Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **5**, Number **2**, May **2020**

Discrete Synchronization Method for Continuous Chaotic Systems and Its Application in Secure Communication

Wangshu Li, Wenhao Yan and Qun Ding

Electronic Engineering College, Heilongjiang university, Harbin 150080, China
Correspondence should be addressed to Qun Ding; qunding@aliyun.com

Ruoxun Zhang

Primary Education College, Xingtai College, Xingtai 054001, China

Yeh-Cheng Chen

department of computer science, University of Califfornia, Davis, CA, USA
ycch@ucdavis.edu

Received March 2019; revised December 2019

Abstract. *The theorem of chaos synchronization has many excellent characteristics and wide application prospect. Because the discrete components of the analog circuit are susceptible to environmental temperature and humidity, the continuous chaotic synchronization system is difficult to achieve in secure communication engineering. Based on the current large-scale digital logic circuit applications, many digital communication synchronization requirements are presented. In this paper, it is proved that that stability principle of the discrete system of Euler method, which is based on the design of discrete synchronous communication system. Three discrete synchronization methods for continuous chaotic systems with simple structures and easy to be implemented by engineering are designed, including discrete chaotic synchronization methods with driving - response, active - passive and self-adaptive methods. And through strict mathematical derivation proves its synchronization system can achieve asymptotically stable. In addition, A discrete chaotic secure speech concealment communication system based on self-adaptive synchronization is designed. The confidentiality and stability of the system is proved by relevant simulation experiments, which promotes the synchronization theorem and engineering application of chaotic secure communication.*
Keywords: Discrete system; Chaotic synchronization; Speech confidential communication; Euler method

1. **Introduction.** Chaos theory, as a new subject, has some excellent characteristics, including sensitivity to initial values, intrinsic randomness, ergodicity, topological transitivity and a positive Lyapunov exponent [1-3]. These characteristics make chaotic systems widely used in secure communication [4-8]. However, chaotic synchronization is the basis of chaotic secure communication. Chaotic synchronization refers to two chaotic systems starting from different initial conditions. With a change in time, the orbit of one system will converge to the same value of the orbit of the other system. The study of chaotic synchronization started in the 1990s. American scientists Pecora and Carroll proved, through experiments, that interconnected chaotic systems can produce synchronization phenomena

under certain conditions [9]. The methods of chaotic synchronization include the driving-response synchronization method, active-passive synchronization method, feedback synchronization method, coupled synchronization method, to self-adaptive synchronization method, impulse synchronization, generalized synchronization method, and a synchronization method based on a state observer [10-17]. Chaotic synchronization schemes also include circuit chaos synchronization and laser chaos synchronization [18-21]. A chaotic synchronization transceiver system also gradually expands from low-dimensional chaos to high-dimensional chaos, since the high-dimensional chaotic system has stronger randomness, higher confidentiality, larger information quantity and a higher communication efficiency. However, the complexity of the system is also higher, and the form of chaos synchronization begins to develop from single to cascade, both of which enrich chaos synchronization. Research on chaos synchronization mainly includes continuous chaotic system synchronization and discrete chaotic system synchronization, which are mainly based on analog and digital circuits, respectively. At present, theoretical research and simulations are dominant. Traditional chaos synchronization research mainly focuses on continuous chaotic systems based on analog circuit design. Due to the sensitivity of simulated chaotic circuits, unavoidable parameter value errors of the circuit elements, environmental impacts, and interference caused by communication links, communication schemes based on this technology show weak robustness, which hinders the application of chaotic secure communication synchronization technology. With the rapid development of digital circuits, especially large-scale integrated circuits, and with the wide application of modern digital communication, the study of chaotic secure communication synchronization is of great significance. The premise of the application of digital chaotic technology is the realization of a discrete chaotic system. Some scholars have studied discrete chaotic system synchronization theory since discrete chaotic systems can achieve strict matching of parameters and have more advantages than continuous chaotic systems. In 2011, M. Eisencraf et al. studied the effect of limited bandwidth on a master-slave synchronization solution in discrete time [22]. It was pointed out that the study of discrete chaotic systems is based on the practical application of a digital signal processor or microcontroller. In 2016, Rodrigo t. Fontes et al. studied a communication system using functions to encode information in chaotic signals [23]. Based on the master-slave chaotic synchronization, the necessary conditions of the synchronization of a k-dimensional chaotic generator were obtained analytically, and the performance of the system was evaluated from the point of error. In 2016, Alexey A. Koronovskiia et al. studied two unidirectional coupled power systems of aperiodic binary sequences [15] and revealed the existence of binary generalized synchronization through auxiliary system method and a maximum condition Lyapunov index calculation. The mechanism of binary generalized synchronization was explained. This research provided new application potential.

The background of this paper is based on secure communication, which is suitable for digital signal synchronous transmission as the main purpose. On this premise, we design a synchronous transmission mode of communication from a continuous chaotic system to a discrete chaotic system and three discrete synchronization methods for continuous chaotic systems with simple structures and straightforward engineering, including driving-response, active-passive and self-adaptive methods. Furthermore, we verify the effectiveness of this method through a theoretical proof and numerical simulations. Lastly, a discrete chaos obscure speech secure communication method based on self-adaptive synchronization is designed.

