Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 567898, 10 pages
http://dx.doi.org/10.1155/2014/567898

Research Article

Modified Projective Synchronization between Different Fractional-Order Systems Based on Open-Plus-Closed-Loop Control and Its Application in Image Encryption

Hongjuan Liu,[1,2] Zhiliang Zhu,[1] Hai Yu,[1] and Qian Zhu[1,2]

[1] *Software College, Northeastern University, Shenyang 110819, China*
[2] *School of Information Science & Engineering, Northeastern University, Shenyang 110819, China*

Correspondence should be addressed to Hongjuan Liu; liuhongjuan0125@163.com

Received 27 November 2013; Accepted 13 February 2014; Published 27 March 2014

Academic Editor: Riccardo Caponetto

Copyright © 2014 Hongjuan Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A new general and systematic coupling scheme is developed to achieve the modified projective synchronization (MPS) of different fractional-order systems under parameter mismatch via the Open-Plus-Closed-Loop (OPCL) control. Based on the stability theorem of linear fractional-order systems, some sufficient conditions for MPS are proposed. Two groups of numerical simulations on the incommensurate fraction-order system and commensurate fraction-order system are presented to justify the theoretical analysis. Due to the unpredictability of the scale factors and the use of fractional-order systems, the chaotic data from the MPS is selected to encrypt a plain image to obtain higher security. Simulation results show that our method is efficient with a large key space, high sensitivity to encryption keys, resistance to attack of differential attacks, and statistical analysis.

1. Introduction

Fractional calculus, which is a mathematical topic with more than 300-year history, was not applied to physics and engineering until recent decades. A fractional-order system is characterized as a dynamical system described by fractional derivatives and integrals. It is demonstrated that some fractional-order differential systems behave chaotically or hyperchaotically, such as the fractional-order Lorenz system [1], fractional-order Lü system [2], fractional-order Rössler system [3], and fractional-order Arneodo system [4]. Recently, the control and synchronization of the fractional-order chaotic systems start to attract a great deal of attention due to their potential applications in secure communication and control processing. Some approaches have been proposed to achieve chaos synchronization between fractional-order chaotic systems, such as adaptive control [5], a scalar transmitted signal method [6], sliding mode control [7], and fuzzy logic constant control [8].

Other than the above studies, the Open-Plus-Closed-Loop (OPCL) control method is a more general and physically realizable coupling scheme that can provide stable synchronization in identical and mismatched oscillators [9, 10]. The advantage of the OPCL coupling includes the following two aspects. First of all, OPCL coupling provides synchronization in all systems without restrictions on the symmetry class of a dynamical system. Secondly, in the synchronization regimes, the OPCL coupling can realize stable amplification or attenuation in identical and mismatched systems. Until now, many researchers have achieved their synchronization scenarios for integer-order or fractional-order systems through OPCL control [11–13]. It should be noted that most of the existing works focus on synchronization between identical chaotic systems. However, in practice applications, most systems are nonidentical and parameter mismatches are inevitable because of noise or other uncertain factors. Our coupling strategies need to be formulated to ensure stable synchronization in the presence of mismatch. As a matter of fact, OPCL control can be utilized to achieve synchronization of fractional-order chaotic systems with different structure.

Specially, we will realize modified projective synchronization (MPS) of two different fractional-order systems with parameter mismatches. In MPS, the states of the drive and response systems synchronize up to a constant scaling matrix

with the complete synchronization, antisynchronization, and projective synchronization as the special cases. Based on the OPCL control, a general coupling method is proposed for MPS of two nonidentical fractional-order systems. The proposed coupling scheme is theoretically proved based on stability theory of linear fractional differential equations and its effectiveness is verified by two groups of numerical simulations. Finally, based on the realized MPS, an image encryption scheme with diffusion and confusion is designed. Both the unpredictability of scaling matrix and the use of fractional-order systems will raise the security level of the encryption scheme. According to the analysis of simulations, really satisfactory results are obtained, with large key space, high sensitivity to initial conditions, and high security.

2. The MPS through OPCL Coupling

2.1. Theory Analysis. There are several definitions of fractional derivatives. The Caputo derivative is more popular in the real applications, because the inhomogeneous initial conditions are allowed, if such conditions are necessary. The Caputo definition of the fractional derivative [15], which sometimes is called smooth fractional derivative, is defined as

$$\frac{d^q f(t)}{dt^q} \equiv D^q f(t) = \frac{1}{\Gamma(m-q)} \int_0^t (t-\tau)^{m-q-1} f^{(m)}(\tau)\, d\tau, \tag{1}$$

where m is the smallest integer larger than q, D^q denotes the Caputo definition of the fractional derivative, $f^{(m)}(t)$ is the m-order derivative in the usual sense, and Γ stands for gamma function.

As to the fractional-order chaotic systems, we will briefly describe how to synchronize two different systems via the OPCL coupling method. Assume the fractional-order chaotic system in the drive part is as follows:

$$D^q x = f(x) + \Delta f(x), \tag{2}$$

where $x \in R^n$, $f : R^n \to R^n$ is a continuous vector function, and $\Delta f(x)$ contains mismatch parameters. If the system parameters are not disturbed in the theory, we set zero to the value of $\Delta f(x)$. $q = (q_1, q_2, \ldots, q_n)^T$ for $0 < q_i < 1$ $(i = 1, 2, \ldots, n)$ is the order of fractional-order system. If $q_1 = q_2 = \cdots = q_n$, we call the system (2) a commensurate fractional-order system, otherwise an incommensurate fractional-order system [16].

Then, the controlled response system is constructed as

$$D^q y = g(y) + u(t), \tag{3}$$

where $y \in R^n$, $g : R^n \to R^n$ is a continuous vector function, and $u(t)$ is the controller to be designed.

Definition 1 (MPS). For the drive system (2) and controlled response system (3), it is said to be modified projective synchronization (MPS), if there exists a constant matrix $k = \mathrm{diag}(k_1, k_2, \ldots, k_n)$, such that $\lim_{t\to+\infty}\|e\| = \lim_{t\to+\infty}\|y - kx\| = 0$.

Remark 2. Due to the vector function $f \neq g$, the systems (2) and (3) are nonidentical chaotic systems.

Remark 3. Complete synchronization, antisynchronization, and projective synchronization are the special cases of MPS, where $k_1 = k_2 = \cdots = k_n = 1$, $k_1 = k_2 = \cdots = k_n = -1$, and $k_1 = k_2 = \cdots = k_n$, respectively.

