Al-Qadisiyah Journal of Pure Science

Volume 26 | Number 2 Article 14

4-7-2021

Chaotic System and DNA Computing operations for Image Encryption Based on Pixels Shuffling

Alaa Kadhim Farhan
Computer Science Department, University of Technology, Baghdad, Iraq, 110030@uotechnology.edu.iq

Ekhlas K. Gbashi
Computer Science Department, University of Technology, Baghdad, Iraq, 110026@uotechnology.edu.iq

Recommended Citation
Farhan, Alaa Kadhim and Gbashi, Ekhlas K. (2021) "Chaotic System and DNA Computing operations for Image Encryption Based on Pixels Shuffling," *Al-Qadisiyah Journal of Pure Science*: Vol. 26: No. 2, Article 14.
DOI: 10.29350/qjps.2021.26.2.1265
Available at: https://qjps.researchcommons.org/home/vol26/iss2/14

QJPS
Al-Qadisiyah Journal of Pure Science

Al-Qadisiyah Journal of Pure Science

ISSN(Printed): 1997-2490 ISSN(Online): 2411-3514

DOI: /10.29350/jops.

http://qu.edu.iq/journalsc/index.php/JOPS

Chaotic System and DNA Computing Operations for Image Encryption Based on Pixels Shuffling

Authors Names

a.Alaa kadhim Farhan

b.Ekhlas K. Gbashi

Article History

Received on: 16/1/2021
Revised on: 15/2/2021
Accepted on: 17/2/ 2021

Keywords:

image encryption, chaotic system ,DNA computing, shuffling .

DOI: https://doi.org/10.29350/jops.2021.26. 2.1265

ABSTRACT

Image encryption is one of the primary approaches which is used to keep image information secure and safe. Recently, image encryption is turning its attention to combination with the field of DNA computing. In the presented study, a novel method of image encryption is suggested and implemented based on the DNA algorithm and Chaos theory, the most important principle in image encryption is breaking the correlation amongst pixels. This algorithm performs well against chosen cipher-text attacks. Furthermore, the proposed approach was implemented and analyzed for the Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), The performance of the encryption method is analyzed using the histogram, Shannon entropy and key space.

a. Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: 110030@uotechnology.edu.iq.

b. Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: 110026@uotechnology.edu.iq

1. Introduction

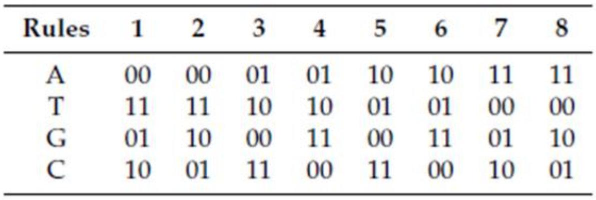
Utilizing digital images for the purpose of expressing information is considered to be informative, vivid, and intuitive; accordingly, so the digital images are the typical approach to express information [1]. As image information are used widely, it is a main issue to ensure the security [2][13]. Recently, the technology of encrypting digital images is of high importance in protecting the security of image information [3]. Because of the high-redundancy characteristics and large data volume of the digital images, the traditional encryption approaches cannot satisfy the requirements of image encryption due to the low-security and low-effectiveness of the encryption process [23].In the year of 1949, the idea of perfect security has been introduced by Shannon, also, he indicated that the one-time pad cryptosystem had ideal security, as indicated in his research “Communication Theory of Secrecy Systems” [22]. Yet, the transfer and the distribution of the one-time pad’s secret key faced certain difficulties. Based on the pseudo randomness [13], chaotic system’s predictive difficulty, the sensitivity to initial value, and chaotic sequence could carry out the same encryption impact with one-time pad as the random key , and theoretically it cannot be broken [24]. The technology of chaotic encryption is extensively applied in information security, particularly in image encryption [17]. one in more using the chaotic theory in A.I algorithm and text preprocessing[4]. Chen et al. presented diffusion and confusion structure of image encryption algorithm according to chaotic system. Nevertheless, because of the limits in the word lengths of the computer, chaotic dynamic degradation could be a result of using chaotic sequences, particularly for the chaotic systems of low-dimension [25]. This could affect the chaotic encryption’s security. Thus, For the purpose of improving the algorithm’s security, hyper chaos system was utilized by a number of scholars for ensuring the chaotic sequence’s complexity [2]. Yet, it is a fact that the security of the encrypted image cannot be guaranteed via a single-encryption algorithm of chaotic mapping. In biology, DNA can be defined as a significant carrier for the genetic information [15], also it is of high importance in genetic organism metabolism. The main benefits of DNA are the low consumption of energy, ultra-high storage density, and extremely large-scale parallelism [5]; the distinctive DNA’s molecular recognition method as well as its molecular structure define its significant information processing and information storage ability [24]. The molecules of DNA have exceptional development ability with regards to hidden certification, information encryption [18], in addition to other aspects of information security that offers a novel approach to develop the current cryptography [26]. In the1995, Dan et al. cracked a 56-key code in a period of four months, which for the first time combined the concept of conventional DES with DNA computing [11]. After that, studying the progress of DNA cryptography became a main research area. In the year of 1999, Gehani et al., utilized DNA as a carrier for information, also, they realized one-time conventional encryption algorithm through the use of bio-chemical technology in DNA molecule [6]. Also in 1999, Celland et al., realized the information hiding through the use of DNA as a carrier for the information, also they hide the well-known information “June 6 invasion: Normandy” in a DNA micro point in WWII, therefore realizing steganography according to the DNA’s natural storage capacity[20]. In the year 2017, Le Goff et al. carried out3-D (array particle) encryption model, also, they efficiently created 3-D DNA hydrogel particle arrays within 100 microns in size via thermal shrinkage film and the technology of DNA particle for fixing the polymers of DNA on polyethylene heat-shrink chip[16].Such algorithms realized the location replacement regarding the pixels of the image, which modified the gray value, yet, have been unsuccessful in achieving the aim of true diffusion .Thus, the proposed study suggests a novel image encryption algorithm through combining DNA code with the chaotic system. DNA coding using in A.I in many field [7]. Using approach substation and shifting as well as DNA operations, therefore improving the properties of diffusion and confusion in the algorithm via iterative chaotic systems and cipher-text feedback.

