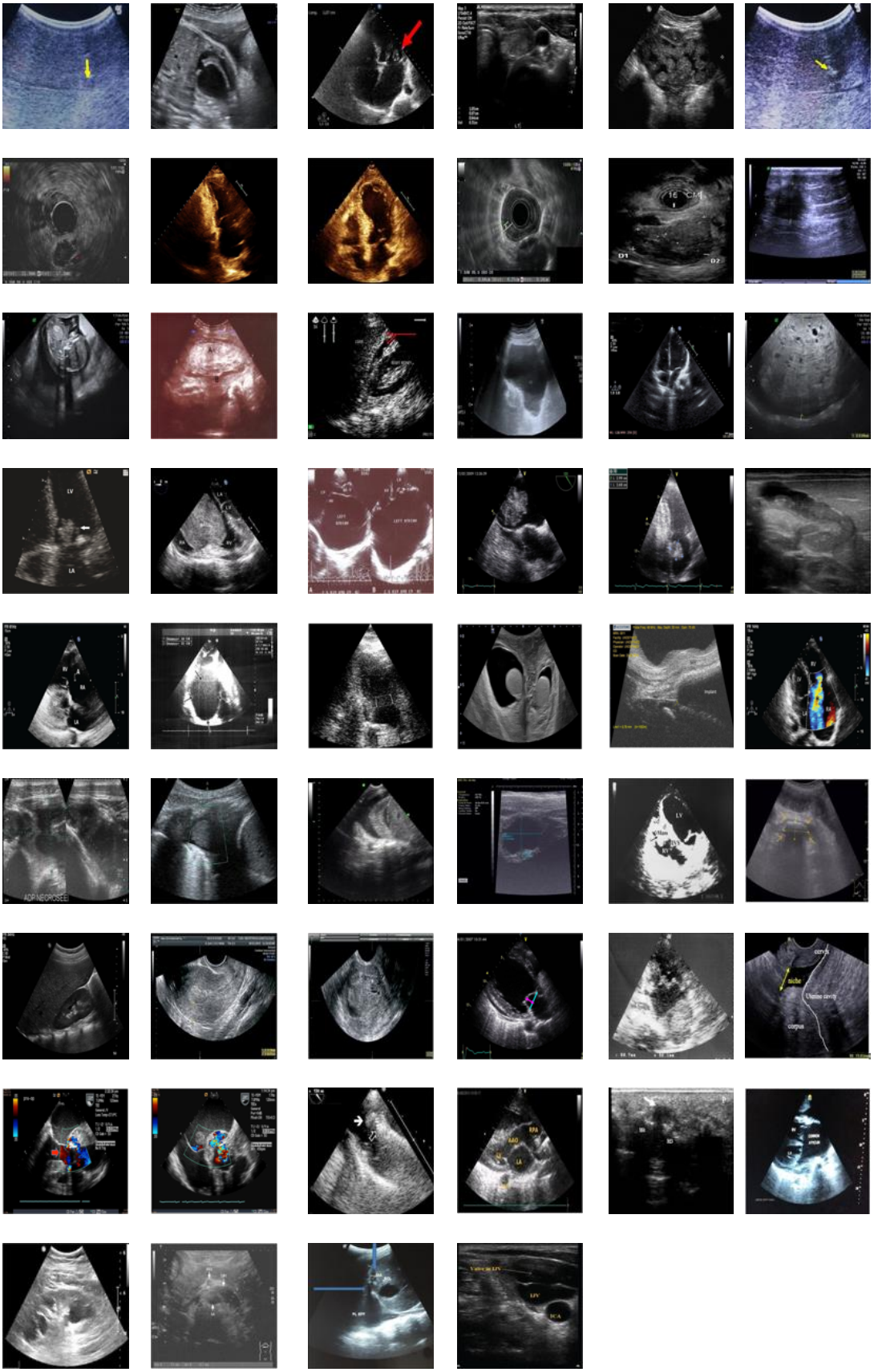


Fig. AI.3 Sample Ultrasound Images



Contd.., Fig. AI.3 Sample Ultrasound Images

X-ray Images:

The 100 sample X-ray images are shown in the Fig. AI.4.

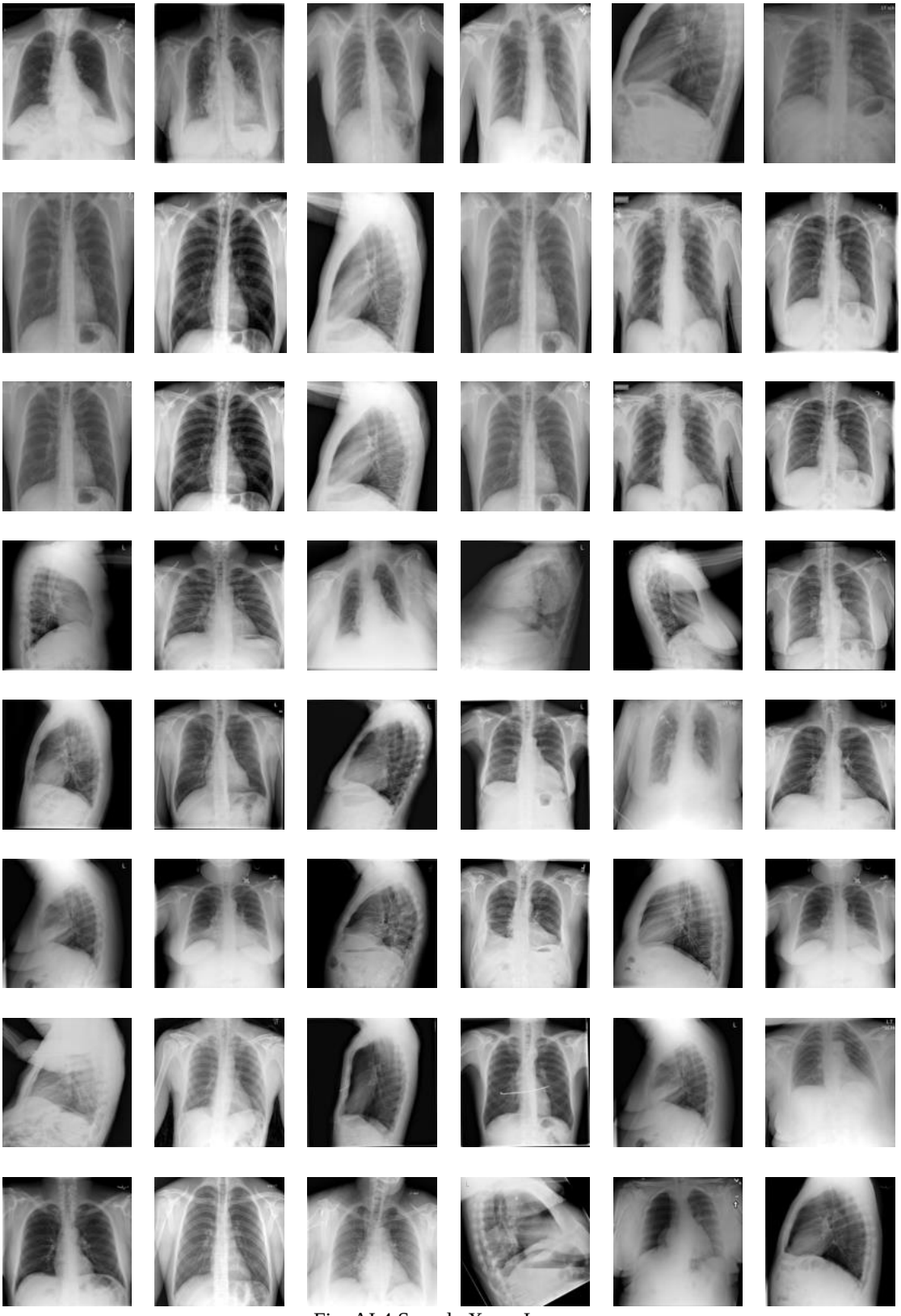
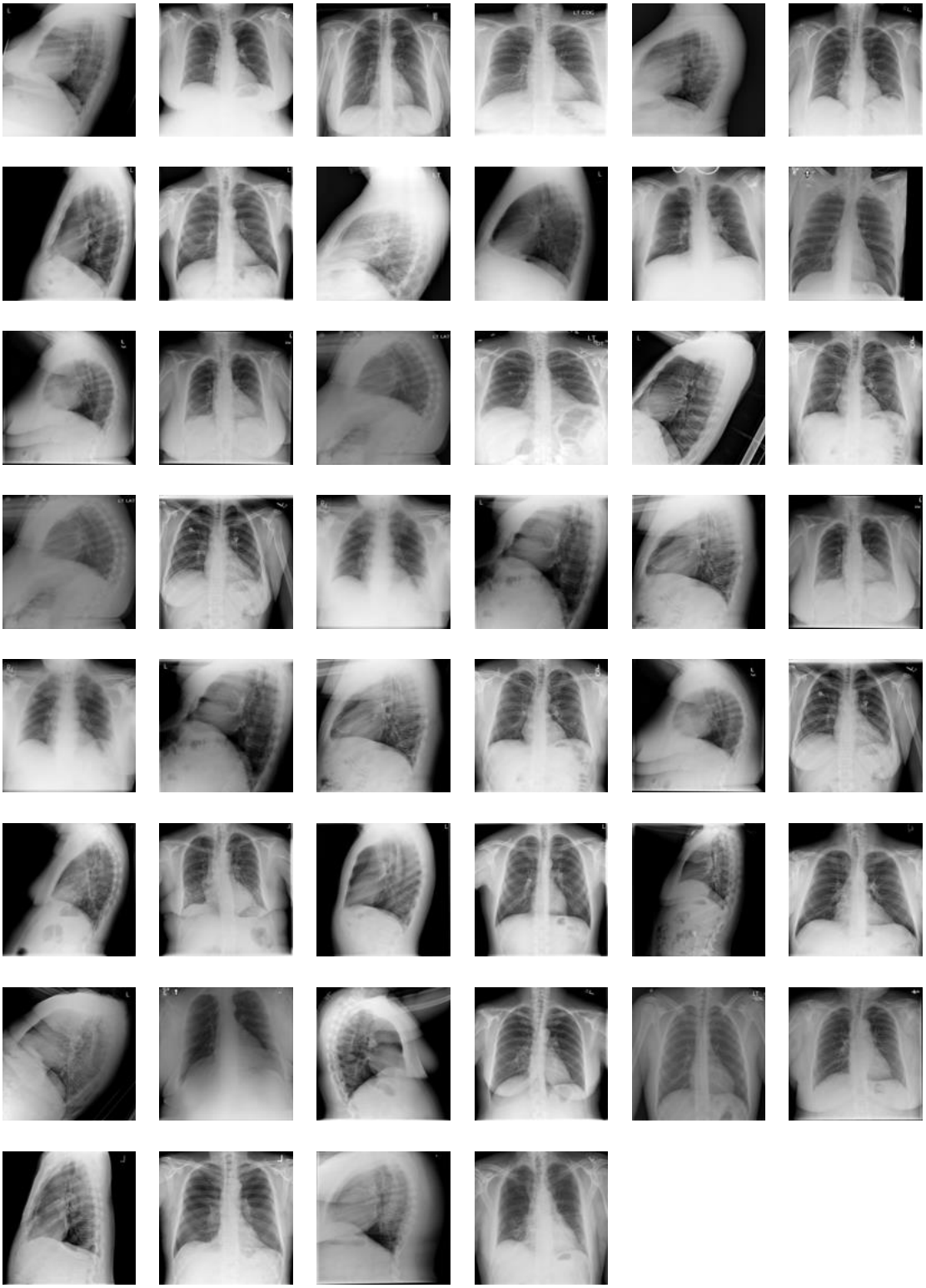


