Image Encryption Using Fractional Order Linear-Nonlinear Chaos

Gao Feng

Key Laboratory for Underwater Test and Control Technology, Dalian 116013, China

E-mail: gaofeng798113@sina.com

Abstract. A fractional order chaos system is first designed. It is a linear-nonlinear hybrid using fractional order logistic map. The fractional order chaos system is closer to the real nature phenomena and has better cryptography features than the integer order chaotic systems in dynamics, such as larger range of key space and almost no periodic windows in bifurcation diagrams. Then, we propose an image encryption scheme employing the superior chaotic features of the fractional order chaos system. Which chaotic sequences generated are used for permutation and addition/subtraction operation of encryption depends on the plaintext image. Security analysis and test results indicate that our encryption scheme has a high efficiency and superior security.

1. Introduction

It is very necessary to protect the confidentiality and security of digital images on unsecured channels, because digital image is usually spread through the Internet and stored in a variety of platforms. Traditional encryption algorithms have been developed for encrypting text data, such as IDEA and AES [1]. And it was claimed that they may not apply to encrypt the image in some cases [2, 3], because the image is high redundant and its adjacent pixels are high correlative. However, chaotic systems have many superior characteristics of meet the needs of the image encryption, such as pseudo-randomness, sensitivity to initial conditions and ergodicity.

Plenty of encryption algorithms in recent years were based on the spatial chaotic systems [4-14], because their high dimensional feature and lots of chaotic sequences can increase the security of cryptosystems. Many encryption scheme using adjacent coupled map lattices (CML) [4-12] were proposed and obtained good results. Zhang [13] designed an image encryption scheme using map lattices coupled in a non-adjacent manner. Then, he developed an image encryption scheme by the use of map lattices coupled in a mixed linear-nonlinear manner [14]. However, the above mentioned chaotic systems all use the integer order logistic mappings. Fractional calculus is more general than integer order calculus because it is an extension of integer order ones. Many fractional dimension phenomena exist in technology and nature [15].

Fractional order chaotic systems have received intensive attentions [16-19] because they have more complex dynamics and is closer to the real nature phenomena than integer order chaotic systems. Some image encryption schemes have used fractional order chaos theory [20-25]. However, the combination of fractional calculus and mixed linear-nonlinear chaotic systems which can describe the real natural phenomena has not been researched. Furthermore, By using chosen plaintext attack, Benyamin [23] cracks an image encryption scheme [24]. The encryption scheme in [24] used an

improper fractional order chaos system and the key stream is independent of either plaintext images or cipher images.

Through the discussions above, we design an encryption scheme employing a fractional order linear-nonlinear chaotic system. Analysis of simulated results attest that our encryption scheme is efficient. The main work are as follows.

- We construct a fractional order linear-nonlinear chaotic system. Its major advantages over other chaotic systems are closer to the real natural phenomena and stronger ergodicity of time series and wider range of key space. Moreover, the range of parameter μ in the chaotic system breaks its limit in the classic logistic map.
- For enhancing the sensitivity of the plaintext images, we use plaintext images to determine which chaotic sequence is used for encrypting image, which can enhance the ability of the resistance to choose plaintext attacks.

In this paper, the rest is organized as follows. The fractional order linear-nonlinear chaos system is introduced in section 2, whose cryptography advantages are also described. The proposed encryption scheme is explained in Section 3. Section 4 analyzes simulated results and security. Finally, Section 5 gives the concluding remarks.

2. The fractional order linear-nonlinear chaos system

Definition 1. The definition of the Caputo fractional derivative [26] is

$$D_t^{\alpha} f(t) = \frac{d^{\alpha} f(t)}{dt^{\alpha}} = \begin{cases} \dfrac{d^n}{dt^n} f(\tau), & (\alpha = m) \\ \dfrac{1}{\Gamma(m-\alpha)} \displaystyle\int_0^t f^m(\tau)(t-\tau)^{m-\alpha-1} d\tau, & (m-1 < \alpha < m) \end{cases} \tag{1}$$

where $\Gamma(\cdot)$ is the Euler's Gamma-function, α is the order, $f(t)$ is a continuous function, m is an integer which is not less than α, and f^m is the mth-order derivative of $f(t)$.

