World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:4, No:5, 2010

Chaos-based Secure Communication via Continuous Variable Structure Control

Cheng-Fang Huang, Meei-Ling Hung*, Teh-Lu Liao, Her-Terng Yau, Jun-Juh Yan

***Abstract*—**The design of chaos-based secure communication via synchronized modified Chua's systems is investigated in this paper. A continuous control law is proposed to ensure synchronization of the master and slave modified Chua's systems by using the variable structure control technique. Particularly, the concept of extended systems is introduced such that a continuous control input is obtained to avoid chattering phenomenon. Then, it becomes possible to ensure that the message signal embedded in the transmitter can be recovered in the receiver.

***Keywords*—**Chaos, Secure communication, Synchronization, Variable structure control (VSC)

I. Introduction

A chaotic system is a very complex, dynamic nonlinear system and its response possesses many intrinsic characteristics such as broadband noise-like waveform, prediction difficulty, sensitivity to initial condition variations, etc. [1, 2]. Although it appears to be stochastic, it occurs in a deterministic nonlinear system under deterministic conditions. Till now, many methods and techniques in synchronizing chaos have been proposed since the pioneering work of Pecora and Carroll in 1990 [1]. Moreover, the synchronization of chaotic circuits for the secure communication has received much attention in the literature [3-10].

The purpose of this paper lies in the development of a VSC-based chaotic communication system. As well known, synchronization of chaos is a key technology in generating an identical chaotic waveform in both transmitter and receiver for signal decoding in communication systems. Therefore, a new adaptive VSC-based control scheme to solve the synchronization problem of chaotic modified Chua's systems is firstly proposed. Then the concept of extended systems developed in [11] is introduced such that a continuous adaptive VSC controller is obtained to avoid chattering phenomenon as frequently in the conventional sliding mode control systems. In our design, a switching surface is first proposed, which makes it easy to guarantee the stability of the extended error dynamics in the sliding mode. And then, based on this switching surface, a continuous adaptive VSC is derived. Moreover, the proposed continuous VSC synchronization scheme is then applied to establish a chaotic secure communication system.

The remainder of this paper is organized as follows. Section 2 formulates the synchronization problem. In Section 3, the switching surface which ensures the stability of the extended error system in the sliding mode is derived. Then a continuous adaptive VSC controller is designed to achieve the hitting. In Section 4, an illustrative example is included. Finally, conclusions are presented in Section 5.

Cheng-Fang Huang, and Teh-Lu Liao are with the Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan.

Meei-Ling Hung is with the Department of Electrical Engineering, Far East University, Tainan 744, Taiwan, R.O.C.

Her-Terng Yau is with the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung County 411, Taiwan.

Jun-Juh Yan is with the Department of Computer and Communication, Shu-Te University, Kaohsiung 824, Taiwan.

II. System description and problem formulation

In this section, the design of secure communication systems via synchronized chaotic circuits is studied. For simplicity, the modified Chua's system is selected for our design. However, the method developed in this paper can be easily extended for the other class of chaotic systems. Before constructing the secure communication system, the first problem undertaken here is how to design a continuous VSC controller to solve the synchronization problem of systems. The master-slave chaotic systems are defined below, respectively [12].

Master system X_m:

$$\begin{aligned}\dot{x}_m &= p(y_m - \tfrac{1}{7}(2x_m^3 - x_m)) + m(t)\\ \dot{y}_m &= x_m - y_m + z_m\\ \dot{z}_m &= -qy_m\end{aligned} \quad , \tag{1}$$

