EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Generalized function projective synchronization of chaotic systems for secure communication

Xiaohui Xu

Abstract

By using the generalized function projective synchronization (GFPS) method, in this paper, a new scheme for secure information transmission is proposed. The Liu system is employed to encrypt the information signal. In the transmitter, the original information signal is modulated into the system parameter of the chaotic systems. In the receiver, we assume that the parameter of receiver system is uncertain. Based on the Lyapunov stability theory, the controllers and corresponding parameter update rule are constructed to achieve GFPS between the transmitter and receiver system with uncertain parameters, and identify unknown parameters. The original information signal can be recovered successfully through some simple operations by the estimated parameter. Furthermore, by means of the proposed method, the original information signal can be extracted accurately in the presence of additional noise in communication channel. Numerical results have verified the effectiveness and feasibility of presented method.

Mathematics subject classification (2010)
68M10, 34C28, 93A30, 93C40

Keywords: Generalized function projective synchronization, Scaling function factor, Liu chaotic system, Secure communication, Parameter modulation

1 Introduction

Chaos is a kind of characteristics for nonlinear systems, which is a bounded unstable dynamic behavior that exhibits sensitive dependence on initial conditions and includes infinite unstable periodic motions. Since Pecora and Carroll [1] presented the conception of chaotic synchronization for two identical chaotic systems with different initial conditions, many synchronization methods have been proposed, such as complete synchronization (CS) [1], generalized synchronization [2], phase synchronization [3], impulse synchronization [4], lag synchronization [5], projective synchronization [6-8], etc. Amongst all kinds of chaos synchronization, projective synchronization, first reported by Mainieri and Rehacek [6], has been especially extensively studied because it can obtain faster communication with its proportional feature [9-12].

However, the above projective synchronization (PS) method is characterized that its drive and response systems are synchronized up to a constant scaling factor. Recently, Chen et al. [13] introduced a new PS scheme which is called function projective synchronization (FPS), where the responses of synchronized dynamical states can synchronize up to a scaling function factor. Let the scaling function be constant or unity, one can obtain PS or CS. So FPS is a more general definition of PS. Be-cause the unpredictability of the scaling function in FPS can additionally enhance security of communication, this feature could be applied to get more secure communication. More recently, many studies concentrate on FPS of chaotic systems and its application to secure communication [13-20]. For instance, FPS of two identical or different chaotic systems was studied in [13,14,16,18]. In [15,20], another new synchronization phenomenon, generalized function projective synchronization (GFPS), was proposed, in which drive and response systems could be synchronized to a scaling function matrix. In [20], Yu and Li investigated GFPS of two entirely different systems with fully unknown

Correspondence: xhxucn@gmail.com
Department of Computer Science and Engineering, Shanghai Jiao Tong University No.800 Dongchuan Road, Minhang District, Shanghai 200240, China

parameters. Du et al. [15] studied GFPS in coupled chaotic systems and its application in secure communication.

In the past decades, the use of chaotic signals for information transmission attracts great attention of modern scientists from various fields [16,17,20-26]. Different approaches for transmission of information signals using chaotic dynamics have been proposed, such as chaotic masking, chaotic modulation, nonlinear mixing, chaotic switching, and others. In a typical chaotic synchronization communication scheme, the information to be transmitted is carried from the transmitter to the receiver by a chaotic signal through an analog channel. In the receiver, chaos synchronization is employed to recover the information signal. In many existing secure communication methods, the information signal is directly added to input of chaotic systems. The magnitude of transmitted signals is required to be sufficiently small, otherwise it may lead to the instability of whole system. On the other hand, although these communication methods have been successfully demonstrated in simulations, performance of communication schemes were usually quantified by assuming the identical chaos synchronization based on exact knowledge of the system parameters [27,28], which may impose some limitations to applicability of these techniques. But in real situation, some or all of parameters are unknown and the noise exists. The effect of these uncertainties and noise will destroy the synchronization and even break it. As a result, one cannot extract the original information in the receiver. Therefore, it is essential to study secure communication in the presence of unknown parameters and noise.

Motivated by the above discussions, this paper proposes a new secure communication scheme based on GFPS of uncertain Liu chaotic system and parameter modulation. In the transmitter, the original information signal is firstly transformed by an invertible function. Then the processed signal is modulated into the parameter of Liu system. The resulting system is still chaotic. In our method, no constraint is imposed on the magnitude of the original information signal. Suppose the parameter of the receiver system is unknown. Based on the Lyapunov stability theory, we design the controllers and the parameter update rule to realize GFPS of uncertain Liu chaotic systems and identify the unknown parameter of the receiver system. Then the information signal in the receiver can be recovered by the estimated parameter. Moreover, it is worth noting that secure communication using GFPS can still be realized fast even if the transmission channel is perturbed by additive noise.

The rest of this paper is organized as follows. In Section 2, Liu system is described briefly and the definition of GFPS is presented. Section 3 gives the chaotic secure communication scheme using GFPS and parameter modulation. By means of the Lyapunov stability theory and adaptive control, the controllers and corresponding parameter update rule are designed to ensure GFPS between two identical Liu chaotic systems with uncertain parameters. Simulation experiments of the proposed secure communication system have been performed in Section 4. The conclusions are finally drawn in Section 5.

2 System description and the definition of GFPS

2.1 The Liu system

In 1963, Lorenz [29] found the first classical chaotic attractor in a three-dimensional autonomous system derived form a simplified model of earth atmospheric convection system. As the first chaotic model, the Lorenz system has become a paradigm of chaos research. Mathematicians, physicists and engineers from various fields have thoroughly studied the essence of chaos, characteristics of chaotic systems, bifurcations, routes to chaos, and many other related topics. There are also some chaotic systems of great significance that are closely related to the Lorenz system but not topologically equivalent to it, such as the Rössler system [30], the Chen system [31] and the Lü system [32]. Recently, Liu et al. [33] proposed a system of three-dimensional autonomous differential equations with only two quadratic terms, which is described as follows:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - xz \\ \dot{z} = -cz + 4x^2 \end{cases} \tag{1}$$

where $(x, y, z) \in R^3$ are state variables, $(a, b, c) \in R^3$ are all positive real parameters and c varies in a certain range. In the Liu system, when the parameter c varies in a big range, the resulting system can still be chaotic and have more abundant and complex behaviors than the original Liu system. And compared to other parameters, the parameter c is more suitable to be used in parameter modulation. Figure 1 displays the Lyapunov exponents spectrum of system (1) with $a = 10$, $b = 40$ and $c \in [0,8]$. Obviously, when $c \in [0.5, 8]$, system (1) is always chaotic. The chaotic attractors of Liu system with different c are shown in Figure 2.

