International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:3, 2010

A New Secure Communication Model Based on Synchronization of Coupled Multidelay Feedback Systems

Thang Manh Hoang

Abstract**—** Recent research result has shown that two multidelay feedback systems can synchronize each other under different schemes, i.e. lag, projective-lag, anticipating, or projective-anticipating synchronization. There, the driving signal is significantly complex due that it is constituted by multiple nonlinear transformations of delayed state variable. In this paper, a secure communication model is proposed based on synchronization of coupled multidelay feedback systems, in which the plain signal is mixed with a complex signal at the transmitter side and it is precisely retrieved at the receiver side. The effectiveness of the proposed model is demonstrated and verified in the specific example, where the message signal is masked directly by the complex signal and security is examined under the breaking method of power spectrum analysis.

Keywords**—**chaos synchronization, time-delayed system, chaos-based secure communications

I. Introduction

Since the idea of synchronizing two identical autonomous chaotic systems was first introduced by Pecora and Carroll [1], chaos synchronization has been received great interest and quickly become an area of active research in nonlinear science. It has been widely investigated in many fields, such as physical [2], chemical and ecological science [3], [4], secure communications [5], etc. General speaking, the synchronization phenomenon of coupled dynamical systems can be interpreted that the master (drive system) sends the driving signal to drive the slave (driven system), and there exists some functional relation in their trajectories during interaction. So far, there are several schemes of synchronization proposed and pursued, i.e. complete synchronization (PC) [1], generalized synchronization [6], projective synchronization [7], lag synchronization [8], anticipating synchronization [9], phase synchronization [10] and their combinations [11], [12].

In a synchronization-based secure communication system, the message signal is concealed by modulating with a complex signal produced by a chaotic system, and it is recovered by synchronizing between the master at the transmitter side and the slave at the receiver side. Moreover, the complex signal produced by the master is a chaotic, broadband, noise-like signal, so it is used as a carrier for secure transmission. In general, the security of chaos-based communication systems is dependent on the complexity degree of master's dynamics, carrying signal as well as the encryption scheme used. According to the method used for encrypting the plain signal, there are five common types of chaos synchronization-based encryption structures: additive masking [13], parametric modulation [13], [14], state variable modulation [15], chaos shift keying (CSK) [16] and synchronization-manifold shift keying (SMSK) [17]. Additive masking is looked as a simplest scheme in which the plain signal is added with the driving signal and the resulting signal is sent to the receiver. In consideration of the complexity degree of master's dynamics, time-delay systems are regarded as a prominent candidate for the application in secure communication due that those produce highly dimensional dynamics [18], [19]. Presented in [20], [11], [12], coupled multidelay feedback systems synchronize each other under different synchronization schemes depending on the relation of the value of time delays and that of system parameters. The driving signal is significantly complicated because it is a combination of nonlinear components of delayed state variable. Moreover, the complexity degree of the driving signal can be customized by changing the number of nonlinear components as well as the appropriate value of delays and parameters.

In this paper, a secure communication model is proposed mainly based on synchronization of coupled multidelay feedback systems, on restriction of existing reconstruction methods in reconstructing a multidelay feedback system by observing multidelay driving signal as well as on exploitation of the complexity of time-delay signal to conceal the message signal. There, the time-delay signal, which is used as a carrying signal, is constituted by nonlinearly transformed components of delayed state variable, and it is used for mixing with the plain signal. The effectiveness of the proposed model is demonstrated and verified in the specific example, where the message signal is masked directly by the complex signal and security is examined under the breaking method of power spectrum analysis.

II. Review of Synchronization of Coupled Multidelay Feedback Systems

In [20], [11], [12], the schemes of synchronization of coupled multidelay feedback systems have been studied with the structure illustrated in Fig. 1. The equations are given in eqs. (1)-(3). The driving signal is generated by a driving signal generator (DSG) in the form of eq. (2).

Master:

$$\frac{dx}{dt} = -\alpha x + \sum_{i=1}^{P} m_i f(x_{\tau_i}) \qquad (1)$$

Dr. Thang Manh Hoang is with the Department of Electronics and Informatics, Faculty of Electronics and Telecommunications, Hanoi University of Technology, 1 Dai Co Viet, Hanoi, Vietnam, email: hmt@mail.hut.edu.vn

Driving signal:

$$DS(t) = \sum_{i=1}^{P} k_i f(x_{\tau_{P+i}}) \tag{2}$$

Slave:

$$\frac{dy}{dt} = -\alpha y + \sum_{i=1}^{P} n_i f(y_{\tau_i}) + DS(t) \tag{3}$$

where $\alpha, m_i, n_i, k_i, \tau_i \in \Re$; integer P, the time-delayed variables x_{τ_i} and y_{τ_i} stand for $x(t-\tau_i)$ and $y(t-\tau_i)$, respectively. $f(.)$ is the differentiable generic nonlinear function. Note that, as given in eq. (2) the driving signal is combination of multiple delay components, thus, the driving signal is highly complex.

