Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 8672716, 10 pages
https://doi.org/10.1155/2017/8672716

Research Article

Image Encryption Algorithm Based on a Novel Improper Fractional-Order Attractor and a Wavelet Function Map

Jian-feng Zhao,[1] Shu-ying Wang,[2] Li-tao Zhang,[3] and Xiao-yan Wang[1]

[1]*Department of Information Engineering, Henan Polytechnic, Zhengzhou, China*
[2]*Department of Minzu, Huanghe Science and Technology College, Zhengzhou, China*
[3]*Department of Mathematics and Physics, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou 450015, China*

Correspondence should be addressed to Shu-ying Wang; wsy0707@126.com

Received 12 November 2016; Revised 21 January 2017; Accepted 8 February 2017; Published 22 March 2017

Academic Editor: Jucheng Yang

This paper presents a three-dimensional autonomous chaotic system with high fraction dimension. It is noted that the nonlinear characteristic of the improper fractional-order chaos is interesting. Based on the continuous chaos and the discrete wavelet function map, an image encryption algorithm is put forward. The key space is formed by the initial state variables, parameters, and orders of the system. Every pixel value is included in secret key, so as to improve antiattack capability of the algorithm. The obtained simulation results and extensive security analyses demonstrate the high level of security of the algorithm and show its robustness against various types of attacks.

1. Introduction

With rapid development of communications, network security of information has become increasingly important for many applications. While high redundancy for image and multimedia information is challenging traditional cryptography algorithms [1, 2], chaotic attractors have orbital pseudorandom properties, good unpredictability, highly sensitivity for initial conditions, topological transitivity features, and so on. These characters indicate that chaos-based cryptosystem is a research hotspot in multimedia security area [3]. In 1949, Shannon created confusion and diffusion in the world of cryptography [4]. To overcome high redundancies and strong correlations of digital images, chaos has been widely applied in traditional encryption algorithm [5–13]. Research proposed that one-dimensional chaotic system has low security [14, 15]. With higher dimension, chaotic attractor occupies more space and winding complexly. The most complex attractor has much more complex output signals so that encryption effect would be better, whereas three-dimensional autonomous chaotic systems with higher fractal dimension are rare [16].

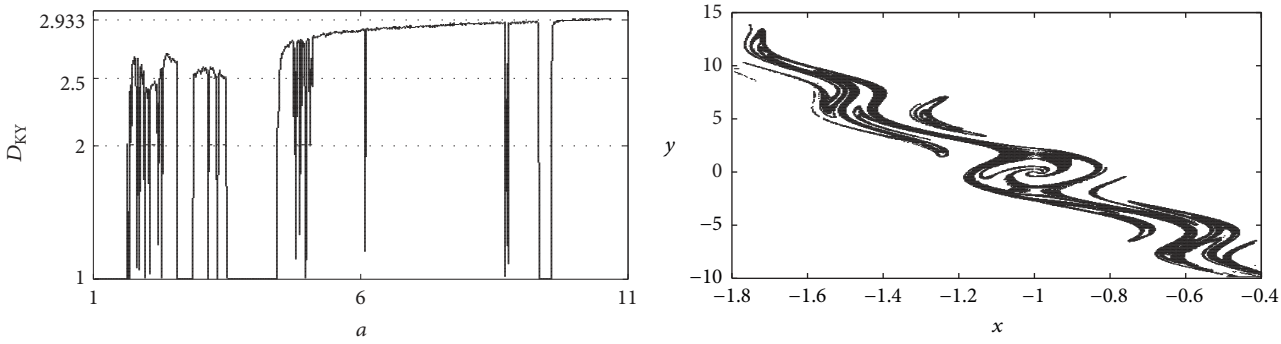
Comparing with integer-order chaotic system, the fractional-order chaotic system is not only related to parameters of the system, but also closely linked with fractional orders of system. Improper fractional-order chaotic system, therefore, has strong nonlinear characters and complexity. In secret communication, it can enhance the density and security so as to enormously increase the difficulty of unmasking signals. The algorithm shows greater application value in communication field [17, 18].

The rest of this paper is organized as follows: Section 2 describes a novel complex attractor. In Section 3, the chaos-based encryption algorithm is proposed. The numerical experimental results of performance analysis are given in Section 4. Finally, Section 5 contains conclusion and perspectives.

2. Improper Fractional-Order Chaotic Flow

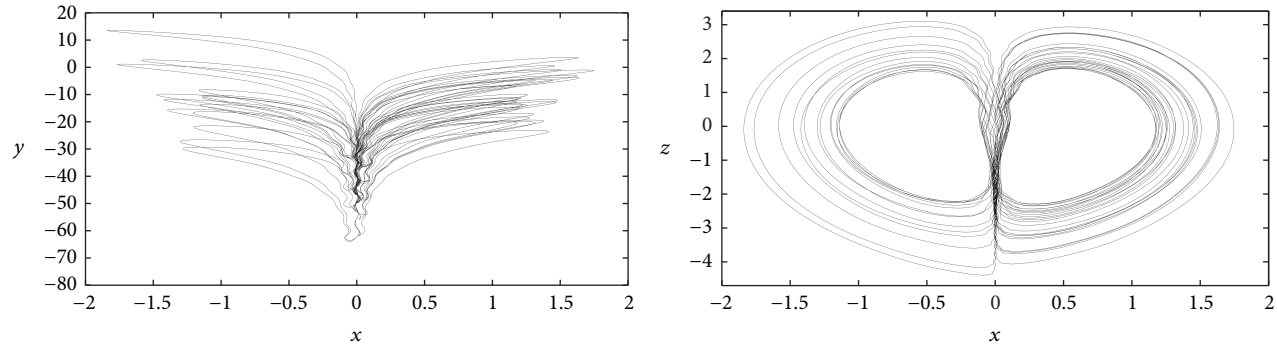
A new three-dimensional autonomous chaotic system with high fraction dimension is constructed, of which the governing fractional-order equation is

$$\frac{d^{q_1}x}{dt^{q_1}} = xz + b\sin(x + y + z),$$
$$\frac{d^{q_2}y}{dt^{q_2}} = az - by,$$



(a) Lyapunov dimensions (b) Poincaré sections of the maximally complex attractor

Figure 1: Chaotic characters of the novel attractor with $q_1 = q_2 = q_3 = 1$.



