Journal of Medical Systems (2019) 43: 267
https://doi.org/10.1007/s10916-019-1389-z

IMAGE & SIGNAL PROCESSING

Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences (NL4DLM_DNA)

Shalini Stalin[1] · Priti Maheshwary[1] · Piyush Kumar Shukla[2] · Manish Maheshwari[3] · Bhupesh Gour[4] · Ankur Khare[5]

Received: 20 March 2019 / Accepted: 14 June 2019 / Published online: 4 July 2019

Abstract

This paper proposes an innovative image cryptosystem algorithm using the properties of the block encryption, 4D logistic map and DNA systems. Multiple key sequences are generated and pixel substitution is performed by using nonlinear 4D logistic map, then encryption is performed by using DNA rules to ensure that the different blocks are encrypted securely. The results of the experiment indicate that the proposed Non Linear 4D Logistic Map and DNA (NL4DLM_DNA) sequence based algorithm gives better performance, which is analyzed on the basis of security, quality, attack resilience, diffusion and running time as compared to some previous works.

Keywords Logistic map · DNA rules · Image encryption · Pixel substitution · Diffusion

Introduction

The Internet and Multimedia Technology are growing continuously day by day. So an exchange of secure and confidential information in the form of text, image, audio and video between people becomes a major issue [1]. Maximum portion of information is covered by the image which is secured by different chaotic based encryption algorithm. Several traditional algorithms like Diffie Hellman, Rivest Shamir Adleman (RSA), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) are developed for encryption, but they frequently cannot be directly used for encryption of images to obtain reasonable results because of a few fundamental characteristics of images such as huge data capability, sturdy correlation and maximum redundancy. The original image is also alienated into small blocks for encryption so every block of the image is independent from each other and encrypted separately to enhance the security [2]. It creates the confusion and diffusion in the mind of attackers because an insignificant adjustment in pixels of the unique image or a parameter of key sequences provides a completely different cipher image. Several authors are

This article is part of the Topical Collection on *Image & Signal Processing*

✉ Shalini Stalin
shalini.stalin@yahoo.com

Priti Maheshwary
pritimaheshwary@gmail.com

Piyush Kumar Shukla
pphdwss@gmail.com

Manish Maheshwari
mcuprof.manish@gmail.com

Bhupesh Gour
bhupesh_gour@rediffmail.com

Ankur Khare
khareankur94@gmail.com

[1] Department of Computer Science and Engineering, Rabindranath Tagore University, Chiklod Road, Near Bangrasia Square, Dist., Raisen 464993, India

[2] Department of Computer Science and Engineering, University Institute of Technology, RGPV, Bhopal 462023, India

[3] Department of Computer Application, MCNUJC, Bhopal, India

[4] Department of Computer Science and Engineering, LNCTS, Bhopal, India

[5] Department of Computer Science, IEHE, Chunabahtti, near Kaliyashot Dam, Bhopal, India

provided their own way to solve the problems arising in image encryption by using different logistic maps and encryption methods [1, 3]. In contrast, A Chaotic logistic scheme is a nonlinear dynamic organization which is taking a part in fast and secure encryption of text and image.

Chaotic systems have various characteristics like highly perceptive of initial state, pseudorandomness and unpredictability, so they are widely used for image encryption by utilizing the pseudorandom number generation, permutation and diffusion. 1D (one dimensional) chaotic logistic systems are easily implemented for image encryption with few parameters. On the other hand, 1D logistic map [4] uses single variable, easy chaotic orbits and structures, so it is easy to evaluate the orbits and to envisage the primary values by small information extraction [5]. Hence, 2D (Two Dimensional) logistic systems [6] have been utilized to improve the security by using two variables for real time image encryption. The complexity of 2D chaotic system is further increased by using sine and cosine 2D logistic map, obtaining good diffusion on the basis of plain text and keys. 2D Arnold cat map and 3D (Three Dimensional) logistic map is combined to form 3D cat map which performs the image encryption based on permutation and diffusion [7]. The hyper chaotic logistic systems are combined into two or more positive Lyapunov exponents to enhance the randomness of key generation. Hyper chaotic systems are more dynamic and random than general logistic system, so they obtained good results with high confusion and diffusion [3].

Generally, most of the researchers are performed pixel or bit level image encryption. However, rapid growth of Bioinformatics, DNA (Deoxyribo Nucleic Acid) [4] based image encryption schemes are introduced utilizing the advantages of DNA such as enormous parallelism, vast storage and small energy consumption. The encoding, operations and decoding on the basis of DNA are performed one by one for DNA based image encryption. Firstly, the image bit streams are replaced by DNA sequences based on encoding rules to perform DNA encoding [6]. After that, some operation like addition, exclusive OR (XOR) and subtraction are applied on DNA sequences by utilizing the chaotic logistic sequences. At last outputs of DNA operations are converted into bits based on encoding rules. The pseudo random number and DNA computation are merged to perform fast encryption, but it is not robust against noise attack [8]. The 2D logistic system is also combined with DNA to obtain highly sensitive and effective results of an image encryption [6]. Though, the two performance parameters such as NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) still need to be enhanced [5].

Analyzing the above study, We proposed a new Non Linear 4D Logistic Map and DNA (NL4DLM_DNA) sequence based algorithm to enhance the performance and security of image encryption. Particularly, the proposed NL4DLM_DNA is performed in six steps: (1) Firstly the plain image is alienated into several blocks; (2) NL4DLM is applied to obtain the chaotic logistic sequences for image encryption; (3) Pixel substitution is carried out on pixels of each block of image to acquire the binary bit sequences according to chaotic logistic maps; (4) the image bit sequence and chaotic logistic sequence are converted into DNA sequences based on DNA encoding rules; (5) Several DNA operations such as addition, complement and subtraction is applied on DNA sequences of both image bits and chaotic logistic sequences to improve the security; (6) The image and chaotic logistic DNA sequences are decoded into bit sequences and XOR operation is performed among them, followed by bit to pixel decoding according to DNA encoding rules to obtain an encrypted image. The main objectives of this research are four aspects: (1) Proposed NL4DLM_DNA utilizes a non linear 4D logistic map rather than simple linear logistic map using in most existing literature; (2) it is proposed an easy but effective pixel substitution based on logistic sequences; (3) DNA operations are performed at several times on both image and chaotic logistic sequences to enhance the security of image encryption; (4) comprehensive experiments express that the NL4DLM_DNA is capable for image encryption. The originality of this research is threefold: (1) it is a high-quality effort to amalgamate non linear 4D logistic map and DNA computing to improve the security of image encryption; (2) the easy pixel substitution can extend the small modification in single pixel to entire pixels; (3) various DNA operations applied several times at different levels can additionally enhance the security.

The paper is prepared as follows: Literature review is analyzed in Sec. 2, epigrammatic explanation of the non linear 4D logistic map and DNA convention is described in Sec. 3. In Sec. 4, we establish the proposed NL4DLM_DNA method in detail. In Sec. 5, the experimental results are discussed to explain the efficiency of the proposed algorithm on the basis of some parameters. The whole work is concluded in Sec. 6.

Literature review

CBM (Chaotic Baker map) and DRPE (Double Random Phase Encoding) are combined to offer two layers optical image encryption. First layer is worked on chaotic Baker map for pre-processing and second layer is utilized by classical DRPE [9]. Digital logic circuits have increased the speed of encryption using the quality of the chaotic scheme to create confusion and diffusion in the algorithm. The vagueness and security of the proposed scheme are analyzed against the cryptanalysis attacks [10]. A classic bi-modular system is combined the features of confusion and diffusion to perform image encryption using the chaotic systems based on

Table 1 Comparison Table

Performance Factor Author	Security	Key Size	Attacks Resiliency	Used Technology	Speed	Limitations
Ankur Khare et al. [10]	High	Small	Cryptanalytic Attacks	Digital Logic	High	Not work on image encryption
Bhaskar Mondal et al. [31]	Average	Large	Statistical & Differential	DNA Computing	Average	Not provide attack resiliency
Hegui Zhu et al. [17]	High	Large	Chosen Plain text and Differential	CDCS	High	Pixel position scrambling is discarded
Hongye Niu et al. [32]	High	Very Large	Statistical & Differential	DNA Computing	High	Not as robust against noise attack
Lars Keuninckx et al. [33]	Average	Large	Brute Force	Nonlinear System	Average	NPCR and UACI have not their maximum values
Lingfeng Liu et al. [20]	Average	Medium	Differential	Dynamic	High	Not provided small changes
Maricela Jiménez-Rodríguez et al. [34]	High	Large	Statistical	Chaotic Synchronization	Average	Not provide key sensitivity
Muhammad Usama et al. [22]	High	Large	Cryptanalysis	PWLM	High	Not applied on colored images
Omar Reyad et al. [23]	Average	Medium	Statistical & Differential	C-D ECPRNG	Average	Most of the digits are not changed during encryption
Shu-Ying Wang et al. [28]	Average	Large	Anti Interference	Laser Chaotic Synchronization	Average	Not support hyperchaotic
Guodong Ye et al. [7]	Average	Medium	Statistical and Drifferential	SHA-3 and ECG	Average	Not support color images
Ye Tian et al. [4]	High	Large	Noise and statistical attack	IESDNA	High	Not support hyperchaotic
Fayza Elamrawy et al. [6]	High	Large	Differential Attacks	2D DNA	High	Not as robust against noise attack
Shuliang Sun [5]	Average	Large	Statistical attacks	2D SIMM	Average	Not support color images

PWLCM (Perturbed Piecewise Linear Chaotic Map). PWLCM based chaotic encryption system is introduced to real time applications in secure WiFi and Zigbee networks to improve the efficiency, speed and security of a cryptosystem. It uses very large keys and low memory spaces [11–13]. Two techniques for image encryption pseudo random number (PRN) and Deoxyribo Nucleic Acid (DNA) computation are combined to give a secure and high performance outputs. This technique is analyzed against the statistical and differential attacks. DNA encoded diffused image is providing confusion using spatiotemporal chaotic system [8].

