International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 7, November-December 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Design of Chaotic Secure Communication System Based on Laser Dynamic Model

Yeong-Jeu Sun[1], Che-Ming Chuang[2], Ting-Chia Chang[2]

[1]Professor, [2]Postgraduate,

[1,2]Department of Electrical Engineering, I-Shou University, Kaohsiung, Taiwan, China

ABSTRACT

In this paper, a novel master-slave secure communication system will be proposed and explored. Based on the state estimator of the laser dynamic system, a new type of chaotic secure communication system will be designed. This secure communication system can not only achieve global exponential tracking, but also accurately calculate the exponential convergence rate. Finally, several numerical simulation results will be provided to demonstrate the correctness and practicality of the main theorem.

KEYWORDS: *Laser dynamic mode, secure communication system, master-slave system, secure communication system, exponential tracking*

How to cite this paper: Yeong-Jeu Sun | Che-Ming Chuang | Ting-Chia Chang "Design of Chaotic Secure Communication System Based on Laser Dynamic Model" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-7, December 2022, pp.370-373, URL: www.ijtsrd.com/papers/ijtsrd52298.pdf

IJTSRD52298

1. INTRODUCTION

In recent years, various theories and designs of secure communication systems have been proposed by many researchers; see, for example, [1]-[6] and the references therein. As we know, secure communication is not only rooted in theoretical basis, but more importantly, it strengthens the security function of the actual communication system.

On the other hand, laser dynamic systems occasionally produce chaotic phenomena; at the same time, the design of their state estimators is quite challenging. The state estimator design has been proposed in [9] to ensure global exponential synchronization for the fifth-order laser dynamic model.

This paper will use the chaotic characteristics of the laser dynamic system to design a new master-slave chaotic secure communication system. Based on the control theory, it is deduced that such a secure communication system can achieve the goal of global exponential tracking. Besides, the guaranteed exponential convergence rate of this secure communication system will be calculated simultaneously. Finally, several computer simulation results will demonstrate the effectiveness of this main theorem. In particular, throughout the paper, $\|x\| := \sqrt{x^T \cdot x}$ represents the Euclidean norm of the column vector x, and $|a|$ represents the absolute value of a real number a.

2. PROBLEM FORMULATION AND MAIN RESULTS

First, we propose a new master-slave secure communication system, and its architecture diagram is shown in Figure 1.

Master System:

$$\dot{x}_1 = -c_1 x_1 - c_1 c_2 x_2 + c_1 x_3, \quad (1a)$$

$$\dot{x}_2 = c_1 c_2 x_1 - c_1 x_2 + c_1 x_4, \quad (1b)$$

$$\dot{x}_3 = c_3 x_1 - x_3 + c_2 x_4 - x_1 x_5, \quad (1c)$$

$$\dot{x}_4 = c_3 x_2 - c_2 x_3 - x_4 - x_2 x_5, \quad (1d)$$

$$\dot{x}_5 = -c_4 x_5 + x_1 x_3 + x_2 x_4 , \quad (1e)$$

$$y_1(t) = c_5 x_3(t) + c_6 x_4(t), \quad (1f)$$

$$y_2(t) = c_7 x_3(t) + c_8 x_4(t), \quad (1g)$$

$$\phi(t) = Dx(t) + m_1(t), \forall t \ge 0. \quad (1h)$$

Slave System:

$$\dot{z}_1 = -c_1 z_1 - c_1 c_2 z_2 + \frac{c_1 \alpha_8 y_1 - c_1 \alpha_6 y_2}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7}, \quad (2a)$$

$$\dot{z}_2 = c_1 c_2 z_1 - c_1 z_2 + \frac{c_1 \alpha_5 y_2 - c_1 \alpha_7 y_1}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7}, \quad (2b)$$

$$z_3 = \frac{\alpha_8}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7} y_1 - \frac{\alpha_6}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7} y_2 , \quad (2c)$$

