Nonlinear Dyn (2015) 80:1721–1729
DOI 10.1007/s11071-015-1911-x

ORIGINAL PAPER

A novel image encryption scheme based on an improper fractional-order chaotic system

Jianfeng Zhao · Shuying Wang · Yingxiang Chang · Xianfeng Li

Received: 8 January 2014 / Accepted: 8 January 2015 / Published online: 21 January 2015

Abstract Based on the features of digital image encryption and high-dimensional chaotic sequences, the paper proposes a symmetric digital image encryption algorithm by a new improper fractional-order chaotic system. The initial conditions, parameters and fractional orders of chaos are influenced by gray value of all pixels and used as secret key. Therefore, the total key length is large enough to resist any brute-force attacks. The original image is divided into four parts and encrypted by different encryption formulas. Theoretical analysis results show that the proposed encryption scheme has effective encryption and efficiencies.

Keywords Image encryption · Chaos · Improper fractional · Secret key

J. Zhao (✉)
Department of Information Engineering, Henan Polytechnic, Zhengzhou, China
e-mail: zjfzwf@126.com

S. Wang
Department of Minzu, Huanghe Science and Technology College, Zhengzhou, China

Y. Chang
Department of Mathematics, Lanzhou Jiaotong University, Lanzhou, China

X. Li
Department of Architecture and Civil Engineering, City University of Hong Kong, Hong Kong, China

1 Introduction

With the development of computer and network technology, information security issues obtain great attention. Data encryption standard (DES) and advanced encryption standard (AES) are two traditional encryption algorithms. Intrinsic properties of chaotic systems lead to natural relationship and structural similarity between chaos and cryptography [1]. Chaos has been a hot topic in recent half-century [2–5]. Many digital image encryption schemes have been proposed based on chaotic systems [6–18]. However, the finite precision effect is a bottleneck of cryptography development.

Fractional-order chaotic systems have more complex characteristics. It has been found that fractional-order chaotic systems have wider applications in secure communication, signal processing, financial field, and digital watermark technology [19–22]. Low-dimensional chaotic systems can be easily implemented based on hardware platform but of weak secrecy, whereas high-dimensional hyper-chaotic systems have opposite characters. In view of their contradictions and characteristics degradation of digital chaotic system under finite precision effect [23–25], theory analysis about fractional-order systems is proposed [26]. The conceptual distinction between proper and improper fractional chaotic systems was put forward by Hu et al. in [27]. Fractional-order chaos has larger key space and more complex random sequences than integer-order chaos [16,17]. But the research of

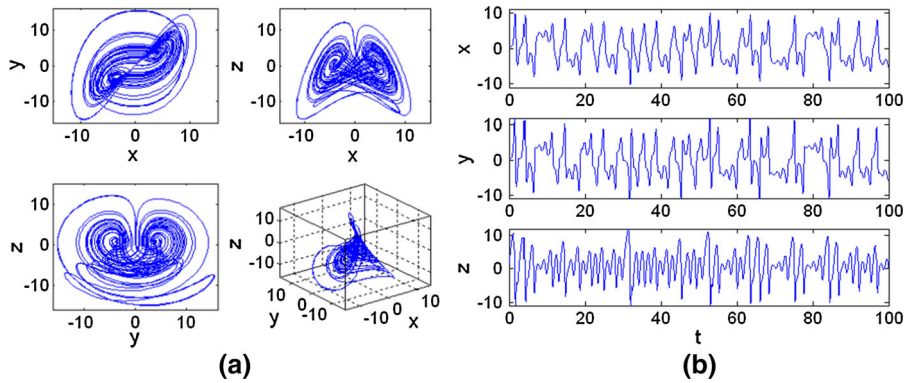

Fig. 1 Improper fractional chaos with $q = 1.1$. **a** Projections of one chaotic attractor. **b** Time histories of three variables

image encryption based on fractional-order chaos is very few and will be a great valuable research topic.

This paper is organized as follows. In Sect. 2, a new fractional-order chaotic system is introduced. A novel image encryption algorithm is proposed in Sect. 3. In Sect. 4, two numerical examples are given to illustrate the effectiveness of the proposed algorithm. Finally, Sect. 5 concludes the paper.

