# Visvesvaraya Technological University

BELAGAVI, KARNATAKA

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ

ಬೆಳಗಾವಿ, ಕರ್ನಾಟಕ

**Report on Project Phase-1**

# "Image encryption using DNA addition combining with chaotic maps"

**Submitted by**

| | | |
|---|---|---|
| 1. | SUSHMA H P | 4JN18IS105 |
| 2. | SYEDA FATHIMA ZAHARA | 4JN18IS108 |
| 3. | ZUBIA A KHAN | 4JN18IS118 |
| 4. | POOJA REDDY K | 4JN19IS408 |

**Under the guidance of**

**Mr. SAYED AFTAB AHAMED B.E, M. Tech.,**

**Assistant Professor,**
**Dept. of IS&E,**
**JNNCE, Shivamogga.**

Department of Information Science & Engineering
J N N College of Engineering
Shivamogga - 577 204
2021-22

National Education Society ®

J N N COLLEGE OF ENGINEERING

SHIVAMOGGA-577204.

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

# CERTIFICATE

This is to certify that Project entitled

## “Image encryption using DNA addition combining with chaotic maps”

### Submitted by

| | | |
|---|---|---|
| 1. | SUSHMA H P | - 4JN18IS105 |
| 2. | SYEDA FATHIMA ZAHARA | - 4JN18IS108 |
| 3. | ZUBIA A KHAN | - 4JN18IS118 |
| 4. | POOJA REDDY | - 4JN19IS408 |

students of 8th semester B.E. ISE, in partial fulfilment of the requirement for the award of degree of Bachelor of Engineering in Information Science and Engineering of Visvesvaraya Technological University, Belagavi during the year 2021-22.

Signature of Guide

**Mr. Sayed Aftab Ahamed** B.E, M.Tech

**Assistant Professor,**
**Dept. of IS&E,**
**JNNCE, Shivamogga**

Signature of HOD

**Dr. R Sanjeev Kunte** M.Tech, Ph.D

**Professor & Head,**
**Dept. of IS&E,**
**JNNCE, Shivamogga**

# ABSTRACT

Image encryption is used to enhance the protection of images when they are transferred over the network. Due to the complex properties of chaotic systems, chaos-based image encryption has been extensively investigated and used for real-time, secure transmission of images over networks. An implementation of digital image encryption scheme based on the mixture of chaotic systems is reported.

In this project an efficient image encryption scheme based on DNA sequence addition operation and chaos been proposed. The proposed algorithm consists of three stages: First, a DNA sequence matrix is obtained by encoding the original image, then, divide the DNA sequence matrix into some equal blocks and use the DNA sequence addition operation to add these blocks. Next, perform the DNA sequence complement operation to the result of the added matrix by using two Logistic maps. Finally, decode the DNA sequence matrix from the third step, and we can get the encrypted image.

# ACKNOWLEDGEMENT

We are grateful for our parents' support. On the very outset of this project report on "Image encryption using DNA addition combining with chaotic maps", we would like to extend our sincere & heartfelt obligation towards all the persons who have helped us in this endeavour. Without their active guidance, help, cooperation & encouragement, we would not have made headway in the project. We are grateful to our institution J N N College of Engineering and the Department of Information Science and Engineering for imparting us the knowledge with which we can do our best.

We would like to express our gratitude and thanks to Principal **Dr. K. Nagendra Prasad,** Principal, JNNCE, Shimoga for providing a good working environment and for his constant support and encouragement.

We would also like to express our gratitude and thanks to Head of the Department **Dr. R. Sanjeev Kunte,** Department of Information Science & Engineering for providing a good working environment and for his constant support and encouragement.

We would like to thank our guide, **Mr. Sayed Aftab Ahamed**, Assistant Professor, Department of Information Science and Engineering, for her expert guidance, initiative, and encouragement that led us through the presentation.

Also, we would like to thank our **Project Coordinators**, Department of Information Science and Engineering. We are highly indebted to them for their guidance and constant supervision as well as for providing necessary information regarding the project.

We are thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of the Department of Information Science and Engineering. Also, we would like to extend our sincere regards to all the non-teaching staff of Department of Information science and Engineering for their timely support.

**SUSHMA H P(4JN18IS105)**

**SYEDA FATHIMA ZAHARA(4JN18IS108)**

**ZUBIA A KHAN(4JN18IS118)**

**POOJA REDDY K(4JN19IS408)**

# CONTENTS

# LIST OF FIGURES

## CHAPTER 1:

# INTRODUCTION

Since computer networks have been widely applied, people's communications have had a revolutionary change, and transmission of digital images over the Internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital images to serious threats in the process of transmission. Consequently, people have to pay more and more attention to security and confidentiality of multimedia information.

Among various protection methods, the image encryption technique is one of the most efficient and common methods for the protection of image information. Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for image encryption. So, a new research method of image encryption is acquired urgently.

The chaotic system is a deterministic nonlinear system. It possesses varied characteristics, such as high sensitivity to initial conditions, determinacy and so on. Chaotic sequences produced by chaotic maps are pseudo-random sequences; their structures are very complex and difficult to analyse and predict. In other words, chaotic systems can improve the security of encryption systems.

The extant cryptography algorithms based on chaotic maps can be classified into two kinds:

permutation and diffusion. In the permutation stage, the positions of pixels from the original image are changed by chaotic sequences or by some matrix transformation. The permutation algorithm has a better encryption effect, but without changing the pixel values, leading to the histogram of the encryption image and the original image being duplicates thus, its security could be threatened the statistical analysis.

In the diffusion stage, the pixel values of the original image are changed by chaotic sequences. Most of these methods are directly implemented encryption by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image. Compared to the permutation, diffusion may lead to higher security, but the encryption effect is not good.

In today's highly information society, images are widely distributed across the Internet. At the same time, the security of digital images faces an increasingly grim threat in the process of dissemination. Unlike text encryption, digital images have the characteristics of a strong correlation between adjacent pixels and high redundancy. These characteristics lead to the traditional methods do not apply in respect of image encryption. The chaotic systems are very applicable for image encryption system because of its sensitivity to initial state and control parameters, good pseudorandom, ergodicity, unpredictability of orbit and soon. Due to these advantages of chaotic systems, researchers in recent years have incorporated it into image encryption systems and have proposed many excellent image encryption algorithms.

In general, image encryption algorithms are divided into two steps: permutation and diffusion. In the permutation stage, the location of pixels is moved; In the diffusion stage, the value of pixels is changed. In fact, the more common way is to combine these two steps to get higher safety. An encryption scheme based on this structure. They scramble the color image at the bit level, and the scramble sequences are generated by piece-wise linear chaotic mapping.

Then they use Chen's system to diffuse and confuse the pixel matrix. Thus, the image encryption algorithm with large key space is obtained. However, due to the limited computing accuracy of computers, the orbits of low-dimensional chaotic systems have short periodicity, thus this has caused some defects such as narrow key space. To overcome this short coming, a lot of (Coupled Map Lattice) CML-based spatiotemporal chaos system image encryption algorithms are proposed. The security of these algorithms is greatly improved because the CML system has more excellent chaotic dynamic characteristics, and a larger key space.

However, these algorithms are not fool proof, and there is still some hidden danger. Some encryption schemes have been shown to be insecure. The main drawback of these encryption schemes is that they are not associated with plain text image information in the encryption process, and therefore cannot effectively resist the chosen plaintext attacks. DNA computing is often used for cryptography systems because of its large amount of huge storage, parallelism and low power consumption.

Many DNA (Deoxyribose Nucleic Acid) sequence-based encryption algorithms have been designed in recent years. The encryption method combined with DNA computing can effectively solve the one-time pad problem, and in the encryption system, a huge one-time pad technology can help to resist the chosen plain text attacks. For instance, it combined the three-dimensional chaotic system with the cyclic operation of DNA sequences to operate plain image. They use the

Chen’s system to generate DNA encoding rules, encode the original image as a DNA matrix. After that, some related DNA sequence operations were performed on the DNA matrix.

A mixed adjacent and non-adjacent coupled mapping lattice. They improved a kind of coupled map lattice, and then encrypted the image with DNA computing. The algorithm achieved better performance. Taking into account the factors of the above analysis, we combine CML and DNA sequences to propose a new encryption scheme. First, we encode the original image to DNA matrix, and then the DNA matrix is performed right cyclic and up cyclic shift on the even rows and columns, respectively. After that, we further scramble the even-numbered rows in the scrambled DNA matrix.

Using the DNA sequence generated by the CML system and the designed DNA calculation rules, the scrambled DNA matrix is further diffused. Finally, the DNA decoding is performed on

DNA matrix to obtain the final cipher image. Simulation experiments and security analysis prove that the algorithm not only has significant effects but also can compete various attack methods.

The significance of information security is increasing with digitization. Cryptography plays a vital role in confidentiality, integrity and availability of information. With growing computability, the digital security stakes are higher than ever. A strong protection is required to tackle data cracking. DNA (Deoxyribose Nucleic Acid) and chaotic system based joint cryptography is an emerging area due to achieving new levels of security, especially that of color images and videos.

In order to effectively and efficiently utilize the security as provided by this joint cryptography, its understanding is an emergent and open challenge. This paper undertakes this research case for the security of color images. Their richness of colours renders them as a popular choice for capturing realistic expressions, whether they are natural scenes or arti-facts. Security concern of color images is highly desired for ensuring their privacy in various application domains, hence cannot be undermined. To this end, we present an encryption algorithm and analyse its security performance.

Efficiency in the bonding of DNA molecular structure enables parallelism and extra ordinary storage, promising bright future for cryptography. DNA is a hereditary material of living organisms and consists of double strands moving antiparallel to each other. It is a long polymer consisting of small units of nucleotides, with each nucleotide made up of nitrogenous base, 5carbon sugar and at least one phosphate group. Depending upon the type of nitrogenous base, there are four different nucleotides called Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Pairs of these bases are connected to each other in specific sequences through hydrogen bonds, thus keeping the two strands connected.

A gene is a distinct sequence of nucleotides that contains genetic information of all living organisms. DNA computing towards information security is promising. Digital DNAs available from public genetic databases have billions of nucleotides, thus enable a huge space with an increased uncertainty. If used effectively by following the DNA sequencing, synthesis, recombination and hybridization operations, it leverages generation of strong cryptographic keys. DNA based cryptography benefits from techniques such as One Time Pad (OTP), DNA fragmentation and DNA amplification through Polymerase Chain Reaction (PCR). As it can be generally noted, information randomization is the fundamental process for securing data. Multiple and independent randomization processes applied to data, introduce multiple security barriers.

Though cryptography methods are majorly based on randomization, they tend to be application area specific. For instance, plaintext can be encrypted using DNA microdots, a technique which is not directly applicable for securing images. Images can be encrypted by processing them in a breadth first pattern. The processing is based on the Chaos Theory and includes scrambling, permutation, shuffling and dynamic diffusion, and 3D permutation. Other than breadth first pattern (row-wise), column-wise and diagonal-wise are also possibilities.

Cryptography can be done using digital watermarking, canny edge detection and visualization. A plain image can be encrypted by fragmenting it into non-overlapping blocks for adding water marks that are followed by DNA addition and complementation using a Logistic Map. The Logistic Map generates the DNA matrix and encoding rules for the plain image. DNA addition on a DNA encoded image and DNA matrix gives additive DNA. The information entropy of additive DNA is diffused through Logistic Map, which increases the degree of confusion and diffusion.

Visual encryption scheme is demonstrated by transforming a plain image into Visually Meaningful Encrypted Image (VMEI) using a Logistic Map and a Gray S-Box. Other than encrypting images offline, there is a possibility of real time encryption. For instance, in a live communication setup, encryption with a low computation overhead is possible using a chaotic map. A highly secured encryption system can be achieved by combining two chaotic systems and four cryptographic phases, namely, diffusion based on XOR, substitution based on S-boxes, diffusion based on a chaotic map and block permutation for reinforcement of the statistical results.

Diffusion in multiple rounds based on bit permutation generator and bit diffusion generator has yielded promising encryption results. These generators rely on SHA-256 bit (Secure Hash Algorithm). In this scheme, an input plain image is divided into small blocks and the blocks having high correlation coefficients are XORed with the threshold values produced by a skew (neither parallel nor intersecting) tent map.

Finally, the entire image is shuffled using two random sequences generated from Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS). Considering the advancement of DNA/quantum computing, it is increasingly becoming likely to breach highly secured information, whether it is text, image or videos. Security methods based on one or multiple chaotic systems mainly rely on PWLCM (piece wise linear chaotic map) an. Still there is little or no work done using 4D Lorenz-type chaotic systems.

Also, though multistage encryption methods are proposed but there is a lack of such method that relies on a real DNA sequence based Linear Feedback Shift Register (DLFSR), which itself is supported by a chaotic generator. We hypothesize that such encryption systems will bring security to another level, especially when multiple security aspects are considered.

Due to exponential increase in usage of social media, secure transmission of images over public networks is one of the prime concerns that have evolved gravely. The current state of affairs in enhanced computability renders the security measures susceptible to potential security breaches.

Thus, the security requirements on sensitive images and video frames of public/private organizations are stringent than ever. To this end, we aim to keep the protection intact as much as practically possible. Motivated by image encryption schemes and cryptanalysis, we contribute by designing and proposing a symmetric image encryption algorithm. It is based on three chaotic systems (PWLCM-piece wise linear chaotic map and Lorenz for permutations, and 4D Lorenztype for key generation), a Scrambler for image jumbling and DNA sequence based Linear Feedback Shift Register (DLFSR) that is supported by a chaotic generator. It also uses a technique to convert binary data to nucleotides bases and vice versa.

## 1.1 PROBLEM DESCRIPTION

In cryptography there is a constraint of co-relation coefficient and it takes long time. To overcome this, we prefer DNA sequence addition operation and chaos. Hence, Chaotic systems are distinguished by sensitive dependence on initial conditions and by having evolution through phase space that appears to be quite random. The behaviour of a Chaotic system is unpredictable. Therefore, it resembles noise. Hence, it is required to design a secure chaotic based encryption system which takes images as input and encrypts the image into Cipher image.

## 1.2 OBJECTIVES

1) To design an image encryption system using DNA sequence addition operation and chaos cryptography having less Peak Signal to Noise Ratio (PSNR) and high Mean Square Error (MSE).
2) To analyse the performance of the developed chaotic cryptography system.
3) To find the Histogram error between the images.
4) To achieve high entropy value.
5) To analyse the Randomness of the generated chaotic sequences.

