The ISC Int'l Journal of Information Security

ISeCure

January 2020, Volume 12, Number 1 (pp. 55–66)

http://www.isecure-journal.org

Modified Sliding-Mode Control Method for Synchronization a Class of Chaotic Fractional-Order Systems with Application in Encryption

Bashir Naderi [1,*], Hossein Kheiri [2] and Vajiheh Vafaei [3]

[1] *Department of Mathematics, Payame Noor University, P.O. Box 19395-3697, Tehran, Iran*
[2] *Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran*
[3] *Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran*

ARTICLE INFO.

Article history:
Received: 16 November 2018
Revised: 28 June 2019
Accepted: 10 October 2019
Published Online: 22 December 2019

Keywords:
Fractional-order Systems, Chaos, Sliding-mode Control, Synchronization, Secure Communication.

Abstract

In this study, we propose a secure communication scheme based on the synchronization of two identical fractional-order chaotic systems. The fractional-order derivative is in Caputo sense, and for synchronization, we use a robust sliding-mode control scheme. The designed sliding surface is taken simply due to using special technic for fractional-order systems. Also, unlike most manuscripts, the fractional-order derivatives of state variables can be chosen differently. The stability of the error system is proved using the Lyapunov stability of fractional-order systems. Numerical simulations illustrate the ability and effectiveness of the proposed method. Moreover, synchronization results are applied to secure communication using the masking method. The security analysis demonstrates that the introduced algorithm has a large keyspace, high sensitivity to encryption keys, higher security, and the acceptable performance speed.

1 Introduction

In recent years, fractional-order systems have been enormously used in different sciences, such as secure communication [1–3], viscoelastic systems [4], heat conduction [5], chemical reactor system [6], image encryption [7], modeling electrical circuits [8], estimate the crankability of lead-acid batteries [9], modeling human T-cell lymphographic virus [10], infection of $CD4^+$ T-cells [10, 11], some finance systems [12].

Researchers have considered chaos and chaotic behavior as real-world phenomena in recent years. The behavior of some fractional dynamical systems can be chaotic. Chaotic systems, as nonlinear deterministic systems, display complex and unusual behaviors. A chaotic system at least has one positive Lyapunov exponents. Researchers have studied some of the fractional-order chaotic systems such as fractional-order Lorenz system [13], fractional-order Rössler system [14], fractional-order chemical reactor model [6], fractional-order Chen system [15], fractional-order Lü system [16], complex fractional-order T-system [17] and some other fractional-order chaotic systems that can be fined in [4, 8, 12, 18].

Although at the beginning of the introduction of chaotic systems, synchronization seemed impossible. The synchronization of chaotic systems was firstly discussed in 1990 by Pecora and Carrol [19]. Then, the synchronization of chaotic systems has been widely

* Corresponding author.
Email addresses: b_naderi@pnu.ac.ir, h-kheiri@tabrizu.ac.ir, v_vafaei@tabrizu.ac.ir
ISSN: 2008-2045

investigated in theory and application such as secure communications, chemical systems, modeling brain activities, etc. [20–26].

In ordinary dynamical system different methods such as adaptive control, active control, sliding-mode control, nonlinear and linear control were used for synchronization [21, 26–30]. Recently the extension of control and synchronization methods in the integer-order dynamical system to the fractional-order dynamical system have been considered. Because, in the case of a fractional system, the presence of an order parameter increases the size of the keyspace and therefore increases the security of encryptions. For example, the methods active control [31], projective synchronization [32], adaptive synchronization [33], complete and generalized synchronization [34], exponential synchronization [35], linear and nonlinear feedback synchronization [36] were successfully applied for synchronization of fractional-order systems. Many researchers have studied the using of synchronizing of fractional-order dynamical systems such as viscoelastic and electromagnetic [37, 38], control theory and robotics [39], gyroscope [40], physiology [41], and physical sciences [42–44].

One of the most important applications of chaos synchronization is secure communication. The general idea for secure communication via chaotic systems is that an information signal is embedded in a transmitter system, which produces a chaotic signal. Then, the sending information signal recovered by the chaotic receiver such that the transmitter and receiver system are synchronized with choosing proper controllers. Chaos and synchronization in the fractional-order dynamical systems have caused these systems to be attention in secure communication. Secure communication based on chaotic techniques includes chaos masking, chaos modulation, and chaos shift keying. In chaos masking, an information signal is combined with a chaotic signal before it is sent. Chaos modulation is based on the synchronization such that the information signal is injected into the transmitter system. In chaos shift keying, an information signal is a binary signal that is mapped into the transmitter and the receiver. In these three cases, the recovering of information signal achieved based on the synchronization of the transmitter and the receiver [45–47]. More information about the chaos masking approach, chaotic shift keying and modulation method can be found in [20, 26, 48–53]. Recently, several fractional-or integer-order chaotic systems have been introduced and the synchronization of them discussed via methods such as adaptive, fractional sliding-mode, and nonlinear feedback control. Some manuscripts used these systems for secure communication [7, 20, 24, 54–58]. The used sliding-mode method in most papers is very complex and designed controllers for synchronization are composed of fractional derivative or fractional integral [40, 59].

Motivated by the applicability of chaotic fractional-order systems and synchronization of them, in this paper, we discuss the synchronization of two identical fractional-order chaotic systems and use it in secure communication. For synchronization, we consider fractional-order chaotic dynamical systems that the diameter of the matrix linear part of the system is non-positive. The robust sliding-mode control scheme with a simple surface is used for synchronization. The stability of the method is investigated by the Lyapunov stability lemma in the fractional-order system. In most articles, Lyapunov functions for synchronizing of two systems were chosen such that the obtained controller has fractional derivative or fractional integral. In this paper, to overcome this difficulty, we use the method introduced in [60]. The designed sliding-mode controller is simple and does not compose of fractional derivative or fractional integral. In this paper, unlike most manuscripts, the fractional-order derivative of state variables can be different and also, the designed sliding surface is simple.

Moreover, the synchronization result is applied to secure communication via the masking method. A digital image and a continuous signal are used to demonstrate the efficiency of the proposed method. We analyze the validity of the proposed scheme by using several security test measures, such as keyspace analysis, key sensitivity analysis, histogram analysis, and speed analysis. The results demonstrate that higher security, large keyspace, and the acceptable encryption speed can be guaranteed to resist all kinds of brute-force and statistical attacks.

