Hindawi
Complexity
Volume 2019, Article ID 7242791, 10 pages
https://doi.org/10.1155/2019/7242791

Research Article

Secure Communication of Fractional Complex Chaotic Systems Based on Fractional Difference Function Synchronization

Jiaxun Liu,[1] Zuoxun Wang,[1] Minglei Shu,[2] Fangfang Zhang,[1] Sen Leng,[1] and Xiaohui Sun[3]

[1]*College of Electrical Engineering and Automation, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China*
[2]*Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), Shandong Artificial Intelligence Institute, Jinan 250101, China*
[3]*College of Pharmacy, Shandong University of Traditional Chinese Medicine, Jinan 250355, China*

Correspondence should be addressed to Fangfang Zhang; zhff4u@163.com

Received 10 April 2019; Accepted 10 July 2019; Published 18 August 2019

Academic Editor: Cornelio Posadas-Castillo

Fractional complex chaotic systems have attracted great interest recently. However, most of scholars adopted integer real chaotic system and fractional real and integer complex chaotic systems to improve the security of communication. In this paper, the advantages of fractional complex chaotic synchronization (**FCCS**) in secure communication are firstly demonstrated. To begin with, we propose the definition of fractional difference function synchronization (**FDFS**) according to difference function synchronization (**DFS**) of integer complex chaotic systems. **FDFS** makes communication secure based on **FCCS** possible. Then we design corresponding controller and present a general communication scheme based on **FDFS**. Finally, we respectively accomplish simulations which transmit analog signal, digital signal, voice signal, and image signal. Especially for image signal, we give a novel image cryptosystem based on **FDFS**. The results demonstrate the superiority and good performances of **FDFS** in secure communication.

1. Introduction

With the booming of multimedia and wireless networks, secure communication of information is more and more significant in real applications. In particular, encryption of voice, images, and other real information has got a lot of attentions, such as recording of business meetings, military and architectural images, computer code, and so on. Many of the theoretical results make improvements in communication complexity as justification and a measure of success, and this seems logical as the communication complexity is the lower bound of the computation complexity [1].

In the last three decades, chaotic synchronization of real variables has been a hotspot in nonlinear science since Caroll and Pecora [2] firstly achieved chaotic synchronization in electronic circuit. Chaos can exhibit a noise-like behavior such as randomicity, ergodicity, unpredictability, high sensitivity for the initial condition, and broadband nature. It is the great advantage in chaos communication and allows chaos to elegantly cover up the communication information. Moreover, chaos communication is usually easy to be realized by numerous simple circuits, which is more convenient than traditional cryptosystem.

Since Fowler et al. [3] came up with the concept of complex chaos in 1982, many studies have been proposed in the field of new complex chaotic systems (**CCS**) and their applications [4–12]. Some actual physical models also were discovered as **CCS**, such as amplitudes of electromagnetic and detuned laser systems [13–17]. The number of the variables in **CCS** is twice as many as real chaotic systems (**RCS**), which is the major difference between **RCS** and **CCS**. In some sense, it means that **CCS** have nature superiority in increasing transformation and channels. Moreover, complex variables are simpler to be accomplished by RLC circuit in actual applications than real variables. Therefore, the complicated

dynamics and easy implementations of **CCS** are born to secure communication. Some methods of integer complex chaotic synchronization (**ICCS**) used in secure communication were discussed in literatures. Reference [18] firstly put complex function projective synchronization (**CFPS**) into secure communication and got the superb result. However, when the signal of the master system is close to zero in **CFPS**, it affects the encryption since the denominator is close to zero. Therefore, [9] gave the definition of difference function synchronization (**DFS**) and solved this problem. **DFS** is proposed to the point of difference in two state variables and breaks the previous concept that scholars only study synchronization from the proportional relation between state variables. It is somewhat great innovation. **DFS** extends the difference between two state variables from zero to any desired functions. Therefore, it is the synchronization with much broader context. Complete synchronization and phase synchronization are its special cases. E.Mahmoud and Abo-Dahab studied another chaotic complex nonlinear framework and achieved communication of analog signal based on complex antisynchronization [19]. As far as we know, all above literatures of secure communication were just on the basis of **ICCS**.

Fractional calculus has been recommended over three hundred years, but it had not received too much attention because of the unclear physical background of fractional calculus. Until the last decade, some scholars found that it is more accurate than integer order calculus in describing some actual physical models, for instance, viscoelastic system [20], viscoelastic material [21], finance system [22], nuclear spin generator system [23], industrial system [24], human immunodeficiency virus model [25], and other interdisciplinary fields. Therefore, fractional chaos also caused abundant interests. Besides, because of complicated geometric interpretation of nonlocal effects of fractional derivatives in time and space [26], fractional chaos exhibits more unpredictable and complex nonlinear dynamic behaviors than integer chaotic systems. These merits were caught hold of by a few researchers who focused on chaos communication. Reference [27] studied the modified generalized projective synchronization of fractional real hyperchaotic systems and applied it to secure communication. Sarah et al. [28] proposed a novel secure image transmission method based on fractional real discrete-time chaotic systems. Muthukumar et al. [29] presented a fractional sliding mode controller and studied its application for a cryptosystem. Li and Wu accomplished secure communication of fractional chaotic systems with teaching-learning-feedback based optimization [30]. Mohammadzadeh and Ghaemi researched a secure communication with uncertain fractional hyperchaotic synchronization [31]. These proposed literatures make significant contributions in secure communication of fractional chaotic systems. However, we find most papers were based on fractional real chaotic synchronization.

Enlightened by the above discussions, we will put the **FCCS** with **DFS** into secure communication in this paper and gain higher security and better reliability than traditional methods and other chaos communication schemes. It will combine the advantages of **DFS** in complex chaotic synchronization and fractional chaotic systems. Compared with secure communication based on integer real chaos synchronization, **FCCS** not only increase the number of potential channels, but also complicate the types of encryption keys. When it comes to secure communication based on fractional real chaos synchronization, **FCCS** have nature superiority in transmitting complex signal and choosing variable signal channels. As for secure communication based on integer complex chaos synchronization, **FCCS** could generate more unpredictable secret keys by means of different fractional orders. Due to the existence of the double variables and fractional derivative factors, it is difficult for the unauthorized third party to extract the useful information because of its complicated dynamic behavior.

The main contributions of this paper are as follows: (1) Firstly, we extend the **DFS** to **FDFS** and investigate the general controller. (2) Four types of transmitted signals including analog signal, digital signal, voice signal, and image signal are accomplished to verify the high security and good performance of the communication scheme based on **FDFS**. (3) As for the image signal, we propose a novel cryptosystem with **FDFS**.

