Complex & Intelligent Systems (2024) 10:745–761
https://doi.org/10.1007/s40747-023-01187-0

ORIGINAL ARTICLE

A new dynamic DNA-coding model for gray-scale image encryption

Yasmine M. Afify[1] · Nada H. Sharkawy[2] · Walaa Gad[1] · Nagwa Badr[1]

Received: 13 March 2023 / Accepted: 15 July 2023 / Published online: 4 August 2023

Abstract
To protect the images and provide a more secure cipher image, DNA encoding is crucial in image encryption. Applying a single, easily detectable coding rule to the image during DNA encoding has no impact on the encryption model's security level. Therefore, using various coding rules while applying encryption to the image, dynamic DNA-coding techniques have emerged to strengthen and improve the encryption of the image and its security. This study integrates a dynamic DNA-coding method with an encryption model. The model is applied to gray-scale images, where using a predetermined coding rule, every two bits are DNA-encoded in the image. The proposed model generates the key by sending the image and its metadata to hash functions. Following that, the hyperchaotic system constructs three chaotic sequences using the key, and the Lorenz–Liu chaotic system generates a sequence of coding rules. Then, the image is passed to Arnold Transform, where the resulted image is diffused by applying five chaotic maps. Last, using the coding rules, it is DNA-encoded, provided with the chaotic sequences to DNA, and DNA-decoded. Twelve metrics were used to assess the proposed model on ten widely used images. Results show a promising improvement in performance, since it enhanced the security of the model.

Keywords LLCS · LCS · DNA · Dynamic DNA coding · Image encryption

Introduction

Currently, image processing has rapidly expanded. Commonly, 2D images are used to apply image processing techniques. These methods are used across a variety of fields, including image search results [1], object identification [2–4], image enhancement [5], and image encryption. Both colourful and grayscale images are subject to image encryption.

Recently, Deoxyribonucleic Acid (DNA) has been employed in cryptography because of its high information density, energy efficiency, and parallelization capability [6]. Therefore, the use of DNA-encoding in cryptography systems has grown. It has been massively useful for preserving the images so they can be perfectly retrieved, in addition to generating new cipher data that cannot be attacked easily.

DNA-encoding using one coding rule is the first and oldest type applied in cryptography. It has been applied in many encryption modes, such as the models in [7–17], which give the system a great amount of information and a huge number of parallelisms while consuming less power. Nonetheless, using one coding rule allows the rule to be predicted easily, and the original image can be recovered.

This shortening is overcome by introducing dynamic DNA coding, in which the image is DNA-encoded using a different number of coding rules. The coding rules can be applied in different ways, including one for each block in the image [18, 19], one for each row in the block [20], one for each pixel [10, 21–23], and one for every two bits of the image [24].

The main challenge is raising the sensitivity of the key and enhancing the encryption layers in the cryptography domain by applying dynamic DNA coding. In this paper, we overcome this challenge by applying dynamic DNA coding to the model proposed in [7]. In the proposed model, dynamic DNA coding is applied, where the model generates a sequence of coding rules using the Lorenz–Liu chaotic system. The sequence contains one coding rule for every two bits of the image. After that, the sequence is used to create a DNA-encoded image. The same sequence is then used for DNA decoding of the image.

To evaluate the efficiency of the model, twelve evaluation metrics are employed on ten popular gray-scale images. The

✉ Yasmine M. Afify
yasmine.afify@cis.asu.edu.eg

[1] Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt

[2] Higher Institute for Computers and Information Technology, ElShorouk, Cairo 11837, Egypt

comprehensive evaluation covers five aspects: key analysis, differential attacks analysis, robustness analysis, statistical attacks analysis, and computational complexity analysis. The evaluation metrics are the key space, key sensitivity, number of pixels change rate (NPCR), unified average changing intensity (UACI), mean square error (MSE), peak signal-to-noise ratio (PSNR), histogram analysis, information entropy, chi-square test (χ^2 test), irregular deviation (ID), correlation coefficient adjacent (CCA), and computational complexity.

The experimental results of the proposed model demonstrate encouraging performance improvements. The key became a wider space and being more sensitive to little changes. The results of NPCR and UACI express the high sensitivity of the model to minor changes in the input images, leading to the generation of completely different cipher images. Regarding MSE and PSNR results, the proposed model contains various encryption layers that perform wider distances between the original image and the cipher image. The color intensity distribution of the encrypted image is much more uniform, as proven by histogram analysis in addition to the results of X^2 and ID. The proposed model implies great randomness in the images demonstrated in information entropy and CCA. The contributions to this work are:

- Introducing a model based on integrating dynamic DNA-coding techniques with the image encryption model.
- The proposed model expands the key space and improves key sensitivity while also enhancing the security of the encryption layers.
- A comprehensive assessment of the proposed model on ten popular images using twelve evaluation metrics.

The paper is structured as follows: the related dynamic DNA-coding models and differences between them are represented in the next section. The following section describes DNA sequences and dynamic DNA coding in addition to the Liu chaotic system and how it is intercepted in the Lorenz–Liu chaotic system. Next section introduces the proposed model. In the following section, the performance measures of the proposed model and its results are presented. Finally, the conclusion of the work and the future directions are expressed in the last section.

Related work

Dynamic DNA coding has been applied in many representations: a coding rule for the image, a coding rule for each block in the image, a coding rule for each row in blocks of the image, a coding rule for each pixel, and a coding rule for every two bits in the image. In this section, these representations are addressed along with how they were used in recent models, with a focus on their strengths and weaknesses.

A coding rule for the image

Signing et al. [16] proposed a model in 2021. The model is joint-based on pseudo-random and sophisticated hyperchaotic behaviour along with DNA-encoding. First, the secret key is obtained using the hyperchaotic system, and the image is exposed to bit-by-bit shuffling. Next, the image is binarized and DNA-encoded using the encoding rule. Finally, the encoded sequence is provided to DNA operations, complemented, and DNA-decoded. The encrypted image is generated from the resulting binary sequence. The model has a large key space and is sensitive to small changes. However, it implies low resistance to differential attacks.

A coding rule for each block in the image

In 2021, Mohamed et al. [19] introduced a new model based on Choquet fuzzy integral (CFI) and dynamic DNA coding. First, the original image is split into four parts. CFI is then applied, and the four S-boxes are generated. Each box is binarized and DNA-encoded with its coding rule generated by the M sequence. Finally, down-sampling is applied to the DNA boxes, which are diffused using Chen's hyperchaotic map sequences, and the sequences are decoded to get a cipher image. The model implies high randomness for the images and is sensitive to the image and key, but with a small key space.

Another model was introduced in 2022 by Wang et al. [18] which applies Zigzag scrambling besides dynamic DNA coding relying on random blocks and the logistic–dynamics-coupled map lattice (LDCML). Using SHA-512, the key is generated. Then, the image is scrambled and split into blocks, then inter-scrambled. Afterward, according to a sequence generated by LDCML, each block is DNA-encoded by a coding rule. Finally, DNA operations are performed, the sequence is decoded, obtaining the cipher image. The model has a wide key space and is overly sensitive to image changes. On the other hand, the model is less robust to differential and robustness attacks.

A coding rule for each row in the image

Bao et al. [20] introduced an encryption model in 2022 that combines compressive sensing and DNA coding. The model begins with creating a key measurement matrix and applying SHA-256 to the image to get the hash sequence. Next, the image is split into four blocks, to which inter-scrambling is applied. Afterward, each block is binarized, and each row in it is DNA-encoded with its coding rule. In the end, the DNA addition operation is applied to the DNA blocks, which are DNA-decoded, recombined, and sorted to obtain a cipher image. The model is sensitive to tiny changes in the original image and the key. Meanwhile, it has a small key space, implies less randomness in the images, and is less robust to differential attacks.

A coding rule for each pixel in the image

Li et al. [23] introduced a new model depending on the memcapacitor chaotic system and DNA coding. First, the key is generated by SHA-3 for the image, where every eight pixels are used as the chaotic system's initial values. Following that, the image is binarized, forming a matrix, and each pixel in the matrix is DNA-encoded with its coding rule. Finally, the chaotic sequence is used for scrambling the DNA-encoded matrix, which is then decoded and converted to decimals, obtaining a cipher image. The model has a large key space in addition to its sensitivity to key and image changes. However, it is less robust to statistical attacks.

Zhu et al. [22] proposed another model depending on the 5D continuous hyperchaotic system and DNA coding. First, the chaotic system generates a chaotic sequence in addition to the coding rules, and the original image is permuted using the chaotic sequence. Then, the image is binarized, forming a matrix, where each pixel is DNA-encoded with its coding rule, DNA complemented, and DNA-decoded. In the end, the decoded matrix is diffused, obtaining the cipher image. The model implies great randomness in the images. Yet, it is less robust to differential attacks, has a small key space, and is less sensitive to tiny changes in the key and images.