The rest of this paper is organized as follows: Section 2 briefly introduces the fractional calculus and stability of fractional-order systems. In Section 3, the synchronization of two identical fractional-order chaotic systems and numerical simulations are addressed. In Section 4, the discussed synchronization is applied in secure communication based on the masking method. The effectiveness of the proposed scheme is evaluated with simulations for continuous signals and digital images. The security analysis of the proposed secure communication method is presented in Section 5. The speed analysis is explained in Section 6 Finally, concluding remarks are presented in Section 7.

2 Fractional Calculus and Stability of Fractional-Order Systems

In this section, we review some fundamental definitions of fractional calculus. Also, we present some useful stability lemmas of fractional-order dynamical systems.

In fractional calculus, the traditional definitions of the integral and derivative of a function were generalized from integer orders to real orders. There are several definitions for fractional derivatives of order $\alpha \geq 0$, but the Caputo definition in 1 has been used in most engineering applications; Because this definition is suitable for fractional order problems with initial conditions. Because the initial condition for Caputo definition is integer-order derivatives at $t = 0$, therefore Caputo is more suited to engineering applications. This definition is suitable for fractional-order problems with initial conditions.

Definition 1. [61] The Caputo fractional derivative for function $f \in C^n[0, +\infty]$ is:

$$ {}^C D_0^\alpha f(\tau) = \frac{1}{\Gamma(n-\alpha)} \int_0^\tau (\tau - t)^{(n-\alpha-1)} f^{(n)}(t) dt, \tag{1}$$

where $\alpha > 0$, $n = [\alpha] + 1$, ${}^C D^\alpha$ is Caputo fractional derivative and Γ is Gamma function

$$\Gamma(\alpha) = \int_0^\infty t^{\alpha-1} e^t dt.$$

In this paper, for simplicity, we use the notation D^α to denote ${}^C D_0^\alpha$.

For stability analysis of the fractional-order system, consider

$$\begin{aligned} D^{\alpha_1} x_1 &= f_1[x_1, x_2 \cdots, x_n] \\ D^{\alpha_2} x_2 &= f_2[x_1, x_2 \cdots, x_n] \\ &\vdots \\ D^{\alpha_n} x_n &= f_n[x_1, x_2 \cdots, x_n], \end{aligned} \tag{2}$$

where $0 < \alpha_i < 1,\ i = 1, 2, \cdots, n$ are real numbers. In this paper, we use the described method in [60] for asymptotic stability analysis of the obtained error system from synchronization of master and slave systems.

Lemma 1. *[60]. If $x(t) \in \mathbb{R}$ be continuous and derivable function, then for any time instant $t > 0$*

$$\frac{1}{2} D^\alpha x^2(t) \leq x(t) D^\alpha x(t), \qquad \forall \alpha \in (0, 1). \tag{3}$$

This property can be extended to vector functions.

Lemma 2. *[60]. The Lemma 1 also holds in the case that x is a vector. It mains $\forall \alpha \in (0, 1)$ and $\forall t > 0$*

$$\frac{1}{2} D^\alpha x^T(t) x(t) \leq x^T(t) D^\alpha x(t), \qquad \forall \alpha \in (0, 1). \tag{4}$$

Using of Lemma 2 we have

Theorem 1. *[60] Let $x = 0$ is an equilibrium point of*

$$D^\alpha x(t) = f(x(t)). \tag{5}$$

If condition

$$x(t)^T f(x(t)) \leq 0, \ \ \forall x \tag{6}$$

is satisfied, then the origin of the system (5) is stable. And if

$$x(t)^T f(x(t)) < 0, \ \ \forall x \neq 0, \tag{7}$$

then the origin of the system (5) is asymptotically stable.

Assume that the results of Theorem 1 are satisfied and $V(x) = \frac{1}{2} ||x||^2 = \frac{1}{2} x^T x$. Then we can result

$$D^\alpha V \leq x(t)^T D^\alpha x(t) = x(t)^T f(x(t)) \leq 0 \ \forall x \tag{8}$$

and

$$D^\alpha V = x(t)^T D^\alpha x(t) = x(t)^T f(x(t)) < 0 \ \forall x \neq 0. \tag{9}$$

Therefor $V(x)$ is a Lyapunov function respect system (5).

3 Synchronization via Modified Sliding-Mode Controller

For synchronization of two identical fractional chaotic systems, we consider the master system as form

$$D^\alpha x = f(x) = Ax + F(x), \tag{10}$$

where $x = [x_1, x_2, \cdots, x_n]^T$, $f = [f_1, f_2, \cdots, f_n]^T$, $D^\alpha x = [D^{\alpha_1} x_1, D^{\alpha_2} x_2, \cdots, D^{\alpha_n} x_n]^T$ and $F = [F_1, F_2, \cdots, F_n]^T$. In (10) Ax is linear part with property $a_{ii} \leq 0, i = 1, 2, \cdots, n$ such that a_{ij} is element of $A = (a_{ij})_{n\times n}$ and $F(x)$ is a nonlinear part of system. We define the slave system as follow

$$D^\alpha y = f(y) = Ay + F(y) + u, \tag{11}$$

where $u = (u_1, u_2, \cdots, u_n)^T$ is control signal. The synchronization error is defined $e = y - x$. Then, the fractional-order error system between master and slave systems is

$$\begin{aligned} D^\alpha e &= f(y) - f(x) = Ae + F(y) - F(x) + u \\ &= Ae + F(e + x) - F(x) + u. \end{aligned} \tag{12}$$

Our aim of synchronization is to design a simple sliding surface and simple controller u, so that for any initial condition y_0 and x_0:

$$\lim_{t\to\infty} \|e\| = \lim_{t\to\infty} \|y(t) - x(t)\| = 0,$$

where $\|.\|$ is the Euclidean norm.

One of the most important methods in the area of robust control is sliding-mode control [62, 63]. The capability of the sliding-mode control approach is its application for systems with uncertainty. In the sliding-mode control scheme, the discontinuous feedback law replaced with high-gain linear feedback. Recently, the sliding-mode method has been used for synchronization of fractional-order systems, such that, the designed controllers and sliding surface are very complex [40, 59]. In this paper, we design the sliding surface and controllers similarity the integer-order dynamical systems but prove the stability of the method based on the Lyapunov theorem in fractional-order system [60]. The first step, to design sliding-mode control is selecting an appropriate sliding surface [40, 62, 63]. In most of the papers the sliding surface has been given in complicated form due to fractional integration. In this paper, we choose it in a simple form

$$S(t) = [s_1, s_2, \cdots, s_n] = [\lambda_1 e_1, \lambda_2 e_2, \cdots, \lambda_n e_n], \tag{13}$$

where λ_i are positive constants. This choice simplifies the later calculations. The next step is to determine the amount of control signal u such that the error system trajectories reach the sliding surface $S(t) = 0$.