2. **Euler method for discrete continuous chaotic systems.** The discretization methods of continuous chaotic systems mainly include Euler method and Runge-Kutta method.

The calculation accuracy of Runge-Kutta method is high, and the algorithm takes up more hardware resources due to complexity, which makes it difficult to design and implement digital system. And Euler method occupies less resources and is convenient for engineering implementation. The Euler algorithm is actually implemented according to the definition of derivative. The Euler method is used to solve the first-order differential equation, as shown in figure 1.

If $y = f(x)$ is any curve, then $P_1(x_1, y_1)$ is a point on the tangent line over the curve P_0 and $x_1 = x_0 + h$, $y_1 \approx y_0 + hf(x_0)$. While the point $P_2(x_2, y_2)$ is the point that goes through P_1 and is parallel to the tangent line at (x_1, y_1) , and $x_2 = x_1+h$, $x_2 = x_1+h$, and $x_2 = x_1+h$, $y_2 \approx y_1+hf(x_1)$. By analogy, the approximate solution of $y_n(n = 0, 1, 2 \cdots N)$ point can be obtained; $hf(x_i) = hy'(x_i)$ is the increment of the numerical solution of the function; the folded line formed by points $P_0, P_1, \cdots P_N$ can be regarded as the approximate curve of the solution curve $y = f(x)$.

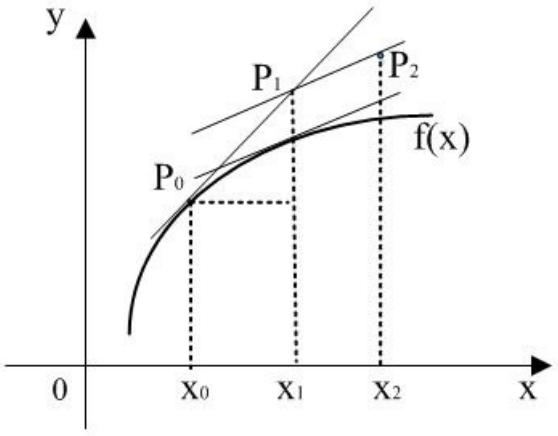

FIGURE 1. Geometric interpretation of Euler method

According to definition of a derivative,

$$\frac{y(x_{n+1}) - y(x_n)}{h} \approx y'(x_n) \approx f(x_n)$$

Then $y(x_{n+1}) \approx y(x_n) + hf(x_n)$ or

$$\Delta y(x_n) = hf(x_n), \text{ where } \Delta y(x_n) = y(x_{n+1}) - y(x_n) \tag{1}$$

For example, the Lorenz equation is discretized into:

$$\begin{cases} x_{n+1} = x_n - 10(x_n - y_n)\, h \\ y_{n+1} = y_n + (28x_n - y_n - x_n z_n\ )h \\ z_{n+1} = z_n + (x_n y_n - \frac{8}{3} z_n)h \end{cases} \tag{2}$$

And, we can get the following equation.

$$\begin{cases} \Delta x_n = -10(x_n - y_n)\, h \\ \Delta y_n = (28x_n - y_n - x_n z_n\ )h \\ \Delta z_n = z(x_n y_n - \frac{8}{3} z_n)h \end{cases} \tag{3}$$

The Euler method needs to set the step length. The step length selection is very important in the numerical solution method. The step length is too large, and the local truncation error generated by each step calculation is also large. The step size is small. Although the value of truncation error calculated in each step is small, the calculation steps that need to be completed are more when choosing a certain range, which not only increases the calculation quantity, but causes the accumulation of calculation error. The digital system should mainly use a small amount of calculation to achieve a certain error requirement, and at the same time it is required to leave out a certain amount of calculation and unnecessary error accumulation.

3. **Stability principle of Euler method for discrete systems.** According to the stability principle of continuous system, Lyapunov and the discrete theory of Euler method, there are the following theories about discrete system.

Theorem 3.1. *for discrete systems (3-3), the Lyapunov function* $V_n = \frac{1}{2}x_n^2 + \frac{1}{2}k_n^2$ *where* $\Delta V_n \leq -ahx_n^2,\ (a > 0), h$ *is walking step. Then* $\lim\limits_{t\to\infty} x_n = 0$

Proof(1): because , $\Delta V_n \leq -ahx_n^2,\ (a > 0), h$ is walking step, and then,

$$\frac{\Delta V_n}{h} \leq -ax_n^2,$$

Thus

$$\dot{V} \approx \frac{\Delta V_n}{h} \leq -ax_n^2$$

According to Barbalat lemma, and then $\lim\limits_{t\to\infty} x_n = 0$. Where Barbalat lemma If $f(t)$ has a finite limit as $t \to \infty$ and if $\dot{f}$ is uniformly continuous (or $\ddot{f}$ is bounded), then $\dot{f}(t) \to 0$ as $t \to \infty$

Theorem 3.2. *For the discrete system variable* $x_n(t)$ *,where* $x_n(t),\ t \in h\mathbb{N}$ *.We can get established equation* $\Delta x_n^2 = 2x_n\Delta x_n$

