



Image Encryption by Using Combination of DNA Sequence and Lattice Map

Ali Asghar Abbasi¹, Mahdi Mazinani^{2✉}, Rahil Hosseini¹

1) Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

2) Department of Electrical Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

abbasi.aliasghar.ai@gmail.com; universitymazinani@gmail.com; rahilhosseini@gmail.com

Manuscript ID: JACR-1809-1640

Received: 2018/09/24; Accepted: 2019/04/20

Abstract

In recent years, the advancement of digital technology has led to an increase in data transmission on the Internet. Security of images is one of the biggest concern of many researchers. Therefore, numerous algorithms have been presented for image encryption. An efficient encryption algorithm should have high security and low search time along with high complexity. DNA encryption is one of the fastest emerging technologies performing based on the concepts of DNA computing and can be used for data storage and transfer. Very high speed and minimum memory and power requirements in the DNA calculations are of the advantages of this new encryption algorithm. In this study, a new encryption algorithm has been proposed for grayscale digital images using DNA algorithm and lattice map function. In the first step, the initial value of the Logistic Map function has been obtained from a 120-bit key using the proposed method, then in the second stage, the original image was encrypted with the Lattice Map function sequence using the logistic map function sequence generated in the previous step and the DNA rules. The results of the simulations showed a high level of resistance and security against statistical attacks, so that the entropy of the proposed method was obtained as 7.9996.

Keywords: Chaos Function, Lattice Map, DNA Sequence

1. Introduction

The risk of data leakage has increased through increasing the use of images and information in communications through the Internet. Therefore, the need for secure data transfer has increased. Cryptography is a mechanism for providing confidentiality of information and thus guarantees data security. The cryptography mechanism can be broadly categorized into two categories:

1. Symmetric key encryption: A shared key is used for encryption and decryption.
2. Asymmetric key encryption: Two key types are used in this mechanism:

Public key and private key; so that the sender and receiver perform data encryption and decryption using the public key and the private key, respectively. This mechanism provides a much better security in comparison to the symmetric key encryption, but has a high cost and complexity.

Nowadays, cryptography is not used only in military and security information, but is also widely applied in many other areas. Today, cryptography is widely applied in medical data and records, televideo conferencing, individual identity information (PII) and organizational information. In addition, individuals' privacy can be protected using

cryptography. The Triple Data Encryption (Triple DES) algorithm was proposed in 1999 as part of data encryption standard using three different keys with a length of 168 bits.

The Advanced Encryption Standard (AES) algorithm was developed by the National Institute of Standards and Technology (NIST) in 2001 for encryption of electronic data, which is the combination of substitution–permutation [19]. RC4 is an encryption algorithm with variable key size and byte-oriented operations proposed by Ronald L. Rivest for RSA security [18, 20, 24, 25]. For the first time, a block cipher encryption, which was the improved proposed standard encryption, was presented in 1991 and developed by Moni Naor and Adi Shamir in 1994 [16, 22, 26]. Since most of the known evolutionary computation methods are computerized simulations of natural and biological processes.

In [2], a new evolutionary computation algorithm was introduced which has been established based on social and political evolution of mankind. Which focused on the image binary encryption using weighted discrete imperialist competitive algorithm (WDICA) and a tent map chaos function. And its goal was to maximize the entropy and minimize the correlation coefficient. To do this, at first, the image is encrypted by chaos function. Then, this process should be repeated in order to create the WDICA population. In the next step, the fitness function, which includes the entropy and correlation coefficients, is used with crossover operator in the assimilation phase.

The method proposed in [1] created some encrypted images using the original image and chaos function. Then in the next step, these encrypted images which are as the initial genetic algorithm (GA) population, were divided into 4 equal parts. Then, a two-point crossover operator and a key were utilized exploiting the fitness function (entropy coefficients). And in each step of the GA iteration, the best encrypted image has been obtained as the image with the highest entropy and lowest correlation coefficient among the adjacent pixels.

The method proposed in [4] was designed to increase the security of digital images in encryption using the permutation method and simultaneous release in order to protect the grayscale image content through the Internet. To implement this method, a simple two-dimensional image is converted to a one-dimensional one. Then, both permutation and release steps are performed simultaneously for each pixel in order to reduce the transmission process time. 3D logical map chaos function and a 240-bit key (80 bits for each sequence) were applied in two simultaneous steps to encrypt the image. In the first step, permutation was used in the first dimension of the logistic map chaos function in order to change the location of pixels and in the second step, the two other dimensions of the logistic map chaos function and DNA sequence were used to change the amount of grayscale image surfaces. The encryption strength is how to choose the key. Detection and guess of the key consisting of various parameters used in encryption should be impossible for unauthorized individuals.

