International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:4, No:5, 2010

A Two-Channel Secure Communication Using Fractional Chaotic Systems

Long Jye Sheu, Wei Ching Chen, Yen Chu Chen and Wei Tai Weng

***Abstract*—**In this paper, a two-channel secure communication using fractional chaotic systems is presented. Conditions for chaos synchronization have been investigated theoretically by using Laplace transform. To illustrate the effectiveness of the proposed scheme, a numerical example is presented. The keys, key space, key selection rules and sensitivity to keys are discussed in detail. Results show that the original plaintexts have been well masked in the ciphertexts yet recovered faithfully and efficiently by the present schemes.

Keywords-fractional chaotic systems, synchronization, secure communication.

I. Introduction

Since the work of Lorenz [1], chaos theory has stimulated intense attentions in recent decades. The random-like behavior of chaotic signals provides the potential for many applications. Among them, the introduction of chaos into secure communication has received a great deal of attentions after the pioneering work of Fujisaka & Yamada [2] and Pecora & Carroll [3]. With chaos-based encryption, a message is encrypted by a master chaotic signal at the transmitter. At the receiver end, a slave chaotic signal synchronized with the master one is necessary to retrieve the message signal. In recent years, a growing number of cryptosystems based on chaos synchronization have been proposed [4]. Many of them fundamentally are flawed by a lack of robustness and security.

In order to enhance the security levels, two-channel chaos-based cryptosystems are proposed [5, 6]. In these cryptosystems the ciphertext consists of a complex nonlinear combination of the plaintext and a variable of a chaotic transmitter's generator. Since it was not possible to synchronize the slave system with such ciphertext, a second channel had to be used in the system for transmitting synchronization signal. The synchronization signal was a different chaotic variable generated by the master system, which was transmitted to the receiver without any modification and does not contain any information of the plaintexts. These schemes are free to attacks if only ciphertext is intercepted by the intruder. However, if the synchronization signal is also intercepted, those schemes have been found to be insecure by Orue et al.[7] because parameter estimation is still possible by analyzing the chaos synchronization channel.

Chaotic attractors have been found in fractional order system in the past decade [8-15]. Compared to integer order system, it is found that the dynamics of fractional order system are more complexity because fractional derivatives have complex geometrical interpretation because of their non-local character [16] and high nonlinearity. Another advantage of using fractional chaotic systems in communication is that the derivative orders can be used as secret keys as well. Kiani et al. [17] proposed a secure communication using fractional chaotic systems based on extended fractional Kalman filter. In this manuscript, we proposed a modification of the two-channel chaos-based cryptosystems by using fractional chaotic systems to increase the security level of communication.

II. Fractional Derivatives

There are several definitions of fractional derivatives [18]. In this study, we use the Caputo-type fractional derivative defined by [19]:

$$\frac{d^{\alpha} y}{dt} = D^{\alpha} y(t) = J^{m-\alpha} y^{(m)}(t), \quad \alpha > 0, \tag{1}$$

where $m = [\alpha]$ is the value α rounded up to the nearest integer, $y^{(m)}$ is the ordinary m^{th} derivative of y, and

$$J^{\beta} y(t) = \frac{1}{\Gamma(\beta)} \int_0^t (t-\tau)^{\beta-1} y(\tau) \, d\tau \tag{2}$$

is the Riemann–Liouville integral operator of order $\beta>0$, where $\Gamma(\beta)$ is the gamma function.

III. Synchronization Bwtween Two Fractional Lorenz Systems by Single Variable

The fractional Lorenz system is given by

L. J. Sheu is with the Dept. of Mechanical Engineering, Chung Hua University, HsinChu, Taiwan (e-mail: ljsheu@chu.edu.tw).

W. C. Chen is with the Dept. of Information Management, YunPei University, HsinChu, Taiwan (corresponding author, Tel: +886-3-6586169, e-mail: wc137@hotmail.com).

