CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.178-187
https://doi.org/10.51537/chaos.1250317

Lossless Image Encryption using Robust Chaos-based Dynamic DNA Coding, XORing and Complementing

Vinod Patidar *,[1] **and Gurpreet Kaur** α,[2]

*School of Computer Science, University of Petroleum and Energy Studies (UPES), Bidholi, Dehradun-284007, India, αAmity Institute of Information Technology, Amity University, Noida-201303, UP, India.

ABSTRACT In this paper, we present a lossless image encryption algorithm utilizing robust chaos-based dynamic DNA coding and DNA operations (DNA XOR and DNA Complement). The entire process of encryption is controlled by the pseudo-random number sequences generated through a 1D robust chaos map that exhibits chaotic behaviour in a very large region of parameter space with no apparent periodic window and therefore possesses a fairly large key space. Due to peculiar feed-forward and feedback mechanisms, which modify the synthetic image (created to initiate the encryption process) at the encryption of each pixel, the proposed algorithm possesses extreme sensitivity to the plain image, cipher image and secret key. The performance analysis proves that the proposed algorithm exhibits excellent features (as expected from ideal image encryption algorithms) and is robust against various statistical and cryptanalytic attacks.

KEYWORDS
Image encryption
DNA encryption
DNA complementing
DNA XORing
Robust chaos

INTRODUCTION

The transmission of images/videos over the networks, and storage of such visual media in the cloud has become increasingly popular due to the proliferation of fast and efficient network technologies as well as the advancement, and miniaturization of computing devices and storage media. It has inevitably posed security threats/concerns for the image/visual media. Images can be securely transmitted and stored in encrypted form to safeguard them from unauthorized access. Since images have different characteristics (bulk data, high spatial correlation, redundancies) than text data, therefore, require special attention and algorithms to encrypt them or hide them from unauthorized uses.

In recent years a variety of image encryption technologies like image encryption based on optical transforms (Hennelly and Sheridan 2003; Kaur *et al.* 2022a,b), based on chaos theory(Patidar *et al.* 2011), DNA-based image encryption (Adleman 1994; Xiao *et al.* 2006; Gehani *et al.* 2004) and algorithms based on the amalgamation of these technologies have been developed. Amongst them, the chaos-based image encryption algorithms have been most successful due to effective confusion and diffusion as recommended by Shannon(Shannon 1949). However, chaos-based image encryptions do suffer from some limitations like floating number-based operations, the existence of periodic windows in parameter space and smaller key space etc. (Teh *et al.* 2020). In recent years DNA computing has also gained popularity due to its huge information-carrying capacity, parallelism and ultra-low energy consumption. Rather than implementing DNA computing at the molecular level (Adleman 1994) which requires highly restricted laboratory conditions, it has been frequently used to carry the digital information (through representing it in DNA sequences) and manipulate it using feasible DNA operations like addition, subtraction, DNA XOR, DNA XNOR, DNA Complement etc.(Xiao *et al.* 2006; Gehani *et al.* 2004).

The sole use of DNA coding and operations does not introduce nonlinearity in the process of information manipulation (scrambling and altering) since these operations are primarily linear therefore have not been very successful in fulfilling Shannon's (Shannon 1949) criteria for developing perfect secrecy in image encryption or steganography algorithms. However, the DNA encoding and corresponding operations are found to be successful when used in combination with the dynamical chaos, which is bounded, aperiodic behaviour having sensitivity to initial conditions/parameters and exhibited by deterministic nonlinear dynamical systems. Such techniques have been termed hybrid DNA-chaos-based image encryption.

Manuscript received: 12 February 2023,
Revised: 6 April 2023,
Accepted: 17 April 2023.

[1]vinod.patidar@ddn.upes.ac.in (**Corresponding author**).
[2]gurpreet.preeti82@gmail.com

In DNA-chaos-based image encryption, the images to be encrypted are transformed into DNA sequences and then the scrambling of DNA bases is executed with the help of dynamical chaos. These scrambled sequences are then encoded with the help of DNA operations under the influence of the chaotic dynamical system(s). Broadly classifying, there are two ways to design a hybrid DNA-Chaos-based encryption algorithm: fixed DNA and dynamic DNA coding (Xue *et al.* 2020). A fixed rule is used for encoding, decoding and DNA operations in a fixed DNA scheme (Zhang *et al.* 2014; Wang *et al.* 2015) whereas rules are dynamically selected for encoding, decoding and DNA operations in dynamic DNA coding (Chai *et al.* 2019; Dagadu *et al.* 2019; Wang *et al.* 2020). For a detailed review and comparison of various existing hybrid DNA-Chaos-based encryption algorithms, we refer the readers to a recent work by Patidar and Kaur (Patidar and Kaur 2023).

In this paper, we propose a novel dynamic DNA coding algorithm for image encryption. All the operations (DNA encoding, DNA-based-XOR, DNA-based-complement and DNA decoding) are used under the control of a robust chaos map whose dynamical behaviour is chaotic in very large parameter space (2 parameter space) with no apparent periodic window. All of the above factors contribute towards a larger key space, thereby eliminating the possibility of brute force attack. The robust chaos map is mainly used in the algorithm to generate some pseudo-random number sequences and the various DNA-based operations in encryption (encoding, XORing, Complementing and decoding) are dynamically selected with the help of these pseudo-random number sequences for each pixel.

All the pseudorandom number sequences are interdependent (as generated sequentially) as well as dependent on the secret keys therefore the algorithm possesses extreme key sensitivity. To start the encryption process, we create a synthetic image (of the same size as the plain image) with the help of the same robust chaos map and the pixels of the synthetic image are modified and used in the encryption of the corresponding pixel of the plain image. The process of modification of each pixel of the synthetic image involves the information from the plain image as well as the cipher image pixels generated till now and hence, is different for each pixel. This interdependency leads to extreme sensitivity concerning plain and cipher images and makes the entire process of encryption super complex.

