Hindawi Publishing Corporation
Journal of Control Science and Engineering
Volume 2015, Article ID 471913, 7 pages
http://dx.doi.org/10.1155/2015/471913

Research Article

Chaotic Secure Communication Systems with an Adaptive State Observer

Wei-Der Chang, Shun-Peng Shih, and Chih-Yung Chen

Department of Computer and Communication, Shu-Te University, Kaohsiung 824, Taiwan

Correspondence should be addressed to Wei-Der Chang; wdchang@stu.edu.tw

Received 8 November 2014; Accepted 23 March 2015

Academic Editor: Lifeng Ma

This paper develops a new digital communication scheme based on using a unified chaotic system and an adaptive state observer. The proposed communication system basically consists of five important elements: signal modulation, chaotic encryption, adaptive state observer, chaotic decryption, and signal demodulation. A sequence of digital signals will be delivered from the transmitter to the receiver through a public channel. It is rather reasonable that if the number of signals delivered on the public channel is fewer, then the security of such communication system is more guaranteed. Therefore, in order to achieve this purpose, a state observer will be designed and its function is to estimate full system states only by using the system output signals. In this way, the signals delivered on the public channel can be reduced mostly. According to these estimated state signals, the original digital sequences are then retrieved completely. Finally, experiment results are provided to verify the applicability of the proposed communication system.

1. Introduction

Over the past two decades, a large number of researches regarding chaotic systems and their related applications have successively been proposed and developed. One of them is about the chaotic secure communication [1–12]. Chaos synchronization that was initially proposed by Pecora and Carroll in [13] is the important factor to achieve the security. For the general chaotic secure communication, the first step is to encrypt the signal which will be delivered. The commonly used scheme is to directly mask the delivered signal by a chaotic state variable. This encrypted signal is then transmitted to the receiver through an open public channel where some information is probably stolen by hacker. When the receiver gets the encrypted signal, certain decryption mechanism is utilized such that the delivered signal can be completely recovered. Once the encrypted signal was stolen on the public channel, it is still difficult to recover the actual signal because of the unpredictable nature of chaotic states and without a corresponding decryption method. Therefore, the secure communication based on chaotic systems can be achieved. In [1], the authors proposed a chaotic secure communication method for analog signal transmission in which the unified chaotic system is used to encrypt the emitted signal and the useful information is embodied into the system parameter. In order to synchronize two identical chaotic systems with matched and mismatched perturbations, an adaptive sliding mode control (ASMC) technique was developed based on using the Lyapunov stability theorem and linear matrix inequality method [7]. The proposed chaotic synchronization is successfully applied to the secure communication. Furthermore, a new technique to securely transmit and retrieve a message signal was presented via chaotic systems [10]. The message signal is particularly encrypted in the frequency of a sinusoidal term, and therefore a novel frequency estimator is developed for retrieving the message to achieve the secure communication.

In the recent years, many researchers focus on the research topic regarding the system observer design. It can widely be used in numerous areas such as the chaos control [14–16], adaptive synchronization [9, 17], and analog chaotic

secure communication [18, 19]. It is well known that the purpose of state observer is to provide the estimates for full system states only using fewer output signals which are available for measurement. Thus, the state observer is rather suitable to be applied in most of chaotic secure communication systems because the information of full state signals is often needed in the chaotic decryption mechanism. By the use of the state observer, the number of signals delivered through the public channel can be greatly decreased in order to further guarantee the security. In [14], the authors developed an adaptive observer-based control for a class of chaotic systems. Based on the obtained state estimates, a nonlinear state feedback controller is then constructed for chaotic systems. In [17], a robust adaptive sliding mode observer-based response system was presented to synchronize a given chaotic system without the knowledge of upper bounds of uncertainties and unknown inputs. By the concept of equivalent control signal, the unknown inputs can be directly recovered. Moreover, an analog chaotic secure communication system was proposed based on the synchronization of uncertain chaotic systems with observers. Lur'e chaotic system is illustrated to demonstrate the effectiveness of the proposed system [18].

