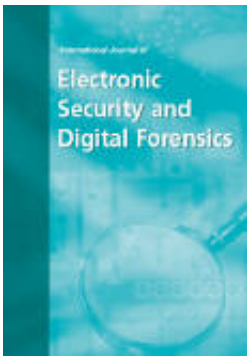


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Colour image encryption based on an improved fractional-order logistic map

Ismail Haddad, Djamel Herbadji, Aissa Belmeguenai, Selma Boumerdassi

DOI: 10.1504/IJESDF.2023.10045890

Article History:
Received: 25 November 2021
Accepted: 18 February 2022
Published online: 15 December 2022

Colour image encryption based on an improved fractional-order logistic map

Ismail Haddad, Djamel Herbadji* and Aissa Belmeguenai

Electronics Research Laboratory,
University 20 August 1955,
Skikda 21000, Algeria
Email: i.haddad@univ-skikda.dz
Email: d.herbadji@univ-skikda.dz
Email: a.belmeguenai@univ-skikda.dz
*Corresponding author

Selma Boumerdassi

Conservatoire National des Arts et Métiers,
292 Rue-Martin, Paris Cédex 03 F-75141, France
Email: selma.boumerdassi@cnam.fr

Abstract: In this work, we use an improved fractional-order logistic map to introduce a new colour image encryption algorithm. By analysing the Lyapunov exponent and the bifurcation diagram, the map provides a wider range and a uniform distribution of data compared to its classical. It also has additional parameters and thus a larger key space, which makes it better in protection and safety against hacker attacks. Our algorithm relies on random input of pixels in order to obtain a different image in each encryption round to ensure greater protection. The algorithm also provides great permutation and diffusion features. The simulation results and security analysis indicate that our scheme has a good impact on encryption and can withstand various attacks, such as statistical attack, differential attack and data loss and noise attacks.

Keywords: fractional-order; logistic map; image encryption; security analysis.

Reference to this paper should be made as follows: Haddad, I., Herbadji, D., Belmeguenai, A. and Boumerdassi, S. (2023) 'Colour image encryption based on an improved fractional-order logistic map', *Int. J. Electronic Security and Digital Forensics*, Vol. 15, No. 1, pp.66–87.

Biographical notes: Ismail Haddad received his Bachelor's in Electronic in 2017 and Master's in Electronic in 2019, where he is currently pursuing his PhD in Communications and Information Processing from the University of Skikda, Algeria. His main research interests include digital watermarking and image encryption.

Djamel Herbadji received his Bachelor's in Computer Science in 2014 and Master's in Telecommunications in 2016, and PhD in Communications and Information Processing from the University of Skikda in 2020, Algeria. His main research interests include authentication, digital watermarking, image encryption and digital signatures.

Aissa Belmeguenai obtained his Engineer and Magister in Electronic from the Annaba University, Algeria in 1995 and 2001. He received his Doctorate in 2009 in Electronic from the Annaba University. In January 2012 he received his HDR in Electronic from 20 August 1955 University – Skikda and he is a member of the Research Laboratory in Electronics of Skikda. He is currently an MC and Researcher at the 20 August 1955 University – Skikda. From 2001 to date, he is working as a Junior Lecturer at the 20 August 1955 University – Skikda. His areas of research are data encryption and Boolean functions intervening in symmetrical cryptography.

Selma Boumerdassi is an Associate Professor at the Conservatoire National des Arts et Metiers, Paris. She received her PhD in Computer Science from the University of Versailles in 1998, where she also served as an Assistant Professor from 1998 to 2000. Her research interests include wireless and mobile networks, with a special focus on the impact and use of social networks. She worked on several national projects and served as an expert for the evaluation of French national projects (ANR). She is an author of more than 50 articles and serves as a TPC member for various international journals and conferences.

1 Introduction

Nowadays, with the great increasing popularity of the internet and with the evolution of network technology, digital images have become very pivotal and of important role, so it has become necessary to secure these images on the network (Enayatifar et al., 2017; Suri and Vijay, 2019). Because of certain intrinsic features that characterise images, such as large data space, correlation between neighbouring pixels and high level of redundancy. The use of some traditional encryption algorithms has become ineffective such as data encryption standard (DES) and advanced encryption standard (AES) and Rivest Shamir-Afleman (RSA) (Liu et al., 2020; Enayatifar et al., 2014; Wu et al., 2015). Furthermore, in order to meet the requirement for the safe transmission of digital images. Encryption algorithm using chaotic systems has attracted considerable interest from researchers because of the important features that these systems provide, such as highly sensitive, dependence on initial conditions and control parameters, unpredictability, pseudo-randomness, ergodicity and complex dynamic characteristic (Li et al., 2017; Wu et al., 2017; Chen et al., 2004; Zhu et al., 2011; Zhou et al., 2016; Xu et al., 2016a, 2016b; Herbadji et al., 2019a, 2019b, 2019c, 2020a, 2020b). Therefore, the chaotic systems can be used to encrypt images.

The fractional differential equations have recently attracted extensive interest from researchers (Lin and Qu, 2019; Shammakh and El-Shahed, 2011; Ruan et al., 2018; Khalil et al., 2014; Singh et al., 2017; Kumar et al., 2017; Tarasov, 2015; Srivastava et al., 2017; Li et al., 2011; El Raheem and Salman, 2017), because of their applications in various fields, for example control (Using et al., 2014), electromagnetics (Shamim et al., 2011) and analog electrical engineering (Radwan et al., 2008; Said et al., 2016). Fractional-order dynamic systems display different and new behaviours in bifurcation and attractors. It also shows different chaotic behaviours compared with the integer-order equation (Zhang et al., 2020), also the encryption algorithms using fractional chaotic systems have a greater security characteristic due to the fractional order parameter, which

provides more range and freedom as pseudorandom number generators (PRNG). Despite the fact that fractional order chaotic systems, such as fractional order logistic map, are preferred over integer order chaotic systems. However, it still suffers from some problems such as uneven distribution of data and limited chaotic behaviour. Many researchers have recently become interested in image encryption based on fractional order chaos, where several encryption methods have been suggested. Zhao et al. (2015) proposed an improper fractional-order chaotic system for image encryption, this scheme relies on splitting the original image into four parts to implement the diffusion and substitution process. Wu et al. (2015) introduced a new encryption model, which includes permutation and diffusion process. They used coupled-map lattices (CML) and a fractional-order chaotic system to encrypt red, green and blue components of the colour image. Yang et al. (2020) suggested a new image encryption technique based on the fractional order hyper-chaotic system, where they confirm that the hyper-chaotic sequence may be used in image encryption since it is more unpredictable. Mani et al. (2019) presented an image encryption algorithm in which fractional order chaotic fuzzy cellular neural networks (FOFCNNs) were employed to produce pseudo-random sequences to implement the diffusion process. Li et al. (2017) suggested a new technique combining the fractional-order hyper-chaotic system with DNA sequence to increase the level of image encryption security. Lui et al. (2020) suggested a fast chaotic image scheme model depend on permutation and diffusing at the same time, which provides more protection against separated attack. Zhang et al. (2020) suggested an image encryption model using S-boxes and fractional order chaotic system, where it was confirmed that the system provides better protection against cryptanalyst attacks due to its wider range and higher chaotic behaviour than its classical one. Xu et al. (2014) designed a novel image encryption method where they used a combination of the fractional chaotic system and its synchronisation system to encrypt and decrypt the image.

This research aims to enhance the fractional-order logistic map in order to overcome its issues to use in image encryption. Therefore, a novel image encryption approach using an improved fractional-order logistic map has proposed. Several analyses have been discussed to ensure the proposed algorithm's effectiveness in protecting the requirements for transferring digital images, such as correlation coefficients, sensitivity analysis, histogram, differential attacks, as well as other analytical measurements.

The architecture of this paper is structured as follows: Section 2 provides analysis of the fractional-order logistic map and the enhanced one. In Section 3, we propose the novel image encryption algorithm in detail. Section 4 summarises the suggested scheme evaluation as well as the simulation results. Finally, the conclusion is given in Section 5.

2 Analysis of the fractional-order logistic map and improved map

Fractional-order calculus is the generalisation of the conventional integer-order calculus. The fractional-order logistic map is calculated using the Caputo fractional-order derivative. The definition of Caputo is presented as follows:

$$D_{t0}^{a} f(t) = \frac{1}{\Gamma(m-a)} \int_{t0}^{t} f^{(m)}(u)(t-u)^{m-a-1} du \tag{2.1}$$

where α is the fractional order, m is an integer thus $(m-1) < a < m$ and $\Gamma(.)$ is the gamma function.

