2019 International Conference of Computer and Applied Sciences (1st CAS2019)
Mustansiriyah University, Education College, Computer Science Department, Baghdad, Iraq

Color Image Encryption Depend on DNA Operation and Chaotic System

Muna R. Salman
Computer Science Dept
Education Col., Mustansiriyah Uni
Baghdad, Iraq
muna.salman20178muna@gmail.com

khalid A.Hussein
Computer Science Dept.
Education Col., Mustansiriyah Uni.
Baghdad, Iraq
dr.khalid.ali68@gmail.com

Alaa K.Farhan
Computer Science Dept
Education Col., Mustansiriyah Uni.
Baghdad, Iraq
110030@uotechnology.edu.iq

***Abstract*—: In the recent years, the interest in information security has increased due to the great development of modern technology in the world, which led to the increase of the various attacks on data and essential information. Therefore it was necessary to have encryption techniques that protect the transmitted information In this study, a new algorithm of colour image encryption based on DNA and the chaotic map is proposed. The diffusion is achieved by using the processes of shifting and permutation, and the confusion is achieved by using the processes of S-box and mathematics. This algorithm was applied to different image sizes and type (bmp, jpeg). The proposed algorithm is intended to be complex and repel attacks. The shifting process is done on colours (R, G, B) from left to right, giving new pixels different from the old ones. The hexadecimal process and box-S are applied to the blue colour to increase confusion. The process of computing of DNA takes place in two colours (red and green). Pixel locations are altered by permutation (R, G, B) become (B, R, G) this process to increase diffusion. Finally, mathematical operation take place (blue, red) decomposes pixels and increase confusion. This algorithm has a highly sensitive key and can cope with various attacks due to the use of DNA computing and chaotic system.**

Keywords— Color image, DNA computing, Chaotic map

I. INTRODUCTION

Information security is generally focused on protecting secrecy, integrity and availability of information. Information security is a set of procedures, processes, personnel and technology aimed at protecting the organisation [1][2][ ]. Deoxyribonucleic acid (DNA) The DNA utilise the alchemical characteristic of these molecules enzymes. Biological motivating can be named "software" utilised to perform the coveted account[3]. Chaos conduct of dynamic systems that are very sentient to primary condition chaotic complex systems, small differences in initial conditions can result in large differences. Dynamical system to display chaotic behaviour, it must chaos it is nonlinear have finite or infinite-dimensional [4]. Qiang Z., Ling G., and Xiaopeng w.,[5]

In this study, the researchers have The encryption process occurs on the grey image using the DNA sequence, addition, and complement to obtain the encrypted image.

Furthermore, used two logistic map (1D and 2D). in third step decode the DNA sequence matrix. This algorithm has a very sensitive key making it good for repelling statistical and differential attacks. The similarities with our proposal are the use of DNA computing and chaos theory and we have a highly sensitive key**.** Sadiq A., and Anwar A., 2018 [6]. In this study color images were encrypted depending on novel 3 dimentional chaotic system and DNA. chaotic system calculate Lypunove exponents if one value positive this chaotic system. When initial sensitivity value, used XOR operation between random value for novel chaotic and DNA. This algorithm has a large space key and high sensitivity. Used both histograms, collaboration, entropy, NPCR and UACI. The results were good and proved to be efficient in encoding images, an algorithm resistant to statistical and differential attacks. The results were good and proved to be efficient in encoding images, an algorithm resistant to statistical and differential attacks. It consumes little time in encrypting images .prove that this algorithm has perfect security. The similarities with our proposal are the use of DNA computing; chaos theory Consume a good time to encrypt images.

II. IMAGE ENCRYPTION

Images play a large and effective role in the life of humanity, especially images that require protection from attacks. **[**7**].** Moreover, consist of two colours, black and white and one bit. The colour image (*RGB*) consists of 24 bits because each colour is 8 bits red, green and blue colours; each of them has 8 bits [8].

A. DNA Sequence

There are four nitrogen rules utilised to make a series of DNA. They are thymine (T), cytosine (C), adenine (A) and guanine (G). These four rules (T, C, A And G) are rules in a way like to letters the alphabet. The series of these DNA rules will symbolise genetic information [9]. Genetic information in DNA is transferred to and from RNA to protein, but not from protein to DNA. The double helix of the DNA has a coupling base C: G and A: T [10].