The Liu system has a butterfly-shaped attractor similar to the Lorenz attractor but not equivalent. The existing studies have shown that the Liu system is equivalent to Shimizu-Morioka system and is a representative example of chaotic attractors. Compared to other chaotic systems, when the system parameters of Liu system vary in a certain range, this chaotic system can still be chaotic, further the dynamical behaviors of this system become

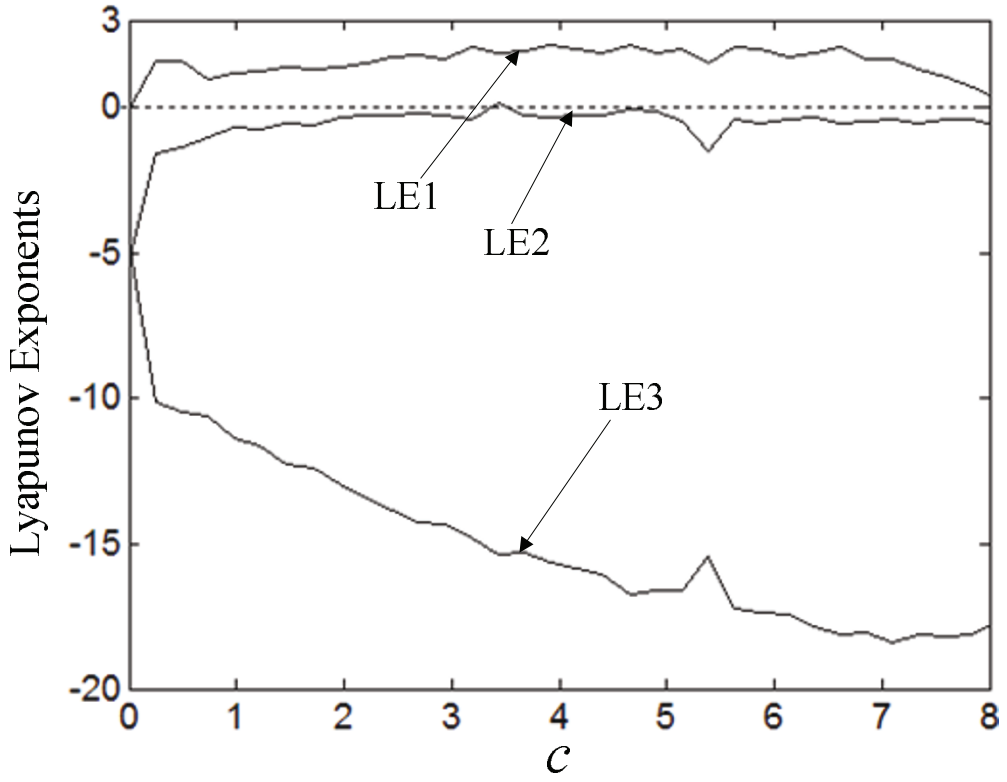

Figure 1 The Lyapunov exponents spectrum of Liu system (1) with $a = 10$, $b = 40$ and $c \in [0, 8]$.

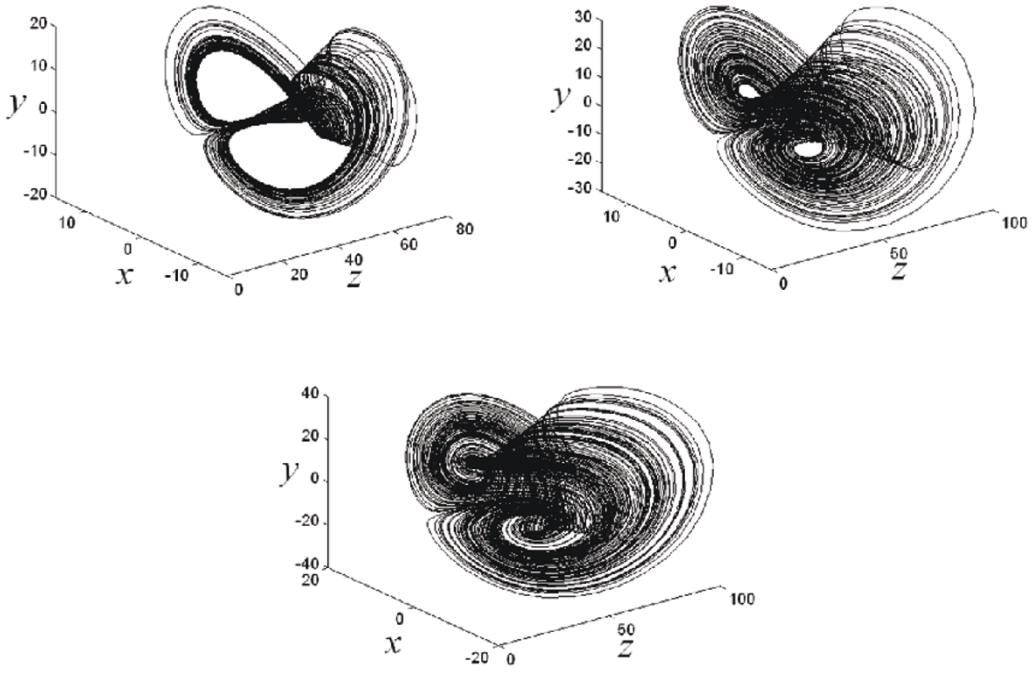

Figure 2 The Chaotic attractors of Liu system (1) with different c.

more abundant and complex. Therefore, it is possible to modulate information signal into the parameter of chaotic systems to realize chaotic secure communication.

Remark 1 It is found that many chaotic systems can maintain chaotic behavior when a system parameter continuously changes in a certain range. We can obtain a "new" system parameter by modulating the information signal into the parameter of chaotic systems. If the "new" system parameter can ensure the corresponding system still be chaotic, the detector cannot extract the information signal from the signals, and transmitted in the channel. So it is possible to modulate the information signal into the parameter of chaotic systems to realize chaotic secure communication.

2.2 The definition of GFPS

The drive system and the response system are defined as follows:

$$\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}) \tag{2}$$

$$\dot{\boldsymbol{y}}(t) = g(\boldsymbol{y}) + U(\boldsymbol{x}, \boldsymbol{Y}) \tag{3}$$

where $\boldsymbol{x} = (x_1, x_2, ..., x_n) \in R^n$, $\boldsymbol{y} = (y_1, y_2, ..., y_n) \in R^n$ are the state vectors; $f, g : R^n \to R^n$ are differentiable functions; $U(x, y)$ is a controller to be designed. Let us define the error vector as

$$\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{\Lambda x} \tag{4}$$

where $\boldsymbol{e} = (e_1, e_2, ..., e_n)^T$, and $\boldsymbol{\Lambda} = \text{diag}(\varphi_1(t), \varphi_2 t, ..., \varphi_n(t))$ is reversible and differentiable, where $\varphi_i(t)$: $R^n \to R(\neq 0)$ is a continuously differentiable functions with bounded.

Definition 1 (**GFPS**) *For the drive system (2) and the response system (3), it is said that system (2) and (3) are GFPS, if there exists a scaling function matrix* Λ *such that* $\lim_{t\to\infty} ||\boldsymbol{e}|| = 0$.

Remark 2 We call Λ a scaling function matrix and $\varphi_i(t)$ a scaling function factor, respectively. It is easy to see that if $\varphi_1(t) = \varphi_2(t) = ... = \varphi_n(t)$, GFPS is simplified to FPS. If $\varphi_i = a_i (i = 1, 2, ..., n)$ where $a_i \in R$ and $a_i \neq 0$, GPS will occur. If $\Lambda = \lambda I$ where $\lambda \in R$ is a constant and I_n is an $n \times n$ identity matrix, GFPS is reduced to PS. In particular, if $\varphi_i(t) = 1$ or $\varphi_i(t) = -1$, the problem further becomes standard CS or anti-synchronization (AS).

3 Secure communication based on GFPS and parameter modulation

3.1 The chaotic secure communication scheme using GFPS and parameter modulation

The secure communication system involves the development of a signal that contains the information which is to remain undetectable by others within a carrier signal. We can ensure the security of this information by inserting it into a chaotic signal which is transmitted to a prescribed receiver that would be able to detect and recover the information from the chaotic signal.

