DOI: 10.24996/ijs.2023.64.5.37

ISSN: 0067-2904

mRNA Approach Image Encryption Using LUC Algorithm

Noor Muneam Abbas *, Matheel E. Abdulmunim

Department of Computer Science, University of Technology, Baghdad, Iraq

Received: 13/6/2022 Accepted: 23/9/2022 Published: 30/5/2023

Abstract

Bioinformatics is one of the computer science and biology sub-subjects concerned with the processes applied to biological data, such as gathering, processing, storing, and analyzing it. Biological data (ribonucleic acid (RNA), deoxyribonucleic acid (DNA), and protein sequences) has many applications and uses in many fields (data security, data segmentation, feature extraction, etc.). DNA sequences are used in the cryptography field, using the properties of biomolecules as the carriers of the data. Messenger RNA (mRNA) is a single strand used to make proteins containing genetic information. The information recorded from DNA also carries messages from DNA to ribosomes in the cytosol. In this paper, a new encryption technique based on (mRNA) amino acids to increase the diffusion of the algorithm was proposed, also using the LUC algorithm with finite field arithmetic to increase the complexity of the algorithm. The results show high resistance against well-known attacks on the proposed method. For Entropy, the achieved value for the encrypted images was above 7.998. The range of peak signal to noise ratio (PSNR) between plain and encrypted images was below 8.7. Finally, the unified average change intensity (UACI) was close to 0.335. The number of changing pixel rates (NPCR) was close to 0.996, which is considered a good result.

Keywords: bioinformatics, RNA, mRNA, Lorenz system, Finite Fields, LUC algorithm.

تشفير الصور باستعمال المعلومات الحيوية (mRNA) مع خوارزمية LUC

نور منعم عباس *, مثيل عماد الدين عبدالمنعم

قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق

الخلاصة

المعلومات الحيوية هي أحد المواضيع الفرعية في علمي الحاسوب والأحياء الذي يهتم بالعمليات المطبقة على البيانات الحيوية، مثل التجميع، المعالجة، الخزن، والتحليل. البيانات الحيوية (الحمض النووي، الحمض النووي الريبوزي، والبروتين) لديها الكثير من التطبيقات والاستعمالات في مجالات عدة (أمنية البيانات، تقسيم البيانات، استخراج الخصائص، الخ). تستعمل سلاسل الحمض النووي في مجال التشفير عبر استعمال خصائص جزيئات الحمض كحامل للبيانات. ال mRNA يحتوي على المعلومات الجينية والتي تكون في DNA. سوف يتم اقتراح خوارزمية تشفير بالاعتماد على الاحماض الامينية المتوفرة في mRNA مع خوارزمية LUC لزيادة التعقيد. اظهرت النتائج انها جيدة في مقاومة الهجمات من الاشخاص غير المخولين.

*Email: 110128@uotechnology.edu.iq

بالنسبة إلى Entropy، كانت نسبة الانتروبي المحققة للصور المشفرة أعلى من 7.998 وأخيرًا كان نطاق
PSNR بين الصورة العادية والصورة المشفرة أعلى من 8.7. واخيرا كانت قيمه UACI مساويه ل 0.355
وNPCR مساوية ل0.996 والتي تعتبر نتائج جيدة.

1. Introduction

The field of image security covers the security needs in storage, transmission, and distribution [1]. This has led to more research and development in this area. The most secure technique used for images is image encryption, and it has been carried out in the spatial and frequency domains, in color, grey, and binary form [2] [3]. Other techniques used to protect the images are watermarking [4], secret sharing [5], and image hiding [6].
In general, encryption relies heavily on randomness, and the chaos system is considered one of the strongest random sequence generator systems [7] [8].

Recently, DNA's biological properties have received high attention and have been employed to enhance the security of cryptography and steganography systems [9] [10]. Others failed to combine DNA with chaotic systems [11] [12], as such a system needs to be built carefully to avoid deteriorating any encryption properties (speed, randomness, correlation, statistical analysis, known attack method, etc.).

Many encryption techniques are used to encrypt an image. Some proved efficient, while others failed to deal with images due to their speed, correlation, or perceptual nature.

The related works will be discussed in the next section, followed by a brief description of DNA, the Hyper Chaotic 4-D Lorenz system, and the LUC public encryption algorithm, which were used in the proposed encryption techniques. A detailed description of the proposed encryption system and the obtained results will follow. The last section presents the conclusions.

2. Related Work

Xingyaun et al. [13] proposed using chaotic scrambling and RNA computing in image encryption to encrypt grey-level images. The analysis revealed that this technique outperformed other methods in terms of encryption quality.
Hua et al. [14] proposed another chaotic system and got a high encryption level [15].
Pak et al. [16] employed bit-level encryption using a one-dimensional logistic map.
Ratnadewi et al. [17] used LUC in their method, with an issue with covering all the 256-pixel levels due to an inability to find sufficient prime numbers to grant the restoration of all pixel values.
RSA, DES, AES [18] [19] and other techniques were used in image encryption and a good security level was obtained.

3. Molecular Biology

Bioinformatics is a research area that acts as a link between biology and computer science. Researchers have suggested various definitions, or on the internet, some of which are more general than others. According to Luscombe et al. [20], bioinformatics involves the technology that uses computers for storage, retrieval, manipulation, and distribution of information related to biological macromolecules such as DNA, RNA, and proteins. A point of interest here is the high computation power required to process genomic data due to its high repetitive frequencies and complex mathematics [21].

The focus of bioinformatics is to decipher the secrets of living cells by studying and analyzing their molecular sequences and building blocks [20].

One of the components of bioinformatics is biological sequences (DNA, RNA, mRNA, and proteins). DNA is considered the storage location for genetic information and genetic features in the field of molecular biology [22]. This genetic information is responsible for all the behavioral and physical properties of living organisms [21], as it controls the organs and their functionalities of all known living organisms [12].

3.1 DNA

DNA is composed of double helices, which are long strands in shape. The building blocks of each helix are called nucleotides. The components of a nucleotide are the triplet: deoxyribose sugar, four bases (A, G, C, and T), which stand for adenine, guanine, cytosine, and thymine, respectively, and a phosphate group as shown in Figure (1) [23].

A DNA nucleotide is one of two groups: either purine, which includes A and G bases, or a pyrimidine base, which includes T and C [24]. The regular rules of interactions between nucleotides are A & T to make hydrogen bonds or C & G [24].