Authentication and security in distributed networks are very important factors now a day. Lin introduces a mobile authentication scheme using chaotic map to identify the vulnerabilities and improve the scalability [14, 15]. Powerful function and tangent function are mainly combined with a chaotic algorithm to perform a fast and secure encryption to conquer the shortcoming of one dimensional chaotic cryptosystem like weak security and small key space [16]. A new 2-D (dimensional) based CDCS (composite discrete chaotic system) is introduced which combines the characteristics of more than one disconnected chaos based scheme. PLD (pixel level diffusion) and BLP (Bit level permutation) are used to enhance the complexity and performance speed [17]. Hardware realization with fast throughput is achieved by using high dimensional chaotic image encryption for real time applications. Fixed point arithmetic for 32 bit precision representation is used to enhance the security under quantization and statistical attacks [18]. Hybrid hyper chaotic key stream generates by mixing two hyper chaotic orbit sequences with the help of ordinary differential equation system than two times diffusion is applied to generate the final encryption keys. These key sequences are adequate to ensure the protection adjacent to brute force attack and performance of the

Table 2 DNA Convention Rules

Rules	Rule1	Rule2	Rule3	Rule4	Rule5	Rule6	Rule7	Rule8
00	A	A	G	G	T	T	C	C
01	C	G	A	T	C	G	A	T
10	G	C	T	A	G	C	T	A
11	T	T	C	C	A	A	G	G

Table 3 DNA Addition

++	C = 00	T = 01	A = 10	G = 11
C = 00	C	T	A	G
T = 01	T	A	G	C
A = 10	A	G	C	T
G = 11	G	C	T	A

Table 5 DNA XOR

⊗⊗	C = 00	T = 01	A = 10	G = 11
C = 00	C	T	A	G
T = 01	T	C	G	A
A = 10	A	G	C	T
G = 11	G	A	T	C

algorithm is analyzed under the factor correlation coefficient, entropy, key sensitivity and differential attacks [19, 20].

A novel image encryption scheme is introduced in photonic, optoelectronic or electronic platforms with the help of chaotic synchronizer to improve the robustness of systems. Rossler oscillator synchronizes the chaotic phase masks and parametric values like integrity, confidentiality and security are calculated at least errors. Synchronized fractional order chaotic systems explore the elevated protection, uniformity, reliability and viability for digital data encryption in real world applications [21]. Data compression and encryption are implemented on PWLCM and TM (Tent Map) developing on Hadoop platforms. The eminence of image encryption is achieved by improving the robustness, security, speed and compression of algorithm [22]. C-D ECPRNG (Chaos-Driven Elliptic Curve Pseudo-Random Number Generator) [23] is an improved form of elliptic curve public key cryptosystem combining the algebraic characteristics of ECPRNG and CPRNG to improve the performance of an image encryption scheme in multimedia systems [23]. A number of chaotic, based encryption algorithms [1] are developed in a wired and wireless environment to achieve the higher security, encryption speed and throughput and low power consumption overcomes the limitations of existing traditional techniques [24, 25]. The color image is encrypted by chaotic cryptosystem based on CTPNCM (Coupled Two-dimensional Piecewise Nonlinear Chaotic Map) [26] using masking techniques to ensure the resistance of the system against plain text attacks. Arnold cat map and laser chaos synchronization based digital image encryption algorithm is introduced in which pixel standards of the original image is developed the encryption keys. This algorithm has characteristics of higher security, flexibility, controllability and the good anti jamming effect [27, 28].

A clatter music file is developed the true arbitrary number stream which is combined with a KTP (Knight's travel path) [29] for data (text & image) encryption to provide a higher degree of confidentiality. Multiple chaotic systems are combined for image cryptosystem by means of self-motivated sequences created by several one-dimension chaotic maps. Statistical, differential and entropy attacks are resisting by this method of encryption. A FOHCS (fractional order hyper chaotic system) [30] is also performed encryption of color images and protection of the algorithm is explained by means of the correlation coefficient, histogram, key sensitivity and large key space [2, 29]. A new 4D chaos based scheme for digital data encryption [3] is introduced in the real time communication environment to enhance the performance with good efficiency and high security. The research papers of different authors are analyzed and compared in tabular form (Table 1).

Table 4 DNA Subtraction

–	C = 00	T = 01	A = 10	G = 11
C = 00	C	G	A	T
T = 01	T	C	G	A
A = 10	A	T	C	G
G = 11	G	A	T	C

Preliminaries

Non linear 4D logistic map (NL4DLM) system

The 4D Logistic Map exists in nonlinear systems having complex and unpredictable dynamical behavior with more than one positive Lyapunov exponents. The randomness, uncertainty and larger key space are greatly enhanced in 4D logistic system to provide higher security and efficiency as compared to 1D chaotic system. We espouse a 4D Logistic system that is dogged by the subsequent nonlinear equations (eq. 1):

$$\begin{cases} \ddot{X}_1 = \sigma(X_2 - X_1) + \ \theta_1 X_4 - X_3 \\ \ddot{X}_2 = \rho X_1 - X_1 X_3 + X_4 \\ \ddot{X}_3 = -\lambda X_3 + X_1 X_2 + \theta_2 X_2 \\ \ddot{X}_4 = -\psi X_1 + X_1 X_4 \end{cases} \tag{1}$$

Where σ, ρ, λ, ψ, θ_1, and θ_2 are the control parameters of the logistic system. We set the parameters as $\sigma = 35$, $\rho = 35$, $\lambda =$

Table 6 DNA Complement

DNA	Complement
C = 00	G = 11
T = 01	A = 10
A = 10	T = 01
G = 11	C = 00

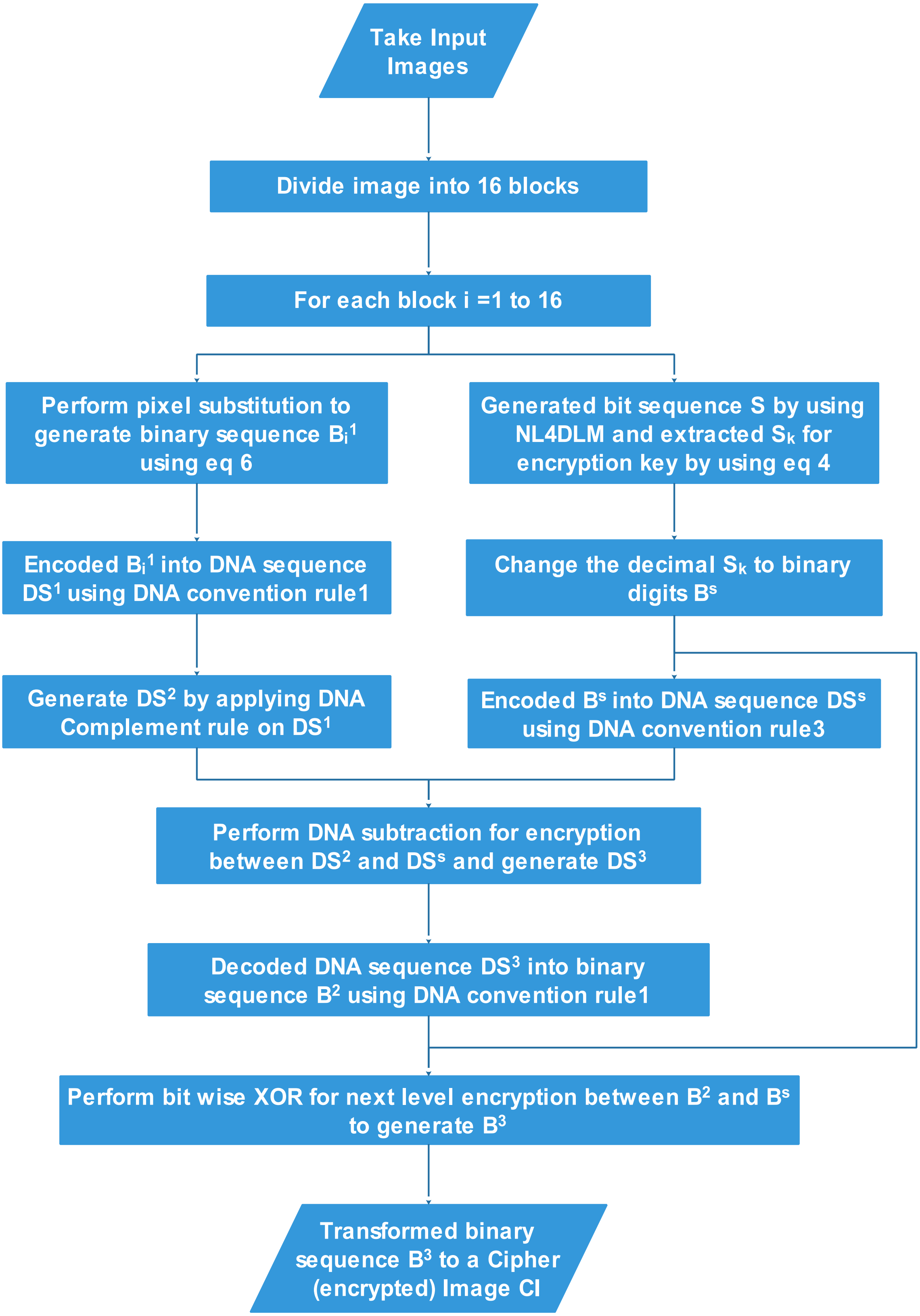

Take Input Images
Divide image into 16 blocks
For each block i =1 to 16
Perform pixel substitution to generate binary sequence B_i^1 using eq 6
Generated bit sequence S by using NL4DLM and extracted S_k for encryption key by using eq 4
Encoded B_i^1 into DNA sequence DS^1 using DNA convention rule1
Change the decimal S_k to binary digits B^s
Generate DS^2 by applying DNA Complement rule on DS^1
Encoded B^s into DNA sequence DS^s using DNA convention rule3
Perform DNA subtraction for encryption between DS^2 and DS^s and generate DS^3
Decoded DNA sequence DS^3 into binary sequence B^2 using DNA convention rule1
Perform bit wise XOR for next level encryption between B^2 and B^s to generate B^3
Transformed binary sequence B^3 to a Cipher (encrypted) Image CI

Fig. 1 Flow Chart of Proposed NL4DLM_DNA system

3, ψ= 5, θ_1= 1, and θ_2=0.3 and initialize the values of X_1=0.14, X_2=0.25, X_3=0.36, and X_4=0.47.

