Alrubaie *et al.*
Journal of Engineering and Applied Science (2023) 70:60
https://doi.org/10.1186/s44147-023-00228-2

Journal of Engineering and Applied Science

RESEARCH Open Access

Image encryption based on 2DNA encoding and chaotic 2D logistic map

Asmaa Hasan Alrubaie[1*], Maisa'a Abid Ali Khodher[2] and Ahmed Talib Abdulameer[3]

*Correspondence: cs.20.41@grad.uotechnology.edu.iq

[1] Computer Sciences Department, University of Technology-Iraq, Baghdad, Iraq
[2] Computer Engineering Department, University of Technology-Iraq, Baghdad, Iraq
[3] IT Department, Middle Technical University, Baghdad, Iraq

Abstract

DNA has recently been investigated as a possible medium concerning ultra-compact information storage and ultra-scale computation. The development of secure image encryption systems has recently received a certain effective and new direction from chaos-based cryptographic algorithms. This paper proposes a novel image encryption algorithm, *2DNALM*, based on double-dynamic DNA sequence encryption and a chaotic 2D logistic map. The three phases regarding the suggested approach are as follows: the first phase involves permuting the positions of the pixels using a position key-based scrambling operation. The second phase involves double DNA encoding on scrambled images using various rules by DNA cryptography concept to produce an encoded image, and in the final step, an image which has been encoded is encrypted using XOR operation and chaotic keys created through a chaotic 2D logistic map. The entropy analysis and experimental findings show that the suggested scheme exhibits great encryption and withstands several common attacks.

Keywords: Image encryption, Image diffusion, Image scrambling, Chaotic 2D logistic maps, 2DNA encoding

Introduction

Recently, there has been an increased demand for secure communication systems for transferring sensitive information, including images, to prevent unauthorized access to important information. Encryption to change the transmitted data's shape is one way to achieve secure communication. An encryption technique and a secret key are used during the encryption process for encrypting the data. Across a wide range of applications, image encryption uses various encryption techniques. As a result, image encryption has emerged as a popular and efficient method for guaranteeing the security of image transmission [1].

Before data is transmitted across an unsecured channel, encryption is defined as transforming it into a structure difficult for unauthorized individuals to decipher or understand. Decryption, opposite to encryption [2], transforms the data into a readable state. Chaos theory is currently referred to as the science of unpredictability. It handles nonlinear events whose behavior is challenging to control or predict. Since it accurately captures the system's complexity, a crucial characteristic in various applications, chaos theory has garnered much interest. This attribute significantly affects cryptography and

its three primary features (positive Lyapunov exponent, sensitive dependence on initial condition, ergodicity, and stochasticity) [3]. It can produce pseudo-random sequences that can be utilized as encryption keys. It takes two steps to create chaotic coding systems: scrambling and diffusion. Scrambling involves shifting the locations of image pixels according to the key—the process of distribution changes pixel values in an image. The two methods produce a new encoded image different from the original [4, 5].

The two-dimensional logistic map used for image encryption is unlike the conventional one-dimensional logistic map; the two-dimensional logistic map has chaotic behaviors—two dimensions with both basins and attractors in evolution. Consequently, the pseudo number sequences generated from the two-dimensional logistic map for image encryption are more random-like and complicated [6].

In living things, genetic information is passed down from generation to generation via deoxyribonucleic acid (DNA). T (thymine), G (guanine), C (cytosine), and A (adenine) are the four major bases. Following its [0, 1] encoding, these are employed in the encryption procedure [7]. One of the coding methods used is DNA coding, which transforms the pixels of a plain image into DNA format utilizing DNA's basic rules. Due to its large storage capacity, parallel processing ability, and other benefits, DNA coding technology can be defined as significant encryption technology. As a result, various researchers have worked to create a variety of cryptosystems depending on DNA technology. Furthermore, DNA coding technology generates an encoded image which differs from the plain image [8].

The benefits of both methods are combined in the case when DNA coding and chaotic coding are used. This mixing results in a robust coding system with high entropy, which is complicated for attackers to attack [9, 10].

This paper suggested that the image encryption algorithm for the first time is 2DNALM based on a combination of double dynamic DNA sequence encryption and chaotic 2D Logistic Map. In the beginning, scrambling for the image is achieved to boost security before using 2DNA coding by applying various rules from Table 1. The outcome is an encoded image encrypted through a chaotic 2D logistic map utilized to generate chaotic keys. The paper focuses on encrypting the image faster than other existing algorithms [11], with more complex chaotic behaviors found in 2D logistic maps than in 1D. This mix protects the suggested technique from differential, statistical, and brute-force attacks. This study's remaining sections are organized in the following way. Related work

Table 1 The encoding and decoding map

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

has been explained in Sect. 2 of the presented work. The chaotic 2D logistic map's preliminaries are described in Sect. 3. Preliminaries of 2DNA encoding are illustrated in Sect. 4. The proposed approach's implementation is described in Sect. 5. The results of an experiment are shown in Sect. 6. The findings of the security analysis have been illustrated in Sect. 7. The relevant findings are provided in Sect. 8.

Related work

Due to the significant degree of pixel correlation in the images and the difficulty in designing an effective image encryption method, chaotic systems are frequently used to generate secret keys in image encryption. A new algorithm of image encryption depending on an established bit-level image encryption method using chaos theory, DNA coding, and the random grid was presented in [2020]. Those security keys are used to dilute and confuse the input images to decrypt the photos. An input image's pixel positions can be changed using permutation operation, and diffusion modifies the values of pixels in an input image. Guanine (G), adenine (A), cytosine (C), and thymine (T) coding sequences are used as information carriers in DNA computing, which has significant benefits in storage capacity, energy consumption, and parallelism. In conjunction with other DNA coding techniques, chaotic mapping transmits image data via DNA coding, producing an effective encryption mechanism [12].

The need for an effective and reliable RGB image encryption method has increased since D. Ibrahim et al. announced their color image encryption approach in 2022. It is one of the most significant fields receiving greater attention for image protection. RGB image encryption guarantees confidentiality regarding color images throughout transmission and storage by combining chaotic logistic functions with multiple DNA encoding rounds. This method produces extremely promising and effective results regarding randomness, nonlinearity, and resistance to common attacks. However, a reliable, effective, and secure method against many threats is still required [11].

Huda Rashid Shakir and colleagues suggested several methods to encrypt image data in [2022], the most effective and popular of which is chaotic-based encryption because it fits the essential characteristics of cryptography by being sensitive to the initial state, randomness, and nonlinear. Because of the DNA molecule's many benefits, including its extremely low power consumption, strong parallel processing ability, and large data capacity, image encryption using DNA, and chaotic systems combined for achieving high degrees of security is effective for color images. Yet, image encryption consisting of chaotic systems and DNA encoding has specific disadvantages, such as independency regarding the key generation approach from the original image, the slow encryption speed, and limitations of DNA operations. The research revealed that unique DNA encoding and 4D-hyperchaotic systems were presented as solutions to the abovementioned issues. Initially, chaotic sequences permute the positions of the pixels. Second, according to DNA cryptography, the DNA encoding sequence is subjected to various operations, including DNA XOR, DNA addition, DNA subtraction, shift left, and shift right, to encrypt color images and produce effective encryption results [13].

The need for information security has become urgent due to the constantly changing nature of the Internet and wireless communications and the daily generation of enormous volumes of multimedia. Mohamed Gabr et al. suggested a 3-stage image

cryptosystem approach in 2022. A tan variation of the logistic map is utilized to carry out deoxyribonucleic acid (DNA) encoding in the first stage. For the second encryption stage, the numerical solution of the Lorenz differential equations and a linear descent algorithm are jointly employed to build a robust S-box. The logistic map in its original form is utilized in the third stage. Diffusion is guaranteed through the first and third encryption stages, while confusion is certified through applying the S-box in the second encryption stage. They carry out the confusion and diffusion-inducing steps, resulting in encrypted images that are completely asymmetric to their original (plain) counterparts. Combining DNA cryptography with chaotic functions and S-boxes in image encryption algorithms provided many security measures that enhanced the amount of data confidentiality and achieved better performance [14].

