Application of a Chaotic Synchronization System to Secure Communication

Her-Terng Yau[1], Yu-Chi Pu[2], Simon Cimin Li[3]

[1] *Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung 411, Taiwan*
e-mail: pan1012@ms52.hinet.net

[2] *Department of Electrical Engineering, Far-East University, Tainan 744, Taiwan*

[3] *Department of Electrical Engineering, National University of Tainan, Tainan 700, Taiwan*

crossref http://dx.doi.org/10.5755/j01.itc.41.3.1137

Abstract. This work describes a novel scheme that applies a Sprott master/slave chaotic synchronization system to secure transmission. A sliding plane is chosen to design a sliding mode controller to ensure robustness. In the presence of an external disturbance and system uncertainty, the slave chaotic circuit system is then synchronized with the master. The Lyapunov theorem verifies that the proposed controller is stable and robust. Simulation results indicate that the synchronization error state asymptotically converges to the origin of the phase plane, implying that the master/slave chaotic system synchronization is achieved while the sliding mode controller is in operation. While consisting of operational amplifiers, resistors, capacitors and diodes, the chaotic circuit system together with a sliding mode controller is subsequently implemented to validate the system synchronization. Finally, the chaotic system combined with cryptography is embedded into a chaotic synchronization cryptosystem to resolve secure communications-related problems.

Keywords: Chaotic synchronization; Sliding mode controller; Sprott system; Lyapunov theorem; secure communication.

1. Introduction

Based on atmospheric simulation, Lorenz pioneered the chaos theory, a seemingly disordered phenomenon [1]. Until the general theory of Feigenbaum in 1978, chaos received scarce scientific attention. As a complex and aperiodic nonlinear system, the time response of chaotic system is extremely sensitive to initial conditions. Otherwise, it also has a wide range of the Fourier spectrum and is characterized by the fractal geometry on the phase plane. That is, even with an identical system, the system response varies significantly with various initial conditions, a phenomenon referred to as the butterfly effect. Having been extensively studied, chaos can be found in a diverse array of research fields, including electrical engineering, electronics, communications, biology, mathematics, physics, chemistry, and economics. The Lorenz system has been applied to atmospheric science, the Duffing system to mechanics, the Rössler system to chemical engineering, and Chua's circuit [2-3] to circuitry.

Chaotic synchronization has been extensively studied in recent decades [4-8]. While normally consisting of a master system, slave system, and synchronization controller, this system transmits a state signal to the controller, followed by processing and subsequent application to the slave system, as an alternative approach to locus synchronization between both systems. The concept of chaotic synchronization has not, until recently, been applied to the communications field [9-16], in which the signal intended for delivering a chaotic signal in the transmitter is modulated and the received signal in the receiver is then demodulated into the original one. However, transmission security is of priority concern [17], largely owing to that an individual familiar with the chaotic theory can easily intercept information during transmission. To resolve such security concerns, a scheme [18-21] based on the original chaotic system in combination with encryption skills utilizes the chaotic system to encrypt the transmitted data by an encryption function, followed by modulation by a chaotic signal to increase the complexity and security of such transmitted signals.

This work develops a novel scheme that ensures robustness of the controlled system to external disturbances. Additionally, system uncertainties incorporate systematic design processes to enable the designer to easily implement the controller. Moreover, the proposed control scheme, in which a continuous function is used to replace the discontinuous sign function in the final design process step, can eliminate chattering in the control input to ensure feasibility for an actual physical system. However, to our knowledge, no previously developed scheme can obtain such a robust continuous controller for chaos synchronization control in a secure communications system, necessitating the development of a sliding mode control scheme. Therefore, based on a sliding mode controller [22], this work addresses the synchronization issue of a chaotic system, while devising a sliding mode control criterion. While implemented with electronic components, system synchronization is validated using the chaotic system and the controller. Finally, by using LabView, the chaotic synchronization system, integrated with cryptography, is applied to secure communication i.e. the encryption and decryption of audio and image signals.

2. System descriptions

This work focuses on a Sprott chaotic system, where the governing equation is expressed in a differential form [23-24] as

$$\dddot{x} + a\ddot{x} + \dot{x} = G_i(x), \tag{1}$$

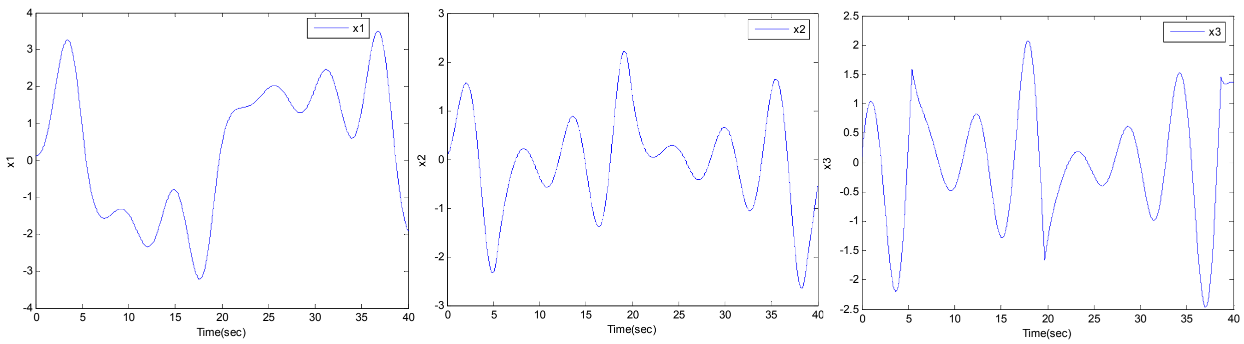
where $G_i(x)$ denotes any of the underlying functions

$$G_1(x) = |x| - 2$$
$$G_2(x) = -6\max(x,0) + 0.5,$$
$$G_3(x) = 1.2x - 4.5sign(x)$$
$$G_4(x) = -1.2x + 2sign(x)$$

where $max(\cdot)$ refers to a maximum value function, as well as $sign(\cdot)$ the sign function. While considering the circuit implementation, the system state variables are assumed to be $x_1 = x$, $x_2 = \dot{x}$, $x_3 = \ddot{x}$. A state equation is subsequently derived as

