A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system*

Wang Zhen(王 震)[a], Huang Xia(黄 霞)[b]†, Li Yu-Xia(李玉霞)[b], and Song Xiao-Na(宋晓娜)[c]

[a] College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China
[b] Key Laboratory of Robotics and Intelligent Technology, College of Information and Electrical Engineering, Shandong University of Science and Technology, Qingdao 266590, China
[c] College of Electronic and Information Engineering, Henan University of Science and Technology, Luoyang 471003, China

(Received 22 April 2012; revised manuscript received 3 August 2012)

We propose a new image encryption algorithm on the basis of the fractional-order hyperchaotic Lorenz system. While in the process of generating a key stream, the system parameters and the derivative order are embedded in the proposed algorithm to enhance the security. Such an algorithm is detailed in terms of security analyses, including correlation analysis, information entropy analysis, run statistic analysis, mean-variance gray value analysis, and key sensitivity analysis. The experimental results demonstrate that the proposed image encryption scheme has the advantages of large key space and high security for practical image encryption.

Keywords: image encryption, fractional order, hyperchaotic Lorenz system

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.1088/1674-1056/22/1/010504

1. Introduction

In the past decade, image encryption has been paid more and more attention owing to the rapid growth of internet and multimedia communications.[1–9] A number of traditional encryption algorithms, such as DES and RSA, have been generally used in data encryption.[10] However, these encryption algorithms may not be so effective due to some intrinsic features of images, such as bulk data capacity, high redundancy, and high correlation of the pixels.[11] As is well known, chaotic systems possess several intrinsic characteristics, e.g., extreme sensitivity to initial conditions, broadband power spectrum, random-like behavior, and tolerance to sufficiently high levels of noise. These traits are favorable to information security and have attracted the attention of cryptographers to develop a variety of novel encryption algorithms. In fact, the fundamental idea of chaos-based encryption could date back to the publication by Shannon,[12] in which the basic stretch-and-fold mechanism of chaos was proposed. Furthermore, the close relationship between chaotic maps and cryptographic algorithms has been discussed in Ref. [13].

Fractional calculus, which deals with derivatives and integrals of arbitrary order, has not been applied in the fields of physics and engineering until recent decades.[14] It has been realized that most systems can be elegantly described with the aid of fractional order, especially in the case of description of memory and hereditary properties of various materials and processes.[15–21] Meanwhile, it has been shown that the chaotic behavior of an integer-order nonlinear system is preserved when the order becomes fractional.[22–24] Compared with its integer-order counterparts, fractional-order nonlinear systems show higher nonlinearity and degrees of freedom in the model. The reason for this lies in the fact that fractional derivatives have complex geometrical interpretation for their nonlocal effects either in space or time.[25]

On the other hand, it is known that the complexity of the attack algorithm is determined by the size of the key space and the complexity of the verification of each key. One advantage of utilizing fractional-order chaotic systems for encryption is for the computational complexity goal. In fact, the fractional-order chaotic systems have a more complexly varying power spectrum, which makes the cryptosystem have the capability of enhancing the security both in frequency and in time domain. Another advantage is that the derivative orders can also be used as secret keys. By adding the derivative order to disguise the portrait of a dynamical system, it is very difficult for an eavesdropper to ascertain the system type. In Ref. [9], Kiani-B *et al*. presented a novel approach to enhance the security of data transmission and to improve the vulnerable points of chaotic masking. It is worth pointing out that it was the first time a fractional-order chaotic system had been employed to illustrate the enhancement of security of a chaotic cryptosystem.

It is obvious that low-dimensional chaotic systems have the advantages of simplicity in form and high-level efficiency in generating chaotic sequences. However, its key space is

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61004078 and 60971022), the Natural Science Foundation of Shandong Province, China (Grant Nos. ZR2009GQ009 and ZR2009GM005), the China Postdoctoral Science Foundation (Grant No. 20100481293), and the Special Funds for Postdoctoral Innovative Projects of Shandong Province, China (Grant No. 201003037).

