Scientia Iranica (2024) 31(21), 2041–2055

Sharif University of Technology
Scientia Iranica
Transactions D: Computer Science & Engineering and Electrical Engineering
https://scientiairanica.sharif.edu

Research Note

A novel image encryption using improved chaotic maps and multiple encryption tables

Muhammed Milani*

Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Bandırma Onyedi Eylül University, Balikesir, Turkey.

Received 15 October 2021; received in revised form 9 October 2022; accepted 19 December 2022

KEYWORDS
Image encryption;
Chaotic map;
DNA strand;
Multiple tables;
Symmetric cryptography.

Abstract. This paper proposes a new symmetric cryptographic system using chaotic systems. The basic idea is that a random strand is generated from chaotic functions. The developed random strand is merged with the strand obtained from the original image. The researcher used tables called multiple encryption tables in the composition of these strands. These tables are produced according to a specific pattern. The strand combination algorithm randomly selects a table from a set of tables and performs the combination operation. This table will be replaced with another table under certain conditions. The diversity of tables and their dynamic selection in the integration operation will increase the resistance to attacks and threats and increase the proposed encryption system's efficiency. To prove the proposed system's efficiency, the obtained results have been evaluated by various tests such as entropy, correlation coefficient, and pixel change rate. Our results show that the proposed cryptographic system is cost-efficient, practical, and resistant, yet further research is required to make a final statement about its competence.

1. Introduction

There are many incentives to share data in the various communication channels regarding internet development and the emergence of fast data transfer methods through various communication channels. However, data dissemination in such environments, often publicly accessible, carries a high-security risk [1,2]. Encryption plays an important role in the highly secure transmission of data over insecure channels. Cryptography can be considered part of a more general concept called cryptology.

Encryption of data is carried out through encryption algorithms and techniques such as traditional or modern cryptography, DNA-based and chaos-based techniques, etcetera. Some techniques, such as quantum Fourier transforms and elliptic curves, are based on mathematical concepts [3].

Encryption algorithms can be classified into stream and block cipher algorithms. The data is considered a stream of data in the stream cipher method, and

*. *Corresponding author.*
E-mail address: mmilani@bandirma.edu.tr (M. Milani)

To cite this article:
M. Milani "A novel image encryption using improved chaotic maps and multiple encryption tables", *Scientia Iranica* (2024), **31**(21), pp. 2041-2055
https://doi.org/10.24200/sci.2022.59249.6138

a secret key generator is used for its encryption. These encryptions include cryptographies obtained using the Linear Feedback Shift Registers method [4]. These types of systems are often based on RC4. Unlike stream methods, Block Cipher methods encrypt a block of data. This encryption method has commonly been used in traditional cryptographic systems such as AES, DES, and TDES [5].

Image cryptography, one of the traditional cryptographic systems, is a popular research area for many researchers. Image encryption is important in multimedia applications for digital security and identification [6]. Moreover, secure storage and digital transmission are the main concerns in multimedia communication [7]. On the one hand, images inherently have strong correlation features, high compatibility, and high data redundancy compared to other data types. On the other hand, this data type has a higher volume than other data types [8].

Additionally, traditional encryption methods such as AES, DES, or 3DES have a small key space and low speed, making them unfeasible for image encryption [9,10]. Different methods have been proposed for image encryption, and many studies have demonstrated and presented effective designs. These include optical image encryption methods [11], fast methods based on parallel computing systems [12], or using image encryption for authentication [13]. Furthermore, image encryption methods in embedded systems have also been proposed [14].

Chaos systems have a set of features that are appropriate for image encryption. These characteristics have high sensitivity to initial conditions, ergodicity, reproduction ability, and non-periodicity in producing pseudo-random numbers. Also, these properties have made several pseudo-random generator methods with high speed and accuracy feasible [15]. Chaotic maps can be divided into two classes which are called one-dimensional and high-dimensional chaotic functions. Functions, known as one-dimensional chaotic functions, have a simple structure and can easily be implemented [16]. However, these functions have problems that have recently led to less interest in their application in cryptographic methods. Among those are the limited chaotic range [17] and vulnerability [18]. Different methods can be developed using High Dimensional chaotic functions considering the abovementioned problems [19,20]. These functions are more complex and have more chaotic behaviors. Therefore, their pseudo-random sequences are not easily predictable [21]. However, cryptographic methods are developed using One-Dimensional chaotic functions [22,23] due to limitations of high-dimensional functions (e.g., high computational cost and the complexity of implementation) [24,25].

Image encryption systems are studied in two main sections: Key generation and image deformation. In the key generation, random sequences are generated by the secret key depending on the cryptographic algorithm type [26]. Correspondingly, chaotic functions can play a major role in developing these random sequences. The high sensitivity of these functions to the initial value can be considered a good starting point. Secret keys with a simple algorithm can generate the initial values required for chaotic functions [27]. Image information is also achieved by changing the pixel values, their position, and/or both through the concepts of Confusion and Diffusion [28]. Considering the issues reviewed in the preceding paragraphs, developing new chaotic systems with a simple and unpredictable structure has become a priority in recent years. We aimed to create a unique design with a high level of security and fast speed in this context.

This paper's proposed system creates a sequence of random numbers using a two-dimensional chaotic function. The initial values for the desired chaotic function are obtained from the value of the secret key. Random numbers generated by a conversion function are converted to a DNA strand. The length of the created strand is equal to the size of the strand obtained from the original image. After combining two DNA strands, a new strand of the same length is created, considered a cipher strand. The encrypted strand can be used as an encrypted image by converting it to an embodiment. In combining strands and creating encrypted strands, instead of using one operator, which is often the XOR operator, this study uses 24 operators, considered tables. At the beginning of the conversion operation, an operator is randomly selected, and the combination operation is performed accordingly. Subsequently, the operator is replaced with others depending on the specific conditions. Using multiple operators and replacing operators based on the original image data increases the system's complexity, making it more resistant to attacks.

The following section of the article and the second part will discuss some issues related to chaos systems and functions. Information about DNA patterns and operator tables is another topic we will address in Section 2. The Section 3 will describe the proposed cryptographic system. The results and analysis of the proposed system will be discussed in Section 4. In this section, various tests will be performed to analyze the capabilities of our proposed system. In Section 5, the conclusion will be presented.

2. Materials and methods

2.1. Chaos-based image encryption and 2D logistic map

Chaos systems are nonlinear systems with high sensitivity to the initial conditions and pseudo-random

behavior. Chaotic signals have a noise-like appearance, and despite their random behavior, being definitive, having initial values and mapping functions, the same previously produced values can be obtained. These systems will be in a chaotic state if they satisfy the Lyapunov exponential equation conditions. The pseudo-random feature in these systems has made them an outstanding alternative for encryption.

Chaotic systems were first used by Matthews [29]. Many algorithms and encryption methods based on chaotic theory were later developed [30,31]. A key point in chaos-based encryption systems is determining a mapping function, which examines initial conditions and areas where it exhibits chaotic features. The correct and appropriate choice for the mapping function would lead to increased encryption system efficiency and more stability of encrypted data against hackers.

Various functions have chaotic properties, which we can mention in the logistic map. These functions are presented in different types, and we will consider the one-dimensional logistic map in this article. The one-dimensional logistics function discussed in Eq. (1) is defined:

$$x_i = FL(\alpha x_{i-1}(1 - x_{i-1})), \tag{1}$$

where FL is the precision function, and α is the control parameters. This function has chaotic behavior when the value of α is in the range (3.5699,4] and leads to the production of a chaotic sequence in the range (0,1].

Although the use of chaotic systems has attracted much attention from cryptographic researchers, there is a risk in estimating these systems. This risk is due to the progress made in chaos theory. Recently, we have seen evidence of attacks on some cryptographic algorithms based on chaotic systems [32]. Therefore, we can claim that classical chaotic systems are insecure.

Various methods have been proposed to reduce the dynamic destruction of chaotic maps to solve the uncertainty of chaos functions [33]. One of these is the increase in the dynamic degradation of chaotic maps. In this article, to increase the efficiency of our proposed system, we used the delayed Logistic map in [34] to generate our random sequence. In this way, we used the improved logistic function in Eq. (2):

$$x_{i+1} = FL(x_i(1 - x_i)(4 - b + bx_{i-1})), \tag{2}$$

where $h(x_{(i-1)} = (4 - b + bx_{i-1})$ is a linear function of delay state x_{i-1}. For the function introduced in Eq. (2) to have a chaotic property, the parameter b should be in the range (0,0.4).

