Received 14 May 2017
Revised 3 August 2017
26 November 2017
Accepted 1 December 2017

On active synchronization of fractional-order Bloch chaotic system and its practical application in secure image transmission

Hamed Tirandaz and Ali Karami-Mollaee
Department of Electrical and Computer Engineering,
Hakim Sabzevari University, Sabzevar, Iran

Abstract

Purpose – The purpose of this paper is to propose a novel and secure image transmission based on the unpredictable behavior of the chaotic systems.

Design/methodology/approach – The proposed approach includes two main contributions: synchronization scheme and transmission scheme. The synchronization scheme benefits the advantage of the fractional-order active synchronization method. A new control law is derived to asymptotically synchronize the underlined fractional-order Bloch chaotic system. The validity of the proposed synchronization scheme is proved by the Lyapunov stability theorem. Then, a novel image transmission scheme is designed to transfer image data via chaotic signals, which modulates the encrypted data in the sender signals and demodulates it at the receiver side.

Findings – Numerical simulations are provided to show the validity and effectiveness of the proposed image transmission system. Furthermore, the performance of the image transmission system is evaluated using some illustrative examples and their corresponding statistical tests. The results demonstrate the effectiveness of the proposed method in comparison with other proposed methods in this subject.

Originality/value – A new chaos-based image transmission system is developed based on the synchronization of Bloch chaotic system. The introduced transmission system is interesting and could be applicable to any kind of secure image/video transmission.

Keywords Active control, Bloch chaotic system, Fractional calculus, Image transmission system, Secure communication

Paper type Research paper

1. Introduction

Sensitivity of chaotic systems to their initial conditions, boundedness, shape regularity, discrete structure of the digital images and also their numerous applications in secure image transformation make chaotic-based encryption systems much popular Alvarez and Li (2006). The objective of synchronization process is that the slave system to asymptotically track the trajectories of the master system.

Nowadays, chaos synchronization between two chaotic/hyper-chaotic systems has attracted a lot of attention by the researchers. The ultimate goal of chaos synchronization is to design a control law to force the state variables of a response system to track the trajectories of the leader system state variables. Since the pioneering work done by Ott *et al.* (1990) at 1990 on chaotic systems, several methods have been investigated on synchronization of two chaotic or hyper-chaotic systems. Active method Nik *et al.* (2014), Richter (2002), Huang and Cao (2017), Adaptive method Adloo and Roopaei (2011), Tirandaz-Hajipour (2017), Ma *et al.* (2015), Hong (2013), impulsive method Li *et al.* (2005), projective method Chun-Lai *et al.* (2016), Tirandaz and Karmi-Mollaee (2017), lag method Rosenblum *et al.* (1997), sliding method Sun *et al.* (2014), Aghababa and Heydari (2012) and backstepping control method Yu *et al.* (2011) are some of the investigated synchronization methods.

International Journal of Intelligent Computing and Cybernetics
Vol. 11 No. 2, 2018
pp. 181-196
© Emerald Publishing Limited
1756-378X
DOI 10.1108/IJICC-05-2017-0048

The subject of synchronization of fractional-order chaotic systems has became a challenging research area since the pioneering work by Deng and Li (2005) due to its effective performances in accurate describing of the chaotic systems. Fractional-order chaotic produce different chaotic signals in comparison with their corresponding integer-one signals due to the slight initial transform of fractional-order chaotic systems. Therefore, fractional-order chaotic systems can introduce some new key information, which results enhancement in secure communication systems Wu *et al.* (2012). In the last decades, the synchronization problem of fractional-order chaotic systems has attracted a great deal of attention by many researchers Huang and Cao (2017), Baleanu *et al.* (2017), and Aguila-Camacho *et al.* (2016). For example, the synchronization problem of fractional-order Lorenz chaotic system was investigated in Aguila-Camacho *et al.* (2016), via designing an adaptive control method. In Xi *et al.* (2014), an adaptive impulsive method for synchronization of a class of fractional-order chaotic systems was achieved. In Huang and Cao (2017), an active control law for synchronization and anti-synchronization problem of fractional-order finance chaotic systems is derived. The synchronization between an integer-order chaotic system and its fractional order system was developed in Ouannas *et al.* (2017). Chaos analysis and stability of generalized fractional-order chaotic system was investigated by Baleanu *et al.* (2017).

Recently, secure image data transformation is an important challenge topic. So many image cryptosystems have been developed during the recent past decades which are established based on the traditional cryptography approaches such as public key cryptosystem for providing secure for digital signature in Rivest *et al.* (1978), and data encryption system in Davio *et al.* (1984) and many others. In this subject, chaos-based secure data transmission systems and cryptography have considerably attracted due to their reliability and their time/space complexity. It has been proved that drive-response communication systems are more reliable than conventional cryptosystems, such as RSA, IDEA and AES, in all aspects of time/space complexity and security concerns. On the other hand, utilizing both shuffling and scrambling techniques can provide a more reliable system with more time complexity than the other proposed methods in the literature, which use either shuffling or scrambling techniques separately. Therefore, a chaos-based data transmission system upon the shuffling and scrambling techniques can provide more secure transmission system. Moreover, the time-complexity resulted from shuffling and scrambling techniques are ignorable with respect to the speed of the chaos-based data transmission systems. In chaos-based cryptosystems, transmitted data would be modulated into the state variables of chaotic systems, which make impossible any outside attack to decrypt encrypted information.

Generally, the chaotic based image data cryptosystems are categorized into: integer-order and fractional-order schemes. The cryptosystems related to the fractional-order systems provide more security in transformation information than their corresponding approaches with the integer-order systems. Therefore, fractional-based image encryption systems, which is focused in this paper, provide more interesting cryptosystems rather than integer ones. An image cryptosystem based on the chaotic map is proposed in Wang and Guo (2014). In Chen *et al.* (2004), a symmetric image data encryption technique is introduced based on 3D chaotic systems. In Wu *et al.* (2014), an image cryptosystem based on two different six-dimensional hyper-chaotic systems is developed. In Zhang and Wang (2008), an image encryption system is developed based on the interference. An image encryption algorithm is proposed in Xu *et al.* (2014) for synchronization between two fractional-order chaotic systems. Then, Ahmad *et al.* in Ahmad *et al.* (2015) extended the proposed method by Xu *et al.*

The majority of the introduced cryptosystem approaches hide image data information in a chaotic signal based on two distinguish techniques: shuffling technique and scrambling technique. But there are minor investigated works concern both of the shuffling and scrambling schemes. Although utilizing both techniques can improve the security level of the data transmission. But, most of the developed cryptosystems are not suitable for real-time encryption/decryption of image or videos. The ultimate goal of designing cryptosystems is to develop a reliable, real-time and simple cryptosystem which is main contribution of this paper. Therefore, the aim of this paper is to develop a new real-time secure image transmission system, which benefits both shuffling and scrambling techniques.