According to the OPCL control [9, 10], we design the controller $u(t)$ as in the form of

$$u(t) = D^q kx - g(kx) + \big(H - Jg(kx)\big)\big(y - kx\big), \tag{4}$$

where $J = \partial/\partial(kx)$ is the Jacobian matrix of the dynamic system and $H \in (n \times n)$ is an arbitrary constant matrix. Then, $g(y)$ can be written, using the Taylor series expansion, by

$$g(y) = g(kx) + Jg(kx)\big(y - kx\big) + \cdots. \tag{5}$$

Keeping the first order terms in (5) and putting (5) and (4) into (3), the error dynamics between systems (2) and (3) is then obtained to be

$$D^q e = D^q y - D^q kx = H\big(y - kx\big) = He. \tag{6}$$

In order to research the synchronization stability of the two incommensurate or two commensurate fractional-order systems by OPCL coupling, we provide the following two theorems.

Theorem 4 (see [17]). *Consider incommensurate fractional-order dynamical system $D^q x(t) = Ax(t)$ with $q = (q_1, q_2, \ldots, q_n)^T$, $0 < q_i < 1$, $(i = 1, 2, \ldots, n)$, $x \in R^n$, and $A \in R^{n\times n}$. Set M to be the lowest common multiple of the denominators u_i of q_i, where $q_i = v_i/u_i$ and $\gcd(u_i, v_i) = 1$. The zero solution of the system is asymptotically stable if all roots λ of the equation $\Delta(\lambda) = \det(\mathrm{diag}(\lambda^{Mq_1}, \lambda^{Mq_2}, \ldots, \lambda^{Mq_n}) - A) = 0$ satisfy the condition $|\arg(\lambda)| > \pi/2M$.*

Theorem 5 (see [18]). *For commensurate fractional-order dynamical system $D^q x(t) = Ax(t)$ with $0 < q < 1$, $x \in R^n$, and $A \in R^{n\times n}$, the system is asymptotically stable if and only if $|\arg(\lambda)| > q\pi/2$ is satisfied for all eigenvalues λ of A. Also, this system is stable if and only if $|\arg(\lambda)| \geq q\pi/2$ is satisfied for all eigenvalues λ of A with those critical eigenvalues satisfying $|\arg(\lambda)| = q\pi/2$ having geometric multiplicity of one.*

From the two theorems, we can easily obtain the following two corollaries.

Corollary 6. *When system* (2) *and system* (3) *are incommensurate fractional-order systems, set M as the lowest common multiple of the denominators u_i of q_i, where $q_i = v_i/u_i$, $\gcd(u_i, v_i) = 1$. The zero solution of the error system* (6) *is asymptotically stable if all roots λ of the equation $\Delta(\lambda) = \det(\mathrm{diag}(\lambda^{Mq_1}, \lambda^{Mq_2}, \ldots, \lambda^{Mq_n}) - H) = 0$ satisfy the condition $|\arg(\lambda)| > \pi/2M$.*

Corollary 7. *When system* (2) *and system* (3) *are commensurate fractional-order systems, the error system* (6) *is asymptotically stable if and only if $|\arg(\lambda)| > q\pi/2$ is satisfied for all eigenvalues λ of H.*

Remark 8. According to the original OPCL control method [9, 10], the control matrix H can be designed as simple as possible as long as the condition $|\arg(\lambda)| > q\pi/2$ or $|\arg(\lambda)| > \pi/2M$ holds. For example, when $[Jg(kx)]_{ij}$ is a constant, we then set $H_{ij} = [Jg(kx)]_{ij}$ such that $[H - Jg(kx)]_{ij} = 0$. When $[Jg(kx)]_{ij}$ is a variable, we choose $H_{ij} = p_{ij}$, where p_{ij} are control parameters.

2.2. Numerical Method for Solving Fractional-Order Systems. An efficient method for solving fractional-order differential equations is the improved predictor-corrector algorithm [19], which will be used in numerical simulation section. The algorithm can be interpreted as a fractional variant of the classical second-order Adams-Bashforth-Moulton method.

Consider the following differential equation:

$$D_t^q x(t) = f(t, x(t)), \quad 0 \le t \le T. \tag{7}$$

The initial values are $x^{(k)}(0) = x_0^{(k)}$, $k = 0, 1, \ldots, m-1$, and $m = [q]$. It is equivalent to the Volterra integral equation. Consider

$$x(t) = \sum_{k=0}^{m-1} x_0^{(k)} \frac{t^k}{k!} + \frac{1}{\Gamma(q)} \int_0^t (t-\tau)^{q-1} f(\tau, x(\tau))\, d\tau. \tag{8}$$

Set $h = T/N, t_n = nh, n = 0, 1, \ldots, N \in Z^+$. Then, (8) can be discretized as follows:

$$\begin{aligned} x_h(t_{n+1}) &= \sum_{k=0}^{m-1} x_0^{(k)} \frac{t_{n+1}^k}{k!} + \frac{h^q}{\Gamma(q+2)} f\left(t_{n+1}, x_h^q(t_{n+1})\right) \\ &\quad + \frac{h^q}{\Gamma(q+2)} \sum_{j=0}^{n} a_{j,n+1} f\left(t_j, x_h(t_j)\right), \end{aligned} \tag{9}$$

where,

$$a_{j,n+1} = \begin{cases} n^{q+1} - (n-\alpha)(n+1)^q, & j = 0 \\ (n-j+2)^{q+1} + (n-j)^{q+1} - 2(n-j+1)^{q+1}, & 1 \le j \le n \\ 1, & j = n+1. \end{cases} \tag{10}$$

The preliminary approximation $x_h^p(t_{n+1})$ is called predictor and is given by

$$x_h^p(t_{n+1}) = \sum_{k=0}^{m-1} x_0^{(k)} \frac{t_{n+1}^k}{k!} + \frac{1}{\Gamma(q)} \sum_{j=0}^{n} b_{j,n+1} f\left(t_j, x_h(t_j)\right), \tag{11}$$

where $b_{j,n+1} = (h^q/q)((n-j+1)^q - (n-j)^q)$.

The error estimate is $\max|x(t_j) - x_h(t_j)| = O(h^p)$ $(j = 0, 1, \ldots, N)$, where $p = \min(2, 1+q)$.

2.3. Numerical Examples. In this section, to demonstrate the effectiveness of the proposed OPCL based MPS scheme for different fractional-order systems, we provide two groups of numerical examples. Firstly, fractional-order Arneodo system and fractional-order Lü system are used to verify the incommensurate synchronization. Secondly, fractional-order Lorenz system and fractional-order financial system are introduced to validate the commensurate case.