The logistic differential equation of fractional order [27] is given

$$D^{\alpha} x(t) = \mu x(t)(1 - x(t)) \tag{2}$$

where the initial condition $x(0) = x_0$. After discretizing the equation (2) by using piecewise constant r, we can get the equation

$$D^{\alpha} x(t) = \mu x\left(\left[\frac{t}{r}\right] r\right)\left(1 - x\left(\left[\frac{t}{r}\right] r\right)\right) \tag{3}$$

By reasoning the solutions of the equation (3), the discretized logistic differential equation of fractional order [28] is obtained

$$x_{t+1} = x_t + \frac{r^{\alpha}}{\Gamma(1+\alpha)} \mu x_t (1 - x_t) \tag{4}$$

The fractional order linear-nonlinear chaotic system is presented as

$$\begin{aligned} x_{t+1}(n) &= (1-\varepsilon)\{x_t(n) + \xi\mu x_t(n)(1 - x_t(n))\} \\ &+ (1-\eta)\frac{\varepsilon}{2}\{x_t(n+1) + \xi\mu x_t(n+1)(1 - x_t(n+1)) + x_t(n-1) + \xi\mu x_t(n-1)(1 - x_t(n-1))\} \\ &+ \eta\frac{\varepsilon}{2}\{x_t(j) + \xi\mu x_t(j)(1 - x_t(j)) + x_t(k) + \xi\mu x_t(k)(1 - x_t(k))\} \end{aligned} \tag{5}$$

where n, j, k ($1 \le n, j, k \le L$) denote the lattices, t is the time index (t = 1, 2, 3, ...), η and ε are the coupling parameter ($0 \le \eta, \varepsilon \le 1$) and $\xi = \dfrac{r^{\alpha}}{\Gamma(1+\alpha)}$. The lattices n, j, k satisfy the Arnold cat map

$$\begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} n \\ n \end{bmatrix} (\mathrm{mod}\, L) \tag{6}$$

where q and p are the Arnold cat map parameters.

Bifurcation diagrams are analyzed theoretically. Lyapunov exponents are further researched by the Kolmogorov-Sinai entropy universality [20]. All simulations are conducted assuming that L = 100, $\mu \in \left(2\Gamma(1+\alpha)/r^{\alpha}, 3\Gamma(1+\alpha)/r^{\alpha}\right)$, r=0.25, $\varepsilon \in (0,1]$ and $\eta \in [0,1]$.

2.1. Bifurcation Behavior

Figure 1(b)-(f) show the bifurcation diagrams of the proposed chaotic system, and the range of parameter μ is $\left(2\Gamma(1+\alpha)/r^{\alpha}, 3\Gamma(1+\alpha)/r^{\alpha}\right)$. We can find that the range of parameter μ in the CML system [29] (Figure 1(a)) is smaller than those in Figure 1(b)-(f). Moreover, in Figure 1(b)-(f), with the increase of the value of parameter η, the bifurcation point is becoming more and more clear, and the periodic windows have become less and less. Thus, for the proposed chaos system, when the parameter η is assigned a suitable value, there is almost no periodic windows in its bifurcation diagrams. Therefore, in comparison with the CML system, our chaos system is more appropriate for cryptography due to almost no periodic windows.