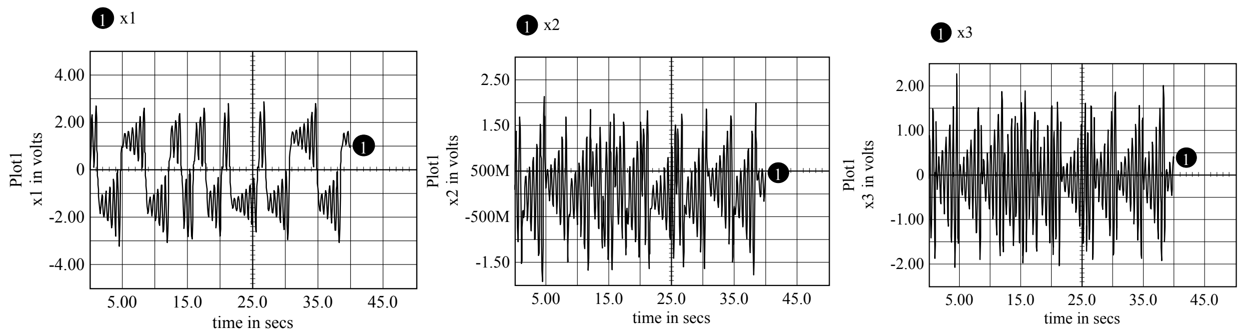
$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= x_3 \\ \dot{x}_3 &= -x_2 - ax_3 + G_i(x). \end{aligned} \tag{2}$$

Consider a situation in which $G_i(x) = G_4(x_1) = -1.2x_1 + 2sign(x_1)$ and a=0.6 are selected since it is easily implemented by electronic circuits and chaotic motion has been proven to exist [23]. The dynamic response is then simulated with Matlab and IsSpice software packages as shown in Figs. 1 and 2. Figure 3 summarizes the implementation results of the electronic circuits indicating that the Sprott system has complex dynamics.



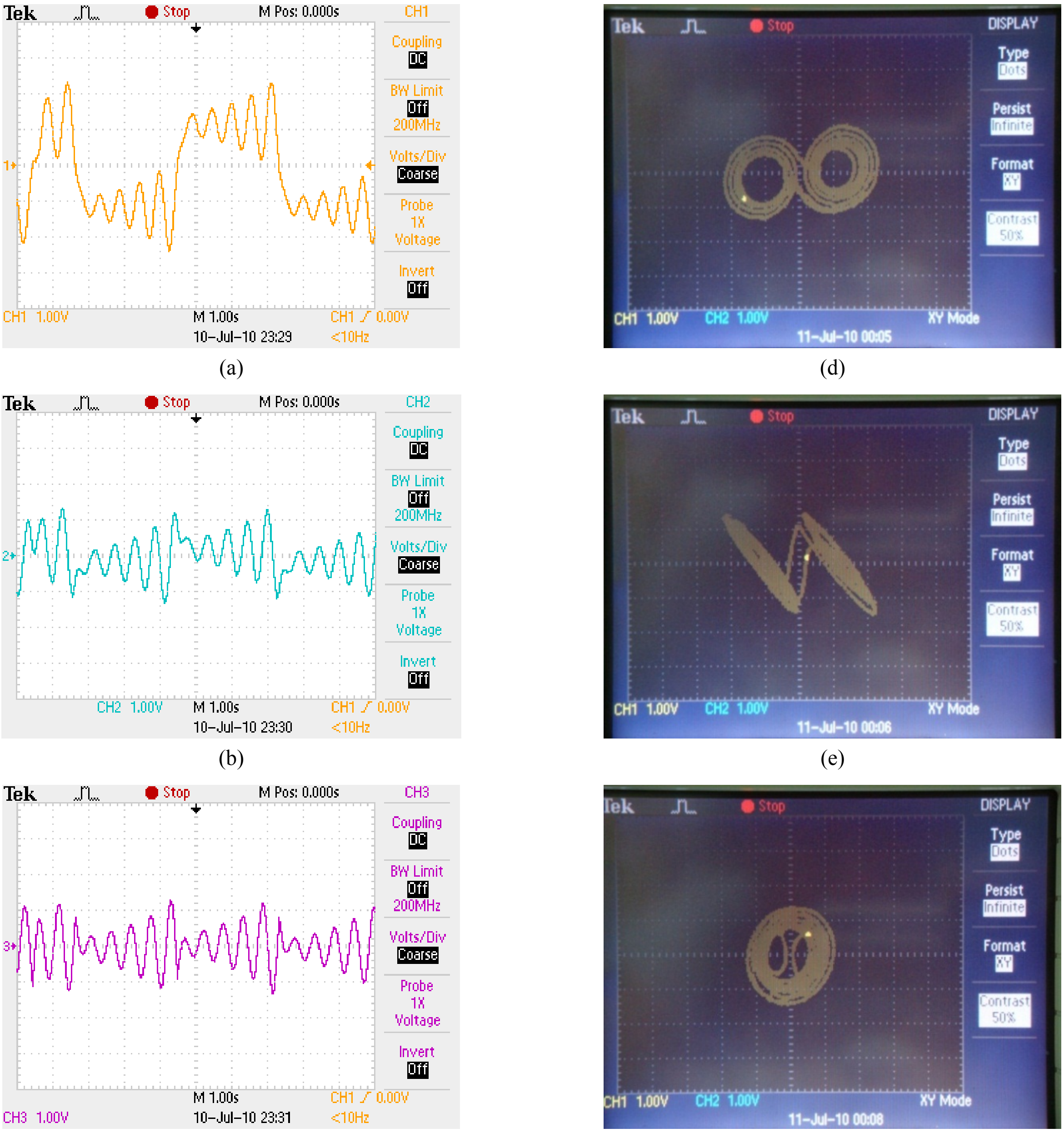
(a) (b) (c)