†Corresponding author. E-mail: huangxia.qd@gmail.com

© 2013 Chinese Physical Society and IOP Publishing Ltd

small and there are many attack methods to decode the information encrypted by this kind of system.[26] Compared with low-dimensional chaotic systems, hyperchaotic systems have more than one positive Lyapunov exponent, and possess more complex dynamical characteristics and higher randomness. Therefore, traditional deciphering algorithms, such as phase-space reconstruction, regression reflection, and nonlinear prediction are difficult to use in deciphering the information encrypted by a hyperchaotic system. Some image encryption schemes based on different hyperchaotic systems have been presented in recent years. We refer the readers to Refs. [27] and [28] and references cited therein for more details. However, it should be noticed that the order of all these involved hyperchaotic systems is integer. To the best of our knowledge, the fractional-order hyperchaotic system has not been employed in image encryption so far.

In consideration of the advantages of the fractional-order system and the hyperchaotic system, this paper addresses a new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. The system parameters and the derivative order are selected as secret keys and embedded in the proposed scheme to enhance the security. The detailed security analyses, including key space analysis, statistical analysis, and sensitivity analysis with respect to the key and plaintext show that the novel image encryption scheme possesses high security for practical image encryption.

2. Algorithm for solving fractional-order differential equations

In this section, the Caputo definition of a fractional-order derivative is introduced, and meanwhile, a modified numerical method for solving fractional-order differential equations (FDEs) is proposed.

Definition[14] The Caputo fractional derivative of order α of a continuous function $f : R^+ \to R$ is defined as follows:

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

where Γ is Γ function, and

$$\Gamma(z) = \int_0^\infty \mathrm{e}^{-t} t^{z-1} \mathrm{d}t, \ \Gamma(z+1) = z\Gamma(z).$$

Due to the nonlocal character of the fractional derivative operator, the numerical methods for solving ODEs have to be modified to cater for solving FDEs.[25] In Ref. [29], Deng improved the predictor–corrector approach proposed by Diethelm *et al*. and attained a more accurate algorithm. Moreover, the new algorithm can reduce half of the computation time. In what follows, we briefly introduce this algorithm.

Consider the FDEs described by

$$\begin{aligned} &D_t^\alpha y(t) = f(t, y(t)), \ a \le t \le b, \\ &y(0) = y_0, \end{aligned} \tag{1}$$

which is equivalent to the Volterra integral equation

$$y(t) = y_0 + \frac{1}{\Gamma(\alpha)} \int_0^t \frac{f(s, y(s))}{(t-s)^{1-\alpha}} \mathrm{d}s. \tag{2}$$

Set $k = t_{j+1} - t_j$ as the step length. Thus, equation (2) can be numerically approximated by

$$y_k(t_{n+1}) = \begin{cases} y_0 + \dfrac{k^\alpha}{\Gamma(\alpha+2)} (f(y_k^{\mathrm{p}}(t_1), t_1) + \alpha f(y_k(t_0), t_0)), & n = 0, \\ y_0 + \dfrac{k^\alpha}{\Gamma(\alpha+2)} (f(y_k^{\mathrm{p}}(t_{n+1}), t_{n+1}) + (2^{\alpha+1} - 2) f(y_k(t_n), t_n)) \\ \quad + \dfrac{k^\alpha}{\Gamma(\alpha+2)} \displaystyle\sum_{j=0}^{n-1} a_{j,n+1} f(y_k(t_j), t_j), & n \ge 1, \end{cases} \tag{3}$$

where the predicted value $y^{\mathrm{p}}(t_{n+1})$ is determined by

$$y_k^{\mathrm{p}}(t_{n+1}) = \begin{cases} y_0 + \dfrac{k^\alpha}{\Gamma(\alpha+1)} f(y_k(t_0), t_0), & n = 0, \\ y_0 + \dfrac{k^\alpha}{\Gamma(\alpha+2)} (2^{\alpha+1} - 1) f(y_k(t_n), t_n) + \dfrac{k^\alpha}{\Gamma(\alpha+2)} \displaystyle\sum_{j=0}^{n-1} a_{j,n+1} f(y_k(t_j), t_j), & n \ge 1, \end{cases} \tag{4}$$

in which

$$a_{j,n+1} = \begin{cases} n^{\alpha+1} - (n-\alpha)(n+1)^\alpha, & j = 0, \\ (n-j+2)^{\alpha+1} + (n-j)^{\alpha+1} - 2(n-j+1)^{\alpha+1}, & 1 \le j \le n, \\ 1, & j = n+1, \end{cases} \tag{5}$$

and

$$b_{j,n+1} = \begin{cases} b_{0,1} = \alpha + 1, & n = 0, \\ \begin{cases} a_{j,n+1}, & 0 \le j \le n-1, \\ 2^{\alpha+1} - 1, & j = n, \end{cases} & n > 0. \end{cases} \tag{6}$$