Slave system X_s:

$$\begin{aligned}\dot{x}_s &= p(y_s - \tfrac{1}{7}(2x_s^3 - x_s)) + d_n(t) + u(t)\\ \dot{y}_s &= x_s - y_s + z_s\\ \dot{z}_s &= -qy_s\end{aligned} \quad , \tag{2}$$

where $p>0$ and $q>0$ are system parameters, $u(t)$ is the control input proposed later to synchronize master and slave systems (1) and (2), $m(t)$ and $d_n(t)$ are the bounded embedded message and external noise, respectively, which satisfy $|m(t)| \le \delta_m \in R^+$ and $|d_n(t)| \le \delta_n \in R^+$. It is assumed that the magnitude of δ_n is much smaller than that of δ_m. Let us define the state errors between the master system Eq. (1) and slave system Eq. (2) as follows:

$$e_x = x_s - x_m,\ e_y = y_s - y_m,\ e_z = z_s - z_m, \tag{3}$$

then the dynamics of the error system is determined directly from Eq. (1) and Eq. (2) as follows:

$$\begin{aligned}\dot{e}_x &= p[e_y - e_x(\tfrac{2}{7}(x_s^2 + x_s x_m + x_m^2) - \tfrac{1}{7})] \\ &\quad - m(t) + d_n(t) + u \\ \dot{e}_y &= e_x - e_y + e_z \\ \dot{e}_z &= -q e_y\end{aligned} \quad . \tag{4}$$

For deriving the main results, the following assumption is made.

Assumption 1: There exists an unknown and sufficiently large constant κ satisfying

$$\left|\frac{d}{dt}\{p[e_y - e_x(\tfrac{2}{7}(x_s^2 + x_s x_{\mathrm{m}} + x_m^2) - \tfrac{1}{7})] - m(t) + d_n(t)\}\right| \le \kappa < \infty \quad . \tag{5}$$

Now newly introducing the concept of extended systems and extending the error dynamics Eq. (4) as

$$\begin{aligned}\dot{e}_x &= p[e_y - e_x(\tfrac{2}{7}(x_s^2 + x_s x_m + x_m^2) - \tfrac{1}{7})] \\ &\quad - m(t) + d_n(t) + u = e_E \\ \dot{e}_y &= e_x - e_y + e_z \\ \dot{e}_z &= -q e_y \\ \dot{e}_E &= \frac{d}{dt}[p(e_y - e_x(\tfrac{2}{7}(x_s^2 + x_s x_m + x_m^2) - \tfrac{1}{7})) \\ &\quad - m(t) + d_n(t)] + \dot{u}\end{aligned} \quad . \tag{6}$$

The goal of this paper is that for any given modified Chua's circuit systems as Eq. (1) and Eq. (2), an adaptive VSC controller is designed such that the asymptotical stability of the resulting extended error system Eq. (6) can be achieved in the sense that $\lim_{t\to\infty}\|e(t)\| \to 0$, where $e(t) = [e_x, e_y, e_z, e_E]$. Then, the message signal embedded in the transmitter (master system) can be recovered in the receiver.

III. Switching surface and adaptive continuous VSC design

To complete the design of secure communication, it is necessary to propose a continuous VSC scheme to stabilize the extended error dynamics Eq. (6) and achieve synchronization. In the following, the design of continuous VSC scheme is separated into two major phases. First, an appropriate switching surface is selected such that the sliding motion on the sliding manifold is stable. Second, a continuous VSC law is established to guarantee the attraction of the sliding manifold. To assure the error dynamics Eq. (6) in the sliding manifold can be stable asymptotically, the designed switching surface $s(t)$ corresponding to $e(t)$ is given as follows:

$$s(t) = k_x e_x + k_y e_y + k_z e_z + e_E, \tag{7}$$

where $s \in R$ and $k_x, k_y, k_z \in R$ are designed constants. According to the works in [13], when the system can operate in the sliding mode, i.e. $s(t) = 0$, the following equation is always satisfied

$$s(t) = k_x e_x + k_y e_y + k_z e_z + e_E = 0. \tag{8}$$

and

$$\dot{s}(t) = k_x \dot{e}_x + k_y \dot{e}_y + k_z \dot{e}_z + \dot{e}_E = 0. \tag{9}$$

