Bol. Soc. Paran. Mat. (3s.) **v. 39** 5 (2021): 57–72.
©SPM –ISSN-2175-1188 on line ISSN-00378712 in press
SPM: www.spm.uem.br/bspm doi:10.5269/bspm.41252

Synchronization of Different Dimensions Fractional-Order Chaotic Systems with Uncertain Parameters and Secure Communication

Vajiheh Vafaei, Hossein Kheiri and Aliasghar Jodayree Akbarfam

Abstract: In this paper, an adaptive modified function projective synchronization (AMFPS) scheme of different dimensions fractional-order chaotic systems with fully unknown parameters is presented. On the basis of fractional Lyapunov stability theory and adaptive control law, a new fractional-order controller and suitable update rules for unknown parameters are designed to realize the AMFPS of different fractional-order chaotic systems with non-identical orders and different dimensions. Theoretical analysis and numerical simulations are given to verify the validity of the proposed method. Additionally, synchronization results are applied to secure communication via modified masking method. Due to the unpredictability of the scale function matrix and using of fractional-order systems with different dimensions and unequal orders, the proposed scheme has higher security. The security analysis demonstrate that the proposed algorithm has a large key space and high sensitivity to encryption keys and it is resistance to all kind of attacks.

Key Words: Fractional-order chaotic system, Synchronization, control, Secure communication, Security.

Contents

2010 *Mathematics Subject Classification:* 34D06, 34H10, 26A33, 34H15.
Submitted January 11, 2018. Published June 21, 2018

1. Introduction

Applications of the fractional-order systems in the fields of physics and engineering have attracted lots of attentions in the recent years [1,2]. Also, many efforts have been devoted to the study of fractional-order chaotic systems. Synchronization of fractional-order chaotic systems has applications in secure communication, cryptography, control processing and etc [1,3]. So far, many synchronization methods for fractional-order chaotic systems have been presented, such as projective synchronization [4], generalized synchronization [5], phase synchronization [6], sliding mode control [7] and etc. Among all of them, projective synchronization (PS) [8] has been attracted increasing attention because it can get fast communication using this feature that drive and response systems can synchronize up to a scaling factor. Then, Li [9] extended the concept of PS and proposed modified projective synchronization (MPS), where the drive and response states can synchronize up to constant scaling matrix. Later on, Chen et al. [10] presented the concept of function projective synchronization (FPS), where the drive and response systems can synchronize up to a scaling function, but not a constant. Thereafter, Du et al. [11] reported a new synchronization scheme, modified function projective synchronization (MFPS), in which the drive and response systems could be synchronized up to a desired scaling function matrix. These methods are presented for the integer order systems and some of them are extended to fractional order systems. On the other hand, in most of the literature, the synchronization of fractional-order systems with same dimensions and identical orders is used. Hence, the absence of the extension of adaptive modified function projective synchronization (AMFPS) for different dimensions fractional order chaotic systems with non-identical fractional-orders is sensible.

In recent years, many encryption algorithms based on chaos synchronization have been proposed but they often lack of security analysis and most of them hold only for the integer order systems [12]. Also, most secure communication schemes using chaotic systems are based on synchronization of identical systems. Therefore, encryption methods based on chaos synchronization of fractional-order systems with different dimensions and unequal orders have not been presented. However, AMFPS method of different fractional-order chaotic systems and unpredictability of uncertain parameters can enhance the security of communication.

Inspired by the above discussions, in this paper, we discuss AMFPS scheme for two different uncertain fractional order chaotic systems with different dimensions. By the Lyapunov stability theory and adaptive control method, we propose a new method of designing fractional-order controller and parameter update rules to ensure the AMFPS is obtained and the parameters are estimated. Numerical simulations are presented to demonstrate the effectiveness of the proposed method. Furthermore, we proposed a new modified chaotic masking secure communication scheme by applying AMFPS of two different fractional-order chaotic systems with unknown parameters and different dimensions. The unpredictability of the scaling functions in AMFPS and the utilization of fractional-order systems with different dimensions and unequal orders can provide additional security in secure communication scheme. The performance of the proposed image cryptosystem is analyzed by using several security test measures, such as key space analysis, key sensitivity analysis, information entropy, histogram analysis and speed analysis. The results demonstrate that high security can be guaranteed to resist all kinds of brute-force and statistical attacks. Therefore, AMFPS of fractional-order systems and its application to secure communication is worth studying.

2. Preliminaries and AMFPS Description

In order to investigate control and synchronization of the chaotic fractional-order dynamic systems, we recall some definitions and lemmas.

Definition 2.1. *Let $q \in \mathbb{R}^+$. The Caputo differential operator [13] of order q is defined by*

$${}_a^C D_t^q f(t) := \frac{1}{\Gamma(m-q)} \int_a^t \frac{f^m(\tau)}{(t-\tau)^{q+1-m}} d\tau,$$

whenever $f^m \in L^1[a,b]$ and $m := \lceil q \rceil = \min\{z \in \mathbb{Z} : z \geq q\}$.

Definition 2.2. *A continuous function $\gamma : [0,t) \to [0,\infty)$ is said to belong to class-K if it is strictly increasing and $\gamma(0) = 0$ [14].*

Lemma 2.3. *([15]) Let $x(t) \in \mathbb{R}^n$ be a vector of differentiable functions and $q \in (0,1]$. For any time instant $t \geq t_0$, the following relationship holds*

$$\frac{1}{2} D^q (x^T(t) P x(t)) \leq x^T(t) P D^q x(t),$$

where $P \in \mathbb{R}^{n \times n}$ is a constant symmetric positive definite matrix.

