RESEARCH ARTICLE

Design and Hardware Implementation of a New Chaotic Secure Communication Technique

Li Xiong[1,2], **Yan-Jun Lu**[1]*, **Yong-Fang Zhang**[3], **Xin-Guo Zhang**[4], **Parag Gupta**[5]

1 School of Mechanical and Precision Instrument Engineering, Xi'an University of Technology, Xi'an, 710048, China, **2** School of Physics and Electromechanical Engineering, He'xi University, Zhang'ye, 734000, China, **3** School of Printing, Packaging Engineering and Digital Media, Xi'an University of Technology, Xi'an, 710048, China, **4** School of Information Science and Engineering, Lan'zhou University, Lan'zhou, 730000, China, **5** Robert R. McCormick School of Engineering and Applied Science, Northwestern University, Evanston, IL, 60208, United States of America

* yanjunlu@xaut.edu.cn

Citation: Xiong L, Lu Y-J, Zhang Y-F, Zhang X-G, Gupta P (2016) Design and Hardware Implementation of a New Chaotic Secure Communication Technique. PLoS ONE 11(8): e0158348. doi:10.1371/journal.pone.0158348

Editor: Jun Ma, Lanzhou University of Technology, CHINA

Received: April 24, 2016

Accepted: June 14, 2016

Published: August 22, 2016

Data Availability Statement: All relevant data are within the manuscript.

Funding: The authors are greatly thankful for the help and support from the National Natural Science Foundation of China (Grant No. 51505375), Open Project of State Key Laboratory of Mechanical Transmission (Grant No. SKLMT-KFKT-201510), Scientific Research Program of Shanxi Provincial Education Department of China (15JS068, 15JK1549).

Competing Interests: The authors have declared that no competing interests exist.

Abstract

In this paper, a scheme for chaotic modulation secure communication is proposed based on chaotic synchronization of an improved Lorenz system. For the first time, the intensity limit and stability of the transmitted signal, the characteristics of broadband and the requirements for accuracy of electronic components are presented by Multisim simulation. In addition, some improvements are made on the measurement method and the proposed experimental circuit in order to facilitate the experiments of chaotic synchronization, chaotic non-synchronization, experiment without signal and experiment with signal. To illustrate the effectiveness of the proposed scheme, some numerical simulations are presented. Then, the proposed chaotic secure communication circuit is implemented through analog electronic circuit, which is characterized by its high accuracy and good robustness.

1. Introduction

Since the American scholars Pecora and Carroll proposed a type of drive-response synchronization scheme [1], researchers on chaos have been greatly inspired. As are well known, the chaotic signals have the following characteristics: sensitive dependence on the initial conditions, unpredictability, similarity to the noise, and difficulty to be deciphered. Therefore, it is especially suitable to be applied to the secure communication field. Chaotic secure communication is one of the most remarkable phenomena in the present physical field, and it is one of the most promising applications in chaotic circuits. What presented is very different from the previous findings. Chaotic secure communication can be shown to correspond to the phenomenon of resonance and mode locking in nature, and it also utilizes the ergodic property that is an important feature of chaos. Thus it has caused huge attention from various industries.

Several works can be found in literature about chaotic secure communications. As early as 1993, Cuomo and Oppenheim implemented the masking secure communication scheme of

Lorenz system [2, 3]. In 1996, Milanović and Zaghloul put forward an improved scheme of chaotic masking secure communication [4]. Later the chaotic secure communication circuit was implemented by electronic components [5] based on Lorenz system according to work [4]. With the fast development of chaotic secure communication, work [6] approached the problem of synchronization of chaotic systems from the perspective of Generalized Hamiltonian systems. Then, that approach was applied to the chaotic secure communication system based on two Chua's oscillators and an experimental implementation was presented by using CCII plus s [7]. In 2009, Arman et al. proposed a fractional chaotic communication method using an extended fractional Kalman [8]. The proposed stabilization conditions were used in work [9] to design a linear-state-observer for the secure communization of a wide class of discrete-time hyperchaotic system via a scalar transmitted signal. In work [10] a new chaotic secure communication scheme was proposed based on chaotic Duffing oscillators and frequency estimation for the transmission of binary-coded messages. In work [11] a chaotic modulation secure communication scheme was proposed based on improved Chua's circuit. In work [12], the design and implementation of adaptive Generalized Projective Synchronization (GPS) are studied between two chaotic circuits (master and slave) via a scalar transmitted signal and by a new method not requiring the same structure of master and slave circuits. In addition, it is well known that chaotic attractor can be properly used in secure communication system. Particularly, the chaotic systems composed of multi-scroll attractors are much preferred to the double-scroll attractors because they offer more dynamical complexity [13–19]. In order to transmit high-speed data, the chaotic attractors should operate at high frequency. However, it is difficult to enhance the frequency response of analog realizations of chaotic oscillator when it is designed with integrated circuit technology. Besides, FPGA based realization emerged as a solution to observe attractors at high frequency. In the paper [20], it has been shown that by using FPGAs one can realize multi-scroll chaotic oscillators that have better behavior than by using active devices like operational amplifiers. In work [21] a FPGA realization of a chaotic communication system was proposed to be applied to image processing. Synchronization can also be extended to complex topologies with multi-scroll attractors [22, 23].

Despite the fact that chaotic secure communication has advantages of strong real-time performance and high security performance, the study of chaotic secure communication is still in the phase of laboratory research [24–27]. Many problems still need to be solved in the study of chaotic secure communication. On one hand, the contradiction between the confidential party and the broken party often leads to a complex circuit implementation [28–37]. Therefore, because most researchers still focus on the study of chaos theory in numerical simulation, there is a certain deviation of the physical circuit system. On the other hand, some shortcomings in terms of fidelity and safety of most chaotic secure communication schemes could not guarantee a system retained synchronization in theory under large signal conditions. In addition, being lack of optimization and improvement on the experimental circuit and measurement method, the comprehensive statements are precluded from being drawn from experimental results. In general, the three main types of chaotic secure communication are chaotic masking [4], chaotic modulation [25] and chaotic shift keying [38]. The chaotic modulation method has the following advantages compared with the other two types: first, it is used to hide the whole range of chaotic signal spectrum information allowing for a wide spectrum of feature; second, it is more sensitive to parameter variation, thereby enhancing the confidentiality. In this paper, a chaotic modulation method is proposed to establish secure communication based on an improved Lorenz chaotic optimization circuit.

The main contributions of this paper include: In Section 2, the active control method is adopted to control the improved Lorenz chaotic system. With active control method, the synchronization error system can be asymptotically stabilized at the origin. In Section 3, the chaotic modulation secure communication scheme is proposed based on synchronization of chaos between a transmitter and a receiver linked by a transmission channel. In the proposed scheme, with an improved Lorenz system as chaos generator, the chaotic modulation secure communication is implemented by using some electronic components containing analog multipliers, operational amplifiers, resistors, and capacitors. In Section 4, because the implementation of the Lorenz circuit needs analog multipliers, higher accuracy requirements on the parameters of the electronic components is necessary. Therefore, the intensity limit and stability of the transmitted signal, the broadband characteristic, and the accuracy requirements of electronic components are presented for the first time by Multisim simulation. In Section 5, some improvements on the experimental circuit and measurement method of the proposed secure communication circuit are introduced. Experiments of chaotic synchronization, experiments of chaotic non-synchronization, experiments without signal, and experiments with signal are presented to verify the comprehensive performance of the proposed scheme. Some numerical simulations are presented to verify the feasibility and effectiveness of the scheme.

Moreover, the study on chaotic circuit is the premise and foundation of the physical circuit verification. Also, it can deepen the understanding of chaos and expand its application scope. In Section 6, the proposed secure communication circuit is implemented in an analog electronic circuit. The analog circuit implementation results match the Multisim and Matlab simulation results. Such measurement method and experimental results have not been reported previously. Thus, the results of this work are quite valuable in practical application. Finally, conclusions and discussions are presented in Section 7. The proposed scheme is not restricted to the Lorenz system and, in fact, can also be used in other chaotic systems.

2. Synchronization of Improved Lorenz Chaotic System

The basic Lorenz equation is described as follows:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = \rho x - y - xz \\ \dot{z} = xy - \beta z \end{cases} \tag{1}$$

When choosing $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$, system (1) is chaotic. However, the numerical solutions of the basic Lorenz equation are not able to be implemented by using general circuit components. Thus, in practice, these variables often needs to be adjusted properly. The introduction of new variables is described as follows:

$$u = \frac{x}{10}, \quad v = \frac{y}{10}, \quad w = \frac{z}{30} \tag{2}$$

Substituting the specific parameter values, eq (1) becomes

$$\begin{cases} \dot{x} = -10x + 10y \\ \dot{y} = 28x - y - 30xz \\ \dot{z} = 3.3xy - (8/3)z \end{cases} \tag{3}$$

This is the improved Lorenz chaotic system. It fully conforms to the requirements of the circuit design in practical applications.