The chaotic systems are very sensitive to initial system state and its parameters and in a set of possible states of parameters, choosing two close initial parameters would lead the system to two different paths. Therefore, if parameters are selected as “key” and “directions” are used for encryption/decryption, an encryption/decryption algorithm will

be obtained. If similar parameters are used for encryption/decryption, the chaos design will be symmetric. Selection of parameters and initial conditions of a large key space will result in the security of the generated code. Chaotic synchronization in analog devices, stability, and deviation are the most important practical problems which must be solved before using them in designs based on synchronization in encryption. In contrast, a software method could be efficient and along with today interests in information processing.

The procedure proposed in [6] is an effort to overcome the aforementioned drawback. For this purpose, to encrypt any pixel of the image, the number of iterations is counted once until the output of the equation lays in the period corresponding to that pixel. The number resulted from counting the encryption code replaces the pixel in the encrypted image. This process continues until encryption of all pixels of the image and conversion of them into a series of numbers. Decryption will be performed with the similar algorithm and the same keys. The number of iterations for encryption is the same numbers with the integers in the encrypted image, and the conversion of numbers to corresponding pixels is performed by an inverse mapping transform.

The paper structure is as follows. Firstly, the chaos function, lattice map function, and DNA sequence are introduced. Then, the proposed algorithm and simulation results are expressed in the next step.

2. In This Part, The Chaos Function, Lattice Map Function and DNA Sequence are Described Briefly.

2.1 Chaos function

The chaos concept is one of the new and essential concepts of the modern science which has extended the horizon of understanding of the universe. In the other words, chaos is a phenomenon occurring in describable nonlinear systems and is an important feature which has been remarkably taken into account in cryptography and steganography. Definability of system along its pseudo random behavior makes the system output seem random for attackers, however, it is a definable system from the prospective of the decryptor, hence capable of being decrypted.

Chaos function-based algorithms introduce quick and at the same time, very secure methods for cryptography and steganography due to sensitivity to initial conditions, apparently random behavior, and deterministic performance.

2.2 Logistic Map

Logistic Map is a nonlinear one-dimensional mapping introduced as follows:

$$x_{n+1} = ax_n(1 - x_n) \quad (1)$$

The behavior of this mapping is unpredictable and depends on the a value. as a control parameter, determines the behavior of this mapping as follows:

For $0 < a < 1$, the point $x = 0$ is an attractor. Its means all circuits starting from any x_0 , reach zero after some iterations. For $1 < a < 3$, the point $x = 1 - 1/a$ is an attractor and all

circuits independent of x_0 , reach $1-1/a$ after some iterations. With increasing a , for $a=3$, the first bifurcation happens and is stable in the distance $1+\sqrt{6} > a > 3$. The next bifurcation happens with further increase of a and 4-period, 8-period, ... , and 2^n -period circuits reveal respectively. Finally, we will have two dimensional waterfalls of bifurcations at $a = 3.82$ after which the chaos can be well observed.

a is a variable parameter in the recursive relation (1). If we want to observe behavior of this relation relative to changes in a , a graph like figure 1, called bifurcation diagram, must be considered.

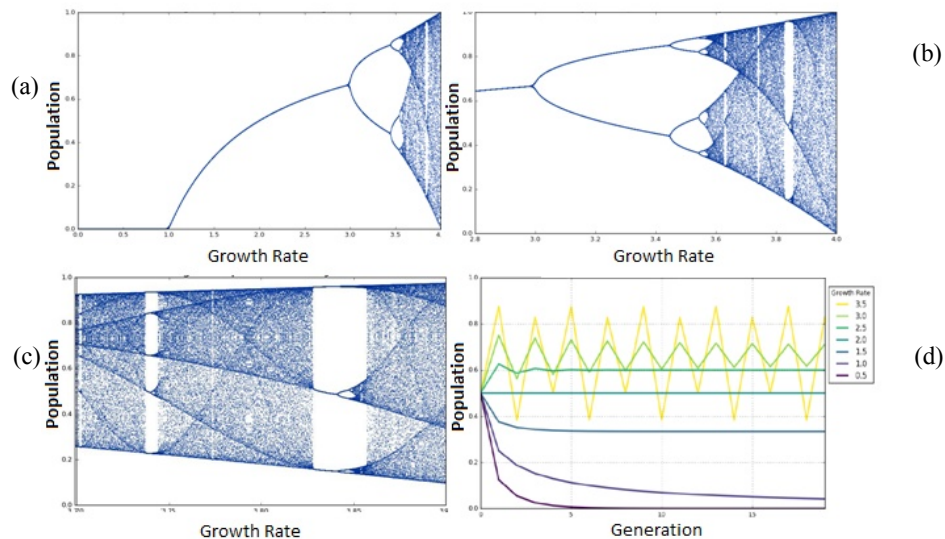


Figure 1. Bifurcation diagrams of Logistic Map chaos function with a growth rate between a (0, 4), b (2.8, 4), c (3.7, 3.9), and (d) logistic map time graph with a growth rate of 7