It is well known that the Bloch system is very important for interpretation of the underlying physical process of nuclear magnetic resonance Liu *et al.* (2017). Recently, time-delayed fractional-order Blaoch chaotic system was reviewed in Bhalekar *et al.* (2011). Furthermore, more interest in the fractional-order Bloch chaotic system has been growing Magin *et al.* (2009) with the goal of improving the modeling of relaxation, diffusion, and perfusion in biological tissues. In Hamri and Houmor (2011), the structure of commensurate fractional-order Bloch chaotic system and its bifurcations were analyzed. In Liu *et al.* (2017), the bifurcation and synchronization problems of a fractional-order Bloch system are studied.

The main highlights of this research are arranged as follows:

- A new active control strategy is utilized for synchronization of the Bloch chaotic system.
- The good performance and flexibility of the introduced synchronization scheme are illustrated by some numerical results.
- A chaos-based image transmission system is developed, which modulates the encrypted image data on state variables signals and transmits the embedded signals to the receiver.

The reminder of this paper is organized as follows: some mathematical discussions and preliminaries about fractional calculus are presented in Section 2. Then, an active synchronization scheme is developed in Section 3, which drives a control law to synchronize two identical drive-response Bloch chaotic systems followed by some numerical results to show its efficiency and its stability. After that, in Section 4, a new image transmission system is provided, which encrypted the image data before transmission, transmit it by modulating into chaotic signals. The performance of the transmission scheme is verified by some illustrative examples. Finally, some concluding remarks are given in Section 5.

2. Mathematical modeling

2.1 Fractional calculus

Fractional calculus is a generalization of the integer order ones. Up to now, some efforts have been devoted to calculate the fractional order differentiation and integration. Among these efforts, there are three commonly used definitions as Grunward-Letnikov method in Podlubny (1999), Caputo (1967), and Riemann-Liouville method in Podlubny (1999) definitions. Fractional-order definition of a typical function *f*(*t*) can be described based on the Grunwald-Letnikov (GL) definition as follows:

$$D^{\alpha}f(t)=\lim_{h\to 0}\sum_{i=0}^{n}\binom{-q}{i}f(t-iq) \tag{1}$$

where $n=\left|t-\alpha/h\right|$ and α denotes the fractional-order which is defined as $-1\leqslant\alpha\leqslant 1$. When $\alpha=1$, it calculate the differntial of *f*(*t*) and when $\alpha=-1$, the integral of *f*(*t*) would be calculated. The Reimann-Liouville (RL) definition for the fractional-order definition of the f(t) can also be described as:

$$D^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)}\frac{d^n}{dt^n}\int_0^t \frac{f(\tau)}{(t-\tau)^{\alpha-1-n}}d\tau \tag{2}$$

where n is the first integer which is not less than q, i.e. $n-1 \leqslant q < n$ and $\Gamma(.)$ denotes the well-known Euler's gamma function which can be calculated as:

$$\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}dt, \quad \Gamma(z+1) = z\Gamma(z) \tag{3}$$

Finally, the Caputo definition for the fractional-order calculation of the *f*(*t*) can be given as follows:

$$D_t^{\alpha} = \begin{cases} \frac{1}{\Gamma(n-\alpha)}\int_0^t (t-\tau)^{n-\alpha-1}\frac{d^n f(\tau)}{d\tau^n}d\tau, & n-1 < \alpha < n \\ \frac{d^n}{dt^n}f(t) & \alpha = n \in N \end{cases} \tag{4}$$

The Laplace transform function for the RL fractional derivative can be represented as:

$$L\{D^{\alpha}f(t)\} = s^{\alpha}L\{f(t)\} - \sum_{k=0}^{n-1} s^k \left[\frac{d^{\alpha-1-k}f(t)}{dt^{\alpha-1-k}}\right]\Bigg|_{t=0} \tag{5}$$

where s denotes a complex variable. It illustrates that the fractional derivative of a function at $t = 0$ is required in the Laplace transform of the Riemann-Liouville non-integer derivative. However, this weakness is not exist furthermore in the Laplace transform of the Caputo definition, which is given by:

$$L\{D^{\alpha}f(t)\} = s^{\alpha}L\{f(t)\} - \sum_{k=0}^{n-1} s^{\alpha-1-k}f^{(k)}(0) \tag{6}$$

From Equation (6), only the integer-order derivative of function *f*(*t*) appears in the Laplace transform of the Caputo derivative. With assigning zero to the initial conditions, the Equation (6) simplified as:

$$L\{D^{\alpha}f(t)\} = s^{\alpha}L\{f(t)\} \tag{7}$$

Furthermore, the GL and RL fractional order definitions are equivalent for a wide class of functions. However, the initial conditions for the fractional calculus with the Caputo derivative are in the same form as for integer-order ones which have well understood physical meaning. Therefore, the Caputo fractional-order derivative is more popular than the RL definition of fractional derivative, when modeling real-world phenomena with FDE. Therefore, the Caputo fractional-order derivative is utilized along this paper.

2.2 Bloch system description

In this paper, a three-dimensional Bloch chaotic system is considered. The Bloch system was firstly studied in analyzing the behavior of spins. In Hamri and Houmor (2011), it is integer-order and fractional order behavior are studied. The integer-order dynamics of this system can be described by the following differential equations:

$$\begin{aligned} \dot{x}_1 &= \delta x_2 + \gamma x_3(x_1 \sin(c) - x_2 \cos(c)) - \frac{x_1}{\Gamma_2} \\ \dot{x}_2 &= -\delta x_1 - x_3 + \gamma x_3(x_1 \cos(c) + x_2 \sin(c)) - \frac{x_2}{\Gamma_2} \\ \dot{x}_3 &= x_2 - \gamma \sin(c)\left(x_1^2 + x_2^2\right) - \frac{x_3 - 1}{\Gamma_1} \end{aligned} \tag{8}$$

where x_1, x_2 and x_3 are the state variables and Γ_1, Γ_2, δ, γ and c stand for the parameters of the system. When $\Gamma_1 = 0.4$, $\Gamma_2 = 0.25$, $\delta = 1.3$, $\gamma = 11$ and $c = 0.76$, it is indicated that the system (8) is chaotic. The chaotic behavior of the system with these parameters are depicted in Figure 1, with initial values $x_1(0) = 0.1$, $x_2(0) = 0.2$ and $x_3(0) = 0.4$.

The Bloch chaotic system with incommensurate fractional time derivative can be given by:

$$D^{\alpha_1}x_1 = \delta x_2 + \gamma x_3(x_1 \ \sin(c) - x_2 \ \cos(c)) - \frac{x_1}{\Gamma_2}$$

$$D^{\alpha_2}x_2 = -\delta x_1 - x_3 + \gamma x_3(x_1 \ \cos(c) + x_2 \ \sin(c)) - \frac{x_2}{\Gamma_2}$$

$$D^{\alpha_3}x_3 = x_2 - \gamma \ \sin(c)\left(x_1^2 + x_2^2\right) - \frac{x_3 - 1}{\Gamma_1} \tag{9}$$

where $\alpha_{1,}$ α_2 and α_3 denote the derivative orders. For the parameters $\Gamma_1 = 0.4$, $\Gamma 0.25$, $\delta = 1.3$, $\gamma = 11$ and $c = 0.76$, the fractional-order system (9) also shows chaotic behavior, with orders: $\alpha_1 = 0.97$, $\alpha_2 = 0.98$ and $\alpha_3 = 0.96$ and system initial values $x_1(0) = 0.1$, $x_2(0) = 0.2$ and $x_3(0) = 0.4$. The phase portraits of the system (9) in the *x-y*, *y-z*, *z-x* planes and the *x-y-z* space are shown through the Figure 2 (a)-(d), respectively.