The drive system is provided for

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1), \\ \dot{x}_2 = bx_1 - x_2 - 30x_1x_3, \\ \dot{x}_3 = 3.3x_1x_2 - cx_3, \end{cases} \tag{4}$$

When choosing $a = 10$, $b = 28$, and $c = 8/3$, system (4) is chaotic, and the response system is described as follows:

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) + u_1, \\ \dot{y}_2 = by_1 - y_2 - 30y_1y_3 + u_2, \\ \dot{y}_3 = 3.3y_1y_2 - cy_3 + u_3, \end{cases} \tag{5}$$

where u_1, u_2, and u_3 are the controllers [39]. When the synchronization error is defined as $\dot{e} = \dot{y} - \dot{x}$, then the synchronization error of systems (4) and (5) can be described as follows:

$$\begin{cases} \dot{e}_1 = a(e_2 - e_1) + u_1, \\ \dot{e}_2 = be_1 - e_2 - 30y_1y_3 + 30x_1x_3 + u_2, \\ \dot{e}_3 = 3.3y_1y_2 - 3.3x_1x_2 - ce_3 + u_3, \end{cases} \tag{6}$$

The controller is constructed as follows:

$$\begin{cases} u_1 = -a(e_2 - e_1) - k_1e_1 \\ u_2 = -30x_1x_3 + 30y_1y_3 + e_2 - be_1 - k_2e_2 \\ u_3 = ce_3 + 3.3x_1x_2 - 3.3y_1y_2 - k_3e_3 \end{cases} \tag{7}$$

where $k_i > 0(i = 1,2,3)$, for controlling the speed of synchronization.

Substituting Eqs (7) into (6), the following is obtained:

$$\begin{cases} \dot{e}_1 = -k_1e_1, \\ \dot{e}_2 = -k_2e_2, \\ \dot{e}_3 = -k_3e_3, \end{cases} \tag{8}$$

To facilitate the control design, the Lyapunov function V [40, 41] is defined as follows:

$$V = (e_1^2 + e_2^2 + e_3^2)/2, \tag{9}$$

Obviously, V is positively definite. It follows from eq (9) that,

$$\begin{aligned} \dot{V} &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 \\ &= e_1(-k_1e_1) + e_2(-k_2e_2) + e_3(-k_3e_3) \\ &= -k_1e_1^2 - k_2e_2^2 - k_3e_3^2 \end{aligned} \tag{10}$$

Then, $\dot{V} = -k_1e_1^2 - k_2e_2^2 - k_3e_3^2 \leq 0$ is obtained. Thus, $\dot{V}$ is negatively semidefinite.

According to Lyapunov stability theory, if V is positively definite and $\dot{V}$ is negatively semidefinite, then the system is consistent and stable at the origin of the equilibrium state. Therefore, the synchronization error system (6) is asymptotically stable at the origin. That is, $\lim_{t\to\infty} |e(t)| \to 0$. This proves that the active synchronization between the drive system and the response system is achieved.

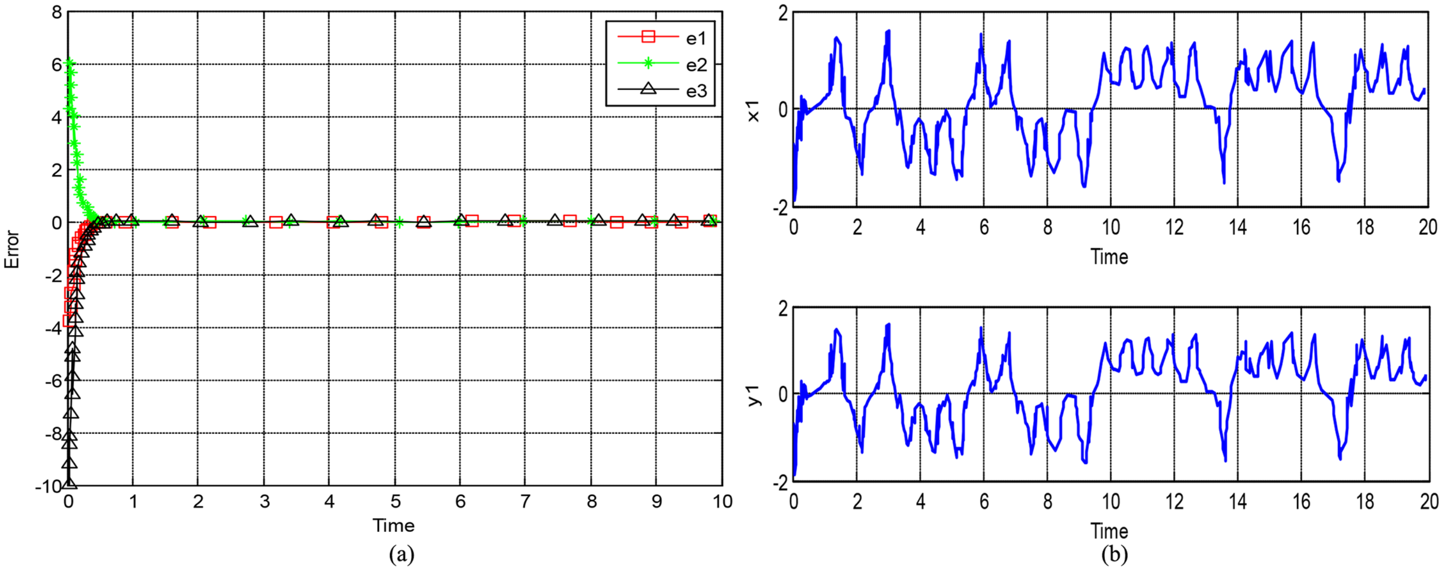


Fig 1. Synchronization error curve and waveform. For **(a)** synchronization error, for **(b)** synchronized waveform of $x_1 - y_1$.

doi:10.1371/journal.pone.0158348.g001

In the following simulation, the initial values of the drive system are chosen as $x_1(0) = 2$, $x_2(0) = -3$, and $x_3(0) = 6$. The initial values of the response system are chosen as $y_1(0) = -3$, $y_2(0) = 5$, and $y_3(0) = -4$. The control gains are chosen as $k_1 = k_2 = k_3 = 10$. The synchronization error curves are shown in Fig 1(a). As can be seen from the figures, for less than 1 second, the synchronization errors e_1, e_2, and e_3 can be asymptotically stabilized at the origin. Fig 1(b) shows the timing diagram of $x_1 - y_1$. The waveforms of the two systems are shown to be the same, and the active control synchronization is implemented. The method is simple and practical, and the synchronization time is very short. As is well known in practical application, the smaller the control signal is, the more easily the hardware circuit of the control process is implemented. Therefore, the proposed scheme is easier to be implemented in the hardware circuit because of its low control signal and low cost.

3. Proposed Chaotic Secure Communication Circuit Scheme

The implementation of chaotic synchronization [42] solves a large and difficult problem of chaotic secure communication technology [43,44]. Although the chaotic system is especially suitable for secure communication, the synchronization between a transmitting system and a receiving system should be completed in order to achieve Lorenz chaotic secure communication. Through analysis and optimization of the improved Lorenz circuit, inverter and adder were added, thus realizing the evolution from freedom chaos after chaotic synchronization to secure communication. Here, the chaotic secure communication is implemented by using chaotic modulation.

The preceding active control scheme of synchronization is applied to establish a chaotic secure communication circuit. The chaotic modulation secure communication circuit schematic based on improved Lorenz system is shown in Fig 2 by using Multisim software. The left side of the circuit is the transmitting system. The right side of the circuit is the receiving system. The uppermost operational amplifiers of the transmitting system are designed as a modulator. The modulation circuit consisting of an inverting adder and an inverter plays a signal superposition function. Its output signal is transmitted to the receiving system through a communication channel (wired or wireless). The chaotic circuit of the receiving system is the same as the

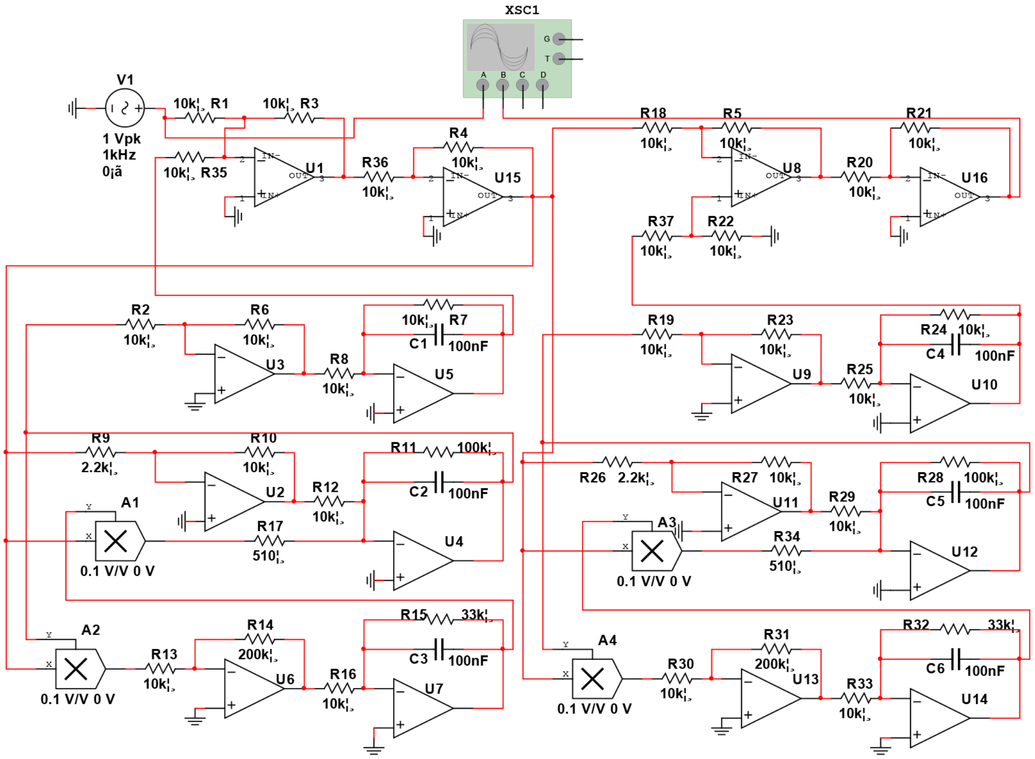


Fig 2. Chaotic secure communication optimization circuit schematic.

doi:10.1371/journal.pone.0158348.g002

transmitting system. The uppermost operational amplifier of the receiving system are designed as a demodulator, which is composed of a same-phase adder. Its input is chaotic signal, and its output is the error signal of two chaotic signals, that just happens to be the transmitted signal of the transmitter, thus completing the chaotic secure communication.