In the present application, we propose a new chaotic secure communication scheme using GFPS of uncertain Liu chaotic system and parameter modulation, as shown in Figure 3. The system consists of a transmitter module, a communication channel and a receiver module. In this scheme, the chaotic signal is generated by using Liu chaotic system which was described by the system model of differential equation (1). For convenience, the chaotic system is written as the following form:

$$\dot{\boldsymbol{X}} = F(\boldsymbol{X}) \tag{5}$$

where the state vector $\boldsymbol{X} = (x, y, z)$.

The transmitter module is composed of a chaotic system $\boldsymbol{S}_1$ and an invertible transformation function ϕ. The "new" parameter β is formulated as a function of the original information signal $f(t)$, i.e., $\beta = \phi(f(t))$, which

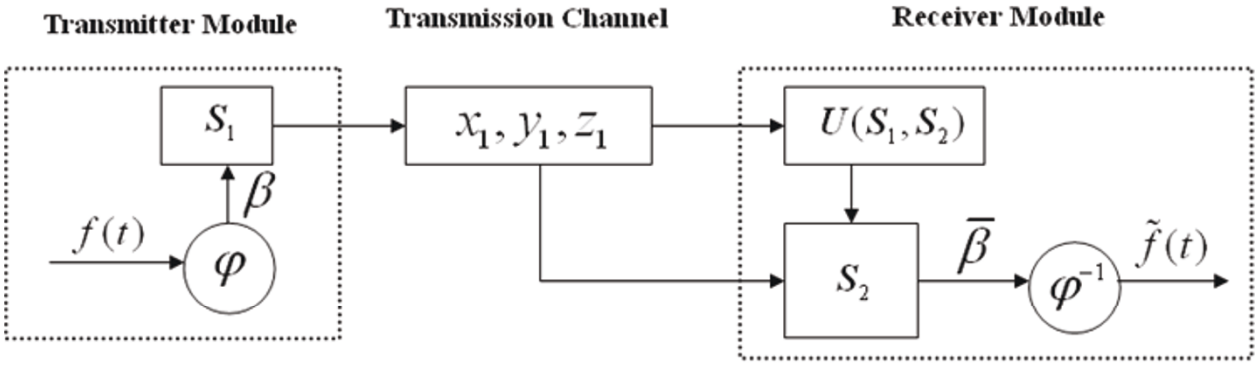

Figure 3 Block diagram of the proposed secure communication scheme.

meets the need of the parameter range of c. So the resulting system still exhibits a chaotic behavior. In our method, the following two cases: no circumstance noise and additive noise in the transmission channel will be considered. The receiver module consists of another chaotic system $\boldsymbol{S}_2$, the controller $\boldsymbol{U}(\boldsymbol{S}_1, \boldsymbol{S}_2)$ and the corresponding inverse function ϕ^{-1}. Assume that the parameter $\bar{\beta}$ of the receiver system $\boldsymbol{S}_2$ is uncertain. In the receiver, with the help of controller $\boldsymbol{U}(\boldsymbol{S}_1, \boldsymbol{S}_2)$, GFPS between systems $\boldsymbol{S}_1$ and $\boldsymbol{S}_2$ can be realized. The unknown parameter $\bar{\beta}$ can be asymptotically identified as GFPS appears. Then the original in-formation can be recovered through some simple operations by the function ϕ^{-1} and the estimated parameter $\bar{\beta}$, i.e., $\tilde{f}(t) = \varphi^{-1}(\bar{\beta})$.

3.2 GFPS of uncertain Liu chaotic system

As we all know, the information signal is often bounded; in other words, the information signal $f(t)$ satisfies

$$m \le f(t) \le M \tag{6}$$

where m and M are known constants.

For the Liu system, we will employ the parameter to transmit the information signal. Define a "new" parameter β as follows:

$$\beta = \frac{f(t) - m}{M - m} + \theta, \quad \theta \in [0.5, 7] \tag{7}$$

Obviously, the "new" parameter satisfies $\beta \in [0.5, 8]$. According to the above description of Liu system, we know the following system

$$\begin{cases} \dot{x}_1 = 10(y_1 - x_1) \\ \dot{y}_1 = 40x_1 - x_1 z_1 \\ \dot{z}_1 = -\beta z_1 + 4x_1^2 \end{cases} \tag{8}$$

will still be chaotic, which has more abundant dynamic behavior. Since the resulting system (8) is chaotic, it is hard to detect information signal from the signals transmit-ted in the channel.

We take the system given by Equation (8) as the transmitter system and the receiver system is constructed as follows:

$$\begin{cases} \dot{x}_2 = 10(y_2 - x_2) + u_1 \\ \dot{y}_2 = 40x_2 - x_2 z_2 + u_2 \\ \dot{z}_2 = -\beta z_2 + 4x_2^2 + u_3 \end{cases} \tag{9}$$

where $u_i(t)$ $(i = 1, 2, 3)$ are controllers to be designed, $\bar{\beta}$ is unknown parameter of receiver system which needs to be estimated.

Define the GFPS error variables as

$$\begin{cases} e_1 = x_2 - \phi_1(t)x_1 \\ e_2 = y_2 - \phi_2(t)y_1 \\ e_3 = z_2 - \phi_3(t)z_1 \end{cases} \tag{10}$$

and denote the parameter estimate error as

$$e_\beta = \bar{\beta} - \beta \tag{11}$$

The time derivative of the error variables (10) and (11) is:

$$\begin{cases} \dot{e}_1 = \dot{x}_2 - \phi_1(t)\dot{x}_1 - \dot{\phi}_1(t)x_1 \\ \dot{e}_2 = \dot{y}_2 - \phi_2(t)\dot{y}_1 - \dot{\phi}_2(t)y_1 \\ \dot{e}_3 = \dot{z}_2 - \phi_3(t)\dot{z}_1 - \dot{\phi}_3(t)z_1 \\ \dot{e}_\beta = \dot{\bar{\beta}} - \dot{\beta} \end{cases} \tag{12}$$

Subtracting Equation (8) from Equation (9) yields the following error dynamical system:

$$\begin{cases} \dot{e}_1 = 10(y_2 - x_2) - 10\phi_1(t)(y_1 - x_1) - \dot{\phi}_1(t)x_1 + u_1 \\ \dot{e}_2 = 40x_2 - x_2 z_2 - 40\phi_2(t)x_1 + \phi_2(t)x_1 z_1 - \dot{\phi}_2(t)y_1 + u_2 \\ \dot{e}_3 = -\bar{\beta} z_2 + 4x_2^2 + \phi_3(t)\beta z_1 - 4\phi_3(t)x_1^2 - \dot{\phi}_3(t)z_1 + u_3 \\ \dot{e}_\beta = \dot{\bar{\beta}} - \dot{f}(t)/(M - m) \end{cases} \tag{13}$$

Our aim is to find appropriate controllers $u_i(t)$ $(i = 1, 2, 3)$ for stabilizing error variables at the origin, i.e., $\lim_{t\to\infty} ||\boldsymbol{e}|| = 0$ and $\lim_{t\to\infty} e_\beta = 0$ where $\boldsymbol{e} = (e_1, e_2, e_3)^T$. That is, GFPS between the transmitter system (8) and the receiver system (9) are globally achieved and the uncertain parameter can be identified asymptotically. To this end, we design controllers as follows:

$$\begin{cases} u_1 = -10(\phi_2(t) - \phi_1(t))y_1 + \dot{\phi}_1(t)x_1 \\ u_2 = -e_2 - 50e_1 + 40(\phi_2(t) - \phi_1(t))x_1 + x_2 z_2 - \phi_2(t)x_1 z_1 + \dot{\phi}_2(t)y_1 \\ u_3 = -4x_2^2 + 4\phi_3(t)x_1^2 + \dot{\phi}_3(t)z_1 \end{cases} \tag{14}$$

and the update rule for unknown parameter as below

$$\dot{\bar{\beta}} = z_2 e_3 + \dot{f}(t)/(M - m) \tag{15}$$

Then we have the following main theorem.