The structure of the remaining paper is organized as follows: some basic mathematical theorems are given in Section 2. Section 3 introduces the **FDFS** and general controllers. The application of **FCCS** is finished by four types of signals and the method of image cryptosystem is proposed in Section 4. Finally, the conclusions are drawn in Section 5.

2. Mathematical Background

There are three main types of definition of fractional derivative, such as Caputo definition, Riemann Liouville definition, and Grunwald Letnikobv definition. In this paper, we use the Caputo definition as it includes the conventional initial conditions and Caputo derivative of the constant is zero.

Definition 1 (see [32]). The Caputo derivative definition is as follows:

$$\mathrm{D}^m f(t) = \frac{1}{\Gamma(n-a)} \int_a^t (t-\tau)^{-a+n-1} f^n(\tau)\, \mathrm{d}\tau, \tag{1}$$

where $n = [m] + 1$, $[m]$ is integer part of m and $\Gamma(*)$ is the gamma function. t and a are the upper and lower bounds, and D^m is called the m order Caputo differential operator. The gamma function is

$$\begin{aligned} \Gamma(w) &= \int_0^\infty e^{-t} t^{w-1} \mathrm{d}t, \\ \Gamma(w+1) &= w\Gamma(w). \end{aligned} \tag{2}$$

Lemma 2 (see [33]). *There is an autonomous fractional system*

$$\begin{aligned} \mathrm{D}^q x(t) &= Qx(t), \\ x(0) &= x_0, \end{aligned} \tag{3}$$

where $x \in R^c, Q \in R^{c\times c}$ *and* $0 < q < 1$. *The system is asymptotically stable if and only if*

$$\left|\arg\left(eig\left(Q\right)\right)\right| > \frac{q\pi}{2}. \tag{4}$$

And the component of the state decays toward 0 *like* t^{-q}.

3. Fractional Difference Function Synchronization

3.1. The Definition of FDFS. Recently, a new type of chaotic synchronization was proposed, which is called **DFS** in [9]. It is the expanding form of complete synchronization (**CS**) and phase synchronization (**PHS**). Particularly, for some signals near zero, it is effective for **DFS** in secure communication. In this part, we expand the **DFS** into **FDFS** and give the general synchronization controller, aiming to lay the foundation for secure communication in the following part.

Delighted by the concept of **DFS**, we firstly present the **FDFS** as follows:

Definition 3. For two r-dimensional and q-order general form of fractional chaotic systems $D^{q_1}\mathbf{X}(t)$ and $D^{q_2}\mathbf{Y}(t)$, we call the difference $D^{q_3}\mathbf{G}(t)$ between $D^{q_1}\mathbf{X}(t)$ and $D^{q_2}\mathbf{Y}(t)$ as the fractional difference function vector,

$$D^{q_3}\mathbf{G}\left(t\right) = D^{q_1}\mathbf{Y}\left(t\right) - D^{q_2}\mathbf{X}\left(t\right), \tag{5}$$

where $\mathbf{G}(t) = [g_1(t),\ g_2(t),\ \cdots,\ g_n(t)]^{\mathrm{T}}$, $\mathbf{X}(t) = [x_1(t),\ x_2(t),\ \cdots,\ x_n(t)]^{\mathrm{T}}$, $\mathbf{Y}(t) = [y_1(t),\ y_2(t),\ \cdots,\ y_n(t)]^{\mathrm{T}}$, and $0 < q_1 \le 1, 0 < q_2 \le 1, 0 < q_3 \le 1$.

Definition 4. For two arbitrary fractional chaotic state vector $x_n(t)$, $y_n(t)$ and difference vector $g_n(t)$ in (5), they are said to be **FDFS** if there exists

$$\lim_{t\longrightarrow+\infty}\left\|e_n\left(t\right)\right\| = \left\|y_n\left(t\right) - x_n\left(t\right) - g_n\left(t\right)\right\| = 0, \tag{6}$$

where $\|\cdot\|$ is the matrix norm.

Remark 5. When $q_1 = q_2 = q_3 = 1$, the **FDFS** would be **DFS**.

Remark 6. **CS** indicates the difference vectors with different or same initial value converge to zero when $D^{q_3}\mathbf{G}(t) = 0$ and $q_1 = q_2 = 1$. The **CS** is a special case of the **FDFS**.

Remark 7. When $q_1 = 1, q_2 = 1, q_3 = 0$, the difference function vector $D^{q_3}\mathbf{G}(t)$ will be a constant value, so **FDFS** is also the extension of **PHS**.

3.2. The Control Laws for FDFS. In order to increase generality, we consider a general form of coupled fractional chaotic system as follows:

$$\begin{aligned} D^w\mathbf{x} &= \mathbf{A}\mathbf{x} + F_1\left(\mathbf{x}\right),\\ \mathbf{u} &= F_2\left(\mathbf{x},\mathbf{y}\right),\\ D^w\mathbf{y} &= \mathbf{B}\mathbf{y} + F_3\left(\mathbf{y}\right) + \mathbf{u}, \end{aligned} \tag{7}$$

where w is the fractional operator and $0 < w \le 1$, F_1, F_3 are nonlinear continuous vector functions, and $\mathbf{A}, \mathbf{B}$ are the Jacobian matrices of systems $D^w x, D^w y$. $\mathbf{u}$ is the controller part of the coupled system and F_2 is the combination between nonlinear and linear function.

As for the state vectors $\mathbf{x}, \mathbf{y}$, one has the following.

Case 1. When they are real vectors, then $\mathbf{x} = [x_1,\ x_2,\ \cdots,\ x_n]^{\mathrm{T}}$, and $\mathbf{y} = [y_1,\ y_2,\ \cdots,\ y_n]^{\mathrm{T}}$, $\mathbf{u} = [u_1,\ u_2,\ \cdots,\ u_n]^{\mathrm{T}}$, where $n = 1, 2, 3, \ldots$.

Case 2. When they are complex vectors, $\mathbf{x} = \mathbf{x}^r + j\mathbf{x}^i, \mathbf{y} = \mathbf{y}^r + j\mathbf{y}^i, \mathbf{u} = \mathbf{u}^r + j\mathbf{u}^i$, where $\mathbf{x}^r, \mathbf{y}^r, \mathbf{u}^r$ are the real parts and $\mathbf{x}^i, \mathbf{y}^i, \mathbf{u}^i$ are the imaginary parts. j is the imaginary unit and $j^2 = -1$. $\mathbf{x}^{\mathrm{r}} = [x_1^r,\ x_2^r,\ \cdots,\ x_n^r]^{\mathrm{T}}$, $\mathbf{x}^{\mathrm{i}} = [x_1^i,\ y_1^i,\ \cdots,\ y_n^i]^{\mathrm{T}}$, $\mathbf{y}^{\mathrm{r}} = [y_1^r,\ y_2^r,\ \cdots,\ y_n^r]^{\mathrm{T}}$, $\mathbf{y}^{\mathrm{i}} = [y_1^i,\ y_2^i,\ \cdots,\ y_n^i]^{\mathrm{T}}$, $\mathbf{u}^{\mathrm{r}} = [u_1^r,\ u_2^r,\ \cdots,\ u_n^r]^{\mathrm{T}}$, and $\mathbf{u}^{\mathrm{i}} = [u_1^i,\ u_2^i,\ \cdots,\ u_n^i]^{\mathrm{T}}$.