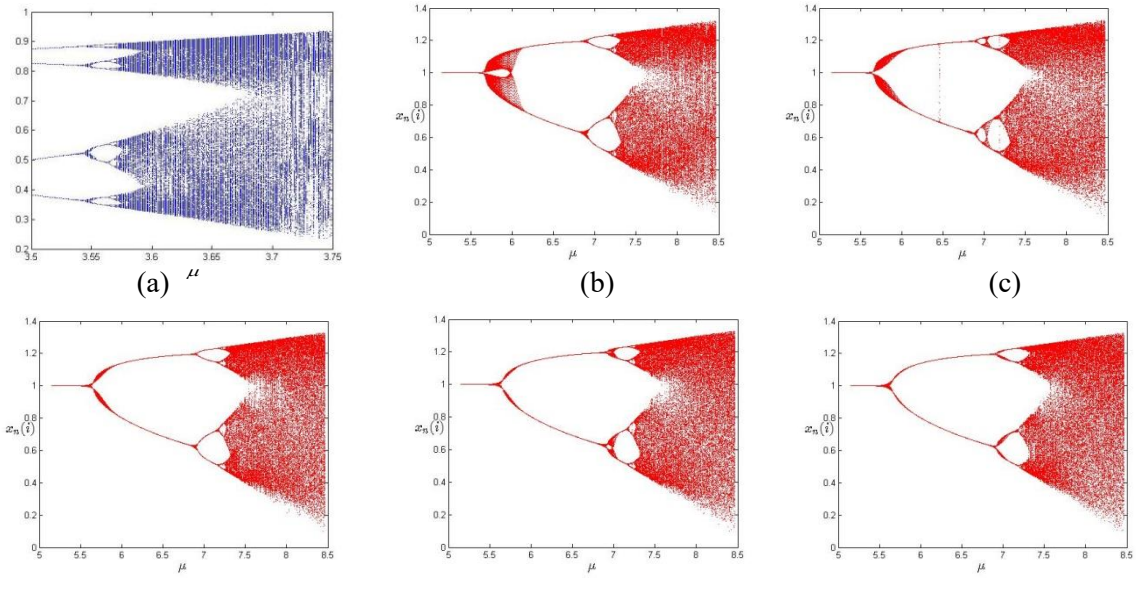


Figure 1. Bifurcation diagrams. (a) the CML system, (b) our chaotic system ($\alpha = 0.8, \eta = 0.4$), (c) our chaotic system ($\alpha = 0.8, \eta = 0.5$), (d) our chaotic system ($\alpha = 0.8, \eta = 0.7$), (e) our chaotic system ($\alpha = 0.8, \eta = 0.8$), (f) our chaotic system ($\alpha = 0.8, \eta = 0.9$).

2.2. Kolmogorov-Sinai entropy universality

At the fewest any chaotic system has one positive Lyapunov exponent. The sum of positive Lyapunov exponents is expressed as the Kolmogorov-Sinai entropy [30]. However, the percentage of the chaotic lattices is expressed as the Kolmogorov-Sinai entropy universality *hu* [19].

From Figure 2, we can find that the spatial chaotic behaviors are different between the proposed chaos system and the CML chaos system. In the proposed chaos system (Figure 2(a)-(e)), its flat area in chaotic behaviors is in $\mu \in (7.2,9]$ and $\varepsilon \in (0,1)$. However, for the CML chaos system (Figure 2(f)), its flat area is only in $\mu \in (3.75,4]$ and $\varepsilon \in (0,1)$. In comparison with the CML chaos system, the proposed chaos system has more parameter pairs of ε and μ, which can cause widespread chaos behaviors. Therefore, the proposed chaos system has a larger range of parameter μ that leads to spatial chaos behaviors than the CML chaos system.