3. Synchronization

In this section, the synchronization problem between two identical fractional-order Bloch chaotic systems is considered. An active control method is derived to achieve this goal.

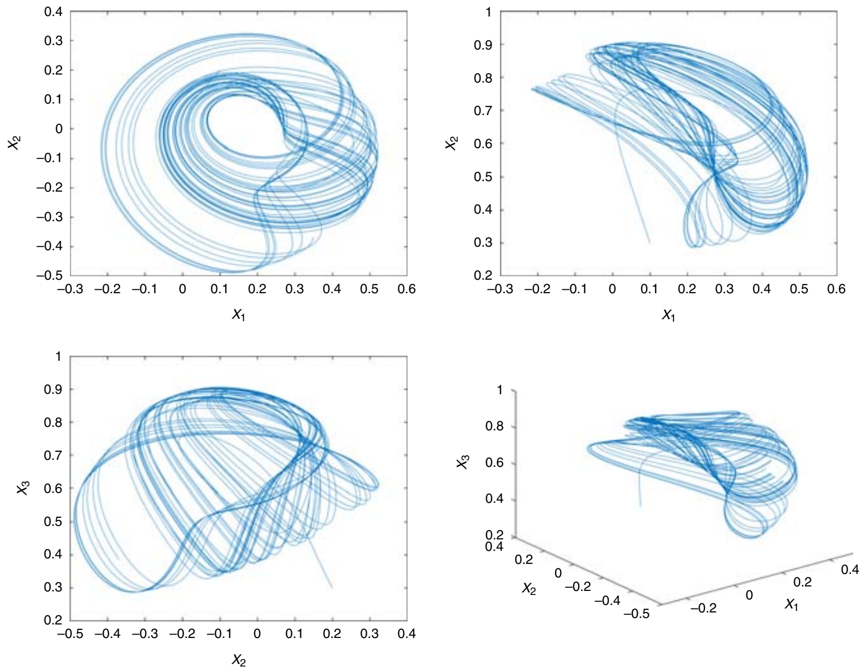

Figure 1.
Phase portraits of the integer-order Bloch chaotic system

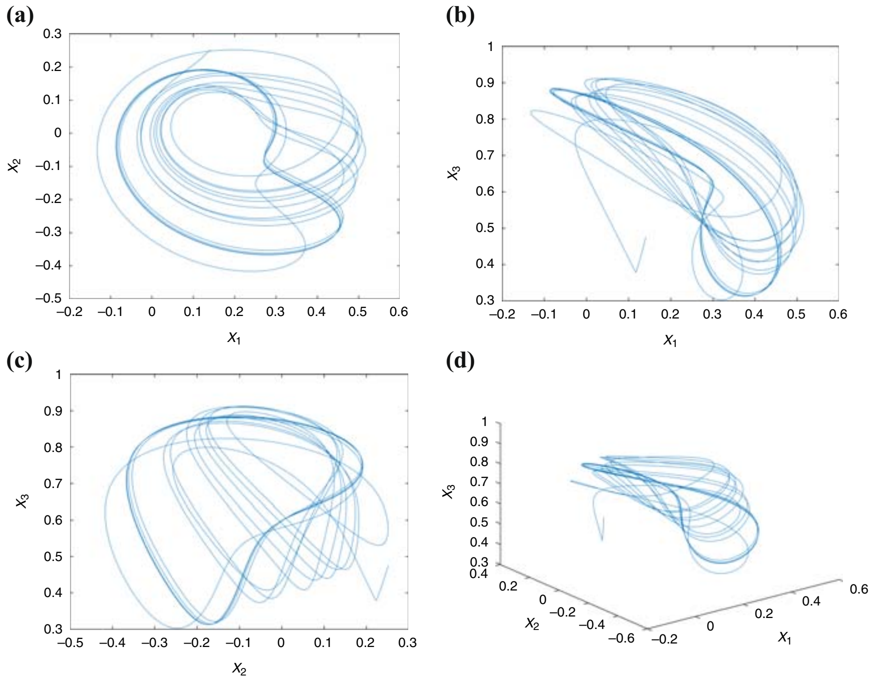

Figure 2.
Phase portraits of the fractional-order Bloch chaotic system

3.1 Control design

Consider the fractional-order Bloch chaotic system (9), as the drive system. Then the identical response system can be described as:

$$D^{\alpha_1}y_1=\delta y_2+\gamma y_3(y_1\ \sin(c)-y_2\ \cos(c))-\frac{y_1}{\Gamma_2}+u_1(t)$$

$$D^{\alpha_2}y_2=-\delta y_1-y_3+\gamma y_3(y_1\ \cos(c)+y_2\ \sin(c))-\frac{y_2}{\Gamma_2}+u_2(t)$$

$$D^{\alpha_3}y_3=y_2-\gamma\ \sin(c)\left(y_1^2+y_2^2\right)-\frac{y_3-1}{\Gamma_1}+u_3(t) \tag{10}$$

where $u_1(t)$, $u_2(t)$ and $u_3(t)$ stand for the control laws to be designed. Then, the synchronization errors between two identical Bloch chaotic systems (9) and (10) can be designed as follows to achieve active synchronization. We have:

$$e_1=y_1-x_1,\quad e_2=y_2-x_2,\quad e_3=y_3-x_3,$$

Thus, the dynamics of synchronization errors can be determined by subtracting the drive system (9) from the response (10), as follows:

$$D^{\alpha_1}e_1=\delta e_2+\gamma\ \sin(c)(y_1e_3+e_1x_3)-\gamma\ \cos(c)(y_2e_3+e_2x_3)-\frac{e_1}{\Gamma_2}+u_1(t)$$

$$D^{\alpha_2}e_2=-\delta e_1-e_3+\gamma\ \cos(c)(y_1e_3+e_1x_3)+\gamma\ \sin(c)(y_2e_3+e_2x_3)-\frac{e_2}{\Gamma_2}+u_2(t)$$

$$D^{\alpha_3}e_3=e_2-\gamma\ \sin(c)(e_1(x_1+y_1)+e_2(x_2+y_2))-\frac{e_3}{\Gamma_1}+u_3(t) \tag{11}$$