Research has shown [35] that the distribution of the chaotic sequence obtained by the chaos functions is not very average, and the chaotic mapping loses its characteristics in the domains of integers. To overcome this problem, it can multiply the random numbers generated in decimal form by a large fixed value. Eq. (3) shows this issue:

$$x'_i = (x_i * C) \ mod \ 256, \tag{3}$$

where x_i is the original generated random numbers, x'_i is the improved random numbers, and C is a conversion factor and the value obtained in the relationship of 3 random numbers is an integer number between 0 and 256. Wang et al. [35] suggest the use of a conversion factor to convert random numbers to a number in a specific interval, namely (0, 255), which, in this case, is set to a $C = 1000000$ in Eq. (3). So, the produced random numbers will have a more uniform distribution.

2.2. DNA patterns and representation by quaternary alphabetic system

DNA series have four types of nucleic acid bases which are known as Adenine (A), Thymine (T), Cytosine (C), and Guanine (G). The main feature of these strings is a complementarity of A with T and C with G. Due to the complementary properties of 0 and 1 in binary numbers, this feature can be easily implemented in the binary number system. The alphabet in the DNA series is 4, which requires 2 bits to encode in the binary system. By choosing one of the four possible states for a letter, only one state can be imagined for the complimentary letter and two possible conditions for the other two letters. Given that there are four modes, the number of possible modes for coding is 8.

Recently, the use of new methods for image encryption has drawn researchers' attention, including the use of DNA calculations in encryption [36]. In 1994, based on performing experiments on DNA calculations, Adelman opened the gate to a new chapter of the information age. Following Adelman's claim on using DNA in calculations, different studies with enormous storage sources and low energy consumption have been conducted for DNA calculations. Also, DNA calculations in encryption have attracted investigators' attention and have been used as information transport and implementation tools.

Gehani et al. [37] suggested an OTP-based method for image encryption using DNA, which was restricted to traditional electronic media; however, it was considered a key in OTP to transport enormous amounts of information using DNA and biological capabilities of suitable media. Recently, other methods have been suggested based on DNA calculations [16,38,39], some of which have been used in massive data transfer.

Image encryption using the DNA method can transfer information about the image from a decimal system to a quaternary alphabetic system. To do so, first, the numerical values of each pixel are converted into binary with eight digits, and then every two digits are converted to a letter. This conversion procedure can be carried out using a transfer function given in Eq. (4):

$$f : A \rightarrow B; \quad A \in \{0, 1..255\}$$

and

$$B \in \{\text{“}A\text{”} = \text{“}00\text{”},\ \text{“}T\text{”} = \text{“}11\text{”},\ \text{“}C\text{”} = \text{“}01\text{”},\ \text{“}G\text{”} = \text{“}10\text{”}\}. \tag{4}$$

Eq. (4) denotes a sample transfer according to first rule of Watson-Cricks. Using Eq. (4) and assuming that the image's dimensions are equal to N and M, a sequence is produced from the DNA alphabet by the size of $4 * N * M$.

Many biological and algebraic operators are disengaged in DNA computing [40]. These operations can be performed on the generated DNA sequence. The three basic operations ($\otimes$, $+$, $-$) for DNA strands are drawn in Table 1.

Table 1 introduces the DNA arrangement in the proper way of XOR operand and according to Equation's function (4). Eq. (4), the transfer function has been created based on the Watson-Crick base-pairing rules [41].

Table 2 depicts eight possible forms of transfer functions according to Watson-Cricks rules.

These rules can be resulted in 8 different tables using the XOR operator. Using other forms not based on Watson-Crick rules is also possible to have these kinds of tables. Therefore, to transfer the 2-bit pairs into the DNA alphabet, 24 different functions should be considered. The obtained tables have these same qualities:

- The last rows and columns (equivalent to the corresponding 00) are neutral members of the tables;
- The diameter of the tables is equal to the neutral member (corresponding letter to 00);
- These traits have been used in this paper.

Also, other operators with similar characteristics can be used to increase the number of tables. Xingyuan Wang and Liu [41] incorporated two operators (i.e., $+$ and $-$), summarized in Table 1. The same functions in Eq. (4) have been used in the design of Table 1. Having 24 cases for each operator means that 48 different operator tables could be designed for the system. These tables were numbered and stored in a database called the operator's database used in the proposed system.

3. Proposed method

This method has four distinct phases, the first of these phases is related to the operators' database, explained in the previous section. Then, as the second phase, the numerical values of pixels are converted into a series of DNA strands. Each pixel is converted to an 8-bit binary format. According to Equation, each bit plane is extracted and converted into the DNA sequence by applying the DNA encoding rule. For instance, if the pixel value is 164, the binary format number is 10100100 in order using Eq. (4), resulting in a DNA sequence of “GGCA”.

One of the images' main characteristics is their high correlation factor of the closest or neighbor picture element. The pixel position can be affected by reducing the most relative picture element's interaction factor. And so, Eq. (5) shows this effect:

$$(p_i + i)\ mod\ 256 \rightarrow P'_i \rightarrow P_{DNA}, \tag{5}$$

where P is the numerical value of the picture element, and i is the index of each pixel. Therefore, a strand of DNA sequence by the size of $4 * n * m$ from the basic image is obtained, shown as *Plainstr*. In phase 3, a random DNA strand by the size of $4 * n * m$ is produced. The paper uses an improved logistic map to create the random sequence.

Table 1. The three basic operations for DNA strands.

	A			**T**			**G**			**C**		
	$\otimes$	$+$	$-$	$\otimes$	$+$	$-$	$\otimes$	$+$	$-$	$\otimes$	$+$	$-$
A	A	A	A	T	T	C	G	G	G	C	C	T
T	T	T	T	A	G	A	C	C	C	G	A	G
G	G	G	G	C	C	T	A	A	A	T	T	C
C	C	C	C	G	A	G	T	T	T	A	G	A

Table 2. Possible forms of transfer functions according to Watson- Cricks.

Rule	**I**		**II**		**III**		**IV**		**V**		**VI**		**VII**		**VIII**	
	0	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**
0	A	C	A	G	T	C	T	G	G	T	G	A	C	T	C	A
1	G	T	C	T	G	A	C	A	A	C	T	C	A	G	T	G

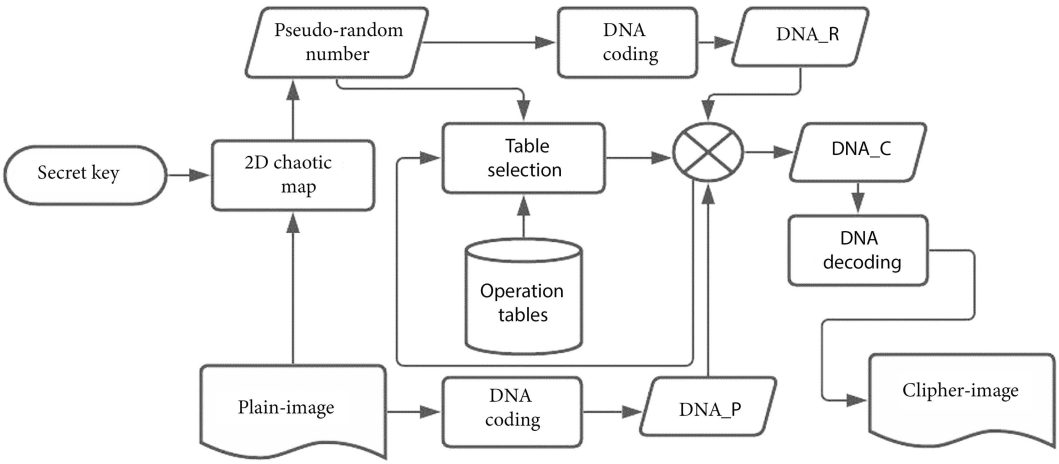

Figure 1. General procedure of the proposed algorithm.

It can be seen that the initial values of x_0 and x_1 are a number between 0 and 1 if the improved logistic map function features are considered. The rest of the function numbers are highly sensitive to the initial values and other parameters. The initial values x_0 and x_1 are calculated as:

$$\begin{cases} x_0 = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{7} k_{i,j} * 2^{i*8+j}}{2^{n+8}} \\ x_1 = \frac{\sum_{i=n-1}^{0} \sum_{j=0}^{7} k_{i,j} * 2^{i*8+j}}{2^{n+8}} \end{cases} \quad (6)$$

where n is the number of characters and $k_{i,0}$, $k_{i,1}$, $\cdots$, $k_{i,7}$ are the bits of ith character.