We assume the difference function is $p_n(t)$, then $\mathbf{P} = D^w p_n(t)$ where $\mathbf{P} = [P_1,\ P_2,\ \cdots,\ P_n]$. According to (7) and the definition of **FDFS**, we have the error system as follows:

$$\begin{aligned} D^w\mathbf{e} &= D^w\mathbf{y} - D^w\mathbf{x} - \mathbf{P}\\ &= \mathbf{B}\mathbf{y} - \mathbf{A}\mathbf{x} + F_3\left(\mathbf{y}\right) - F_1\left(\mathbf{x}\right) + F_2\left(\mathbf{x},\mathbf{y}\right) - \mathbf{P} + \mathbf{u}, \end{aligned} \tag{8}$$

where $\mathbf{e} = [e_1,\ e_2,\ \cdots,\ e_n]^{\mathrm{T}}$.

According to the fractional stable theory and Lemma 2, we will get the following theorem.

Theorem 8. *For the coupled fractional chaotic system (7) with the difference function* $p_n(t)$ *and the initial value* $x(0), y(0)$, *it could accomplish* ***FDFS*** *with the following controller:*

$$\mathbf{u} = \mathbf{A}\mathbf{x} - \mathbf{B}\mathbf{y} + F_1\left(\mathbf{x}\right) - F_3\left(\mathbf{y}\right) + \mathbf{P} + \mathbf{k}\mathbf{e}, \tag{9}$$

where parameter matrix $\mathbf{k}$ *satisfies* $|\arg(\mathrm{eig}(\mathbf{k}))| > w\pi/2$.

Proof. In order to verify the effect of the control law, we put (9) into (8) and get

$$\begin{aligned} D^w\mathbf{e} &= \mathbf{B}\mathbf{y} - \mathbf{A}\mathbf{x} + F_3\left(\mathbf{y}\right) - F_1\left(\mathbf{x}\right) - \mathbf{P} + \mathbf{A}\mathbf{x} - \mathbf{B}\mathbf{y}\\ &\quad + F_1\left(\mathbf{x}\right) - F_3\left(\mathbf{y}\right) + \mathbf{P} + \mathbf{k}\mathbf{e} = \mathbf{k}\mathbf{e}. \end{aligned} \tag{10}$$

According to Lemma 2, since $|\arg(eig(\mathbf{k}))| > w\pi/2$ in the coupled fractional chaotic system, the system could arrive **FDFS** asymptotically with the controller (9) and the error function $D\mathbf{e}^w$ could tend to zero. □

4. Secure Communication of FCCS

In this section, we focus on secure communication of **FDFS** with complex variables. Due to the broadband characters of chaotic systems, we could effectively cover up the signal by the chaos carrier. The block diagram of information transmission based on **FDFS** is illustrated in Figure 1. From Figure 1, we can know that the overall structure is composed of two

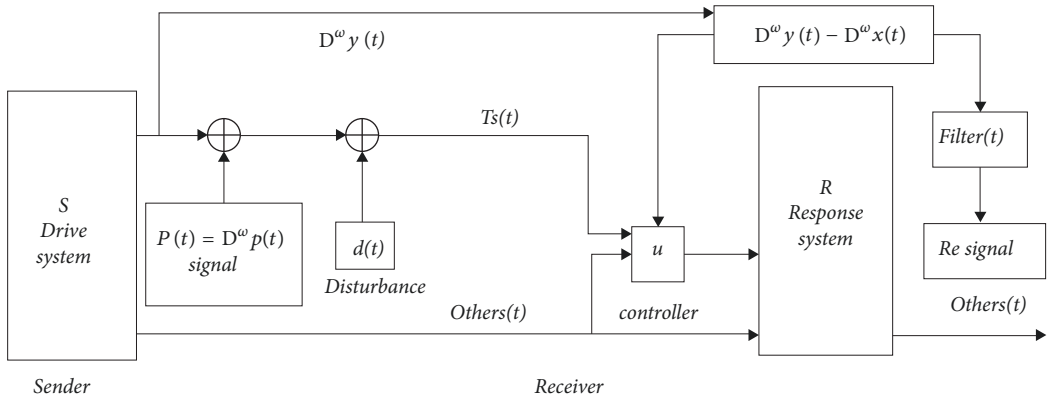

Figure 1: The block diagram of secure communication based on **FDFS**.

parts approximately. One part $\boldsymbol{S}$ is the sending end, which provides the carrier of chaotic masking. Message modulation between chaotic driver system and information signal occurs here. The other main part $\boldsymbol{R}$ is receiving end, which aims at information demodulation. Response system and received signal have demodulated with the controller in part $\boldsymbol{R}$. $P(t)$ is the information signal and $d(t)$ is the potential disturbance signal in process of transmitting. $Ts(t)$ is the transmission signal, where $Ts(t) = D^{w} y(t) + P(t) + d(t)$. $Others(t)$ are the other alternative transmission channels. $Fliter(t)$ is used for filter interference and we can get accurate recovered signals.

In order to verify the security of the proposed cryptosystem, we will simulate the transmission of four kinds of information signals in this part. In 2013, the coupled complex fractional Lorenz system was presented in [8], which is described as follows:

$$S: \begin{cases} D^{w} y_1 = b_1 (y_2 - y_1) + u_1, \\ D^{w} y_2 = b_2 y_1 - y_2 - y_1 y_3 + u_2, \\ D^{w} y_3 = \dfrac{1}{2} (\overline{y}_1 y_2 + y_1 \overline{y}_2 - b_3 y_3) + u_3, \end{cases} \tag{11}$$

and

$$R: \begin{cases} D^{w} x_1 = a_1 (x_2 - x_1), \\ D^{w} x_2 = a_2 x_1 - x_2 - x_1 x_3, \\ D^{w} x_3 = \dfrac{1}{2} (\overline{x}_1 x_2 + x_1 \overline{x}_2 - a_3 x_3), \end{cases} \tag{12}$$

where $x_1 = x_1^r + j x_1^i, x_2 = x_2^r + j x_2^i, y_1 = y_1^r + j y_1^i, y_2 = y_2^r + j y_2^i$ and the overbar of $\overline{x}_1, \overline{x}_2, \overline{y}_1, \overline{y}_2$ means the complex conjugate of $x_1, x_2, y_1, y_2, a_1 = b_1 = 10, a_2 = b_2 = 28, a_3 = b_3 = 8/3$. $u_1 = u_1^r + j u_1^i, u_2 = u_2^r + j u_2^i, u_3$ are correlation controllers.

