Color Image Encryption using Chaotic Maps, Triangular Scrambling, with DNA Sequences

Haider M. Al-Mashhadi- MIEEE
Information Systems Dept., College of Computer Science and Information Technology,
Basrah, Iraq.
mashhad01@gmail.com

Iman Q. Abduljaleel
Computer Science Dept., College of Computer Science and Information Technology,
Basrah, Iraq.
emankais@yahoo.com

***Abstract*— Applying security to the transmitted image is very important issues, because the transmission channel is open and can be compromised by attackers. To secure this channel from the eavesdropping attack, man in the middle attack, and so on. A new hybrid encryption image mechanism that utilize triangular scrambling, DNA encoding and chaotic map is implemented. The scheme takes a master key with a length of 320 bit, and produces a group of sub-keys with two length (32 and 128 bit) to encrypt the blocks of images, then a new triangular scrambling method is used to increase the security of the image. Many experiments are implemented using several different images. The analysis results for these experiments show that the security obtained on by using the proposed method is very suitable for securing the transmitted images. The current work has been compared with other works and the result of comparison shows that the current work is very strong against attacks.**

Keywords— Chaos; DNA encoding; Image encryption; triangular scrambling.

I. INTRODUCTION

The cryptography is very important field that provides a security services for data transferred on computer networks. By converts the plain data into a form that cannot be recognized.

There are many applications in computer networks that use images. They transmit secret images on public network.

There are distinct properties between image and text, such as big data space and intense interconnection within pixels make some classic encryption schemes so inconvenient for encryption of digital images [1, 2]. Therefore, some motivating and favorable schemes, such as chaotic maps [1, 2] and DNA [3, 4, 5] have been exercised in the digital image encryption.

Here in this encryption method we present an encryption scheme that contains a key generator which depending on the dynamic manner of chaotic map to generate PRNG keys, and in the next stage we carry out a new color image scrambling named the scrambling by triangle segmentation then the final stage using DNA sequences with keys generation above to obtain the encrypted image. This technique provides high security with less time and computation comparing with other image encryption methods depending on image encryption analysis tests.

The research is organized as follows. In Section 2, a review for some theories behind the suggested algorithm. The basic concepts of the primitive methods used in security scheme are characterized in section 3.The description and discussion of the suggested encryption algorithm is presented in section 4. In section 5, the experiments results and analysis are described in details. In section 6, the conclusions are discussed.

II. RELATED WORK

There are many studies in this field, this section summaries some of them. There are several papers that utilize chaos maps in encryption algorithms. Abdullah et al. [6] in this research, uses Discrete Cosine Transform (DCT) with Henon map to get the chaos encryption method. In [7] a new digital image shuffling scheme is proposed, by replacing the spatial location of the pixel with its value using logistic map decomposition and recombination of pixel values. Ramadan et al. [8] introduce an image encryption scheme by utilizing pair of chaotic maps. The first scheme is Chepyshev chaotic to make the scrambling of the pixels. The scrambling pixels are submitted to the diffusion stage using the modified Quadratic map in an encryption mechanism. Alshibani et al. [9] introduce an image encryption scheme depending on Tinkerbell map; Zaslavsky Map and Arnold Transform to generate keys that used in the permutation and substitution stages.Wei et al. [10] develop an image encryption mechanism depending on Deoxyribonucleic-acid (DNA) and chaotic combination, with Hamming distance to produce the cryptographic keys. Qiang Zhang et al. [11] presented an algorithm depending on DNA sequence addition process with chaos to encrypt images. First, encoding the image by using DNA sequence matrix, second, segmenting the DNA sequence matrix into segments and carry out the adding process among these segments, then using two Logistic maps to perform complement operation to the DNA sequence. In the end, decode the DNA sequence matrix produced from the last stage to get the encrypted image.

978-1-5386-2955-0/17/$31.00 ©2017 IEEE

III. BASIC CONCEPTS

A. Chaotic map

There are some dynamic properties that can be utilized in chaotic map, such as ergodicity, pseudo-randomness and unpredictable behavior.

This paper uses the skew Tent Map [12, 13] in the key generation procedure. It can be defined as [14]:

$$F(a,b_i)=\begin{cases} b_i/a & b_i = [0,a) \\ (1-b_i)/(1-a) & b_i =(a,1] \end{cases} \quad (1)$$

Where, (a and bi) are system variable and initial state of the map respectively. The transformation is non-invertible on itself interval and the system variable that determines the peak of the tent in the interval [0, 1] is (a) variable. By using iterating F(a, b), we can obtain on the values of chaotic sequence that are between [0, 1].