Lemma 2.4. *(Fractional comparison principle [14]). Let $D^q x(t) \geq D^q y(t)$, $q \in (0,1)$ and $x(t_0) = y(t_0)$. Then $x(t) \geq y(t)$.*

Lemma 2.5. *(Relationship between positive definite functions and class-K functions [16]). A function $V(x,t)$ is locally (or globally) positive definite if and only if there exists a class-K function γ_1 such that $V(0,t) = 0$ and $V(x,t) \geq \gamma_1(\|x\|)$, $\forall t \geq t_0$ and $\forall x$ belonging to the local space (or the whole space).*

A function $V(x,t)$ is locally (or globally) decrescent if and only if there exists a class-K function γ_2 such that $V(0,t) = 0$ and $V(x,t) \leq \gamma_2(\|x\|)$, $\forall t \geq t_0$ and $\forall x$ belonging to the local space (or the whole space).

Lemma 2.6. *(Fractional-order extension of Lyapunov direct method [14]). Let $x = 0$ be an equilibrium point for the fractional-order system*

$$D^q x(t) = f(t,x). \tag{2.1}$$

Assume that there exists a Lyapunov function $V(t, x(t))$ and class-K functions γ_i, $i = 1,2,3$, satisfying

$$\begin{aligned} &\gamma_1(\|x\|) \leq V(t,x(t)) \leq \gamma_2(\|x\|), \\ &D^q V(t,x(t)) \leq -\gamma_3(\|x\|), \end{aligned}$$

where $q \in (0,1)$. Then the system (2.1) is asymptotically stable.

Now, before studying an adaptive modified function projective synchronization (AMFPS) scheme of fractional-order systems, we present a stability theory of fractional-order dynamic systems.

Theorem 2.7. *Consider the fractional-order system*

$$D^q x = f(x), \tag{2.2}$$

where $x \in \mathbb{R}^n$ and $q \in (0,1]$. Let $x = 0$ is the equilibrium point of the system (2.2) and P is a real positive definite matrix. Then for any initial values, the origin of the system (2.2) is

(a) stable if $x^T P D^q x \leq 0$, $\forall x \in \mathbb{R}^n$;

(b) asymptotically stable if $x^T P D^q x < 0$, $\forall x \neq 0$,

where T stands for transpose of a matrix.

Proof: When $q = 1$, this is the case of stability for integer order dynamic system, the conclusion is evident.

When $0 < q < 1$, choose the positive definite Lyapunov function

$$V(x(t)) = \frac{1}{2} x^T(t) P x(t).$$

Using Lemma 2.3, results

$$D^q V(x(t)) = \frac{1}{2} D^q (x^T(t) P x(t)) \leq x^T(t) P D^q x(t). \tag{2.3}$$

If $x^T(t) P D^q x(t) \leq 0$, then $D^q V(x(t)) \leq 0$. Hence, the fractional derivative (2.3) of the Lyapunov function is negative semidefinite. Using the Lemma 2.4, it follows that $V(x(t))$ is decrescent, i.e. $V(x(t)) \leq V(x(0))$, $\forall x \in \mathbb{R}^n$. Therefore, according to the Lyapunov stability theorem, the origin of the system (2.2) is stable.

If $x^T(t) P D^q x(t) < 0$, $\forall x \neq 0$, then $D^q V(x(t)) < 0$. So the fractional derivative (2.3) of the Lyapunov function is negative definite. Using the Lemma 2.4, it follows that $V(x(t))$ is strictly decreasing, i.e. $V(x(t)) < V(x(0))$, $\forall x \in \mathbb{R}^n$.

Since $V(x(t))$ is positive definite and strictly decrescent, using the Lemma 2.5 there exists two class-K functions γ_1 and γ_2 such that $\gamma_1(\|x\|) \leq V(x(t)) \leq \gamma_2(\|x\|)$. Using Lemma 2.6 it is concluded that the origin of the system (2.2) is asymptotically stable. □

Corollary 2.8. *Consider the following fractional-order dynamic system*

$$D^q x = A(x) x, \tag{2.4}$$

with $x \in \mathbb{R}^n$, $A(x) \in \mathbb{R}^{n \times n}$ and $q \in (0,1]$. If there exist two real symmetric positive definite Matrices P and Q such as $PA(x) + A(x)^T P = -Q$, Then for any initial values, system (2.4) is asymptotically stable, i.e., $\lim_{t \to +\infty} ||x|| = 0$.

Proof: Since for all $x \in \mathbb{R}^n$, $x^T PAx = 1/2x^T(PA + A^T P)x = -1/2x^T Qx < 0$, using Theorem 2.7 the origin of the system (2.4) is asymptotically stable. □

Now, we will discuss AMFPS scheme of different dimensions fractional-order chaotic systems with fully unknown parameters.

The fractional order chaotic drive and response systems are defined as

$$D^{q_d} x = f(x, \alpha), \tag{2.5}$$
$$D^{q_r} y = g(y, \beta), \tag{2.6}$$

where q_d and q_r are fractional orders satisfying $0 < q_d < 1$, $0 < q_r < 1$, and q_r may be different with q_d; $x = (x_1, x_2, \ldots, x_n)^T \in \mathbb{R}^n$, $y = (y_1, y_2, \ldots, y_m)^T \in \mathbb{R}^m$ (m may be different with n) are the state vectors of systems (2.5) and (2.6), respectively; $\alpha \in \mathbb{R}^l$ and $\beta \in \mathbb{R}^k$ are unknown parameter vectors of systems (2.5) and (2.6) to be estimated and $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^m \to \mathbb{R}^m$ are two continuous vector functions.