(a) x-y phase plane (b) x-z phase plane

Figure 2: The fractional-order chaos with $q_1 = 1.01$, $q_2 = 1.1$, and $q_3 = 1.11$.

$$\frac{d^{q_3} z}{dt^{q_3}} = 1 - cx^2, \tag{1}$$

where $X = (x, y, z)^T$ are state variables and a, b, c are parameters. Three fractional orders are q_1, q_2, q_3; if $\max(q_1, q_2, q_3) < 1$, system (1) is a true fractional-order system, if $q_1 = q_2 = q_3 = 1$, system (1) is an integer-order system, and if $\max(q_1, q_2, q_3) > 1$, system (1) is an improper fractional-order system. Based on stability theory and numerical analysis of fractional-order system, when $(a, b, c) = (6, 5, 0.12)$ and $(q_1, q_2, q_3) = (1, 1, 1)$, the Lyapunov dimension D_{KY} is shown in Figure 1(a) with varying parameter a in interval $[1, 11]$. Almost all D_{KY} of chaotic attractors are larger than 2.5. With increasing control parameters, D_{KY} reaches as high as 2.9336 at some special parameters. As shown in Figure 1(b), the Poincaré section of the maximally complex attractor has hierarchical structure composed of dense points. When $(q_1, q_2, q_3) = (1.01, 1.1, 1.11)$, the improper fractional-order chaos presents interesting and complex dynamic behavior represented in Figure 2.

3. Image Encryption Algorithm

Algorithm process is shown in Figure 3.

Encryption Procedure. Image encryption algorithm mainly consists of two processes: confusion and diffusion.

Step 1 (pixel confusion). Suppose that the size of plaintext image is $L = M \times N$. Scanning the plaintext image line by line in order to obtain pixel matrix P is as follows:

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

In confusion procedure, the wavelet function map is taken as follows [21]:

$$x_{n+1} = k \cdot \left(1 - x_n^2\right) \cdot e^{-(x_n+\mu)^2/2}, \tag{3}$$

where $n \in N$ is the number of iterations. For numerical simulations, we take the initial value of the discrete system (3) as $x_0 = 0.3$, parameter $k = 1.33$, and $\mu = -0.6$. The chaotic characteristics of wavelet function map are shown in Figure 4(a), and its interesting bifurcation diagram varying with $\mu \in [-0.77, -0.29]$ is displayed in Figure 4(b).

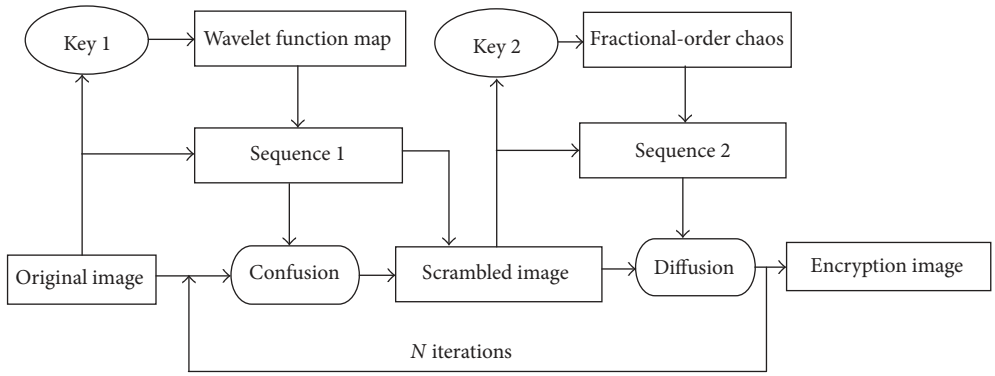
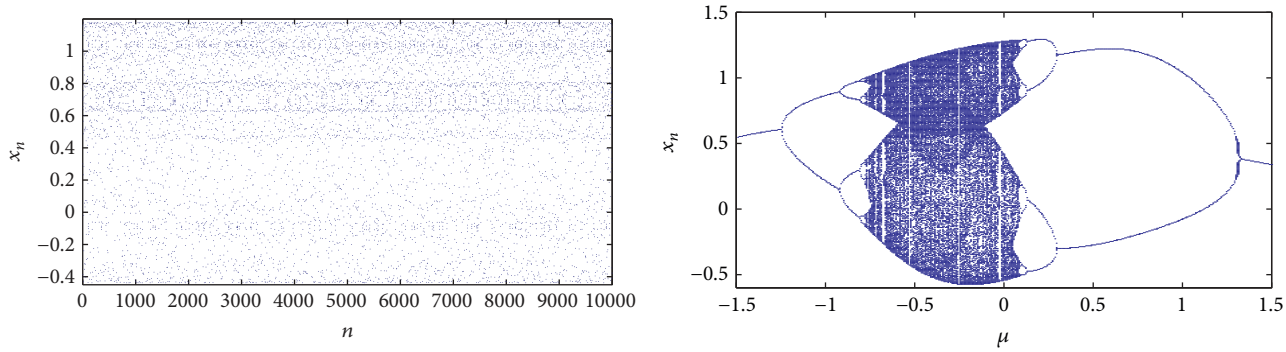


Figure 3: Encryption process.



(a) Wavelet function map

(b) Bifurcation of wavelet function map

Figure 4: Wavelet function map.