Tian et al. [10] proposed a model relying on dynamic DNA coding and piecewise linear chaotic map-based coupled map lattices (SPWLCM map-based CML). The chaotic sequences are obtained using CML, which is then used to generate DNA-encoding rules in addition to DNA-decoding rules. The original image is scrambled and diffused with the chaotic sequences, and it is binarized. Then, relying on the encoding rule for each pixel, the image is DNA-encoded and permuted. At the end, the DNA-encoded image is decoded, converted to decimals, and diffused to obtain a cipher image. The model is sensitive to small changes and implies high randomness in the images. However, it is less robust to differential attacks and has a small key space.

Zhang et al. [21] introduced a model relying on the sine-piecewise linear chaotic map (SPWLCM) and DNA coding. To begin, SPWLCM generates key and coding rules. Then, the image is shuffled and binarized, forming a matrix. Next, each pixel in the matrix is DNA-encoded using its own coding rule. Finally, the DNA encryption algorithm is applied to the encoded matrix. The matrix is decoded and converted to decimals, obtaining the cipher image. The model is sensitive to minor changes and implies high randomness in the images. On the other hand, it has a small key space and less protection for differential attacks.

A coding rule for each two bits in the image

Wang et al. [24] introduced a new model that depends on random embedding and DNA coding. The 4D memristive hyperchaotic system creates the control parameters, whereas the image is preprocessed based on random number embedding. Following that, the coding rules are obtained using the 4D memristive hyperchaotic system. Afterward, the image is binarized, and each two bits in the image is encoded using its coding rule. At the end, the image is scrambled and diffused, and then DNA operations are applied to it before it is decoded and converted to decimals to obtain the cipher image. The model has a wide key space, which is sensitive to minor changes and implies high randomness to the images. Nonetheless, it is less robust to differential attacks.

Table 1 lists the models that employ the previous dynamic DNA-coding techniques, along with their benefits and drawbacks. The conducted comparison highlights significant findings. First, the randomness of generating the encrypted images is outstanding in the case of applying DNA-encoding using a coding rule for each pixel technique and a coding rule for each two bits technique. It is noted that the key space and its sensitivity depend on the algorithm used in the key generation. On the other hand, the robustness of the model to statistical and differential attacks relies on the encryption model. The differential attacks are found to be the biggest challenge for the researchers.

Fundamental knowledge (preliminaries)

This section presents a detailed description of the DNA sequences, the application of dynamic DNA coding, the Lorenz–Liu chaotic system, and the Liu chaotic system.

DNA sequence

DNA, or Deoxyribonucleic acid, is a biological macromolecule that carries hereditary genetic information about living organisms [25]. It consists of nucleic acid bases bonded to form two strands using phosphodiester bonds. These strands are linked with hydrogen bonds, forming a helix structure. There are four kinds of bases: adenine (A), thymine (T), cytosine (C), and guanine (G). A and T are bonded together using two hydrogen bonds; therefore, they are purines. Meanwhile, C and G are bonded together using three hydrogen bonds, since they are pyrimidines [7]. DNA has recently been used in cryptography for its high information density, its energy efficiency, and its parallelization capability [6].

Table 1 Dynamic DNA-coding techniques

Dynamic DNA-coding technique	Model	Features	Drawbacks
Coding rule for image	[16]	Large key space Sensitive key	Less resistant to differential attacks
Coding rule for each block	[18]	Large key space Sensitive key	Less resistant to differential attacks Less randomness of image
	[19]	High randomness of image Sensitive key	Small key space
Coding rule for each row in block	[20]	Sensitive key	Small key space Less resistant to differential attacks Less randomness of image
Coding rule for each pixel	[10]	High randomness of image Sensitive key	Small key space Less resistant to differential attacks
	[21]	High randomness of image Sensitive key	Small key space Less resistant to differential attacks
	[22]	High randomness of image	Small key space Less resistant to differential attacks Key is less sensitive
	[23]	Large key space Sensitive key	Less resistant to statistical attacks
Coding rule for every two bits	[24]	Large key space Sensitive key High randomness of image	Less resistant to differential attacks

Dynamic DNA coding

Data can be encoded into a DNA sequence using its binary representation, since each base is represented by two bits. There are eight effective DNA rules that can be achieved based on Watson and Crick's complementary model: purines and pyrimidines. These rules are listed in Table 2 [7].

The dynamic DNA-coding technique encodes each pixel into a DNA sequence of four bases. Each two bits in one pixel is DNA-encoded using chosen coding rules [26]. For example, if pixel x contains a value equal to 125, its binary representation is "01111101". Assuming the chosen coding rules for the pixel are {3, 4, 5, 8}, then the DNA-encoded sequence is "GAGA". The decoding operation will be based on the chosen coding rules.

Lorenz–Liu chaotic system (LLCS)

The Lorenz–Liu chaotic system (LLCS) is constructed by considering the Liu chaotic system state variables as the Lorenz chaotic system parameters. The generated system is described in Eqs. (1–3) [26]:

$$l_1(1, i+1) = (r_1 + \lambda m_1(1, i))(l_2(1, i) - l_1(1, i)) \tag{1}$$

$$l_2(1, i+1) = (s_{1+}\lambda m_2(1, i))l_1(1, i) - l_1(1, i)l_3(1, i) - l_2(1, i) \tag{2}$$

$$l_3(1, i+1) = l_1(1, i)l_2(1, i) - (t_1 + \lambda m_3(1, i)) \tag{3}$$

where l_1, l_2, and l_3 are stateful variables; r_1, s_1, and t_1 are the parameters of the system with values $r_1 = 10$, $s_1 = 28$, and $t_1 = 8/3$ [26]; m_1, m_2, and m_3 are the disturbances of the system parameter provided by the Liu chaotic system; and λ is the LLCS disturbance intensity. The LLCS is provided to mod 1000.

Liu chaotic system (LCS)

The Liu chaotic system (LCS) is a system that reveals properties of Lyapunov exponents, Poincare mapping, fractal dimension, continuous spectrum, and chaotic behaviours. It can be described in Eqs. (4–6) [26, 27]:

$$m_1(1, i+1) = r_2(m_2(1, i) - m_1(1, i)) \tag{4}$$

$$m_2(1, i+1) = s_2 m_1(1, i) - u m_1(1, i)m_3(1, i) \tag{5}$$

$$m_3(1, i+1) = -t_2 m_3(1, i) - v m_1(1, i)^2 \tag{6}$$

where m_1, m_2, and m_3 are the stateful variables; and r_2, $s_2 t_2$, u, and v are the system parameters with values $r_2 = 10$, $s_2 = 40$, $t_2 = 2.5$, $u = 1$, and $v = 4$ [26]. The LCS is provided to mod 1000.

Proposed model

This section describes in detail the proposed model, its components, the encryption, and decryption schemes. The model in [7] generates a key through the incorporation of the MD5 and SHA-256 hash algorithms. With the aid of a memristor hyperchaotic system, it produces four matrices. Once the key was generated, Arnold's transform is applied to the original image. Five chaotic maps are then used to scramble the image. The image is then DNA encoded, followed by being diffused using three of the four matrices generated using the hyperchaotic system, and finally DNA decoded. This model is adapted as follows:

Proposed encryption model

The proposed encryption model applied to the $M \times N$ grayscale image is described in Fig. 1. It consists of the following steps:

Step 1: 256-bit Hash value generation. MD5 hash function is applied to the original image and its metadata, where the generated 128-bit hash values are concatenated and provided to SHA-256, generating a 256-bit hash value H:

$$H = [h_1, h_2, \ldots, h_{64}]$$

Step 2: Generation of parameters. The image is split into four parts. The average of each part and H are applied to equations in model [7] resulting in the Arnold Transform parameters a, b, and c; and Hyper-Chaos system initial values w_0, x_0, y_0, and z_0. The values of Liu chaotic system parameters are $r_2 = 10$, $s_2 = 40$, $t_2 = 2.5$, $u = 1$, and $v = 4$. Meanwhile, the values of Lorenz–Liu chaotic system parameters are $r_1 = 10$, $s_1 = 28$, and $t_1 = 8/3$.