Bioinformatics has many fields in computer science. The fields that bioinformatics is used in are sequence analysis, genome mapping, expression analysis, molecular recognition (docking), molecular modeling, Intellectual Property Rights (IPR) data, profile generation, structure analysis, data integration, biological graphics, and data management [12]. Each of these components is a subject by itself.

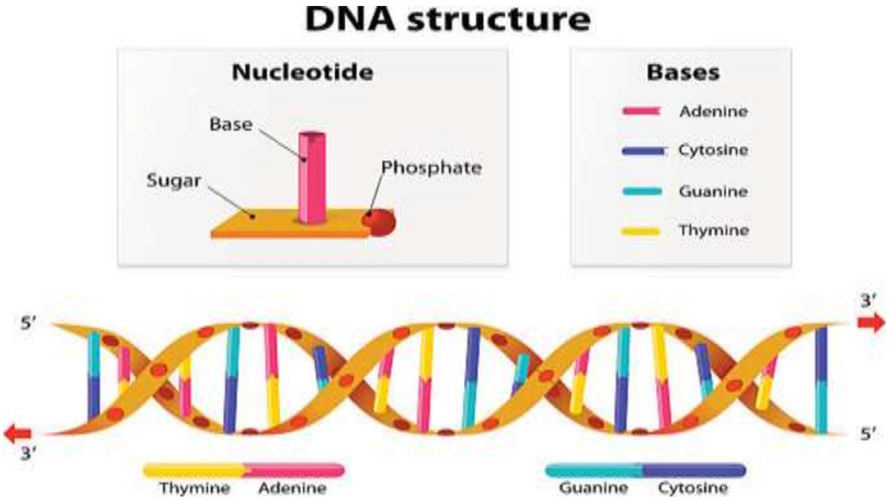


Figure -1 DNA structure.

3.2 RNA

RNA is a molecule like DNA. Contrasting to DNA, RNA is single-stranded. RNA consists of four bases: adenine (A), uracil (U), cytosine (C), or guanine (G). There are three types of RNA that exist in the cell: messenger RNA (mRNA), ribosomal RNA (rRNA), and transfer RNA (tRNA). Each one has its own structure according to its functions. Figure (2) below shows the RNA structure.

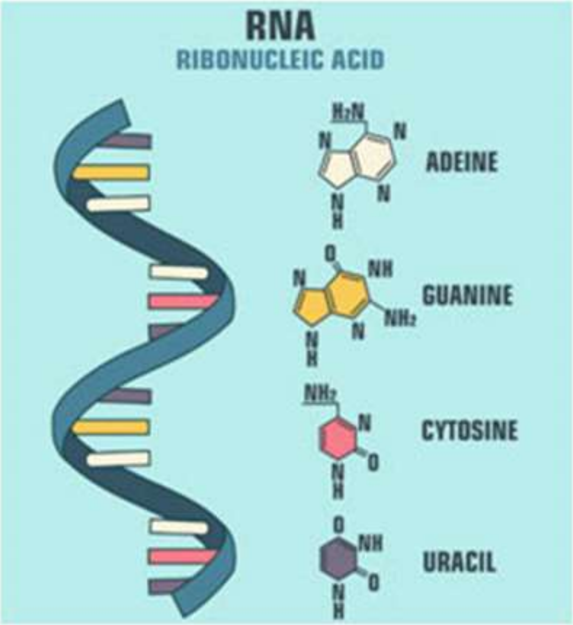
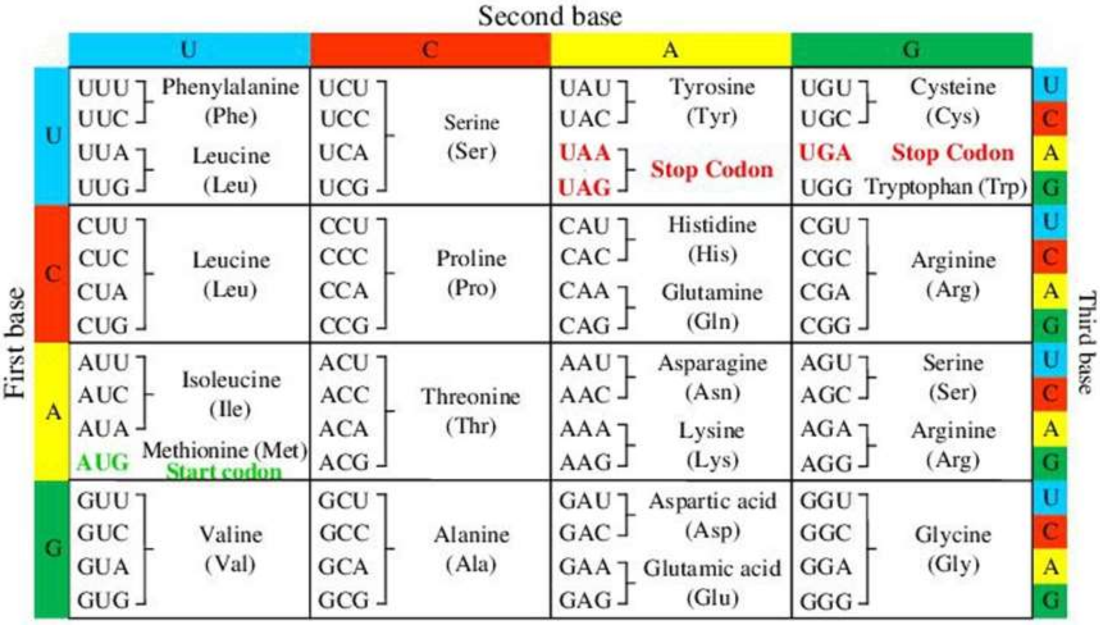


Figure 2: RNA structure.

3.3 mRNA

mRNA is a single strand used to make proteins and contains genetic information recorded from deoxyribonucleic acid (DNA). It also carries messages from DNA to ribosomes in the cytosol. Every three consecutive bases of the mRNA molecule can define an amino acid. Every three adjacent nucleotides in the mRNA molecule form a term known as a codon. It contains several codons to represent the amino acids. It has twenty (20) amino acids that make proteins. Figure (3) below shows the amino acids in mRNA. Table 1 contains a comparison between DNA and RNA.