2.3.1. MPS between Fractional-Order Arneodo System and Fractional-Order Lü System. The fractional-order incommensurate Arneodo system with parameter perturbation is defined as

$$\begin{aligned} D^{q_1} x_1 &= x_2, \\ D^{q_2} x_2 &= x_3, \\ D^{q_3} x_3 &= (\alpha + \Delta\alpha) x_1 + (\beta + \Delta\beta) x_2 + (\gamma + \Delta\gamma) x_3 + x_1^3, \end{aligned} \tag{12}$$

where $\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$ are the mismatches in parameters. When $(\alpha, \beta, \gamma) = (5.5, -3.5, -1)$ and $(q_1, q_2, q_3) = (0.9, 0.92, 0.96)$, the Arneodo system exhibits chaotic behavior.

The fractionalized version of Lü system reads

$$\begin{aligned} D^{q_1} y_1 &= a(y_2 - y_1), \\ D^{q_2} y_2 &= c y_2 - y_1 y_3, \\ D^{q_3} y_3 &= y_1 y_2 - b y_3. \end{aligned} \tag{13}$$

It has been shown that system (13) will exhibit chaotic behavior when $a = 36$, $b = 3$, $c = 20$, and $(q_1, q_2, q_3) = (0.9, 0.92, 0.96)$.

From system (13), we can obtain the Jacobian matrix:

$$Jg(kx) = \frac{\partial g(kx)}{\partial(kx)} = \begin{pmatrix} -a & a & 0 \\ -k_3 x_3 & c & -k_1 x_1 \\ k_2 x_2 & k_1 x_1 & -b \end{pmatrix}. \tag{14}$$

The constant matrix H for response Lü system is selected as

$$H = \begin{pmatrix} -a & a & 0 \\ p_1 & c & p_2 \\ p_3 & p_4 & -b \end{pmatrix}. \tag{15}$$

On the basis of Definition 1, the error vector of MPS can be expressed by

$$e = He = (e_1, e_2, e_3)^T = (y_1 - k_1 x_1, y_2 - k_2 x_2, y_3 - k_3 x_3)^T. \tag{16}$$

Consequently, define (12) as the drive system and the response system controlled by OPCL coupling is obtained as

$$\begin{aligned} D^{q_1} y_1 &= a(y_2 - y_1) + k_1 x_2 - a(k_2 x_2 - k_1 x_1), \\ D^{q_2} y_2 &= c y_2 - y_1 y_3 + k_2 x_3 - (c k_2 x_2 - k_1 x_1 k_3 x_3) \\ &\quad + (p_1 + k_3 x_3) e_1 + (p_2 + k_1 x_1) e_3, \end{aligned}$$

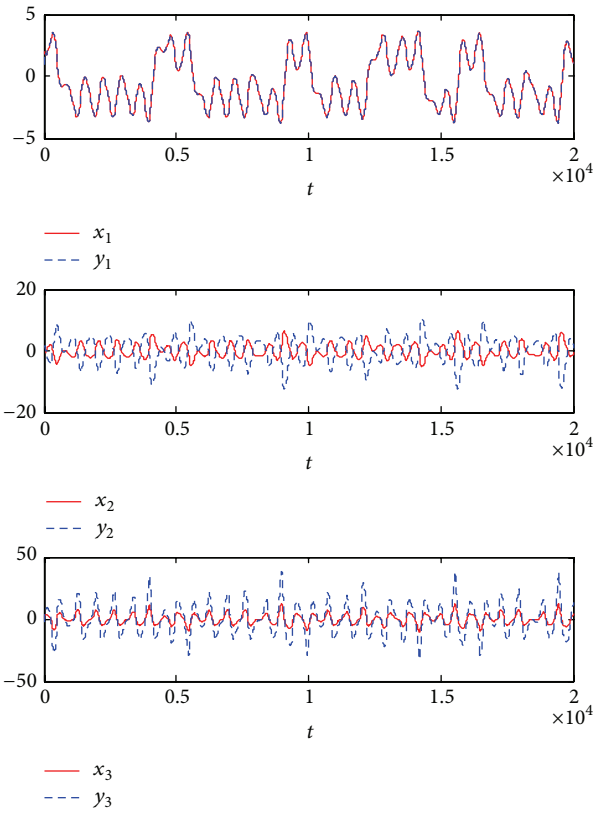


FIGURE 1: The time evolutions of states for coupled system (12) and system (17).

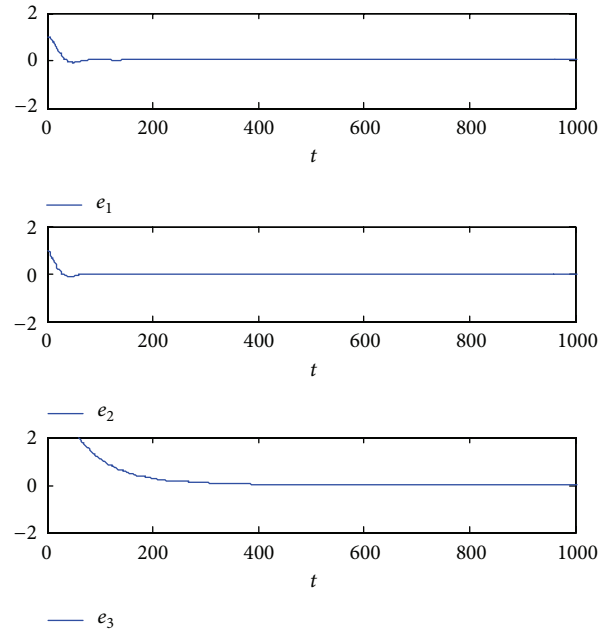


FIGURE 2: The time evolutions of MFPS errors between system (12) and system (17).

$$
\begin{aligned}
D^{q_3} y_3 = {} & y_1 y_2 - b y_3 + k_3 \left((\alpha + \Delta\alpha) x_1 + (\beta + \Delta\beta) x_2 \right. \\
& \left. + (\gamma + \Delta\gamma) x_3 + x_1^3 \right) \\
& - \left(k_1 x_1 k_2 x_2 - b k_3 x_3 \right) \\
& + \left(p_3 - k_2 x_2 \right) e_1 + \left(p_4 - k_1 x_1 \right) e_2.
\end{aligned} \tag{17}
$$

Thus, by choosing appropriate p_1, p_2, p_3, and p_4, we can stabilize the error vector (16). Now we choose $p_1 = -30$, $p_2 = 0$, $p_3 = 0$, and $p_4 = 0$, where p_1 decides the rate of achieving synchronization. Let us determine the stability of (16) for these p_i's. According to Corollary 6, we constitute $\Delta(\lambda)$ for (15) as follows:

$$
\Delta(\lambda) = \det\left(\operatorname{diag}\left(\lambda^{45}, \lambda^{46}, \lambda^{48} \right) - \begin{pmatrix} -36 & 36 & 0 \\ -30 & 20 & 0 \\ 0 & 0 & -3 \end{pmatrix} \right) = 0. \tag{18}
$$

Solving this equation for λ, we can see that $\min(|\arg(\lambda_i)|) = 0.0452$ which is greater than $\pi/2M = 0.0314$. Therefore, based on Corollary 6, we conclude the stability of (16), implying that the MPS between fractional-order system (12) and system (17) can be achieved theoretically.