To achieve the stability of the error system in the sliding surface, we assume that each element of the main diagonal of matrix A is non-positive. So, we have the following results.

Theorem 2. *Consider the error system (12) with $\alpha_1 = \alpha_2 = \cdots = \alpha_n$ and*

$$u = -F(y) + F(x) - (A - D)e - \eta sign(e), \tag{14}$$

where $\eta = (\eta_1, \eta_2, \cdots, \eta_n)$ and D is the diagonal of A with non-positive elements. Then the error system will converge to zero and synchronization properties between two master and slave system will achieve.

Proof. We define the Lyapunov function on surface S in (13), as follow

$$V(t) = \tfrac{1}{2} S S^T = \textstyle\sum_{i=1}^{n} \frac{s_i^2}{2\lambda_i^2}. \tag{15}$$

Therefor

$$\begin{aligned} D^\alpha V &= \textstyle\sum_{i=1}^{n} \frac{s_i D^\alpha s_i}{\lambda_i^2} = \sum_{i=1}^{n} e_i D^\alpha e_i = e(D^\alpha e)^T \\ &= e(Ae + F(e+x) - F(x) + u)^T \\ &= e(Ae + F(e+x) - F(x) - F(y) + F(x) \\ &-(A-D)e - \eta sign(e)) \\ &= e(De - \eta sign(e)) \\ &= \textstyle\sum_{i=1}^{n} (e_i^2 a_{ii} - \eta_i |e_i|). \end{aligned} \tag{16}$$

According to $a_{ii} \le 0$, we have

$$D^\alpha V = \textstyle\sum_{i=1}^{n} (e_i^2 a_{ii} - \eta_i |e_i|) \le 0. \tag{17}$$

Then the slave system is synchronized with master system via the sliding-mode control. □

Despite of theorem 2 in the following theorem we let α_i $(i = 1, ..., n)$ be different.

Theorem 3. *Consider the error dynamical system (12) with $\alpha_i \neq \alpha_j$ for some i and j and controller (14). Then the error system will converge to zero and synchronization properties between two master and slave system will achieve.*

Proof. We define a Lyapunov function in surface S given (13) in vector form

$$V(t) = (V_1, V_2, \cdots, V_n) = \tfrac{1}{2}(\tfrac{s_1^2}{\lambda_1^2}, \tfrac{s_2^2}{\lambda_2^2}, \cdots, \tfrac{s_n^2}{\lambda_n^2}). \tag{18}$$

Therefor

$$\begin{aligned} D^\alpha V &= (D^{\alpha_1} V_1, D^{\alpha_2} V_2, \cdots, D^{\alpha_n} V_n) \\ &= (\frac{s_1 D^{\alpha_1} s_1}{\lambda_1^2}, \frac{s_2 D^{\alpha_2} s_2}{\lambda_2^2}, \cdots, \frac{s_n D^{\alpha_n} s_n}{\lambda_1^2}) \\ &= (e_1 D^{\alpha_1} e_1, e_2 D^{\alpha_2} e_2, \cdots, e_n D^{\alpha_n} e_n) \\ &= (e_1(f_1(y) - f_1(x) + u_1), \cdots, \\ &\quad e_n(f_n(y) - f_n(x) + u_n). \end{aligned} \tag{19}$$

Now by substituting $u = (u_1, u_2, \cdots, u_n)$ from (14) in (19), we have

$$\begin{aligned} D^\alpha V = &(e_1^2 a_{11} - \eta_1 |e_1|, e_2^2 a_{22} - \eta_2 |e_2|, \cdots, \\ &e_n^2 a_{nn} - \eta_n |e_n|). \end{aligned} \tag{20}$$

Considering $a_{ii} \le 0$, we conclude

$$e_i^2 a_{ii} - \eta_i |e_i| \le 0. \tag{21}$$

So the condition of Lemma 1 is satisfied for any element of error system. It implies the error system is stable. Then the master-slave system is synchronized via the sliding-mode control. □

Remark 1. [64] The $sign(e_i)$ function, as a rigid switcher, in the control law (14), may cause undesirable oscillations. In order to avoid this problem, the $sign(e_i)$ function in the controller (14) is approximated by the $\tanh(e_i)$.

3.1 Numerical Simulation of Synchronization

In this subsection, a numerical simulation is given to illustrate the theoretical results of the mentioned theorems. For this purpose, we consider the chaotic fractional-order Lorenz system

$$\begin{cases} D^{\alpha_1} x_1 &= \sigma(x_2 - x_1) \\ D^{\alpha_2} x_2 &= \rho x_1 - x_2 - x_1 x_3 \\ D^{\alpha_3} x_3 &= x_2 x_1 - \beta x_3, \end{cases} \tag{22}$$

where $\sigma = 10$, $\rho = 28$, $\beta = \frac{8}{3}$ and $0.993 \le \alpha_i < 1$ [13].

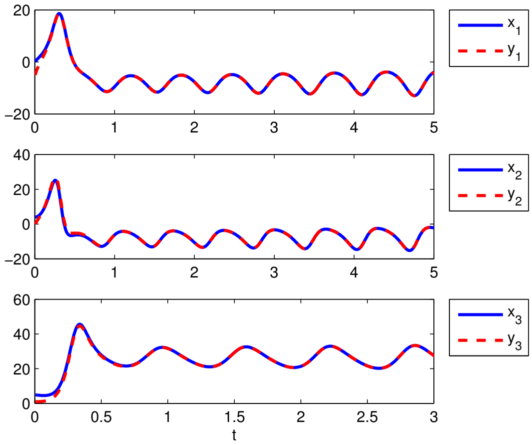


Figure 1. Synchronization of two identical Lorenz fractional-order systems with same order

Assume the system (22) is the master system and define the slave system as follow

$$\begin{cases} D^{\alpha_1} y_1 &= \sigma(y_2 - y_1) + u_1 \\ D^{\alpha_2} y_2 &= \rho y_1 - y_2 - y_1 y_3 + u_2 \\ D^{\alpha_3} y_3 &= y_2 y_1 - \beta y_3 + u_3. \end{cases} \tag{23}$$

According to Theorems 2, 3 and Remark 1, we have

$$\begin{cases} u_1 &= -3\tanh(y_1 - x_1) - \sigma(y_2 - x_2) \\ u_2 &= -5\tanh(y_2 - x_2) - (\rho + x_3)(y_1 - x_1) \\ &\quad +(y_3 - x_3)y_1 \\ u_3 &= -2\tanh(y_3 - x_3) - x_1(y_2 - x_2) \\ &\quad -x_2(y_1 - x_1) - (y_1 - x_1)(y_2 - x_2). \end{cases} \tag{24}$$

Numerical simulations are given for the following cases

- ***The order of derivatives be same***
  Let $\alpha_1 = \alpha_2 = \alpha_3 = 0.995$ and assume the initial conditions $x(0) = (0.1, 4, 5)$ and $y(0) = (-5, 0, 1)$. The results are given in Figure 1 and Figure 2.
- ***The order of derivatives be different***
  Let $\alpha_1 = 0.995$, $\alpha_2 = 0.997$ and $\alpha_3 = 0.994$, and assume the initial conditions $x(0) = (-0.1, 1, 5)$ and $y(0) = (-4, -1, 3)$. The results are given in Figure 3 and Figure 4.

