Journal of Engineering and Applied Sciences 13 (22): 9705-9714, 2018
ISSN: 1816-949X

Image Encryption Depend on DNA Encoding and a Novel Choatic System

Sadiq A. Mehdi and Anwar Abbas Hattab
Department of Computer Science, Al-Mustansiriyah University, Baghdad, Iraq

Abstract: This study proposes a new algorithm of color image encryption depend on Deoxyribo Nucleic Acid (DNA) and a novel 3-dimentianal chaotic system. The chaotic system was tested by calculating the Lyapunov exponents where show that it has one positive value which means that it is chaotic and the system's sensitivity to the initial values has been proved. By using operation XOR between the random values got from the novel chaotic method and DNA encoding for plain image. The same operation will be done by chaotic sequences. So that, we determine some operation rules which can be utilized between plain image and chaotic sequences. The proposed algorithm has been experimentally evaluated where it has large key space and the encryption algorithm has high resistance to statistical attacks where histogram test for encrypted image is completely uniform and correlation values for encrypted image is small and about to zero while the entropy values for encrypted image are close to optimal value, the encryption algorithm also has high resistance to differential attack where the values for Number of Changing Pixel Rate (NPCR) and Unified Averaged Changed Intensity (UACI) is pass the all theoretical intervals and in addition to that the encryption algorithm has good sensitivity to key change and the time image encryption/decryption was very small, all these improves the security and can resist most popular attacks which appears that proposed algorithm has a perfect security.

Key words: A novel 3D chaotic system, DNA, encryption image, Lyapunov exponents, theoretical intervals, plain image

INTRODUCTION

With the growth of network, huge data such as audio files, video files and images can easily be transmitted to the internet. Therefore, it is necessary to protect them from impermissible access. One way of keeping secret data transmission secure is encryption. Encryption is the knowledge of changing message body or information by the help of a code key and an encryption algorithm, so that, only the person who knows keys and algorithm can extract the original information from encryption information and a person who does not know one or both cannot have access to them. Chaotic sequences are pseudo-random sequences generated by chaotic maps, chaotic maps structures are exceptionally difficult and complicated to analysis and forecast, so, the security of encryption systems can enhance depend on chaotic systems, thus, some scientists suggested using chaotic map for image encryption algorithms (Sathishkumar *et al*., 2011). Recently, several algorithms supported chaotic systems are suggested (Sathishkumar *et al*., 2011, Shekhar *et al*., 2012) and have found intensive interest by researchers. owing to the chronic characteristics of chaotic systems, just like the sensitivity of initial conditions and randomness, the chaotic systems based totally image coding methodology shows to be acceptable for more-security coding. Provision map having of fine chaotic properties, it's used as a pseudo-random generator. every these maps have big key house are reaching to be making the image away stronger (Shekhar *et al*., 2012). One of the latest and most created image coding algorithms that supported DNA writing (Zhang *et al*., 2013). As a proposal for a sturdy image coding rule, throughout this study an innovative technique of DNA sequence, chaotic system has been developed. Inside the initial stage of the rule, some DNA masks unit created using logistic map and DNA sequence (Divya *et al*., 2012; Pareek *et al*., 2006; Naskar and Chaudhuri, 2015, 2016). Once generating polymer key worth, XOR operation is performed between image and DNA key value to provide cipher image (Kanso and Smaoui, 2009). In this study, DNA with a novel 3D chaotic system has been used to get generate pseudo-random sequences for image encryption.

Literature review: Enaytifar *et al*. (2015) discussed a new technique which is depend on hybrid model of DNA (Deoxyribonucleic Acid), chaotic map and CA (Cellular Automata). To encrypt the pixels of plain image CA rules and DNA series XOR operator are utilized concurrently. Two dimensional chaotic maps are used to find the rule number in CA as well as DNA. This techniques revels

Corresponding Author: Sadiq A. Mehdi, Department of Computer Science, Al-Mustansiriyah University, Baghdad, Iraq

various attacks. Wang *et al.* (2015) discussed a hybrid approach for image encryption which is depend on chaotic system and Deoxyribonucleic Acid (DNA). First of all bitwise XOR operation is performed depend on the pixels of the plain by pseudorandom sequence generated by chaos system, i.e., Coupled Map Lattice (CML). After that with the help of DNA encoding procedure image is encoded to obtain a DNA matrix. After that DNA matrix based initial conditions are generated for CML. And then rows as well as columns of DNA matrix are basically permuted. It creates the confusion. Then finally depend on the DNA decoding procedure confused matrix is decoded. Zhang *et al.* (2013) discussed also, the hybrid approach used chaotic system and DNA subsequence. It basically uses the concept of subsequence operations of DNA rather than complex biological operations (i.e., deletion, elongation and truncation). After that addition operation depend on DNA using Chen's hyper chaotic map is performed in the cipher image.

MATERIALS AND METHODS

DNA and encryption: DNA is incorporates four components A (Adenine), G (Guanine), C (Cytosine), T (Thymine) where G and C are complementary, thus, A and T too . Generally which might be encoded by 0 or 1 and 0 or 1 complement every each to other in binary system of numeration. Then every alphabet image is encoded by a triplet of deoxyribonucleic acid bases components in such the simplest method that the natural construction of the amino acids is simulated. Figure 1 shows the deoxyribonucleic acid structure. There 4! = 24 kinds of deoxyribonucleic acid coding ways consistent with combinatorics, however, out of that alone eight secret writing combos unit of measurement effective owing to the complementary relationship between the four. For example, pixel with gray scale value 228 = $(11100100)_2$ is represented in DNA using rules in Table 1 : (TCGA) in Rule 1, (TGCA) in Rule 2, (CTAG) in Rule 3, (GTAC) in Rule 4, (CATG) in Rule 5, (GATC) in Rule 6, (ACGT) in Rule 7 and (AGCT) in Rule 8 (Zhang *et al.*, 2011; Liu *et al.*, 2012).