## 1.3 ORGANIZATION OF REPORT

The further report includes following contents, Chapter 2 consists of literature survey of different reference papers, Chapter 3 represents system design of the proposed work, and Chapter 4 consists of conclusion of the proposed work and includes references of the proposed work.

## CHAPTER 2:

# LITERATURE SURVEY

Qiang Zhang et.al. [1]. Proposed Image encryption using DNA addition combining with chaotic maps. Since computer networks have been widely applied, people’s communications have had a revolutionary change, and transmission of digital images over the Internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital images to serious threats in the process of transmission. Consequently, people have to pay more and more attention to security and confidentiality of multimedia information. Among various protection methods, the image encryption technique is one of the most efficient and common methods for the protection of image information.

Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for image encryption. So, a new research method of image encryption is acquired urgently. The chaotic system is a deterministic nonlinear system. It possesses varied characteristics, such as high sensitivity to initial conditions, determinacy and so on [1–6]. Chaotic sequences produced by chaotic maps are pseudo-random sequences; their structures are very complex and difficult to analyse and predict. In other words, chaotic systems can improve the security of encryption systems.

The extant cryptography algorithms based on chaotic maps can be classified into two kinds: permutation and diffusion. In the permutation stage, the positions of pixels from the original image are changed by chaotic sequences or by some matrix transformation. The permutation algorithm has a better encryption effect, but without changing the pixel values, leading to the histogram of the encryption image and the original image being duplicates; thus its security could be threatened the statistical analysis. In the diffusion stage, the pixel values of the original image are changed by chaotic sequences.

Most of these methods are directly implemented encryption by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image. Compared to the permutation, diffusion may lead to higher security, but the encryption effect is not good.

Thereby, in order to improve the security and the encryption effect, some researchers have combined permutation and diffusion.

In this paper, we used 2D Logistic and 1D Logistic maps whose definitions are as follows. 2D Logistic map is described as Eq. (1):

$$\begin{cases} x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_i^2; \\ y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i); \end{cases} \quad (1)$$

When $2.75 < \mu 1 \leq 3.4$, $2.75 < \mu 2 \leq 3.45$, $0.15 < \gamma 1 \leq 0.21$, $0.13 < \gamma 2 \leq 0.15$

The system is in a chaotic state and can generate two chaotic sequences in the region (0,1]. Due to the system parameters γ1 and γ2 having a smaller value range, we set $\gamma 1 = 0.17$ and $\gamma 2 = 0.14$, the other parameters can be seen as secret keys. 1D Logistic map is an example chaotic map, it is described as follows:

$$xn+1 = \mu xn\ (1 - xn). \quad (2)$$

Where $\mu \in [0, 4]$, $xn \in (0, 1)$, n = 0, 1, 2, . . . the research result shows that the system is in a chaotic state under the condition that $3.56994 < \mu \leq 4$.

**Advantages:**

- The simulation experimental results and security analysis show that our scheme not only can achieve good encryption, but can also resist exhaustive attack, statistical attack and differential attack.
- Compared to the permutation, diffusion may lead to higher security.

**Disadvantages:**

- Its security could be threatened the statistical analysis in Permutation algorithm.
- The encryption effect is not good.

Tian Tian Zhang et.al. [2]. Proposed Image Encryption using Based on DNA Sequence and Chaos Theory. Encryption is an efficient way to keep image data free from attackers. In these encryption techniques, the chaotic image encryption method is more and more concerned because of the unpredictability of chaotic signals, the sensitivity to control parameters, the presence of the initial value, etc. Many scholars are engaged in the research on the application of the combination of chaos theory and cryptography in encrypting image and improving the encryption level of cipher. Chaos theory has been widely applied to many subjects and become an important frontier science.

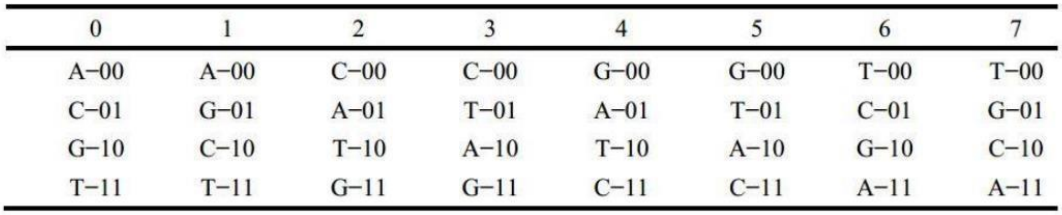
The basic concept and the results of the study:

- **Chaos theory:**

Chaotic system is a kind of peculiar motion form, which has a very good randomness. We often use this property to generate random sequences, thus disrupting the original image and getting satisfactory results. In this paper, we will choose one-dimensional logistic mapping as the chaotic system.

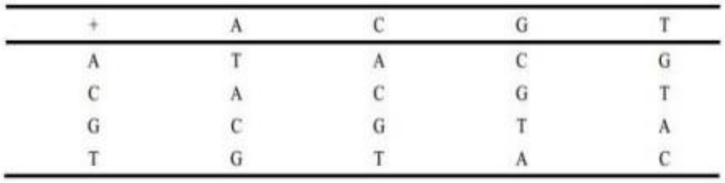
- **DNA (Deoxyribose nucleic acid):**

DNA is like the human body's password, its code word is A, T, C, G appearing with pairs. In image encryption, we can apply this rule to the encoding. Figure 1 shows the coding depending on DNA. Figure 2,3 propose DNA addition and subtraction rules.



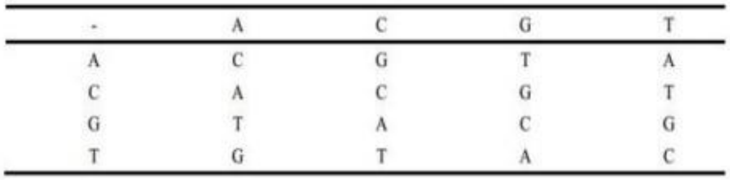
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| A−00 | A−00 | C−00 | C−00 | G−00 | G−00 | T−00 | T−00 |
| C−01 | G−01 | A−01 | T−01 | A−01 | T−01 | C−01 | G−01 |
| G−10 | C−10 | T−10 | A−10 | T−10 | A−10 | G−10 | C−10 |
| T−11 | T−11 | G−11 | G−11 | C−11 | C−11 | A−11 | A−11 |

**Fig 2.1: Eight encoding rules for DNA sequences.**



| + | A | C | G | T |
|---|---|---|---|---|
| A | T | A | C | G |
| C | A | C | G | T |
| G | C | G | T | A |
| T | G | T | A | C |

**Fig 2.2: DNA Addition rule.**

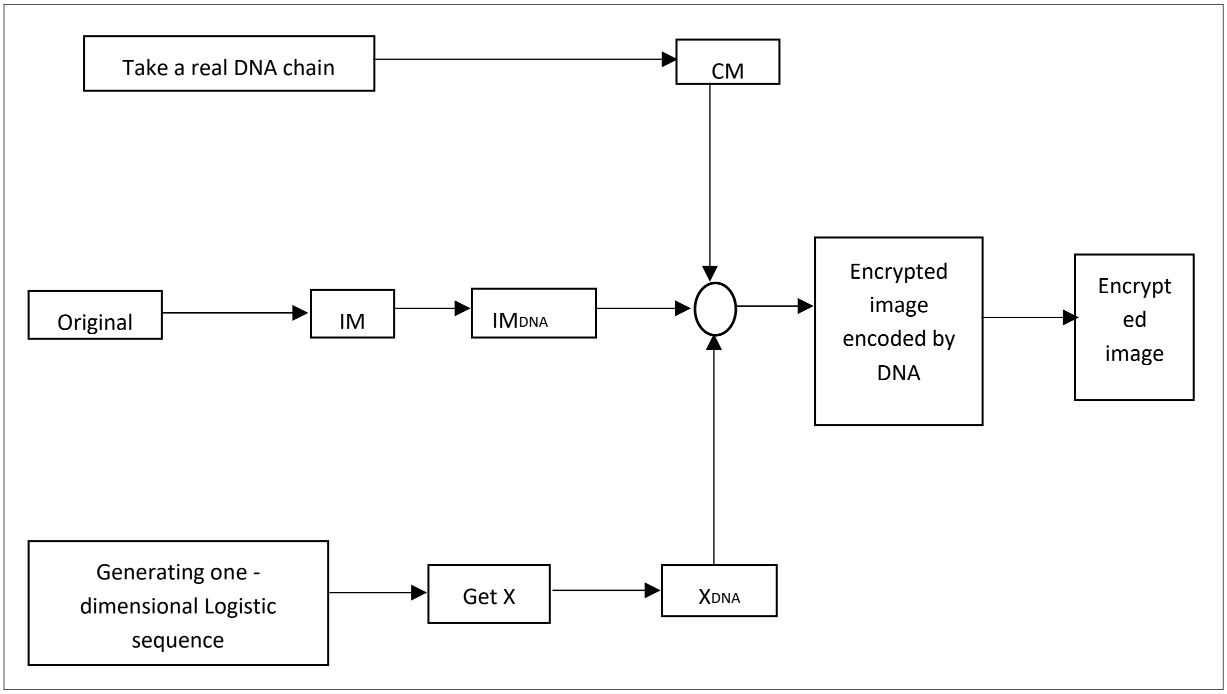


| - | A | C | G | T |
|---|---|---|---|---|
| A | C | G | T | A |
| C | A | C | G | T |
| G | T | A | C | G |
| T | G | T | A | C |

**Fig 2.3: DNA Subtraction rule.**

### 1.1 Flow chart

This flow chart of this algorithm is shown as figure 4, which uses DNA encoding and DNA sequence:



Take a real DNA chain
CM
Original
IM
IMDNA
Encrypted image encoded by DNA
Encrypted image
Generating one -dimensional Logistic sequence
Get X
XDNA

**Fig 2.4: Flow chart of algorithm.**

**Key generation**

**Input**: Original image, DNA, value of Logistic mapping

**Output**: Encrypted image

### 3.2.1. Pre-treatment

**Step1**：Choose a real DNA sequence.

**Step2**：Arrange the sequence into a matrix (512*4*512), which is named CM.

**Step3**：Using a programmer to produce a sequence of a one-dimensional logistic chaotic mapping, which is given initial value: μ=4, $X_0 = 0.53$.

**Step4**：Choose the eighth bit of each number, named as X. If X is even, change the value into 0, or into 1.

**Step5**：Using the former DNA method to encode X, then we get $X_{DNA}$.

### 3.2.2. Encryption

**Step 6**: Convert the image into a matrix, whose grey value is between 0-255, named as

IM. (two-dimensional)

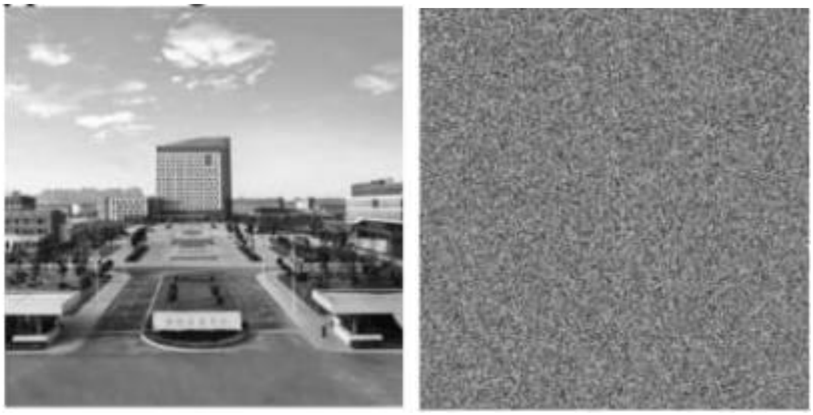
**Step 7**: Using the DNA encoding method again to encode the matrix IM. The result is named as $IM_{DNA}$.

**Step8**: Adding the previous three matrices, which is from step 2, step 5 and step 7, the result is called matrix P.

**Step9**: Applying the selective transformation into P. Define the formula of supplemental transformation: (it is the key step in the algorithm).

$$\text{Complement}_z(Y)= \begin{cases} Y, \text{ if } X_i=0 \\ \text{Complement}(Y), \text{ if } X_i=1 \end{cases}$$

End: Obtain the encrypted image, which is shown in figure 5.



(a) Original image. (b) Encrypted image.

**Fig 2.5: The result using the MATLAB software (a) original image (b) encrypted image**

**Advantages:**

- This algorithm can also reverse the above operations and obtain the original image.

**Disadvantages:**

- It has complicated operations and difficult to grasp its biotechnology.

Muhammad Samiullah et.al.[3]. Proposed An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems. The significance of information security is increasing with digitization. Cryptography plays a vital role in confidentiality, integrity and availability of information. With growing computability, the digital security stakes are higher than ever. A strong protection is required to tackle data cracking. DNA (Deoxyribo Nucleic Acid) and chaotic system based joint cryptography is an emerging area due to achieving new levels of security, especially that of color images and videos. In order to effectively and efficiently utilize the security as provided by this joint cryptography, its understanding is an emergent and open challenge. This paper undertakes this research case for the security of colour images. Their richness of colours renders them as a popular choice for capturing realistic expressions, whether they are natural scenes or arti-facts. Security concern of colour images is highly desired for ensuring their privacy in various application domains, hence cannot be undermined. To this end, we present an encryption algorithm and analyse its security performance.

We propose a symmetric key DNA extended chaotic encryption algorithm; hereafter called SDC-Encryption (SHA DNA Chaotic Encryption) that aims at improving the information security (refers Algorithm SDC-Encryption). DNA is considered a high-speed cryptography technique, which is suitable to encrypt large volume of data [41]. SDC-Encryption is applied on plain colour image.

## INITIAL CONDITIONS AND CHAOS:

SDC-Encryption uses a chaotic system to increase randomness in the encryption image. Let PI denote the plain RGB image (m × n). Initial conditions for the chaos are set as follows.

The average of first row, first four-pixel values, Algorithm SDC-Encryption. Input: A plain colour image (m × n), initial conditions for three chaotic systems (PWLCM, Lorenz and 4D Lorenz-type) and seeds for the chaotic generator and the Shift register. Output: An encrypted image (m × n).

**Step 1:** Choose the SHA based on the average value of first four pixels of the plain color image and generate new initial conditions (details in Section III A).

**Step 2:** Take transpose of the plain color image (details in Section III B).

**Step 3:** Generate two fake images (of same size as the plain color image) and split them into their R, G and B components.