The whole process of the proposed chaotic secure communication can be expressed as follows: suppose $x(t)$ is a transmitted signal, $s(t)$ is a chaotic signal, and $y_1(t)$ is superimposed signal. Then the superimposed signal is described as:

$$y_1(t) = x(t) + s(t) \tag{11}$$

$-y_1(t)$ is the output from the inverting adder of modulation circuit, given by

$$-y_1(t) = x(t) + s(t) \tag{12}$$

The output after the inverter becomes

$$y_2(t) = -y_1(t) \tag{13}$$

The superimposed signal is described as

$$y_1(t) = -x(t) - s(t) \tag{14}$$

$y_2(t)$ is the output signal from the modulation circuit, given that

$$y_2(t) = x(t) + s(t) \tag{15}$$

$m(t)$ is a received signal, given that

$$m(t) = -[s(t) - y_2(t)] = x(t) \tag{16}$$

In this way, the receiving system maintains synchronized with the transmitting system more easily, and the robustness of the circuit is maintained. Such an approach can prevent the effective information from being intercepted in the process of communication.

4. Multisim Simulation Experiments

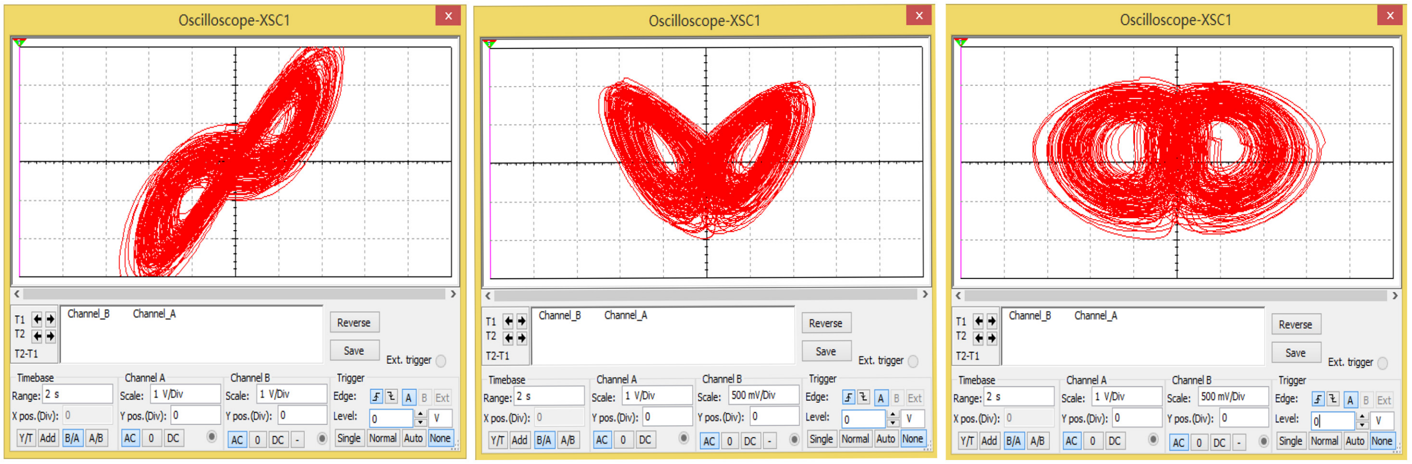
Before making the actual circuit, some simulations for the proposed chaotic secure communication optimization circuit by using Multisim software were conducted. The chaotic simulation phase diagrams of *xy*, *xz*, and *zy* are shown in Fig 3 by using Multisim software.

4.1. Synchronous Experiments

Here, the verification of whether two identical parameters of Lorenz optimization circuit can achieve the signal transmission and reception without distortion through synchronous experiments was conducted. The experimental circuit is shown in Fig 2, and the component parameters of the transmitting circuit are completely consistent with the receiving circuit.

(1) Given an input sine wave with amplitude of 1 V and frequency of 1 kHz, the simulation results are shown as Fig 4. In order to verify that the proposed circuit can transmit various signals without distortion, square wave and triangular wave with amplitude of 1 V and frequency of 1 kHz were input. Simulation results show that, no matter what kind of signal is input, the two chaotic circuits can be completely synchronized if the component parameters of the transmitting circuit are entirely same as the receiving circuit. The modulation-demodulation signal waveform and the synchronous phase diagram of the receiver and the transmitter are shown in Fig 4(a), 4(b) and 4(c). Negligible distortion can be observed. The carrier signal waveform of the receiver and the transmitter is shown in Fig 4(d), and it is chaotic.

(2) In order to verify whether the proposed circuit has a choice for the intensity of various input signals, sine wave with frequency of 1 kHz and amplitude of 10 mV, 100 mV, 1 V, 5 V, 7 V, 10 V, 13 V, 15 V were input, and some simulation results are shown in Fig 5. From these



Timebase Range: 2 s X pos.(Div): 0
Channel A Scale: 1 V/Div Y pos.(Div): 0
Channel B Scale: 1 V/Div Y pos.(Div): 0
Trigger Edge: A Level: 0 V

Timebase Range: 2 s X pos.(Div): 0
Channel A Scale: 1 V/Div Y pos.(Div): 0
Channel B Scale: 500 mV/Div Y pos.(Div): 0
Trigger Edge: A Level: 0 V

Timebase Range: 2 s X pos.(Div): 0
Channel A Scale: 1 V/Div Y pos.(Div): 0
Channel B Scale: 500 mV/Div Y pos.(Div): 0
Trigger Edge: A Level: 0 V

(a) (b) (c)

Fig 3. Chaotic phase diagram with Multisim. (a) *xy* phase diagram, **(b)** *xz* phase diagram, **(c)** *zy* phase diagram.

doi:10.1371/journal.pone.0158348.g003

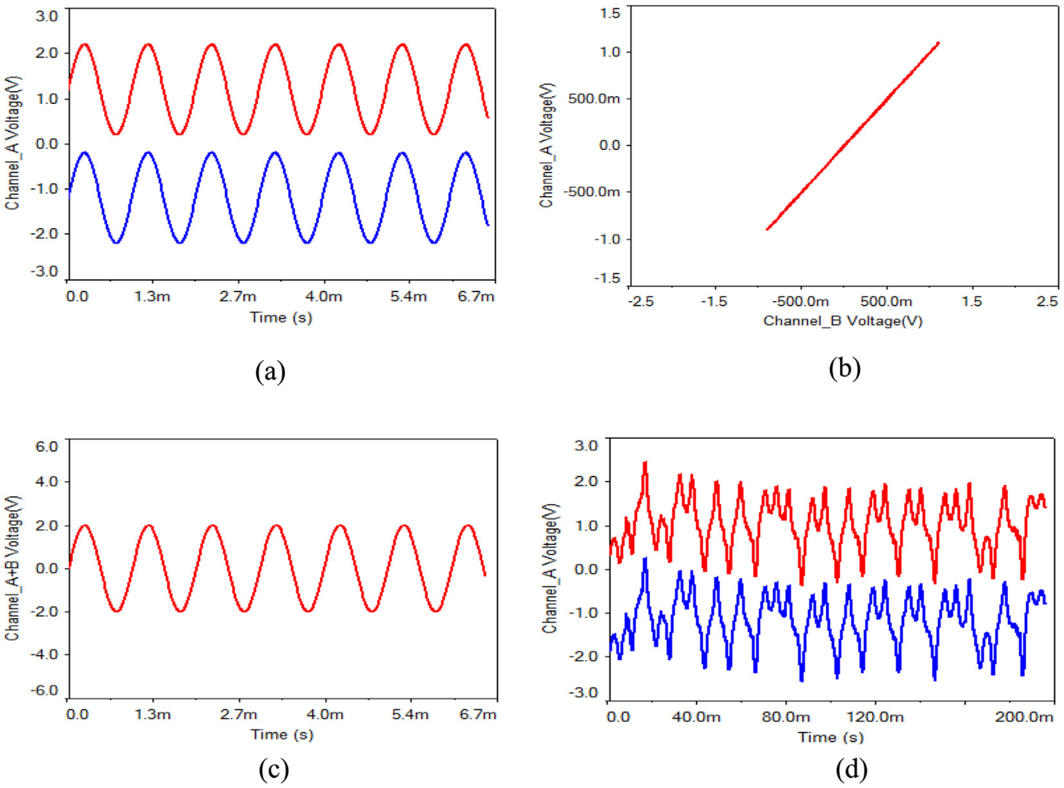


Fig 4. Waveforms of input sine wave with amplitude of 1 V and frequency of 1 kHz. (a) transmitting and receiving waveform, **(b)** synchronous phase diagram, **(c)** superimposed signal waveform, **(d)** carrier signal waveform.

doi:10.1371/journal.pone.0158348.g004

waveforms, it is concluded that signal transmission distortion will appear when the signal amplitude reaches 13 V, as shown in Fig 5(e) and 5(f). When the signal amplitude reaches 15 V, the signal distortion is very obvious, as shown in Fig 5(g) and 5(h).