DNA and cryptography is a new field developed as a result of the advancement in DNA computation. Recently, it was discovered that DNA is able to store large amounts of data (Landry *et al.*, 2013). DNA cryptography is an emerging technology. It is a new technique used to store data safely in rest and in motion as well. It was invented by Leonard Max Adelman in 1994 to solve complex problems like the Hamilton path problem (Hsieh and Chen, 2008). DNA cryptography has shown

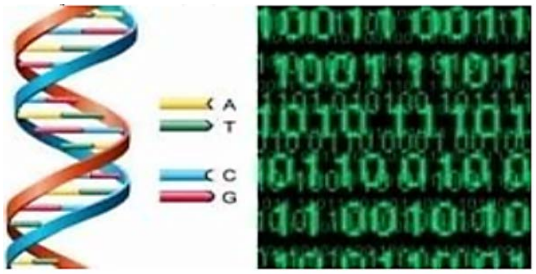

Fig. 1: The DNA structure

Table 1: Encoding and decoding rules

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

new ways to secure data. DNA provides data security with the help of its nucleotides. These nucleotides are made up of four nitrogen bases a carbon sugar and a phosphate group which are Adenine, Cytosine, Guanine and Thymine abbreviated as A, C, G and T. These have a unique sequence structure, making them the basis of DNA cryptography. As this DNA structure; Make living things unique, likewise, using its techniques in cryptography make encryption algorithms unbreakable. According to a rough estimate, a gram of DNA can contain 10^8 terabytes of data. So, a few grams of DNA could contain all the data in the world.

RESULTS AND DISCUSSION

Construction of the novel three-dimensional chaotic system: The novel three-dimensional chaotic system has been created with two nonlinearities terms and Trigonometric function, given by three first order differential Eq. 1:

$$\begin{aligned} \frac{dx}{dt} &= \alpha(y-x)+\beta y \,\text{Sin}(z) \\ \frac{dy}{dt} &= -\delta xz+\gamma y+\lambda x \\ \frac{dz}{dt} &= \mu xy-\psi z+\omega x \end{aligned} \quad (1)$$

Here, x, y and z are real numbers called the states system and $\alpha, \beta, \delta, \gamma, \lambda, \mu, \psi$ and ω are positive parameters of the system. The 3-dimensional system 1 is chaotic system when the system parameter values are chosen as: $\alpha = 20.5, \beta = 15, \delta = 3, \gamma = 8, \lambda = 10, \mu = 2, \psi = 5$ and $\omega = 0.5$ and we take initial conditions as: $x_0 = 0.2, y_0 = 0.4$ and $z_0 = 0.6$.

Lyapunove exponents and Lyapunov dimension: Depending on the non-linear dynamical theory, a technique of quantitative measure of the sensitivity to the initial conditions is calculate the Lyapunov exponent. it's the average rate of divergence of 2 neighboring orbits. Moreover, the 3 Lyapunov exponents of the nonlinear dynamical system Eq. 1 with parameters $\alpha = 20.5$, $\beta = 15$, $\delta = 3$, $\gamma = 8$, $\lambda = 10$, $\mu = 2$, $\psi = 5$ and $\omega = 0.5$. Are obtained as $LE_1 = 1.51259$, $LE_2 = -0.826731$ and $LE_3 = -18.1471$ .It can be seen that the largest Lyapunov exponent is positive that shows the system has chaotic attributes. Since, the LE_1 is a positive Lyapunov exponent and the remainder Lyapunov exponents is negative. So, the method is chaotic. The fractal dimension is also a typical characteristic of chaos calculated Kaplan-Yorke dimension by Lyapunov exponents and D_{KY} can be shown as:

$$D_{KY} = j+\frac{1}{|LE_{j+1}|}\sum_{i=1}^{j} LE_i \quad (2)$$

where, j says the first j Lyapunov exponent is non-negative, namely, j is the maximum value of i value which meets both:

$$\sum_{i=1}^{j} LE_i > 0 \text{ and } \sum_{i=1}^{j+1} LE_i < 0$$

at the same time. Le_idescending order of the sequence according to the sequence of Lyapunov exponents. D_{KY} is the upper limit of the dimension of the system information. For the system in this work by observing the values of ten Lyapunov exponents in the above, we determine that the value of j is nine and then the Kaplan-Yorke dimension can be expressed from the above due to $LE_1+LE_2>0$ and $LE_1+LE_2+LE_3<0$, the Lyapunov dimension of the novel chaotic system is (Mehdi and Qasim, 2017):

$$D_{KY} = j+\frac{1}{|LE_{j+1}|}\sum_{i=1}^{j} LE_i$$

$$D_{KY} = 2+\frac{1}{|LE_{j+1}|}\sum_{i=1}^{2} LE_i = 2+\frac{LE_1+LE_2}{LE_3}$$

$$= 2+\frac{1.51259+-0.826731}{18.14719} = 2.03779$$

which means that the Lyapunov dimension of system Eq. 1 is fractional. Because of the fractal nature, the new system has non-periodic orbits what is more its near by trajectories diverge. Thus, there is truly chaos in this nonlinear method.