This paper will develop another new chaotic secure communication system especially for digital signal transmissions. An adaptive state observer to chaotic systems is applied. In the previous work [12], a particular chaotic system called the unified system has been utilized to the design of digital secure communication system. Under the proposed structure, in the decryption mechanism it requests the information of all the chaotic states. Thus, full state signals need to be delivered from the transmitter to the receiver via a public channel in order to achieve the secure communication. In this paper, we extend this kind of digital communication system by adding the design of an adaptive state observer. The observer is located at the front of the receiver. Under the proposed system construction, only partial system information, not full state signals, is requested to be delivered. The adaptive state observer can solve for all the state estimates according to the partial information, and they will be used in the chaotic decryption method instead of original real state signals. As a result, the total of delivered signals on the public channel is decreased to further improve the security of the communication system. The proposed digital communication system contains five main components including the signal modulation, chaotic encryption, adaptive state observer, chaotic decryption, and signal demodulation. Each of them will be clearly explained in the following sections. The remainder of this paper is organized as follows. Section 2 will give the complete system descriptions for the adaptive state observer design. In Section 3, the chaotic encryption and corresponding decryption method based on using the unified system are addressed. A complete communication system for digital signal transmissions is clearly presented in Section 4. Section 5 demonstrates experiment results to validate the efficiency of the proposed digital communication system. Finally, a brief conclusion is stated in Section 6.

2. System Description for an Adaptive State Observer

Let us consider a class of continuous-time chaotic systems by the following dynamical equations:

$$\dot{x} = Ax + Bf(x), \tag{1a}$$

$$y = Cx, \tag{1b}$$

where $x \in R^n$ is the vector of system states, $y \in R^q$ denotes the vector of measurable output signals which includes only partial information of states, $f(\cdot)$ is the nonlinear function vector, and A, B, and C are the known matrices with compatible dimensions. Equations (1a) and (1b) can represent some chaotic systems such as Lorenz, Chen, and unified systems with different matrices A, B, and C. If we want to design an adaptive state observer for such a chaotic system of (1a) and (1b), the following assumption is required [14].

Assumption 1. There exist a matrix L and positive matrices P and Q such that the following two equalities are satisfied:

$$\begin{aligned} P(A - LC) + (A - LC)^T P &= -Q, \\ B^T P &= C. \end{aligned} \tag{2}$$

If the system of (1a) and (1b) satisfies this assumption, then an adaptive state observer to estimate the full system states can be designed as

$$\dot{\hat{x}} = A\hat{x} + Bf(\hat{x}) + u, \tag{3a}$$

$$\hat{y} = C\hat{x}, \tag{3b}$$

where $\hat{x}$ is the estimate of the state vector x, $\hat{y}$ is the estimate of the output vector y, and u is the external control input that needs to be designed. According to the results of [14], if we choose

$$u = \frac{1}{2}\phi B(y - \hat{y}), \tag{4a}$$

$$\dot{\phi} = l\|y - \hat{y}\|^2, \tag{4b}$$

where l is a positive constant, then the estimate $\hat{x}$ of the state observer can approximate the state vector x of (1a) and (1b) asymptotically. It means that the full system states are obtained only by the output signal y. Figure 1 displays a simple illustration for such a state observer design.

3. Chaotic Encryption and Decryption

In the secure communication, it often requires certain encryption mechanisms to encrypt the actual information for the security. In this study, a special chaotic system which is

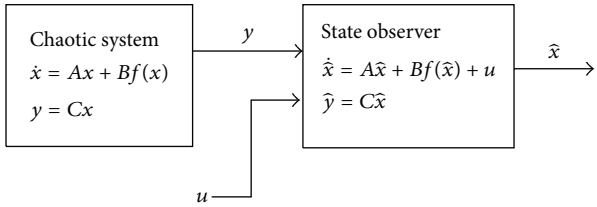

Figure 1: Adaptive state observer design.