We choose (9) as the controller in secure communication and the controller is

$$\begin{aligned} u_1^r &= -a_1 e_2^r + k_1 e_1^r + p_1^r, \\ u_1^i &= -a_1 e_2^i + k_2 e_1^i + p_1^i, \\ u_2^r &= -a_2 e_1 + y_1^r y_3 - x_1^r x_3 + k_3 e_2^r + p_2^r, \\ u_2^i &= -a_2 e_1^i + y_1^i y_3 - x_1^i x_3 + k_4 e_2^i + p_2^i, \\ u_3 &= -y_1^r y_2^r + x_1^r x_2^r - y_1^i y_2^i + x_1^i x_2^i + k_5 e_3 + p_3, \end{aligned} \tag{13}$$

where $k_1, k_2, \ldots, k_5$ are the scale parameters of controller and p_1, p_2, p_3 are the difference factors of **FDFS** which also represent information signal ($p(t) = \{p_1, p_2, p_3\}^{\mathrm{T}}$) in secure communication.

For the disturbance signal, we choose the stochastic Gaussian noise as the $d(t)$, which is described as follows:

$$n(d) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(d - d_0)^2}{2\sigma^2}\right) s, \tag{14}$$

where the mean value $d_0 = 0$ and variance $\sigma = 1$ and s is the scale parameter of stochastic Gaussian noise.

4.1. Communication of Analog Signals. In this section, we put the analog signal into transmission system. In order to get the clear result of simulations, we firstly choose the information signal $p(t) = 10 \sin(0.1\pi t) + j15 \cos(0.1\pi t)$; then we have

$$P(t) = \begin{cases} P^r(t) = 10 \sin(0.1\pi t + 0.5\pi w), \\ P^i(t) = 15 \cos(0.1\pi t + 0.5\pi w), \end{cases} \tag{15}$$

where $P(t)$ is the w-order derivative of $p(t)$. $P^r(t), P^i(t)$ are the real and imaginary parts of $P(t)$, respectively.

As for the choice of communication channels, we select y_1^r, y_1^i as the sending end to transmit the real and imaginary part of analog signal and x_1^r, x_1^i as the receiving end to compute the real and imaginary part of encrypted analog signal. To further enhance the confidentiality of the transmission system and simulate the potential disturbance signal, we add stochastic Gaussian noise into transmitting process. Set $s = 10$ in (14). In the receiving end, we could use some easy filters in real engineering and it allows assuring the accuracy of recovered information.

Figure 2 shows the encrypted transmission signal, which is complicated and irregular. It is hard for unauthorized third party to find the information signal. The recovered signal,

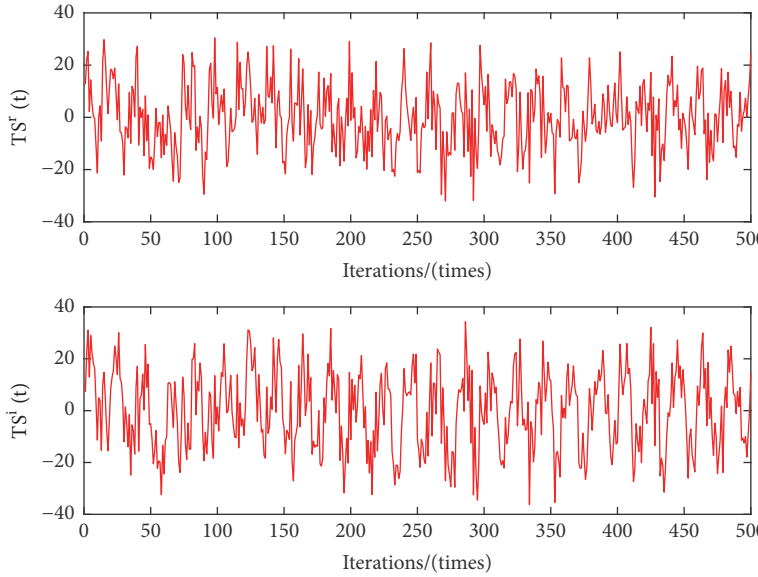

FIGURE 2: Picture of transmitted signal $Ts(t)$, where $s = 10, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 500.

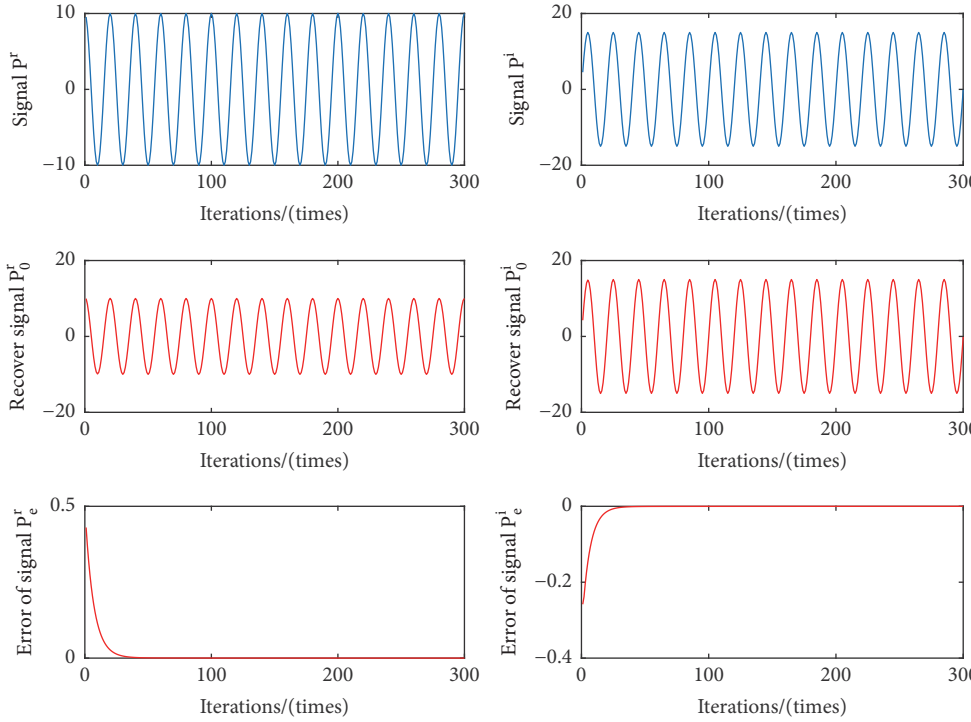

FIGURE 3: Picture of original signal and recover signal, where $s = 10, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 300.

original signal, and their error are shown in Figure 3. With the controller (13) in the receiving end, information signal has been recovered correctly in Figure 3. Figure 4 shows the error of receiving end and sending end. According to the definition of **FDFS**, as the choice of communication channel is complex variable y_1 and x_1, their error is the information signal. Other errors of complex variables y_2 and x_2 and real variables y_3 and x_3 are zero asymptotically.