DNA (Deoxyribo Nucleic Acid) convention

A DNA is prepared from 4 nucleic acid bases specifically; ‘A’ (Adenine), ‘C’ (Cytosine), ‘G’ (Guanine) and ‘T’ (Thymine) where ‘A’ and ‘T’ are complements and ‘C’ and ‘G’ are complements. Since 0 and 1 are also complemented in the binary representation. If 00, 01, 10 and 11 are encoded by four bases ‘A’, ‘C’, ‘G’, and ‘T’ then we can obtain 24 types of coding rules in which only 8 types of rules assure the Watson-Crick complement rule in Table 2. Every 8-bit pixel significant of the image can be articulated as a four length DNA sequence it means bit sequence “10,110,100” is represented as “GACT” by using encoding rule5 and as “AGTC” by using encoding rule8. Hence, the output will absolutely different if any other DNA convention rules are utilized to encode the same binary bit sequences.

In DNA Convention, the DNA addition, subtraction, XOR and complement are deliberated according to the usual binary operations listed in Tables 3, 4, 5 and 6.

Block image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA)

Preprocessing of plain image

Devoid of failure of generalization, suppose that the dimension of the original plain-image P is a $U \times V$ with the range from 0 to 255 of pixel values. P is alienated into $u \times v$ blocks, the dimension of every block is $U/u \times V/v$ (U, V is multiple of u, v respectively). Every block is represented as matrix u X v.

Non linear 4D logistic sequence generation

Non Linear 4D logistic systems have better statistical characteristics and pseudorandomness. It helps us to obtain highly secure pseudorandom sequence discussed in Sec 3.1. The logistic sequence generation contains following steps:

1. The NL4DLM system (eq. 1) is firstly repeated N times to enhance the security and remove the adverse effects. After that, the system is repeated another u × v times. It uses m to represent the repetition index. In each repetition m, four status values $\{X_1^m, X_2^m, X_3^m, X_4^m\}$ have been obtained via fourth-order Runge-Kutta scheme with step size 0.001.
2. During repetition, each status value X_l^m is used to create several 8 bit key values $(K_l^a)^m \in [0, 255]$ and $(K_l^b)^m \in [0, 255]$, (l =1,2,3,4). They are evaluated by eq. 2 & 3.

$$\left(K_l^a\right)^m = \mathrm{mod}\left\{\left\lceil {}^{\left[\left(\lceil |X_l^m| \rceil - |X_l^m|\right)\times 10^{14}\right]}\Big/_{10^7} \right\rceil, 256\right\} \tag{2}$$

$$\left(K_l^b\right)^m = \mathrm{mod}\left\{\left\lceil {}^{\left[\left(|X_l^m| - \lfloor |X_l^m| \rfloor\right)\times 10^{14}\right]}\Big/_{10^7} \right\rceil, 256\right\} \tag{3}$$

Where mod (•) indicates the modulo operation, | • | indicates absolute value,⌊•⌋ indicates flooring operation, and ⌈•⌉ indicates the ceiling operation.

After the complete repetition, logistic sequences are combined with Eq. (5) to obtain S (set of several 8 bit keys) in eq. (4),

$$S = [S_i] = \left[K^1, K^2, K^3, \ldots\ldots\ldots\ldots., K^{u\times v}\right] \tag{4}$$

Where $i \in [1, 8uv]$ and

$$K^m = \left[\left(K_1^a\right)^m, \left(K_2^a\right)^m, \left(K_3^a\right)^m, \left(K_4^a\right)^m, \left(K_1^b\right)^m, \left(K_2^b\right)^m, \left(K_3^b\right)^m, \left(K_4^b\right)^m\right] \tag{5}$$

Where $m = 1, 2, 3, \ldots\ldots\ldots\ldots\ldots, u \times v$.

Pixel substitution

An input image P is alienated into $u \times v$ blocks, the dimension of every block is $U/u \times V/v$ (U, V is multiple of u, v respectively). Each block is with value in the range of [0, 255] has eight bits which are twisted bit by bit in instructing to diminish the correlation between adjoining pixels. Firstly, The pixel substitution is applied to each block of images by the converting pixel value as 8 bit binary digits to create 1D binary sequence$B^0$and chaotic logistic sequence S is precised in ascending order to obtain the index sequence S^x. After that, the binary sequence $B^0$is jumbled to be a 1D binary sequence B_i^1 according to the index sequence $S^x$by using eq. 6.

$$B_i^1 = B_{S_i^x}^0 \tag{6}$$

Where $i \in [1, 8uv]$

Table 7 Testing Images

Images	Size
Lena	256 X 256
Cameraman	256 X 256
Circuit	280 X 272
Peppers	512 X 512
Humanbrain	248 X 200
Aerial	364 X 368

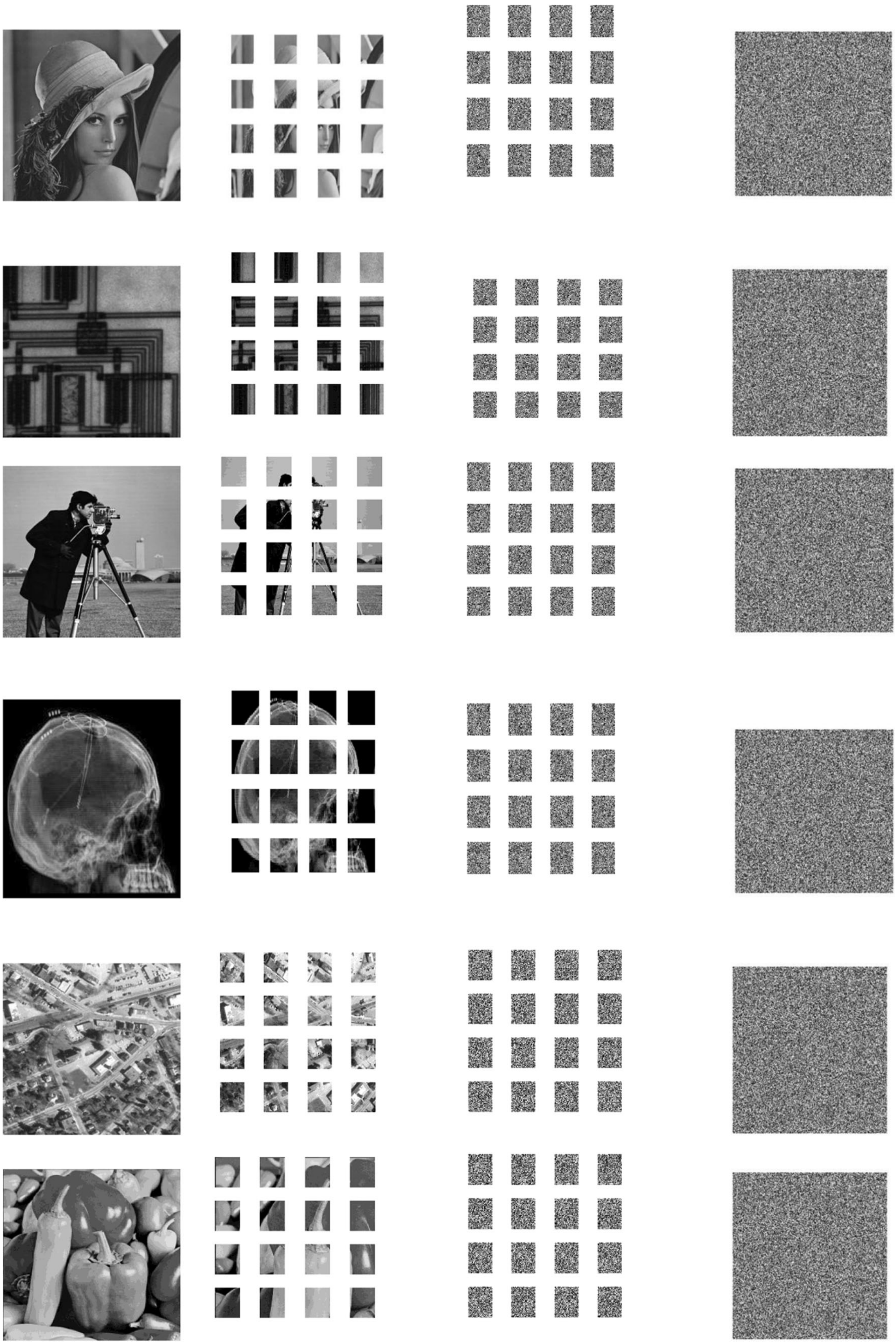


Fig. 2 Encrypted Images of Lena, Circuit, cameraman, Humanbrain, Aerial and Peppers. First Column is Plain Images, Second is Block Dividation of images, Third is encrypted blocks of images and forth is fully encrypted images