Step 3: Calculate initial values of LLCS. The initial values of LCS are calculated, as shown in Eqs. (7–9):

$$m_1 = (h_1 \oplus h_2 \oplus \ldots \oplus h_{10})/256 \quad (7)$$

$$m_2 = (h_{11} \oplus h_{12} \oplus \ldots \oplus h_{20})/256 \quad (8)$$

$$m_3 = (h_{21} \oplus h_{22} \oplus \ldots \oplus h_{32})/256 \quad (9)$$

Meanwhile, the initial values of LLCS are obtained by Eqs. (10–12):

$$l_1 = (h_1 + h_2 + \ldots + h_{10})/(10 * max(h_1, h_2, \ldots, h_{10})) \quad (10)$$

$$l_2 = (h_{11} + h_{12} + \ldots + h_{20})/(10 * max(h_{11}, h_{12}, \ldots, h_{20})) \quad (11)$$

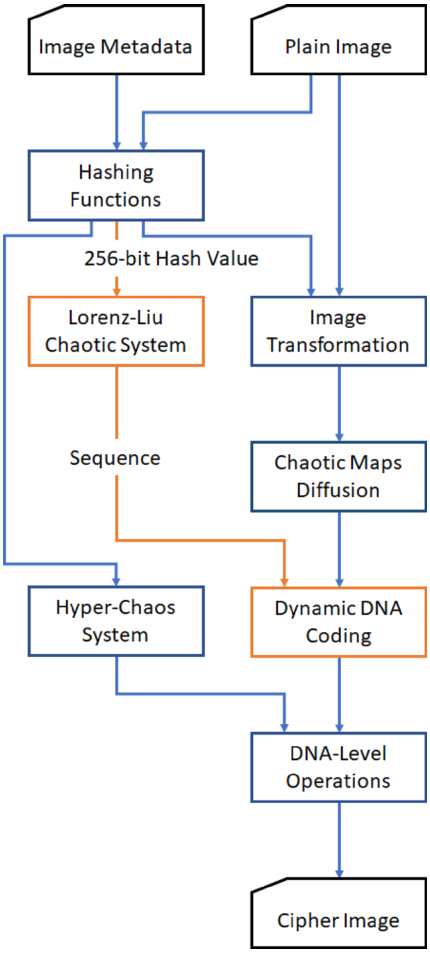

Fig. 1 Proposed encryption model

$$l_3 = (h_{21} + h_{22} + \ldots + h_{32})/(12 * max(h_{21}, h_{22}, \ldots, h_{32})) \quad (12)$$

λ is calculated by Eq. (13):

$$\lambda = mod((l_1 + l_2 + l_3 + m_1 + m_2 + m_3)/6, 0.02) \quad (13)$$

The secret key is $\{a, b, c, w_0, x_0, y_0, z_0, r_2, s_2, t_2, u, v, r_1, s_1, t_1, \lambda, m_1, m_2, m_3, l_1, l_2, l_3\}$, which are obtained in steps 2 and 3.

Step 4: Image transformation using Arnold transform. The image is provided to Arnold Transform using a, b, and c to obtain scrambled image I_1.

Table 2 Rules for DNA encoding

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

Step 5: Get coding rules using the Lorenz–Liu chaotic system. LLCS is iterated using the parameters and initial values, creating three sequences: L_1, L_2, and L_3. Equation (14) is applied to generate the coding rules for the chaotic sequence CR:

$$\mathrm{CR} = \mathrm{mod}\Big(\mathrm{floor}\Big(\mathrm{abs}(L_1) \times 10^3\Big), 8\Big) + 1. \tag{14}$$

Step 6: Hyper-chaos sequence generation. Memristor HCS is applied to initial values w_0, x_0, y_0, and z_0 to obtain four chaotic sequences, W, X, Y, and Z, which are applied to equations in model [7] resulting in three $M \times N$ sequences, Y_2, Z_2, and W_2.

Step 7: Encryption using chaotic maps. I1 is provided to sequences of five XOR operations within five chaotic maps, where the sequence of maps is Tent, Logistic, Piecewise, Gauss, and Henon maps: yielding I_2.

Step 8: Dynamic DNA coding of the image. I_2, W_2, Y_2, and Z_2 are binarized and DNA-encoded using the *CR* sequence to determine the coding rule for each two bits, creating $4 \times M \times N$ DNA sequences: I_2, W_2, Y_2, and Z_2.

Step 9: Applying DNA operations. I_2 and Y_2 are provided to the XOR operation, resulting in I_3. Then, Z_2 is added to I_3 to generate I_4 which is then sorted based on W_2 to achieve I_5.

Step 10: Dynamic DNA decoding. I_5 is DNA-decoded using *CR* and converted from binary to decimal, achieving cipher image C.

Proposed decryption model

The decryption model depends on the opposite operations applied in the encryption model. The HCS is applied on w_0, x_0, y_0, and z_0 creating chaotic sequences W, Y, and Z. Next, the CR sequence is achieved by applying LLCS on l_1, l_2, l_3, m_1, m_2, m_3, r_1, r_2, s_1, s_2, t_1, t_2, u, v, and λ. Afterward, the encrypted image *C,* in addition to W, Y, and Z, are DNA-encoded using CR. The created DNA sequences, I_5, W_2, Y_2, and Z_2, are supplied to inverse DNA operations: I_5 is inverse-sorted based on W_2 yielding I_4, Z_2 is subtracted from I_4 generating I_3 which is provided with Y_2 to the XOR operation to obtain I_2. Then, I_2 is DNA-decoded. Finally, XOR operations are applied to I_2 and the inverse sequence of chaotic maps, and the resulting matrix I_2 is provided to the Arnold Transform, obtaining the original image I.

Experimental evaluation

The model is implemented on a 64-bit machine with an Intel® Core™ i7-4500U CPU @ 1.80 GHz processor and 8 GB RAM in MATLAB R2021b platform on the Windows 10 operating system. The data set, the evaluation metrics, the evaluation results, and their interpretation are described in the following subsections:

Data set

The data set used for assessing the model holds the most popular ten 256 × 256 Gy-scale images: Cameraman, Lena, Baboon, House, Peppers, Barbara, QR code, Couple, White, and Black [12, 14, 16, 18–21, 24].

Experimental results

The experimental evaluation metrics are divided into five main categories: key analysis, differential attacks analysis, robustness analysis, statistical attacks analysis, and computational complexity analysis. Table 3 lists some of the comprehensive evaluation results of the proposed model. The following subsections describe the evaluation metrics in detail.

Key analysis

The strength of the key is one of the main purposes of encryption models. Therefore, the encryption model should have a strong key that is robust to attacks. The strength of the key is measured by the key space and its sensitivity to minor changes.

Key space analysis: The key space is calculated based on the number of variables and their probabilities, and its value should exceed 2^{100} [17, 28]. In the proposed model, the key contains $2^{256} \times 2^{128 \times 2} \times 10^{14 \times 4}$ of the parameters of the main module of [7]; the selected DNA-encoding rule for each two bits of the image (8 kinds); and the initial values in addition to the parameters of LCS and LLCS l_1, l_2, l_3, m_1, m_2, m_3, r_1, r_2, s_1, s_2, t_1, t_2, u, v, and λ. Therefore, the key space is:

$K = 2^{256} \times 2^{128 \times 2} \times 10^{14 \times 4} \times 2^8 \times 10^{15 \times 15} = 2^{1453}$, which is extremely higher than 2^{100}. This value signifies that the secret key is particularly safe, because it makes it very difficult for attackers to guess the proper values.

Key sensitivity analysis: The key sensitivity affects the robustness to brute force attacks. It is detected by changing a tiny part of the key and testing the retrieved image [29]. Some variables: $x_0, y_0, z_0, w_0, l_1, l_2, l_3, m_1, m_2, m_3, r_1, r_2, s_1, s_2, t_1, t_2, u, v$ and λ are altered by only the 10th digit before their decimal point by adding 10^{-10} to test key sensitivity on an image, for example, Lena image. The results on Lena image are shown in Figs. 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20 for variables x_0, y_0, z_0, w_0, l_1, l_2, l_3, m_1, m_2, m_3, r_1, r_2, s_1, s_2, t_1, t_2, u, v and λ. The results imply that the model is susceptible to these minor changes,

Table 3 Experimental results of the proposed model

Criteria	Cameraman	Lena	Baboon	House	Peppers	Barbara	QR Code	Couple	White	Black
NPCR	99.64%	99.61%	99.58%	99.62%	99.63%	99.62%	99.59%	99.63%	99.61%	99.56%
UACI	33.39%	33.42%	33.48%	33.52%	33.39%	33.39%	33.42%	33.45%	33.40%	33.44%
MSE	16,016	9010	8579	7733	11,957	7448	21,591	7697	21,774	21,712
PSNR	6.1	8.6	8.8	9.2	7.4	9.4	4.8	9.3	4.8	4.8
Information entropy	7.997	7.9975	7.9974	7.9976	7.9972	7.9973	7.9967	7.9976	7.9973	7.9974
Chi-square	275	225	236	221	256	248	300	222	248	233
Irregular deviation	4702	10,077	10,397	11,180	6928	11,596	1309	11,621	905	1
CCA horizontal	0.0033	0.0012	− 0.00002	0.0039	− 0.0023	0.002	0.0018	− 0.0025	0.0084	− 0.0063
CCA vertical	0.0003	− 0.0031	− 0.0006	0.0038	− 0.0024	0.0015	− 0.0012	0.0034	0.0008	0.0035
CCA diagonal	0.0067	0.0034	− 0.0016	− 0.0055	− 0.0067	− 0.0029	0.0013	− 0.003	0.0013	− 0.0028

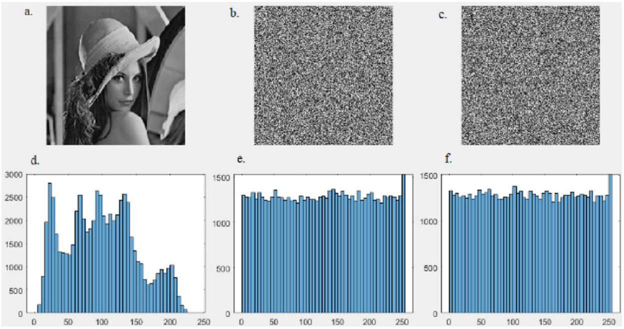

Fig. 2 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after x_0 change, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after x_0 change

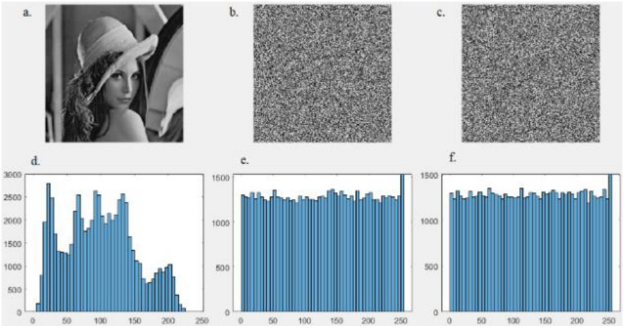

Fig. 3 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after y_0 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after y_0 changed

leading to difficulty in predicting the image under different attacks.