Proof: because $\frac{dx_n^2}{dt} = 2x_n\frac{dx_n}{dt}$, according to the Euler method discrete theorem,

$$\frac{dx_n^2}{dt} \approx \frac{\Delta x_n^2}{h}, \frac{dx_n}{dt} \approx \frac{\Delta x_n}{h} \tag{4}$$

Then

$$\Delta x_n^2 = 2x_n\Delta x_n$$

4. **Discrete synchronized methods of the continuous chaos system.**

4.1. **Discrete chaotic synchronization based on driving - response method.** Taking Lorenz chaotic system as an example, discrete chaotic synchronization of the driving-response method is realized. The Lorenz driving system equation is discretized by Euler method. We can obtain the following:

$$\begin{cases} \Delta x_n = \sigma(y_n - x_n)h \\ \Delta y_n = h(\gamma x_n - x_n z_n - y_n) \\ \Delta z_n = h(x_n y_n - \beta z_n) \end{cases} \tag{5}$$

When variable parameters $\sigma = 10, \gamma = 28, \beta = 8/3$, system equation is chaotic. The chaotic at-tractor is shown in Figure 3-3, where h=0.01. The chaotic signal x_n is used

as the driving variable to transmit the signal $u_n = x_n$. We can get the following Lorenz response system equation.

$$\begin{cases} \Delta y'_n = h(\gamma x_n - x_n z'_n - y'_n) \\ \Delta z'_n = h(x_n y'_n - \beta z'_n) \end{cases} \tag{6}$$

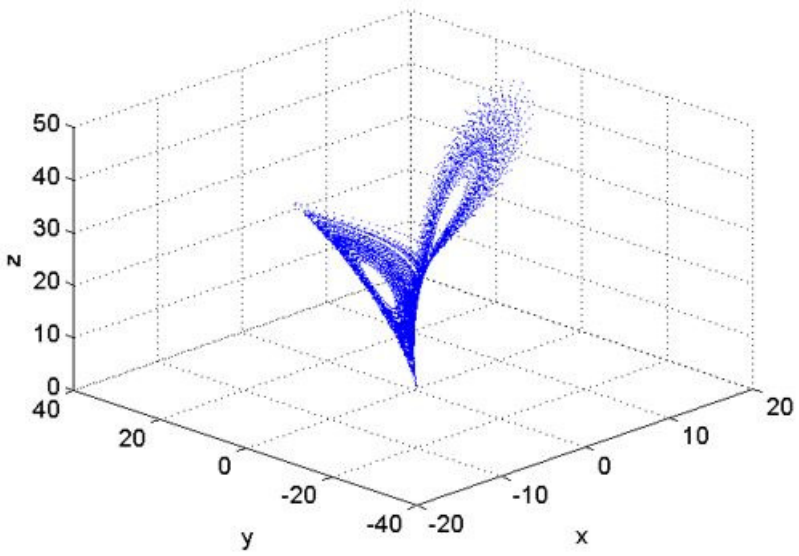

FIGURE 2. Discrete attractor of Lorenz chaotic system

Correspondingly, we can define system error $e_{1n} = y'_n - y_n,\ e_{2n} = z'_n - z_n$. Thus, the dynamic system of synchronous error of the driving system (5) and response system (6) is represented by the equation (7).

$$\begin{cases} \Delta e_{1n} = h(-e_{1n} - x_n e_{2n}) \\ \Delta e_{2n} = h(x_n e_{1n} - \beta e_{2n}) \end{cases} \tag{7}$$

Then, we can assume discrete Lyapunov function $V(e_n)$ as follows.

$$V(e_n) = \frac{1}{2}(e_{1n}^2 + e_{2n}^2) \geq 0 \tag{8}$$

We can get

$$\frac{\Delta V(e_n)}{h} = e_{1n}\frac{\Delta e_{1n}}{h} + e_{2n}\frac{\Delta e_{2n}}{h}$$

Then

$$\begin{aligned} \Delta V(e_n) \quad &= e_{1n}\Delta e_{1n} + e_{2n}\Delta e_{2n} \\ &= e_{1n}h(-e_{1n} - x_n e_{2n}) + e_{2n}h(x_n e_{1n} - \beta e_{2n}) = -he_{1n}^2 - h\beta e_{2n}^2 \end{aligned}$$

According to theory 3.1, if $\beta > 0$, thus $\Delta V \leq 0$, The error dynamics of the driving system and response system can be asymptotically stable, that is to say, the system (5) and the system (6) can ach- ieve synchronization.