The estimation error is

$$e = \max |y(t_j) - y_j| = O(k^{\mathrm{p}}), \ j = 0, 1, \ldots, N, \tag{7}$$

where $p = \min(2, 1 + 2\alpha)$. Applying the aforementioned method, numerical solution of a fractional-order system can be determined.

3. Fractional encryption algorithm

In this section, the fractional-order hyperchaotic Lorenz system is presented, and a novel image encryption scheme is described in detail.

3.1. Fractional-order hyperchaotic Lorenz system

The fractional-order hyperchaotic Lorenz system is used in the encryption algorithm, which is described by

$$\begin{cases} D_t^{\alpha_1} x = a(y - x) + w, \\ D_t^{\alpha_2} y = cx - y - xz, \\ D_t^{\alpha_3} z = xy - bz, \\ D_t^{\alpha_4} w = -yz + rw, \end{cases} \tag{8}$$

where α_i $(i = 1, 2, 3, 4)$, a, b, c, and r are system parameters. When $\alpha_i = 0.98$, $a = 10$, $b = 8/3$, $c = 28$, $r = -1$, and the initial values $x_0 = 12$, $y_0 = 22$, $z_0 = 31$, and $w_0 = 4$, the four Lyapunov exponents of system (8) are calculated to be $\lambda_1 = 0.3392$, $\lambda_2 = 0.1577$, $\lambda_3 = 0$, and $\lambda_4 = -15.2624$. As the system has two positive Lyapunov exponents, it is obvious that system (8) exhibits hyperchaotic behavior. The projections of the attractor are shown in Fig. 1.

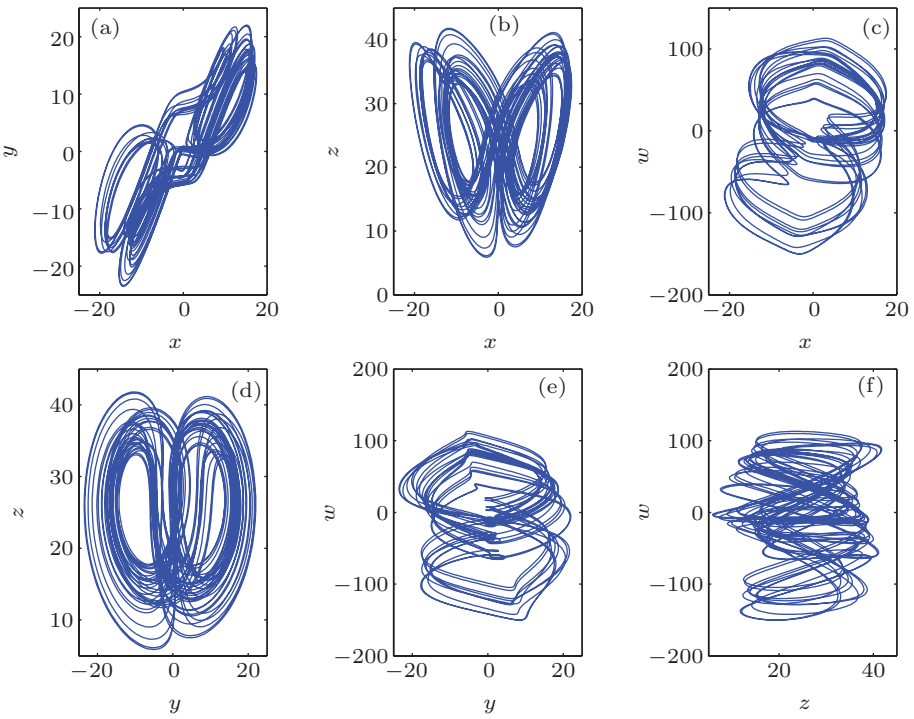


Fig. 1. (color online) Projections of the chaotic attractor of system (8) with $\alpha = 0.98$. (a) x–y, (b) x–z, (c) x–w, (d) y–z, (e) y–w, (f) z–w.

