General Projective Synchronization and Fractional Order Chaotic Masking Scheme

Shi-Quan Shao

Abstract—In this paper, a fractional order chaotic masking scheme used for secure communication is introduced. Based on the general projective synchronization of two coupled fractional Chen systems, a popular masking scheme is designed. Numerical example is given to demonstrate the effectiveness of the proposed method.

Index Terms—Chaotic systems, chaotic masking, fractional order system.

1. Introduction

In the past years, chaotic synchronization and its applications in secure communications has received a great deal of attention[1]-[5]. There are various kinds of synchronization schemes, including projective synchronization, general projective synchronization (GPS), lag synchronization, and so on. There are a lot of approaches about how to control two coupled systems to achieve synchronization[6]-[12]. After synchronization, one may add the message to the master chaotic signal as a new signal and transmit this signal as an input to the slave system. This is the well known “chaotic masking”. Many methods can help one recover the original message [8], [9]. This is just a typical application of chaos in secure communication systems.

General projective synchronization for fractional order chaotic system has been studied well in the recent years[13],[14]. On this base, a fractional order chaotic masking scheme will be discussed in this paper. Firstly, we construct the two coupled fractional order chaotic systems. Then, we consider the general projective synchronization scheme and the related message transmission scheme. Lastly, we will present some simulation results and give some concluding remarks.

2. General Projective Synchronization of the Fractional Order Chen System

We consider two coupled fractional order Chen systems as follows.

Master system:

\[
\begin{align*}
\frac{d^\alpha x_m}{dt^\alpha} & = -a (y_m - x_m) \\
\frac{d^\alpha y_m}{dt^\alpha} & = (c - a) x_m + cy_m - x_m z_m \\
\frac{d^\alpha z_m}{dt^\alpha} & = x_m y_m - b z_m
\end{align*}
\]

Slave system:

\[
\begin{align*}
\frac{d^\alpha x_s}{dt^\alpha} & = -a (y_s - x_s) \\
\frac{d^\alpha y_s}{dt^\alpha} & = (c - a) x_s + cy_s - x_s z_s \\
\frac{d^\alpha z_s}{dt^\alpha} & = x_s y_s - b z_s
\end{align*}
\]

where \(m\) and \(s\) means master system and slave system respectively.

In this paper, we choose \(a=35\), \(b=3\), and \(c=28\), and use the fractional order operator for \(\alpha = 0.9\):

\[
\frac{1}{s^{0.9}} = \frac{c_1 s^2 + c_2 s + c_3}{s + c_4 s^2 + c_5 s + c_6}
\]

where \(c_1 = 1.766\), \(c_2 = 38.27\), \(c_3 = 4.914\), \(c_4 = 36.15\), \(c_5 = 7.789\), and \(c_6 = 0.01\). Now we make the following definitions:

\[
\begin{align*}
& x_m = x_{1m}, \ y_m = x_{4m}, \ z_m = x_{7m} \\
& x_s = x_{1s}, \ y_s = x_{4s}, \ z_s = x_{7s} \\
& \frac{dx_m}{dt} = x_{2m}, \ \frac{d^2 x_m}{dt^2} = x_{5m} \\
& \frac{dx_s}{dt} = x_{2s}, \ \frac{d^2 x_s}{dt^2} = x_{5s}
\end{align*}
\]

\[
\begin{align*}
& \frac{dx_m}{dt} = x_{1m}, \ \frac{d^2 x_m}{dt^2} = x_{4m} \\
& \frac{dx_s}{dt} = x_{1s}, \ \frac{d^2 x_s}{dt^2} = x_{4s}
\end{align*}
\]

\[
\begin{align*}
& \frac{dx_m}{dt} = x_{6m}, \ \frac{d^2 x_m}{dt^2} = x_{9m} \\
& \frac{dx_s}{dt} = x_{6s}, \ \frac{d^2 x_s}{dt^2} = x_{9s}
\end{align*}
\]

\[
\begin{align*}
& \frac{dx_m}{dt} = x_{6m}, \ \frac{d^2 x_m}{dt^2} = x_{9m} \\
& \frac{dx_s}{dt} = x_{6s}, \ \frac{d^2 x_s}{dt^2} = x_{9s}
\end{align*}
\]
and
\[
\begin{align*}
\mathbf{x}_m &= (x_{t_1}, x_{2t_1}, x_{3t_1}, x_{4t_1}, x_{5t_1}, x_{6t_1}, x_{7t_1}, x_{8t_1})^T \\
\mathbf{x}_s &= (x_{t_2}, x_{2t_2}, x_{3t_2}, x_{4t_2}, x_{5t_2}, x_{6t_2}, x_{7t_2}, x_{8t_2})^T \\
\mathbf{x} &= (x_{t_1}, x_{2t_1}, x_{3t_1}, x_{4t_1}, x_{5t_1}, x_{6t_1}, x_{7t_1}, x_{8t_1})^T
\end{align*}
\]

where \( \mathbf{x}_m \in \mathbb{R}^{9t_1}, \mathbf{x}_s \in \mathbb{R}^{9t_1} \), and

\[
\frac{d\mathbf{x}_m}{dt} = A\mathbf{x}_m + \Phi(\mathbf{x}_m)
\]
\[
\frac{d\mathbf{x}_s}{dt} = A\mathbf{x}_s + \Phi(\mathbf{x}_s)
\]