	Second base				
First base	U	C	A	G	Third base
U	UUU Phenylalanine (Phe)	UCU Serine (Ser)	UAU Tyrosine (Tyr)	UGU Cysteine (Cys)	U
	UUC	UCC	UAC	UGC	C
	UUA Leucine (Leu)	UCA	UAA Stop Codon	UGA Stop Codon	A
	UUG	UCG	UAG	UGG Tryptophan (Trp)	G
C	CUU Leucine (Leu)	CCU Proline (Pro)	CAU Histidine (His)	CGU Arginine (Arg)	U
	CUC	CCC	CAC	CGC	C
	CUA	CCA	CAA Glutamine (Gln)	CGA	A
	CUG	CCG	CAG	CGG	G
A	AUU Isoleucine (Ile)	ACU Threonine (Thr)	AAU Asparagine (Asn)	AGU Serine (Ser)	U
	AUC	ACC	AAC	AGC	C
	AUA	ACA	AAA Lysine (Lys)	AGA Arginine (Arg)	A
	AUG Methionine (Met) Start codon	ACG	AAG	AGG	G
G	GUU Valine (Val)	GCU Alanine (Ala)	GAU Aspartic acid (Asp)	GGU Glycine (Gly)	U
	GUC	GCC	GAC	GGC	C
	GUA	GCA	GAA Glutamic acid (Glu)	GGA	A
	GUG	GCG	GAG	GGG	G

Figure 3: mRNA Amino acids.

Table 1: DNA vs RNA

	DNA	RNA
Base	*Consist of the 4 bases: A, G, C, T*	*Consist of 4 bases A, G, C, U*
Shape and structure	*Double helix strand*	*Single strand*
Age	*Longer life than RNA*	*Shorter life*
Process	*Main process is transcription*	*Main process is translation to protein*
Job	*Lead to produce RNA strand*	*Lead to the creation of proteins*
Types	*DNA is of a single type*	*RNA is of multiple type such as mRNA, tRNA, and rRNA*

4. 4D Lorenz System

Lorenz is a hyper-chaotic system of ordinary differential equations studied by Edward Lorenz, an American mathematician. This system is very sensitive to initial values and produces very different and chaotic results by changing any initial parameter by a small offset.

It was used as a three-dimensional model for many subjects, but then it was extended to cover many dimensions. A four-dimensional Lorenz system was used based on the following equations and initial parameters:

$$\begin{cases} \frac{dx}{dt} = a(y-x) - ew & \dots\dots\dots(1) \\ \frac{dy}{dt} = xz - hy & \dots\dots\dots(2) \\ \frac{dz}{dt} = b - xy - cz & \dots\dots\dots(3) \\ \frac{dw}{dt} = ky - dw & \dots\dots\dots(4) \end{cases}$$

Where x, y, z, and w are initial state variables and a, b, c, d, e, and h are parameters of the system [25] [26].

5. LUC Algorithm

LUC is a public key encryption algorithm built upon the Lucas function. LUC is similar in design to RSA, with a difference in the way of calculating the cipher by replacing the exponential operation of RSA with the Lucas function. The following represent the general steps of the LUC encryption algorithm [27]:

a- Select two large different prime numbers p, q.
b- Compute $n = p \times q$.
c- Choose public key e where $e < n$ and e is relatively prime to s(n) where:

$$s(n) = lcm\ (e, p-1, q-1, p+1, q+1)$$

d- Calculate d where $ed \equiv 1\ mod\ s(n)$
e- Compute cipher c by repeating the following formula e times

$$v_{i+1} = m \times v_i - Q \times v_{i-1}\ mod\ n$$

Where m = message, $v_1 = m$, Q =1,
For the decryption process, m is calculated using the following formula d times:

$$v_{i+1} = c \times v_i - Q \times v_{i-1}\ mod\ n$$

6. The Proposed Encryption Algorithm

The proposed encryption technique consists of four stages as shown in Figure (4) and algorithm 1. The first stage is to generate four-dimensional Lorenz sequences based on a processed encryptor input. The second stage is to shuffle the image rows and columns based on the proposed technique. The third stage is to use the proposed mRNA technique to process image pixels, which will change the pixel's color values dramatically to eliminate correlation and statistical information. The final stage is to use a modified LUC public encryption technique based on finite field arithmetic over the Galois field (GF 2^n), where n is the size of a pixel or color in bits.

Algorithm 1: proposed work.

```
Input: Original image (N * M), key.
Output: Encrypted image (N * M).
Begin
Step 1: Generate 4-D Lorenz system hyperchaotic sequences ($X_0$, $Y_0$, $Z_0$, $W_0$).
Step 2: Shuffle images rows and columns using algorithm 2, shuffle (Image, X, Y).
Step 3: Code resultant image with algorithm 3, mRNA Amino acids (shuffled image, Z, W).
Step 4: Encrypt coded image using LUC using algorithm 4, LUC (coded image, key).
End.
```

Four hyper chaotic sequences are generated using the following initial conditions: a=5, b=20, c=1, d=0.1, e=20.6, k=0.1, h=1, and dt=0.01 and four seeds (X, Y, Z, and W) were supplied by the encryptor or derived from a key. X and Y sequences are used to generate rows and columns of shuffling indices using the following steps and as stated in algorithm 2:

1- Generate indices for rows and columns sorted incrementally.
2- Re-order these indices according to the sorting of X and Y incrementally.
3- Re-arrange rows and columns of the images' pixels based on the re-ordered indices.