The subsequent sections of this paper are structured as: In Section 2, we briefly introduce the robust chaos map, in Section 3, the DNA coding, XORing and Complementing. In Section 4 all the steps of the proposed image encryption algorithm are described, in Section 5, the results of the performance analysis of the proposed algorithm are presented and finally, in Section 6 the conclusions are drawn.

THE ROBUST CHAOS MAP

The robust chaos is defined as the absence of periodic windows and co-existing attractors in some neighbourhoods within the parameter space (Zeraoulia 2012). We use the following form of an iterative one-dimensional map in the proposed image encryption algorithm as the source of robust chaos (Andrecut and Ali 2001; Patidar 2022).

$$x_{n+1} = F(x_n, a, v), (F(x, a, v) = \frac{1 - v^{-ax(1-x)}}{1 - v^{-(\frac{a}{4})}} \forall v \neq 1, v > 0, a > 0) \quad (1)$$

Here x is the state variable, a and v are the parameters. This iterative map is an S-unimodal map and has a negative Schwarzian derivative. The function has a unique maximum at $x = 0.5$ (Figure 1), hence there can be at most one attracting periodic orbit with the critical point in its basin of attraction. The orbit with initial condition $x = 0.5$ will approach to x = 0 in two iterates. Since the point $x = 0$ will be unstable if

$$(F'(0, a, v) = |\frac{ln(v)a}{1 - v^{-(\frac{a}{4})}}| > 1 \forall v \neq 1, v > 0, a > 0) \quad (2)$$

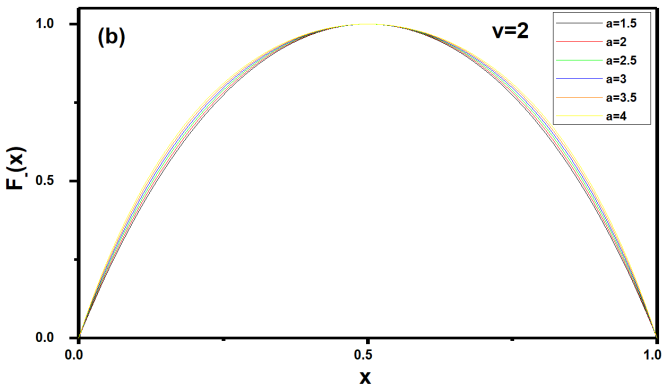

Figure 1 Function plots of robust chaos map maps (Eq.(1))

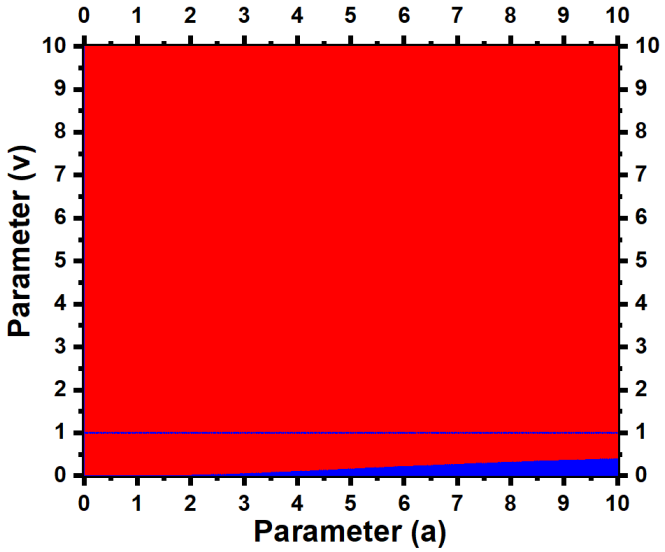

Figure 2 Derivative of the function F'(0,a,v), (Eq.2) red correspond to the positive value and blue corresponds to the negative value

In such a case, the map does not possess any stable periodic orbit hence a chaotic attractor/orbit prevails. In Figure 2, we have depicted the regions of the parameter space (a, v) where the derivative $F'(0,\ a, v)$ is positive and negative respectively through the red and blue colours. In the red region, the point x = 0 is unstable therefore the chaotic orbit may exist here. We have also plotted the bifurcation diagram for the robust chaotic map (Eq.1) by iterating the map for 5000 iterations and skipping the initial 500 iterations for (i) a fixed value of parameter $a = 7.1$ and varying v from 0 *to* 10 in the step of 0.01 and (ii) a fixed value of parameter $v = 4.3$ and varying a from 0 *to* 10 in the step of 0.01. The results have been depicted in Figure 3. We observe from the top frame

(for $a = 7.1$) that point $x = 0$ is stable up to $v = 0.25$ and then it becomes unstable and a chaotic orbit prevails. This fact may be verified with the quantitative results of the stability condition (Eq.2) depicted in Figure 2 and the Lyapunov exponent results depicted in Figure 4. In the bottom frame (for $v = 4.3$) of Figure 3, we observe that chaos is present for the entire range of parameter a which is also confirmed from the quantitative results of stability condition (Eq.2) depicted in Figure 2 and the Lyapunov exponent results depicted in Figure 4.