$$z_4 = \frac{-\alpha_7}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7} y_1 + \frac{\alpha_5}{\alpha_5 \alpha_8 - \alpha_6 \alpha_7} y_2 , \quad (2d)$$

$$\dot{z}_5 = -c_4 z_5 + z_1 z_3 + z_2 z_4 , \quad (2e)$$

$$m_2(t) = \phi(t) - Dz(t), \forall t \ge 0, \quad (2f)$$

where $x(t) := [x_1(t) \quad x_2(t) \quad x_3(t) \quad x_4(t) \quad x_5(t)]^T \in \Re^{5\times 1}$ is state vector of the master system, $y(t) \in [y_1(t) \quad y_2(t)] \in \Re^{2\times 1}$ is output vector of the master system, $z(t) := [z_1(t) \quad z_2(t) \quad z_3(t) \quad z_4(t) \quad z_5(t)]^T \in \Re^{5\times 1}$ is state vector of the slave system, $D \in \Re^{1\times 5}$ is the two-party confidentiality matrix, and $c_1, c_2, \cdots, c_8$ are the parameters of the system, with $c_1 > 0$, $c_4 > 0$, $c_1 \ne c_4$, and $c_5 c_8 \ne c_6 c_7$. Besides, $m_1(t)$ is the information vector, $m_2(t)$ is the signal recovered from $m_1(t)$, and we assume that the signals of $x_3(t)$ and $x_4(t)$ are bounded.

Remark 1: It is noted that the master system is a fifth-order laser dynamic system, and when the parameters of the system (1) are the following values, chaos will occur in the main system [7-9]: $c_1 = 2, c_2 = 0.002, c_3 = 20,$ and $c_4 = 0.25$.

As we all know, a high-quality master-slave secure communication system should at least make the error signal $\tilde{e}(t) = m_2(t) - m_1(t)$ approach zero in some sense. A definition related to the master-slave secure communication system is introduced as follows.

Definition 1 [10]: The master-slave system (1) with (2) is called secure communication system with exponential convergence type if there are positive numbers k and α such that, for every $t \ge 0$,

$$|\tilde{e}(t)| = |m_2(t) - m_1(t)| \le k \exp(-\alpha t). \quad (3)$$

In this situation, the positive number α is called the exponential convergence rate.

The main theorem of this paper is presented below.

Theorem 1: The system (1) with (2) is a secure communication system with exponential convergence type. Meanwhile, the guaranted exponential convergence rate is given by $\alpha := \min\{c_1, c_4\}$.

Proof. Define $M \ge |x_i(t)|, \forall i \in \{3,4\}$ and

$$e_i(t) := x_i(t) - z_i(t), \quad \forall i \in \{1,2,3,4,5\}. \quad (4)$$

Thus, one has, for every $t \ge 0$,

$$|e_i(t)| \le e^{-c_1 t} \sqrt{e_1^2(0) + e_2^2(0)}, \forall i \in \{1,2\}; \quad (5a)$$

$$e_3(t) = e_4(t) = 0; \quad (5b)$$

$$|e_5(t)| \le \left[\frac{4M\sqrt{e_1^2(0) + e_2^2(0)}}{|c_4 - c_1|} + |e_5(0)| \right] e^{-\min\{c_1, c_4\} t}, \quad (5c)$$

in view of the Theorem 1 of [9]. It can be readily obtained that

$$\begin{aligned} |\tilde{e}(t)| &= |m_2(t) - m_1(t)| \\ &= |\phi(t) - Dz(t) - \phi(t) + Dx(t)| \\ &= |D[x(t) - z(t)]| \\ &\le \|D\| \times \\ &\quad \left\| [e_1(t) \quad e_2(t) \quad e_3(t) \quad e_4(t) \quad e_5(t)]^T \right\| \\ &\le k \cdot e^{-\alpha t}, \forall t \ge 0, \end{aligned}$$

where

$$k = \|D\| \times \sqrt{e_1^2(0) + e_2^2(0) + \left[\frac{4M\sqrt{e_1^2(0) + e_2^2(0)}}{|c_4 - c_1|} + |e_5(0)| \right]^2},$$

and $\alpha = \min\{c_1, c_4\}$, in view of (1)-(5). This completes the proof.