Fig. AI.4 Sample X-ray Images

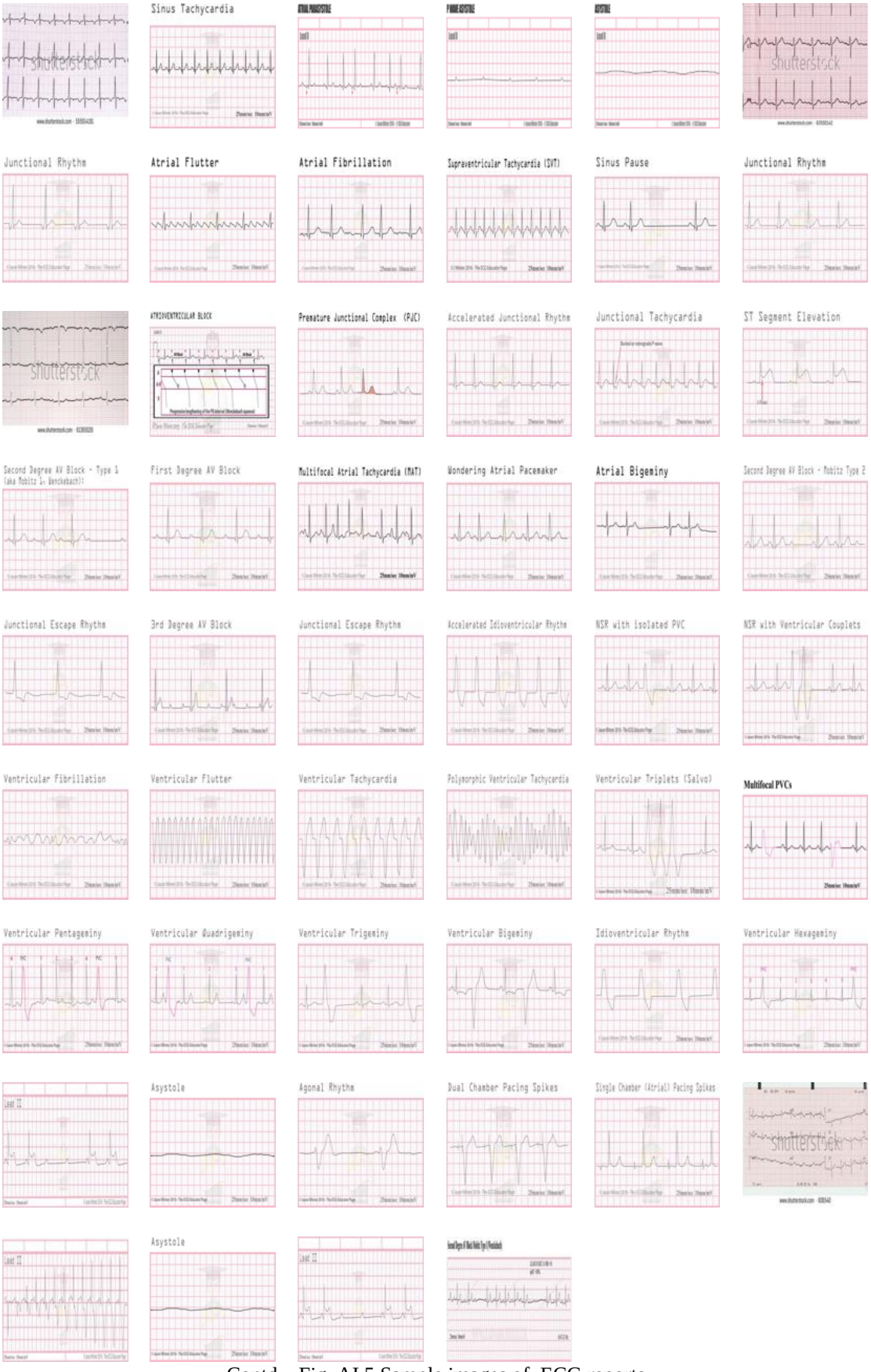


Contd.., Fig. AI.4 Sample X-ray Images

ECG Images:

The 100 sample images of ECG report are shown in the Fig. AI.5.

Fig. AI.5 Sample images of ECG report



Contd.., Fig. AI.5 Sample images of ECG reports

Appendix II

Medical Image Encryption with Integrity

AII.1 SHA-256

The SHA-256 is the most widely used hash function. The calculation of hash values is very fast using this function. The hash function SHA-256 generates a fixed 256-bit hash value for varying size input up to 2^{64} bits. The DNA sequence M of length $l < 2^{64}$ bits is divided into several chunks as depicted in Eq. (AII.1).

$$M = M_1 + M_2 + M_3 + \ \ldots. \ + \ M_{64} \qquad (AII.1)$$

Each chunk is of size 512 bits and if the last chunk size is less than 512 bits then it is added with '1' followed by '0' bits. In the last chunk, 448 bits hold the DNA sequence, and remaining the 64 bits are reserved to specify the total length of DNA sequence 'M' before padding as shown in Fig.AII.1.

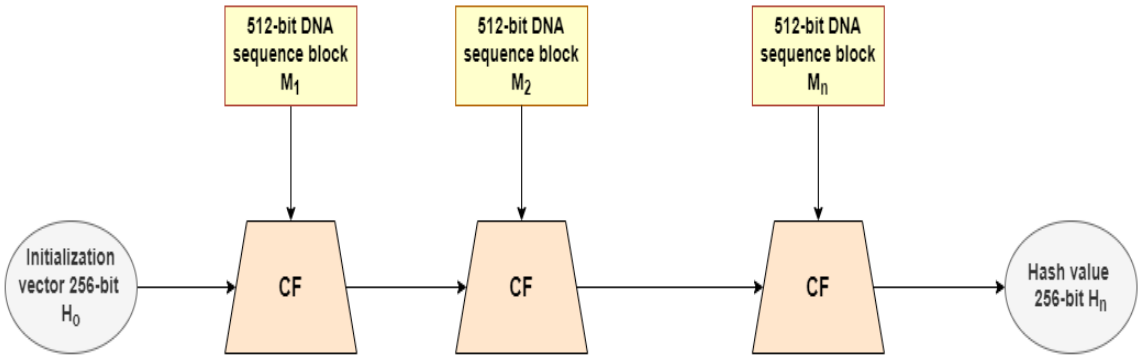


Fig.AII.1 Hash function SHA-256

The initialization vector is the initial hash value of H_0 of length 256 bits. The initial block buffer H_0 is further divided into eight blocks of each 32 bits size. The eight blocks are considered eight registers and initialized with constant values.

H_0^1 = 0x6a09e667 H_0^5 = 0x510e527f

H_0^2= 0xbb67ae85 H_0^6= 0x9b05688c

H_0^3 = 0x3c6ef372 H_0^7= 0x1f83d9ab

H_0^4= 0xa54ff53a H_0^8= 0x5be0cd19

The 256-bit initial hash value and 512-bit DNA sequence chunk are input to compress function.

Compression Function (CF)

In compression function, each DNA sequence chunk is further subdivided into 16 blocks of size 32-bit words each as depicted in Eqn. AII.2.

$$M^1 = M_1^1 + M_1^2 + M_1^3 + \ldots\ldots\ldots + M_1^{16} \quad \text{(AII.2)}$$

The 64-entry message schedule array is created as A [0…63] of 32-bit words. The first 16 blocks of DNA sequence chunk are copied into message schedule array A [0…15]. These 16 words of 32-bits are extended to the remaining 48 words of the message schedule array A [16….63]. It is depicted in Eqs. (AII.3 – AII.6).

$$A[t] = M_t^1 \quad \text{for } 1 <= t <= 16 \quad \text{(AII.3)}$$

A[t] = Sigma1(A[t-2]) + A[t-7] + Sigma0(A[t-15]) + A[t-16] for 16 <= t <= 63 (AII.4)

Sigma0 = (A[t-15] rightrotate 7) ⊕ (A[t-15] rightrotate 18) ⊕ (A[t-15] rightshift 3) (AII.5)

Sigma1= (A[t-2] rightrotate 17) ⊕ (A[t-2] rightrotate 19) ⊕ (A[t-2] rightshift 10) (AII.6)

These are repeated in 64 rounds for 32-bit words of message schedule array ‘A’ for each DNA sequence chunk. The compression function input of size 768 is compressed into a fixed 256-bit output i.e. intermediate hash value for the first DNA sequence chunk is generated. This compressed 256-bit intermediate hash key is utilized as an input for the

next DNA sequence chunk. This process is repeated until it reaches the big-endian of DNA sequence. The final output is the hash key for the given input DNA sequence M. This hash key is utilized to offer tamper-proof for the medical images.