Y. C. Chen is with Institute of Information Management, National Chiao Tung University, HsinChu, Taiwan. She is now with Dept. of Information Management, Hsiuping Institute of Technology, Taichung, Taiwan (e-mail: yenchuchen@gmail.com)

W. T. Weng is with the Dept. of Industrial Engineering and Management, MingChi University of Technology, Taipei, Taiwan (e-mail: wtweng@mail.mcut.edu.tw)

$$\begin{aligned} D^{\alpha_1} x_1 &= a(x_2 - x_1) \\ D^{\alpha_2} x_2 &= -x_1 x_3 + b x_1 - x_2 \\ D^{\alpha_3} x_3 &= x_1 x_2 - c x_3 \end{aligned} \quad (3)$$

where $(\alpha_1, \alpha_2, \alpha_3)$ are the fractional orders, (a, b, c) are parameters of this system. It has been shown that the fractional Lorenz system exhibits chaotic attractor. The first signal $x_1(t)$ of system (3) is chosen as synchronization signal to drive another Lorenz system

$$\begin{aligned} D^{\alpha_1} y_1 &= a(y_2 - y_1) \\ D^{\alpha_2} y_2 &= -x_1 y_3 + b x_1 - y_2 \\ D^{\alpha_3} y_3 &= x_1 y_2 - c y_3 \end{aligned} \quad (4)$$

Systems (3) and (4) are called the master and slave systems, respectively. It is noted that the sybsystem (y_2, y_3) is dependent on the signal $x_1(t)$, but the behavior is not influenced by the behavior of $x_2(t)$ and $x_3(t)$.

Synchronization means the trajectories of one of the systems will converge to the same values of the other. Define the state errors between the master and slave system as $e_1 = x_1 - y_1, e_2 = x_2 - y_2, e_3 = x_3 - y_3$. Subtracting system (3) by system (4) leads to

$$\begin{aligned} D^{\alpha_1} e_1 &= a(e_2 - e_1) \\ D^{\alpha_2} e_2 &= -x_1 e_3 - e_2 \\ D^{\alpha_3} e_3 &= x_1 e_2 - c e_3 \end{aligned} \quad (5)$$

By taking Laplace transform of both side of system (5), Let $E_i(s) = L[e_i(t)]$ where *i=1,2,3*, and applying $L[d^{\alpha} e_i / dt] = s^{\alpha} E_i(s) - s^{\alpha-1} e_i(0)$, we obtain

$$\begin{aligned} s^{\alpha_1} E_1(s) - s^{\alpha_1 - 1} e_1(0) &= a[E_2(s) - E_1(s)] \\ s^{\alpha_2} E_2(s) - s^{\alpha_2 - 1} e_2(0) &= -L[x_1 e_3] - E_2(s) \\ s^{\alpha_3} E_3(s) - s^{\alpha_3 - 1} e_3(0) &= L[x_1 e_2] - c E_3(s) \end{aligned} \quad (6)$$

Proposition: If $E_1(s), E_2(s)$ are bounded, then the master and slave systems will be synchronized.

Proof: Rewrite (6) as follows,

$$\begin{aligned} E_1(s) &= \frac{a E_2(s)}{s^{\alpha_1} + a} + \frac{s^{\alpha_1 - 1} e_1(0)}{s^{\alpha_1} + a} \\ E_2(s) &= -\frac{L[x_1 e_3]}{s^{\alpha_2} + 1} + \frac{s^{\alpha_2 - 1} e_2(0)}{s^{\alpha_2} + 1} \\ E_3(s) &= \frac{L[x_1 e_2]}{s^{\alpha_3} + c} + \frac{s^{\alpha_3 - 1} e_3(0)}{s^{\alpha_3} + c} \end{aligned} \quad (7)$$

Using the final value theorem of Laplace transform, it follows that

$$\begin{aligned} \lim_{t\to\infty} e_1(t) &= \lim_{s\to 0^+} s E_1(s) = \lim_{s\to 0^+} s E_2(s) = \lim_{t\to\infty} e_2(t) \\ \lim_{t\to\infty} e_2(t) &= \lim_{s\to 0^+} s E_2(s) = -\lim_{s\to 0^+} s L[x_1 e_3] \\ \lim_{t\to\infty} e_3(t) &= \lim_{s\to 0^+} s E_3(s) = \frac{1}{c} \lim_{s\to 0^+} s L[x_1 e_2] \end{aligned} \quad (8)$$

Since $E_1(s), E_2(s)$ are bounded, we have $\lim_{t\to\infty} e_1(t) = \lim_{t\to\infty} e_2(t) = 0$. Now, owing to the attractiveness of the attractors of system (3) and (4), there exists $\eta > 0$ such that $|x_i(t)| \le \eta < \infty, |y_i(t)| \le \eta < \infty$ where *i* refers to the index of the master or slave variables. Therefore, $\lim_{t\to\infty} e_3(t) = 0$. This implies that

$$\lim_{t\to\infty} e_i(t) = 0, \quad i = 1,2,3 \quad (9)$$

Consequently, the synchronization between the master and slave systems (3) and (4) is achieved.