B. DNA cryptography

Deoxyribonucleic Acid or DNA is an entity that storing information of all life kinds. Every living creature have DNA that keeps the specific features of this creature, giving it the natural features like color, shape, sight, brain etc. Since DNA has a huge information capacity, it can be used to store a vast quantity of information. This essential feature of DNA led to the developing a field called DNA computing.

DNA computing is the domain of computer science that performs the computation depending on DNA logic instead the classical bit logic. In classical computers, there are only two digits i.e. the binary 0 and 1, Whereas DNA computers are depending on the DNA word logic. Adleman [15] carried out the first experiment on DNA computing in 1994. The information is stored in DNA words that consist of four characters. DNA characters are named nucleotides in the biological sciences. The four types of Nucleotides: A (Adenine), C (Cytosine), G (Guanine) and T (Thymine). A four letter sequence of the nucleotides can be expressed a DNA word. Where the binary sequence 01 is replaced by A and its complementary 10 is obviously replaced by T similarly 00 is replaced by Cytosine(C) and 11 is replaced by Guanine, as shown in table I.

TABLE I. DNA ENCODING

Binary Value	Replaced With
00	C (Cytosine)
01	A (Adenine)
10	T (Thymine)
11	G (Guanine)

DNA cryptography is a subject of study about how to use DNA as an information carrier and it utilize modern biotechnology as a mean to modulate ciphertext into plaintext.

IV. THE ALGORITHM

The algorithm consists of many phases as shown in Figure (1).

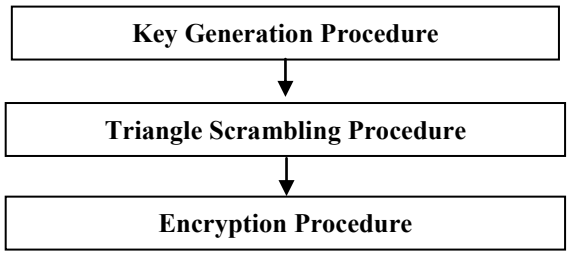


Fig. 1. Encryption algorithm Flowchart.

Phase (1): Key Generation

1. Enter the Master Key MK with length 320 bit (40 Byte).
2. Divide the MK into 5 Sub-Keys SK with length 64 bit.
3. Then generate 5 keys from the Complement of SK. Now we have 10 keys of length 64 bit for each
4. Generate 56 keys with length 64 bit using Chaotic Tent Map.
5. For each MK, SK and Chaotic Keys do the following:
6. For i=1 to 5

If mod(k,2) =0
Key_i=concat(SK_i, $Chao_i$, $compKey_i$, $Chao_{i+1}$)
Else
Key_i=concat($compKey_i$, $Chao_i$, $Chao_{i+1}$, Sk_i)
End; End;

Where SK is the SubKey, compKey is the complement of SK, $Chao_i$ and $Chao_{i+1}$ is the chaotic keys from the Tent Map equation. So in every step the keys are merges to generate 140 keys in every cycle.

The algorithm operates on two modes, 32 and 128 block length. So as in the key generation algorithm, it generates a number of keys equal to the number of image blocks that can be equal to 32 and 128 bit length for each block.

Phase (2): New Triangle Scrambling Procedure

1. Read color image (256*256 Pixels).
2. Split the input image into R, G, B levels.
3. Divide each level into 16 sub-blocks with length 64*64 pixel blocks.
4. Using Triangular Scrambling the proposed Algorithm, figure 2(a) and 2(b), to divide each sub block into 5 vectors with different size as:

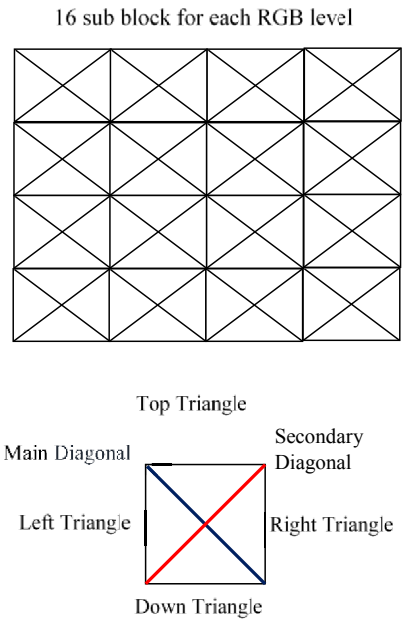
Vector1: have 128 pixels from main and second diagonal.
Vector2: 992 pixels of the top triangle.
Vector3: 992 pixels of the down triangle.
Vector4: 992 pixels of the left triangle.
Vector5: 992 pixels of the right triangle.