AII.2 DNA Cryptosystem with Integrity

The medical images integrity and confidentiality are preserved using hash function SHA-256. The Chen's chaotic map and DNA cryptography are used for security. In proposed en/decryption method, Canis lupus DNA sequence ID (MW549038) of varying size is taken as an input for the SHA-256 to get a fixed 256-bit hash value. The Fig. AII.2 shows the overall process of encryption methodology using SHA-256. The original medical image is transformed into a binary image. The hash key is embedded in the LSB of binary image.

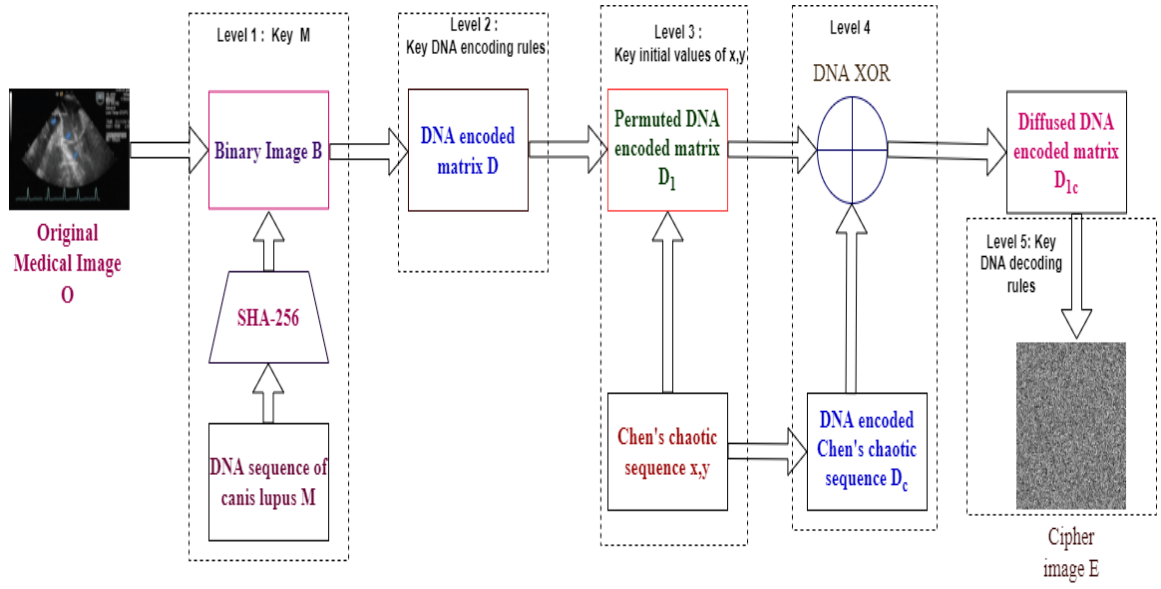


Fig.AII.2 Block diagram of proposed medical image encryption using SHA-256

The encoded DNA matrix is generated for the embedded binary image by DNA encoding rules specified in Section 1.6 of Chapter 1. The encoded DNA matrix are permuted by chaotic sequence of Chen's chaotic map depicted in Section 1.5 of Chapter 1. The DNA XOR operation specified in Section 1.6 of Chapter 1 is utilized for the diffusion of scrambled DNA encoded matrix. The DNA decoding rules are utilized to gain a cipher image as exhibited in Fig.4.3. The expansive description of this cryptosystem is illustrated in medical image encryption and decryption using SHA-256.

AII.2.1 Algorithm for Medical Image Encryption using SHA-256

In proposed encryption using SHA-256, to offer integrity and confidentiality for medical images, the SHA-256 and DNA sequence are used respectively. The high dimensional chaotic map and DNA cryptography are used to offer security for medical images. The expansive steps of proposed encryption method for medical images using SHA-256 are depicted in Algorithm AII.1.

Algorithm AII.1: Medical Image Encryption using SHA-256

//Input: Original medical image O (r, c)

//Output: Cipher image E (r, c)

Step 1 : Start

Step 2 : The hash function SHA-256 generates a hash value 'H' for Canis lupus DNA sequence.

Step 3 : Original medical image O (r, c) is renovated into 8-bit binary image B (r, c×8) of size r rows and c×8 columns. The hash value H is embedded into the LSB of binary image B (r, c×8).

Step 4 : DNA encoding rules are mapped to transform a binary image into encoded DNA matrix D (r, 4×c) of size r rows and 4×columns.

Step 5 : The Chen's chaotic sequence x and y are arranged in ascending order.

Step 6 : The position of the sorted sequences is referred for the permutation of the D(r, 4×c). The permuted matrix is represented as D_1(r, 4×c).

Step 7 : Chen's chaotic sequence x_1 and y_1 are encoded into a DNA encoded matrix using DNA encoding rules D_c (r, 4×c).

Step 8 : The DNA XOR operation is used between D_1(r, 4×c) and D_c (r, 4×c) to diffuse the pixels of DNA encoded matrices. The diffused DNA matrix is represented as D_{1c} (r, 4×c).

Step 9 : The DNA decoding rules are applied for D_{1c} (r, 4×c) to get the binary image.

Step 10 : The binary image is renovated into cipher image E (r, c).

Step 11 : Stop

The cipher image is transferred through an insecure channel and it is decrypted at the receiver end using decryption process.

AII.2.2 Algorithm for Medical Image Decryption using SHA-256

The decryption method is the inverse process of encryption method. The expansive steps of proposed decryption of cipher image into decipher image process are illustrated in Algorithm AII.2.

Algorithm AII.2: Medical Image Decryption using SHA-256

//Input: Cipher image E (r, c)

//Output: Decipher medical image O (r, c)

Step 1 : Start

Step 2 : The cipher image is transformed as a binary image.

Step 3 : The binary image is renovated into DNA encoding matrix D_{1c} (r, 4×c) using DNA encoding rules.

Step 4 : Chen's chaotic sequence *x* and *y* are arranged in decreasing order.

Step 5 : The DNA encoding rules are mapped to generate encoded DNA matrix D_c (r, 4×c) for chaotic sequences.

Step 6 : The DNA XOR operation is used between D_{1c} (r, 4×c) and D_c (r, 4×c) to revert the pixel values of DNA encoded matrices. The resultant matrix is denoted as D_1(r, 4×c).

Step 7 : Index of sorted sequences is referred to reshuffle the pixels of D_1(r, 4×c). The reshuffled pixels of DNA encoded matrix is denoted as D (r, 4×c).

Step 8 : The DNA decoding rules are applied to transform D (r, 4×c) into 8-bit binary image B (r, c×8).

Step 9 : The 256-bit hash key is extorted from LSB of B (r, c×8). The SHA-256 is used to compute the hash key for Canis lupus DNA sequence. The extracted hash value is compared with obtained hash value. If both are same, means integrity is preserved otherwise the medical image is modified during transmission.

Step 10 : The binary image is renovated into decipher image **O** (r, c).

Step 11 : Stop

Medical images play an important tool in diagnosing diseases with remote access. The medical images must have tampered proof while communicating through insecure communication channels. In proposed cryptosystem, hash function SHA-256 is used as a tamper-proof for medical images. SHA-256 produces a 256-bit hash value for the Canis

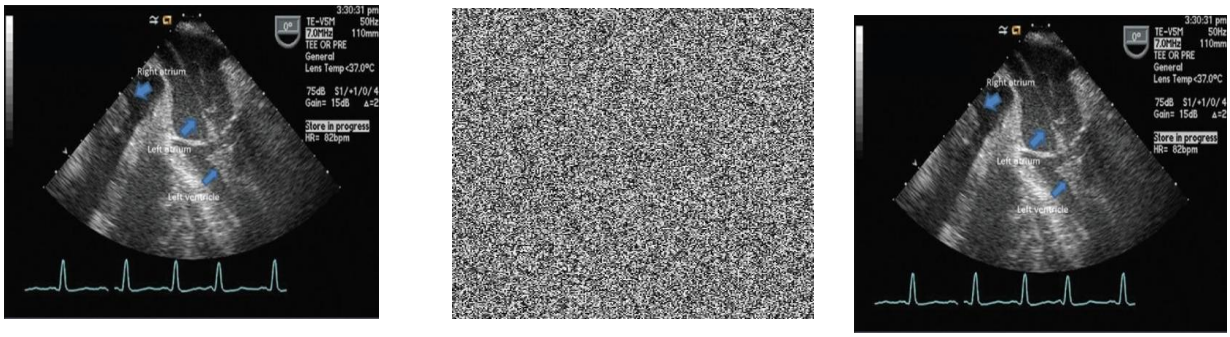
lupus DNA sequence. The original medical image is transformed as a binary image. The hash key is embedded with LSB of binary image to check integrity at the receiver end. The DNA structure is constructed for embedded binary image using DNA encoding rules. Chen's chaotic sequence are mapped for permutation of DNA structure. The DNA XOR operation has used the change the pixel value scrambled DNA structure. The inverse of DNA encoding rules are applied to DNA structure for reconstruction of a binary image. The binary image is transformed into a cipher image. The Canis lupus DNA sequence and hash key are used to prove confidentiality and integrity and Chen's chaotic map and DNA operations are utilized to provide security.