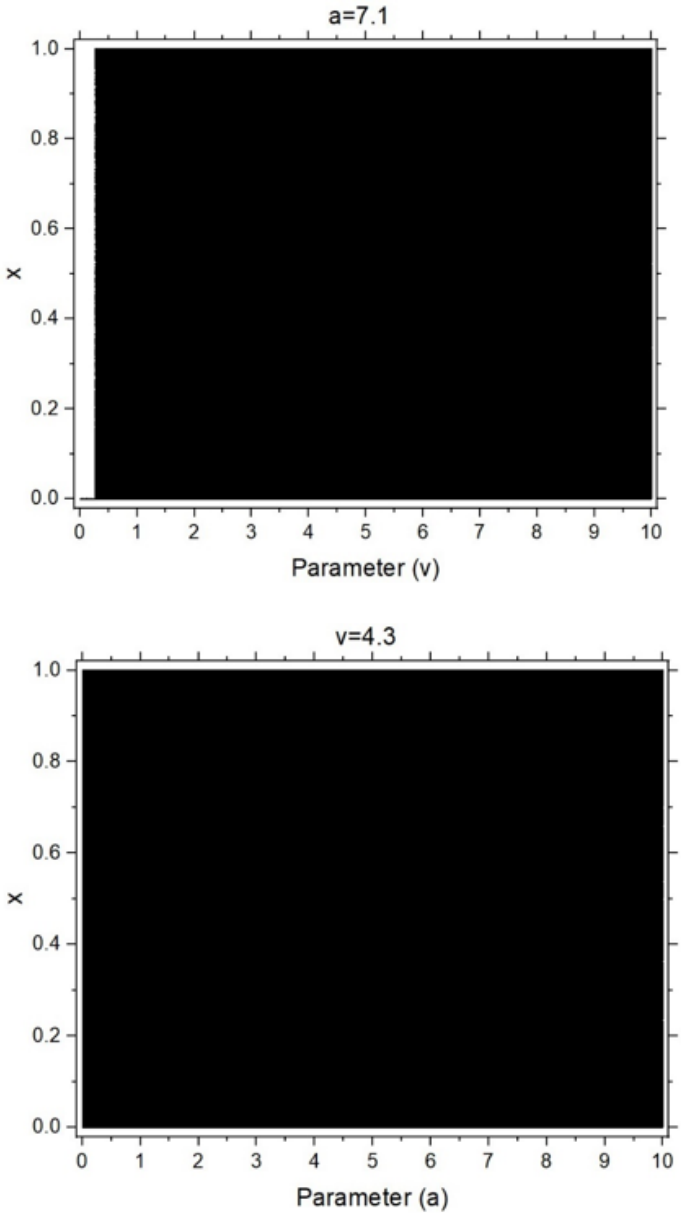

Figure 3 Bifurcation plot for the robust chaos map (Eq.(1)): Top frame for a=7.1 and bottom frame for v=4.3.

To confirm the existence of chaotic orbit and robust chaos, we have numerically computed the Lyapunov exponent for the above iterative map and the results are shown in Figure 4. It is clear that the Lyapunov exponent is positive in the entire parameter space (without any periodic window) defined by $v > 0, a > 0$ except for $v = 1$ and a very small region near $v = 0$. In the proposed image encryption algorithm, we use the above-mentioned iterated function in the parameter space defined by $v > 1, a > 1$ for generating the pseudorandom sequences.

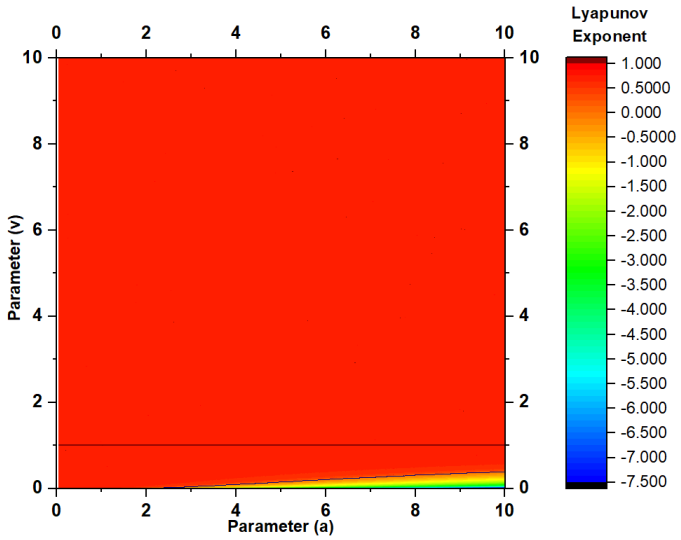

Figure 4 Lyapunov Exponent for the robust chaos map (1)

DNA CODING, XORING AND COMPLEMENTING

In DNA computing 4 nucleic acid bases: Adenine, Thymine, Cytosine and Guanine (A, T, C and G) are encoded as 00, 01, 10 and 11. There can be a total of 24 different possibilities for such coding out of them only eight comply with both the binary and DNA complement rules. In Table 1, we have summarized these eight rules (Wang *et al.* 2020). For each DNA rule, addition, subtraction and XOR operations can be formulated by following the conventional binary operations. Since in the present algorithm we are using XOR operation on DNA sequences therefore we are giving one such operation table (Table 2) for the XOR operation on DNA bases corresponding to the DNA encoding rule 3 (Wang *et al.* 2020).

The complement rules for the DNA sequences are defined based on the double helix structure of the DNA strand. If the complement operation is defined by the function $f_c(b_i)$ where b_i is one of the nucleic bases of DNA, then the following relation is satisfied:

$$b_i \neq f_c(b_i) \neq f_c\left(f_c\left(b_i\right)\right) \neq f_c\left(f_c\left(f_c\left(b_i\right)\right)\right)$$

$$b_i = f_c\left(f_c\left(f_c\left(f_c\left(b_i\right)\right)\right)\right)$$

According to the above-mentioned relation, there are six different complement base-pair relations (rules) possible. These are listed in Table 3 (Wang *et al.* 2020).

Rule 1, in Table 3, may be interpreted as follows:

$$f_c(A) = T;$$

$$f_c(f_c(A)) = f_c(T) = C$$

$$f_c\left(f_c\left(f_c(A)\right)\right) = f_c\left(f_c(T)\right) = f_c(C) = G$$

The $f_C(f_c(A))$ is the Level 2 complement of A that is equal to C as per the complement rule 1.