When parameters α and β in drive and response systems are unknown, a controller u and parameter update laws are added to systems (2.5) and (2.6). Then, we obtain the drive system (2.7) and the controlled response system (2.8) with parameter update laws (2.9) and (2.10),

$$D^{q_d} x = f(x, \tilde{\alpha}), \tag{2.7}$$
$$D^{q_r} y = g(y, \tilde{\beta}) + u(x, y), \tag{2.8}$$
$$D^{q_r} \tilde{\alpha} = r(x, y, \tilde{\alpha}), \tag{2.9}$$
$$D^{q_r} \tilde{\beta} = s(x, y, \tilde{\beta}), \tag{2.10}$$

where $\tilde{\alpha}$ and $\tilde{\beta}$ are the estimated vectors of unknown parameters, vector $u : \{\mathbb{R}^n, \mathbb{R}^m\} \to \mathbb{R}^m$ is the controller vector to be designed and vector $r(x, y, \tilde{\alpha}) \in \mathbb{R}^l$ and $s(x, y, \tilde{\beta}) \in \mathbb{R}^k$ are real vectors to be designed.

The error vector for AMFPS are defined as $e = y - K(x)x$ where $e = (e_1, e_2, \ldots, e_m)^T$ and

$$e_i = y_i - \sum_{j=1}^{n} k_{ij}(x) x_j, \qquad i = 1, 2, \ldots, m, \tag{2.11}$$

and scaling function factors $k_{ij}(x)$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, are real continuous differentiable bounded functions, which compose the scaling function matrix $K(x) = (k_{ij}(x)) \in \mathbb{R}^{m \times n}$. Also, the error vectors of estimation unknown parameters are

$$e_\alpha = (e_{\alpha_1}, e_{\alpha_2}, \ldots, e_{\alpha_l})^T, \qquad e_{\alpha_i} = \tilde{\alpha}_i - \alpha_i, \qquad i = 1, 2, \ldots, l,$$
$$e_\beta = (e_{\beta_1}, e_{\beta_2}, \ldots, e_{\beta_k})^T, \qquad e_{\beta_i} = \tilde{\beta}_i - \beta_i, \qquad i = 1, 2, \ldots, k.$$

Note that α_i $(i = 1, 2, \ldots, l)$ and β_i $(i = 1, 2, \ldots, k)$ are true values of the unknown parameters $\tilde{\alpha}_i$ and $\tilde{\beta}_i$, respectively.

Definition 2.9. *It is said that the drive system* (2.7) *and the controlled response system* (2.8) *are AMFPS if there exists vector functions* $u(x,y)$, $r(x,y,\tilde{\alpha})$ *and* $s(x,y,\tilde{\beta})$ *such that*

$$\begin{aligned}\lim_{t\to\infty}||e|| &= \lim_{t\to\infty}||y-K(x)x|| = 0,\\ \lim_{t\to\infty}||e_\alpha|| &= \lim_{t\to\infty}||\tilde{\alpha}-\alpha|| = 0,\\ \lim_{t\to\infty}||e_\beta|| &= \lim_{t\to\infty}||\tilde{\beta}-\beta|| = 0.\end{aligned}$$

Remark 2.10. *It is easy to show that AMFPS is generalization of many synchronization schemes such as adaptive projective synchronization (APS), adaptive modified projective synchronization (AMPS), adaptive function projective synchronization (AFPS), adaptive generalized function projective synchronization (AGFPS), adaptive complete synchronization, adaptive anti-phase synchronization, chaos control problem and etc.*

Remark 2.11. *For a system with unknown parameters in this paper it is only considered that its parameters cannot be known in advance, but it has a certain structure.*

Now, we will discuss how to choose a controller u and parameter update laws. We consider the controller structure as follows

$$u(x,y) = u_1(x) + u_2(x,y),$$

where $u_1(x), u_2(x,y) \in \mathbb{R}^m$. Now by choosing

$$u_1(x) = D^{q_r}(K(x)x) - g(K(x)x,\beta) + K(x)(f(x,\tilde{\alpha}) - f(x,\alpha)),$$

the controlled response system (2.8) can be rewritten as

$$\begin{aligned}D^{q_r}y =& g(y,\tilde{\beta}) + D^{q_r}(K(x)x) - g(K(x)x,\beta)\\ &+ K(x)(f(x,\tilde{\alpha}) - f(x,\alpha)) + u_2(x,y).\end{aligned} \tag{2.12}$$

It follows from (2.11) and (2.12) that we have the following error system

$$D^{q_r}e = g(y,\tilde{\beta}) - g(K(x)x,\beta) + K(x)(f(x,\tilde{\alpha}) - f(x,\alpha)) + u_2(x,y). \tag{2.13}$$

We have

$$g(y,\tilde{\beta}) - g(K(x)x,\beta) + K(x)(f(x,\tilde{\alpha}) - f(x,\alpha)) = C_1(x,y,\alpha,\beta)\begin{pmatrix} e\\ e_\alpha\\ e_\beta\end{pmatrix}, \tag{2.14}$$

where $\begin{pmatrix} e\\ e_\alpha\\ e_\beta\end{pmatrix} = (e_1,\ldots,e_m,e_{\alpha_1},\ldots,e_{\alpha_l},e_{\beta_1},\ldots,e_{\beta_k})^T \in \mathbb{R}^{(m+l+k)}$ and $C_1(x,y,\alpha,\beta)$ is an $m\times(m+l+k)$ real matrix.

Therefore, the AMFPS between drive system (2.7) and controlled response system (2.8) is transformed into choose a suitable vector function $u_2(x, y)$ such that system (2.13) is asymptotically converged to zero.