4.2. Communication of Digital Signal. Firstly, the original digital signal produced by the random function is shown in Figure 5. In order to achieve a fast transmission without increasing the system complexity, the O binary bits are transformed into one corresponding fractional difference functions by 2^O-ary. In this part, we set $O = 4$ and transform digital signal to the fractional difference function by $2^O = 16$-ary. The signal duration is 200 iterations. We choose the y_1^i

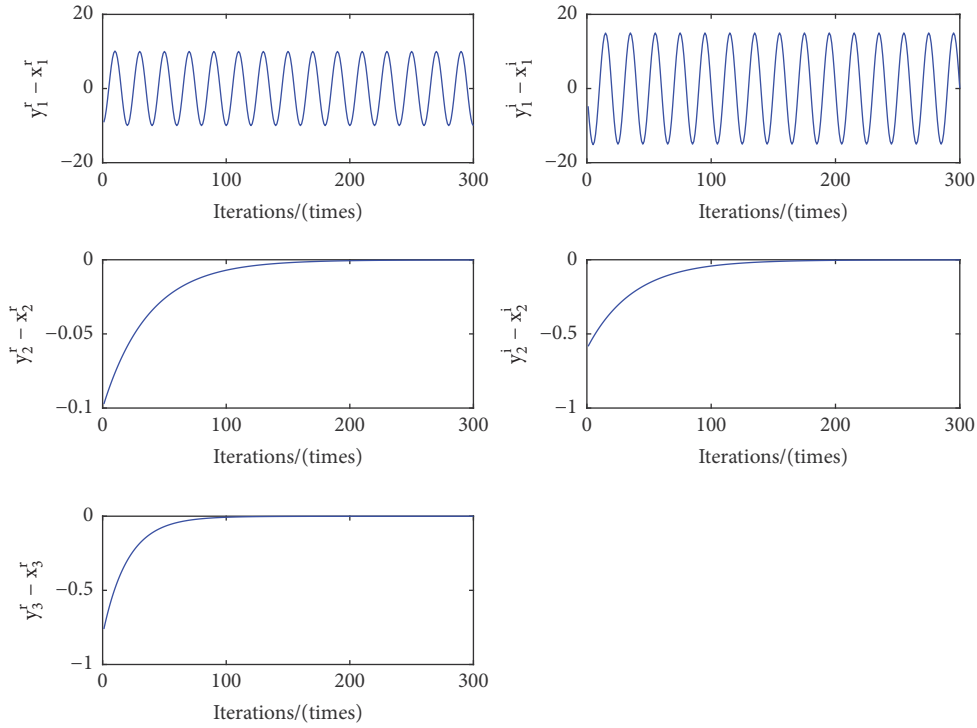

FIGURE 4: Diagram of error of receiving end and sending end, where $s = 10, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 300.

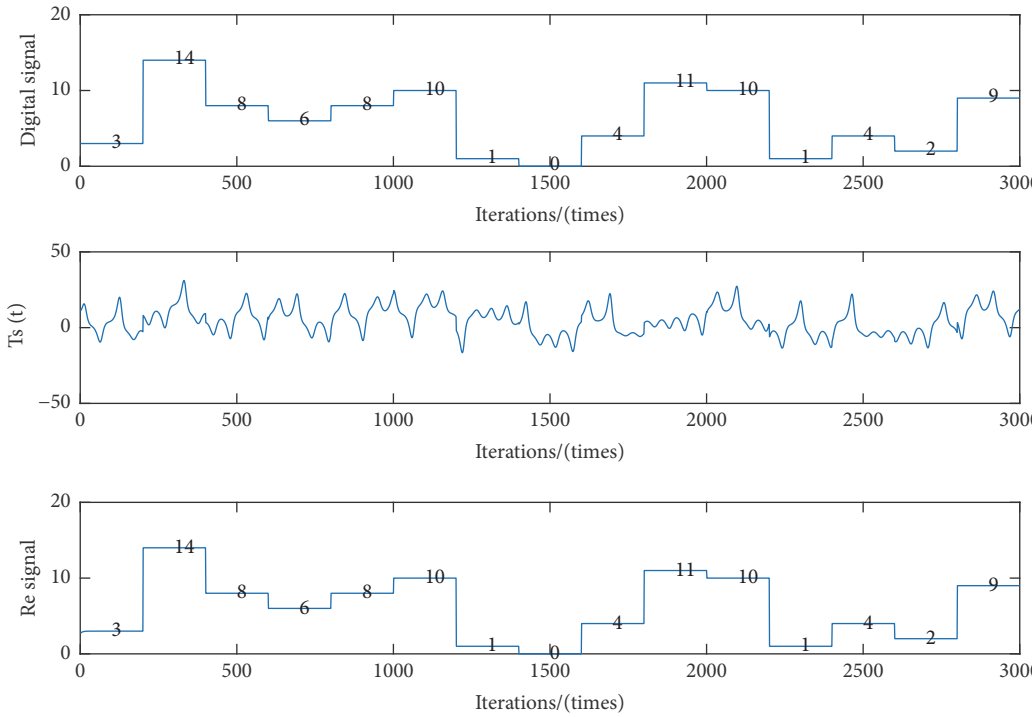

FIGURE 5: Diagram of digital signals transmission without noise, where $s = 0, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 3000.