From Eq. (8), it is obtained

$$e_E = -k_x e_x - k_y e_y - k_z e_z. \tag{10}$$

By (6) and (10), it yields

$$\begin{bmatrix}\dot{e}_x \\ \dot{e}_y \\ \dot{e}_z\end{bmatrix} = \begin{bmatrix}-k_x & -k_y & -k_z \\ 1 & -1 & 1 \\ 0 & -\mathrm{q} & 0\end{bmatrix}\begin{bmatrix}e_x \\ e_y \\ e_z\end{bmatrix} = A\begin{bmatrix}e_x \\ e_y \\ e_z\end{bmatrix}. \tag{11}$$

Obviously, the error dynamics Eq. (11) is exponentially stable if the constants k_x, k_y, k_z are suitable chosen such that the eigenvalues of matrix A in Eq. (11) are with negative real parts. Also the convergence rate of Eq. (11) can be determined by the eigenvalues of matrix A. Furthermore, by Eq. (10), e_E converges to zero when e_x, e_y and e_z converge to zero.

After establishing an appropriate sliding surface, the next step is to establish a robust control law not only to guarantee the occurrence of the sliding mode but also ensure that the state trajectory can stay on the sliding mode $s = 0$ thereafter even undergoing the unknown message signal. To ensure the occurrence of the sliding motion, an adaptive VSC scheme is proposed as

$$\begin{aligned}\dot{u}(t) &= -[k_y e_x - (k_y + q k_z) e_y + k_y e_z + k_x e_E] \\ &\quad - r\hat{\kappa}(t) sign(s(t)), u(0) = u_0\end{aligned}, \tag{12}$$

where $r > 1$ and u_0 is the bounded initial value of $u(t)$. The adaptive law is

$$\dot{\hat{\kappa}}(t) = \theta|s(t)|, \hat{\kappa}(0) = \hat{\kappa}_0 \tag{13}$$

where $\theta > 0$ and $\hat{\kappa}_0$ is the bounded initial value of $\hat{\kappa}(t)$.

The adaptive SMC controller (12) can be also written in the integral form as

$$\begin{aligned}u(t) = -\int_0^t \{&[k_y e_x - (k_y + q k_z) e_y + k_y e_z + k_x e_E] \\ &+ r\hat{\kappa}(t) sign(s(t))\} dt + u_0\end{aligned} \tag{14}$$

and

$$\hat{\kappa}(t) = \theta \int_0^t |s(t)| dt + \hat{\kappa}_0 \tag{15}$$

Next, the proposed adaptive VSC of Eq. (12) will be proved to be able to drive the extended error dynamics Eq. (6) onto the sliding mode $s(t) = 0$.

Theorem 1: Consider the extended error dynamics Eq. (6), if the control input $u(t)$ is suitably designed as Eq. (12) with adaptation law Eq. (13), then the trajectory of the error dynamics Eq. (6) converges to the switching surface $s(t) = 0$.

Proof: Consider the following Lyapunov function candidate

$$V(t) = \tfrac{1}{2}(s^2 + \theta^{-1}\delta^2); \theta > 0\,, \tag{16}$$

where $\delta(t) \in R$ denotes the adaptation error which will be defined later. Taking the derivative of $V(t)$ with respect to time, one has

$$\begin{aligned}\dot{V}(t) &= s\dot{s} + \theta^{-1}\delta\dot{\delta} \\ &= s(k_x\dot{e}_x + k_y\dot{e}_y + k_z\dot{e}_z + \dot{e}_E) + \theta^{-1}\delta\dot{\delta} \\ &= s\{\frac{d}{dt}[p(e_y - e_x(\tfrac{2}{7}(x_s^2 + x_s x_m + x_m^2) - \tfrac{1}{7})) - m(t) + d_n(t))] \\ &\quad + k_y e_x - (k_y + qk_z)e_y + k_y e_z + k_x e_E + \dot{u}\} + \theta^{-1}\delta\dot{\delta} \\ &\le |s|\kappa - \mathrm{r}\cdot\hat{\kappa}(t)\cdot s\cdot sign(s) + \theta^{-1}\,\delta\dot{\delta} \\ &\le [\kappa - r\hat{\kappa}(t)]|s| + \theta^{-1}\delta\dot{\delta}\end{aligned} \tag{17}$$