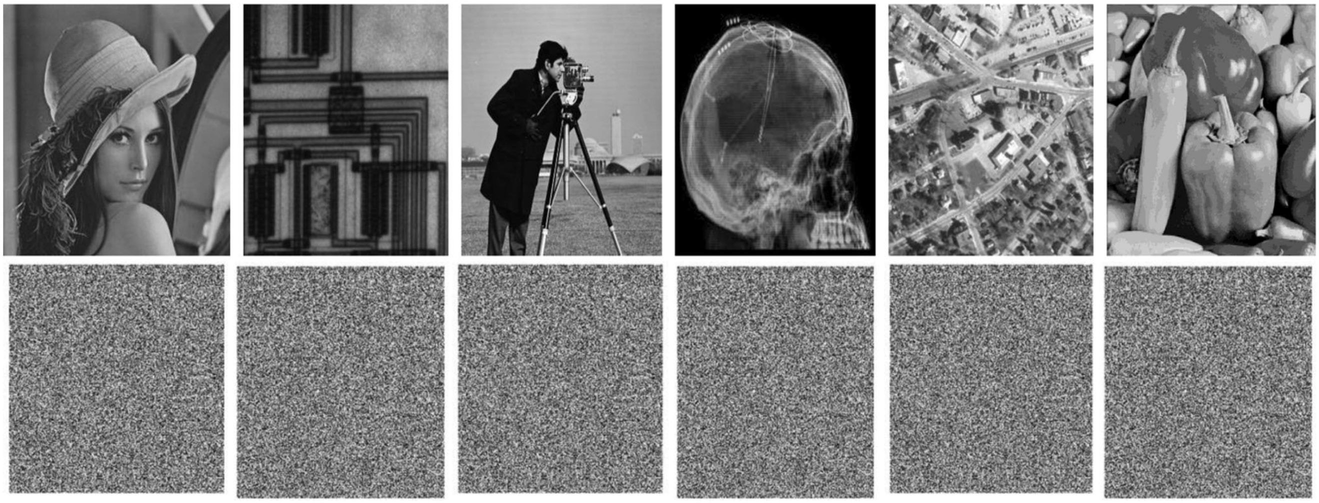


Fig. 3 Decrypted images of Lena, Circuit, Cameraman, Humanbrain, Aerial, and Peppers

Block image encryption

The block image encryption system is explained in following steps and shown in Fig. 1.

Step 1: Let u × v denotes the size of each block in which the image P is divided. As shown in Sec. 4.1, pixel substitution is performed on each block of image P one by one to acquire the bit binary sequenceB_i^1 for every block of the image.

Step 2: First DNA coding rule (see Table 2) is used to encode binary sequenceB_i^1 of image block into a DNA sequenceDS^1. The DNA Complement (see Table 6) on each element of DS^1 is calculated to generateDS^2.

Step 3: A sequence $S^k = [S_1, S_2, S_3, \ldots\ldots\ldots\ldots, S_{uv}]$is extracted from S for the encryption key, and the decimal S^k is changed to binary digitsB^s. Third DNA coding rule (see Table 2) is used to encode B^s into a DNA sequenceDS^s. The DNA subtraction between DS^2andDS^s is applied for encryption to generate a sequence DS^3.

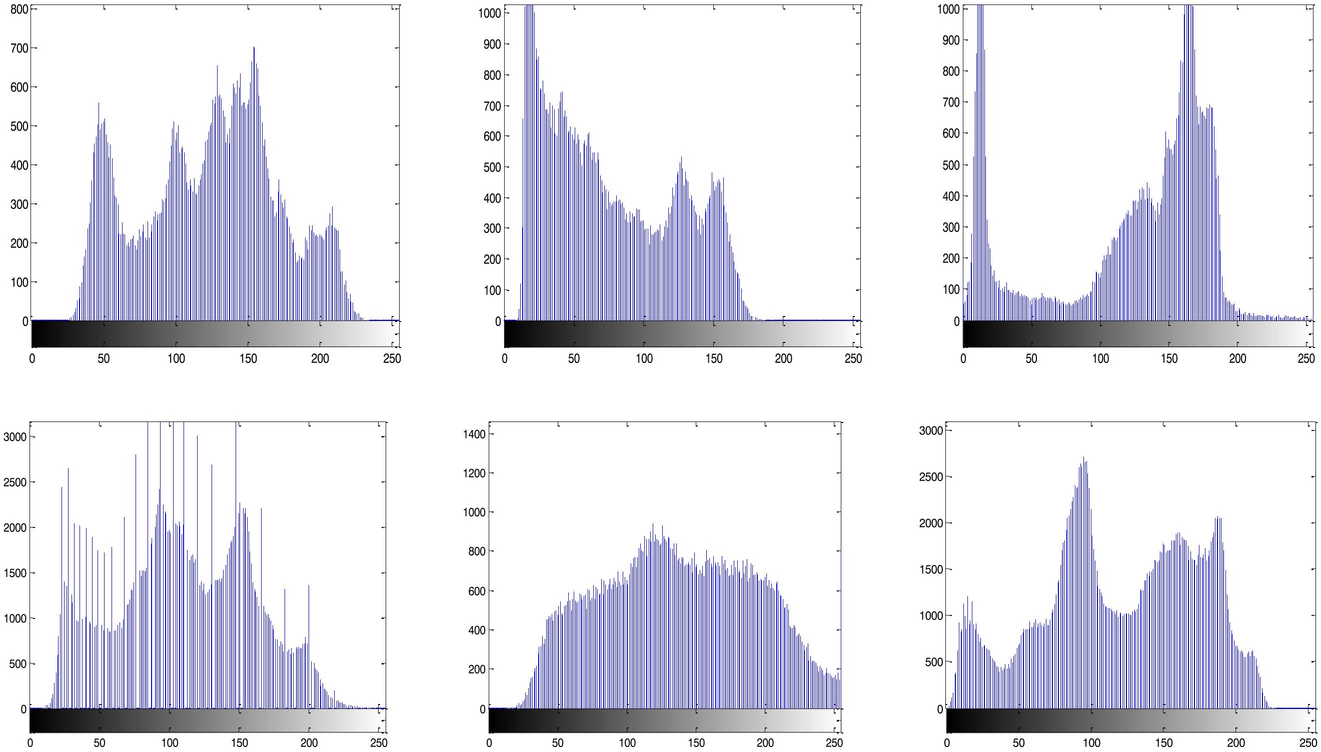


Fig. 4 Histograms of Lena, Circuit, Cameraman, Humanbrain, Aerial, and Peppers images respectively

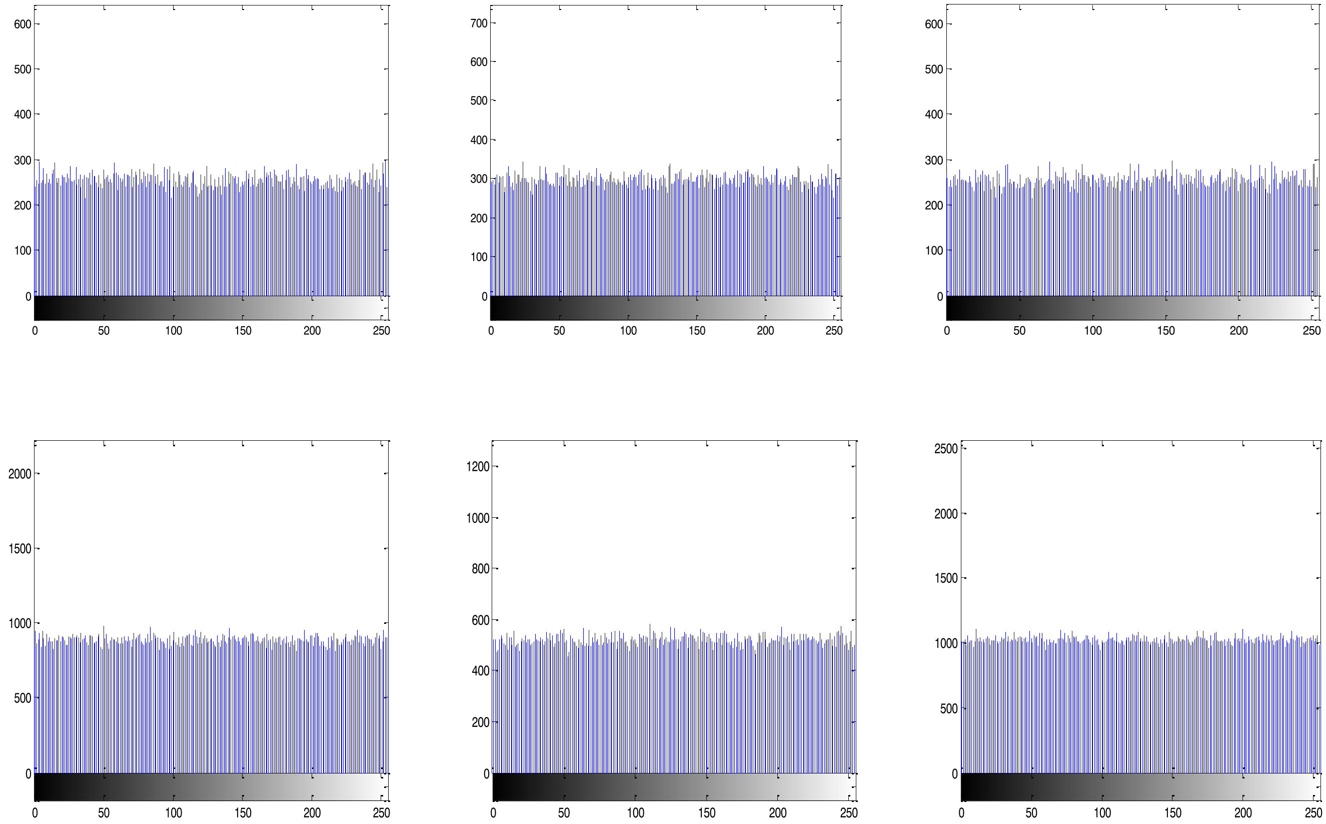


Fig. 5 Histograms of encrypted Lena, Circuit, Cameraman, Humanbrain, Aerial, and Peppers images respectively

Step 4: The DNA sequenceDS^3 is decoded into a binary sequenceB^2 by using first DNA coding rule.
Step 5: Bitwise XOR is applied for next level encryption between B^2 and B^s to generate the cipher binary sequenceB^3.
Step 6: The binary sequence $B^3$is transformed to a cipher (encrypted) image CI.