AII.3 Experimental Results and Discussion

The medical image en/decryption algorithm using SHA-256 is implemented on system intel Core i7, a 9th Gen processor with 16 GB RAM. The software tool Matlab R2016b is used to experiment on 500 medical image samples of size 512×512. The 100 medical image samples are taken from each category like CT, MRI, Ultrasound, X-ray, and ECG. The original medical image as shown in Fig.AII.3(a), is transformed as binary image. The SHA-256 generates a hash value for the Canis lupus DNA sequence (ID MW549038 in GenBank). The hash value is embedded in the LSB of binary image for verification of integrity of medical image. The DNA encoding rule Rule-6 discussed in Table 1.1 of Section 1.6 of Chapter 1 is utilized for the construction of encoded DNA matrix. The Chen's chaotic sequences are obtained from Chen's chaotic map specified in Eqs. (1.5.1) – (1.5.4) of Chapter 1. These sequences are arranged in ascending order, and position of ordered sequence is considered for the permutation of encoded DNA matrix. The DNA XOR specified in Table 1.4 of Section 1.6 of Chapter 1 is applied for the diffusion of permuted DNA encoded matrix. The DNA decoding rule Rule-4 are mapped to reconstruct a binary image from diffusion matrix. The binary image is translated as a cipher image is exhibited in Fig.AII.3(b).

In proposed medical image decryption using SHA-256, the cipher is converted into a binary image. The encoded DNA matrix is constructed for binary image using DNA encoding rule Rule-4. The DNA XOR method is operated to restore the diffusion matrix. Chen's chaotic sequences are referred to reshuffle the pixels of diffusion matrix. DNA decoding Rule-6 is mapped to reconstruct a binary image. The hash value is extorted from binary image. The

binary image is converted into decipher image as shown in Fig.AII.3©. At the receiver end once again hash value is produced for the Canis lupus DNA sequence using SHA-256. If both hash values are similar means integrity of the medical image is maintained.



(a) (b) (c)

Fig.AII.3 Ultrasound image samples: (a) Original image (b) Cipher image (c) Decipher image

The hash key ‘Hk’ is produced for Canis lupus DNA sequence ‘M’ using hash function SHA-256. The ‘Hk’ is embedded in the LSB of a medical image ‘o’. The embedded medical image is encrypted using Algorithm AII.1. The encrypted image is decrypted using Algorithm AII.1. The hash function SHA-256 is utilized by receiver to produce a 256-bit hash value ‘Hk1’ for Canis lupus DNA sequence. The Hk1 is matched with extracted Hk. The integrity is preserved, if hash keys are same, as exhibited in Fig.AII.4. The initial values of heterogeneous chaotic maps are the secret keys used for encipher (Enc) and decipher (Dec).

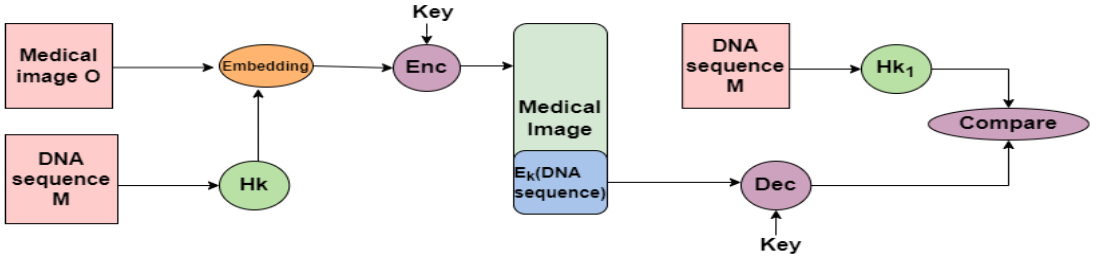


Fig.AII.4 Block diagram for Integrity verification

AII.3.1 Performance and Security Analysis

The performance of proposed medical image en/decryption using SHA-256 depends on the fortification of a medical image against different attacks. The security analysis is to prove

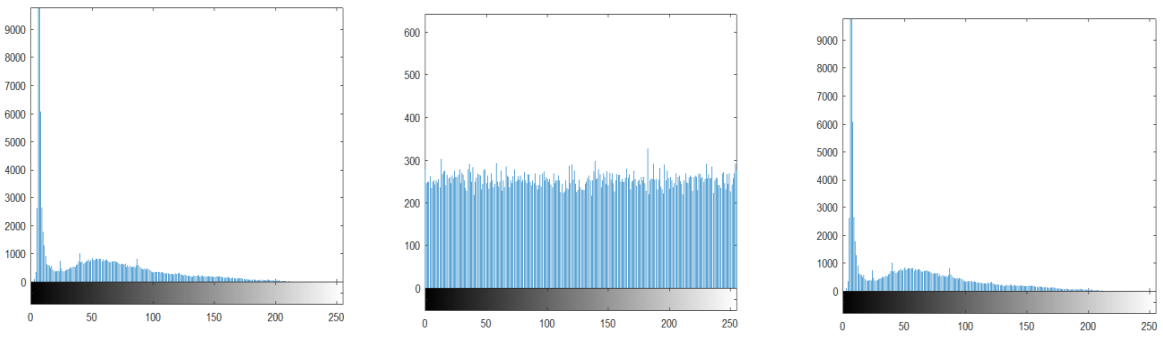
the resistance of the medical image en/decryption against statistical attacks, differential attacks, and exhaustive attacks.

A. Statistical Attack

The statistical attack depends on examining the pixels of cipher image. The encryption technique is strong if the pixels of cipher image are absolutely varied from original medical image. Then, it is extremely impractical for invaders to predict the secret keys and original medical by observing the pixels of the cipher images.

Histogram Analysis

The histogram analysis is performed to analyse the dispersal of pixels. The attacker intends to predict the original medical image by studying the dispersal of pixels of cipher image. The pixels are supplied arbitrarily in the original medical image and decipher image as exhibited in Fig.AII.5(a) and Fig.AII.5(c). The pixels are distributed consistently in the cipher image as exhibited in Fig.AII.5(b). From these figures, it is observed that pixels are changed in cipher image. The prediction of secret keys and original medical image by observing the dispersal of pixels is not possible. This proves that proposed en/decryption using SHA-256 has good confusion properties.



(a) (b) (c)

Fig.AII.5 Histogram analysis: (a) Original ultrasound image (b) Cipher image (c) Decipher image

Correlation Coefficient Analysis

The adjacent pixels of medical images are highly correlated. The correlation coefficient analysis is to verify the correlation between adjacent pixels. The coefficient value ‘1’

Table AII.1 Correlation coefficient of proposed medical image en/decryption using SHA-256

Medical image type	Direction	Cipher image	Decipher image
MR	*Horizontal*	0.017	0.997
	Vertical	0.018	0.998
	Diagonal	0.018	0.997
CT	*Horizontal*	0.020	0.992
	Vertical	0.019	0.999
	Diagonal	0.016	0.991
X-ray	*Horizontal*	0.010	0.991
	Vertical	0.013	0.990
	Diagonal	0.012	0.991
Ultrasound	*Horizontal*	0.016	0.999
	Vertical	0.013	0.992
	Diagonal	0.015	0.993
ECG	*Horizontal*	0.015	0.999
	Vertical	0.014	0.998
	Diagonal	0.017	0.990
Average		**0.016**	**0.994**

indicates that pixels are correlated strongly i.e. adjacent pixels are similar. The coefficient value '0' indicates that pixels are not correlated i.e. adjacent pixels are different. The coefficient value '-1' indicates that pixels are negatively correlated. The correlation coefficient values of the cipher image and decipher image are depicted in Table AII.1. From Table AII.1, it is examined that neighboring pixels are associated in original medical image and decipher images. The adjacent pixels are not correlated in cipher image because the coefficient value is almost equal to '0'.

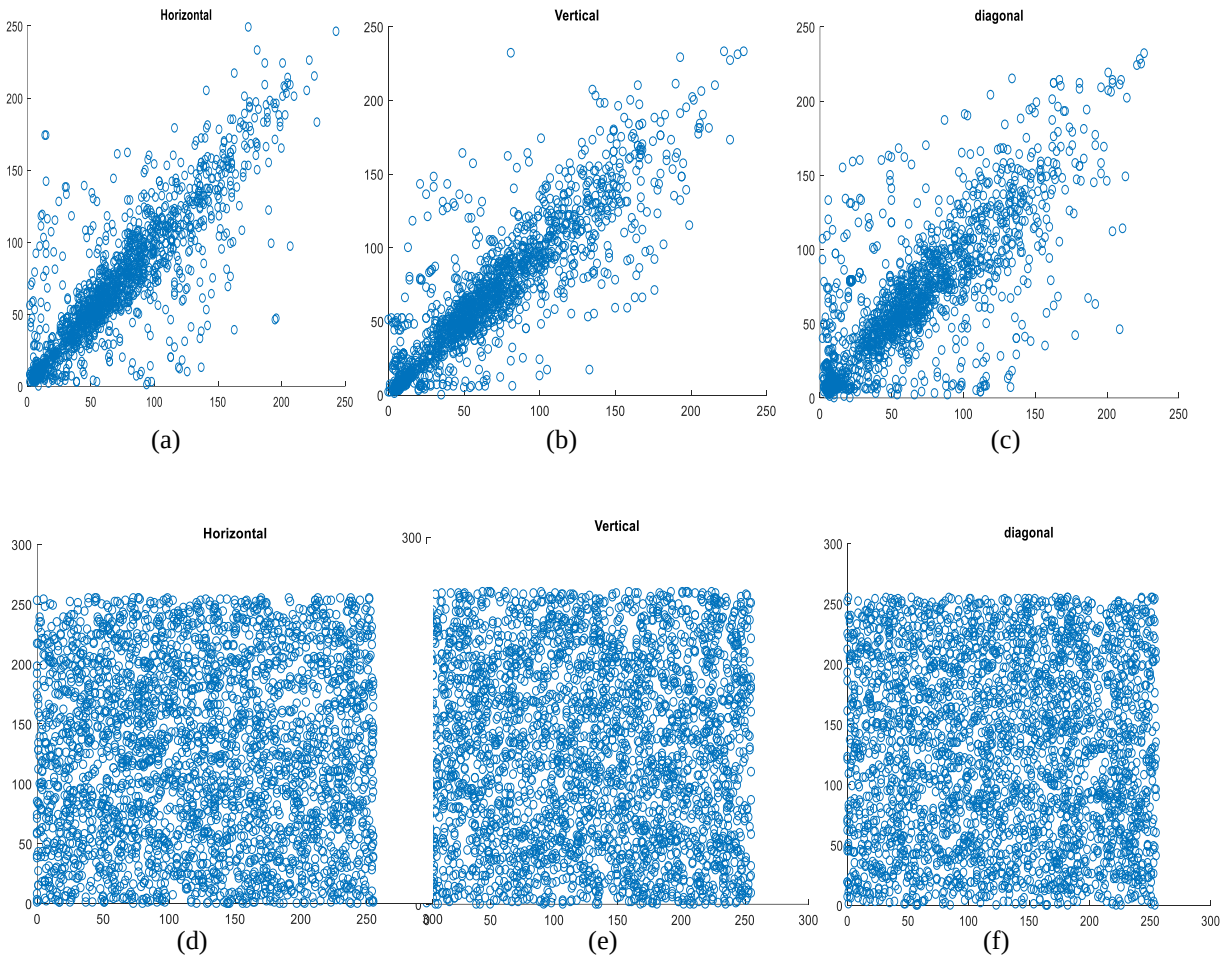


Fig.AII.6 Scatter plot of original ultrasound image in horizontal, vertical and diagonal directions (a) –(c); Scatter plot of cipher image in horizontal, vertical and diagonal directions (d) -(f)

The scatter plot for the original medical image and cipher image in three different directions namely, horizontal, vertical, and diagonal respectively is shown in Fig. AII.6. From Fig. AII.6(a and b and c), it is seen that neighboring pixels of an original medical image are linearly related. From Fig.AII.6(d and e and f), it is proved that neighboring pixels of cipher image are consistently scattered means there is a no association among pixels.