2 A new fractional-order chaotic system

Based on the famous Lorenz chaotic system, Chu et al. [28] proposed a new three-dimensional chaotic system. The fractional-order form of it is given as follows:

$$\begin{cases} \frac{d^{q_1}x}{dt^{q_1}} = a(\mathrm{y} - \mathrm{x}) \\ \frac{d^{q_2}y}{dt^{q_2}} = xz - y \\ \frac{d^{q_3}z}{dt^{q_3}} = b - xy - cz \end{cases} \tag{1}$$

where $X = (x, y, z)^T$ is the state vector, and $(a, b, c)^T$ is the parameter vector. System (1) will be a true fractional-order system, if the maximum of three fractional orders q_1, q_2, q_3 less than 1, i.e.,$\max(q_1, q_2, q_3) < 1$. It is an integer-order chaotic system if $q_1 = q_2 = q_3 = 1$. If $\max(q_1, q_2, q_3) > 1$, system (1) is called an improper fractional-order chaotic system. Using theoretical analysis of fractional-order stability [29] and numerical simulations, the system can be chaotic when three fractional orders are commensurate, and $q_1 = q_2 = q_3 = q \in (0.912202, 1.2)$, while parameters $a = 5, b = 16$, and $c = 1$. Starting from $(x(0), y(0), z(0)) = (0.2, 0.21, 0.3)$, 2D projections and 3D phase space of one typical chaotic attractor with $q = 1.1$ are shown in Fig. 1a, respectively. Correspondingly, time histories of three variables are plotted in Fig. 1b.

3 A novel digital image encryption algorithm

The original image (with $M*N$ pixels size) is imported and transformed line by line to obtain the matrix of pixel as formula (2). The whole encryption process is shown in Fig. 2.

$$P = \begin{bmatrix} P(1) & P(2) & \cdots & P(N) \\ P(N+1) & P(N+2) & \cdots & P(2N) \\ \vdots & \vdots & \vdots & \vdots \\ P((M-1)N+1) & P((M-1)N+2) & \cdots & P(L) \end{bmatrix} \tag{2}$$

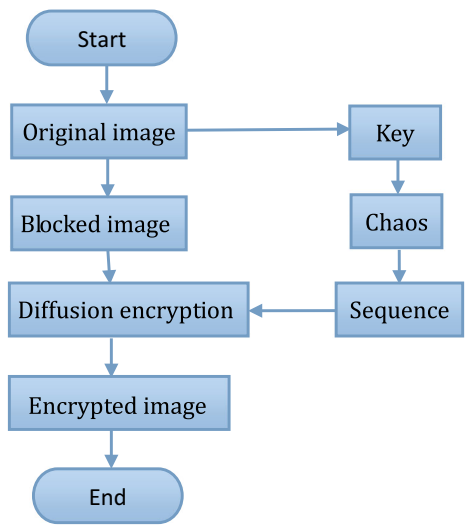

Fig. 2 Block diagram of the chaotic encryption algorithm

Table 1 The combination form of chaotic sequences

$m=0$	$m=1$	$m=2$	$m=3$
$B=\{B,x,y,z\}$	$B=\{B,z,x,y\}$	$B=\{B,y,z,x\}$	$B=\{B,x,z,y\}$

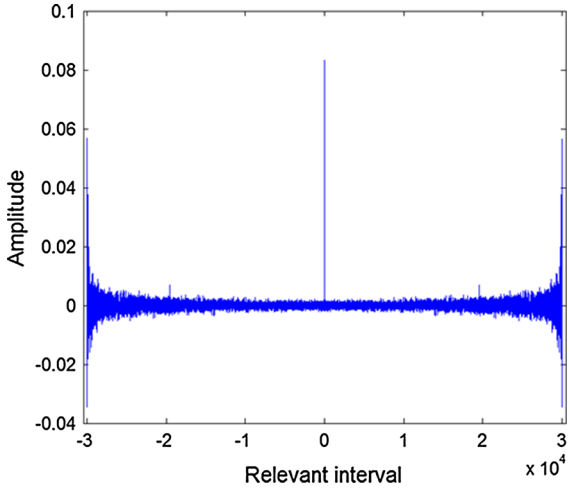

Fig. 3 Autocorrelation of sequence K

The key stream is constituted by initial state variables $(x(0), y(0), z(0))$, parameters (a, b, c), and fractional orders (q_1, q_2, q_3) of a chaotic system. In fact, the fractional-order chaotic system is highly sensitive to the secret key [26,27]. In diffusion, parameter $T = \mathrm{mod}\,(\sum_{i=1}^{L} P(i), L)/(L-1)$ is used to disturb key, in order to ensure that the encrypted image is sensitive enough to original image. Based on initial condition key, the fractional-order chaotic system (1) generates chaotic sequences and iterates one thousand times in advance to eliminate transient response.