Consider the fractional differential equations given by (Akbergenov and Pelyukh, 2016; El-Sayed and Salman, 2013):

$$D^a x(t) = \rho x(t)\big(1 - x(t)\big), \quad t > 0 \tag{2.2}$$

with $x(0) = x_0$ is the initial condition, α is the fractional-order parameter and ρ is the growth rate.

In the next section, we present the process of discretisation to discretise the counterpart of equation (2.2) with piecewise constant arguments

$$D^a x(t) = \rho x\left(\left\lceil \frac{t}{r} r \right\rceil\right)\left(1 - x\left(\left\lceil \frac{t}{r} r \right\rceil\right)\right), \tag{2.3}$$

where $x(0) = x_0$ the initial condition, r is is a constant.

Let $t \in \lceil 0, r \rceil$, then $\frac{t}{r} \in \lceil 0, r \rceil$ so, we obtain:

$$D^a x(t) = \rho x_0(t)\big(1 - x_0\big), \quad t \in \lceil 0, r \rceil \tag{2.4}$$

The solution of equation (2.3) is given by:

$$\begin{aligned} x_1(t) &= x_0 + I^a \rho x_0 \left(1 - x_0\right) \\ &= x_0 + \rho x_0 \left(1 - x_0\right) \int_0^t \frac{(t-s)^{\alpha-1}}{\Gamma(\alpha)} ds \\ &= x_0 + \rho x_0 \left(1 - x_0\right) \frac{t^\alpha}{\Gamma(1+\alpha)} \end{aligned} \tag{2.5}$$

Let $t \in \lceil r, 2r \rceil$, then $\frac{t}{r} \in \lceil 1, 2 \rceil$ so, we obtain:

$$D^a x(t) = \rho x_1(t)\big(1 - x_1\big), \quad t \in \lceil 0, 2r \rceil \tag{2.6}$$

The following is the solution of equation (2.3):

$$\begin{aligned} x_2(t) &= x_1(r) + I_t^\alpha \rho x_1 \left(1 - x_1\right) \\ &= x_1(r) + \rho x_1 \left(1 - x_1\right) \int_r^t \frac{(t-s)^{\alpha-1}}{\Gamma(\alpha)} ds \\ &= x_1(r) + \rho x_1(r)\big(1 - x_1(r)\big) \frac{(t-s)^\alpha}{\Gamma(1+\alpha)} \end{aligned} \tag{2.7}$$

We can easily find the solution of equation (2.3) by repeating the process. This solution is given as follows:

$$x_{n+1}(t) = x_n(nr) + \frac{(t-nr)^\alpha}{\Gamma(1+\alpha)} \rho x_n(nr)\big(1 - x_n(nr)\big), t \in \lceil nr, (n+1)r \rceil \tag{2.8}$$

Let $t \to (n+1)r$ the discretisation is obtained

$$x_{n+1}\left((n+1)r\right) = x_n(nr) + \frac{r^{\alpha}}{\Gamma(1+\alpha)}\rho x_n(nr)\left(1-x_n(nr)\right) \tag{2.9}$$

Consequently, the fractional-order logistic map is obtained:

$$x_{n+1} = x_n + \frac{r^{\alpha}}{\Gamma(1+\alpha)}\rho x_n\left(1-x_n\right) \tag{2.10}$$

where r is a constant, α is the fractional-order parameter, ρ is the growth rate and x_n is the current population.

To overcome the issues of the fractional order logistic map, we suggest improving it by applying basic mathematical operation and the use of the modular arithmetic (mod1).The mathematical equation for the improved map is presented as follows:

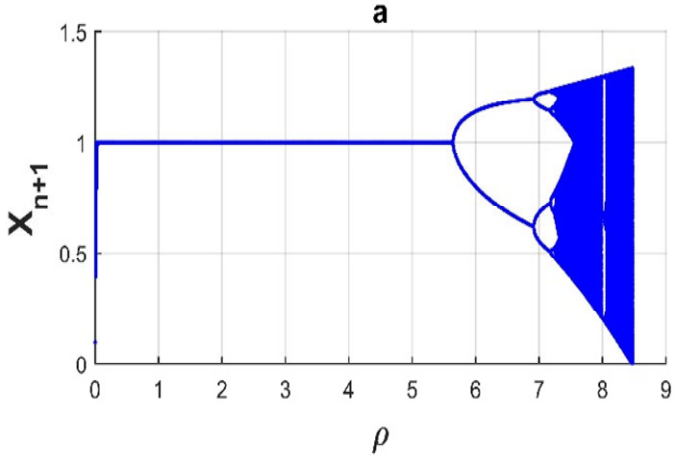
$$x_{n+1} = 2^k \times x_n + \frac{r^{\alpha}}{\Gamma(1+\alpha)}\rho \times 2^k \times x_n\left(1-2^k \times x_n\right) \bmod 1 \tag{2.11}$$

where k is a constant, x_n in equation (2.10) is replaced with the term $(2^k \times x_n)$.

2.1 Bifurcation diagram

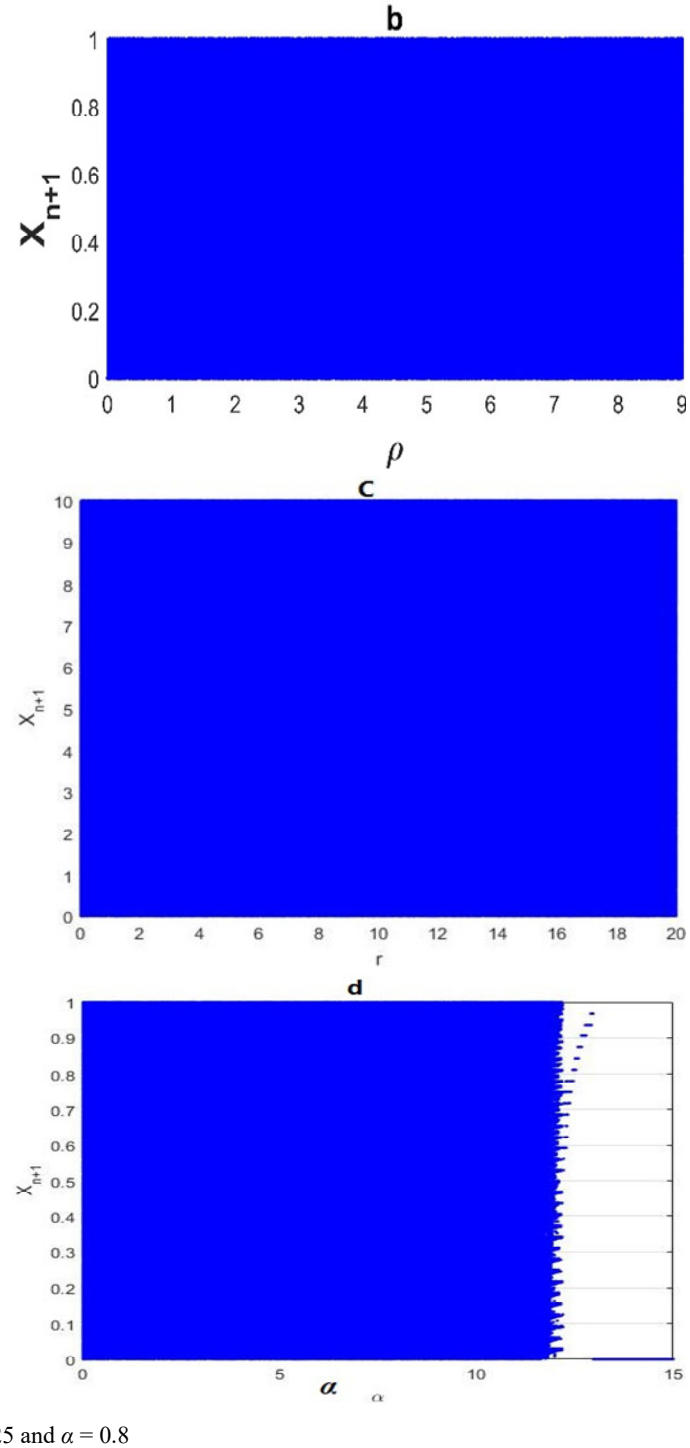
Bifurcation diagram is the study of the dynamic behaviour of a system in terms of control parameter values (Ramadan et al., 2016). Figure 1 presents the diagram of the bifurcation of the improved map and the fractional-order logistic map. The dotted area indicates that the system is chaotic, and the empty zone proves that the system behaviour is not chaotic.