Suppose τ_d be the time length of delay between state variable of master and that of slave. According to Krasovskii-Lyapunov theory [21], [22], the sufficient condition for different schemes of synchronization, together with the supposed relation between the value of delays and parameters, is

(i) For the scheme of lag synchronization, synchronization manifold $y(t) = x(t-\tau_d)$:

$$\begin{cases} \alpha > \sum_{i=1}^{P} |n_i| \, |\sup f'(x_{\tau_d+\tau_i})| \\ \tau_{P+i} = \tau_d + \tau_i \\ m_i - k_i = n_i \end{cases} \tag{4}$$

(ii) For the scheme of anticipating synchronization, synchronization manifold $y(t) = x(t+\tau_d)$:

$$\begin{cases} \alpha > \sum_{i=1}^{P} |n_i| \, |\sup f'(x_{\tau_i-\tau_d})| \\ \tau_{P+i} = \tau_i - \tau_d \quad (\tau_i \geq \tau_d \ for \ \forall i) \\ m_i - k_i = n_i \end{cases} \tag{5}$$

(iii) For the scheme of projective-lag synchronization, synchronization manifold $ay(t) = bx(t-\tau_d)$:

$$\begin{cases} \alpha > \sum_{i=1}^{P} |an_i| \, |\sup f'(x_{\tau_d+\tau_i})| \\ \tau_{P+i} = \tau_i + \tau_d \\ bm_i - ak_i = an_i \end{cases} \tag{6}$$

(iv) For the scheme of projective-anticipating synchronization, synchronization manifold $ay(t) = bx(t+\tau_d)$:

$$\begin{cases} \alpha > \sum_{i=1}^{P} |an_i| \, |\sup f'(x_{\tau_d-\tau_i})| \\ \tau_{P+i} = \tau_i - \tau_d \quad (\tau_i \geq \tau_d \ for \ \forall i) \\ bm_i - ak_i = an_i \end{cases} \tag{7}$$

where a and b are non-zero real. It is easy to realize that the lag/projective-lag synchronization is turned into the anticipating/projective-anticipating synchronization by changing the relation between the value of delays from $\tau_{P+i} = \tau_i + \tau_d$ to $\tau_{P+i} = \tau_i - \tau_d$.

III. Proposed Secure Communication Model

As assumed in the literature, chaotic modulation is an adequate means for secure transmission due to the properties presented by chaotic systems, i.e. sensitive dependence on parameters and initial conditions, ergodicity, mixing and dense sinusoidal points. Thus, chaotic signal is similar to pseudo random noise and used as a masking signal for cryptographic purposes. A requirement of the pseudo random noise used in cryptography is that its spectrum should be infinitely broad and flat. In addition, its power density is higher than that of the plain signal, in other words, power spectrum of message signal is buried into that of masking signal. Accordingly, time delay signal produced by multidelay feedback systems can be considered for such purpose.

In this section, a secure communication model based on synchronization of coupled multidelay feedback systems is presented in which the analogous plain signal is concealed by a time delay complex signal (called a *carrier*). In addition, the number of possible models is equal to that of synchronous schemes of coupled multidelay feedback systems as described above. In fact, the difference among structures of such models is very small. For simplicity, the secure communication model considered in the present section is that the master and the slave synchronize each other under the scheme of lag synchronization with the synchronization manifold $y(t) = x(t-\tau_{d_{ref}})$. The other ones will be given in the section V.

The configuration of the proposed secure communication model is depicted in Fig. 2 where the transmitter consists of the master, DSG, and encryptor. The driving signal produced by DSG is used for synchronizing the slave in the receiver. The message signal $i(t)$ is mixed with the carrier in Encryptor. Since the master and the slave synchronize each other, the difference between their state variables is only the time length of delay $\tau_{d_{ref}}$, thus, the equation for transmitted signal (called a *ciphertext signal*) is $C(t) = EN[i(t), x_{\tau_{d_{ref}}+\tau_{d_1}}, x_{\tau_{d_{ref}}+\tau_{d_2}} ... x_{\tau_{d_{ref}}+\tau_{d_N}}]$. Then, the resulting signal is sent to the receiver. At the receiver side, the state variable of the slave is used as a reference signal by Decryptor to retrieve the decrypted plain signal $i'(t)$ and the equation employed by Decryptor is $i'(t) = DE[C(t), y_{\tau_{d_1}}, y_{\tau_{d_2}} ... y_{\tau_{d_N}}]$.