Phase portraits: Set the parameters $\alpha = 20.5$, $\beta = 15$, $\delta = 3$, $\gamma = 8$, $\lambda = 10$, $\mu = 2$, $\psi = 5$ and $\omega = 0.5$. The phase portraits have been showed in Fig. 2. It shows that the novel chaotic attractor display a very interesting, chaotic dynamical behavior and complicated. The Lyapunov exponents of system 1 are found to be $LE_1 = 1.51259$, $LE_2 = -0.826731$and $LE_3 = -18.1471$. There is one positive Lyapunov exponents and it is clears that the system is truly a chaotic system. Using mathematica program, the numerical simulation have been achieved. This nonlinear system shows the abundant chaotic dynamics manners and complex, the attractors in three-dimensions are display in Fig. 2 and the attractors in two-dimensions are display in Fig. 3.

Waveform analysis 0f the novel chaotic system: The waveform of a chaotic system should be aperiodic. So, as

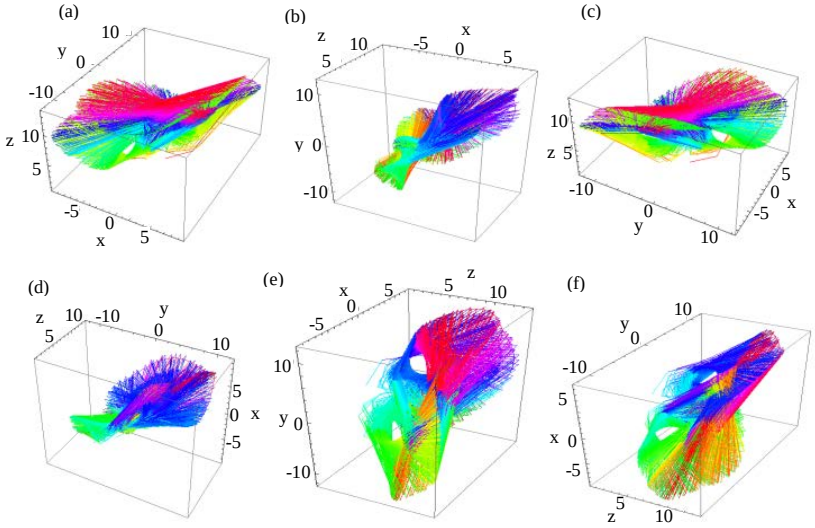

Fig. 2: a-f) Chaotic attractors, three 3-dimensional (z-x)

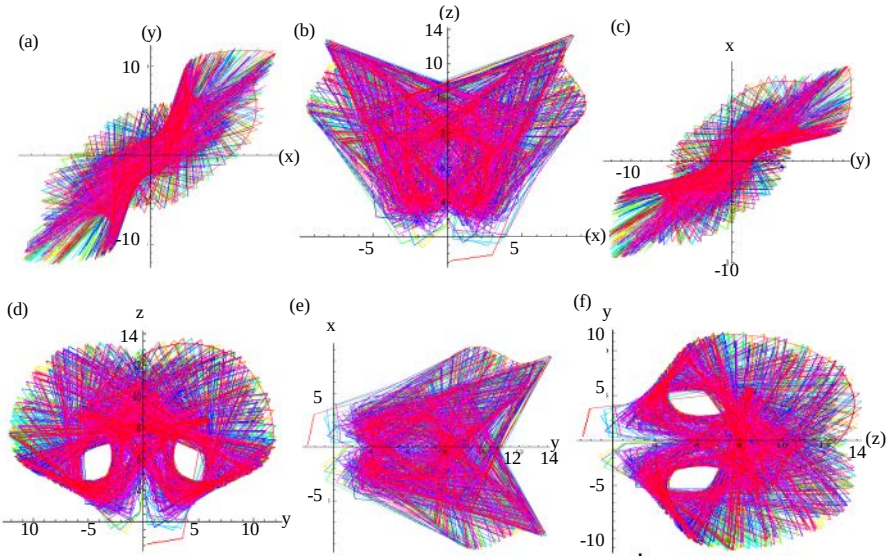

Fig. 3: a-f) Chaotic attractors, two-dimensional view

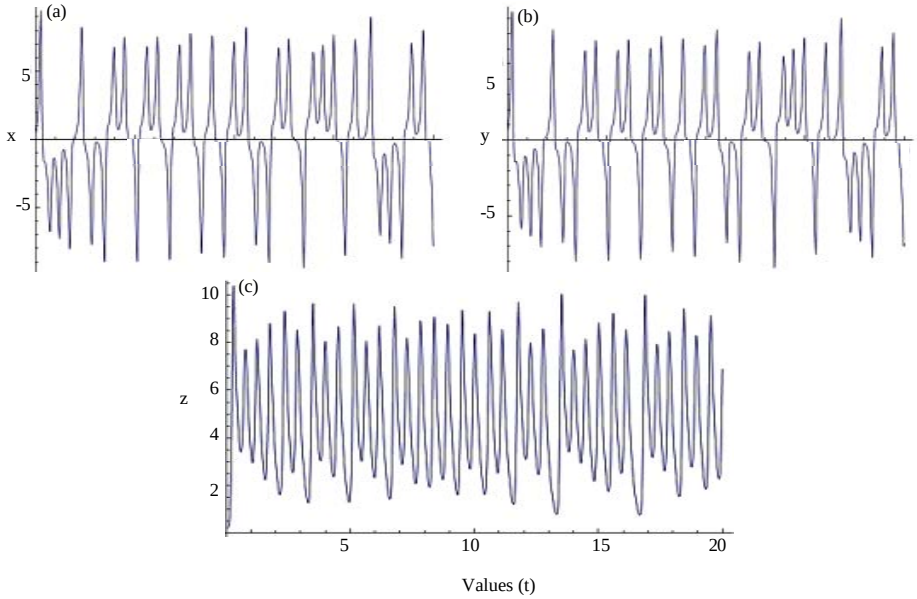

Fig. 4: a-c) Time versus (x, y, z) of the novel chaotic system

to demonstrate that the proposed system is a chaotic system. Figure 4 shows the time versus the states plot obtained from the mathematica simulation. The waveforms of (x (t), y (t), z (t))) in time domain are express in Fig. 4.The waveforms of (x (t), y (t), z (t)) are aperiodic. In order to discriminate between a multiple periodic move that can display also a complicated manner and a chaotic move and it can be cleared that the time domain waveform has non-cyclical features.