The figures 1-4 display that the slave and master systems are synchronized after a short time. For more explanation, the synchronization times are given in Table 1. Also, figures 5 and 6 shows the numerical simulation of controllers, such that the controllers, like the error synchronization, arrive to zero after a short time.

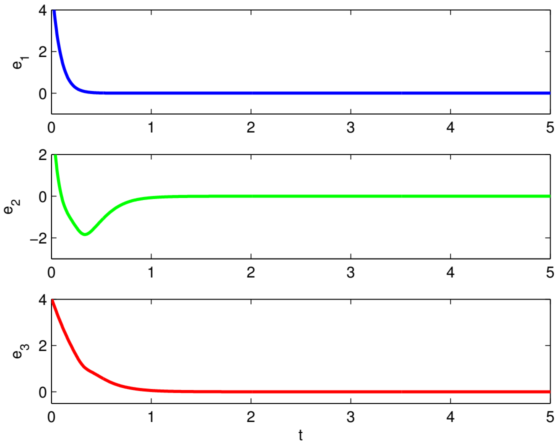


Figure 2. Error synchronization of two identical Lorenz fractional-order systems with same order

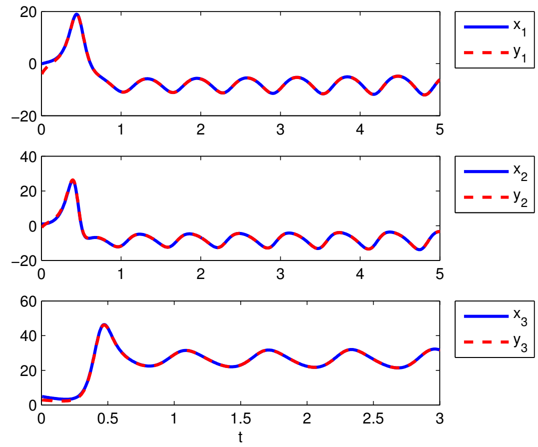


Figure 3. Synchronization of two identical Lorenz fractional-order systems with different order

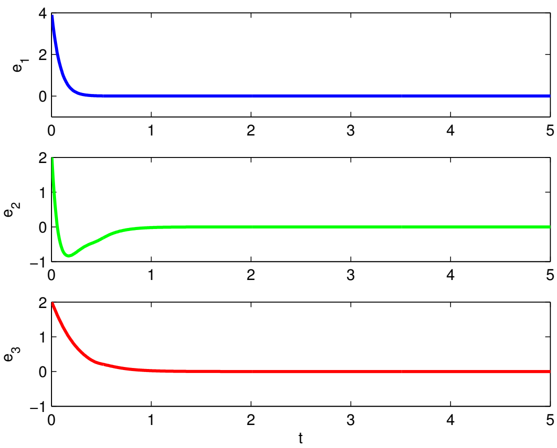


Figure 4. Error synchronization of two identical Lorenz fractional-order systems with different order

Table 1. Synchronization time

Error of state	e_1	e_2	e_3
Same order	0.38	0.85	0.93
Different order	0.35	0.75	0.90

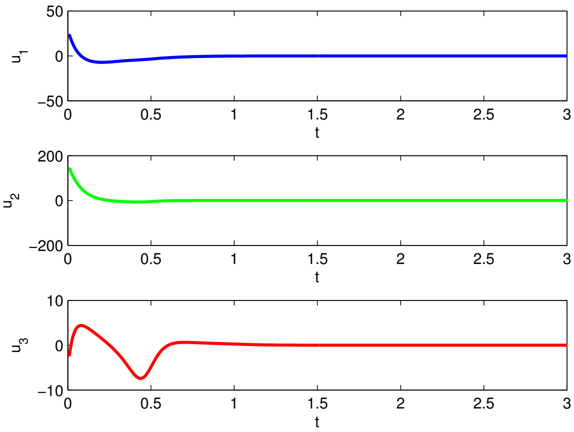


Figure 5. Control signal for synchronization of different order fractional-order Lorenz system

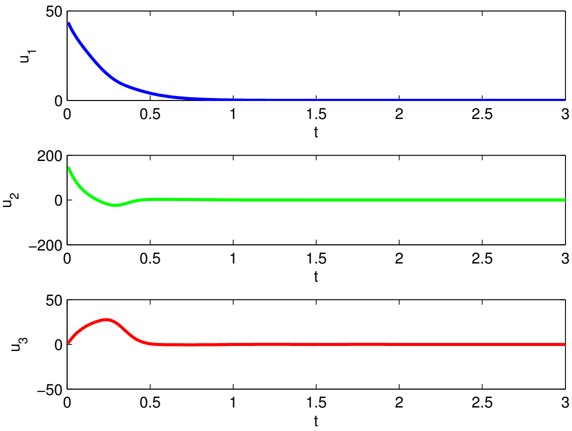


Figure 6. Control signal for synchronization of same order fractional-order Lorenz system

4 Secure Communication based on Masking Method

This section addresses masking method for secure communication scheme based on synchronization of two fractional-order chaotic systems.

According Theorems 2 and 3, the architecture of the proposed secure communication scheme is established by two fractional-order chaotic systems and designed sliding mode controllers. The overall process of the secure communication is shown in Figure 7.