The state vector $\{x, y, z\}$ is obtained from all of iterations to generate encryption sequence. The combination form of chaos sequences is generated using parameter $m = \mathrm{mod}\,(\mathrm{abs}(x+y+z), 4)$. Temporally, one empty matrix B is created. Then, B is assigned variably with respect to parameter m. The assignments of B are shown in Table 1.

Suppose that $K(i) = 10^n(B(i) - round(B(i)))$, where $n = 14$ is a positive integer. Self-correlations of sequence K fluctuate around zero. As shown in Fig. 3, vast majority of them locate in the interval of $[-0.005, 0.005]$.

The original image is divided into four parts to diffuse the pixel values one by one. For any pixel at position i, pixel substitution abides by the following algorithm:

$$
\begin{aligned}
&C(1) = [P(1) + K(1)] \bmod 256 \\
&\quad \oplus [P(L) + K(L)] \bmod 256 \\
&for\ i = 2 : \frac{L}{4} \\
&C(i) = [P(i) + K(i)] \bmod 256 \oplus [C(i-1) \\
&\quad + K(L)] \bmod 256 \\
&end \\
&C\left(\frac{L}{4}+1\right) = \left[P\left(\frac{L}{4}+1\right) + K\left(\frac{L}{4}+1\right)\right] \bmod 256 \\
&\quad \oplus [P(L) + K(L)] \bmod 256 \\
&for\ i = \frac{L}{4}+2 : \frac{L}{2} \\
&C(i) = [P(i) + K(i)] \bmod 256 \oplus [2^{*}C(i-1) \\
&\quad + K(L)] \bmod 256 \\
&end \\
&C\left(\frac{L}{2}+1\right) = \left[P\left(\frac{L}{2}+1\right) + K\left(\frac{L}{2}+1\right)\right] \bmod 256 \\
&\quad \oplus [P(L) + K(L)] \bmod 256 \\
&for\ i = \frac{L}{2}+2 : \frac{3L}{4} \\
&C(i) = [P(i) + K(i)] \bmod 256 \oplus [3^{*}C(i-1) \\
&\quad + K(L)] \bmod 256 \\
&end \\
&C\left(\frac{3L}{4}+1\right) = \left[P\left(\frac{3L}{4}+1\right) + K\left(\frac{3L}{4}+1\right)\right] \bmod 256 \\
&\quad \oplus [P(L) + K(L)] \bmod 256 \\
&for\ i = \frac{3L}{4}+2 : L \\
&C(i) = [P(i) + K(i)] \bmod 256 \oplus [4^{*}C(i-1) \\
&\quad + K(L)] \bmod 256 \\
&end
\end{aligned}
\tag{3}
$$

A pixel value sequence $\{C(i),\ i = 1, 2, \ldots, L\}$ is hereby transformed into an $M \times N$ matrix. Whereby, an encrypted image 256×256 is generated. For the given symmetric algorithm, decryption is the inverse-operation of encryption.

Time complexity is an important index for all of algorithms. Time complexity of generating key is