We use the Matlab software to achieve the system simulation, and assume the initial value of system (5) and (6) as (x_0, y_0, z_0) and (y'_0, z'_0). Where $(x_0, y_0, z_0) = (-1, -2, 6)$,

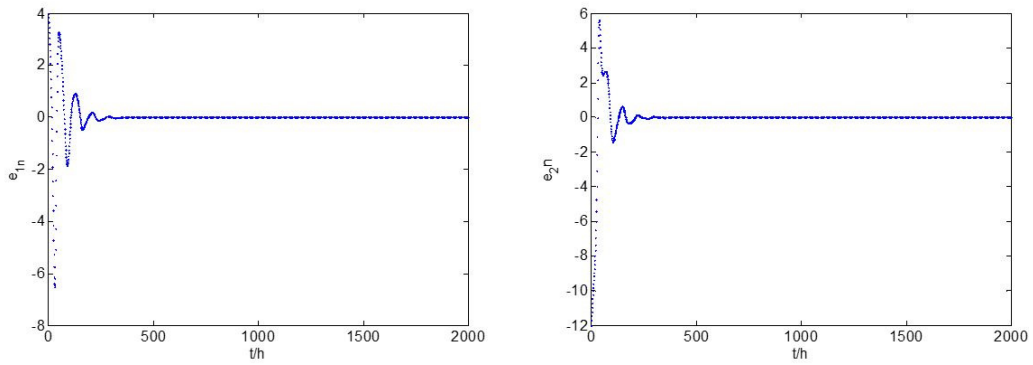

FIGURE 3. synchronous error based on driving - response method

$(y_0', z_0') = (2, -6)$. Then, the simulation results of synchronization error are shown in figure 3. The synchronization error sharply approaches to zero. Thus, we can state that the transceiver system is synchronized.

4.2. **Chaotic synchronization based on active - passive method.** Sending and receiving systems of Lorenz system are driven by the similar signal $s(n) = a\,y_n$. Driving system is as follows.

$$\begin{cases} \Delta x_n = h(-a x_n + s(n)) \\ \Delta y_n = h(c x_n - x_n z_n - y_n) \\ \Delta z_n = h(x_n y_n - b z_n) \end{cases} \tag{9}$$

With coping, we also get response system.

$$\begin{cases} \Delta x'_n = h(-a x'_n + s(n)) \\ \Delta y'_n = h(c x'_n - x'_n z'_n - y'_n) \\ \Delta z'_n = h(x'_n y'_n - b z'_n) \end{cases} \tag{10}$$

Similarly, we can define system error $e_{1n} = x'_n - x_n$, $e_{2n} = y'_n - y_n$, $e_{3n} = z'_n - z_n$. Thus, the dynamic system of synchronous error of the driving system (9) and response system (10) is represented by the equation (11).

$$\begin{cases} \Delta e_{1n} = -ah e_{1n} \\ \Delta e_{2n} = h(c\,e_{1n} - x_n e_{3n} - z_n e_{1n} - e_{1n} e_{3n} - e_{2n}) \\ \Delta e_{3n} = h(x_n e_{2n} + y_n e_{1n} + e_{1n} e_{2n} - b e_{3n}) \end{cases} \tag{11}$$

Then, we can assume discrete Lyapunov function $V(e_n)$ as follows.

$$V(e_n) = \frac{\eta}{2} e_{1n}^2 + \frac{1}{2}(e_{2n}^2 + e_{3n}^2) \qquad \eta > 0 \tag{12}$$

Then, we can get the following expression.

$$\frac{\Delta V(e_n)}{h} = \eta e_{1n} \frac{e_{1n}}{h} + e_{2n} \frac{e_{2n}}{h} + e_{3n} \frac{e_{3n}}{h}$$

$$\begin{aligned} \Delta V(e_n) &= \eta e_{1n} \Delta e_{1n} + e_{2n} \Delta e_{2n} + e_{3n} \Delta e_{3n} \\ &= h(-a\eta e_{1n}^2 + c e_{1n} e_{2n} - z_n e_{1n} e_{2n} + y_n e_{1n} e_{3n} - e_{2n}^2 - b e_{3n}^2) \\ &\le h(-a\eta e_{1n}^2 + \tfrac{c^2 e_{1n}^2 + e_{2n}^2}{2} + \tfrac{m^2 e_{1n}^2 + e_{2n}^2}{2} + \tfrac{m^2 e_{1n}^2 + e_{3n}^2}{2} - e_{2n}^2 - b e_{3n}^2) \\ &= -h(a\eta - c^2/2 - m^2) e_{1n}^2 - h(b - 1/2) e_{3n}^2 \end{aligned} \tag{13}$$

Where $m = \max(|y_n|, |z_n|)$, because equation 9 is chaotic function, thus y_n, z_n have a boundary. Apparently, if $\eta > \frac{c^2}{2a} + \frac{m^2}{a}, b > \frac{1}{2}$, and

$$\Delta V(e_n) \leq -h(a\eta - c^2/2 + m^2)e_{1n}^2 - h(b - 1/2)e_{3n}^2 < 0$$

According to theorem 1, at this point, the system is asymptotically stable and maintains a stable synchronous state, that is, the synchronization of two systems can be achieved.