**Step 4:** The found R, G and B components are passed to a PWLCM system for iterations, producing three processed R, G and B components that are concatenated to form a processed image whose pixel values are then sorted.

**Step 5:** Generate a new image by permuting the pixel values of Step 2 image. Permutation is done by considering the pixel values of Step 4 image as indices into Step 2 image.

**Step 6:** Step 5 image is split into R, G and B components.

**Step 7:** Step 6 R, G and B components are passed to a Lorenz chaotic system, producing three R, G and B com-ponents whose pixel values are then sorted individually.

**Step 8:** Generate three new R, G and B components by per-muting the R, G and B components of Step 6. Permutation is done by considering Step 7 component pixel values as indices into Step 6 corresponding R, G and B components.

**Step 9:** A Scrambler function maps each of Step 8 components and corresponding keys to new R, G and B components. The corresponding keys are generated using Fourth Order Runge Kutta method, a hyperchaotic system (details in Section III C).

**Step 10:** The R, G and B components of Step 9 undergo DNA sequence encoding, which is based on DNA encoding rules, DNA complementing and DNA XORing.

**Step 11:** Symbols in the DNA encoded chain of Step 10 undergo DNA sequence decoding. The result is considered as encrypted R, G and B components, which are concatenated to form an encrypted image.

**Step 12:** The final post processing key, fkey, is generated by XORing the output of the Logistic Map based chaotic generator and DLFSR. The DLFSR is activated by the real DNA sequence. The encrypted image of Step 11 is XORed with key to get the final encrypted image (details in Section III D).

The significance of information security is increasing with digitization. Cryptography plays a vital role in confidentiality, integrity and availability of information. With growing computability, the digital security stakes are higher than ever. A strong protection is required to tackle data cracking. DNA (Deoxyribo Nucleic Acid) and chaotic system based joint cryptography is an emerging area due to achieving new levels of security, especially that of color images and videos.

In order to effectively and efficiently utilize the security as provided by this joint cryptography, its understanding is an emergent and open challenge. This paper undertakes this research case for the security of color images. Their richness of colours renders them as a popular choice for capturing realistic expressions, whether they are natural scenes or artifacts. Security concern of color images is highly desired for ensuring their privacy in various application domains, hence cannot be undermined. To this end, we present an encryption algorithm and analyse its security performance.

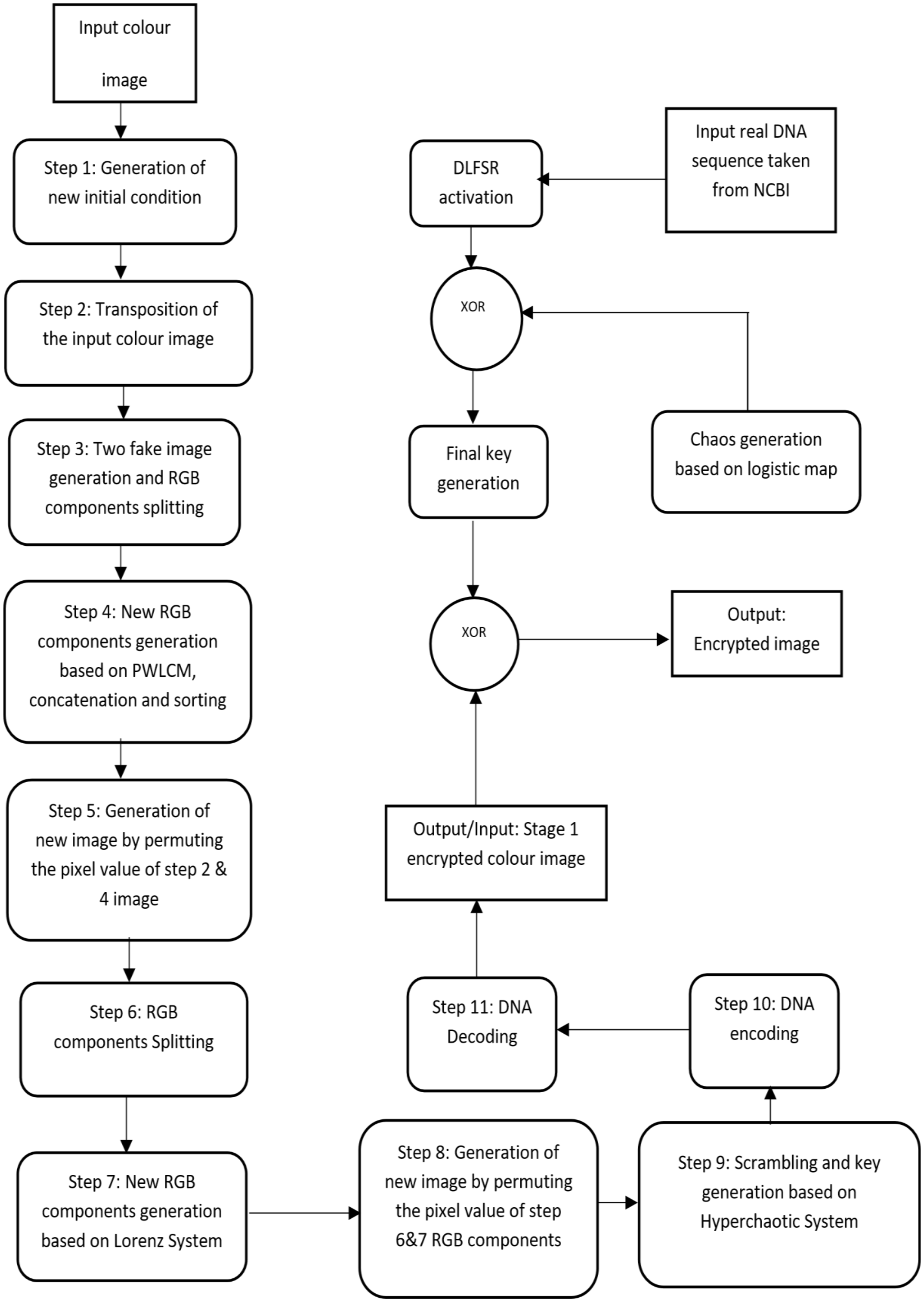

Input colour image
Step 1: Generation of new initial condition
Step 2: Transposition of the input colour image
Step 3: Two fake image generation and RGB components splitting
Step 4: New RGB components generation based on PWLCM, concatenation and sorting
Step 5: Generation of new image by permuting the pixel value of step 2 & 4 image
Step 6: RGB components Splitting
Step 7: New RGB components generation based on Lorenz System
Step 8: Generation of new image by permuting the pixel value of step 6&7 RGB components
Step 9: Scrambling and key generation based on Hyperchaotic System
Step 10: DNA encoding
Step 11: DNA Decoding
Output/Input: Stage 1 encrypted colour image
Input real DNA sequence taken from NCBI
DLFSR activation
XOR
Chaos generation based on logistic map
Final key generation
XOR
Output: Encrypted image

**Fig 2.6: The flowchart of SDC-Encryption algorithm.**

These are the steps involved in the flowchart of SDC-Encryption Algorithm

**Step 1:** Generation from new initial condition comes from input color image.

**Step 2:** Transposition of the input color image.

**Step 3:** Two fake image generation and RGB components splitting.

**Step 4:** New RGB components generation placed on PWLCM, concatenation and sorting.

**Step 5:** Generation of new image by permuting the pixel value of step 2 and 4 image.

**Step 6:** RGB components splitting.

**Step 7:** New RGB components generation based on Lorenz system.

**Step 8:** Generation of new image by permuting the pixel value of step 6 & 7 RGB components.

**Step 9:** Scrambling and key generation based on Hyperchaotic system.

**Step 10:** DNA coding.

**Step 11:** DNA decoding.

**Step 12:** Output or input.

In output, Stage 1: Encrypted color image forward to XOR goes to Output as an encrypted image from final generation to XOR. Input real DNA sequence taken from NCBI is DLFSR activation after this XOR to final generation from Chaos generation based on logistic map to XOR then Final key generation.

**Advantages:**

- DNA computing is applied to in cryptography. DNA cryptogram utilises DNA as information carrier and takes advantage of biological technology to achieve encryption.

**Disadvantages:**

- Right secret key must be used to decrypt the cipher image to the original image.

Zeeshan Ahmad et.al.[4]. Proposed A DNA-Based Security solution Using Aggregated Chaos Cross and Cubic Map. Chaos, cryptography and DNA, are three different kinds of disciplines, but they are closely related with different aspects. The research framework generated by the combination of these three disciplines is called Discrete Chaotic Cryptography (DCC). In this proposed a new methodology to scramble an image using Cross and cubic chaotic maps. Chaotic map is utilized to generate the more complicated pseudo random sequence with the help of binary key to generate the initial values and parameters. The key is modified after every step of encryption. We map the image pixels with the cross chaotic sequence and after scrambling, divide the permuted image into Least Significant Bits (LSB) and Most Significant Bits (MSB). Furthermore, the LSB and MSB are divided into two blocks each, which are L1, L2 and M1, M2. These blocks are then encoded by the DNA addition. Simulations results show the validity and superiority of the proposed methodology.

Figure 2.7 shows the permuted image by cross chaotic map.

$$\begin{cases} X_{i+1} = 1 - \mu . Y_{\mathbf{i}} . Y \\ Y_{i+1} = cos[kcos^{-1} x_{\mathbf{i}}]; \end{cases} , x, y \acute{I}[-1,1]$$

To reduce the computational complexity, we change the Equation 5 to one dimensional.

$$x_{i+i} = 1 - \mu(cos(k\,cos^{-1} x_i)^2$$

Where µ and k are the control parameters of the systems, µ=2 and k=6. The system shows great diversity of dynamic behaviour.

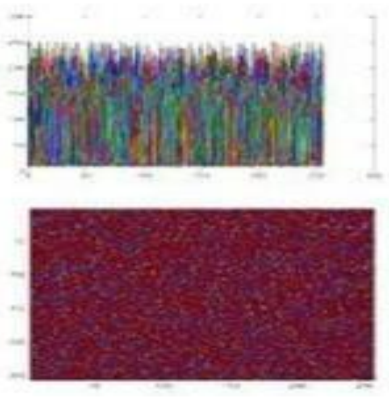


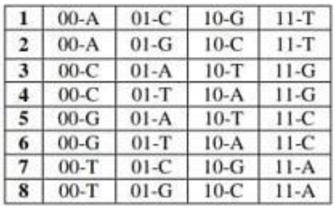
**Fig 2.7: Permuted image by cross chaotic map**

DNA Addition and Subtraction Rule Cryptography attracts extensive concerns from both public and government sides in recent years. Among various technologies we can use Biotechnological methods for cryptography. The transformation of data from digital to DNA bases is called encoding and the reverse process is called decoding. In cryptography of digital images, different cryptographic methods based on DNA binary strands exist.

The most common techniques to select one of the 8 rules for encoding and another rule from remaining 7 rules for decoding of all pixels of an image which reduces the capabilities of DNA transformation for early diffusion process. In confusion phase we convert the permutated image into binary image and divide the pixels into LSB and MSB blocks. Each block of the permutated image is encoded by the DNA encoding rule from Table1. L1 is encoded by rule 2 and L2 is encoded by rule 3. M1 is encoded by the rule 6 and M2 is encoded by the rule 7.

Next step is the DNA encoding phase. We add the L1 and L2 by using Table 2 and obtain a DNA sequence L-DNA and M-DNA next to combine them we apply the XOR algebraic operation with the help of key k2. Finally cipher image is obtained. Finally cipher image is obtained. Similarly, subtraction rules are given in Table 3.

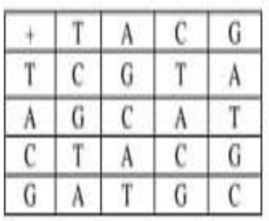
Table 1.



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

**Fig 2.8: DNA encoding rules.**

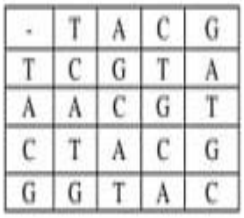
Table 2.



| + | T | A | C | G |
|---|---|---|---|---|
| T | C | G | T | A |
| A | G | C | A | T |
| C | T | A | C | G |
| G | A | T | G | C |

**Fig 2.9: Addition for DNA sequence.**

Table 3.



| - | T | A | C | G |
|---|---|---|---|---|
| T | C | G | T | A |
| A | A | C | G | T |
| C | T | A | C | G |
| G | G | T | A | C |

**Fig 2.10: Subtraction for DNA sequence.**

**Step 1:** Initial conditions are calculated using 96 bit long external key. The key is divided into twelve blocks of 8 bits.

K=K1, K2, K3, K4… K12 (6)

Here, each K represents the 8 bits of the secret key.

**Step 2:** To calculate X0, we choose the three blocks of the key.

B=K7, K8, K9

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K71 | K72 | K73 | .. | K78 | K81 | K82 | .. | K88 | K91 | K92 | K93 | .. | K98 |

Here Kij is the binary representation of the block; we compute the real number X01 using the following formula.

X1 = (K71 × 20 +K72 × 21 +……. K78 × 27 +

K81 × 28 +K82 × 29 +……K88 × 215 +

K91 × 216 +K92 × 217 +…. K98 × 223)/224

**Step 3:** Another real number Y is calculated using the blocks K4, K5 and K6 as below:

$$X_2 = \left[ \sum_{i=23}^{0} (K_i x 2^i) \right] / 2^{24}$$

$$X0 = (X1 + X2) mod 1$$

**Step 4:** Permute the image 'I' by using cross chaotic map Equation 5 and initial condition X0 and control parameters µ=2 and K= 6 obtained from Equation 6.

**Step 5:** The permuted image I is converted into binary image 'B'. Divide each pixel of the permutated image 'B' into LSB and MSB.

**Step 6:** LSB and MSB are further divided into L1, L2 and M1, M2 respectively.

**Step 7:** Encode each bit of L1 to obtain a sequence LY′1 by selecting DNA rules from encoding group of Table 1 and repeat the process for L2, M1 and M3.