Example: To demonstrate the operation of the proposed system, in this example, the dynamical equations are in the form of six-delay Mackey-Glass system as:

Master:

$$\frac{dx}{dt} = -\alpha x + \sum_{i=1}^{P=6} m_i \frac{x_{\tau_i}}{1 + x_{\tau_i}^c} \tag{8}$$

Driving signal:

$$DS(t) = \sum_{i=1}^{P=6} k_i \frac{x_{\tau_{P+i}}}{1 + x_{\tau_{P+i}}^c} \tag{9}$$

Slave:

$$\frac{dy}{dt} = -\alpha y + \sum_{i=1}^{P=6} n_i \frac{y_{\tau_i}}{1 + y_{\tau_i}^c} + DS(t) \tag{10}$$

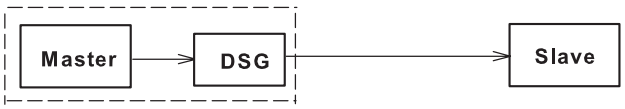


Fig. 1: Structure of synchronization system

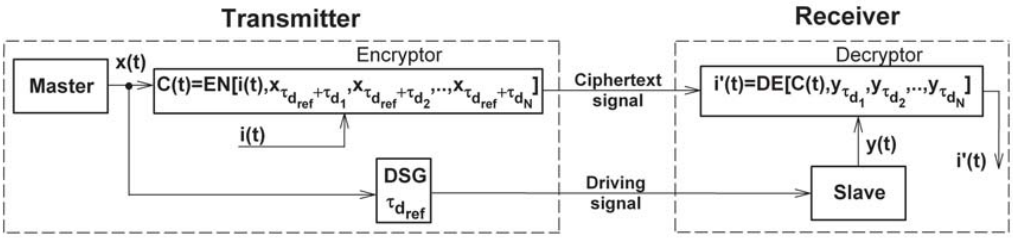


Fig. 2: Structure of the proposed secure model using the scheme of lag synchronization

As an exemplar case, the chosen equation to encrypt the plain signal is in the form of

$$\begin{aligned} C(t) &= EN[i(t), x_{\tau_{d_1}+\tau_{d_{ref}}}, x_{\tau_{d_2}+\tau_{d_{ref}}} ... x_{\tau_{d_N}+\tau_{d_{ref}}}] \\ &= \sum_{s=1}^{N=4} r_s \frac{x_{\tau_{d_s}+\tau_{d_{ref}}}}{1+x^c_{d_{\tau_s}+\tau_{d_{ref}}}} + i(t) \end{aligned} \tag{11}$$

Assumed that the ciphertext signal is reached the receiver without disturbance. Hence, the equation to decrypt the recovered message signal is

$$\begin{aligned} i'(t) &= DE[C(t), y_{\tau_{d_1}}, y_{\tau_{d_2}} ... y_{\tau_{d_N}}] \\ &= \sum_{s=1}^{N=4} r_s \frac{y_{\tau_{d_s}}}{1+y^c_{\tau_{d_s}}} - C(t) \end{aligned} \tag{12}$$

The adopted value of parameters and delays for simulation as: $y(t) = x(t - \tau_{d_{ref}})$, $\tau_{d_{ref}} = 1.4$, $c = 10$, $\alpha = 8.0$, $m_1 = -20.0$, $m_2 = -15.0$, $m_3 = -0.6$, $m_4 = -16.0$, $m_5 = -25.0$, $m_6 = -0.9$, $n_1 = -0.7$, $n_2 = -0.8$, $n_3 = -0.6$, $n_4 = -0.4$, $n_5 = -0.5$, $n_6 = -0.9$, $k_1 = -19.3$, $k_2 = -14.2$, $k_3 = k_6 = 0$, $k_4 = -15.6$, $k_5 = -24.5$, $\tau_1 = 3.4$, $\tau_2 = 6.7$, $\tau_3 = 1.2$, $\tau_4 = 5.6$, $\tau_5 = 4.5$, $\tau_6 = 2.3$, $\tau_7 = 4.8$, $\tau_8 = 8.1$, $\tau_9 = 7.0$, $\tau_10 = 5.9$, $r_1 = -19.6$, $r_2 = -14.5$, $r_3 = -15.3$, $r_4 = -24.2$, $\tau_{d_1} = 7.2$, $\tau_{d_2} = 8.3$, $\tau_{d_3} = 10.5$, $\tau_{d_4} = 11.6$.