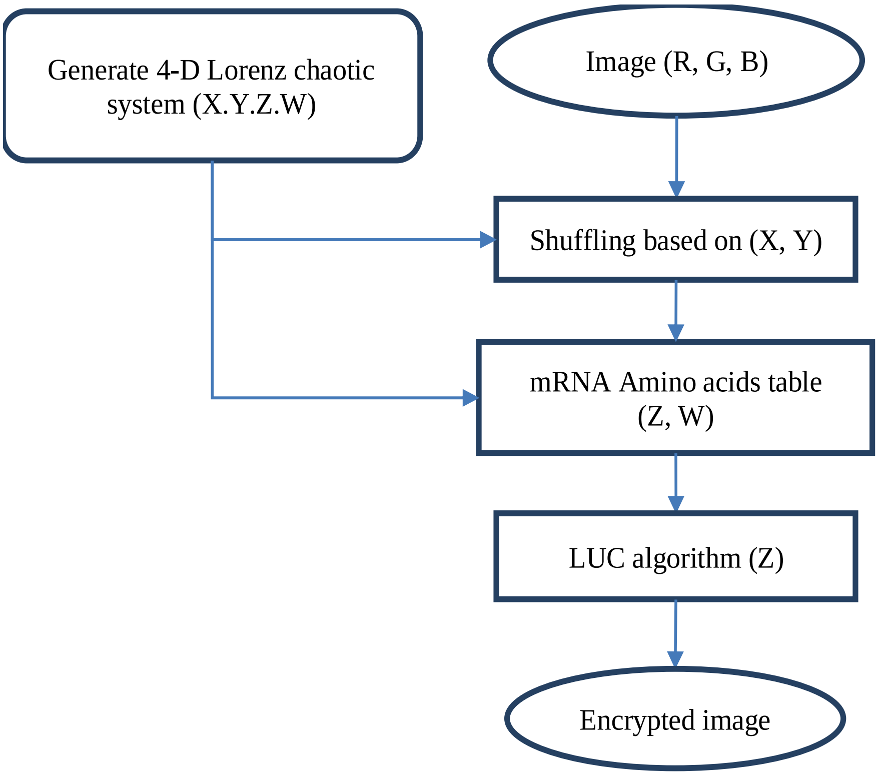

Generate 4-D Lorenz chaotic system (X.Y.Z.W)
Image (R, G, B)
Shuffling based on (X, Y)
mRNA Amino acids table (Z, W)
LUC algorithm (Z)
Encrypted image

Figure 4: Proposed algorithm.

```
Algorithms 2: Image shuffling.
Input: Original image, Hyper-chaotic sequences X and Y.
Output: Shuffled image.
Begin
Step1: generate row shuffling index row_index table based on sequence X by sorting X incrementally and sort row_index accordingly.
    a-  Create row_index table where table index represents image row and table value represent current row location.
    b-  Sort X values and record each X sequence value new location in row_index table.
    c-  Re-order image rows based on row_index new values.
Step2: perform same sub steps of step 1 on columns using column_index and Y sequence in same fashion to re-order image columns.
End.
```

The third stage of this work starts by taking the output of the previous stage. In the proposed mRNA-based substitution technique, the pixel (24 bits) is divided into 12 pairs and converted to 12 DNA codons using the default coding. Then the complement of each codon is taken to convert it into an mRNA codon. The twelve codons are then divided into 4 amino acids each (3 codons each).

The pixel's four amino acids are then rearranged based on four indices extracted from the third-dimension values of the Lorenz system (Z) for each pixel.

The rearranged amino acids are then substituted with other triplets that belong to the same amino acid based on a substitution index extracted from the fourth-dimension values of the Lorenz system (W) for each triplet. The following example illustrates the full process of MRNA substitution:
Let pixel (R=50, G=100, B=150), the current four Z values are (3, 2, 4, 1), and the current four W values are (5, 2, 3, 1).

First, convert 50, 100, and 150 to DNA. The result will be TGTA, CACT, and ACCA. Then take its complement and convert it to MRNA codon T=A, G=C, C=G, A=U, yielding ACAU, GUGA, UGGU.
Second, divide them into four MRNA amino acids by
D1=most 6 bits of red = 110011 = 51
D2= least 2 bits of red followed by most 4 bits of green = 01 1001 = 25
D3= least 4 bits of green followed by most 2 bits of blue = 1011 01 = 45
D4= least 6 bots of blue = 101001 = 41

The results are the four amino acids : ACA, UGU, GAU, and GGU.
Third, the four amino acids are shuffled based on index (3,2,4,1) and the result is GAU, UGU, GGU, ACA.
Fourth, each triplet is substituted with another one that belongs to the same amino acid based on substitution index.

GAU = Asp where Asp= (GAU, or GAC) using index 5 we ended with GAC
UGU = Cys where Cys= (UGU, or UGC) using index 2 we ended with UGU
GGU = Gly where Gly= (GGU, GGC, GGA, or GGG) using index 4 gives GGC
ACA = Thr where Thr= (ACU, ACC, ACA, or ACG) using index 1 we ended with ACG
The new four triplets are GAC, UGU, GGC, and ACG.

The final step is to code the MRNA triplet back to DNA and then to pixel values.
a- Complement: GAC= CTG, UGU= ACA, GGC= CCG, ACG= TGC

b- Convert four triplets to three quartet: CTGA, CACC, GTGC
c- Convert back to pixel values CTGA= 78, CACC= 101, GTGC= 205
Plain pixels (50, 100, 150) yield ciphered pixels (78, 101, 205) and the difference is that 11 bits out of 24 bits are changed. Algorithm 3 shows mRNA amino acids.

```
Algorithm 3: mRNA amino acids.
Input: Shuffled image, Hyper-chaotic sequences Z and W.
Output: coded image using mRNA.
Begin
Step 1: Image pixel (24 bits) is divided into 12 pair and converted to 12 DNA codons using the default coding.
Step 2: The complement of each codon is taken to convert it into mRNA codon, the twelve codons are then divided into 4 amino acids (3 codons each).
Step 3: Re-arrange pixels based on four indices extracted from the third-dimension values of the Lorenz system (Z) for each pixel.
Step 4: Substitute triplet with other triplets which belong to the same amino acid based on a substitution index extracted from the fourth-dimension values of the Lorenz system (W) for each triplet.
Step 5: Final step is to code mRNA triplet back to DNA then to pixel values to generate the output image.
End.
```

The final stage is to encrypt the coded image using LUC encryption over Galois fields GF(2^8) using algorithm 4. Although LUC, like RSA, is a public key encryption system based on prime numbers, many researchers used LUC in image encryption, using two prime numbers whose product is less than 256, causing a loss in some color information. Although it is a small loss, it is unacceptable in some applications.
To overcome this issue, LUC over finite field (GF2^n) is proposed.