Then, the active control laws $u_1(t)$, $u_2(t)$ and $u_3(t)$ can be defined as:

$$\begin{aligned} u_1(t) &= -\gamma\ \sin(c)(y_1e_3+e_1x_3)+\gamma\ \cos(c)(y_2e_3+e_2x_3)+v_1(t) \\ u_2(t) &= -\gamma\ \cos(c)(y_1e_3+e_1x_3)-\gamma\ \sin(c)(y_2e_3+e_2x_3)+v_2(t) \\ u_3(t) &= +\gamma\ \sin(c)(e_1(x_1+y_1)+e_2(x_2+y_2))+v_3(t) \end{aligned} \tag{12}$$

Then, the error system can be simplified as:

$$\begin{aligned} D^{\alpha_1}e_1 &= \delta e_2-\frac{e_1}{\Gamma_2}+v_1(t) \\ D^{\alpha_2}e_2 &= -\delta e_1-e_3-\frac{e_2}{\Gamma_2}+v_2(t) \\ D^{\alpha_3}e_3 &= e_2-\frac{e_3}{\Gamma_1}+v_3(t) \end{aligned} \tag{13}$$

where $v_1(t)$, $v_2(t)$ and $v_3(t)$ represent the linear feedback controllers, which can be chosen in such way that the error system 13 would be stable. Let the linear controllers $v_1(t)$, $v_2(t)$ and $v_3(t)$ as:

$$\begin{bmatrix} v_1(t) \\ v_2(t) \\ v_3(t) \end{bmatrix} = A \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} \tag{14}$$

where A is a 3×3 matrix of real values. To stabilized the synchronization error system (13), one have to assign the eigenvalues λ_i of the error system (13) such that $|\arg(\lambda_i)| > \max\{\alpha_1,\alpha_2,\alpha_3\}\pi/2$. Let $\lambda_1=-1$, $\lambda_2=-1$ and $\lambda_3=-1$, then we have:

$$A = \begin{bmatrix} \frac{1}{\Gamma_2}-1 & -\delta & 0 \\ \delta & \frac{1}{\Gamma_2}-1 & 1 \\ 0 & -1 & \frac{1}{\Gamma_1}-1 \end{bmatrix} \tag{15}$$

Now, the error system (13) would be stabilized with considering the proposed feedback control laws and also the synchronization between the two identical Bloch chaotic systems (9) and (10) would be achieved.

3.2 Numerical simulations

In this subsection, we have presented two numerical examples to demonstrate and verify the performance of the introduced synchronization scheme. To this end, the fourth Runge-Kutta method is utilized in order to solve the synchronization problem with time step size 10E-7.

Example1. In the first simulation, the parameters of the system are considered as $\Gamma_1=0.4$, $\Gamma_2=0.25$, $\delta=1.2$, $\gamma=11$ and $c=0.76$. The initial conditions of the system state variables of the drive system are assigned as $(x_1(0), x_2(0), x_3(0))=(0.1, 0.2, 0.3)$ and also the response system are assigned as $(y_1(0), y_2(0), y_3(0))=(5, -1, 3)$. In addition, the fractional derivatives of the Bloch chaotic system are considered as $\alpha_1=0.97$, $\alpha_2=0.98$ and $\alpha_3=0.96$. The obtained result from this simulation is depicted in Figure 3. As we can see, the active synchronizations between the leader (9) and the follower (10) fractional-order Bloch chaotic system is achieved. Furthermore, the synchronization errors converge to zero as time goes to infinity. In addition, the trajectories of the control feedback law is depicted in Figure 4, to show its stability.

Example2. As the second simulation, the parameters of the system are considered as $\Gamma_1=0.6$, $\Gamma_2=0.3$, $\delta=1.3$, $\gamma=11$ and $c=0.78$. The initial conditions of the system state variables of the drive system are assigned as $(x_1(0), x_2(0), x_3(0))=(1, -1, 2)$ and also the response system are assigned as $(y_1(0), y_2(0), y_3(0))=(10, 12, 9)$. In addition, the fractional derivatives of the Bloch chaotic system are considered as $\alpha_1=0.99$, $\alpha_2=0.95$ and $\alpha_3=0.97$. The obtained result from this simulation is depicted in Figure 5. As we can see, the active synchronizations between the leader (9) and the follower (10) fractional-order Bloch chaotic system is achieved. Furthermore, the synchronization errors converge to zero as time goes to infinity. In addition, the trajectories of the control feedback law is depicted in Figure 6, to show its stability.

4. Image transmission system

In this section, the structure of a new public key cryptosystem is provided to hide image into chaotic system state variables. The ultimate objective of a public key cryptography is to

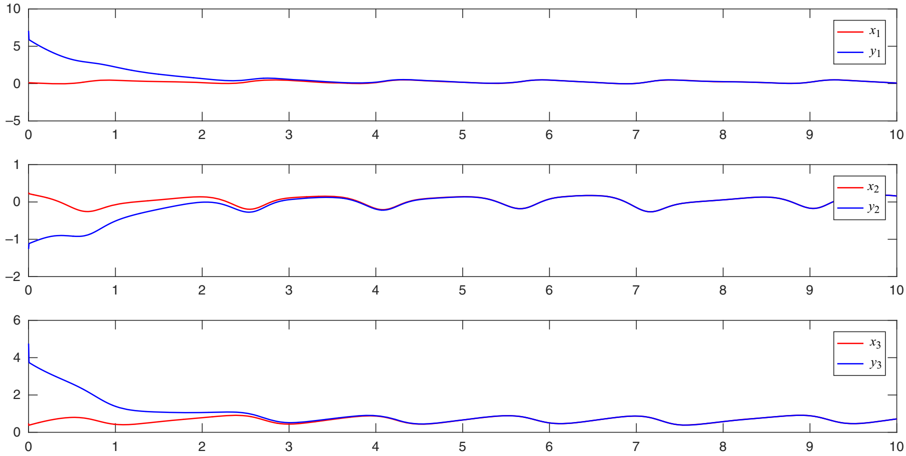

Figure 3.
Active synchronization between the drive fractional-order Bloch system (9) and the response system (9) with different fractional orders $(\alpha_1, \alpha_2, \alpha_3)=(0.97, 0.98, 0.96)$ – Example1