In numerical simulation, for further reduction in coupling complexity, we set the parameter mismatches in drive system (12) as $\Delta\alpha = 1$, $\Delta\beta = 0$, and $\Delta\gamma = 0$. Then, choose scale constant vector as $k = (1, -2, 3)$, the initial conditions as $(x_1(0), x_2(0), x_3(0)) = (2, -1, 1,)$, $(y_1(0), y_2(0)$, and $y_3(0)) = (1, -2, 3)$. The corresponding numerical results are shown in Figures 1 and 2. Figure 1 depicts the time evolutions of state variables in the drive system (12) and the response system (17) with the scaling matrix k.

Figure 2 displays the error state trajectories of the two systems. And the error state trajectories asymptotically converge to zero, which implies that the MPS between the incommensurate system (12) and system (17) is realized.

2.3.2. MPS between Fractional-Order Lorenz System and Fractional-Order Financial System. The fractional-order Lorenz system with parameter perturbation is expressed as

$$
\begin{aligned}
D^q x_1 &= (\alpha + \Delta\alpha)(x_2 - x_1), \\
D^q x_2 &= (\beta + \Delta\beta) x_1 - x_1 x_3 - x_2, \\
D^q x_3 &= x_1 x_2 - (\gamma + \Delta\gamma) x_3,
\end{aligned} \tag{19}
$$

where $\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$ are the mismatches in parameters. When $(\alpha, \beta, \gamma) = (10, 28, 8/3)$ and $q \geq 0.993$, the Lorenz system exhibits chaotic behavior.

The fractional-order financial system reads

$$
\begin{aligned}
D^q y_1 &= y_3 + (y_2 - a) y_1, \\
D^q y_2 &= 1 - b y_2 - y_1^2, \\
D^q y_3 &= -y_1 - c y_3.
\end{aligned} \tag{20}
$$

It has been shown that system (20) will exhibit chaotic behavior when $a = 3, b = 0.1, c = 1$, and $q \geq 0.85$.

Therefore, we can obtain the Jacobian matrix of system (20):

$$Jg(kx) = \frac{\partial g(kx)}{\partial (kx)} = \begin{pmatrix} k_2x_2 - a & k_1x_1 & 1 \\ -k_1x_1 & -b & 0 \\ -1 & 0 & -c \end{pmatrix}. \quad (21)$$

The constant matrix H for response system is selected as

$$H = \begin{pmatrix} p_1 & p_2 & 1 \\ p_3 & -b & 0 \\ -1 & 0 & -c \end{pmatrix}. \quad (22)$$

According to the error vector defined by (16), if system (19) is considered as drive system, the response system controlled by OPCL coupling is obtained as

$$\begin{aligned} D^q y_1 &= y_3 + (y_2 - a) y_1 + k_1 (\alpha + \Delta\alpha)(x_2 - x_1) \\ &\quad - k_3 x_3 - (k_2 x_2 - a) k_1 x_1 \\ &\quad + (p_1 - k_2 x_2 + a) e_1 + (p_2 - k_1 x_1) e_2, \\ D^q y_2 &= 1 - b y_2 - y_1^2 \\ &\quad + k_2 ((\beta + \Delta\beta) x_1 - x_1 x_3 - x_2) - 1 \\ &\quad + b k_2 x_2 + (k_1 x_1)^2 + (p_3 + k_1 x_1) e_1, \\ D^q y_3 &= -y_1 - c y_3 \\ &\quad + k_3 (x_1 x_2 - (\gamma + \Delta\gamma) x_3) + k_1 x_1 + c k_3 x_3. \end{aligned} \quad (23)$$

Thus by choosing appropriate p_1, p_2, and p_3, we can stabilize the error vector (16). Here, we choose $p_1 = -30$, $p_2 = -10$, and $p_3 = 10$, where p_1 decides the rate of achieving synchronization. In numerical simulation, for further reduction in coupling complexity, we set the parameter mismatches in drive system (19) as $\Delta\alpha = 0.01$, $\Delta\beta = 0$, and $\Delta\gamma = 0$. Then, set the fractional-order of two systems as $q = 0.998$ and choose scale constant vector as $k = (2, -1, -3)$ and the initial conditions as $(x_1(0), x_2(0), x_3(0)) = (2, -1, 1)$ and $(y_1(0), y_2(0), y_3(0)) = (1, 1, -2)$. The corresponding simulation results for the time evolutions of state errors are shown in Figure 3, from which we can see that the MPS between two commensurate fractional-order chaotic systems can also be achieved.

The simulation results of the two examples demonstrate that the nonidentical fractional-order chaotic systems with mismatches can achieve the MPS under the OPCL coupling.

3. A Novel Image Encryption Scheme Based on MPS

3.1. Scheme Description. Based on the MPS between fractional-order Arneodo system and fractional-order Lü system, an image encryption scheme is designed for the sake of higher security.

Sender A has the drive system (12) and the response system (17). Receiver B only holds the drive system (12) and

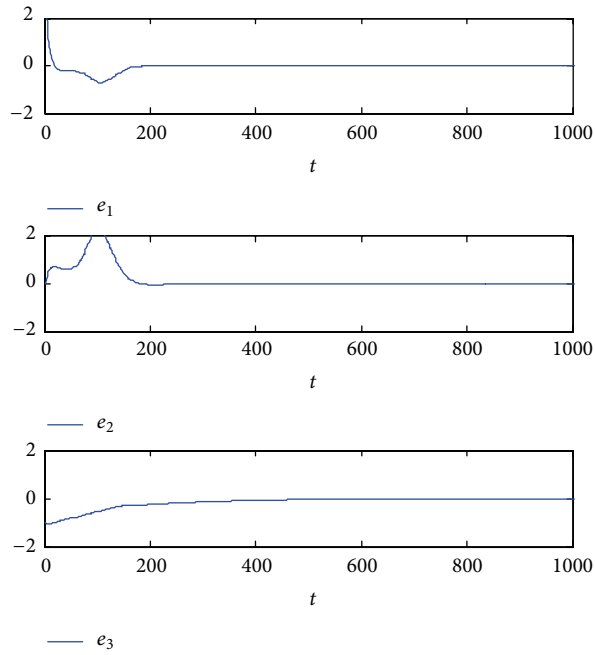


Figure 3: The time evolutions of MFPS errors between system (19) and system (23).

scaling matrix k. A and B share the initial conditions of system (12) and a symmetric key set. Consider

$$H_s = \{h_1, h_2, \ldots, h_{12}\}. \quad (24)$$

Here, $h_1 = \alpha$, $h_2 = \beta$, and $h_3 = \gamma$ are parameters of drive system (12), $h_4 = q_1$, $h_5 = q_2$, and $h_6 = q_3$ are fractional derivatives of drive system (12), $h_7 \sim h_9$ are initial conditions of system (12), and $h_{10} \sim h_{12}$ are the main diagonal elements of scaling matrix k.