Shown in Fig. 3 is the simulation result for the message signal $i(t) = 0.1sin(40\pi t)$. The synchronization manifold is illustrated on the portrait of $y(t)$ versus $x(t - \tau_{dref})$ in Fig. 3(a). Since the synchronous regime gets stable, the recovered plain signal is retrieved precisely at the receiver as presented in Fig. 3(b) and its waveform is nearly identical to that of message signal given in Fig. 3(c). Shown in Figs. 3(d)-3(f) is the waveform of the driving signal, carrier, and ciphertext signal.

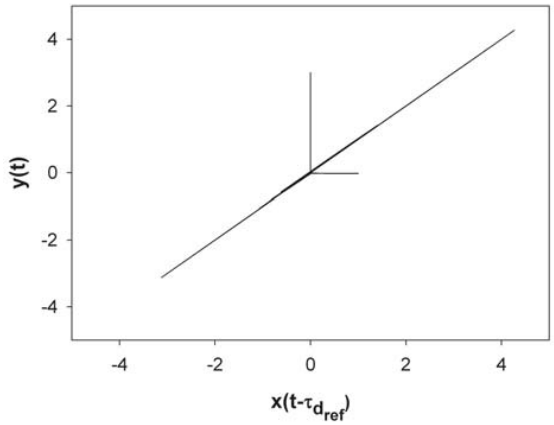
IV. Security Analysis

In this section, security of the proposed model is discussed and the simulation result of above example is used in the analysis. Specifically, the breaking method based on power spectrum analysis is realized to verify the security.

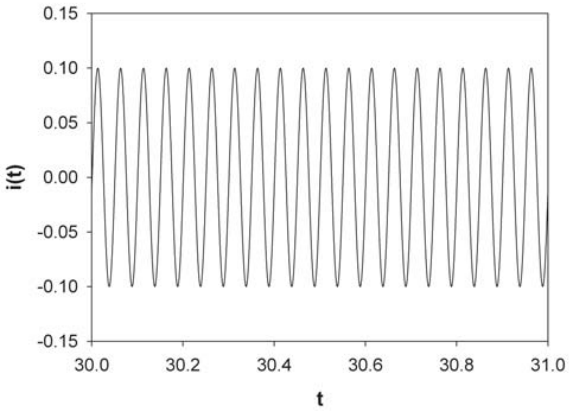
So far, there exists two main types of breaking methods used to unmask the message signal from the ciphertext signal transmitted in chaotic secure communication systems, i.e. identification-based methods and characteristic-based methods. In operation, while identification-based methods need to reconstruct dynamics of transmitters, characteristic-based ones exploit different properties of chaotic system and/or different features of ciphertext to extract the message signal. For the identification-based methods, as discussed in [17] and therein, a multidelay feedback system can not be reconstructed by existing reconstruction methods, in other words, the proposed secure model must not be broken by observing either the driving signal or the ciphertext signal.

In the literature [23], [24], [25], [26], [27], [28], [29], [30], [31], each characteristic-based breaking method is designed to attack a specific secure communication system. However, the breaking method based on power spectrum analysis is a simplest one and used widely as a basic test in most security schemes, thus, any secure communication system should, at least, be able to resist from this kind of breaking method. The effectiveness of the breaking method is represented in successful attacks on a series of chaotic secure systems [27], [29], [31]. Accordingly, the security of the proposed model will be checked by such breaking method by means of specific example.

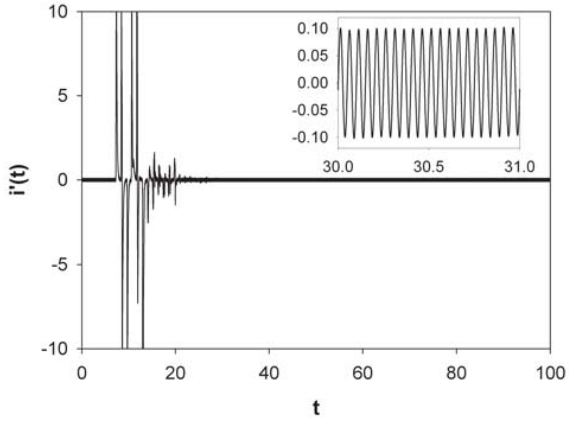
Illustrated in Fig. 4 is relative power spectrum of the carrier and that of the ciphertext for the case of $i(t) = 0.1sin(40\pi t)$ in above example. It is easy to observe from Fig. 4(c) that the spectrum of the plain signal is buried in that of the carrier. However, the plain signal is revealed for the case of $i(t) = 0.5sin(40\pi t)$ as illustrated in Fig. 4(e). It can be observed that the frequency of the plain signal clearly emerges at $f = 20$ Hz over the background noise as a prominent peak. As a result, it is impossible to extract the information of the plain signal by analyzing the power spectrum of the ciphertext if the power of the plain signal is sufficiently small.