5. Convert each vector into two dimension Matrix as:

Vector1: Matrix of 4*32 pixels.
Vector2: Matrix of 31*32 pixels.
Vector3: Matrix of 31*32 pixels.

Vector4: Matrix of 31*32 pixels.
Vector5: Matrix of 31*32 pixels.

The length of each pixel block and the key generated has the same length, (32 bits). If we use the second mode (128 bits) then the length of pixel block and the key generated will be 128 bit.



(b)
Fig. 2. Triangular Scrambling (a): dividing the image into blocks, (b): the components of each block.

Phase (3): Encryption Procedure

1. Key generation generates keys to encrypt the blocks of image pixels with length of 32 or 128 bit.
2. After implement the Triangular Scrambling Proposed Algorithm to get image matrices.
3. Convert each block of image and key to DNA sequences.
4. Xor the DNA sequence of image with DNA sequence of key.
5. Return the result into normal value of RGB to resemble encryption image.

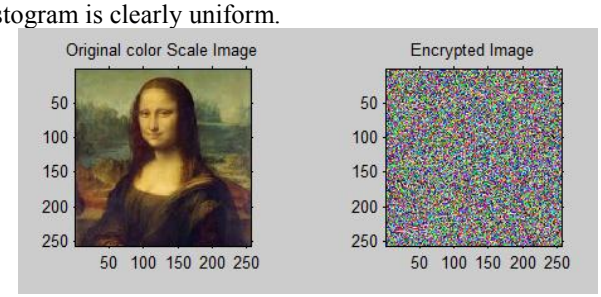
V. Experimental Results

To test the efficiency of the proposed mechanism, many experiments have been implemented using six [256*256] color images with different security analysis methods.

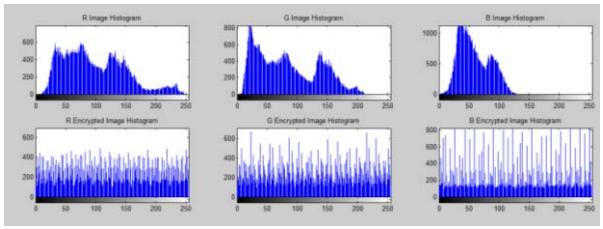
A. Histogram Analysis

To show the frequency allocation of pixel weights in an image. The resulting histogram from the ciphered image must be very uniformed to withstand against the statistical attack, the attackers may return sufficient information of the plain image [16].

Figure 3(a), 4(b) shows the compared histogram between plain image and cipher image of "Mona Liza". The resulting histogram is clearly uniform.



(a)



(b)

Fig. 3. (a) Mona Liza image, original and cipher, (b) Histogram for original image.

B. Entropy Analysis

The significant property that explains the randomness of information that can be presented by Shannon's equation [17],

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i). \qquad (2)$$

where $p(x_i)$ is the probability of r. n is the number of bits to represent x_i. Based on the entropy formula the ideal value of entropy for a scrambled encrypted image is 8. Table (2) shows the experimental results of the security analysis with different images and tests. From Table II, the values of entropy for all images are very close to the typical value 8. From this result we can conclude that the encrypted image have a very good randomness and have it ability to resists the statistical analysis attacks.

TABLE II. THE RESULTS OF ENTROPY TEST.

Color image	32 bit sub-key length		128 bit sub-key length	
	Entropy original image	entropy encrypted image	entropy image	entropy encrypted image
Monkey	7.59767	7.90062	7.59767	7.89655
Lena	7.01601	7.94368	7.01601	7.94085
Pepper	7.16815	7.95412	7.16815	7.95264
Mona Liza	6.56262	7.82914	6.56262	7.82243
Flower	7.40305	7.94235	7.40305	7.94246
Baby	7.78638	7.90529	7.78638	7.90176

C. PSNR Analysis

PSNR usually uses to compute the difference ratio between the actual image and the cipher image depending on the MSE that can be used to compute the different mean square error ratio of plain image and cipher image [18]. MSE and PSNR are clarifying by equations (3) and (4).