3.2. Description of the encryption/decryption algorithm

Based on the fractional-order hyperchaotic Lorenz system (8), the encryption scheme is then described step by step. The numerical method presented in Section 2 is employed to solve the fractional-order hyperchaotic Lorenz system. In order to enhance the difficulty of deciphering and to resist an exhaustive search, we use the following skill to produce the chaotic sequences. The fractional order α_i varies as follows:

$$\alpha_i = \alpha_{i0} + \frac{0.3k}{\mathrm{ceil}(256 \times 256/1000)}, \tag{9}$$

where α_{i0} is the initialization of the fractional derivative order, and $k = 0, 1, \ldots, \mathrm{ceil}(256 \times 256/1000)$, $\mathrm{ceil}(\cdot)$ denotes the nearest integer towards plus infinity).

It is worth noting that this skill makes the chaotic sequences distribute in different orbits, which can efficiently prevent the decryption by using chaotic synchronization. Now,

we discuss in detail the procedure of the encryption in the proposed cryptosystem.

Step 1 Suppose that $M \times N$ matrix $\boldsymbol{B}$ is the matrix of the original image, and $B_{i,j}$ is the pixel value at the position (i,j), with $i \in [1,M]$ and $j \in [1,N]$. Compute the mean pixel value c of the initial image by

$$c = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} B_{i,j}}{M \times N}.$$

Step 2 The value of α_i is renewed by $\alpha_i + c/1000$, where c is determined in Step 1. The modified algorithm proposed in Section 2 is used to compute the fractional-order system (8). Thus, four chaotic sequences $\{X_n\}$, $\{Y_n\}$, $\{Z_n\}$, and $\{W_n\}$ are produced.

Step 3 For each x_i in the chaotic sequence $\{X_n\}$, let $x_i = \dfrac{|x_i|}{\max(|x_i|)} \times 255$. This makes x_i range from 0 to 255. Create a matrix $\boldsymbol{A}$ with its line being chaotic sequence $\{X_n\}$, that is,

$$A = \begin{bmatrix} x_1 & x_2 & \cdots & x_N \\ x_{N+1} & x_{N+2} & \cdots & x_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ x_{(M-1)N+1} & x_{(M-1)N+2} & \cdots & x_{M\times N} \end{bmatrix}.$$

Step 4 Execute a bitwise exclusive OR operation between the corresponding elements of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ to obtain matrix $\boldsymbol{C}$.

Step 5 Execute an addition operation on chaotic sequences $\{Y_n\}$, $\{Z_n\}$, and $\{W_n\}$ to obtain chaotic sequence $\{U_n\}$. Meanwhile, define Y as the arithmetic sequence $\{1,2,\ldots,M \times N\}$.

Step 6 Rearrange the elements of the $M \times N$ chaotic sequence $\{U_n\}$ in descending order, in order to record the change in position of $\{U_n\}$. Correspondingly, rearrange the arithmetic sequence Y to Y'.

Step 7 According to Y', rearrange the position of the elements of matrix $\boldsymbol{C}$ to $\boldsymbol{D}$, where $\boldsymbol{D}$ is an $M \times N$ matrix that contains the data of the encryption image.

The decryption is the inverse operation of the encryption, which can be performed by the following procedure:

Step 1 Compute the fractional-order system (8) to produce four chaotic sequences denoted by $\{X_n\}$, $\{Y_n\}$, $\{Z_n\}$, and $\{W_n\}$.

Step 2 Execute an addition operation on chaotic sequences $\{Y_n\}$, $\{Z_n\}$, and $\{W_n\}$ to yield chaotic sequence $\{U_n\}$. Meanwhile, define Y as the arithmetic sequence $\{1,2,\ldots,M \times N\}$.

Step 3 Rearrange the elements of the $M \times N$ chaotic sequence $\{U_n\}$ in descending order, in order to record the change in position of $\{U_n\}$. Correspondingly, rearrange the arithmetic sequence Y to Y'.