To improve the sensitivity of original image to encryption image, secret keys are distracted by plain image. In confusion procedure, $T = \mathrm{mod}\left(\sum_{i=1}^{L} P(i), L\right)/(L-1)$ is initial vector of wavelet function map. Sequence $x(n)$ is rearranged by wavelet function map so as to engender position matrix $lx(n)$. Then $lx(n)$ is used to confuse position of image pixels and get matrix $\{C(i) \mid i = 1, 2, \ldots, L\}$. Finally matrix $\{C(i) \mid i = 1, 2, \ldots, L\}$ is transformed into permutation image C of size $M \times N$.

Step 2 (pixel diffusion). Confusion only changes the position of pixel point while the pixel value is fixed, so the attacker may break down the algorithm though the statistics.

In diffusion, T is used to disturb parameter $a = a + T$ of system (1). Then the chaos generates chaotic sequences and makes N_0 times preiteration to eliminate some harmful effect of chaos transient process. Matrix B is created and initialized as an empty sequence. State vector $\{x(1), x(2), x(3)\}$ is generated in every iteration and a parameter $m = \mathrm{mod}\,(\mathrm{abs}(x(1) + x(2) + x(3)), 3)$ is derived. Then, matrix B is assigned according to parameter m. When $m = 0$, $B = \{B, x_1, x_2\}$, when $m = 1$, $B = \{B, x_1, x_3\}$, and when $m = 2$, $B = \{B, x_3, x_1\}$.

In every interaction, sequence B has strong randomness after $2L + N_0$ times iteration. Then B is preprocessed in the following form:

$$K(i) = \mathrm{mod}\left(\mathrm{temp}, 256\right), \quad i = 1, 2, \ldots, L, \tag{4}$$

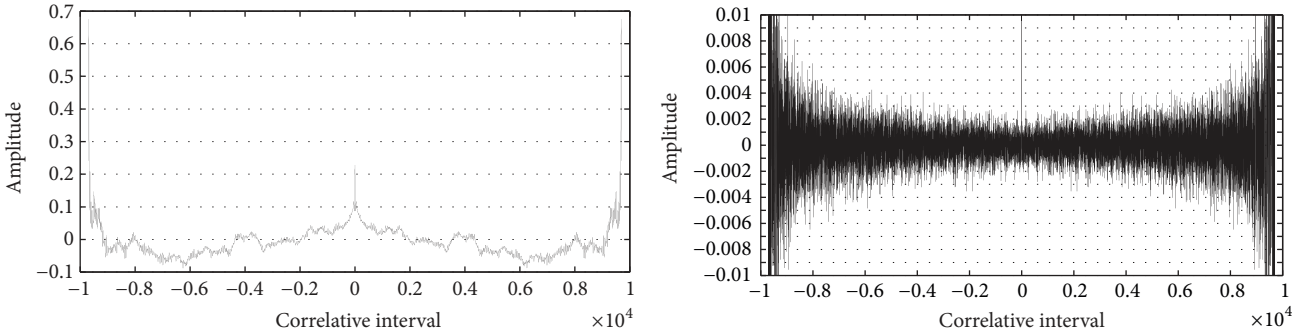
where $\mathrm{Temp} = \mathrm{floor}\left((|B(i)| - \mathrm{floor}\left(|B(i)|\right)\right) \times 10^m)$, $|x|$ is absolution of x, and $\mathrm{floor}\,(x)$ expresses downrounding. The positive integer $m = 12$. The autocorrelation of sequence B focuses on the interval $[-0.1, 0.1]$ and is shown in Figure 5(a), whereas the autocorrelation of sequence K after the pretreatment focuses on a smaller interval $[-0.003, 0.003]$ processed in Figure 5(b).

During diffusion, first pixel of permutation image C is encrypted as follows:

$$\begin{aligned} C(1) &= [C(1) + K(1)] \bmod 256 \\ &\quad \oplus [C(L) + K(1 + L + T)] \bmod 256. \end{aligned} \tag{5a}$$

However, for pixel at position $i > 1$, pixel substitution is made according to

$$\begin{aligned} C(i) &= [C(i) + K(i)] \bmod 256 \\ &\quad \oplus [C(i-1) + K(i + L + T)] \bmod 256, \\ &\qquad i = 1, 2, \ldots, L. \end{aligned} \tag{5b}$$



(a) Autocorrelation of sequence B

(b) Autocorrelation of improved sequence K

Figure 5: Autocorrelation of sequences.

Then sequence $\{C(i),\ i = 1, 2, \ldots, L\}$ is conversed into matrix with size of $M \times N$.

Decryption is inverse operation of encryption process. Decryption image D is scanned line by line to get sequence $\{D(i) \mid i = 1, 2, \ldots, L\}$ $(L = M \times N)$.

$$\begin{aligned} \text{temp} &= C(i) \oplus [C(i-1) + K(i+L+T)] \bmod 256, \\ D(i) &= [\text{temp} - K(i)] \bmod 256, \\ & \qquad i = L, L-1, \ldots, 2, \end{aligned} \tag{6a}$$

$$\begin{aligned} \text{temp} &= C(1) \oplus [C(L) + K(1+L+T)] \bmod 256, \\ D(1) &= [\text{temp} - K(1)] \bmod 256. \end{aligned} \tag{6b}$$

Then, inverse scrambling operation for matrix $\{D(i) \mid i = 1, 2, \ldots, L\}$ is made. Firstly, sequence $x(n)$ is generated by wavelet function map to produce position matrix $lx(n)$. Then $lx(n)$ is arranged by the same law so as to get position matrix $llx(n)$. At last we use $llx(n)$ to confuse pixel position of image D to get matrix $\{E(i) \mid i = 1, 2, \ldots, L\}$ and change matrix E into $M \times N$ two-dimension matrix to observe final decrypted image.