At the transmitter side, fractional-order system (10)

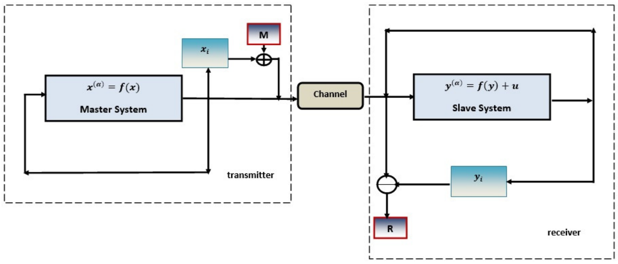


Figure 7. Diagram of secure communication based on synchronization of two identical fractional-order system

with state variables $x_i(t)$ generates chaotic signals, are used as the master system. In the receiver side, system (11) has the same structure as system (10) with state variables $y_i(t)$, such that the sliding mode controller is employed to synchronizing the two fractional-order chaotic systems. At the transmitter side, the original message $M(t)$ is combined by the chaotic signal $x_1(t)$. The combined message is shown with $T(t)$ and is defined

$$T(t) = M(t) + x_1(t). \tag{25}$$

$M(t)$ must be well chosen in a way that it can be successfully masked by $x_1(t)$. Otherwise, the original message $M(t)$ is multiplied by a scaling factor [23] is used for resizing the original message.

For sending all signals (state variables and $T(t)$) from a transmitter to receiver, a public channel is used. By Theorems 2 and 3, the chaotic synchronization will be achieved by the sliding mode controller. After T_c a time greater than T_s (T_s is the synchronization time) synchronization will occur. The received signal by the receiver is recoverable with following equation:

$$R(t) = T(t) - y_1 \cong M(t). \tag{26}$$

Because, according to the concept of synchronization we have:

$$R(t) = M(t) + x_1(t) - y_1(t) \cong M(t). \tag{27}$$

The encrypted signal is transmitted through the public channel, which is open to any intruder. However, the infiltrators are not able to decode the message, even if they are aware of the structure of the chaotic system in the sender. Since the initial conditions, the designed controller, and the synchronized time T_c are completely unknown, it would be extremely difficult for an intruder to recover the masked messages. It is also noted that even an extremely small deviation of the correct encryption keys will lead to a completely different result due to the systems chaotic nature, thus increasing the difficulty for intruders to recover the original message. Therefore, the secure communication design based on the masking technique and the proposed method for the

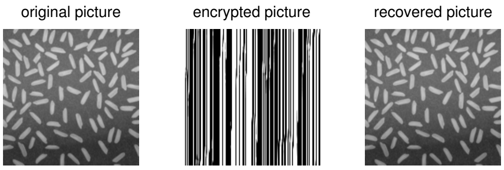


Figure 8. Secure communication based on synchronization for Black-white digital image

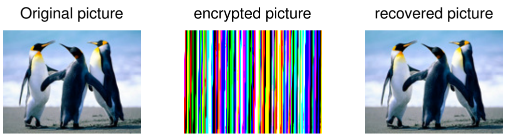


Figure 9. Secure communication based on synchronization for colored digital image

synchronization of fractional-order systems by the sliding method is stable and practical.

In subsection 3.1, the numerical simulation of the synchronization of fractional-order Lorenz system via the sliding mode control method was discussed. To evaluate the feasibility of the proposed secure communication scheme, numerical simulations are given in the following subsection.

4.1 Numerical Simulation of Secure Communication

To check the validity of the mentioned technic, we illustrate the simulation results for the encryption and decryption of continuous signal and digital images. All the simulations are carried out by the MATLAB software. We assume the initial conditions and requirement parameters similar to those in subsection 3.1. Encryption and decryption happen after synchronization time T_s. When an image is obtained using MATLAB in data form in a matrix, directly combined with the signal dynamical system is not possible. So we first convert the obtained matrix in a vector form with elements that are written in double format. For illustrating the ability of the presented method we apply it on the continues signal $M(t) = 0.8\sin(10\pi t)$, black-white and color digital images. Simulation results are shown in figures 8-10 with encryption and decryption rules (25) and (26).

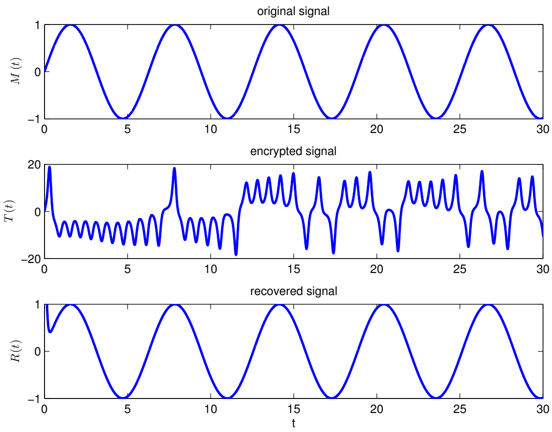


Figure 10. Secure communication based on synchronization for continuous signal

Table 2. Comparison of our proposed method and some other cryptosystems.

Algorithm	keyspace size	Encryption Time (seconds)
The proposed algorithm	2^{558}	< 0.23
Ref. [66]	2^{144}	> 0.22
Ref. [67]	2^{96}	10.9689
Ref. [56]	2^{280}	1.25
Ref. [68]	2^{40}	2.901

5 Security Analysis

In this section, we analyzed the effectiveness of the proposed secure communication scheme by several security tests, such as keyspace analysis, key sensitivity analysis, statistical analysis, and speed analysis. We consider the color digital image in the case that the order of derivatives is the same. The security analysis of other cases is similar.

5.1 Keyspace Analysis

From the standpoint of encryption, the size of the keyspace should be greater than 2^{100} to confirm higher security [65]. The introduced scheme contains twelve key parameters. When the precision is 10^{-14}, the keyspace size is $10^{168} \approx 2^{558}$, which is large to resist all kinds of brute-force attacks. This amount is larger than those in references [56, 66–68]. Table 2 shows the comparison of the keyspace analysis between the proposed encryption method and other image cryptosystems in [56, 66–68].

5.2 Key Sensitivity Analysis

To analyze sensitivity, we change the key parameter $x_2(0) = 4$ to $x_2(0) = 4 + 10^{-3}$. The encrypted picture

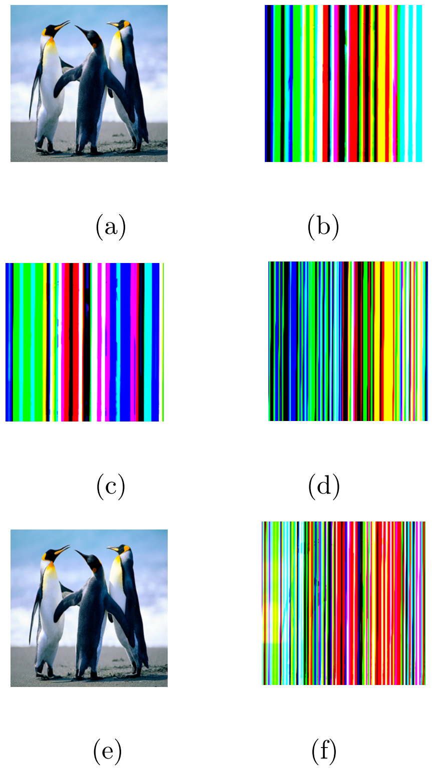


Figure 11. Key sensitivity test. (a) Original picture; (b) encrypted picture with the secret key $x_2(0) = 4$; (c) encrypted picture with the secret key $x_2(0) = 4+10^{-3}$; (d) difference picture; (e) decrypted picture (b) with the correct key $x_2(0) = 4$ and (f) decrypted picture (b) with the incorrect key $x_2(0) = 4 + 10^{-3}$.