Figure 1. Given initial condition $(x_1(0), x_2(0), x_3(0)) = (0.1, 0.1, 0.1)$, the simulated time response by MATLAB to (a) x1, (b) x2, (c) x3



(a) (b) (c)

Figure 2. Given initial condition $(x_1(0), x_2(0), x_3(0)) = (0.1, 0.1, 0.1)$, the simulated time response by IsSpice to (a) x1, (b) x2, (c) x3



(a) (d)

(b) (e)

(c) (f)

Figure 3. Circuit hardware responses to (a) x1, (b) x2, (c) x3, and phase plane of (d) x1 versus x2, (e) x1versus x3, (f) x2versus x3

The dynamic equations of both the master and slave chaotic systems in the Sprott circuit addressed here, are expressed as

Master:

$$
\begin{aligned}
\dot{x}_{m,1} &= x_{m,2} \\
\dot{x}_{m,2} &= x_{m,3} \\
\dot{x}_{m,3} &= -1.2x_{m,1} - x_{m,2} - 0.6x_{m,3} + 2\cdot \operatorname{sign}(x_{m,1})
\end{aligned} \tag{3}
$$

Slave:

$$
\begin{aligned}
\dot{x}_{s,1} &= x_{s,2} \\
\dot{x}_{s,2} &= x_{s,3} \\
\dot{x}_{s,3} &= -(1.2+\Delta\xi)x_{s,1} - x_{s,2} - 0.6x_{s,3} + 2\cdot \operatorname{sign}(x_{s,1}) \\
&\quad + d(t) + u
\end{aligned} \tag{4}
$$

where $\Delta\xi$ denotes system uncertainty, $d(t)$ external disturbance, and u the controller added. The control target is specified as

$$\lim_{t\to\infty}\left\| x_s(t) - x_m(t) \right\| \to 0 \tag{5}$$

indicating that the slave synchronizes with the master.

3. Robust synchronization controller design

This section discusses the sliding mode controller designed for the system synchronization, which is simulated with MATLAB software. Following Eqs. (3) and (4), the master-slave system's error states are defined as

$$\begin{aligned} e_1 &= x_{s,1} - x_{m,1} \\ e_2 &= x_{s,2} - x_{m,2} \\ e_3 &= x_{s,3} - x_{m,3} \end{aligned} \tag{6}$$

From Eq. (6), it then follows that

$$\begin{aligned} \dot{e}_1 &= e_2 \\ \dot{e}_2 &= e_3 \\ \dot{e}_3 &= \left[-(1.2+\Delta\xi)x_{s,1} - x_{s,2} - 0.6x_{s,3} \right. \\ &\quad \left. + 2\cdot sign(x_{s,1}) + d(t) + u\right] - 1.2x_{m,1} \\ &\quad - x_{m,2} - 0.6x_{m,3} + 2\cdot sign(x_{m,1}) \\ &= -1.2(x_{s,1}-x_{m,1}) - (x_{s,2}-x_{m,2}) \\ &\quad - 0.6(x_{s,3}-x_{m,3}) + 2\cdot sign(x_{s,1}) \\ &\quad - 2\cdot sign(x_{m,1}) - \Delta\xi(x_{s,1}) + d(t) + u \\ &= -1.2e_1 - e_2 - 0.6e_3 + 2\cdot sign(x_{s,1}) \\ &\quad - 2\cdot sign(x_{m,1}) - \Delta\xi\cdot x_{s,1} + d(t) + u \end{aligned} \tag{7}$$

First, a sliding plane is chosen as

$$s = c_1e_1 + c_2e_2 + c_3e_3. \tag{8}$$

In the sliding mode, $\dot{s} = 0$ holds true, and the equivalent controller is expressed as

$$\begin{aligned} &\dot{s} = c_1\dot{e}_1 + c_2\dot{e}_2 + c_3\dot{e}_3 = 0 \\ &\Rightarrow c_1e_2 + c_2e_3 + c_3\left[-1.2e_1 - e_2 - 0.6e_3 \right. \\ &\quad + 2\cdot sign(x_{s,1}) - 2\cdot sign(x_{m,1}) \\ &\quad \left. - \Delta\xi\cdot x_{s,1} + d(t) + u_{eq}\right] = 0 \\ &\Rightarrow -1.2c_3e_1 + (c_1-c_3)e_2 + (c_2-0.6)e_3 \\ &\quad + 2c_3\cdot sign(x_{s,1}) - 2c_3\cdot sign(x_{m,1}) \\ &\quad - c_3\cdot\Delta\xi\cdot x_{s,1} + c_3d(t) + c_3u_{eq} = 0 \\ &u_{eq} = \left[1.2c_3e_1 - (c_1-c_3)e_2 - (c_2-0.6)e_3 \right. \\ &\quad - 2c_3\cdot sign(x_{s,1}) + 2c_3\cdot sign(x_{m,1}) \\ &\quad \left. + c_3\cdot\Delta\xi\cdot x_{s,1} - c_3d(t)\right]/c_3 \end{aligned} \tag{9}$$