B. DNA Encoding and Decoding

The DNA series consists of bases of thymine, guanine, adenine, and cytosine, when C, G are complementary, T and Aare complementary, and each of T, C, A and G have binary numbers 00, 11,01and 10, using this any 8-bit. e.g "AGCT",", "CATG" ,"GATC", "GTAC", "TGCA", "CTAG", "ACGT" and "TCGA" " [11].

TABLE I: DNA CODING RULES[4]

Rules of DNA			
00	01	10	11
A	T	C	G

TABLE II :COMPLEMENTS OPERATION[4]

chromosomes	A	T	G	C
complements	T	A	C	G

C. Chaos Theory

It is one of the important systems because of two important results of this dynamic nonlinear behaviour is irreversibility and unpredictability, because of the chaotic behaviour that this type of system may carry it.[12][15].The Two-dimensional Chaotic System:
Given the following two first-order differential equations[13]:

$$\frac{dx}{dt}=ay^2\text{- b}x^2\text{-c} \quad \ldots(1)$$

$$\frac{dy}{dt}=dxy-ex \quad \ldots(2)$$

X=1.2, y=0.8, a=4, b=1.1, c=4.4, d=0.1, e=8.
x, y true number a, b, c, d, e positive values. Lyapunov exponents and Lyapunov dimensions an attraction dynamics limited. Susceptible to primary stipulations.

- Fragmentary due fractal type.
- non- cyclic tropic.
- Close paths space.

The proposed non-longitudinal system is chaotic conduct. The stage portraits performance by using an arithmetical program which exhibitions complexity and copious chaotic system conduct with strange attractors in two-dimensions(x-y).

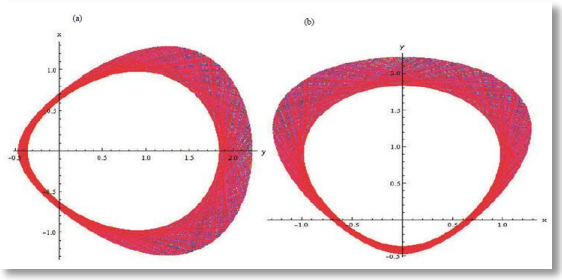

Fig. 1: (i) Two- dimensions sight (x-y).
(ii) Two- dimensions sight (x-y).

D. Proposal Approach to Encrypt Image Based on DNA and Chaotic Theory.

Initially, the original image is divided into channels blue, red and green. When using colours separately. The secret keys generated from chaotic there using in many operations as shifting. The first channel(red) using shift depend on secret key1 (shift (R, secret key1mod8)). The second channel(green) using shift depend on secret key2 (shift (G, secret key2 mod 8)). The Third channel (blue) uses the shift based on two secret keys from chaotic (shift (B, (secret key1+secret key2) mod 8)). Both channels red and green using DNA table of one column consist characters A, T, C and G. for G DNA with its complement by using the following rules, then Let it be G DNA comp. Implementation of DNA addition operation for R DNA and X DNA depending on DNA addition table rules. Applying of DNA addition operation for G DNA and YDNA depending on DNA addition rules table. Convert B to hexadecimal and then applying substitution operation. Applying for permutation operation by replacing the locations of the colour of the colours resulted from the previous step. And then apply an arithmetic operation to provide a cipher image. In this proposal achieved diffusion and great confusion. In step, the shift achieved the diffusion, in S-box confusion. Increase the security level and increase the complex level. One of the advantages of this algorithm is to encode any images may be Bitmap or Joint Photographic Experts Group. The following diagram can explain the main idea of encryption

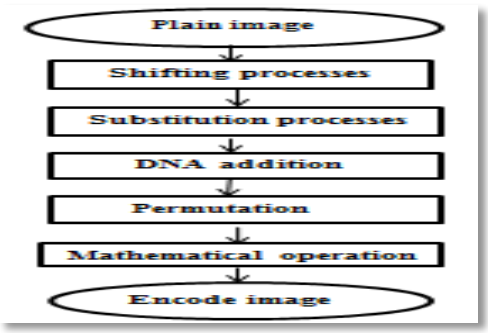

Fig. 2: diagram of proposed structure encryption.