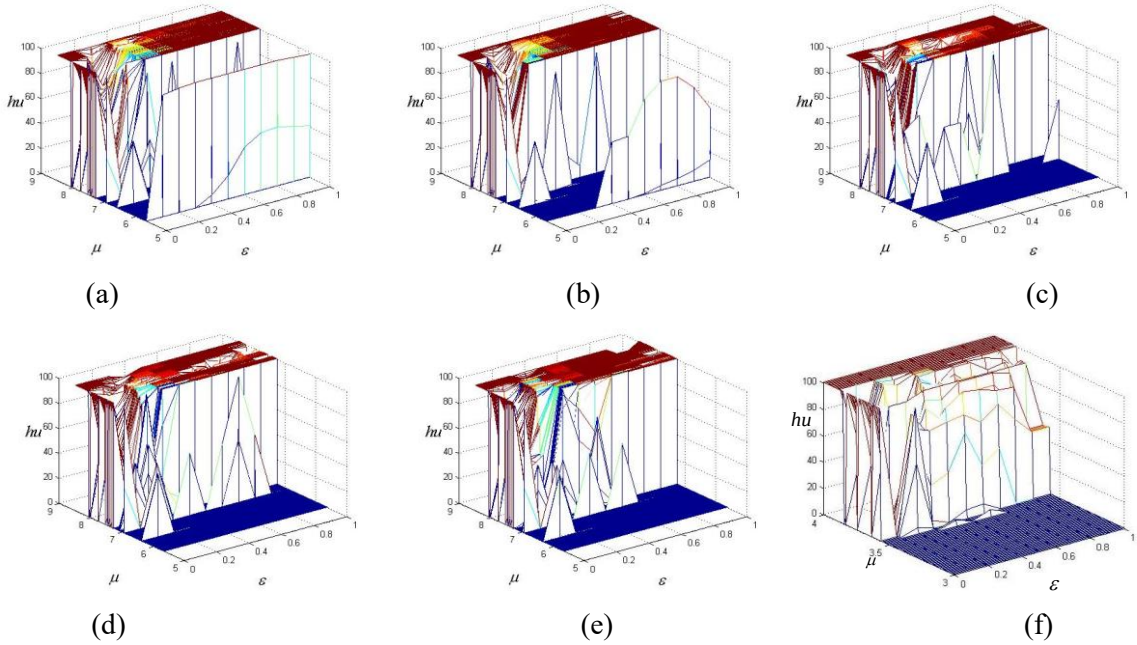


Figure 2. Kolmogorov-Sinai entropy universality. (a) our chaos system ($\eta = 0.4$), (b) our chaos system ($\eta = 0.5$), (c) our chaos system ($\eta = 0.7$), (d) our chaos system ($\eta = 0.8$), (e) our chaos system ($\eta = 0.9$), (f) the CML system.

Our chaos system has a new feature that the range of its parameter μ is wider compared with that of the CML chaos system. The parameter μ is often as a secret key in image encryption, therefore, our chaos system has a larger key space compared with the CML system. Therefore, our chaos system is very appropriate for encrypting image.

3. The proposed image encryption scheme

We design a scheme for encrypting an $M \times N$ gray image. The new chaotic features of our chaos system are used in the permutation, diffusion and nonlinear addition/subtraction phase. For increasing the sensitivity to the plaintext images, we use the sum of plaintext image pixel values to decide which chaotic sequence is used for permutation and addition/subtraction operation.

Input: L=100 and the original image (plaintext image) I. The secret keys μ, ε, η, $x_1(1)$ and α.

Output: The cipher image C.

Step1. Obtain L chaotic sequences by iterating Equation (5) $M \times N$ times.

Step2. Perform diffusion operation and obtain an $M \times N$ matrix D, which is described as

$$D(s) = \mathrm{mod}\{[\mathrm{mod}(\lfloor x_{200+s}(\mathrm{mod}(D(s-1), L)+1) \times 10^{14} \rfloor, 256) + \mathrm{mod}(I(s) + D(s-1), 256)], 256\} \quad (7)$$

where the initial value $D(0) = 0$. Suppose I is a pixel sequence, $I(s)$ is the sth pixel of I.

Step3. Update each value of the *i*th chaotic sequence

$$x_i = \mathrm{mod}(\lfloor x_i \times 10^{14} \rfloor, 256) \tag{8}$$

where $i = \mathrm{mod}(\sum_{l=1}^{M\times N} I(l), L) + 1$. Transform the matrix D and the sequence x_i into $M \times (N \times 4)$ quaternary matrices $D1$ and $D2$, respectively.

Step4. Create a new sequence $y = [x_i, x_{2i}, x_{3i}, x_{4i}]$ and perform the permutation operation

$$\begin{cases} D1(:, j) \leftrightarrow D1(:, \lfloor \mathrm{mod}(y(j), N\times 4 - j) \rfloor + j), \ j \in [1, N\times 4], \\ D1(k,:) \leftrightarrow D1(\lfloor \mathrm{mod}(y(k), M - k) \rfloor + j, :), k \in [1, M]. \end{cases} \tag{9}$$

Step5. Perform nonlinear addition/subtraction operation and obtain an $M \times (N \times 4)$ quaternary matrix $D3$, which is described as

$$D3 = \begin{cases} \mathrm{mod}(D1(k, j) + D2(m, n), 4) & (k + j)/2 = 1 \\ \mathrm{mod}(D1(k, j) - D2(m, n), 4) & (k + j)/2 = 0 \end{cases} \tag{10}$$

where the relationship between m, n and k, j conforms to the Arnold cat map in Equation (6).

Step6. Alter the matrix $D3$ into a decimal matrix C with the size of $M \times N$.

Step7. The value i is assigned to the (M, N)-pixel of C. C is the final cipher image.