The decryption system is same as encryption in a reverse direction.

Case study of proposed NL4DLM_DNA

We set the parameters as $\sigma = 35$, ρ= 35, λ= 3, ψ= 5, θ_1= 1, and θ_2=0.3 and initialize the values of X_1=0.14, X_2=0.25, X_3=0.36, and X_4=0.47.

Step1: The image of Lena (256 X 256) is divided into 16 blocks (size of 64 X 64). We explain the encryption of only first block and the same process is performed on other blocks of image.
Step 2: The NL4DLM system (eq. 1) is firstly repeated 1000 times. After that, the system is further repeated 64 X 64 = 4096 (block size) (m = 4096) times for a single block of the image. In each repetition, a set of 4 values $\{X_1, X_2, X_3, X_4\}$has been evaluated and each value is converted into two key values $K^a$and $K^b$by using eq. 2 & eq. 3.

Example For m = 1 (first repetition), evaluated values of $\{X_1, X_2, X_3, X_4\}$= {−3.5551, −1.6464, 41.8318, 5.3350}.

Table 8 NPCR (%) Comparison

Images	NL4DLM_DNA	Xiaojun Tong et al. [2]	Xia Huang et al. [1]	Guodong Ye et al. [7]	Ye Tian et al. [4]
Lena	99.64	99.37	99.6013	99.6277	99.62
Circuit	99.64	99.49	99.6123	99.574	99.58
Cameraman	99.61	99.47	99.654	99.5837	99.61
Humanbrain	99.68	99.384	99.64	99.603	99.58
Aerial	99.71	99.54	99.684	99.6743	99.60
Peppers	99.69	99.467	99.656	99.5934	99.57

Table 9 UACI (%) Comparison

Images	NL4DLM_DNA	Xiaojun Tong et al. [2]	Xia Huang et al. [1]	Guodong Ye et al. [7]	Ye Tian et al. [4]
Lena	33.63	33.45	33.41	33.3961	33.61
Circuit	33.58	33.47	33.46	33.40	33.25
Cameraman	33.493	33.46	33.45	33.48	33.59
Humanbrain	33.488	33.457	33.487	33.37	33.59
Aerial	33.59	33.419	33.435	33.40	33.57
Peppers	33.58	33.28	33.439	33.4245	33.49

Then calculated key values $\{X_1\} = \left\{K_1^a, K_1^b\right\}$ = {24, 134}, $\{X_2\} = \left\{K_2^a, K_2^b\right\}$ = {149, 164}, $\{X_3\} = \left\{K_3^a, K_3^b\right\}$ = {36, 99}, & $\{X_4\} = \left\{K_4^a, K_4^b\right\}$ = {43, 15}.

These values are combined to form a set of 8 key values (K) using eq. 5.

$K = \left\{K_1^a, K_2^a, K_3^a, K_4^a, K_1^b, K_2^b, K_3^b, K_4^b\right\}$ = {24, 149, 36, 43, 134, 164, 99, 15}.

For m = 2, 3, 4,..............., 4096, the process is repeated and a set of 8 key values (K) is obtained in each repetition and these values of K are combined to form set S (contains 4096 X 8 = 32,768 key values) by using eq. 4.

S = {24, 149, 36, 43, 134, 164, 99, 15, 198, 177, 123, 201, 62, 108, 31, 50, 220, 217,121, 88, 22, 111, 1, 201,...}

Step3: Pixel substitution is performed on each block 64 X 64 of image. Firstly, the pixel values of a block of the image are converted into 1D binary sequenceB^0(64 X 64 X 8 = 32,768 bits) and chaotic logistic sequence S is précised in ascending order to give the index sequence S^x. $B^0$is jumbled to binary sequenceB^1(32,768 bits) according to S^x.

B^0 = {10,000,111, 100,001,111,000,011,010,000,101,100,001,001,000,001,010,000.............................}

S^x= {88, 235, 400, 822, 1047, 1259, 1645, 2396, 2449, 2532, 2687, 2711, 3182, 3602, 3687, 3765, 3919, 5607, 6039, 6317, 6387, 6521, 6580, 6937, 7354,...}

B^1= {100,100,100,010,000,010,110,111,000,000,010,011,011,111,001,101,000,010............................}

Step4: $B^1$is converted into a DNA sequence DS^1(16,384 elements) using first coding rules (Table 2).

DS^1= {GCAGAGAAGTCTAAACATCTTATCAAG..}

DNA complement of $DS^1$is generated DS^2.

DS^2={CGTCTCTTCAGATTTGTAGAATAGTTC..}

Step5: A sequence extracted from S (4096 key values) for encryption and changed to binary digits (8 bits for each key value)B^s.

S = {24, 149, 36, 43, 134, 164, 99, 15, 198, 177, 123, 201, 62, 108, 31, 50, 220, 217,121, 88, 22, 111, 1, 201,...}

B^s = {0001100010 010101001001000010101110000110101001000110001 1....-.....................}

$B^s$is converted into a DNA sequence DS^susing third coding rule (Table 2).

DS^s= {CTACATTTCATCCAAGACTAAATCTACG...}

Table 10 Information Entropy Comparison

Images	Input Images	Cipher Image				
		NL4DLM_DNA	Guodong Ye et al. [7]	Ye Tian et al. [4]	Fayza Elamrawy et al. [6]	Shuliang Sun [5]
Lena	7.2278	7.9975	7.9974	7.9974	7.9972	7.9971
Circuit	7.2156	7.9983	7.9975	7.9972	7.9973	7.9967
Cameraman	7.1053	7.9976	7.9978	7.9975	7.9972	7.9971
Humanbrain	7.1734	7.9982	7.9970	7.9974	7.9957	7.9878
Aerial	7.7432	7.9991	7.9991	7.9973	7.9953	7.9873
Peppers	7.5932	7.9994	7.9993	7.9973	7.9970	7.9973

The DNA subtraction between $DS^2$and $DS^s$to generateDS^3.

$$DS^3 = DS^2 - DS^s$$

DS^3= {CAGCGGCCCCAATGGCGAACCGTGCGC……………………………………………}

Step6: $DS^3$is converted into a binary sequence $B^2$by using first DNA coding rule.

B^2 = {010010011010010101010000111010011000000101101110011001………………………}

Step7: Perform XOR between $B^2$and $B^s$to generate a binary sequenceB^3.

$$B^3 = B^2 \otimes B^s$$

B^3 = {0101000100110000011101001100001000000111110010100000001………………………}

Step8: the binary sequence is converted into pixel values which are transformed to a cipher (encrypted) image CI.

Experimental results

The subsequent experiments are performed on a processor (Intel core 2 duo), Windows XP operating system with 2 GB RAM, 2.7 GHz CPU in Matlab environment. NL4DLM_DNA is compared with a number of state-of-the-art schemes, such as the 3D logistic Map [7], and Chaotic Dynamic S-box and DNA sequence [4], 2D logistic map and DNA sequence [6], and DNA complements rules based encryption [5]. The parameters for these schemes are set as given by the authors. We put the parameters of the NL4DLM_DNA as follows. The initial values for the system are the repeating 픽=1000 times.