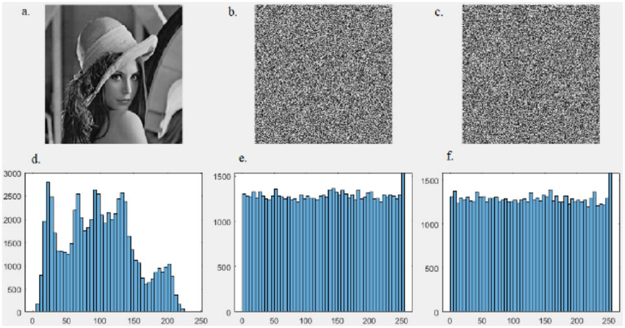

Fig. 4 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after z_0 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after z_0 changed

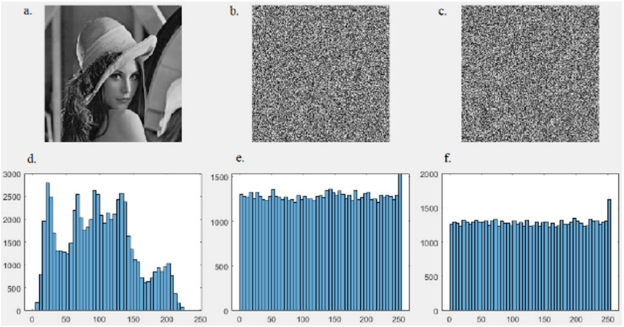

Fig. 5 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after w_0 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after w_0 changed

Differential attack analysis

Differential attacks analysis tests determine the link between the original image and the cipher image by measuring the sensitivity of the model to the original image. The analysis is applied by assessing the number of pixels change rate

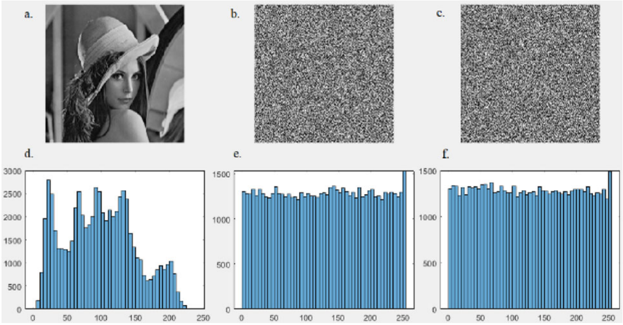

Fig. 6 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after l_1 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after l_1 changed

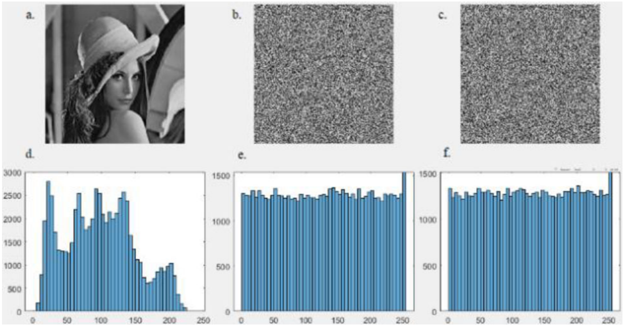

Fig. 7 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after l_2 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after l_2 changed

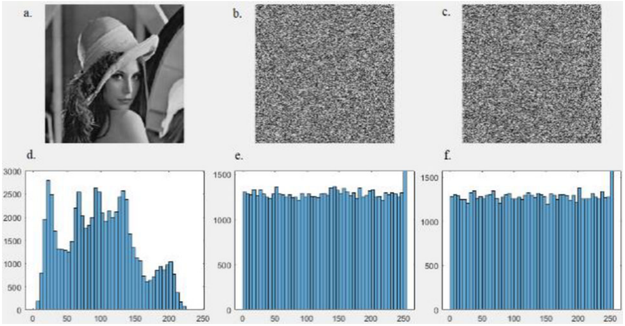

Fig. 8 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after l_3 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after l_3 changed

(NPCR) and the unified average changing intensity (UACI) which are described as follows.

Number of pixel change rate (NPCR): It determines the rate of changing the value of cipher image pixels before and after changing one pixel of the original image. It is calculated using Eqs. (15), (16) [7, 14, 30]:

$$\text{NPCR} = \sum_{i,j} \frac{D(i,\ j)}{MN} \times 100\% \tag{15}$$

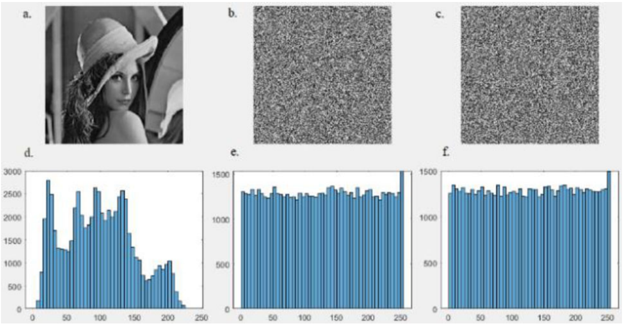

Fig. 9 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after m_1 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after m_1 changed

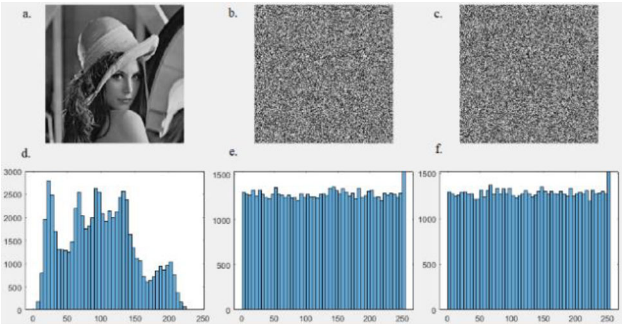

Fig. 10 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after m_2 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after m_2 changed

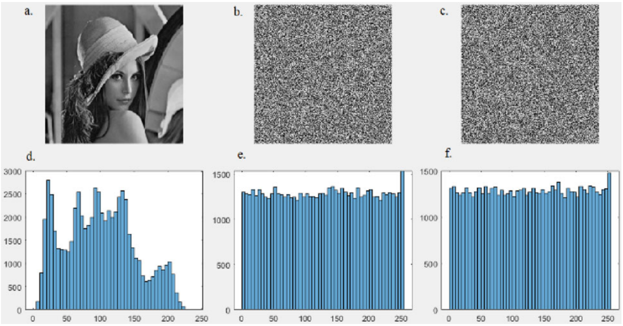

Fig. 11 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after m_3 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after m_3 changed

$$D(i,\ j) = \begin{cases} 0\, if\ C_1(i,\ j) = C_2(i,\ j) \\ 1\, if\ C_1(i,\ j) \neq C_2(i,\ j) \end{cases}, \tag{16}$$

where $C_1(i,\ j)$ and $C_2(i,\ j)$ are cipher image before and after one pixel changed. Moreover, the perfect value for NPCR is near 100% [31].

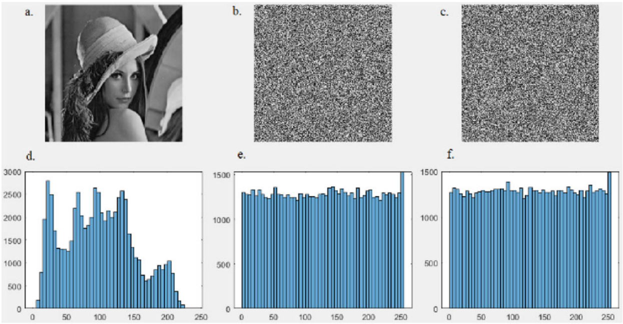

Fig. 12 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after r_1 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after r_1 changed

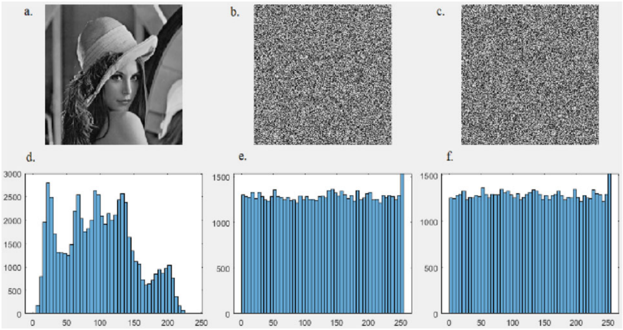

Fig. 13 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after r_2 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after r_2 changed

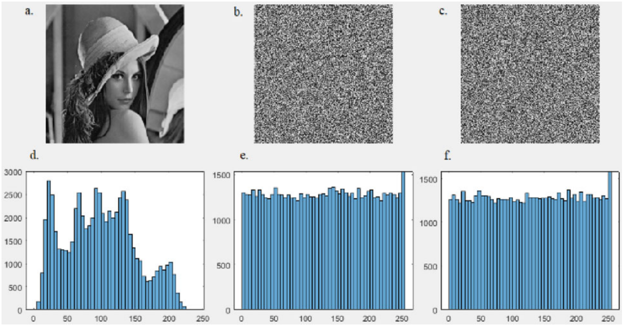

Fig. 14 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after s_1 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after s_1 changed

The proposed model results are compared to [16, 18–21, 24] results on Cameraman, Lena, Baboon, Peppers, White, and Black images in terms of NPCR in Table 4. The proposed model achieves higher results on Cameraman, Peppers, and White images with values of 99.64%, 99.63%, and 99.61%, respectively. On the other hand, the results are comparable to others on Lena, Baboon, and Black with values of 99.61%, 99.58%, and 99.56%, respectively. The proposed model is comparable to others with slightly higher performance.