2. DNA Computing

2.1 DNA computing is an evolving branch of computing that, instead of conventional electronic computing, uses DNA, biochemistry, and molecular biology hardware. In this field, research and development concerns theory, experiments, and DNA computing applications. While the field originally began with Len Adleman's presentation of a computer application in 1994, it has now been extended.

DNA sequences are used to encrypt information in the encryption of the communication methods, mainly the ones that need a robust data encryption scheme to challenge unauthorized access [12]. In this section, the DNA coding rules and spatiotemporal chaos used in Reference [7] are introduced, and then the specific steps of IEA-DESC are detailed .There are 4 kinds of nucleic acids bases on the DNA sequence: A, T, C, and G. With regard to the 4 bases, the total number of coding combinations is 4! = 24. Yet, there are just 8 kinds of coding combinations since the4 bases fulfill the principle of complementary base pairs. More accurately, T and A are considered to be complementary to each other, as G and C. Table 1 displays the 8DNA coding rules.

Table 1. Eight kinds of DNA coding rules.



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

2.2 Chaos theory is a branch of mathematics that focuses on the study of chaos, complex systems that are actually governed by fundamental patterns and deterministic rules that are extremely sensitive to initial conditions, seemingly random states of disorder and irregularities. Chaos theory is an interdisciplinary theory that there are underlying patterns, interconnectedness, continuous feedback loops, repetition, self-similarity, fractals, and self-organization within the apparent randomness of chaotic complex systems. The butterfly effect, an underlying chaos concept, explains how a slight shift in one state of a deterministic nonlinear system will result.

In 1976, the logistic map was discovered by the biologist Robert may. It is a simple nonlinear polynomial mapping equation, its main idea, and its objective was to study and describe the biological populations and their growth. Its important parameters are shown in equation (1): the 1D logistic map is represented in figure (1). [8][19]

$$f(y_i) = ry_i(1 - y_i) \tag{1}$$

Where the parameter represents the state variable, r Є[1,4],and it is considered to be the control parameter [20]The phase plan for the logistic map is illustrated in Figure below.

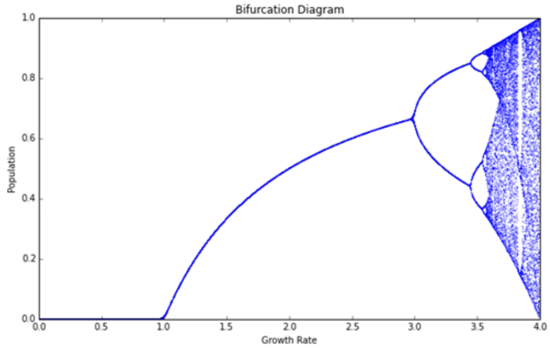


Figure (1): The Logistic map phase plane [9]

The 2D-Logistic map has been introduced by Liu [9], as described in Eq.(2).

$$\begin{aligned} f(X_i) &= R_1X\,(1 - X_i) + Q_1z_i^2 \\ f(Y_i) &= R_2y_i(1 - z_i) + Q_2(y_i^2 + y_iz_i) \end{aligned} \tag{2}$$

This map depends on two main parameters, (Y) and (Z) that control the behavior of this map. The experiments show a considerable improvement in terms of complexity and security where their values belong to [0, 1].The chaotic behavior appears when the values of the control parameters are; [0.15 < Q1 < 0.21, 0.13 < Q2 < 0.15, 2.75 < R1< 3.4, and 2.7 < R2< 3.45] [8].Where the initial values of Xn,Yn[0,1].After some iterations the resulting values of X and Y also belong to[0,1].