The proposed method requires a random sequence by the size of the produced sequence. Therefore, using logistic mapping, $4 * n * m$ pseudo-random numbers between 0 and 3 with the initial values of x_0 and x_1 are made. These numbers are converted into DNA sequences using the same procedure as phase 2. In the paper, to produce random numbers through an improved logistic map, b parameter in Eq. (2) is set to 0.1. The logistic function aims to generate one string of numbers between 0 and 1, converted to a series of binary numbers. By combining the bits of these two series, a random strand can be created. The random strand made in this phase plays an important role in encryption and decryption operations and is named *RndStr*.

In the final phase, an encrypted sequence of *CipherStr* is produced using *RndStr*, *PlainStr*, and the operators' database. The key point in encryption and decryption is how to follow the tables of operators. Algorithm 1 and Algorithm 2 summarize encryption and decryption algorithms.

An image can be encrypted in DNA sequences by going through the proposed phases. These sequences can be biologically transferred or converted to decimal equivalents and used as an encrypted image. Figure 1 shows the general procedure of the proposed method.

ALGORITHM Encryption (PlainStr, RndStr, OTable, StartTable)

```
Ind ←StartTable
Op ← OTable_ind
for each PlainStr_i in PlainStr
    CopherStr_i ← Op [PlainStr_i, RndStr_i]
    if CipherStr_i is a neutral member in Op
        ind ← (ind++) mod TableNumber
        Op ← OTable_ind
return CipherStr
```

Algorithm 1. Encryption phases algorithm.

ALGORITHM Decryption (CipherStr, RndStr, OTable, StartTable)

```
Ind ←StartTable
Op ← OTable_ind
for each CipherStr_i in CipherStr
    PlainStr_i ← Op [CipherStr_i, RndStr_i]
    if PlainStr_i == RndStr_i
        ind ← (ind++) mod TableNumber
        Op ← OTable_ind
return PlainStr
```

Algorithm 2. Dencryption phases algorithm.

4. Result and analysis of proposed method

We can build a system in the *Matlab* environment to display the efficiency of the suggested method. The user selects an image and defines a security key. According to the proposed algorithm, color images are converted to three colors and then individually encrypted and decrypted. Figure 2 shows the result of the encryption phases of the algorithm for an image and its three colors separately.

Clearly, the decrypted and original images must be the same. If the security key for decryption differs from the security key for encryption, the decrypted image will differ from the original image. This is demonstrated in Figure 3. To demonstrate the effectiveness of the suggested system, the system is tested with several simple images. The image chosen

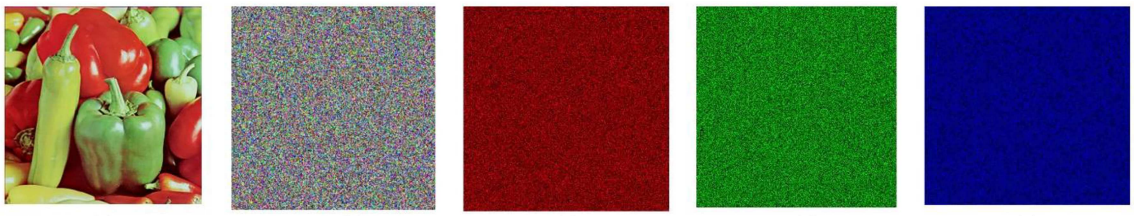

Figure 2. (a) Plain image; (b) Cipher image; (c) Red component of Cipher image; (d) Green component of Cipher image; and (e) Blue component of Cipher image.

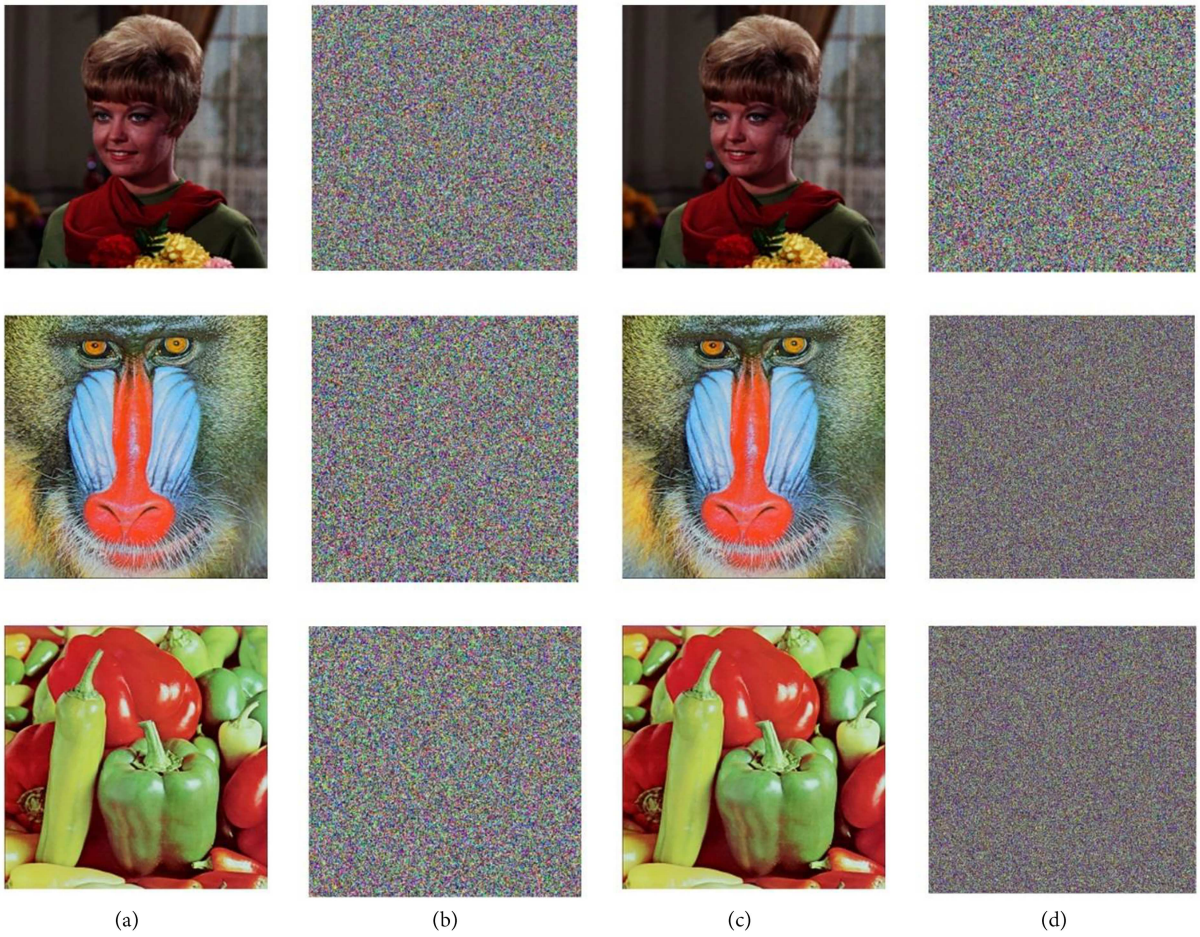

Figure 3. (a) Plain images; (b) Cipher images with key = A; (c) Decrypted images with key = A; and (d) Decrypted images with key ≠ A.

regarding the USC-SIPI. The results show the high performance of the system.

4.1. Differential attack analysis

An appropriate encryption method must be consistent against all kinds of cryptanalysis. One of the types of attacks that can occur for encrypted images is the differential attack. The discovery of differential inversion is usually related to Biham and Shamir [42,43].

For the first time, these tests were applied in 2004 [44], and today they are widely used in security analysis for image encryption [45]. *NPCR* is defined as Eq. (7):

$$NPCR = \frac{\sum_{i=1}^{L}\sum_{j=1}^{C} D(i,j)}{L \times C} \times 100\%, \tag{7}$$

where L and C are the width and length of the image [46], and $D(i,j)$ is obtained by Eq. (8):

$$D(i,j) = \begin{cases} 0 & \text{if } img_1(i,j) = img_2(i,j) \\ 0 & \text{if } img_1(i,j) \neq img_2(i,j) \end{cases} \tag{8}$$

where $img_1(i,\ j)$ and $img_2(i,\ j)$ are the $(i,\ j)$th pixel of two images img_1 and img_2, respectively. Moreover,

$UACI$ is described as Eq. (9):

$$UACI = \frac{\sum_{i=1}^{L}\sum_{j=1}^{C}|img_1(i,j) - img_2(i,j)|}{255 \times L \times C} \times 100\% \quad (9)$$

The research related to gray images with 256 levels show the expected values for $NPCR = 99.6938$ and $UACI = 33.4862$ [47,48]. Tables 3 and 4 summarizes $NPCR$ and $UACI$ values for seven standard gray images according to the critical values in [45]. The encrypted images of img_1 and img_2, related to two images with only one pixel changed, are considered to calculate these values.