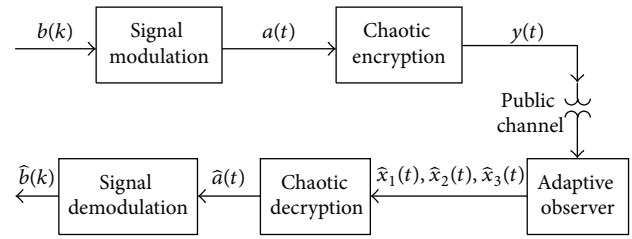

Figure 2: The proposed chaotic secure communication system.

called the unified system is utilized to be an encrypting tool. It can be expressed by

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -25a - 10 & 25a + 10 & 0 \\ 28 - 35a & 29a - 1 & 0 \\ 0 & 0 & -\dfrac{a+8}{3} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \tag{5}$$

where x_1, x_2, and x_3 are the states of the chaotic system and $a \in [0, 1]$ is an important chaotic parameter that controls its chaotic type; for example, if $a \in [0, 0.8)$, then the system belongs to the Lorenz system; if $a = 0.8$, then the system is the Lü system; if $a \in (0.8, 1]$, then the system belongs to Chen's system. Regardless of variation of parameter a, the chaotic behavior of (5) still holds. Due to such a characteristic, this kind of chaotic system is suitably applied to the secure communication. In this study, the useful information that will be delivered is directly regarded as the chaotic parameter a. The transmitter further sends these three system states to the receiver through an open channel in which the signals sent probably are caught. Even if these signals are stolen, the actual information a is still undiscovered. This is the advantage of chaotic secure communication. At the receiver, a decryption method is taken to recover the useful information according to the following adaptive laws [1, 12]:

$$\dot{\theta} = -r\frac{x_1 x_2}{x_3} + r\beta, \tag{6a}$$

$$\beta = -0.5r \ln x_3^2 - \theta, \tag{6b}$$

$$\hat{a} = 3\beta - 8, \tag{6c}$$

where r is a positive constant controlling the convergence speed and $\hat{a}$ is the recovered information for a. From (6a), (6b), and (6c), it is clear that the signals required in the decryption are all of the system states x_1, x_2, and x_3. In this study, we attempt to reduce the number of delivered signals on the public channel by introducing a state observer design as shown in Section 2. The security will be prompted because of fewer delivered signals. The state observer of (3a) and (3b) with the control input of (4a) and (4b) is designed at the front of the receiver in order to derive all estimates of system states. From (4a) and (4b), we know that the signals delivered on the channel are only the chaotic output y, not full system states. The estimated states then take the place of the real system states used in (6a) and (6b).

4. Digital Secure Communication System

Figure 2 displays an adaptive state observer-based digital chaotic communication system in which five main components are included: signal modulation, chaotic encryption, adaptive state observer, chaotic decryption, and signal demodulation, respectively. In the proposed communication system, $b(k)$, $k = 0, 1, 2, \ldots$, is a series of digital sequences that will be delivered, $a(t)$ is a continuous carrier signal obtained from the signal modulation method, and this signal is taken to be the chaotic parameter of the unified system as described in (5) to achieve the chaotic encryption, $y(t)$ is the measurable output signal that contains only partial information of states, $\hat{x}_1(t)$, $\hat{x}_2(t)$, and $\hat{x}_3(t)$ produced by an adaptive state observer are the estimates of chaotic states, respectively, $\hat{a}(t)$ is then the decrypted signal for a, and the recovered digital sequence $\hat{b}(k)$ will eventually be obtained after executing certain demodulation method. In the following subsections, we introduce the detailed descriptions for signal modulation, modified chaotic decryption, and signal demodulation.