Now, we can selecte vector $u_2(x, y)$ as

$$u_2(x,y) = C_2(x,y,\alpha,\beta)\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}, \tag{2.15}$$

where $C_2(x, y, \alpha, \beta)$ is an $m \times (m + l + k)$ real matrix to be designed. Using Eqs. (2.14) and (2.15), so the error system (2.13) can be rewritten as follows:

$$D^{q_r}e = (C_1(x,y,\alpha,\beta) + C_2(x,y,\alpha,\beta))\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}. \tag{2.16}$$

The parameter adaptation laws can be designed as

$$D^{q_r}\tilde{\alpha} = r(x,y,\tilde{\alpha}) = A\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}, \tag{2.17}$$

$$D^{q_r}\tilde{\beta} = s(x,y,\tilde{\beta}) = B\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}, \tag{2.18}$$

where A and B are $l \times (m+l+k)$ and $k \times (m+l+k)$ real matrices to be designed, respectively. Because the Caputo derivative of a constant is zero, so Eqs. (2.17) and (2.18) can be rewritten as

$$D^{q_r}e_\alpha = D^{q_r}(\tilde{\alpha} - \alpha) = D^{q_r}\tilde{\alpha} = A\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}, \tag{2.19}$$

$$D^{q_r}e_\beta = D^{q_r}(\tilde{\beta} - \beta) = D^{q_r}\tilde{\beta} = B\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}. \tag{2.20}$$

Combining (2.16) with (2.19) and (2.20) we have

$$\begin{pmatrix} D^{q_r}e \\ D^{q_r}e_\alpha \\ D^{q_r}e_\beta \end{pmatrix} = \begin{pmatrix} C_1(x,y,\alpha,\beta) + C_2(x,y,\alpha,\beta) \\ A \\ B \end{pmatrix}\begin{pmatrix} e \\ e_\alpha \\ e_\beta \end{pmatrix}, \tag{2.21}$$

where $\begin{pmatrix} C_1(x,y,\alpha,\beta) + C_2(x,y,\alpha,\beta) \\ A \\ B \end{pmatrix}$ is an $(m+l+k)\times(m+l+k)$ real matrix.

So our aim is to find suitable matrices $C_2(x, y, \alpha, \beta)$, A and B such that the error system (2.21) is asymptotically converged to zero.

Theorem 2.12. *If matrices $C_2 \in \mathbb{R}^{m\times(m+l+k)}$, $A \in \mathbb{R}^{l\times(m+l+k)}$ and $B \in \mathbb{R}^{k\times(m+l+k)}$ in system (2.21) are selected such as*

$$P\begin{pmatrix} C_1(x,y,\alpha,\beta)+C_2(x,y,\alpha,\beta) \\ A \\ B \end{pmatrix} + \begin{pmatrix} C_1(x,y,\alpha,\beta)+C_2(x,y,\alpha,\beta) \\ A \\ B \end{pmatrix}^T P = -Q,$$

where P and Q are real symmetric positive definite matrices, Then for any initial values, system (2.21) is asymptotically stable and AMFPS between systems (2.7) and (2.8) can be achieved, i.e., $\lim_{t\to\infty}||e|| = \lim_{t\to\infty}||e_\alpha|| = \lim_{t\to\infty}||e_\beta|| = 0$.

Proof: According to the Corollary 2.8, the equilibrium point of error dynamical system (2.21) is asymptotically stable. Therefore, the AMFPS between drive and response systems is realized. The proof is completed. □

3. Numerical simulation

In order to verify the effectiveness of the proposed synchronization scheme, we illustrate an example. For the numerical solution of fractional differential equation, the Adams-type predictor-corrector method is used [17].

The fractional-order Chen system [18], as the drive system, is given by

$$\begin{aligned} D^{q_d}x_1 &= \tilde{a}_1(x_2 - x_1), \\ D^{q_d}x_2 &= (\tilde{c}_1 - \tilde{a}_1)x_1 - x_1x_3 + \tilde{c}_1x_2, \\ D^{q_d}x_3 &= x_1x_2 - \tilde{b}_1x_3, \end{aligned} \tag{3.1}$$

where $0 < q_d < 1$ is the fractional-order; x_1, x_2, and x_3 are state variables; $\tilde{a}_1$, $\tilde{b}_1$,$\tilde{c}_1$ are unknown parameters to be estimated. System (3.1) exhibits a chaotic attractor for $(a_1, b_1, c_1) = (35, 3, 28)$ and $q_d = 0.93$ [18].

The fractional-order hyperchaotic Chen system [19], as the response system, is described as follows:

$$\begin{pmatrix} D^{q_r}y_1 \\ D^{q_r}y_2 \\ D^{q_r}y_3 \\ D^{q_r}y_4 \end{pmatrix} = \begin{pmatrix} y_4 + \tilde{a}_2(y_2 - y_1) \\ y_1(\tilde{d}_2 - y_3) + \tilde{c}_2y_2 \\ y_1y_2 - \tilde{b}_2y_3 \\ y_2y_3 + \tilde{r}_2y_4 \end{pmatrix} + u, \tag{3.2}$$

where $0 < q_r < 1$ is the fractional-order;y_1, y_2, y_3 and y_4 are state variables; $\tilde{a}_2$, $\tilde{b}_2$, $\tilde{c}_2$, $\tilde{d}_2$ and $\tilde{r}_2$ are unknown parameters to be estimated. System (3.2) is hyperchaotic for $(a_2, b_2, c_2, d_2, r_2) = (35, 3, 12, 7, 0.5)$ and $q_r = 0.95$ [19].