3. The Proposed Method

Image data have strong correlations among adjacent pixels. For the purpose of disturbing the high-correlations between pixels, the pixel positions of the plain image will be shifted. With no loss of generality, the dimension of the plain image will be N × N. In this suggested approach, we focus on principles as confusion and diffusion to break the correlation between the pixels.

Encryption: in the beginning, the original image is broken to three channels as (R,G,B) after that, the channels are converted from decimal to DNA char as (C,T,G,A) to be ready to DNA operation with security keys(R,G,B),in example can take one pixel in (R,G,B) after split ,the value for channal R equal 1 byte as (255) ,after that we convert to binary sequnce as (11111111),this sequence binary split to 2 bits blocks, and each block match with DNA table to get the char as(A) and so on for each values in channels. the security keys also as DNA chars. The new (R,G,B) values using Decoding operation to convert from DNA chars to decimals for shifting to left based on security decimal keys(K1,K2, and K3). The substitution operation is an important process to break the correlation between pixels for (R, G, B) using AES S-Box to get new pixels. The process of swap is done between (R,G) to become (G,R), it is more important as Fiestel mod operation, the location of the G channel is reordered based on the IP DES table to get new pixels, construct (R,G,B) to get the cipher image. Decryption: the same process but in the reverse order. The secret keys are generated form 1D logistic map equation depending on initial and condition parameters used in encryption and decryption processes. Figures (2, 3) and algorithms1, 2, and 3 are explain all processes:

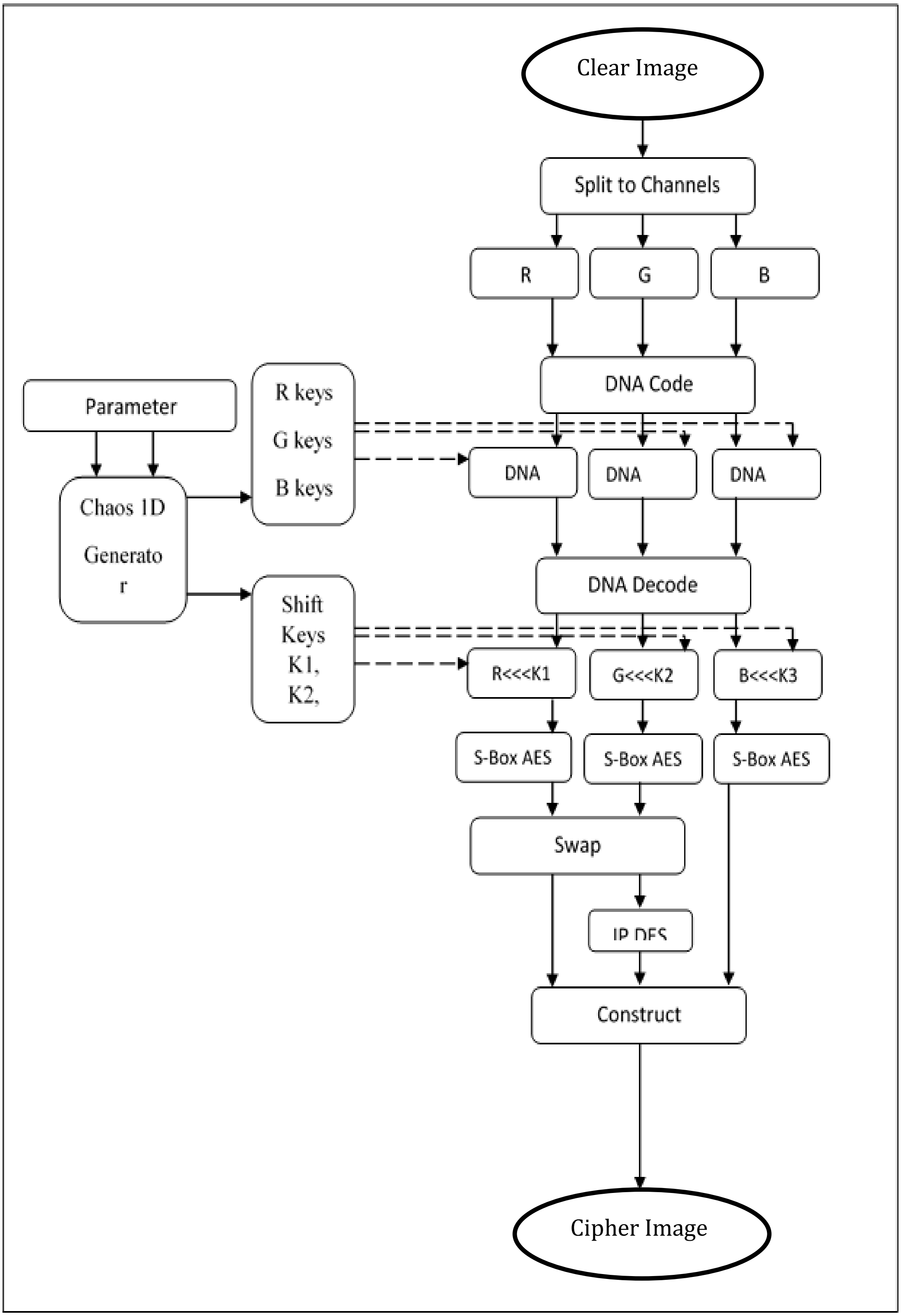


Figure (2): Encryption for the Proposed Method

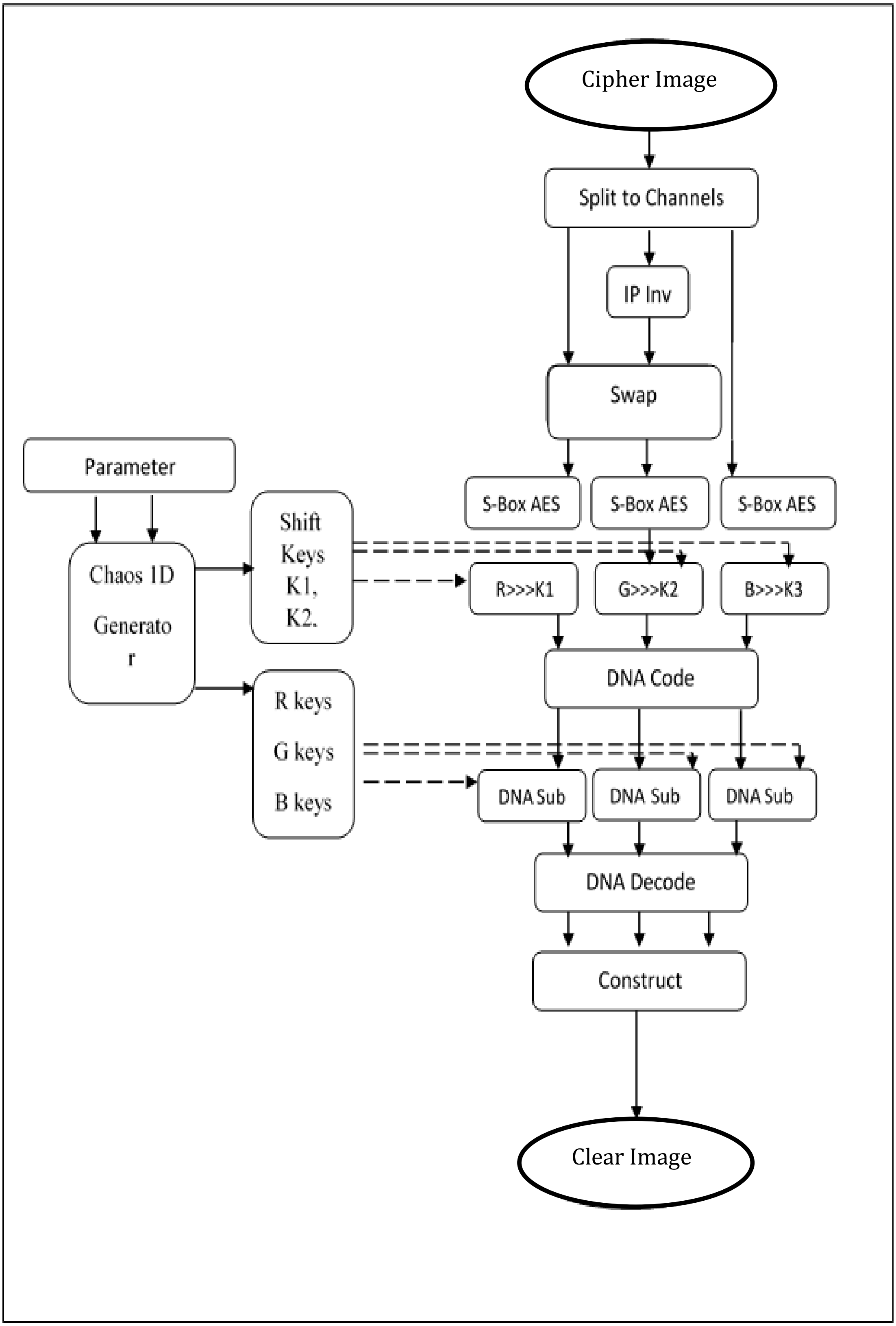

Cipher Image
Split to Channels
IP Inv
Swap
Parameter
S-Box AES
S-Box AES
S-Box AES
Chaos 1D Generator
Shift Keys K1, K2.
R>>>K1
G>>>K2
B>>>K3
DNA Code
R keys
G keys
B keys
DNA Sub
DNA Sub
DNA Sub
DNA Decode
Construct
Clear Image

