Image encryption based on a delayed fractional-order chaotic logistic system*

Wang Zhen(王 震)[a], Huang Xia(黄 霞)[b]†, Li Ning(李 宁)[a], 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 9 October 2011; revised manuscript received 19 December 2011)

A new image encryption scheme is proposed based on a delayed fractional-order chaotic logistic system. In the process of generating a key stream, the time-varying delay and fractional derivative are embedded in the proposed scheme to improve the security. Such a scheme is described in detail with security analyses including correlation analysis, information entropy analysis, run statistic analysis, mean-variance gray value analysis, and key sensitivity analysis. Experimental results show that the newly proposed image encryption scheme possesses high security.

Keywords: image encryption, fractional-order chaotic logistic system, delay

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.1088/1674-1056/21/5/050506

1. Introduction

In recent years, image encryption has drawn more and more attention because of the wide applications of image data over the internet.[1−12] Some traditional encryption algorithms, such as data encryption standard (DES) and River–Shamir–Adleman (RSA), have been generally used in data encryption.[13] However, these encryption algorithms are not so effective owing to some intrinsic features of images, such as bulk data capacity, high redundancy, and high correlation of pixels.[14] Chaotic systems possess several inherent characteristics favorable to information security, including extreme sensitivity to initial conditions and control parameters, broadband power spectrum, random-like behaviour, and tolerance to sufficiently high levels of noise. These characteristics have drawn much attention of cryptographers to develop new encryption algorithms. In fact, the fundamental idea of chaos-based encryption can be traced back to the classical Shannon's paper, in which the basic stretch-and-fold mechanism of chaos was proposed.[15] The close relationship between chaotic maps and cryptographic algorithms has been explored.[16,17]

Fractional calculus, which dates back to the 17th century, has been applied to physics and engineering in recent decades.[18] A fractional-order system is characterized of a dynamical system described by fractional derivatives and integrals. It has been found that most systems can be elegantly described with the help of fractional-order systems, especially the description of memory and hereditary properties of various materials and processes.[19] Meanwhile, it has been shown that the chaotic behaviour of an integer-order nonlinear system is maintained when the order becomes fraction.[20−27] In comparison with their integer-order counterparts, fractional-order nonlinear systems in general show higher nonlinearity and more degrees of freedom in the model due to the existence of fractional derivatives. In fact, fractional derivatives have a complex geometrical interpretation for their nonlocal (or long-range dependence) effects either in space or time.[28]

As is well known, the complexity of an attack algorithm is determined by the size of key space and the complexity of verification of each key. One advantage of fractional-order chaotic systems for encryption is computational complexity goal. Fractional-order chaotic systems have a more complex varying power

*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, and the Special Funds for Postdoctoral Innovative Projects of Shandong Province, China.

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

© 2012 Chinese Physical Society and IOP Publishing Ltd

spectrum, making a cryptosystem enhance the security both in frequency and time domains. Another advantage lies in the fact that derivative orders can be also used as secret keys. By adding a free parameter (i.e., derivative order) to disguise the portrait of a dynamical system, it is very difficult for an eavesdropper to ascertain system type. Kiani-B *et al.* presented a novel approach to enhance the security of data transmission and improve the vulnerable points of chaotic masking.[12] In fact, it was the first time that a fractional-order chaotic system was used to illustrate the enhancement of security of a chaotic cryptosystem. In addition, one-dimensional chaotic maps have the advantages of simplicity and high-level efficiency, and are generally considered as a good candidates for image encryption.[6,7]

Time delay is ubiquitous in the real world. It has been known that the introduction of time delay enriches the dynamics of models, and causes complex dynamics such as periodic, quasi-periodic, and chaotic motions in fractional-order systems.[29] A delayed fractional-order chaotic system exhibits remarkably strong nonlinear characteristics and is expected to greatly enhance the security of a cryptosystem. However, to the best of our knowledge, the delayed fractional-order chaotic system has not been employed in encryption so far. Although extracting information masked by the chaotic signal of a time-delayed system has been considered,[30] the order of the involved delayed chaotic system is integer.