The diagram can explain the main idea to decryption:

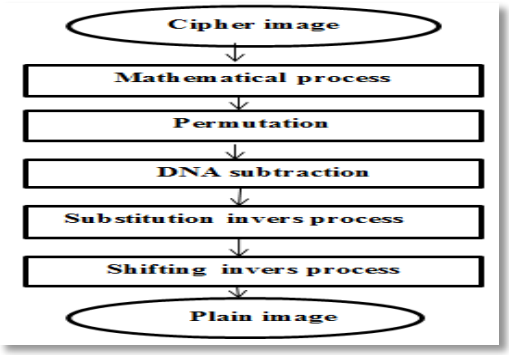

Fig. 3: diagram of proposed structure decryption.

- The steps will justify as:

Algorithm(1): Encoding Algorithm
Input: plain image , k1, k2,k3.
Output: cipher image
Begin
Step1: Read and split image to three-channel R, G, B.
Step2: For i= 1 to length R.
shift left R by k1(i)mod8 let it be $\bar{R}$ // I is an account

for keys 0,1,…no. of keys
$\bar{R}$ =shift left$(R, 9mod\ 8)$=shift left$(R, 1)$
$\bar{R}$ =shift left$(R, 6mod\ 8)$=shift left$(R, 6)$

Step3**:** For i=1 to length G.shift left G by
k2(i)mod 8 let it be $\bar{G}$ // I is account for keys 0,1,. .no .of keys
$\bar{G}$=shift left$(G, 7mod\ 8)$=shift left$(G, 7)$.
$\bar{G}$=shift left$(G, 3mod\ 8)$=shift left$(G, 3)$.

Step4**:** for i= 1 to length B
Shift left B by k3$\Big(\big(k1(i) + k2(i)\big)mod8\Big)$ let it be
$\bar{B}$ // I is account for keys 0,1,…no. of keys
$\bar{B}$= shift left$(B, (9 + 7)mod\ 8)$= shift left $(B16mod8\ 8)$ = shift left$(B, 0)$.
$\bar{B}$= shift left$(B, (6 + 3)mod\ 8)$=shift left$(B, 9mod\ 8)$ = shift left $(B, 1)$.

Step5: Conversion for all $\bar{R}$ and $\bar{G}$ to binary let it be $\bar{R}$ binary and $\bar{G}$ binary respectively
Step6:Conversionof $\bar{R}$bin and $\bar{G}$ bin to DNA codes by using table I
Step7: Replacing for G DNA with its complement by using the table II.
Step8: Convert $\bar{B}$ to Hexa and let it be $\bar{B}$ hex.
Step9: Implementation of DNA addition operation for $\bar{R}$ DNA Furthermore, X DNA depending on DNA addition table rules. //X DNA is a result of applying the algorithm to the X keys
Step10: Applying of DNA addition operation for $\bar{G}$DNA and Y DNA depending on DNA addition table rules
Step11: Applying of substitution operation by entering $\bar{B}$hex to AES s-box.
Step12: Convert the result of steps(10 and 11) to Binary
Step13: Convert the result of steps(12 and 13) to integer, then let it be($\bar{R}$ int,$\bar{G}$int,$\bar{B}$int) respectively.
Step14: Applying for permutation operation by replacing the locations of the colours that have resulted from the previous step, such instead of saving colours in ($\bar{R}$ int,$\bar{G}$int,$\bar{B}$int) form.
The replacement will be ($\bar{B}$int, $\bar{R}$int, $\bar{G}$int)
Step15**:** Apply a mathematic operation to $\bar{B}$int and $\bar{R}$ int such that $\bar{\bar{R}}$=$\big(\bar{R}\ int + (i * j)\big)mod256$,
$\bar{\bar{B}}$=$(\bar{B}int + (i * j) + 2)mod256$ //I and J are the image width and Height
Step16: Save pixel colour value as ($\bar{\bar{B}}$,$\bar{\bar{R}}$,$\bar{G}$) to provide cipher image.
End
Can explain this algorithm in flowchart encryption:

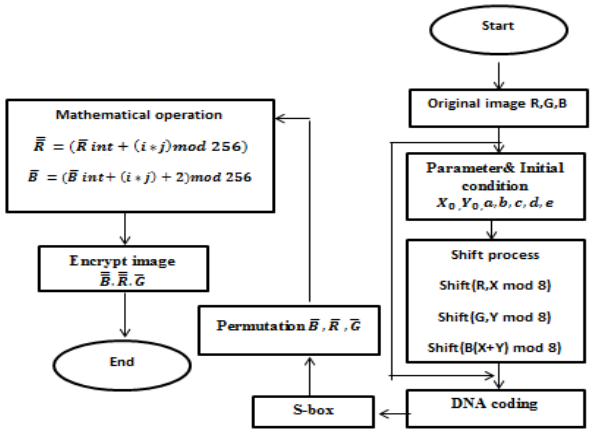

Fig. 4: flowchart encryption

Notice decryption algorithm below:

Algorithm(2): Decrypt Algorithm

Input: cipher image, k1,k2,k3.
Output: Original image
Begin
Step1: Read and split three channel R G B.
Step2: Applying a mathematic operation to R and B such that: $\bar{\bar{R}}$=$\big(\bar{R} - (i * j)\big)mod256$
$\bar{\bar{B}}$=$(\bar{B} - (i * j) - 2)mod256$
If $\bar{\bar{R}} < 0$ then $\bar{\bar{R}} = 256 + \bar{R}$
If $\bar{\bar{B}} < 0$ then $\bar{\bar{B}} = 256 + \bar{B}$
Step3: applying a permutation operation to If $\bar{R}$ If $\bar{G}$ $\bar{B}$such that: $\bar{\bar{R}}$= $\bar{G}$ $\bar{G}$=$\bar{B}$ $\bar{\bar{B}}$=$\bar{R}$
Step4: Conversion of $\bar{R}$ and $\bar{G}$ to binary and let it be $\bar{R}$bin and $\bar{G}$ bin respectively.
Step5: Convert $\bar{B}$ to Hexa; let it be $\bar{B}$ Hexa.
Step6: Convert results of step4 to DNA by using the table I.
Step7: Applying DNA subtraction operation between $\bar{R}$ DNA and X DNA depending on the table of DNA subtraction rules, then let it be $\bar{R}$ sub //X DNA resulted from applying algorithm 3.
To x keys
Step8: Implementation of DNA subtraction operation between $\bar{G}$ DNA and YDNA depending on the table of DNA subtraction rules,
then let it be $\bar{G}$ sub //YDNA resulted from applying algorithm 3
To Y keys.
Step9: Implementation a subtraction operation for the result of step5($\bar{B}$hex) by entering it to AES S-box let it be $\bar{B}$s-box
Step10: Replacing $\bar{G}$ sub-codes with its complement by using the table II. Let result be $\bar{G}$ comp.
Step11: For i= 1 to length $\bar{R}$.
Shift right $\bar{R}$ sub by k1 (i)mod 8. //I is a count for keys 0… no. of keys
$\bar{R}$ 5=shift right($\bar{R}$ sub,9 mod 8) = shift right($\bar{R}$ sub,1)
$\bar{R}$ 5 become $\bar{R}$ 5 =shift right($\bar{R}$ sub,6 mod 8) = shift right ($\bar{R}$ sub,6).
Step12: For i= 1 to length $\bar{G}$.

Shift right $\bar{G}$comp by k2(i)mod 8. // I is a count for keys 0… no.
of keys
$\bar{G}$ 5=shift right($\bar{G}$comp,7mod8)= shift right($\bar{G}$comp,7)
$\bar{G}$5=shift right($\bar{G}$comp,3mod8)= shift right($\bar{G}$comp,3)
Step13: For i= 1 to length $\bar{B}$.Shift right $\bar{B}$s-box by k3 (k1(i)+k2(i)mod 8). // I is a count for keys 0… no. of key
$\bar{B}$5=shift right($\bar{B}$s-box,(9+7)mod8)=shift right($\bar{B}$s-box,0)
$\bar{B}$5=shift right($\bar{B}$s-box,(6+3)mod8)=shift right($\bar{B}$s-box,1)
Step14:Convert the result of steps(12,13 and 14) to integer and let it be (Rint, Gint, Bint)
Step15: Save the value of step15 into the image to retrieve the original image
End
And can explain this algorithm in flowchart decryption:

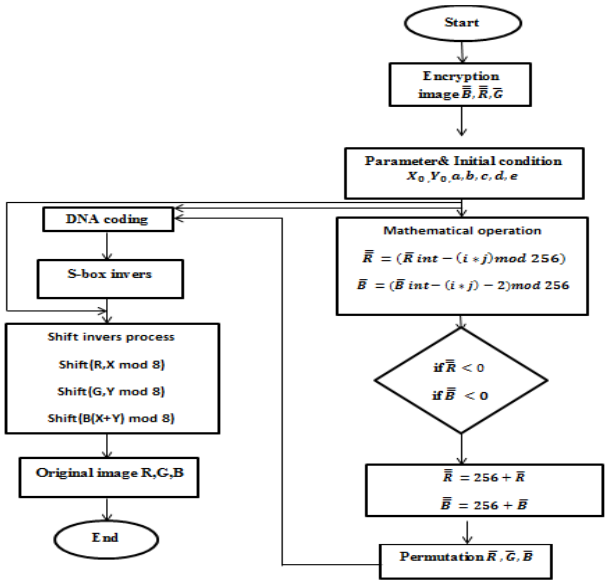

Fig. 5: flowchart decryption

- The steps will justify as:

Algorithm(3): DNA Coding Algorithm
Input: Red, Green.
Output: DNA Red, DNA Green.
Begin
Step1: Read byte for red.
Step2: Split 2-bits for each byte.
Step3: Replace each two-bit from the above step to DNA char based on the table I.
Step4: Repeat to step 2, and continue for each (Red, Green)
End

III. Experimental Results Of Statistical And Security Analysis

A. Application System

Colour channels encrypt based on DNA and chaotic map. Initially, many conditions and parameters value are needed as (a=4, b=1.1, c=4.4, d=0.1, e=8) for the chaotic map after that; two secret keys are selected secret key1 and secret key2. Generated the 5000 key 4998 key are used half of it was classified as the first key 2499 and the second half of the second key 2499. In the structure used keys in the image. The image consists of the number of pixels if the number of pixels is more than the number of keys, the keys will return to the beginning. Each secret key enters the different channel from colours; each secret key gets 4 characters as DNA (T, C, G, A).

Furthermore, each channel colour (R, G, B) gave 4 characters. A, T, C, and G. So on (R, G, B) the interface requires information from the main image such as statistical measurements (SIM, SNR, NAE, EQ, SC, NC, MAE, PSNR, MD, MSE, and AD) and the amount of time consumed in the process of encoding and decoding, can applying on images bmp and jpeg.

B. Performance Analysis

To encode the original image, there is a set of measurements that will be applied to these images of different sizes to obtain a coded image collection depending on DNA computing and chaotic theory. The process is sensitive due to any change in the parameter and condition value. Any change in the values(initial value x=1.2, y=0.8) will lead to a large noise, and the keys will vary and thus show different results affect each structure. In the structure has been achieved confusion in the S-box and diffusion in the shift. The statistical test of the equality encryption image.

- Original image and cipher image (SIM, SNR, NAE, EQ, SC, NC, MAE, PSNR, MD, MSE, and AD)
- Both have been achieved diffusion and confusion at different stages from the structure. Presence in any structure will open the bond between the pixels and increase distortion; this, in turn, strengthened the algorithm's strength.
- A process was performed shifting because any pixels do have a process shifting new pixels appear, the old pixels are different from the new pixels that emerged after the process of shifting, so the disengagement between the pixels increased diffusion.
- Hexadecimal process because S-box do not deal with binary because it is from zero to F in the column and from zero to F in row
- S-box to switch the value of another value place until we increase confusion.
- Coding process to prepare them for operations addition, subtraction and complement. Moreover, we used DNA because it works on the separation of pixels; DNA is not like conventional processes.
- Permutation process to exchange pixel locations and thus decompose them to increase diffusion. There is a set of algorithms used permutation as heap's algorithm. To increase the broken bond between colour values.
- Mathematics process to produce a new value instead of the old value and the subsequent increase in confusion.