Figure 4 shows an image, its corresponding encrypted images for RGB bounds, and the encrypted ones with only one-pixel change. Figure 4, along with Tables 3 and 4, demonstrates that the proposed method produces encrypted images that are resistant to differential attacks.

4.2. Statistical attack

To evaluate the abilities of this method, a statistical analysis is conducted on the differential attack. In the following sections, Correlation Coefficient and Histogram analyses are employed for both plain image and cipher image to investigate the effects of the system separately.

4.2.1. Correlation coefficient

The high correlation in adjacent pixels is one of the features in images. The correlation factor of adjacent pixels of the plain image should be reduced in the

Table 3. The values of NPCR by changing a pixel at (226,346).

Image name	NPCR	$\alpha = 0.001$		$\alpha = 0.01$		$\alpha = 0.05$	
		Limit	Situation	Limit	Situation	Limit	Situation
Female ($256 * 256$)	99.6019	99.5341	Passed	99.5527	Passed	99.5693	Passed
House ($256 * 256$)	99.6108	99.5341	Passed	99.5527	Passed	99.5693	Passed
Tree ($256 * 256$)	99.6112	99.5341	Passed	99.5527	Passed	99.5693	Passed
Mandrill ($512 * 512$)	99.6203	99.5717	Passed	99.5810	Passed	99.5893	Passed
Peppers ($512 * 512$)	99.5972	99.5717	Passed	99.5810	Passed	99.5893	Passed
Male ($1024 * 1024$)	99.6202	99.5906	Passed	99.5952	Passed	99.5994	Passed
Airport ($1024 * 1024$)	99.6169	99.5906	Passed	99.5952	Passed	99.5994	Passed

Table 4. The values of UACI by changing a pixel at (226,346).

Image name	UACI	$\alpha = 0.001$		$\alpha = 0.01$		$\alpha = 0.05$	
		Limit	Situation	Limit	Situation	Limit	Situation
Female ($256 * 256$)	31.2912	33.1594 33.7677	Passed	33.2255 3.7016	Passed	33.2824 3.6447	Passed
House ($256 * 256$)	31.2881	33.1594 33.7677	Passed	33.2255 33.7016	Passed	33.2824 33.6447	Passed
Tree ($256 * 256$)	31.2902	33.1594 33.7677	Passed	33.2255 3.7016	Passed	33.2824 3.6447	Passed
Mandrill ($512 * 512$)	33.4437	33.1594 3.7677	Passed	33.2255 33.7016	Passed	33.2824 33.6447	Passed
Peppers ($512 * 512$)	33.6142	33.1594 33.7677	Passed	33.2255 33.7016	Passed	33.2824 33.6447	Passed
Male ($1024 * 1024$)	33.4712	33.1594 33.7677	Passed	33.2255 33.7016	Passed	33.2824 33.6447	Passed
Airport ($1024 * 1024$)	33.4039	33.1594 33.7677	Passed	33.2255 33.7016	Passed	33.2824 33.6447	Passed

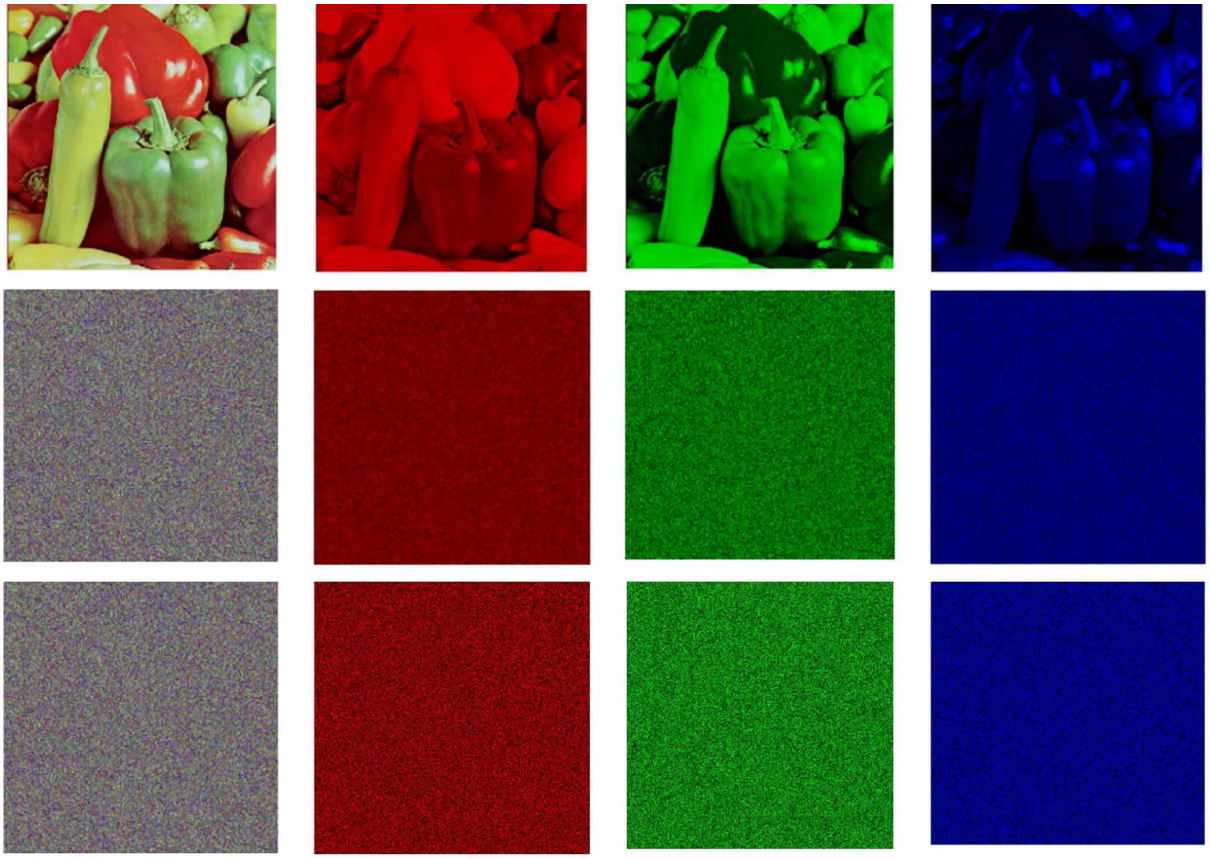

Figure 4. (a) Plain images, encrypted by (P, key_1), and decrypted by (P, key_2); (b) Red bounds of the corresponding images in (a); (c) Green bounds of the corresponding images in (a); and (d) Blue bounds of the corresponding images in (a).

ciphered image to investigate diffusion and confusion. Therefore, 3000 pairs of adjacent pixels are randomly chosen, and their horizontal, vertical, and diagonal correlation factors are calculated in both the plain and ciphered images as follows:

$$r_{x,y} = \frac{E\left\{[x - E(x)]\,[y - E(y)]\right\}}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{10}$$

$$E(x) = \frac{1}{s}\sum_{i=1}^{s} x_i, \tag{11}$$

$$D(x) = \frac{1}{s}\sum_{i=1}^{s} \left[x_i - E(x)\right]^2, \tag{12}$$

where x and y are the numbers of closest pixels. $E(x)$ is expectation and $D(x)$ shows x variance. Tables 5 and 6, along with Figure 5, illustrate the results of this analysis.

Table 6 compares the correlation coefficient of the proposed method and some of the other methods. This table shows that the proposed scheme understandably decreases a strong interaction in a clear image.

4.2.2. Using histogram analysis against statistical attacks

Histogram analysis is another test that shows the quality of the proposed method against statistical attacks. A histogram shows the distribution of the pixels in the image. Histogram uniformization of the ciphered image is one of the effects of encryption algorithms on plain images. Considering the histograms in Figure 6. This uniformization is examined through chi-squared analysis [57] as Eq. (13):

$$X^2_{test} = \sum_{i=1}^{t} \frac{(o_i - e_i)^2}{e_i}, \tag{13}$$

where t is the number of gray areas, o_i and e_i are noticed and assumed the number of each grey position, appropriately. Table 7 shows Chi-square test for some obtained cipher images. In the examined images, $t = 256$, coupled with the size of images $(256 * 256)$, e_i is equal to $\frac{256*256}{256} = 256$.

4.3. The importance of key analysis on the attacks

Two tests for the secret key are employed. These tests

Table 5. Correlation coefficient analysis.