Figure 1 Fractional order logistic map (a) and the improved map (b–d) bifurcation diagrams (see online version for colours)



Notes: $r = 0.25$ and $\alpha = 0.8$

Figure 1 Fractional order logistic map (a) and the improved map (b–d) bifurcation diagrams (continued) (see online version for colours)



Notes: $r = 0.25$ and $\alpha = 0.8$

As the Figure 1 shows, the improved map has chaotic characteristics over the entire parameter field $\rho \in [0, 9]$. While, the range of the chaotic behaviour of the fractional order logistic map is $\rho \in [7.30, 8.47]$. Which means that the improved map provides better chaotic performance than the fractional order logistic map.

2.2 Lyapunov exponent

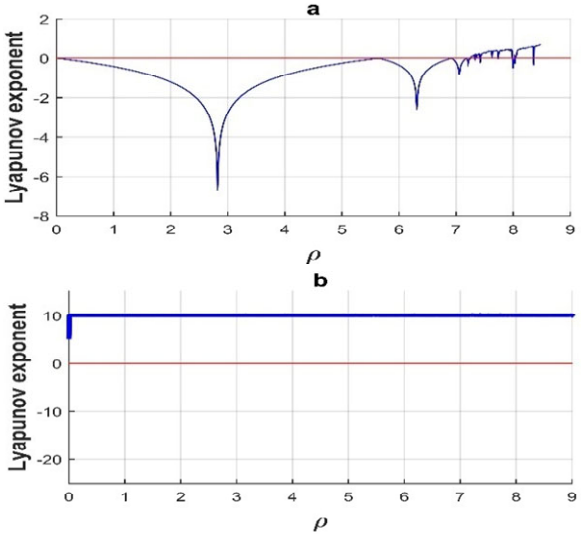
Lyapunov exponent is an important measure for assessing dynamic behaviour and identifying the system chaotic degree (Nosrati and Shafiee, 2018). The equation of Lyapunov exponent is given as follows.

$$ly = \lim_{n \to +\infty} \frac{1}{n} \sum_{i=1}^{N} \ln \left| f\left(x_i\right)' \right| \tag{2.12}$$

where f' is the derivation function of the chaotic system f. When the Lyapunov exponent exceeds zero $ly > 0$, this indicates that the behaviour of the system is chaotic.

The improved map and the fractional-order logistic map Lyapunov exponents are shown in Figure 2.

Figure 2 (a) Lyapunov exponent curves of the fractional-order logistic map and (b) the improved map (see online version for colours)



As the Figure 2 shows, the range of positive Lyapunov exponent values for the improved map is greater than the fractional order logistic map.

2.3 Randomness

NIST is a collection of 15 critical tests for measuring the quality of a binary sequence randomness (Wu et al., 2015). For every test, the P value must be greater than 0.01 to confirm the success of the binary sequence in the test (Herbadji et al., 2020b).

In order to make sure that the improved fractional-order chaotic system can be used for image encoding, we performed a NIST-800-22 test on the sequences generated by this

system. The results for NIST tests shown in the Table 1, where we can see that the improved map successfully passed every 15 tests. As a result, the sequences created by this system contain a high degree of randomness and are suited for image encryption.

Table 1 NIST-800-22 test results of the improved fractional order logistic map

NIST tests	*P value*	*Results*
Frequency	0.638355017565112	Success
Block frequency test	0.388233403726571	Success
Runs test	0.958352670669443	Success
Longest runs of ones test	0.201377525588149	Success
Binary matrix test	0.421450616751419	Success
DFT test	0.594556664151719	Success
Non-overlapping template matching	0.0712333835934371	Success
Overlapping template matching	0.324397624273318	Success
Maurer's universal statistical test	0.645937742145016	Success
Linear complexity	0.3988135818906010	Success
Serial test	0.899825376592255	Success
Approximate entropy test	0.89331304289261	Success
Cumulative sums	0.627394094334661	Success
Random excursions	0.988758946011156	Success
Random excursions variant	0.990123446161416	Success

3 Proposed colour image encryption algorithm

In this part, we propose a novel algorithm for image encryption using improved fractional-order logistic map. The latter has more parameters and a wider key than the classic map. The key for the proposed algorithm consists of 18 parameters presented as follows:

$$x_{0.1}, \rho_{0.1}, \alpha_{0.1}, x_{0.2}, \rho_{0.2}, \alpha_{0.2}, x_{0.3}, \rho_{0.3}, \alpha_{0.3}, x_{0.4}, \rho_{0.4}, \alpha_{0.4}, x_{0.5}, \rho_{0.5}, \alpha_{0.5}, x_{0.6}, \rho_{0.6}, \alpha_{0.6}$$

The suggested algorithm is illustrated in Figure 3. The proposed algorithm uses a two-round encryption structure, as seen in Figure 3. Random pixel insertion, permutation, and diffusion processes are all used in each encryption round. The details of the encryption scheme are shown in the steps that follow:

Step 1 Read the colour image $\boldsymbol{O}_{\boldsymbol{n}\times\boldsymbol{m}\times 3}$, in the beginning of each row of the original image, we add a pixel with a random value. To do the random input of pixels we use the function Rand that produces random numbers. The aim of inserting a random pixel is to obtain a random, different image for each round of encryption.

Step 2 In this part, we introduce a permutation algorithm to break the correlation between pixels. This algorithm simultaneously alters the image's row and

column. In the following, we will show the details of the suggested permutation algorithm:

- Let X, Y two random sequences, $\boldsymbol{X} = \{\boldsymbol{X}_1, \boldsymbol{X}_2 \ldots \ldots \ldots \ldots \boldsymbol{X}_M\}$ of length $\boldsymbol{M}$ and, $\boldsymbol{Y} = \{\boldsymbol{Y}_1, \boldsymbol{Y}_2 \ldots \ldots \ldots \ldots \boldsymbol{Y}_N\}$ of length $(\boldsymbol{N}+1)$ generated by the equation (2.11) with the initial values $(\boldsymbol{x}_{0.1}, \boldsymbol{\rho}_{0.1}, \boldsymbol{\alpha}_{0.1})$, $(\boldsymbol{x}_{0.2}, \boldsymbol{\rho}_{0.2}, \boldsymbol{\alpha}_{0.2})$.
- We get two index sequences $\boldsymbol{I}$, $\boldsymbol{J}$ by sorting the chaotic sequences $\boldsymbol{X}$ and $\boldsymbol{Y}$.
- We generate tow random matrices $\boldsymbol{V}$ of length $\boldsymbol{M} \times 2$ and $\boldsymbol{G}$ of length $(\boldsymbol{N}+1) \times 2$ by using the equation (2.11) with the initial values $(\boldsymbol{x}_{0.3}, \boldsymbol{\rho}_{0.3}, \boldsymbol{\alpha}_{0.3})$, $(\boldsymbol{x}_{0.4}, \boldsymbol{\rho}_{0.4}, \boldsymbol{\alpha}_{0.4})$ respectively.
- The aim of these two matrix is to determine the scan and permutation direction. **When** $\boldsymbol{V}(\boldsymbol{I}(\boldsymbol{i}), 1) > \boldsymbol{V}(\boldsymbol{I}(\boldsymbol{i}), 2)$ the row $\boldsymbol{I}(\boldsymbol{i})$ of the image $\boldsymbol{O}$ is flipped from the left to right. **Otherwise**, the row $\boldsymbol{I}(\boldsymbol{i})$ of the image $\boldsymbol{O}$ is flipped from the right to left finally we get the permuted image $\boldsymbol{P}$.

Step 4 We generate two different chaotic sequence $\boldsymbol{S} = \{\boldsymbol{S}_1, \boldsymbol{S}_2 \ldots \ldots \ldots \ldots \boldsymbol{S}_{SW}\}$, $\boldsymbol{Z} = \{\boldsymbol{Z}_1, \boldsymbol{Z}_2 \ldots \ldots \ldots \ldots \boldsymbol{Z}_{ZH}\}$ of size $\boldsymbol{M} \times \boldsymbol{N} \times 3$ by using the equation (2.11) with initial values $(\boldsymbol{x}_{0.5}, \boldsymbol{\rho}_{0.5}, \boldsymbol{\alpha}_{0.5})$, $(\boldsymbol{x}_{0.6}, \boldsymbol{\rho}_{0.6}, \boldsymbol{\alpha}_{0.6})$ respectively. Then S and Z are transformed into integer by using the following function:

$$key1(i) = floor\left(S(i) \times 10^{15}\right) \bmod 256. \tag{3.1}$$

$$key2(i) = floor\left(Z(i) \times 10^{15}\right) \bmod 256. \tag{3.2}$$

where the floor function approximates the value of X to integers.