4.1. Signal Modulation. In the proposed communication system, a digital sequence $b(k)$ must initially be transformed into a continuous signal to meet the chaotic system behavior. In order to achieve this, each bit of $b(k)$ is necessarily modulated as a continuous-time carrier signal with N periods and this carrier signal is requested to satisfy the condition $a(t) \in [0, 1]$ as well. Thus, the following modulation technology is adopted [12]:

$$a(t) = \begin{cases} 0.5 + 0.5\cos\dfrac{2\pi}{T}t, & \text{if } b(k) = 1, \\ 0.5 - 0.5\cos\dfrac{2\pi}{T}t, & \text{if } b(k) = 0, \end{cases} \tag{7}$$

where $kNT \le t < (k+1)NT$, for $k = 0, 1, 2, \ldots$, and T is the period of the carrier signal.

4.2. Modified Chaotic Decryption. We have clearly addressed the design method of an adaptive state observer for a class

of chaotic systems in Section 2. According to the proposed method, the chaotic decryption of (6a), (6b), and (6c) should be modified as

$$\dot{\theta} = -r\frac{\widehat{x}_1\widehat{x}_2}{\widehat{x}_3} + r\beta, \tag{8a}$$

$$\beta = -0.5r\ln\widehat{x}_3^2 - \theta, \tag{8b}$$

$$\widehat{a} = 3\beta - 8, \tag{8c}$$

where $\widehat{x}_1$, $\widehat{x}_2$, and $\widehat{x}_3$ are the observer outputs and also the estimates of system states x_1, x_2, and x_3, respectively, and $\widehat{a}$ is the decrypted carrier signal for a.

4.3. Signal Demodulation. After obtaining the carrier signal $\widehat{a}$, a signal demodulation method is executed to retrieve the original digital sequence. According to (7), it is reasonable to choose $c(t) = 0.5 + 0.5\cos(2\pi/T)t$ as a reference level signal. Once the difference between the reference signal $c(t)$ and decrypted signal $\widehat{a}(t)$ approaches zero, it means that the bit recovered is $\widehat{b}(k) = 1$. Conversely, if the difference is close to the value $\cos(2\pi/T)t$, we obtain $\widehat{b}(k) = 0$. Based on these inferences, the signal demodulation method can be defined by [12]

$$\widehat{b}(k) = \begin{cases} 1, & \text{if } \displaystyle\int_{kNT}^{(k+1)NT} |c(t) - \widehat{a}(t)|\,dt \le \frac{NT}{\pi}, \\ 0, & \text{if } \displaystyle\int_{kNT}^{(k+1)NT} |c(t) - \widehat{a}(t)|\,dt > \frac{NT}{\pi}, \end{cases} \quad \text{for } k = 0, 1, 2, \ldots. \tag{9}$$

This is due to $\int_{kNT}^{(k+1)NT} |c(t) - \widehat{a}(t)|dt \approx \int_{kNT}^{(k+1)NT} |c(t) - a(t)|dt = \int_{kNT}^{(k+1)NT} |\cos(2\pi/T)t|dt = 2NT/\pi$, and we choose one half of this value, NT/π, as a reference for demodulation.

5. Experiment Results

In this section, some computer simulations are provided to verify feasibility of the proposed digital communication system. In the simulation, the initial conditions of the unified system are given by $(x_1(0), x_2(0), x_3(0)) = (1, 1, -1)$. Besides, for meeting the form of the observer design, another output equation should be incorporated to the original unified chaotic system (5) as (10b):

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -25a - 10 & 25a + 10 & 0 \\ 28 - 35a & 29a - 1 & 0 \\ 0 & 0 & -\dfrac{a+8}{3} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -x_1x_3 \\ x_1x_2 \end{bmatrix}, \tag{10a}$$

$$y = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \tag{10b}$$

Hence, in comparison with (1a) and (1b), we have

$$A = \begin{bmatrix} -25a - 10 & 25a + 10 & 0 \\ 28 - 35a & 29a - 1 & 0 \\ 0 & 0 & -\dfrac{a+8}{3} \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad f(x) = \begin{bmatrix} -x_1x_3 \\ x_1x_2 \end{bmatrix}. \tag{11}$$

For the adaptive state observer design, we give the initial conditions $(\widehat{x}_1(0), \widehat{x}_2(0), \widehat{x}_3(0)) = (2, 2, 1)$ and the constant in the adaptive law (4b) is simply set to $l = 1$ for simulations.