For simplicity, by allowing $c_3 = 1$, Eq. (9) is rewritten as

$$\begin{aligned} u_{eq} &= 1.2e_1 - (c_1-1)e_2 - (c_2-0.6)e_3 \\ &\quad - 2\cdot sign(x_{s,1}) + 2\cdot sign(x_{m,1}) \\ &\quad + \Delta\xi\cdot x_{s,1} - d(t) \end{aligned} \tag{10}$$

Subsequently, the approaching law is designed as $u_{sw} = -W\cdot sign(s)$, where the sign function $sign(\cdot)$ is defined as

$$sign(s) = \begin{cases} 1 & , s > 0 \\ -1 & , s < 0 \end{cases}.$$

With a lack of knowledge concerning uncertainty $\Delta\xi$ and external disturbance $d(t)$, the system implemented in practice can be expressed as

$$\begin{aligned} u &= u_{eq} + u_{sw} \\ &= 1.2e_1 - (c_1-1)e_2 - (c_2-0.6)e_3 \\ &\quad - 2\cdot sign(x_{s,1}) + 2\cdot sign(x_{m,1}) \\ &\quad - W\cdot sign(s) \end{aligned} \tag{11}$$

Remark: The controller in (11) demonstrates discontinuous control laws and chattering occurs as well. From reference [25], chattering is eliminated by modified the controller as

$$\begin{aligned} u &= u_{eq} + u_{sw} \\ &= 1.2e_1 - (c_1-1)e_2 - (c_2-0.6)e_3 \\ &\quad - 2\cdot sign(x_{s,1}) + 2\cdot sign(x_{m,1}) \\ &\quad - W\cdot\frac{s}{|s|+\delta} \end{aligned} \tag{12}$$

where δ denotes a sufficiently small design constant. Here, constant δ is selected as 0.05. Therefore, the controllers can be implemented in a real world system. Next, the stability and robustness of the controller of Eq. (11) are proven in the following.

Via the Lyapunov theorem, the system stability is verified as

$$V(t) = \frac{1}{2}s^2 \cdot$$

The first order time derivative is written as

$$\begin{aligned} \dot{V} &= s\dot{s} = s\left[c_1\dot{e}_1 + c_2\dot{e}_2 + c_3\dot{e}_3\right] \\ &= s\{c_1e_2 + c_2e_3 + c_3[-1.2e_1 - e_2 - 0.6e_3 \\ &\quad + 2\cdot sign(x_{s,1}) - 2\cdot sign(x_{m,1}) - \Delta\xi x_{s,1} \\ &\quad + d(t) + u]\} \\ &= s\{[-1.2e_1 + (c_1-1)e_2 + (c_2-0.6)e_3 \\ &\quad + 2\cdot sign(x_{s,1}) - 2\cdot sign(x_{m,1}) - \Delta\xi x_{s,1} \\ &\quad + d(t)] + [1.2e_1 - (c_1-1)e_2 - (c_2-0.6)e_3 \\ &\quad - 2\cdot sign(x_{s,1}) + 2\cdot sign(x_{m,1}) \\ &\quad - W\cdot sign(s)]\} \\ &= s\left[-\Delta\xi x_{s,1} + d(t) - W\cdot sign(s)\right] \end{aligned} \tag{13}$$

The physical meanings of external disturbances and system uncertainties $d(t)$ and $\Delta\xi$ denote models of the unstructured system models and uncorrected system parameters of Sprott systems. Otherwise, the system states of the Sprott system are also attracted to a bounded attractor. Therefore, they can be assumed to be bounded that is $|x_{s,1}| < \beta$, $|\Delta\xi| \le \gamma$, $|d(t)| \le \delta$. Then Eq. (13) can be rewritten as

$$\begin{aligned} \dot{V} &\le |s|\left[|\Delta\xi|\cdot|x_{s,1}| + |d(t)|\right] - W|s| \\ &\le |s|\cdot(\gamma\beta+\delta) - W|s| \\ &\le |s|\cdot(\gamma\beta+\delta-W) \end{aligned} \tag{14}$$

If

$$W > (\gamma\beta+\delta), \tag{15}$$

then $\dot{V} < 0$ ensures a stable system. By using Matlab software, feasibility of the controller in Eq. (12) is verified, with the parameters $c_1 = 10$, $c_2 = 10$, W=0.9, while those in Eq. (4) are $\Delta\zeta = 0.1\sin(t)$, $d(t) = 0.1\cos(t)$, i.e. $\gamma = 0.1, \delta = 0.1$. Therefore, according to Fig. 4, $x_{s,1} \leq 4.33$, a substitution of which into Eq. (14) yields $W > 0.533$. To maintain a stable system, a choice of W=0.9 is made accordingly.