Sensitivity to initial condetions: The lonng term unpredictability is one of the chaotic system characteristic because of sensitive depenedence to initial values, such that if a small change is happened between two initial values will become widely separated and the way in which the system is evaluated cannot be predicted, Fig. 5 demonstrate the evolution of the chaotic trajectories has high sensitivity towards initial values. Here, initial values of system 1 are $x_0 = 0.2$, $y_0 = 0.4$, $z_0 = 0.6$ for solid line and $x_0 = 0.2$, $y_0 = 0.400000001$, $z_0 = 0.6$ for dashed linne.

Proposed the encryption algorithm depend on dna and the novel chaotic system: The new image encryption algorithm depend on DNA coding and the novel chaotic system has been used to cipher image information by chaotic keys which created by anovel system. “Chaotic

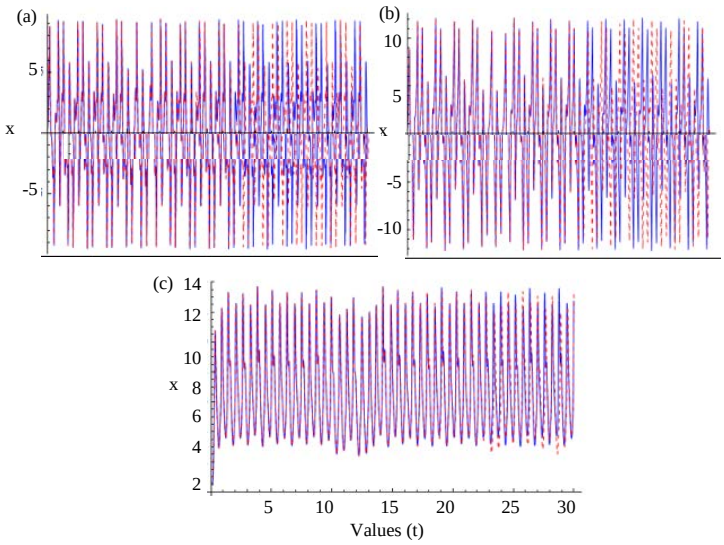

Fig. 5: a-c) Sensitivity tests of the novel system (x (t), y(t), z(y))

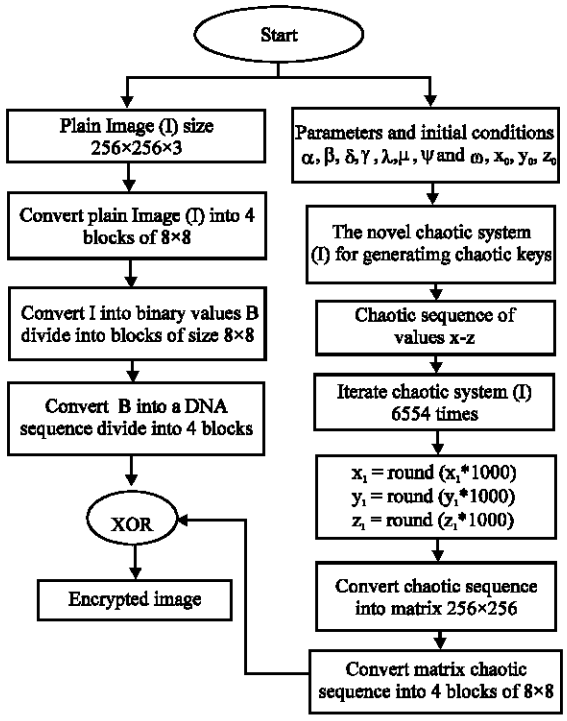

Fig. 6: The block diagram of the chaotic and DNA encryption algorithm

values consists of decimal fractions. images are all digital. Therefore a spherical map is defined to remodel the chaotic series to a different sequence that contains of integers". Then original-image are often encrypted by utilised of XOR operation with the integer-sequence. Figure 6 displays the diagram of the chaotic and DNA encoding algorithm.

The steps will justify as:

Step 1: Read the Plain Image (I) and split the color image into R, G, B components. i.e. size of (I) M×N×3

Step 2: Covert Plain Image into blocks of size 8×8

Step 3: Convert I into binary values B divide into blocks of size 8×8

Step 4: Covert B into a DNA sequence divide into blocks of size 8×8

Step 5: Set encryption key for the original-image including structural parameters $\alpha, \beta, \delta, \gamma, \lambda, \mu, \psi$ and ω and initial values x_0, y_0 and z_0

Step 6:Generate three sequences $\{(x_i, y_i, z_i); i = 1, 2, \ldots, 65554\}$ according to the novel chaotic system (1)

Step 7: Round the chaotic sequences x_i = round (x_i*1000), y_i = round (y_i*1000), z_i = round(z_i*1000)

Step 8: Covert chaotic sequences into matrix 256×256

Step 9: Covert matrix chaotic sequences into 8 blocks of size 8×8

Step 10: Preform XOR operation between 8 chaotic keys and blocks of Plain Image after diffusion process

Experimental tests: In this part, the proposed algorithm was analyzed depend on set of images. Figure 7 displays the experimental results with 3 images. Figure 7a is the original-images of size 256×256. Figure 7b is its encrypted images. Figure 7c is the images.