The typical image encryption framework is used to encrypt plain image, which is illustrated in Figure 4.

The image cryptosystem in Figure 4 includes two stages, chaotic confusion and pixel diffusion, where the former process permutes a plain image and the latter process changes the value of each pixel one by one. As shown in Figure 4, the confusion and diffusion processes are both repeated several times to enhance the security of this cryptosystem. Suppose that the size of image is $M \times N$ and the detailed encryption algorithm is described as follows.

(1) A first selects the initial conditions and scaling matrix k and then uses them and systems (12) and (17) to generate chaotic data; set the chaotic stream after synchronous time t_0 as $S = (x_1(t), x_2(t), x_3(t), y_1(t), y_2(t), y_3(t))$, $t > t_0$.

(2) In the confusion process, A utilizes the discrete data of system (17) to permute the position of pixel; set $r_x = \text{abs}(\text{fix}(y_3(t_1)))$ and $r_y = \text{abs}(\text{fix}(y_3(t_1 + t_2)))$, where $\text{fix}(\cdot)$ is the function to obtain the integer part, $t_1 > t_0$, and t_2 is the

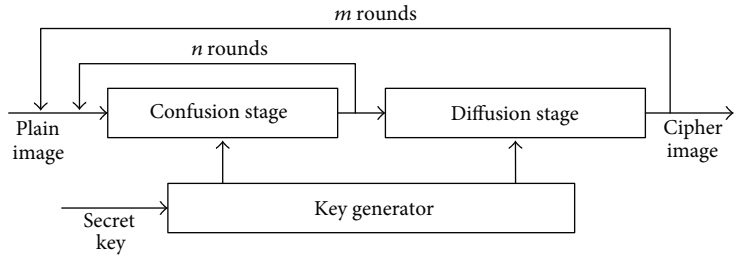


Figure 4: Block diagram of the image cryptosystem.

time interval of the two parameters; the position of pixel is permuted as follows:

$$x_{i+1} = \left(x_i + y_i + r_x + r_y\right) \bmod M,$$
$$y_{i+1} = \left(y_i + r_y + C \sin \frac{2\pi x_{i+1}}{N}\right) \bmod N, \tag{25}$$

where (x_i, y_i) and (x_{i+1}, y_{i+1}) are considered as the positions of image pixel before and after permutation.

(3) In the diffusion stage, the pixel value of image is substituted with its position information by A; according to the chaotic stream S, we can obtain two substitution parameters:

$$c = \text{abs}\left(10^l y_1 - \text{round}\left(10^l y_1\right)\right) \times 10^3,$$
$$d = \text{abs}\left(10^l y_2 - \text{round}\left(10^l y_2\right)\right) \times 10^3, \tag{26}$$

where round( ) is rounding function and l is a positive integer; the biggest value of the parameter l relates to the precision of the computer; therefore, the range of parameter l is from 1 to 14 in current experiment, which can be used as secret key; the substitution of pixel value is in the form of

$$v = p \oplus \left(c \times x_i + d \times y_i\right) \bmod L, \tag{27}$$

where p and v are the pixel values of image before and after substitution and L is the grey level of pixel.

The decryption procedure is similar to that of encryption process with reverse operational sequences to those described above. When B receives the cipher image, it uses the chaotic stream $S_1 = (x_1(t), x_2(t), x_3(t))$, $t > t_0$, generated by the system (12) and the initial condition of system (12) and scaling matrix k to generate $S_2 = (y_1(t), y_2(t), y_3(t))$, $t > t_0$, by $y_1(t) = k_1 x_1(t)$, $y_2(t) = k_2 x_2(t)$, and $y_3(t) = k_3 x_3(t)$. Firstly, substitute the grey values in cipher image back to original ones, namely, for every position (x_i, y_i) and corresponding grey value v of cipher image; compute original grey value as follows:

$$p = v \oplus \left(c \times x_i + d \times y_i\right) \bmod L, \tag{28}$$

where substitution parameters c and d can be computed by (26). After all pixels return to original grey values, then, the pixel in position (x_{i+1}, y_{i+1}) should be moved back to the original position (x_i, y_i) by following inverse operation:

$$y_i = \left(y_{i+1} - 1 - r_y - C \sin \frac{2\pi x_{i+1}}{N} + 2N\right) \bmod N,$$
$$x_i = \left(x_{i+1} - 1 - y_i - r_x - r_y + 2M\right) \bmod M, \tag{29}$$

where the values of r_x and r_y are the same as they are in (25). After the two steps are followed, the plain image can be resumed and the process of decipher is over.

3.2. Experimental Results and Security Analysis. To demonstrate the validity and efficiency of our scheme, a group of experiments for gray Lena image (256 × 256) is carried out with results shown in Figure 5. Here, the key set is selected the same as Section 2.2. Figure 5(b) is the cipher image for original image in Figure 5(a). The histograms of plain image and cipher image illustrated in Figures 5(c) and 5(d) demonstrate that although the grey distribution of original images is not uniform, the grey values of cipher images become uniformly distributed and their statistical property is absolutely changed. A good encryption should be able to resist all kinds of known attacks and some security analyses have been performed on the proposed image encryption scheme.

3.2.1. Key Space. The key space of a good image encryption algorithm should be sufficiently large to make brute-force attack infeasible. The key space of the proposed method is much larger than those of previous methods because system parameters, fractional derivative, and initial conditions of drive system (12) and diagonal elements of scaling matrix k are all cipher key ones; moreover, the mismatch parameters $\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$ of drive system (12), time point t_1, time interval t_2, and positive integer l are all also secret keys. So this is enough to resist all kinds of brute-force attacks.

3.2.2. Key Sensitivity. A good encryption scheme should be sensitive to cipher keys in process of both enciphering and deciphering. Namely, when an image is encrypted, tiny change of keys should receive two completely different cipher images and, when an image is decrypted, tiny change of keys can cause the failure of deciphering.