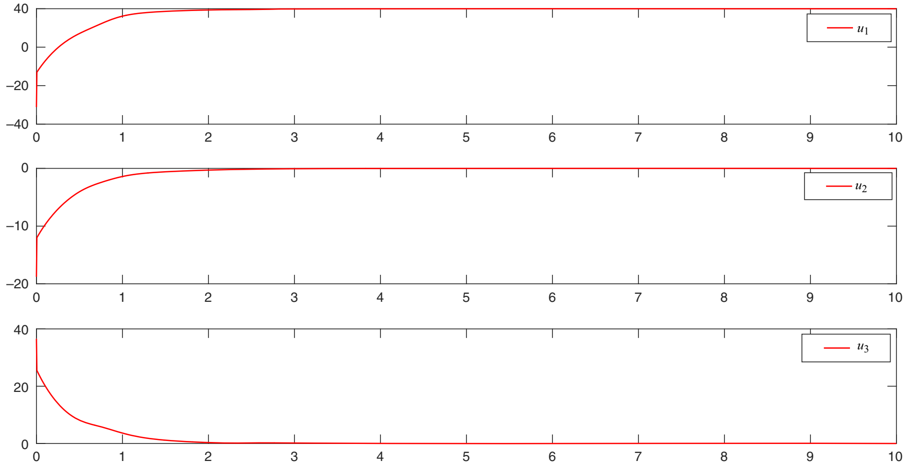

Figure 4.
Time-series of the designed feedback controller $U=(u_1, u_2, u_3)$ for synchronization of different fractional orders $(\alpha_1, \alpha_2, \alpha_3)=(0.97, 0.98, 0.96)$ – Example1

develop a cryptosystem that allows every one encrypt a pattern and send it to the interesting person using his public key. But decrypt pattern without corresponding private key would be impossible. The block diagram of the image cryptosystem is illustrated in Figure 7. As it can be seen, the encryption/decryption algorithms established based on a hybrid shuffling-scrambling techniques. Firstly, the queue order of image pixels for encryption procedure is determined in the shuffling step. Then the procedure of the data encryption is executed over the raw pixel values organized at the previous step. This procedure perform conversely in the decryption algorithm.

Consider the drive fractional order Bloch chaotic system in (9) as the sender system, the response Bloch chaotic system in (10) as the receiver system. Let $I(m, n) \in R^{M \times N} (1 \leqslant m \leqslant 7M, 1 \leqslant n \leqslant N)$ as the input original gray image. It is worth mention that a color image can be seen as a three gray-level images. For example: R, G and B equivalent to Red, Green and Blue in the RGB color space model, respectively. Then the steps of the image encryption/decryption cryptosystem can be given as follows.

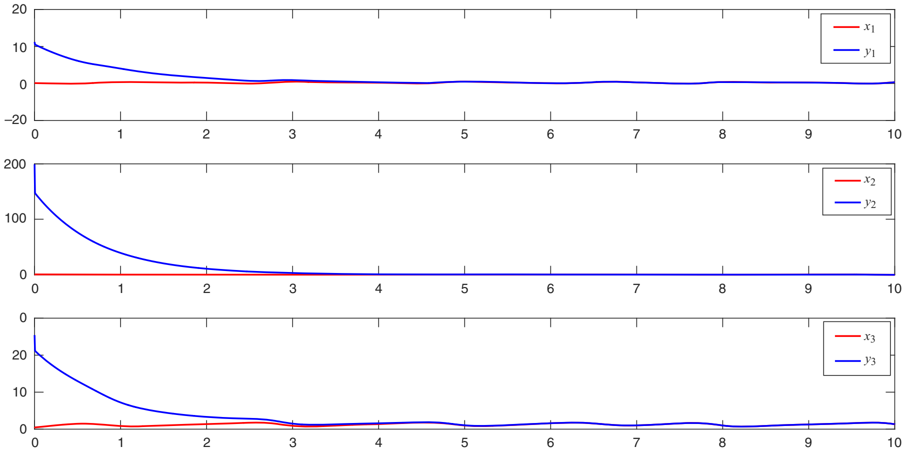

Figure 5. Active synchronization between the drive Bloch system (9) and the response system (10) with different fractional orders $(\alpha_1, \alpha_2, \alpha_3) = (0.99, 0.95, 0.97)$ – Example2

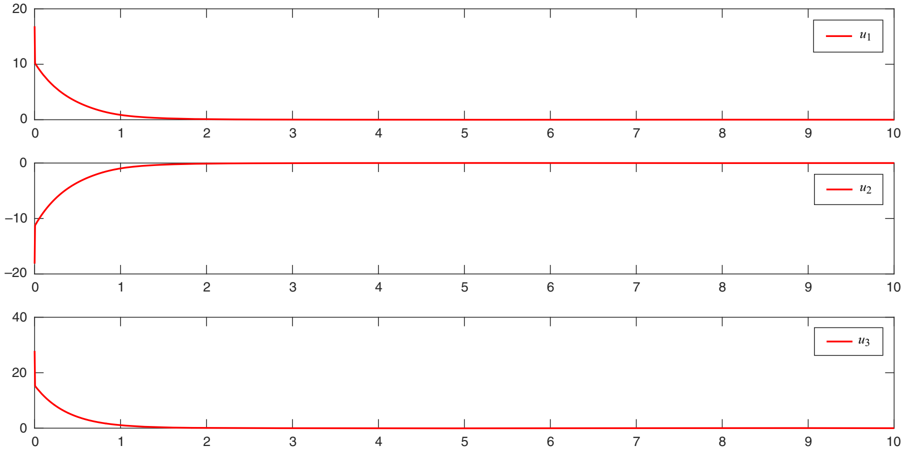

Figure 6. Time-series of the designed feedback controller $U = (u_1, u_2, u_3)$ for synchronization of different fractional orders $(\alpha_1, \alpha_2, \alpha_3) = (0.99, 0.95, 0.97)$ – Example2

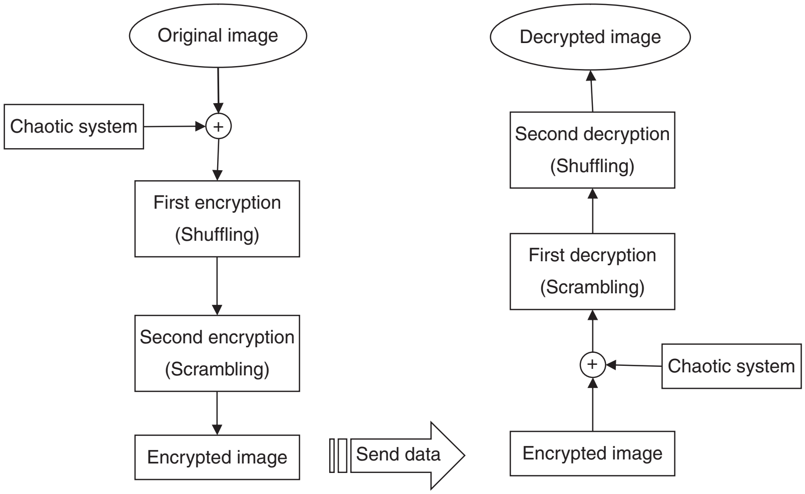
Original image
Chaotic system
+
First encryption (Shuffling)
Second encryption (Scrambling)
Encrypted image
Send data
Decrypted image
Second decryption (Shuffling)
First decryption (Scrambling)
+
Chaotic system
Encrypted image

Figure 7. Block diagram of the proposed image encryption/decryption system

4.1 Image cryptosystem algorithm

Let $\eta = M \times N$ and choose the suitable value e, arbitrary. Then any Image I can be hidden into the values of the sender state signals as follows.

Step 1: (Shuffling)

For each pixel position (m, n), calculate:

$$((m+1)N+n)^e \overset{\eta}{\equiv} i(m,n)$$

where $i(m, n) \in \boldsymbol{N}$ is the Shuffling position of the image pixel (m, n). When the position $i(m, n)$ has occupied by another pixel $(i(m, n) = i(m', n'))$, then the position of the pixel (m, n) would be shifted to the subsequent empty position.