As can be seen, for the parameter a between 0 and 1, the sequence tends to zero. In addition, for values between 1 and 3, it will converge into a certain value. In the next distance, the sequence becomes as two-valued, meaning converging into two values. Finally, from a value of 3.82 afterwards, the sequence final value is not known, being completely chaotic and no iterative values between 0 and 1.

2.3 Lattice Map Function

A Lattice Map function is a dynamical system that models the activities of non-linear systems. They are mostly used to qualitatively study the chaotic dynamics of spatially extensive systems. This consists of the dynamics of spatiotemporal chaos somewhere the number of effective degrees of freedom diverges as the volume of the system increases.

Features of the Lattice Map are separated, discrete underlying spaces, and incessant state variables. The desired systems include biological networks, chemical reactions, populations, fluid flow, etc. Recently, Lattice Map has been applied to hide vital information.

$$x_{n+1}(i) = (1 - \varepsilon)f [x_n(i)] + \varepsilon/2\{f [x_n(i + 1)] + f [x_n(i - 1)]\} \quad (2)$$

2.4 Image encryption and decryption using DNA

In 1994, Adelman performed the first computational experimentation of DNA and established a new molecular computing science for solving compound problems in the information field [34]. With the onset of research in DNA calculations, a new ground was formed which used the DNA sequence as information bearer and this new technology was used as an implementation tool. For example, if the letters A and B are respectively displayed as the sequences CGA and CCA, then AB is equal to CCGCCA. Each DNA sequence contains four basic nucleic acid, which include A, C, G, T. A, T and G, C are complementary. Since 0 and 1 are complementary, therefore, 00 and 11 will also be complementary. Similarly, 01 and 10 have the same status and are complementary. Using these four combinations, there are 24 different modes for encryption. However, given the complementarity of the rules A, T and G, C, only 8 states presented in table 1 will be valid [35,36].

Table 1. Valid modes of DNA strands for encryption and decryption

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

As shown in this table, each element is repeated only once in the row or column. Different operators such as addition and subtraction, and XOR and XNOR are used in image encryption; XOR and its complement XNOR, are usually used in encryption and decryption, respectively.

Table2: XOR operations for DNA sequence

	A	G	C	T
A	A	G	C	T
G	G	T	T	A
C	C	C	A	G
T	T	A	G	C

3. Proposed Method

The proposed method is described as follows:

For an 8-bit grayscale image, each pixel can be represented as DNA sequences of length 4. For instance, if the value of an image pixel is 173 (the equivalent binary is 10101101), its DNA sequence will be equal to TTGA using Rule 3 given in table 1.

Therefore, after converting the pixels of the image into DNA strands, using the chaotic sequence, which is also converted to DNA strands in this way, the XOR is performed using table 2, and then the results of the XOR operation are converted to binary strings using table 1 and then converted to decimal numbers in the next step. In the following of the study, the proposed method will be explained in more details.

3.1 Secret key

In the proposed method, first, a key was used for Lattice Map function which was performed by a sequence generated from the Logistic Map. The Logistic Map function needs an initial value (X_0) to commence; this value is produced from a 120-bit key.

$$K = K_0, K_1, \dots, K_{14} \text{ (Hexadecimal)} \quad (3)$$

Where, K_i can represent characters 0-9 and A to F. This key can be defined as American Standard Code for Information Interchange (ASCII) as follows:

$$K = K_0, K_1, \dots, K_{14} \text{ (Ascii)} \quad (4)$$

In this key, K_i specifies an 8-bit block of the key. In this algorithm, a Logistic Map chaos signal was used according to equation (4). To determine the initial value of the signal, X_0 , the key has been converted to binary form.

$$K = (K_{01}, K_{02}, \dots, K_{119} \text{ (Binary)}) \quad (5)$$

Where, K_i specifies the j -th bit of the i -th key. X_{01} value can be calculated as follows:

$$X_{01} = (K_{01} \times 2^{119} + K_{03} \times 2^{118} + \dots + K_{n5} \times 2^1 + K_{n7} \times 2^0) / 2^{120} \quad (6)$$