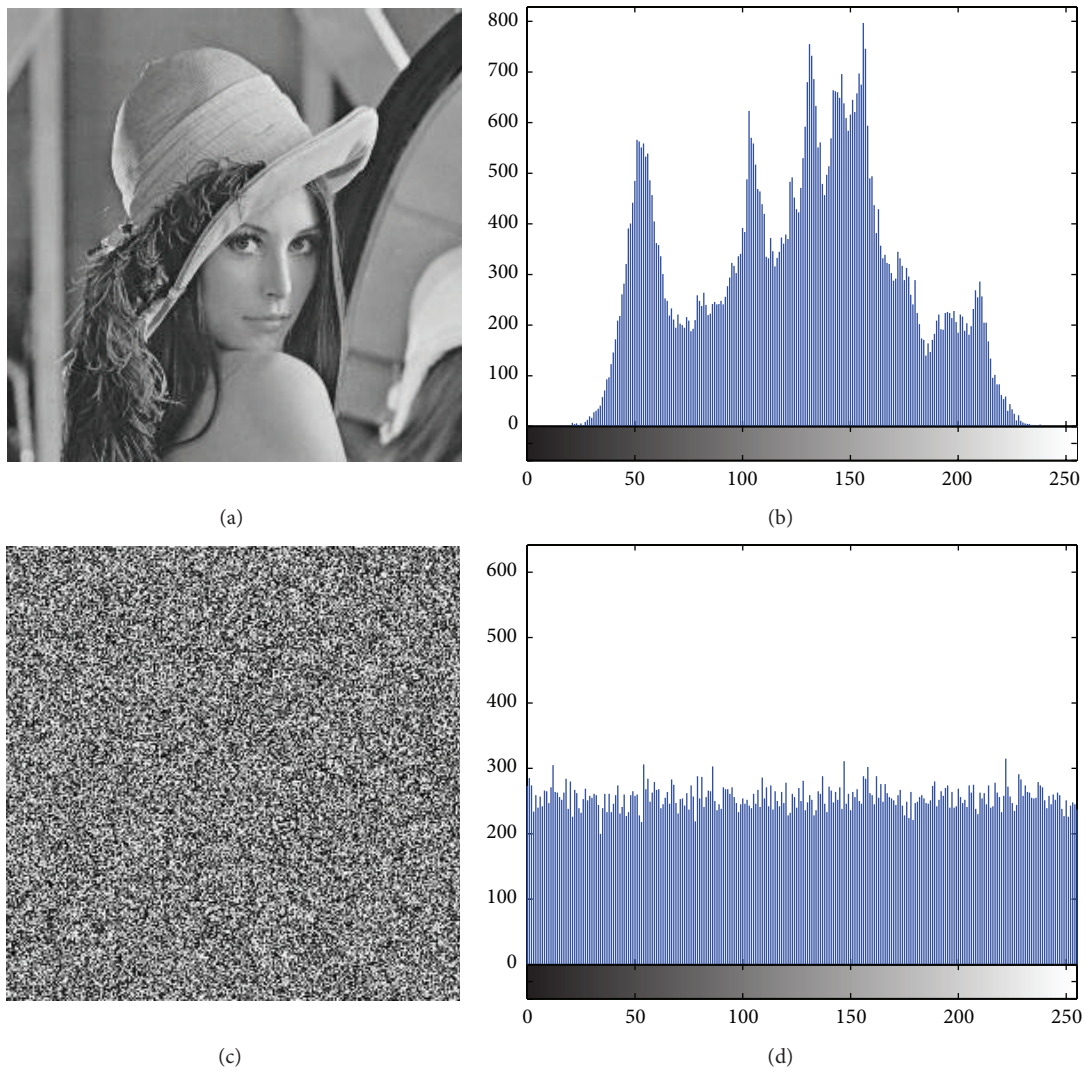


Figure 5: The encrypted results for Lena image: (a) plain Lena image; (b) histogram of Lena image; (c) cipher image; (d) histogram of cipher image.

(1) *Key Sensitivity in Encryption*. The following key sensitivity tests in encryption have been performed based on the 256 × 256 gray Lena image.

Test 1. One of the initial conditions of the drive system (12) is changed a bit; here, we let the first initial condition of system (12) be changed, using $x_1(0) = x_1(0) + 10^{-4}$.

Test 2. One of the system parameters of the drive system (12) is changed slightly; here, we alter the second parameter, using $\beta = \beta + 10^{-4}$.

Test 3. One of the fractional derivatives of the drive system (12) is changed, using $q_1 = q_1 + 0.01$.

Test 4. One element of the scaling matrix is altered, using $k_1 = k_1 + 1$.

Table 1: Percentage difference between cipher images.

	Test 1	Test 2	Test 3	Test 4
Two cipher images	99.56%	99.60%	99.59%	99.51%

The differences of the two cipher images for the four tests are given in Table 1. From the table, it can be concluded that the proposed method is very sensitive to the key; a small change of the key will generate a different decryption result and one cannot get the correct plain image.

(2) *Key Sensitivity in Decryption.* In the encryption scheme, small changes to key can lead to completely incorrect image. For the image of gray Lena shown in Figure 5(a), the decryption result with right key is shown in Figure 6(a) and the incorrect decrypted image is shown in Figure 6(b) when the

Table 2: The comparison of NPCR and UACI between proposed method and literature [14].

(m, n)	NPCR		UACI	
	Our method	Literature [14]	Our method	Literature [14]
(1, 2)	0.0016	0.0002	0.0004	0.00004
(2, 2)	0.1260	0.0110	0.0440	0.0027
(2, 3)	0.4697	0.0173	0.1628	0.0046
(3, 2)	0.8840	0.4388	0.3006	0.1195
(3, 3)	0.9866	0.5662	0.3326	0.1554
(4, 4)	0.9959	0.9899	0.3358	0.3109
(6, 4)	0.9961	0.9961	0.3351	0.3346

Table 3: The comparison of correlation coefficients between two adjacent pixels.

	Gray Lena image	Encrypted image with our method	Encrypted image in literature [14]	Random image
Horizontal	0.965	0.002952	0.002453	0.001562
Vertical	0.941	−0.001829	0.004864	0.005962
Diagonal	0.915	0.001236	0.007525	0.004006

value of x_0 has tiny change (10^{-14}). That is, tiny deviation of decryption key can lead to completely meaningless image.

3.2.3. Differential Attack. One of the security requirements of an effective image encryption scheme is its ability to resist differential attacks. To measure the influence of one-pixel change on the cipher image, two common quantitative measures are adopted.