Step 5 The cipher image C is obtained from the scrambling image $\boldsymbol{P}$ and the key1 using the following equations:

$$\begin{cases} \boldsymbol{c}(\boldsymbol{i},\boldsymbol{j}) = \boldsymbol{p}(\boldsymbol{i},\boldsymbol{j}) \oplus \boldsymbol{key1}(\boldsymbol{i}) \ \boldsymbol{if} \ \ (\boldsymbol{i} = \boldsymbol{1} \ \boldsymbol{and} \ \boldsymbol{j} = \boldsymbol{1}) \\ \boldsymbol{c}(\boldsymbol{i},\boldsymbol{j}) = \left(\boldsymbol{p}(\boldsymbol{i},\boldsymbol{j}) \oplus \boldsymbol{key1}(j)\right) \oplus \boldsymbol{c}(\boldsymbol{i}-\boldsymbol{1},\boldsymbol{n}) \ \boldsymbol{elsif} \ \ (\boldsymbol{i} \neq \boldsymbol{1} \ and \ \boldsymbol{j} = \boldsymbol{1}) \\ \boldsymbol{c}(\boldsymbol{i},\boldsymbol{j}) = \left(\boldsymbol{p}(\boldsymbol{i},\boldsymbol{j}) \oplus key1(\boldsymbol{i})\right) \oplus \boldsymbol{c}(\boldsymbol{i},\boldsymbol{j}-\boldsymbol{1}) \ \boldsymbol{otherwise} \end{cases} \tag{3.4}$$

where $\oplus$ is the XOR operator.

Algorithm 2 describes the proposed scheme diffusion process. We use the key2 in the second round.

Figure 3 Block diagram of the proposed encryption algorithm (see online version for colours)

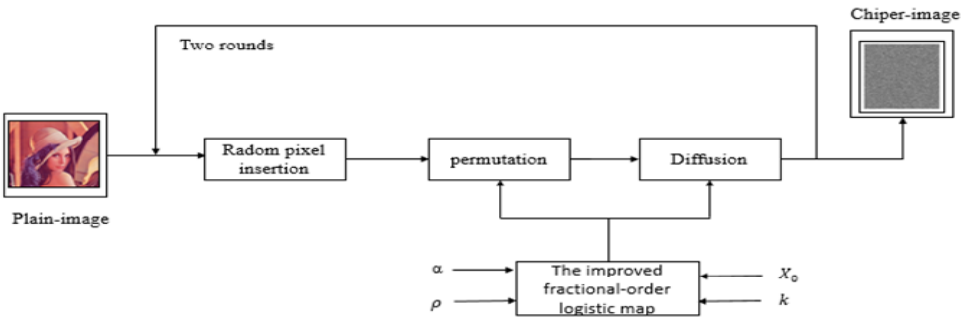


Figure 4 An example of creating chaotic sequences (a) creating two index J and I (b) creating two matrices V and G (see online version for colours)

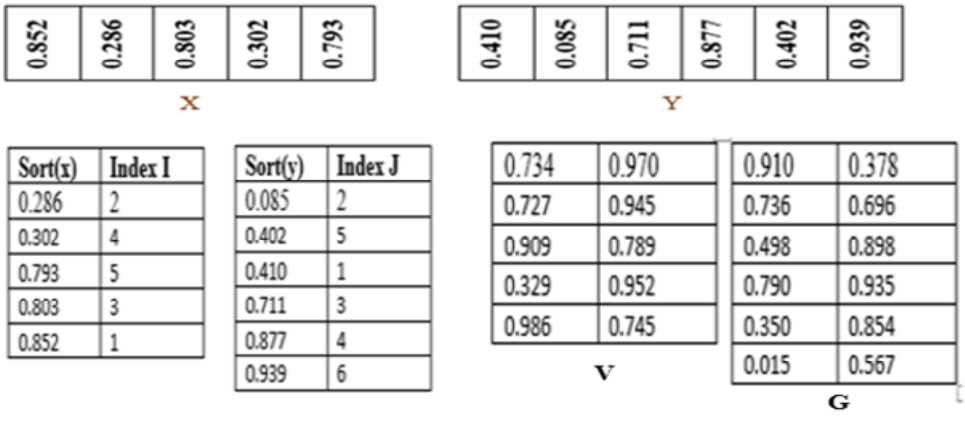
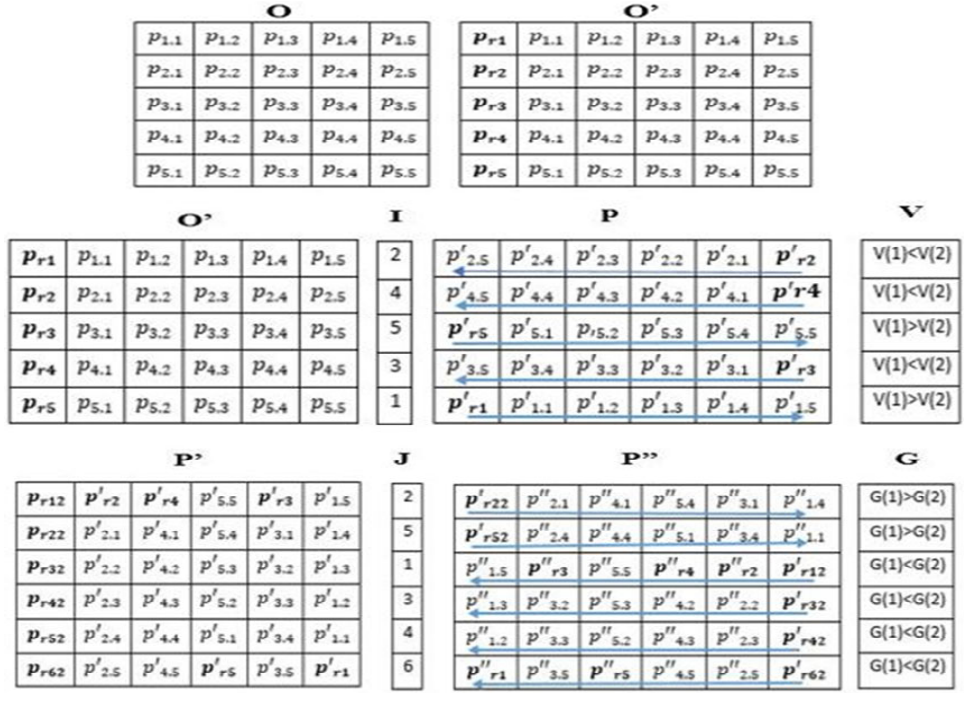


Figure 5 Permutation and diffusion process (a) inserting random pixels into each line of the plain image O (b) permutation and diffusion to P using I (c) rotate the image 90 degrees counterclockwise with random pixel insertion (p') to start the second encryption round (d) permutation and diffusion to P" using J (see online version for colours)



We will present an example with an image of size 5 × 5 to understand how the proposed algorithm works. The numerical example is shown in Figure 4 and Figure 5. As shown in Figure 4 and 5:

- Two random sequences X and Y of size M, $N + 1$ respectively were generated.
- We arrange ascending sequences to get two index J and I.
- We generate two random matrices V and G of size $M \times 2$ and $(N + 1) \times 2$ respectively, where V and I are used in permutation in the first round and G, J are used for the second round.
- We insert random pixels (p_{r1}, p_{r2}, p_{r3}, p_{r4}, p_{r5}) in the beginning of each row of the original image O.
- We use I and V to permute the image where we flip the rows depending on I. For example, the row of image P is replaced by the second row of the original image O where if $V(I(i), 1) > V(I(i), 2)$ the row is switched from the left to right. Otherwise, the row is flipped from the right to left and so on.
- We diffuse by using algorithm 2 to get the encrypted image p for the first round.
- In the second round, we rotate the image p by 90 degrees, and we insert random pixels (p_{r12}, p_{r22}, p_{r32}, p_{r42}, p_{r52}, p_{r52}) at the beginning of each line. We get the image P'.
- We use J and G to permute the image P' and diffuse through the algorithm 2 to get the encrypted image p''.
- The encrypted image size is $(M + 1) \times (N + 1)$ due to the entry of pixels at the beginning of each row of the original image

We reverse the steps of the encryption method to decrypt the image, using the same key.