Can be applying measurements on images e.g lena, baboon:

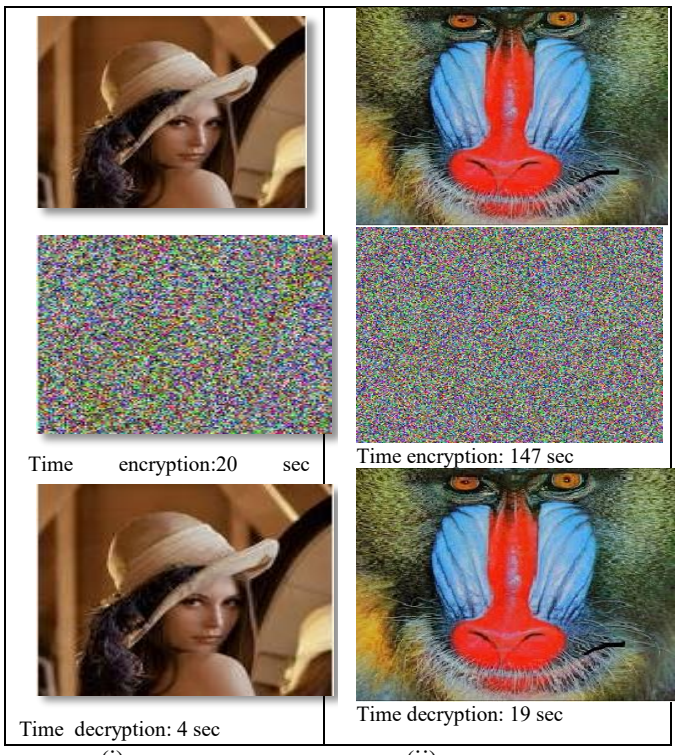

Fig. 6:(i)Lena jpeg, (ii)Baboon bmp

TABLE III: TIME CONSUMPTION IN IMAGES WITH RELATED WORK (ENCRYPTION AND DECRYPTION)

methods	Images	Time encryption sec	Time decryption sec
S.Ali and A. Abas	Lake	0.2141 sec	0.2042 sec
	Baboon	0.4825 sec	0.3821 sec
proposal	Lena	20 sec	4 sec
	Baboon	174 sec	19 sec

TABLE IV : TESTED UACI IN THE ENCRYPTED IMAGE WITH RELATED WORK

UACI / methods	Image 1	Image 2
S.Ali and A. Abas	33.5787	33.7895
proposal	32.5103	33.2269

TABLE V : I) RESULT OF STATISTICAL TEST FOR PROPOSAL (BETWEEN PLAIN AND CIPHER IMAGE)

(i) Lena jpeg, Size (146X 146)			
PSNR	0.001530749	NAE	0.484353212
MSE	31442	SC	2.529235767
AD	31442	SNR	0.881514998
MD	255	SIM	0.692599417
NC	0.484353212	EQ	20902.71093
MAE	31442		

TABLE V : II) RESULT OF STATISTICAL TEST FOR PROPOSAL (BETWEEN PLAIN AND CIPHER IMAGE)

(ii) Baboon bmp, Size (256X256)			
PSNR	0.001907920	NAE	0.385533894
MSE	25226	SC	1.739654254
AD	25226	SNR	1.734744990
MD	253	SIM	0.749078034
NC	0.385533894	EQ	58087.10156
MAE	25226		

TABLE VI : RESULT OF STATISTICAL TEST FOR PROPOSAL (BETWEEN PLAIN AND CIPHER IMAGE)

UACI / methods	Image 1	Image 2
S.Ali and A. Abas	33.5787	33.7895
proposal	32.5103	33.2269

C.Time, complexity and efficiency of the proposed structure

In this paper, one will try to find out some side of evaluation estimate speed, complexity and efficiency. The abundance of processes in this algorithm led to the efficiency of performance is a simple algorithm that led to the speed of implementation and applied this algorithm many images, measured KB such 192 KB and 4.33 KB. With different extensions, JPEG and BMP. To lossless image and higher resolution. The encryption and decryption run time is calculated for each image. This structural complexity has made confusion and diffusion.