Security analysis: The encryption key for good cipher algorithm must have length of the key space should be greater than 2^{128} and very sensitive to its alteration to avoid brute force attack.

Key space analysis: To frustration the threat of brute force attack and make it infeasible the size of key space must be large enough where key space mean all possible and different keys can be utilized in encryption process and the minimum key size must at least 2^{100} (bits) to withstand brute force attack (Vaidyanathan *et al*., 2014).

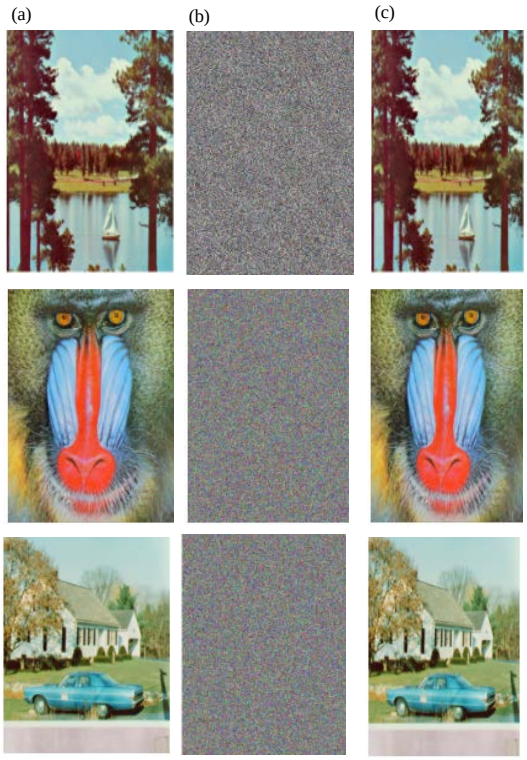

Fig. 7: Image encryption and decryption experimental result: a) Oiginal-images; b) Ecrypted images and c) Dcrypted images

In the presented encryption algorithm secret key is initial conditions and parameters: (x_0, y_0, z_0, α, β,δ, γ, λ, μ, ψ and ω), precision for each one is 10^{-14}, so, the key space calculated as $10^{154} \approx 2^{508}$, They key space is large enough and thwarted brute-force attacks.

Key sensitivity analysis: The proposed has sensitivity to initial values used to build the server key make it resistant to exhaustive attack for example if one value of initial values of private server key change to (x_0 = 0.2, y_0 = 0.4×10^{-14} and z_0 = 0.6) the decode shares are changed to a different one and become impossible rebuild the secret image. In case of the user key if click which perform on loaded image changed one pixel the value of user key changed and if the function control used with user key does not exist in the server information become hardly rebuild the random key. Large key space makes the algorithm resistant to exhaustive attack. The results are illustrated in Fig .8.

Statistical analysis: To show the toughness of the proposed image encryption algorithm it is subjected to statistical analysis on the encrypted image to determine

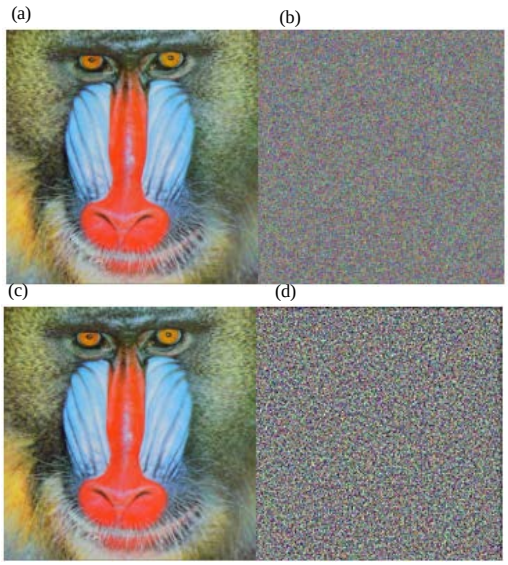

Fig. 8: Results of sensitivity test: a) Plain image of Baboon; b) Encrypted image of (a); c) Decrypted image of; a) with the correct key and d) Decrypted image of (a) with a change in key y_0 (y_0 = 0.40000000000001)

the characteristics of the confusion and diffusion. The cryptographic algorithm must be very effective and powerful against statistical attacks by testing these analyzes including: histogram, the information entropy and the correlation coefficient test of the encrypted image.

Histogram analysis: To block attacker from leakage information for plain image must avoid any statistical relationship or similarities between the clear image and ciphered image where statistical properties for image can be deduced from histogram analysis and to make cipher image more withstand to statistical attacks the form of histogram for cipher image must be completely uniform or flat or horizontal distributed in different with histogram for plain image (Mehdi and Kareem, 2017). Figure 9 shows histograms for encrypted image (red, green, blue) fairly uniform due to robust proposed encryption scheme diffusion stage and there isn't any statistical similarities where histogram for plain image and histogram for cipher image dissimilar and different in appearance.