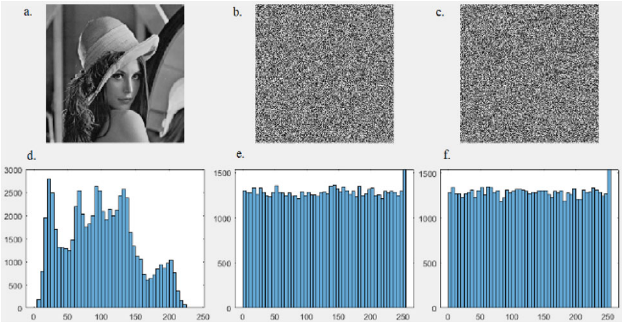

Fig. 15 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after s_2 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after s_2 changed

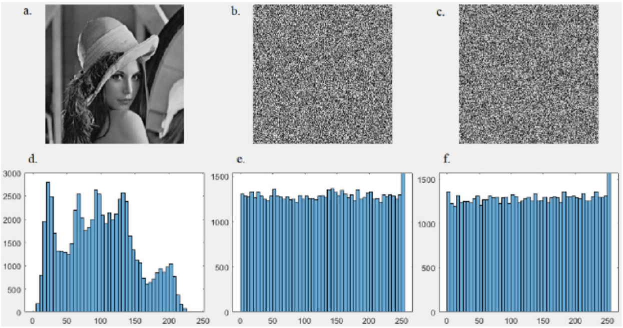

Fig. 16 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after t_1 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after t_1 changed

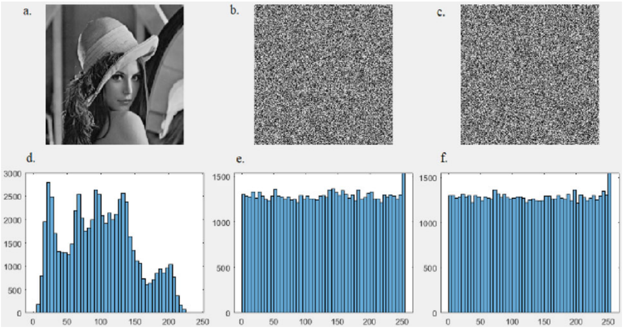

Fig. 17 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after t_2 changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after t_2 changed

Unified average changing intensity (UACI): It detects the average of the distance intensity between the cipher image before and after changing one pixel in the original image. The UACI value is calculated by Eq. (17) [7, 14, 30]:

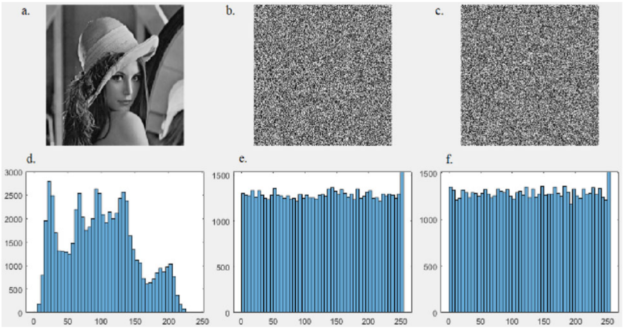

Fig. 18 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after *u* changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after *u* changed

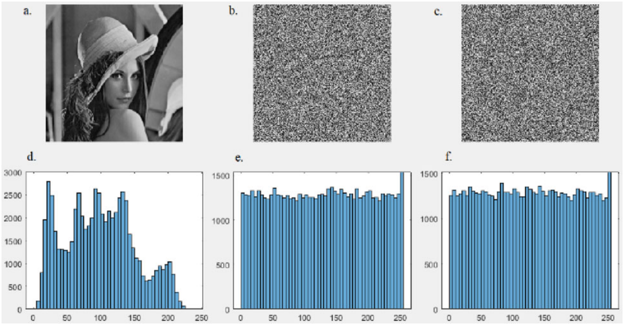

Fig. 19 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after *v* changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after *v* changed

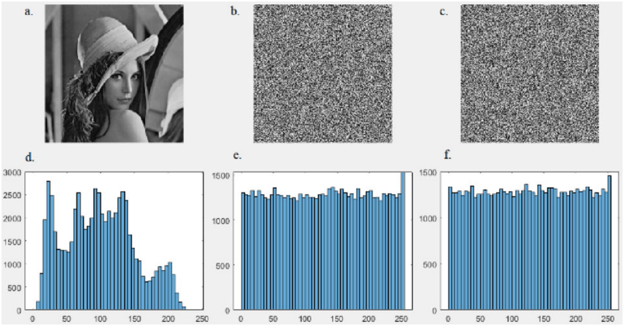

Fig. 20 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image after **λ** changed, **d** histogram of original image, **e** histogram of cipher image, **f** histogram of restored image after **λ** changed

$$\mathrm{UACI} = \sum_{i,j} \frac{|C_1(i,\ j) - C_2(i,\ j)|}{255 \times MN} \times 100\%, \tag{17}$$

where $C_1(i,\ j)$ and $C_2(i,\ j)$ are cipher image before and after changing one pixel. It is worth mentioning that the ideal value for UACI is near 33.33% [31].

With respect to UACI in Table 5, the proposed model results are compared to [16, 18–21, 24] results on Cameraman, Lena, Baboon, Peppers, White, and Black images. The proposed model surpasses the others on Cameraman, Lena, Peppers, and White images with values of 33.39%, 33.42%, 33.39%, and 33.4%, respectively. For Baboon and Black, the proposed model results are comparable to others with values of 33.48% and 33.44%, respectively. In general, the proposed model's efficiency slightly surpasses the others in respect of UACI.

Robustness analysis

The robustness of the model is analysed by applying mean square error (MSE) and peak signal-to-noise ratio (PSNR) analysis.

Mean square error test (MSE): It describes the diffusion characteristics of the model. It is calculated using Eq. (18) [7, 11]:

$$\mathrm{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,\ j) - C(i,\ j))^2, \tag{18}$$

where $I(i,\ j)$ and $C(i,\ j)$ are the values of pixel in the original and cipher images, respectively. The ideal value for MSE should be > 10,000 [13].

In terms of MSE, the proposed model results are compared to [18] on Cameraman, Lena, Baboon, Peppers, White, and Black images, as shown in Table 6. The model outperforms [18].

Peak signal-to-noise ratio (PSNR): It represents the peak of the error between the original and cipher images to describe the quality of the reconstruction of the image. It is calculated using Eq. (19) [11]:

$$\mathrm{PSNR} = 20 \log_{10}\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right). \tag{19}$$

The value of PSNR should be near 0 [11].

The proposed model results in Table 7 are compared to [18, 19] on Cameraman, Lena, Baboon, Peppers, White, and Black images regarding PSNR. The proposed model results surpass others on Cameraman, Lena, Peppers, White, and Black images with values of 6.1, 8.6, 7.4, 4.8, and 4.8. For the Baboon image, it is comparable to others with a minor difference of 0.3.

Statistical attacks analysis

The model should be robust to the statistical characteristics of the original images. Therefore, statistical analysis should be applied to the proposed model, including histogram analysis, information entropy, chi-square χ^2, irregular deviation ID, and correlation coefficient adjacent CCA.