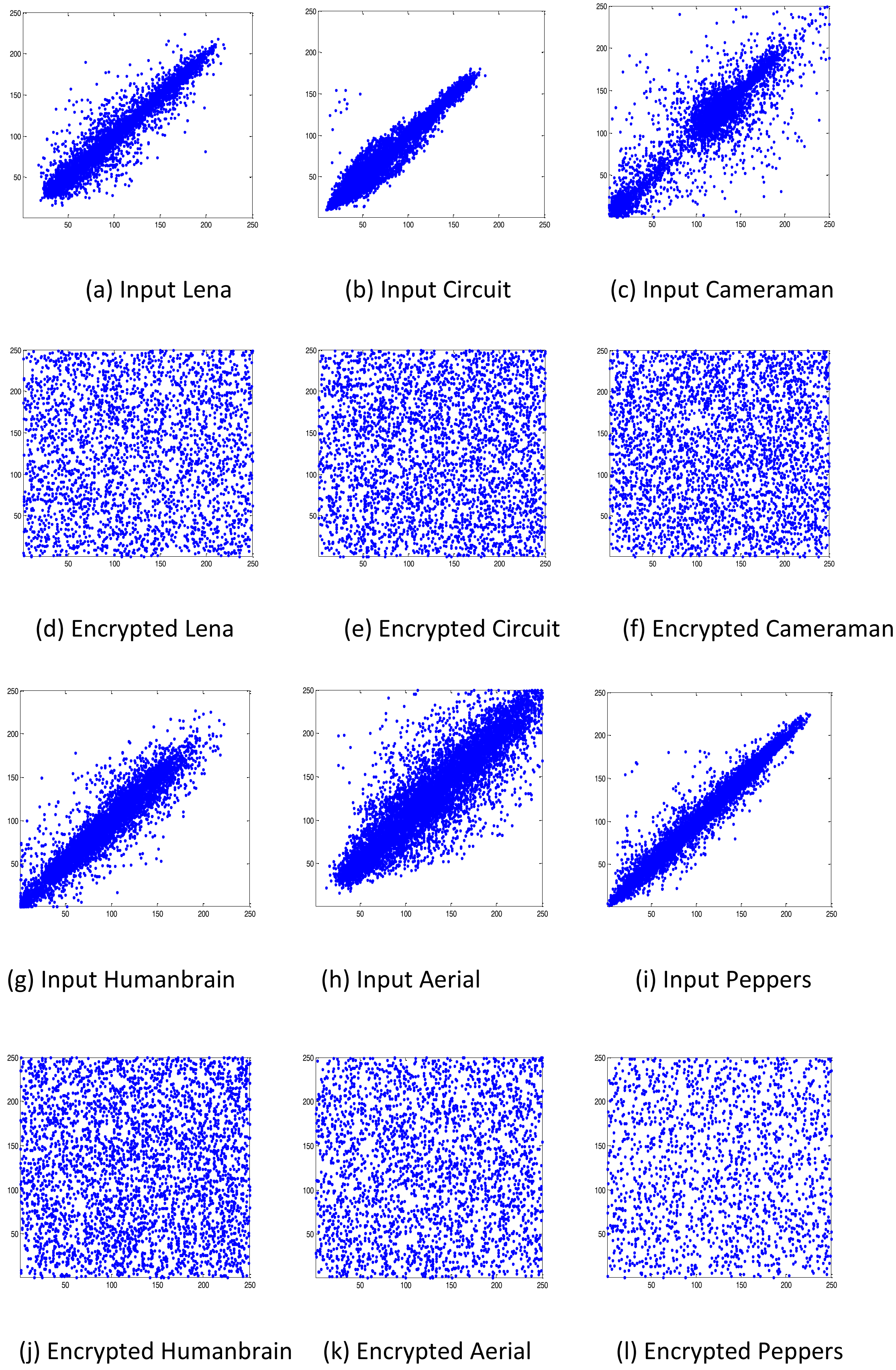
Six widely used images with same sizes are used to analysis NL4DLM_DNA, as given in Table 7.

Encryption test

The image of Lena of 256 X 256 is divided into 16 blocks of size of 64 X 64, the image of Cameraman of 256 X 256 is divided into 16 blocks of size of 64 X 64, the image of Circuit of 280 X 272 is divided into 16 blocks of size of 70 X 68, the image of Peppers of 512 X 512 is divided into 16 blocks of size of 128 X 128, the image of Humanbrain of 248 X 200 is divided into 16 blocks of size of 62 X 50, and the image of

Table 11 Correlation Coefficients Comparison

Images	γ	Input Image	Cipher Image				
			NL4DLM_DNA	Xia Huang et al. [1]	Ye Tian et al. [4]	Fayza Elamrawy et al. [6]	Shuliang Sun [5]
Lena	γ_v	0.9675	0.0031	0.0002	−0.0015	−0.0037	0.0021
	γ_h	0.9492	0.0052	−0.0157	−0.0010	0.0015	0.0013
	γ_d	0.9462	0.0019	0.0034	−0.0012	0.0079	−0.0024
Circuit	γ_v	0.9783	−0.0074	0.0043	−0.0003	0.0024	−0.0016
	γ_h	0.9765	0.0015	0.0020	−0.0016	−0.0014	−0.0014
	γ_d	0.9725	−0.0003	−0.0011	−0.0007	−0.0010	−0.0008
Cameraman	γ_v	0.9554	−0.0079	−0.0087	−0.0056	−0.00049	−0.0045
	γ_h	0.9328	−0.0010	0.0076	−0.0023	−0.0040	−0.0073
	γ_d	0.9231	0.0029	−0.0013	0.0048	0.0015	0.0010
Humanbrain	γ_v	0.9624	−0.0034	0.0008	−0.0039	0.0004	−0.0015
	γ_h	0.8387	0.0010	0.0011	−0.0028	0.0035	−0.0021
	γ_d	0.8421	0.0008	−0.0040	−0.0005	0.0008	0.0004
Aerial	γ_v	0.8787	−0.0026	0.0035	0.0010	−0.0042	0.0026
	γ_h	0.9086	0.0015	−0.0010	−0.0008	−0.0028	−0.0017
	γ_d	0.8479	−0.0014	0.0024	0.0030	−0.0016	−0.0012
Peppers	γ_v	0.9754	−0.0020	0.0042	−0.0013	0.0031	−0.0004
	γ_h	0.9834	−0.0008	0.0008	−0.0015	−0.0028	−0.0017
	γ_d	0.9642	−0.0013	0.0009	0.0016	0.0026	−0.0008



(a) Input Lena

(b) Input Circuit

(c) Input Cameraman

(d) Encrypted Lena

(e) Encrypted Circuit

(f) Encrypted Cameraman

(g) Input Humanbrain

(h) Input Aerial

(i) Input Peppers

(j) Encrypted Humanbrain

(k) Encrypted Aerial

(l) Encrypted Peppers

Fig. 6 The adjoining pixel allotment maps of the input images and equivalent encrypted images in straight direction

Table 12 Association of Chaotic Sequence Generation Time (Seconds)

Images	NL4DLM_DNA	Xiaojun Tong et al. [2]	Xia Huang et al. [1]	Guodong Ye et al. [7]	Ye Tian et al. [4]
Lena	0.2876	0.3419	3.1559	0.7834	1.2724
Circuit	0.3172	0.3682	3.324	0.7823	1.1287
Cameraman	0.297	0.34	3.154	0.8123	1.26
Humanbrain	0.30	0.32	3.245	0.8342	1.13
Aerial	0.2735	0.3172	3.292	0.8432	1.362
Peppers	0.2653	0.3352	3.725	0.910	1.432

Aerial of 364 X 368 is divided into 16 blocks of size of 91 X 92, shown in Fig. 2. Same operations are performed on all the images given in Table 7 and shown the fully encrypted images in Fig. 2.

Key protection analysis

A protected image encryption algorithm should be sensitive to the key sequences so small variations among the preliminary principles will escort towards the entirely different cipher-images.

In Fig. 3 first row represents the secret message images using the correct keys initial values $\{X_{10} = 0.13, X_{20} = 0.35, X_{30} = 0.57, X_{40} = 0.79\}$and second row represents the secret message images with incorrect keys initial values $\{X_{10} = 0.13 + 10^{-15}, X_{20} = 0.35, X_{30} = 0.57, X_{40} = 0.79\}$ respectively. Within malice of small differences between key sequences, images cannot decode the accurately. The high sensitivity of NL4DLM_DNA shows that it has adequate capability of resisting exhaustive attack.

Key length security

The key space is the combination of 4 initial values$\{X_{10} = 0.13, X_{20} = 0.35, X_{30} = 0.57, X_{40} = 0.79\}$. If the precision is 10^{-15} then the key length space is $10^{15X4} = 10^{60} \approx 2^{200}$ very large to provide resistance against the brute force attack [1].

Statistical attack (Histogram) examination

The encrypted images are publicized in the form of a histogram which is providing comparatively uniform pixel distribution to decrease the association among pixel value in Figs. 4 and 5. So the cipher images are not proficient to give any statistical data of the consequent input images, then NL4DLM_DNA provides resistance against statistical attacks efficiently.

Differential attack analysis

The attacker may search for a small variation of the plaintext and ciphertext to discover the association among the plaintext, key cipher text [2]. If a small alteration within the plain image be able to escort towards huge modification within cipher image, after that the technique can efficiently defend against these differential attacks [1]. Usually, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) [2] is usually put in use to analyze the potential for finding the defending against disparity hit [1]. The formulas are as follows in eq. 7 and 8.

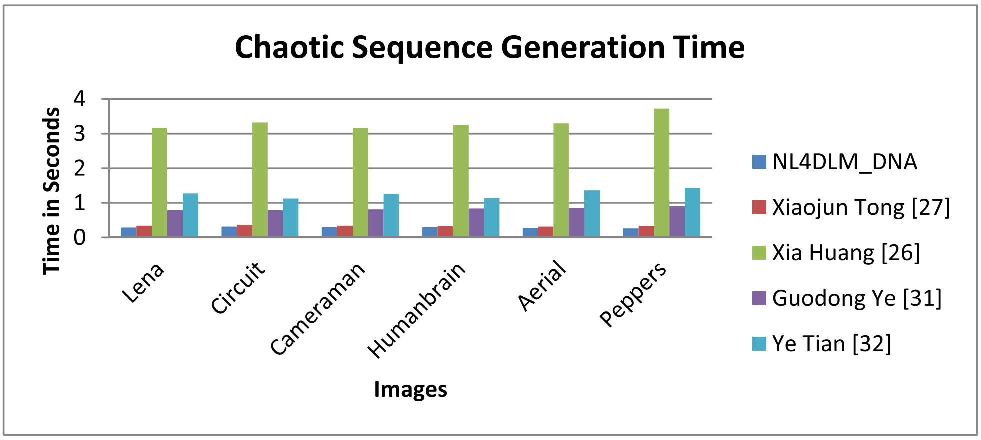


Fig. 7 Chaotic sequence generation time of Lena, Circuit, Cameraman, Humanbrain, Aerial, and Peppers images respectively

$$NPCR = \frac{\sum_{u,v} Di(u,v)}{Wi\ X\ Ht}\ X\ 100\% \quad (7)$$

$$UACI = \frac{1}{Wi\ X\ Ht}\left[\sum_{u,v}\frac{|CT_1(u,v)-CT_2(u,v)|}{255}\right] X\ 100\% \quad (8)$$

Here,

Wi The width of the image,
Ht Height of image,

$CT1\ (u, v)$ & $CT2\ (u, v)$ = Equivalent pixels of 2 images.