4. Numerical Simulation and Performance Analysis

The proposed encryption technique is implemented in MATLAB 7.1. In the experiment, different types of digital images are tested, such as gray image, binary image, and color image.

4.1. 3D Histogram Analysis. Histogram is a graphical representation of the pixels intensity distribution of an image, and it can measure the capacity of resisting attack. The gray Lena image of size 256×256 is encrypted as shown in Figure 6(c) and the 3D histogram of the encrypted Lena image is shown in Figure 6(d). The binary image has only two colors and is sensitive to the change of pixel. 3D histograms of a binary image are encrypted and encrypted binary images are demonstrated in Figures 7(b) and 7(d), respectively. Figure 8(a) shows the color image and its RGB histograms; Figure 8(b) shows the encrypted color image of Figure 8(a) and its RGB histograms. The histogram of the encrypted image is fairly uniform and significantly different from that of the original image, so the information is unpredictable and histogram attack can be avoided.

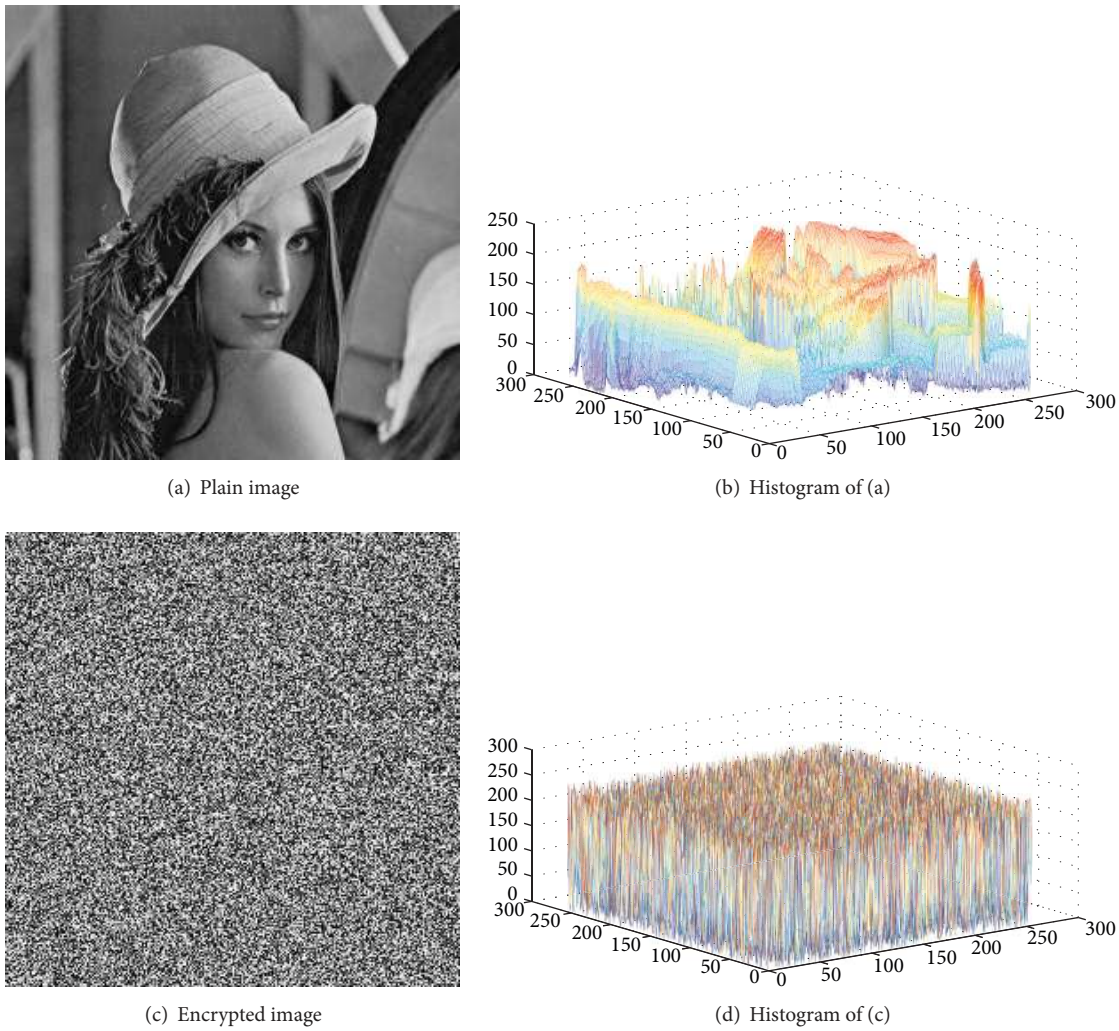
4.2. Information Entropy. Information entropy, firstly proposed by Shannon in 1949, is a significant property that reflects the randomness and the unpredictability of an information source [4]. With bigger entropy image has more uniform gray distribution. The entropy $H(x)$ is defined by the following formula: $H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$, where $p(x_i)$ denotes the probability of symbol x_i. When $p(x_i) = 1/256$, the 256×256 gray image has maximum entropy of 8. Entropy of gray Lena image and binary image is 7.447144 and 0.593165, respectively, while its encryption is 7.988847 and 7.972069, respectively. Considering RGB components of color image Lena, average information entropy of the color Lena and encrypted color Lena is 7.198813 and 7.997281, respectively. It is obvious that the entropies of the cipher images are very close to the theoretical value of 8, which means that the encryption algorithm has ability of resisting statistical attack.

4.3. Correlation Coefficients of Adjacent Pixels. In the section, we aim at checking up the correlation of two adjacent pixels between the original image and encrypted image. In this simulation, randomly selected 1000 pairs of adjacent pixels (horizontally, vertically, and diagonally) are determined. The correlation coefficient between two adjacent pixels in an image is determined according to the following formula:

$$R_{xy} = \frac{\text{Conv}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

where

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2, \\ \text{Conv}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]\,[y_i - E(y)]. \end{aligned} \tag{8}$$



(a) Plain image

(b) Histogram of (a)

(c) Encrypted image

(d) Histogram of (c)

Figure 6: The gray Lena image.