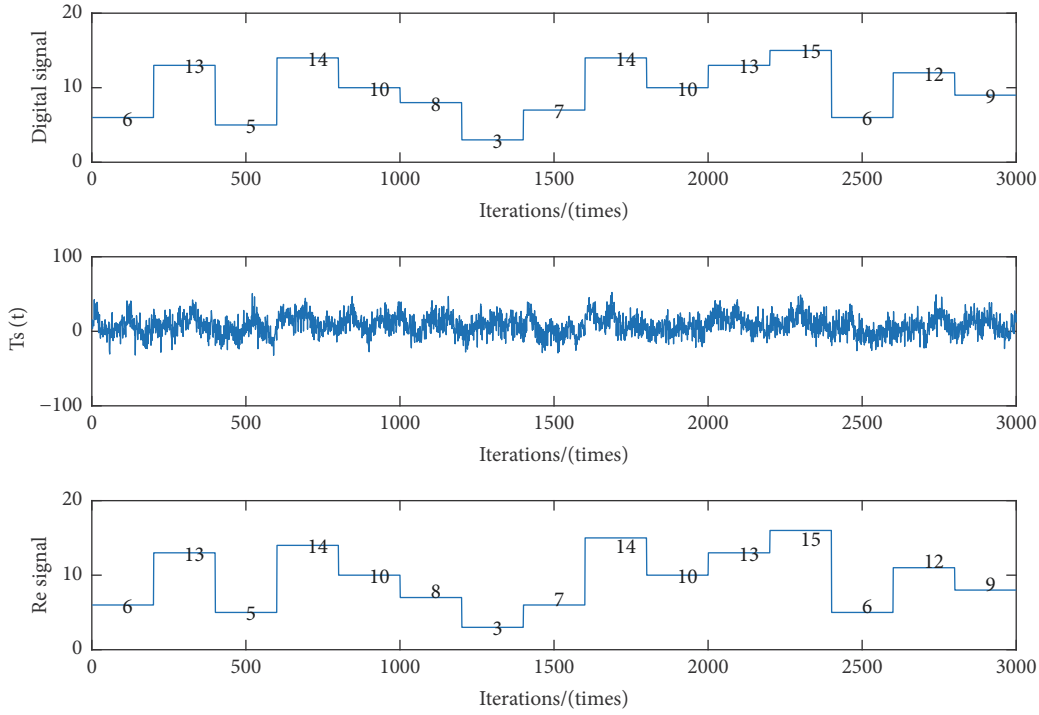

FIGURE 6: Diagram of digital signals transmission with noise, where $s = 10, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 3000.

of the drive system as the sending terminal and x_1^i as the receiving terminal. Figure 5 shows the transmitted process of digital signals without noise, where the error between original digital signal and the recovered signal is zero and the transmitted signal $Ts(t)$ is an analog signal which completely covers up the binary digital sequence.

Considering that there is potential disturbance in transmitting process of digital signals, we get the transmitting process shown in Figure 6. The transmitted signal $Ts(t)$ is almost noise-like and someone like espionage hardly extracts the information signal without authorization. In order to reduce the effect of noise, we firstly compute the average value of the fractional difference function during each signal duration and then round off to the nearest integer that is bounded between 0 and $2^O - 1$. Therefore, this scheme guarantees the accuracy and low bit error rate in process of recovery.

4.3. Communication of Voice Signal. In this section, a novel audio cryptosystem is presented for transmitting voice signal. In the sending end, we choose the mellifluous song "traveling light" as the information signal, which is shown in Figure 7.

There are five alternative communication channels to transmit the voice signal. We choose y_1^r, x_1^r to encrypt and decrypt the information signal.

Because the voice signal has a great number of samples, we extract the sample from 30000th to 33000th, which is enough to get an excellent simulation. From Figure 8, the error between the original voice and recovered voice approaches to zero quickly and the transmitted signal of encryption voice completely covers the information signal. Moreover, due to the existence of five alternative communication channels, there is less possibility for the eavesdropper to extract the original voice.

4.4. Communication Image Signal. In this section, a new key cryptosystem is presented for sharing image messages to increase the security and anticrack ability of secure communication. Generally speaking, the purpose of key cryptography is to allow two different organizations to communicate the confidential message, even though they have never met and communicated with each other or they are supervised by an adversary. The proposed cryptosystem consists of three parts: key generation, encryption, and decryption.

Key generation

Sending end and receiving end both agree on this:

(1) The fractional order w.

(2) Complex variable x_1, x_2, y_1, y_2 and the real variable x_3, y_3 of couple system.

(3) Initial value of fractional order complex chaotic system.

(4) The parameters of couple system.

(5) Scaling parameters b_1, b_2, b_3, b_4, b_5.

Encryption

(1) The pixel matrix of original picture is $\mathbf{MM}_{(c\times d)}$.

(2) There are also five zeros matrices, $\mathbf{M1}_{(c\times d)}$, $\mathbf{M2}_{(c\times d)}, \mathbf{M3}_{(c\times d)}, \mathbf{M4}_{(c\times d)}, \mathbf{M5}_{(c\times d)}$. As the coupled chaotic system has five alternative encryption sending terminals, $y_1^r, y_1^i, y_2^r, y_2^i, y_3$, we could generate five arrays s_1, s_2, s_3, s_4, s_5 with the initial value of coupled system, where the number

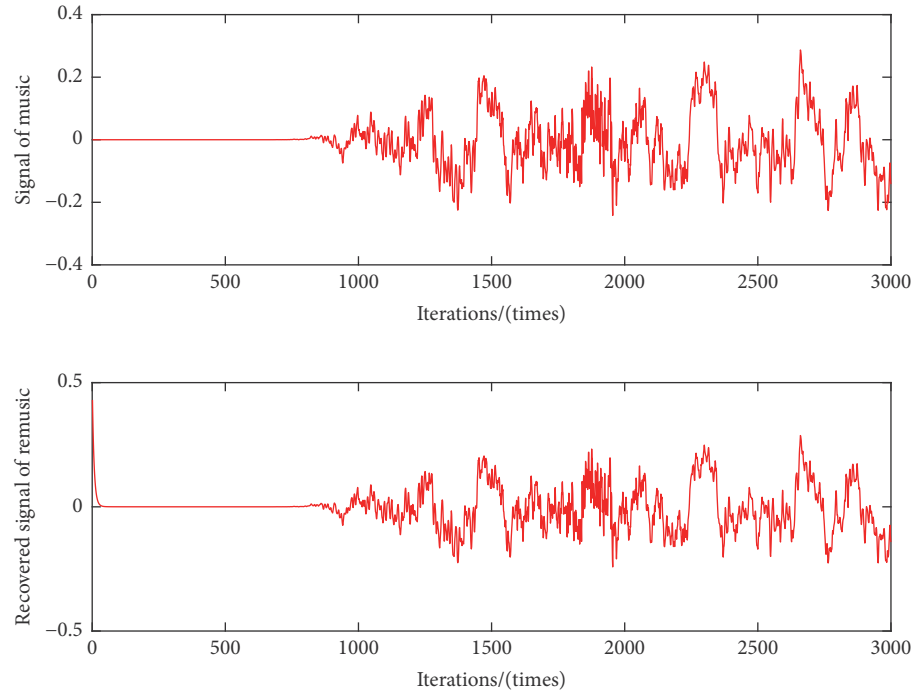

Figure 7: Diagram of information signal and recovered voice signal, where $s = 0, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8, w = 0.995)$, and all iterations are 3000.