Correlation coefficient analysis: One of basic characteristics of plain image is high correlation or relationship between adjacent pixels, correlation is a measure of the level of likeness between two pixels,

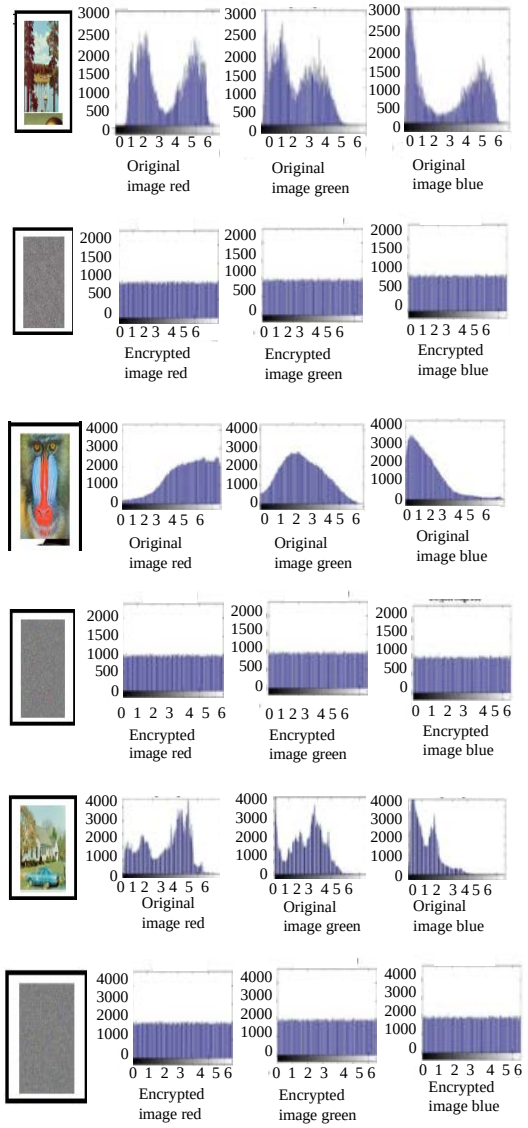

Fig. 9: Histogram for plain images and its encryption

encryption scheme must be reduce the correlation among adjacent pixels to prevent the attacker from speculated the values for neighbors pixel, encryption scheme trying to make the correlation close to zero to avoid any statistical attacks with respect to plain image where value for correlation close to one, correlation coefficient for two neighboring pixels can be computed by formula:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3)$$

$$\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (4)$$

Table 2: Correlation values for plain image lake and corresponding ciphered image

Variables	Vertical	Horizontal	Diagonal
PlainImage	0.9836	0.9884	0.9848
Encrypted Image	0.0006	-0.0011	0.00015

Table 3: Correlation values for plain image baboon and corresponding ciphered image

Variables	Vertical	Horizontal	Diagonal
Plainimage	0.99765	0.9976	0.9964
Encrypted image	0.0023	0.0008	0.0004

Table 4: Correlation values for plain image house and corresponding ciphered image

Variables	Vertical	Horizontal	Diagonal
Plainimage	0.9835	0.9734	0.9913
Encrypted image	-0.0023	0.0001	-0.0018

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \quad (5)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (6)$$

where $\sqrt{D(x)} \neq 0$ and $\sqrt{D(y)} \neq 0$

Where:

x_i and y_i = The values of two neighboring pixels
E(x) = The mean of x_i
E (y) = The mean of y_i
N = The number of pair's pixels x_i, y_i (Wang, 2013)

Correlation for adjacent pixels vertically, horizontally and diagonally has been analyzed for plain image and corresponding encrypted image where Fig. 10-12 shows the allocation vertically, horizontally and diagonally of pixels for plain and encrypted image, high correlation between two adjacent pixels for plain image appear while correlation for cipher image very small and close to zero when the proposed encryption scheme utilized, Table 2-4 displays the values of correlation for two contiguous pixels in the clear image and encrypted image.

Information entropy analysis: Entropy is the most significant characteristic of randomness or unpredictability in information theory, entropy H (m) for a message m is measured by following form:

$$H(m) = -\sum_{i=0}^{2^n-1} P(m_i)\log_2[P(m_i)] \quad (7)$$

where, p (mi) rpresented the probability of appearance of symbol m_i and the entropy is expressed in bits, perfect

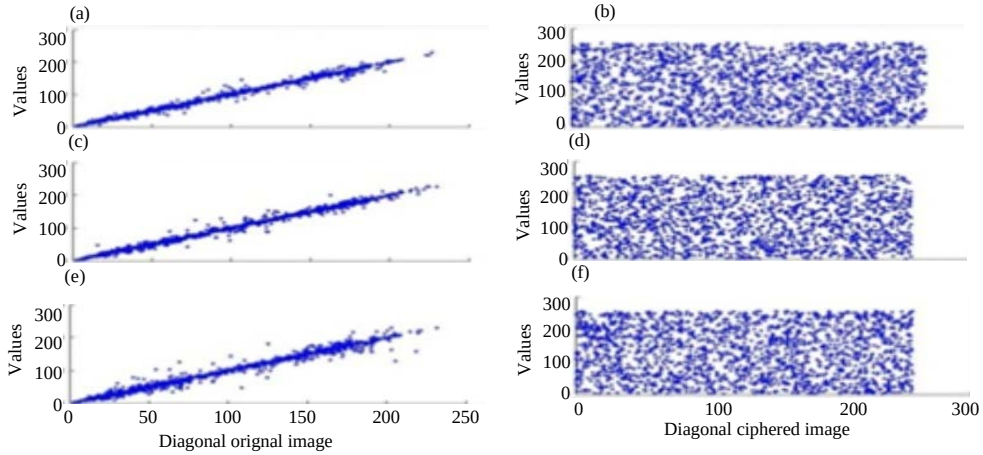

Fig. 10: a-f) Plot describe correlation values for two adjacent pixels in plain and encrypted lake image