Figure 9 displays correlation coefficients of adjacent pixels in four directions of Lena plain image and cipher image. The result emphasizes that there is hardly any correlation of adjacent pixels in encryption images. Correlation coefficients of the encrypted Lena image are smaller than other methods shown in Table 1. The statistical properties of original image have randomly spread to encryption image.

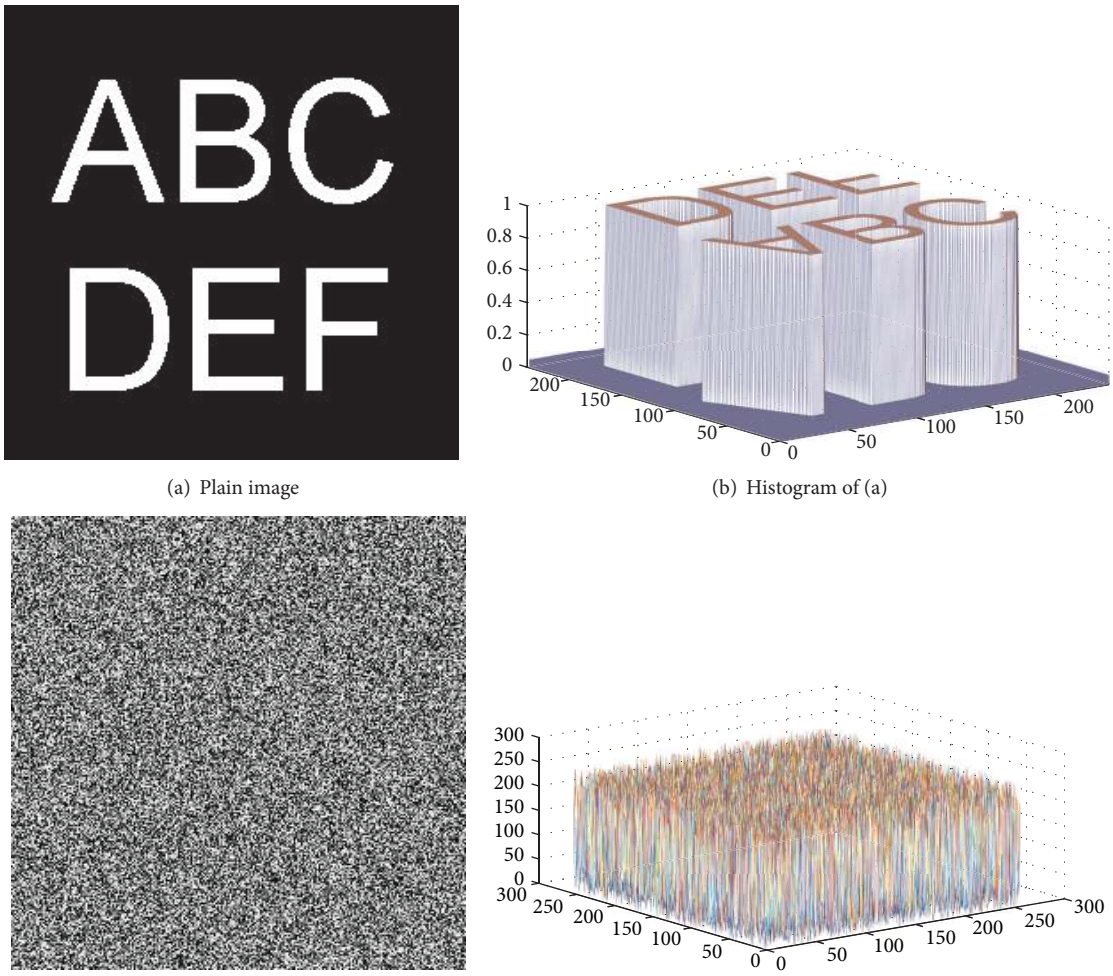
4.4. Resistance to Differential Attack. The attacker may observe the change of decryption by the tiny change of plaintext to find the correlation between plain image and cipher image. Based on principles of cryptology, a good encryption algorithm should be sensitive to plaintext sufficiently. In general, attacker makes a slight change (e.g., modify only one pixel) for plaintext to find out some relationships between plain image and encrypted image. If tiny change of original image can bring great changes to cipher image, the effect of differential attack will be reduced. Sensitivity of the plaintext encryption algorithm can be quantified by NPCR (number of pixels changing rate) and UACI (unified average changing intensity). They are defined as follows:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j), \end{cases}$$

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{9}$$

$$\text{UACI} = \frac{1}{255 \times M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| C_1(i,j) - C_2(i,j) \right| \times 100\%,$$

where $C_1(i, j)$ and $C_2(i, j)$ indicate pixel value of two encryption images at location (i, j). M and N present number of rows and columns of the original image.