The software of Borland C++ 5.02 is utilized to program the computer codes of the proposed communication system under the environment of Pentium(R) 4 CPU 2.0 GHz. Simulation results are demonstrated in Figures 3–9. In Figures 3–5, they show the comparisons between the actual chaotic states and the corresponding estimates for x_1, x_2, and x_3, respectively. It is obvious from these figures that the adaptive state observer can exactly and quickly estimate the system states in a short time. These states obtained are then used in the modified chaotic encryption of (8a), (8b), and (8c) to get the decrypted carrier signal. Here, we want to further evaluate the system performance by testing different values of r in the chaotic decryption of (8a), (8b), and (8c). Figures 6–8 display the comparison between the actual carrier signal a and the decrypted carrier signal $\widehat{a}$ for $r = 1$, $r = 5$, and $r = 10$, respectively. As expected, it is concluded that a large value for r can derive a better and more exact decrypted carrier signal. Furthermore, based on these resulting carrier signals, the digital signal sequence can be solved by the proposed demodulation method of (9). Simulation results

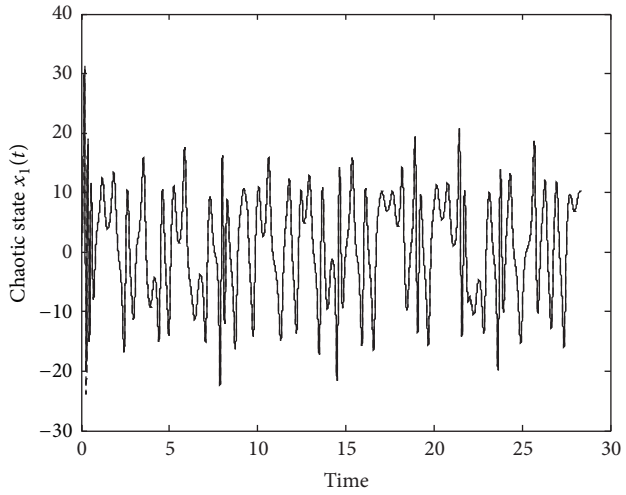

Figure 3: Actual chaotic state x_1 (dashed line) and its estimate $\widehat{x}_1$ (solid line).

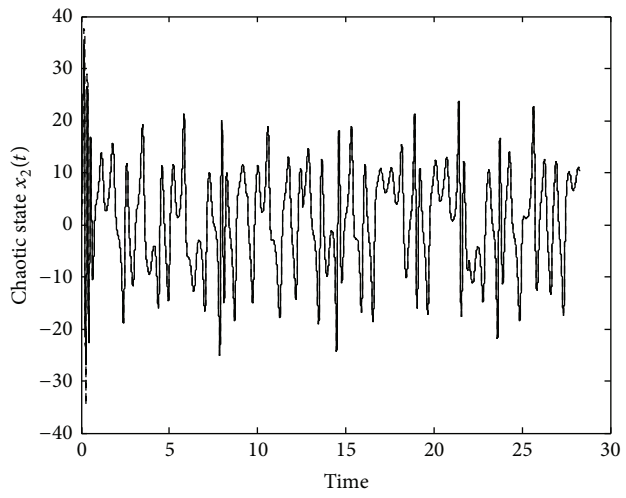

Figure 4: Actual chaotic state x_2 (dashed line) and its estimate $\widehat{x}_2$ (solid line).