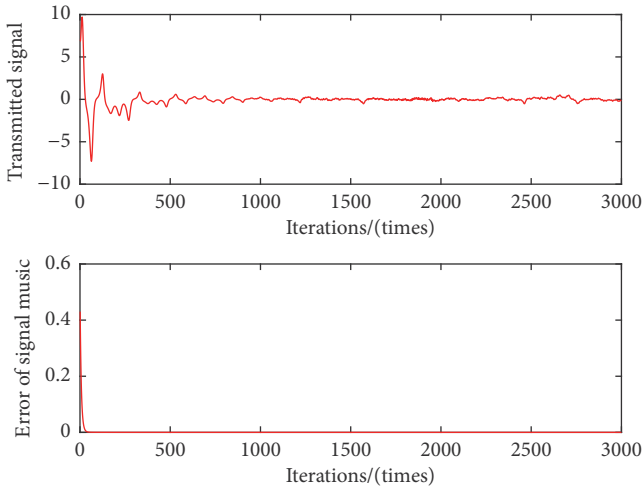

Figure 8: Diagram of voice encryption transmitted signal and the error between original and recovered signal, where $s = 10, k = -1, w = 0.995$, the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$, and all iterations are 3000.

of every array is more than $(1/5)c \times d$ and c, d are the matrix size parameters.

(3) Let $\mathbf{M1}(1 : (c \times d)/5) = s_1(301 : (c \times d)/5 + 300)$ and $\mathbf{M2}((c \times d)/5 + 1 : (2c \times d)/5) = s_2(301 : (c \times d)/5 + 300)$,

$\mathbf{M3}((2c \times d)/5 + 1 : (3c \times d)/5) = s_3(301 : (c \times d)/5 + 300)$ and $\mathbf{M4}((3c \times d)/5 + 1 : (4c \times d)/5) = s_4(301 : (c \times d)/5 + 300)$,

$\mathbf{M5}((4c \times d)/5 + 1 : (5c \times d)/5) = s_5(301 : (c \times d)/5 + 300)$; if $(c \times d)/5$ has remainder, we could adjust the number of M5, s_5 correspondingly.

Figure 9: Diagram of original picture, where $s = 0, k = -1, w = 0.995, b_1 = 2000, b_2 = 20000, b_3 = 2000, b_4 = 20000, b_5 = 35$, and the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$.

(4) $\mathbf{M}_{(c\times d)} = b_1\mathbf{M1} + b_2\mathbf{M2} + b_3\mathbf{M3} + b_4\mathbf{M4} + b_5\mathbf{M5} + \mathbf{MM}$.

(5) The sending end sent $\mathbf{M}$ to the receiving end.

Decryption

(1) On condition that we received the $\mathbf{M}$ and agree on the keys, we must form corresponding five decryption matrices $\mathbf{N1}_{(c\times d)}$, $\mathbf{N2}_{(c\times d)}$, $\mathbf{N3}_{(c\times d)}$, $\mathbf{N4}_{(c\times d)}$, and $\mathbf{N5}_{(c\times d)}$ in the decryption receiving terminal, $x_1^r, x_1^i, x_2^r, x_2^i, x_3$ with the controller (9). The method of generation of these five decryption matrices is similar to encryption.

(2) $\mathbf{N}_{(c\times d)} = b_1\mathbf{N1} + b_2\mathbf{N2} + b_3\mathbf{N3} + b_4\mathbf{N4} + b_5\mathbf{N5}$.

The recovered image pixel matrix $\mathbf{RI}_{(c\times d)} = \mathbf{M} - \mathbf{N}$.

(3) We can get the recovered image by the pixel matrix $\mathbf{RI}$.

Figures 9 and 10 are the diagrams of original information image and recovered image, respectively. The picture of

Figure 10: Diagram of recovered picture, where $s = 0, k = -1, w = 0.995, b_1 = 2000, b_2 = 20000, b_3 = 2000, b_4 = 20000, b_5 = 35$, and the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$.

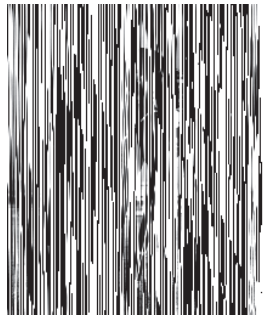

Figure 11: Diagram of encrypted matrix, where $s = 0, k = -1, w = 0.995, b_1 = 2000, b_2 = 20000, b_3 = 2000, b_4 = 20000, b_5 = 35$, and the initial value is $(y_1^r(0) = 7, y_1^i(0) = 8, y_2^r(0) = 5, y_2^i(0) = 6, y_3(0) = 12, x_1^r(0) = 6.5, x_1^i(0) = 8.3, x_2^r(0) = 5.1, x_2^i(0) = 6.6, x_3(0) = 12.8)$.

encrypted matrix is shown in Figure 11, where the encryption image completely covers the information picture. Due to the complexity of the secret key and the process of encryption, the unauthorized organization cannot recover the original image absolutely without the whole information of the secret key.

5. Conclusions

In the last two decades, chaos communication has been a hotspot and got astonishing progress. In this paper, we propose a novel secure communication scheme of fractional complex chaotic systems based on **FDFS**. We firstly extend the **DFS** from integer complex chaotic systems to fractional complex chaotic systems and design corresponding controller. **FDFS** is one of **FCCS** in essence. In order to verify the effectiveness and advantages of **FCCS**, we present novel secure communication schemes based on **FDFS** and transmit analog signal, digital signal, voice signal, and image. Moreover, we design an image cryptosystem with high security. The numerical simulations demonstrate the great effect of encryption, transmission, and decryption. Particularly, the results exhibit the advantages of **FDFS** integrating with fractional complex chaotic system.

Secure communication of **FCCS** is a completely new field. We hope that more and more researchers will extend some traditional synchronization to **FCCS** and increase the diversity of **FCCS** in secure communication, which will deeply develop chaos communication.

Data Availability

The Matlab programs used to support the findings of this study are currently under embargo while the research findings are not published. Requests for data, 6 months after publication of this article, will be considered by the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially supported by Young doctorate Cooperation Fund Project of Qilu University of Technology (Shandong Academy of Sciences) (no. 2018BSHZ001), International Collaborative Research Project of Qilu University of Technology (no. QLUTGJHZ2018020), National Nature Science Foundation of China (nos. 61603203 and 61773010), and Nature Science Foundation of Shandong Province (no. ZR2017MF064).

References

[1] F. Kerschbaum, D. Dahlmeier, A. Schröpfer, and D. Biswas, "On the practical importance of communication complexity for secure multi-party computation protocols," in *Proceedings of the the 2009 ACM symposium*, pp. 2008–2015, Honolulu, Hawaii, 2009.

[2] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 38, no. 4, pp. 453–456, 1991.