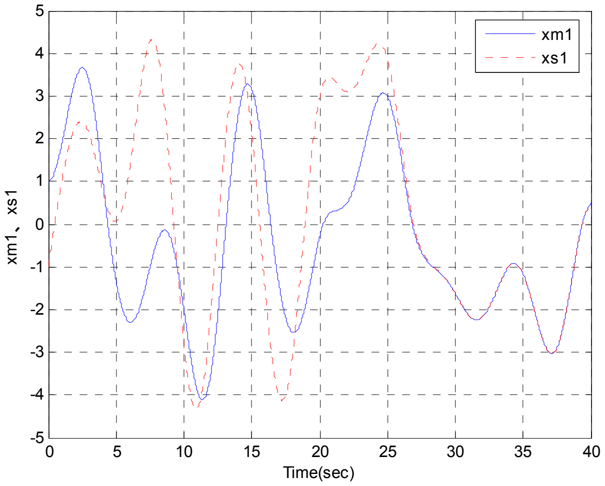


Figure 4. Time response to $x_{m,1}, x_{s,1}$. The control is active at t=25 sec

4. Applications in secure communication

This section describes the application of a cryptosystem, constructed based on the Sprott chaotic synchronization system integrated with cryptography to secure communications. The transmission link is established via the Internet and National Instruments LabView, with the information encrypted and decrypted in the transmitter and the receiver, respectively, by computers. The audio signal is transmitted as follows. First, the initial conditions of the system and the sampling amount are determined. An identical number of keys are then generated, with which the audio signal is mixed accordingly. Figures 5 to 7 display the audio processing system, as well as summarize the experimental results. The image counterpart is described as follows. The encryption process is divided into two phases. The first one is the image itself, with both the symmetric key cryptosystem (SKC) and the master/slave system as the key, through which the image signal is encoded despite the same set of initial values. The initial values subsequently vary with the master/slave system status. The second one is the encryption of the master/slave system signal, with a Lorenz system as the key, as a means of removing the interception likelihood during data transmission. Figure 8 illustrates the image encryption/decryption system, where the Lorenz system is of invariant initial conditions; meanwhile, the master chaotic system randomly generates the initial conditions. Figures 9 to 11 summarize the experimental results. An entity photo of a Sprott master/slave system and a sliding mode controller are shown in Fig. 12.

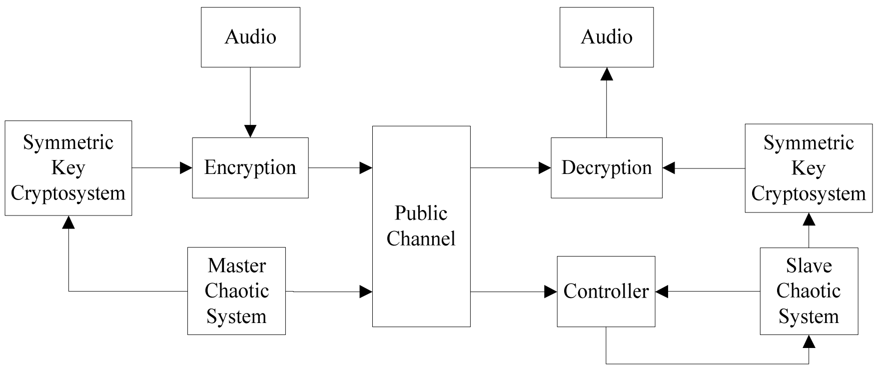
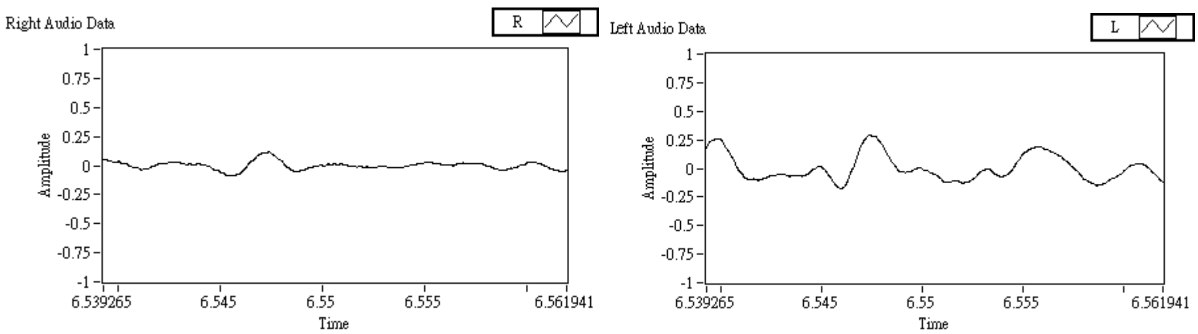
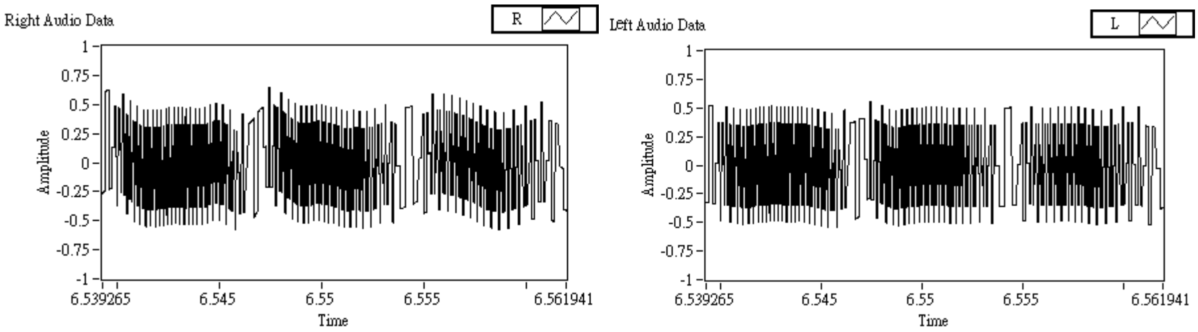


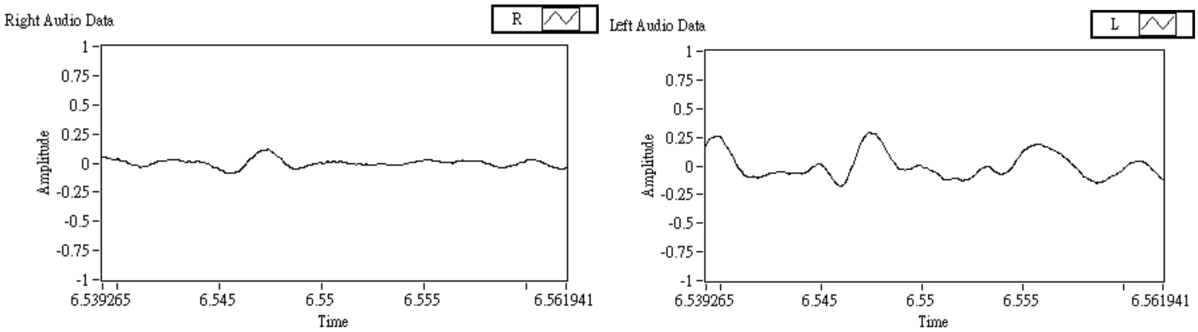
Figure 5. An audio encryption/decryption flow in a chaotic synchronization cryptosystem