Now let $\delta(t) = \kappa - \hat{\kappa}(t)$ denote the adaptation error. Since κ is constant, $\dot{\kappa} = 0$ and the following expression holds.

$$\dot{\delta}(t) = -\dot{\hat{\kappa}}(t) \tag{18}$$

Inserting Eq. (18) into the right hand of inequality (17), this yields

$$\dot{V}(t) \le \{[\overbrace{\kappa - \hat{\kappa}(t)}^{\delta}] + (1-r)\hat{\kappa}(t)\}|s| - \theta^{-1}\,\delta\dot{\hat{\kappa}}(t) \tag{19}$$

By placing (13) into (19), it yields

$$\dot{V}(t) \le (1-r)\hat{\kappa}(t)|s| \le -F(t) \le 0\,, \tag{20}$$

where $F(t) = (r-1)\hat{k}(t)|s| \ge 0$. Integrating the above equation from zero to *t*, it yields

$$V(0) \ge V(t) + \int_0^t F(\lambda)d\lambda \ge \int_0^t F(\lambda)d\lambda. \tag{21}$$

As *t* goes infinite, the above integral is always less than or equal to $V(0)$. Since $V(0)$ is positive and finite, $\lim_{t\to\infty}\int_0^t F(\lambda)d\lambda$ exists and is finite. Thus according to Barbalat lemma [14], it yields

$$\lim_{t\to\infty} F(t) = \lim_{t\to\infty}(r-1)\hat{\kappa}(t)|s| = 0 \tag{22}$$

Since both $(r-1)$ and $\hat{\kappa}(t)$ are greater than zero, Eq. (22) implies $s = 0$. Hence the proof is achieved completely.

Theorem 2: The error system Eq. (4) driven by the controller u(t) expressed in Eq. (12) with adaptation law Eq. (13) is globally stable.

Proof: Using the concept of extended systems, the error dynamics Eq. (4) can be extended as the extended error dynamics Eq. (6). When the extended error dynamics Eq. (6) is driven by the control input $u(t)$ given in Eq. (12) with adaptation law Eq. (13), as previously discussed in Theorem 1, the trajectory of the error dynamics system Eq. (6) surely converges to the sliding mode $s = 0$. Thus the equivalent error dynamics in the sliding mode is obtained as

$$\begin{bmatrix}\dot{e}_x \\ \dot{e}_y \\ \dot{e}_z\end{bmatrix} = \begin{bmatrix}-k_x & -k_y & -k_z \\ 1 & -1 & 1 \\ 0 & -q & 0\end{bmatrix}\begin{bmatrix}e_x \\ e_y \\ e_z\end{bmatrix} = A\begin{bmatrix}e_x \\ e_y \\ e_z\end{bmatrix} \tag{23}$$

Furthermore, since the design parameters k_x,k_y and k_z are specified to ensure $\lambda_{\max}(A) < 0$, the stability of Eq. (23) is surely guaranteed, that is $\lim_{t\to\infty}\left\|\begin{bmatrix}e_x & e_y & e_z\end{bmatrix}\right\| = 0$. By the relation of $s(t) = k_x e_x + k_y e_y + k_z e_z + e_E = 0$, $e_E(t)$ is also stable, that is $\lim_{t\to\infty} e_E(t) = 0$. Consequently, the asymptotical stability of the closed-loop error system is also ensured. The theorem is therefore proved.

When the error dynamics converges to zero as discussed in Theorem 2, the following result can be obtained from Eq. (4):

$$\begin{aligned}\dot{e}_x &= p(e_y - \mathrm{e}_x(\tfrac{2}{7}(x_s^2 + x_s x_m + x_m^2) + \tfrac{1}{7}) \\ &\quad - m(t) + d_n(t) + u = 0 \\ \dot{e}_y &= e_x - e_y + e_z = 0 \\ \dot{e}_z &= -qe_y = 0\end{aligned} \tag{24}$$

Then, from Eq. (24), it yields that

$$\lim_{t\to\infty}(u(t) - m(t) + d_n(t)) = 0 \tag{25a}$$

If the magnitude of δ_n is much smaller than that of δ_m, then

$$u(t) = m(t) - d_n(t) \cong m(t) \tag{25b}$$

In other words, the message signal $m(t)$ can be recovered in the receiver from the continuous control input $u(t)$.