Theorem 1 *For given nonzero scaling functions $\varphi_i(t)(i = 1, 2, 3)$, GFPS between the transmitter system (8) and the receiver system (9) can occur by the controllers (14) and the parameter update rule (15). It implies that the GFPS errors satisfy* $\lim_{t\to\infty} e_i(t) = 0$. *The uncertain parameter is well estimated from the system parameter in the sense of* $\lim_{t\to\infty}(\bar{\beta} - \beta) = 0$.

Proof We choose the following Lyapunov function for the error system (13):

$$V(t) = (e_1^2 + e_2^2 + e_3^2 + e_\beta^2)/2 \tag{16}$$

Taking the time derivative of $V(t)$ along the trajectories of the error system (13) yields

$$\begin{aligned}\dot{V}(t) &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + e_\beta\dot{e}_\beta \\ &= e_1[-10e_1 + 10e_2 + 10(\phi_2(t) - \phi_1(t))\gamma_1 - \dot{\phi}_1(t)x_1 + u_1] \\ &+ e_2[40e_1 - 40(\phi_2(t) - \phi_1(t))x_1 - x_2z_2 + \phi_2(t)x_1z_1 - \dot{\phi}_2(t)\gamma_1 + u_2] \\ &+ e_3[-\beta e_3 - e_\beta z_2 + 4x_2^2 - 4\phi_3(t)x_1^2 + x_2\gamma_2 - \phi_3(t)x_1\gamma_1 - \dot{\phi}_3(t)z_1 + u_3] \\ &+ e_\beta[\dot{\bar{\beta}} - \dot{\tilde{f}}(t)/(M-m)]\end{aligned} \quad (17)$$

Substituting Equations (14) and (15) into Equation (17), one can obtain

$$\begin{aligned}\dot{V}(t) &= e_1(-10e_1 + 10e_2) + e_2(-e_2 - 10e_1) + e_3(-\beta e_3 - e_\beta z_2) + e_\beta(\dot{\bar{\beta}} - \dot{\beta}) \\ &= -10e_1^2 - e_2^2 - \beta e_3^2 \\ &= -e^TQe\end{aligned}$$

where Q = diag(10, 1, β) and $\beta \in$ [0.5, 8]. Clearly, Q is a positive definite matrix and $\dot{V}(t)$ is negative definite. Based on the Lyapunov stability theory, the error dynamical system (13) is globally and asymptotically stable at the origin, and we have $e_\beta \to 0$, as $t \to \infty$. Hence GFPS between the transmitter system (8) and the receiver system (9) is achieved and the uncertain parameter is also identified in the receiver end simultaneously under the controllers (14) and the parameter update rule (15). The proof is completed.

When GFPS between the transmitter system and the receiver system appear, ac-cording to Theorem 1, the uncertain parameter $\bar{\beta}$ can be estimated asymptotically, i.e., $\bar{\beta} \to \beta$. So the original information signal can be recovered in the receiver as

$$\tilde{f}(t) = (M-m)(\bar{\beta} - \theta) + m \quad (18)$$

where $\tilde{f}(t)$ denotes the recovered signal. Thus we have

$$\tilde{f}(t) = (M-m)(\bar{\beta} - \theta) + m \to (M-m)(\beta - \theta) + m = f(t) \text{as} t \to \infty$$

which implies that the original information signal can be recovered successfully in the receiver end.

Remark 3 In practical situations, if the information signal to be transmitted is too large, it will result in a chaotic system to be asymptotically stable or emanative. In this case, one may fail to extract the information signal. In the presented method, no constraint is imposed on the information signal. The original information signal is firstly transformed by an invertible function. Then the transformed signal is used as the parameter of Liu system. The resulting system exhibits more abundant chaotic behavior. The interceptor cannot extract the information from the transmitted signals in the channel.

4 Simulation results

To verify and demonstrate the effectiveness of the proposed chaotic secure communication scheme, some numerical examples are performed in this section. In the simulations, the ODE45 algorithm is applied to solve the differential systems. The initial states of the transmitter system (8) and the receiver system (9) are arbitrarily taken as $x_1(0)$, $y_1(0)$, $z_1(0)$ = (2, 1, - 1) and (x_2 (0), $y_2(0)$, $z_2(0)$) = (-3, -2, 4), respectively. The initial values of the unknown parameter is chosen arbitrarily as $\bar{\beta}(0) = 0.01$.

4.1 Secure communication without circumstance noise

In this section, we focus on considering the case of no circumstance noise in the transmission channel. We choose the original information signal as $f(t)$ = 1.5 + 2.5 sin(2t). The scaling functions are selected arbitrarily as $\varphi_1(t)$ = 0.5 sin t+2, $\varphi_2(t)$ = 3 cos(2 * t) - 1 and $\varphi_3(t)$ = - 1.5. It is obvious that -1 ≤ $f(t)$ ≤ 4. Let θ = 2, by Equation (7), we obtain the "new" parameter as β = 0.5 sin (2t) + 2.5. Clearly, $\beta \in$ [2,3]. Therefore, the resulting system (8) is still chaotic, as depicted in Figure 4. So one cannot extract the information signal from the transmitted signals x_1, y_1 and z_1. The simulation results of the proposed secure communication scheme using GFPS between systems (8) and (9) by the controllers (14) and the parameter update rule (15) are shown in Figure 5. Figure 5 plots the original information signal f (t). Figure 5 displays the time evolution of the GFPS errors, which shows that the time response of the GFPS errors $e_i(t)(i$ = 1, 2, 3) converge to zero after t > 0.4. The recovered signal $\tilde{f}(t)$ is shown in Figure 5 and and the error signal between the original information signal and the recovered one is plotted in Figure 5. From Figure 5, one can easily see that the original information signal $f(t)$ is recovered accurately after t > 0.4.