Algorithm 1 Permutation

```
Input: V, G, I, J, O'
Output: scrambling image p''
k ← M
for l ← 1 to 3 do
    for i ← 1 to M do
        if V(I(i), 1) ≥ V(I(i),2) then //
            for j ← 1 to N do
                by using the following, switch the row I(i) from left to right
                    p(I(i), j(l)) ← O'(i, j, l)
            End
        Else
            for j ← 1 to N do
                by using the following, switch the row I(i) from right to left:
                    p(I(i), K(l)) ← O'(i, j, l)
                    k ← k–1;
            End
        End
```

$k \leftarrow M$
End
The second round of permutation
$p' \leftarrow rot90(p)$
Add a random pixel at the beginning of each row to the image p'
$k \leftarrow N$
for $l \leftarrow 1$ ***to*** 3 ***do***
  for $i \leftarrow 1$ ***to*** M ***do***
    if $G(J(i), 1) \geq G(J(i), 2)$ ***then*** //
      for $j \leftarrow 1$ ***to*** N ***do***
        switch the row J(i) from left to right by using the following:
        $p''(J(i), j(l)) \leftarrow p'(i, j, l)$
      End
    Else
      for $j \leftarrow 1$ ***to*** N ***do***
        switch the row J(i) from right to left by using the following:
        $p''(J(i), j(l)) \leftarrow p'(i, j, l)$
        $k \leftarrow k–1;$
      End
    End
  $k \leftarrow N$
End

Algorithm 2 Diffusion

Input: scrambling image p''; *Secret keys:* $x_{0.5}$, $\rho_{0.5}$, $\alpha_{0.5}$, $x_{0.6}$, $\rho_{0.6}$, $\alpha_{0.6}$

Output: encrypted image: C

Use secret keys to get the chaotic sequence S and Z of size $M \times N \times 3$ *then S and Z are transformed into integer by using the following function:*

key1(i) = floor(S(i) $\times 10^{15}$*) mod 256, key2(i) = floor(Z(i)* $\times 10^{15}$*) mod 256*

Read permuted image p''

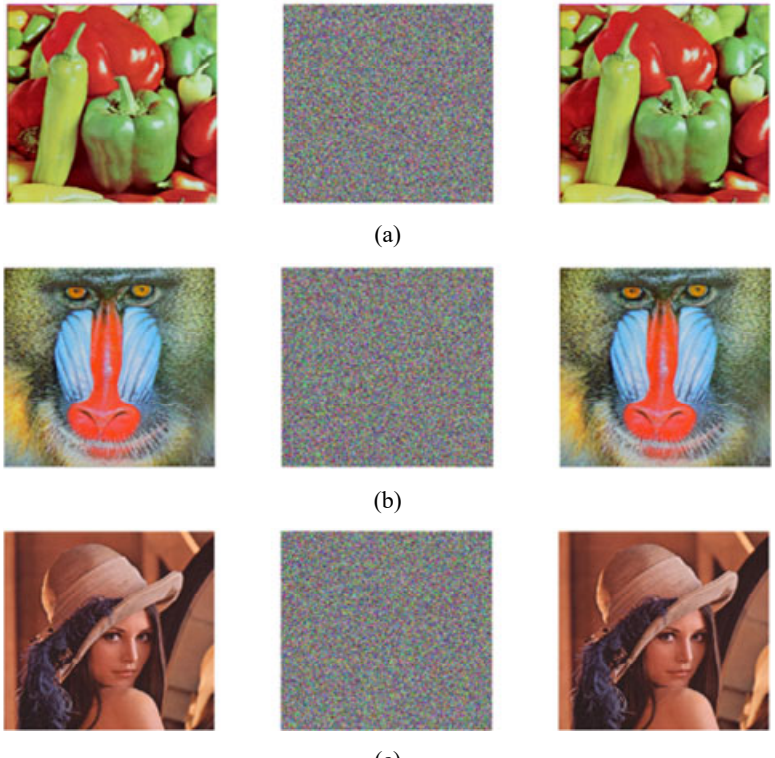
for $l \leftarrow 1$ ***to*** 3 ***do***
  for $i \leftarrow 1$ ***to*** M ***do***
    for $j \leftarrow 1$ ***to*** N ***do***
      if $(i = 1$ *and* $j = 1)$ ***then*** //
        $c(i, j, l) = p''(i, j, l) \oplus key1$
      Elsif $(i \neq 1$ *and* $j = 1)$ ***then*** //
        $c(i, j, l) = (p''(i, j, l) \oplus key1) \oplus c(i - 1, n, l)$
      Else
        $c(i, j, l) = (p''(i, j, l) \oplus key1) \oplus c(i, j - 1, l)$

End
End
End
End

4 Simulation results

In this section, three image data of size 512 × 512 × 3 will be used as input for evaluating the performance of the suggested algorithm. In addition, it will be compared to other algorithms in the literature to clarify the effectiveness of this algorithm. Figure 6 depicts the outcome of the image encryption and decryption process.

Figure 6 Encryption and decryption results (a) peppers (b) baboon (c) Lena (see online version for colours)



(a)

(b)

(c)

Notes: The second and the third column show the encrypted and decrypted images.

All tests and experiments were done on a Matlab (R2015a) software and 2.7 GHz I7 CPU with 8 GB memory.

4.1 Key space analysis

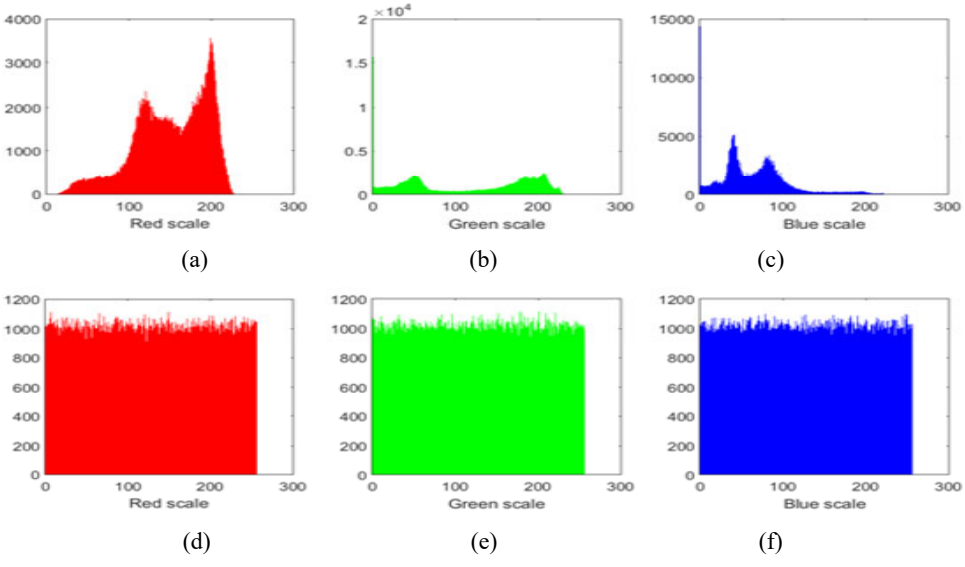
A Good cryptographic algorithm should have a wide key space in order to enhance their resistance to brute force attack. As it is known, the key space must be greater than 2^{100} (Seyedzadeh et al., 2015; Yang and Liao, 2018; Chen et al., 2020).

As we mentioned earlier, the security keys of our algorithm includes 18 parameters, such as 6 control parameters $\rho_{0.1}$, $\rho_{0.2}$, $\rho_{0.3}$, $\rho_{0.4}$, $\rho_{0.5}$, $\rho_{0.6}$, 6 fractional-order parameters $\alpha_{0.1}$, $\alpha_{0.2}$, $\alpha_{0.3}$, $\alpha_{0.4}$, $\alpha_{0.5}$, $\alpha_{0.6}$ and 6 initial values $x_{0.1}$, $x_{0.2}$, $x_{0.3}$, $x_{0.4}$, $x_{0.5}$, $x_{0.6}$. The precision of every initial value is 10^{14}, so the key space size of our algorithm is $10^{18\times14} = 10^{252} = 2^{837}$. As a result, our algorithm key space is wide enough to withstand brute force attacks.

4.2 Histogram analysis

For studying the effectiveness of encryption algorithms against statistical attacks, we use histogram that represents the image pixel value distribution. In which the cipher image must have a flat histogram (Li et al., 2015). Figure 7 shows the histograms of the pepper image and its cipher image. From Figure 7, it can be seen that the histogram of the cipher image looks uniform and completely different from the original image. This means that our scheme prevents the attacker from collecting any statistical data and thus prevents him from carrying out statistical attacks.

Figure 7 Histogram of peppers image and encrypted image (a)–(c) histogram of R, G, B components of original image (d)–(f) histogram of R, G, B components of encrypted image (see online version for colours)



4.3 Information entropy analysis

Information entropy is an important indicator in measuring randomness and unpredictability (Cao et al., 2018). The entropy equation is presented as follows:

$$H(m) = -\sum_{i=0}^{2^n} p(m_i)\log_2\left(p(m_i)\right) \tag{4.1}$$

where m denotes the information source, n denotes the bit number needed for the symbol m_i, and $p(m_i)$ denotes the probability of symbol m_i.