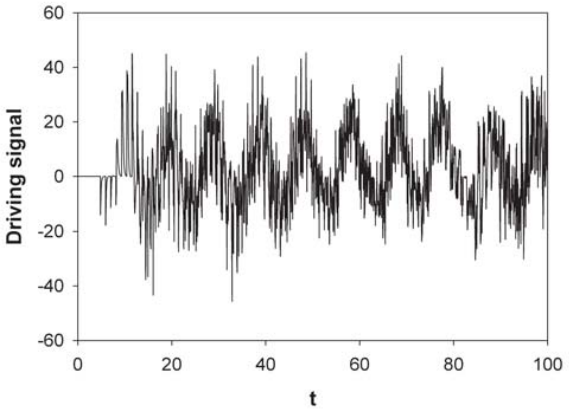
(a) Portrait of $y(t)$ versus $x(t - \tau_{d_{ref}})$



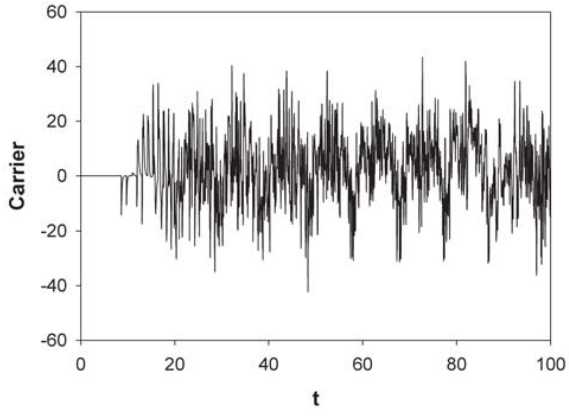
(b) Part of plain signal



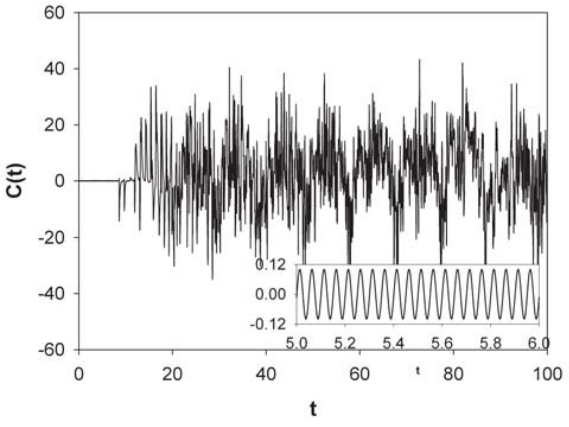
(c) Recovered plain signal



(d) Driving signal

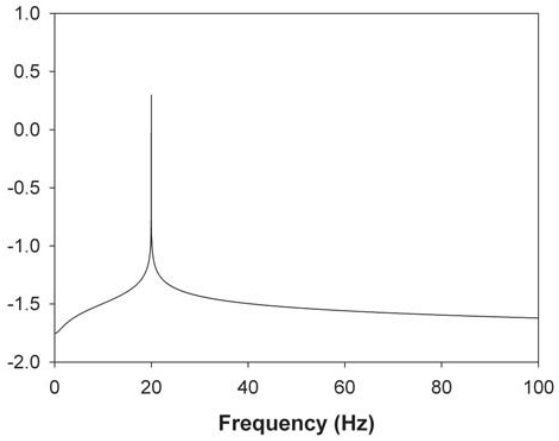


(e) Carrier