The information signal $f(t)$ and the scaling functions $\varphi_i(t)$ are chosen as those above. Set θ = 4. Then the "new" parameter β = 0.5 sin(2t) + 4.5. Obviously, $\beta \in$ [4,5]. Figure 6 displays that the resulting system (8) exhibits chaotic behavior. The numerical results of the proposed secure communication scheme are illustrated in Figure 7. Figure 7 shows that the synchronization errors $e_i(t)$ have been stabilized at the origin after t > 0.25, which implies that GFPS between the transmitter system (8) and the receiver system (9) is achieved. The original information signal and the recovered one are depicted in Figure 7. Figure 7 displays the error signal between the original information signal and the recovered one, from which it is found that the original information signal $f(t)$ can be extracted exactly after t > 0.25. Figure 8 describes the logarithm of the absolute value of the error signal when β = 0.5 sin(2t) + 2.5 and β = 0.5 sin(2t) + 4.5, respectively. From Figure 8, we find that the synchronization rate when β = 0.5 sin(2t) + 4.5 is faster than that when β = 0.5 sin(2t) + 2.5, and

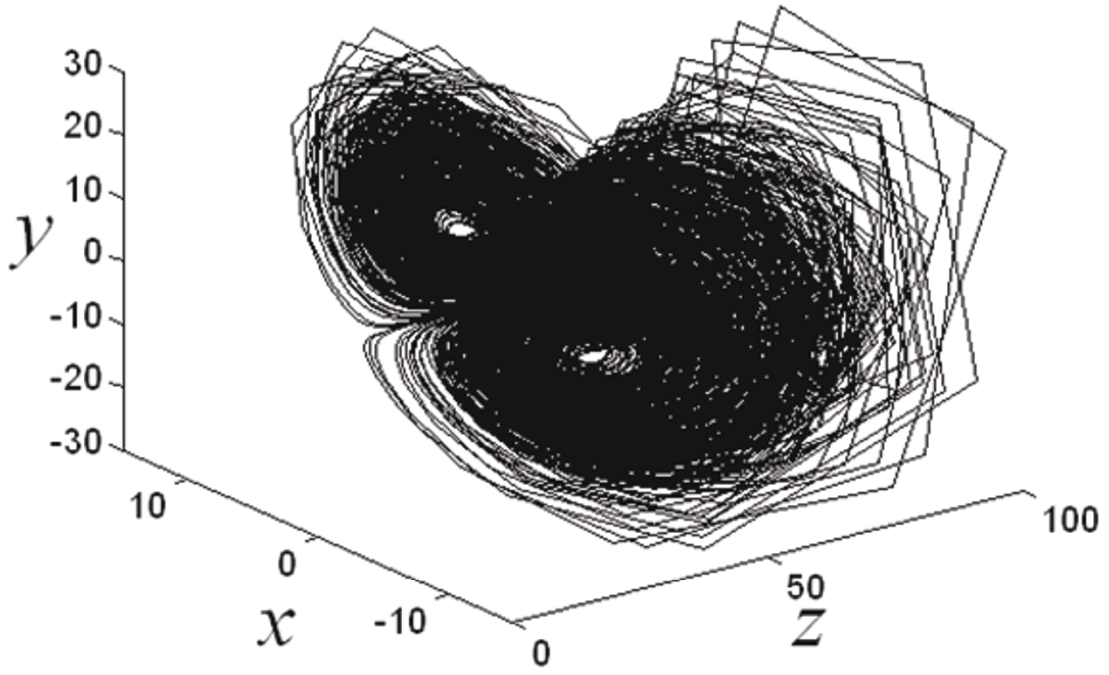

Figure 4 The chaotic attractors of the resulting system (8) with $\beta = 0.5 \sin t + 2.5$.

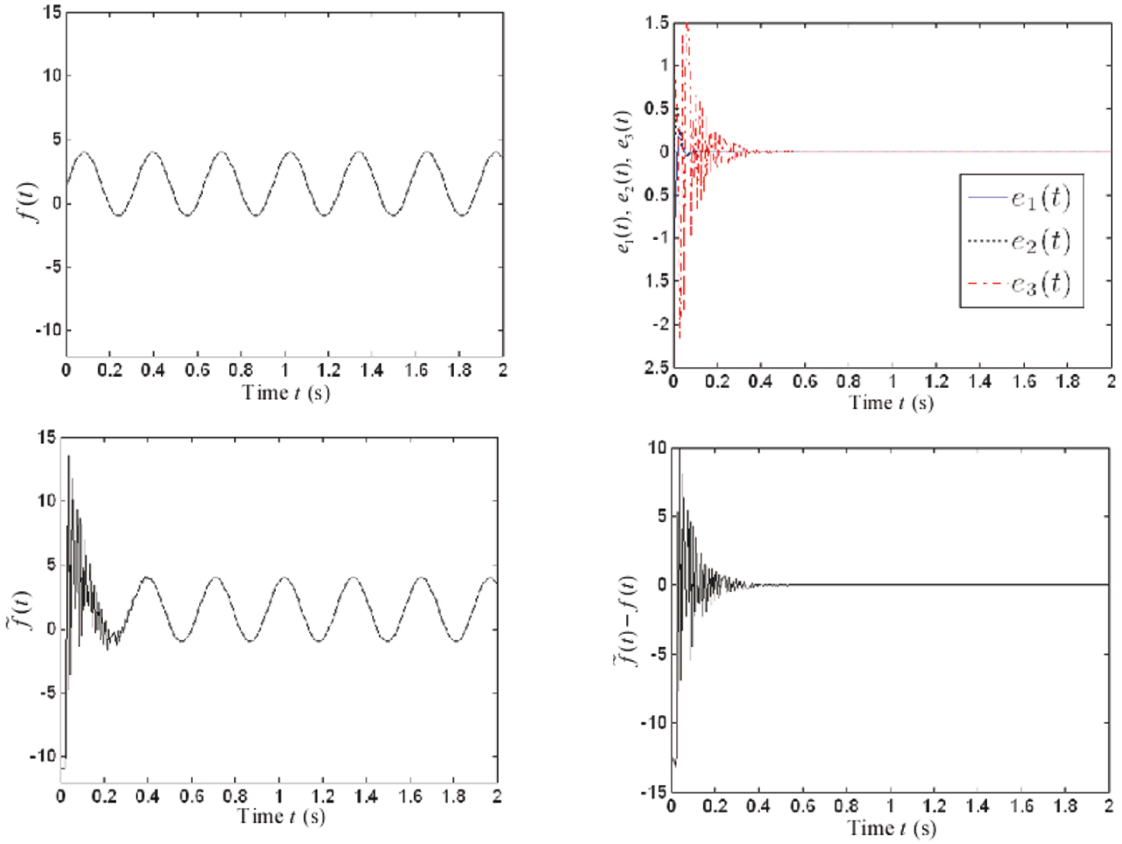

Figure 5 Simulation results of the proposed secure communication scheme using GFPS with $\beta = 0.5 \sin t + 2.5$.