Figure (3): Decryption for the Proposed Method

```
Algorithm (1):The Encryption Algorithm
Input: Clear Image, Secrete Keys
Output: Encrypted Image
Begin
Step 1:Split the image to (R,G,B)
Step 2: Convert Channels(R, G, B) decimal number to DNA coding operation on table 1.
Step 3: ADD DNA operation for (R, G, B) with (K1,K2, K3)
Step 4: Convert Channels(R, G, B) DNA$_s$ to Decimal based on Decoding operation.
Step 5:Shift  to left operation on (R,G,B ) using (K1,K2,K3)
Step 6:Substitution process in S-Box of AES for (R,G,B)
Step 7:Swap(R,G) to (G,R)
Step 8:Use IP table in DES to (G) Channel
Step 9:Construct (R,G,B) into the Cipher Image
End
```

```
Algorithm (2):The Decryption Algorithm
Input: Cipher Image, Secrete Keys
Output: Clear Image
Begin
Step 1:Split the image to (R,G,B)
Step 2:Using IP table in DES to (G) Channel
Step 3:Swap(R,G) to (G,R)
Step 4:Substitution process using AES S-Box for (R,G,B)
Step 5:Shiftto right operation to (R,G, B) using (K1,K2,K3)
Step 6:Convert Channels(R, G, B) from decimal numbers to DNA coding operation in table 1.
Step 7:Sub DNA operation for (R,G, B) with (K1, K2, K3)
Step 4:Convert Channels(R, G, B) DNA to Decimal based on the Decoding operation.
Step 9:Construct (R,G,B) into the Cipher Image
End
```

```
Algorithm (3):Secret Key Generation Algorithm
Input:  Parameter and Condition of 2D Chaotic Map
Output: K1,K2 and K3 Sequences
Begin
Step 1: Apply the equation of 2D chaotic map to get a huge sequence of Xi, Yi and store it in the buffer.
Step 2: Convert Xi and Yi from float to integer numbers by deleting the real part.
Step 3:ConcatX and Y to obtain one sequence
```

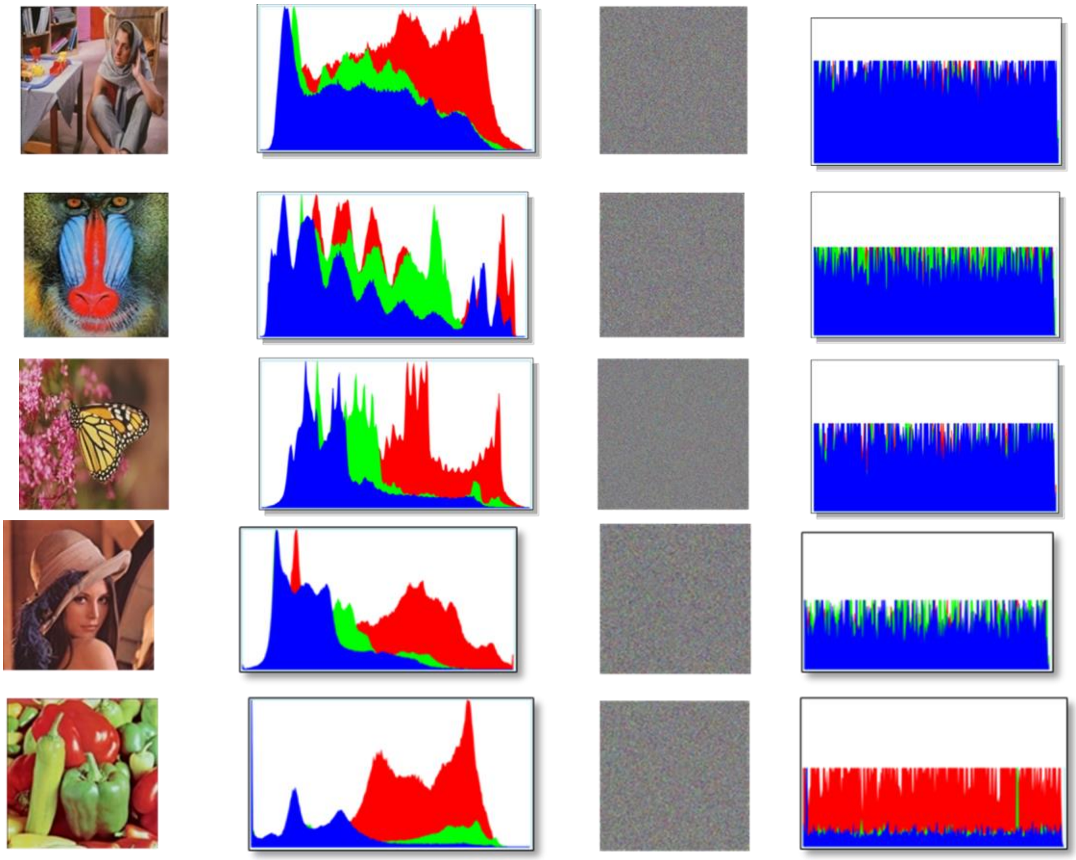
Step 4:Split the sequence in step 3 to three keys as (K1,K2, and K3)
End

4. Performance of the Proposed Encryption Method

To analyze and test the performance of encryption and decryption, some measures are applied; these measures help us to study the performance of security of the encryption method.