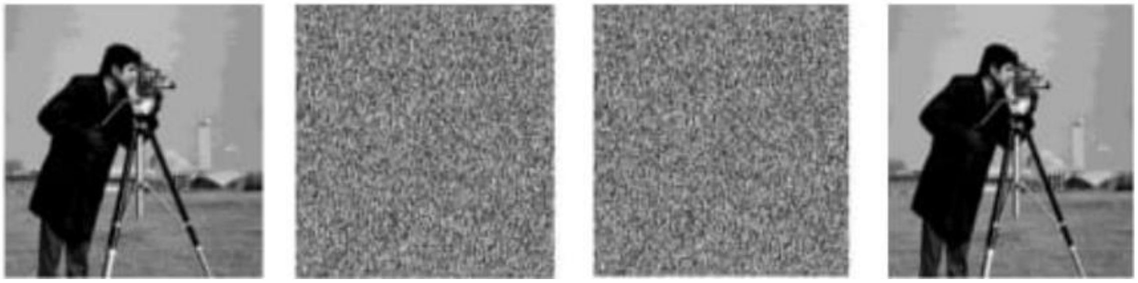
**Step 8:** Combine all LSB and MSB to get a new sequence C.

**Step 9:** Chaotic sequence is generated by CMM to permute the key.

**Step 10:** XOR operation is applied on the combined image using the permuted key.

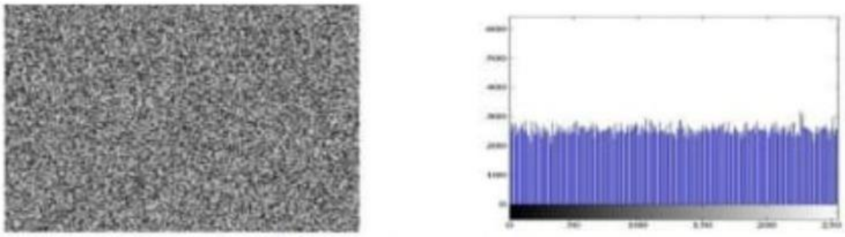
The key K1 is modified to K12 for the XOR operation.

(Ki)10= ((Ki)10+(K12)10) mod 256.



(a) Original image (b) Encrypted image (c) Decrypted image (d) Decrypted image with value.
Value correct initial value. with different initial value.

**Fig 2.11: Impact of initial value on decryption.**



(a) Decrypted image with different key space.

(b) Corresponding Histogram.

**Fig 2.12: Impact of key space on decryption.**

Result 2.11 and 2.12 shows that the proposed DNA insertion rule-based security solution is sensitive to the encryption key for both processes encryption and decryption with good confusion properties.

Saleh Ibrahim et.al.[5]. Proposed Framework for Efficient Medical Image Encryption using Dynamic S-Boxes and Chaotic Maps. The rapid development in networking and communication technology has led to significant advancement in multimedia and digital image communication. Medical images are important for assisting medical crews through diagnosis. Computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, and X-ray, provide a visual representation of body organs and tissue to help diagnosis and treatment planning. This valuable information includes the physical characteristics of the internal body organs such as size, shape, intensity, and position. With the global growth interest in patient records, all these important data including medical images are stored in Picture-and-Communication Servers. Moreover, many healthcare providers may need to exchange these records using convenient public networks to have access to the patients' health history. Medical images contain confidential information about patient health conditions.

Therefore, there is a need to protect and secure patients' privacy when using storage and communication technologies with various applications platforms. As a matter of fact, medical images can be vulnerable to security threats including unauthorized data access and tampering. Encryption schemes are usually employed to protect stored and communicated images against these threats. In addition to the high spatial correlation, medical images are characterized by their large volume.

High resolution imaging and 3D imaging produce large volumes of data per second. Image data need to be encrypted in real time before storage or transmission. Therefore, medical images require more efficient encryption algorithms capable of handling high data transmission rates. The performance of recent medical image encryption schemes, such as and generic image encryption schemes such as [9, 10] fall short of achieving real- time encryption speed.

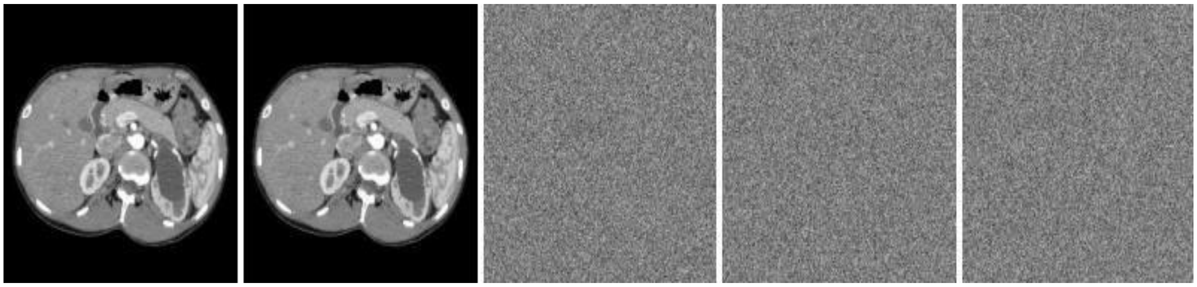

(a) **Original image** (b) **Changed image** (c) **original cipher image** (d) **Changed cipher image** (e) **Difference between cipher images**

**Fig 2.13: Visual results of plain image sensitivity analysis with Baker map showing.**

Results of encryption key sensitivity analysis, with respect to the dynamic S-box key are presented in Table XI. Results include correlation coefficient, UACI and NPCR for three medical images encrypted using two related dynamic S-box keys $KS$ and $K$. Results indicate high sensitivity to changes in dynamic S-box key.

Results of chaotic map encryption key sensitivity analysis are presented in Table XII. Each row indicates the results for one of the investigated chaotic maps, including the correlation coefficient, the UACI and the NPCR for three medical images encrypted using two related chaotic maps keys $KC$ and $KC$ such that $KC \oplus KC' = 1$. Results indicate high sensitivity to changes in chaotic map keys.

In this paper, we take advantage of two of the most efficient encryption constructs, S-boxes and chaotic maps to propose a generic framework for medical image encryption. The proposed framework combines the desirable statistical properties and diffusion of chaotic maps and the confusion power of dynamic key-dependent S-boxes.

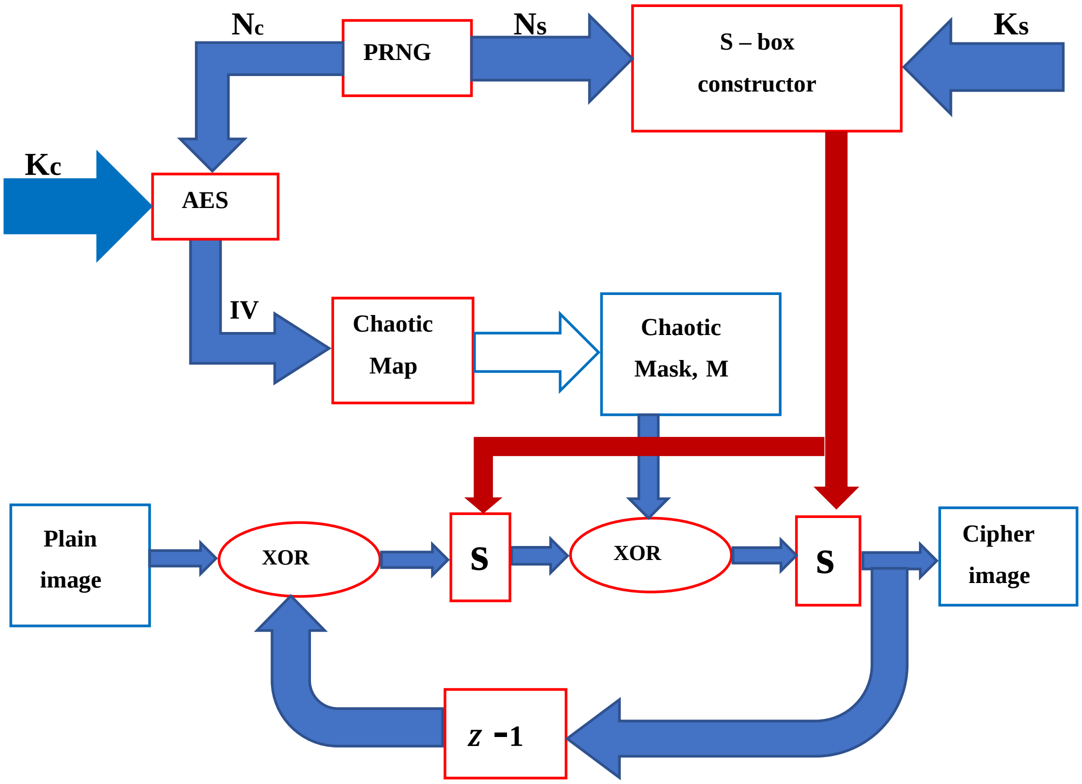


**Fig 2.14: Proposed image encryption framework.**

The proposed image encryption framework is based on two generic components. The first generic component is a key-dependent S-box construction algorithm, denoted $\mathbb{S}Ks$, where $KS$ is the key. Given an $\alpha$-bit initialization vector, $NS$ ∈$\{0,1\}\alpha$, $\mathbb{S}Ks(NS)$ produces a bijective 8 × 8 S-box. The second generic component is a chaotic pseudorandom source, denoted $\mathbb{C}$. Given a $\beta$-bit initialization vector, $IV$ ∈ {0,1} $\beta$, $\mathbb{C}(IV)$ can generate a pseudorandom byte stream of arbitrary length. $\mathbb{S}$ and $\mathbb{C}$ can be realized by many existing key-dependent S-box construction methods and chaotic systems

It is assumed that an encryption key is secretly shared by the communicating parties prior to the image communication session. The encryption key has two parts, $KS$, which controls the S-box construction and $KC$, which controls the generation of the chaotic sequence.

Given a plain image, $I$, to encrypt, the proposed framework works in two phases, as shown in Figure 1. During the preparation phase, a PRNG generates two nonce random numbers, $NS$ and $NC$, then $NS$is AES encrypted using key $KC$ to obtain the chaos initialization vector $IV$ = AES$Ks(NC)$. $\mathbb{S}$ constructs a dynamic S-box, $S$ = $\mathbb{S}Ks(N)$ and the initialized chaos source $\mathbb{C}(IV)$ generates a pseudorandom byte stream, $M$, of the same size of the plain image, $I$.

During the encryption phase, the constructed $S$ and $M$ are utilized to transform plain image pixels to cipher image pixels. A plain image pixel is first XORed with the previous cipher image pixel, indicated by the ($z$−1) in the block diagram. The result is then substituted using the S-box, $S$, then XORed with the corresponding value of the chaotic sequence, $M$. The result is finally substituted again using the same S-box, $S$, to produce the corresponding cipher image pixel. The nonce numbers $NS$ and $NC$ are stored in the cipher image header to facilitate decryption.

**Algorithm 1: Image Encryption**

**Input:** plain image, $I$, shared key ($KS$, $KC$), chaotic transient length $NT$

**Output:** cipher message, ($NS$, $NC$, $IC$)

1. Use the PRNG to generate two nonce, $NS$ and $NC$.

2. Construct a dynamic S-Box $S$ = $\mathbb{S}Ks(NS)$.

3. Initialize the chaotic source $\mathbb{C}$ using $IV$ = AES$Ks(NC$ ).

4. Iterate ℂ for $NT$ times to skip the transient effect.

5. Use ℂ to generate a chaotic sequence, $M$, of length #$I$.

6. For each plain image pixel $I(i, j)$, calculate $IC\ (i,j) = ck = S(S(I(i,j) \oplus ck{-}1\ ) \oplus mk\ )$, where $1 \leq k \leq \#I$, $c0 = 0$.

Output the cipher message ($NS$, $NC$, $IC$). As shown in Figure 2.15, to decrypt a cipher image, $NS$ and $NC$ are extracted from its header and used along with the shared secret keys, $KS$ and $KC$, to construct the corresponding chaotic sequence, $M$, and inverse S-box ($S{-}1$). Each cipher image pixel is substituted, XORed with the corresponding chaotic sequence value, substituted again, and finally XORed with the previous cipher image pixel. The encryption and decryption procedures are listed in Algorithm 1 and Algorithm 2, respectively.

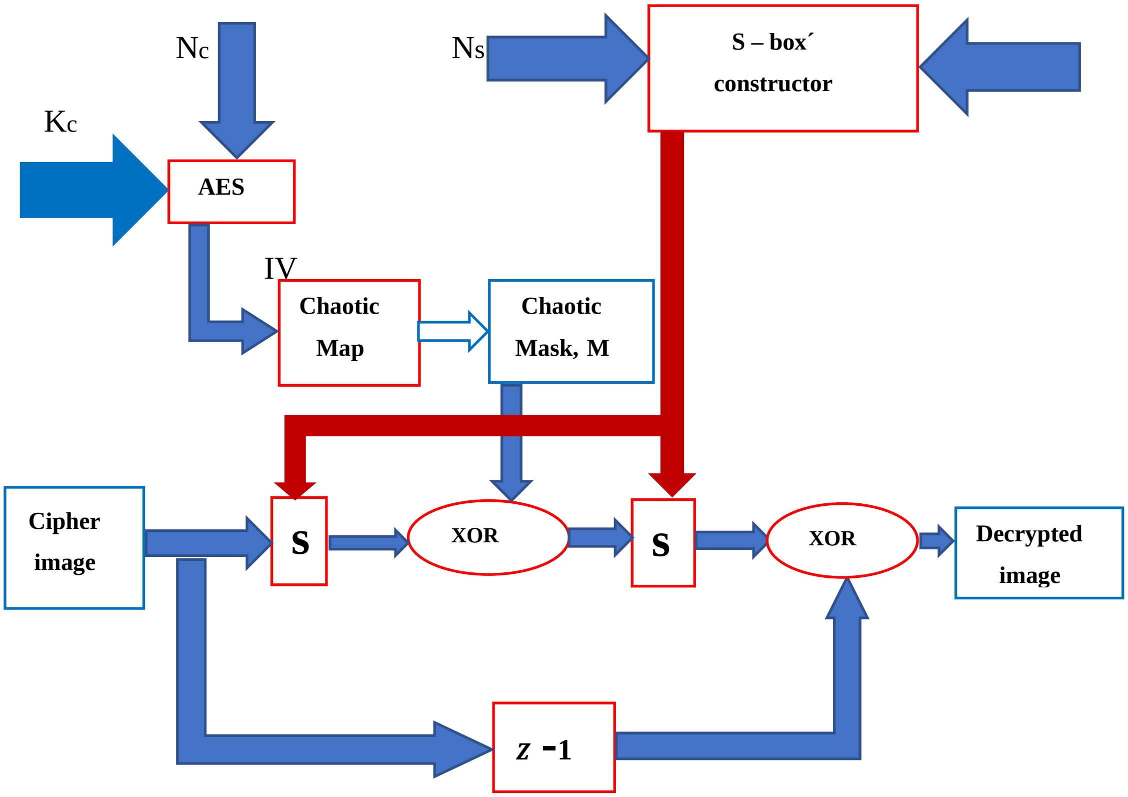


**Fig 2.15. Proposed image decryption framework.**

**Algorithm 2: Image Decryption**

**Input:** cipher message ($NS$, $NC$, $IC$), shared key ($KS$, $KC$), chaotic transient length $NT$

**Output:** decrypted image, $ID$

1. Construct the inverse S-box $S -1$ = $inv$ ($\mathbb{S}Ks$ ($NS$)).

2. Initialize the chaotic source $\mathbb{C}$ using $IV$ = AES$Ks$ ($NC$).

3. Iterate $\mathbb{C}$ for $NT$ times to skip the transient effect.

4. Use $\mathbb{C}$ to generate a chaotic sequence, $M$, of length $\#IC$.

5. For each cipher image pixel $ck$ = $IC$ ($i$,$j$), calculate $ID$($i$,$j$) = $S -1$ ($S -1$ ($ck$ ) $\oplus$ $mk$) $\oplus$ $ck{-}1$ , where 1 ≤ $k$ ≤ $\#I$, $c$0 = 0.