NPCR (number of pixels change rate);

$$\mathrm{NPCR} = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \tag{30}$$

UACI (unified average changing intensity):

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{ij} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{31}$$

where C_1 and C_2 are the pixel value matrices of two different cipher images, respectively; D is the change of the corresponding pixel value, which is defined as

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{32}$$

Next, two plain images are considered: one is the original image shown in Figure 5(a); the other is a changed image that adds 1 to the pixel value in the lower right corner of original image. When we encrypt the two plain images with the same encryption key, we can obtain two different cipher images C_1 and C_2. Several comparisons of NPCR and UACI between our method and literature [14] with different values of m and n are given in Table 2. Compared with the results of literature [14], we can achieve a much more better performance NPCR > 0.996 and UACI > 0.334 with $m = n = 4$, which can be obtained with $m = 6$ in literature [14].

3.2.4. Statistical Analysis. To test the correlation between two adjacent pixels, the following procedures are carried out. The correction coefficients r_{xy} of two horizontally, vertically, and diagonally adjacent pixels in the plain image and the cipher image are calculated according to the following formulas:

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$E(x) = \frac{1}{S} \sum_{i=1}^{S} x_i, \tag{33}$$

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

where x and y are pixel values of two adjacent pixels in the image, $E(x)$ is the mean value of x, and $D(x)$ is the variance of x, $S = M \times N/2$.

Here, we use the 256×256 gray Lena image, encrypted image with our method, encrypted image in literature [14], and random image for simulation. The results are given in Table 3.

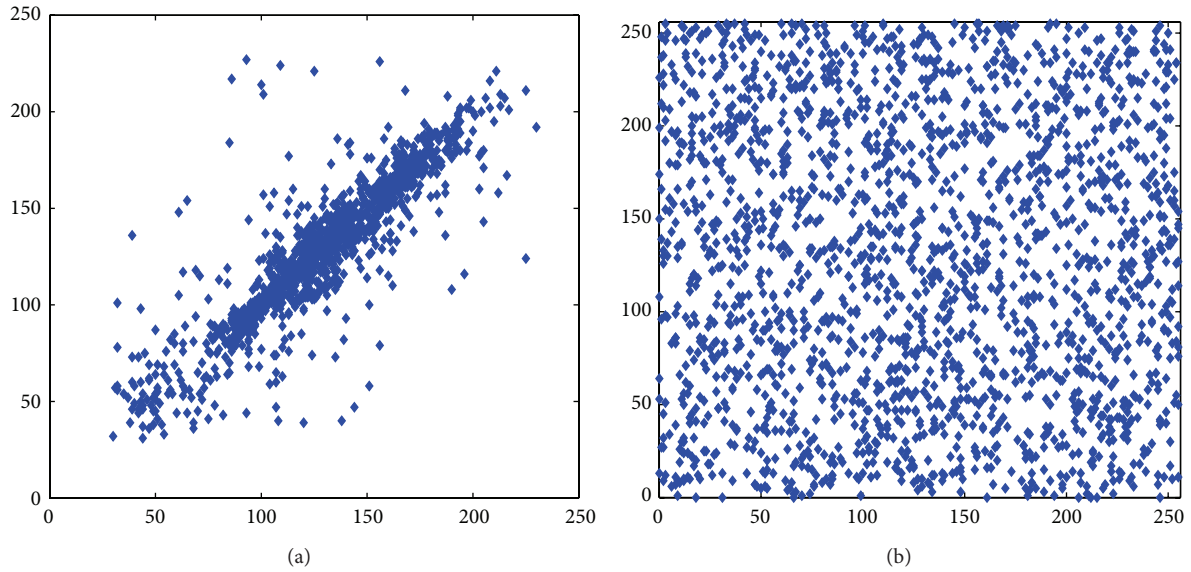
Meanwhile, we randomly select 2000 pairs of two horizontally adjacent pixels from the Lena image. The correlation distribution of the pixels in the plain image and the cipher image is illustrated in Figure 7. Both the correlation coefficients and the figures justify that neighboring pixels of the plain image can be decorrelated by the proposed cryptosystem effectively. Therefore, the proposed algorithm has high security against statistical attacks.

4. Conclusions

In this paper, for the first time, an OPCL coupling scheme is utilized to achieve the MPS between two different fractional-order dynamical systems in the presence of mismatch. Based on the stability theory of fractional-order system, the MPS

(a) (b)

Figure 6: The decrypted results for Lena image: (a) decrypted image with correct key; (b) decrypted image with wrong key.



(a) (b)

Figure 7: Correlation analysis of two horizontally adjacent pixels in (a) the plain Lena image and (b) the cipher image obtained by the proposed scheme.

of two incommensurate or commensurate fractional-order systems can be achieved. Both numerical simulations and computer graphics show that the developed coupling scheme works well. Apparently, the proposed method possesses generality and is still appropriate for the case of MPS between two fractional-order systems without parameter mismatch. Meanwhile, because the complete synchronization, antisynchronization, and projective synchronization are all included in modified projective synchronization, our results contain and extend most of the existing works.

In image encryption application, we adopt the data from the MPS to encrypt the image. Experimental results and security analysis show that the algorithm can be easily implemented and its encryption effect is satisfactory. Moreover, the algorithm possesses high security in terms of the resistance to exhaustive attack, statistical attack, and differential attack. This scheme is particularly suitable for Internet image encryption and transmission applications.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant nos. 60872040 and 61104074), the Fundamental Research Funds for the Central Universities (Grant nos. N100604007, N110417004, N110417005, and N110617001), and the Ph.D. Start-up Foundation of Liaoning Province, China (Grant nos. 20111001 and 20100471462).

References

[1] I. Grigorenko and E. Grigorenko, "Chaotic dynamics of the fractional Lorenz system," *Physical Review Letters*, vol. 91, Article ID 034101, 2003.

[2] W. Deng and C. Li, "Chaos synchronization of the fractional Lü system," *Physica A*, vol. 353, pp. 61–72, 2005.

[3] C. Li and G. Chen, "Chaos and hyperchaos in the fractional-order Rössler equations," *Physica A*, vol. 341, pp. 55–61, 2004.

[4] J. Lu, "Chaotic dynamics and synchronization of fractional-order Arneodo's systems," *Chaos, Solitons & Fractals*, vol. 26, no. 4, pp. 1125–1133, 2005.

[5] R. Zhang and S. Yang, "Adaptive synchronization of fractional-order chaotic systems via a single driving variable," *Nonlinear Dynamics*, vol. 66, no. 4, pp. 831–837, 2011.

[6] J. G. Lu, "Nonlinear observer design to synchronize fractional-order chaotic systems via a scalar transmitted signal," *Physica A*, vol. 359, pp. 107–118, 2006.