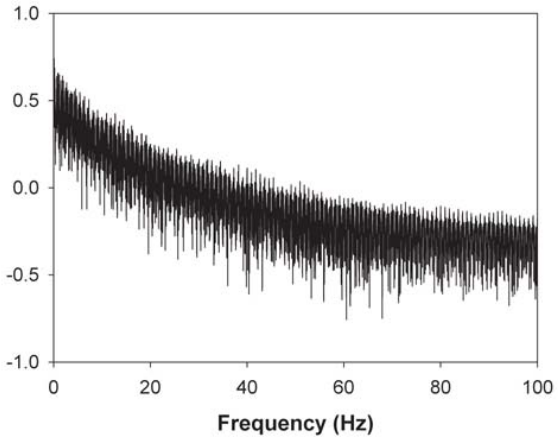


(f) Ciphertext

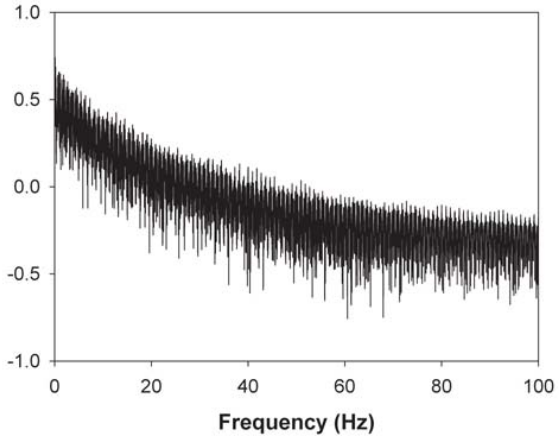
Fig. 3: Simulation result



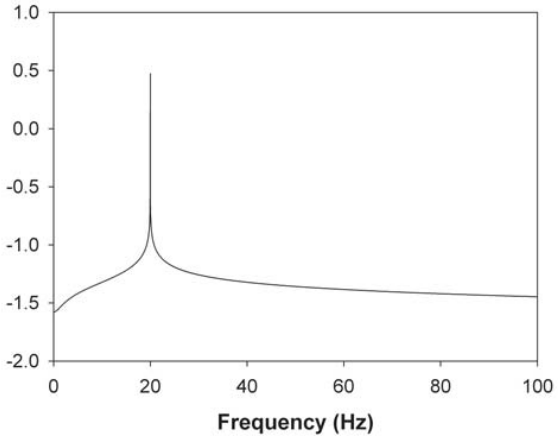
(a) Logarithmic power spectrum of $i(t) = 0.1sin(40\pi t)$



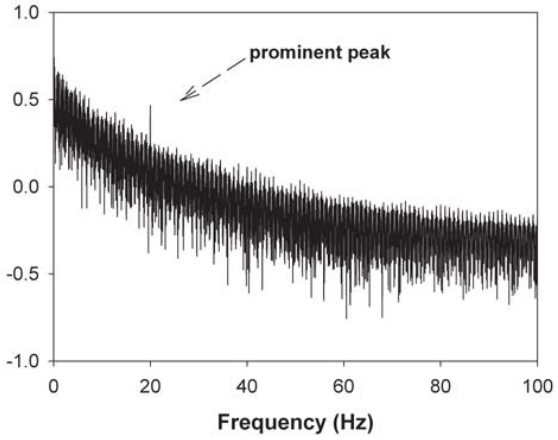
(b) Logarithmic power spectrum of the carrier