The AMFPS error between the systems (3.1) and (3.2) is defined by

$$\begin{array}{llll} e_i = y_i - \sum\limits_{j=1}^{3} k_{ij}x_j, & i = 1, 2, \ldots, 4, & & \\ e_{a_1} = \tilde{a}_1 - a_1, & e_{b_1} = \tilde{b}_1 - b_1, & e_{c_1} = \tilde{c}_1 - c_1, & e_{a_2} = \tilde{a}_2 - a_2, \\ e_{b_2} = \tilde{b}_2 - b_2, & e_{c_2} = \tilde{c}_2 - c_2, & e_{d_2} = \tilde{d}_2 - d_2, & e_{r_2} = \tilde{r}_2 - r_2. \end{array}$$

According to the AMFPS scheme, we get $C_1(x, y, \alpha, \beta) = (M\ N\ R)$ where

$$M = \begin{pmatrix} -a_2 & a_2 & 0 & 1 \\ d_2 - \sum\limits_{j=1}^{3} k_{3j}x_j & c_2 & -y_1 & 0 \\ \sum\limits_{j=1}^{3} k_{2j}x_j & y_1 & -b_2 & 0 \\ 0 & \sum\limits_{j=1}^{3} k_{3j}x_j & y_2 & r_2 \end{pmatrix},$$

$$N = \begin{pmatrix} (x_2 - x_1)k_{11} - x_1k_{12} & -x_3k_{13} & (x_1 + x_2)k_{12} \\ (x_2 - x_1)k_{21} - x_1k_{22} & -x_3k_{23} & (x_1 + x_2)k_{22} \\ (x_2 - x_1)k_{31} - x_1k_{32} & -x_3k_{33} & (x_1 + x_2)k_{32} \\ (x_2 - x_1)k_{41} - x_1k_{42} & -x_3k_{43} & (x_1 + x_2)k_{42} \end{pmatrix},$$

$$R = \begin{pmatrix} y_2 - y_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & y_2 & y_1 & 0 \\ 0 & -y_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & y_4 \end{pmatrix}.$$

Now, we can choose real matrix $C_2(x, y, \alpha, \beta) = (H\ O)$ where

$$H = \begin{pmatrix} 0 & 0 & 0 & -1 \\ -d_2 + \sum\limits_{j=1}^{3} k_{3j}x_j - a_2 & -2c_2 & 0 & 0 \\ -\sum\limits_{j=1}^{3} k_{2j}x_j & 0 & 0 & -y_2 \\ 0 & -\sum\limits_{j=1}^{3} k_{3j}x_j & 0 & -2r_2 \end{pmatrix},$$

and O is a 4×8 zero matrix and the parameters update laws as

$$\begin{aligned}
D^{q_r}\tilde{a}_1 =& -(x_2-x_1)(k_{11}e_1+k_{21}e_2+k_{31}e_3+k_{41}e_4)\\
&+x_1(k_{12}e_1+k_{22}e_2+k_{32}e_3+k_{42}e_4)-e_{\tilde{a}_1},\\
D^{q_r}\tilde{b}_1 =& x_3(k_{13}e_1+k_{23}e_2+k_{33}e_3+k_{43}e_4)-e_{\tilde{b}_1},\\
D^{q_r}\tilde{c}_1 =& -(x_1+x_2)(k_{12}e_1+k_{22}e_2+k_{32}e_3+k_{42}e_4)-e_{\tilde{c}_1},\\
D^{q_r}\tilde{a}_2 =& -(y_2-y_1)e_1-e_{\tilde{a}_2},\\
D^{q_r}\tilde{b}_2 =& y_3e_3-e_{\tilde{b}_2},\\
D^{q_r}\tilde{c}_2 =& -y_2e_2-e_{\tilde{c}_2},\\
D^{q_r}\tilde{d}_2 =& -y_1e_2-e_{\tilde{d}_2},\\
D^{q_r}\tilde{r}_2 =& -y_4e_4-e_{\tilde{r}_2}.
\end{aligned}\tag{3.3}$$

Consequently, we obtain the error dynamical system as

$$\begin{aligned}
D^{q_r}e_1 =& a_2(e_2-e_1)+((x_2-x_1)k_{11}-x_1k_{12})e_{a_1}-x_3k_{13}e_{b_1}\\
&+(x_1+x_2)k_{12}e_{c_1}+(y_2-y_1)e_{a_2},\\
D^{q_r}e_2 =& -a_2e_1-c_2e_2-y_1e_3+((x_2-x_1)k_{21}-x_1k_{22})e_{a_1}-x_3k_{23}e_{b_1}\\
&+(x_1+x_2)k_{22}e_{c_1}+y_2e_{c_2}+y_1e_{d_2},\\
D^{q_r}e_3 =& y_1e_2-b_2e_3-y_2e_4+((x_2-x_1)k_{31}-x_1k_{32})e_{a_1}-x_3k_{33}e_{b_1}\\
&+(x_1+x_2)k_{32}e_{c_1}-y_3e_{b_2},\\
D^{q_r}e_4 =& y_2e_3-r_2e_4+((x_2-x_1)k_{41}-x_1k_{42})e_{a_1}-x_3k_{43}e_{b_1}\\
&+(x_1+x_2)k_{42}e_{c_1}+y_4e_{r_2}.
\end{aligned}\tag{3.4}$$

If we choose matrices P and Q in Theorem 2.12 as I (I is an 12×12 identity matrix) and $diag(a_2,c_2,b_2,r_2,1,1,1,1,1,1,1,1)$, respectively, then the AMFPS between systems (3.1) and (3.2) is obtained, and the unknown parameters are estimated using the parameter update laws (3.3).

We choose the fractional orders and the initial values as $q_d=0.93$, $q_r=0.95$, $(x_1(0),x_2(0),x_3(0)) = (1,-4,5)$, $(y_1(0),y_2(0),y_3(0),y_4(0)) = (1,0.1,2,-0.5)$, $(a_1(0),b_1(0),c_1(0))=(28,5,25)$, $(a_2(0),b_2(0),c_2(0),d_2(0),r_2(0))=(32,1,15,10,2)$. Without loss of generality, the scaling function matrix are chosen as

$$K(x)=\begin{pmatrix} x_1+0.4 & -1 & -2\\ -3 & 1 & 0.2x_3-2\\ x_2+3 & 2 & 0.6x_1\\ -0.02x_1x_2 & x_2+2 & x_1-3\end{pmatrix}.$$

Figure 1 displays the convergence of the AMFPS errors. Figure 2 shows the estimated values of the unknown parameters converge to chaotic values.