Table 4 NPCR against other benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	99.61%	99.62%	NA	NA	NA	NA
[20]	99.61%	99.61%	NA	NA	NA	NA
[16]	NA	99.65%	NA	NA	NA	NA
[21]	99.63%	99.62%	NA	NA	99.6%	99.62%
[24]	NA	99.62%	NA	NA	NA	NA
[19]	99.6%	99.62%	99.6%	99.61%	NA	99.55%
Proposed model	99.64%	99.61%	99.58%	99.63%	99.61%	99.56%

Table 5 UACI against other benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	33.46%	33.47%	NA	NA	NA	NA
[20]	33.55%	33.59%	NA	NA	NA	NA
[16]	NA	33.45%	NA	NA	NA	NA
[21]	33.56%	33.5%	NA	NA	33.41%	33.54%
[24]	NA	30.64%	NA	NA	NA	NA
[19]	33.44%	33.44%	3.46%	33.46%	NA	33.4%
Proposed model	33.39%	33.42%	33.48%	33.39%	33.40%	33.44%

Table 6 MSE against other benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	9411	NA	NA	NA	NA	NA
Proposed model	16,016	9010	8579	11,957	21,774	21,712

Table 7 PSNR against other benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	8.4	NA	NA	NA	NA	NA
[19]	9.4	9.4	8.5	8.8	NA	NA
Proposed model	6.1	8.6	8.8	7.4	4.8	4.8

Histogram analysis: It describes the allocation of the pixel intensity values. The even distribution of the histogram implies great hiding of the image [9]. The results of the histogram of the images are represented in Figs. 21, 22, 23, 24, 25, 26, 27, 28, 29 and 30.

Information entropy: It measures the randomness of the images. It is calculated using Eq. (20) [32]:

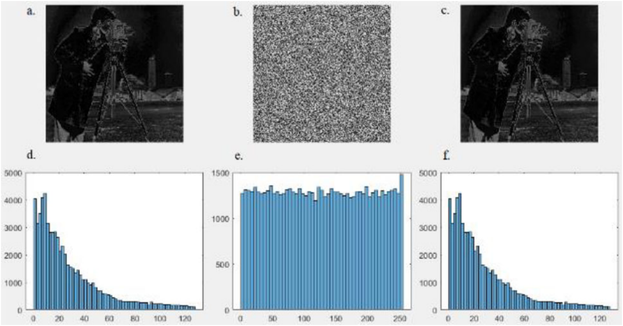

Fig. 21 Cameraman image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

$$H = -\sum_{i=1}^{M}\sum_{j=1}^{N}\big(p(C(i,\ j)) \times \log_{10} p(C(i,\ j))\big), \tag{20}$$

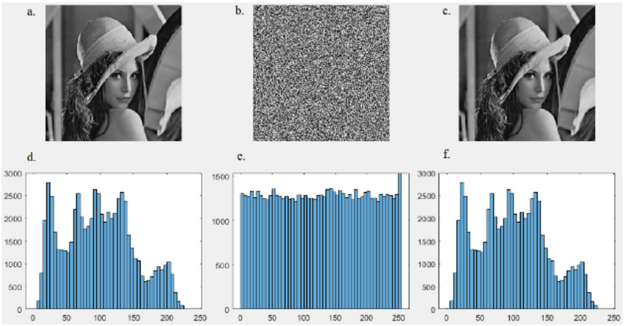

Fig. 22 Lena image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

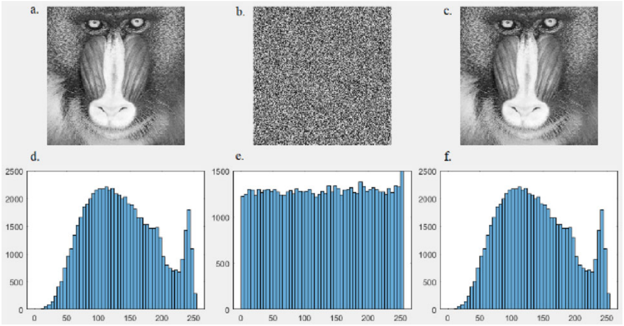

Fig. 23 Baboon image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

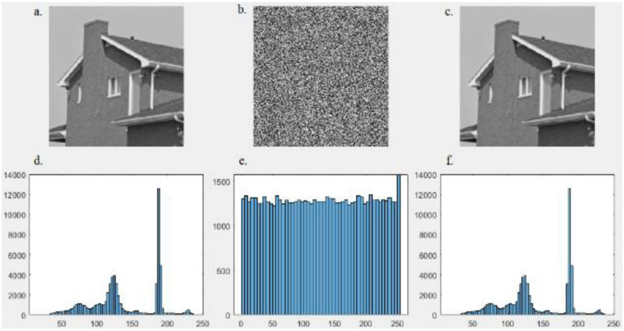

Fig. 24 House image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

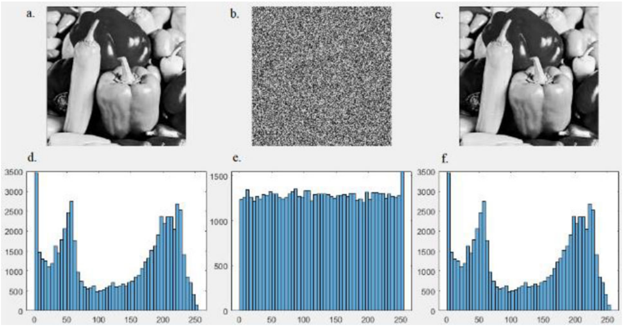

Fig. 25 Peppers image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

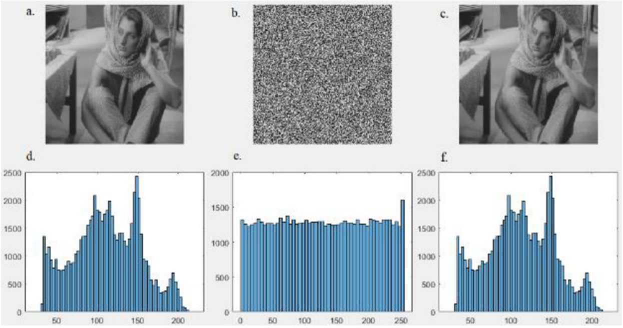

Fig. 26 Barbara image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

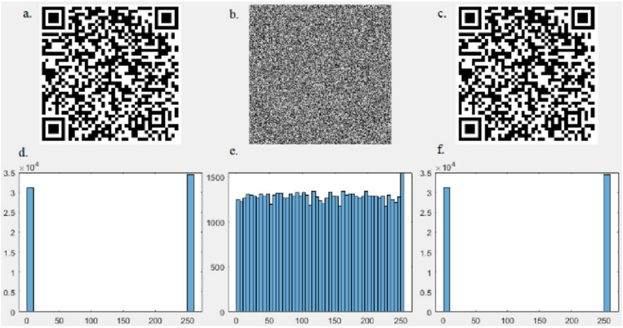

Fig. 27 QR Code image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

where $C(i,\ j)$ is the value of the pixel in the cipher image, $p(C(i,\ j))$ is the occurrence probability of $C(i,\ j)$. The ideal value for information entropy should be near 8 [33].

Table 8 compares the proposed model results to [16, 18–21, 24] results on Cameraman, Lena, Baboon, Peppers, White, and Black images in respect of information entropy. The results of the proposed model outperform others in Baboon and White images with values of 7.9974 and 7.9973, respectively, while being comparable to others in Cameraman, Lena, Peppers, and Black images with values of 7.997, 7.9975, 7.9972, and 7.9974, respectively. To sum up, the proposed model implies comparable performance with the other approaches.

Chi-square test: The test quantitatively describes the distribution of the values of image pixels and justifies their uniformity. It is calculated using Eq. (21) [18, 19]:

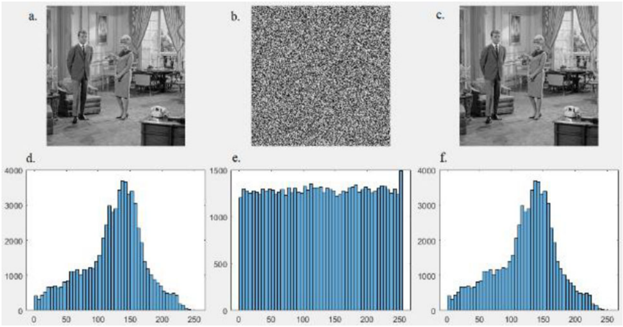

Fig. 28 Couple image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

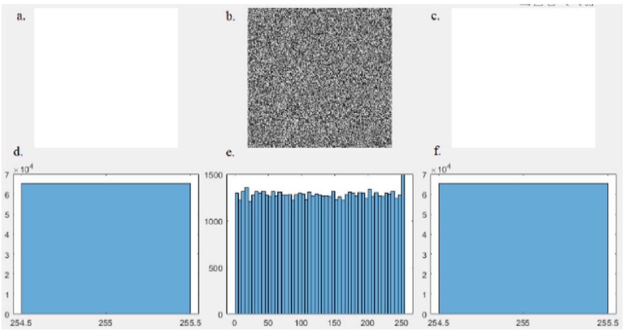

Fig. 29 White image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

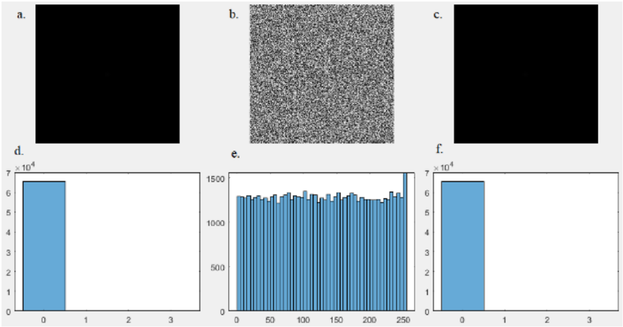

Fig. 30 Black image histogram. **a** Original image, **b** cipher image, **c** restored image, **d** original image histogram, **e** cipher image histogram, **f** restored image histogram

$$x^2 = \sum_{i=0}^{255} \frac{(x_i - \overline{x})^2}{\overline{x}}, \tag{21}$$

where x_i is the pixel value frequency, $\overline{x}$ is the average of pixel value frequencies from 0 to 255.