Every image encryption algorithm aims to generate a noisy image's top-quality to keep information secret. Additionally, digital communication has become broader by the fast development of Internet technology. People can send digital images on the Internet anytime and anywhere. It has resulted in the development of digital image encryption. Recently, many scholars have combined DNA technology with chaos theory and applied them in the field of image encryption. Simiao Wang et al. The proposed combines a four-dimensional chaotic system with DNA technology to design a color image encryption algorithm [2022]. The algorithm converts each pixel value into two 4-bit binary using the windmill-like scanning scrambling method (WSSM). The proposed 4D chaotic system generates four sequences to determine the DNA encoding, decoding, and calculation rules. Finally, the three R, G, and B matrices are divided into blocks and scrambled. And by this, the image encryption algorithm can effectively resist various attacks [15].

Digital images are widely used in numerous fields of society with ever-increasing developments in computer network technology. On the other hand, the security of the digital image is threatened critically. We should take precautions to prevent illegal data and information distribution. Digital images are supposed to be built, transmitted, and received securely. Because of this, cryptography becomes an effective way to transmit images securely. For this purpose, Melih Yildirim proposed using deoxyribonucleic acid (DNA) encoding as an encryption method with Rössler in [2022]. The number of DNA encoding rules in the proposed study has excessively increased compared to previous studies on DNA encoding techniques. Rössler attractor is employed as a chaotic system consisting of three differential equations. Thus, the security of the encryption scheme is enhanced [16].

Encryption algorithms are one of the methods to protect data during its transmission through an unsafe transmission medium. But encryption methods need a lot of time during encryption and decryption, so it is necessary to find encryption algorithms that consume little time while preserving the security of the data. Rawia Abdulla Mohammed and colleagues suggested a method to encrypt images in 2023; this method combined more than one algorithm to obtain high security with a short implementation time. A chaotic system, DNA computing, and Salsa20 were integrated. A proposed 5D chaos system was used to generate more robust keys in a Salsa algorithm and DNA computing. Also, the confusion is performed using a new SBox. The proposed chaos system achieves three positive Lyapunov values. So results demonstrate that the proposed scheme has a sufficient peak signal-to-noise ratio, a low correlation, and a large key space. These

factors make it more efficient than its classical counterpart and can resist statistical and differential attacks [17].

The limitations of related works are the following:

Year	authors	The limitations
2020	Babu M, et al	The techniques utilize a single encryption algorithm for encrypting the entire data, posing a security threat. Therefore, this paper has adapted multiple image encryption algorithms for each segmented image to enhance security. Due to this, the complexity of the proposed algorithm is increased, thereby making the proposed framework vulnerable to attacks and taking more time to encrypt the image
2022	Dina Ibrahim et al	The running time of the proposed technique on a core i5 processor with 8 GB of RAM, the proposed approach takes 7–9 s on average to encrypt a 256 × 256 RGB image. However, the proposed algorithm is 16 rounds, which is a lot of work. A smaller number of rounds, such as 4 rounds of DES, can be used to reduce time constraints, and it is still robust and secure
2022	Huda Rashid Shakir et al	Because employing only DNA to encode images is insecure, recent research combined DNA coding with chaotic systems to improve image encryption techniques. However, image encryption made up of DNA encoding and chaotic systems has certain drawbacks, like the independency of the key generation method from the original image, the limitations of DNA operations, and the slow encryption speed
2022	Mohamed Gabr et al	The proposed S-box design did not score optimal values in all metrics. Due to not achieving better values in all evaluation metrics, the Lorenz system constructs the S-box; the Lorenz system is continuous, with its computation heavily depending on the numerical method adopted in solving it. A better choice would be any discrete chaotic function
2022	Simiao Wang et al	The chaotic sequences are generated by a Sine-Logistic map to obtain better results. We can design more complex composite discrete hyper chaotic dynamical systems with different simple chaotic systems, such as a 2-dimensional logistic-modulated-sine-coupling-logistic chaotic map (LSMCL). We use the logistic map to modulate the Sine map and couple the result of the modulation and Sine map together. Compared with other existing chaotic maps, we can observe that LSMCL has better chaotic performance in terms of chaotic trajectory, Lyapunov exponent, and Kolmogorov entropy
2022	Melih Yildirim	In the proposed study, the number of DNA encoding rules has excessively increased compared to previous studies on DNA encoding techniques, which leads to slow encryption speed
2023	Rawia Abdulla Mohammed et al	Even though the proposed scheme has useful applications in image transmission, it still requires profound improvement in implementing the high-intelligence scheme and verifying its feasibility on devices with the Internet of Things (IoT) enabled

Preliminaries of chaotic 2D logistic map

In the investigation of dynamic nonlinear systems, chaotic maps frequently appear. Mathematical equations govern its behavior, and even a small alteration in the initial position could result in a noticeably different result. Although they appear disorganized and random, they follow certain patterns. A cryptosystem's diffusion and confusion operations involve chaotic output signals that exhibit random statistical features. The control system used to generate chaotic maps could be complex or simple; thus, the chaotic maps show characteristics of chaotic systems. Several well-known maps include logistic, quadratic, tent, and others. There are two fundamental problems with chaos-based cryptography: (a) 1D chaotic maps that do not meet the characteristic of unpredictability and (b) high-dimensional (HD) chaotic maps that, despite having chaotic and complex behavior, demand more processing complexity [18].

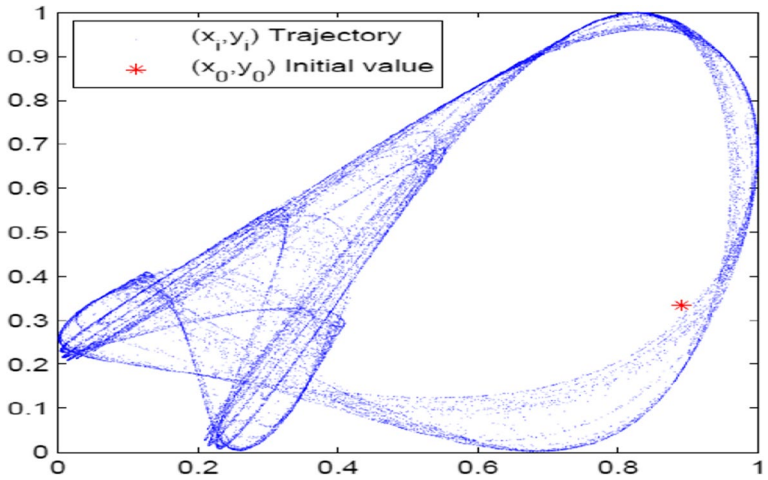

Fig. 1 shows the 2D logistic map trajectory

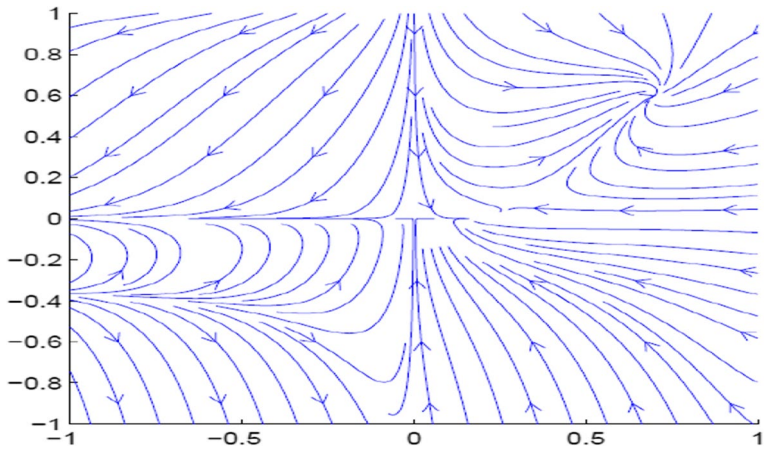

Fig. 2 Shows the 2D logistic map phase portrait

More complex chaotic behaviors can be found on a 2D logistic map compared to 1D. Equation (1), in which (xi; yi) is the pair-wise point at *i*th iteration, and *r* represents the system parameter, could be used to define such a 2D logistic map mathematically [19] discretely.