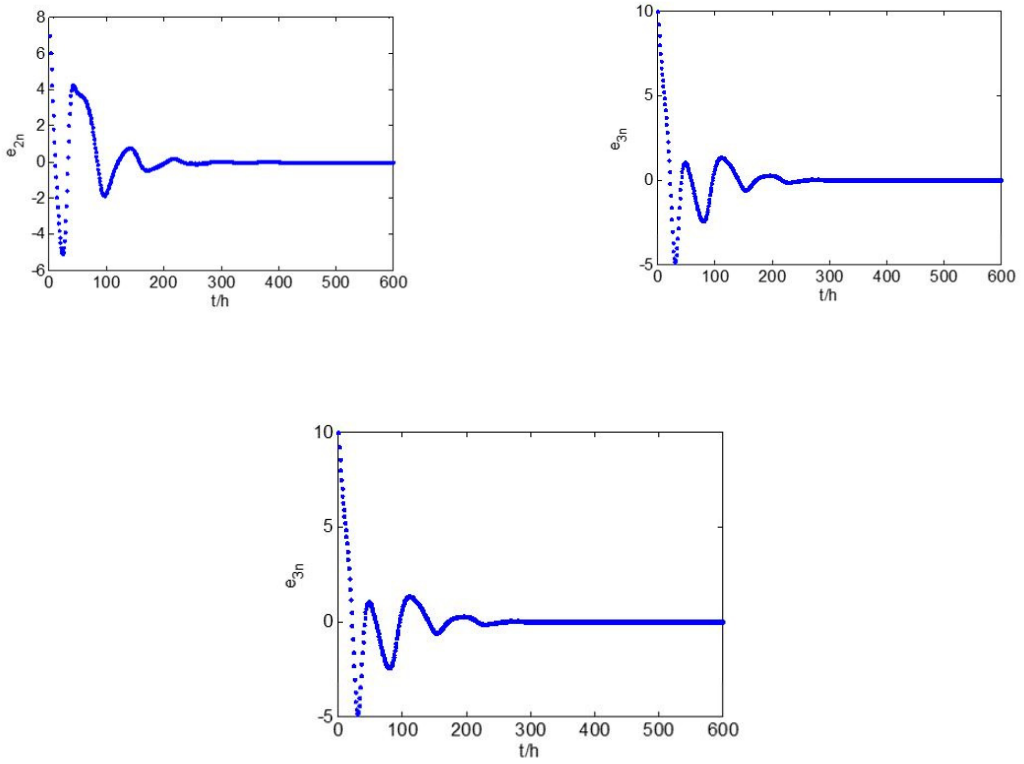

FIGURE 4. Synchronous error based on active - passive method

Parameters are taken during experimental simulation. $a = 10, c = 28, b = 8/3$. We can assume the initial value of system (9) and (10) as (x_0, y_0, z_0), (x_0', y_0', z_0'). Where $(x_0, y_0, z_0) = (1, 3, 6)$, $(x_0', y_0', z_0') = (-6, 10, 16)$. Then, the simulation results of discrete synchronization error are shown in figure 4. Thus, the two systems are synchronized.

4.3. **Chaotic synchronization based on self-adaptive method.** The self-adaptive method can automatically adjust the control gain, and the controller is simple and has high practical value. Some chaotic systems can achieve single variable synchronization. The following is an adaptive synchronization of two Chen systems through a single state variable.

According to the Euler method, Chen system is discrete as

$$\begin{cases} \Delta x_n = ah(y_n - x_n) \\ \Delta y_n = h(dx_n - x_n z_n + cy_n) \\ \Delta z_n = h(x_n y_n - bz_n) \end{cases} \tag{14}$$

Where $a = 35,\ b = 3,\ c = 28,\ d = -7$, The system (14) has typical attractors, as shown in figure 5. Taking system (14) as the driving system, the response system with a single

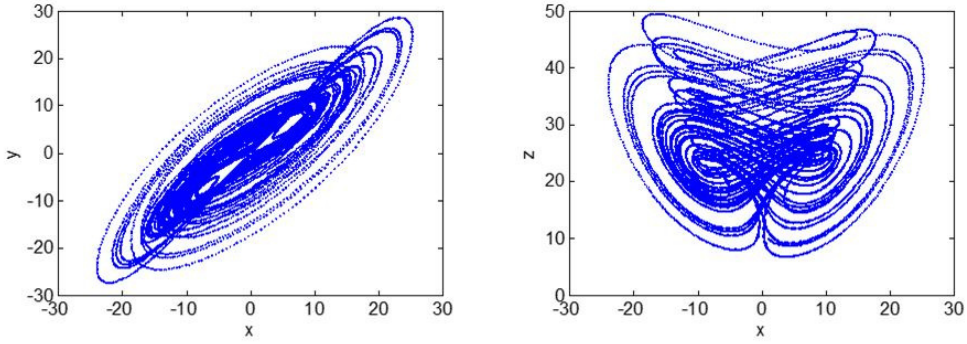

FIGURE 5. Chen chaotic system discrete attractors

controller is as follows.

$$\begin{cases} \Delta u_n = ah(v_n - u_n) \\ \Delta v_n = h(du_n - u_n w_n + cv_n + U_n) \\ \Delta w_n = h(u_n v_n - bw_n) \end{cases} \tag{15}$$

It can be seen from above that we can define Chen chaotic synchronized error $e_{1n} = u_n - x_n$, $e_{2n} = v_n - y_n, e_{3n} = w_n - z_n$. We have the following theorem:

Theorem 4.1. *Set the controller as $U_n = -k_n(v_n - y_n) = -k_n e_{2n}$, (The driver system outputs a single control variable y_n), The self- adaptive law $\Delta k_n = h\theta e_{2n}^2, \quad (\theta > 0)$, then the system (14) and (15) asymptotically synchronize.*