Test images	Plain image			Cipher image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Female	0.9683	0.9649	0.9405	0.0028	0.0048	0.0036
House	0.9778	0.9619	0.9355	0.0034	0.0052	0.0042
Tree	0.9652	0.9427	0.9228	0.0037	0.0048	0.0018
Mandrill	0.9038	0.8453	0.8345	0.0018	0.0049	0.0023
Peppers	0.9781	0.9816	0.9705	0.0038	0.0038	0.0031
Splash	0.9887	0.9926	0.9866	0.0046	0.0052	0.0018

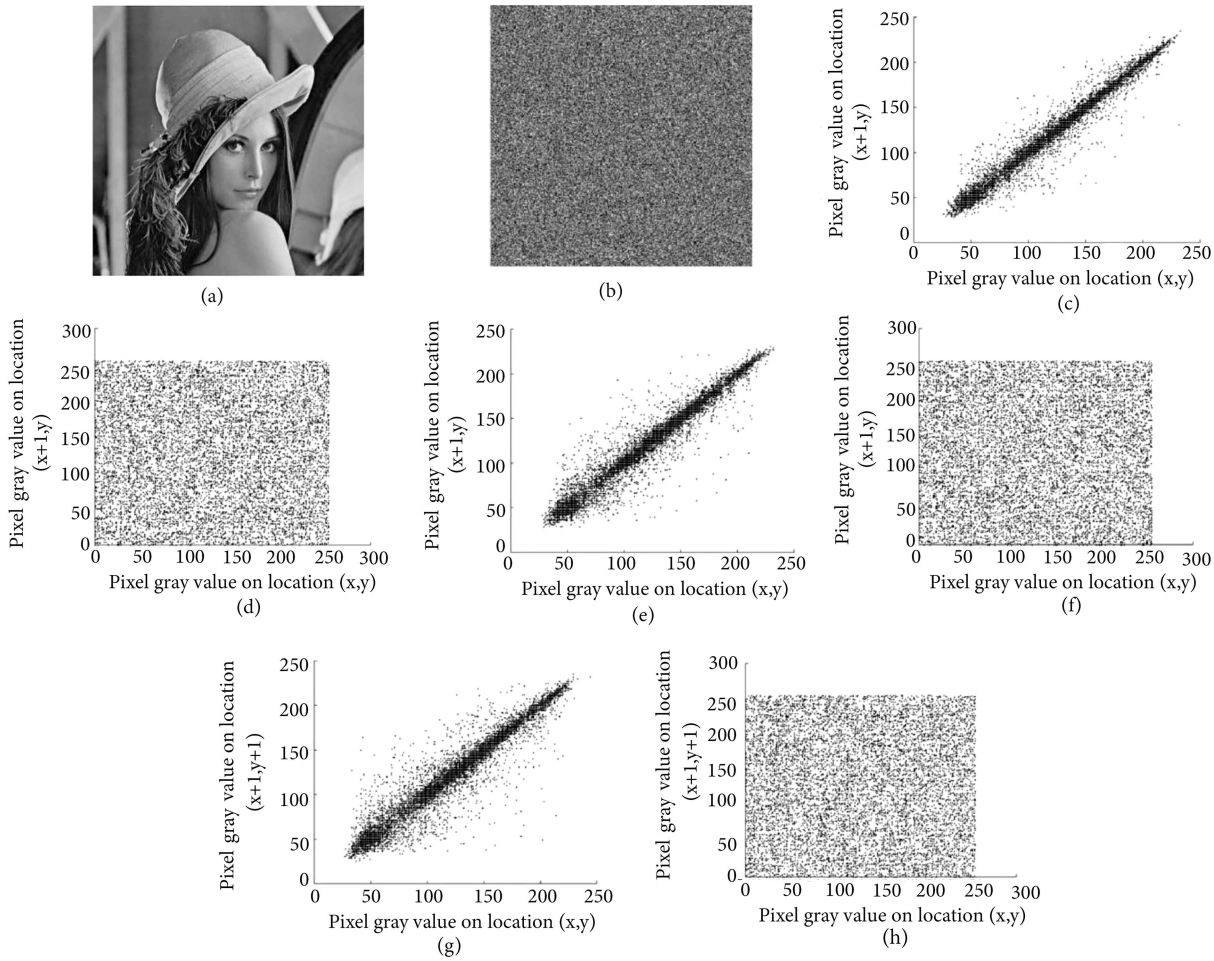

Figure 5. Correlation of two adjacent pixels (a) plain image of Lena; (b) Encrypted image of Lena; (c) vertical correlation of the plain image; (d) vertical correlation of the cipher image; (e) horizontal correlation of the plain image; (f) horizontal correlation of the cipher image; (g) diagonal correlation of the plain image; and (h) diagonal correlation for the cipher image.

include sensitivity and key space for the key. Enormous key space and high sensitivity play an important role against attacks such as brute force.

4.3.1. Key space analysis for brute-force attack

One of the methods used by the attackers is called a brute-force attack. In these attacks, all the possible states for the secret key are checked automatically, and their results are analyzed by special software. The secret key space should be as big as possible for the encryption to hold against these attacks. In the discussed method, along with producing random images, there are six parameters (x_0, x_1, and b) for the logistic map and 48 tables, one of which gets selected at the beginning of the encryption process. If the precision of numbers is 10–12, the proposed secret key

Table 6. Contribution of correlation for the offered method and some different methods for Lena's image.

	Vertical	Horizontal	Diagonal
Plain Lena image	**0.9883**	**0.9906**	**0.9823**
Zhang [49]	−0.0084	−0.0223	0.0086
Xu and Tian [50]	0.0053	−0.0067	0.0022
Zahmoul et al. [51]	−0.047	0.0015	0.0030
Zhang et al. [52]	0.0048	0.0022	0.0023
Wang et al. [53]	0.0022	0.0031	−0.0035
Wang and Su [54]	−0.0020	0.0023	0.0073
Alawida et al. [55]	−0.0017	−0.0084	−0.0019
Farah et al. [56]	−0.0173	0.0118	0.0080
Proposed method	**0.0047**	**0.0051**	**0.0011**

Table 7. Chi-square test for some obtained cipher images.

Image name	Calculated (R)	Status	Calculated (G)	Status	Calculated (B)	Status
Lena	254.83	Passed	260.89	Passed	256.35	Passed
Splash	246.13	Passed	264.76	Passed	229.14	Passed
Mandrill	274.45	Passed	256.75	Passed	215.15	Passed
Peppers	205.91	Passed	274.150	Passed	277.35	Passed