Motivated by the above-mentioned reasons, this paper proposes a new image encryption scheme based on a delayed fractional-order logistic system. The time-varying delay and fractional order are selected as secret keys and embedded in the proposed scheme to enhance the security. Detailed security analyses, including correlation analysis, information entropy analysis, run statistic analysis, mean-variance gray value analysis, and key sensitivity analysis, indicate that the novel image encryption scheme possesses high security.

2. Basic definition and preliminary

There are several different definitions of fractional integration and differential so far.[18] The most frequently used are the Grünwald–Letnikov (G–L) definition, the Riemann–Liuville (R–L) definition, and the Caputo definition. For a wide class of functions, the G–L and R–L definitions are equivalent. In this paper, the G–L definition is used.

Definition[18] The Grünwald–Letnikov fractional derivative of function $y(t)$ of order α is defined as follows:

$$ {}_a\mathrm{D}_t^{\alpha} y(t) = \lim_{h\to 0} \frac{1}{h^{\alpha}} \sum_{j=0}^{[\frac{t-a}{h}]} (-1)^j \binom{\alpha}{j} y(t-jh), $$

where $[\cdot]$ denotes the integer part, $\alpha \in \mathbb{R}$ is the order of derivative, a and t are the bounds of operation ${}_a\mathrm{D}_t^{\alpha}$, and h is the sampling time.

Due to the nonlocal characteristic of the fractional derivative operator, the numerical methods of solving ordinary differential equations have to be modified to cater for fractional differential equations (FDEs).[28] We have proposed a numerical scheme to solve the delayed FDEs.[31] The method is briefly introduced below.

Consider the following delayed FDE:

$$ \begin{aligned} &{}_a\mathrm{D}_t^{\alpha} y(t) = f(t, y(t), y(t-\tau)), \\ &a \le t \le b, \quad m-1 < \alpha \le m, \\ &y(t) = \varphi(t), \quad t \le a, \end{aligned} \tag{1} $$

where α is the order of the differential equation, $\varphi(t)$ is the initial value, τ is the time-varying delay and m is an integer.

Supposing $(m+\delta)h = \tau$, $0 \le \delta < 1$, $h = T/N$, $t_n = nh$, and $n = 1, 2, \cdots, N$, the iteration algorithm can be constructed as follows:

$$ y_n^{(l)} = \frac{1}{\omega_0^{\alpha}} [h^{\alpha} f(t_n, y_n^{(l-1)}, v_n^{(l-1)}) - \sum_{j=1}^{n} \omega_j^{(\alpha)} y_{n-j}], \tag{2} $$

$$ v_n^{(l-1)} = \begin{cases} (1-\delta) y_{n-m} + \delta y_{n-m-1}, & (n > m,\ m > 0), \\ (1-\delta) y_{n-m}^{(l-1)} + \delta y_{m-1}, & (n > m,\ m = 0), \\ \varphi(t_n - \tau), & (n \le m), \end{cases} \tag{3} $$

$$ y_0 = \varphi(a),\ y_n^{(0)} = 1, \tag{4} $$

where $l = 1, 2, \ldots$ is the iteration number, and

$$\omega_j^{(\alpha)} = \frac{1}{2\pi \mathrm{i}} \int\limits_{|x|\leq 1} \frac{W_2(x)}{x^{j+1}} \mathrm{d}x$$
$$= \frac{1}{2\pi} \int\limits_0^{2\pi} W_2(\mathrm{e}^{-\mathrm{i}\phi}) \mathrm{e}^{j\mathrm{i}\phi} \mathrm{d}\phi, \quad (5)$$

where

$$W_2(x) = \left(\frac{3}{2} - 2x + \frac{x^2}{2}\right)^{\alpha}.$$

If $|y_n^{(l)} - y_n^{(l-1)}| < \varepsilon$ ($\varepsilon = 10^{-6}$ is the given error), we need to consider y_n as $y_n^{(l)}$.

It has been proved that the approximation error of this algorithm is $O(h^{2+\alpha})$.[31] In this paper, the above-mentioned algorithm is employed as the numerical method to calculate the delayed FDE.

3. Fractional encryption algorithm

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

3.1. The delayed fractional-order chaotic logistic system

The delayed fractional-order logistic system can be described by

$${}_a\mathrm{D}_t^{\alpha} y(t) = -ay(t) + ry(t-\tau)(1 - y(t-\tau)), \quad (6)$$

where $y(t)$ is the state variable, q ($0 < q < 1$) is the derivative order, a and r are constant scalars. It has been shown that system (6) can exhibit chaotic phenomenon,[32] and Fig. 1 shows its chaotic attractor.