Step 4 According to Y', rearrange the position of the elements of matrix $\boldsymbol{D}$ to $\boldsymbol{C}$, where $\boldsymbol{C}$ is an $M \times N$ matrix that contains the data of the encryption image.

Step 5 For the chaotic sequence $\{X_n\}$, let $x_i = \dfrac{|x_i|}{\max(|x_i|)} \times 255$. Then, create a matrix $\boldsymbol{A}$ with its line being chaotic sequence $\{X_n\}$.

Step 6 Execute a bitwise exclusive OR operation between the corresponding elements of matrices $\boldsymbol{A}$ and $\boldsymbol{C}$ to obtain matrix $\boldsymbol{B}$, and $\boldsymbol{B}$ is the matrix of the decryption image.

3.3. Experimental results

Now, we provide some experimental results to illustrate the performance of the proposed chaotic cryptosystem. We select the parameters as $a = 10$, $b = 8/3$, $c = 28$, $d = 7$, $r = -1$, $x_0 = 12$, $y_0 = 22$, $z_0 = 31$, $w_0 = 4$, $N = 256 \times 256$, and $\alpha_{i0} = 0.95$. According to the devised algorithm, we encrypt the Cameraman image, and the plain image and the encrypted image are depicted in Fig. 2.

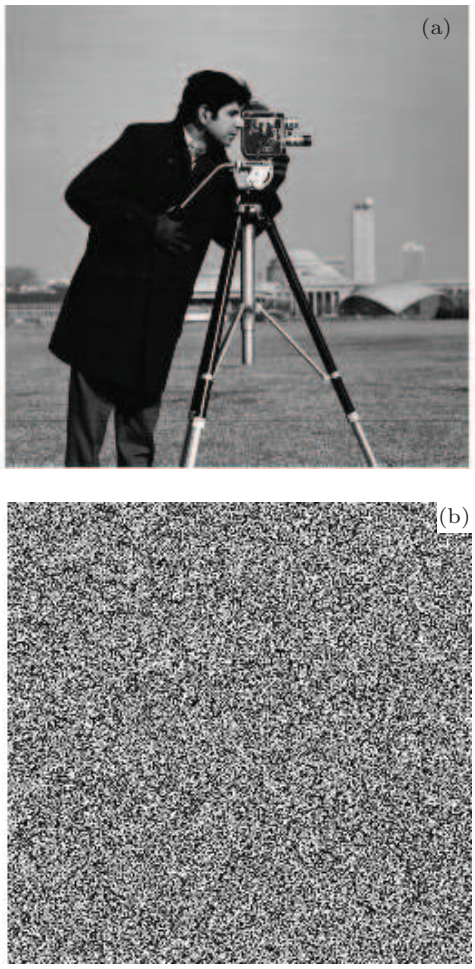


Fig. 2. (a) Plain image; (b) encrypted image.

4. Security analysis

In order to demonstrate that the proposed cryptosystem is secure against most common attacks, detailed security analyses of the proposed image encryption scheme are carried out, including key space analysis, statistical analysis, and sensitivity analysis with respect to the key and plaintext.

4.1. Key space analysis

It is known that key space size is the total number of different keys that can be used in the encryption. A good encryption scheme should be sensitive to the secret keys. In our encryption algorithm, the initial values x_0, y_0, z_0, w_0, and the fractional orders α_i $(i = 1,2,3,4)$ of the hyperchaotic Lorenz system are used as secret keys. If the precision is 10^{-14}, the key space size is 10^{98}. It seems that the size of key space is large enough, compared with Ref. [27], to resist all kinds of brute-force attacks.

4.2. Statistic analysis

4.2.1. Histograms of ciphered image

The original image and the ciphered image are shown in Figs. 3(a) and 3(b), respectively. The histogram of the encrypted image is nearly uniformly distributed, which can well protect the information of the image to withstand the statistical attack.