$$2-D \text{ Logistic map}: \begin{cases} \text{xi}+1=\text{r}(3\text{yi}+1)\text{xi}(1-\text{xi}) \\ \text{yi}+1=\text{r}(3\text{xi}+1+1)\text{yi}(1-\text{yi}) \end{cases} \tag{1}$$

A scatter plot of 30,000 points from the trajectory is shown in Fig. 1. The 2D logistic map with initial value (x_0, y_0) at (0:8909; 0:3342) and the parameter $r=1.19$.

For $r=1.19$, Fig. 2 depicts the phase portrait regarding the 2D logistic map. Such phase portrait agrees with the 2D logistic map's mathematical representation for $r=1.19$. An (x; y) trajectory about chaotic behavior is random-appearing yet is entirely predictable in the case where r and (x_0, y_0) are both known; hence, it could be utilized as the pseudo-number generator for cryptograph.

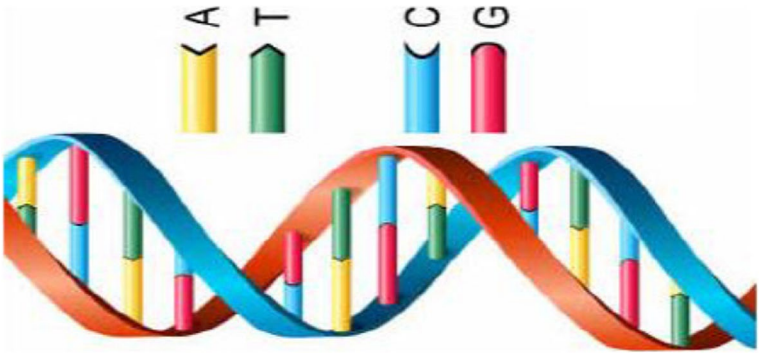

Fig. 3 Simple DNA structure

Table 2 The XOR operation for the sequences of DNA

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

Preliminaries of 2DNA encoding

Knowledge of DNA sequences has become crucial for basic biological research and many practical fields, including diagnostics, forensics, biotechnology, and biological systematic. In a DNA sequence, there are four distinct nucleic acids: T (thymine), A (adenine), G. (guanine), and C (cytosine). Purine adenine (A) and pyrimidine thymine (T), and pyrimidine cytosine (C) always couple with each other according to the rules of base pairing (G). A basic DNA structure is shown in Fig. 3. One can conclude that C and G are also complementary to T and A [20].

Those relations are called Watson–Crick base pairing rules after the two scientists discovered their structural basis. As we all know, 0 and 1 are complementary in the binary system; hence, it may be said that 01 and 10 are complementary, as well as numbers 00 and 11. Table 1 introduces the decoding and coding map rules for the DNA sequence utilized in this study. Table 2 displays the XOR operation for DNA sequences for satisfying Watson–Crick base pairing rules [21].

Method

This work aims to create an image encryption/decryption scheme that can be used to transfer a secure image in an untrusted channel. This scheme is inspired by a combination of some functions from double DNA encoding and chaotic 2D logistic map (2DNALM) algorithms for the first time. This scheme breaks the link between the pixels and mostly concentrates on concepts such as the scrambling algorithm. This scheme was developed to achieve high encryption efficiency, resistance to various assaults with an appropriate execution time, memory savings, and complexity reduction. Figure 4 presents the structure of the proposed scheme.

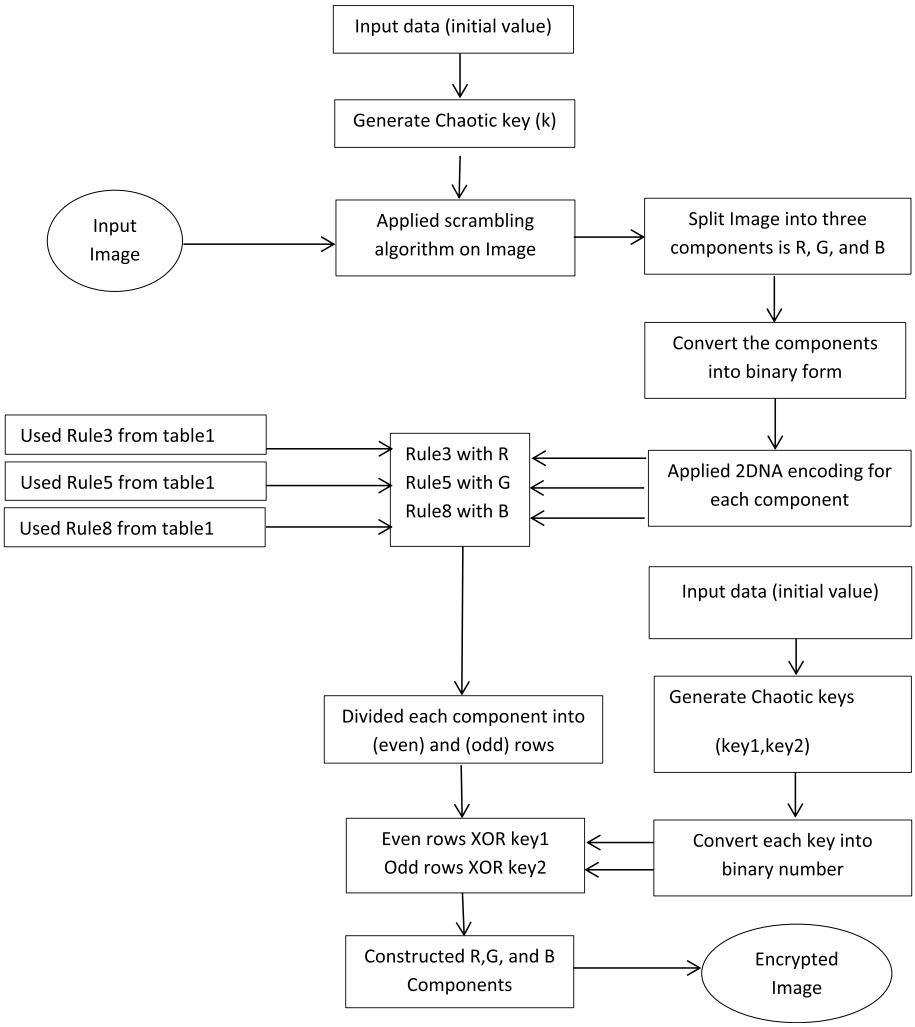

Fig. 4 The general structure of the proposed scheme

To achieve the aim of the proposed methodology used decryption and encryption stages on different images as samples are Lena [22], House [23], Baboon [24], and Peppers [25], as explained in the following paragraphs:

Encryption stage

There are various steps in this stage. The general steps of the encryption are shown in Fig. 5.