The recovery of the complement, for Rule 1, in Table 3, may be done in the following way:

Table 1 The Eight DNA Encoding Rules

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

Table 2 The XOR Operation (for DNA Encoding Rule 3)

$\oplus_{DNA}$	**A**	**T**	**C**	**G**
A	T	A	G	C
T	A	T	C	G
C	G	C	T	A
G	C	G	A	T

Table 3 Six DNA Complement Rules

Rule	Complement base pairs			
1	AT	TC	CG	GA
2	AT	TG	GC	CA
3	AC	CG	GT	TA
4	AC	CT	TG	GA
5	AG	GC	CT	TA
6	AG	GT	TC	CA

$$f_{cr}(A) = G;$$

$$f_{cr}(f_{cr}(A)) = f_{cr}(G) = C$$

$$f_{cr}\left(f_{cr}\left(f_{cr}(A)\right)\right) = f_{cr}\left(f_{cr}(G)\right) = f_{cr}(C) = T$$

The $f_{cr}\left(f_{cr}\left(f_{cr}(A)\right)\right)$ is the Level 3 complement recovery of A that is equal to T as per the complement rule 1.

THE PROPOSED ALGORITHM

Encryption Algorithm

In the proposed image encryption algorithm, the plain image is a grey image of dimension H × W and the secret key is a set of 15 floating-point numbers and one integer $(x_0, a_1, v_1, N, a_2, v_2, a_3, v_3, a_4, v_4, a_5, v_5, a_6, v_6, a_7, v_7)$. Here $0 < x_0 < 1$ and all $a > 1$, $v > 1$ and N is an integer preferably between 100 to 999.

1. Iterate the robust chaos map N times with the initial condition x_0 and parameters a_1, v_1 and throw the iterates and record the last value x_N for further use.
2. Iterate the robust chaos map HW times with the initial condition x_N and parameters a_1, v_1. These iterates are used to create a synthetic image (SI) of dimension H × W

   $SI(k) = \lfloor x_k \times 256 \rfloor$, k=1 to HW
3. A pseudo-random number sequence (PRS1) is generated having numbers 1 to 8 by iterating the robust chaos map with the initial condition x_{N+HW} and parameters a_2, v_2

   $$PRS1_i = \lfloor x_i \times 8 \rfloor + 1; i = 1 \; to \; HW$$
4. Step 3 is repeated with x_{N+2HW} and parameters a_3, v_3 to generate $PRS2_i$
5. Step 3 is repeated with x_{N+3HW} and parameters a_4, v_4 to generate $PRS3_i$

6. A pseudo-random number sequence (PRS4) is generated having numbers 1 to 6 by iterating the robust chaos map 4HW times with the initial condition x_{N+4HW} and parameters a_5, v_5

$$PRS4_i = \lfloor x_i \times 6 \rfloor + 1; i = 1 \; to \; 4HW$$

7. A pseudo-random number sequence (PRS5) is generated having numbers 0 to 3 by iterating the robust chaos map 4HW times with the initial condition x_{N+8HW} and parameters a_6, v_6

$$PRS5_i = \lfloor x_i \times 4 \rfloor ; i = 1 \; to \; 4HW$$

8. Step 3 is repeated with x_{N+12HW} and parameters a_7, v_7 to generate $PRS6_i$

   Now the process of encryption of ith pixel of the plain image is done in the following way:

9. Calculate the two terms PIS and CIS dependent on the plain and cipher images

$$PIS(i) = mod(sum\left(PI(i+1:HW)\right), 256)$$

$$CIS(i) = mod(sum(CI(1:i-1)), 256)$$

For $i = 1$ the value of the previous cipher image pixel $CI(i-1)$ is 0.

10. Using PIS and CIS calculated above, the ith pixel of the synthetic image is modified

$$SI(i) = (SI(i) \oplus PIS(i)) \oplus CIS(i)$$

11. Convert the $SI(i)$ into the DNA sequence ($SIDNA(i)$) using the $PRS1_i^{th}$ DNA encoding rule

12. Convert the $PI(i)$ into the DNA sequence ($PIDNA(i)$) using the $PRS2_i^{th}$ DNA encoding rule

13. (i)DNA XORing using the $PRS3_i^{th}$XORing

$CIDNA1(i) = (PIDNA(i) \oplus_{DNA} SIDNA(i)) \oplus_{DNA} CIDNA1(i-1)$.

For $i = 1$ the DNA sequence for the previous cipher image pixel $CIDNA1(i-1)$ is 'ATCG'.

(ii) DNA Complement using $PRS4_i^{th}$ DNA Complement rule at the $PRS5_i^{th}$ level

$$CIDNA(i) = f_c(CIDNA1(i))$$

14. Convert the $CIDNA(i)$ into the binary form using the $PRS6_i^{th}$ DNA decoding rule.

    The process from Steps 9 to 14 is repeated for all the pixels of the plain image.

For a complete reference of the proposed image encryption algorithm and flow of operations, please refer to the block diagram given in Figure 5.

Decryption Algorithm

In the proposed image encryption method, the decryption process is identical to the encryption algorithm discussed earlier, except for the fact that it is executed in reverse order. This means that the last pixel of the cipher image is decrypted first, followed by the decryption of each pixel in reverse order until the first pixel is reached. If the same secret key is used, the original plain image can be fully recovered.

The decryption starts with the same secret key (x_0, a_1, v_1, N, a_2, v_2, a_3, v_3, a_4, v_4, a_5, v_5, a_6, v_6, a_7, v_7) followed by execution of Steps 1 to 8 of the encryption algorithm (as explained in subsection 4.1) to generate the synthetic image SI and pseudo-random sequences PRS1 to PRS6.

Now the process of decryption of ith pixel (starting from the last pixel) of the cipher image is done in the following way:

9. Calculate the two terms CIS and PIS dependent on the cipher and plain images

$$CIS(i) = mod(sum(CI(1:i-1)), 256)$$

$$PIS(i) = mod(sum\left(PI(i+1:HW)\right), 256)$$

For $i = 1$ (i.e., the last pixel to decrypt) the value of the previous cipher image pixel $CI(i-1)$ is 0.