The normal LUC uses two different large prime numbers, which are replaced by two irreducible polynomials whose product equals the number of bits required (in the case of image encryption, it is 8 bits for each color, or 24 if we want to encrypt the whole pixel).
For the general encryption formula:

$$V_{i+1} = M * v_i - Q * v_{i-1} Mod\ n$$

where v_1=M=message, v_0 =2 Q=1, referring to the original paper of LUC [27] v_0 is equal to 2 since $v_n = \alpha^n + \beta^n$ and n=0, when using (GF2^n) arithmetic v_0 will become 0 since 1+1 equals 0 in (GF2^n).

```
Algorithm 4: LUC encryption over finite fields arithmetic GF($2^n$).
Input: coded image in mRNA amino acids, key.
Output: encrypted image.
Begin
Step 1: Select two different irreducible polynomials (p and q) where the sum of p and q degrees equal to 8 (color size).
Step 2: Calculate N which is the product of p and q over GF (2)
                    $N = p * q$
Step 3: Select encryption key e where GCD (e, N) ==1.
Step 4: Calculate R where $R = lcm(2^p - 1, 2^p + 1, 2^q - 1, 2^q + 1)$.
Step 5: Calculate private key d where $d \equiv e^{-1} mod\ R$.
Step 6: encrypt all pixel colors using the following formula:
        For i =1 to e
                    $v_{i+1} = m \times v_i - Q \times v_{i-1}\ mod\ n$
        Next
                    $c = v_i$
Where Encryption result C = $V_e$
End.
```

7. Decryption Algorithm

The decryption process is straightforward for all stages except for the LUC, and it is carried out in reverse order. That is, for the first decryption stage after generating Lorenz sequences using the same initial parameters, it is LUC decryption using algorithm 5:

```
Algorithm 5: LUC decryption over finite fields arithmetic GF($2^n$).
Input: encrypted image, decryption key.
Output: mRNA encrypted image.
Begin
Step 1: Select two different irreducible polynomials (p and q) where the sum of p and q degrees equal to 8 (color size).
Step 2: Calculate N which is the product of p and q over GF (2)
                                        $N = p * q$
Step 3: Select encryption key e where GCD (e, N) ==1.
Step 4: Calculate R where $R = lcm(2^p - 1, 2^p + 1, 2^q - 1, 2^q + 1)$.
Step 5: Calculate private key d where $d \equiv e^{-1} mod\ R$.
Step 6: decrypt all pixel colors using the following formula:
        For i =1 to d
                                $v_{i+1} = c \times v_i - Q \times v_{i-1}\ mod\ n$
        Next
                                        $m = v_d$
Where Encryption result m = $v_d$
End.
```

Next stage of decryption, is the inverse of mRNA amino acid using algorithm 6:

```
Algorithm 6: mRNA amino acids.
Input: Decrypted image from LUC, Hyper-chaotic sequences Z and W.
Output: decrypted image.
Begin
Step 1: pixel (24 bits) is divided into 12 pair and converted to 12 DNA codons using the default coding.
Step 2: generate the complement of each codon is taken to convert it into mRNA codon, the twelve codons are then divided into 4 amino acids (3 codons each).
Step 3: substitute with other triplets which belong to the same amino acid based on an inverse substitution index extracted from the fourth-dimension values of the Lorenz system (W) for each triplet.
Step 4: rearrange pixels based on four inverse indices extracted from the third-dimension values of the Lorenz system (Z) for each pixel.
Step 5: Final step is to code mRNA triplet back to DNA then to pixel values to generate the output image.
End.
```

In the de-shuffling stage, the steps are the same as the shuffling in the encryption but using the offset as index, the result of this step is the original image.

8. Results and Quality metrics

The following are the perceptual results of encryption and decryption for some images, along with the statistics of encryption and decryption.

The first used image was Lena 256*256, as shown with its encryption stages in Figure (5).

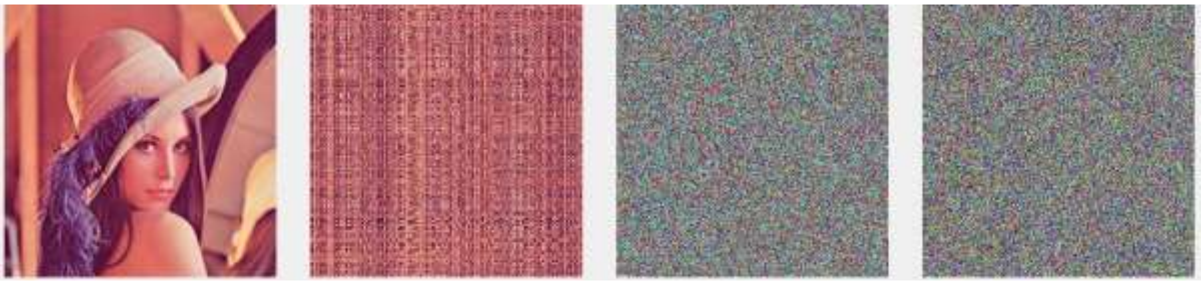


Figure 5: Lena image encryption (a- original image b- shuffling process c- mRNA amino acids d- Luc algorithm).

The decryption process stages of this image are shown in Figure (6):

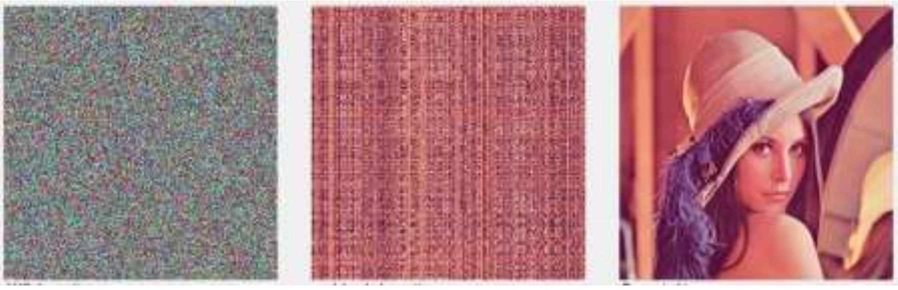


Figure 6: Lena image decryption a-Luc decryption b- decryption of mRNA c- decrypted image.