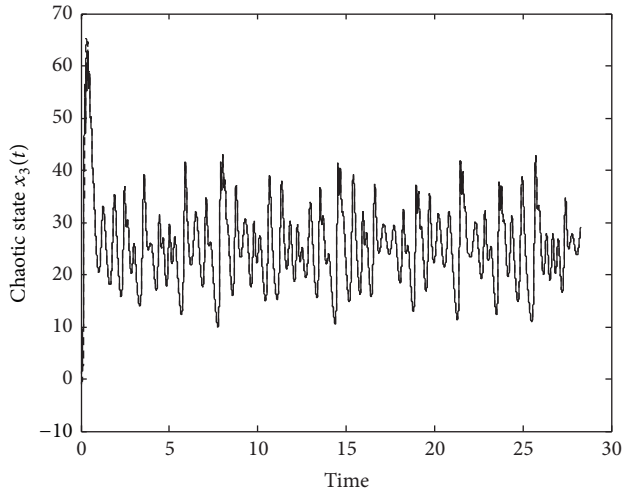

Figure 5: Actual chaotic state x_3 (dashed line) and its estimate $\widehat{x}_3$ (solid line).

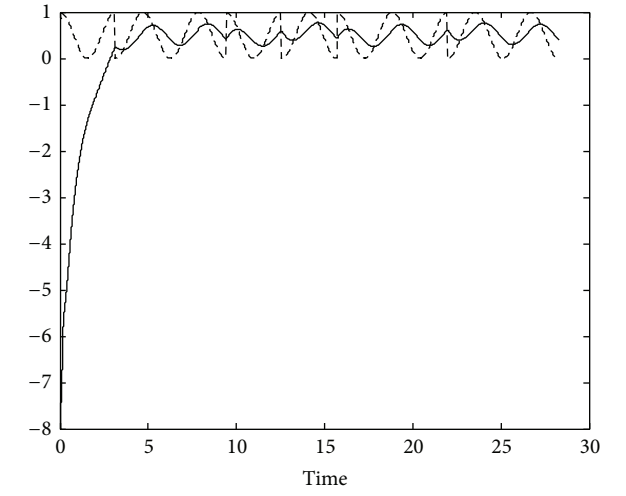

Figure 6: Actual carrier signal a (dashed line) and decrypted carrier signal $\widehat{a}$ (solid line) when $r = 1$.

are shown in Figure 9. All of transmitted digital sequences for any r are completely solved except for the first delivered bit. As a comparison, the design methods presented in [1] and [12], respectively, still request full state signals of the unified chaotic system to fulfill the analog and digital signal communication. Figure 10 displays the simulation results by the method of [12] which needs the full system states. It is clearly seen from Figures 9 and 10 that both results are the same for recovered digital signals. However, the proposed communication structure in this paper can use fewer delivered signals to achieve the same work due to the consideration of an adaptive state observer. From simulation results and comparison descriptions, it is concluded that the superiority and applicability of the proposed scheme can be verified.

6. Conclusion and Future Work

For the digital signal transmissions, this paper has successfully developed a new chaotic communication system combined with an adaptive state observer. The purpose of the observer is to estimate the full system states only from the measurable output signal. These state signals estimated further replace the original system states in the decryption method. In this way, the number of delivered signals on the public channel can be reduced to guarantee more the communication security. Simulation results sufficiently reveal that the proposed communication system is satisfied in the digital sequence transmissions.

In the future study, the proposed communication system is probably combined with the data-driven and/or data-based techniques [20–22]. The core of data-based scheme is to take full advantage of the huge amounts of available process

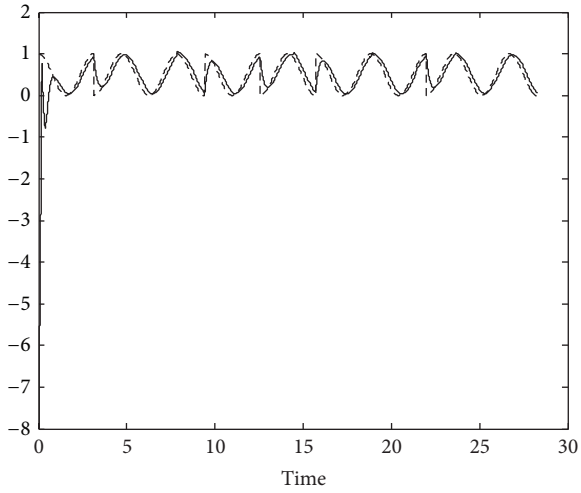

Figure 7: Actual carrier signal a (dashed line) and decrypted carrier signal $\widehat{a}$ (solid line) when $r = 5$.