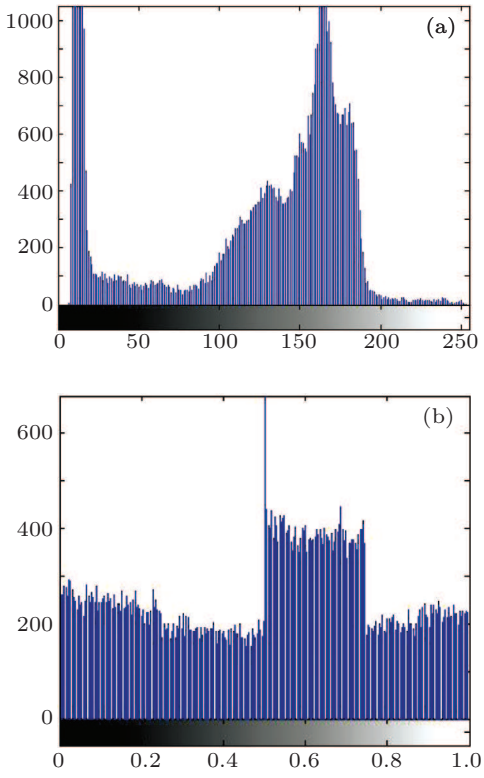


Fig. 3. (color online) (a) Histogram of initial image, (b) histogram of encrypted image.

4.2.2. Correlation of two adjacent pixels

We analyze the correlation between two adjacent pixels along the vertical and horizontal directions in the plain image and its encrypted images. The following formula is adopted

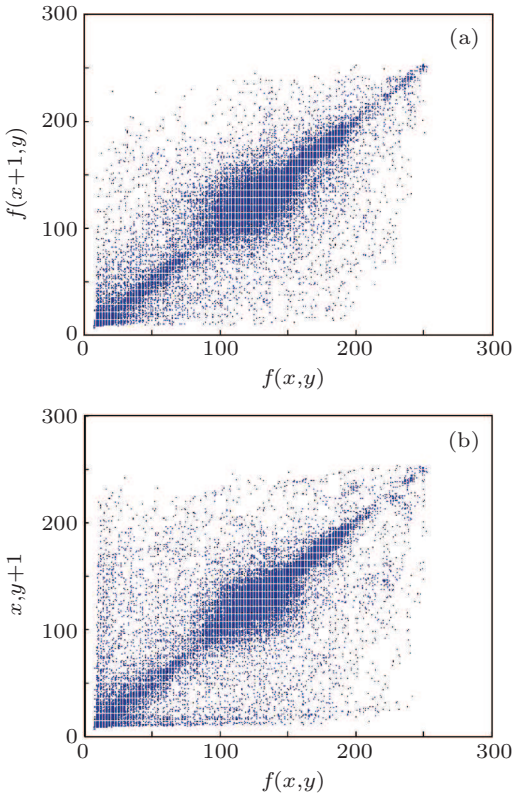


Fig. 4. (color online) Correlation of the plain image: (a) horizontal correlation, (b) vertical correlation.

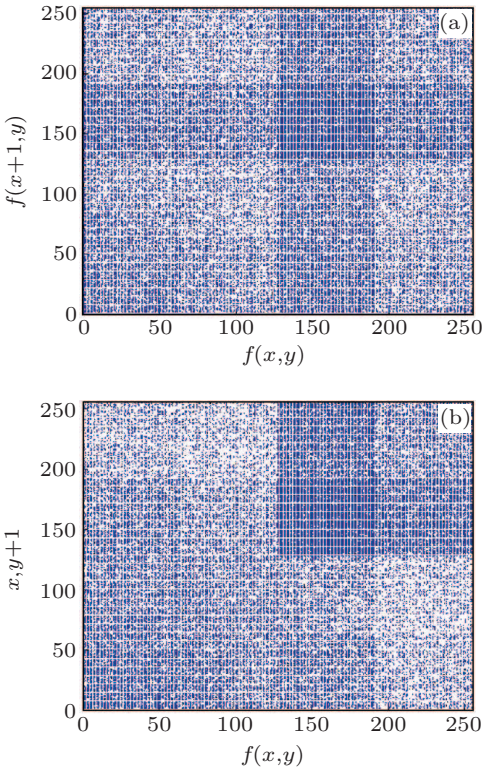


Fig. 5. (color online) Correlation of the encrypted image: (a) horizontal correlation, (b) vertical correlation.

for the purpose of calculation:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i,\quad D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2,$$
$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)),$$
$$\rho_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}},\tag{10}$$

where x and y are the values of two adjacent pixels in the image, and N is the total number of pixels selected from the image. Figures 4 and 5 show the correlation of the plain image and the encrypted image. It can be easily found that the correlation of the initial image is an obvious linear relationship, whereas the correlation of the encrypted image is a stochastic relationship.