IV. Proposed Scheme of Secure Communication

Fig. 1 illustrates the overall architecture of a secure communication scheme with two transmission channels. In the encryption step, we use a highly nonlinear function ϕ to encrypt the plaintexts $S(t)$ with the chaotic signals $x_2(t)$. The ciphertexts $T_1(t)$ are transmitted to the receiver. In the second step, we transmit the synchronization signal $x_1(t)$ in a separate channel to the receiver. In this channel, $x_1(t)$ is used for synchronization and does not contain any information of the plaintexts.

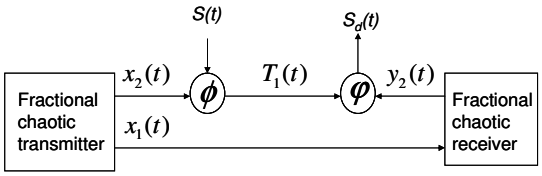

Fig. 1 Architecture of the secure communication scheme

Once synchronization between drive and response systems are reached, the plaintexts can be recovered ($S_d(t)$) simply using the nonlinear function φ to decrypt the ciphertexts. It is noted that our secure communication scheme shares a common feature with [5]. However, this scheme is different from [5] in that we applied a fractional chaotic system. In the following section, we will show that the use of fractional chaotic system expands the key space and increase the security levels.

V. Analysis

A. Numerical results

In this section, we present simulation results to demonstrate the efficiency of our new secure communication scheme. An efficient method for solving fractional order differential equations is the predictor corrector scheme or more precisely, PECE (Predict, Evaluate, Correct, Evaluate) technique. The detailed algorithm of the scheme was developed by Diethelm et al. [20]. The scheme has been adopted to simulate the fractional chaotic system in many researches [11, 14, 17]. It is used throughout this paper.

The following choices of fractional orders, parameters and initial conditions for the master and slave systems were selected for simulations:

$$\begin{aligned}&(\alpha_1,\alpha_2,\alpha_3)=(0.96,0.98,1.1)\\&(a,b,c)=(10,28,8/3)\\&[x_1(0),\,x_2(0),\,x_3(0)]=[-1,-2,5]\\&[y_1(0),\,y_2(0),\,y_3(0)]=[1,2,1]\end{aligned}. \qquad (10)$$

The encryption/decryption pairs, $\psi(\bullet)$ and $\phi(\bullet)$, can be chosen according to different system demands for higher security/privacy. In this work, we follow the work of [5] and take the encryption and decryption functions to be

$$\begin{aligned}&\psi(\bullet)=x_2^2(t)+(1+x_2^2(t))S(t)\\&\phi(\bullet)=-\frac{y_2^2(t)}{1+y_2^2(t)}+\frac{T_1(t)}{1+y_2^2(t)}\end{aligned}. \qquad (11)$$

In the following simulation, a total simulation time of 40 seconds with 10000 time steps was used. The sampling frequency was 250 Hz. A sinusoidal signal with a frequency of 2 Hz was used as the plaintext signal, $S(t)=0.05\sin(4\pi t)$. Fig. 2 shows the synchronization between fractional master and slave systems. It is shown that two fractional systems have been synchronized. Fig. 3 shows the ciphertexts through the channels. With nonlinear mix of plaintexts and chaotic signal, it's impossible to obtain the useful plaintexts from the ciphertexts.

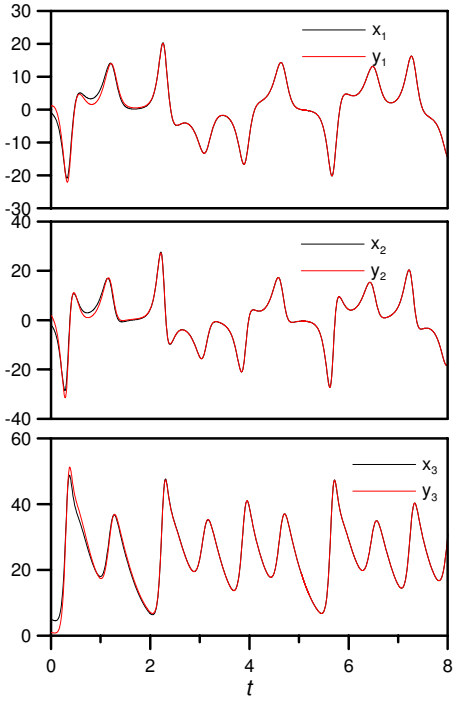

Fig. 2. The response and synchronization of master and slave system.