10. Using PIS and CIS calculated above, the ith pixel of the synthetic image is modified

$$SI(i) = (SI(i) \oplus PIS(i)) \oplus CIS(i)$$

11. Convert the $SI(i)$ into the DNA sequence ($SIDNA(i)$) using the $PRS1_i^{th}$ DNA encoding rule

12. Convert the $CI(i)$ into the DNA sequence ($CIDNA(i)$) using the $PRS6_i^{th}$ DNA encoding rule

13. (i) DNA Complement recovery using $PRS4_i^{th}$ DNA Complement rule at the $PRS5_i^{th}$ level

$$CIDNA1(i) = f_{cr}(CIDNA(i))$$

(ii)DNA XORing using the $PRS3_i^{th}$XORing

$PIDNA(i) = (CIDNA1(i) \oplus_{DNA} CIDNA1(i-1)) \oplus_{DNA} SIDNA1(i)$.

For $i = 1$ (i.e., the last pixel to decrypt) the DNA sequence for the previous cipher image pixel $CIDNA1(i-1)$ is 'ATCG'.

14. Convert the $PIDNA(i)$ into the binary form using the $PRS2_i^{th}$ DNA decoding rule.

    The process from Steps 9 to 14 is repeated for all the pixels of the cipher image in reverse order i.e. from the last pixel to the first pixel.

NIST testing of pseudorandom sequences

To verify the pseudorandomness of the sequences generated through the robust chaotic map and used in the proposed image encryption scheme, we have used the NIST test suite. For testing purpose we have generated 100 sequences of 10^6 bits each starting with the randomly chosen initial conditions and parameters within the allowed robust chaos range as specified above (i.e. $0 < x_0 < 1$ and all $a > 1$, $v > 1$).

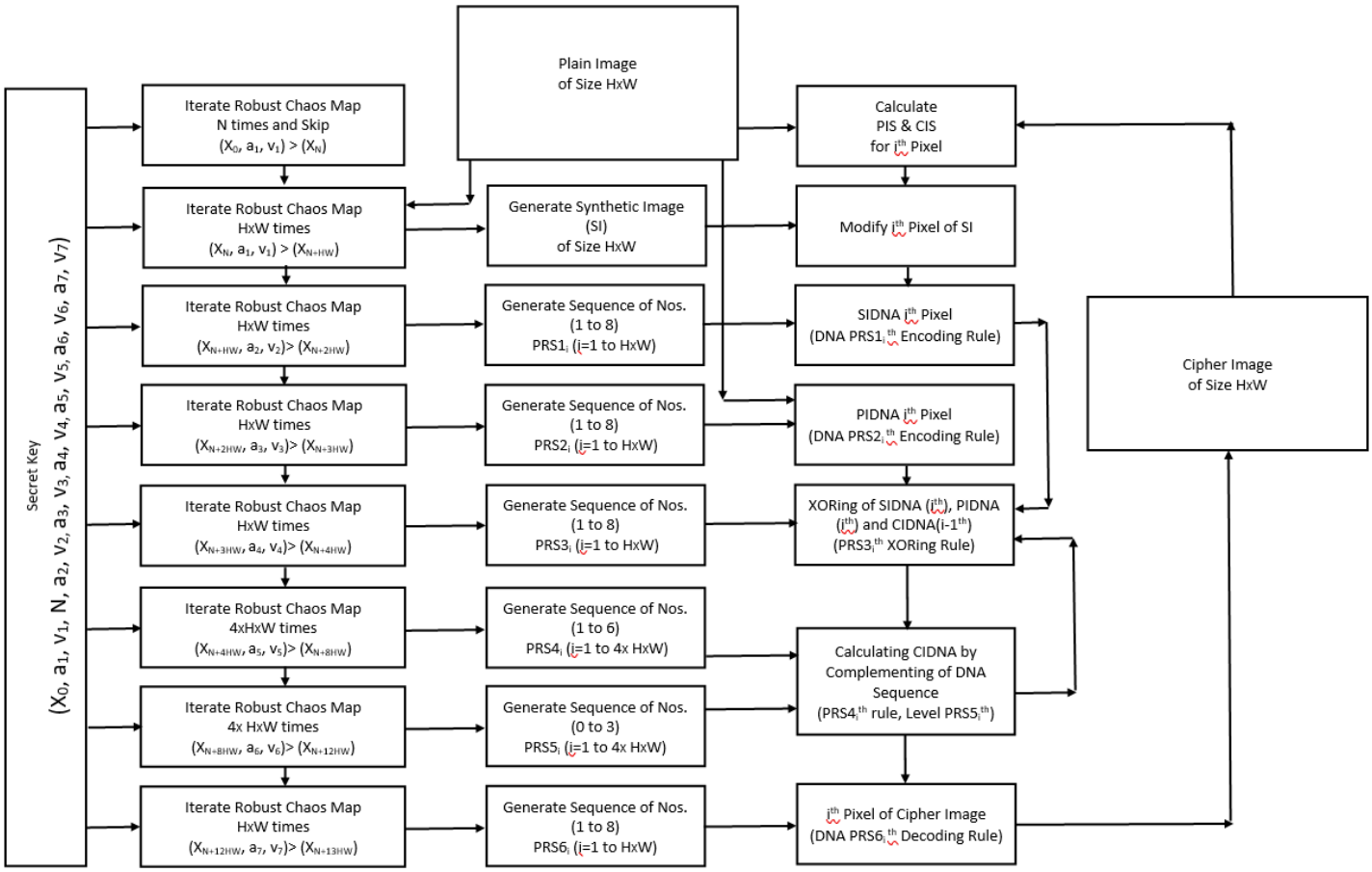

Figure 5 The image encryption algorithm

We have then run the entire NIST test suite comprising 15 parametric and nonparametric tests that generate a total of 188 p-values for each test statistic (there are multiple numbers of variants corresponding to some of the tests). Considering the significance level of 0.01, a p-value greater than 0.01 indicates that a particular test is passed by the sequence. We also find the total number of sequences passing the test out of the total sequences i.e. proportion for each test statistics and as per the chosen significance level 0.01, if it falls within the range (0.9833245, 0.9966745), the pseudorandom sequence generator qualifies for the cryptographic applications. For each test statistic, we may also observe the uniformity of all 100 p-values in the entire range [0,1] through the Chi-square test on the 100 p-values for each test statistic and generating the p-value of p-values i.e $p - value_T$. If $p - value_T > 0.0001$ then the distribution of the p-values for that particular test is declared uniform.