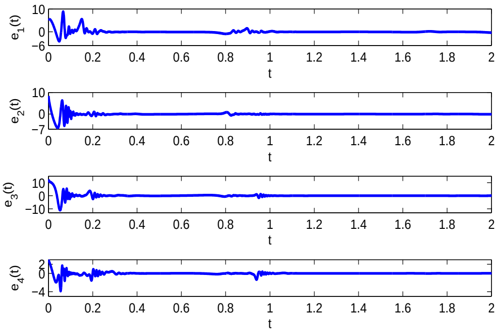
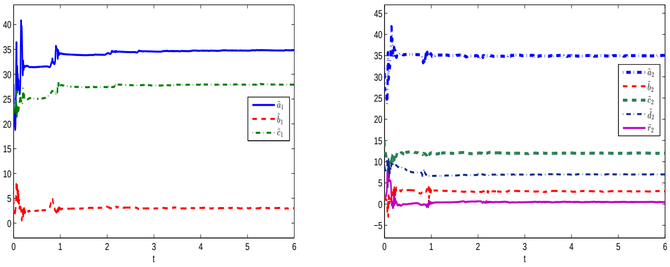


Figure 1: Time evolutions of the error system (3.4).



(a)

(b)

Figure 2: The estimation of the unknown parameters for: (a) chaotic Chen system; (b) hyperchaotic Chen system for AMFPS.

4. Secure communication

In this section, based on the AMFPS scheme, a modified chaotic masking (MCM) digital secure communication method is performed.

The transmitter system is the fractional-order system (2.7) with state variables $x_i(t)$, $i = 1, \ldots, n$ and parameters $(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_l)$ and the receiver system is the fractional-order system (2.8) with different state variables $y_i(t)$, $i = 1, \ldots, m$ and parameters $(\tilde{\beta}_1, \ldots, \tilde{\beta}_k)$.

Assume that $M(t)$ is the original message. At the transmitter, the $M(t)$ is added into the drive system and chaotic signal $\sum_{j=1}^{n} k_{ij}(x(t))x_j(t)$, $i = 1, 2, \ldots, m$, mask the original message. We obtaine the encryption signal $T(t)$ as:

$$T(t) = M(t) + \sum_{j=1}^{n} k_{1j}(x(t))x_j(t) + \ldots + \sum_{j=1}^{n} k_{mj}(x(t))x_j(t). \qquad (4.1)$$

The signal $T(t)$ from the transmitter is sent to the receiver. We can decrypt the encrypted message in receiver by subtracting the synchronized signal from the transmitted signal. Thus, the received signal $R(t)$ by the receiver is as follows:

$$R(t) = T(t) - \sum_{i=1}^{m} y_i(t). \tag{4.2}$$

Using the equation (4.1) and the concept of AMFPS, we have:

$$R(t) = M(t) + \sum_{j=1}^{n} k_{1j}(x(t))x_j(t) + \ldots + \sum_{j=1}^{n} k_{mj}(x(t))x_j(t) - \sum_{i=1}^{m} y_i(t) \cong M(t),$$

and thus we can realize secure communication.

Now, we present the simulations results for the encryption and decryption of the color digital image of Peppers to verify the effectiveness of the proposed scheme. To this end, we use the system (3.1) with state variables $x_i(t)$, $i = 1, 2, 3$ and parameters $(\tilde{a}_1, \tilde{b}_1, \tilde{c}_1)$ as transmitter and the system (3.2) with different state variables $y_i(t)$, $i = 1, 2, 3, 4$ and parameters $(\tilde{a}_2, \tilde{b}_2, \tilde{c}_2, \tilde{d}_2, \tilde{r}_2)$ as receiver. We assume the initial conditions are similar to those in the section 3. Simulation results are shown in Figure 3 with encryption and decryption rules (4.1) and (4.2) for $n = 3$ and $m = 4$.

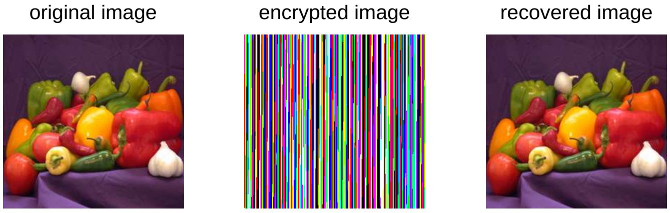


Figure 3: Secure communication based on AMFPS.

5. Security analysis

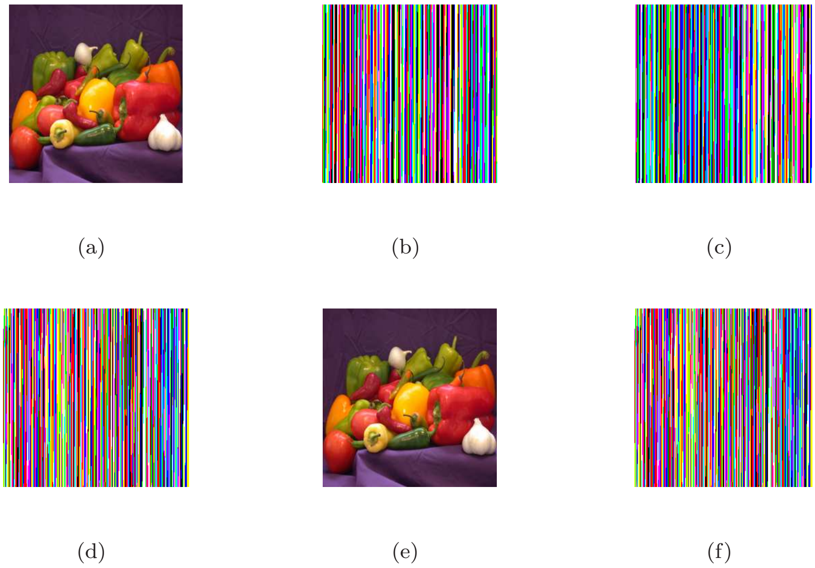
In this section, we analyzed the efficiency of the proposed image cryptosystem by using several security tests, such as: key space analysis, key sensitivity analysis, information entropy, histogram analysis and speed analysis.