with $x_2(0) = 4$, the encrypted one with $x_2(0) = 4 + 10^{-3}$ and the difference between two encrypted pictures are shown in Figure 11(b), Figure 11(c) and Figure 11(d), respectively. The black pixels in Figure 11(d) are the same parts in two encrypted picture. The results show that the difference ratio is really high. That means the proposed algorithm is highly sensitive to key parameters. Also, the test results in decryption process are shown in Figure 11. The decrypted pictures by the correct key $x_2(0) = 4$ and the incorrect key $x_2(0) = 4 + 10^{-3}$ are displayed in Figure 11(e) and Figure 11(f), respectively. As we see in Figure 11(e) and Figure 11(f), only one correct key can decrypt an encrypted picture. The sensitivity of the other parameters are similar to $x_2(0)$.

5.3 Histogram Analysis

A histogram of image is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to recognize the entire tonal distribution at a glance. Histogram images are plotted to show the distribution of tonal in the encrypted image. For more detail, interesting reader can see [7, 69]. The histograms of picture (Figure 11(a)) and encrypted picture (Figure 11) in each channel are shown in Figure 12. The histograms of the encrypted picture are almost uniformly distributed and noticeably different from those of the original image.

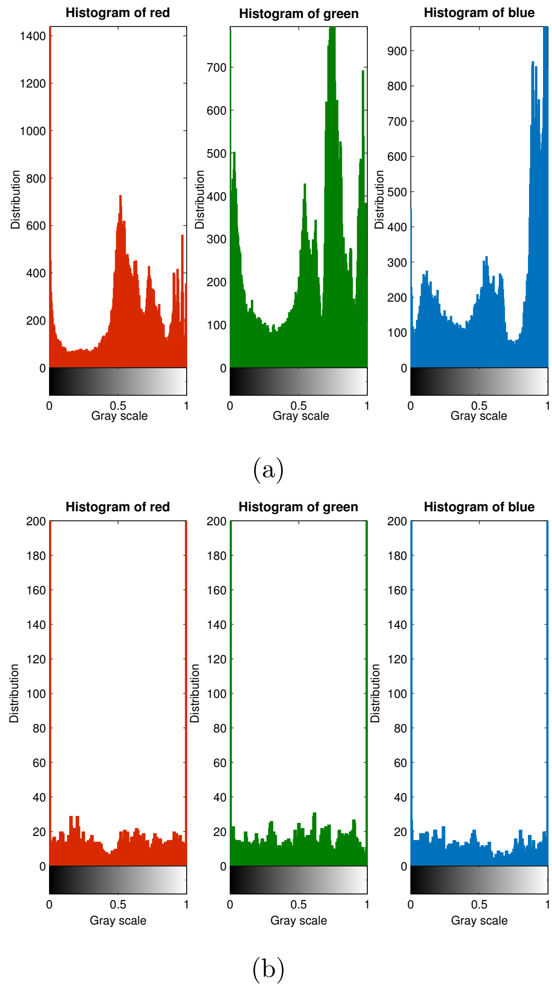


Figure 12. Histograms of (a) original picture; (b) encrypted picture.

6 Speed Analysis

The speed performance is tested in a personal computer with an Intel(R) Core(TM) i7-7700K CPU 4.20 GHz, 8.00GB Memory and 1TB hard-disk capacity, by using Matlab 8.2 and the operating system is Windows 7. The average time used for encryption and decryption on Figure 11(a) with size 256×256 for 10 times is 0.12 s. We can see that the operation speed of this scheme is very fast compared to the other encryption methods such as [56, 66–68]. Table 2 shows the comparison of the speed analysis between the proposed scheme and other image cryptosystems in [56, 66–68, 70].

7 Conclusions

In this paper, a secure communication based on synchronization of two identical chaotic fractional-order system via masking method presented. For synchronization, a robust sliding mode controller was designed to study the synchronization of two identical fractional-order systems. The obtained control was satisfied Lyapunov stability theorem of fractional-order. In comparing similar works, the considered sliding surface was simple. The results of the synchronization showed that the errors are asymptotically convergent. Security analysis of the proposed masking secure communication method showed the effectiveness of the proposed method. In future work, we will try to implement the modulation method to fraction order differential equations with different orders and unknown parameters.

References

[1] Rui-Guo Li and Huai-Ning Wu. Adaptive synchronization control based on "qpso" algorithm with interval estimation for fractional-order chaotic systems and its application in secret communicatio. *Nonlinear Dynamics*, 92(3):935–959, 2018.

[2] Maamar Bettayeb, Ubaid Muhsen Al-Sagga, and Said Djennoune. Single channel secure communication scheme based on synchronization of fractional-order chaotic chua's systems. *Transactions of the Institute of Measurement and Control*, 40(13):3651–3664, 2017.

[3] Jialin Hou, Rui Xi, Ping Liu, and Tianliang Liu. The switching fractional order chaotic system and its application to image encryption. *IEEE/CAA Journal of Automatica Sinica*, 4(2), 2017.

[4] Bagley R. L. and Calico R. A. Fractional-order state equations for the control of viscoelastically damped structures. *Journal of Guidance, Control, and Dynamics*, pages 304–311.

[5] Jenson V. G. and Jeffreys G. V. Mathematical methods in chemical engineering. In *Elsevier*, page 559, 1977.

[6] Vijay K. Yadav, Subir Das, Beer Singh Bhadauria, Ashok K. Singh, and Mayank Srivastava. Stability analysis, chaos control of a fractional order chaotic chemical reactor system and its function projective synchronization with parametric uncertainties. *Chinese Journal of Physics*, 55(3):594–605, 2017.

[7] Yong Xu, Hua Wang Yongge Li, and Bin Pei. Image encryption based on synchronization of fractional chaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, 19:3735–3744, 2014.

[8] Ying Luo, YangQuan Chen, and Youguo Pi. Experimental study of fractional-order proportional derivative controller synthesis for fractional-order systems. *Mechatronics*, 21:204–214, 2011.