Some of the quality metrics were used to evaluate this work, such as:

1- MSE: mean squared error measures the average squared difference between the original image and the resultant image; in encryption, the higher the MSE, the better the encryptor is. To measure MSE, the following equation is used [28]:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - x_i)^2$$

2- PSNR: Peak signal to noise ratio is the similarity ratio between the two images (encrypted and original). A high PSNR means images are more similar to each other. In encryption, it is desired that PSNR is low and fall below 10 dB. To measure PSNR the following equation is used [29]:

$$PSNR = 10\log\frac{\max pixel\ value^2}{MSE}$$

3- EQ: Encryption Quality represents the average number of changes to each grey level L and is computed using the following equation [23]:

$$EQ = \frac{\sum_{L=0}^{255}|P_L(y) - P_L(x)|}{256}$$

4- AD and MD: average difference and maximum difference, are two measures used to evaluate decryption quality. They show if there is any difference between the original and the decrypted image. A value of zero means the two images are identical and any other value means the opposite. To calculate these metrics, the following equations are used [23]:

$$AD = \sum\nolimits_{i=1}^{n}\frac{|y_i - x_i|}{n}\ , \qquad MD = MAX\,|y_i - x_i|$$

5- Correlation coefficients: correlation is the measure of correlation between adjacent lines of pixels. It is calculated for vertical and horizontal lines and sometimes diagonally. The lower it is (near zero), the better it is. To calculate correlation coefficients, the following equation is used [12]:

$$CC = \frac{covariance\ (x, y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Table 2 shows the results of Lena image encryption quality.

Table 2: Results of Lena 256*256.

image	PSNR (original & decrypted)	PSNR (original & encrypted)	MSE	SAD	EQ	AD	MD	NCC	Correlation Coefficient
Lena 256	∞	8.741	0	0	58650.63	0	0	1	-0.009 V -0.006 H

The result in Table (2) indicates the following:

a- The decrypted image is identical to the plain image based on the values of MSE and PSNR.

b- The vertical and horizontal correlation coefficients indicate that the correlation between adjacent rows and columns has been removed, and the encrypted image has no correlation in it.

c- The encryption quality is very high, indicating that the encryption technique has changed everything in the plain image.

The second image used was of size 512 *512, with its results in Figure (7) and its decryption process stages in Figure (8):

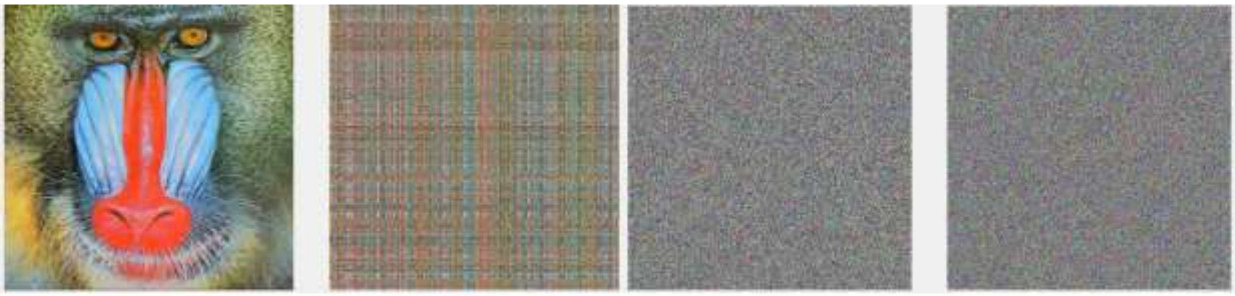

(a) (b) (c) (d)

Figure 7: 512 image encryption a. original image b. shuffling process c. RNA amino acids d. LUC algorithm.

The decryption process is shown in figure (8):

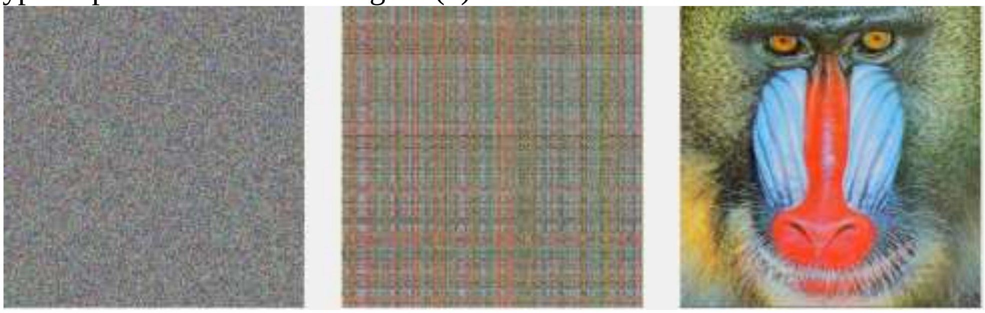

(a) (b) (c)

Figure 8: 512 image decryption a-Luc decryption b- decryption of mRNA amino acids c- original image.

Table 3 shows the results of Baboon image encryption quality.

Table 3: Results of Baboon 512 *512.

Image	*PSNR (original & decrypted)*	*PSNR (original & encrypted)*	*MSE*	*SAD*	*EQ*	*AD*	*MD*	*NCC*	*Correlation Coefficient*
Baboon 512	∞	8.778	0	0	234500.12		0	1	-0.06 V -0.01 H

The results in Table (3) indicate the following:

a- The decrypted image is identical to the plain image based on the values of MSE and PSNR.

b- The vertical and horizontal correlation coefficients indicate that the correlation between adjacent rows and columns has been removed, and that the encrypted image has no correlation in it.

c- The encryption quality is very high, indicating that the encryption technique has changed everything in the plain image.

8.1 Encryption and Decryption Runtime

Table (4) shows the run time for image encryption and decryption. It takes a few milliseconds.

Table 4: Runtime images

Name	dimension	size	Encryption time (seconds)	Decryption time (seconds)
Lena	256*256	192kb	00.01	00.03
Baboon	512*512	768kb	00.03	00.15
Peppers	512*512	768kb	00.03	00.15

8.2 Entropy

One of the most essential characteristics of the cipher image measurement is the entropy, which measures the diversity. For a perfectly diverse image, entropy should be 8, and any close value to 8 indicates a strong diversity. To measure entropy, the following equation is used:

$H(x) = -\sum_{i=0}^{m} p(x_i)\, log\, p(x_i)$, where p is the probability of each pixel value

Table (5) shows the entropy of different images.

Table 5: Entropy of different images

Image	Entropy
Lena	7.997
Baboon	7.998
Peppers	7.998
Barbara	7.997
Flowers	7.995

The entropy of the encrypted images is very close to the unified distribution of 8, which is very desirable in encryption techniques to eliminate most types of attacks and to eliminate any analysis capability to determine the geometry, shape, contents, color information, etc. The figures (9, 10, and 11) show the histogram of (Lena, Baboon, and Peppers) images.