If $CT1(u, v) = CT2(u, v)$, then $Di(u, v) = 0$, otherwise $Di(u, v) = 1$.

The standard of UACI and NPCR are 33.46% and 99.61% respectively. The pixels are selected randomly from the equivalent cipher texts of a modified image in addition to the real image [2] which is generated by the planned technique. Approximately 500 examinations are analyzed in addition to equivalent ideals of NPCR and UACI are generated and average standards of NPCR and UACI can be calculated publicized in the Tables 8 and 9.

As of Tables 8 and 9, it can observe that the standards of NPCR and UACI are near to the principle standards and better to the previous systems [1, 2, 4–7]. It illustrates that single bit variation in real picture is capable of disperse for entire cipher image providing the resistance against differential attacks.

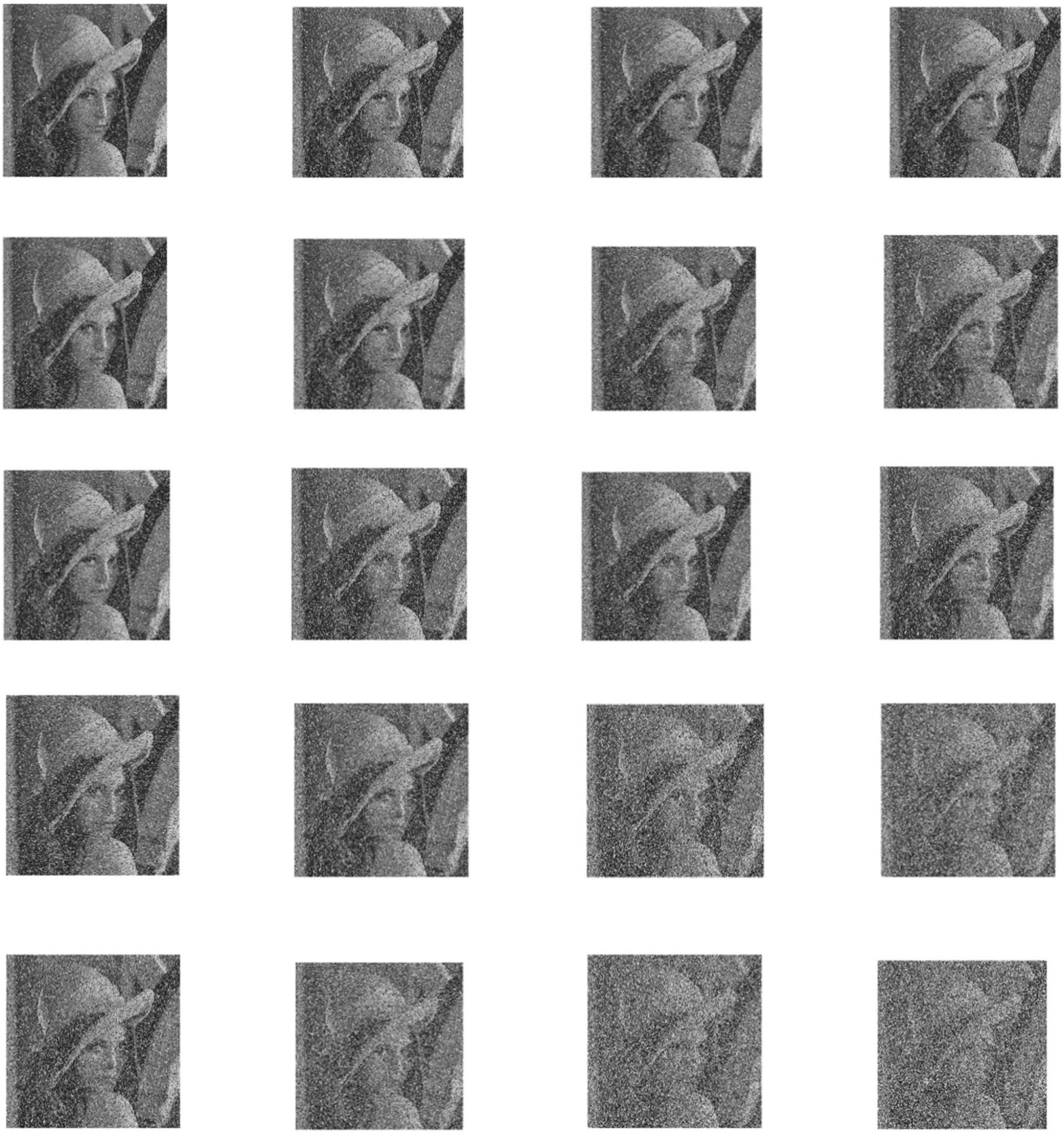


Fig. 8 Decrypted efficiency with exact key (introducing the salt and pepper noise to an encrypted image (Lena) from top to bottom with noise density from 0.05 to 0.25 with 0.05 intervals). From left to right column, the images are decrypted by NL4DLM_DNA, Fayza Elamrawy et al. [6], Shuliang Sun [5] and Guodong Ye et al. [7]

Information entropy analysis

Information entropy of image can determine the allocation and randomness of image gray standards by eq. (9). The system has higher security if an attacker can be generated only small information of original plain image from image gray standard distribution of the cipher image.

$$H = -\sum_{m=1}^{256} PR_m log\, PR_m \tag{9}$$

Here PR_m is the image gray standard probability.

The principal standard of the information entropy of cipher image is 8. The proposed scheme is obtained the information entropy of the complete cipher-image is shown in Table 10 which are very near to the principal standard of information entropy and give better performance compare to previous algorithms [4–7]. It shows that cipher image pixels are completely independent of each other for the cipher text attackers to ensure the difficulty for decrypting the cipher text.

Correlation analysis

Two adjoining pixels in an image frequently have high correlation. A high-quality image encryption scheme should be proficient of decreasing such correlation considerably. The formula of Correlation (eq. 10) coefficient 훼 is an admired metric as follows:

$$\begin{cases} \mu(X) = \frac{1}{N}\sum\limits_{l=1}^{N} X_l \\ \alpha(X) = \frac{1}{N}\sum\limits_{l=1}^{N} (X_l - \mu(X))^2 \\ \alpha(Y) = \frac{1}{N}\sum\limits_{l=1}^{N} (Y_l - \mu(Y))^2 \\ \mathrm{cov}(X, Y) = \frac{1}{N}\sum\limits_{l=1}^{N} (X_l - \mu(X))(Y_l - \mu(Y)) \\ \gamma = \frac{\mathrm{cov}(X, Y)}{\sqrt{\alpha(X)\alpha(Y)}} \end{cases} \tag{10}$$

Where X and Y are two adjoining pixel values in an image and N is the total number of pixels in the image. The correlation coefficients are evaluated in several directions (horizontal γ_h, verticalγ_v, and diagonalγ_d) and analyzed in several works [1, 4–6] in tabular form (Table 11).

Table 11 shows the proposed NL4DLM_DNA gives value of correlation coefficients nearly 0 for cipher image and nearly 1 for input image which represents that the cipher neighboring pixels are not correlated.

Correlation is further analyzed by arbitrarily selecting 4000 pairs of adjoining pixels in a straight direction from all the input images and equivalent encrypted images by NL4DLM_DNA respectively, to represent the adjoining pixel allotment maps in Fig. 6. It is observed that pixel values are allotted close to the diagonal of synchronize plane showing the strong correlation in the input images. Therefore NL4DLM_DNA is totally destroyed the correlation and pixel values are allotted over almost the complete plane representing the weak correlation in encrypted images.

Table 13 Decryption efficiency with exact key (introducing the salt and pepper noise)

Performance Factor	Density	NL4DLM_DNA	Fayza Elamrawy et al. [6]	Shuliang Sun [5]	Guodong Ye et al. [7]
NPCR (%)	0.05	0.2436	0.0637	0.1425	0.4367
	0.10	0.4326	0.1146	0.2738	0.5378
	0.15	0.5467	0.1747	0.3728	0.6187
	0.20	0.6598	0.2145	0.4837	0.6937
	0.25	0.7423	0.2745	0.5546	0.7436
UACI (%)	0.05	0.0435	0.0174	0.04027	0.1245
	0.10	0.0687	0.0342	0.08362	0.1645
	0.15	0.0836	0.0463	0.1193	0.1839
	0.20	0.1183	0.0601	0.1435	0.2046
	0.25	0.1345	0.0789	0.1637	0.2124
γ_h	0.05	0.6839	0.7352	0.5463	0.2047
	0.10	0.5326	0.6028	0.3245	0.1436
	0.15	0.4352	0.4839	0.2548	0.0926
	0.20	0.3212	0.3927	0.1536	0.0454
	0.25	0.2536	0.3182	0.1039	0.0317

Key sequence generation time

We generate 256 X 256 key sequences using the proposed algorithm and compare the running time with previous schemes [1, 2, 4–7], correspondingly and show in Table 12.

The Table 12 and Fig. 7 illustrates that the running time of the proposed algorithm is very small for generating the key sequences compared to other works [1, 2, 4, 7]. So proposed algorithm is highly efficient for image encryption with higher speed.