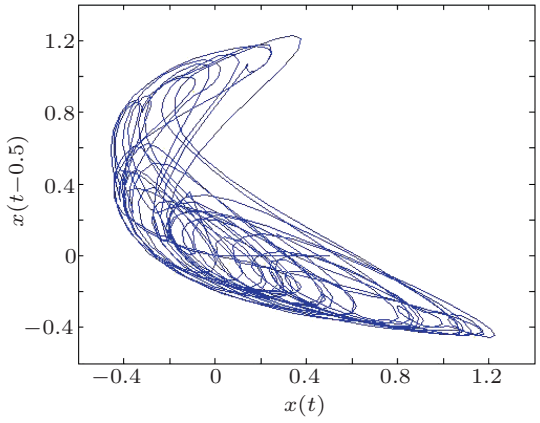


Fig. 1. (colour online) The chaotic attractor of the delayed fractional-order logistic system with $r = -53$ and $q = 0.95$.

3.2. Description of the encryption algorithm

In this subsection, we will give the encryption scheme based on the delayed fractional-order chaotic logistic system.(6) We employ the numerical method presented in Section 2 to solve the delayed chaotic system. The time step size $h = (a - b)/N$, where N is a variable and selected as one of the secret keys. In order to integrate the information of the initial image into the encryption algorithm, we select the initial function as follows:

$$\varphi(t) = \sum_{i=1}^{256} \sum_{j=1}^{256} \boldsymbol{B}(i,j)/256^3, \quad (7)$$

where $\boldsymbol{B}(i,j)$ is the matrix of the original image.

Most scrambling technologies use chaotic sequences created by some specified chaotic systems to build the scrambling address code. Supposing that the secret key is accurate at the Nth significant digit, then in the interval [0, 1], there are $K = 10^N + 1$ points at most without repeating. When the iteration time is greater than K, there will be a cycle in the algorithm. In order to avoid this situation, enhance the difficulty of deciphering and resist exhaustive search, we employ the following technique to produce chaotic sequences.

1) In the produce of every M chaotic sequence, the fractional derivative q is modified as follows:

$$q = q_0 + \frac{0.3 \times k}{\mathrm{ceil}(256 \times 256/1000)}, \quad (8)$$

where $k = 0, 1, \cdots, \mathrm{ceil}(256 \times 256/1000) - 1$, $\mathrm{ceil}(\cdot)$ denotes the nearest integer towards $+\infty$.

2) Meanwhile, for a given time delay τ, a perturbation is added to τ in every M chaotic sequence, that is, $\tau = \tau_0 + \tau_0 \sin(t)$.

It is worth noting that this technique makes chaotic sequences distribute in different orbits, which can prevent decryption by using chaotic synchronization. In particular, cycling in the algorithm can greatly enhance the encryption speed.

Now, we discuss in detail the procedure of encryption and decryption in the proposed cryptosystem.

Step 1 Select the parameters τ, q, N, and the initial value y_0.

Step 2 Use the delayed fractional-order logistic system to produce an $M \times N$ chaotic sequence $k_1, k_2, \ldots, k_{M\times N}$. In accordance with this sequence, construct an arithmetic sequence $Y : 1, \ldots, M \times N$.

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

Step 4 According to Y', rearrange the matrix B to Z, where Z is an $M \times N$ matrix containing the data of encryption image.

A block diagram, as shown in Fig. 2, illustrates the complete procedure of the proposed scheme for encryption/decryption.

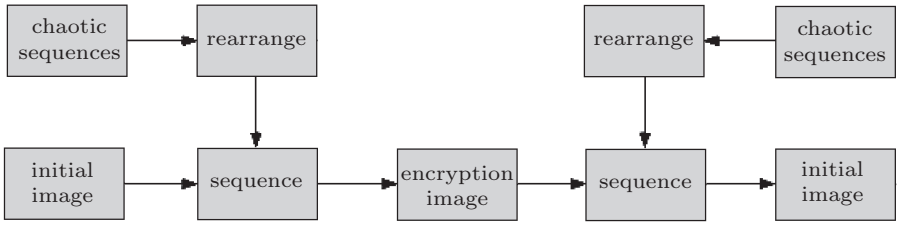


Fig. 2. Block diagram of the proposed scheme for encryption/decryption.