Image scrambling operation

Image scrambling operations are carried out to improve the encryption technique's security by breaking the correlation of adjacent pixels. This procedure involves scrambling image I with the dimensions ($M \times N$), where M stands for the image's height and N for its width. The pixel value of any coordinate (i,j) is expressed by A (i,j) where $i = 0,1,2, \ldots$. M-1 and $j = 0,1,2,\ldots N$-1. To create a scrambled image that scrambles the elements of I, as can be seen in algorithm1, the image is moved using a chaotic key

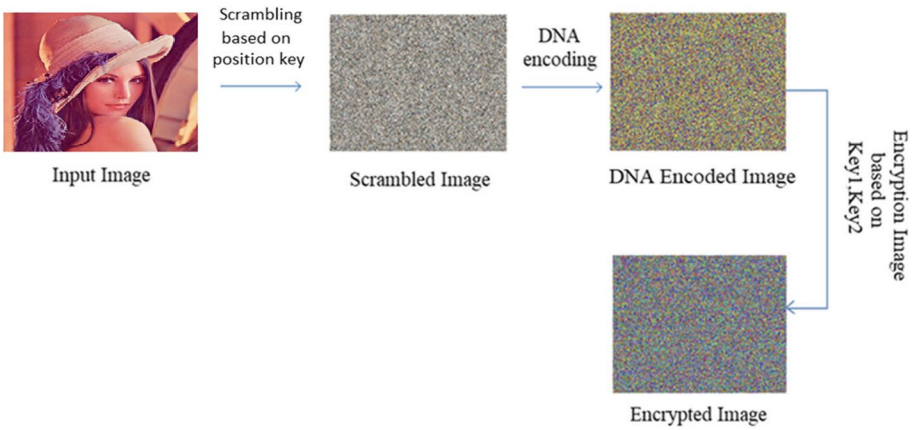

Fig. 5 The general encryption process steps

(k), representing a random matrix. The permutation of the image's pixels is carried out by the scrambling operations utilizing a symmetric key, with the key value as a straight swap. The random matrix elements act as new coordinates of the pixels in the scrambled image I'.

Algorithm 1. The scrambling pixels algorithm.

Input: I (i, j) the original image with dimension (M × N).
Output: I' (i, j) the scrambled image.
Begin: **Step 1:** Generate chaotic sequence K by equation (1) in section 3. The length of the sequence is K0+M×N. **Step 2:** Convert the digital image matrix I with the size of M × N into a one-dimensional sequence P with the length of M ×N. P = (p (1), p (2) . . . p (MN)). **Step 3:** Arrange the chaotic sequences K in ascending order to obtain the index sequences B; at this time, the size of B's new index sequences is 1×MN. **Step 4:** Scramble the array P according to the index sequence B to obtain a new array Q, Q (i)=P (B(i)),i=1,2,3,...,M×N (13) **Step 5:** Convert the one-dimensional array Q into an image matrix I' of size M×N. **End.**

Image double DNA encoding

The 2DNA coding was applied to the permutation result from the preceding step. An RGB scrambling image is disintegrated into three components R, G, and B. Then, each component is converted separately to binary numbers, with every two bits converted to one of DNA symbols A, C, G, and T based on Rule 1 in Table 1 to produce three encoding components Rc, Gc, and Bc. Next, each component is encoded for the second time based on different rules in Table 1. The Rc component is encoding based on Rule 3, The Gc component is encoding based on Rule 5, and the Bc component is encoding based on Rule 8 to produce three encoding components: Rcc, Gcc, and Bcc, that combined into one image that represents the encoding image as shown in the algorithm 2.

Algorithm 2. The double DNA encoding algorithm.

Input: I' (i,j) the scrambled image with dimension (M × N).
Output: I'' (i,j) the encoded image.
Begin: **Step 1:** Loading scrambled image in I'. **Step 2:** Divide I' into three components, R, G, and B. Find an 8-bit binary representation of each R, G and B, and store the result in Rb, Gb, and Bb. **Step 3:** Converted every two bit of each Rb, Gb, and Bb into one of DNA symbols A, C, G, and T according Rule 1 , Rule 5, and Rule 8, respectively from Table 1, and store DNA symbols in Rc, Gc, and Bc. **Step 4:** Repeat the step3, and store the result in Rcc, Gcc, and Bcc. // Double DNA **Step 5:** Find a DNA sequence Rcc, Gcc, and Bcc in 8-bit binary representation, and store binary expression in Rbb, Gbb, and Bbb. **Step 6:** Constructed Rbb, Gbb, and Bbb components into encoding image and stored the result in I''. **End.**

Image encryption process

The proposed method uses Eq. 1 to build two chaotic sequences regarding real numbers, which are then transformed into two vectors as keys (key1, key 2), depending on the chaotic 2D logistic map produced by entering parameters and initial conditions. Each vector has a size equal to the (h*w) original image dimensions. The encryption operation is displayed in algorithm 3. At this stage, the image encoded with key1 is put into an even array after the DNA-XOR operation in Table 2 has been done to the pixels of even rows. The pixels regarding the image's odd rows encoded using key2 are saved in an odd array. The encrypted image is created by combining the two 2D arrays created after the encoded arrays from the two XOR operations.

Algorithm 3. The image encryption algorithm.

Input: I'' (i, j) the encoded image with dimension (M × N).
Output: I''' (i, j) the encryption image.
Begin: **Step 1:** Generate two chaotic sequence keys, K1, and K2, by equation (1) in section 3. The length of each sequence key is K0+M×N. **Step 2:** Loading encoded image in I''. **Step 3:** Divide I'' into groups A and B, A for even rows position pixels, B for odd rows position pixels. **Step 4:** Split pixels of A into three components, Reven, Geven and Beven, and B into Rodd, Godd and Bodd. **Step5:** Apply XOR operation on Reven, Geven and Beven with K1, and Rodd, Godd and Bodd with K2 by using the following equations: REeven = Reven XOR K1 (2) GEeven = Geven XOR K1 (3) BEeven = Beven XOR K1 (4)

Decryption stage

The decryption process is the inverse operation of the encryption process, as shown in algorithm 4. Figure 6 shows the proposed decryption process.

Algorithm 4. The image decryption algorithm.

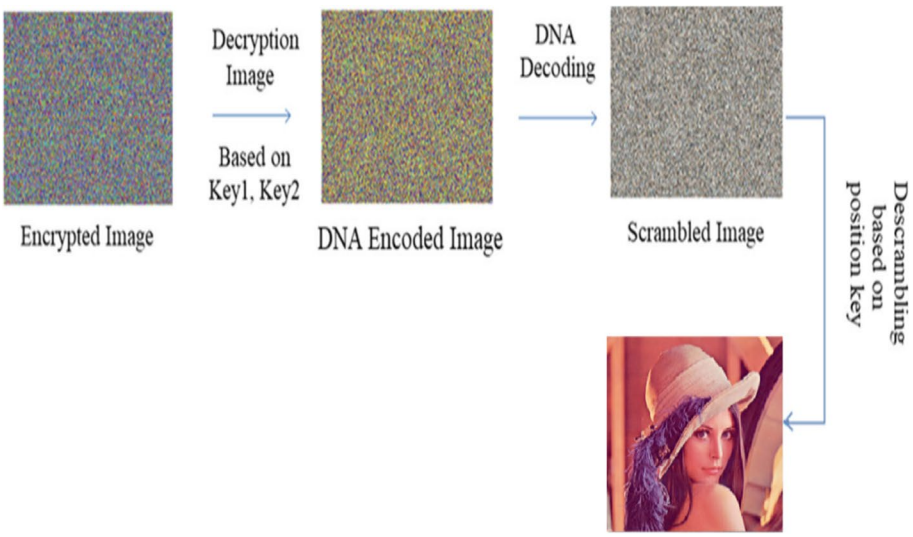

Fig. 6 The general steps of the decryption process

Input: I''' (i, j) the encryption image with dimension (M × N), chaotic keys (K1, K2, K).
Output: I (i, j) decryption image.
Begin: **Step 1:** Loading encryption image in I'''. **Step 2:** Divide I'' into two groups, A and B, A for even rows position pixels, and B for odd rows position pixels. **Step 3:** Split pixels of A into three components, Reven, Geven and Beven, and B into Rodd, Godd and Bodd. **Step4:** Apply XOR operation on Reven, Geven and Beven with K1, and Rodd, Godd and Bodd with K2 by using the following equations: RDeven = Reven XOR K1 (8) GDeven = Geven XOR K1 (9) BDeven = Beven XOR K1 (10)

Experiment

Some experimental setup is presented in this section. The test image is used for the experimental analysis picture of "Lena" (356*242 pixel) to evaluate the suggested image encryption's performance algorithms. The simulation is done by Python 3.10 in a computer of Core i7, 8th Gen, CPU 2.20 GHz and memory 8.00 GB, to implement the entire encryption/decryption process, as shown in Fig. 7.