χ^2 test results are presented in Table 9. It is apparent that the values of the images are extremely high, ranging from 20,856 to 16,711,680. Yet, the values of encrypted images vary between 221 and 300, which implies a uniform distribution of pixel intensity when applying the proposed model.

Irregular deviation: It detects the variation of image deviation from uniform distribution by calculating the pixel deviation before and after the encryption process. Equation (22) [7, 12] calculates ID:

$$\mathrm{ID} = \sum_{i=0}^{255} |\mathrm{HD}_i - \mathrm{MH}|, \tag{22}$$

where HD_i is the histogram of the absolute values of the variation between the original image and the encrypted image, and MH is the HD average. The ideal value of ID should be the minimum to imply the uniformity of the histogram [34]. The results of the ID of the proposed model were shown earlier in Table 3.

Correlation coefficient adjacent (horizontal, vertical, diagonal): It calculates the similarity between each two adjacent pixels. It is calculated using Eq. (23) [35]:

$$\mathrm{cc} = \frac{\left|\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{A1}(i,j) - \overline{C_{A1}}(i,j)][C_{A2}(i,j) - \overline{C_{A2}}(i,j)]\right|}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{A1}(i,j) - \overline{C_{A1}}(i,j)]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{A2}(i,j) - \overline{C_{A2}}(i,j)]^2}}, \tag{23}$$

where $C_{A1}(i, j)$ and $C_{A2}(i, j)$ are gray-scale values of adjacent pixels, M and N are the image dimensions, $\overline{C_{A1}}(i, j) = \sum_{i=1}^{M}\sum_{j=1}^{N} C_{A1}(i, j)/MN$ and $\overline{C_{A2}}(i, j) = \sum_{i=1}^{M}\sum_{j=1}^{N} C_{A2}(i, j)/MN$. It is applied in horizontal, vertical, and diagonal directions. Its value for the original image should be near 100%, that for the encrypted image should be near 0%.

Table 8 Information entropy against other benchmark approaches

Model	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	7.9974	7.9974	NA	NA	NA	NA
[20]	7.9951	7.9951	NA	NA	NA	NA
[16]	NA	7.9973	NA	NA	NA	NA
[21]	7.9973	7.9969	NA	NA	7.9972	7.9973
[24]	NA	7.9973	NA	NA	7.9972	7.9975
[19]	7.9986	7.9989	7.9965	7.9975	NA	7.9971
Proposed model	7.997	7.9975	7.9974	7.9972	7.9973	7.9974

Table 9 χ^2 results

Criteria	Cameraman	Lena	Baboon	House	Peppers	Barbara	QR Code	Couple	White	Black
Plain Image	299,789	30,666	20,856	299,789	28,838	53,078	8,343,778	45,732	16,711,680	16,641,637
Encrypted Image	275	225	236	221	256	248	300	222	248	233

Table 10 CCA against other benchmark approaches

Model		Cameraman	Lena	Baboon	Peppers	White	Black
[18]	H	– 0.0013	0.0058	NA	NA	NA	NA
	V	0.0016	– 0.0051	NA	NA	NA	NA
	D	0.0058	– 0.003	NA	NA	NA	NA
[20]	H	0.0040	0.0088	NA	NA	NA	NA
	V	0.0088	0.0008	NA	NA	NA	NA
	D	0.0180	0.0022	NA	NA	NA	NA
[16]	H	NA	– 0.0016	NA	NA	NA	NA
	V	NA	0.0002	NA	NA	NA	NA
	D	NA	– 0.0035	NA	NA	NA	NA
[21]	H	– 0.0031	0.004	NA	0.0013	NA	0.005
	V	– 0.0006	– 0.0012	NA	0.0032	NA	0.0038
	D	0.0012	– 0.0021	NA	– 0.0068	NA	0.0026
[24]	H	NA	0.0084	NA	NA	NA	NA
	V	NA	– 0.0039	NA	NA	NA	NA
	D	NA	– 0.0013	NA	NA	NA	NA
[19]	H	0.0002	0.0002	0.0002	NA	0.0007	0.0012
	V	0.0001	0.0005	0.00005	NA	0.0005	0.0014
	D	0.0025	0.0024	0.0026	NA	0.0013	0.0022
Proposed model	H	0.0033	0.0012	– 0.00002	0.0084	– 0.0023	– 0.0063
	V	0.0003	– 0.0031	– 0.0006	0.0008	– 0.0024	0.0035
	D	0.0067	0.0034	– 0.0016	0.0013	– 0.0067	– 0.0028

Regarding CCA, the proposed model results are compared to [16, 18–21, 24] results in Table 10 on Cameraman, Lena, Baboon, Peppers, White, and Black images. The results are comparable to others and tend to be zero [36]. To detect the improvement of the model, the average CCA is applied using Eq. (24) [14]:

$$\text{Correlation coefficient} = (|\text{HC}| + |\text{VC}| + |\text{DC}|)/3, \qquad (24)$$

where HC, VC, and DC are the correlation coefficient horizontally, vertically, and diagonally, respectively.

In Table 11, it is obvious that the proposed model results overcome the others on the Baboon image with a value of 0.0007 while being comparable to others on Cameraman, Lena, Peppers, White, and Black images with values of 0.0034, 0.0026, 0.0038, 0.0035, and 0.0042, respectively.

Table 11 CCA average against other benchmark approaches

Criteria	Cameraman	Lena	Baboon	Peppers	White	Black
[18]	0.0029	0.0046	NA	NA	NA	NA
[20]	0.0103	0.0039	NA	NA	NA	NA
[16]	NA	0.0018	NA	NA	NA	NA
[21]	0.0016	0.0024	NA	NA	0.0038	0.0038
[24]	NA	0.0045	NA	NA	NA	NA
[19]	0.0009	0.001	0.001	0.0008	NA	0.0016
Proposed model	0.0034	0.0026	0.0007	0.0038	0.0035	0.0042

Computational complexity analysis

Computational complexity measures the steps executed in the encryption model [15]. The computational complexity of the main module of [7] is $O(M \times N)$. The computational complexity of generating the sequence of coding rules is $O(4 \times M \times N)$. Therefore, the proposed model's computational complexity is $O(M \times N + 4 \times M \times N) \approx O(M \times N)$, which is linear and depends on the original image size.

Results interpretation

Evaluating the proposed model against recent models was challenging. Two main factors influenced the choice of the benchmark approaches. First is the evaluation metrics factor, where a minimum of four metrics should be used. The second factor is the number of images in the data set. Existing models were assessed using different numbers of images. Only one model [19] was applied to five images, one model [21] was applied to four images, one model [24] was applied to three images, whereas models [18, 20] were applied to two images, and one model [16] was applied to one image.

The models represent different techniques for dynamic DNA coding. The technique of a coding rule for the image is represented in [16], whereas the technique of a coding rule for each block in the image is represented in [18, 19]. Meanwhile, the technique of a coding rule for each row in block is represented in [20], the technique of a coding rule for each pixel is represented in [21], and the model of [24], in addition to the proposed model, represents the technique of a coding rule for every 2 bits of the image.

As shown in the experimental results section, the robustness of the model to statistical attacks depends on both the structure of the encryption model and the color intensity of different images. The diversity of the encryption layers and their number affect the distribution of the pixel values' intensity in the encrypted image. This effect is demonstrated by information entropy and CCA. Moreover, the color distribution of the image has a great effect on its robustness to statistical attacks. By studying the histogram of the original images, the images with a more uniform distribution of the histogram perform better in terms of CCA, information entropy, and the X^2 test. In contrast, by decreasing the uniformity of the histogram of the original images, the irregular deviation tends to the ideal value.

Also, the structure of the encryption model has a great impact on the generation of the encrypted image and its robustness for extracting the original image. Increasing the encryption layers with various properties and the applied technique of dynamic DNA coding led to the generation of an encrypted image with completely different pixel values. Some algorithms, such as shuffling algorithms [7, 14, 18, 20, 21, 24], change the position of the pixel value, which generates randomness in the image. Other algorithms [7, 10, 16, 19] change the value of the pixel, for example, addition, subtraction, and XOR operations. This effect is supported by the results of MSE and PSNR listed in Tables 6 and 7. Besides, the dynamic DNA-coding technique used also affected the results of MSE and PSNR. The technique increases the difference between the pixel values of the original image and the cipher image.

Furthermore, the layers of generation of the key affect the robustness of the model to differential attacks. These layers increase the level of security of the model, generating a more secure encrypted image. The sensitive algorithms used in key generation imply an effect on the security of the proposed model, which is proven by the results of NPCR and UACI in Tables 4 and 5. In addition to the proposed model, models in [16, 21] have an extremely sensitive algorithm for generating the key. These models imply superior performance in NPCR and UACI. The sensitivity of the key also supports this effect.