4.2.3. Information entropy

The information theory is a mathematical theory copying data communication and storage founded by Shannon. It is well known that the information entropy $H(s)$ of a plaintext message s can be computed by

$$H(s)=\sum_{i=1}^{N}P(s_i)\log_2\frac{1}{P(s_i)},\tag{11}$$

where $P(s_i)$ is the probability of symbol s_i. In fact, given that a real information source seldom transmits random messages, the entropy value of the source is commonly smaller than the ideal one. It has been pointed out in Ref. [32] that when these messages are encrypted, their information entropy should ideally be 8, and if the entropy of such an encrypted message is less than 8, then there will be a predictability which threatens its security. According to Eq. (11), the information entropy for the encrypted image is calculated to be 7.9963, which is very close to the theoretical value of 8.

4.2.4. Run statistic

A new evaluation criterion for the image encryption effect, called the run statistic, is proposed in Ref. [33]. The run statistic can be used in the effect evaluation of the image encryption algorithm based on the image pixel coordinate permutation. The advantages of this criterion lie in the simplicity in expression and convenience in computation. In particular, it is independent of the size of the image. The definition of the run statistic is given by

$$R=\frac{S}{M\times N}=\frac{\sum_{i=1}^{M}S_i}{M\times N},\tag{12}$$

where $M\times N$ is the size of the initial image, and S_i is the number of the run length in line i. The amount of the grayscale S increases with increasing run length statistic. As a result, there will be a severe change in grayscale value in adjacent pixels, that is, the confusion degree of the image is increased. By using the definition (12), the run statistic of the initial image and the encrypted image are calculated to be 0.0886 and 0.3388, respectively.

4.2.5. Mean-variance gray value

The definition of mean-variance gray value is

$$G=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|B_{i,j}-\bar{B}|}{M\times N},\tag{13}$$

where $\bar{B}$ denotes the average of all the gray values of image pixels, and $M\times N$ is the size of the initial image. In general, the larger the mean-variance gray value is, the more uniform the difference of the grayscale between the plain image and the encrypted image should be, and as a consequence, the better the scramble performance will be. The mean-variance gray values of the plain image and the encrypted image are 0.0039 and 60.3210, respectively.

4.3. Key sensitivity analysis

Key sensitivity is an essential property for any good cryptosystem, which ensures the security of the cryptosystem against brute-force attacks. The encrypted image produced by the cryptosystem should be sensitive to the secret key. That is to say, if the attacker uses two slightly different keys to decrypt the same plain image, the two encrypted images should be completely independent of each other. Recall that Fig. 3(a) is encrypted by using the secret keys $x_0=12$, $y_0=22$, $z_0=31$, $w_0=4$, and $\alpha_{i0}=0.95$. Now, we attempt to decrypt the encrypted images (see Fig. 3(b)) with different keys. Given that there is a change in the value of x_0 (e.g., $x_0=12.000001$), which is slightly different from the encryption key, the resultant decrypted image is shown in Fig. 6. Obviously, the

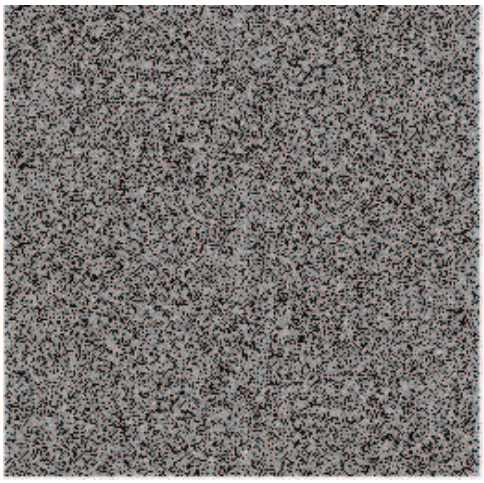


Fig. 6. Decrypted image with a slight change in x_0.

decrypted image produced by using a slightly different key is completely different from the original one in Fig. 3(a). It should be noted that other experimental tests, including individual changes in the value of y_0, z_0, w_0, or q_0 can be implemented in a similar way.