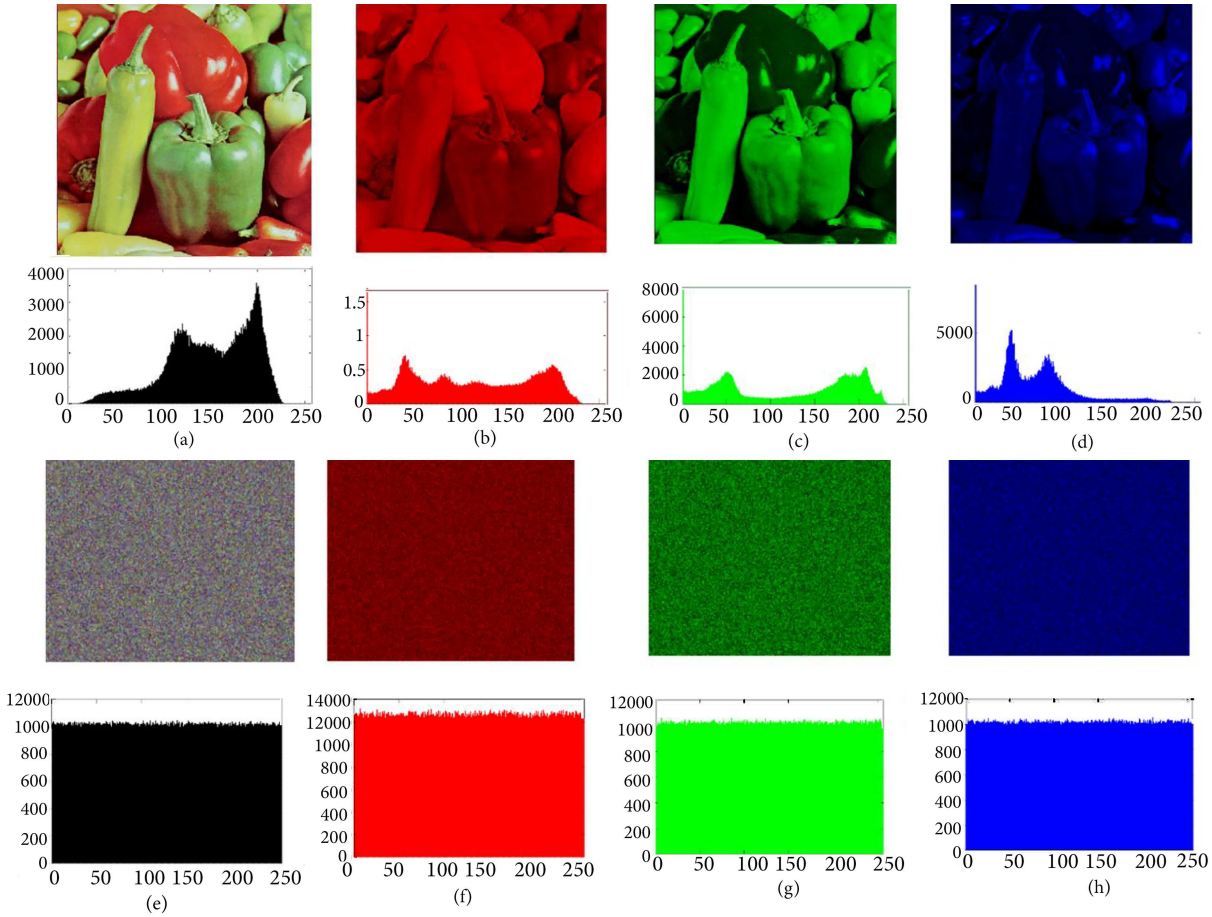

Figure 6. Plain image and its histogram for (a) original peppers, (b) red component, (c) green component, and (d) blue component. Cipher image and its histogram for (e) original peppers, (f) red component, (g) green component, and (h) blue component.

Table 8. Entropy results of plain and cipher images.

	Test images							
	Female	**House**	**Tree**	**Mandrill**	**Peppers**	**Splash**	**Male**	**Airport**
Plain image	6.8981	7.0686	7.5371	7.7624	7.6698	7.2428	7.5237	6.8303
Cipher image	7.9973	7.9970	7.9983	7.9996	7.9985	7.9987	7.9993	7.9978

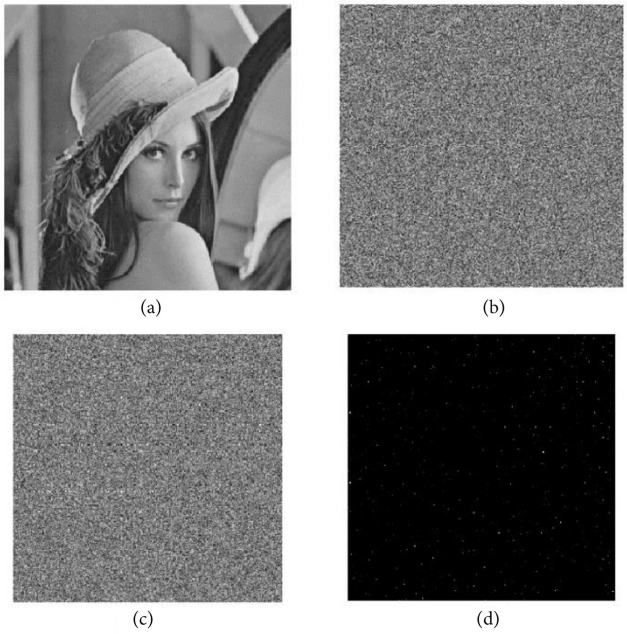

Figure 7. (a) Plain image of Lena; (b) Cipher image of Lena with initial value $x_0 = 0.1$ and $x_1 = 0.2$; (c) Cipher image of Lena with initial values $x_0 = 0.1000000001$ and $x_1 = 0.2000000001$; and (d) Differences between two cipher images.

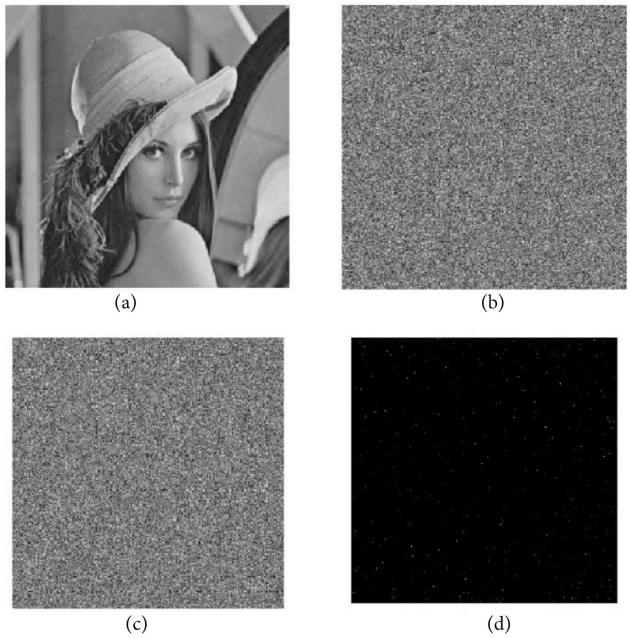

Figure 8. (a) Plain image of Lena; (b) cipher image of Lena with initial values $x_0 = 0.1$ and $x_1 = 0.2$; (c) decrypted image of Lena with initial values $x_0 = 0.099999999$ and $x_1 = 0.1999999999$; and (d) difference image showing the differences between (b) and (c).

space is $48 * (10^{12})^6 = 48{*}10^{72}$, which seems enough to resist brute-force attacks.

4.3.2. Key sensitivity test

Two issues should be considered in the sensitivity evaluation stage:

1. The encrypted images should have considerable differences if a plain image is encrypted via two keys with only one-bit alteration;
2. If a cipher image, with only one-bit alteration, is decrypted, the obtained image should have considerable differences from the plain image itself.

An image the size of $(512 * 512)$ is selected to examine the performance of the proposed system (Figure 7(a)). This image is encrypted twice with different keys with only one-bit alteration in initial values x_0 and x_1 (Figure 7(b) and (c)). Figure 7(d) illustrates the difference between two encrypted images. In this picture, the black color represents pixels with different values, and the white color represents pixels with similar colors; therefore, 99.62% of pixels have different values.

Moreover, Figure 8 depicts plain image, encrypted image using k_1, decrypted image using k_2, and the difference between plain and decrypted images. k_1 and k_2 are two keys with only one-bit alteration, and 99.58% of pixels have different values in the plain and decrypted images. The obtained results from these tests and analyses show a high sensitivity of the system to the secret key.

4.4. Information entropy to determine system uncertainty

In principle, information entropy determines to what extent an event is random. Information entropy, also known as Shannon entropy, reports the importance of being random with a mathematical value. Information entropy is a measure that indicates the randomness and unpredictability of a source, and it can be used as a tool for determining system uncertainty [58]. One can use

Table 9. Comparing entropy results.

Images	Plain	Proposed method	Zhang [49]	Xu and Tian [50]	Zahmoul et al. [51]	Zhang et al. [52]
Lena	7.4472	7.9993	7.9974	7.99928	7.9991	7.9991
			Wang et al. [53]	Wang and Su [54]	Alawida et al. [55]	Farah et al. [56]
			7.9992	7.9960	7.9975	7.9970

it to assess and measure image pixel value distribution in expressing uncertainty about image information. If the value related to entropy is high, it represents the more uniform distribution of pixel values. In general, information entropy is defined as [59]:

$$H(S) = \sum_{i=0}^{2N-1} P(s_i) \log\left(\frac{1}{p(s_i)}\right). \tag{14}$$

The nearer the value of the equation is to 8, the more uniform the distribution of pixels. A study on a sample image indicates that the equation's value is 7.408,491, whereas this value for an encrypted image related to the same image is 7.995,178. Table 8 shows the entropy of the results for some plain and encrypted images.

Considering the examinations conducted in this section, one can recognize the uniform and suitable distribution of encrypted images by the system that shows its resistance to attacks. Also, in Table 9, an information entropy comparison is made between the proposed method and some other methods.

4.5. Encryption Quality (EQ) measurement

To evaluate the EQ, we use the following quantitative analysis measure based on the difference between corresponding pixels in the two images, which is defined by Farah et al. [56]:

$$EQ = \frac{\sum_{i=0}^{255} |o_i(P) - o_i(C)|}{256}, \tag{15}$$

where o_i (P) and o_i (C) are the observed occurrences for the byte level i in the plain image P and ciphered image C, respectively. This measurement implies that the security level of the encryption method increases as the value of EQ increases. For a gray image with L lines and C columns, the upper value of EQ, represented as EQ_{upper}, can be derived from Eq. (15) as follows:

$$EQ_{upper} = \frac{510 \times L \times C}{256^2} \tag{16}$$

As a comparison with EQ_{upper}, the values of EQ for some standard images encrypted by the proposed method are listed in Table 10.