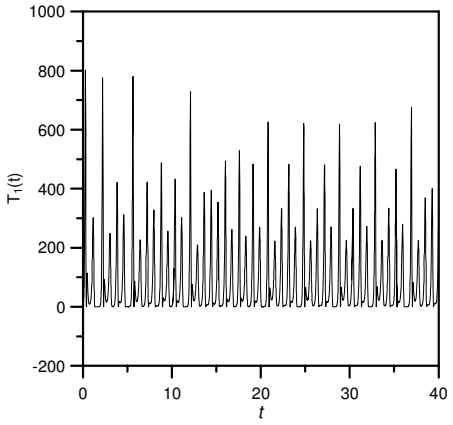

Fig. 3 ciphertexts $T_1(t)$ through the channel

Fig. 4 shows the results of the recovery using this scheme. The decrypted plaintexts in the initial time stage are clipped to scale of the vertical axis in this figure. The plaintexts are recovered with errors during the initial synchronization time. However, the error of recovery, $E(t)=S(t)-S_d(t)$, approaches zero very quickly. The initial synchronization time was estimated to be about 4 seconds.

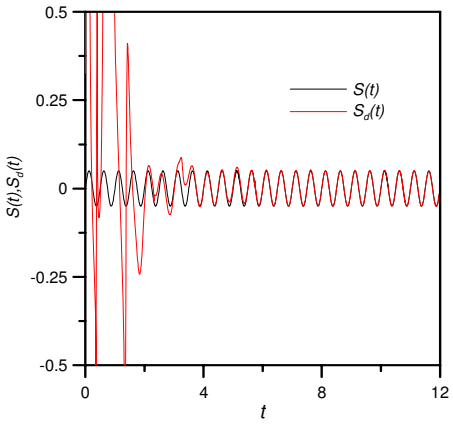

Fig. 4. Original and recovered plaintexts

After the initial synchronization time, the plaintexts can be successfully recovered as shown in Fig. 4.

B. Keys, key space, selection rules of keys and sensitivity

In the present scheme, the encryption signals, $x_2(t)$, are generated from the fractional Lorenz system with fractional derivative orders $(\alpha_1, \alpha_2, \alpha_3)$ and the parameters (a, b, c). The fractional derivative orders can be used as secret keys as well. Hence, the secret key consists of six numbers $(\alpha_1, \alpha_2, \alpha_3, a, b, c)$. Since these six numbers could be real numbers, the space of the keys will be a 6-dimensional space. The space is nonlinear since all of the keys are not equally strong. In the subspace where the fractional derivative orders or parameters of the fractional Lorenz system originate periodic orbits, the sub-key space is degenerative because it is relatively easy to break. Values of $(\alpha_1, \alpha_2, \alpha_3, a, b, c)$ which give rise to periodic windows should be avoided since chaotic bands are preferred for encryption.

The security of chaos-based cryptosystems relies on the secret key consisting of the chaotic system's parameters and/or some other complementary parameters that control how the plaintext is included. Hence, finding the parameters is equivalent to breaking the system. The two-channel secure communication proposed by Jiang [5] has been broken by [7] because the parameters of integer Lorenz chaotic system can be estimated by simply geometrical properties. In our scheme, as fractional derivative order are also regarded as keys, the breaking method described by Orue et al. [7] are not effective because estimation of fractional derivative orders is not possible in their method.

Next, we demonstrate the sensitivity of our communication system to keys. Consider an intruder intercept both the ciphertexts and synchronization signals. Assume the intruder get an approximate estimate of keys, say $(\alpha_1, \alpha_2, \alpha_3, a, b, c) = (0.96, 0.97, 1.1, 10, 28, 8/3)$ in which there is a slight mismatch with the real keys in α_2.

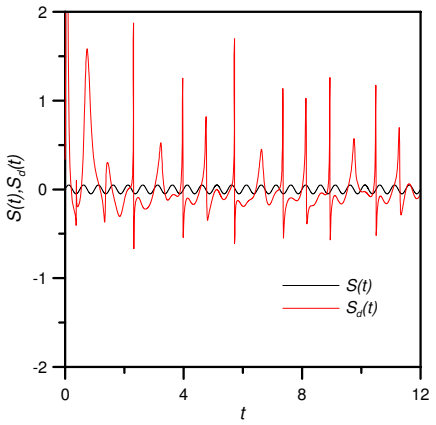

Fig. 5 Sensitivity of present secure communication scheme to mismatch of keys.