We have depicted the results of proportions and the p-value$_T$ obtained through the NIST test suite for each test statistic in Figure 6 that shows the pseudorandom sequence generator qualifies the NIST test suite criteria for the cryptographic applications.

PERFORMANCE AND ANALYSIS RESULTS

The performance of the proposed image encryption method is analyzed through various perceptual quality metrics, statistical measures, information entropy, plaintext sensitivity measures (NPCR, UACI), and measures based on DNA sequences (Hamming distance, base ratio) etc. The details and results of the analysis are presented below.

We have used two images *'Peppers'* and *'Lena'* and encrypted them with the secret key (x0=0.787; a1=1.65; v1=4.57; N=123; a2=6.73; v2=5.46; a3=2.57; v3=7.35; a4=6.54; v4=9.83; a5=6.27; v5=4.76; a6=3.52; v6=2.43; a7=8.53; v7=5.32).

In Figure 7, we have shown the plain images and corresponding cipher images generated with the help of the proposed image encryption algorithm. The cipher images look random. In Figure 8, we have depicted the histograms of the plain and cipher images shown in Figure 7. Visually, the histograms of the cipher images appear uniform. To confirm the uniformity of the histograms of cipher images quantitatively, we have calculated two statistical measures: Chi-square and variance of the histograms for the plain and cipher images. The results are given in Table 4. It can be observed that Chi-square and histogram variance are very small for the cipher images (almost 1% of plain images) which confirms the uniformity of the cipher image histograms.

The deviations of the cipher image histogram from the ideal (perfect uniform distribution) histogram are computed using the metric 'Deviation from Ideality'. The results are shown in Table 5. As is evident from the values thus obtained, the deviation from the ideality is negligible. This substantiates that the cipher image pixel distributions are nearly ideal/uniform.

Also, the deviations between the plain and cipher image histograms are computed using two metrics 'Maximum Deviation' and 'Irregular Deviation'. Observations are listed in Table 5. As is evident from the values, the deviations are quite large. This substantiates the fact that the proposed image encryption algorithm generates the cipher images with histograms significantly different

Table 4 Chi-Square and Histogram Variance

		Peppers	Lena
Chi-Square	Plain Image	1.9280e+04	2.5400e+04
	Cipher Image	218.3680	245.5680
Histogram Variance	Plain Image	1.1768e+04	1.5503e+04
	Cipher Image	133.2813	149.8828

Table 5 Deviation from Ideality, Maximum Deviation and Irregular Deviation

	Peppers	Lena
Deviation from ideality	0.0587	0.0618
Maximum Deviation	0.5676	0.6620
Irregular Deviation	0.6446	0.6908

Table 6 Correlation Coefficients

		Peppers	Lena
Horizontal Adjacent Pixels	Plain Image	0.9544	0.9322
Horizontal Adjacent Pixels	Cipher Image	0.0020	7.5469e-04
Vertical Adjacent Pixels	Plain Image	0.9646	0.9684
Vertical Adjacent Pixels	Cipher Image	0.0038	-8.3144e-04
2D Correlation Coefficients between plain image and cipher image		-0.0045	-0.0077

Table 7 Perceptual Quality Metrics

	Peppers	Lena
MAE	75.3073	72.9944
MSE	8.3264e+03	7.7428e+03
PSNR	8.9262	9.2418
SD	1.4226e+04	1.4087e+04
SSIM	0.0093	0.0066
FSIM	0.3689	0.3614

than the histograms of corresponding plain images.

2D correlation coefficients for various pairs of plain and cipher images as well as the correlation between the adjacent pixels (horizontally as well as vertically) in the plain and cipher images are evaluated. The results for correlation coefficients are summarized in Table 6. The correlation of two similar images in an ideal case is unity. As the values obtained for the proposed scheme are negligible as compared to the ideal value which clearly shows that the proposed image encryption algorithm is capable of removing the high correlation that exist in the plain image pixels.

Table 8 Hamming Distance (DNA)

	Peppers	Lena
Hamming Distance	119900	119682

Table 9 DNA Base Ratio (%)

	DNA Base	Peppers	Lena
Plain Image	A	25.6631	25.7550
	T	25.7494	25.0525
	C	24.1581	24.4994
	G	24.4294	24.6931
Cipher Image	A	25.1038	25.0575
	T	25.1713	25.1025
	C	24.8988	25.1438
	G	24.8263	24.6962

Table 10 Global and Local Information Entropy

		Block Size	Peppers	Lena
Global Information Entropy	Plain Image	200 X 200	7.5820	7.4351
	Cipher Image		7.9960	7.9956
Local Information Entropy	Plain Image	50 X 50	6.9406	6.6886
	Cipher Image		7.9230	7.9260
	Plain Image	40X 40	6.7164	6.5113
	Cipher Image		7.8806	7.8800
	Plain Image	25 X 25	6.2370	6.0016
	Cipher Image		7.6697	7.6724

Table 11 Plaintext Sensitivity

	Peppers	Lena	Theoretical Value/Range (Wu *et al.* 2011) (Significance Level 0.01)
NPCR	99.6450	99.7000	99.5527
UACI	33.4561	33.4321	[33.2255, 33.7016]

The perceptual quality analysis results for the cipher images produced by the proposed image encryption algorithm are summarized in Table 7. Ideally, the image encryption algorithm should be able to have significant quality degradation in the images so that no pattern/feature remains present in the cipher images leading to a clue for analysing and decoding the information about plaintext