IV. Numerical Simulation

In this section, simulation results are presented to demonstrate and verify the performance of the present design. The parameters p and q are chosen as $p = 10$ and $q = \frac{100}{7}$ in the simulation to ensure the existence of chaos for the master system (1). Assume $d_n(t) = 0.01\sin(10t)$ and the initial states of the master system (1) are $x_m(0) = 0.65$, $y_m(0) = 0$, $z_m(0) = 0$ and initial states of the slave system Eq. (2) are $x_s(0) = -1$, $y_s(0) = 1$, $z_s(0) = -2$. For simulation, a sin wave $m(t) = 0.2\sin(2t)$ is embedded into the dynamics of master system. And then, according to (11), $k_x = 8, k_y = 3.7143$ and $k_z = 6.32$ are selected such that $\lambda(A) = (-2,-3,-4)$ and the switching surface equation is obtained as

$$s(t) = 8e_x + 3.7143e_y + 6.32e_z + e_E \tag{26}$$

From Eq. (14) and Eq. (15), the continuous control input is determined as

$$\begin{aligned}u(t) = -\int_0^t \{[k_y e_x - (k_y + qk_z)e_y + k_y e_z + k_x e_E] \\ + r\hat{\kappa}(t)sign(s(t))\}dt + u_0\end{aligned} \tag{27}$$

where $r = 1.1 > 1$ to guarantee the existence of the sliding motion and $u_0 = 0$. The adaptive law is

$$\hat{\kappa}(t) = \theta\int_0^t |s(t)|dt + \hat{\kappa}_0 \tag{28}$$

where $\theta = 1$ and $\hat{\kappa}_0 = 1$.

The simulation results are shown in Figures 1-3 under the proposed continuous adaptive SMC Eq. (27). Fig. 1 shows the time responses of corresponding $s(t)$ and adaptation parameter $\hat{\kappa}(t)$. Fig. 2 shows, the error state responses of the controlled master-slave modified Chua's system. From the simulation result, as expected, it shows that the trajectory of error dynamics do converge to $s(t) = 0$ and the synchronization error also converges to zero. Finally, Fig. 3 depicts the simulations of chaotic secure communication for message signal given above. The solid line indicates the transmitted message signal $m(t)$ and the dash line denotes the recovered message under the effect of external noise $d_n(t)$. Obviously, these results prove that the master and slave systems synchronization can be achieved as well as the hidden message for secure communication can be recovered in the slave system.

V. Conclusion

In this paper, a secure communication system via synchronized modified Chua's systems has been presented. A continuous adaptive sliding mode controller has been proposed to ensure the synchronization between the master and the controlled slave systems. Then the proposed scheme has been also successfully applied to establish the secure communication system. Numerical simulations have verified the effectiveness of the proposed method.