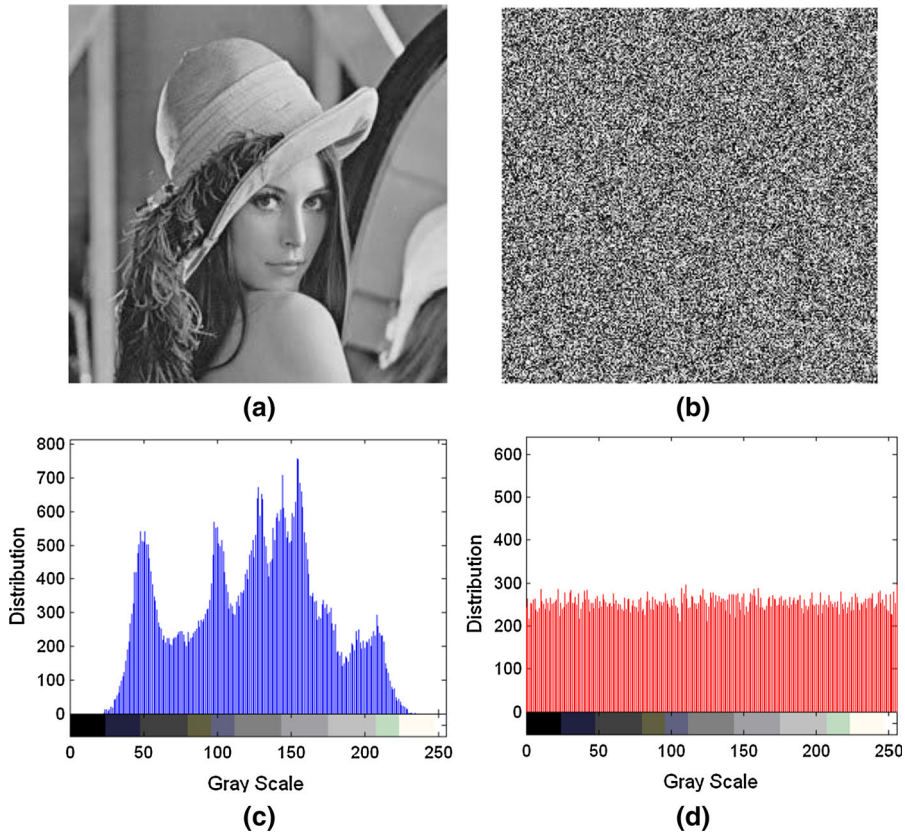

Fig. 4 Lena image.
a Plain Lena.
b Encrypted Lena.
c Histogram of plain image.
d Histogram of encrypted image

$O(M \cdot N)$ and image block is $O(1)$. Fractional-order chaotic systems generate chaos sequences with time complexity $O(T^2)$. Pixel substitution has time complexity $O(M \cdot N)$. At each step, the total time complexity is:

$$O(M \times N) + O(1) + O(T^2) + O(M \times N) = \begin{cases} O(T^2), & if\ M \times N \leq T \\ O(M \times N), & if\ M \times N > T \end{cases}, \quad (4)$$

where T is the iterate number of fractional-order chaos.

4 Numerical simulations and performance analysis

4.1 Histogram analysis

In the following implementations, an 8-bit gray level (standard) Lena image (Fig. 4a) with 256×256 pixels and a Babara image (Fig. 5a) with 720×580 pixels are taken as the original images. After one round of pixel value substitution encryption, there is no visual information can be observed in the encryption images, as shown in Figs. 4b and 5b, respectively. Histogram distributions of the encrypted images (Figs. 4b, 5b) are uniform comparatively. It is clearly shown that the encrypted images completely abide by obscure gray distribution law. The simulations show that the novel algorithm improves the resistance on spiteful attacks effectively.

4.2 Information entropy

For an image with n gray level, the information entropy of it can be calculated quantitatively with

$$H(x) = -\sum_{i=1}^{n} p(x_i)\ \log_2 p(x_i), \quad (5)$$

in which $p(x_i)$ indicates the probability of pixel value x_i.

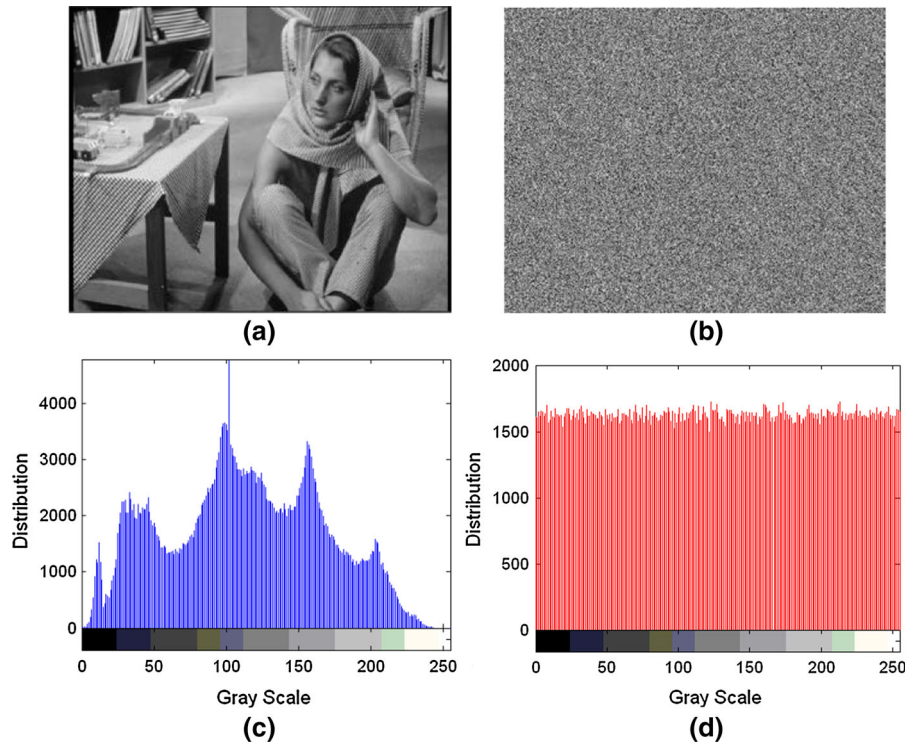

Fig. 5 Babara image. **a** Plain Babara. **b** Encrypted Babara. **c** Histogram of plain Babara. **d** Histogram of encrypted Babara

The entropies of plain image Lena and Babara are 7.447144 and 7.670496, respectively. Nevertheless, the entropies of encrypted Lena image and Babara image are 7.989529 and 7.991614, respectively. The entropies of encrypted images are so close to the ideal information ones that their gray distributions are relatively uniform. Therefore, the encrypted algorithm has better ability to resist statistical attacks. That is to say, the information leakage in present encryption process is negligible.