The ideal entropy value is near to 8. Table 2 shows the entropy values of the various encrypted image. Through the results of the table, the entropy values of the various images encrypted by our algorithms are near to eight. Our algorithm also provides better results compared to those obtained in Liu et al. (2020), Li et al. (2017) and Yang and Liao (2018).

Table 2 Entropy analysis of peppers, baboon and Lena

Image	*Plain image*	*Our method*	*Liu et al. (2020)*	*Li et al. (2017)*	*Yang and Liao (2018)*
Peppers	7.6698	7.9998	7.9971	7.9994	7.9984
Baboon	7.7624	7.9997	7.9967	/	7.9989
Lena	7.4767	7.9998	7.9972	7.9971	7.9997

4.4 Correlation coefficient

Correlation analysis is an important index for studying the quality of image encryption algorithms. It is well known that image pixels are characterised by their strong correlation with each other on the horizontal, vertical and diagonal levels. Therefore, good encryption scheme algorithms are required to break this link between pixels (Hu and Li, 2021). Correlation coefficient is given by:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{4.2}$$

$$\operatorname{cov}(x) = E\left(\left[x - E(x)\right]\left[y - E(y)\right]\right), \tag{4.3}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4.4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]^2 \tag{4.5}$$

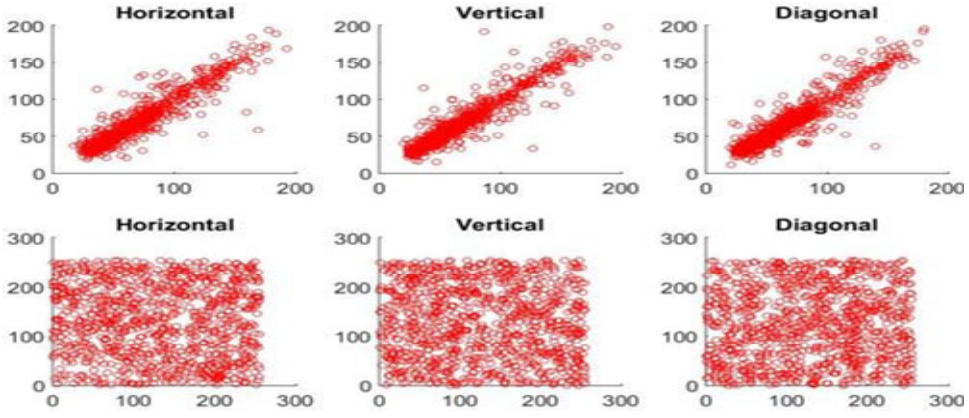
where N is the total number of pixels, $E(x)$, $E(y)$ are the means of pixel x_i and y_i, respectively. Table 3 displays the results of the correlation coefficient of the Lena cipher image of our algorithm compared to other algorithms found in the literature. As shown, the correlation values for the original image are close to 1 in all directions while the correlation in the cipher image is nearly zero.

Table 3 Correlation coefficient in the cipher and original Lena and compare with different algorithms

Channels	*Direction*	*Original Lena image*	*Our algorithm*	*Li et al. (2019)*	*Chen et al. (2020)*
R channel	Horizontal	0.9556	0.0026	–0.0025	0.0001
	Vertical	0.9780	–0.0002	0.0913	0.0091
	Diagonal	0.9434	–0.0005	0.0011	–0.0023
G channel	Horizontal	0.9443	–0.0023	0.0058	−0.0025
	Vertical	0.9711	0.0008	–0.0372	−0.0061
	Diagonal	0.9301	–0.0016	–0.0014	0.0058
B channel	Horizontal	0.9280	0.0007	–0.0058	−0.0074
	Vertical	0.9575	–0.0017	0.0036	−0.0059
	Diagonal	0.9030	0.0003	2.1180e–04	0.0015

The results obtained through our algorithms are much better than those mentioned in (Chen et al., 2020; Li et al., 2019). So, our algorithms are able to break the correlation between pixels, which is shown in Figure 8. Therefore, our scheme is able to block statistical attacks.

Figure 8 Neighbouring pixel distribution in different directions of Lena (see online version for colours)



Notes: The first row shows the original image; the second row shows the encrypted image.

4.5 Differential attack analysis

In cryptography, two percentage (NPCR) the number of pixel change rate and (UACI) unified average changing intensity, are usually used to measure the sensitivity of the slight change in the original image and what results when encrypted. Therefore, these two percentages are of great importance in determining the effectiveness of the suggested scheme facing differential attacks (Wang et al., 2020).The following formulas are used to measure NPCR and UACI:

$$NPCR = \frac{1}{L}\sum_{i,j} D(i,j)\times 100\% \tag{4.6}$$

$$UACI = \frac{1}{L}\sum_{i,j} \frac{|c(i,j)c_1(i,j)|}{255}\times 100\% \tag{4.7}$$

where L is the total number of pixels, C and C_1 are pixel value before and after the same modification, respectively. The rules for determining $D(i, j)$ are as follows: If $c(I, j) \neq c_1(i, j)$ then $d(i, j) = 1$, otherwise $d(i, j) = 0$.

The optimum value mentioned in the literature for *NPCR* and *UACI* are 99.6094% and 33.4635% respectively (Zhan et al., 2017). We have changed a single pixel of the original images to get NPCR and UACI values. The results obtained are shown in Table 4. The NPCR and UACI values of our algorithm are very nearly to the ideal values compared to the methods mentioned in Liu et al. (2020), Li et al. (2017) and Yang and Liao (2018). Thus, the suggested algorithm is very effective against differential attacks.

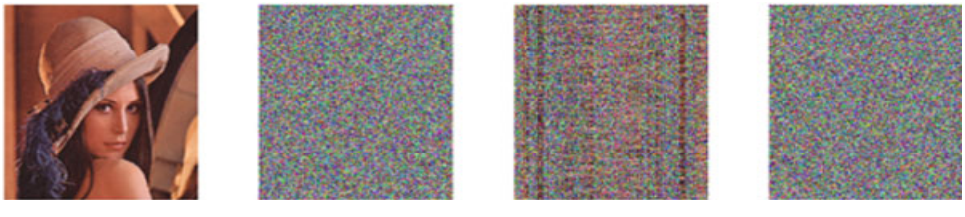
Table 4 NPCR and UACI of peppers, baboon and Lena with just one pixel adjustment

Images	*NPCR (%)*			*UACI (%)*		
	Peppers	*Baboon*	*Lena*	*Peppers*	*Baboon*	*Lena*
Proposed	99.60	99.61	99.61	33.46	33.47	33.49
Liu et al. (2020)	/	99.636	99.6216	/	33.4702	33.4994
Li et al. (2017)	99.5845	/	99.5723	33.2703	/	33.3159
Yang and Liao (2018)	99.61	99.62	99.61	31.03	33.46	32.23

4.6 Key sensitivity analysis

Extreme key sensitivity is necessary for any encryption algorithm, as once the key is changed by a very small amount, it will result in a massive failure to decrypt and get an entirely different cipher image. It means that if the secret key is changed, the decryption result will be entirely different. To see the impact of our key sensitivity, we changed the value of each key by 10^{-14}, the obtained results are shown in Figure 9. As we can see, once the key changes by a small percentage (10^{-14}), we get a different image compared to the one that is decrypted with the right key.

Figure 9 The key sensitivity test of the decrypted image (a) with correct key (b) with fractional-order $\alpha_{0.1} + 10^{-14}$ (c) with wrong $x_{0.1} + 10^{-14}$ (d) with wrong $\alpha_{0.6} + 10^{-14}$ (see online version for colours)



(a) (b) (c) (d)

4.7 Data loss and noise attacks

When transmitting the cipher image across the network, it can be dispersed by phenomena such as data loss and noise. For this purpose, the noise attack and data loss are used to determine the quality of the encryption algorithm in preventing these attacks. We added salt and pepper noise of level 1%, 5% and 10% to the encrypted Lena image for performing an anti-noise test.

The obtained results are shown in Figure 10; we have also cropped the encrypted image in different sizes, which is shown in Figure 11. Through Figures 10 and 11, and despite the noise and data loss, the decipher image contains the majority of the original image information, which shows that our algorithms are effective against noise attacks and data loss.