Where, $n = \{0, 1, \dots, 9\}$ represents the key number and K_{ij} designates the j -th bit of the i -th key, so that $j = \{1, 3, 5, 7\}$. We can also calculate the X_{02} value as follows:

$$X_{01} = (K_{02} \times 2^{119} + K_{04} \times 2^{118} + \dots + K_{n6} \times 2^1 + K_{n8} \times 2^0) / 2^{120} \quad (7)$$

Where, $n = \{0, 1, \dots, 9\}$ represents the key number and K_{ij} designates the j -th bit of the i -th key, so that $j = \{2, 4, 6, 8\}$. In the end, the X_0 initial value will be calculated as follows:

$$X_0 = (X_{01} + X_{02}) \bmod 1 \quad (8)$$

In the following, the Lattice Map function consecutive series is produced according to the X_0 value and Logistic Map function. Then, pixel displacement is first performed (without changing grayscale level) using Logistic Map sequence for greater complexity and higher security in encryption algorithm. In the next step, relation 8 was used to encrypt the first pixel of the original image:

$$\begin{aligned} & \text{Floor}(X_1 * 255) \text{ XOR Image}(i, j) \\ & i \in [0 \dots i * j + 1], i \in [1 \dots \text{Image}_{\text{row}}], j \in [1 \dots \text{Image}_{\text{column}}] \end{aligned} \quad (9)$$

Then, the encrypted image from original image will be generated as the initial population to begin the genetic algorithm using the sequence of numbers of Lattice Map function.

3.2 Our method

The proposed encryption system uses a key called K with a length of 120 bits, which has been considered as the initial number of the logical map function to increase the encryption security. Then, using the generated chaotic sequence as input to the lattice map function, the chaotic sequence is generated for the encryption operation. The original image is then converted to a one-dimensional array, and the chaotic sequence generated by the lattice map function is shifted from 0 to 255, and the selected pixel is converted to binary by the chaotic sequence. In the next step, in order to select the DNA rules, numbers should be selected as the number of pixels from the chaotic sequence and shifted to the interval 1 to 8. Then using the table, the DNA sequence of the image pixels are converted to DNA strands. In the next step, these generated strands become XOR by the chaotic sequence numbers and using table 2. Then, the DNA strands are converted to binary and decimal numbers using table 1.

```

Start
  K ← Input key
  L_X ← Initialize lattice Map Parameters Based on K and Logistic Map
  IMG ← Convert Input Image to one Dimension Array
  Label 1: L_N ← Round ( L_X[i]*255 )
          B_L ← Convert L_N to Binary
          B_I ← Convert IMG[i] to Binary
          Rule_NUM ← Round( L_X[i]*7+1 )
          L_DNA ← Convert B_L to DNA Sequence Based on Rule_NUM
          I_DNA ← Convert B_I to DNA Sequence on Rule_NUM
          New_N ← Apply DNA XOR Between L_DNA and I_DNA
          New_B ← Convert New_N to Binary Based on Rule_NUM
          IMC[i] ← Convert New B to Decimal
          i ← i+1
          If i ≤ Length (IMG)   Label 1
          else
          End

```

Semi-code of image encryption algorithm using combination of DNA sequence and Lattice Map

4. Experimental Results

In this section, the efficiency of the proposed method will be investigated as follows.

4.1 Statistical analysis

An ideal hiding algorithm should resistance against statistical attacks. To prove this strength, statistical analysis through calculating image histogram, calculating correlation between adjacent pixels for various images and also calculation of this parameter have been used for these images from USC-SIPI database.

4.2 Histogram analysis

Histogram illustrates the number of pixels in every grayscale level for an image. In general, it can be shown that the more uniform the image histogram obtained in encryption algorithm, the less the possibility of a statistical attack on the image. Therefore, the encrypted image histogram showed the efficiency of the proposed method. In figure 2, histogram of the pepper image has been showed before and after encryption using the proposed method. As seen in the image, the histogram of image is uniform after encryption. Figure 2c indicates the image histogram before encryption and figure 2d demonstrates histogram of the encrypted images. It can be seen that the histogram of the encrypted images is uniform after implementing the algorithm.