(3) In order to verify whether the proposed circuit has a choice for the input signal frequency, sine wave with amplitude of 1 V and frequency of 10 Hz, 100 Hz, 1 kHz, 10 kHz, 100 kHz, 500 kHz were input, and some simulation results are shown in Fig 6. From these waveforms, it is concluded that the proposed circuit can transmit the signal from 1 Hz to 50 kHz without distortion. When the signal frequency reaches 100 kHz, the signal distortion is very obvious, as shown in Fig 6(c) and 6(d). Therefore, it can be seen that the circuit is broadband.

4.2. Error Experiments

If an error exists in the parameter of a certain circuit component in the proposed chaotic secure communication circuit, whether or not the circuit can also keep synchronized is a question worthy to consider. In the experiments, we choose analog multiplier, capacitor, and operational amplifier to carry out the error analysis for the proposed chaotic secure communication circuit.

(1) Analog multiplier: As is shown in Fig 2, the output gains of four analog multipliers are 0.1 V/V. In the experiments, when a multiplier parameter of the receiving circuit is chosen as 0.11 V/V, the waveform and the phase diagram are shown in Fig 7(a) and 7(b). What can be seen is that the synchronization can be implemented when a multiplier parameter of the receiving circuit has a small error of 0.1%, but there is a faint noise.

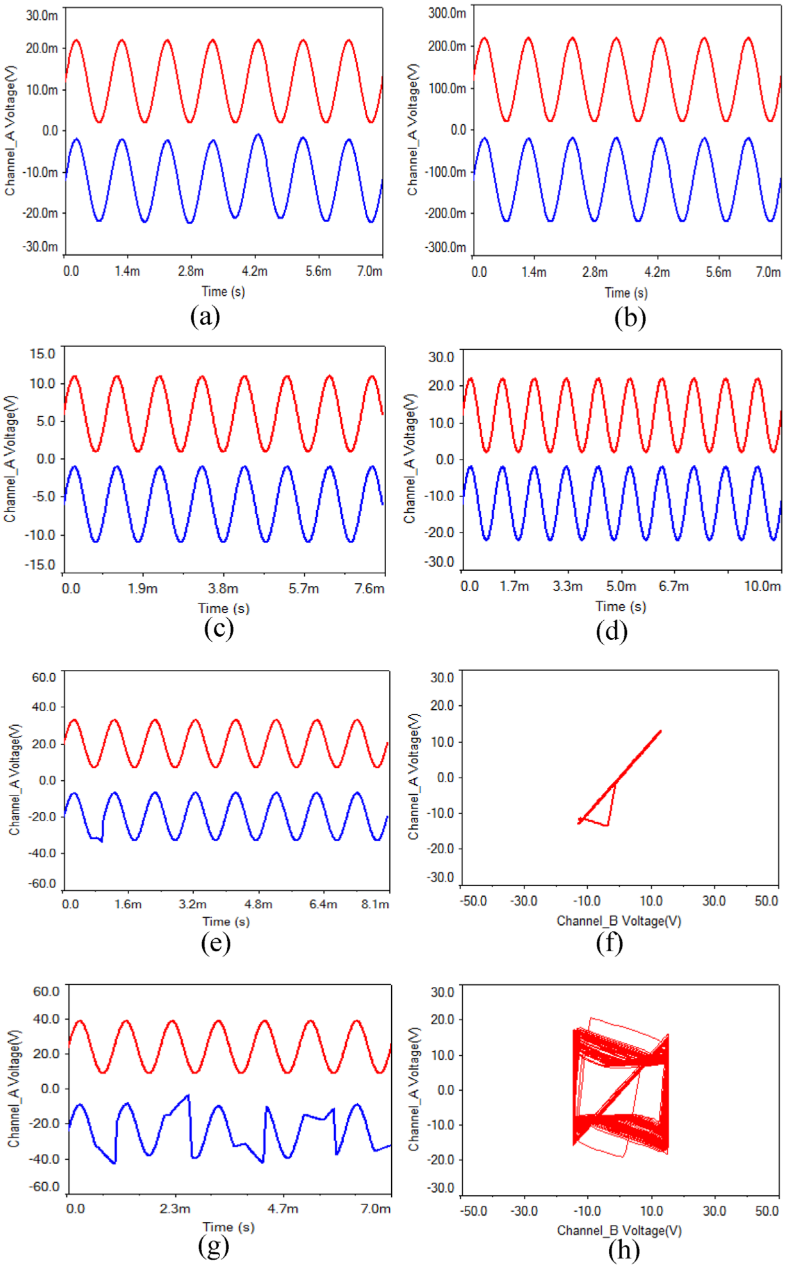
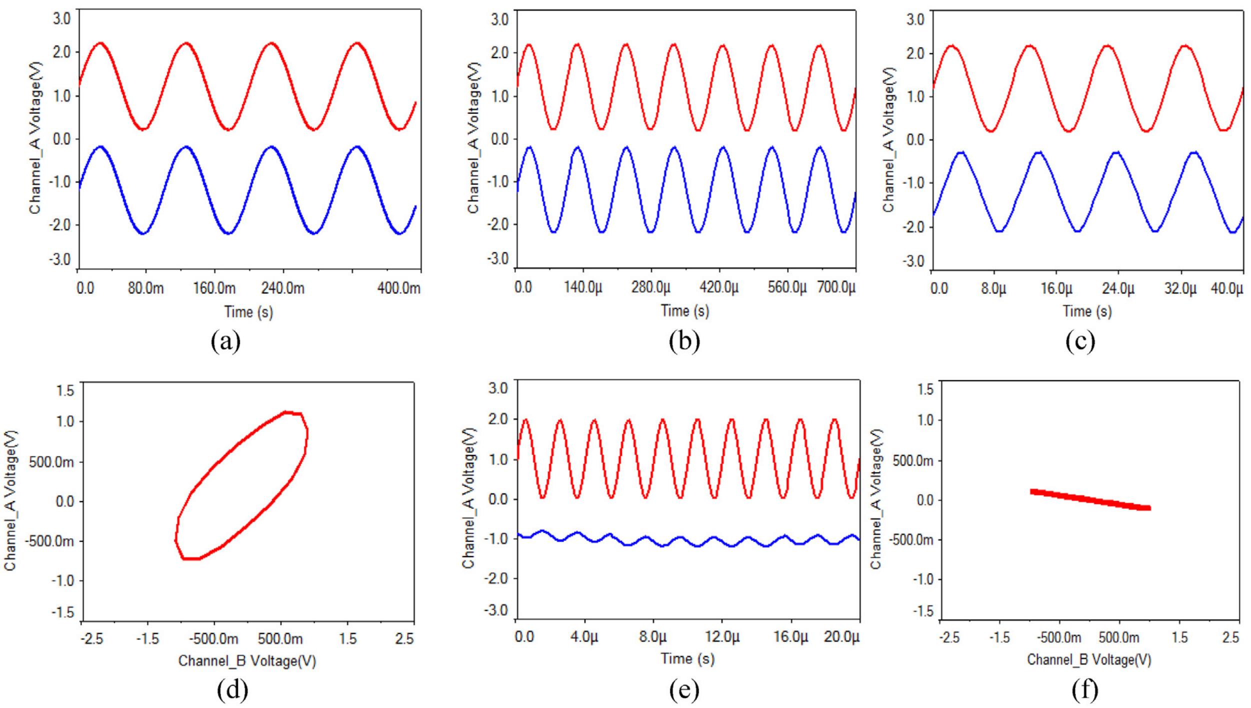


Fig 5. Waveforms of input sine wave with different amplitude. (a) 10 mV, **(b)** 100 mV, **(c)** 5 V, **(d)** 10 V, **(e)** 13 V, **(f)** synchronous phase diagram of 13 V, **(g)** 15 V, **(h)** phase diagram of 15 V.

doi:10.1371/journal.pone.0158348.g005

Then, when a multiplier parameter of the receiving circuit is chosen as 0.2 V/V, the waveform and the phase diagram are shown in Fig 8(a) and 8(b). From the experimental results, what can be seen is that the synchronization can be still realized when an analog multiplier parameter of the receiving circuit has an error of 1%, but the noise is obvious.

(2) Capacitor: As is shown in Fig 2, the capacitor values of the transmitting circuit and the receiving circuit are 100 nF. In the experiments, when the value of C4 is chosen as 101 nF, the waveform and the phase diagram are shown in Fig 9(a) and 9(b). What can be seen is that the



(a) (b) (c)

(d) (e) (f)

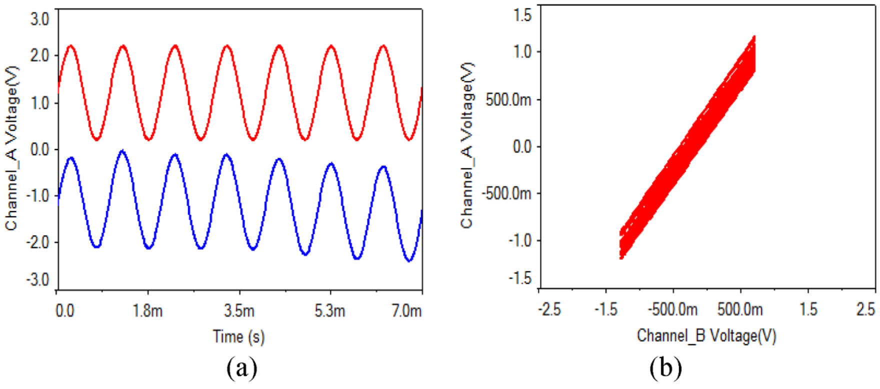
Fig 6. Waveforms of input sine wave with different frequency. (a) 10 Hz, **(b)** 10 kHz, **(c)** 100 kHz, **(d)** phase diagram of 100 kHz, **(e)** 500 kHz, **(f)** phase diagram of 500 kHz.

doi:10.1371/journal.pone.0158348.g006

synchronization can be implemented when a capacitor value of the receiving circuit has an error of 1%, and there is almost no noise.