B. Exhaustive attack

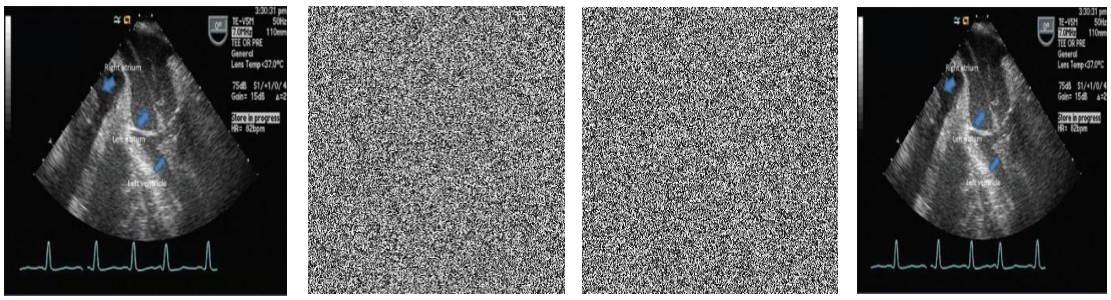
The encryption methods are used to provide security for medical images while transmitting through vulnerable communication networks. The secret keys used in encryption methods play the main role in providing security for medical images. Hence, attackers attempt to get the secret keys. To identify the weakness of secret keys in the proposed cryptosystem, key space, and key sensitive analysis are performed.

Key space analysis

The preliminary values of position variables and control factors of Chen's chaotic map are used as a secret key in a proposed DNA cryptosystem with integrity. A total of four secret keys (x_0, y_0, z_0, w_0,) are used. The 256-bit DNA sequence is also used as a secret key. Then, size of four secret keys is $(10^{15})^4 \approx 2^{200}$, and 2^8 is the hash key size. The total key space is 2^{208} and is adequate to survive against brute force attack.

Key sensitivity analysis

The preliminary values of state and control factors of high dimensional Chen's chaotic map are very sensitive. Hence, decrypting the original medical image with an exceptionally slight variation in initial values is extremely impractical. In the medical image en/decryption method, among five secret keys if we slightly change the preliminary value of anyone's secret keys, then decrypting the original medical image with a modified value is not possible. If one of the secret key preliminary value w_0=1 is slightly varied like w_0=0.9999 then decrypting of cipher image as shown in Fig.AII.7 (b) into an original medical image is not possible. Fig.AII.7(c) shows the decipher image decrypted using w_0=0.9999, it is not an original medical image. Fig.AII.7(d) shows the decipher image decrypted using w_0=1 and decipher image is an original medical image as shown in



(a) (b) (c) (d)

Fig. AII.7 Key sensitivity analysis: (a) Original ultrasound image (b) Cipher image (c) Decipher image decrypted with the wrong key w_0=0.9999 (d) Decipher image with correct key w_0=1

C. Differential attack

In differential attack, cryptanalyst used NPCR and UACI as discussed in Section 1.9.2 of Chapter 1 to validate strength of medical image encryption method against differential

attack. The NPCR average value is 99.574 and UACI average value is 32.52 almost equal to ideal value as depicted in Table AII.2. From Table AII.2 it is proved that proposed en/decryption method is suitable to offer security for medical images.

Table AII.2 Performance analysis of proposed medical image en/decryption using SHA-256

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.58	31.57	7.98	2.3038e+03	10.67
CT	99.59	33.23	7.76	3.7184e+03	10.89
X-ray	99.54	32.43	7.93	2.8754e+03	10.54
Ultrasound	99.57	32.34	7.96	3.9210e+03	10.69
ECG	99.59	33.02	7.98	2.3701e+03	10.95
Average	**99.57**	**32.52**	**7.92**	**3.0400e+3**	**10.75**

The metrics MSE, PSNR, and entropy discussed in Section 1.10 of Chapter 1 are applied to measure the quality of developed medical image encryption method. The values of MSE, PSNR, and entropy between the original medical image and cipher image are tabulated in Table AII.2. From Table AII.2, it is stated that MSE is very big and PSNR value is very small. Hence, the proposed medical image encryption using SHA-256 is secure and suitable to provide confidentiality and integrity. The entropy average value is 7.922 is almost equal to ideal value. This demonstrated that proposed encryption method using SHA-256 has good confusion properties.

AII.3.2Computation Time of Proposed DNA Cryptosystem with Integrity

The time efficiency of the proposed en/decryption using SHA-256 for original medical image of size (m×n) is calculated as follows:

Step 1: Generating hash key: m

Step 2: Binary conversion of original medical image: (m×n)

Step 3: Embedding hash key LSB: m

Step 4: Construction DNA structure: (m×n)

Step 5: Permutation process: (m×n)

Step 6: Diffusion process: (m×n)

Step 7: DNA decoding: (m×n)

Step 8: Generating cipher image: (m×n)

Total time complexity of the proposed encryption algorithm is given below:

$T(n)= 2m + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) + (m\times n) = 7(m\times n) +2m$

If m=n then $T(n)=7(n^2)\in O(n^2)$.

The space efficiency of the proposed cryptosystem for a given original medical image of size (m×n) is $O(n^2)$ assuming m=n.

AII.3.3 Comparative Analysis

The proposed en/decryption method using SHA-256 for the medical image is compared with the methods specified in Chapter 2 and Chapter 3. The results tabulated in Table AII.3 prove that the, proposed en/decryption method is suitable to provide security and confidentiality, and integrity.

Table AII.3 Comparative analysis of proposed medical image en/decryption using SHA-256

Methods	NPCR (%)	UACI (%)	Entropy	Keyspace
multistate en/decryption	99.66	33.67	7.99923	2^{268}
Inensity based en/decryption	99.66	33.87	7.99943	2^{400}
Proposed En/decryption using SHA-256	**99.57**	**33.67**	**7.922**	**2^{208}**

This method concentrates on providing integrity which is not considered in the methods specified in Chapter 2 and Chapter 3. The key space of the proposed en/decryption method is smaller than the methods of Chapter 2 and Chapter 3. Hence, enhancement in security is necessary for medical images. This method is improved by considering SHA-512 and the details are described in the Chapter 4.

Appendix III

Graphical Interface Based DNA Cryptosystem for Secure e-Health System

Creating a graphical user interface (GUI), useful for users to easily interact with the systems and perform the tasks with effortless elements like menus, command buttons and scroll bars. The GUI is implemented using licensed MATLAB 2020b software with a parallel computing toolbox. The GUI for the secure e-health system is shown in Fig. AII.1, which is based on the proposed parallel DNA cryptosystem discussed in Chapter 7.

Fig. AII.1 GUI for secure e-health system

The GUI contains command buttons namely Browse Image, Encrypt Image, Save Encrypted Image, Decrypted Image, Save Decrypted Image, and Exit. Browse Image command is for browsing medical image from the folder. The selection of the medical image using Browse Image is shown in Fig.AII.2.

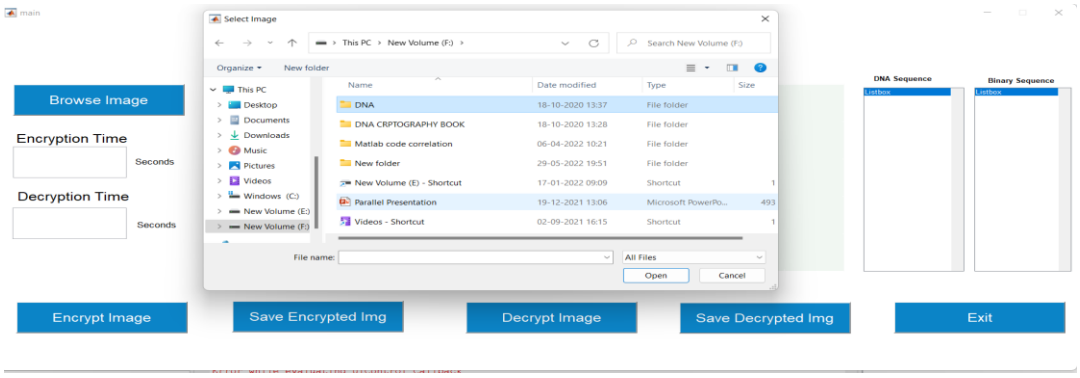


Fig. AII.2 Browse for medical image

The selected medical image is displayed in the Original Image box as exhibited in Fig.AII.3.