References

[1] L. M. Pecora and T. L Carroll, "Synchronization in chaotic systems," Physical Review Letters, vol .64(8), pp. 821–824, 1990.
[2] C. K. Huang, S. C. Tsay and Y. R. Wu, "Implementation of chaotic secure communication systems based on OPA circuits," Chaos, Solitons & Fractals, vol. 23(1), pp. 589-600, 2005.
[3] N. Reddell, E. Bollt, and T. Welch, "A Dual-Synchrony Chaotic Communication Scheme," Circuits, Systems, and Signal Processing, vol. 24(5), pp. 557-570, 2005.
[4] S. Wang, J. Feng, and S. Xie, "A Multiuser Chaotic Communication Scheme by Parameter Division Multiple Access." Circuits, Systems, and Signal Processing, vol. 26, pp. 839-852, 2007.
[5] X. Zhang, and L. Min, "A generalized chaos synchronization based encryption algorithm for sound signal communication," Circuits, Systems, and Signal Processing, vol. 24(5), pp. 535-548, 2005.
[6] J. Zhou, T. Chen, and L. Xiang, "Chaotic lag synchronization of coupled delayed neural networks and its applications in secure communication," Circuits, Systems, and Signal Processing, vol. 24(5), pp. 599-613, 2005.
[7] J. Zhou, H. B. Huang, G. X. Qi, P. Yang, and X. Xie, "Communication with spatial periodic chaos synchronization," Physics Letters A, vol. 335, pp. 191-196, 2005.
[8] T. I. Chien, and T. L. Liao, "Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization," Chaos, Solitons and Fractals, vol. 24(1), pp. 241-255, 2005.
[9] Z. Li, K. Li, C. Wen, and Y. C. Soh, "A new chaotic secure communication system," IEEE Trans on Commun, vol. 51(8), pp. 1306-1312, 2003.
[10] Z. Li, and D. Xu, "A secure communication scheme using projective chaos synchronization," Chaos, Solitions & Fractal, vol. 22(2), pp. 477-481, 2004.
[11] H. T. Yau, C. K. Chen, and C. L. Chen, "Sliding mode control of chaotic systems with uncertainties," International Journal of Bifurcation and Chaos, vol. 10(5), pp. 1139-1147, 2000.
[12] M. T. Yassen, "Adaptive control and synchronization of a modified Chua's circuit system," Applied Math. and Computation, vol. 135, pp. 113-128, 2003.
[13] V. I. Utkin, "Sliding Mode and Their Applications in Variable Structure Systems," Mir: Moscow, 1978.
[14] V. M. Popov, Hyperstability of Control System, Springer: Berlin, 1973.

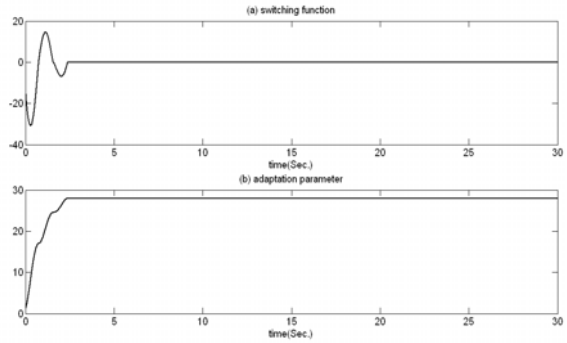

Fig. 1 (a) switching function $s(t)$; (b) adaptation parameter $\hat{\kappa}(t)$.

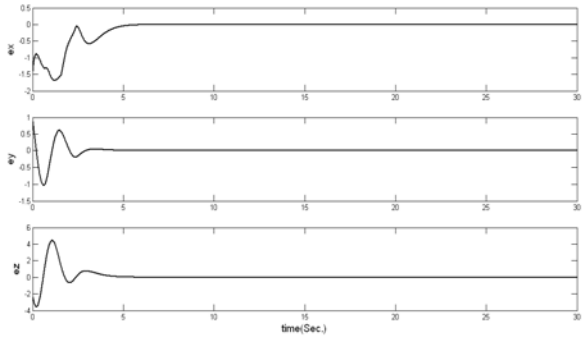

Fig. 2 The time responses of synchronization error.

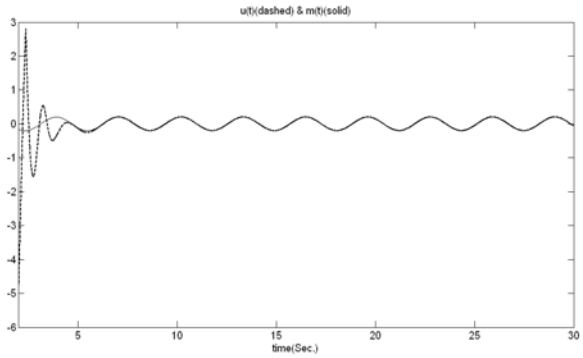

Fig. 3 The original and recovered message signals.