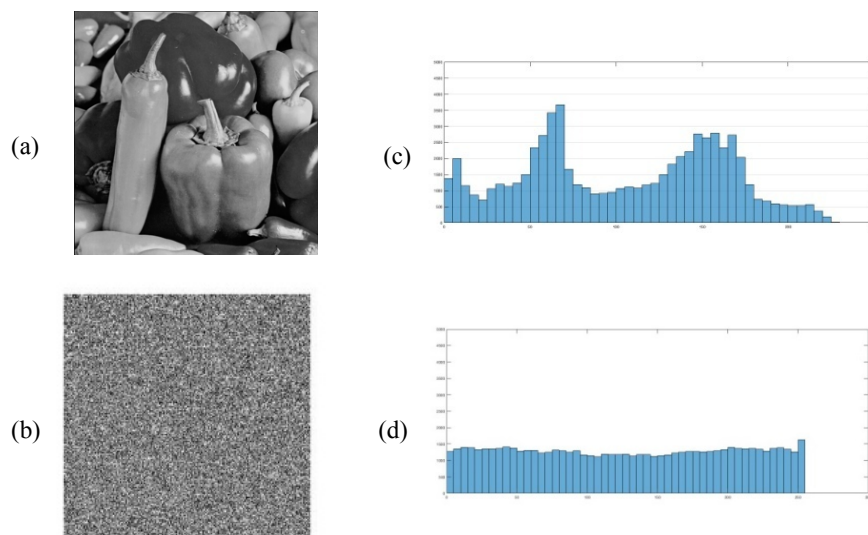


Figure 2. Original image (a), original image histogram (b,d), histogram and the encrypted image of original image after encryption

4.3 Analysis of correlation coefficients

To compare the obtained results, the average of (horizontal, vertical, and diagonal) correlation coefficients is calculated among several special points for each pair of encrypted images to show its sensitivity to even small changes in the key. For this purpose, 4096 pairs of adjacent pixels have been considered horizontally, vertically, and diagonally as sample. The correlation coefficient for two adjacent pixels is calculated using relation 9.

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

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

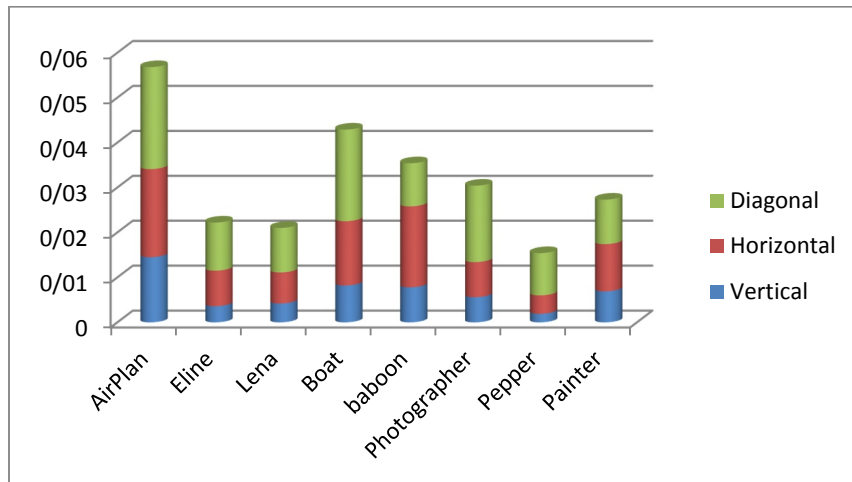
$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x_i))(y_i - E(y_i))$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$
(10)

In another test, 8 images were selected to study the results of correlation coefficients for two adjacent pixels in horizontal, vertical, and diagonal situations. The results are shown in table 3. Comparison of the results of the proposed method for correlation coefficients with the introduced method is provided in table 1 [1, 2].

Table 3. Correlation coefficient analysis in images from USC-SIPI database

Correlation	Painter	Pepper	Photographer	Baboon	Boat	Lena	Elaine	Airplane
Vertical	0.0069	0.0019	0.0056	0.0078	0.0082	0.0042	0.0036	0.0145
Horizontal	0.0105	0.0041	0.0078	0.0180	0.0143	0.0069	0.0079	0.0196
Diagonal	0.0099	0.0094	0.0170	0.0096	0.0204	0.0099	0.0107	0.0227



Graph 1. Correlation coefficient analysis in USC-SIPI database images

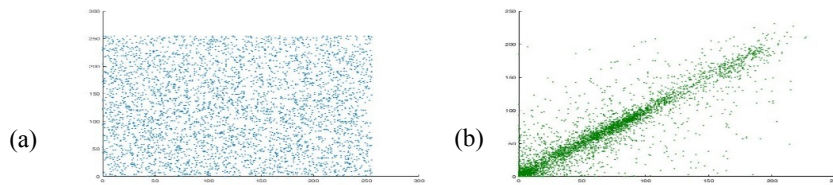


Figure 2. (a) Original image correlation analysis and (b) encrypted image

4.4 Analysis of state space and sensitivity to key

In an appropriate image encryption procedure, the key space should be large enough to resist against unbridled attacks and be sensitive to key small changes. It means that changes of a bit in the key should result in very different result. A 120-bit key was used in the proposed method. So that the key state space is as 2^{120} . Therefore, the state space is large enough.