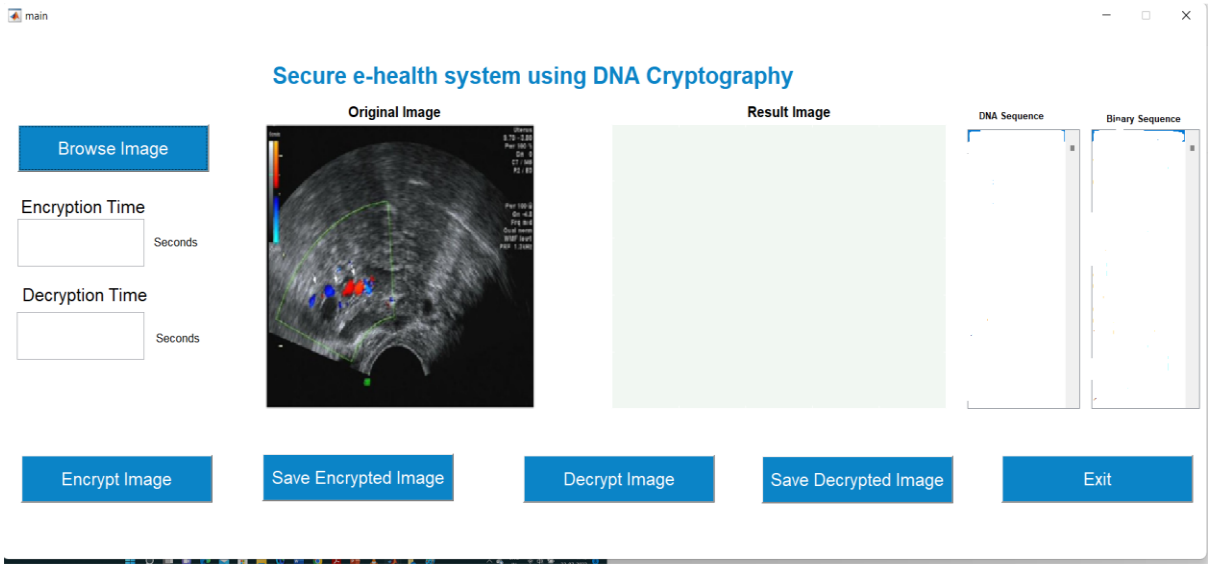


Fig. AII.3 Original medical image

After the user presses Encrypt Image button, the secure e-health parallel encryption method converts the original medical into a binary sequence matrix, the result is displayed in the list box of Binary Sequence. The binary sequence matrix is renovated into a DNA sequence as shown in the list box of DNA sequences. The final encrypted cipher image is displayed in the Result Image box as shown in Fig. AII.4. The runtime of the parallel encryption method is displayed in the Encryption Time text box.

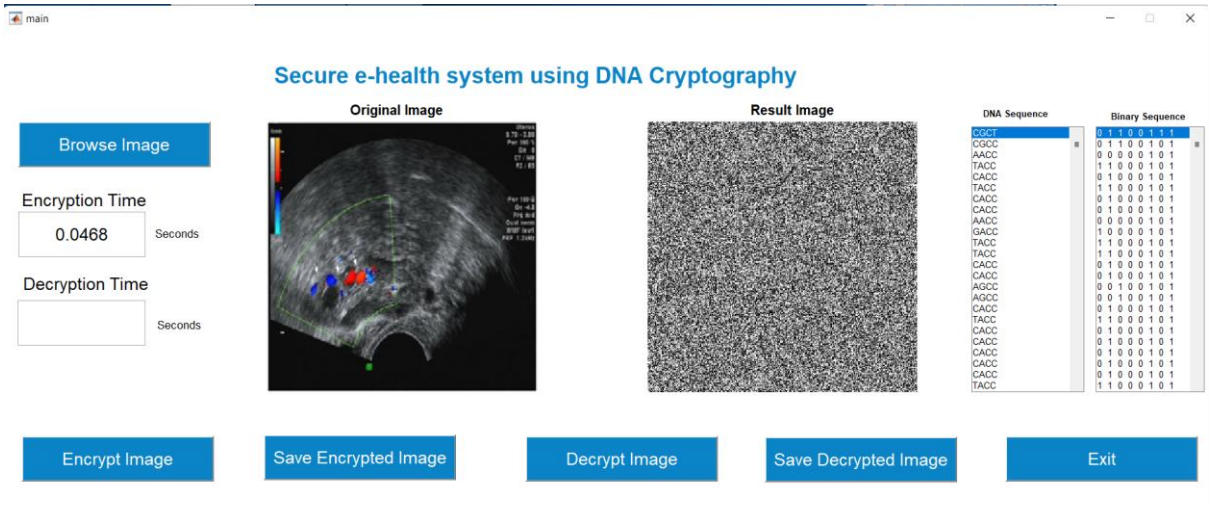


Fig. AII.4 Cipher image

The cipher image is saved in a selected folder using Save encrypted Image button as shown in Fig. AII.5.

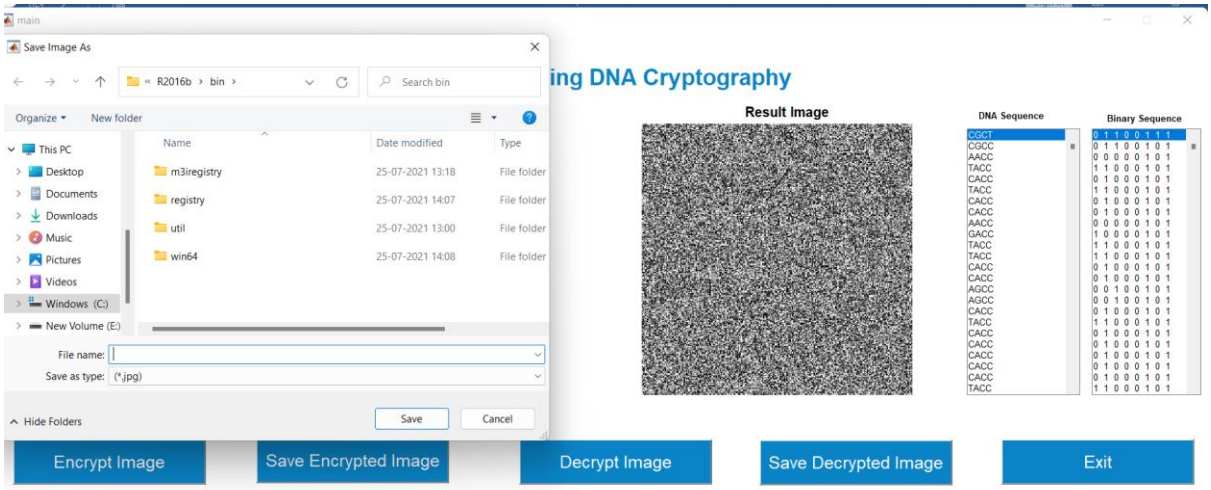


Fig. AII.5 Save cipher image

The cipher image is communicated through an open-source network. At the receiver end, the user needs to press the command button Decrypt Image button to get decipher the image. The cipher image is deciphered by secure e-health parallel decryption method. The decipher image is the original medical image as exhibited in the Result Image box in Fig. AII.6. The runtime of the parallel decryption method is shown in the Decryption Time text box of Fig. AII.6.

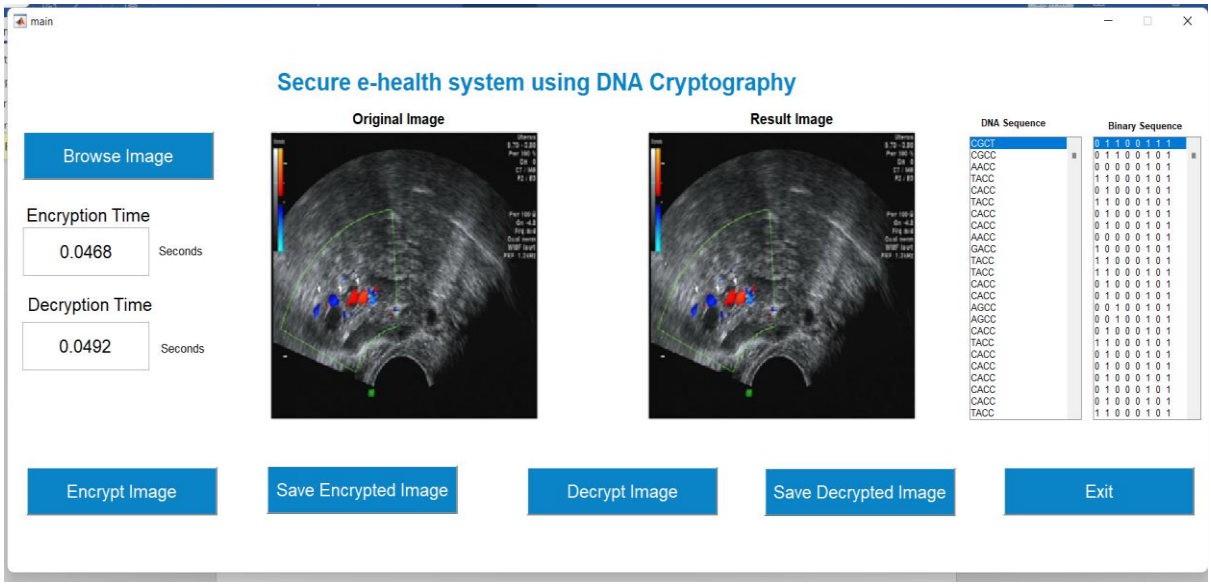


Fig. AII.6 Decipher image

The decipher image can save in the selected folder by pressing the Save Decrypted Image button. This user-friendly secure e-health system is useful for the secure transmission of

medical images through an open source network and storing of medical images in a third-party cloud.

AUTHOR'S PUBLICATIONS

No. of Journal Papers (International)	**02**
No. of Book Chapters	**01**
No. of Conference papers (International)	**02**
No. of Conference papers (National)	**01**
No. of Journal Papers Under review	**02**

Grants Utilized for the Research

The research work is carried under the financial assistance of Vision Group of Science and Technology, Government of Karnataka, under Research Grant Scheme for Scientists/Faculty (RGS/F) GRD No.851/315 in the year 2018-2019. I would like to thank Vision Group of Science and Technology, Karnataka, India for the financial assistance of Rs.**5,00,000.00**.