3.3. Experimental results

In this subsection, we provide some experimental results to illustrate the performance of the proposed chaotic cryptosystem. We set the parameters as $y_0 = 0.5$, $\tau = 0.5+0.5\sin(t)$, $N = 1000$, and $q_0 = 0.92$. According to the devised algorithm proposed in Section 3.2, we encrypt the Cameraman image. The plain image and its encrypted image are depicted in Fig. 3, respectively.

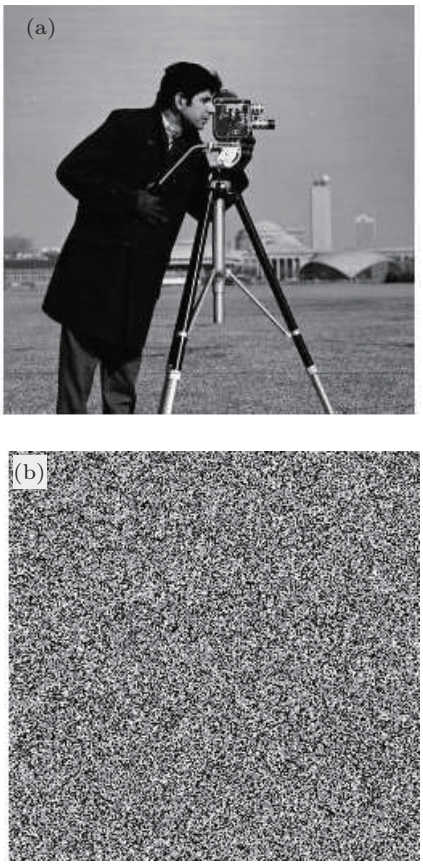


Fig. 3. (a) Plain image, (b) encrypted image.

4. Security analysis

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

4.1. Statistic analysis

Correlation of two adjacent pixels We analyse the correlation between two vertically and horizontally adjacent pixels in the plain image and its encrypted images. For the purpose of calculation, we use the following formula:

$$
\begin{aligned}
&E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,\\
&\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),\\
&\rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}},
\end{aligned}
\tag{9}
$$

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 between the plain image and its 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.

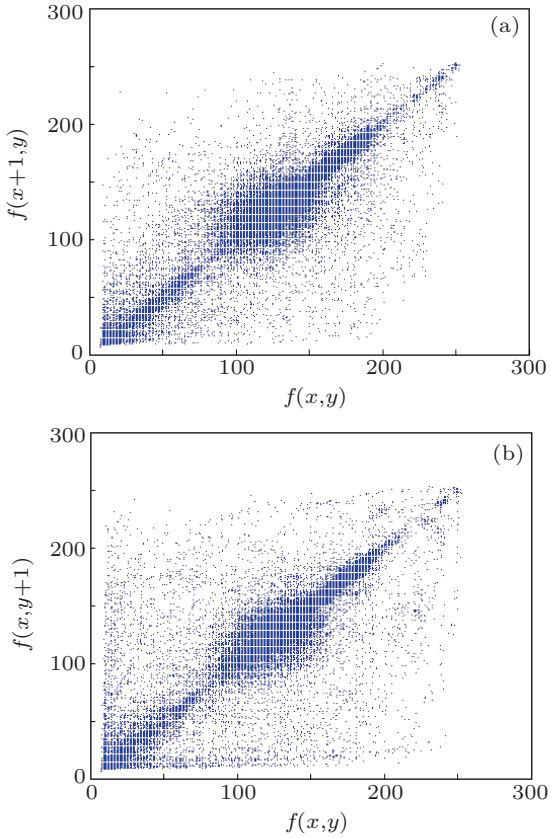


Fig. 4. (colour online) (a) The horizontal and (b) vertical correlations of the plain image.