(3) Operational amplifier: What can be seen from Fig 10 is that the synchronization can be implemented when an operational amplifier parameter of the receiving circuit has an error of 1%, and there is almost no noise.

Consequently, it is very important to select appropriate circuit components in the practical chaotic secure communication experiments. For the Lorenz system, the choice of analog multiplier is the most critical one. The sensitivity of chaotic circuit to initial value also requires that



(a) (b)

Fig 7. Analog multiplier of receiving circuit with 0.1% error. (a) transmitting and receiving waveform, **(b)** phase diagram.

doi:10.1371/journal.pone.0158348.g007

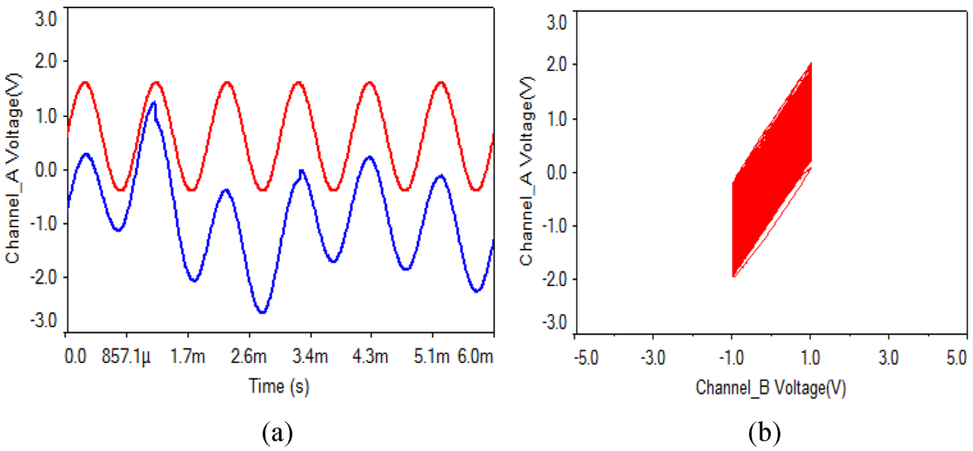


Fig 8. Analog multiplier of receiving circuit with 1% error. (a) transmitting and receiving waveform, **(b)** phase diagram.

doi:10.1371/journal.pone.0158348.g008

the accuracy of synchronous circuit be improved greatly. In particular, the noise may be caused due to the discretization of the parameters of the analog multipliers.

5. Experimental Improvement and Numerical Analysis

In order to facilitate the experiments of chaotic synchronization, experiments of chaotic non-synchronization, experiments without signal, and experiments with signal, the following improvements are carried out to verify the comprehensive performance of the proposed scheme in the experiments. The improved chaotic secure communication circuit schematic is shown in Fig 11. The improved principles are given as follows:

1. $k(1)$ is set up to control the transmitted signal $m(t)$ with or without signal. The formula is expressed as $m(t)\times k(1)$. When the signal is not modulated, $k(1) = 0$. When the signal is modulated, $k(1) = 1$.
2. $k(2)$ is set up to control the transmission system, which is an independent Lorenz chaotic circuit without modulation or with modulation. For Lorenz chaotic circuit without

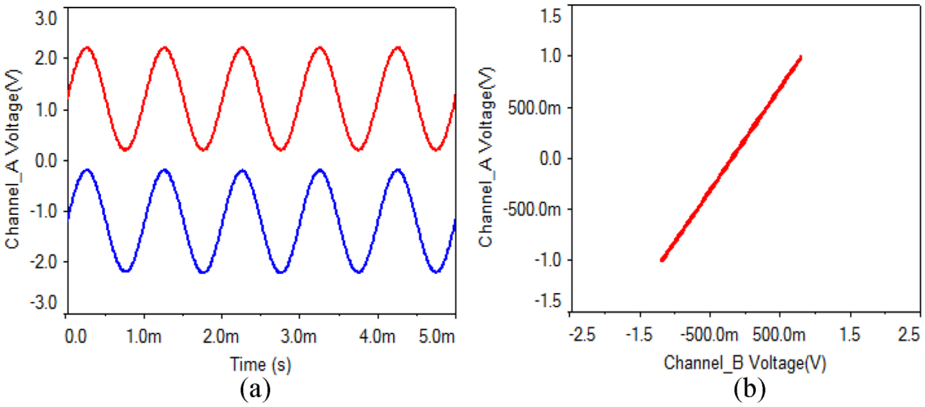


Fig 9. Capacitor of receiving circuit with 1% error. (a) transmitting and receiving waveform, **(b)** phase diagram.

doi:10.1371/journal.pone.0158348.g009

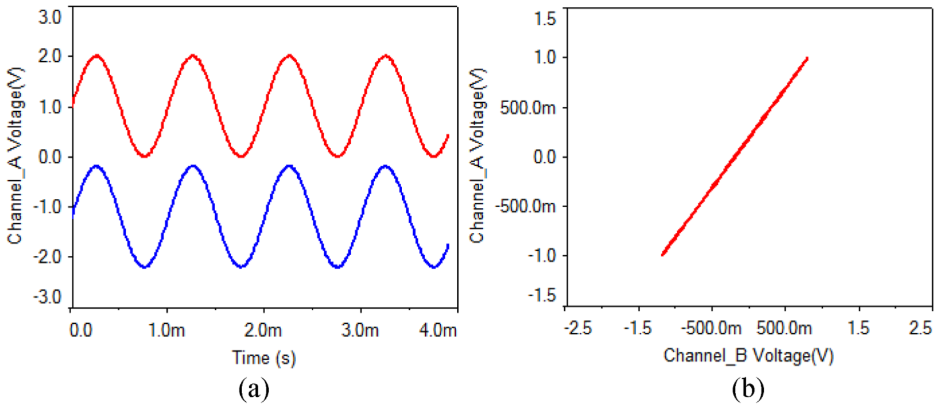


Fig 10. Operational amplifier of receiving circuit with 1% error. (a) transmitting and receiving waveform, **(b)** phase diagram.

doi:10.1371/journal.pone.0158348.g010

modulation, $k(21) = 0$ and $k(23) = 1$. The formula is expressed as $s(t) = x_1 + m(t)\times k(1)$. For modulated Lorenz chaotic circuit, $k(21) = 1$ and $k(23) = 0$.

3. $k(3)$ is set up to control whether the receiving system is synchronized with the transmitting system. When they are not synchronized, $k(31) = 0$ and $k(33) = 1$. At that time, the circuit is an independent Lorenz chaotic circuit, and the non-synchronization experiments can be made by two independent Lorenz circuits. When synchronized, $k(31) = 1$ and.$k(33) = 0$ The formula is expressed as $n(t) = s(t)\times k(31)+x_2\times k(33)$.

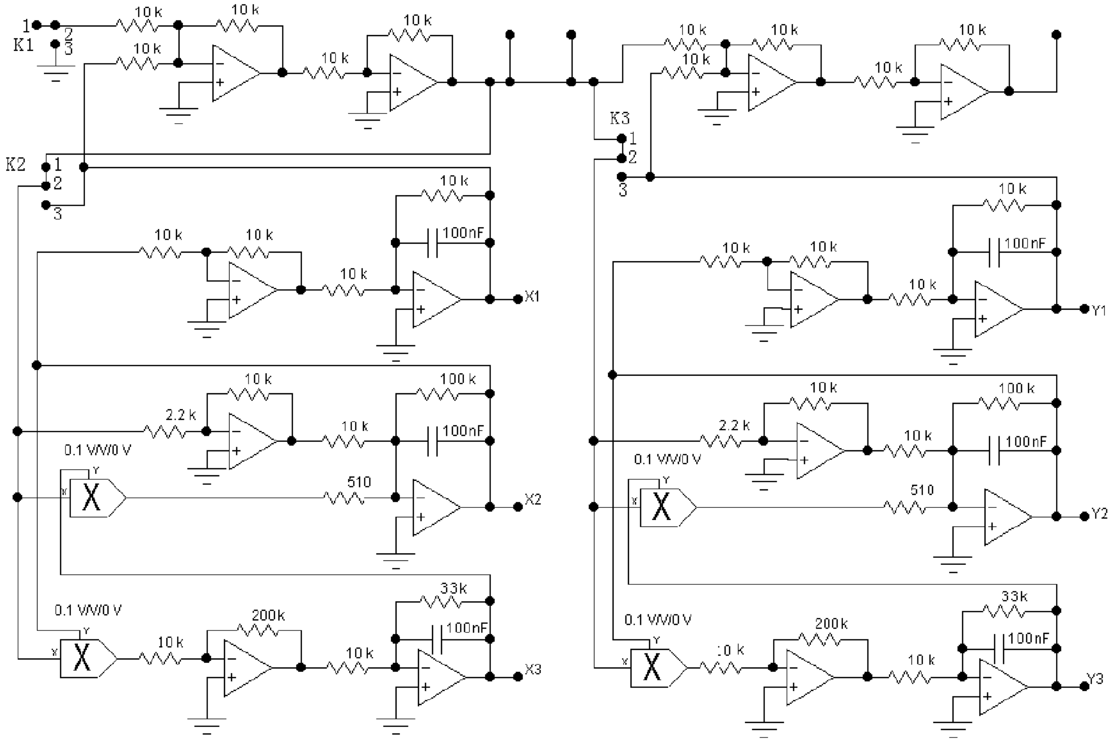


Fig 11. Experimental improvement circuit schematic.