The encryption operation was performed on the Camera Man image in figure 3(a) by AYL8DJH59HGSYD4 key 3(b). Then this operation was performed on the same image by AYL8DJH59RGSYD4 key 3(c).As shown in figure 3(d), the difference between encrypted images is large although being small (with changes in a character).

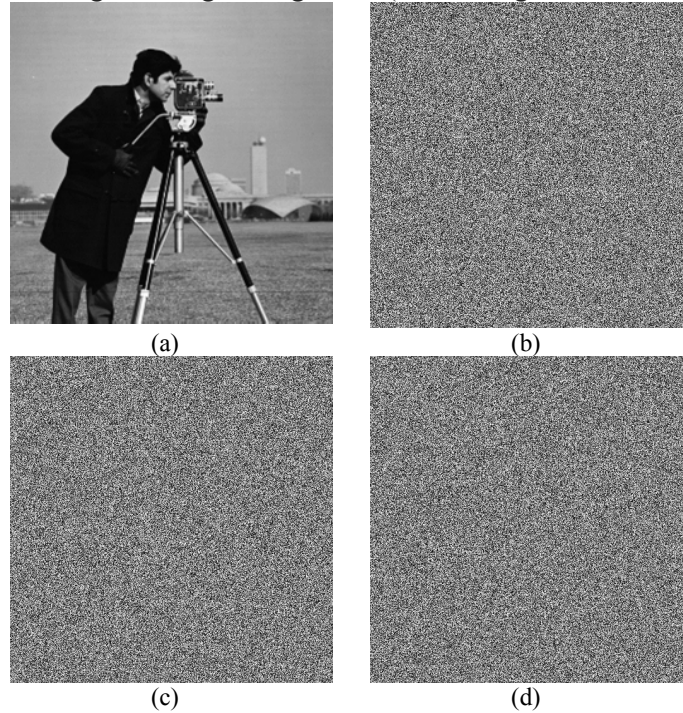


Figure 3. Cammea Man Image (a), Encrypted image - Key = AYL8DJH59HGSYD4 (b), Encrypted image - Key = AYL8DJH59RGSYD4 (c), Difference between Fig 3b and Fig 3c (d)

4.5 Information entropy

Randomness is the most striking feature of entropy. Information entropy is a mathematic theory for data communication and storage which was introduced by Claude E Shannon in 1949.

One of the most well-known formula to calculate the entropy is as follows:

$$H(S) = \sum_{i=0}^{2^N-1} P(s_i) \log\left(\frac{1}{P(s_i)}\right) \quad (11)$$

Where, N is equal to the number of grayscale level used in image (equal to 256 in 8-bit images) and $P(s_i)$ indicates the probability of occurrence of a grayscale level in the image. This value is equal to 8 in fully randomly generated images; this is considered as the ideal value. The closer the obtained entropy value to 8 using a method, the less the predictability of this method, hence more security in this method. In the proposed algorithm, the entropy values obtained for the images have been presented in figure 4. The highest entropy value for 8 different images can be observed in table 4. Among which, the maximum entropy is 7.9996 belonging to pepper image.

4.6 Evaluation of NPCR and UACI criteria

These criteria can be used to examine the effect of changing one pixel in the original image on encrypted image. NPCR can be defined as pixel change rate in encrypted images against changing a pixel in the original image. In addition, UACI can be calculated as the average of these changes according to relation (11, 12).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (12)$$









$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%$$

Where, H and W respectively designate the image length and width and C_1 and C_2 are two encrypted images taken from two images with a difference of 1 pixel and D is defined as below:

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{otherwise} \end{cases} \quad (13)$$

As can be seen in table 4, these values are too high for the proposed method. Meaning that, changing 4 pixel in the input image causes larger variations in the output image.

Table 4. Results of NPCR, UACI, and Entropy using the proposed method

256 × 256								
NPCR	0.9961	0.9969	0.9970	0.9956	0.9949	0.9962	0.9971	0.9957
UACI	0.3291	0.3408	0.3393	0.3311	0.3222	0.3386	0.3403	0.3382
Entropy	7.9963	7.9996	7.9987	7.9974	7.9956	7.9989	7.9991	7.9985