5.1. Key space analysis

From the cryptographical standpoint, the size of the key space should be greater than 2^{100} to confirm a high level of security [20]. The proposed encryption scheme contains twenty nine key parameters. If the precision is 10^{-14}, the key space size is $10^{406} \approx 2^{1348}$, which is very large to resist all kinds of brute-force attacks.

5.2. Key sensitivity analysis

In encryption process, we alter the key parameter $x_1(0) = 1$ slightly. For this, we select $x_1(0) = 1 + 10^{-3}$. The encrypted image with $x_1(0) = 1$, the encrypted one with $x_1(0) = 1 + 10^{-3}$ and the difference between two encrypted images are shown in Figures 4(b), 4(c) and 4(d), respectively. The black pixels in Figure 4(d) are the same parts in two encrypted images. The results show that the difference ratio is really high. That means proposed encryption algorithm is so sensitive to key parameters. Also, the test result in decryption process are shown in Figure 4. The decrypted images by using the correct key $x_1(0) = 1$ and the incorrect key $x_1(0) = 1 + 10^{-3}$ are displayed in Figures 4(e) and 4(f), respectively. The sensitivity of the other parameters are similar to $x_1(0)$.



(a) (b) (c)

(d) (e) (f)

Figure 4: Key sensitivity test. (a) Original image; (b) encrypted image with the secret key $x_1(0) = 1$; (c) encrypted image with the secret key $x_1(0) = 1 + 10^{-3}$; (d) difference image; (e) decrypted image (b) with the correct key $x_1(0) = 1$ and (f) decrypted image (b) with the incorrect key $x_1(0) = 1 + 10^{-3}$.

5.3. Information entropy

The information entropy of an information source s is calculated by

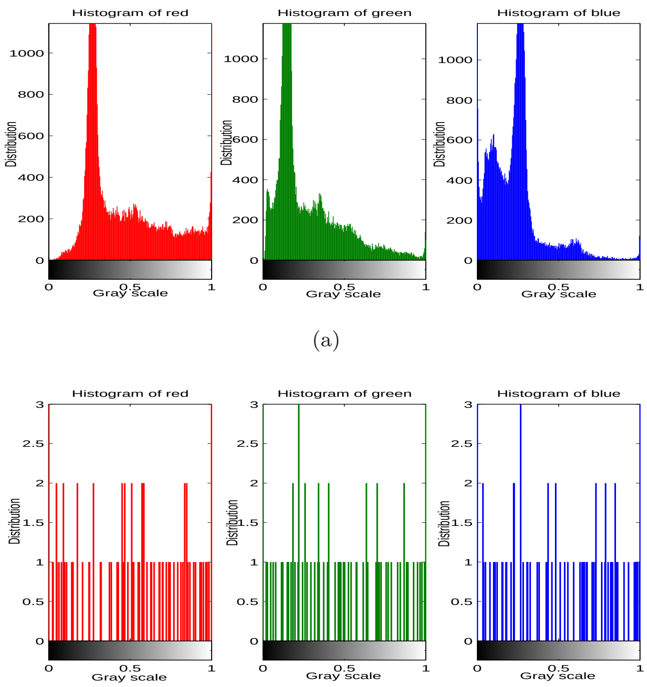
$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i),$$

where N is the number of bits to represent a symbol $s_i \in s$, $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits [21].

The entropy for the three color components of the encrypted image (Figure 4(b)) are $H_R(s) = 7.9259$, $H_G(s) = 7.8422$ and $H_B(s) = 7.9329$. The obtained values are very close to the theoretical maximum value N = 8. This indicate leak of information in the encryption process is negligible and the encryption system is secure against the entropy attack.

5.4. Histogram analysis

The histograms of original image (Figure 4(a)) and encrypted image (Figure 4(b)) in each channel are shown in Figure 5. The histograms of the encrypted image are nearly uniformly distributed. So, no useful information can be extracted from encrypted images and high security can be guaranteed to resist statistical attacks.



(a)

(b)

Figure 5: Histograms of (a) original image; (b) encrypted image.

5.5. Speed analysis

We implement the proposed technique by using Matlab 8.2. The speed performance is tested in a personal computer with an Intel(R) Core(TM) i5-2410M CPU 2.30 GHz, 4.00GB Memory and 1TB hard-disk capacity, and the operating system is Windows 7. The average time used for encryption and decryption on color image Peppers (Figure 4(a)) with size 256 × 256 for 10 times is 0.17 s. We can see that the operation speed of proposed algorithm is very fast compared to the other encryption methods such as [3,22]. Therefore, encryption scheme can be used in internet applications.

6. Conclusions

In this paper, an AMFPS scheme of different dimensions fractional-order chaotic systems with uncertain parameters is discussed. Based on the Lyapunov stability theory of fractional-order systems and the adaptive control theory, the appropriate adaptive controllers and the parameter update laws for estimating the unknown parameters of the systems are gained via novel fractional order controller. The proposed synchronization scheme shows that the AMFPS between drive and response systems with same and different dimensions can be achieved. The theoretical analysis and numerical simulations are provided to show the effectiveness of the proposed methods. Due to the unpredictability of the scaling function matrix and the utilization of different fractional-order systems with different dimensions and unequal orders, this synchronization method can provide additional security in secure communication. Hence, we have proposed a new image encryption algorithm based on AMFPS of fractional-order chaotic system via modified chaotic masking method. Security analysis by using several security test measures is analyzed. Results have demonstrated that the proposed encryption algorithm has a better performance in terms of the sensitivity, security, speed and robustness.