doi:10.1371/journal.pone.0158348.g011

Therefore, the complete formula can be described as follows:

$$\begin{cases} s(t) = x_1 + m(t) \times k(1), \\ \dot{x}_1 = -10x_1 + 10y_1, \\ \dot{y}_1 = 45s(t) - y_1 - 19.6s(t)z_1, \\ \dot{z}_1 = 20s(t)y_1 - 3z_1, \end{cases} \tag{17}$$

And

$$\begin{cases} n(t) = s(t) \times k(31) + x_2 \times k(33) \\ \dot{x}_2 = -10x_2 + 10y_2 \\ \dot{y}_2 = 45n(t) - y_2 - 19.6n(t)z_2 \\ \dot{z}_2 = 20n(t)y_2 - 3z_2 \end{cases} \tag{18}$$

In the following, Matlab simulation results are shown in Fig 12. Fig 12(a) and 12(b) show the chaotic attractors of the transmitter and the receiver. The waveforms for the state variables of x, y, and z are given in Fig 12(c), 12(d) and 12(e). Fig 12(f), 12(g) and 12(h) show the non-synchronization phase diagrams of x_1x_2,y_1y_2, and z_1z_2. Fig 12(i) shows the modulation and demodulation phase diagram. Fig 12(j) shows the modulation signal and the demodulation signal waveforms. The frequency spectrum of the transmitted signal and the recovered signal are given in Fig 12(k). What can be seen from Fig 12(k) is that the spectrum of the transmitted signal is fully embedded into the chaotic signal spectrum, and the transmitted signal is recovered after synchronization.

6. Hardware Implementation

In this paper, the proposed Lorenz chaotic secure communication circuit is characterized by its high accuracy and good robustness. In order to verify this conclusion, a new master-slave chaotic modulation communication circuit is tested. The actual circuit diagram is shown in Fig 11. The key to a successful circuit experiment and high or low output indicator is the consistency of the corresponding components of the transmitting circuit and the receiving circuit. The standard error is defined as follows:

$$R_e = \sqrt{\frac{\sum_{i=1}^{n} (e_{si} - e_{ri})^2}{n}}, \tag{19}$$

where e is the measurement parameter of resistor and capacitor. The subscript s and r respectively represent the transmitting end and the receiving end, and i is a label. Then R_e represents the total error of the circuit parameters. Here, the operational amplifiers are considered as ideal components.

K_1: When the modulation signal is not added, the modulation signal input of the transmitting system needs to be grounded in order to eliminate interference. At this point, the 2–3 terminal of K_1 is connected, and it is changed to the 1–2 terminal coupled with the signal.

K_2: It is not only the circuit control of the transmitting system, but also the experimental control of synchronization and non-synchronization. When the 2–3 terminal is connected, the transmitting system constitutes an independent Lorenz unit circuit. When the 1–2 terminal is connected, the transmitting system is connected with the modulation circuit.

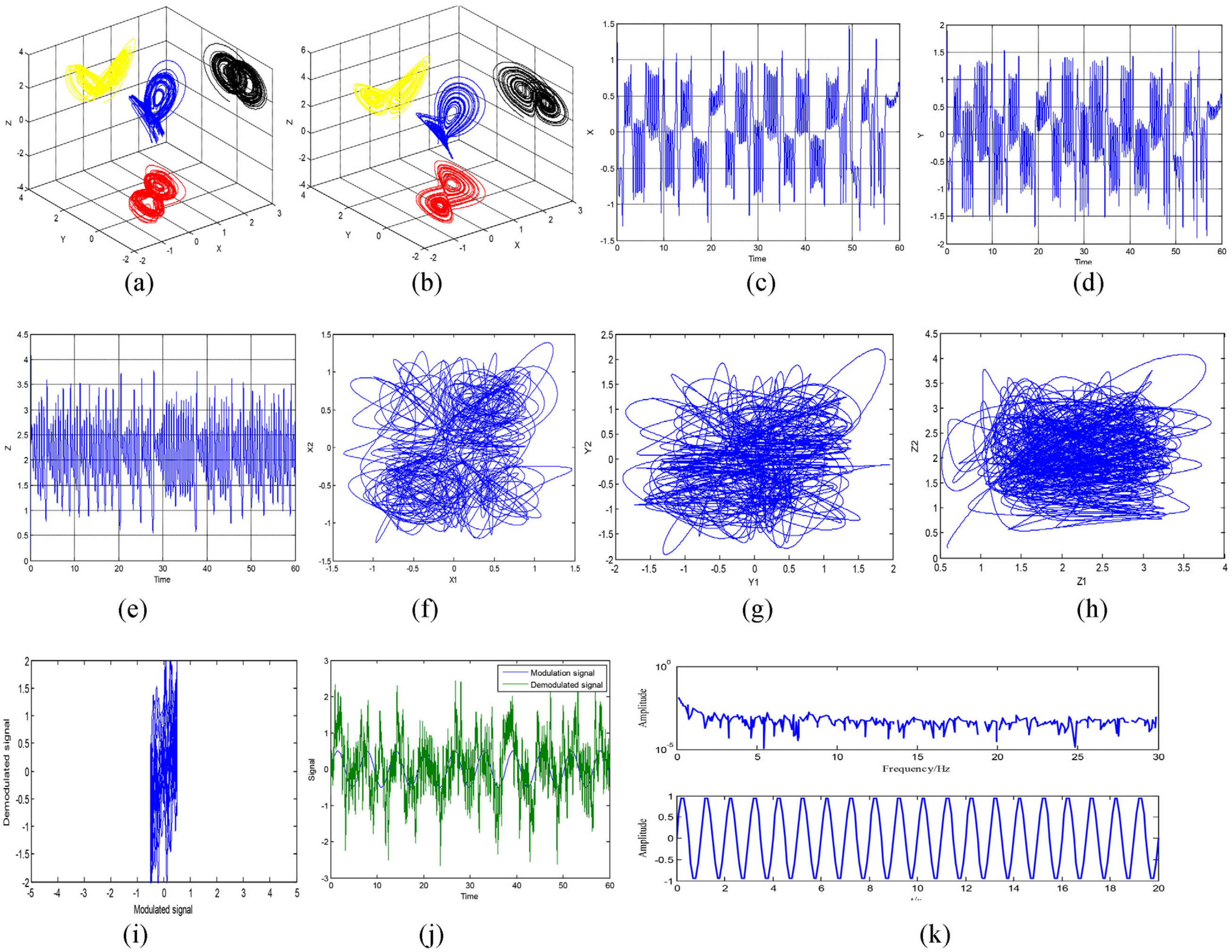


Fig 12. Simulation results. (a) attractors for transmitter, **(b)** attractors for receiver, **(c)** *x* waveform, **(d)** *y* waveform, **(e)** *z* waveform, **(f-h)** non-synchronization phase diagram, **(i)** modulation-demodulation phase diagram, **(j)** modulation signal and demodulation signal, **(k)** the power spectrum of the transmitted signal and the recovered signal.

doi:10.1371/journal.pone.0158348.g012

K_3: It is not only the circuit control of the receiving system, but also the experimental control of synchronization and non-synchronization. When the 2–3 terminal is connected, the receiving system constitutes an independent Lorenz unit circuit. When the 1–2 terminal is connected, the receiving system is connected with the modulation circuit.

In the following, the actual hardware circuit is built to make experiment measurements according to Fig 11. As long as the circuit components are selected carefully, the circuit can be achieved as desired. An oscilloscope is used to measure the circuit. The displayed photos of the actual experiment circuit are shown in Fig 13. Fig 13(a), 13(b) and 13(c) show the phase diagrams of three output variables. The non-synchronization phase diagrams of the receiver and the transmitter are shown in Fig 13(d), 13(e) and 13(f). The synchronization phase diagrams of the receiver and the transmitter are shown in Fig 13(g), 13(h) and 13(i). Fig 14(a), 14(b) and 14(c) show the modulation signal of the transmitter and the demodulation signal of the receiver after accessing the radio. What is found is that the speech signal is basically demodulated by the receiver. That is to say, the secure reception is implemented. However, the effect of the speech communication is not perfect because the multipliers with