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[x(m,n) - \hat{x}(m,n)]^2 \quad (3)$$

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (4)$$

PSNR is measure in decibel (dB), MN is the height and width of the image, x(m,n) is the source image, x'(m,n) is the reconstructed image. Table III and table IV, shows the results of MSE and PSNR tests. The PSNR values between the original image and the reconstructed image denoted that the two image is almost identical. Whereas the PSNR values between the original image and cipher image are very low that means the encrypted image does not similar to original image, and it very strong against the attacks.

TABLE III. THE RESULTS OF MSE AND PSNR TESTS BETWEEN THE ORIGINAL IMAGE AND RECONSTRUCTED IMAGE.

Color image	32 bit sub-key length		128 bit sub-key length	
	MSE	PSNR	MSE	PSNR
Monkey	0	INF	0	INF
Lena	0	INF	0	INF
Pepper	0	INF	0	INF
Mona Li-za	0	INF	0	INF
Flower	0	INF	0	INF
Baby	0	INF	0	INF

TABLE IV. THE RESULTS OF MSE AND PSNR TESTS BETWEEN THE ORIGINAL IMAGE AND THE CIPHERIMAGE.

Color Image	32 bit sub-key Length		128 bit sub-key Length	
	MSE	PSNR	MSE	PSNR
Monkey	0	53.7359	0	53.7359
Lena	0	53.8528	0	53.8528
Pepper	0	54.0027	0	54.0027
Mona Liza	0	56.5335	0	56.5335
Flower	0	54.9365	0	54.9365
Baby	0	50.7034	0	50.7034

D. Correlation Analysis

Correlation is used to measure the similarity between the original image and the cipher image. The correlation can be defined as in equation (5) [19].

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad (5)$$

Figure (4) shows the correlation on cipher image.

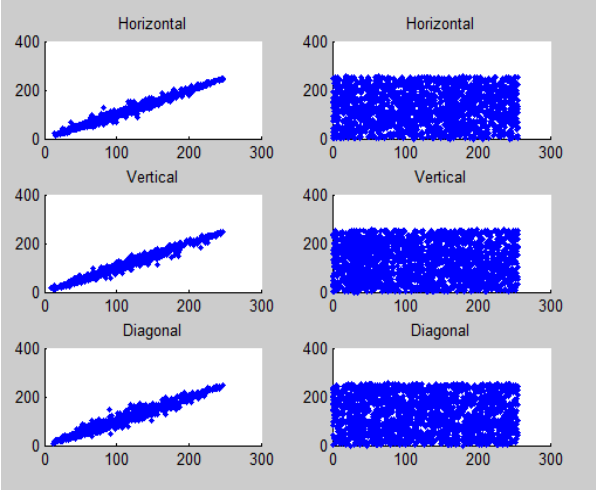


FIGURE (4), THE CORRELATION OF CIPHER IMAGE.

Table V, and table VI, shows the result of the correlation test for six original and cipher images using 32 bit sub-key and 128 bit sub-keys. The correlation values among the original pixels are very high, whereas the correlation values among the cipher images are very low values that indicates the neighbor pixels have been highly irrelevant after encryption operation.

TABLE V. THE RESULT OF CORRELATION VALUES FOR 32 BIT SUB-KEY LENGTH.

Chosen image		Adjust pixels in correlation analysis		
Image	Image type	Diagonal correlation	Vertical cor-relation	Horizontal correlation
Monkey	Original image	0.9437	0.9635	0.9694
	Encrypted image	0.00189	0.00064	0.00544
Lena	Original image	0.9212	0.9720	0.9460
	Encrypted image	0.00276	-0.00564	0.00124
Pepper	Original image	0.9478	0.9773	0.9715
	Encrypted image	0.00050	0.00108	0.00850
Mona Lisa	Original image	0.9866	0.9927	0.9932
	Encrypted image	0.00141	0.00277	0.00962
Flowers	Original image	0.9636	0.9868	0.9736
	Encrypted image	-0.00146	0.01304	0.01911
Baby	Original image	0.9567	0.9741	0.9727
	Encrypted image	0.01457	0.02853	0.04446

TABLE VI. THE RESULT OF CORRELATION VALUES FOR 128 BIT SUB-KEY LENGTH.