(a)

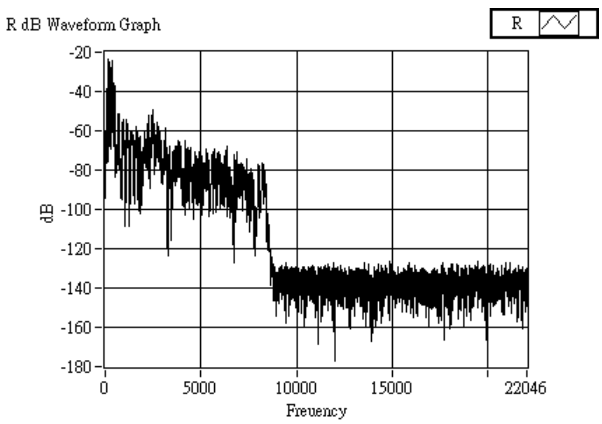


(b)

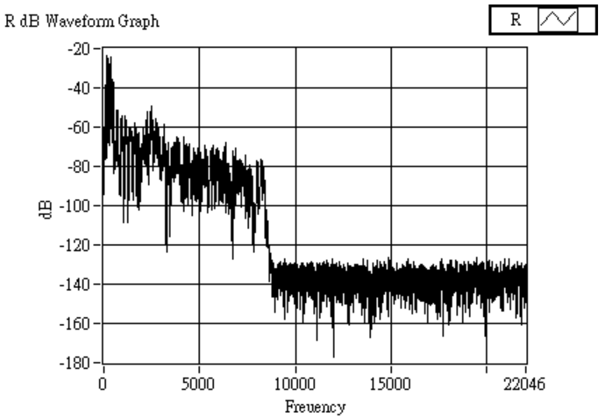


(c)

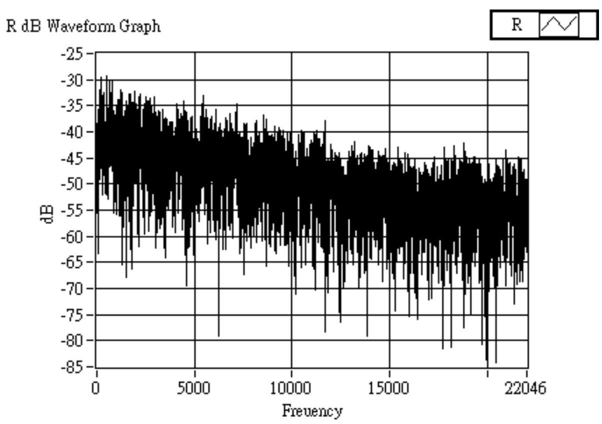
Figure 6. An audio signal zoomed in. (a) The original audio zoomed in; (b) An encrypted version of (a); (c) A decrypted version of (b).



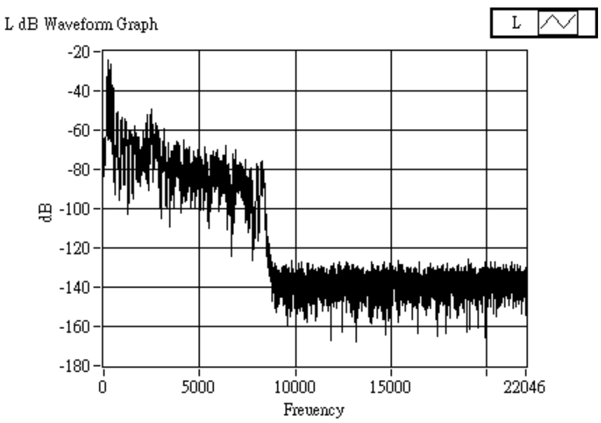
(a) The spectrum of the original right channel audio



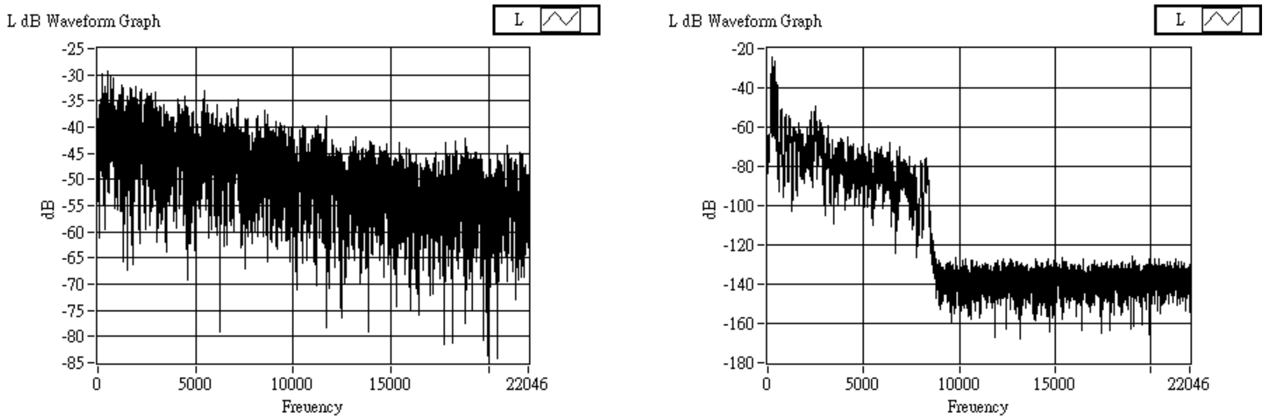
(c) The spectrum of the decrypted right channel audio