6. Output the decrypted image Ip

**Algorithm 3: Construct Key-dependent S-box**

**Input:** nonce, $NS$, shared S-box key, $KS$

**Output:** S-box, $s$ (0: 255)

```
1. Calculate the seed = $AESKs(NS)$.
2. Initialize the MT19937 PRNG, $\mathbb{R}$, using the seed.
3. Initialize collision vector $a$(0: 255) ← false
4. for $i$ = 0: 255
5. repeat
6. $j$ ← next random from $\mathbb{R}$ mod 256.
7. until $a(j)$ = false
8. $a(j)$ ← true, $s(i)$ = $j$
9. end for
```

10. Output $s$ (0: 255)

**Advantages:**

1. Protecting patient privacy and medical records is a legal requirement.
2. Special precautions are taken to fend off the reset attack against pseudorandom number generators.

**Disadvantages:**

1. Digital Imaging and Communications in Medicine (DICOM) is not used here.

E.E. García-Guerrero et.al.[6]. Proposed Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channel. With the rapid development of internet, multimedia technologies, communication technologies, microcontroller units (MCU) and internet protocols, the number of services and multiple modern electronic applications that carry out the exchange of confidential information through public telecommunications channels using electronic devices or embedded systems (ES) is growing exponentially. These developments make necessary the discovery of new methods to guarantee that the information being transmitted is secure against known attacks. For several years, researchers have applied classical encryption schemes, like Data Encryption Stan- dard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), International Data Encryption Algorithm (IDEA) and Rivest Cipher 4 (RC4), which are based on iterated processes, series of linked mathematical operations and Feistel structure, where several rounds of substitution boxes (S-boxes) and permutation boxes (P-boxes) are programmed with exclusive-or (XOR) or bitwise rotation.

However, these schemes are excellent algorithms just for text encryption but they are not suitable to encrypt digital images securely and because of its distinguishing features including bulk data capacity, high redundancy among the raw pixels and strong adjacent pixels correlation. These issues make the classical schemes be unsuitable for fast communications or real time encryption mainly due to the fact that these ciphers require a large computational time and high energy consumption. Nevertheless, chaotic cryptography is being considered as one of the most secure methods to protect confidential information because of its particular properties, such as high sensitivity and dependence to initial conditions, unpredictable behaviour, ergodicity, randomness, topology complexity and excellent adaptability to secure communication, among others.

Besides, some research efforts deal with the combination of AES/DES with chaotic algorithms even combining up to four encryption algorithms (DNA-RSA-DES-Chebyshev) with the aim of improving security. However, the execution of these algorithms is too much computational load for an embedded system or MCU. Although, Microchip manufacturer offers a hardware crypto engine on the PIC24F and PIC 32MZ devices for cryptographic functions with AES, DES and 3DES algorithms, this solution is provided by means of a single library for typical applications, such as: web access, secure XML transactions, virtual private networks (VPN) and secure transfer of stored calibration data. As one can infer, a better solution is needed to cope with the modern applications devoted to the Internet of Things (IoT), which expects that by the year 2020 more than 50,000 million devices with digital communication technology will be connected to Internet using embedded systems.

The IoT enables exchange of information in a wide variety of applications such as smart buildings, smart health, smart transport, Industry 4.0, and so on. As billions of connected things communicate with each other and can exchange sensitive information that may be leaked. The IoT can connect people to people, people to machine or machine to machine (M2M), for example: Fig. 1 depicts the architecture of a (M2M) system. One can see that a better method must be required to guarantee security in the IoT and protect the information against several attacks. Also, it must be required to perform cryptanalysis to cryptosystems as reported in the literature. The problem is more complex because nowadays intruders and hackers continue to become more sophisticated, so that encryption technology must evolve as well. This problem makes necessary the development of new embedded cryptosystems with greater complexity (enhanced security) and efficiency. In this manner, main contribution of this work focuses on adding security in M2M Area Network by performing chaotic encryption on a wireless communication scheme with Zigbee/IEEE 802.15.4 protocol Designing secure M2M systems requires the ability to design fast and secure cryptographic modules, in which the main component is the pseudorandom number generator (PRNG), which can be built using chaotic maps. From our knowledge and based on the reviewed literature, few works report the use of embedded systems for the chaotic encryption of information and its application for M2M and IoT.

In this manner, the aim of this paper is the introduction of a secure algorithm to improve the dynamics of five chaotic maps implemented on PIC-microcontrollers, with application to encrypt digital images as a confidential information for secure wireless communications on M2M systems and analyse its feasibility to be conditioned for IoT applications. The rest of this paper is organized as follows: Section 2 presents the proposed chaotic maps to encrypt digital images. Section 3 describes the proposed scheme for M2M solution. Section 4 provides the results of security analysis, performance and comparison with related work.

**Advantages:**

1. The main cryptography requirements demand that the new embedded cryptosystems have to be more efficient and secure, it means that they must be faster and offer greater security.
2. It is more secure.

**Disadvantages:**

1. It was proved that it is not necessary to combine several algorithms in the encryption process.
2. The performance and speed of the chaotic encryption algorithms is slow.

`Qian Liu et.al.[7]. Proposed Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System. The rapid development of the Internet has ushered in a new era of global economy, culture, military, education, and other fields. In the new era, people can easily realize the transmission of image information. However, digital images may involve private or confidential information, which may cause incalculable consequences when leaked. The most common approach to protect the security of image information is image encryption.

This paper combines DNA computing with double-chaos systems and proposes an algorithm for color image encryption at the bit level. First, we use Arnold algorithm to scramble the three components of the color image, and the number of iterations was determined by the average of the three components, which improved the scrambling effect of Arnold algorithm. Secondly, after a lot of experiments, we propose a double-chaos system composed of Lorenz chaotic mapping with variable parameters and fourth-order Rossler hyperchaotic mapping to generate three sets of chaotic sequences for diffusion operation. The double-chaos system compensates the pseudo-randomness of the two types of chaotic mappings, making chaotic sequences more difficult to predict. Then, we transform the chaotic component images and chaotic sequences into DNA sequences in accordance with eight DNA coding rules, and the coding rules are determined by plaintext information or generated chaotic sequences.

We also perform addition, subtraction, and XOR operations on them. DNA computation can realize color image bit-level diffusion and reduce the computational cost. The plaintext information is embedded in the encryption process to achieve ‘‘One-Time Pad’’. Simulation experiments and detailed analysis are conducted with the proposed encryption scheme to prove that the algorithm has good security performance and can effectively resist all types of attacks, indicating that the proposed algorithm is competitive. Digital image encryption is the main method of image information security protection.

Traditional encryption technologies, such as data encryption standard, advanced encryption standard, public key cryptography algorithm, and international data encryption algorithm, convert plaintext data into a binary stream for processing during encryption.

## ENCRYPTION ALGORITHM

The complete encryption algorithm can be described by the following steps:

**Step 1:** Ciphertext image C is read. The size of ciphertext image C is 256×256. The grayscale images CR, CG, and CB of the R, G, and B components of the color ciphertext image are separated, and the size of the three grayscale images is 256 × 256.

**Step 2:** The parameters of Lorenz mapping are set as follows: x0 = [x01, x02, x03], p. The parameters of Roessler mapping are set as follows: Y0 = [Y01, Y02, Y03, Y04], a, b, c, d, k. The three sets of parameters related to plaintext information are n1 = mean (PR), n2 = mean (PG), and n3 = mean (PB).

**Step 3:** Three sets of chaotic sequences {x1(i)}, {x2(i)}, and {x3(i)} are generated by the Lorenz chaotic system with variable parameters. Four sets of chaotic sequences {Y1(i)}, {Y2(i)}, {Y3(i)}, and {Y4(i)} are generated by the fourth order Roessler chaotic system.

**Step 4:** Three sets of random chaotic sequences {z1(i)}, {z2(i)}, and {z3(i)} for diffusion operations are obtained using Formula (5).

**Step 5:** The images CR, CG, and CB obtained in Step 1 and the three sets of random chaotic sequences obtained in Step 4 are converted into DNA sequences in accordance with the eight DNA coding rules. The encoding rules used are determined by key1, key2, and key3. The three sets of DNA sequences {D1}, {D2}, and {D3} generated by CR, CG, and CB and the three sets of DNA chaotic sequences {Z1(i)}, {Z2(i)}, and {Z3(i)} produced by chaotic sequences are obtained.

**Step 6:** DNA sequence {C1} is obtained using {Z1(i)} to recover {D1} according to DNA addition. DNA sequence {C2} is obtained using {Z2(i)} to recover {D2} according to DNA subtraction. DNA sequence {C3} is obtained using {Z3(i)} to recover {D3} according to the DNA XOR operation.

**Step 7:** {C1}, {C2}, and {C3} are decoded and restored to the pixel values in the interval of [0, 255] and reconstructed into images.

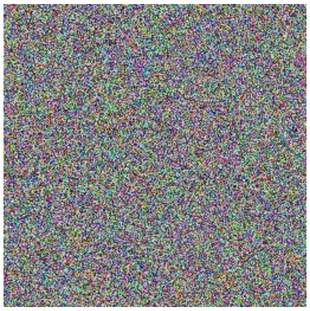
**Step 8:** The scrambled image is restored using the reversal function of Arnold scrambling, and PR, PG, and PB are obtained.

**Step 9:** PR, PG, and PB are merged to obtain the final decrypted image P'.

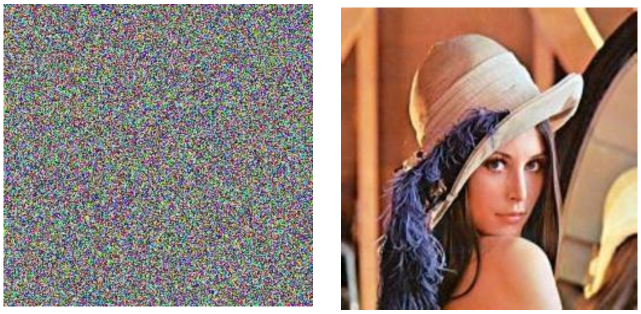
## ENCRYPTION AND DECRYPTION TEST

We set the system parameters of Lorenz chaos as $x_0$ = [0.9613; 0.5201; 0.1314].

When cos (5.3t) $\geq 0$, p = 1; otherwise, p = −1. We set the system parameters of Roessler chaos as $Y_0$ = [−11.0431, −7.9989, 26.8729, 2.34109], a = 36, b = 3, c = 28, d = 16, and k = 0.5.



**(a)Original plaintext image. (b) The encrypted cipher text image.**



**(c) The incorrectly decrypted image. (d) The correctly decrypted image.**

**Fig 2.16: Encryption and decryption test.**

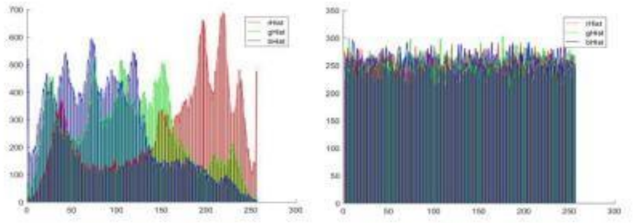
`In Fig. 2.16, a, b, c, and d are the original plaintext image, the encrypted ciphertext image, the incorrectly decrypted image, and the correctly decrypted image, respectively. In Fig. 2.16 (b), the encrypted ciphertext image is not clear, and the plaintext image information cannot be recognized by the naked eye. In Fig. 2.16 (c), we change only the initial value of the third bit of $Y_0$. When the decryption key used is not correct, the image cannot be restored effectively, and the plaintext image information cannot be recognized by the naked eye. In Fig. 2.16 (d), we decrypt Fig. 2.16 (b) with the correct key, thereby effectively restoring the plaintext image.

## HISTOGRAM ANALYSIS

A favourable encryption algorithm must have a smooth histogram of the encrypted image. Fig.2.16 shows the color histogram before (a) and after (b) encryption. The encrypted color image histogram is evenly distributed compared with the plaintext image, and the distribution probability in the interval is approximately equal. Thus, using statistical analysis to predict the original image is difficult for attackers. The results show that the algorithm can effectively prevent statistical attacks.

## KEY SPACE

An ideal image encryption algorithm must have a sufficiently large key space and be sensitive to its key. The size of the key space is the total number of different keys that can be used in the cryptographic system; thus, the key space must be greater.



(a) (b)

**Fig 2.17: Histogram analysis: (a) Original plaintext image; (b) The encrypted ciphertext image.**

Mapping, the initial value Y0 = [Y01, Y02, Y03, Y04] and the parameters a, b, c, d, and k of Roessler mapping, and three sets of parameters n1 = mean (PR), n2 = mean (PG), and n3 = mean (PB) related to plaintext information. Therefore, in accordance with the IEEE floating point standard, the overall key space of this algorithm is Key space = 1015×16 2 128 This equation satisfies the security requirements that are outlined in the standard. Therefore, our encryption algorithm has a sufficiently large key space to resist various brute-force attacks.

**Advantages:**

1. The chaos system is complex, deterministic.
2. Protect the security of image information is image encryption.
3. DNA computation can realize color image bit-level diffusion and reduce the computational cost.

**Disadvantages:**

1. In image transmission, the data or information in the image may be lost or changed due to transmission.
2. A good encryption algorithm should have a certain resistance ability to prevent data change or loss caused by attacks.