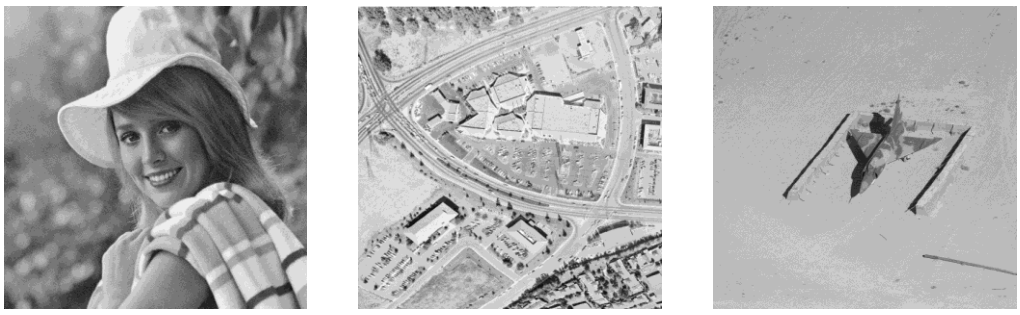
We have finished the encryption process. The decryption operation is its inverse process.

4. Security analysis and simulation results

For next simulation experiments, we employ 3 testing images of USC-SIPI Image Database [31]: Aerial (5.2.09), Airplane (7.1.02) and Elaine. The 3 standard test images are 8-bit monochrome images and have the size of 512×512, as shown in Figure 3. Figure 4 shows encryption and decryption results of Elaine.

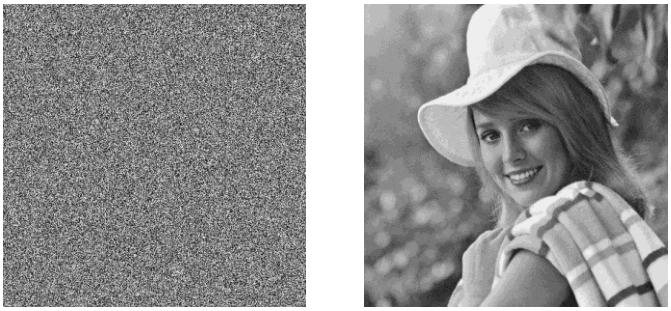
4.1. Statistical analysis

4.1.1. Histogram analysis. We can find the distribution information of the image pixel values from the histogram of the image. The histograms are performed on all original images in Figure 3 and their cipher images. The histogram of the original image of Elaine is indicated in Figure 5(a), and the histogram of the cipher image of Elaine is indicated in Figure 5(b). The results of other 2 test images are similar to that of Elaine. Obviously, the cipher image has a fairly uniform histogram, which resists statistical attacks.



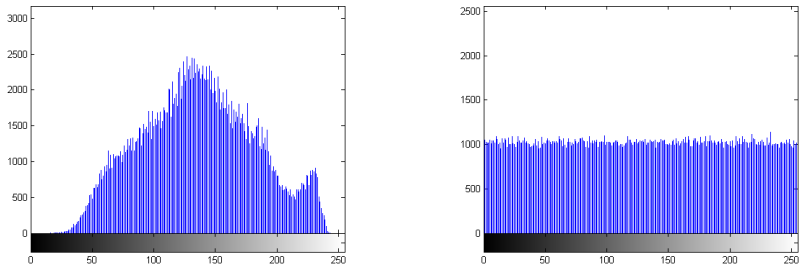
(a) (b) (c)

Figure 3. The 3 test images. (a) Elaine, (b)Aerial, (c) Airplane.



(a) (b)

Figure 4. The encryption and decryption results. (a) cipher image of Elaine, (b) decrypted image of Elaine.