4.3 Correlation coefficients of adjacent pixels

Encryption algorithm is designed to reduce the correlation coefficients of adjacent pixels between the plain images and encrypted images for resisting statistical attacks. Correlation coefficients of entire randomly selected 3,000 pairs of horizontally, vertically, diagonally adjacent pixels are determined. The correlation coefficients between two adjacent pixels in an image are determined by the following formula:

$$R_{xy} = \frac{\mathrm{Conv}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{6}$$

where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \ \text{ and}$$

$$\mathrm{Conv}(x, y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)].$$

Figures 6, 7 and Table 2 display the distributions of the randomly selected pairs of adjacent pixels in three directions of the original and encrypted images. The graphical results emphasize that there is hardly any correlation between the pixels in encrypted images. It is clear that the correlation coefficient of the proposed algorithm is smaller than that of other methods proposed in Refs. [30,31] and AES.

4.4 Resistance to differential attacks

Based on principles of cryptology, a good encryption algorithm should be sensitive to the plaintext sufficiently. The sensitivity of the encryption algorithm can be quantified as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity

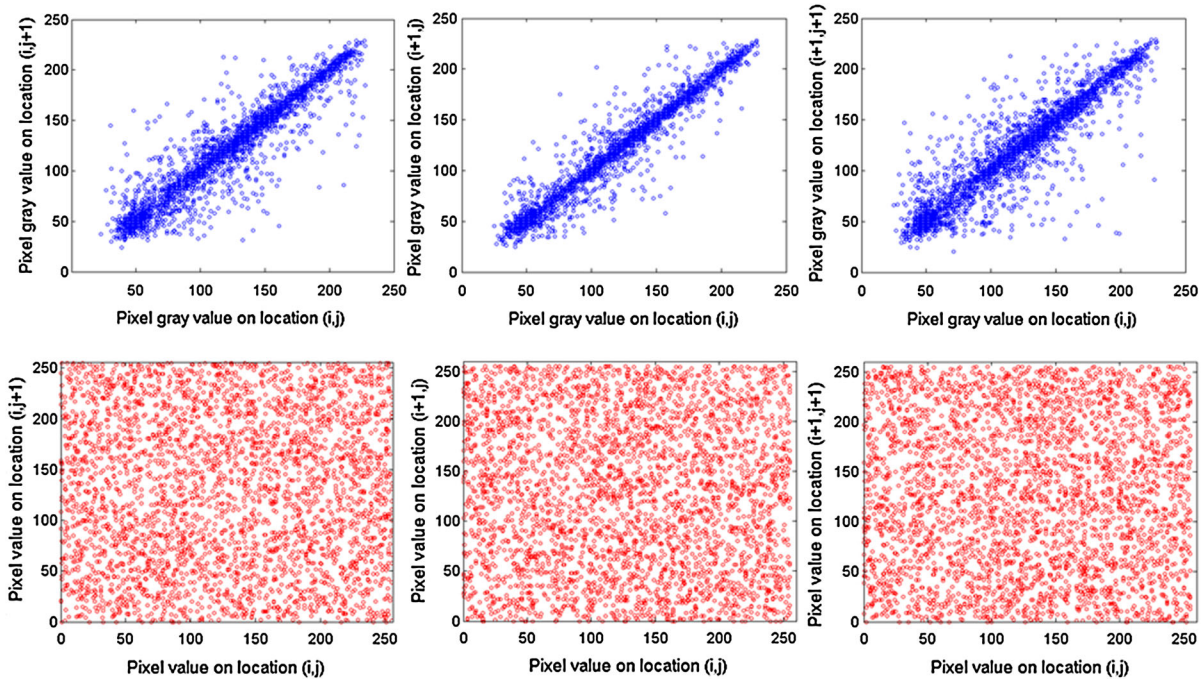

Fig. 6 Correlation coefficients of original and encrypted Lena images, from *left to right*: in *horizontal*, *vertical*, *diagonal direction*, respectively