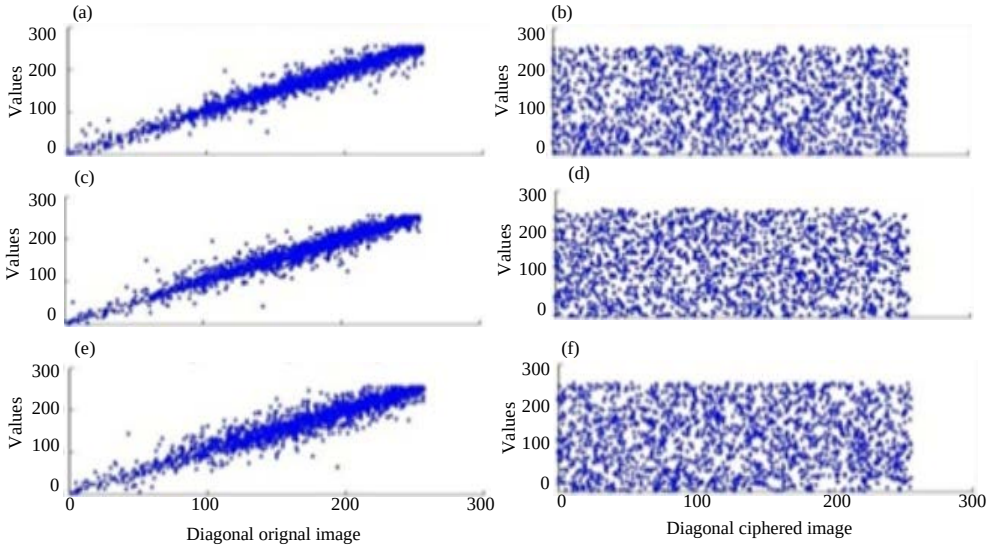

Fig. 11: a-f) Plot describe correlation values for two adjacent pixels in plain and encrypted Baboon" image

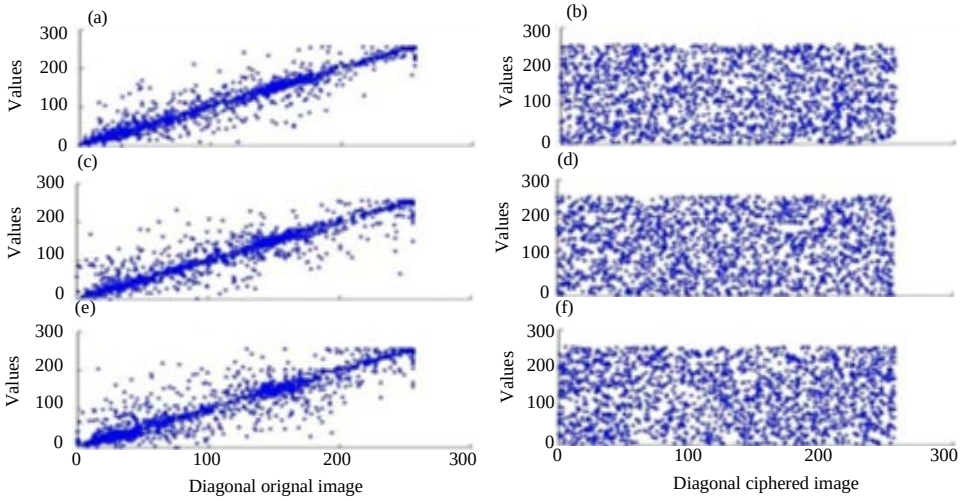

Fig. 12: a-f) Plot describe correlation values for two adjacent pixels in plain and encrypted house image

Table 5: Information entropy for plain and cipher images

Image	Image size	Plain encrypted	Red plane	Green plane	Blue plane
	256×256	Plain	7.9986	7.9765	7.9849
		encrypted	7.9815	7.9924	7.9980
	256×256	Plain	7.9936	7.9864	7.9909
		encrypted	7.9913	7.9721	7.9978
	256×256	Plain	7.8996	7.9570	7.9866
		encrypted	7.9983	7.9838	7.9982

randomly source emitting 2^8 symbols the entropy is H(m) = 8, this mean the ciphered image has better random characteristic and the proposed scheme for encryption is highly secure and more resist against entropy attack (Wang, 2013). The entropy values for cipher images between 7.9815 and 7.9983 are obtained for three test images in Table 5 show high security against entropy attack with less degree of predictability that threatens the security.

Defferential attacks: Good encryption scheme must has ability to withstand differential attack, the test for differential attack include encrypted two plain images P1 and P2 with very small different one bit and evaluate the impact of that difference on the result cipher images, two important measures used, NPCR in addition to, UACI where (NPCR) measure percentage of various pixels among two ciphered images C^1, C^2 and can expressed by the following Eq. 7 and 8:

$$D(i,j) = \begin{Bmatrix} 0, \text{if } C^1(i,j) = C^2(i,j) \\ 1, \text{if } C^1(i,j) \neq C^2(i,j) \end{Bmatrix} \quad (8)$$

$$\text{NPCR: } N(C^1, C^2) = \frac{\sum_i D(i,j)}{T} \times 100\% \quad (9)$$

where, UACI used to measure the average intensity of various between the two ciphered images and expressed by Vaidyanathan (2016):

$$\text{UACI}: U(C^1, C^2) = \frac{\sum_{i,j} \left| C^1(i,j) - C^2(i,j) \right|}{F \times T} \times 100\% \quad (10)$$

Table 6 shows NPCR and UACI values for five test images Lake , Baboon and House. From Table 6 and in comparison with theoretical values in (Mehdi and Kareem, 2017) the result values for NPCR between (99.9962-99.9991) and pass the test where the result values for UACI between (32.6813-33.5787) and some of these values pass the test where others are close to theoretical values from above the presented encryption algorithm has high ability to frustration the differential attacks.