(c) Logarithmic power spectrum of the ciphertext with $i(t) = 0.1sin(40\pi t)$

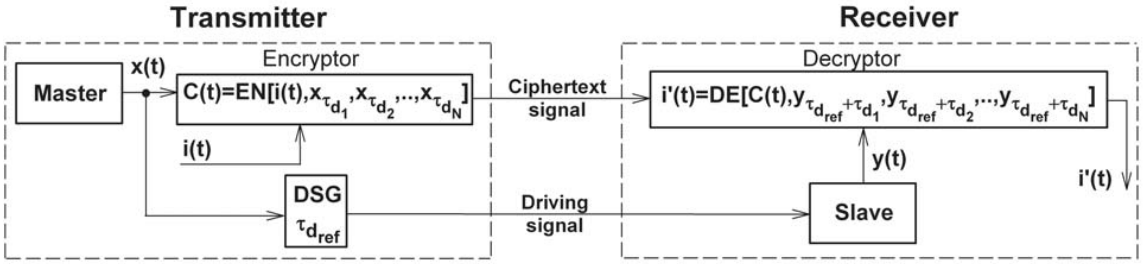


(d) Logarithmic power spectrum of $i(t) = 0.5sin(40\pi t)$

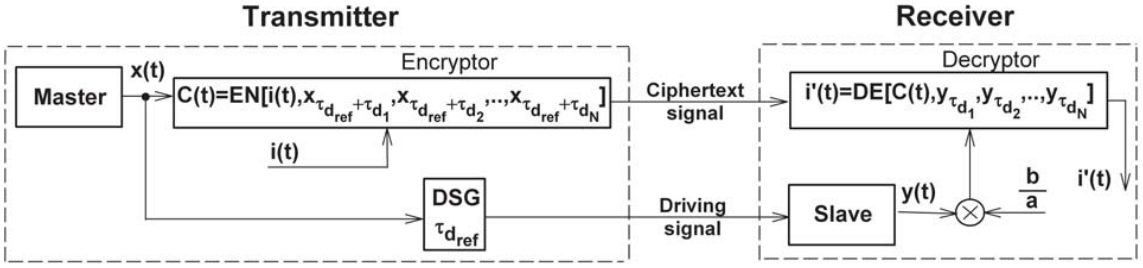


(e) Logarithmic power spectrum of the ciphertext with $i(t) = 0.5sin(40\pi t)$

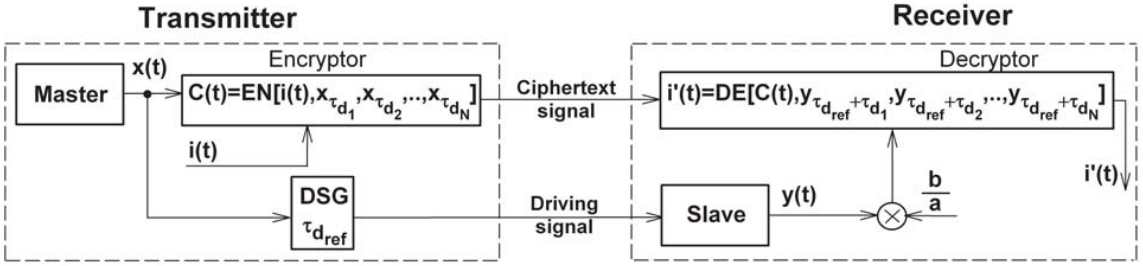
Fig. 4: Relative power spectra



(a) Structure utilizing anticipating synchronization



(b) Structure utilizing projective-lag synchronization



(c) Structure utilizing projective-anticipating synchronization

Fig. 5: Various structures

V. Conclusions

In this paper, the secure communication model using synchronization of coupled multidelay feedback systems has been described and the security of the exemplar system is checked by analyzing the power spectrum. The simulation result shows that the secure communication system can resist from the breaking method of power spectrum analysis, as a result, the message signal is securely transmitted and precisely recovered at the receiver side even using a simplest scheme of masking modulation. Thus, the scheme of multiplicative modulation may also be applied in this model. In addition, the proposed model allows to choose suitable encryption algorithms which assure the security. Moreover, the small power of the message signal can be precisely recovered at the receiver side due to the presence of the reference channel.

It can be observed from the small graph of Fig. 3(f) that the message signal is clearly exposed in the ciphertext signal since the synchronous regime between the master and the slave has not been reached stable. To remove this drawback, the plain signal is transmitted after the synchronization is established completely. Furthermore, the security of the proposed model can be enhanced significantly by changing the value of manifold's delay and/or that of system parameters as the proposed schemes shown in [32]. However, for the proposed model the change in the value of manifold's delay and/or that of system parameters can occur correspondingly to transmission sessions. That is because the change can not take place during transmission, otherwise large synchronization error may cause a distortion in recovered message signal.

In consideration of the diversification of the model, the other schemes of synchronization of coupled multidelay feedback systems can be utilized in the proposed model. Given in § III is the secure communication model utilizing the scheme of lag synchronization. To use the scheme of anticipating synchronization of coupled multidelay feedback systems, the structure of Fig. 2 is modified to as shown in Fig. 5(a). Comparing the structure given in Fig. 5(a) to that illustrated in Fig. 2, the change is very small because the difference between lag synchronization and anticipating one is in the relative delay of state variables as shown in §II. Hence, addition delay of $\tau_{d_{ref}}$ is applied to retard the state variable of the slave in Decryptor. Besides, under similar