References

1. M.A. Ansari, D. Arora and S.P. Ansari, *Chaos control and synchronization of fractional order delay-varying computer virus propagation model*, Math. Meth. Appl. Sci., 39, 1197-1205, (2016). DOI: 10.1002/mma.3565.

2. D. Wei, X. Wang, J. Hou and P. Liu, *Hybrid projective synchronization of complex Duffing-Holmes oscillators with application to image encryption*, Math. Meth. Appl. Sci., 40(12), 4259-4271, (2017). DOI: 10.1002/mma.4302.

3. X. Wu, Y. Li and J. Kurths, *A new color image encryption scheme using CML and a fractional-order chaotic system*, PLOS ONE, 10(3), 1-28, (2015). DOI:10.1371/journal.pone.0119660.

4. S. K. Agrawal and S. Das, *Projective synchronization between different fractional-order hyperchaotic systems with uncertain parameters using proposed modified adaptive projective synchronization technique*, Math. Meth. Appl. Sci., 37(14), 2164-2176, (2014). DOI: 10.1002/mma.2963.

5. H. Liang, Z. Wang, Z. Yue and R. Lu, *Generalized synchronization and control for incommensurate fractional unified chaotic system and applications in secure communication*, Kybernetika, 48(2), 190-205, (2012).

6. C. Feng, X. Lei and L. Chun-Guang, *Wavelet Phase Synchronization of fractional-order Chaotic Systems*, CHIN. PHYS. LETT., 29(7), 070501, (2012). DOI:10.1088/0256-307X/29/7/070501.

7. Y. Xu, H. Wang, D. Liu and H. Huang, *Sliding mode control of a class of fractional chaotic systems in the presence of parameter perturbations*, J. Vib. Control, 21(3), 435-448, (2015). DOI:10.1177/1077546313486283.

8. R. Mainieri and J. Rehacek, *Projective synchronization in three dimensional chaotic systems*, Phys. Rev. Lett., 82(15), 3042-3045, (1999).

9. G.H. Li, *Modified projective synchronization of chaotic system, Chaos Solitons Fractals*, 32(5), 1786-1790, (2007). DOI:10.1016/j.chaos.2005.12.009.

10. Y. Chen and X. Li, *Function projective synchronization between two identical chaotic systems*, Internat. J. Modern Phys. C, 18(5), 883-888, (2007). DOI:10.1142/S0129183107010607.

11. H.Y. Du, Q.S. Zeng and C.H. Wang, *Modified function projective synchronization of chaotic system*, Chaos Solitons Fractals, 42(4), 2399-2404, (2009). DOI:10.1016/j.chaos.2009.03.120.

12. H.T. Yau, Y.C. Pu and S.C. Li, *Application of a Chaotic Synchronization System to Secure Communication*, Inf. Technol. control, 41(3), 274-282, (2012). DOI:10.5755/j01.itc.41.3.1137.

13. M. Caputo, *Linear models of dissipation whose Q is almost frequency independent-II*, Geophys J. R. Astron. Soc., 13(5), 529-539, (1967). DOI:10.1111/j.1365-246X.1967.tb02303.x.

14. Y. Li, Y. Chen and I. Podlubny, *Stability of fractional-order nonlinear dynamic systems: Lyapunov direct method and generalized Mittag Leffler stability* Comput Math Appl., 59(5), 1810-1821, (2010). DOI:10.1016/j.camwa.2009.08.019.

15. M.A. Duarte-Mermoud, N. Aguila-Camacho, J.A. Gallegos and R. Castro-Linares, *Using general quadratic Lyapunov functions to prove Lyapunov uniform stability for fractional order systems*, Commun. Nonlinear Sci. Numer. Simul., 22(1), 650-659, (2015). DOI:10.1016/j.cnsns.2014.10.008.

16. J.J. Slotine and W. Li, *Applied nonlinear control*, Prentice Hall, (1991).

17. K. Diethelm, N. Ford and A. Freed, *A predictor-corrector approach for the numerical solution of fractional differential equations*, Nonlinear Dynam., 29(1), 3-22, (2002). DOI:10.1023/A:1016592219341.

18. C.G. Li and G.R. Chen, *Chaos in the fractional order Chen system and its control*, Chaos Solitons Fractals, 22(3), 549-554, (2004). DOI:10.1016/j.chaos.2004.02.035.

19. X. Wu and Y. Lu, *Generalized projective synchronization of the fractional-order Chen hyperchaotic system*, Nonlinear Dynam, 57(1), 25-35, (2009). DOI:10.1007/s11071-008-9416-5.

20. D.R. Stinson, *Cryptography: Theory and Practice*, Boca Raton, CRC Press, (2005).

21. C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell Syst. Tech. J., 28(4), 656-715, (1949). DOI:10.1002/j.1538-7305.1949.tb00928.x.

22. N.K. Pareek, *Design and analysis of a novel digital image encryption schem*, Internat. J. Netw. Secur. Appl., 4(2), 95-108, (2012). DOI: 10.5121/ijnsa.2012.4207.

Vajiheh Vafaei,
Faculty of Mathematical Sciences,
University of Tabriz,
Tabriz-Iran.
E-mail address: v_vafaei@tabrizu.ac.ir

and

Hossein Kheiri,
Faculty of Mathematical Sciences,
University of Tabriz,
Tabriz-Iran.
E-mail address: h-kheiri@tabrizu.ac.ir

and

Aliasghar Jodayree Akbarfam,
Faculty of Mathematical Sciences,
University of Tabriz,
Tabriz-Iran.
E-mail address: akbarfam@yahoo.com