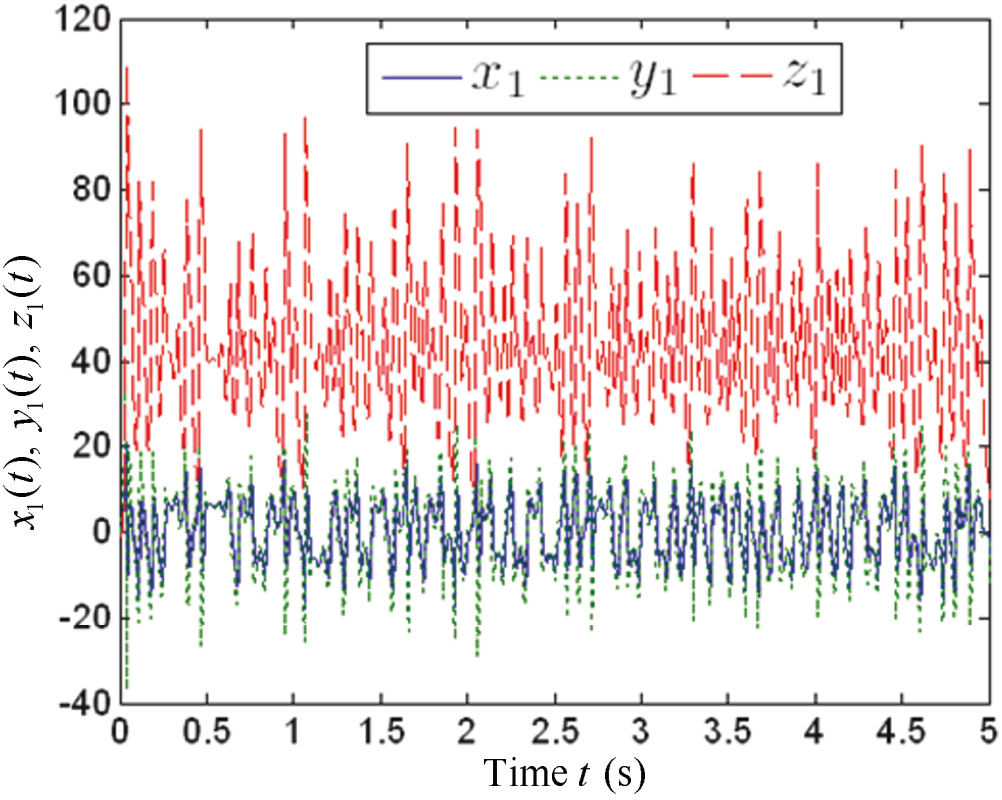

Figure 6 The state trajectories of the resulting system (8) with $\beta = 0.5 \sin t + 4.5$.

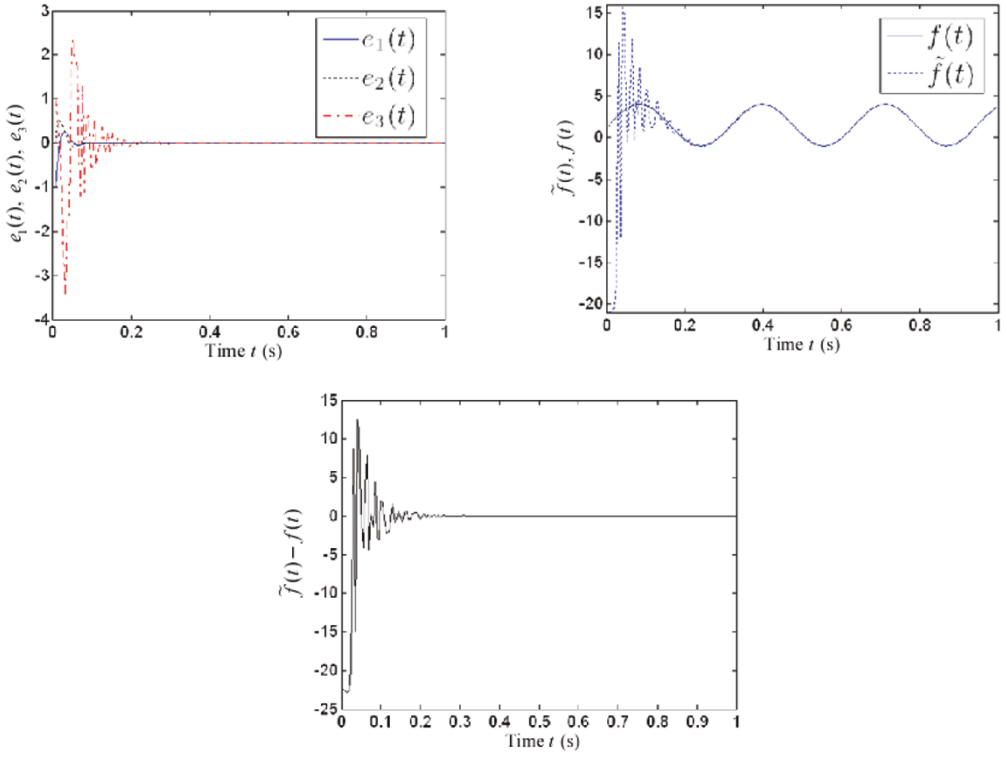

Figure 7 Simulation results of the proposed secure communication scheme using GFPS with $\beta = 0.5 \sin t + 4.5$.

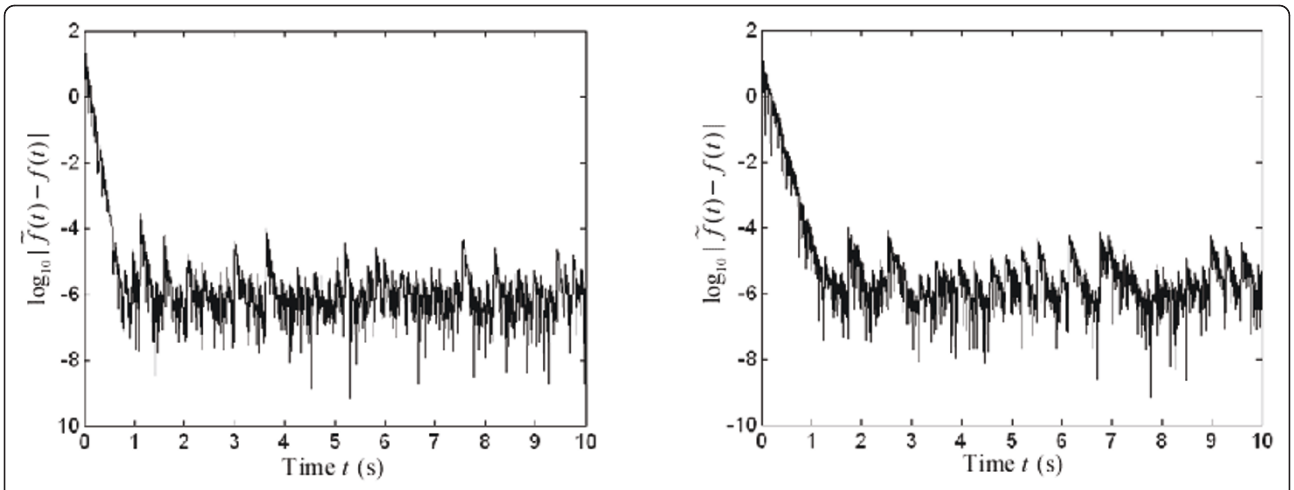

Figure 8 The error signal $\log_{10}|\tilde{f}(t)-f(t)|$.

the recovered signal when $\beta = 0.5\sin(2t) + 4.5$ is more accurate than that when $\beta = 0.5\sin(2t) + 2.5$.

Similarly, we have also tested the proposed secure communication scheme for other values of θ. Limited to the length of this paper, we omit these results here. Numeric evidence shows that the larger the value of θ, the faster to achieve GFPS, and the more accurate the recovered signal is.

4.2 Secure communication with additive noise

Here, we will study the proposed chaotic secure communication scheme when there exists additive noise in the channel. Suppose the additive noise $N(t)$ = (0.01 sin(10t), 0.02 sin(20t), 0.03 sin(30t)). Choose the information signal as $f(t) = 4\cos(0.5t) - 3$. The scaling functions are selected randomly as $\varphi_1(t) = 1 + e^{-t}$, $\varphi_2(t) = 2.5 + 3\sin(0.5 * t)$ and $\varphi_3(t) = 1.2 + 0.3\cos(10t)$. Take $\theta = 3$. Thus the "new" parameter $\beta = 0.5\cos(0.5t) + 3.5$ and $\beta \in [3,4]$. So the resulting system (8) is still chaotic, as depicted in Figure 9. The simulation results of the proposed chaotic secure communication scheme with additive noise are displayed in Figure 10. The synchronization errors e_1, e_2 and e_3 are shown in Figure 10, from which we can see that the required synchronization has been achieved quickly with our designed controllers (14) and the parameter update rule (15). The information signal $f(t)$ and the recovered one $\tilde{f}(t)$ are displayed in Figure 10. Figure 10 plots the error signal between the original information signal and the recovered one. From Figure 10, it is easy to see that the information signal $f(t)$ is recovered accurately after a very short transient.