Step 2: (Scrambling)

Let $I(i) = (I_r(i), I_g(i), I_b(i))$ the three components of a color image in the RGB color space. Then transform every pixel values $I(i) = (I_r(i), I_g(i), I_b(i))$ to the $O(i) = (O_r(i), O_g(i), O_b(i))$ by the following mathematical operations:

$$O_r(i) = (I_r(i) \oplus \tilde{x}_1(\tau+i)) + \tilde{x}_1(\tau+i)$$

$$O_g(i) = \left(I_g(i) \oplus \tilde{x}_2(\tau+i)\right) + \tilde{x}_2(\tau+i)$$

$$O_b(i) = (I_b(i) \oplus \tilde{x}_3(\tau+i)) + \tilde{x}_3(\tau+i) \qquad (16)$$

Where i denotes the position of the pixel value in the image queue order. and $\tilde{x}_k(t)$ indicates the integer part of the $x_k(t) \times 10^4$ for $k = 1, 2, 3$. Then the output encrypted signal values O_r, O_g, O_b will be send to the receiver.

4.2 Image decryption algorithm

Receiver gets the encrypted signals $O = (O_r, O_g, O_b)$. Then calculates the original image data $I = (I_r, I_g, I_b)$ by performing the decryption procedure shown in block diagram (7) (Figure 8):

Step 1: (Scrambling)

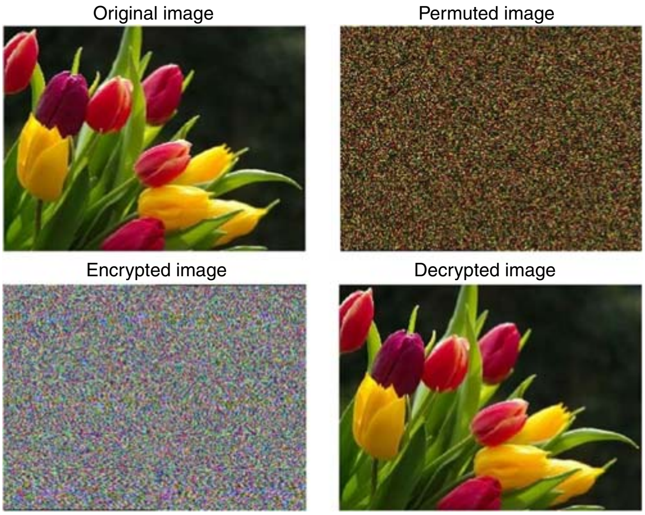

Figure 8.
Image encryption-decryption process

In this step, the encrypted values I_r, I_g and I_b can be recovered as follows:

$$\tilde{I}_r(i) = (O_r(i) - \tilde{y}_1(\tau + i)) \oplus \tilde{y}_1(\tau + i)$$
$$\tilde{I}_g(i) = \left(O_g(i) - \tilde{y}_2(\tau + i)\right) \oplus \tilde{y}_2(\tau + i)$$
$$\tilde{I}_b(i) = (O_b(i) - \tilde{y}_3(\tau + i)) \oplus \tilde{y}_3(\tau + i) \tag{17}$$

where y_1, y_2 and y_3 are the reciever state values, and the decrypted image data are denoted by the $\tilde{I} = (\tilde{I}_r, \tilde{I}_g, \tilde{I}_b)$.

4.3 Image correlation analysis

Its evident that in a plain image, the color spectrum of a pixel is almost isochromatic with the colors of its neighborhood pixels. It means that a plain image has high correlation between its adjacent pixels either in vertical, horizontal or diagonal directions. On the other hand, the correlation between the neighborhood pixels of an encrypted image has to be as least as possible to reduce the possible outsider attacks. In this paper, the correlation between all two horizontal, vertical and diagonal pixels of both original image and its encrypted image is calculated based on the following correlation formula:

$$r_{xy} = \frac{\mathrm{cov}\left(I_x, I_y\right)}{\sqrt{D(x)D(y)}} \tag{18}$$

where I_x, I_y are the gray-level of the corresponding image in the position of x and I, respectively and:

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

The diagonal correlation between two adjacent pixels of the original image and its encrypted image is depicted in Figure 9 for R, G and B color channels. The correlation of the original plain image and encrypted image is given in Table I. It can be clearly seen from these results that the pixels of a plain image have high correlations with their adjacent pixels while pixels of an encrypted image have low correlation. In other words, a plain image is almost uniform while an encrypted image is fairly uniform (Figure 10).

4.4 Image entropy

Image entropy is another performance evaluation method to assess the robustness of the image encryption algorithm. Based on the information theory founded by Shannon (1948), the image entropy can be given as:

$$H(x) = \sum_{i=0}^{255} p(x_i)\log_2 \frac{1}{p(x_i)} \tag{19}$$

where $H(x)$ denotes the entropy of image x and $p(x_i)$ indicates the statistical probability of the gray-level x_i in the image x. The entropy of a random gray-level image is 8. The calculated entropy of the obtain encrypted image from our proposed method is 7.9981, which is almost near to 8. Table II presents the comparison between the image entropy obtained by different methods. This implicates that the information leakage rate of the proposed cryptosystem is almost zero.

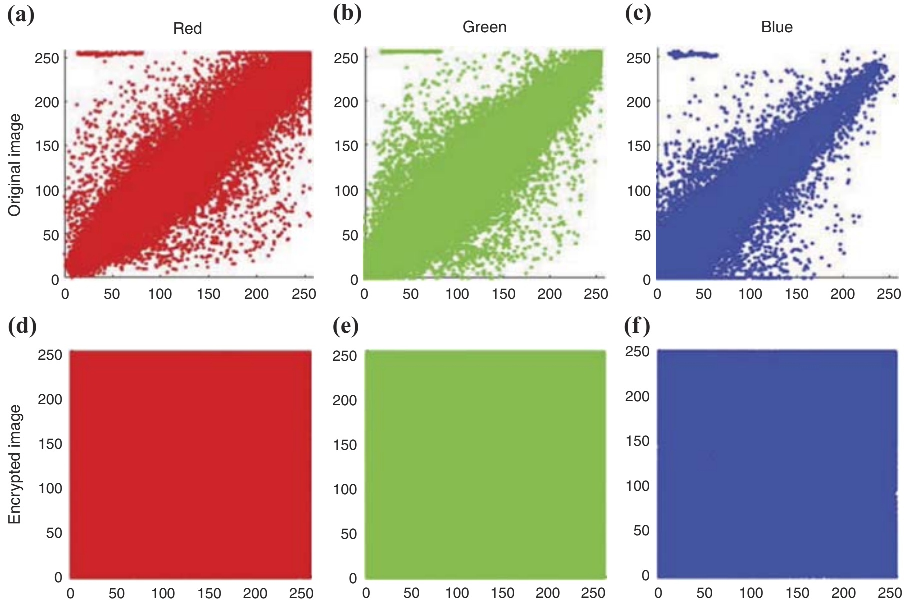

Figure 9.
Red, Blue and Green color channel Correlation analysis between (x, y) and $(x+1, y+1)$,two diagonal adjacent pixels of the original and the encrypted images, respectively