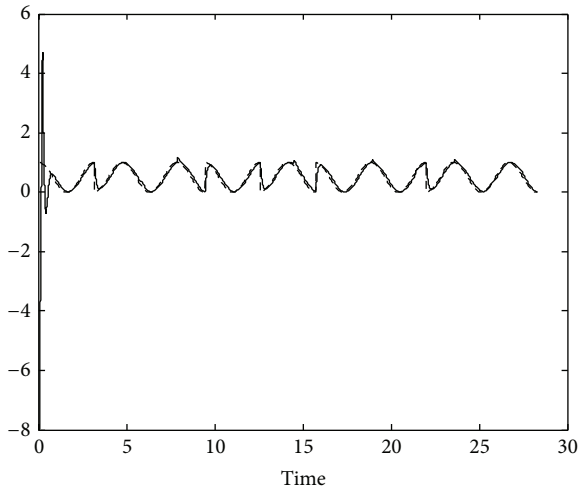

Figure 8: Actual carrier signal a (dashed line) and decrypted carrier signal $\widehat{a}$ (solid line) when $r = 10$.

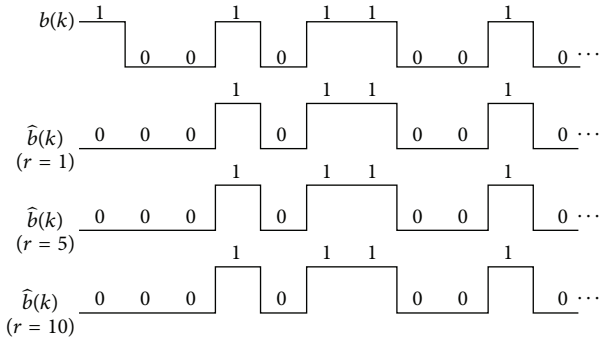

Figure 9: The recovered digital sequences for $r = 1$, $r = 5$, and $r = 10$, respectively, by the proposed demodulation method.

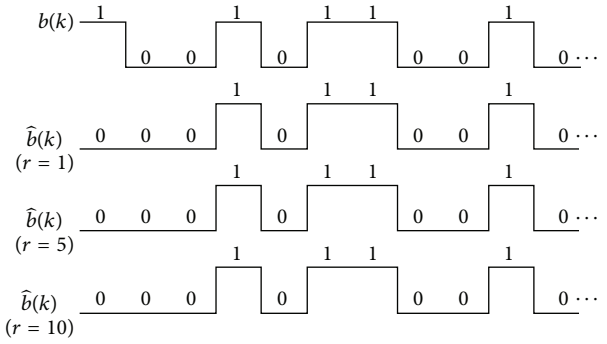

Figure 10: The recovered digital sequences for $r = 1$, $r = 5$, and $r = 10$, respectively, by the method of [12].

data, aiming to acquire the useful information within. The data-based scheme provides efficient alternative solutions to different industrial issues under various operating conditions [20]. Besides, the data-driven method is an alternative way to obtain the process model from the process history data, which is simpler than constructing the process model. The connection between the proposed communication system with the data-driven and data-based schemes may be further made in our future work.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was partially supported by the Ministry of Science and Technology of Taiwan under Grants nos. MOST 103-2221-E-366-004 and MOST 103-2632-E-366-001.

References

[1] C. Hua, B. Yang, G. Ouyang, and X. Guan, "A new chaotic secure communication scheme," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 342, no. 4, pp. 305–308, 2005.

[2] X.-L. An, J.-N. Yu, Y.-Z. Li, Y.-D. Chu, J.-G. Zhang, and X.-F. Li, "Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation," *Mathematical and Computer Modelling*, vol. 54, no. 1-2, pp. 7–18, 2011.