4.1 Differential Attacks Analysis

The pixel strength diffusion measurements for a picture are represented in a histogram from a picture. A secure encryption system should provide identical histograms to survive statistical attacks. The histogram in Figure 4(a, b, c, d) depicts Lena, Pepper, Barbara, Baboon and Pepper's regular and encrypted pictures. We evaluated from Figure 4(a, b, c, d) that the histograms of regular images are not accurate, while the histograms of the digital images that have been encrypted are reliable. The uniformity of the pixel heights of the histograms of the encrypted image makes it hard to find an insight into the maximum information region for attackers.



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

Figure (4): histogram of Lena, Pepper, Barbara, Baboon and Pepper (a) plain image, (b) histogram of plain image, (c) cipher image, (d) histogram of cipher image.

And in figure 5, The histogram in Figure 4(a, b, c, d) shows the standard and decryption images of Lena, Pepper, Barbara, Baboon and Pepper, added to the decryption method to see the original image. Figure 4(a, b, c, d) indicates that standard image histograms are not reliable, whereas digital image histograms that have been decrypted are accurate.

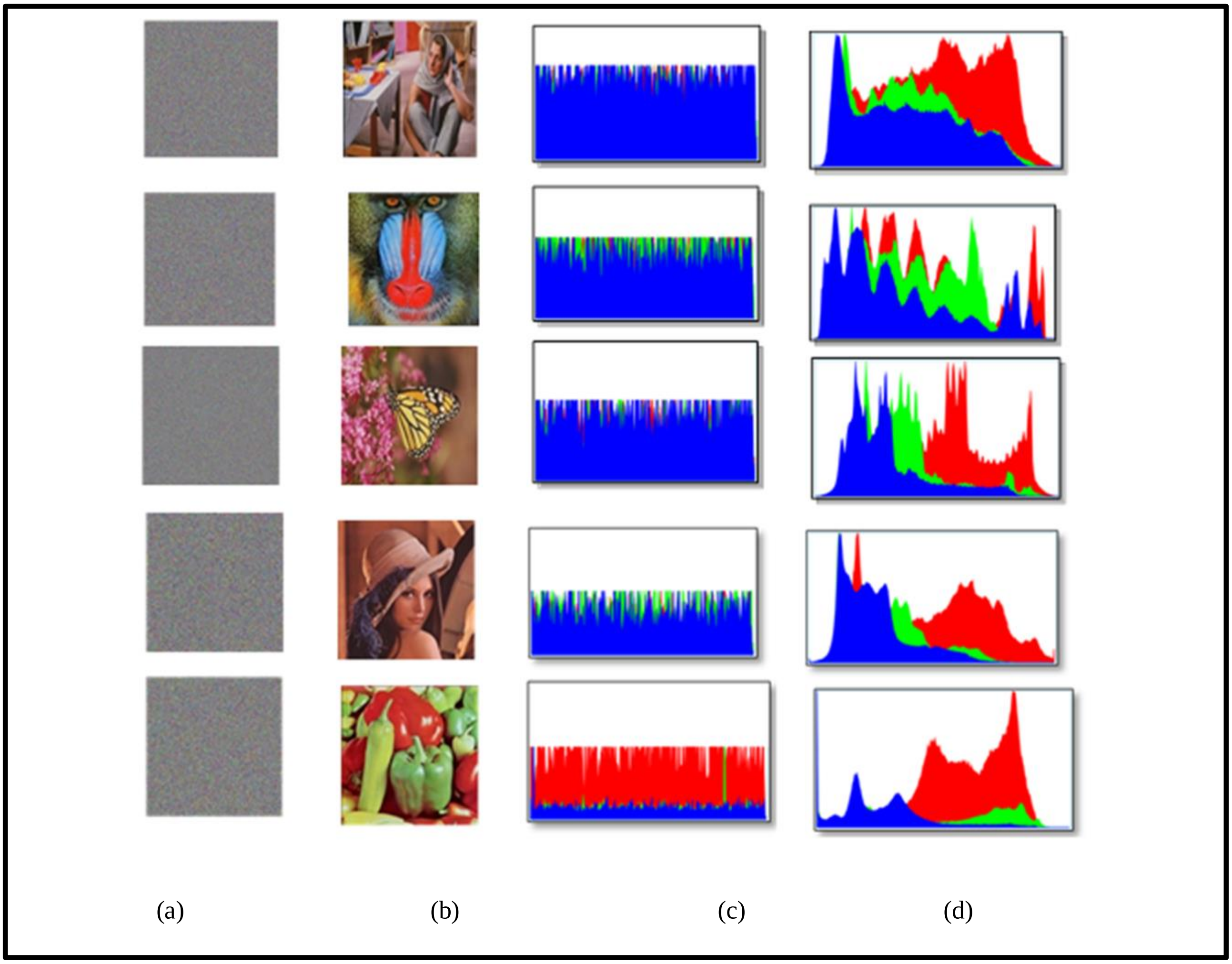


Figure (5): (a) cipher image ,histogram of Lena, Pepper, Barbara, Baboon and Pepper (b) plain image, (c) histogram of cipher image, (d) histogram of plain image.