Table I.
Image correlations

Image	Horizontal	Vertical	Diagonal
Plain image	0.9869	0.9922	0.9776
Encrypted image	0.0395	0.0202	0.4005

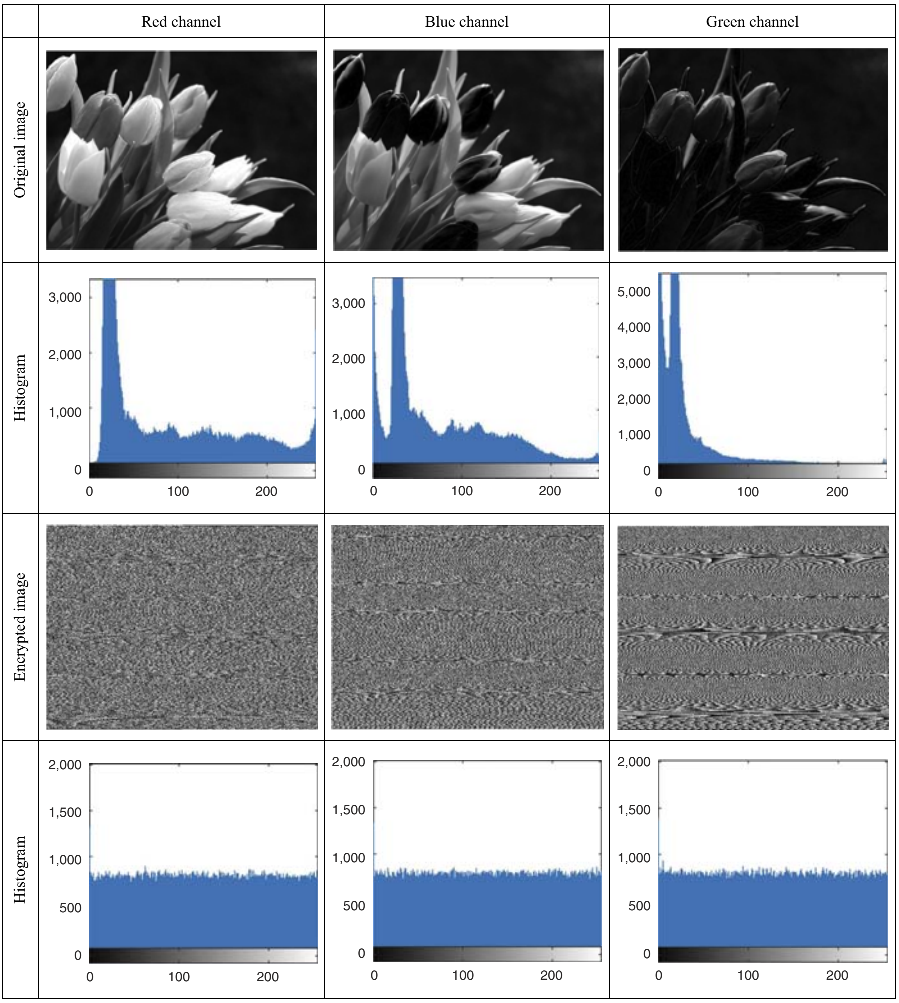

Figure 10. Red, Blue and Green color channel encryption and their corresponding histograms

Method	Image entropy
Wang and Guo (2014)	7.9977
Akhavan *et al.* (2011)	7.9978
Xu *et al.* (2014)	7.9896
Ahmad *et al.* (2015)	7.989576
Proposed method	7.9981

Table II. Image entropy

5. Conclusion

In this research, a new active control strategy is utilized for synchronization of two identical fractional-order Bloch chaotic system. An appropriate feedback control law are derived to achieve synchronization. Some numerical simulations are presented to show the convergence of the proposed synchronization method. Then, a novel cryptosystem based on drive-response system signals is developed for secure image data transformation. The encrypted image data have fed back to the drive chaotic system, as the sender. Then the decrypted image data will extracted in the receiver using response signal and decryption algorithm. The operating mechanism of the cryptosystem is illustrated by some examples. Finally, some statistical analysis were performed to measure the security of the proposed cryptosystem. The results demonstrate the high security of our proposed method and its robustness in comparison with other well-known cryptosystems. It is worth pointing out that the proposed cryptosystem is applicable to any other chaotic systems as it has no restrictions to be controlled.

References

Adloo, H. and Roopaei, M. (2011), "Review article on adaptive synchronization of chaotic systems with unknown parameters", *Nonlinear Dynamics*, Vol. 65 No. 1, pp. 141-159.

Aghababa, M.P. and Heydari, A. (2012), "Chaos synchronization between two different chaotic systems with uncertainties, external disturbances, unknown parameters and input nonlinearities", *Applied Mathematical Modelling*, Vol. 36 No. 4, pp. 1639-1652.

Aguila-Camacho, N., Duarte-Mermoud, M.A. and Delgado-Aguilera, E. (2016), "Adaptive synchronization of fractional Lorenz systems using a reduced number of control signals and parameters", *Chaos, Solitons & Fractals*, Vol. 87 No. 1, pp. 1-11.

Ahmad, M., Shamsi, U. and Khan, I.R. (2015), "An enhanced image encryption algorithm using fractional chaotic systems", *Procedia Computer Science*, Vol. 57 No. 1, pp. 852-859.

Akhavan, A., Samsudin, A. and Akhshani, A. (2011), "A symmetric image encryption scheme based on combination of nonlinear chaotic maps", *Journal of the Franklin Institute*, Vol. 348 No. 8, pp. 1797-1813.

Alvarez, G. and Li, S. (2006), "Some basic cryptographic requirements for chaos-based cryptosystems", *International Journal of Bifurcation and Chaos*, Vol. 16 No. 8, pp. 2129-2151.

Baleanu, D., Wu, G.C. and Zeng, S.D. (2017), "Chaos analysis and asymptotic stability of generalized Caputo fractional differential equations", *Chaos, Solitons & Fractals* Vol. 102 No. 1, pp. 99-105.

Bhalekar, S., Daftardar-Gejji, V., Baleanu, D. and Magin, R. (2011), "Fractional Bloch equation with delay", *Computers & Mathematics with Applications*, Vol. 61 No. 5, pp. 1355-1365.

Caputo, M. (1967), "Linear models of dissipation whose Q is almost frequency independent II", *Geophysical Journal International*, Vol. 13 No. 5, pp. 529-539.

Chen, G., Mao, Y. and Chui, C.K. (2004), "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons & Fractals*, Vol. 21 No. 3, pp. 749-761.

Chun-Lai, L., Mei, Z., Feng, Z. and Xuan-Bing, Y. (2016), "Projective synchronization for a fractional-order chaotic system via single sinusoidal coupling", *Optik-International Journal for Light and Electron Optics*, Vol. 127 No. 5, pp. 2830-2836.