Proof: equation (15) minus equation (14), plug the controller in above equation, and get the dynamic system of synchronous error:

$$\begin{cases} \Delta e_{1n} = ah(e_{2n} - e_{1n}) \\ \Delta e_{2n} = h(de_{1n} - x_n e_{3n} - z_n e_{1n} - e_{1n}e_{3n} + ce_{2n} - k_n e_{2n}) \\ \Delta e_{3n} = h(x_n e_{2n} + y_n e_{1n} + e_{1n}e_{2n} - be_{3n}) \end{cases} \tag{16}$$

Then, we can assume discrete Lyapunov function as follows.

$$V(e_n) = \frac{1}{2}(\lambda e_{1n}^2 + e_{2n}^2 + e_{3n}^2) + \frac{1}{2\theta}(k_n - k^*)^2 \tag{17}$$

Where $\lambda > 0, k^* > 0$, λ and k^* are the undetermined constant.

According to Theorem 3, system error (16) and the self- adaptive law $\Delta k_n = h\theta e_{2n}^2, \quad (\theta > 0)$. We can get the following.

$$\frac{\Delta V(e_n)}{h} = \lambda e_{1n}\frac{\Delta e_{1n}}{h} + e_{2n}\frac{\Delta e_{2n}}{h} + e_{3n}\frac{\Delta e_{3n}}{h} + \frac{1}{\theta}(k_n - k^*)\frac{\Delta k_n}{h}$$

$$\begin{aligned} \Delta V(e_n) &= \lambda e_{1n}\Delta e_{1n} + e_{2n}\Delta e_{2n} + e_{3n}\Delta e_{3n} + \tfrac{1}{\theta}(k_n - k^*)\Delta k_n \\ &= h[-a\lambda e_{1n}^2 + (a\lambda + d - z_n)e_{1n}e_{2n} - (k^* - c)e_{2n}^2 + y_n e_{1n}e_{3n} - be_{3n}^2] \end{aligned} \tag{18}$$

Given the bounds of chaos, we set max $(|x_n|, |z_n|) < m$, $|a\lambda + d - z_n| < l$, and get the following expressions.

$$\begin{aligned}\Delta V(e_n) &= h\left[-a\lambda e_{1n}^2 + (a\lambda + d - z_n)e_{1n}e_{2n} - (k^* - c)e_{2n}^2 + y_n e_{1n}e_{3n} - be_{3n}^2\right] \\ &\le h[-a\lambda e_{1n}^2 + l|e_{1n}e_{2n}| - (k^* - c)e_{2n}^2 + m|e_{1n}e_{3n}| - be_{3n}^2] \\ &\le h[-a\lambda e_{1n}^2 + \frac{e_{1n}^2}{2} + \frac{l^2 e_{2n}^2}{2} - (k^* - c)e_{2n}^2 + \frac{e_{3n}^2}{2} + \frac{m^2 e_{1n}^2}{2} - be_{3n}^2]h \\ &= h[-(a\lambda - \frac{1+m^2}{2})e_{1n}^2 - (k^* - c - \frac{l^2}{2})e_{2n}^2 - (b - 1/2)e_{3n}^2]\end{aligned} \tag{19}$$

If $\lambda = \frac{3+m^2}{2a}$, $k^* = c + \frac{l^2}{2} + 1$, $(a = 35,\ b = 3,\ c = 28,\ d = -7)$ and then

$$\Delta V(e_n) \le h[-e_{1n}^2 - e_{2n}^2 - (b - 1/2)e_{3n}^2] < 0$$

According to Theorem 3, The system (14) and (15) are asymptotically synchronized. Parameters are taken during experimental simulation. $a = 35, b = 3, c = 28, d = -7$ .We can assume the initial value of system (14) and (15) as (x_0, y_0, z_0), (x_0', y_0', z_0'). Where $(x_0, y_0, z_0) = (1, 2, 10)$, $h = 0.001$. Then, the simulation results of discrete synchronization error are shown in figure 6. Thus, the two systems are synchronized.