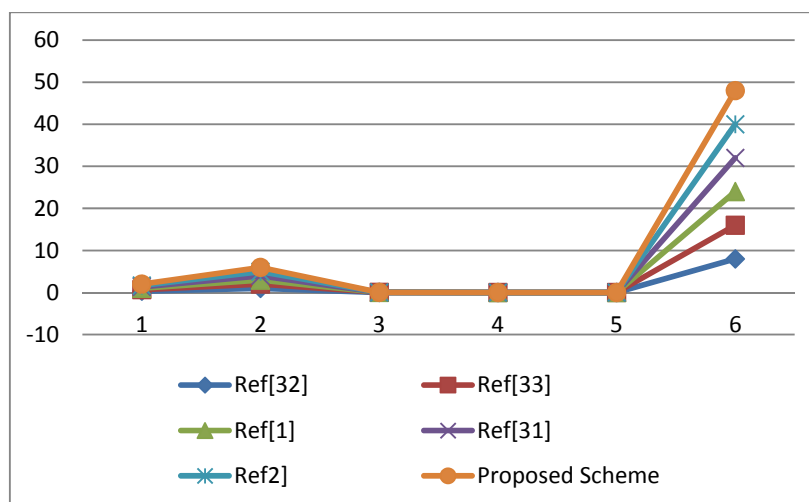
4.7 Comparison

To evaluate the method proposed in this study, the performance of this method was compared with references [1, 2, 31, 32, 33] using Pepper image and the results have

been demonstrated in table 5. The results indicate that the proposed method has high security and strength.

Table 5. Comparison of performance of the proposed method with other methods

	Entropy	Correlation coefficient			NPCR	UCAI
		Vertical	Horizontal	Diagonal		
Chaos and bit level permutation [32]	7.9993	0.0009	0.0020	0.0016	0.996273	0.334815
Chaos [33]	7.9994	-0.0023	0.0007	0.0149	0.996427	0.335615
Chaos and GA[1]	7.9978	0.0093	-0.0054	-0.0009	0.971394	0.331084
Total Shuffling scheme [31]	7.9975	0.0038	0.0009	-0.0002	0.996253	0.334758
Chaos and WDICA [2]	7.9996	-0.0009	0.0008	0.0001	0.996837	0.335735
Lattice map and DNA	7.9996	0.0019	0.0011	0.0073	0.996900	0.336110



Graph 2. Comparison of performance of the proposed method with other methods

5. Conclusion

DNA-based image encryption is one of the newest and most successful encryption methods. Since features like sensitivity to the initial and randomized value are the inherent characteristics of chaos systems, the chaos-based image encryption methods appear to be suitable for high-security encryption. In this study, a new, robust, and highly secure method has been suggested for image encryption using combination of lattice map function and DNA for more complexity of the encryption algorithm.

Evaluation of the encrypted images indicate that the histogram is very uniform, the correlation between the pixels is reduced and the entropy is equal to 7.9996. In addition, the proposed algorithm also benefits from the large space of the key and the high security, and especially the high execution speed.

References

- [1] Abdul Hanan Abdullah, Rasul Enayatifar, Malrey Lee, "A hybrid genetic algorithm and chaotic function model for image encryption", *Int. J. Electron. Commun. (AEÜ)* 66, 2012

- [2] Rasul Enayatifar a,n, Abdul Hanan Abdullah a, Malrey Lee.” A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption”, *Optics and Lasers in Engineering* 51,2013
- [3] Rasul Enayatifar,AbdulHananAbdullah n, IsmailFauziIsnin,”Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence”,*OpticsandLasersinEngineering*56,2014
- [4] Hossein Javedani Sadaei, RasulEnayatifar,Abdul Hanan Abdullah,Ismail FauziIsnin, Image Encryption Using a Synchronous Ayman Altameem,Malrey Lee,” *Permutation-Diffusion Technique*”,2017
- [5] Zhang Ying-Qiana,b, Wang Xing-Yuana,*,” A new image encryption algorithm based on non-adjacent coupled map lattices”, *Applied Soft Computing* 26 ,2015
- [6] Q.V. Lawande,B. R. Ivan and S. D. Dhodapkar,” *CHAOS Chaos Based Cryptography : A New Approach to Secure Communications*”, No. 258 July 2005
- [7] Hongxing Yao , Meng Li,” *An Approach of Image Hiding and Encryption Based on a New Hyper-chaotic System*”, *International Journal of Nonlinear Science* Vol.72009
- [8] Zhu Z-l, Zhang W, Wong K-W, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inform Sci* 2011
- [9] Wang Y, Wong K-W, Liao X, Chen G. A new chaos-based fast image encryption algorithm. *Appl Soft Comput* 2011
- [10] Abdullah AH, Enayatifar R, Lee M. A hybrid genetic algorithm and chaotic function model for image encryption. *AEU: Int J Electron Commun* 2012
- [11] Zhang G, Liu Q. A novel image encryption method based on total shuffling scheme. *Opt Commun* 2011
- [12] M. Amin, O. S. Faragallah, A. A. Abd El-Latif, “A chaotic block cipher algorithm for image cryptosystems”,*ELSEVIER, Commun Nonlinear Sci Number Simulat*,2010
- [13] W. Xing-Yuan, C. Feng, W. Tian, “A new compound mode of confusion and diffusion for block encryption of image based on chaos”, *ELSEVIER, Commun Nonlinear Sci Number Simulat*,2010
- [14] J. Jin, "An image encryption based on elementary cellular automata," *Optics and Lasers in Engineering*,Elsevier, Vol. 50, No. 12, pp. 1836-1843, 2012
- [15] A. Abdo, S. Lian, I. Ismail, M. Amin, and H. Diab,"A cryptosystem based on elementary cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, Elsevier, Vol. 18, No. 1,pp. 136-147, 2013
- [16] G. W. Reitwiesner, “Binaryarithmetic”, in *Advances in Computers*, Academic Press New York, vol. 1,1960
- [17] M. P. Leong, O. Y. H. Cheung, K. H. Tsoi and P. H. W. Leong, "A bit-serial implementation of the international data encryption algorithm IDEA", in the proceedings of *Field-Programmable Custom Computing Machines*, IEEE,2000
- [18] S. Fluthrer, I. Mantin and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, *SAC2001* (S. Vaudenay, A. Youssef,eds.), col. 2259 of LNCS, springer-Verlag,2001
- [19] M. Zehgid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, “ A Modified AES Based Algorithm for Image Encryption” in *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 1,2007