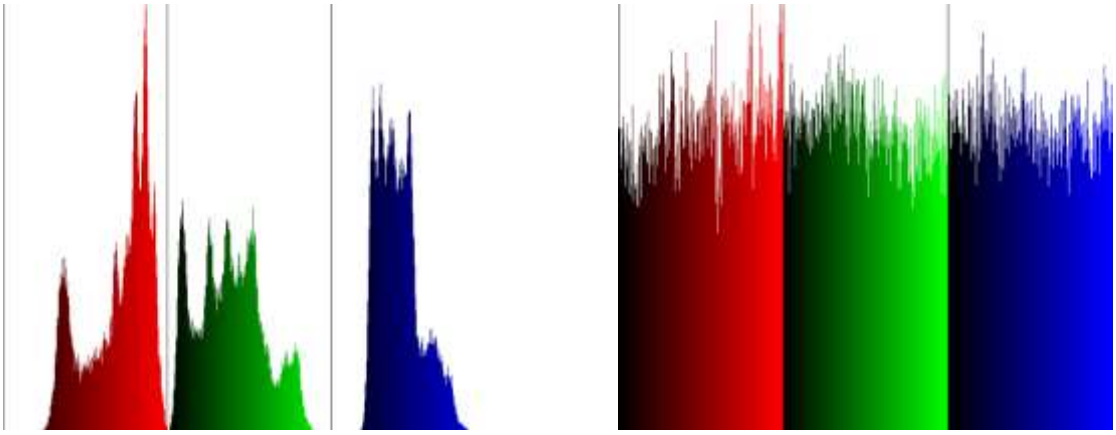

(a) (b)

Figure 9: Histogram of Lena image a- histogram of plain image, b- histogram of encrypted image.

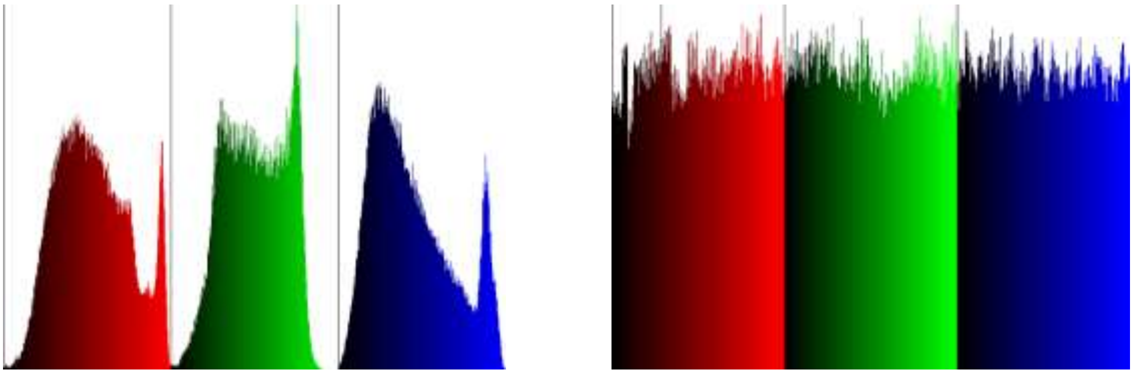

(a) (b)

Figure 10: Histogram of Baboon image a- histogram of plain image, b- histogram of encrypted image.

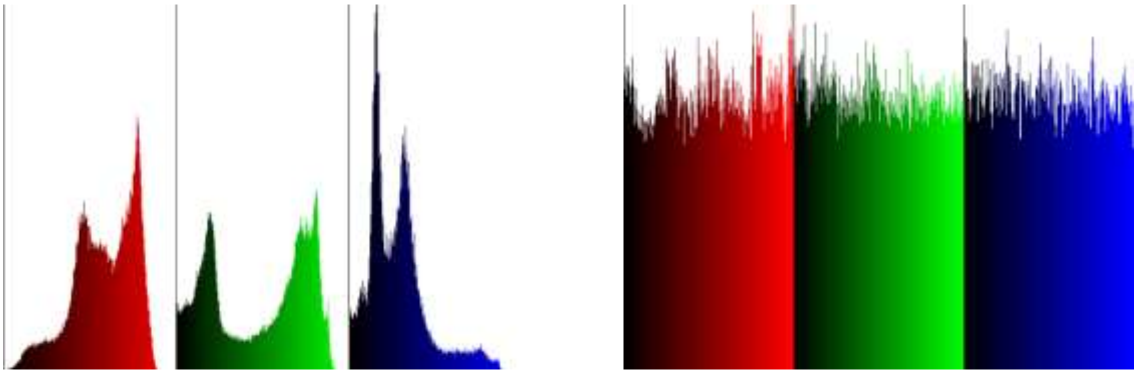

(a) (b)

Figure 11: Histogram of pepper image a- histogram of plain image, b- histogram of encrypted image.

Also, one of the desired properties of any encryption technique is to produce a close to uniform distribution from a non-uniform plain image, and that is what has been achieved using our technique.

8.3 Differential Attacks Analysis

The Number of Modifying Pixel Rate (NPCR) and Unified Average Adjusted Intensity (UACI) are two of the most commonly used measurements to estimate the strength of image encryption algorithms. These measurements were taken after a single bit in the key was changed.

Table 6: NPCR and UACI of different images when key is differed by one bit

Name	NPCR	UACI
Lena	0.995	0.335
Baboon	0.996	0.336
Peppers	0.995	0.335

Considering that the NPCR value is close to 0.996 and the UACI value is close to 0.3346, it indicates that the randomness effect of the key is very high, and according to the measured values, changing one bit of the key causes the desired change in the ciphered image.

9. Comparison study.

Tables (7-8-9) show comparison studies between the proposed algorithm and others:

Table 7: Comparison of entropy with other algorithms

Image	proposed system	Ref **[30]**	Ref **[31]**
Lena	7.9978	7.9979	7.9973

Table 8: Comparison of Encryption Quality (EQ) with other algorithms

Image	proposed system	Ref **[29]**
Lena	58650.636	3765.887
Baboon	234500.125	6879.435

Table 9: Comparison of time encryption

Image	proposed system (seconds)	Ref **[28]**
Lena	0.01	0.709

According to the above tables, this work is getting better or very close in score to some of the related works, but in terms of time, this work is dominating others and is getting a superior score.