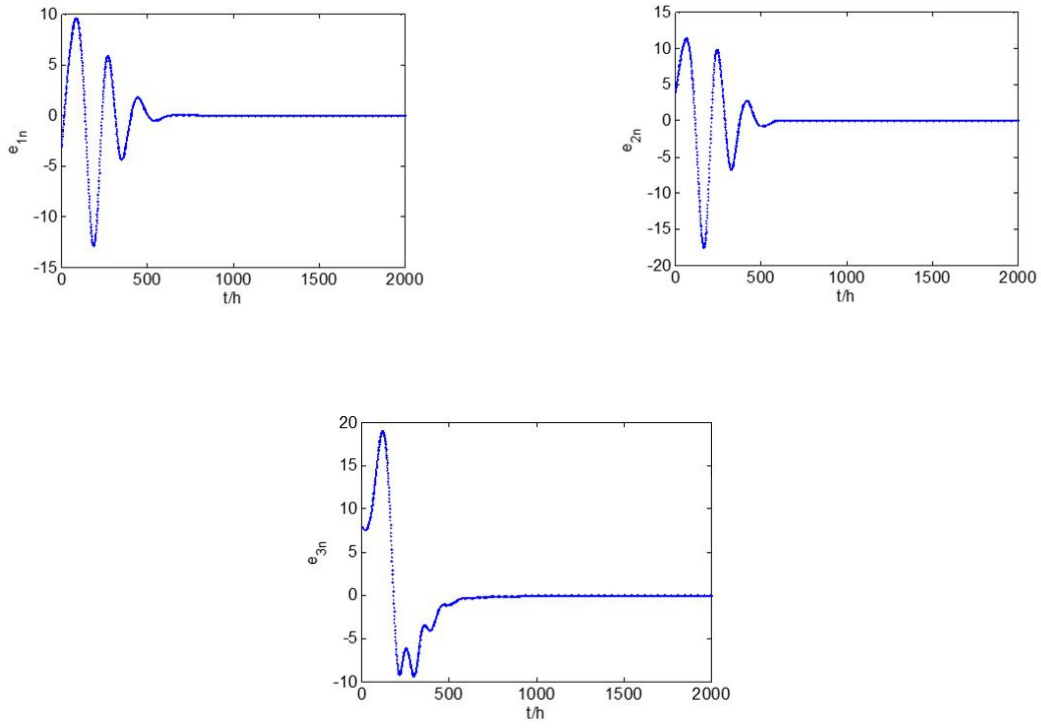

FIGURE 6. Chen chaotic system discrete adaptive synchronization error

5. **Discrete chaos obscures speech secure communication.** With the development of chaotic secure communication research [25-27], the application of chaotic secure communication to voice communication research has continuously increased [28-29]. In this paper, a dual-channel speech secure communication system based on discrete chaotic synchronization is proposed, in which the first channel is used to send the voice transmission signal and the second channel is used to send the synchronous signal. The synchronous

signal consists of different chaotic variables generated by the driving system, which does not contain any information in plain text and is sent to the receiver after a function transformation. This design uses the continuous chaotic system discretization method to achieve speech and synchronization signal bidirectional transmission. A discrete chaotic masking speech secret communication system is constructed by using the self- adaptive synchronization method. System synchronization is achieved by using single state parameters. The step length of discrete chaos in communication can also be used as a key, which increases the key space and improves the safety level of speech communication. More importantly, the discrete synchronization system can promote the practical application of the chaos-based secure communication process.

5.1. **secure communication scheme.** The speech signal $m(t)$ is masked by the state variables x_n and z_n of the discrete Chen chaotic system to form a signal M^e . The state variable y_n is converted to signal $f(y_n)$ by function. The signal $f(y_n)$ and mask state M^e are transmitted to the receiving side over the common channel. If the attacker intercepts the driver signal after function transformation or concealment, it cannot normally drive the two communication systems of the transmitter and receiver, which increases the difficulty of decoding the signal after being intercepted and improves the security of information transmission.

On the receiving end, the function $f(y_n)$ is converted to the state variable y_n by the inverse function $f^{-1}(\cdot)$, so that the discrete Chen chaotic system is synchronized with both end. In this way, state variables x_n and z_n are restored as state variables x'_n and z'_n on the receiving end, and then these state variables will be used to recover speech signals $m'(t)$ from M^e .

We use the scheme indicated in figure 7 to securely encrypt and decrypt speech signals. Consider transmitting voice signals shown in figure 8. When $m(t)$ is concealed by the state variables x_n and z_n of the discrete chaotic system (14). To increase the complexity of the encryption rules, the following encryption rules are defined:

$$M^e = \frac{x_n + m(t)}{z_n} \tag{20}$$

The cover state of M^e is shown in figure 9. The state variable y_n in the public channel is converted to $f(y_n)$, and the transformation function $f(y_n) = y_n^3/1000$, which is shown in figure 10.

The receiving end receives $f(y_n)$ and M^e . $f(y_n)$ is first restored to the state variable y_n by reverse-transforming $f^{-1}(\cdot)$, and then the state variable y_n and y'_n are used to set the self- adaptive controller to synchronize the two discrete Chen systems. As shown in figure 6, the synchronization error e_{1n}, e_{2n}, e_{3n} asymptotically approach zero. The synchronous state of x_n and z_n is x'_n and z'_n , decrypt M^e is $m'(t)$, and the rule is as follows.

$$m'(t) = M^e * z'_n - x'_n \tag{21}$$

Figure 11 shows the restored signal, while figure 12 shows the error between the restored signal and the original signal. Clearly the signal has been completely restored.

(1) Synchronization testing The driving part of discrete Chen chaotic system is as follows.

$$\begin{cases} \Delta x_n = ah(y_n - x_n), \\ \Delta y_n = h(dx_n - x_n z_n + cy_n), \\ \Delta z_n = h(x_n y_n - bz_n). \end{cases}$$

The response part of discrete Chen chaotic system is as follows.

$$\begin{cases} \Delta x'_n = ah(y_n - x'_n), \\ \Delta y'_n = h(dx'_n - x'_n z'_n + cy'_n + U_n), \\ \Delta z'_n = h(x'_n y'_n - bz'_n). \end{cases}$$

Where self-adaptive controller $U_n = -k_n(y'_n - y_n) = -k_n e_{2n}$, and self-adaptive law $\Delta k_n = h\theta e_{2n}^2, \quad (\theta > 0)$ .We can easily get the system error of Chen chaotic system, which is shown the following.