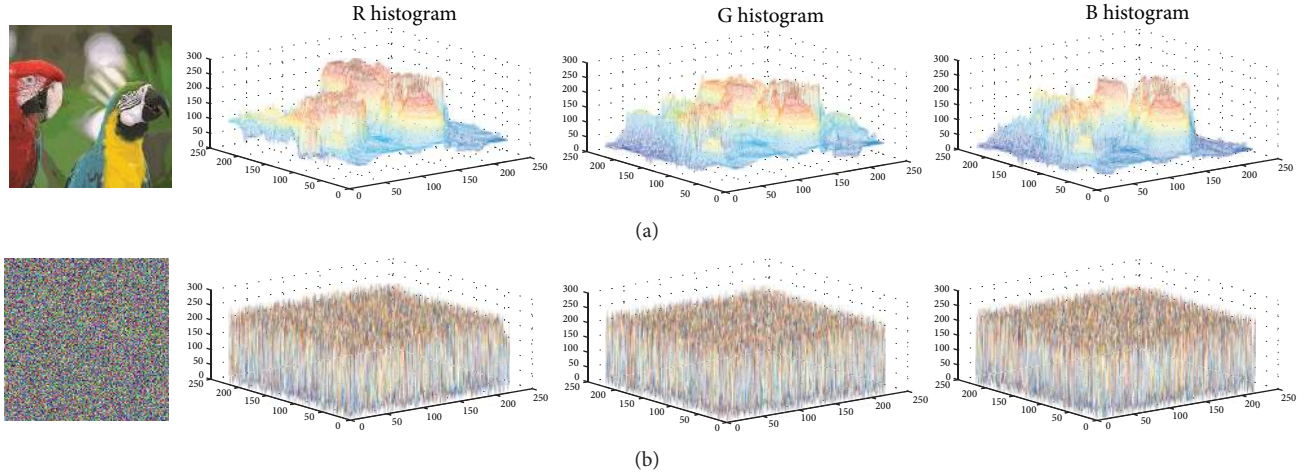
(a) Plain image

(b) Histogram of (a)

(c) Encrypted image

(d) Histogram of (c)

Figure 7: The binary image.



(a)

(b)

Figure 8: The color parrot image: (a) the plain image and its RGB histograms; (b) the encrypted image and its RGB histograms.

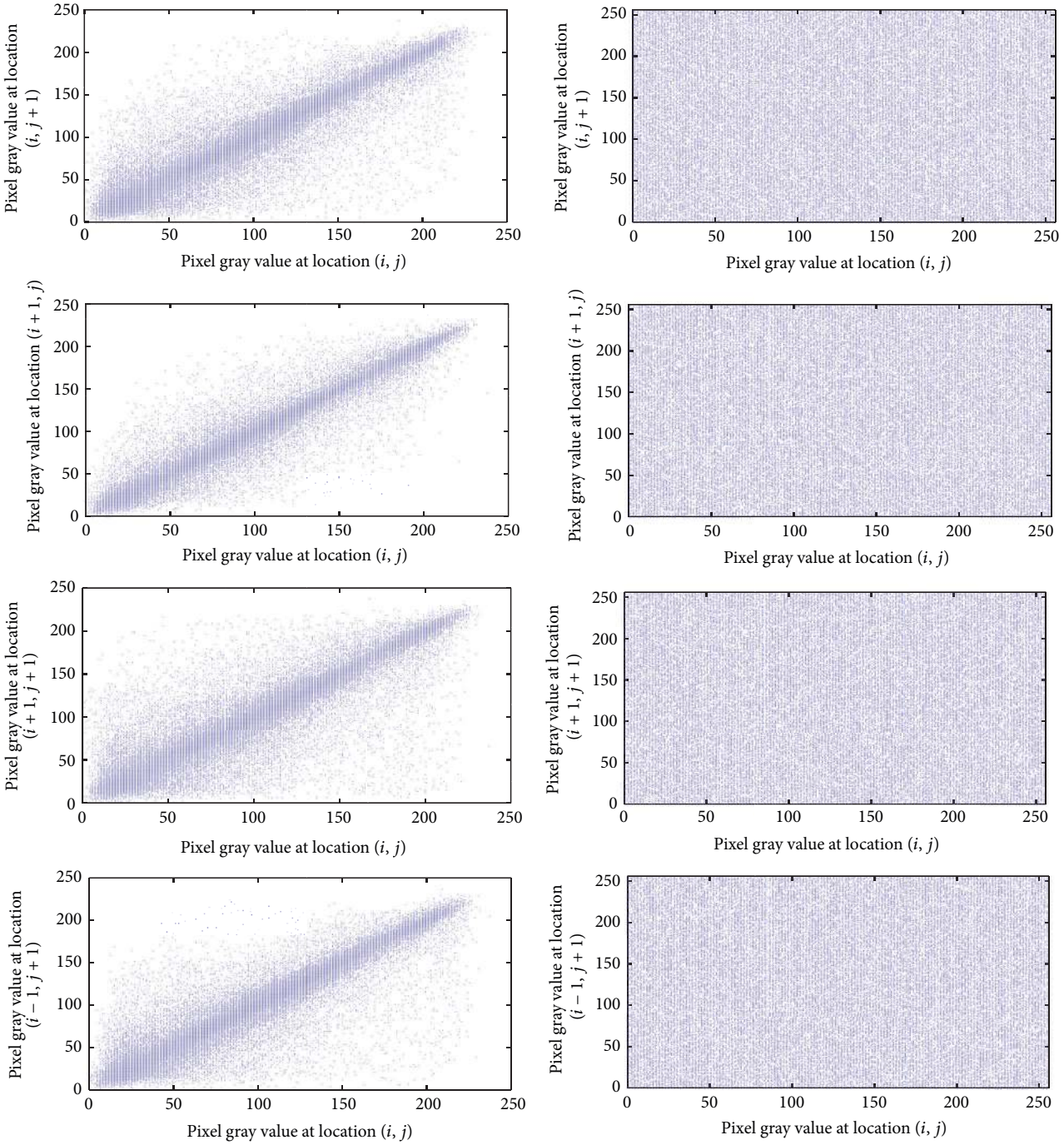


Figure 9: Correlation coefficients of original and encryption image: horizontal; vertical; diagonal; counterdiagonal.