10. Conclusions.

The following points were concluded from the proposed work:

1- The encryption time is very low and it is desirable in communication to have a very fast encryption scheme.

2- It uses a public-key encryption scheme to encrypt the image, and this system is more desirable because of the problem of key exchange, which is not available in such schemes compared to symmetric encryption.

3- The mRNA technique helps in destroying the inner relationship of pixel values.

4- The image shuffling technique removes cross-pixel relations to eliminate correlation between pixels.

5- The Lorenz attractor assists in the generation of a one-time pad-like random key that is used to encrypt each pixel individually and prevent attackers from discovering any relationships between pixels.
6- This is the first time that LUC is used with finite field arithmetic to make it more suitable for bit-sized data values.
7- The quality metric values of this work show high encryption quality, and changing the key by a small value generates a very different result.

References

[1] G. Singh and S. , "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33-38, 2013.

[2] M. Subhedar and V. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vols. 13-14, pp. 95-113, 2014.

[3] G. Hamed, M. Marey, S. A. El-Sayed and M. F. Tolba, "Comparative study for various DNA based steganography techniques with the essential conclusions about the future research," 11th *International Conference on Computer Engineering & Systems* (ICCES), vol. 11th, pp. 220-225, 2016.

[4] R. Abdulrida, M. E. Abdulmunem and A. M. Jaber, "Quantum image watermarking based on wavelet and geometric transformation," *Iraqi Journal of Science*, vol. 61, no. 1, pp. 153-163, 2020.

[5] Z. Radeef and A. Hashim, "Multiple Image Secret Sharing based on Linear System," *Indian Journal of Science and Technology*, vol. 10, no. 33, pp. 1-17, 2017.

[6] M. Abdulmunim and A. N. , "Proposed advanced hiding method on color images based on DMWT," *European Journal of Scientific Research*, vol. 79, pp. 385-392, 2012.

[7] A. K. Jabbar, A. T. Hashim and Q. F. Al-Doori, "Secured Medical Image Hashing Based on Frequency Domain with Chaotic Map," *Engineering and Technology Journal*, vol. 39, no. 5A, pp. 711-722, 2021.

[8] A. Hamad and A. K. Farhan, "Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme," *Engineering and Technology Journal*, vol. 38, no. 3B, pp. 98-103, 2020.

[9] M. T. Sulaiman and N. F. Hassan, "Propose an Arabic CAPTCHA System," *Engineering and Technology Journal*, vol. 36B, no. 1, pp. 48-52, 2018.

[10] S. Hamad, A. Elhadad and A. Khalifa, "DNA Watermarking Using Codon Postfix Technique," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1605 - 1610, 2017.

[11] F. Elamrawy, M. Sharkas and . A. M. Nasser, "An Image Encryption Based on DNA Coding and 2DLogistic Chaotic Map," *International Journal of Signal Processing*, 2018.

[12] X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, 2018.

[13] X. Wang and L. Liu, "Application of chaotic Josephus scrambling and RNA computing in image encryption," *Multimedia Tools and Applications*, vol. 80, p. 23337–23358, 2021.

[14] Z. Hua, F. Jin, B. Xu and H. Huang, "2D Logistic-Sine-Coupling Map for Image Encryption," *Signal Processing* , vol. 149, pp. 148-161, 2018.

[15] Z. Hua, B. Xu, F. Jin and H. Huang, "Image encryption using Josephus problem and filtering diffusion," *IEEE*, vol. 7, pp. 8660 - 8674, 2019.

[16] C. Pak, K. An, P. Jang, . J. Kim and S. Kim , "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools and Applications*, vol. 78, p. 12027–12042, 2019.

[17] R. Ratnadewi, C. D. Alpha G, D. Napitupulu and H. Nurdiyanto, " Ratnadewi Ratnadewi," *Journal of Physics Conference Series*, 2018.

[18] R. R. P. Adhie, Y. Hutama and A. S. Ahmar, "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System

Based Near Field Communication (NFC)," *Journal of Physics: Conference Series*, Volume 954, Issue 1, 2018.

[19] R. Y. Hutama, R. Adhie, J. Christian and D. Wijaya, "Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system," *World Transactions on Engineering and Technology Education*, vol. 15, no. 2, pp. 178-183, 2017.

[20] J. Xiong, *Essential Bioinformatics, Cambridge University Press*, 2012.

[21] H. B. Abdul wahab and T. M. Abed, "Anti Phishing Based On Visual Cryptography And 4D Hyperchaotic System," *Iraqi Journal of Information Technology*, vol. 9, no. 1, pp. 1-27, 2018.

[22] K. Zhan, D. Wei, J. Shi and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, 2017.

[23] M. E. Abdulmunim and Z. Mohammad, "Image encryption using DNA addition," Thesis submitted to computer science at university of technology.

[24] R. A. Hussain, M. E. Abdulmunim and A. M. J. Abdul-Hossen, "Propose Image Encryption Watermarking Algorithm Based on Frequency and Geometric Transform," 2019 *2nd Scientific Conference of Computer Sciences* (SCCS), pp. 143-147, 2019.

[25] R. Enayatifar, H. Abdullah and I. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83-93, 2014.

[26] F. Zhang, X. Liao and G. Zhang, "Qualitative behaviors of the continuous-time chaotic dynamical systems describing the interaction of waves in plasma," *Nonlinear Dynamics*, vol. 88, no. 3, p. 1623–1629, 2017.

[27] P. J. Smith and M. J. J. Lennon, "LUC: A New Public Key System," Tech. Reports, 1993.

[28] L. L. Xingyuan Wang1, "Image encryption based on hash table scrambling and DNA substitution," *IEEE Access*, 2020. 10.1109/ACCESS.2020.2986831.

[29] A. K. Farhan and A. A. Abdallah, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi Journal of Science*, vol. 63, no. 1, pp. 324-337, Jan 2022. DOI: 10.24996/ijs. 2022.63.1.31.

[30] Liu, Hui et al., "Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling," *Entropy* (Basel, Switzerland), vol. 21, No. 4, Mar. 2019. doi:10.3390/e21040343

[31] Xiuli, Chai., Fu, Xianglong., Zhihua, Gan., Yang, Lu., Yi, Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol.155, pp. 44-62, 2019.
doi: 10.1016/J.SIGPRO.2018.09.029