(a) (b)

Figure 5. Histograms for Elaine image. (a) the original image's histogram of Elaine, (b) the cipher image's histogram of Elaine

4.1.2. Correlation coefficient analysis. A good encryption algorithm can decrease the correlation of adjacent pixels, because the adjacent pixels of an ordinary image are highly correlative. For checking the correlative feature of adjacent pixels, 2000 pairs of two adjacent pixels are randomly chosen from the plaintext image and the corresponding cipher image. And we evaluate the correlation coefficients of adjacent pixels in diagonal, vertical and horizontal directions using the equations

$$r_{ij} = \frac{\mathrm{cov}(i, j)}{\sqrt{D(i)}\sqrt{D(j)}} \tag{11}$$

$$E(i) = \frac{1}{T}\sum_{n=1}^{T} i_n \tag{12}$$

$$D(i) = \frac{1}{T}\sum_{n=1}^{T} (i_n - E(i))^2 \tag{13}$$

$$\mathrm{cov}(i, j) = \frac{1}{T}\sum_{n=1}^{T} (i_n - E(i))(j_n - E(j)) \tag{14}$$

where T denotes all the number of duplets (i, j), i and j are two adjacent pixels, D(i) is the variance and E(i) is the expectation. For the 3 test images, their correlation coefficients results are shown in Table 1. We can easily find that all the adjacent pixels of the cipher images are weakly correlative; by comparison, the adjacent pixels of the original images are highly correlative. Thus, we can conclude that uncovering some information about the plaintext image from its cipher image is very difficult.

Table 1. The test result of correlation coefficients

Test images	Directions	Original images	Cipher images
Elaine	horizontal	0.977407	0.000893
	vertical	0.976693	-0.000663
	diagonal	0.972571	-0.000284
Aerial	horizontal	0.907963	-0.000793
	vertical	0.874697	-0.000429
	diagonal	0.820951	-0.000857
Airplane	horizontal	0.957875	-0.000107
	vertical	0.957543	0.000540
	diagonal	0.943487	-0.000358

4.1.3. Information entropy analysis. The entropy defined by Shannon [32] expresses the uncertainty of an image information. The Shannon entropy is defined as

$$H(I) = -\sum_{n=0}^{255} p(n)\log_2 p(n) \tag{15}$$

where I is an image, the entropy is represented in bits, n denotes a pixel value ($0 \le n \le 255$) and $p(n)$ is the probability of n. Table 2 shows the calculation results of the Shannon entropy of the 3 test images. For an image, the ideal Shannon entropy is 8. From Table 2, we can find that the Shannon entropy tends on the ideal value of 8. It proves that our encryption scheme can resist the entropy attack.

4.2. Differential attack analysis

We usually employ UACI (unified average changing intensity) and NPCR (number of pixels change rate) to check the resistance of differential attack. NPCR and UACI are defined as

$$\begin{cases} D(i,j) = \begin{cases} 1, & c_1(i,j) \neq c_2(i,j) \\ 0, & \text{otherwise} \end{cases} \\ \text{NPCR} = \dfrac{\sum_{ij} D(i,j)}{H \times W} \times 100\% \end{cases} \tag{16}$$

$$\text{UACI} = \frac{1}{H \times W}\left[\sum_{ij} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100\% \tag{17}$$

where H is the height of an image and W is the width of an image, $c_1(i,j)$ and $c_2(i,j)$ are the two different cipher images in which their plaintext images have only one pixel difference from each other. In [33], the maximum expected UACI value is 33.463541%, and the maximum expected NPCR value is 99.609375%. Table 2 shows the calculation results of UACI and NPCR values for our encryption scheme. We can find that UACI and NPCR values very verge on the above values in [33]. It proves that our encryption scheme makes the differential attack difficult.

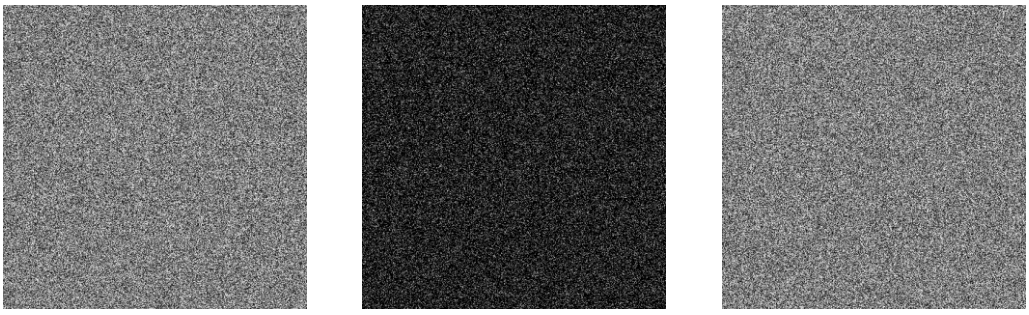
Table 2. Entropy, UACI and NPCR values

Ciphered	Entropy	NPCR	UACI
Elaine	7.999246	99.620819	33.441856
Aerial	7.999382	99.606705	33.466385
Airplane	7.999314	99.612808	33.549496