Table 10. Encryption quality analysis.

Images	EQ	EQ_{upper}
Female $(256 * 256)$	325.3901	510
House $(256 * 256)$	274.2891	510
Tree $(256 * 256)$	378.9712	510
Mandrill $(512 * 512)$	776.9688	20408
Peppers $(512 * 512)$	568.3047	2040
Splash $(512 * 512)$	946.5128	2040

4.6. Time performance of a cryptosystem

For the time performance of a cryptosystem, there is a need for both the algorithm's complexity and implementation. The complexity is analyzed from the perspective of mathematical and logical calculations and read-write operations on memory cells. The performance is evaluated in terms of run-time overheads imposed by the Encryption Throughput (ET) and the number of cycles needed for one-byte encryption [60]. The following definitions give the ET and the number of cycles in one-byte encryption or decryption.

$$ET = \frac{Image_{size}(MByte)}{Encryption_{Time}(second)}, \tag{17}$$

$$NC = \frac{SC}{ET}, \tag{18}$$

where NC is the cycle number for each byte, SC is the speed of cpu. Using Eq. (18), the comparison between cryptographic systems can be made independently of the operating systems and hardware used. Table 11 shows the values calculated via Eq. (17) and (18) for some particular images

5. Conclusion

On the one hand, an image encryption method is presented, using chaos features and DNA patterns. The use of DNA patterns results in increased system efficiency and fast encryption of images of very high volume. In the system, the increased security against attacks is focused in two ways. On the other hand, random DNA strands are created through the chaotic system, further applied in the algorithm's coding. The intrinsic nature of chaotic systems and their sensitivity to the initial value make the performance of the

Table 11. Throughput and speed analysis.

Images	Lena	Mandrill	Airplane	Couple
Encryption Throughput (ET)(MB/s)	10.777777	10.346666	9.264462	11.294117
Number of cycles per byte	173.5051	180.7345	201.8465	165.5729
Encryption Throughput (ET)(MB/s)	10.777777	10.346666	9.264462	11.294117
Number of cycles per byte	173.5051	180.7345	201.8465	165.5729

proposed method and its sensitivity to the key security very appealing. Moreover, this method implicates 48 tables, as operators, that are highly dependent on the plain image and initial values, which in turn increase the stability of the proposed encryption system against cryptanalysts in a way that the whole image would not be easily accessed, even if part of the plain data is at hand. Therefore, the suggested system will have high security in terms of keys and algorithms.

References

1. Li, M., Lu, D., Xiang, Y., et al. "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion", *Nonlinear Dynamics*, **96**(1), pp. 31-47 (2019). DOI: 10.1007/s11071-019-04771-7
2. Chen, L., Chen, J., Ma, L., et al. "Cryptanalysis of a chaotic image cipher based on plaintext-related permutation and lookup table", *Nonlinear Dynamics*, **100**(4), pp. 3959-3978 (2020). DOI: 10.1007/s11071-020-05735-y
3. Gong, L.H., He, X.T., Tan, R.C., et al. "Single channel quantum color image encryption algorithm based on HSI model and quantum Fourier transform", *International Journal of Theoretical Physics*, **57**(1), pp. 59-73 (2018). DOI: 10.1007/s10773-017-3541-1
4. Tong, X.J., Zhang, M., Wang, Z., et al. "An image encryption scheme based on dynamical perturbation and linear feedback shift register", *Nonlinear Dynamics*, **78**(3), pp. 2277-2291 (2014). DOI: 10.1007/s11071-014-1564-1
5. Kumar, P. and Rana, S.B. "Development of modified AES algorithm for data security", *Optik*, **127**(4), pp. 2341-2345 (2016). DOI: 10.1016/j.ijleo.2015.11.188
6. Zhou, M. and Wang, C. "A novel image encryption scheme based on conservative hyper-chaotic system and closed-loop diffusion between blocks", *Signal Processing*, **171**, 107484 (2020). DOI: 10.1016/j.sigpro.2020.107484
7. Abdelfatah, R.I., Nasr, M.E., and Alsharqawy, M.A. "Encryption for multimedia based on chaotic map: Several scenarios", *Multimedia Tools and Applications*, **79**(27), pp. 19717-19738 (2020). DOI: 10.1007/s11042-020-08788-8
8. Darwish, S.M. and Noori, Z.H. "Secure image compression approach based on fusion of 3D chaotic maps and arithmetic coding", *IET Signal Processing*, **13**(3), pp. 286-295 (2018). DOI: 10.1049/iet-spr.2018.5063
9. Wang, X. Y., Yang, L., Liu, R., et al. "A chaotic image encryption algorithm based on perceptron model", *Nonlinear Dynamics*, **62**(3), pp. 615-621 (2010). DOI: 10.1007/s11071-010-9749-8
10. Lan, R., He, J., Wang, S., et al. "Integrated chaotic systems for image encryption", *Signal Processing*, **147**, pp. 133–145 (2018). DOI: 10.1016/j.sigpro.2018.01.026
11. Liu, S., Guo, C., and Sheridan, J.T. "A review of optical image encryption techniques", *Optics and Laser Technology*, **57**, pp. 327–342 (2014). DOI: 10.1016/j.optlastec.2013.05.023
12. Wang, X., Feng, L., and Zhao, H. "Fast image encryption algorithm based on parallel computing system", *Information Sciences*, **486**, pp. 340–358 (2019). DOI: 10.1016/j.ins.2019.02.049
13. Selimović, F., Stanimirović, P., Saračević, M., et al. "Authentication based on the image encryption using delaunay triangulation and catalan objects", *Acta Polytechnica Hungarica*, **17**(6) (2020).
14. Lin, Z., Liu, J., Lian, J., et al. "A novel fast image encryption algorithm for embedded systems", *Multimedia Tools and Applications*, **78**(14), pp. 20511-20531 (2019). DOI: 10.1007/s11042-018-6824-5
15. Rashid, M.I., Ferdaus, F., Talukder, B.B., et al. "True random number generation using latency variations of FRAM", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **29**(1), pp. 14-23 (2020). DOI: 10.1109/TVLSI.2020.3018998
16. Reddy, M.I., Kumar, A.S., and Reddy, K.S. "A secured cryptographic system based on DNA and a hybrid key generation approach", *Biosystems*, **197**, 104207 (2020). DOI: 10.1016/j.biosystems.2020.104207
17. Norouzi, B., Seyedzadeh, S.M., Mirzakuchaki, S., et al. "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos", *Multimedia Tools and Applications*, **74**(3), pp. 781-811 (2015). DOI: 10.1007/s11042-013-1699-y
18. Yavuz, E., Yazıcı, R., Kasapbaşı, M.C., et al. "A chaos-based image encryption algorithm with simple logical functions", *Computers and Electrical Engineering*, **54**, pp. 471-483 (2016). DOI: 10.1016/j.compeleceng.2015.11.008
19. Masood, F., Ahmad, J., Shah, S.A., et al. "A novel hybrid secure image encryption based on julia set of

fractals and 3D Lorenz chaotic map", *Entropy*, **22**(3), 274 (2020). DOI: 10.3390/e22030274