In general, the structure of the encryption model, the dynamic DNA-coding technique used, the sensitivity of the key generation, and the variation of the color intensity of the original images are cornerstones of the security of the proposed model. The results of the information entropy, CCA, and X^2 test are affected by the image characteristics and encryption model. The encryption model also affects, in addition to the dynamic DNA-coding technique, the results of MSE and PSNR. The algorithms used in key generation and their sensitivity affect NPCR and UACI.

Conclusion

Dynamic DNA coding has recently been shown to have a crucial role in image encryption. It increases the randomness of the images and strengthens the model's security. This study proposes a grayscale image encryption model with dynamic DNA coding. The original image and its metadata are hashed using the MD5 and SHA-256 procedures to generate a secret key. The image is then provided to the Arnold Transform method. The key is then assigned to HCS, which creates three chaotic sequences. The coding rules' sequence is subsequently generated by LLCS using the key. The Arnold transform's resulting image then gets dispersed outward using five chaotic maps. The last step in the process is to perform DNA operations using the chaotic sequences generated by HCS after DNA-encoding the resultant image using the coding rules sequence. The cipher image is then obtained by applying DNA-decoding to the image.

The model is assessed based on key analysis, differential attack analysis, robustness analysis, statistical attack analysis, and computational complexity analysis. Cameraman, Lena, Baboon, House, Peppers, Barbara, QR code, Couple, White, and Black were used as the ten prevalent images for the evaluation. Twelve metrics are used during the evaluation, including key space, key sensitivity, NPCR, UACI, MSE, PSNR, histogram, information entropy, χ^2, ID, CCA, and computational complexity.

The proposed model's key space is 21,453, and the results of the NPCR and UACI tests ranged between 99.56% and 99.64% and 33.39% and 33.48%, respectively. The results for MSE varied from 8579 to 21,774, while those for PSNR varied from 4.8 to 8.8. According to the results, the information entropy varied between 7.997 and 7.9976. The χ^2 test had a range of 221 to 300, but the ID test had a range of 1 to 11,621 results. Between 0.0007 and 0.0042 were the results of the average CCA. The proposed model is O(4MN) in terms of complexity. In terms of NPCR, UACI, MSE, and PSNR, the model outperforms others. Information entropy and CCA are comparable to those of other models. The cipher image will be incorporated into a DNA sequence to strengthen the model's security, in addition to enhancing the runtime of the model in the future.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). On behalf of all authors, the corresponding author states that there is no fund received for this work.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Tekli J (2022) An overview of cluster-based image search result organization: background, techniques, and ongoing challenges. Knowl Inf Syst 64:589–642
2. Prakash CD, Karam LJ (2021) It Gan do better: GaN-based detection of objects on images with varying quality. IEEE Trans Image Process 30:9220–9230
3. Shen L, Tao H, Ni Y, Wang Y, Stojanovic V (2023) Improved YOLOv3 model with feature map cropping for multi-scale road object detection. Meas Sci Technol 34:045406
4. Song X, Wu C, Stojanovic V, Song S (2023) 1 bit encoding–decoding-based event-triggered fixed-time adaptive control for unmanned surface vehicle with guaranteed tracking performance. Control Eng Pract. https://doi.org/10.1016/j.conengprac.2023.105513
5. Al Sobbahi R, Tekli J (2022) Low-light image enhancement using image-to-frequency filter learning. In: Sclaroff S, Distante C, Leo M, Farinella GM, Tombari F (eds) Image analysis and processing—ICIAP 2022. Springer International Publishing, Cham, pp 693–705
6. Sanober A, Anwar S (2022) Crytographical primitive for blockchain: a secure random DNA encoded key generation technique. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-13063-z
7. Sharkawy NH, Afify YM, Gad W, Badr N (2022) Gray-scale image encryption using DNA operations. IEEE Access 10:63004–63019
8. Wang X, Li Y (2021) Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Opt Lasers Eng. https://doi.org/10.1016/j.optlaseng.2020.106393
9. Wang X, Xue W, An J (2021) Image encryption algorithm based on LDCML and DNA coding sequence. Multimed Tools Appl 80:591–614
10. Tian J, Lu Y, Zuo X, Liu Y, Qiao B, Fan M, Ge Q, Fan S (2021) A novel image encryption algorithm using PWLCM map-based CML chaotic system and dynamic DNA encryption. Multimed Tools Appl 80:32841–32861
11. Elamir MM, Al-atabany WI, Mabrouk MS (2021) Hybrid image encryption scheme for secure E-health systems. Netw Model Anal Health Inform Bioinform. https://doi.org/10.1007/s13721-021-00306-6
12. El-Khamy SE, Korany NO, Mohamed AG (2020) A new fuzzy-DNA image encryption and steganography technique. IEEE Access 8:148935–148951
13. Xu J, Mou J, Xiong L, Li P, Hao J (2021) A flexible image encryption algorithm based on 3D CTBCS and DNA computing. Multimed Tools Appl 80:25711–25740
14. Zhang Y, Zhang L, Zhong Z, Yu L, Shan M, Zhao Y (2021) Hyperchaotic image encryption using phase-truncated fractional Fourier

transform and DNA-level operation. Opt Lasers Eng. https://doi.org/10.1016/j.optlaseng.2021.106626
15. Aouissaoui I, Bakir T, Sakly A (2021) Robustly correlated key-medical image for DNA-chaos based encryption. IET Image Process 15:2770–2786
16. Signing VRF, Mogue RLT, Kengne J, Kountchou M, Saïdou (2021) Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption. Multimed Tools Appl 80:32689–32723
17. Uddin M, Jahan F, Islam MK, Rakib Hassan M (2021) A novel DNA-based key scrambling technique for image encryption. Complex Intell Syst 7:3241–3258
18. Wang X, Du X (2022) Chaotic image encryption method based on improved zigzag permutation and DNA rules. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-13012-w
19. Mohamed AG, Korany NO, El-Khamy SE (2021) New DNA coded fuzzy based (DNAFZ) S-boxes: application to robust image encryption using hyper chaotic maps. IEEE Access 9:14284–14305
20. Bao W, Zhu C (2022) A secure and robust image encryption algorithm based on compressive sensing and DNA coding. Multimed Tools Appl 81:15977–15996
21. Zhang S, Liu L (2021) A novel image encryption algorithm based on SPWLCM and DNA coding. Math Comput Simul 190:723–744
22. Zhu S, Zhu C (2020) Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. Entropy. https://doi.org/10.3390/e22070772
23. Li N, Sun J, Wang Y (2019) A novel memcapacitor model and its application for image encryption algorithm. J Electr Comput Eng. https://doi.org/10.1155/2019/8146093
24. Wang J, Zhi X, Chai X, Lu Y (2021) Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-10413-7
25. De Dieu NJ, Ruben FSV, Nestor T, Zeric NT, Jacques K (2022) Dynamic analysis of a novel chaotic system with no linear terms and use for DNA-based image encryption. Multimed Tools Appl 81:10907–10934
26. Shen Y, Zou T, Zhang L, Wu Z, Su Y, Yan F (2022) A novel solar radio spectrogram encryption algorithm based on parameter variable chaotic systems and DNA dynamic encoding. Phys Scr. https://doi.org/10.1088/1402-4896/ac65bf
27. Liu C, Liu T, Liu L, Liu K (2004) A new chaotic attractor. Chaos Solitons Fractals 22:1031–1038
28. Paul LSJ, Gracias C, Desai A, Thanikaiselvan V, Suba Shanthini S, Rengarajan A (2022) A novel colour image encryption scheme using dynamic DNA coding, chaotic maps, and SHA-2. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-13095-5
29. Liu X, Tong X, Wang Z, Zhang M (2022) A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation. Multimed Tools Appl 81:21779–21810
30. Chen X, Gong M, Gan Z, Lu Y, Chai X, He X (2022) CIE-LSCP: color image encryption scheme based on the lifting scheme and cross-component permutation. Complex Intell Syst. https://doi.org/10.1007/s40747-022-00835-1
31. Folifack Signing VR, Fozin Fonzin T, Kountchou M, Kengne J, Njitacke ZT (2021) Chaotic jerk system with hump structure for text and image encryption using DNA coding. Circuits Syst Signal Process 40:4370–4406
32. Yoosefian Dezfuli Nezhad S, Safdarian N, Hoseini Zadeh SA (2020) New method for fingerprint images encryption using DNA sequence and chaotic tent map. Optik (Stuttg). https://doi.org/10.1016/j.ijleo.2020.165661
33. Liu M, Ye G (2021) A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm. Math Biosci Eng 18:3887–3906
34. Ahmed N, Shahzad Asif HM, Saleem G (2016) A benchmark for performance evaluation and security assessment of image encryption schemes. Int J Comput Netw Inf Secur 8:28–29
35. Wang X, Zhu X, Zhang Y (2018) An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access 6:23733–23746
36. Hu W-W, Zhou R-G, Jiang S, Liu X, Luo J (2020) Quantum image encryption algorithm based on generalized Arnold transform and Logistic map. CCF Trans High Perform Comput 2:228–253

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