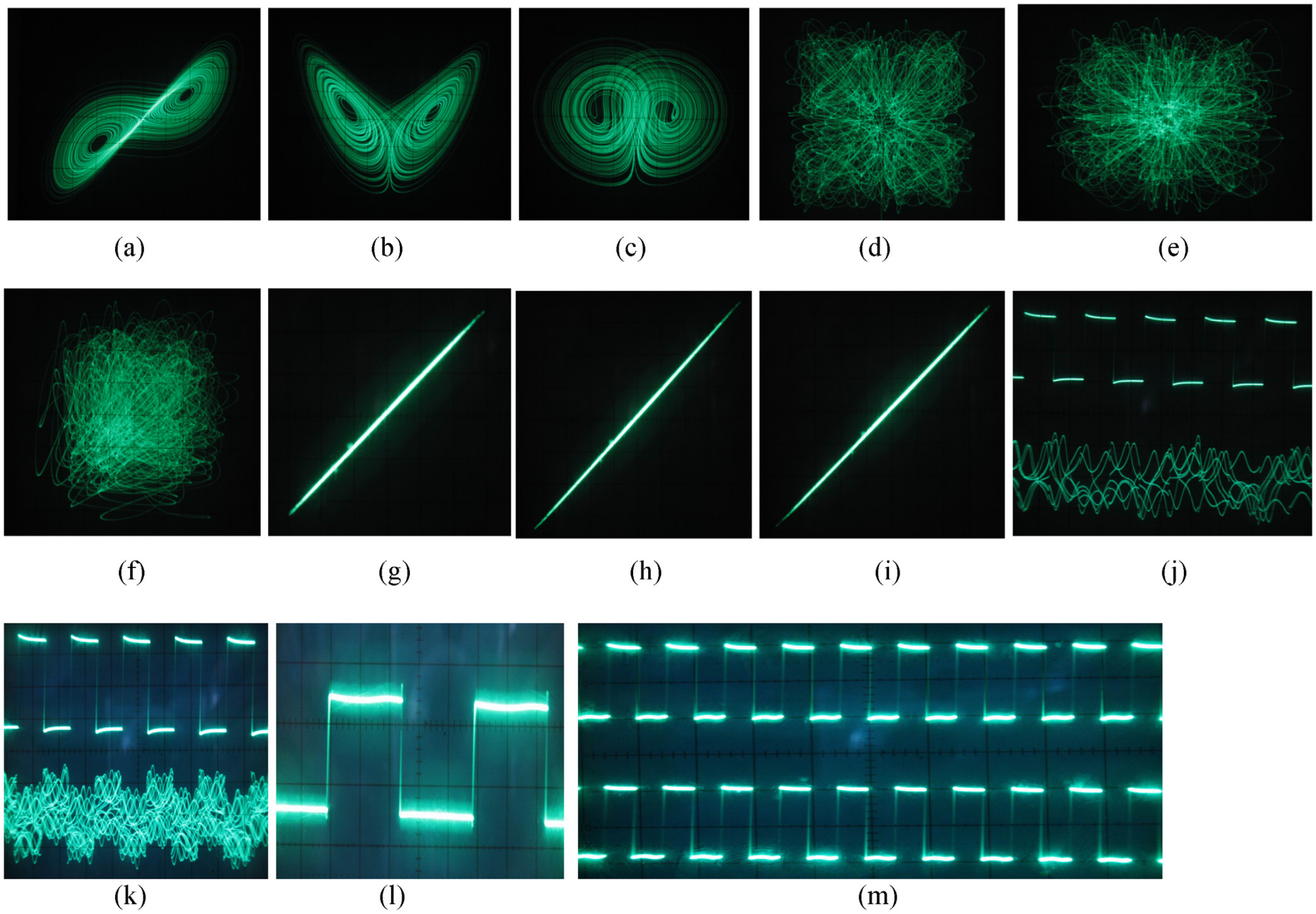


Fig 13. Chaotic secure communication circuit signal photos. (a) ***xy*** phase diagram, **(b)** *xz* phase diagram, **(c)** *zy* phase diagram, **(d-f)** non-synchronization phase diagrams, **(g-i)** synchronization phase diagrams, **(j)** signal and channel waveform, **(k)** signal and channel waveform, **(l)** modulation-demodulation signal amplification, **(m)** transmitting and receiving waveform.

doi:10.1371/journal.pone.0158348.g013

discrete parameters produce relatively large synchronization noises. The experimental circuit board photo is shown in Fig 15.

From the experimental results, what can be concluded is that the synchronization effect of the Lorenz chaotic circuit is robust. Taking into account the magnitude of the chaotic signal is

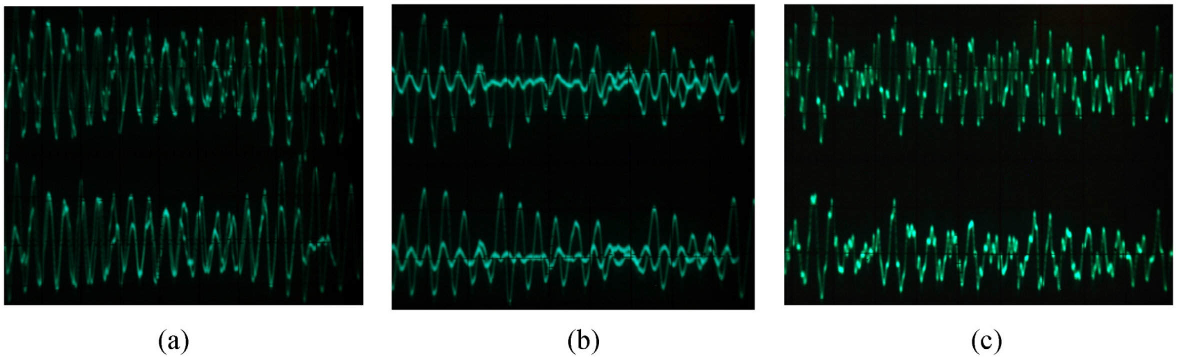


Fig 14. The transmitter input modulation signal and the receiver demodulation output signal.

doi:10.1371/journal.pone.0158348.g014

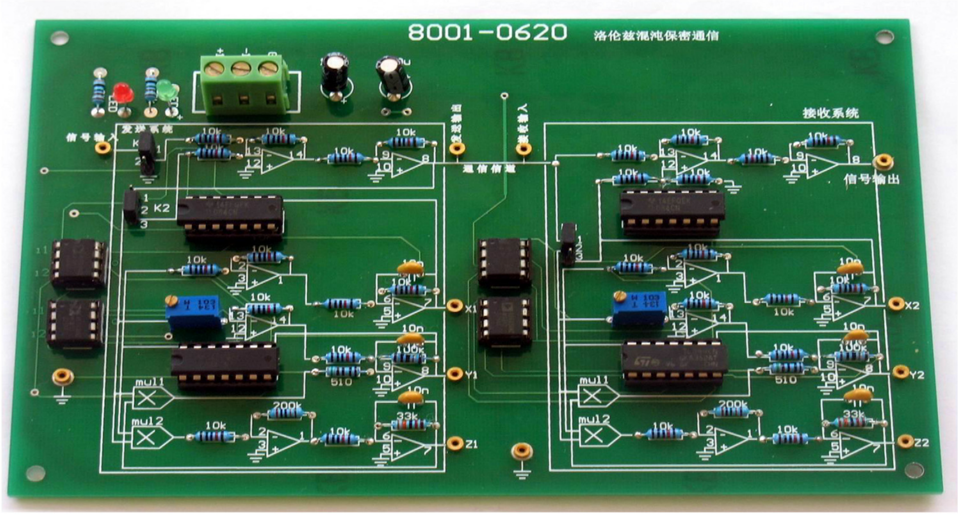


Fig 15. Experimental circuit board photo.

doi:10.1371/journal.pone.0158348.g015

a voltage magnitude, the noise coefficient of the circuit is $\delta_N < 10^{-5}$. What can be seen from Fig 13(m) is that the amplitude of the modulation signal is 10 mV. The distortion degree of $\delta_N < 10^{-2}$ is measured by oscilloscope using the same method. Several actual measurement circuit boards were welded carefully, and all the experimental results and the index were repeated. Such measurement method and experimental results have not been reported to date; therefore, it is of great practical significance.

However, the proposed chaotic secure communication method still has certain limitation. On one hand, because traditional amplifiers and current conveyors have frequency limitations, they have limited performance in implementing nonlinear circuits. On the other hand, it is well known that most of the chaotic system can generate finite chaotic attractors. However, some evidences have confirmed that the chaotic system composed of multi-scroll attractor shows more complex dynamical behaviors. Therefore, nonlinear oscillators composed of multi-scroll chaotic attractor show more complicate and rich chaotic dynamics. And they are often used for generating complex secure keys and carrying wave for chaotic secure communication or image encryption [18, 19]. That is, it is more reliable to use chaotic system composed of multi-scroll attractors to implement chaotic secure communication or image encryption. Moreover, another issue is how to improve the unpredictability of the chaotic communication system. Those designs can be enhanced if the chaotic oscillator possesses more positive Lyapunov exponents, because it determines the unpredictability grade of the chaotic oscillator [45, 46]. Therefore, using chaotic system composed of multi-scroll attractors to achieve secure communication will be the next problem to be addressed.

7. Conclusion

In this paper, a novel approach is presented to enhance the security performance of transmission signal and improve the vulnerability of chaotic modulation. For the first time, the improved Lorenz chaotic system in a simple chaotic modulation method is implemented to illustrate the heightening of security in communication. In this research, the receiving system is easier to maintain good synchronization with the transmitting system by using the Lorenz chaotic optimization circuit, and the robustness of the proposed secure communication scheme was validated. Another advantage of the proposed scheme guarantees an effective inspection of the comprehensive performance of the circuit by improving the experimental circuit and measurement method. Moreover, in order to verify the strength limit of the transmitted signal, the characteristic of being broadband and the required accuracy for the electronic components, some numerical simulations are presented by Multisim. The simulation results verify that the proposed scheme can implement the effective transmission and reception of the signals. The intensity of per transmitted signal strength must be far less than that of the chaotic signal in order to achieve the effective transmission and reception of the signal. What can be seen from the simulation results and the experimental results is that the comprehensive performance of the proposed scheme seems to be satisfactory for the chaotic secure communication applications. More specifically, the debugging difficulty of Lorenz chaotic secure communication circuit is much larger than that of Chua's circuit. In future, this scheme will be verified for its' application into other chaotic systems.

Author Contributions

Conceived and designed the experiments: LX XGZ YJL.

Performed the experiments: LX YJL XGZ.

Analyzed the data: LX YJL YFZ XGZ.