4.2 NPCR and UACI Tests

NPCR indicates the number of pixels change rate while a single pixel of the plain image changes. It converges to 100%, which is mean the sensitivity of the cryptosystem to changing in the plain image, also the results showed that the effectiveness of the proposed crypto-system to resist plain-text attacks where the value of UACI indicates the mean value of the intensity of differences between plain and cipher images, and it converges to 33.333%, that is mean the cryptosystem is effective and robust against differential attacks. Those two metrics are calculated from the following equations [10]:

$$\text{UACI} = \frac{1}{\text{Width}\times\text{Height}} \sum_{i,j} \left(\frac{c_1(i,j) - c_2(i,j)}{255} \right) \times 100\% \tag{3}$$

$$\text{NPCR} = \frac{\sum_{i,j} D\,(i,j)}{\text{Width}\times\text{Height}} \times 100\% \tag{4}$$

c1(i, j) and c2(i, j) are the encrypted-image prior to changing one pixel of the plain image and after it, respectively. And in the case wherec1(i,j) ≠c2(i,j), then D(i, j) = 1otherwise,D(i, j) = 0.The results after changing a pixel'sR value are shown in table (2) and also see the Correlation Coefficients Analysis between images. In table (3) comparison between the original image and retrieval image after decryption, we found no loss in pixels and can get the original image.

Table2: NPCR and UACI Results

Name	NPSR	UACI	CC
Paper	0.99209	0.3328	0.0054
Barbara	0.99209	0.3335	0.00113
Baboon	0.99211	0.3320	0.00017
Lena	0.99420	0.3341	0.00235
Monarch	0.99710	0.3325	0.000061

Table3: Comparison between original and decryption images in MSE and PSNR

name	MSE	PSNR
Paper	0.00004	99.99991
Barbara	0.00001	99.99990
Baboon	0.00003	99.99989
Lena	0.00020	98.9900
Monarch	0.00001	99.99988

4.3 Information Entropy

Image information entropy may be represented by the following equation:

$$\text{H}\,(\text{m}) = \sum_{i=0}^{2N-1} p\,(m_i) \log_2 \frac{1}{p\,(m_i)} \tag{5}$$

Where p(mi) is the probability of (mi), and log2 is base 2 logarithm which expresses the entropy, N is the number of bits that are utilized for representing a pixel, and for a pixel's one color channel, it is obvious that N = 8. In case where the image is ideally random, which is mean that for every i, p (mi) = 1/256, and it is easily found that H(m) = 8. the results of cipher image have been listed in table(4).

Table 4: Information Entropy

Name	Paper	Barbara	Baboon	Lena	Monarch
Information Entropy	7.9977	7.9972	7.9982	7.9980	7.9975

4.4 Security Analysis

Security is the most important part of many cryptosystems. A good encryption algorithm should be sensitive to the secret keys and have large key space to resist all kinds of known attacks [19].

- **Key Space**

It is a set of possible permutations of the key where a master space is usually designed so that it is large enough to make it an opponent consuming considerable time to try to break it where the key is chosen randomly for other key variations but many people do not randomly choose passwords. So, attackers often try to use the dictionary attack before apply the brute force attack and this method can produce the correct answer in a much less time than brute force search for all the possibilities being possible, the key space of our work are large possible if our key space 9 digits .We mean the attacker must get all 9 digital numbers to get and know the secrete key ,so $(2^{9\text{digtal}} *^{8\text{ bit}} = 2^{78})$ possible key space the modified in secret key that lead to modified in add, sub and shifting operations.

- **Key Sensitivity**

Key sensitivity is an another important metric needed by a cryptosystem which is ensure that no data can be recovered from the cipher text even though there is only a minor difference between the encryption and decryption keys, in chaos theory any one-bit change in initial value (in 1D chaos theory in X_0 or in condition values) lead to change the key. Key sensitivity can be observed if slightly different keys are applied to encrypt the same plain than completely different cipher, and if a negligible difference exists in decryption key, then the cipher could not be decrypted correctly. And can explain the effective modified secret key to retrieval plain image can see in table (6).in this table when modified simple initial sensitive key in decryption that lead to unclear u(decryption) image.

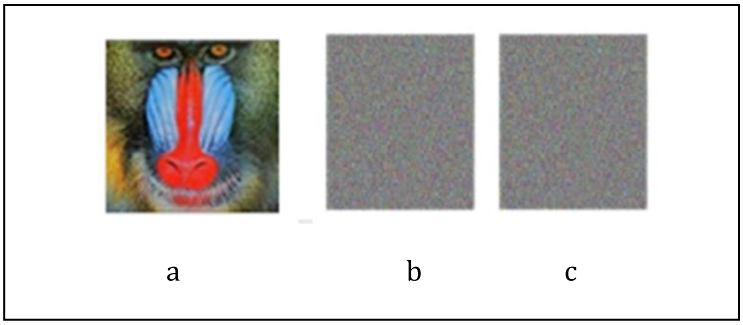


Figure (6): (a) plain image, (b) cipher image (Pepper), (c) plain image (noise),

5. Conclusions

The results of the implementation and evaluation of the suggested system proved its efficiency, where the values of each of the Correlation, NPCR, UACI, and entropy are considerably close to the optimum values. In addition to that, the proposed algorithm has provided an additional level of confusion because of the S-box transformation. Mainly, this algorithm hits the S-P (P via shift and rotate) network idea of Shanon principle as diffusion and confusion.