- [20] M. Kolhekar and A. Jadhav, "Implementation of Elliptic Curve Cryptography on Text and Image" in *International Journal of Enterprise Computing and Business Systems*, vol. 1, no. 2, 2011
- [21] R. Rhouma, S. Belghith, Cryptanalysis of a new image encryption algorithm based on hyper-chaos, *Physics Letters A*, 372 (2008) 5973-5978.
- [22] M. E. Hodeish and Dr. V. T. Humbe, "State-of-the-Art Visual Cryptography Schemes", in *International Journal of Electronics Communication and Computer Engineering*, vol. 5, no. 2, 2014
- [23] P. V. Chavan, Dr. M. Atique and Dr. L. Malik, "Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares", in *International Journal of Network Security & Its Applications*, vol. 6, no. 1, 2014
- [24] A. Cilaro, L. Coppolino, N. Mazzocca and L. Romano, "Elliptic Curve Cryptography Engineering", *IEEE*, vol. 94, no. 2, 2006
- [25] M. Amara and A. Siad, "Elliptic Curve Cryptography and its Applications" in 7th International workshop on Systems, Signal Processing and their applications (WOSSPA), 2011
- [26] V. Alikkal, Dr. T. S. Prakash and A. Hussain, "Enhanced Hierarchical Design for Visual Cryptography-Overview", in *International Journal on Engineering Technology and Sciences*, vol. 2, no. 4, 2015
- [27] <http://chettinadtech.ac.in/storage/12-09-01/12-09-01-15-19-28-1569-mrajendiranece.pdf>
- [28] N. K. Pareek, V. Patidar and K. K. Sud, "Discrete chaotic cryptography using external key", in *Physics Letters A*, vol. 309, 2003
- [29] M. Francois, T. Grosjes, D. Barchiesi and R. Erra, "A New Image Encryption Scheme Based on Chaotic Function" in *Signal Processing-Image Communication Elsevier*, 2011
- [30] G. Hanchinamani and L. Kulkarni, "An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher" in 3D Research Center, Kwangwoon University and Springer-Verlag Berlin Heidelberg, DOI 10.1007/s13319-015-0062-7, 2015
- [31] Zhang G, Liu Q. "A novel image encryption method based on total shuffling scheme". *OptCommun*, 2011
- [32] Zhu Z-l, Zhang W, Wong K-w, Yu H. "A chaos-based symmetric image encryption scheme using a bit-level permutation", *InfSci* 2011; 181:1171-86.
- [33] ang Y, Wong K-W, Liao X, Chen G., A new chaos-based fast image encryption Algorithm, *Apply Soft Comput*, 2011
- [34] Adleman, "Molecular Computation of Solutions of Combinatorial Problems," *Science*, 1994
- [35] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A Novel Color Image Encryption Algorithm based on DNA Sequence Operation and Hyper-Chaotic System," *Journal of Systems and Software*, 2012
- [36] Q. Zhang, L. Guo, and X. Wei, "Image Encryption using DNA Addition Combining with Chaotic Maps," *Journal of Mathematical and Computer Modelling*, 2010