Davio, M., Desmedt, Y., Fosseprez, M., Govaerts, R., Hulsbosch, J., Neutjens, P., F'iret, P., Quisquater, J.J., Vandewalle, J. and Wouters, P. (1984), "Analytical characteristics of the DES", in Chaum, D. (Ed.) *Advances in Cryptology Proc. Crypto '83*, Plenum, New York, NY, pp. 171-202.

Deng, W.H. and Li, C.P. (2005), "Chaos synchronization of the fractional lü system", *Physica A: Statistical Mechanics and its Applications*, Vol. 353 No. 1, pp. 61-72.

Hamri, N.E. and Houmor, T. (2011), "Chaotic dynamics of the fractional order nonlinear Bloch system", *Electronic Journal of Theoretical Physics*, Vol. 8 No. 25, pp. 233-244.

Hong, K.S. (2013), "Adaptive synchronization of two coupled chaotic HindmarshRose neurons by controlling the membrane potential of a slave neuron", *Applied Mathematical Modelling*, Vol. 37 No. 4, pp. 2460-2468.

Huang, C. and Cao, J. (2017), "Active control strategy for synchronization and anti-synchronization of a fractional chaotic financial system", *Physica A: Statistical Mechanics and its Applications*, Vol. 473 No. 1, pp. 262-275.

Li, C., Liao, X., Yang, X. and Huang, T. (2005), "Impulsive stabilization and synchronization of a class of chaotic delay systems", *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Vol. 15 No. 4, p. 043103.

Liu, X., Hong, L., Dang, H. and Yang, L. (2017), "Bifurcations and synchronization of the fractional-order Bloch system", *Discrete Dynamics in Nature and Society*, 10pp, available at: https://doi.org/10.1155/2017/4694305

Ma, T., Zhang, J., Zhou, Y. and Wang, H. (2015), "Adaptive hybrid projective synchronization of two coupled fractional-order complex networks with different sizes", *Neurocomputing*, Vol. 164 No. 1, pp. 182-189.

Magin, R., Feng, X. and Baleanu, D. (2009), "Solving the fractional order Bloch equation", *Concepts in Magnetic Resonance Part A*, Vol. 34 No. 1, pp. 16-23.

Nik, H.S., Saberi-Nadjafi, J., Effati, S. and Van Gorder, R.A. (2014), "Hybrid projective synchronization and control of the BaierSahle hyperchaotic flow in arbitrary dimensions with unknown parameters", *Applied Mathematics and Computation*, Vol. 248 No. 1, pp. 55-69.

Ott, E., Grebogi, C. and Yorke, J.A. (1990), "Controlling chaos", *Physical Review Letters*, Vol. 64 No. 11, pp. 1196-1199.

Ouannas, A., Azar, A.T., Ziar, T. and Radwan, A.G. (2017), "Generalized synchronization of different dimensional integer-order and fractional order chaotic systems", *Fractional Order Control and Synchronization of Chaotic Systems*, Springer International Publishing, Cham, pp. 671-697.

Richter, H. (2002), "Controlling chaotic systems with multiple strange attractors", *Physics Letters A*, Vol. 300 No. 2, pp. 182-188.

Rivest, R.L., Shamir, A. and Adleman, L. (1978), "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, Vol. 21 No. 2, pp. 120-126.

Rosenblum, M.G., Pikovsky, A.S. and Kurths, J. (1997), "From phase to lag synchronization in coupled chaotic oscillators", *Physical Review Letters*, Vol. 78 No. 22, pp. 4193-4196.

Shannon, C.E. (1948), "A mathematical theory of communication, Part I, Part II", *Bell System Technical Journal*, Vol. 27 No. 1, pp. 623-656.

Sun, J., Shen, Y., Wang, X. and Chen, J. (2014), "Finite-time combination-combination synchronization of four different chaotic systems with unknown parameters via sliding mode control", *Nonlinear Dynamics*, Vol. 76 No. 1, pp. 383-397.

Tirandaz, H. and Hajipour, A. (2017), "Adaptive synchronization and anti-synchronization of TSUCS and L unified chaotic systems with unknown parameters", *Optik-International Journal for Light and Electron Optics*, Vol. 130, pp. 543-549.

Tirandaz, H. and Karmi-Mollaee, A. (2017), "Modified function projective feedback control for time-delay chaotic Liu system synchronization and its application to secure image transmission", *Optik-International Journal for Light and Electron Optics*, Vol. 147 No. 1, pp. 187-196.

Wang, X. and Guo, K. (2014), "A new image alternate encryption algorithm based on chaotic map", *Nonlinear Dynamics*, Vol. 76 No. 4, pp. 1943-1950.

Wu, X., Bai, C. and Kan, H. (2014), "A new color image cryptosystem via hyperchaos synchronization", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 19 No. 6, pp. 1884-1897.

Wu, X., Wang, H. and Lu, H. (2012), "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.

Xi, H., Yu, S., Zhang, R. and Xu, L. (2014), "Adaptive impulsive synchronization for a class of fractional-order chaotic and hyperchaotic systems", *Optik-International Journal for Light and Electron Optics*, Vol. 125 No. 9, pp. 2036-2040.

Xu, Y., Wang, H., Li, Y. and Pei, B. (2014), "Image encryption based on synchronization of fractional chaotic systems", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 19 No. 10, pp. 3735-3744.

Yu, J., Chen, B., Yu, H. and Gao, J. (2011), “Adaptive fuzzy tracking control for the chaotic permanent magnet synchronous motor drive system via backstepping”, *Nonlinear Analysis: Real World Applications*, Vol. 12 No. 1, pp. 671-681.

Zhang, Y. and Wang, B. (2008), “Optical image encryption based on interference”, *Optics Letters*, Vol. 33 No. 21, pp. 2443-2445.

Further reading

Podlubny, I. (1998), *Fractional Differential Equations: An Introduction to Fractional Derivatives, Fractional Differential Equations, to Methods of their Solution and some of their Applications*, Vol. 198, Academic Press, San Diego, CA.

About the authors

Hamed Tirandaz received the BEng Degree in Applied Mathematics from the University of Sabzevar Tarbiat Moallem University, Sabzevar, Iran, in 2006, and PhD Degree in Mechatronics Engineering from Semnan University, Semnan, Iran, in 2009. He is been working as a Lecturer at Hakim Sabzevari University since 2010. His research interests include mainly Chaos control and synchronization. He has published several papers in the above mentioned area. Hamed Tirandaz is the corresponding author and can be contacted at: hamedtirandaz@gmail.com

Ali Karami-Mollaee received the BSc Degree in Electrical Engineering from Ferdowsi University in 2002 and MSc in Control Engineering from Tarbiyat Modares University in 2005 and PhD Degree in Control Engineering from Ferdowsi University in 2010. His research interests include nonlinear control, adaptive control and system identification. At Present he is a Assistant Professor in Hakim Sabzevari University, Iran.