(b) The spectrum of the encrypted right channel audio



(d) The spectrum of the original left channel audio



(e) The spectrum of the encrypted left channel audio

(f) The spectrum of the decrypted left channel audio

Figure 7. The Spectrum of the original and encrypted audio

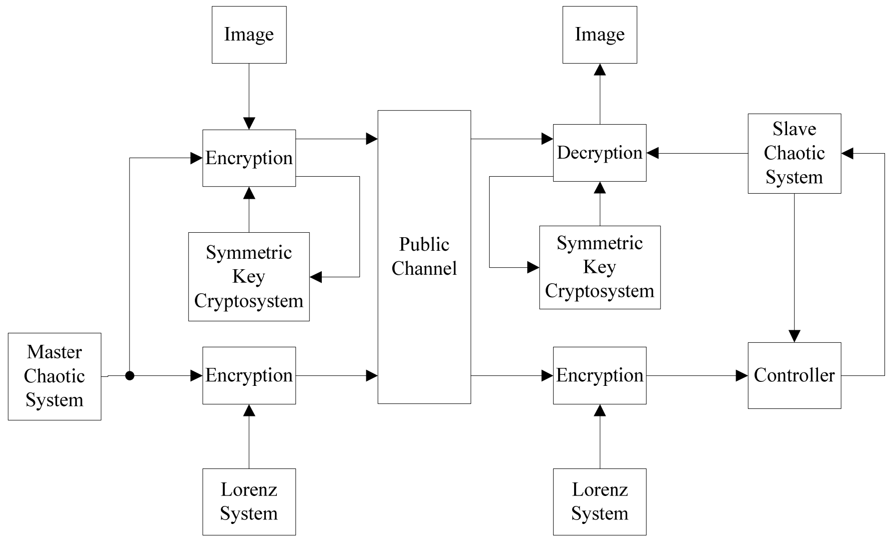
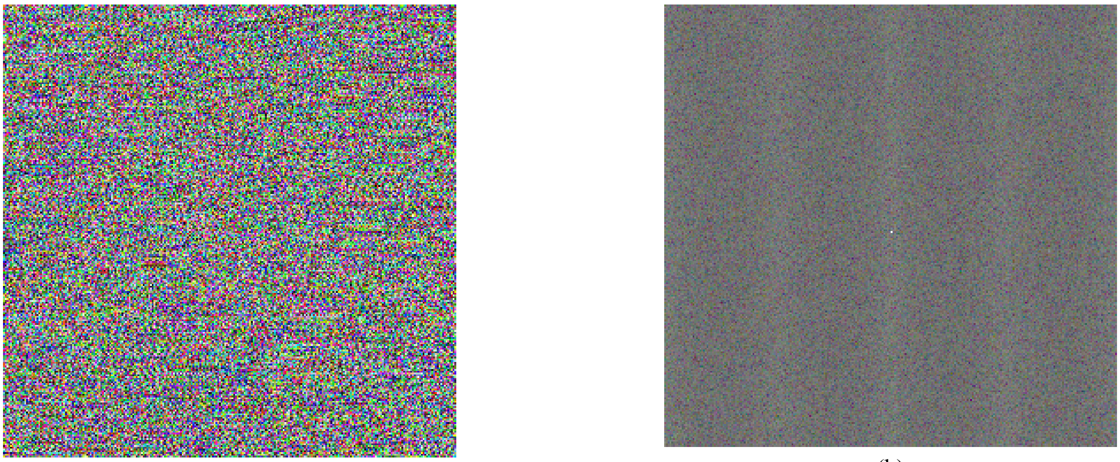


Figure 8. Image encryption/decryption flow of a chaotic synchronization cryptosystem

(a) (b)

Figure 9. The original image Lenna and its spectrum. (a) An original image; (b) The spectrum of (a)



(a) (b)

Figure 10. The encrypted image of Lenna and its spectrum. (a) An encrypted image; (b) The spectrum of (a)

(a) (b)

Figure 11. The decrypted image of Lenna and its spectrum. (a) A decrypted image; (b) The spectrum of the decrypted image

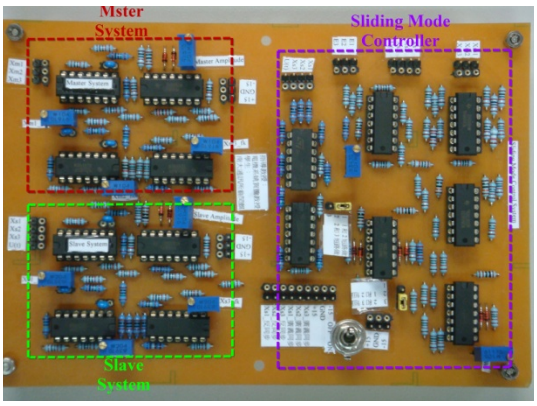


Figure 12. An entity photo of a Sprott master/slave system and a sliding mode controller

5. Conclusion

This work presents a novel robust controller scheme which operates in the sliding mode. The proposed scheme is also applied to a chaotic circuit system in order to derive a solution to the synchronization problem. Based on MATLAB and IsSpice software, simulation results indicate that the adequately designed sliding mode controller is robust and stable. This study schematically depicts the circuit hardware, implemented with OP amplifiers and RC elements. Highly promising for communications-related applications, the encryption/decryption system of audio and image signals exhibits elevated security and confidentiality during data transmission.