Figure 8 shows the cipher and original images. The findings demonstrate that all cipher images are completely distorted, demonstrating the effectiveness of the suggested approach for encryption.

Results and discussion

Several tests are applied to the suggested approach to assess the effectiveness of the provided encryption algorithm, key space, entropy, differential attack analysis, histogram analysis, image quality, correlation analysis, and time analysis. For evaluation and testing

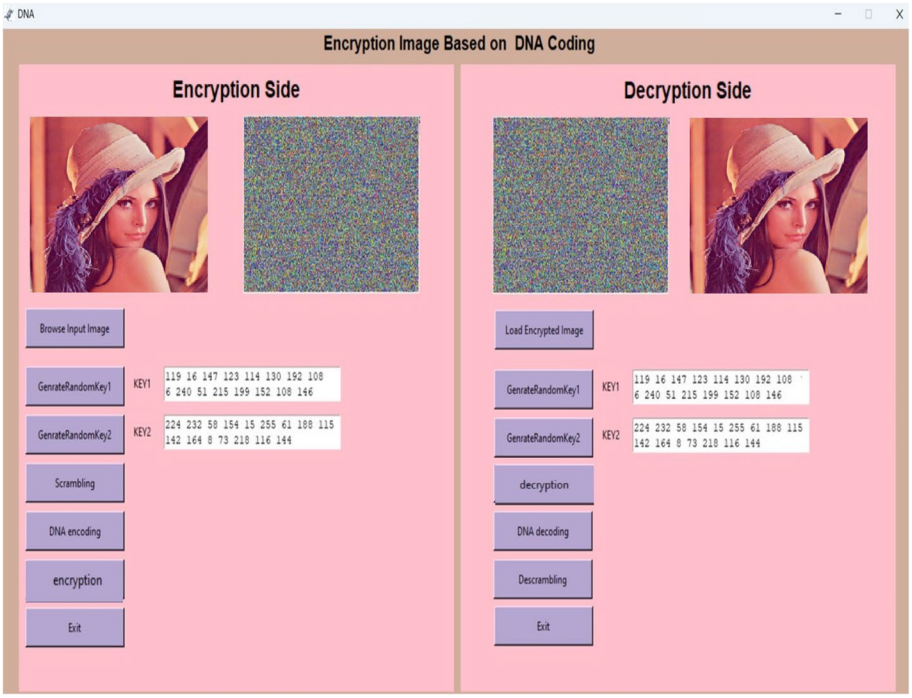

Fig. 7 The final result of the encryption and decryption process

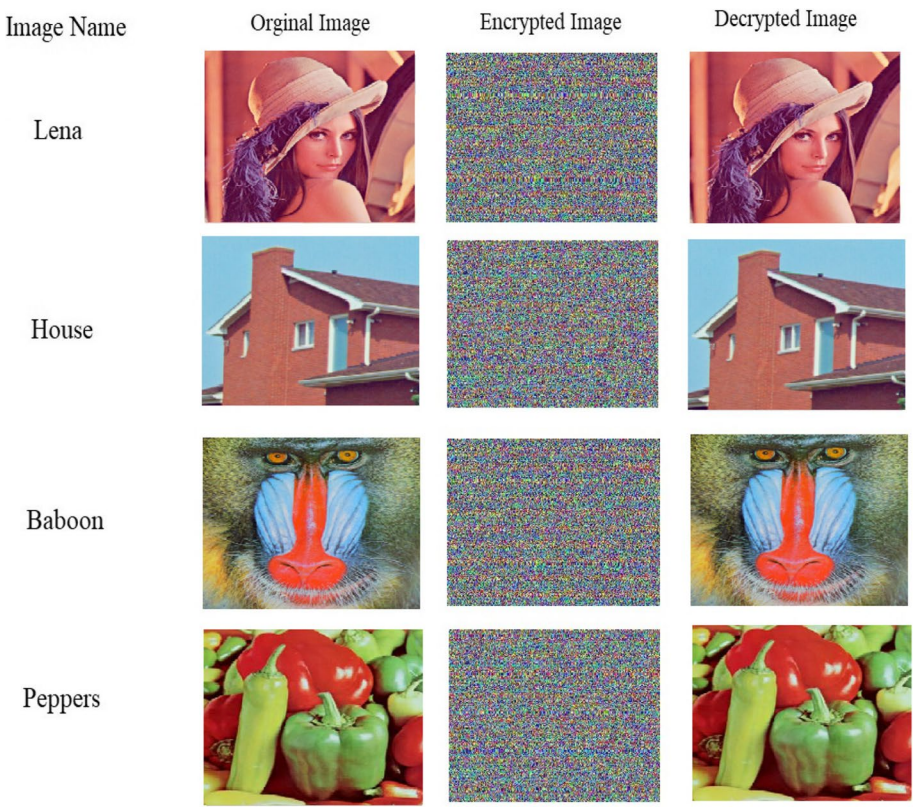

Fig. 8 The original, encrypted, and decrypted images with the proposed method

of results, a set of colored images are utilized. The following the illustration of these tests:

Key space and sensitivity analysis

It is regarded as a crucial metric for assessing encryption systems. It evaluates how sensitive an encryption system is to even the smallest change to the secret key used for decryption and encryption. In the suggested system, the secret key value that was produced by 2D logistic map encryption with the use of parameter $r = 1.19$ and the initial value $(x_0; y_0)$ at (0:8909; 0:3342) that is explained in Eq. 1 was utilized to encrypt (Lena) image, as can be seen in Fig. 9a, b, and decrypted in Fig. 9c. After that change, the parameter was $r = 1.12000001$ and applied for decrypted the image, as shown in Fig. 9d; the image we obtained after decoding by slightly altering the secret key was entirely different from the original image. The suggested approach is, therefore, extremely sensitive to even the slightest modification in the secret key [26].

Entropy

Entropy, a measure of how much information is present in a dataset, shows how gray-scale values are distributed in the image. Entropy is a constant positive value; the more it suggests that a variable carries much information, the more it indicates this. Equation 13 could be used to compute the entropy [27].

$$\mathrm{H(s)} = \sum_{i=0}^{n-1} -\mathrm{P}(s_i)\ \log 2\ P(s_i) \tag{13}$$

$P(\mathrm{s_i})$ stands for probability of (s_i), s_i stands for gray scale, and n represents the total number of the gray scale. The results of the entropy test for encryption images and