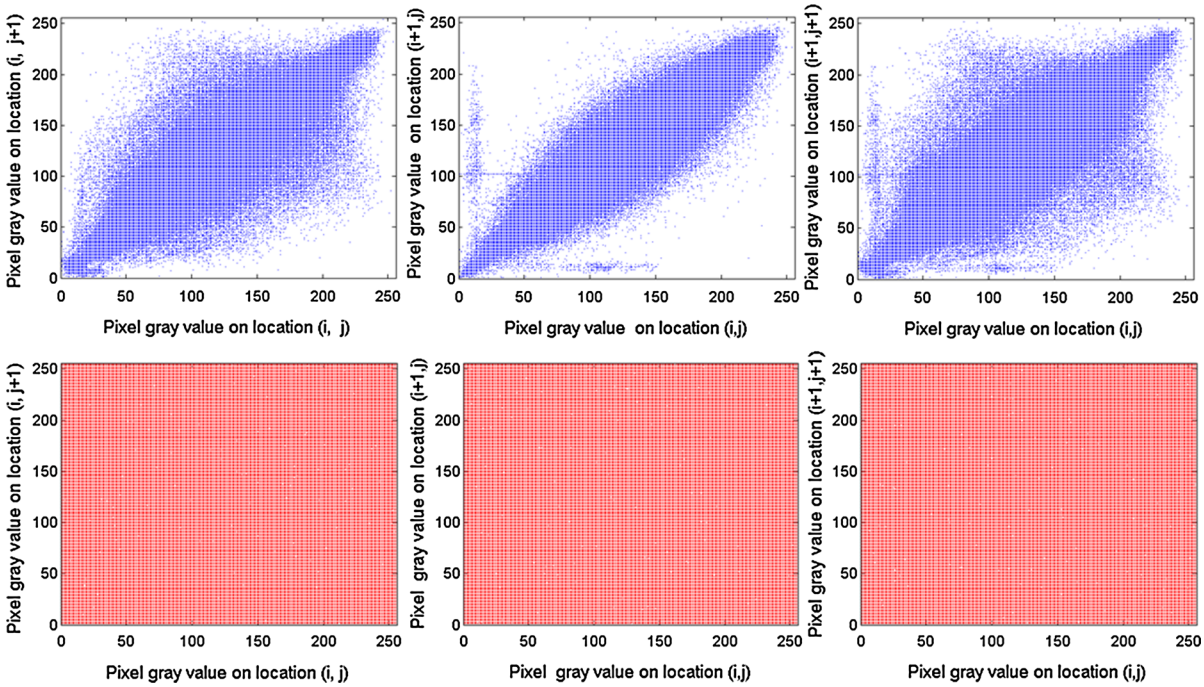

Fig. 7 Correlation coefficients of original and encrypted Babara images, from *left to right*: in *horizontal*, *vertical*, *diagonal direction*, respectively

Table 2 Correlation coefficients of the original and the encrypted images in three directions

Image	Horizontal	Vertical	Diagonal
Original image Lena	0.946401	0.969981	0.893969
Encrypted Lena	−3.219847e−006	−1.220718e−005	−5.840803e−005
Encrypted Lena [16]	0.0008213	0.0008423	0.0005083
Encrypted Lena [17]	0.01589	0.06538	0.03231
AES	−0.003129	0.002284	0.001328
Original image Babara	0.983267	0.980141	0.957314
Encrypted Babara	0.001953	−9.523236e−005	1.763753e−005

Table 3 Measurements of the sensitivity of the plain image and encrypted image

	(1,2) (%)	(2,3) (%)	(3.4) (%)	(4.5) (%)	Ideal value (%)
NPCR	99.6398	99.6139	99.5925	99.5880	99.6094
UACI	33.6270	33.4854	33.5630	34.6711	33.4635

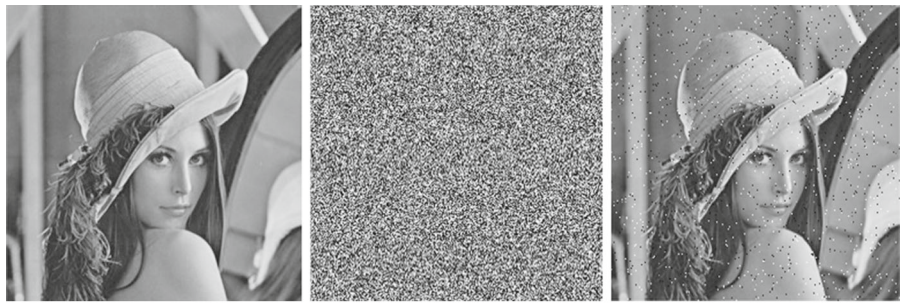

Fig. 8 Sensitivity tests of different keys: **a** decrypted Lena when $q_2 = 1.1$, **b** decrypted Lena when $q_2 = 1.1 + 10^{-12}$, **c** decrypted Lena image under salt-and-pepper noise