[9] Sabatier J., Cugnet M., Laruelle S., Grugeon S., Sahut B., Oustaloup A., and Tarascon J. M. A fractional-order model for lead-acid battery crankability estimation. *Communications in Nonlinear Science and Numerical Simulation*, 15:1308–1317, 2010.

[10] Vedat Suat Erturk, Zaid M. Odibat, and Shaher Momani. An approximate solution of a fractional-order differential equation model of human t-cell lymphotropic virus i (htlv-i) infection of cd4+ t-cells. *Computers and Mathematics with Applications*, 62:996–1002, 2011.

[11] Aida Mojaver and Hossein Kheiri. Mathematical analysis of a class of hiv infection models of cd4+ t-cells with combined antiretroviral therapy. *Applied Mathematics and Computation*, 259:258–270, 2015.

[12] Nick Laskin. Fractional market dynamics. *Physica A*, 287:482–492, 2000.

[13] Yongguang Yu, Han-Xiong Li, Sha Wang, and Junzhi Yud. Dynamic analysis of a fractional-order lorenz chaotic system. *Chaos, Solitons and Fractals*, 42:1181–1189, 2009.

[14] Chunguang Li and Guanrong Chen. Chaos and hyperchaos in the fractional-order rösslere quations. *Physica A: Statistical Mechanics and its Applications*, 341:55–61, 2004.

[15] Mohammad Mostafa Asheghan, Mohammad Taghi Hamidi, Beheshti, and Mohammad Saleh Tavazoei. Robust synchronization of perturbed chen's fractional-order chaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, 16(2):1044–1051, 2011.

[16] Jun Guo Lu. Chaotic dynamics of the fractional-order lü system and its synchronization. *Physics Letters A*, 354(4):305–311, 2006.

[17] Xiaojun Liu, Ling Hong, and Lixin Yang. Fractional-order complex t system: bifurcations, chaos control and synchronization. *Nonlinear Dynamics*, 75(3):586–602, 2014.

[18] Runzi Luo, Haipeng Su, and Yanhui Zeng. Synchronization of uncertain fractional-order chaotic systems via a novel adaptive controller. *Chinese Journal of Physics*, 55(2):342–349, 2017.

[19] Louis M. Pecora and Thomas L. Carroll. Synchronization in chaotic systems. *PHYSICAL REVIEW LETTERS*, 64:821–824, 1990.

[20] Bashir Naderi and Hossein Kheiri. Exponential synchronization of chaotic system and application in securecommunication. *Optik-International Journal for Light and Electron Optics*, 127(5):2407–2412, 2016.

[21] Hossein Kheiri and Bashir Naderi. Dynamical behavior and synchronization of chaotic chemical reactors model. *Iranian Journal of Mathematical Chemistry*, 6(1):81–92, 2015.

[22] Hossein Kheiri and Bashir Naderi. Dynamical behavior and synchronization of hyperchaotic complex t-system. *Journal of Mathematical Modelling*, 3(1):15–32, 2015.

[23] Chao-Jung Cheng. Robust synchronization of uncertain unified chaotic systems subject to noise and its application to secure communication. *Applied Mathematics and Computation*, 219:2698–2712, 2012.

[24] Fei Yu and Chunhua Wang. Secure communication based on a four-wing chaotic system subjectto disturbance inputs. *Optik*, 125:5920–5925, 2014.

[25] N.Smaoui, A.Karouma, and M.Zribi. Secure communications based on the synchronization of the hyperchaotic chen and the unified chaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, 16:3279–3293, 2011.

[26] Amin Kajbaf, Mohammad Ali Akhaee, and Mansour Sheikhana. Fast synchronization of non-identical chaotic modulation-based secure systems using a modified sliding mode controller. *Chaos Solitons And Fractals*, 84:49–57, 2016.

[27] M.Mossa Al-sawalha and M.S.M.Noorani. On anti-synchronization of chaotic systems via nonlinear control. *Chaos Solitons and Fractals*, 2009:170–179, 2009.

[28] Zuolei Wang. Anti-synchronization in two non-identical hyperchaotic systems with known or unknown parameters. *Communications in Nonlinear Science and Numerical Simulation*, 14(5):2366–2372, 2009.

[29] E.M.E labbasy and M.M.El-Dessoky. Adaptive anti-synchronization of different chaotic dynamical systems. *Chaos Solitons Fractals*, 42:2174–2180, 2009.

[30] Synchronization and anti-synchronization of a hyperchaotic chen system.

[31] Sachin Bhalekar Varsha and Daftardar-Gejji. Synchronization of different fractional-order chaotic systems using active control. *Communications in Nonlinear Science and Numerical Simulation*, 15:3536–3546, 2010.

[32] Razminia A. Full state hybrid projective synchronization of a novel incommensurate fractional-order hyperchaotic system using adaptive mechanism. *Indian Journal of Physics*, 87(2):161–167, 2013.

[33] Agrawal S. K. and Das S. A modified adaptive control method for synchronization of some fractional chaotic systems with unknown parameters. *Nonlinear Dynamics*, 73:907–919, 2013.

[34] Abolhassan Razminia and Dumitru Baleanu. Complete synchronization of commensurate fractional-order chaotic systems using sliding mode control. *Mechatronics*, 23:873–879, 2013.

[35] Kalidass Mathiyalagan, Ju H. Park, and Rathinasamy Sakthivel. Exponential synchronization for fractional-order chaotic systems with mixed uncertainties. *Complexity*, 21(1):114–125, 2015.

[36] P. Muthukumar and P. Balasubramaniam. Feedback synchronization of the fractional-order reverse butterfly-shaped chaotic system and its application to digital cryptography. *Nonblinear Dynamics*, 74:1169–1181, 2013.

[37] Mohammad Pourmahmood Aghababa. Finite-time chaos control and synchronization of fractional-order nonautonomous chaotic (hyperchaotic) systems using fractional nonsingular terminal sliding mode technique. *Nonlinear Dynamic*, 69:247–261, 2012.

[38] T.T. Hartley, C.F. Lorenzo, and H. Killory Qammer. Chaos in a fractional-order chua's system. circuits and systems i: Fundamental theory and applications. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 42(8):485–490, 1995.

[39] J. Tenreiro Machado, Virgini aKiryakova, and Francesco Mainardi. Recent history of fractional calculus. *Communications in Nonlinear Science and Numerical Simulation*, 16(3):1140–1153, 2011.