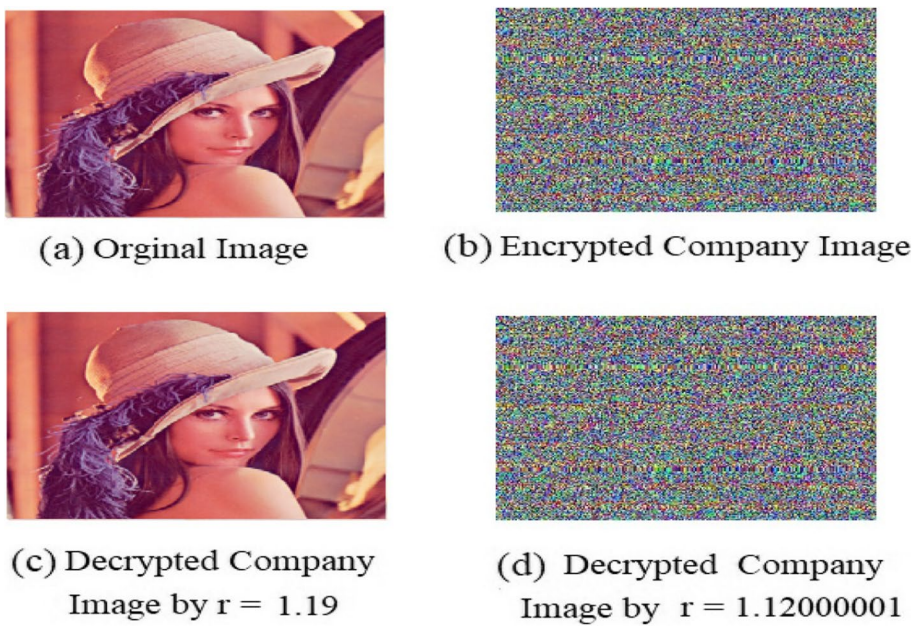

Fig. 9 The sensitivity of the encryption process to the secret keys

Table 3 Entropy values of the proposed method compared with the literature

Image	Proposed	[14]	[29]	[13]	[24]
Lena	7.9898	7.9856	8.6237	7.9998	7.9980
House	7.9950	7.9577	8.9130	N/A	N/A
Baboon	7.9975	N/A	N/A	7.9965	7.9982
Peppers	7.9893	7.9951	8.1112	N/A	7.9977

Table 4 UCAI values compared with the literature

Image name	Proposed	[32]	[33]	[22]	[30]
Lena	32.8111	N/A	33.502	33.5255	N/A
House	33.9025	N/A	N/A	N/A	N/A
Baboon	33.8000	33.56153	33.392	33.4846	33.5531
Peppers	32.9625	33.45786	N/A	33.5301	33.4862

counterpart algorithms from the literature are displayed in Table 3. The findings show that the encryption image's information entropy is close to 8, indicating that the system can resist attacks [28].

Differential attack analysis

The normalized mean change intensity (UACI) and pixel change rate (NPCR) detect differential attack factors and indicate important image information. NPCR stands for the percentage of pixels in the encrypted image that changes after a pixel's value is arbitrarily changed in the original image. The pixel value change in the encrypted image after the original image's pixel value has been modified at random is represented by UACI. The encryption algorithm could efficiently resist differential attacks when the pixel change regarding the original plain-text image is minor, and the encrypted image varies significantly [18]. The equation is as follows:

$$\mathrm{NPCR} = \sum_{i=0}^{W}\sum_{j=0}^{H} D(i,j) \times 100\% \tag{14}$$

H and W represent the columns and rows for the image, respectively, and D is estimated depending on the following formula:

$$D(i,j) = \begin{Bmatrix} 0 \text{ if } C_1(\mathrm{i},\mathrm{j}) = C_2(\mathrm{i},\mathrm{j}) \\ 1 \text{ if } C_1(\mathrm{i},\mathrm{j}) \neq C_2(\mathrm{i},\mathrm{j}) \end{Bmatrix} \tag{15}$$

$$UCAI = \frac{1}{W \times H} = \left(\sum_{i=0}^{W}\sum_{j=0}^{H} \frac{C_1(i,j) - C_2(i,j)}{2^{L-1}} \right) \times 100\% \tag{16}$$

$C_1(i,j)$ and $C_2(i,j)$ represent pixel values of the cipher images, L represents the number of gray levels, and H and W are the image's column and row, respectively. Table 4 shows the computed UCAI values, and Table 5 shows the computed NPCR values for various input

Table 5 NPCR values compared with the literature

Image name	Proposed	[32]	[33]	[22]	[30]
Lena	99.5519	N/A	99.624	99.6277	N/A
House	99.5450	N/A	N/A	N/A	N/A
Baboon	99.5450	99.62387	99.6174	99.6475	99.6125
Peppers	99.7328	99.62209	N/A	99.6078	99.6218

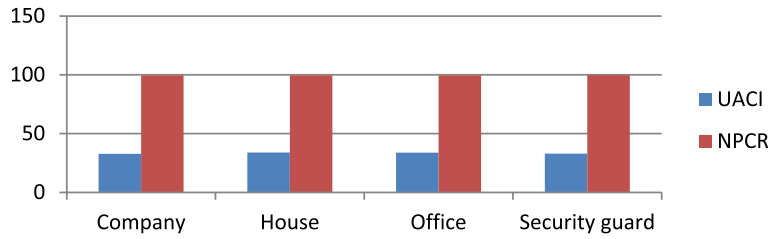

Fig. 10 The NPCR and UCAI test using the suggested system

image examples, showcasing how these values stand compared to other encryption techniques in the literature and demonstrating comparable results. Figure 10 displays each value of UCAI and NPCR after a series of images was tested using the suggested system [30].

Reporting UCAI and NPCR values when analyzing image encryption algorithms is common practice, and this is because the computation of NPCR is based on the value of UCAI. Table 4 displays columns of N/A under the headings of [31], not mentioning the UCAI values.

Histogram analysis

The encrypted image's histogram should be smooth for an encryption algorithm to be effective. Figure 11 displays the color histogram of four images before and after encryption, as implemented by Matlab in 2013. Compared to plaintext images, the encrypted color image histogram's distribution is equally distributed, and the interval's distribution probability is roughly equal. As a result, it is challenging for attackers to predict the original image using statistical analysis. The findings demonstrate that the algorithm could successfully prevent statistical attacks [34].

Image quality

A standard requirement for image encryption methods is that the cipher image deviates greatly from the original image. Two criteria, the MSE and PSNR, could be used to compare the encrypted and original images, and they may be calculated with the use of (17) and (18) [35, 36].

$$\text{PSNR} = 10\ log_{10}(\frac{(255)^2}{MSE})\text{dB} \tag{17}$$

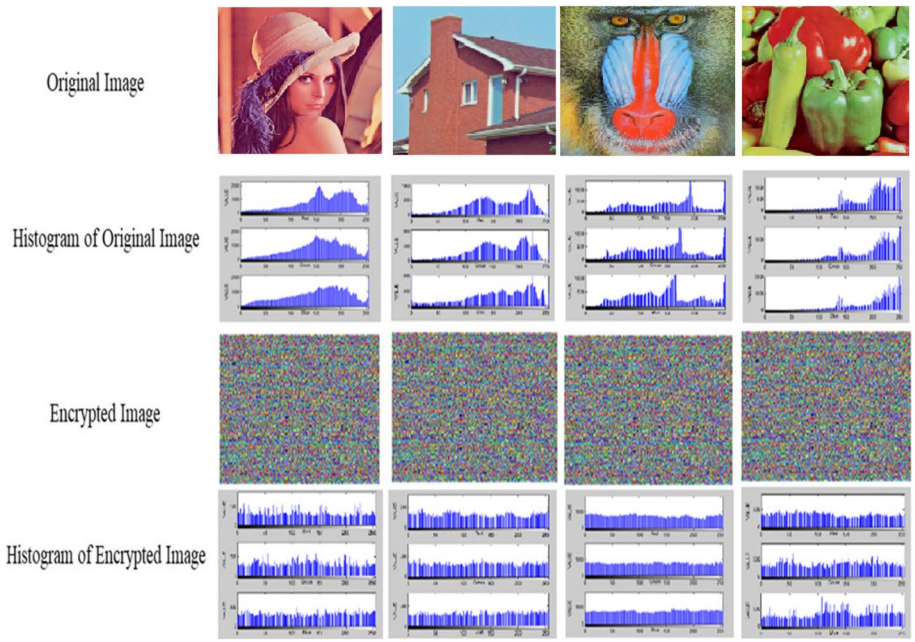

Fig. 11 The histogram analysis of the proposed method

$$\mathrm{MSE} = \frac{1}{W \times H} \sum_{i=0}^{W} \sum_{j=0}^{H} (\mathrm{P(i,j)} - \mathrm{C(i,j)})2 \tag{18}$$

where H and W represent the height and width of the image, respectively, $p(i, j)$ and $C(i, j)$ are the pixel values of the plaintext image and the cipher image at position (i, j), respectively.