Figure 10 Decryption process with salt and pepper nose (see online version for colours)

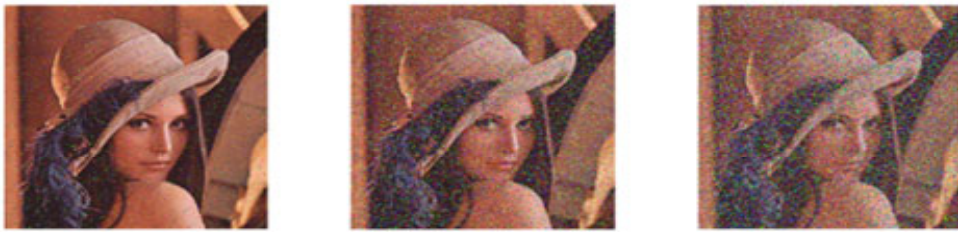
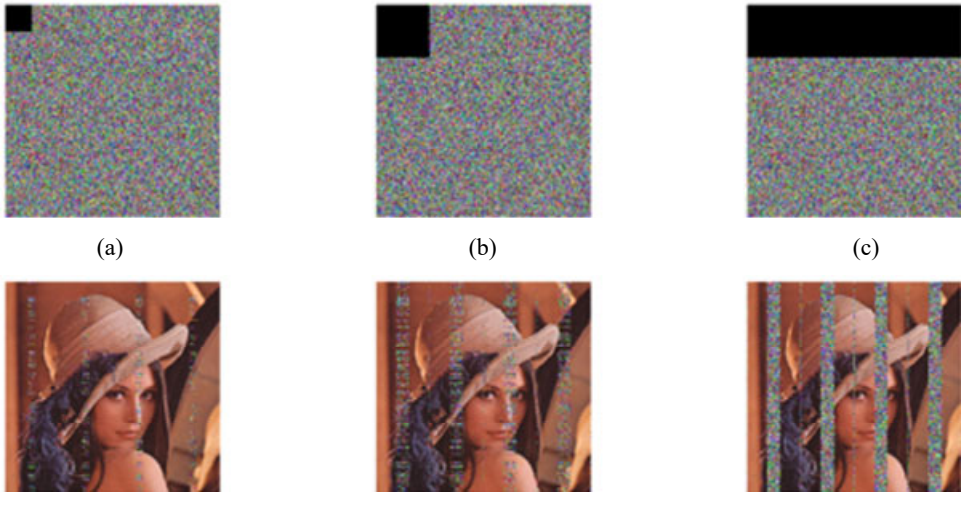


Figure 11 Data loss attack analysis results (a) 64 × 64 data loss (b) 128 × 128 data loss (c) 128 × 513 data loss (d) decipher image of (a) (e) decipher image of (b) (f) decipher image of (c) (see online version for colours)



4.8 Speed analysis

In terms of cryptography, a good encryption scheme must be characterised by high operating speed. We used the Matlab R2015a environment with an Intel I7-7500U CPU with @ 2.7 GHZ and 8 GB RAM on Windows 10 to run our algorithm. Table 5 shows the results of the encryption speed test. As can be shown, our scheme is faster than the other algorithms in Huang et al. (2019) and Wu et al. 2017 so it is reliable for real applications.

Table 5 Speed analysis

Image	*Proposed scheme*	*Huang et al. (2019)*	*Wu et al. 2017*
512 × 512	2.32 s	3.5145 s	3.76s

5 Conclusions

In this paper, we proposed new image encryption algorithms using an improved fractional-order logistics map, where this map has better features than the classic fractional logistic map, including a larger key space, a wider range, a uniform data distribution and more parameters. Which is confirmed by the analysis of the bifurcation diagram and the Lyapunov exponent.

The results of performance simulations and analyses proved that our algorithm possesses excellent properties, including a large key space in addition to the sensitivity to small key changes and a low correlation compared to previous algorithms. It also provides better protection against hacker attacks such as statistical and differential attacks.

References

Akbergenov, A.A. and Pelyukh, H.P. (2016) 'Continuous solutions of systems of nonlinear difference equations', *J. Math. Sci.*, United States, Vol. 215, No. 3, pp.267–273, doi: 10.1007/s10958-016-2836-8.

Cao, C., Sun, K. and Liu, W. (2018) 'A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map', *Signal Processing*, Vol. 143, No. 2, pp.122–133, doi: 10.1016/j.sigpro.2017.08.020.

Chen, G., Mao, Y. and Chui, C.K. (2004) 'A symmetric image encryption scheme based on 3D chaotic cat maps', *Chaos, Solitons and Fractals*, Vol. 21, No. 3, pp.749–761, doi: 10.1016/j.chaos.2003.12.022.

Chen, L.P., Yin, H., Yuan, L.G., Lopes, A.M., Machado, J.A.T. and Wu, R.C. (2020) 'A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations', *Front. Inf. Technol. Electron. Eng.*, Vol. 21, No. 6, pp.866–879, doi: 10.1631/FITEE.1900709.

El Raheem, Z.F. and Salman, S.M. (2014) 'On a discretization process of fractional-order Logistic differential equation', *J. Egypt. Math. Soc.*, Vol. 22, No. 3, pp.407–412, doi: 10.1016/j.joems.2013.09.001.

El-Sayed, A.M.A. and Salman, S.M. (2013) 'On a discretization process of fractional order Riccati differential equation', *J. Fract. Calc. Appl.*, Vol. 4, No. 2, pp.251–259, 2013.

Enayatifar, R., Abdullah, A.H. and Isnin, I.F. (2014) 'Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence', *Opt. Lasers Eng.*, Vol. 56, No. 5, pp.83–93, doi: 10.1016/j.optlaseng.2013.12.003.

Enayatifar, R., Abdullah, A.H., Isnin, I.F., Altameem, A. and Lee, M. (2017) 'Image encryption using a synchronous permutation-diffusion technique', *Opt. Lasers Eng.*, October, Vol. 90, pp.146–154, doi: 10.1016/j.optlaseng.2016.10.006.

Herbadji, D. et al. (2019c) 'A new image encryption scheme using an enhanced logistic map', *Proc. 2018 Int. Conf. Appl. Smart Syst. ICASS 2018*, November, pp.24–25, doi: 10.1109/ICASS.2018.8652065.

Herbadji, D., Belmeguenai, A., Derouiche, N. and Liu, H. (2020b) 'Colour image encryption scheme based on enhanced quadratic chaotic map', *IET Image Process.*, Vol. 14, No. 1, pp.40–52, doi: 10.1049/iet-ipr.2019.0123.

Herbadji, D., Belmeguenai, A., Derouiche, N., Zennir, Y. and Ouchtati, S. (2019b) 'A novel color image encryption scheme using logistic map and quadratic map systems', *4th Inernational conference on Mobile,Secure and Programable Networking*, Vol. 11005 LNCS, Springer International Publishing, Paris, France, doi:10.1007/978-3-030-03101-5_2.

Herbadji, D., Derouiche, N., Belmeguenai, A., Herbadji, A. and Boumerdassi, S. (2019a) 'A tweakable image encryption algorithm using an improved logistic chaotic map', *Trait. du Signal*, Vol. 36, No. 5, pp.407–417, doi: 10.18280/ts.360505.

Herbadji, D., Derouiche, N., Belmeguenai, A., Tahat, N. and Boumerdassi, S. (2020a) 'A new colour image encryption approach using a combination of two 1D chaotic map', *Int. J. Electron. Secur. Digit. Forensics*, Vol. 12, No. 4, pp.337–356, doi: 10.1504/IJESDF.2020.110649.

Hu, G. and Li, B. (2021) 'Coupling chaotic system based on unit transform and its applications in image encryption', *Signal Processing*, Vol. 178, No. 1, p.107790, doi: 10.1016/j.sigpro.2020.107790.

Huang, L., Cai, S., Xiong, X. and Xiao, M. (2019)'On symmetric color image encryption system with permutation-diffusion simultaneous operation', *Opt. Lasers Eng.*, July 2018, Vol. 115, pp.7–20, doi: 10.1016/j.optlaseng.2018.11.015.

Khalil, R., Al Horani, M., Yousef, A. and Sababheh, M. (2014) 'A new definition of fractional derivative', *J. Comput. Appl. Math.*, Vol. 264, No. 1, pp.65–70, doi: 10.1016/j.cam.2014.01.002.

Kumar, D., Singh, J. and Baleanu, D. (2017) 'A hybrid computational approach for Klein-Gordon equations on cantor sets', *Nonlinear Dyn.*, Vol. 87, No. 1, pp.511–517, doi: 10.1007/s11071-016-3057-x.

Li, C., Zhao, Z. and Chen, Y. (2011) 'Numerical approximation of nonlinear fractional differential equations with subdiffusion and superdiffusion', *Comput. Math. with Appl.*, Vol. 62, No. 3, pp.855–875, doi: 10.1016/j.camwa.2011.02.045.