Chosen image		Adjust pixels in correlation analysis		
image	Image type	diagonal correlation	vertical correlation	Horizontal correlation
Monkey	Original image	0.9437	0.9635	0.9694
	Encrypted image	0.0025	-0.0008	0.00153
Lena	Original image	0.9212	0.9720	0.9460
	Encrypted image	0.00803	0.00023	-0.00157
Pepper	Original image	0.9478	0.9773	0.9715
	Encrypted image	-0.0016	0.00152	0.00405
Mona Liza	Original image	0.9866	0.9927	0.9932
	Encrypted image	-0.00557	-0.00240	0.02157
Flowers	Original image	0.9636	0.9868	0.9736
	Encrypted image	0.003569	0.00336	0.02119
Baby	Original image	0.9567	0.9741	0.9727
	Encrypted image	0.01777	0.026511	0.05015

E. Differential Attack Analysis

The encryption algorithm should be susceptible to any simple change in the original image [19, 20, 21]. We can measure this feature by using two criteria which are called NPCR (number of pixels change rate) and UACI (unified average changing intensity) to analyze the strength of the encrypted method against the differential attack.

Consider that C_1 is a ciphertext image without any change in the original image; C_2 is the ciphertext image after one pixel in the original image has been changed. The NPCR can be defined as:

$$NPCR= \sum(D(i,j)/T*100\%) \quad (6)$$

$$UACI=(1/T)[\sum(|C1(i,j)-C2(i,j)|/255)*100\% \quad (7)$$

Where D(i,j) is the pixel value in the position (i,j), and can be defined as:

D(i,j)= 0 if C1(i,j) is equal to C2(i,j) or
D(i,j)= 1 if C1(i,j) is not equal to C2(i,j)

T denotes to the total number of pixels in the ciphertext i.e (W*H) width and height of the image,

Table VII, shows the result of these two criteria for 32 bit and 128 bit experiments.

TABLE VII. NPCR AND UACI RESULTS TEST.

Color image	32 bit sub-key length		128 bit sub-key length	
	NPCR	UACI	NPCR	UACI
Monkey	0.996175	0.289361	0.996312	0.289074
Lena	0.996312	0.305125	0.996109	0.304277
Pepper	0.996012	0.281469	0.996231	0.320882
Mona Liza	0.996378	0.320056	0.995961	0.320398
Flower	0.996185	0.336763	0.996175	0.336510
Baby	0.996398	0.371159	0.996526	0.371342

Table VIII shows the comparison between the current work and the similar works in Refs. [22- 24]. The results depending on Lena image. From the comparison the value of correlation for the proposed algorithm is very close to zero like the other works, that can be conclude is very strong against the attacks. The NPCR and UACI results show that the performance of the proposed algorithm is better or equal to the schemes in Refs. [22- 24].

TABLE VIII. THE COMPARISON OF CORRELATION COEFFICIENTS.

Algorithm	Horizontal Direction	Vertical Direction	Diagonal Direction
Original Image	0.9460	0.9720	0.9212
Proposed Algorithm	0.0124	-0.00564	0.0276
Ref [22]	0.0004	0.0021	-0.0038
Ref [23]	0.0062	0.0052	0.0069
Ref [24]	0.0020	-0.0007	-0.0014

TABLE IX. THE COMPARISON OF NPCR & UACI.

Algorithm	NPCR	UACI
Proposed Algorithm	99.63	30.51
Ref [22]	99.60	28.13
Ref [23]	99.21	33.28
Ref [24]	99.65	33.43

VI. CONCLUSIONS

Applying security to the transmitted image is very important issue, because the transmission channel is opened and can be compromised by attackers. To secure this channel, an image encryption algorithm is implemented. The algorithm is implemented a combination of Chaotic maps and DNA sequence with triangular scrambling to increase the strong of the method. The algorithm using a new key generator by enters the master key with length of 320 bit (40) Byte then using the chaotic map to generate the sub keys with two keys length types (32 bit and 128 bit) so the algorithm can be operates using 32 bit or 128 bit modes. The proposed scheme uses a new triangular scrambled method by divides the image into 6 matrices of interest and then utilizing the DNA sequence to enhance the scrambled and encryption mechanism. Several statistical tests have been used like (Histogram, Entropy, MSE, PSNR, Correlations, NPCR and UACI). The results show that the proposed mechanism gave an optimal analysis result that can resist different attacks. The current work has been compared with other works and the result of comparison shows that the current work is very strong against attacks and have a very good degree of security that can be using to send the images through the insecure channels.

REFERENCES

[1] Li, S.; Chen, G.; Zheng, X. "Chaos-based encryption for digital images and videos," In *Multimedia Security Handbook*; Furht, B., Kirovski, D., Eds.; CRC Press: Boca Raton, FL, USA, 2004; pp. 133–167.