Strength against noise attack

Encrypted images are typically corrupted by noise in the communication. An accurate key is still capable to decrypt the encrypted images to the input images. Pixels of noise are nonignorablely effected the quality of decrypted images so it is necessary for image encryption technique to resist the noise attack to a definite level. Here, a salt and pepper noise is introduced to the encrypted images and outputs of the decryption process are represented in Fig. 8. The results are analyzed in terms of NPCR and UACI of Input Lena and decrypted Lena and straight (horizontal) direction $\gamma_h$of decrypted Lena and represented in Table 13. The universal characteristic of the image can be obviously illustrious, while the decrypted image becomes distorted.

Conclusion

An innovative image encryption algorithm is projected for the block cryptosystem based on non linear 4D logistic map and the DNA system in this paper. Multiple key sequences and pixel scrambling are obtained by using 4D logistic map, then encrypted by DNA rules and operations, not by binary operations to make surety that the different key sequences are encrypted multiple blocks of the image to increase the security. The length of the key is sufficiently large to provide resistance against several attacks like a brute force attack. The results illustrate that NL4DLM_DNA is obtained the higher protection, attack resiliency, and robustness against differential attacks and statistical attacks due to pixel substitution and nonlinear DNA operations. If any bit of the input image is modified, then NL4DLM_DNA gives better NPCR and UACI values as compared to other algorithms and performance of NL4DLM_DNA technique against noise attack is better than other algorithms. NL4DLM_DNA has minimum chaotic sequence generation time and value of entropy near to the ideal entropy value. In future, the performance of image encryption algorithm is enhanced to give better NPCR and UACI values in noise attack environment.

Compliance with ethical standards

Conflict of interest Shalini Stalin declares that she has no conflict of interest. Priti Maheshwari declares that she has no conflict of interest. Piyush Kumar Shukla declares that he has no conflict of interest. Manish Maheshwari declares that he has no conflict of interest. Bhupesh Gour declares that he has no conflict of interest. Ankur Khare declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Huang, X., Sun, T., Li, Y., and Liang, J., A color image encryption algorithm based on a fractional-order Hyperchaotic system. Entropy, MDPI 17:28–38, 2015. https://doi.org/10.3390/e17010028.
2. Tong, X., Yang, L., Zhang, M., Xu, H., and Zhu, W., An image encryption scheme based on Hyperchaotic Ra, binovich and exponential Chaos maps. Entropy, MDPI 17:181–196, 2015. https://doi.org/10.3390/e17010181.
3. Huang, X., A new digital image encryption algorithm based on 4D chaotic system. International Journal of Pure and Applied Mathematics 80(4):609–616, 2012.
4. Tian, Y., and Lu, Z., Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation. AIP Advances:1–23, 2017.
5. Sun, S., Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules. Optical Engineering 56(11):1–10, 2017.
6. Elamrawy, F., Sharkas, M., and Nasser, A. M., An image encryption based on DNA coding and 2DLogistic chaotic map. International Journal of Signal Processing 3:27–32, 2018.
7. Ye, G., Jiao, K., Pan, C., and Huang, X., An effective framework for chaotic image encryption based on 3D logistic map. Hindawi Security and Communication Networks:1–11, 2018. https://doi.org/10.1155/2018/8402578.
8. Song, C., and Qiao, Y., A novel image encryption algorithm based on DNA encoding and spatiotemporal Chaos. MDPI, Entropy 17:6954–6968, 2015. https://doi.org/10.3390/e17106954.
9. Elshamy, A. M., Rashed, A. N. Z., Mohamed, A. E.-N. A., Faragalla, O. S., Yi, M., Alshebeili, S. A., and Abd El-Samie, F. E., Optical image encryption based on chaotic baker map and double random phase encoding. Journal Of Lightwave Technology 31(15):2533–2539, 2013.
10. Khare, A., Shukla, P. K., Rizvi, M. A., and Stalin, S., An intelligent and fast chaotic encryption using digital logic circuits for ad-hoc and ubiquitous computing. Entropy, MDPI 18(201):1–27, 2016. https://doi.org/10.3390/e18050201.
11. D_asc_alescu, A. C., Boriga, R., and Mih_ailescu, M. I., A novel chaos-based image encryption scheme. Annals of the University of Craiova, Mathematics and Computer Science Series 41(1):47–58, 2014.
12. Bakhache, B., Ahmad, K., and Assad, S. E. I., Chaos based improvement of the security of ZigBee and Wi-fi networks used for industrial controls. IEEE:139–145, 2011.
13. Wang, X., and Chen, D., A parallel encryption algorithm based on piecewise linear chaotic map. Mathematical problems in engineering, Hindawi:1–8, 2013. https://doi.org/10.1155/2013/537934.
14. Haddush Fitwi, A., and Nouh, S., Performance analysis of chaotic encryption using a shared image as a key. Journal of EEA 28:17–29, 2011.

15. Guo, D., Wen, Q., Li, W., Zhang, H., and Jin, Z., Analysis and improvement of 'chaotic map based Mobile dynamic ID authenticated key agreement scheme. Wireless Pers Commun, springer science+business media New York:1–14, 2015. https://doi.org/10.1007/s11277-015-2378-2).
16. Gao, H., Zhang, Y., Liang, S., and Li, D., A new chaotic algorithm for image encryption. Chaos, Solitons and Fractals, Elsevier 29: 393–399, 2006. https://doi.org/10.1016/j.chaos.2005.08.110.
17. Zhu, H., Zhang, X., Yu, H., Zhao, C., and Zhu, Z., A novel image encryption scheme using the composite discrete chaotic system. Entropy , MDPI 18(276):1–27, 2016. https://doi.org/10.3390/e18080276.
18. Kwok, H. S., and Tang, W. K. S., A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons and Fractals, Elsevier 32:1518–1529, 2007. https://doi.org/10.1016/j.chaos.2005.11.090.
19. Junming, M., and Ruisong, Y., An image encryption scheme based on hybrid orbit of hyper-chaotic systems. I. J. Computer Network and Information Security, MECS (5):25–33, 2015. https://doi.org/10.5815/ijcnis.2015.05.04.
20. Liu, L., and Miao, S., A new image encryption algorithm based on logistic chaotic map with varying parameter. Springer Plus 5(289): 1–12, 2016. https://doi.org/10.1186/s40064-016-1959-1.
21. Ahmada, M., Shamsib, U., and Khan, I. R., An Enhanced Image Encryption Algorithm Using Fractional Chaotic Systems. Third International convention on Recent Trends in Computing, Procedia Computer Science, Elsevier 57:852–859, 2015. https://doi.org/10.1016/j.procs.2015.07.494.
22. Usama, M., and Zakaria, N., Chaos-based simultaneous compression and encryption for Hadoop. PLoS ONE 12(1):1–29, 2017. https://doi.org/10.1371/journal.pone.0168207.
23. Reyad, O., Kotulski, Z., and Abd-Elhafiez, W. M., Image encryption using Chaos-driven elliptic curve Pseudo-random number generators. Appl. Math. Inf. Sci. 10(4):1283–1292, 2016. https://doi.org/10.18576/amis/100407.
24. Shukla, P. K., Khare, A., Rizvi, M. A., Stalin, S., and Kumar, S., Applied cryptography using Chaos function for fast digital logic-based Systems in Ubiquitous Computing. Entropy, MDPI 17:1387 1410, 2015. https://doi.org/10.3390/e17031387.
25. Wei, X., Wang, B., Zhang, Q., and Che, C., Image encryption based on chaotic map and reversible integer wavelet transform. Journal of Electrical Engineering 65(2):90–96, 2014.
26. Seyed Mohammad Seyedzadeh and Sattar Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing, Elsevier, vol. 92, 1202–1215, 2012. doi:https://doi.org/10.1016/j.sigpro.2011.11.004
27. Soleymani, A., Nordin, M. J., and Sundararajan, E., A chaotic cryptosystem for images based on Henon and Arnold cat map. The scientific world journal, Hindawi:1–21, 2014. https://doi.org/10.1155/2014/536930.
28. Shu-Ying Wang, Jian-Feng Zhao, Xian-Feng Li and Li-Tao Zhang, Image blocking encryption algorithm based on laser Chaos synchronization, journal of electrical and computer engineering, Hindawi, pp-1-15, 2016.
29. Kumar, T. S., and Venkatesan, R., A new Image Encryption Method Based on Knight's Travel path and True random number. Journalof Information Science and Engineering 32:133–152, 2016.
30. Xing-yuan, W., and Qing, Y., A block encryption algorithm based on dynamic sequences of multiple chaotic systems. Communications in Nonlinear Science and Numerical Simulation, Elsevier 14:574–581, 2009. https://doi.org/10.1016/j.cnsns.2007.10.011.
31. Mondal, B., and Mandal, T., A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University, Computer and Information Sciences:1–6, 2016. https://doi.org/10.1016/j.jksuci.2016.02.003.
32. Niu, H., Zhou, C., Wang, B., Zheng, X., and Zhou, S., Splicing model and hyper–chaotic system for image encryption. Journal of Electrical Engineering 67(2):78–86, 2016. https://doi.org/10.1515/jee-2016-0012.
33. Keuninckx, L., Soriano, M. C., Fischer, I., Mirasso, C. R., Nguimdo, R. M., and Van der Sande, G., Encryption key distribution via chaos synchronization. Scientific Reports:1–14, 2017. https://doi.org/10.1038/srep43428.
34. Jiménez-Rodríguez, M., González-Novoa, M. G., Estrada-Gutiérrez, J. C., Acosta-Lúaa, C., and Flores-Siordia, O., Secure point-to-point communication using chaos. Universidad Nacional de Colombia, DYNA 83(197):180–186. June, 2016. https://doi.org/10.15446/dyna.v83n197.53506.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.