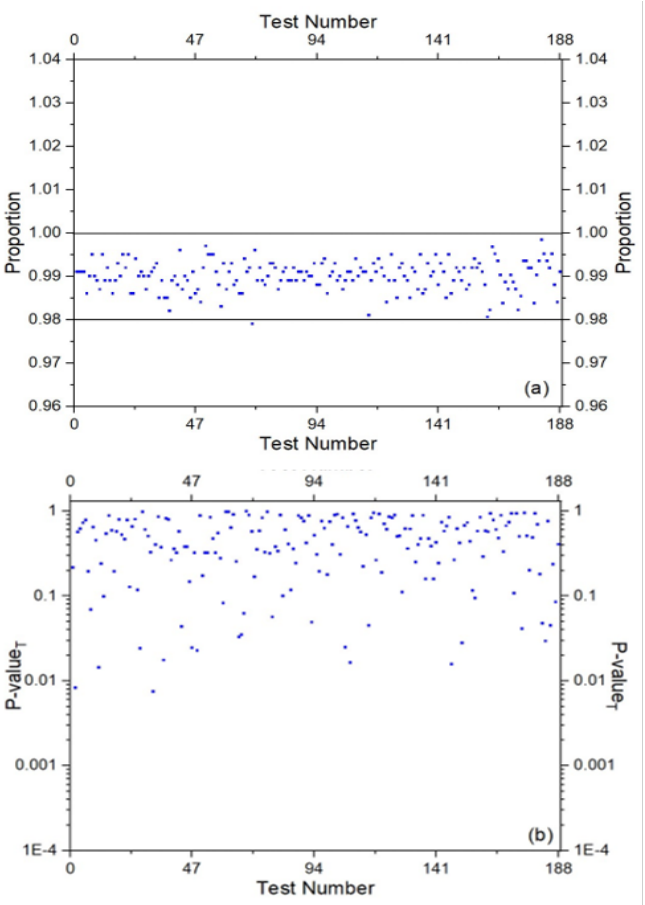

Figure 6 NIST Testing of pseudorandom sequences

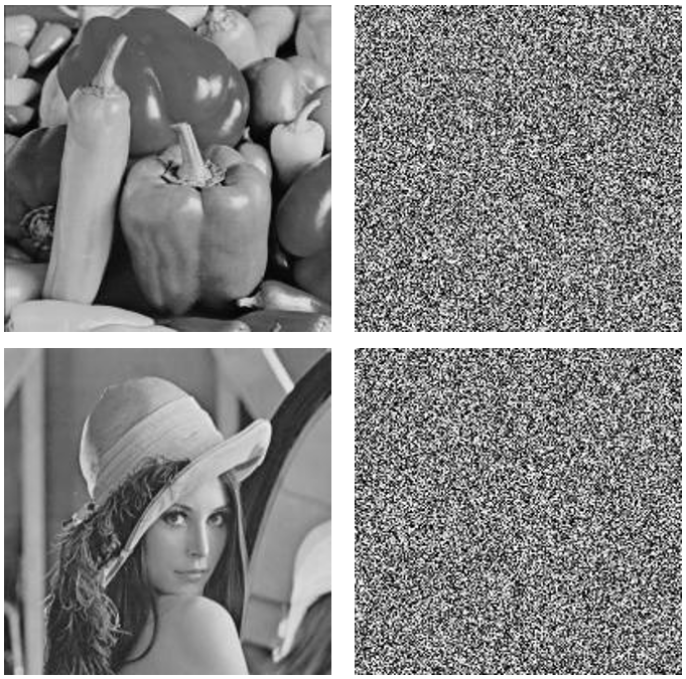

Figure 7 Plain images 'Peppers' and 'Lena' (first column) along with corresponding cipher images (second column) obtained with the proposed image encryption algorithm.

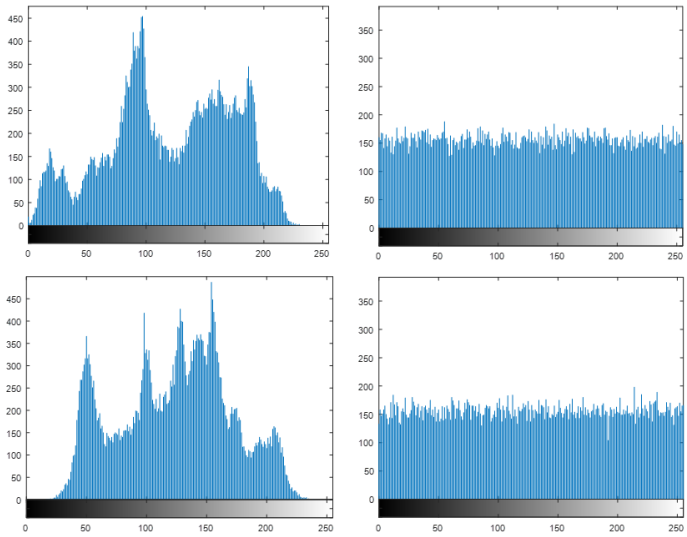

Figure 8 Histograms of 'Peppers' and 'Lena' (first column) and corresponding encrypted images (the second column).

images. The results of our computation of various perceptual quality metrics are given in Table 7. We may observe that the encrypted images possess very low perceptual quality.

As the proposed image encryption is based on the conversion of image pixels into DNA sequences followed by operations like XORing and complementing of the DNA bases in the DNA sequences of the image pixels, we have also done some analysis on the DNA sequences of the plain images and the cipher images generated through the proposed image encryption technique. We have computed the 'Hamming distance' between the DNA sequences of plain and cipher images, it measures the dissimilarity between the sequences in terms of DNA bases. The results have been shown in Table 8 which shows that the hamming distance is very large (almost 120K) which indicates the 75% dissimilarity in the DNA sequences of cipher and plain images. We have also computed the 'Base Ratio' for all the four DNA bases (A, T, C and G) in the DNA sequences of plain and cipher images. The base ratio is the percentage of occurrence of a particular base in the given sequence. The results have been summarized in Table 9. It is clear that all the bases have almost 25% occurrence in the plain as well as cipher images. It also conveys that while encoding the plain image into the DNA sequence in the proposed image encryption algorithm, sufficient randomness has been introduced so that the base distribution is almost uniform even in the DNA sequence of the plain image.