Amira G. Mohamed et.al.[8]. Proposed New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps. The current availability of various mobile applications and related technologies have made the different types of multimedia files important. This article proposes a novel approach of improvising the cryptographic features of substitution-boxes (S-Box) based on the Choquet Fuzzy Integral (CFI) and DNA techniques.

First, we propose a strong structure for the construction of four S-Boxes using CFI. The key for generating the CFI based (FZ) S-Boxes consists of two parts, namely, an external secret key and a secret image. Each of these FZ S-boxes is then encoded using DNA techniques, with dynamic rules selection which is dictated by a secret control code.

The resultant four S-boxes are designated as DNAFZ S-Boxes. To apply for image encryption, the plain image is, at first 8-bit binary-coded, shuffled by an M-sequence, and down sampled into four sub-images. Subsequently, the pixel values of each sub-image are replaced with the corresponding values of one of the four DNAFZ S-Boxes. Next, each DNAFZ encoded sub-image is diffused with a different DNA encoded chaotic sequence from Chen’s hyper-chaotic map. Finally, the four DNAFZ/Chaotic encoded sub-images are combined to build the final encrypted image. The proposed DNAFZ S-boxes shows excellent statistical properties under majority logic criterions such as correlation, homogeneity, energy, entropy, and contrast.

Moreover, numerical simulation is used to examine the efficacy of encrypted images against different attacks. In particular, the values of the pixel correlation coefficient are found to be quite small either horizontally, vertically, or diagonally (between 7.8597e-04 and 0.00527, between 8.7856e-04 and 0.00452, and between 0.00241 and 0.00021, respectively). In addition, the information entropy of the encrypted image is found to be within the range of (7.9965:7.9989) which is very near to the ideal value of 8. As for the UACI and the NPCR, they are in the ranges between 33.46 and 33.32 and between 99.58 and 99.62, respectively. These values are also very close to the optimum ones.

The results are compared to those of other encryption and proved that the proposed encryption method delivers better results than other conventional ones including LSS chaotic map, Arnold transforms, Dynamic Henon map, Hybrid chaotic map optimized substitution, and cubic S-Box. DNA cryptography has evolved as a result of the similarities found between biology and computer science. It has been used as a system of data security. DNA or deoxyribose nucleic acid is the material inside every living cell.

It holds all the genetic features, carrying them from one generation to the next, through hereditation. DNAs is made of four nitrogenous bases, cytosine, thymine, adenine, and guanine. The fact that they can store massive amounts of data and the ideas of based complementation and parallelism play an important role in their ability to secure data.

DNA encryption of photos involves the following steps: using a DNA-encoding rule to encode the image into a DNA matrix, followed by conversions between the four DNA nitrogenous bases in what is known as DNA level permutation and/or DNA level diffusion. This step takes place on the DNA matrix. The final step involves decoding the DNA matrix to obtain the cipher image Fuzzy set theory involves various paradigms used for fuzzy neural computations, which are quite interesting. Regarding decision analysis, several operators are employed for aggregation. For X, a finite set, a fuzzy measure is required to base a fuzzy integral upon.

This is done as a computational scheme, when dealing with fuzzy sets that have dependent input, in order to nonlinearly integrate all values from individual subsets. This required fuzzy rules to be set in place, where fuzzy measures are the basis for the consequent. These rules gave way to a defuse field output, which was also a Choquet fuzzy integral (CFI). CFI, with its set of benefits, added great value to the area of image encryption. These benefits include that it is easy to implement, simple to compute, effective in reaching high level security, high in speed and sensitivity Several features characterize chaotic systems. These include, but are not limited to, periodicity, determinacy, and the fact that they are highly sensitive to initial conditions.

Chaotic maps produce chaotic sequences, which are pseudorandom, complex in structure and not easy to analyse and predict. Despite the fact that their security is not very high, these sequences possess large key spaces that are very sensitive to any changes that occur in their key. This is the reason for the development of hyper-chaotic systems for use in algorithms that deal with image encryption. To create a four-dimensional hyper-chaotic system, an extra dimension is added. This takes place in accordance with Chen’s chaos theory. In recent years, the characteristics of hyper-chaotic systems have been improved by adding several positive

Lyapunov exponents, complex and dynamical characteristics, as well as improved sensitivities and bigger key spaces.

The results are compared to those of other encryption and proved that the proposed encryption method delivers better results than other conventional ones including LSS chaotic map, Arnold transforms, Dynamic Henon map, Hybrid chaotic map optimized substitution, and cubic S-Box. DNA cryptography has evolved as a result of the similarities found between biology and computer science. It has been used as a system of data security. DNA or deoxyribose nucleic acid is the material inside every living cell.

**Algorithm 1:** Sequence Generation

```
Input: External Key with size 128-bit ($K$), Secret Image
$I$ ($M$ $N$)
Output: Random sequences $C_j$
    1: Divide $K$ into four blocks ($K_1$, $K_2$, $K_{16}$)
    2: Calculate key parameters ($A$, $B$, $C$, $D$) 3: # Eq. (9, 10, 11, 12)
    4: Divide secret ×image into 2 blocks
    5: XOR Operation for each of the grey levels within each block
    6: Calculate initial inputs ($h_1$, $h_2$, $h_3$, $h_4$) 7: # Eq. (14, 15, 16, 17)
    8: Calculate Membership Grades ($g_1$, $g_2$, $g_3$, $g_4$) 9: # Eq. (18)
    10: Calculate $\lambda$ based on Eq. (3)
    11: Calculate fuzzy measures ($F$ ($A_i$)) 12: # Eq. (2)
    13: Use Eq. (4) to calculate CFI
    14: Generate random sequences $C_j$ based on Eq. (19)
    15: return $C_{j.}$
```

**Advantages:**

1. These benefits include that it is easy to implement, simple to compute, effective in reaching high level security, high in speed and sensitivity.
2. values of the pixel correlation coefficient are found to be quite small either horizontally, vertically or diagonally.

3. In addition, the information entropy of the encrypted image found to be within the range of which is very near to the ideal value of 8.

**Disadvantages:**

1. Do not provide enough security for the transfer of such files.
2. This insecurity has been increasing due to vast leaps in technology over the past few years.

Hegui Zhu et.al.[9]. Proposed 2D Logistic-modulated-Sine-coupling-Logistic chaotic map For Image Encryption: With the development of Internet and computer technology, everyone can process various texts, videos and audio information through Internet. Due to the danger of transmitting confidential information in the public channel, it is necessary to encrypt the image information to ensure the security in the transmission process. To solve this problem, researchers have proposed many image encryption algorithms, such as chaotic cryptography, DNA code, and quantum theory. Chaotic cryptography is an interdisciplinary subject which integrates chaos theory into cryptography, and it is more suitable for cryptography with unique characteristics. Existing chaotic maps can be classified into two categories: one-dimensional (1D) chaotic maps and high dimensional (HD) chaotic maps. However, 1D chaotic maps have many disadvantages, such as simple structures and few parameters. Their chaotic orbits, parameters and initial values may be predicted with little extracted information. Therefore, 1D chaotic maps are not dominant in the security field. HD chaotic maps usually have more complex structures and better chaotic performance than 1D chaotic maps, so they become a good choice for encryption. For example, Jan et al. proposed TD-ERCS chaotic system and used the system to generate two random sequences for image encryption.

There are many ways to construct complex chaotic systems to improve the chaotic characters, so they can be applied to image encryption. On one hand, modulation is a very feasible and effective approach. In the experiment of eavesdropper attacking chaotic communication system, chaotic modulation system is more difficult to be attacked. The reason is that chaotic trajectories become dependent on time and information, which makes it very difficult to unfold by using established reconstruction techniques, it can increase the practicality of this approach in secure communications. On the other hand, coupling is also a safe and effective method.

**Advantages:**

1. With the development of Internet and computer technology, everyone can process various texts, videos and audio information through Internet.

**Disadvantages:**

1. Simple structures and few parameters.

Aqeel Ur Rehman et.al.[10]. Proposed A selective cross-substitution technique for encrypting color images using Chaos, DNA rules and SHA-512. The momentum has seen advancements in computing, physical networks and software protocols. The big share of bandwidth across all mediums has now gone to multimedia communications; the users have come way forward from exchange of simple texts. It's the era of embedded media, real streams, live videos, 3D pictures and videos, virtual reality and lot more. The variety of forms a multimedia message can take is huge, so are the sources and applications using it. Along with it conventional theories and soft technologies are revolutionizing like vision tech, robotic eyes, pattern classifications, medical sensing and imaging, laser and ultraviolet imaging, 3D plans for remote video assistance, security camera and situation detections.

These all demand a secure transmission of underlying image and video streams and messages. The internet being public and highly accessible in terms of network and applications is insecure by nature and any multimedia communication inherits this limitation. The researchers have seen the significance of the algorithms, encryption schemes, crypto systems that can solve this problem efficiently, systematically and without the loss of actual media.

The images by nature contain high correlation and duplication of grayscale values in all neighbouring groups of pixels, this makes the existing crypto schemes like IDEA, RS4 and IDEAS inefficient and inappropriate Theory of chaos mothered a new breed of encryption algorithms with its determinable but non-predictive characteristics.

DNA was firstly brought by L. Adleman in encryption schemes to help to resolve computational complexity. The DNA encoding was used to convert digital data into cipher and then revert it back. The DNA sequence-based algorithms have properties of parallelism and info density like DNA molecules. The researchers have made a clear dent in improving existing cryptosystems in terms of their robustness to text-attacks by using DNA sequencing. The DNA based schemes being new and less mature has seen cracking due to low dimensionality of chaotic maps causing periodicity. According to Zhang et al. binary coded algos depict low efficiency on the other side chaotic controlled key is vulnerable to cracking. Similarly, Xie et al suggests crypto schemes by only using scrambling, having no diffusion functions, are less secure causing disassociation of cipher with the plaintext. Liu et al recreated the parallel key by using known partial values of plain or cipher and cracked a crypto scheme built upon DNA sequencing with the help of differential attack.

**Permutation:**

The correlation in the adjacent pixels of a channel and correlation between the channels of the color image are very strong in the plain image. The permutation is a method to reduce the correlation of an image. For this, a chaotic sequence W is generated by iterating Equation (2) 3MN + t times using µ 0 1 and w 0 0. The first t elements are discarded to avoid transient effect and then W is sorted and record their index as shown in Equation. A copy of W before sorting is maintained which will be used later. The 24-bit color image is transformed into 1D vector of size 1×3MN. The recorded index array few is used to shuffle the positions of pixels to permute the image P as shown below.

$$[l_w, f_w] = sort(W)$$

The Equation depicts sequencing index functionality as [•, •] = sort (•), lw is the generated sequence, where W is sorted in ascending. The fw holds index value of lw to rearrange the items of P depicted by Equation.

$$P' = P\,[f_w]$$

**DNA encoding:**

Now split P into three vectors, each of size 1 × MN representing a color channel called R, G and B. These permuted channels are encoded into DNA bases using DNA complementary rules according to Table 4. This operation requires three pseudo-random sequences for the selection of DNA rules, which are obtained by splitting copy of W into three sub-arrays called W1, W2 and W3. R0 = Encode (R, W1) G0 = Encode (G, W2) B0 = Encode (B, W3).

**Advantages:**

1. Encryption takes 1/4th time the decryption process takes.
2. Encryption is a technique used to secure and protect the images from unfair means.

**Disadvantages:**

1. Decryption takes 4 times larger the time taken by encryption.
2. There is drawback like small key space and weak security.

# CHAPTER 3:

## SYSTEM DESIGN

### Proposed System Design

In this section, we will study the procedure of image encryption based on the DNA sequence addition operation in detail. Firstly, produce secret keys. Secondly, divide the original image into blocks and add these blocks by using the DNA sequence addition operation. Thirdly, carry out the DNA sequence complement operation for the resulting added matrix using two Logistic maps. Lastly, decoding the result from the third stage, we obtain the encrypted image. The process of the proposed image encryption algorithm is shown in Fig. 3.1.

**The proposed encryption algorithm can be divided into the following steps:**

**Step 1:** Convert the image into a binary matrix, then carry out DNA encoding for the binary matrix according to obtain a coding matrix Ab, the size of Ab is (m, n × 4);

**Step 2:** Divide Ab into some equal blocks Ab {i, j}, i = 1, 2, . . ., m 4, j = 1, 2, . . ., n, where the size of blocks is 4 × 4;

**Step 3:** Generate two chaotic sequences X = {x1, x2, . . ., x m 4}, Y = {y1, y2, . . ., yn}, through 2D Logistic map under the condition that the initial values are x0, y0 and system parameters are µ1, µ2;

**Step 4:** Sorting X, Y in ascending order, we get two new sequences X 0, Y 0;

Step 5: Let the location value of sequences X 0, Y 0 be row coordinates and column coordinates of Ab {i, j}, in other words, it can be expressed as Ab {x 0 p, y 0 q}, where {x 0 1, x 0 2, . . ., x 0 p, . . ., x 0 m 4} and {y 0 1, y 0 2, . . ., y 0 q, . . ., x 0 n} are the location values of sequences X 0, Y 0, respectively;

**Step 6:** Add Ab {i, j} and Ab {x 0 p, y 0 q} according to the rules in Section 2.2.2, obtaining the result as blocks B {i, j}.

**Step 7:** Recombining these blocks, B {i, j}, we will get a new sequence matrix C.

**Step 8:** Two chaotic sequences z1 and z2 are produced by two 1D Logistic maps, whose lengths are m and n×4. Reconstruct z1 and z2 as two matrices Z1 (m, 1) and Z2 (1, n × 4). Performing the multiply operation for Z1(m, 1) and Z2(1, n × 4), we obtain the matrix Z whose size is m × n × 4.

Map the value of Z into (0,1) by mod (Z, 1). Then use the following threshold function f(x) to get a binary sequence matrix:

$$f(x) = \begin{cases} 0, 0 < Z(i,j) \le 0.5; \\ 1, 0.5 < Z(i,j) \le 1; \end{cases}$$

**Step 9:** If Z {i, j} = 1, C {i, j} is complemented, otherwise it is unchanged. After the complementing operation, we get a new coding matrix C 0;

**Step 10:** Carry out the inverse process of the step 1 for the coding matrix C 0, we will obtain a real value matrix D, then output image D, which is our encrypted image.