[7] D. Chen, Y. Liu, X. Ma, and R. Zhang, "Control of a class of fractional-order chaotic systems via sliding mode," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 893–901, 2012.

[8] S. Li and Z. Ge, "Generalized synchronization of chaotic systems with different orders by fuzzy logic constant controller," *Expert Systems with Applications*, vol. 38, no. 3, pp. 2302–2310, 2011.

[9] E. Jackson and I. Grosu, "An open-plus-closed-loop (OPCL) control of complex dynamic systems," *Physica D*, vol. 85, no. 1-2, pp. 1–9, 1995.

[10] I. Grosu, E. Padmanaban, P. K. Roy, and S. K. Dana, "Designing coupling for synchronization and amplification of chaos," *Physical Review Letters*, vol. 100, Article ID 234102, 2008.

[11] K. S. Sudheer and M. Sabir, "Modified function projective synchronization of hyperchaotic systems through open-plus-closed-loop coupling," *Physics Letters A*, vol. 374, no. 19-20, pp. 2017–2023, 2010.

[12] X. Wang, R. Liu, and N. Zhang, "Function projective synchronization of fractional-order hyperchaotic system based on open-plus-closed-looping," *Communications in Theoretical Physics*, vol. 55, no. 4, pp. 617–621, 2011.

[13] J. Wang, Z. Li, and Q. Ma, "Inverse synchronization of coupled fractional-order systems through open-plus-closed-loop control," *Pramana*, vol. 76, no. 3, pp. 385–396, 2011.

[14] S. G. Lian, J. S. Sun, and Z. Q. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

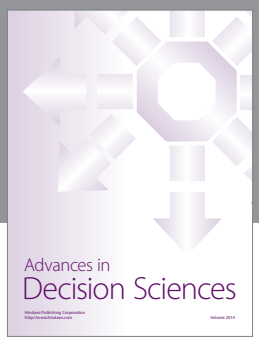
[15] M. Caputo, "Linear models of dissipation whose Q is almost frequency independent-II," *Geophysical Journal of the Royal Astronomical Society*, vol. 13, no. 5, pp. 529–539, 1967.

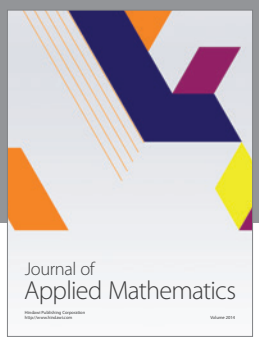
[16] M. S. Tavazoei and M. Haeri, "Chaotic attractors in incommensurate fractional order systems," *Physica D*, vol. 237, no. 20, pp. 2628–2637, 2008.

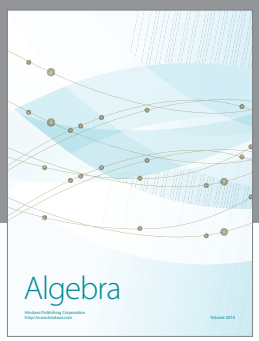
[17] W. Deng, C. Li, and J. Lü, "Stability analysis of linear fractional differential system with multiple time delays," *Nonlinear Dynamics*, vol. 48, no. 4, pp. 409–416, 2007.

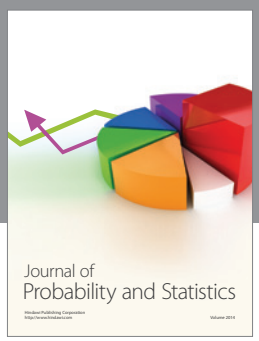
[18] D. Matignon, "Stability results for fractional differential equations with applications to control processing," *Computational Engineering in Systems Applications*, vol. 2, pp. 963–968, 1996.

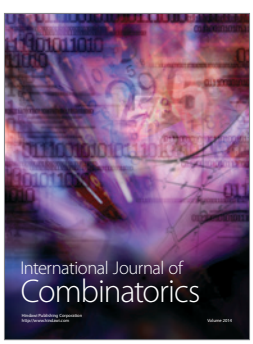
[19] K. Diethelm, N. Ford, and A. Freed, "A predictor-corrector approach for the numerical solution of fractional differential equations," *Nonlinear Dynamics*, vol. 29, no. 1–4, pp. 3–22, 2002.

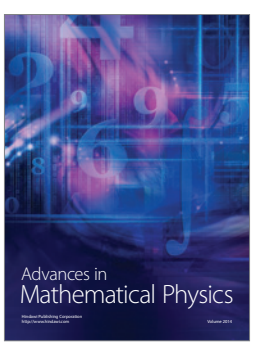


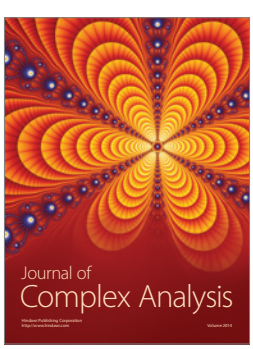


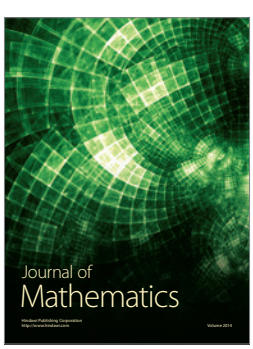


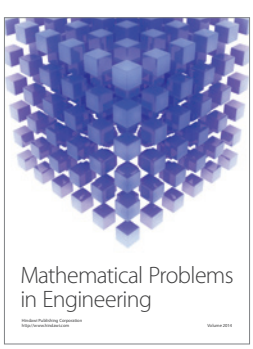


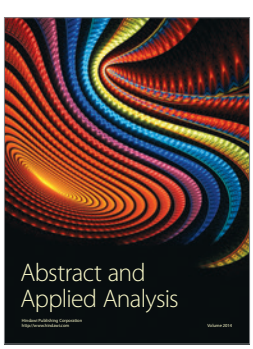


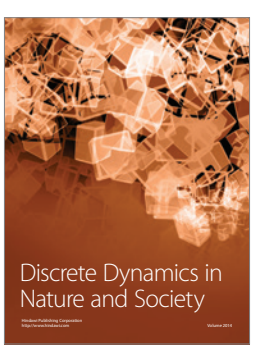


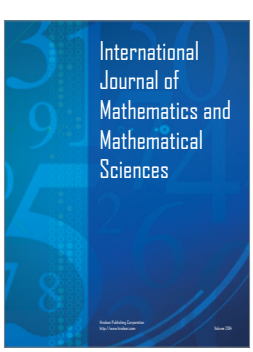












Hindawi

Submit your manuscripts at
http://www.hindawi.com