4.3. Key sensitivity analysis

To check the key sensitivity, we test 3 plaintext images in Figure 3 and all of the secret keys. For example, 10^{-14} is added in α and the other keys are not changed, and then we obtain the encrypted image of Elaine shown in Figure 6 (a). The difference between two encrypted images is indicated in Figure 6 (b). By analyzing all of the test results, we can conclude that our encryption scheme is sensitive to small change of the secret key.

Furthermore, the decryption scheme has also the sensitivity to small change of the secret key. By using the secret key α with only 10^{-14} differences from its original value, we obtain the decrypted image of Elaine shown in Figure 6(c). We can find that Elaine's decrypted image of is completely different with its plaintext image. It proves that the proposed decryption scheme is sensitive to small change of the secret key, too.



(a) (b) (c)

Figure 6. The analysis of key sensitivity. (a) Elaine's encrypted image using changed α, (b) difference between (a) and Figure 3(a), (c) Elaine's decrypted image using changed α.

4.4. Key space analysis

For resisting brute-force attacks, the key space of a good encryption system must be large enough. The fractional order linear-nonlinear chaos system has a strong sensitivity even to small change in the control parameters and initial condition, so we use a high precision real type data to implement our encryption system. There are five secret keys in our encryption system: μ, η, ε, α and $x_1(1)$, and the real type data has the accuracy of 10^{-14}. Therefore, the key space size of our encryption system would be at least 10^{70}. It means that our encryption system holds a wide enough key space against a brute-force attack.

4.5. Performance comparison

The comparative results between our encryption system and other cryptosystems [3, 6, 13, 20, 25] are indicated in Table 3. We can find that our encryption system has an ideal safety and similar or better performances.

Table 3. Comparative results between our encryption system and other cryptosystems.

Criteria		Proposed scheme	[3] after 58	[6] (averag	[13] (average)	[20]	[25]
Correlation coefficients	H	0.000367	0.0139	0.0134	-0.0017	0.015134	0.012401
	V	0.000325	-0.0231	0.0096	-0.0031	0.056865	N/A
	D	0.000354	-0.0040	0.0122	0.000089	0.001875	N/A
Entropy		7.999282	7.9966	N/A	N/A	N/A	7.995351

NPCR	99.6065%	99.67%	99.5659	99.6%	99.8268%	N/A
UACI	33.4526%	33.32%	33.3186	33.5%	10.9112%	N/A

5. Conclusions and future work

By using the defined fractional order linear-nonlinear chaos system, we design a scheme for encrypting a gray image. The given dynamical features of the fractional order linear-nonlinear chaos system, such as almost no periodic windows and stronger ergodicity of time series, are applied to the encryption scheme. The plaintext images decide which chaotic sequence is used for permutation and addition/subtraction operation of encryption. The corresponding experimental results indicate that our encryption scheme holds a wide enough key space, good sensitivity and high secure performances. In future practical research work, we intend to apply the fractional order linear-nonlinear chaos system to the encryption in a parallel architecture.