[2] Mazloom, S.; Eftekhari-Moghadam, A.M. "Color image encryption based on coupled nonlinear chaotic map," *Chaos Soliton Fract.* 2009, *42*, 1745–1754.

[3] Adleman, "Molecular computation of solutions of combinatiorial problems," Science 266 (1994) 1021–1024.

[4] A. Gehani, T.H. LaBean, J.H. Reif, "DNA-based cryptography," DIMACS series in discrete mathematics, Theoretical Computer Science 54 (2000) 233–249.

[5] Qiang Zhang, Lili Liu, Xiaopeng Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," Computers and electrical engineering volume 38 issue 5 (2012) 1240-1248.

[6] Abdullah M. Awad, Rehab F. Hassan, Ali M. Sagheer, "Chaos Image Encryption based on DCT Transforms and Henon Map," International Journal of Computer Applications, Volume 127 – No.11, October 2015.

[7] Dong Wang, Chin-Chen Chang, Yining Liu, Guoxiang Song, Yunbo Liu, " Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values," International Journal of Network Security, Vol.17, No.3, PP.322-327, May 2015.

[8] Noha Ramadan, Hossam Eldin H. Ahmed, Said E. Elkhamy, Fathi E. Abd El-Samie, "Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map," American Journal of Signal Processing, Vol. 6 No. 1, PP 1-13, 2016.

[9] Dina Riadh Alshibani, Rasha Shaker Ibrahim, "Implementation of Gray Image Encryption using MultiLevel of Permutation and Substitution," International Journal of Applied Information Systems (IJAIS), Vol. 10, No.1, November 2015.

[10] Wei X., Guo L., Zhang Q., Zhang J., and Lian S. "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", The Journal of Systems and Software, Vol. 85, No. 2, PP 290-299, 2012.

[11] Qiang Zhang , Ling Guo, Xiaopeng Wei, "Image encryption using DNA addition combining with chaotic maps," Mathematical and Computer Modelling, Vol. 52, PP. 2028–2035, 2010.

[12] Haider M. Al-Mashhadi, Hala B. Abdul-Wahab, Rehab F. Hassan, "Data Security Protocol for Wireless Sensor Network using Chaotic Map," International Journal of Computer Science and Information Security, Vol. 13, No. 8, August 2015.

[13] Stojanovski T., Pihl J., and Kocarev L., "Chaos-based random number generators - Part II: Practical realization," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, no. 3, pp. 382-385, 2001.

[14] Zhang, G.J., Liu, Q. "A novel image encryption method based on total shuffling scheme," Optics Communications vol. 284, pp. 2775–2780, 2011.

[15] Adleman, "Molecular computation of solutions of combinational problems," Science, 266, pp. 1021-1024, 1994.

[16] Behnia, S.; Akhshani, A.; Ahadpour, S.; Mahmodi, H.; Akhavan, A. "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Phys. Lett. A*, *366*, pp: 391–396, 2007.

[17] Shannon, C.E. "Communication theory of secrecy systems," Bell Syst. Tech. J., 28, 656–715, 1949.

[18] Thakur N, Devi S, "A new method for color image quality assessment" International Journal Computer Application. Vol. 15, No.2, pp: 10–17, 2011.

[19] Haider M. Al-Mashhadi, "Quality Assessment for Image Encryption Techniques using Fuzzy Logic System," International Journal of Computer Applications, Vol. 157, No 5, January 2017.

[20] Qiang Zhang ∗, Ling Guo, Xiaopeng Wei, "Image encryption using DNA addition combining with chaotic maps," Mathematical and Computer Modelling, vol. 52. PP: 2028–2035, 2010.

[21] Y. Wang, K-W. Wong, X. Liao, G. Chen, "A new chaos-based fast image encryption algorithm," Applied Soft Computing, vol. 11 (1), PP: 514-522, 2011.

[22] Liu HJ, Wang XY. A. kadir, "Image encryption using DNA complementary rule and chaotic maps," ApplSoftComput 2012; 12 (5):1457–66.

[23] Wei XP, Guo L, Zhang Q, Zhang JX, Lian. SG, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," J Syst Softw 2012; 85(2):290–9.

[24] Xing-Yuan Wang , Ying-Qian Zhang, Xue-Mei Bao "A novel chaotic image encryption scheme using DNA sequence operations," Optics and Lasers in Engineering73(2015), pp. 53–61, 2015.