Contributed reagents/materials/analysis tools: LX YJL YFZ XGZ.

Wrote the paper: LX YJL PG.

References

1. Pecora L M, Carroll T L. Synchronization in chaotic systems. Physical Review Letters 1990, 64(8): 821–824. PMID: 10042089
2. Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of Lorenz-based chaotic circuits with applications to communications. Circuits and systems II: Analog and digital signal processing, IEEE Transactions on 1993, 40(10): 626–633.
3. Cuomo K M, Oppenheim A V. Circuit implementation of synchronized chaos with applications to communications. Physical review letters 1993, 71(1): 65–68. PMID: 10054374
4. Milanović V, Zaghloul M E. Improved masking algorithm for chaotic communications systems. Electronics Letters 1996, 32(1): 11–12.
5. Yu-Min L, Yu-Hong Z, Jin-Quan Y. Circuit implementation of secure communication system based on improved chaotic masking algorithm. Journal of circuits and systems 2009, 14(1): 116–118.
6. Sira-Ramirez H, Cruz-Hernandez C. Synchronization of chaotic systems: A generalized Hamiltonian systems approach. International Journal of Bifurcation and Chaos 2001, 11(5): 1381–1395.
7. Trejo-Guerra R, Tlelo-Cuautle E, Cruz-Hernandez C. Chaotic communication system using Chua's oscillators realized with CCII+s. International Journal of Bifurcation and Chaos 2009, 19(12): 4217–4226.
8. Arman Kiani-B, Fallahi Kia, Pariz Naser, Leung Henry. A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter. Communications in Nonlinear Science and Numerical Simulation 2009, 14: 863–879.
9. Filali R L, Benrejeb M, Borne P. On observer-based secure communication design using discrete-time hyperchaotic systems. Communications in Nonlinear Science and Numerical Simulation 2014, 19(5): 1424–1432.
10. Zapateiro M, Vidal Y, Acho L. 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 2014, 19(4): 991–1003.
11. Xin-Guo Z, Hong-Tao S, Jin-Lan Z. Equivalent circuit in function and topology to Chua's circuit and the design methods of these circuits. Acta Physica Sinica 2014, 63(20): 1–8.
12. Mbe E S K, Fotsin H B, Kengne J. Parameters estimation based adaptive generalized projective synchronization (GPS) of chaotic Chua's circuit with application to chaos communication by parametric modulation. Chaos, Solitons & Fractals 2014, 61: 27–37.

13. Sanchez-Lopez C, Trejo-Guerra R, Munoz-Pacheco J M. N-scroll chaotic attractors from saturated function series employing CCII+s. Nonlinear Dynamics 2010, 61(1–2): 331–341.

14. Munoz-Pacheco J M, Tlelo-Cuautle E, Toxqui-Toxqui I, Sanchez-Lopez C, Trejo-Guerra R. Frequency limitations in generating multi-scroll chaotic attractors using CFOAs. International Journal of Electronics 2014, 101(11): 1559–1569.

15. Trejo-Guerra R, Tlelo-Cuautle E, Jimenez-Fuentes J M, Sanchez-lopez C, Munoz-Pacheco J M. Integrated circuit generating 3-and 5-scroll attractors. Communications in Nonlinear Science and Numerical Simulation 2012, 17(11): 4328–4335.

16. Trejo-Guerra R, Tlelo-Cuautle E, Jimenez-Fuentes J M, Munoz-Pacheco J M, Sanchez-Lopez C. Multiscroll floating gate-based integrated chaotic oscillator. International Journal of Circuit Theory and Applications 2013, 41(8): 831–843.

17. Nunez J C, Tlelo E, Ramirez C, Jimenez J M. CCII plus Based on QFGMOS for Implementing Chua's Chaotic Oscillator. IEEE Latin America Transactions 2015, 13(9): 2865–2870.

18. Fan L, Jun M. Pattern selection in network of coupled multi-scroll attractors. Plos One 2016, 11(4): 0154282.

19. Fan L, Cheng-Gui Y. The infinite-scroll attractor and energy transition in chaotic circuit. Nonlinear Dynamics 2016, 84: 2305–2315.

20. Tlelo-Cuautle E, Rangel-Magdaleno J J, Pano-Azucena A D, Obeso-Rodelo P J, Nunez-Perez J C. FPGA realization of multi-scroll chaotic oscillators. Communications in Nonlinear Science and Numerical Simulation 2015, 27(1–3): 66–80.

21. Tlelo-Cuautle E, Carbajal-Gomez V H, Obeso-Rodelo P J. FPGA realization of a chaotic communication system applied to image processing. Nonlinear Dynamics 2015, 82(4): 1879–1892.

22. Soriano-Sanchez A G, Posadas-Castillo C, Platas-Garza M A, Cruz-Hernandez C, Lopez-Gutierrez R M. Coupling strength computation for chaotic synchronization of complex networks with multi-scroll attractors. Applied Mathematics and Computation 2016, 275: 305–316.

23. Garza-Gonzalez E, Posadas-Castillo C, Rodriguez-Linan A. Chaotic synchronization of irregular complex network with hysteretic circuit-like oscillators in hamiltonian form and its application in private communications. Revista Mexicana De Fisica 2016, 62(1): 51–59.

24. Boutayeb M, Darouach M, Rafaralahy H. Generalized stated-space observers for chaotic synchronization and secure communication. IEEE Transactions on Circuit and Systems Fundamental, Theory and Applications 2002, 49(3): 345–349.

25. Li S, Alvarez G, Chen G. Breaking a chaos-based secure communication scheme designed by an improved modulation method. Chaos, Solitons and Fractals 2005, 25(1):109–120.

26. Ekhande Rahul, Deshmukh Sanjay. Chaotic synchronization in digital communication. International Journal of Engineering Research 2014, 3(07): 458–461.

27. Merah Lahcene, Ali-Pacha Adda, Hadj Said Naima, Mamat Mustafa. Design and FPGA implementation of Lorenz chaotic system for information security issues. Applied Mathematical Sciences 2013, 7(5): 237–246.

28. NI W, WANG L. Research on chaos communication based on Chua's circuit. Computer and Modernization 2005 7: 96–98.

29. Muthuswamy B, Chua L O. Simplest chaotic circuit. International Journal of Bifurcation and Chaos 2010, 20(05): 1567–1580.

30. Chen Hsin-Chieh, Liau Ben-Yi, Hou Yi-You. Hardware implementation of Lorenz circuit systems for secure chaotic communication applications. Sensors 2013, 13: 2494–2505. doi: 10.3390/s130202494 PMID: 23429512

31. Halimi M, Kemih K, Ghanes M. Circuit simulation of an analog secure communication based on synchronized chaotic Chua's system. Appl. Math 2014, 8(4): 1509–1516.

32. Lin T C, Huang F Y, Du Z. Synchronization of fuzzy modeling chaotic time delay memristor-based Chua's circuits with application to secure communication. International Journal of Fuzzy Systems 2015, 17(2): 206–214.

33. El-Sayed A M A, Nour H M, Elsaid A. Circuit realization, bifurcations, chaos and hyperchaos in a new 4D system. Applied Mathematics and Computation 2014, 239: 333–345.

34. Rui W, Hui S, Jie-Zhi W. Applications of modularized circuit designs in a new hyper-chaotic system circuit implementation. Chinese Physics B 2015, 24(2): 020501.

35. Pehlivan I, Moroz I M, Vaidyanathan S. Analysis, synchronization and circuit design of a novel butterfly attractor. Journal of Sound and Vibration 2014, 333(20): 5077–5096.

36. Swathy P S, Thamilmaran K. Hyperchaos in SC-CNN based modified canonical Chua's circuit. Nonlinear Dynamics 2014, 78(4): 2639–2650.

37. Feng C, Cai L, Kang Q. Novel hyperchaotic system and its circuit implementation. Journal of Computational and Nonlinear Dynamics 2015, 10(6): 061012.

38. Galias Z, Maggio G M. Quadrature chaos-shift keying: theory and performance analysis. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on 2001, 48(12): 1510–1519.

39. Yan X G, Chen I M, Li H S. Robust control for a class of modified Duffing equations. Transactions of the Institute of Measurement and Control 2002, 24(4): 263–275.

40. Ge S S, Li Z. Robust adaptive control for a class of MIMO nonlinear systems by state and output feedback. Automatic Control, IEEE Transactions on 2014, 59(6): 1624–1629.

41. XG Yan C Edwards. Adaptive sliding-mode-observer-based fault reconstruction for nonlinear systems with parametric uncertainties. Industrial Electronics, IEEE Transactions on 2008, 55(11): 4029–4036.

42. Chen G R, Lü J H. Dynamical analyses, control and synchronization of the Lorenz system family. Science Press, Beijing 2003. (in Chinese).

43. Zhang X G, Ma Y D, Li S L. Nonlinear circuit—based analysis and design. Beijing: Higher Education Press 2011. (in Chinese).

44. Lü J H, Chen G R, Celikovsky S. Bridge the gap between the Lorenz system and Chen system. Int J Bifurc Chaos 2002, 12(12): 2917–2928.

45. Carbajal-Gomez V H, Tlelo-Cuautle E, Fernandez F V. Optimizing the positive Lyapunov exponent in multi-scroll chaotic oscillators with differential evolution algorithm. Applied Mathematics and Computation 2013, 219(15): 8163–8168.

46. Gerardo de la Fraga Luis, Tlelo-Cuautle Esteban. Optimizing the maximum Lyapunov exponent and phase space portraits in multi-scroll chaotic oscillators. Nonlinear Dynamics 2014, 76(2): 1503–1515.