[40] Mohammad Pourmahmood Aghababa. A novel terminal sliding mode controller for a class of non-autonomous fractional-order systems. *Nonlinear Dynamics*, 73(1):679–688, 2o13.

[41] Leon Glass. Synchronization and rhythmic processes in physiology. *Nature*, 410(6825):277–284, 2001.

[42] W.H. Deng and C.P. Li. deng. *Physica A: Statistical Mechanics and its Applications*, 353:61–72, 2005.

[43] Weihua Deng and Changpin Li. Synchronization of chaotic fractional chen system. *Journal of the Physical Society of Japan*, 74(6):1645–1648, 2005.

[44] Ping Zhou and Wei Zhu. Function projective synchronization for fractional-order chaotic systems. *Nonlinear Analysis: Real World Applications*, 12(2):811–816, 2012.

[45] Lj Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz. Experimental demonstration of secure communication via chaotic synchronization. *International Journal of Bifurcation and Chaos*, 2:709–713, 1992.

[46] M. Boutayeb, Mohamed Darouach, Mohamed Darouach, Hugues Rafaralahy, and Hugues Rafaralahy. Generalized state observers for

chaotic synchronization and secure communication. *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications*, 49(3):345–349, 2002.

[47] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, and A. Shang. Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, 2:937–977, 1992.

[48] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems*, 40:626–633, 1993.

[49] H. Dedieu, M.P. Kennedy, and M. Hasler. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Transactions on Circuits and Systems II*, 40:634–642, 1993.

[50] Tao Yang and L.O. Chua. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 43:817–819, 1996.

[51] Rafael Martinez-Guerra, Juan J.Montesinos Garcia, and Sergio M.Delfín Prieto. Secure communications via synchronization of liouvillian chaotic systems. *Journal of the Franklin Institute*, 353:4384–4399, 2016.

[52] Bashir Naderi, Hossein Kheiri, Aghileh Heydari, and Reza Mahini. Optimal synchronization of complex chaotic t-systems and its application in secure communication. *Journal of Control, Automation and Electrical Systems*, 27(4):379–390, 2016.

[53] Chih-Chiang, Cheng Yan-SiLin, and Shiue-Wei Wu. Design of adaptive sliding mode tracking controllers for chaotic synchronization and application to secure communications. *Journal of the Franklin Institute*, 349:2626–2649, 2012.

[54] Chaohai Tao and Xuefei Liu. Feedback and adaptive control and synchronization of a set of chaotic and hyperchaotic systems. *Chaos, Solitons and Fractals*, 32(4):1572–1581, 2007.

[55] Wang Xingyuan and Wang Mingjun. Adaptive synchronization for a class of high-dimensional autonomous uncertain chaotic systems. *International Journal of Modern Physics C*, 18(3):399–406, 2007.

[56] Wu Xiangjun, Li Yang, and Kurths Jurgen. A new color image encryption scheme using cml and a fractional-order chaotic system. *PLOS ONE*, 10(3):1–28, 2015.

[57] Francis Austin, Wen Sun, and Xiaoqing Lu. Estimation of unknown parameters and adaptive synchronization of hyperchaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, 14(12):4264–4272, 2009.

[58] Mohamad F. Haroun and T. Aaron Gulliver. A new 3d chaotic cipher for encrypting two data streams simultaneously. *Nonlinear Dynamics*, 81:1053–1066, 2015.

[59] Mohammad PourmahmoodAghababa. Robust stabilization and synchronization of a class of fractional-order chaotic systems via a novel fractional sliding mode controller. *Communications in Nonlinear Science and Numerical Simulation*, 17:2670–2681, 2012.

[60] Norelys Aguila-Camacho, Manuel A. Duarte-Mermoud, and Javier A. Gallegos. Lyapunov functions for fractional-order systems. *Communications in Nonlinear Science and Numerical Simulation*, 19(9):2951–2957, 2014.

[61] A.A. Kilbas, H. M. Srivastava, and J.J. Trujillo. Theory and applications of fractional differential equations. In *Amsterdam: Elsevier*, page 540, 2006.

[62] Hassan K. Khalil. Nonlinear systems. In *Nonlinear systems*, page 748, 1950.

[63] Jean-Jacques Slotine and Weiping Li. Applied nonlinear control. In *New York, Prentice-Hall*.

[64] Mohammad Pourmahmood Aghababa and Hasan Pourmahmood Aghababa. Adaptive finite-time synchronization of non-autonomous chaotic systems with uncertainty. *Journal of Computational and Nonlinear Dynamics*, 8(3):1–11, 2013.

[65] Douglas Robert Stinson. Cryptography: Theory and practice. page 580. CRC Press, 2005.

[66] Narendra K. Pareek. Design and analysis of a novel digital image encryption schem. *International Journal of Network Security and Its Applications*, 4(2):95–108, 2012.

[67] Lilian Huang, Donghai Shi, and Jie Gao. The design and its application in secure communication and image encryption of a new lorenz-like system with varying parameter. *Mathematical Problems in Engineering*, (8973583):1–11, 2016.

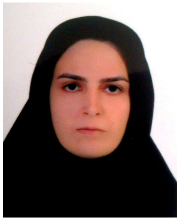
[68] Abdul Hanan Abdullah, Rasul Enayatifar, and Malrey Lee. A hybrid genetic algorithm and chaotic function model for image encryption. *AEU - International Journal of Electronics and Communications*, 66:806–816, 2012.

[69] Ch. K. Volos, I. M. Kyprianidis, and I.N.Stouboulos. Image encryption process based on chaotic synchronization phenomena. *Signal Processing*, 93:1328–1340, 2013.

[70] Shannon C. E. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

Bashir Naderi has got a Ph.D. degree in applied mathematics from the Pyame Noor University(PNU), Iran, in 2016. Now he is an Assistant Professor of mathematics at Payame Noor University (PNU), Iran. His main research interests include Dynamical system, Optimal control, Chaotic systems, Secure communication and Chaos control.

Hossein Kheiri has got a Ph.D. degree in applied mathematics from the University of Tabriz in 2005, and now he is a professor at the faculty of mathematical sciences of the University of Tabriz. His main research interests include Chaos dynamical systems, Control problems, Mathematical Modeling, Biomathematics, and fractional-order differential equations.



Vajiheh Vafaie received a B.Sc. degree in pure mathematics from Azarbaijan Shahid Madani University, Tabriz, Iran, in 2007. She received the M.Sc. and Ph.D. degrees in 2010 and 2018, respectively, from Tabriz University, Tabriz, Iran, both in applied mathematics. Her current research interests include areas of control and synchronization of fractional-order chaotic dynamical systems and their applications in secure communication and cryptography.