Fig. 5 shows the sensitivity of present secure communication scheme to slight mismatch of keys. It is noted that the recovered plaintexts is totally different from the real plaintexts.

VI. Conclusions

In this paper chaos synchronization between two fractional Lorenz systems by using single variable has been studied. Conditions for chaos synchronization have been investigated theoretically by using Laplace transform. A two-channel communication scheme using the fractional Lorenz systems has been presented. With usage of fractional derivative order as the keys, the key space is expanded and guarantees higher security.

Acknowledgment

The authors acknowledge the financial support received under the Grant NSC99-2218-E-264-001 from the National Science Council, R.O.C.

References

[1] E. N. Lorenz, "Deterministic nonperiodic flow," Journal Atmospheric Sciences, Vol. 20, pp. 130-141, 1963.

[2] H. Fujisaka and T. Yamada, "Stability theory of synchronized motion in coupled-oscillator systems," Progress in Theoretic Physics, Vol. 69, pp. 32-47, 1983.

[3] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Physical Review Letters, Vol. 64, pp. 821-824, 1990.

[4] T. Yang, "A survey of chaotic secure communication systems," International Journal of Computational Cognition, Vol. 2, pp. 81-130, 2004.

[5] Z. P. Jiang, "A note on chaotic secure communication systems," IEEE Trans. Circuits Syst.-I Fund. Theory Appl., Vol. 49, pp. 92-96, 2002.

[6] Z. Li and D. Xu, "A secure communication scheme using projective chaos synchronization," Chaos Solitons Fractals, Vol. 22, pp. 477-481, 2004.

[7] A. B. Orue, V. Fernandex, G. Alvarez, G. Pastor, M. Romera, S. Li and F. Montoya, "Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems," Physis Letters A, Vol. 372, pp. 5588-5592, 2008.

[8] I. Petras, "A note on the fractional-order Chua's system," Chaos Solitons Fractals, Vol. 38, pp. 140-147, 2008.

[9] T. T. Hartley, C. F. Lorenzo and H. K. Qammer, "Chaos in a fractional Chua's system," IEEE Circuit Systems Theory Application, Vol. 42, pp. 485-490, 1995.

[10] L. J. Sheu, H. K. Chen, J. H. Chen and L. M. Tam, "Chaotic dynamics of the fractionally damped Duffing equation," Chaos Solitons Fractals, Vol. 32, pp. 1459-68, 2007.

[11] C. P. Li and G. J. Peng, "Chaos in Chen's system with a fractional order," Chaos Solitons Fractals, Vol. 20, pp. 442-450, 2004.

[12] W. H. Deng and C. P. Li, "Chaos synchronization of the fractional Lu system," Physica A, Vol. 353, pp. 61-72, 2005.

[13] L. J. Guo, "Chaotic dynamics and synchronization of fractional-order Arneodo's systems," Chaos Solitons Fractals, Vol. 26, pp. 1125-1133, 2005.

[14] L. J. Sheu, H. K. Chen, J. H. Chen and L. M. Tam, "Chaos in a new system with fractional order," Chaos Solitons Fractals, Vol. 31, pp. 1203-1212, 2007.

[15] W. Zhang, S. Zhou, H. Li and H. Zhu, "Chaos in a fractional-order Rossler system," Chaos Solitons Fractals, Vol. 42, pp. 1684-1691, 2009.

[16] I. Podlubny, "Geometric and physical interpretation of fractional integral and fractional derivatives," Journal of Fractional Calculus, Vol. 5, pp. 367-386, 2002.

[17] A. Kiani-B, K. Fallahi, N. Pariz and H. Leung, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter," Commu. Nonlin. Sci. Num. Simul., Vol. 14, pp. 863-879, 2009.

[18] I. Podlubny, Fractional differential equations, Academic Press, New York, 1999.

[19] M. Caputo, "Linear models of dissipation whose Q is almost frequency independent-II," Geophys J R Astron. Soc., Vol. 13, pp. 529-539, 1967.

[20] K. Diethelm, N. J. Ford and A. D. Freed, "A predictor–corrector approach for the numerical solution of fractional differential equations," Nonlinear Dynamics, Vol. 29, pp. 3-22, 2002.