The equivalent integer order system of (1) and (2) is

\[
\begin{align*}
0 &= 1 0 0 0 0 0 0 0 0 \\
0 &= 0 1 0 0 0 0 0 0 0 \\
ac_1 - c_6 &= ac_2 - c_3 \\
ac_1 - c_4 &= -ac_3 - ac_2 \\
0 &= 0 0 0 0 1 0 0 0 0 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
(c - a)c_3 &= (c - a)c_2 \\
cc_2 - c_5 &= cc_3 - c_4 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
0 &= 0 0 0 0 0 0 0 0 0 \\
0 &= -bc_3 - c_6 \\
0 &= -bc_2 - c_5 \\
0 &= -bc_1 - c_4
\end{align*}
\]

To make the two systems (1) and (2) to achieve general projective synchronization, a controlling item \( u(t) \) is added to the slave system of (6), then, one can get

\[
\begin{align*}
\frac{d\mathbf{x}_m}{dt} &= A\mathbf{x}_m + \Phi(\mathbf{x}_m) \\
\frac{d\mathbf{x}_s}{dt} &= A\mathbf{x}_s + \Phi(\mathbf{x}_s) + u(t)
\end{align*}
\]

Now, the problem is that what kind of \( u(t) \) can make system (6) achieve general projective synchronization.

**Theorem 1**: If the control input \( u(t) \) in (7) takes the form

\[
u = \beta(\Phi(\mathbf{x}_m) - \Phi(\mathbf{x}_s)) + K(\beta\mathbf{x}_m - \mathbf{x}_s)
\]

where \( \beta \) is the general projective scalar factor and

\[
K = \begin{bmatrix}
k_1 \\
\vdots \\
k_n
\end{bmatrix}
\]

and the following condition is satisfied:

\[
\mathbf{A} - K < 0,
\]

then the general projective synchronization can be achieved between the master and the slave systems in the integer order system (6) and its corresponding fractional order systems (1) and (2).

**Proof**: Define the error vector of synchronization of (6)

\[
\mathbf{e} = \beta\mathbf{x}_m - \mathbf{x}_s
\]

Construct the Lyapunov function

\[
\frac{dv}{dt} = \mathbf{e}^T\mathbf{e}/2,
\]

then

\[
\frac{dv}{dt} = \mathbf{e}^T\frac{de}{dt} = \mathbf{e}^T\left(\beta\frac{dx_m}{dt} - \frac{dx_s}{dt}\right)
\]

\[
= \mathbf{e}^T\left\{[\mathbf{A}/\beta\mathbf{x}_m + \beta\Phi(\mathbf{x}_m)] - \mathbf{A}\mathbf{x}_s - \Phi(\mathbf{x}_s) - \beta\Phi(\mathbf{x}_m) + \Phi(\mathbf{x}_s)\right\}
\]

\[
= \mathbf{e}^T(\mathbf{A} - K)\mathbf{e}
\]

Consider (10), obviously, \( \mathbf{dv}/dt < 0 \). So \( \lim_{t \to \infty} \mathbf{e} = 0 \), this means \( \lim_{t \to \infty} \mathbf{x}_s = \beta\mathbf{x}_m \), the GPS of (3) is achieved. And because (6) is the approximation of the fractional systems (1) and (2), the GPS will also be achieved in systems (1) and (2). The proof is completed.

In this paper, a simple masking scheme shown in Fig. 1 will be used.
3. Abstract and Index Terms

Let \( m(t) = 0.1 \sin(2\pi \cdot t) \), and \( \beta = 0.2 \), and add \( m(t) \) on the first state variable of master system. By using the method mentioned above, the simulation results are achieved as shown in the next figures.

Fig. 2 shows the original signal to be transmitted; Fig. 3 is the signal which has been encrypted by the mentioned masking scheme described above; Fig. 4 displayed both the transmitted signal and recovered signal and Fig. 5 is the errors of signal transmission.

4. Conclusions

In this paper, we discussed a general masking scheme in secret communication. Different from the traditional method, a fractional order chaotic system was applied in the consider system. General projective synchronization of two coupled fractional order Chen systems has been discussed. Finally, a simulation result verifies the effectiveness of the masking scheme.

Acknowledgment

The work was supported by the Key Science Research Project of Southwest University for Nationalities under Grant No. 234778.

References


(Continued from page 308)

Shi-Quan Shao was born in Sichuan Province, China, in 1976. He received the M.S. degree from the University of Electronic Science and Technology of China, Chengdu, in 2005. Now he works with Southwest University for Nationalities, Chengdu. His research interests are in nonlinear systems.