The information entropy is the measure of disorder. We have computed the information entropy for the whole of plain and cipher images (i.e., global information entropy) as well as the average of information entropy by dividing it into a finite number of non-overlapping blocks (i.e., local information entropy). The results have been shown in Table 10 which confirms that for the encrypted images, the global information entropy is very near to 8-bits and the local information entropy is also close to the global entropy and well above the desired thresholds.

To check the robustness of the proposed image encryption algorithm against the known-plaintext attack, we have also done a differential analysis of the proposed image encryption. For this purpose, we make a small change in the plain image (usually only one pixel) and compare the cipher images corresponding to two

plain images with only a one-pixel difference and encrypted with the same secret key. We compute two metrics Net Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) and the results are shown in Table 11. It shows that these computed values of NPCR are higher than the theoretical/ideal critical value and computed values of UACI lie within the theoretical/ideal range obtained for a pair of random images, therefore, the two encrypted images, produced for the two plain images differing by only one-pixel value, are random like. Hence, the proposed image encryption algorithm is sensitive to the plaintext and robust against any differential attack.

For brevity, we have not provided the mathematical details/statistics of all the metrics used in the performance analysis. We refer the readers to (Kaur *et al.* 2022a; Patidar *et al.* 2011; Xue *et al.* 2020; Patidar and Kaur 2023; Wu *et al.* 2011) for complete details.

CONCLUSION

A novel image encryption algorithm utilizing the robust chaos-based dynamic DNA coding, DNA XORing and DNA Complementing is proposed. Though there are other DNA-Chaos-based schemes already available in literature but to the best of our knowledge, the proposed scheme is novel in its approach towards utilizing the dynamical behaviour of chaos for random selection of one of the DNA rules. Secondly, the chaotic map is carefully selected for its robustness due to the absence of periodic windows over the entire key space. The proposed algorithm possesses all the essential features of a practical image encryption algorithm. Various statistical measures, perceptual quality metrics, information entropy, plaintext sensitivity measures (NPCR, UACI), measures based on DNA sequences (Hamming distance, base ratio) etc. have been used to analyze the performance of the proposed image encryption algorithm and the results show the robustness of the proposed image encryption algorithm against any statistical or cryptanalytic attacks. In future, we will present different combinations of chaos/hyperchaos and DNA rules for a comparative analysis of our proposed work with the existing schemes in terms of speed and complexity as well.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Adleman, L. M., 1994 Molecular computation of solutions to combinatorial problems. science **266**: 1021–1024.

Andrecut, M. and M. Ali, 2001 Robust chaos in smooth unimodal maps. Physical Review E **64**: 025203.

Chai, X., X. Fu, Z. Gan, Y. Lu, and Y. Chen, 2019 A color image cryptosystem based on dynamic dna encryption and chaos. Signal Processing **155**: 44–62.

Dagadu, J. C., J. Li, E. O. Aboagye, and F. K. Deynu, 2019 Medical image encryption scheme based on multiple chaos and dna coding. Int. J. Netw. Secur. **21**: 83–90.

Gehani, A., T. LaBean, and J. Reif, 2004 Dna-based cryptography. Aspects of molecular computing: essays dedicated to tom head, on the occasion of his 70th birthday pp. 167–188.

Hennelly, B. M. and J. T. Sheridan, 2003 Image encryption and the fractional fourier transform. Optik **114**: 251–265.

Kaur, G., R. Agarwal, and V. Patidar, 2022a Color image encryption scheme based on fractional hartley transform and chaotic substitution–permutation. The Visual Computer **38**: 1027–1050.

Kaur, G., R. Agarwal, and V. Patidar, 2022b Image encryption using fractional integral transforms: Vulnerabilities, threats, and future scope. Frontiers in Applied Mathematics and Statistics **8**: 1039758.

Patidar, V., 2022 Development of new designs of secure image encryption schemes utilizing robust chaos & discrete fractional transforms. SERB India MATRICS Project Completion Report, SERB/MTR/2018/000203 .

Patidar, V. and G. Kaur, 2023 A novel conservative chaos driven dynamic dna coding for image encryption. Frontiers in Applied Mathematics and Statistics **8**: 1100839.

Patidar, V., N. Pareek, G. Purohit, and K. Sud, 2011 A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Optics communications **284**: 4331–4339.

Shannon, C. E., 1949 Communication theory of secrecy systems. The Bell system technical journal **28**: 656–715.

Teh, J. S., M. Alawida, and Y. C. Sii, 2020 Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications **50**: 102421.

Wang, X., Y. Wang, X. Zhu, and C. Luo, 2020 A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level. Optics and Lasers in Engineering **125**: 105851.

Wang, X.-Y., Y.-Q. Zhang, and X.-M. Bao, 2015 A novel chaotic image encryption scheme using dna sequence operations. Optics and Lasers in Engineering **73**: 53–61.

Wu, Y., J. P. Noonan, S. Agaian, *et al.*, 2011 Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) **1**: 31–38.

Xiao, G., M. Lu, L. Qin, and X. Lai, 2006 New field of cryptography: Dna cryptography. Chinese Science Bulletin **51**: 1413–1420.

Xue, X., D. Zhou, and C. Zhou, 2020 New insights into the existing image encryption algorithms based on dna coding. Plos one **15**: e0241184.

Zeraoulia, E., 2012 *Robust chaos and its applications*, volume 79. World Scientific.

Zhang, J., D. Fang, and H. Ren, 2014 Image encryption algorithm based on dna encoding and chaotic maps. Mathematical Problems in Engineering **2014**: 1–10.

How to cite this article: Patidar, V., and Kaur, G. Lossless Image Encryption using Robust Chaos-based Dynamic DNA Coding, XORing and Complementing. *Chaos Theory and Applications*, 5(3), 178-187, 2023.