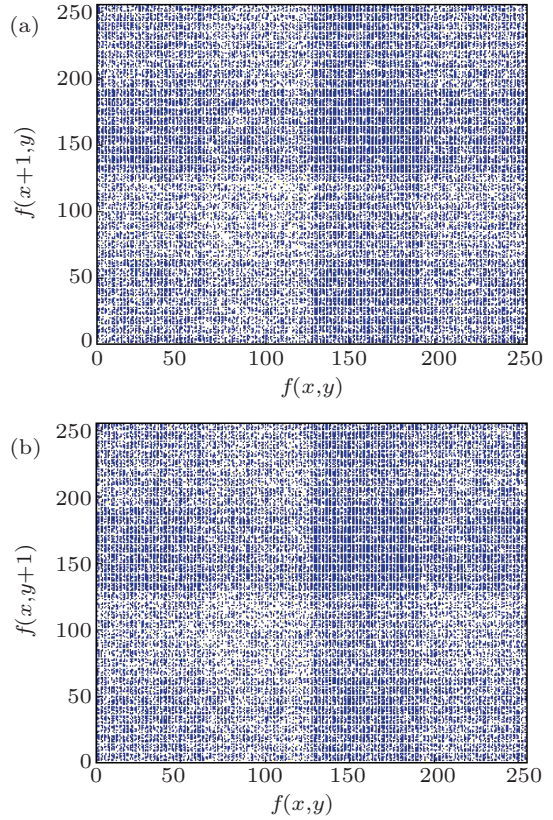


Fig. 5. (colour online) (a) The horizontal and (b) vertical correlations of the encrypted image.

Information entropy Information theory is a mathematical theory of data communication and storage founded by Shannon. It is well known that the information entropy $H(s)$ of a plaintext message s can be calculated as follows:

$$H(s) = \sum_{i=1}^{N} P(s_i) \log_2 \frac{1}{P(s_i)}, \tag{10}$$

where $P(s_i)$ is the probability of symbol s_i. Given that a real information source seldom transmits random messages, in general, the entropy value of the source is smaller than the ideal one. However, when these messages are encrypted, their information entropy should ideally be 8. If the entropy of such an encrypted message is smaller than 8, then there will be a predictability, which threatens its security.[33] According to Eq. (10), we compute the information entropy for the encrypted image, i.e., 7.9702, which is very close to the theoretical value of 8.

Run statistic A new evaluation criterion for the image encryption effect is proposed, that is, the run statistic.[34] The run statistic can be used in the effect evaluation of image encryption algorithm based on the image pixel coordinate permutation. This criterion is simple in expression and convenient in computation. In particular, it is independent of the image size. The definition of the run statistic is given as follows:

$$R = \frac{n^{\mathrm{R}}}{M \times N} = \frac{\sum\limits_{i=1}^{M} n_i^{\mathrm{R}}}{M \times N}, \tag{11}$$

where $M \times N$ is the size of the initial image, and n_i^{R} is the number of the run length in line i. When the run length statistic increases, it indicates that the number of the grayscale increases. Correspondingly, there will be a severe change in grayscale value in adjacent pixels, that is, the confusion degree of the image increases. By definition, the run statistics of the plain image and its encrypted image are calculated to be 0.0884 and 0.4561, respectively.

Mean-variance gray value The definition of mean-variance gray value is as follows:

$$G = \frac{\sum\limits_{i=1}^{M} \sum\limits_{j=1}^{N} |\boldsymbol{B}(i,j) - a_{\mathrm{g}}|}{M \times N}, \tag{12}$$

where a_{g} 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 its encrypted image is, and

thus the better the scramble performance will be. The mean-variance gray values of the plain image and its encrypted image are 0.0039 and 52.8358, respectively.

4.2. 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 secret keys. In other words, 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. Figure 3(a) is encrypted by using the secret keys $y_0 = 0.5$, $\tau = 0.5 + 0.5\sin(t)$, $N = 1000$, $q_0 = 0.92$. We try to decrypt the encrypted images using different keys. Given that there is a change of the value of y_0, e.g., $y_0 = 0.500001$, which is slightly different from the encryption key, the resultant decrypted image is shown in Fig. 6. Obviously, the decrypted image using a slightly different key is completely different from that in Fig. 3(a). It should be noted that other experimental tests including individual change of τ, N, or q_0 can be implemented in a similar way.