[3] A. C. Fowler, J. D. Gibbon, and M. J. McGuinness, "The complex Lorenz equations," *Physica D: Nonlinear Phenomena*, vol. 4, no. 2, pp. 139–163, 1981/82.

[4] C. Jiang, F. Zhang, H. Qin, and T. Li, "Anti-synchronization of fractional-order chaotic complex systems with unknown parameters via adaptive control," *The Journal of Nonlinear Science and Applications*, vol. 10, no. 11, pp. 5608–5621, 2017.

[5] F. Zhang, M. Li, S. Leng, and J. Liu, "Linear correlation of complex vector space and its application on complex parameter identification," *Journal of Qilu University of Technology*, vol. 1, pp. 70–73, 2019.

[6] F. Zhang, K. Sun, Y. Chen, H. Zhang, and C. Jiang, "Parameters identification and adaptive tracking control of uncertain complex-variable chaotic systems with complex parameters," *Nonlinear Dynamics*, pp. 1–16, 2019.

[7] Z. Wang, J. Liu, F. Zhang, and S. Leng, "Hidden Chaotic Attractors and Synchronization for a New Fractional-Order Chaotic System," *Journal of Computational and Nonlinear Dynamics*, vol. 14, no. 8, p. 081010, 2019.

[8] C. Luo and X. Wang, "Chaos in the fractional-order complex Lorenz system and its synchronization," *Nonlinear Dynamics*, vol. 71, no. 1-2, pp. 241–257, 2013.

[9] Y. Chen, H. Zhang, and F. Zhang, "Difference function projective synchronization for secure communication based on complex chaotic systems," in *Proceedings of the 5th IEEE International Conference on Cyber Security and Cloud Computing and 4th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud/EdgeCom 2018*, pp. 52–57, China, June 2018.

[10] H. S. Nik, S. Effati, and J. Saberi-Nadjafi, "Ultimate bound sets of a hyperchaotic system and its application in chaos synchronization," *Complexity*, vol. 20, pp. 30–44, 2014.

[11] S. Zheng, "Further results on the impulsive synchronization of uncertain complex-variable chaotic delayed systems," *Complexity*, vol. 21, no. 5, pp. 131–142, 2016.

[12] B. Sun, M. Li, F. Zhang, H. Wang, and J. Liu, "The characteristics and self-time-delay synchronization of two-time-delay complex Lorenz system," *Journal of The Franklin Institute*, vol. 356, no. 1, pp. 334–350, 2019.

[13] C.-Z. Ning and H. Haken, "Detuned lasers and the complex Lorenz equations: subcritical and supercritical Hopf bifurcations," *Physical Review A: Atomic, Molecular and Optical Physics*, vol. 41, no. 7, pp. 3826–3837, 1990.

[14] V. Y. Toronov and V. L. Derbov, "Boundedness of attractors in the complex Lorenz model," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 55, no. 3, pp. 3689–3692, 1997.

[15] A. D. Mengue and B. Z. Essimbi, "Secure communication using chaotic synchronization in mutually coupled semiconductor lasers," *Nonlinear Dynamics*, vol. 70, no. 2, pp. 1241–1253, 2012.

[16] L. F. Abdulameer, J. D. Jignesh, U. Sripati, and M. Kulkarni, "BER performance enhancement for secure wireless optical communication systems based on chaotic MIMO techniques," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 7–16, 2014.

[17] Y. Fu, M. Cheng, X. Jiang et al., "Wavelength division multiplexing secure communication scheme based on an optically coupled phase chaos system and PM-to-IM conversion mechanism," *Nonlinear Dynamics*, vol. 94, no. 3, pp. 1949–1959, 2018.

[18] S. Liu and F. Zhang, "Complex function projective synchronization of complex chaotic system and its applications in secure communication," *Nonlinear Dynamics*, vol. 76, no. 2, pp. 1087–1097, 2014.

[19] E. E. Mahmoud and S. M. Abo-Dahab, "Dynamical properties and complex anti synchronization with applications to secure communications for a novel chaotic complex nonlinear model," *Chaos, Solitons & Fractals*, vol. 106, pp. 273–284, 2018.

[20] R. L. Bagley and R. A. Calico, "Fractional order state equations for the control of viscoelastically damped structures," *Journal of Guidance, Control, and Dynamics*, vol. 14, no. 2, pp. 304–311, 1991.

[21] G. T. Oumbé Tékam, C. A. Kitio Kwuimy, and P. Woafo, "Analysis of tristable energy harvesting system having fractional order viscoelastic material," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 25, no. 1, 013112, 10 pages, 2015.

[22] N. Laskin, "Fractional market dynamics," *Physica A: Statistical Mechanics and its Applications*, vol. 287, no. 3-4, pp. 482–492, 2000.

[23] S. Hassan Hosseinnia, R. L. Magin, and B. M. Vinagre, "Chaos in fractional and integer order NSG systems," *Signal Processing*, vol. 107, pp. 302–311, 2015.

[24] M. Ö. Efe, "Fractional order systems in industrial automation—a survey," *IEEE Transactions on Industrial Informatics*, vol. 7, pp. 582–591, 2011.

[25] Y. Ding, Z. Wang, and H. Ye, "Optimal control of a fractional-order HIV-immune system with memory," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 3, pp. 763–769, 2012.

[26] I. Podlubny, "Geometric and physical interpretation of fractional integration and fractional differentiation," *Fractional Calculus and Applied Analysis*, vol. 5, no. 4, pp. 367–386, 2002.

[27] X. Wu, H. Wang, and H. Lu, "Modified generalized projective synchronization of a new fractional-order hyperchaotic system and its application to secure communication," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 3, pp. 1441–1450, 2012.

[28] S. Kassim, H. Hamiche, S. Djennoune, and M. Bettayeb, "A novel secure image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems," *Nonlinear Dynamics*, vol. 88, no. 4, pp. 2473–2489, 2017.

[29] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "Fast projective synchronization of fractional order chaotic and reverse chaotic systems with its application to an affine cipher using date of birth (DOB)," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1883–1897, 2015.

[30] R. Li and H. Wu, "Secure communication on fractional-order chaotic systems via adaptive sliding mode control with teaching–learning–feedback-based optimization," *Nonlinear Dynamics*, vol. 95, no. 2, pp. 1221–1243, 2019.

[31] A. Mohammadzadeh and S. Ghaemi, "Synchronization of uncertain fractional-order hyperchaotic systems by using a new self-evolving non-singleton type-2 fuzzy neural network and its application to secure communication," *Nonlinear Dynamics*, vol. 88, no. 1, pp. 1–19, 2017.

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

[33] D. Matignon, "Stability results for fractional differential equations with applications to control processing," in *Proceedings of the IMACS IEEE-SMC*, pp. 963–968, Lille, France, 1996.