reasoning, the structures for the cases of utilizing the schemes of projective-lag and projective-anticipating synchronizations are shown in Figs. 5(b) and 5(c), respectively. It is clear that the state variable of the slave must be scaled back before fed to the decoder.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.
[2] M. Lakshmanan and K. Murali, *Chaos in Nonlinear Oscillators: Controlling and Synchronization*. Singapore: World Scientific, 1996.
[3] S. K. Han, C. Kurrer, and Y. Kuramoto, "Dephasing and bursting in coupled neural oscillators," *Phys. Rev. Lett.*, vol. 75, pp. 3190–3193, 1995.
[4] B. Blasius, A. Huppert, and L. Stone, "Complex dynamics and phase synchronization in spatially extended ecological systems," *Nature*, vol. 399, pp. 354–359, 1999.
[5] T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comp. Cog.*, vol. 2, pp. 81–130, 2004.
[6] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp. 980–994, 1995.
[7] R. Mainieri and J. Rehacek, "Projective synchronization in three-dimensional chaotic systems," *Phys. Rev. Lett.*, vol. 82, pp. 3042–3045, 1999.
[8] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "From phase to lag synchronization in coupled chaotic oscillators," *Phys. Rev. Lett.*, vol. 78, pp. 4193–4196, 1997.
[9] H. U. Voss, "Anticipating chaotic synchronization," *Phys. Rev. E*, vol. 61, pp. 5115–5119, 2000.
[10] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "Phase synchronization of chaotic oscillators," *Phys. Rev. Lett.*, vol. 76, pp. 1804–1807, 1996.
[11] T. M. Hoang and M. Nakagawa, "Projective-lag synchronization of coupled multidelay feedback systems," *J. Phys. Soc. Jpn.*, vol. 75, pp. 094801.1–094801.6, 2006.
[12] T. M. Hoang and M. Nakagawa, "Anticipating and projective–anticipating synchronization of coupled multidelay feedback systems," *Phys. Lett. A*, vol. 365, pp. 407–411, 2007.
[13] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.
[14] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *Int. J. Bifur. Chaos*, vol. 2, pp. 973–977, 1992.
[15] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communication using chaos–Part I: Fundamentals of digital communications," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 927–936, 1997.
[16] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using seft-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634–642, 1993.
[17] T. M. Hoang and M. Nakagawa, "New encoding model for chaos-based secure communication," *J. Phys. Soc. Jpn.*, vol. 75, pp. 034801.1–034801.10, 2006.
[18] J. D. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, vol. 4, pp. 366–393, 1982.
[19] K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," *Phys. Rev. E*, vol. 58, pp. 1159–1162, 1998.
[20] T. M. Hoang, D. T. Minh, and M. Nakagawa, "Synchronization of multi-delay feedback systems with multi-delay driving signal," *J. Phys. Soc. Jpn.*, vol. 74, pp. 2374–2378, 2005.
[21] N. N. Krasovskii, *Stability of Motion*. Standford: Standford University Press, 1963.
[22] J. K. Hale and S. M. V. Lunel, *Introduction to Functional Differential Equations*. New York: Springer, 1993.
[23] G. Perez and H. A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, pp. 1970–1973, 1995.
[24] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 1062–1067, 1998.
[25] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic secure communication using a spectrogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998.
[26] T. Yang, "Recovery of digital signals from chaotic switching," *Int. J. Circuit Theory & Applications*, vol. 23, pp. 611–615, 1995.
[27] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking two secure communication systems based on chaotic masking," *IEEE Trans. Circuits Syst. II*, vol. 51, pp. 505–506, 2004.
[28] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value," *Chaos, Solitons and Fractals*, vol. 23, pp. 1749–1756, 2005.
[29] G. Álvarez and S. Li, "Breaking network security based on synchronization chaos," *Computer Communication*, vol. 27, pp. 1679–1681, 2004.
[30] S. Li, G. Álvarez, and G. Chen, "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos, Solitons and Fractals*, vol. 25, pp. 109–120, 2005.
[31] S. Li, G. Álvarez, G. Chen, and X. Mou, "Breaking a chaos-noise-based secure communication scheme," *Chaos*, vol. 15, pp. 013703.1–013703.10, 2005.
[32] T. M. Hoang and M. Nakagawa, "Enhancing security for chaos-based communication system with change in synchronization manifolds' delay and in encoder's parameters," *J. Phys. Soc. Jpn.*, vol. 75, pp. 064801.1–064801.12, 2006.

Thang Manh Hoang received the B.S. and M.S. degrees in Electronics and Telecommunications from Hanoi University of Technology in 1998 and in 2001, respectively. During 1998-2004, he had stayed with Faculty of Electronics and Telecommunications, Hanoi University of Technology. He received a PhD degree in 2007, from Department of Electrical Engineering, Nagaoka University of Technology, Japan. Now, he is the assistant professsor at Department of Electronics and Informatics, Faculty of Electronics and Telecommunications, Hanoi University of Technology, Hanoi, Vietnam.