References

[1] Schneier B 1995 *Cryptography: theory and practice* (Boca Raton, FL: CRC Press)
[2] Furht B and Kirovski D 2005 *Multimedia Security Handbook* (CRC Press)
[3] Zhou Q and Liao X F 2012 Collision-based flexible image encryption algorithm Journal of Systems & Software **85** 400-7
[4] A N, Flores-Carmona N J and Carpio-Valadez M 2006 Encryption and decryption of images with chaotic map lattices Chaos **16** 821
[5] Rhouma R and Belghith S 2009 Cryptanalysis of a spatiotemporal chaotic cryptosystem Chaos Solitons & Fractals **411** 718-22
[6] Tang Y, Wang Z and Fang J A 2010 Image encryption using chaotic coupled map lattices with time-varying delays *Communications in Nonlinear Science & Numerical Simulation* **15** 2456-68.
[7] Wang X Y and Bao X M 2013 A novel block cryptosystem based on the coupled chaotic map lattice *Nonlinear Dynamics* **72** 707-15
[8] Wang Y, Liao X F, Xiao D and Wong K W 2008 One-way hash function construction based on 2d coupled map lattices *Information Sciences* **178** 1391-406
[9] Wang X Y and Teng L 2011 An image blocks encryption algorithm based on spatiotemporal chaos *Nonlinear Dynamics* **67** 365-71
[10] Wang X Y, Zhang N, Ren X L and Zhang Y L 2011 Synchronization of spatiotemporal chaotic systems and application to secure communication of digital image *Chinese Physics B* **20** 020507
[11] Hussain I and Gondal M A 2014 An extended image encryption using chaotic coupled map and S-box transformation *Nonlinear Dynamics* **76** 1355-63
[12] Arroyo D, Rhouma R, Alvarez G, Li S and Fernandez V 2008 On the security of a new image encryption scheme based on chaotic map lattices *Chaos* (Woodbury, N.Y.)
[13] Zhang Y Q and Wang X Y 2015 A New Image Encryption Algorithm Based on Non-adjacent Coupled Map Lattices *Applied Soft Computing* **26** 10-20
[14] Zhang Y Q and Wang X Y 2014 A Symmetric Image Encryption Algorithm Based on Mixed Linear-Nonlinear Coupled Map Lattice *Information Sciences* **273** 329-51
[15] Mandelbrot and Benoit B 1983 The fractal geometry of nature *American Journal of Physics* **51** 286
[16] Grigorenko I and Grigorenko E 2006 Erratum: chaotic dynamics of the fractional lorenz system *Phys.Rev. Lett.* **91** 034101
[17] Li C and Chen G 2004 Chaos in the fractional order Chen system and its control *Chaos Solitons & Fractals* **22** 549-54
[18] Zhang Y Q, Wang X Y, Liu L Y, He Y and Liu J 2017 Spatiotemporal Chaos of Fractional Order Logistic Equation in Nonlinear Coupled Lattices *Communications in Nonlinear Science & Numerical Simulation* 52
[19] Wang T S and Wang X Y 2009 Generalized synchronization of fractional order hyperchaotic Lorenz system *Mod. Phys. Lett. B* **23** 2167-78

[20] Wu X J and Lu Y 2009 Generalized projective synchronization of the fractional order Chen hyperchaotic system *Nonlinear Dyn.* **57** 25-35
[21] Xu Y, Wang H, Li Y and Pei B 2014 Image encryption based on synchronization of fractional chaotic systems *Communications in Nonlinear Science & Numerical Simulation* **19** 3735-44
[22] Wu X, Li Y and Kurths J 2015 A new color image encryption scheme using CML and a fractional-order chaotic system *Plos One* **10** e0119660
[23] Norouzi B and Mirzakuchaki S 2017 Breaking a novel image encryption scheme based on an improper fractional order chaotic system *Multimedia Tools & Applications* **76** 1817-26
[24] Zhao J, Wang S, Chang Y and Li X 2015 A novel image encryption scheme based on an improper fractional-order chaotic system *Nonlinear Dynamics* **80** 1721-9
[25] Yang Q, Chen D, Zhao T and Chen Y Q 2016 Fractional calculus in image processing: a review *Fractional Calculus & Applied Analysis* **19** 1222-49
[26] Srivastava H M 2006 Theory and applications of fractional differential equations
[27] May R M 1976 Simple mathematical models with very complicated dynamics, *Nature* **261** 459-67
[28] Raheem Z F E and Salman S M 2013 On a discretization process of fractiona-order Logistic differential equation *Journal of the Egyptian Mathematical Society* **22** 407-12
[29] Kaneko K 1989 Pattern dynamics in spatiotemporal chaos *Physica D* **34** 1-41
[30] Shibata H 2001 KS entropy and mean Lyapunov exponent for coupled map lattices *Physica A* **292** 182-92
[31] USC-SIPI Image Database 2013 (University of South California, Signal and Image Processing Institute: http://sipi.usc.edu/database/database.php)
[32] Shannon C E 1948 Communication theory of secrecy systems *Bell System Technical Journal* **28** 656–715
[33] Kwok H S and Tang W K S 2007 A fast image encryption system based on chaotic maps with finite precision representation *Chaos Solitons & Fractals* **32** 1518-29