(UACI). NPCR is defined to find out some meaningful relationships between the original image and encrypted image. UACI is used to measure average of two different encrypted images. Respectively, NPCR and UACI are defined as following,

$$\begin{aligned} \mathrm{NPCR} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\,\%, \\ \mathrm{UACI} &= \frac{1}{255 \times M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |C_1(i, j) \\ &\quad - C_2(i, j)| \times 100\,\%. \end{aligned} \tag{7}$$

In (7), $D(i, j) = \begin{cases} 0\ , & C_1(i, j) = C_2(i, j), \\ 1\ , & C_1(i, j) \neq C_2(i, j), \end{cases}$ where $C_1(i, j)$ and $C_2(i, j)$ indicate pixel value of two encrypted images at location (i, j). M and N represent the number of row and column of the original image, respectively.

In addition, the ideal values of NPCR and UACI can be calculated by the following formula,

$$\begin{aligned} \mathrm{NPCR}_E &= (1 - 2^{-n}) \times 100\,\%, \\ \mathrm{UACI}_E &= \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n - 1} i(i+1)}{2^n - 1} \times 100\,\% \\ &= \frac{1}{3}(1 + 2^{-n}) \times 100\,\%, \end{aligned} \tag{8}$$

where n is the number of bits used to represent the different bit planes of an image. A gray scale image is 8 bits per pixel, $n = 8$.

In our experiment, five groups of Lena images are encrypted. In every group, one is the original image, while the other is the original image with only one randomly changed pixel value. The test results are shown in Table 3. It can be found that every value fluctuates nearby the ideal values. Obviously, the given encryption algorithm is very sensitive to small changes in the plain image such that it has great capacity of resistance to differential attacks.

4.5 Key space and key sensitivity analysis

In the algorithm, every number consists of two integers and fourteen decimals. If the state variables and parameters are included in secret key, the key space is 2^{318}. If fractional orders are added as secret key, the key space increases to 2^{478}, which is equivalent to binary key with 478-bits. Obviously, larger key space improves the ability to resist exhaustive attacks. A good encryption algorithm should be sensitive to secret key. Little changes of decryption key will lead to failed decrypted images. In the following simulations, when $q_2 = 1.1$ and $q_2 = 1.1 + 10^{-12}$ are selected in key space, the decrypted images are shown in Fig. 8a, b, respectively. The decryption is successful even though the images are attacked by the salt-and-pepper noise. It can be seen that some important features of the original image are preserved in Fig. 8c.

5 Conclusions

Based on an improper fractional-order chaotic system, a new chaotic encryption algorithm is proposed. The modified chaotic sequence has good random uniform distributions, and every pixel value of the original image affects the secret key. Small changes of the plain images may arouse great difference in encrypted images. The results demonstrate that the algorithm is so strong that it can resist differential attacks. The ability is strutted by two metrics, namely, NPCR and UACI. Compared with AES and other algorithms, the present algorithm has better performance.

Acknowledgments The research is supported by NNSFs of China (Grant Nos. 11161027, 11262009), Key FSN of Gansu Province, China (Grant No. 1104WCGA195), and Specialized RF for DPHE of China (Grant No. 20136204110001).