V.Conclusion

In this proposal, DNA computing and chaos system was encrypted to obtain a high level of security and increased complexity against attacks. This algorithm achieved diffusion and confusion through processes shift, hexadecimal, S-box, DNA addition, permutation and mathematics operation. Many images were used in different sizes and extensions. All encoded images have high encryption rates based on the standard encryption quality (EQ) between original images and encrypted images. They were evaluated through tests (PSNR, MSE, MAE, AD, MD, NC, NAE, SIM, SC, SNR) between the original and retrieved image and between the original image and the encoder and the results were good where the amount of error (MSE) between the original image and the image after decoding is zero leading to that value (PSNR) is a value that can be converted to 100% or has no end between the original and retrieved images.UACI everything close to zero was better the proposed algorithm has good results, has a good level of complexity, and consumes an appropriate time during implementation.

REFERENCE

[1] H.A Kruger., and W.D Kearney., " A Prototype for Assessing Information Security Awareness" Elsevier, computers & security, Vol 2 5, page 2 8 9 – 296. 2 0 0 6.
[2] P. Shamala., R.Ahmed., A.Hussein.,and S. Bin., "Collective Information Structure model for Information Security Risk Assessment (ISRA) "Journal of Systems and Information Technology, Vol. 17, page 193-219, 17 No. 2, 2015.
[3] P Sugathan., "DNA Computing", M.Sc. Thesis, Cochin University of Science and Technology, Department of Computer Science, CUSAT 2010.
[4] Wikipedia ., " Chaos Theory " 6 April 2019.
[5] Q. Zhang., L. Guo., and X. wei.," Image Encryption Using DNA addition Combining with Chaotic map", Elsevier, Mathematical and Computer Modelling Vol 52, page 2028_2035, 2010

[6] S. Ali., and A. Abas., "Image Encryption Depend on DNA Encoding and A Novel Chaotic System " Journal of Engineering And Applied Sciences vol13, issue 22, page 9705-9714,2018.

[7] Z. Mohamed., "Image Encryption Using DNA Addition" M.Sc. Thesis, University of Technology,2017

[8] P. Kaler., " Study of Grayscale image in Image processing ", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Vol: 4 Issue: 11, IJRITCC, November 2016.

[9] R..Terec., M.Vaida., L.Alboaie and L.Chiorean..," DNA Security using Symmetric and Asymmetric Cryptography " January 2011, Genetics Home Reference .U.S. National Library of Medicine, 2011. http://ghr.nlm.nih.gov/handbook/basics/dna.

[10] S. Sarkar., "Decoding "Coding": Information and DNA ", University of California Press, journals Digital Publishing, Vol. 46, p.p857-864 , No. 11, Dec., 1996.

[11] K. Chao., " Basic Concepts of DNA, Proteins, Genes", National Taiwan University, Taipei, Taiwan 106, October 2, 2006.

[12] M..H.F Wilkinson., "Nonlinear Dynamics, Chaos- theory, and the "Sciences of Complexity": Their Relevance to the Study of the Interaction between Host and HERBORN UNIVERSITY SEMINAR MONOGRAPH INST MICROECOLOGY & BIOCHEM Germany,Vol 10, pages111-130, ISBN 3-923022-20-4,NO 20, 1997.

[13] K. Ali., and S Abdulhadi., " A Parallel Programming for Robust Chaotic Map Generation Based on Two and Dimensional Equation System" Journal of engineering Applied Sciences vol 14,isuee11:page 3741-3745,2019.

[14] S. B. Sadkhan, and B. S. Yyaseen, " A DNA-Sticker Algorithm for Cryptanalysis LFSRs and NLFBSRs based Stream cipher ", 2018 International Conference on Advanced Science and Engineering (ICOASE)

[15] A. M. Raheema ; S. B. Sadkhan; and S. M. Abdul Sattar, "Performance Comparison of Hybrid Chaotic Maps Based on Speech Scrambling for OFDM Techniques ", 2018 Third Scientific Conference of Electrical Engineering (SCEE)