3. NUMERICAL SIMULATIONS

Consider the master-slave secure communication system of (1) and (2) with

$$c_1 = 2, c_2 = 0.002, c_3 = 20, \ c_4 = 0.25, \quad (6a)$$

$$c_5 = 2, \ c_6 = c_7 = -1, \ c_8 = 1, \quad (6b)$$

and $D = [0.1 \quad 0.1 \quad -0.5 \quad -0.4 \quad 0]$. (6c)

According to Theorem 1, this secure communication system (1), (2) with (6) can not only make the signals $m_1(t)$ and $m_2(t)$ achieve global exponential synchronization targets, but also the guaranteed exponential convergence rate can be calculated as $\alpha = 0.25$. Furthermore, the signals $m_1(t)$, $m_2(t)$ and the error signal $m_2(t) - m_1(t)$ are shown in Figures 2 to 4, respectively, and from Figure 4, it can be known that the signals $m_1(t)$ and $m_2(t)$ can be synchronized after about 5 seconds.

4. CONCLUSION

In this paper, a new master-slave secure communication system has been proposed and investigated. Based on the state estimator of the laser dynamic system, a novel type of chaotic secure communication system has been designed. This secure communication system can not only achieve global exponential tracking, but also accurately calculate the exponential convergence rate. Finally, several numerical simulation results have been presented to show the correctness and practicality of the main theorem.

ACKNOWLEDGEMENT

The authors thank the Ministry of Science and Technology of Republic of China for supporting this work under grant MOST 109-2221-E-214-014.

REFERENCES

[1] X. Liu, C. Li, S. S. Ge, and D. Li, "Time-synchronized control of chaotic systems in secure communication," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 9, pp. 3748- 3761, 2022.

[2] Y. Xu, "Resilient secure control of networked systems over unreliable communication networks," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 4069-4077, 2022.

[3] J. C. L. Chan, T. H. Lee, and C. P. Tan, "Secure communication through a chaotic system and a sliding-mode observer," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 3, pp. 1869-1881, 2022.

[4] M. Iqbal, L. Velasco, N. Costa, A. Napoli, J. Pedro, and M. Ruiz, "LPsec: a fast and secure cryptographic system for optical connections," Journal of Optical Communications and Networking, vol. 14, no. 4, pp. 278-288, 2022.

[5] P. Angueira, I. Val, J. Montalbán, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 810-838, 2022.

[6] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2704-2713, 2022.

[7] R. Gilmore and C. Letellier, "The Symmetry of Chaos," Oxford University Press, New York, 2007.

[8] H. Zeghlache and P. Mandel, "Influence of detuning on the properties of laser equations," Journal of Optical Society of America B, vol. 2, pp. 18-22, 1985.

[9] Y. J. Sun, C. M. Chuang, and S. C. Chen, "A nonlinear state estimator design of the laser dynamic system," International Journal of Trend in Scientific Research and Development, vol. 6, no. 6, pp. 2109-2112, 2022.

[10] Y. J. Sun, "An exponential observer design for a class of chaotic systems with exponential nonlinearity," International Journal of Trend in Scientific Research and Development, vol. 5, no. 1, pp. 1550-1552, 2020.