Li, P., Xu, J., Mou, J. and Yang, F. (2019) 'Fractional-order 4D hyperchaotic memristive system and application in color image encryption', *Eurasip J. Image Video Process.*, Vol. 2019, No. 1, pp.1–11, doi: 10.1186/s13640-018-0402-7.

Li, T., Yang, M., Wu, J. and Jing, X. (2017) 'A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA computing', *Complexity*, Vol. 2017, doi: 10.1155/2017/9010251.

Lin, F.R. and Qu, H. (2019) 'A Runge-Kutta Gegenbauer spectral method for nonlinear fractional differential equations with Riesz fractional derivatives', *Int. J. Comput. Math.*, Vol. 96, No. 2, pp.417–435, doi: 10.1080/00207160.2018.1487059.

Liu, L., Lei, Y. and Wang, D. (2020) 'a fast chaotic image encryption scheme with simultaneous permutation-diffusion operation', *IEEE Access*, Vol. 8, No. 8, pp.27361–27374, doi: 10.1109/ACCESS.2020.2971759.

Mani, P., Rajan, R., Shanmugam, L. and Hoon Joo, Y. (2019) 'Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption', *Inf. Sci. (Ny).*, Vol. 491, No. 22, pp.74–89, doi: 10.1016/j.ins.2019.04.007.

Nosrati, K. and Shafiee, M. (2018) 'Fractional-order singular logistic map: stability, bifurcation and chaos analysis', *Chaos, Solitons and Fractals*, Vol. 115, No. 10, pp.224–238, doi: 10.1016/j.chaos.2018.08.023.

Radwan, A.G., Soliman, A.M. and Elwakil, A.S. (2008) 'Design equations for fractional-order sinusoidal oscillators: four practical circuit examples', *Int. J. Circuit Theory Appl.*, Vol. 36, No. 4, pp.473–492, Jun. doi: 10.1002/cta.453.

Ramadan, N., Ahmed, H.E.H., Elkhamy, S.E. and El-samie, F.E.A. (2016) 'Chaos-based image encryption using an improved quadratic chaotic map', *Am. J. Signal Process.*, Vol. 6, No. 1, pp.1–13, doi: 10.5923/j.ajsp.20160601.01.

Ruan, J., Sun, K., Mou, J., He, S. and Zhang, L. (2018) 'Fractional-order simplest memristor-based chaotic circuit with new derivative', *Eur. Phys. J. Plus*, Vol. 133, No. 1, pp.1–12, doi: 10.1140/epjp/i2018-11828-0.

Said, L.A., Radwan, A.G., Madian, A.H. and Soliman, A.M. (2016) 'Fractional order oscillator design based on two-port network', *Circuits, Syst. Signal Process.*, Vol. 35, No. 9, pp.3086–3112, doi: 10.1007/s00034-015-0200-8.

Seyedzadeh, S.M., Norouzi, B., Mosavi, M.R. and Mirzakuchaki, S. (2015) 'A novel color image encryption algorithm based on spatial permutation and quantum chaotic map', *Nonlinear Dyn.*, Vol. 81, Nos. 1–2, pp.511–529, doi: 10.1007/s11071-015-2008-2.

Shamim, A., Radwan, A.G. and Salama, K.N. (2011) 'Fractional smith chart theory', *IEEE Microw. Wirel. Components Lett.*, Vol. 21, No. 3, pp.117–119, doi: 10.1109/LMWC.2010.2098861.

Shammakh, W.M. and El-Shahed, M. (2011) 'Existence of positive solutions for m-point boundary value problem for nonlinear fractional differential equation', *Abstr. Appl. Anal.*, Vol. 2011, pp.1–20, doi: 10.1155/2011/986575.

Singh, J., Kumar, D. and Nieto, J.J. (2017) 'Analysis of an El Nino-Southern oscillation model with a new fractional derivative', *Chaos, Solitons and Fractals*, Vol. 99, No. 6, pp.109–115, doi: 10.1016/j.chaos.2017.03.058.

Srivastava, H.M., Kumar, D. and Singh, J. (2017) 'An efficient analytical technique for fractional model of vibration equation', *Appl. Math. Model.*, Vol. 45, No. 5, pp.192–204, doi: 10.1016/j.apm.2016.12.008.

Suri, S. and Vijay, R. (2019) 'A bi-objective genetic algorithm optimization of chaos-DNA based hybrid approach', *J. Intell. Syst.*, Vol. 28, No. 2, pp.333–346, doi: 10.1515/jisys-2017-0069.

Tarasov, V.E. (2015) 'Lattice fractional calculus', *Appl. Math. Comput.*, Vol. 257, No. 8, pp.12–33, doi: 10.1016/j.amc.2014.11.033.

Using, M., Pi, F., Control, D., Dumlu, A. and Erenturk, K. (2014) 'Trajectory tracking control for a 3-DOF parallel', *IEE Transactions on industrial Electronics*, Vol. 61, No. 7, pp.3417–3426, DOI: 10.1109/TIE.2013.2278964.

Wang, X., Xue, W. and An, J. (2020) 'Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household', *Chaos, Solitons and Fractals*, Vol. 141, No. 12, p.110309, doi: 10.1016/j.chaos.2020.110309.

Wu, J., Liao, X. and Yang, B. (2017) 'Color image encryption based on chaotic systems and elliptic curve ElGamal scheme', *Signal Processing*, Vol. 141, No. 12, pp.109–124, doi: 10.1016/j.sigpro.2017.04.006.

Wu, X., Kan, H. and Kurths, J. (2015) 'A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps', *Appl. Soft Comput. J.*, Vol. 37, No. 12, pp.24–39, doi: 10.1016/j.asoc.2015.08.008.

Wu, X., Li, Y. and Kurths, J. (2015) 'A new color image encryption scheme using CML and a fractional-order chaotic system', *PLoS One*, Vol. 10, No. 3, pp.1–28, doi: 10.1371/journal.pone.0119660.

Wu, X., Zhu, B., Hu, Y. and Ran, Y. (2017) 'A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps', *IEEE Access*, Vol. 5, No. 5, pp.6429–6436, doi: 10.1109/ACCESS.2017.2692043.

Xu, L., Gou, X., Li, Z. and Li, J. (2016b) 'A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion', *Opt. Lasers Eng.*, October, Vol. 91, pp.41–52, doi: 10.1016/j.optlaseng.2016.10.012.

Xu, L., Li, Z., Li, J. and Hua, W. (2016a) 'A novel bit-level image encryption algorithm based on chaotic maps', *Opt. Lasers Eng.*, Vol. 78, No. 3, pp.17–25, doi: 10.1016/j.optlaseng.2015.09.007.

Xu, Y., Wang, H., Li, Y. and Pei, B. (2014) 'Image encryption based on synchronization of fractional chaotic systems', *Commun. Nonlinear Sci. Numer. Simul.*, Vol. 19, No. 10, pp.3735–3744, doi: 10.1016/j.cnsns.2014.02.029.

Yang, B. and Liao, X. (2018) 'A new color image encryption scheme based on logistic map over the finite field ZN', *Multimed. Tools Appl.*, Vol. 77, No. 16, pp.21803–21821, doi: 10.1007/s11042-017-5590-0.

Yang, F., Mou, J., Liu, J., Ma, C. and Yan, H. (2020) 'Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application', *Signal Processing*, Vol. 169, No. 4, p.107373, doi: 10.1016/j.sigpro.2019.107373.

Zhan, K., Wei, D., Shi, J. and Yu, J. (2017) 'Cross-utilizing hyperchaotic and DNA sequences for image encryption', *J. Electron. Imaging*, Vol. 26, No. 1, p.013021, doi: 10.1117/1.jei.26.1.013021.

Zhang, Y.Q., Hao, J.L. and Wang, X.Y. (2020) 'An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map', *IEEE Access*, Vol. 8, No. 8, pp.54175–54188, doi: 10.1109/ACCESS.2020.2979827.

Zhao, J., Wang, S., Chang, Y. and Li, X. (2015) 'A novel image encryption scheme based on an improper fractional-order chaotic system', *Nonlinear Dyn.*, Vol. 80, No. 4, pp.1721–1729, doi: 10.1007/s11071-015-1911-x.

Zhou, N., Pan, S., Cheng, S. and Zhou, Z. (2016) 'Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing', *Opt. Laser Technol.*, Vol. 82, No. 8, pp.121–133, doi: 10.1016/j.optlastec.2016.02.018.

Zhu, Z.L., Zhang, W., Wong, K.W. and Yu, H. (2011) 'A chaos-based symmetric image encryption scheme using a bit-level permutation', *Inf. Sci. (Ny).*, Vol. 181, No. 6, pp.1171–1186, doi: 10.1016/j.ins.2010.11.009.