References

[1] A. K. Farhan, N. M. G. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," Entropy, vol. 21, no. 10, p. 958, 2019.

[2] A. K. Farhan, M. R. Salman, and others, "Color Image Encryption Depend on DNA Operation and Chaotic System," in 2019 First International Conference of Computer and Applied Sciences (CAS), 2019, pp. 267–272.

[3] A Kadhim, RM Mohamed ,"Visual cryptography for Image depend on RSA & AlGamal algorithms", 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA),PP 1-6,May.2016.

[4] Abdul Monem S Rahma, Suhad M Kadhem, Alaa Kadhim Farhan, "Finding the Relevance Degree between an English Text and its Title," Engineering and Technology Journa, vol. 30, issue 9,pp 1625-1640, 2012.

[5] Alaa Kadhim, Sura Khalaf, "New approach for security chatting in real time," International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), 2015, Volume 4, Issue 3

[6] A. Gahlaut, A. Bharti, Y. Dogra, and P. Singh, "DNA based cryptography," in Communications in Computer and Information Science, 2017.

[7] AMS Rahma, SM Kadhem, AK Farhan,"Finding the Relevance Degree between an English Text and its Title", Engineering and Technology Journal 30 (9), 1625-1640

[8] A. T. Sadiq, A. K. Farhan, and S. A. Hassan, "A proposal to improve RC4 algorithm based on hybrid chaotic maps," J. Adv. Comput. Sci. Technol. Res., vol. 6, no. 4, pp. 74–81, 2016.

[9] A. Kadhim F. and H. Emad M., “Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers,” Diyala J. Pure Sci., vol. 13, no. 3, pp. 24–39, 2017.

[10] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, “Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder,” Entropy, vol. 21, no. 10, pp. 1–14, 2019.

[11] D. Boneh, C. Dunworth, and R. Lipton, “Breaking DES using a molecular computer,” 1996.

[12] Ekhlas K. Gbashi “Text Compression & Encryption Method Based on RNA and MTF”, Journal of science(IJS),university of Baghdad,VOL 58,ISSUE (2C),2017.

[13] Farhan AK, Ali MA. “Database protection system depend on modified hash function. In Conference of Cihan University-Erbil on Communication Engineering and Computer Science 2017 Mar 29 (p. 84).

[14] F. A. Kadhim and H. I. Mhaibes, “Quantum Random Bits Generator based on Phase Noise of Laser,” J. Eng. Appl. Sci., vol. 13, no. 3, pp. 629–633, 2018.

[15] F. A. Kadhim, G. H. A. A. Majeed, and R. S. Ali, “Proposal new s-box depending on DNA computing and mathematical operations,” in 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), 2016, pp. 1–6.

[16] G. C. Le Goff, L. J. Blum, and C. A. Marquette, “Shrinking hydrogel-DNA spots generates 3D microdots arrays,” Macromol. Biosci., 2013.

[17] H. Rathod, M. S. Sisodia, and S. K. Sharma, “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm),” vol. 1, no. 3, pp. 7–13.

[18] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, “A new hyper chaotic map and its application for image encryption,” Eur. Phys. J. Plus, 2018.

[19] H. Natiq, M. R. M. Said, N. M. G. Al-Saidi, and A. Kilicman, “Dynamics and complexity of a new 4D chaotic laser system,” Entropy, 2019.

[20] H. Natiq, S. Banerjee, M. R. K. Ariffin, and M. R. M. Said, “Can hyper chaotic maps with high complexity produce multistability?,” Chaos, 2019.

[21] K. Menaka, “Message encryption using DNA sequences,” in Proceedings - 2014 World Congress on Computing and Communication Technologies, WCCCT 2014, 2014.

[22] M. Y. Rhee, Internet security: cryptographic principles, algorithms, and protocols. 2003.

[23] N. K Pareek, “Design and Analysis of a Novel Digital Image Encryption Scheme,” Int. J. Netw. Secur. It’s Appl., vol. 4, no. 2, pp. 95–108, 2012.

[24] R. A. Mollin, An introduction to cryptography, second edition. 2006.

[25] R. Pakshwar, V. Trivedi, and V. Richhariya, “A survey on different image encryption and decryption techniques,” Int. J. Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 113–116, 2013.

[26] W. Cao, Y. Mao, and Y. Zhou, “Designing a 2D infinite collapse map for image encryption,” Signal Processing, 2020.