5. Conclusions

In this paper, a novel encryption algorithm to enhance the security of image encryption is presented. For the first time, we implement the fractional-order hyperchaotic Lorenz system in a simple chaotic masking scheme to demonstrate the enhancement of security. The scheme is described in detail, and the security analyses including correlation analysis, information entropy analysis, run statistic analysis, mean-variance gray value analysis, and key sensitivity analysis, are carried out to testify the security of the newly proposed image encryption scheme. The experimental results show that our algorithm has an advantage of high security for practical image encryption.

References

[1] Yu W W and Cao J D 2006 *Phys. Lett.* A **356** 333
[2] Wang K, Pei W J, Zhou J T, Zhang Y F and Zhou S Y 2011 *Acta Phys. Sin.* **60** 070503 (in Chinese)
[3] Wang Z, Huang X, Li N and Song X N 2012 *Chin. Phys.* B **21** 050506
[4] Tang Y, Wang Z D and Fang J A 2010 *Commun. Nonlinear Sci. Numer. Simulat.* **15** 2456
[5] Tong X J and Cui M G 2009 *Signal Processing* **89** 480
[6] Kocarev L and Jakimoski G 2001 *Phys. Lett.* A **289** 199
[7] Yang T, Wu C W and Chua L O 1997 *IEEE Trans. Circuits Syst.* I **44** 469
[8] Wang X Y and Zhao J F 2010 *Neurocomputing* **73** 3224
[9] Kiani-B A, Fallahi K, Pariz N and Leung H 2009 *Commun. Nonlinear Sci. Numer. Simulat.* **14** 863
[10] Schneier B 1996 *Applied Cryptography* (New York: John Wiley & Sons)
[11] Chang C C, Hwang M S and Chen T S 2001 *Journal of System and Software* **58** 83
[12] Shannon C E 1949 *Bell System Technical Journal* **28** 656
[13] Fridrich J 1998 *Int. J. Bifurcat. Chaos* **8** 1259
[14] Podlubny I 1999 *Fractional Differential Equations* (New York: Academic)
[15] Heaviside O 1971 *Electromagnetic Theory* (New York: Chelsea)
[16] Sun H G, Chen W and Chen Y Q 2009 *Physica* A **388** 4586
[17] Sun H G, Chen W, Li C P and Chen Y Q 2010 *Physica* A **389** 2719
[18] Zhang R X and Yang S P 2009 *Acta Phys. Sin.* **58** 2957 (in Chinese)
[19] Zhang R X and Yang S P 2009 *Chin. Phys.* B **18** 3295
[20] Chen Y Q, Ahn H S and Xue D Y 2006 *Signal Processing* **86** 2794
[21] Liu Y and Xie Y 2010 *Acta Phys. Sin.* **59** 2147 (in Chinese)
[22] Yu Y G, Li H X, Wang S and Yu J Z 2009 *Chaos Soliton. Fract.* **42** 1181
[23] Li C P and Chen G R 2004 *Physica* A **341** 55
[24] Lu J G 2005 *Chaos Soliton. Fract.* **26** 1125
[25] Podlubny I 2002 *J. Fract. Calc.* **5** 367
[26] Wang S H, Kuang J Y, Li J H, Luo Y L, Lu H P and Hu G 2002 *Phys. Rev.* E **66** 065202
[27] Gao T G and Chen Z Q 2008 *Phys. Lett.* A **372** 394
[28] Rhouma R and Belghith S 2008 *Phys. Lett.* A **372** 5790
[29] Deng W H 2007 *J. Comput. Appl. Math.* **206** 174
[30] Dadras S and Momeni H R 2010 *Physica* A **389** 2434
[31] Tavazoei M S and Haeri M 2008 *Physica* A **387** 57
[32] Behnia S, Akhshani A, Akhavan A and Mahmpdi H 2009 *Chaos Soliton. Fract.* **40** 505
[33] Zhang X F and Fan J L 2010 *Comput. Sci.* **2** 264 (in Chinese)