As Eq. (17) shows, the PSNR is inversely proportional to MSE. Such mathematical representation steers the preference of the PSNR to be the inverse of the preference of MSE; hence, a minimal value is ideal. Table 6 shows the computed MSE values, and Table 7 shows the computed PSNR values for various input image examples, showcasing how

Table 6 MSE values compared with the literature

Image name	Proposed	[37]	[38]	[39]	[40]
Lena	3238.1500	7802.8866	4859.03	N/A	8925.257
House	3287.6925	8454.3259	N/A	8771.9	N/A
Baboon	3236.6520	N/A	N/A	N/A	8333.303
Peppers	3245.6325	8193.0659	7274.44	N/A	11,168.606

Table 7 PSNR values compared with the literature

Image name	Proposed	[37]	[31]	[30]	[32]
Lena	13.0618	9.2083	8.617	N/A	N/A
House	12.9958	8.8600	8.935	N/A	N/A
Baboon	13.0638	N/A	N/A	8.7880	8.64496
Peppers	11.8378	8.9963	8.1156	8.6210	7.44729

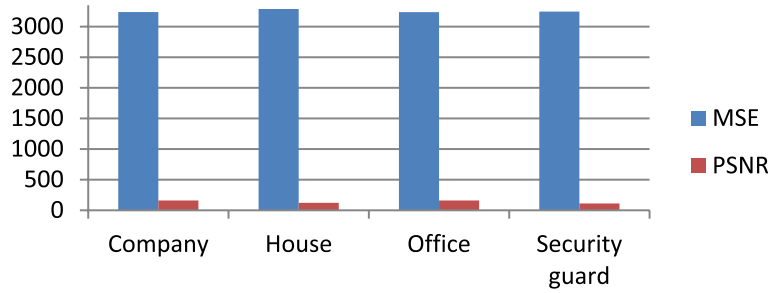

Fig. 12 The MSE and PSNR tests using the suggested system

Table 8 The correlation test of original and encrypted images

Image name	Lena	House	Baboon	Peppers
Original image	0.9550	0.9064	0.9534	0.9203
Encrypted image	− 0.0432	− 0.0324	− 0.0300	− 0.0210

these values stand compared to other encryption techniques in the literature and demonstrating comparable results. Figure 12 displays each value after a series of images was tested using the suggested system.

Correlation coefficient

The correlation coefficient, or c, measures the linear group regarding two random variables' range and trend. The correlation coefficient is near a value of 1 when two variables are closely connected, and the two variables are unrelated if the coefficient is near 0. Equation (19) could be used for calculating the coefficient c [41].

$$c = \frac{\sum_i (x_{i-}x_{m)(y_i-y_m)}}{\sqrt{\sum_i (x_i - x_m)^2}\sqrt{\sum_i (y_i - y_m)^2}} \tag{19}$$

When the correlation coefficient's value is close to 0, the correlation coefficient's value is close to 1. Since it uses a 2D-chaotic method for encrypting the image and 2DNA encoding, this system has a high correlation coefficient. As indicated in Table 8 and Fig. 13, the range of the value correlation coefficient for the four original tests was between 0.9550 and 0.9064, and the range for the encryption image was between − 0.0210 and − 0.0432. The correlation coefficient between the encryption and the original images is different, as shown in Fig. 14. This status showed an extremely robust system [42].

Time analysis

Since our technique is based on the direct manipulation of each pixel's bits, the cryptographic speed's complexity is determined by the pixel count in the image. That makes the proposed technique very efficient concerning the time consumed for encryption and memory allocation. The proposed approach takes 6–8 s on average to encrypt a 256×256 RGB image used to evaluate the running time of the proposed method on a core i7 processor

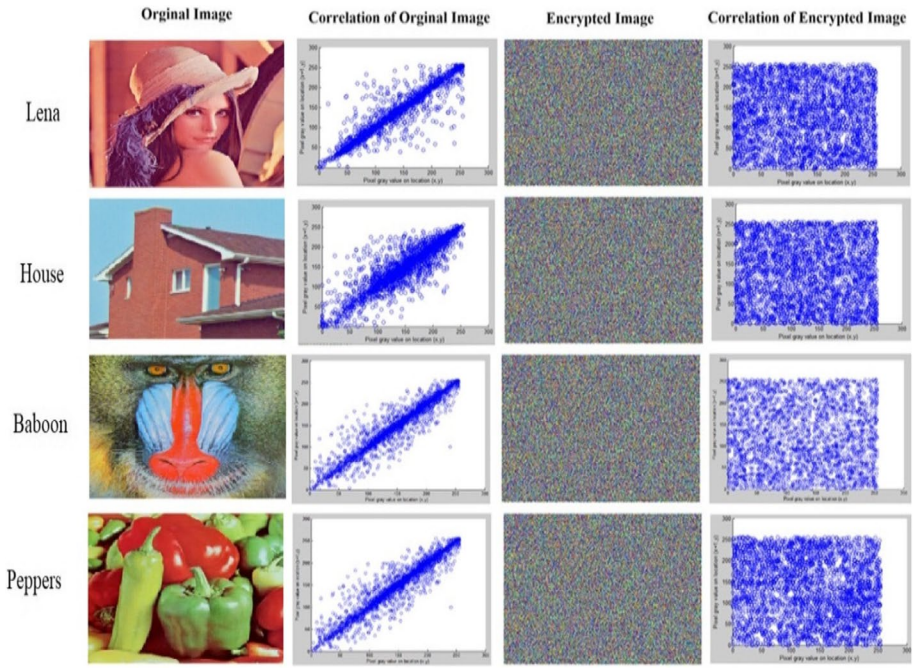

Fig. 13 The correlation test of original and encrypted images of the proposed method

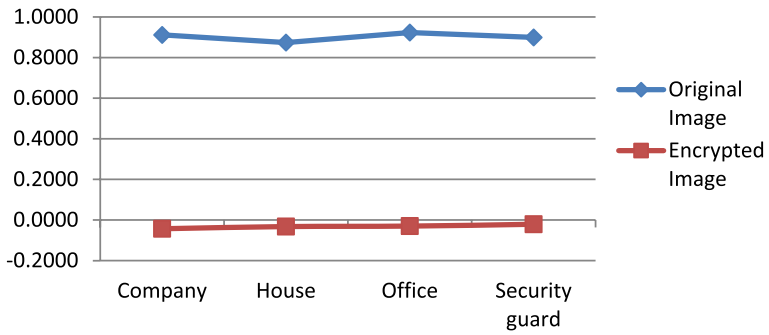

Fig. 14 The correlation test of original and encrypted images

with 8 GB of RAM; the proposed approach takes 6–8 s on average to encrypt a 256×256 RGB image. However, a GPU processor can be used to reduce time constraints and is still robust and secure. In the future, we intend to present a parallel version of the algorithm to make it more efficient. Moreover, a customized parallel version of the algorithm can divide the image into blocks. Encrypting these blocks in parallel as if each block was an independent image can reduce the time greatly.

As presented in Sect. 7, it is obvious that the performance of the combined DNA coding and chaotic coding technique gives good results within a short time and could successfully resist different threats.