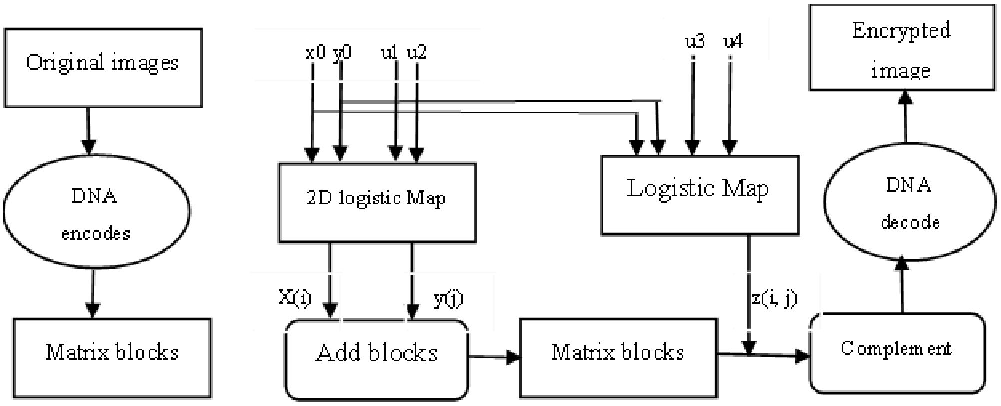


**Fig 3.1 Block diagram for the image encryption algorithm.**

## Generation of the secret key:

We will generate the secret key. Input an 8-bit grey image A as the original image, A = A(aij), i = 1, 2, . . ., m, j = 1, 2, . . ., n. Here, aij is the value of the image pixel, (i, j) is pixel position, and (m, n) is the size of image. Using following formulas, we can calculate k1 and k2.

$$k_1 = \frac{1}{256}\text{mod}\left(\sum_{i=1}^{\frac{m}{2}}\sum_{j=1}^{n} a_{ij}, 256\right)$$

$$k_2 = \frac{1}{256}\text{mod}\left(\sum_{i=\frac{m}{2}}^{m}\sum_{j=1}^{n} a_{ij}, 256\right)$$

Then choose two initial values x1, y2, and four system parameters µ1, µ2, µ3, µ4. Use following pseudo-code to calculate x0 and y0. We set x0, y0, µ1, µ2 as the parameters of the 2D Logistic map and x0, y0, µ3, µ4 as the parameters of two 1D Logistic maps. Thus, these parameters can be seen as secret keys. The pseudo-code is:

```
$x0 \leftarrow x1 + k1$
if $x0 > 1$
    then $x0 \leftarrow \mathrm{mod}\ (x0, 1)$
    else $x0 \leftarrow x0$
end if.
```

**The security analysis:**

A good encryption algorithm should resist all kinds of known attacks, such as exhaustive attack, statistical attack and differential attack. In this section, we will discuss the security analysis of the proposed encryption scheme.

**Secret key's space analysis:**

In our algorithm, the initial value and the system parameter of the chaotic maps can be seemed as secret key. Thus, there are six secret keys (x1, y1, µ1, µ2, µ3, µ4) in our algorithm. If the precision is $10^{-12}$ the secret key's space is

$$10^{12} \times 10^{12} \times 10^{12} \times 10^{12} \times 10^{12} \times 10^{12} = 10^{72}.$$

The secret key's space is large enough to resist exhaustive attack

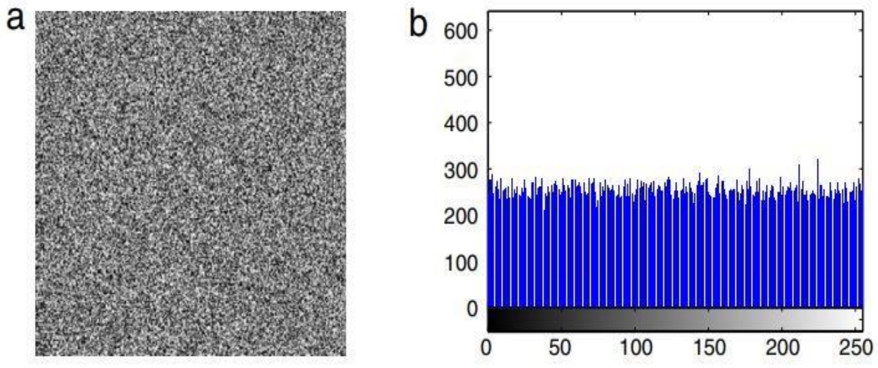


**Fig 3.2: The sensitivity to the secret key x1**

**(a) The decrypted image whit secret key (0.62000000000001, 0.12, 3.2, 3, 3.9, 3.85)**

**(b) The corresponding histogram.**

**Secret key's sensitivity analysis:**

The 2D Logistic and 1D Logistic chaotic maps are sensitive to the system parameters and initial values. If they have a slight difference, the decrypted image has no connection with the original image. Some secret key sensitivity tests are shown here. Using the secret key in the Section 4 to encrypt the original image, we have obtained the encrypted image shown Fig.3.2(b) in the Section 4, next utilize the secret key (0.62000000000001, 0.12, 3.2, 3, 3.9, 3.85) to decrypt for the encrypted image.

The result of decrypting is shown in Fig. 3.2. In Fig. 3.2(a) shows the decrypted image and the corresponding grey histogram of the decrypted image is shown in Fig. 3.2(b). We can see that the histogram of the decrypted image is fairly uniform and the decrypted image is different from the original image. As the sensitivities of the other parameters are the same as for x1, we omit examples of them here. Based on the above argument, our algorithm is sensitive to the secret key, which demonstrates it has the ability to resist exhaustive attack.

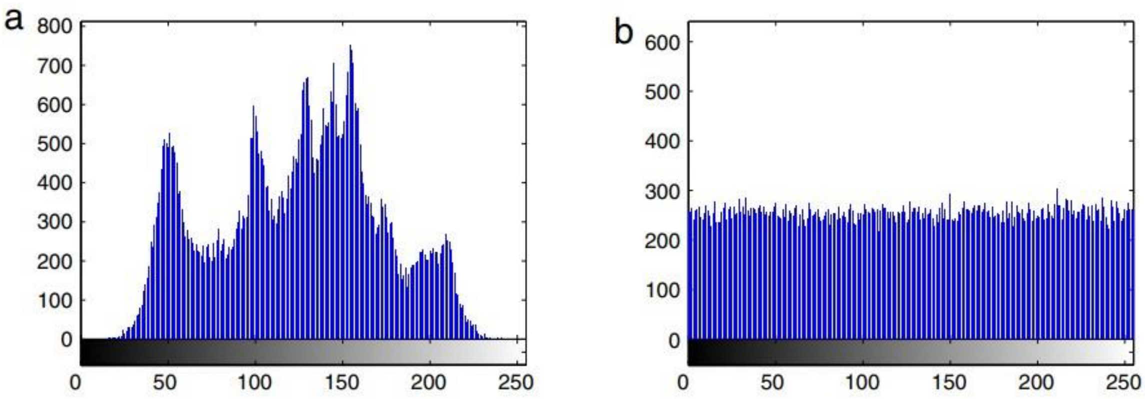


**Fig. 3.3: The grey histogram of the original image and the encrypted image.**

**(a) The grey histogram of the original image.**

**(b)The grey histogram of the encrypted image.**

**The grey histogram analysis:**

Considering the statistical analysis of the original image and the encrypted image, Fig. 3.4(a) and 3.4(b) shows the grey-scale histograms of the original image and the encrypted image, respectively. Comparing the two histograms we find that the pixel grey values of the original image are concentrated on some values, but the histogram of the encrypted image is very uniform, which makes statistical attacks difficult.

A histogram tells us the frequency of each intensity value in the gray-scale scale equivalent of a picture. It plots each of the intensity values versus the number of pixels that has that value. It is conceptually important, as it gives us an idea of the distribution of various intensity values in a picture.

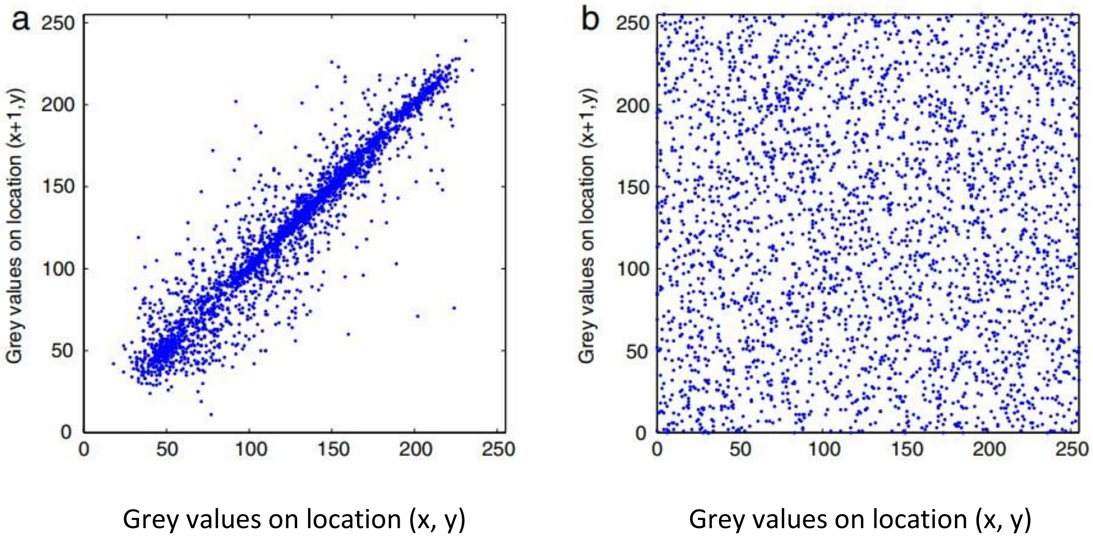


**Fig 3.4: Correlation of two horizontally adjacent pixels in the original image and in the encrypted image**.

## Correlation coefficient analysis:

As far as we know the correlation of between adjacent pixels in the original image is very high. An effective encryption algorithm can reduce the correlation between adjacent pixels, in order to test the correlation of two adjacent pixels; we randomly select 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image.

Fig 3.4 (a), (b) shows the correlation of two horizontally adjacent pixels in the original image and its encrypted image, where the correlation coefficients are 0.9468 and 0.0036, respectively. Fig 3.4(b) shows that the correlations of adjacent pixels in the encrypted image are greatly reduced. By this we can clearly be seen that our algorithm can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statistical attack.

**Resistance to differential attack:** Attackers often make a slight change to the original image, and use the proposed algorithm to encrypt for the original image before and after changing, through comparing two encrypted image to find out the relationship between the original image and the encrypted image. It is called differential attack.

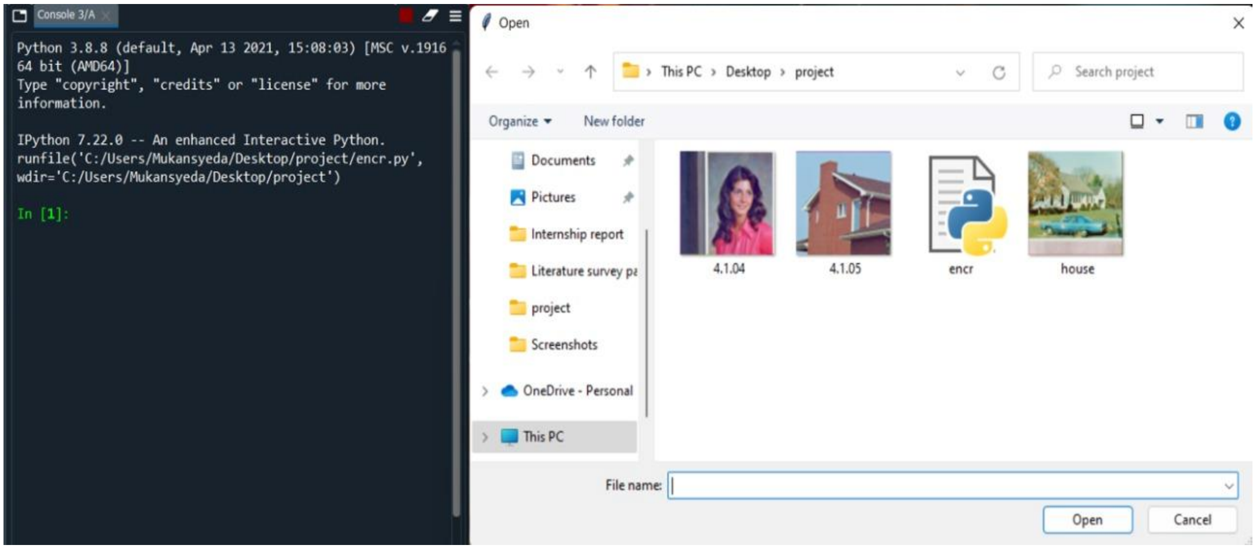
**Information entropy**: The information entropy is defined as expressing the degree of uncertainty in the system. We can also use it to express uncertainties in the image information. The information entropy can measure the distribution of grey values in the image. If the distribution of grey values is more uniform, the information entropy is greater.

# CHAPTER 4:

## RESULT AND ANALYSIS

In cryptography, encryption is defined as the process of converting useful information into an unrecognizable form to protect it from unauthorized access. The image content occupies vital characteristics like high redundancy, space, capacity and correlation among the bit pixels, that demands some kind of encryption technique where the primary purpose is to securely transfer the image.

In other words, an encryption algorithm is used to transform the plain image into a cipher image, i.e., the useful actual information is obscured. The encrypted image can then be securely transmitted over the network; therefore, no unauthorized person is able to decrypt the image. Hence, at the receiving end of the network, a decryption algorithm is utilized to decipher the cipher image into the original image. Moreover, in the process of image encryption, the original image is incorporated with a key to encode the image, whereas, for the image decryption process, a decryption algorithm is used to decode the encrypted image in order to recover the original image.