References

1. Kocaerv, L.: Chaos-based cryptography: a brief overview. IEEE. Trans. Circuits Syst. **1**(3), 6–21 (2001)
2. Aguilar-Bustos, A.Y., Cruz-Hernández, C.: Synchronization of discrete-time hyperchaotic systems: an application in communications. Chaos Solitons Fract. **41**(3), 1301–1310 (2009)
3. López-Gutiérrez, R.M., Posadas-Castillo, C., López-Mancilla, D., Cruz-Hernández, C.: Communicating via robust synchronization of chaotic lasers. Chaos Solitons Fract. **42**(1), 277–285 (2009)
4. Van Wiggeren, G.D., Roy, R.: Communication with chaotic lasers. Science **279**(20), 1198–1200 (1998)
5. Gao, T.G., Chen, Z.Q.: A new image encryption algorithm based on hyperchaos. Phys. Lett. A **372**(4), 394–400 (2007)
6. Li, X.F., Chlouverakis, K.E., Xu, D.L.: Nonlinear dynamics and circuit realization of a new chaotic flow: a variant of Lorenz, Chen and Lü. Nonlinear Anal. Real World Appl. **10**, 2357–2368 (2009)
7. Guan, Z.H., Huang, F., Guan, W.: Chaos-based image encryption algorithm. Phys. Lett. A **346**(1–3), 153–157 (2005)
8. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perception model. Nonlinear Dyn. **62**(3), 615–621 (2010)
9. Fu, C., Lin, B.B., Miao, Y.S., Liu, X., Chen, J.J.: A novel chaos-based bit-level permutation scheme for digital image encryption. Opt. Commun. **28**(4), 5415–5423 (2011)
10. Zhang, G., Liu, Q.: A novel image encryption method based on total shuffl-ing scheme. Opt. Commun. **28**(4), 2775–2780 (2011)
11. Behnia, S., Akhshani, A., Mahmodi, H.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fract. **35**(2), 408–419 (2008)
12. Zhang, Q., Guo, L., Wei, X.P.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. **52**(11–12), 2028–2035 (2010)
13. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(8), 2129–2151 (2006)
14. Chen, G.R., Mao, Y.B., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fract. **21**(3), 749–761 (2004)
15. Zhang, L.H., Liao, X.F., Wang, X.B.: An image encryption approach based on chaotic maps. Chaos Solitons Fract. **24**(3), 759–765 (2005)
16. Kanso, A., Ghebleh, M.: A novel image encryption algorithm based on a 3D chaotic map. Commun. Nonlinear Sci. Numer. Simul. **17**(7), 2943–2959 (2012)
17. Ye, G.D., Wong, K.W.: An image encryption scheme based on time-delay and hyperchaotic system. Nonlinear Dyn. **71**(1–2), 259–267 (2013)
18. Bigdeli, N., Farid, Y., Afshar, K.: A novel image encryption/decryption scheme based on chaotic neural networks. Eng. Appl. Artif. Intell. **25**(4), 753–765 (2012)
19. Wu, X.J., Lu, Y.: Generalized projective synchronization of the fractional order Chen hyperchaotic system. Nonlinear Dyn. **57**(1–2), 25–35 (2009)
20. Arman, K.B., Kia, F., Naser, P., Leung, H.: A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter. Commun. Nonlinear Sci. Numer. Simul. **14**(3), 863–879 (2009)
21. Wang, Y.Q., Zhou, S.B.: Image encryption algorithm based on fractional-order Chen chaotic system. J. Comput Appl. **33**(4), 1043–1046 (2013)
22. Ismail, A.I., Mohammed, A., Hossam, D.: A digital image encryption algorithm based a composition of two chaotic logistic maps. Int. J. Netw. Secur. **11**(1), 1–5 (2010)
23. Peng, F., Qiu, S.S., Long, M.: An image encryption algorithm based on mixed chaotic dynamic systems and external keys. IEEE Trans. Circuits Syst. **46**(5), 1135–1139 (2005)

24. Yang, T., Yang, L.B., Yang, C.M.: Breaking chaotic switching using generalized synchronization: examples. IEEE Trans. Circuits Syst. Part I **45**(10), 1062–1067 (1998)
25. Seyedzadeh, S.M., Mirzakuchaki, S.: A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Process. **92**(5), 1202–1215 (2012)
26. Tavazoei, M.S., Haeri, M.: A necessary condition for double scroll attractor existence in fractional-order systems. Phys. Lett. A **367**(1–2), 102–113 (2007)
27. Hu, J.B., Xiao, J., Zhao, L.D.: Synchronization improper fractional Chen chaotic system. J. Shanghai Univ. **17**(6), 734–739 (2011). (in Chinese)
28. Chu, Y.D., Li, X.F., Zhang, J.G., Chang, Y.X.: Computer simulation and circuit implementation for a new autonomous chaotic system. J. Sichuan Univ. **44**(3), 550–556 (2007). (in Chinese)
29. Rosenstein, M.T., Collins, J.J., Luca, C.J.D.: A practical method for calculating largest Lyapunov exponents from small data sets. Phys. D **65**(1–2), 117–134 (1993)
30. Norouzi, B., Seyed, M.S., Sattar, M., Mohammad, R.M.: A novel image encryption based on hash function with only two-round diffusion process. Multimed. Syst. **20**(1), 45–64 (2014)
31. Gao, H.J., Zhang, Y.S., Liang, S.Y., Li, D.Q.: A new chaotic algorithm for image encryption. Chaos Solitons Fract. **29**(2), 393–399 (2006)