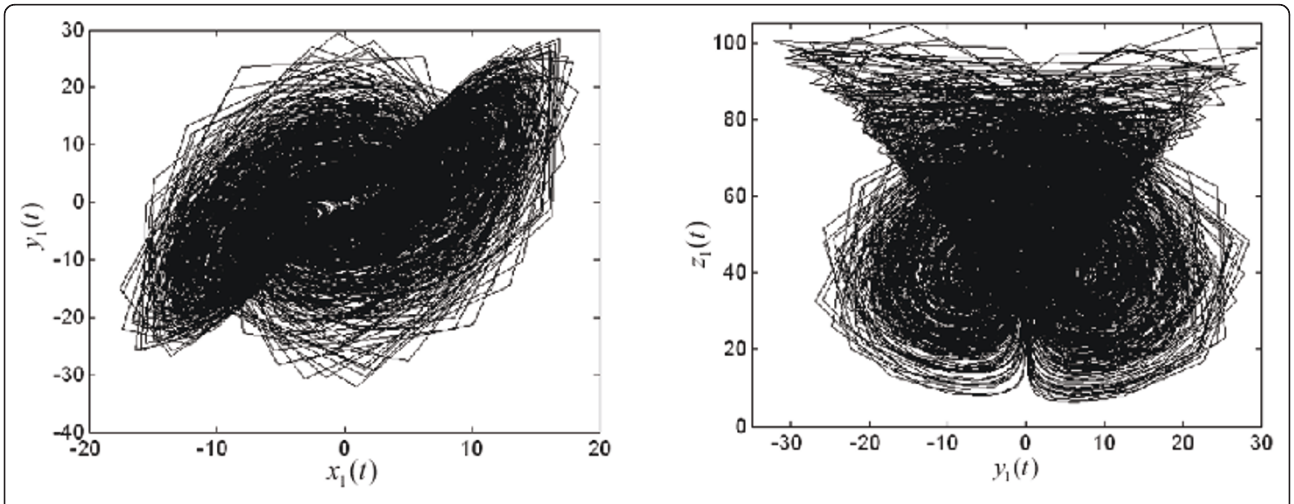

Figure 9 Phase diagrams of the resulting system (8) in the plane.

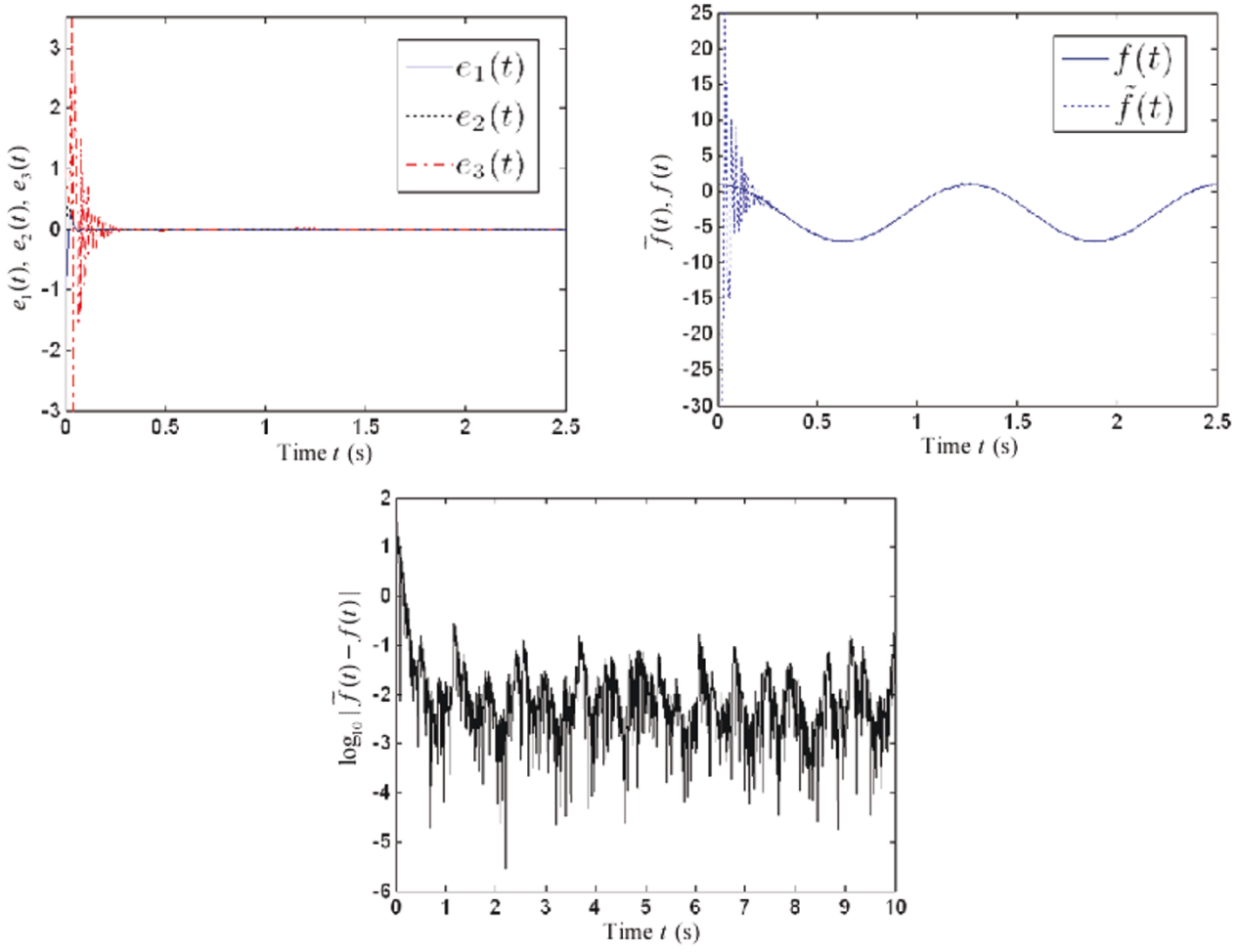

Figure 10 Simulation results of the proposed secure communication scheme using GFPS with additive noise.

5 Conclusions

In this paper, a novel chaotic secure communication scheme based on GFPS and parameter modulation is proposed. In the transmitter end, the original information signal is modulated into the parameter of the chaotic system and the resulting system still chaotic. There is no constraint posed on the original information signal. In the receiver, we assume that the parameter of the receiver system is uncertain. On the basis of the Lyapunov stability theory, the controllers and corresponding parameter update rule are devised to make the states of two identical Liu chaotic systems with unknown parameter synchronized. Simultaneously the uncertain parameter of the receiver system is also identified. Furthermore, the information signal can also be recovered accurately and fast by applying our secure communication method when additive noise exists in the transmission channel. Numerical simulations show the effectiveness and feasibility of the proposed chaotic secure communication scheme based on GFPS and parameter modulation.