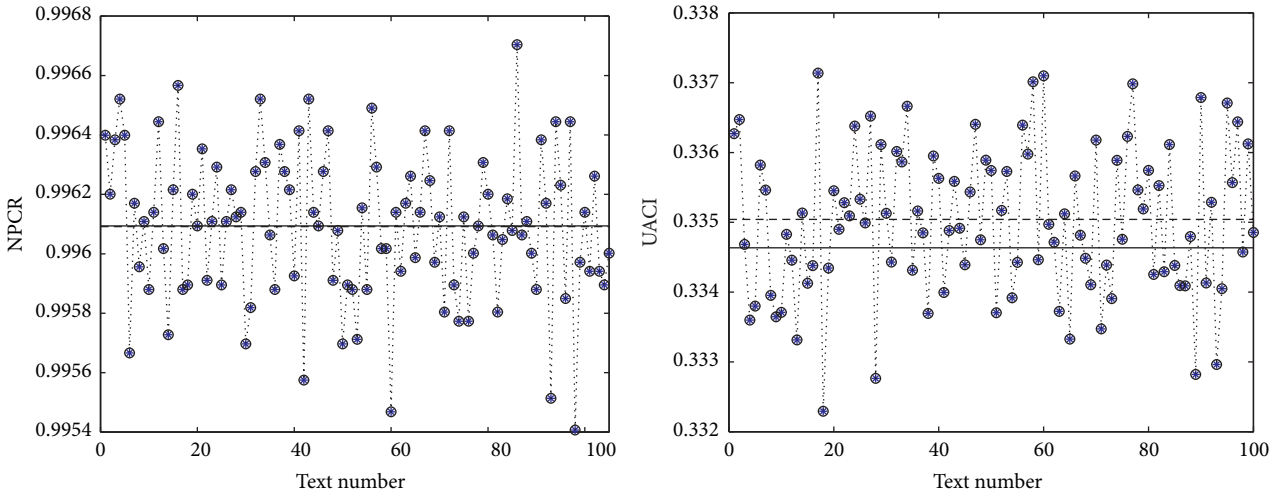
The ideal expectations of NPCR and UACI can be calculated by the following simplified formulas:

$$\begin{aligned} \mathrm{NPCR}_{\mathrm{E}} &= \left(1 - 2^{-n}\right) \times 100\%, \\ \mathrm{UACI}_{\mathrm{E}} &= \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n-1} i\,(i+1)}{2^n - 1} \times 100\% \\ &= \frac{1}{3}\left(1 + 2^{-n}\right) \times 100\%, \end{aligned} \tag{10}$$

where n is the number of bits used to represent the different bit planes of an image. For gray scale image parameter $n = 8$ (8 bits per pixel). Hence expected NPCR and expected UACI are $\mathrm{NPCR}_{\mathrm{E}} = 99.6094\%$ (horizontal solid line in Figure 10(a)) and $\mathrm{UACI}_{\mathrm{E}} = 33.4635\%$ (horizontal solid line in Figure 10(b)), respectively. From the above formula we can see that relation $\mathrm{NPCR}_{\mathrm{E}} + 3\mathrm{UACI}_{\mathrm{E}} = 2$, so any value of the ideal expectations can illustrate the capability of algorithm to attack resisting plaintext.

Table 1: Correlation coefficient of different plain image and cipher image.

Plain image	Horizontal	Vertical	Diagonal	Counterdiagonal
Gray Lena				
Plain image	0.972953	0.970462	0.916925	0.938441
Encrypted image	-4.097226×10^{-5}	1.158832×10^{-4}	4.620716×10^{-5}	4.539076×10^{-4}
Encrypted image [19]	0.000417	−0.002048	−0.001554	
Encrypted image [20]	0.023	0.028	0.023	
Binary image				
Plain image	0.915352	0.922622291	0.868221	0.857255
Encrypted image	-3.811868×10^{-6}	-7.131676×10^{-4}	-9.372164×10^{-4}	-3.496642×10^{-4}
Color parrot				
R				
Plain image	0.945140	0.950725	0.919702	0.937272
Encrypted image	−0.001678	3.514572×10^{-4}	-9.329940×10^{-4}	-4.626904×10^{-5}
G				
Plain image	0.948746	0.941403	0.910118	0.929873
Encrypted image	-8.326210×10^{-4}	-4.626904×10^{-5}	1.484844×10^{-5}	6.479456×10^{-4}
B				
Plain image	0.956960	0.924891	0.924891	0.941023
Encrypted image	-7.902728×10^{-6}	1.1520873×10^{-4}	9.66501×10^{-4}	-1.766560×10^{-4}



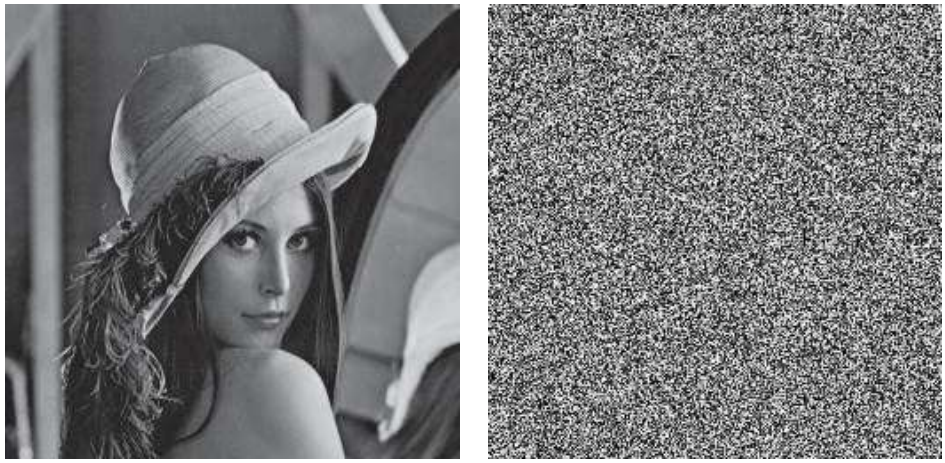
(a) Number of pixels changing rate

(b) Unified average changing intensity

Figure 10: Measured sensitivity of cipher image to plain image.