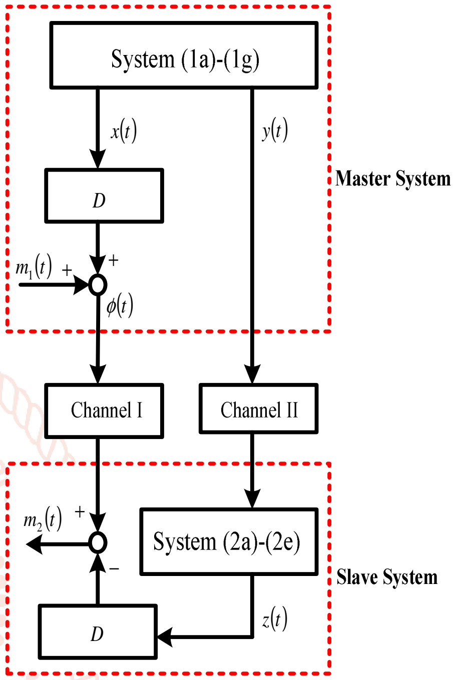

Figure 1: Architecture diagram of secure communication system.

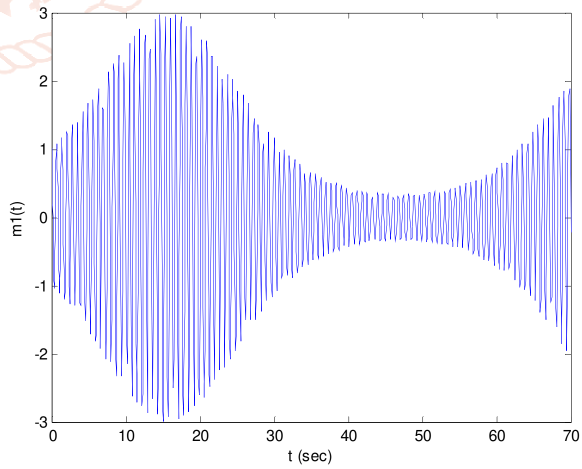

Figure 2: Real message of $m_1(t)$ described in the master system of (1).

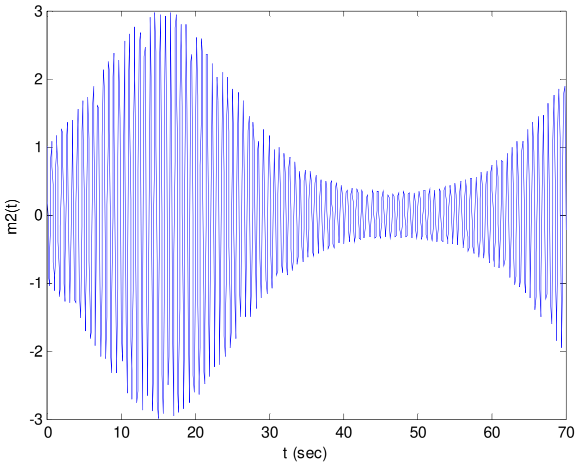

Figure 3: Recoverd message of $m_2(t)$ described in the slave system of (2).

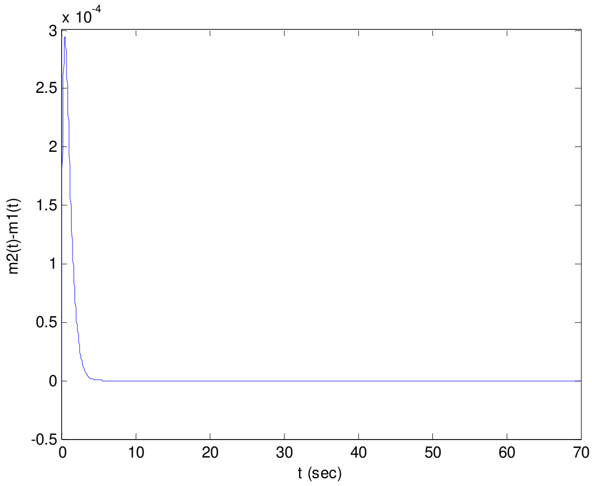

Figure 4: Error signal of $m_2(t)-m_1(t)$.