Conclusions and future works

A reliable decryption and encryption approach was suggested in this study and used for the first time image encryption algorithm is 2DNALM based on a combination of two dynamic DNA sequence encryption and a chaotic 2D Logistic Map. Before performing 2DNAencoding, the image is scrambled using various methods to increase the security layer. The encryption process is completed later, resulting in an encrypted image. The inverse operation from encryption is used for decryption. An encryption approach was suggested for the simulation experiment—entropy, differential attack analysis, histogram analysis, sensitivity analysis, key space, and image quality. The results of the experiments demonstrate that the algorithm has good safety performance and can successfully resist different threats. According to the findings of the experiments, our proposed solution is competitive with previous chaotic image encryption algorithms and meets the criteria for image security. Future works could (a) attempt used other types of data encryption, like audio and video encryption, and (b) boost security; a higher-order 5D logistic chaotic map can produce chaotic keys instead of a chaotic 2D logistic map.

Abbreviations

DNA	Deoxyribonucleic acid
2DNALM	2 DNA logistic map
RGB	Red, green, and blue
D	Dimension
T	Thymine
G	Guanine
C	Cytosine
A	Adenine

Acknowledgements
Not applicable.

Authors' contributions
Each author has made substantial contributions to the conception and design of the work. AH has analyzed and designed the work and created a new method presented in the work. MAA has performed the data curation formal analysis and interpretation of the data, has utilized the software, and has attained manuscript review and editing. AT has substantively revised it. The authors read and approved the final manuscript.

Funding
The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Availability of data and materials
All data generated or analyzed during this study are included in the article (and in its supplementary materials).

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 1 March 2023 Accepted: 23 May 2023
Published online: 16 June 2023

References

1. Ullah A et al (2022) An efficient lightweight image encryption scheme using multichaos. Secur Commun Networks 2022:1–16
2. Pronika S, Tyagi S (2021) Performance analysis of encryption and decryption algorithm. Indones J Electr Eng Comput Sci 23(2):1030–1038

3. Kamal B, Al-Saidi N (2021) Extended chaotic nonlinear programming technique constructing with genetic algorithms J. Appl Sci Nanotechnol 1(1):15–22
4. Sheng Y, Li J, Di X, Li X, Xu R (2022) An image encryption algorithm based on complex network scrambling and multi-directional diffusion. Entropy 24(9):1247
5. Kodher M, Saud JH, Hassan HS (2021) Wheelchair movement based on convolution neural network. Eng Technol J 39(6):1019–1030
6. Wu Y, Yang G, Jin H, Noonan JP (2012) Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 21(1):13014
7. Nandy N, Banerjee D, Pradhan C (2021) Color image encryption using DNA based cryptography. Int J Inf Technol 13(2):533–540
8. Zhou S, Wei Y, Zhang Y, Teng L (2022) Novel chaotic image cryptosystem using dynamic DNA coding
9. Patidar V, Kaur G (2022) A novel conservative chaos driven dynamic DNA coding for image encryption, arXiv Prepr. arXiv2207.05475
10. Alabaichi A, Altameemi AA (2022) Steganography encryption secret message in video raster using DNA and chaotic map. Iraqi J Sci 63:5534–5548
11. Ibrahim D, Ahmed K, Abdallah M, Ali AA (2022) A new chaotic-based RGB image encryption technique using a nonlinear rotational 16× 16 DNA playfair matrix. Cryptography 6(2):28
12. Babu M, Devi GS, Iswarya N, Prasanna MV, Krishna MY (2020) Image encryption using chaotic maps and DNA encoding. J. Xidian Univ 14(4):2020
13. Shakir HR, Mehdi SAA, Hattab AA (2022) Chaotic-DNA system for efficient image encryption. Bull Electr Eng Informatics 11(5):2645–2656
14. Gabr M et al (2022) Application of DNA coding, the Lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem. Symmetry (Basel) 14(12):2559
15. Wang S, Peng Q, Du B (2022) Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Opt Laser Technol 148:107753
16. Yildirim M (2022) Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. Chaos, Solitons Fractals 155:111631
17. Mohammed RA, Khodher MAA, Alabaichi A (2023) A novel lightweight image encryption scheme. C Mater Contin 75(1):2137–2153
18. Laiphrakpam DS, Thingbaijam R, Singh KM, Al Awida M (2022) Encrypting multiple images with an enhanced chaotic map. IEEE Access 10:87844–87859
19. Hadi SA, Ali SA, Jawad MJ (2021) Binary image encryption based on chaotic and DNA encoding. Next Generation of Internet of Things: Proceedings of ICNGIoT 2021. pp 295–312
20. Manihira NR, Dauda AK (2022) Image encryption using chaotic maps and DNA encoding. International Journal of Engineering Research & Technology 10(11):1-5
21. Wen H et al (2022) Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. Mathematics 10(17):3180
22. Liu Q, Liu L (2020) Color image encryption algorithm based on DNA coding and double chaos system. IEEE Access 8:83596–83610
23. Lin R, Li S (2021) An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm. Secur Commun Networks 2021:1–18
24. Abdallah AA, Farhan AK (2022) A new image encryption algorithm based on multi chaotic system. Iraqi J Sci 63:324–337
25. Malik MGA, Bashir Z, Iqbal N, Imtiaz MA (2020) Color image encryption algorithm based on hyper-chaos and DNA computing. IEEE Access 8:88093–88107
26. Xu D, Li G, Xu W, Wei C (2023) Design of artificial intelligence image encryption algorithm based on hyperchaos. Ain Shams Eng J 14(3):101891
27. Du S, Ye G (2023) IWT and RSA based asymmetric image encryption algorithm. Alexandria Eng J 66:979–991
28. H. G. A. U. L. Sahib, Comparison of three proposal methods in steganography encryption secret message using PVD and MapReduce, IRAQI J. Comput. Commun. Control Syst. Eng. 2021;21(2):2021.
29. Alexan W, ElBeltagy M, Aboshousha A (2021) Image encryption through lucas sequence, s-box and chaos theory, in 2021 8th NAFOSTED Conference on Information and Computer Science (NICS). pp 77–83
30. Alghamdi Y, Munir A, Ahmad J (2022) A lightweight image encryption algorithm based on chaotic map and random substitution. Entropy 24(10):1344
31. Paul LS, 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 81(26):37873–37894
32. Alanezi A et al (2021) Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment. Secur Commun Networks 2021:1–17
33. Jirjees SW, Alkalid FF, Shareef WF (2023) Image encryption using dynamic image as a key based on multilayers of chaotic permutation. Symmetry (Basel) 15(2):409
34. Al Maisa'a Abid Ali K, Alabaichi A, Abbas AS (2020) Dual method cryptography image by two force secure and steganography secret message in IoT. TELKOMNIKA (Telecommunication Comput. Electron. Control 18(6):2928–2938
35 Mahdi SA, Maisa'a AK (2021) An improved method for combine (LSB and MSB) based on color image RGB. Eng. Technol. J 39(1B):231–242
36. Hassan HH, Khodher MAA (2021) Data hiding by unsupervised machine learning using clustering K-mean technique, *IRAQI*. J Comput Commun Control Syst Eng 21(4):37–49
37. Tian P, Su R (2022) A novel virtual optical image encryption scheme created by combining chaotic S-box with double random phase encoding. Sensors 22(14):5325
38. Younas I, Khan M (2018) A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. Entropy 20(12):913

39. Abu-Faraj M et al (2023) Protecting digital images using keys enhanced by 2D chaotic logistic maps. Cryptography 7(2):20
40. Al-Tuwaijari JM (2018) Image encryption based on fractal geometry and chaotic map. Diyala J Pure Sci 14(1):166–182
41. Alabaichi A (2021) Concealing a secret message in a colour image using an electronic workbench. Iraqi J Sci 62:4964–4977
42. Gao S et al (2023) A 3D model encryption scheme based on a cascaded chaotic system. Signal Process 202:108745

Publisher's Note