Journal papers

[1] Prema T Akkasaligar, Sumangala Biradar, "***Selective Medical Image Encryption using DNA Cryptography***" Information Security Journal: A Global Perspective Volume 29(2), 2020, pp. 91-101**.** (**Scopus Indexed, Citations : 25, Q2-SJR:0.52)** DOI:10.1080/19393555.2020.1718248.

[2] Prema T. Akkasaligar and Sumangala Biradar, "***Multilevel Security for Medical Image using Heterogeneous Chaotic Map and Deoxyribonucleic Acid Sequence Operations***", Concurrency and Computation: Practice Experience. 2022; e7222, vol.34, issue 20/10, pp.1-21. **(Scopus Indexed, Impact factor:1.831, Q2-SJR:0.52)** . DOI:10.1002/cpe.7222.

Book Chapter

[1] Prema T. Akkasaligar and Sumangala Biradar, "***Medical Image Encryption with Integrity using DNA and Chaotic Map*** ", Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2018. Communications in Computer and Information Science, vol. 1036, Chapter 18, part 2, Springer Nature Singapore

Ple. Ltd. 2019, pp. 143-153. (**Scopus Indexed, Citations : 3)** DOI:10.1007/978-981-13-9184-2_13.

Conference papers

[1] Prema T. Akkasaligar, Sumangala Biradar, "***Multiphase Image Encryption using Chen's Hyper Chaotic Map, Biological and Logical Operator***", National conference on Recent Trends in Image Processing and Pattern Recognition, April 2-3 2016, Organized by Department of Computer Science, Karnataka Arts, Science and commerce College, Bidar, pp.103-113.

[2] Prema T. Akkasaligar, Sumangala Biradar, "***Secure Medical Image Encryption Based on Intensity Level using Chao's Theory and DNA Cryptography***", 2016 IEEE International Conference on Computational Intelligence and Computing Research, 15-17 December 2016, pp. 958-963. (**Scopus Indexed, Citations : 14)** DOI: 10.1109/ICCIC.2016.7919681

[3] Prema T. Akkasaligar, Sumangala Biradar, "***Medical Image Compression and Encryption using Chaos Based DNA Cryptography***," IEEE Bangalore Humanitarian Technology Conference (B-HTC-2020), 8-10 October 2020, pp.261-265. **(Scopus Indexed)** DOI:10.1109/B-HTC50970.2020.9297928

Journal Papers (Under Review):

[1] Prema T. Akkasaligar, Sumangala Biradar**, "*A Novel Approach for Medical Image Encryption using Multiple Chaotic Maps and DNA Diffusion Operations***", Communicated to Pattern Recognition and Image Analysis, Pleiades Publishing Ltd.

[2] Prema T. Akkasaligar, Sumangala Biradar, "***A Parallel Algorithm Approach for Medical Image using DNA Cryptography***", Communicated to Journal of The Institution of Engineers (India)-Series B.

REFERENCES

[1] Abbas, Alaa M., Ayman A. Alharbi, and Saleh Ibrahim, "A Novel Parallelizable Chaotic Image Encryption Scheme Based on Elliptic Curves," IEEE Access, volume 9, 2021, pp.54978-54991.

[2] Abhishek Jain and Navin Rajpal, "Adaptive key length-based encryption algorithm using DNA approach," IEEE International Conference on Machine Intelligence and Research Advancement (ICMIRA) 2013, pp. 140-144.

[3] Abraham Lini and Neenu Daniel, "An Improved Color Image Encryption Algorithm with Pixel Permutation anXing-Yuan Wang d Bit Substitution," International Journal of Research in Engineering and Technology volume 02, issue 11, 2013, pp.333-338.

[4] Adelman L, "Molecular computation of solutions to combinatorial problems", Science in JSTOR, 266(5187), pp.1021-1025, 1994. doi:10.1126/science.7973651 PMID:7973651.

[5] Adleman, L. M., "Molecular computation of solutions to combinatorial problems", Science, volume 266, issue 5187, pp.1021-1024.

[6] Akram Belazi , Houcemeddine Hermassi ,Rhouma Rhouma and Safya Belghith ,"Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map," Nonlinear Dynamics, volume 76, issue 4 ,2014, pp.1989- 2004.

[7] Al-Haj, Ali Noor Hussein and Gheith Abandah," Combining cryptography and digital watermarking for secured transmission of medical images," IEEE Second International Conference on Information Management (ICIM) 2016, pp.40-46.

[8] Anchal Jain, Pooja Agarwal, Rashi Jain and Vyomesh Singh "Chaotic Image Encryption Technique using S-box based on DNA Approach," International Journal of Computer Applications, volume 92, issue13, 2014, pp.30-34.

[9] Arya Sebastian, Delson T R,"Secure Magnetic Resonance Image transmission and tumor detection techniques," IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT) 2016, pp.1-5.

[10] Bishop, Robert, "Chaos," in Zalta, Edward N. (ed.), The Stanford Encyclopedia of Philosophy (Spring 2017 ed.), Metaphysics Research Lab, Stanford University, retrieved 2019-11-24.

[11] Brindha M, "Confidentiality, integrity and authentication of DICOM medical images," IEEE 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 71-75.

[12] Chen, J.X., Zhu, Z.L., Fu, C., Yu, H. and Zhang, L.B., "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," Communications in Nonlinear Science and Numerical Simulation, volume 20, issue 3, 2015. pp.846-860.

[13] Chen, Junxin, Yu Zhang, Lin Qi, Chong Fu, and Lisheng Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," Optics & Laser Technology, volume 99, 2018, pp. 238-248.

[14] Chen, Xiao, and Chun-Jie Hu. "Medical image encryption based on multiple chaotic mapping and wavelet transform", Biomedical Research, volume 28, issue 20, 2017, pp. 9901-9004.

[15] Enayatifar Rasul, Abdul Hanan Abdullah, and Ismail Fauzi Isnin, "Chaos-based Image encryption using a hybrid genetic algorithm and a DNA sequence," Optics and Lasers in Engineering, volume 56, 2014, pp. 83-93.

[16] Ghaffari A, "Image compression-encryption method based on two-dimensional sparse recovery and chaotic system," Scientific Reports, volume 11, 2021, pp.1-19.

[17] Gong L., Deng C., Pan S., Zhou N., "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," Opt. Laser Technol, 2018, volume 103, pp.48–58.

[18] Gupta, Shreya, and Anchal Jain, "Efficient image encryption algorithm using DNA approach," IEEE Second International Conference on Computing for Sustainable Global Development (INDIACom) 2015, pp. 726-731.

[19] Hua, Zhongyun, Shuang Yi, and Yicong Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing, volume 144, 2018, pp. 134-144.

[20] Hussein, Khalid Ali, Sadiq A. Mehdi, and Salam Ayad Hussein. "Image Encryption Based on Parallel Algorithm via Zigzag Manner with a New Chaotic System," Journal of Southwest Jiaotong University, volume 54, issue 4 ,2019, pp. 1-9.

[21] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra and F. Khalifa, "A Robust Chaos-Based Technique for Medical Image Encryption," in IEEE Access, volume10, 2022, pp. 244-257.

[22] Jain, A., Rajpal, N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications, volume 75, 2016, pp. 5455–5472.

[23] Jain Sonal and Vishal Bhatnagar, "Bit based symmetric encryption method using DNA Sequence," IEEE Fifth International Conference on Confluence the Next Generation Information Technology Summit (Confluence) 2014, pp.495-498.

[24] Janakiraman Siva, Karuppusamy Thenmozhi, John Bosco,Balaguru Rayappan, and Rengarajan Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller," Microprocessors and Microsystems, volume 56 ,2018, pp. 1-12.

[25] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "An Introduction to Mathematical Cryptography," Springer-Verlag – Undergraduate Texts in Mathematics, ISBN: 978-1-4939-1710-5, Second Edition, 2014, pp. 34-47.

[26] K. Anusudha, N. Venkateswaran and J. Valarmathi," Secured medical image watermarking with DNA codec," Multimedia Tools and Applications, volume 76, issue 2, 2017, pp.2911-2932.

[27] Kalpana J and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," Optik-International Journal for Light and Electron Optics, volume 126, issue 24 ,2015, pp. 5703-5709.

[28] Kanso A and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," Communications in Nonlinear Science and Numerical Simulation, volume 24, issue 1, 2015, pp. 98-116.

[29] Kellert, Stephen H, "In the Wake of Chaos: Unpredictable Order in Dynamical Systems," University of Chicago Press, ISBN 978-0-226-42976-2, 1993, pp.32-42.

[30] Khan S, Nazir S, Hussain A, Ali A, Ullah A, "An efficient JPEG image compression based on Haar wavelet transform, discrete cosine transform, and run length encoding techniques for advanced manufacturing processes," Measurement and Control, volume 52, 2019, pp. 1532-1544. doi:10.1177/0020294019877508.

[31] Kuldeep Singh and Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it," International Journal of Computer Applications, volume 23, issue 6, 2011, pp. 17-24.

[32] Kumar, P. Kranthi, BV Nagendra Prasad, Gelli MBSS Kumar, V. Chandrasekaran, and P. K. Baruah, "FIELA: A Fast Image Encryption with Lorenz Attractor using Hybrid Computing."

[33] L Gong, C Deng, S Pan, N Zhou, "Image compression encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," Opt Laser Technol, volume103, Jul 2018, issue1, pp.48-58.

[34] Lakshmi C, Karuppusamy Thenmozhi, John Bosco, Balaguru Rayappan, and Rengarajan Amirtharajan, "Encryption and watermark-treated medical image against hacking disease-An immune convention in spatial and frequency domains," Computer methods and programs in biomedicine, volume 159, 2018, pp.11-21.

[35] Li T, Shi J, Li X, Wu J, Pan F, "Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes," Entropy, volume 21, issue 3, 2019, pp. 1-21.

[36] Li, Shanshan, Li Zhao, and Na Yang, "Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion," Security and Communication Networks, 2021, pp. 1-23.