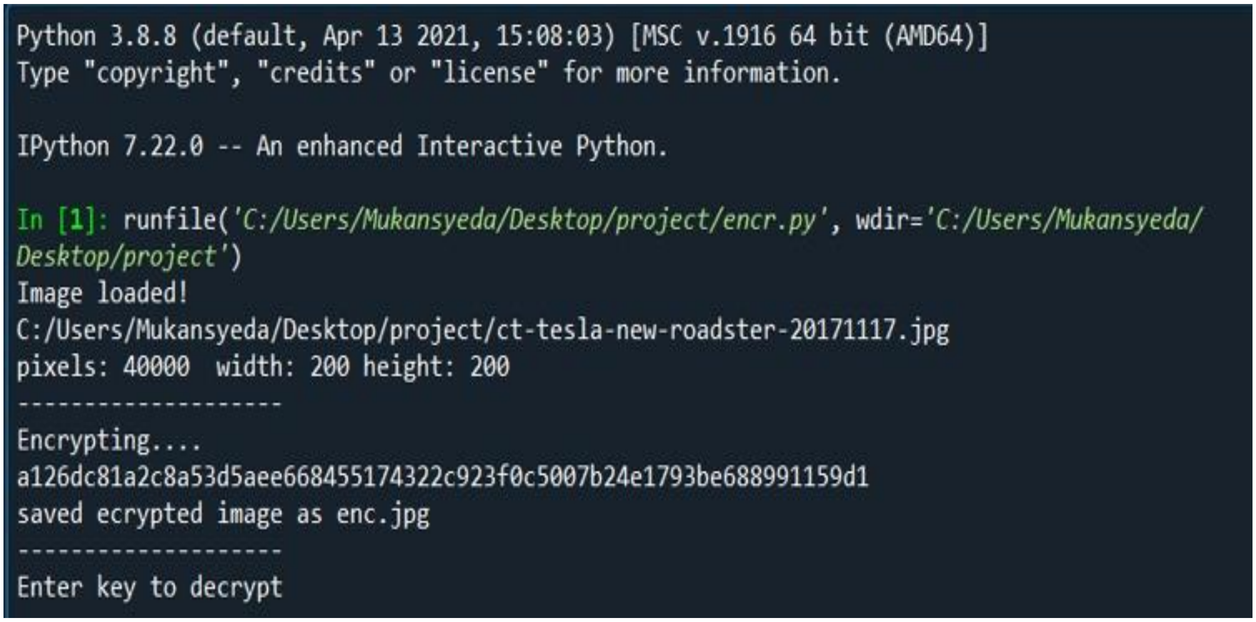


```
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916
64 bit (AMD64)]
Type "copyright", "credits" or "license" for more
information.

IPython 7.22.0 -- An enhanced Interactive Python.
runfile('C:/Users/Mukansyeda/Desktop/project/encr.py',
wdir='C:/Users/Mukansyeda/Desktop/project')

In [1]:
```

**Fig 4.1: After running of code, we get the option to choose which image is to be encrypted.**



```
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/Mukansyeda/Desktop/project/encr.py', wdir='C:/Users/Mukansyeda/
Desktop/project')
Image loaded!
C:/Users/Mukansyeda/Desktop/project/ct-tesla-new-roadster-20171117.jpg
pixels: 40000  width: 200 height: 200
--------------------
Encrypting....
a126dc81a2c8a53d5aee668455174322c923f0c5007b24e1793be688991159d1
saved ecrypted image as enc.jpg
--------------------
Enter key to decrypt
```

**Fig 4.2: In this we got the encryption key after running of code and selecting an image which is to be decrypted.**

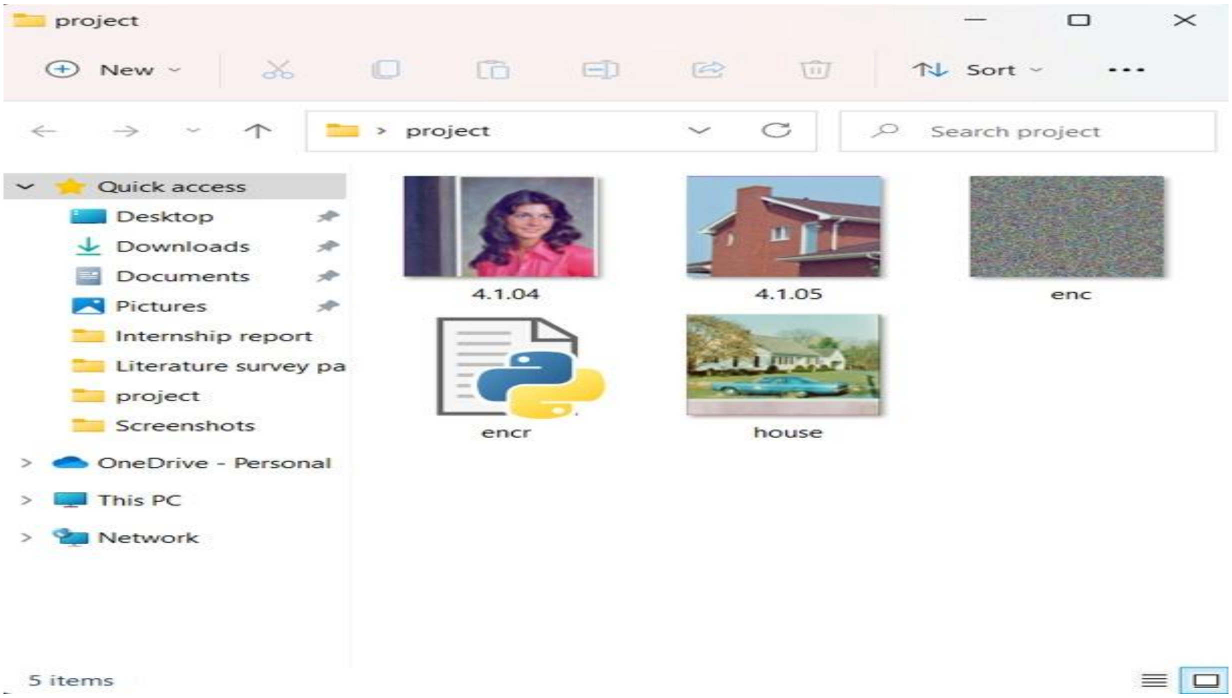
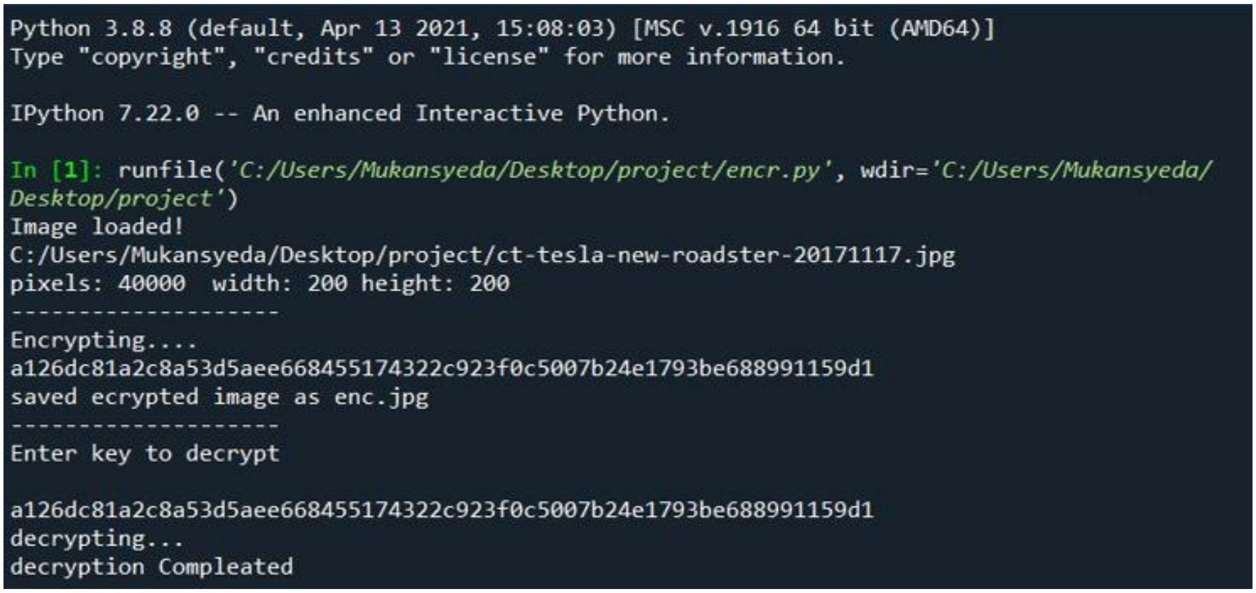


**Fig 4.3: Encrypted image is shown.**



```
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/Mukansyeda/Desktop/project/encr.py', wdir='C:/Users/Mukansyeda/
Desktop/project')
Image loaded!
C:/Users/Mukansyeda/Desktop/project/ct-tesla-new-roadster-20171117.jpg
pixels: 40000  width: 200 height: 200
--------------------
Encrypting....
a126dc81a2c8a53d5aee668455174322c923f0c5007b24e1793be688991159d1
saved ecrypted image as enc.jpg
--------------------
Enter key to decrypt

a126dc81a2c8a53d5aee668455174322c923f0c5007b24e1793be688991159d1
decrypting...
decryption Compleated
```

**Fig 4.4: To decrypt the code is to be pasted and run the program.**

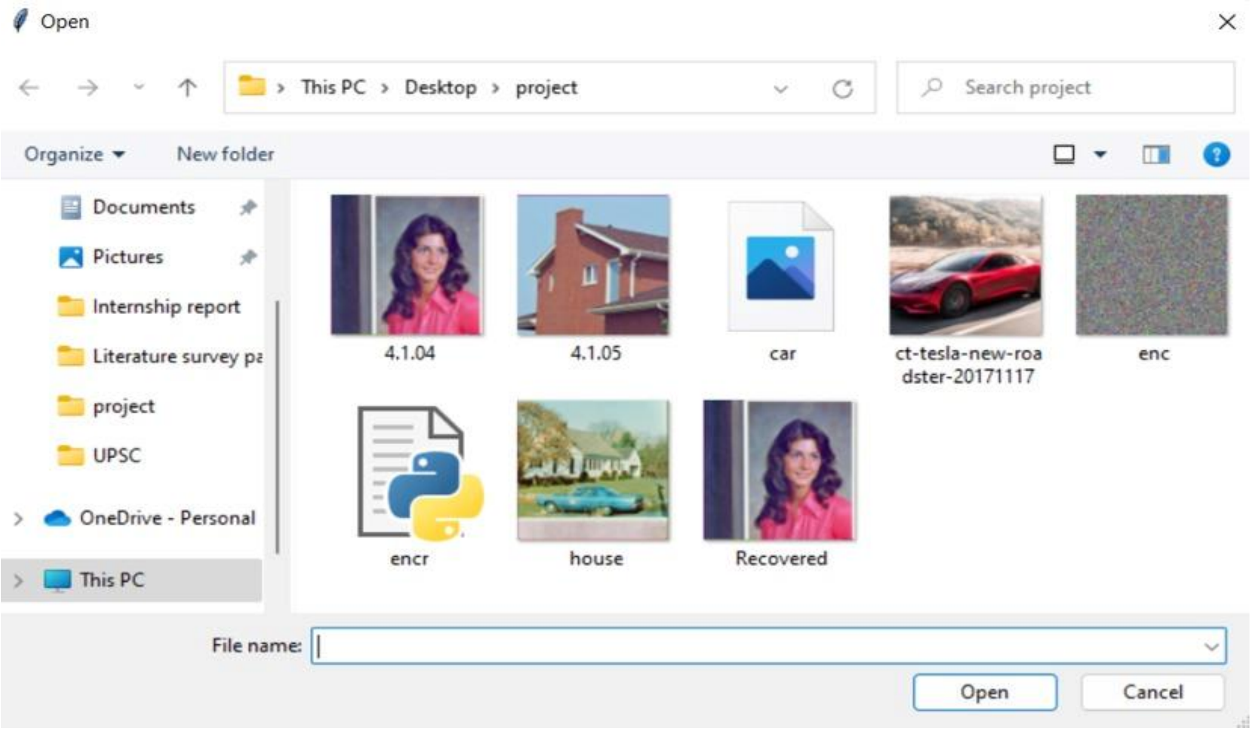


**Fig 4.5: This is the last stage where we can get to see the recovered image after decryption.**

## CHAPTER 5:

# CONCLUSION

In this project, we proposed a new image encryption algorithm based on DNA sequence addition. From above discussion, the pixel grey values of the original image are completely scrambled by the DNA sequence addition operation and the DNA complement operation. Through the experimental result and security analysis, we find that our algorithm has a better encryption, a larger secret key space and is highly sensitive to the secret key. Furthermore, the proposed algorithm can also resist most known attacks, such as exhaustive attacks, statistical attacks and differential attacks. All these features show that our algorithm is very suitable for image encryption.

## REFERENCES

1. Qiang Zhang, Ling Guo, Xiaoping Wei, "Image encryption using DNA addition combining with chaotic maps", In proceedings of
2. Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gul, Ran Ren1 and Kai Xin Liao, "Encryption is an efficient way to keep image data free from attackers", In proceedings of
3. Muhammad Samiullah, Waqar Aslam, Hira Nazir, M. Ikramullah Lali, Basit Shahzad, Muhammad Rafiq Mufti, And Humaira Afzal, "The significance of information security is increasing with digitization", In proceedings of
4. Zeeshan Ahmad, Hafiz Umar, Chundong Li, and Ling Chen, "A DNA-Based Security solution Using Aggregated Chaos Cross and Cubic Map", In proceedings of
5. Saleh Ibrahim, Hesham Alhumyani, Mehedi Masud, Sultan S Alshamrani, Omar Cheikhrouhou, Ghulam Muhammad, M. Shamim Hossain, AND Alaa M. Abbas, "Framework for Efficient Medical Image Encryption using Dynamic S-Boxes and Chaotic Maps", In proceedings of
6. E.E. García-Guerreroa, E. Inzunza-González a, O.R. López-Bonillaa, J.R. Cárdenas-Valdez b, E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channel", In proceedings of
7. Qian Liu And Lingfeng Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System", In proceedings of Ling feng Liu, from April 22 2020, To May 15 2020.
8. Amira G. Mohamed 1, Noha O. Korany 2, And Said E. El-Khamy 2. "New DNA Coded Fuzzy Based (DNAFZ) S-Boxes", In proceedings of Amira G. Mohamed, from January 12 2021, To January 26, 2021.
9. Hegui Zhu, Yiran Zhao, And Yujia Song, "A selective cross-substitution technique for encrypting color images using Chaos, DNA rules and SHA-512", In proceedings of Hegui Zhu, from 2019 to 2020.

10. Aqeel Ur Rehman, Huiwei Wang, Malik M. Ali Shahid, Salman Iqbal, Zahid Abbas, Amnah Firdous, "A selective cross-substitution technique for encrypting color images using Chaos, DNA rules and SHA-512", In proceedings of of Huiwei Wang, from February 14, 2020 to June 1, 2020