20. Zhang, Q. and Han, J. "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding", *Multimedia Tools and Applications*, **80**(9), pp. 13841–13864 (2021). DOI: 10.1007/s11042-020-10437-z
21. François, M., Grosges, T., Barchiesi, D., et al. "Image encryption algorithm based on a chaotic iterative process", *Applied Mathematics*, **3**(12), pp. 1910–1920 (2012). DOI: 10.4236/am.2012.312262
22. Midoun, M.A., Wang, X., and Talhaoui, M.Z. "A sensitive dynamic mutual encryption system based on a new 1D chaotic map", *Optics and Lasers in Engineering*, **139**, 106485 (2021). DOI: 10.1016/j.optlaseng.2020.106485
23. Xian, Y. and Wang, X. "Fractal sorting matrix and its application on chaotic image encryption", *Information Sciences*, **547**, pp. 1154-1169 (2021). DOI: 10.1016/j.ins.2020.09.055
24. Wang, Y., Wong, K.W., Liao, X., et al. "A new chaos-based fast image encryption algorithm", *Applied Soft Computing*, **11**(1), pp. 514–522 (2011). DOI: 10.1016/j.asoc.2009.12.011
25. Talhaoui, M.Z. and Wang, X. "A new fractional one-dimensional chaotic map and its application in high-speed image encryption", *Information Sciences*, **550**, pp. 13-26 (2021). DOI: 10.1016/j.ins.2020.10.048
26. Li, S., Mou, X., and Cai, Y. "Improving security of a chaotic encryption approach", *Physics Letters A*, **290**(3-4), pp. 127-133 (2001).
27. Milani, M.M.R.A., Pehlivan, H., and Pour, S.H. "Kaos tabanlı bir şifreleme yöntemi ve analizi. XIII", *Akademik Bilişim Konferansi Bildiriler Kitabi*, pp. 2-4 (2013). DOI: 10.1007/s11554-023-01289-5
28. Anderson, D.R. "Model based inference in the life sciences: a primer on evidence", *Springer Science and Business Media* (2007). DOI: 10.1007/s11235-016-0212-0
29. Matthews, R. "On the derivation of a "chaotic" encryption algorithm", *Cryptologia*, **13**(1), pp. 29–42 (1989). DOI: 10.1080/0161-118991863745
30. Daneshgar, A. and Khadem, B. "A self-synchronized chaotic image encryption scheme", *Signal Processing: Image Communication*, **36**, pp. 106–114 (2015). DOI: 10.1016/j.image.2015.06.005
31. Wang, X., Chen, S., and Zhang, Y. "A chaotic image encryption algorithm based on random dynamic mixing", *Optics and Laser Technology*, **138**, 106837 (2021). DOI: 10.1016/j.optlastec.2020.106837
32. Zhang, Y.Q. and Wang, X.Y. "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation", *Nonlinear Dyn*, **77**, pp. 687–698 (2014). https://dergipark.org.tr/en/download/article-file/2554292
33. Liu, L., Xiang, H., and Li, X. "A novel perturbation method to reduce the dynamical degradation of digital chaotic maps", *Nonlinear Dynamics*, **103**(1), pp. 1099–1115 (2021). DOI: 10.1007/s11071-020-06113-4
34. Liu, L. and Miao, S. "Delay-introducing method to improve the dynamical degradation of a digital chaotic map", *Information Sciences*, **396**, pp. 1–13 (2017). DOI: 10.1016/j.ins.2017.02.031
35. Wang, Q., Zhang, Q., and Wei, X. "Image encryption algorithm based on DNA biological properties and chaotic systems", *In 2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA)*, pp. 132-136, IEEE (2010). DOI: 10.1109/BICTA.2010.5645338
36. Masood, F., Masood, J., Zhang, L., et al. "A new color image encryption technique using DNA computing and chaos-based substitution box", *Soft Computing*, pp. 1-17 (2021). DOI: 10.1007/s00500-021-06459-w
37. Gehani, A., LaBean, T., and Reif, J. "DNA-based cryptography", *In Aspects of Molecular Computing*, pp. 167-188. Springer, Berlin, Heidelberg (2003). DOI: 10.1007/978-3-540-24635-0_12
38. Kalsi, S., Kaur, H., and Chang, V. "DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation", *Journal of Medical Systems*, **42**(1), pp. 1-12 (2018).
39. Elmoselhy, A. and El-Alfy, E.S. "On DNA cryptography for secure data storage and transfer", In *3rd Smart Cities Symposium (SCS 2020)*, 2020 (174-180), IET (2020). DOI: 10.1007/s10916-017-0851-z
40. Niu, Y., Zhou, Z., and Zhang, X. "An image encryption approach based on chaotic maps and genetic operations", *Multimedia Tools and Applications*, **79**(35), pp. 25613-25633 (2020). DOI: 10.1007/s11042-020-09237-2
41. Wang, X. and Liu, C. "A novel and effective image encryption algorithm based on chaos and DNA encoding", *Multimedia Tools and Applications*, **76**(5), pp. 6229–6245 (2017). DOI: 10.1007/s11042-016-3311-8
42. Biham, E. and Shamir, A. "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, **4**(1), pp. 3–72 (1991). DOI: 10.1007/BF00630563
43. Biham, E. and Shamir, A. "Differential cryptanalysis of the full 16-round DES", In *Annual International Cryptology Conference*, pp. 487–496, Springer, Berlin, Heidelberg (1992). DOI: 10.1007/3-540-48071-4_34
44. Mao, Y., Chen, G., and Lian, S. "A novel fast image encryption scheme based on 3D chaotic baker maps", *International Journal of Bifurcation and Chaos*, **14**(10), pp. 3613–3624 (2004). DOI: 10.1142/S021812740401151X
45. Wu, Y., Noonan, J.P., and Agaian, S. "NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology", *Journal of Selected Areas in Telecommunications (JSAT)*, **1**(2), pp. 31–38 (2011). https://www.cyberjournals.com/Papers/Apr2011

46. Huang, C.K., and Nien, H.H. "Multi chaotic systems-based pixel shuffle for image encryption", *Optics Communications*, **282**(11), pp. 2123–2127 (2009). DOI: 10.1016/j.optcom.2009.02.044

47. Fu, C., Chen, J.J., Zou, H., et al. "A chaos-based digital image encryption scheme with an improved diffusion strategy", *Optics Express*, **20**(3), pp. 2363–2378 (2012). DOI: 10.1364/OE.20.002363

48. Wu, Y., Zhou, Y., Saveriades, G., et al. "Local Shannon entropy measure with statistical tests for image randomness", *Information Sciences*, **222**, pp. 323–342 (2013). DOI: 10.1016/j.ins.2012.07.049

49. Zhang, Y. "The fast image encryption algorithm based on lifting scheme and chaos", *Information Sciences*, **520**, pp. 177–194 (2020). DOI: 10.1016/j.ins.2020.02.012

50. Xu, M. and Tian, Z. "A novel image cipher based on 3D bit matrix and latin cubes", *Information Sciences*, **478**, pp. 1–14 (2019). DOI: 10.1016/j.ins.2018.11.010

51. Zahmoul, R., Ejbali, R., and Zaied, M. "Image encryption based on new Beta chaotic maps", *Optics and Lasers in Engineering*, **96**, pp. 39-49 (2017). DOI: 10.1016/j.optlaseng.2017.04.009

52. Zhang, Y.Q., He, Y., Li, P., et al. "A new color image encryption scheme based on 2DNL-CML system and genetic operations", *Optics and Lasers in Engineering*, **128**, 106040 (2020). DOI: 10.1016/j.optlaseng.2020.106040

53. Wang, X., Xue, W., and An, J. "Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household", *Chaos, Solitons and Fractals*, **141**, 110309 (2020). DOI: 10.1016/j.chaos.2020.110309

54. Wang, X. and Su, Y. "Image encryption based on compressed sensing and DNA encoding", *Signal Processing: Image Communication*, **95**, 116246 (2021). DOI: 10.1016/j.image.2021.116246

55. Alawida, M., Samsudin, A., Teh, J.S., et al. "A new hybrid digital chaotic system with applications in image encryption", *Signal Processing*, **160**, pp. 45-58 (2019). DOI: 10.1016/j.sigpro.2019.02.016

56. Farah, M.A., Farah, A., and Farah, T. "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box", *Nonlinear Dynamics*, **99**(4), pp. 3041-3064 (2020). DOI: 10.1007/s11071-019-05413-8

57. Kwok, H.S. and Tang, W.K. "A fast image encryption system based on chaotic maps with finite precision representation", *Chaos, Solitons and Fractals*, **32**(4), pp. 1518-1529 (2007). DOI: 10.1016/j.chaos.2005.11.090

58. Shannon, C.E. "Communication theory of secrecy systems", *The Bell System Technical Journal*, **28**(4), pp. 656-715 (1949). DOI: 10.1002/j.1538-7305.1949.tb00928.x

59. Amin, M., Faragallah, O.S., and Abd El-Latif, A.A. "A chaotic block cipher algorithm for image cryptosystems", *Communications in Nonlinear Science and Numerical Simulation*, **15**(11), pp. 3484-3497 (2010). DOI: 10.1016/j.cnsns.2009.12.025

60. Farajallah, M. "Chaos-based crypto and joint crypto-compression systems for images and videos", *Doctoral dissertation, Universite de Nantes* (2015). https://hal.science/tel-01179610

Biography

Muhammed Milani was born in Tabriz. He got his BSc degree in 1997 on Computer Engineering, MSc degree in 2006 on Information Technology at Amir Kabir Technical University, Tehran, and PhD degree in 2015 on Computer Engineering at Karadeniz Technical University, Trabzon. His primary research area is Symbolic Computing, Functional Programming and Cryptography. Since 2019, he has been working as an Assistant Professor at Department of Computer Engineering in Bandırma Onyedi Eylül University.