[37] Li, Taiyong, and Duzhong Zhang., "Hyperchaotic Image Encryption Based on Multiple Bit Permutation and Diffusion," Entropy (Basel, Switzerland) volume 23, issue 5, 2021, pp. 1-22. doi:10.3390/e23050510.

[38] Lima J. B, F. Madeiro and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," Signal Processing: Image Communication, volume 35, 2015, pp.1-8.

[39] Lipton, R. J. "DNA solution of hard computational problems", Science, volume 268, issue 5210, 1995, pp. 542–545.

[40] Liu M, Ye G.," A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm", Math Biosci Eng. 2021 May 6,volume 8, pp. 3887-3906. doi: 10.3934/mbe.2021194. PMID: 34198416.

[41] Lone PN, Singh D, Mir UH. “A novel image encryption using random matrix affine cipher and the chaotic maps”, Journal of Modern Optics. 2021 Jun 7, volume 68,issue 10, pp.507-21.

[42] Masood, Fawad, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan, "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," Wireless Personal Communications, 2021, pp. 1-28.

[43] Mokhtar M, Amr Sameh N. Gobran and El-Sayed A-M. El-Badawy, "Colored Image Encryption Algorithm Using DNA Code and Chaos Theory," IEEE International Conference on Computer and Communication Engineering (ICCCE) 2014, pp.12-15.

[44] Mondal Bhaskar, and Tarni Mandal, "A light weight secure image encryption scheme based on chaos and DNA computing," Journal of King Saud University-Computer and Information Sciences, 2016, pp. 1-5.

[45] N Zhou, S Pan, S Cheng, Z Zhou, " Image compression– encryption scheme based on hyper-chaotic system and 2D compressive sensing," Optical Laser Technology, volume 82, Aug 2016, pp.121- 133.

[46] Ozkaynak Fatih and Sirma Yavuz, "Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," Nonlinear Dynamics, volume 78, issue 2, 2014, pp.1311-1320.

[47] Quist-Aphetsi Kester, Laurent N,Anca Christine P, Sophie G,Jojo M E and Nii Narku Q, "A Cryptographic Technique for Security of Medical Images in Health Information Systems," Procedia Computer Science, volume 58, 2015, pp.538-543.

[48] R. Guesmi ,M. A. B. Farah ,A. Kachouri and M. Samet , "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2," Nonlinear Dynamics 83, volume 3, 2016, pp.1123-1136.

[49] R. K. Jangid, N. Mohmmad, A. Didel and S. Taterh, “Hybrid approach of image encryption using DNA cryptography and TF Hill Cipher Algorithm,” International Conference on Communication and Signal Processing, 2014, pp. 934-938.

[50] Raghu M, E. and K. Ravishankar “Encryption and Decryption of an Image Data – a Parallel Approach,” International journal of engineering and technology, volume 7, 2018, pp. 674-677.

[51] Rakesh Kumar Jangid, Noor Mohmmad, Abhishek Didel and Swapnesh Taterh "Hybrid approach of image encryption using DNA cryptography and TF Hill Cipher Algorithm," IEEE International Conference on Communications and Signal Processing (ICCSP) 2014, pp.934-938.

[52] Rakesh, S., Kaller, A.A., Shadakshari, B.C. and Annappa, B., "Image encryption using block based uniform scrambling and chaotic logistic mapping," International Journal on Cryptography and Information Security (IJCIS), volume 2, issue 1, 2012, pp.49-57.

[53] Rasul Enayatifar, Hossein Javedani Sadaei, Abdul H. A,Malrey Lee and Ismail F. I, "A novel chaotic based image encryption using a hybrid model deoxyribonucleic acid and cellular automata," Optics and Lasers in Engineering 71, 2015, pp.33-41.

[54] Rivest, Ronald L, "Cryptography," In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science, Elsevier, 1990, pp. 6-14.

[55] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in IEEE Access, volume 9, 2021, pp.37855-37865.

[56] Safwan El, "A new chaos−based image encryption system," Journal of Signal Processing: Image Communication, volume 41, 2016, pp. 144–157.

[57] Samar M. Ismail, Lobna A. Said, Ahmed G. Radwan, Ahmed H. Madian , Mohamed F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," Journal of advanced research, volume 10 , 2018, pp. 85-98.

[58] Samiullah, Muhammad, Waqar Aslam, Hira Nazir, Muhammad Ikram Ullah Lali, Basit Shahzad, Muhammad Rafiq Mufti and Humaira Afzal, "An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems." IEEE Access, volume 8, 2020, pp. 25650-25663.

[59] Saranya M. R, Arun K. Mohan and K. Anusudha, "A hybrid algorithm for enhanced image security using chaos and DNA theory," IEEE International Conference on Computer Communication and Informatics (ICCCI) 2015, pp. 8-10.

[60] Saranya M. R, Arun K. Mohan and K. Anusudha, "Algorithm for enhanced image Security using DNA and genetic algorithm," IEEE International Conference on

Signal Processing, Informatics, Communication and Energy Systems (SPICES) 2015, pp.1-5.

[61] Soni, Ranu, Arun Johar, and Vishakha Soni, "An Encryption and Decryption Algorithm for Image Based on DNA," IEEE International Conference on Communication Systems and Network Technologies (CSNT) 2013, pp. 478-481.

[62] Sukalyan Som, Ayantika Chatterjee and Atanu Kotal "A colour image encryption based on DNA coding and chaotic sequences," IEEE First International Conference on Emerging Trends and Applications in Computer Science (ICETACS) 2013, pp. 108-114.

[63] Tanveer, Md Siddiqur Rahman, Kazi Md. Rokibul Alam, and Yasuhiko Morimoto, "A multi-stage chaotic encryption technique for medical image," Information Security Journal: A Global Perspective, 2021, pp. 1-19.

[64] Tong X.-J., Chen P., Zhang M., "A joint image lossless compression and encryption method based on chaotic map," Multimedia Tools and Applications, volume 76, 2017, pp. 13995–14020.

[65] Vallathan G, G. Gayathri Devi and A. Vinoth Kannan, "Enhanced data concealing technique to secure medical image in telemedicine applications," IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) 2016, pp.186-190.

[66] Wang Qian, Qiang Zhang and Changjun Zhou, "A multilevel image encryption algorithm-based chaos and DNA coding," IEEE Fourth International Conference on Bio-Inspired Computing (BIC-TA'09) 2009, pp. 70-74.

[67] Wang Qian, Qiang Zhang and Xiaopeng Wei,"Image encryption algorithm based on DNA biological properties and chaotic systems", IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Application (BIC-TA) 2010, pp.132-136.

[68] Wang Xingyuan and Chuanming Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," Multimedia Tools and Applications, 2016, pp.1-17.

[69] Wang Xing-Yuan, Ying-Qian Zhang and Xue-Mei Bao, "A novel chaotic image encryption scheme using DNA sequence operations," Optics and Lasers in Engineering, volume 73, 2015, pp. 53-61.

[70] Wang Xing-Yuan, Ying-Qian Zhang and Yuan-Yuan Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," Nonlinear Dynamics, volume 82, issue 3, 2015, pp.1269-1280.

[71] X. Zhang, Z. Zhao, J. Wang, “Chaotic image encryption based on circular substitution box and key stream buffer”, Signal Process.: Image Communication, volume 29, issue 8, 2014, pp. 902-913.

[72] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyperchaotic system," Nonlinear Dynamics, volume 84, issue 4, Jun 2016, pp. 2333-2356.

[73] Xiangjun Wu, Haibin Kan and Jurgen Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," Applied Soft Computing, volume 37, 2015, pp.24-39.

[74] Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, Shiguo Lian, “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system,” Journal of Systems and Software, volume 85, issue 2, 2012, pp. 290-299.

[75] Xie, Yaqin, Jiayin Yu, Shiyu Guo, Qun Ding, and Erfu Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system," Entropy, volume 21, issue 9, 2019, pp. 819-836.

[76] You, Lin, Ersong Yang, and Guangyi Wang, "A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation," Soft Computing, 2020, pp. 1-15.

[77] Yu, Jiayin, Chao Li, Xiaomeng Song, Shiyu Guo, and Erfu Wang, "Parallel mixed image encryption and extraction algorithm based on compressed sensing." Entropy, volume 23, issue 3, 2021, pp.278-298.

[78] Zhang H., Wang X., Sun Y., Wang X., “A novel method for lossless image compression and encryption based on LWT, SPIHT and cellular automata,” Signal Processing: Image Communication, volume 84, 2020.

[79] Zhang Linlin, Tiegang Gao and Rui Yang, "DNA coding and central dogma-based Image encryption using vigenere cipher and chaos map," IEEE Fifth International Conference on Intelligent Control and Information Processing (ICICIP) 2014, pp.80-85.

[80] Zhang Quang, Ling Guo, Xianglian Xue, and Xiaopeng Wei, “An image encryption algorithm based on DNA sequence addition operation,” IEEE Fourth International Conference on Bio-Inspired Computing (BIC-TA'09) 2009, pp. 75-79.

[81] Zhen P, Zhao G, Min L, Jin X, “Chaos-based image encryption scheme combining DNA coding and entropy,” Multimedia Tools and Applications, volume 75, issue 11, 2016, pp. 6303-19.

[82] Zhou S, He P, Kasabov N, “A Dynamic DNA Color Image Encryption Method Based on SHA-512”, Entropy, 2020, volume 22, issue 10, 1091, pp. 1-23.

[83] Zhou Shihua, Qiang Zhang and Xiaopeng Wei, "An image encryption algorithm based on DNA self-assembly technology," IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS) volume 2, 2010, pp.315-319.

[84] Zhou Shihua, Qiang Zhang and Xiaopeng Wei, "Image encryption algorithm based on DNA sequences for the big image,” IEEE International Conference on Multimedia Information Networking and Security (MINES) 2010, pp.884-888.

[85] Zhou, Qing, Kwok-wo Wong, Xiaofeng Liao, Tao Xiang, and Yue Hu. "Parallel image encryption algorithm based on discretized chaotic map," Chaos, Solitons and Fractals, volume 38, issue 4, 2008, pp.1081-1092.