In this experiment, one hundred groups of Lena images are encrypted. In every group image, one is original image and the other is original image with only one changed pixel value (including border points and intermediate points, each time the changed amount is only 1). Then the test results are shown in Figure 10; every value fluctuates up and down near ideal value. The average values are $\overline{\text{NPCR}} = 99.6091\%$ (horizontal dotted line in Figure 10(a)) and $\overline{\text{UACI}} = 33.5038\%$ (horizontal dotted line in Figure 10(b)), respectively. Obviously the given encryption algorithm greatly improves the sensitivity of plaintext, thereby enhancing capacity of resistance to differential attacks.

4.5. Key Sensitivity Test. Lena gray image is used to make experimental analysis. With right key, the decrypted image is clear and correct without any distortion in Figure 11(a). Decryption using keys with slight mismatch is performed so as to evaluate the key sensitivity. With a subtle change, the new key $q_1 = 1.01000000001$, and the decrypted image is incorrect, proposed in Figure 11(b). Subtle change of key



(a) Decrypted image (b) Error decrypted image

Figure 11: The decrypted Lena image.

yields greatly different decrypted images. It is fully convincing that the algorithm has steady and superior secure performance in the first encryption round and will well resist differential attack.

4.6. Algorithmic Complexity Analyses. The time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the size of the input to the problem. The time complexity is commonly described using the big-O notation, which suppresses multiplicative constants and lower order terms. Time complexity of generating key is $O(M \cdot N)$. The maximum complexity chaos and wavelet function map generate chaos sequences with time complexities $O(T_1^2)$ and $O(T_2^2)$, respectively. Pixel diffusion and substitution have the same time complexity $O(M \cdot N)$. At each step, the worst total time complexity is

$$\begin{aligned} &O(M \times N) + O\left(T_1^2\right) + O\left(T_2^2\right) + O(M \times N) \\ &\quad = O(T), \end{aligned} \tag{11}$$

where $T = \max\{M \cdot N, T_1^2, T_2^2\}$. T_1 and T_2 represent iterate numbers of maximum complexity chaos and wavelet function map, respectively.

5. Conclusion

This paper presents a novel fractional-order complex attractor with high fraction dimension, and the preprocessed chaotic sequence has good random character. Secret key is disturbed by every order and pixel value of plaintext; thus slight change of plaintext can bring vast differentness in encrypted image. Theoretical analysis and experimental results indicate that the encryption algorithm has some good characters, such as resistance for different attack, better information entropy, and low coefficient correlation. Comparing with some chaos-based algorithms, the estimated results demonstrate the strong capabilities and the effectiveness of the proposed algorithm. The time complexity of the algorithm is proposed and an example is investigated to verify its validity and practicability. Our future works will focus on video encryption using fractional-order chaotic system.

Conflicts of Interest

The authors declare that they have no competing interests.

Acknowledgments

This research is supported by NNSFs of China (Grant no. 11501525), Science & Technology Innovation Talents in Universities of Henan Province (Grant no. 16HASTIT040), Teacher Education Curriculum Reform of Henan Province (Grant no. 2017-JSJYYB-190), Project of Youth Backbone Teachers of College and Universities in Henan Province (Grant nos. 2013GGJS-142 and 2015GGJS-179), and Basic & Advanced Technological Research Project of Henan Province (Grant no. 162300410261).

References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1996.

[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.

[3] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '98)*, pp. 514–517, IEEE, Monterey, Calif, USA, June 1998.

[4] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters. A*, vol. 309, no. 1-2, pp. 75–82, 2003.

[6] X. Wang and L. Teng, "An image blocks encryption algorithm based on spatiotemporal chaos," *Nonlinear Dynamics. An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, vol. 67, no. 1, pp. 365–371, 2012.

[7] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[8] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[9] X.-Y. Wang and X.-M. Bao, "A novel block cryptosystem based on the coupled chaotic map lattice," *Nonlinear Dynamics*, vol. 72, no. 4, pp. 707–715, 2013.

[10] G. Jakimoski and L. C. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters. A*, vol. 291, no. 6, pp. 381–384, 2001.

[11] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[12] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 557–566, 2012.

[13] Y. Wang, K.-W. Wong, X. F. Liao, and G. R. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.

[14] A. I. Ismail, A. Mohammed, and D. Hossam, "A digital image encryption algorithm based a composition of two chaotic Wavelet function map," *International Journal of Network Security*, vol. 11, no. 1, pp. 1–10, 2010.

[15] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 38, pp. 5973–5978, 2008.

[16] X.-F. Li, K. E. Chlouverakis, and D.-L. Xu, "Nonlinear dynamics and circuit realization of a new chaotic flow: a variant of Lorenz, Chen and Lü," *Nonlinear Analysis. Real World Applications. An International Multidisciplinary Journal*, vol. 10, no. 4, pp. 2357–2368, 2009.

[17] J. F. Zhao, S. Y. Wang, Y. X. Chang, and X. F. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721–1729, 2015.

[18] X. Wu, H. Wang, and H. Lu, "Modified generalized projective synchronization of a new fractional-order hyperchaotic system and its application to secure communication," *Nonlinear Analysis. Real World Applications*, vol. 13, no. 3, pp. 1441–1450, 2012.

[19] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dynamics*, vol. 82, no. 1-2, pp. 107–117, 2015.

[20] Q. Liu, P.-Y. Li, M.-C. Zhang, Y.-X. Sui, and H.-J. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 506–515, 2015.

[21] W.-B. Yu and X.-P. Wei, "Bifurcation diagram of a wavelet function," *Acta Physica Sinica*, vol. 55, no. 8, pp. 3969–3973, 2006.