Acknowledgements

We would like to thank Prof. Linpeng Huang and Dr. Xiangjun Wu for their valuable suggestions and discussion. In addition, we would like to thank the anonymous reviewers who have helped to improve the paper. This paper is partially supported by the National Natural Science Foundation of China (NSFC) under Grant No.60673116, 60970010, the National Grand Fundamental Research 973 Program of China under Grant No.2009CB320705, and the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant No.20090073110026.

Received: 17 January 2011 Accepted: 27 June 2011
Published: 27 June 2011

References

1. LM Pecora, TL Carroll, Synchronization in chaotic systems. Phys Rev Lett. **64**(8), 821–824 (1990). doi:10.1103/PhysRevLett.64.821
2. Z Ge, C Chang, Generalized synchronization of chaotic systems by pure error dynamics and elaborate Lyapunov function. Nonlinear Anal Theory Methods Appl. **71**(11), 5301–5312 (2009). doi:10.1016/j.na.2009.04.020

3. FA Breve, L Zhao, MG Quiles, EEN Macau, Chaotic phase synchronization and desynchronization in an oscillator network for object selection. Neural Netw. **22**(5–6), 728–737 (2009). doi:10.1016/j.neunet.2009.06.027
4. Q Ren, J Zhao, Impulsive synchronization of coupled chaotic systems via adaptive-feedback approach. Phys Lett A. **355**(4–5), 342–347 (2006). doi:10.1016/j.physleta.2006.02.053
5. C Li, X Liao, K Wong, Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication. Physica D Nonlinear Phenom. **194**(3–4), 187–202 (2004). doi:10.1016/j.physd.2004.02.005
6. R Mainieri, J Rehacek, Projective synchronization in three-dimensional chaotic systems. Phys Rev Lett. **82**(15), 3042–3045 (1999). doi:10.1103/PhysRevLett.82.3042
7. D Xu, Control of projective synchronization in chaotic systems. Phys Rev E. **63**, 27201–27204 (2001)
8. D Xu, CY Chee, Controlling the ultimate state of projective synchronization in chaotic systems of arbitrary dimension. Phys Rev E. **66**(4), 046218–046222 (2002)
9. CY Chee, D Xu, Secure digital communication using controlled projective synchronization of chaos. Chaos Soliton Fract. **23**(3), 1063–1070 (2005)
10. J Chen, L Jiao, J Wu, X Wang, Projective synchronization with different scale factors in a driven-response complex network and its application in image encryption. Nonlinear Anal Real World Appl. **11**(4), 3045–3058 (2010). doi:10.1016/j.nonrwa.2009.11.003
11. TM Hoang, M Nakagawa, A secure communication system using projective-lag and/or projectiveanticipating synchronizations of coupled multidelay feedback systems. Chaos Soliton Fract. **38**(5), 1423–1438 (2008). doi:10.1016/j.chaos.2008.02.008
12. Z Li, D Xu, A secure communication scheme using projective chaos synchronization. Chaos Soliton Fract. **22**(2), 477–481 (2004). doi:10.1016/j.chaos.2004.02.019
13. Y Chen, X Li, Function projective synchronization between two identical chaotic systems. Int J Mod Phys C. **18**(5), 883–888 (2007). doi:10.1142/S0129183107010607
14. H Du, Q Zeng, C Wang, Function projective synchronization of different chaotic systems with uncertain parameters. Phys Lett A. **372**(33), 5402–5410 (2008). doi:10.1016/j.physleta.2008.06.036
15. H Du, Q Zeng, C Wang, Modified function projective synchronization of chaotic system. Chaos Soliton Fract. **42**(4), 2399–2404 (2009). doi:10.1016/j.chaos.2009.03.120
16. H Du, Q Zeng, C Wang, M Ling, Function projective synchronization in coupled chaotic systems. Nonlinear Anal Real World Appl. **11**(2), 705–712 (2010). doi:10.1016/j.nonrwa.2009.01.016
17. H Du, Q Zeng, N Lü, A general method for modified function projective lag synchronization in chaotic systems. Phys Lett A. **374**(13-14), 1493–1496 (2010). doi:10.1016/j.physleta.2010.01.058
18. R Luo, Adaptive function projective synchronization of Rösler hyperchaotic system with uncertain parameters. Phys Lett A. **372**(20), 3667–3671 (2008). doi:10.1016/j.physleta.2008.02.035
19. KS Sudheer, M Sabir, Adaptive function projective synchronization of two-cell Quantum-CNN chaotic oscillators with uncertain parameters. Phys Lett A. **373**(21), 1847–1851 (2009). doi:10.1016/j.physleta.2009.03.052
20. Y Yu, H Li, Adaptive generalized function projective synchronization of uncertain chaotic systems. Nonlinear Anal Real World Appl. **11**(4), 2456–2464 (2010). doi:10.1016/j.nonrwa.2009.08.002
21. G Chen, X Dong, *From Chaos to Order: Methodologies, Perspectives and Applications*. (World Scientific, Singapore, 1998)
22. L Kocarev, U Parlitz, General approach for chaotic synchronization with applications to communication. Phys Rev Lett. **74**(25), 5028–5031 (1995). doi:10.1103/PhysRevLett.74.5028
23. J-S Lin, C-F Huang, T-L Liao, J-J Yan, Design and implementation of digital secure communication based on synchronized chaotic systems. Digital Signal Process. **20**(1), 229–237 (2010). doi:10.1016/j.dsp.2009.04.006
24. OI Moskalenko, AA Koronovskii, AE Hramov, Generalized synchronization of chaos for secure communication: remarkable stability to noise. Phys Lett A. **374**(29), 2925–2931 (2010). doi:10.1016/j.physleta.2010.05.024
25. X Wu, A new chaotic communication scheme based on adaptive synchronization. Chaos: An Inter-disciplinary J Nonlinear Sci. **16**(4), 043118 (2006). doi:10.1063/1.2401058
26. F Zhu, Observer-based synchronization of uncertain chaotic system and its application to secure communications. Chaos Soliton Fract. **40**(5), 2384–2391 (2009). doi:10.1016/j.chaos.2007.10.052
27. B Andrievsky, Adaptive synchronization methods for signal transmission on chaotic carriers. Math Comput Simul. **58**(4–6), 285–293 (2002). doi:10.1016/S0378-4754(01)00373-1
28. EW Bai, KE Lonngren, A Ucar, Secure communication via multiple parameter modulation in a delayed chaotic system. Chaos Soliton Fract. **23**(3), 1071–1076 (2005)
29. EN Lorenz, Deterministic nonperiodic flow. J Atmos Sci. **20**, 130–141 (1963). doi:10.1175/1520-0469(1963)0202.0.CO;2
30. OE Rösler, An equation for continuous chaos. Phys Lett A. **57**(5), 397–398 (1976). doi:10.1016/0375-9601(76)90101-8
31. G Chen, T Ueta, Yet another chaotic attractor. Int J Bifurc Chaos. **9**(7), 1465–1466 (1999). doi:10.1142/S0218127499001024
32. J Lü, G Chen, S Zhang, The compound structure of a new chaotic attractor. Chaos Soliton Fract. **14**(5), 669–672 (2002). doi:10.1016/S0960-0779(02)00007-3
33. C Liu, T Liu, L Liu, K Liu, A new chaotic attractor. Chaos Soliton Fract. **22**(5), 1031–1038 (2004). doi:10.1016/j.chaos.2004.02.060

doi:10.1186/1687-6180-2011-14
Cite this article as: Xu: Generalized function projective synchronization of chaotic systems for secure communication. *EURASIP Journal on Advances in Signal Processing* 2011 **2011**:14.