Table 6: NPCR and UACI result values

Image	NPCR	UACI
Lake	99.9991	33.5787
Baboon	99.9973	33.7895
House	99.9962	32.6813

Table 7: Encryption and decryption speed

Image	Encryption time (sec)	Decryption time (sec)
Lake	0.2141	0.2042
Baboon	0.4825	0.3821
House	0.3467	0.2512

Speed performance: Speed of proposed cryptosystem is very important factor to measure the efficiency where the proposed scheme realized by MATLAB 2013a under Windows 7 ultimate (64-bit) using a personal computer Intel (R) Core(TM) i7 @2.67GHz CPU and 4GB RAM and the Table 7 shows encryption and decryption speed. Table 7 show that encryption and decryption time for proposed encryption algorithm with real time and it is very small.

CONCLUSION

In this study, a new image cryptography algorithm depend on deoxyribonucleic acid codes and a novel chaotic system has been proposed here. the novel 3D chaotic system in this study has been used to generating random values. Figure 2 and 3 shows the attractor and sensitivity analysis for proposed system and it is clearly display chaotic behavior. Simulation results and security testes show that the proposed algorithm is efficient where it has large key space ($10^{154} \approx 2^{508}$) and the encryption algorithm has high resistance to statistical attacks where histogram test for encrypted image is completely uniform and correlation values for encrypted image between (0.0004-0.0007) is very small and close to zero while the entropy values for encrypted image about (7.997) are close to optimal value, the encryption algorithm also has high resistance to differential attack where the values for NPCR and UACI is pass the all theoretical intervals and in addition to that the encryption algorithm has good sensitivity to key change and the time image encryption/decryption was very small about (0.2141) sec, all these enhances the protection and might resist commonest attacks that shows that our encryption algorithm includes a sensible security.

REFERENCES

Divya, V.V., S.K. Sudha and V.R. Resmy, 2012. Simple and secure image encryption. Intl. J. Comput. Sci. Issues, 9: 286-289.

Enayatifar, R., H.J. Sadaei, A.H. Abdullah, M. Lee and I.F. Isnin, 2015. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt. Lasers Eng., 71: 33-41.

Hsieh, S.Y. and M.Y. Chen, 2008. A DNA-based solution to the graph isomorphism problem using Adleman-Lipton model with stickers. Appl. Math. Comput., 197: 672-686.

Kanso, A. and N. Smaoui, 2009. Logistic chaotic maps for binary numbers generations. Chaos Solutions Fractals, 40: 2557-2568.

Landry, C.D., E.R. Kandel and P. Rajasethupathy, 2013. New mechanisms in memory storage: PiRNAs and epigenetics. Trends Neurosci., 36: 535-542.

Liu, H., X. Wang and A. Kadir, 2012. Image encryption using DNA complementary rule and chaotic maps. Applied Soft Comput., 12: 1457-1466.

Mehdi, S.A. and H.A. Qasim, 2017. Analysis of a new hyper chaotic System with six cross-product nonlinearities terms. Am. J. Eng. Res., 6: 248-252.

Mehdi, S.A. and R.S. Kareem, 2017. Using fourth-order runge-kutta method to solve Lu chaotic system. Am. J. Eng. Res., 6: 72-77.

Naskar, P.K. and A. Chaudhuri, 2015. A robust image encryption technique using dual chaotic map. Intl. J. Electron. Secur. Digital Forensics, 7: 358-380.

Naskar, P.K. and A. Chaudhuri, 2016. Secured secret sharing technique based on chaotic map and DNA encoding with application on secret image. Imaging Sci. J., 64: 460-470.

Pareek, N.K., V. Patidar and K.K. Sud, 2006. Image encryption using chaotic logistic map. Image Vision Comput., 24: 926-934.

Sathishkumar, G.A., K. Bhoopathy bagan and N. Sriraam, 2011. Image encryption based on diffusion and multiple chaotic maps. Intl. J. Network Secur. Appl., 3: 181-194.

Shekhar, S., H. Srivastava and M.K. Dutta, 2012. An efficient adaptive encryption algorithm for digital images. Intl. J. Comput. Electr. Eng., 4: 380-383.

Vaidyanathan, S., C. Volos and V.T. Pham, 2014. Hyperchaos, adaptive control and synchronization of a novel 5-D hyperchaotic system with three positive Lyapunov exponents and its SPICE implementation. Arch. Control Sci., 24: 409-446.

Wang, M., 2013. Analysis and numerical simulation of a novel four-dimensional dynamic evolution system with multilayer chaotic attractors. Intl. J. Signal Process. Image Process. Pattern Recognit., 6: 309-322.

Wang, X.Y., Y.Q. Zhang and X.M. Bao, 2015. A novel chaotic image encryption scheme using DNA sequence operations. Opt. Lasers Eng., 73: 53-61.

Zhang, Q. and X. Wei, 2013. A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Opt. Intl. J. Light Electron Opt., 124: 6276-6281.

Zhang, Q., L. Guo and X. Wei, 2013. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-Int. J. Light Electr. Opt., 124: 3596-3600.

Zhang, Q., S. Zhou and X. Wei, 2011. An efficient approach for DNA fractal-based image encryption. Appl. Math. Inf. Sci., 5: 445-459.