References

[1] **E. N. Lorenz.** Deterministic non-periodic flow. *Journal of the Atmospheric Sciences*, Vol. 20, 1963, 130–141. http://dx.doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[2] **L. O. Chua, G. N. Lin.** Canonical realization of Chua's circuit family. *IEEE Transactions on Circuits and Systems*, Vol. 37, 1990, 885-902. http://dx.doi.org/10.1109/31.55064.

[3] **A. I. Lerescu, N. Constandache, S. Oancea, I. Grosu.** Collection of master–slave synchronized chaotic systems. *Chaos, Solitons & Fractals,*

Vol. 22(3), 2004, 599–604. http://dx.doi.org/10.1016/j.chaos.2004.02.039.

[4] **E. Ott, C. Grebogi, J. A. Yorke.** Controlling Chaos. *Phys. Rev. Lett., Vol.* 64, 1990, 1196-1199. http://dx.doi.org/10.1103/PhysRevLett.64.1196.

[5] **L. M. Pecora, T. L. Carroll.** Synchronization in chaotic systems. *Phys Rev Lett Vol.* 64, 1990, 821–824. http://dx.doi.org/10.1103/PhysRevLett.64.821.

[6] **S. Chen, J. Lü.** Synchronization of an uncertain unified chaotic system via adaptive control. *Chaos, Solitons and Fractals, Vol.* 14,2002, 643-647. http://dx.doi.org/10.1016/S0960-0779(02)00006-1.

[7] **G. Wen, Q. G. Wang, C. Lin, X. Han, G. Li.** Synthesis for robust synchronization of chaotic systems under output feedback control with multiple random delays. *Chaos , Solitons and Fractals, Vol.* 29, 2006, 1142-1146. http://dx.doi.org/10.1016/j.chaos.2005.08.078.

[8] **H. Zhang, X. K. Ma, W. Z. Liu.** Synchronization of chaotic systems with parametric uncertainty using active sliding mode control. *Chaos , Solitons and Fractals, Vol.* 21,2004, 1249-1257. http://dx.doi.org/10.1016/j.chaos.2003.12.073.

[9] **T. Yang, L. O. Chua.** Impulsivee stabilization for control and synchronization of chaotic systems: theory and application to secure communication. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.* 44(10), 1997, 976-988. http://dx.doi.org/10.1109/81.633887.

[10] **H. Dedieu, M. Ogorzalek.** Signal coding and compression based on chaos control techniques. *IEEE International Symposium on Circuits and Systems, Vol.* 2, 1991, 1191-1194.

[11] **A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, K. M. Cuomo.** Signal processing in the context of chaotic signals. *IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol*. 4, 1992, 117-120.

[12] **H. Dedieu, M. P. Kennedy, M. Hasler.** Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Vol.* 40, 1993, 634-642. http://dx.doi.org/10.1109/82.246164.

[13] **N. J. Corron, D. W. Hahs.** A new approach to communications using chaotic signals. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 44, 1997, 373-382. http://dx.doi.org/10.1109/81.572333.

[14] **K. M. Short.** Uumasking a modulated chaotic communications scheme. *International. Journal of Bifurcation and Chaos, Vol.* 6, 1996, 367-375. http://dx.doi.org/10.1142/S0218127496000114.

[15] **D. R. Frey.** Chaotic Digital Encoding : An Approach to Secure Communication. *IEEE Transactions on IEEE Trans. Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 40, 1993, 660-666.

[16] **T. L. Liao, S. H. Tsai.** Adaptive synchronization of chaotic systems and its application to secure communications. *Chaos Solitons and & Fractals, Vol.* 11(9), 2000, 1387-1396. http://dx.doi.org/10.1016/S0960-0779(99)00051-X.

[17] **T. Yang, L. B. Yang, C. M. Yang.** Breaking chaotic switching using generalized synchronization: Examples. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.* 45, 1998, 1062-1067. http://dx.doi.org/10.1109/81.728860.

[18] **T. Yang, C. W. Wu, L. O. Chua.** Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.* 44, 1997, 469-472. http://dx.doi.org/10.1109/81.572346.

[19] **G. Grassi, S. Mascolo.** A system theory approach for designing cryptosystems based on hyperchaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 46, 1999, 1135-1138. http://dx.doi.org/10.1109/81.788815.

[20] **T. Y. Chang, M. S. Hwang, W. P. Yang.** An improved multi-stage secret sharing scheme based on the factorization problem. *Information Technology and Control, 2011, Vol*. 40(3), 246-251. http://dx.doi.org/10.5755/j01.itc.40.3.633.

[21] **J. W. Hong, S. Y. Yoon, D. I. Park, M. J. Choi, E. J. Yoon, K. Y. Yoo,** Anew efficient key agreement scheme for vsat satellite communications based on elliptic curve cryptosystem. *Information Technology and Control, 2011, Vol*. 40(3), 252-259.

[22] **A. G. AK, G. Cansever, A. Delibasi.** Robot trajectory tracking with adaptive RBFNN-based fuzzy sliding mode control. *Information Technology and Control, 2011, Vol*. 40(2), 151-156.

[23] **J. C. Sprott.** A new class of chaotic circuits. *Phys Lett A Vol.* 266, 2000, 19–23. http://dx.doi.org/10.1016/S0375-9601(00)00026-8.

[24] **D. I. R. Almeida, J. Alvarez, J. G. Barajas.** Robust synchronization of Sprott circuits using sliding mode control. *Chaos, Solitons and Fractals Vol.* 30(1), 2006, 11-18. http://dx.doi.org/10.1016/j.chaos.2005.09.011.

[25] **J. E. Slotine, W. Li.** *Applied Nonlinear Control*, New Jersey, Prentice-Hall, 1991.

Received February 2011.