[3] Y.-C. Hung, T.-L. Liao, and J.-J. Yan, "Adaptive variable structure control for chaos suppression of unified chaotic systems," *Applied Mathematics and Computation*, vol. 209, no. 2, pp. 391–398, 2009.

[4] X. Yang, Z. Yang, and X. Nie, "Exponential synchronization of discontinuous chaotic systems via delayed impulsive control and its application to secure communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 5, pp. 1529–1543, 2014.

[5] Y. Ji, C. Wen, and Z. G. Li, "Chaotic communication systems in the presence of parametric uncertainty and mismatch,"

International Journal of Communication Systems, vol. 21, no. 11, pp. 1137–1154, 2008.

[6] B. Jovic, C. P. Unsworth, G. S. Sandhu, and S. M. Berber, "A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems," *Signal Processing*, vol. 87, no. 7, pp. 1692–1708, 2007.

[7] C.-C. Cheng, Y.-S. Lin, and S.-W. Wu, "Design of adaptive sliding mode tracking controllers for chaotic synchronization and application to secure communications," *Journal of the Franklin Institute*, vol. 349, no. 8, pp. 2626–2649, 2012.

[8] M. F. Hassan, "Observer design for constrained nonlinear systems with application to secure communication," *Journal of the Franklin Institute. Engineering and Applied Mathematics*, vol. 351, no. 2, pp. 1001–1026, 2014.

[9] A. Abdullah, "Synchronization and secure communication of uncertain chaotic systems based on full-order and reduced-order output-affine observers," *Applied Mathematics and Computation*, vol. 219, no. 19, pp. 10000–10011, 2013.

[10] M. Zapateiro, Y. Vidal, and L. Acho, "A secure communication scheme based on chaotic Duffing oscillators and frequency estimation for the transmission of binary-coded messages," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 991–1003, 2014.

[11] C.-J. Cheng, "Robust synchronization of uncertain unified chaotic systems subject to noise and its application to secure communication," *Applied Mathematics and Computation*, vol. 219, no. 5, pp. 2698–2712, 2012.

[12] W.-D. Chang, "Digital secure communication via chaotic systems," *Digital Signal Processing: A Review Journal*, vol. 19, no. 4, pp. 693–699, 2009.

[13] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[14] C. Hua, X. Guan, X. Li, and P. Shi, "Adaptive observer-based control for a class of chaotic systems," *Chaos, Solitons & Fractals*, vol. 22, no. 1, pp. 103–110, 2004.

[15] S. H. Mahboobi, M. Shahrokhi, and H. N. Pishkenari, "Observer-based control design for three well-known chaotic systems," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 381–392, 2006.

[16] C.-S. Ting, "An observer-based approach to controlling time-delay chaotic systems via Takagi–Sugeno fuzzy model," *Information Sciences*, vol. 177, no. 20, pp. 4314–4328, 2007.

[17] S. Bowong and J. J. Tewa, "Unknown inputs' adaptive observer for a class of chaotic systems with uncertainties," *Mathematical and Computer Modelling*, vol. 48, no. 11-12, pp. 1826–1839, 2008.

[18] F. Zhu, "Observer-based synchronization of uncertain chaotic system and its application to secure communications," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2384–2391, 2009.

[19] M. Chen, D. Zhou, and Y. Shang, "A sliding mode observer based secure communication scheme," *Chaos, Solitons & Fractals*, vol. 25, no. 3, pp. 573–578, 2005.

[20] S. Yin, X. Li, H. Gao, and O. Kaynak, "Data-based techniques focused on modern industry: an overview," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 1, pp. 657–667, 2014.

[21] S. Yin, S. X. Ding, A. Haghani, H. Hao, and P. Zhang, "A comparison study of basic data-driven fault diagnosis and process monitoring methods on the benchmark Tennessee Eastman process," *Journal of Process Control*, vol. 22, no. 9, pp. 1567–1581, 2012.

[22] S. Yin, H. Luo, and S. X. Ding, "Real-time implementation of fault-tolerant control systems with performance optimization," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 5, pp. 2402–2411, 2014.