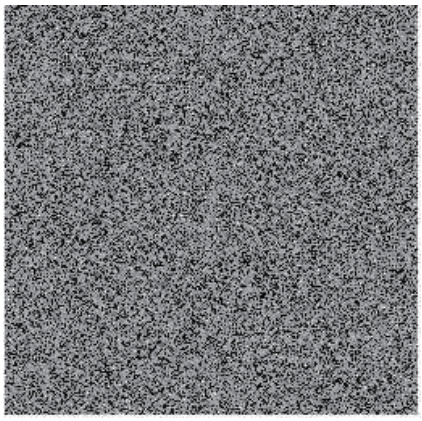


Fig. 6. Decrypted image when there is a slight change of y_0.

5. Conclusion

In this paper, a novel approach to enhance the security of image encryption is presented. For the first time, we implement the delayed fractional-order chaotic logistic system in a simple chaotic masking method to illustrate the security enhancement. The scheme is described in detail. 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 the novel image encryption scheme possesses high security.

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] Tang Y, Wang Z D and Fang J A 2010 *Commun. Nonlinear Sci. Numer. Simulat.* **15** 2456
[4] Tong X J and Cui M G 2009 *Signal Process.* **89** 480
[5] Pareek N K, Patidar V and Sud K K 2006 *Image Vision Comput.* **24** 926
[6] Kocarev L and Jakimoski G 2001 *Phys. Lett.* A **289** 199
[7] Pareek N K, Patidar V and Sud K K 2005 *Commun. Nonlinear Sci. Numer. Simulat.* **10** 715
[8] Yang T, Wu C W and Chua L O 1997 *IEEE Trans. Circuits Syst.* I **44** 469
[9] Alvarez G and Li S 2009 *Commun. Nonlinear Sci. Numer. Simulat.* **14** 3743
[10] Wang X Y and Zhao J F 2010 *Neurocomputing* **73** 3224
[11] Akhshani A, Behnia S, Akhavan A, Hassan H A and Hassan Z 2010 *Opt. Commun.* **283** 3259
[12] Kiani-B A, Fallahi K, Pariz N and Leung H 2009 *Commun. Nonlinear Sci. Numer. Simulat.* **14** 863
[13] Schneier B 1996 *Applied Cryptography* (New York: John Wiley & Sons)
[14] Chang C C, Hwang M S and Chen T S 2001 *J. Syst. Software* **58** 83
[15] Shannon C E 1949 *Bell System Technical J.* **28** 656
[16] Fridrich J 1998 *Int. J. Bifurcation and Chaos* **8** 1259
[17] Kocarev L 2001 *IEEE Cir. Syst. Mag.* **1** 6
[18] Podlubny I 1999 *Fractional Differential Equations* (New York: Academic)
[19] Heaviside O 1971 *Electromagnetic Theory* (New York: Chelsea)
[20] Hartley T T, Lorenzo C F and Qammer H K 1995 *IEEE Trans. Circuits Syst.* I **42** 485
[21] Zhang R X and Yang S P 2009 *Acta Phys. Sin.* **58** 2957 (in Chinese)
[22] Zhang R X and Yang S P 2009 *Chin. Phys.* B **18** 3295
[23] Liu Y and Xie Y 2010 *Acta Phys. Sin.* **59** 2147 (in Chinese)
[24] Yu Y G, Li H X, Wang S and Yu J Z 2009 *Chaos Soliton. Fract.* **42** 1181
[25] Li C P and Chen G R 2004 *Physica* A **341** 55
[26] Varsha D and Sachin B 2010 *Comput. Math. Appl.* **59** 1117
[27] Lu J G 2005 *Chaos Soliton. Fract.* **26** 1125
[28] Podlubny I 2002 *J. Fract. Calc.* **5** 367
[29] Wang Z, Huang X and Shi G D 2011 *Comput. Math. Appl.* **62** 1531
[30] Ponomarenko V I and Prokhorov M D 2002 *Phys. Rev.* E **66** 026215
[31] Wang Z and Huang X 2012 *Applied Mathematics & Information Science* (accepted)
[32] Wang D P and Yu J B 2008 *J. Electron. Sci. Tech.* **6** 289
[33] Behnia S, Akhshani A, Akhavan A and Mahmpdi H 2009 *Chaos Soliton. Fract.* **40** 505
[34] Zhang X F and Fan J L 2010 *Comput. Sci.* **2** 264 (in Chinese)