$$\begin{cases} \Delta e_{1n} = ah(e_{2n} - e_{1n}), \\ \Delta e_{2n} = h(de_{1n} - x_n e_{3n} - z_n e_{1n} - e_{1n}e_{3n} + ce_{2n} - k_n e_{2n}), \\ \Delta e_{3n} = h(x_n e_{2n} + y_n e_{1n} + e_{1n}e_{2n} - be_{3n}). \end{cases}$$

And then select Lyapunov function as:

$$V_{(en)} = \frac{1}{2}(\lambda e_{1n}^2 + e_{2n}^2 + e_{3n}^2) + \frac{1}{2\theta}(k_n - k^*)^2$$

Where $\lambda = \frac{3+m^2}{2a}$, $k^* = c + \frac{l^2}{2} + 1$, $(a = 35,\ b = 3,\ c = 28,\ d = -7)$ we can easily get $\Delta V_{(en)} < 0$. Thus, we can surely state that the discrete Chen chaotic system is synchronized.

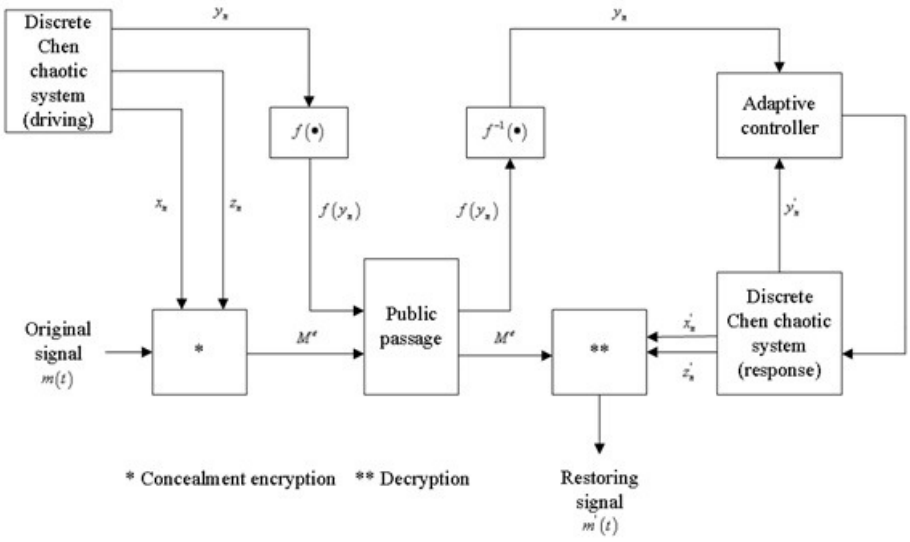

FIGURE 7. Speech security communication scheme

5.2. **safety analysis.** (a)key space, and key selection rules

In good encryption schemes, the key space should be large enough. In this scheme, the encrypted sequences x_n and z_n are generated by the Chen system with the distance discrete walking length and the parameters (a, b, c). Discrete walking length can also be used as a key. Therefore, the key consists of four Numbers (h, a, b, c). Since these four Numbers can be real number, the space of the key will be a four-dimensional space.

(b) key sensitivity analysis

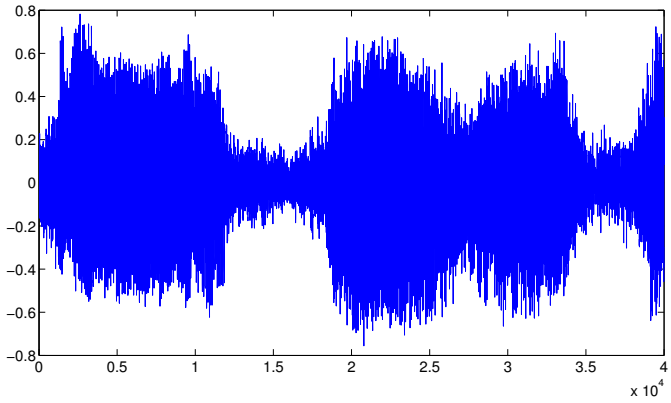

FIGURE 8. Original speech signal at the transmitter

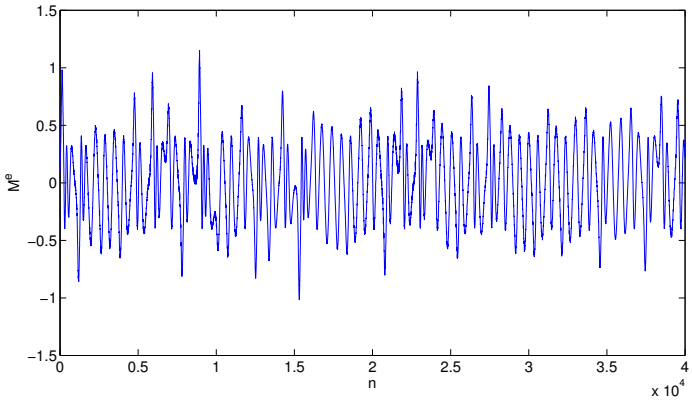

FIGURE 9. Speech signal after chaos cover up

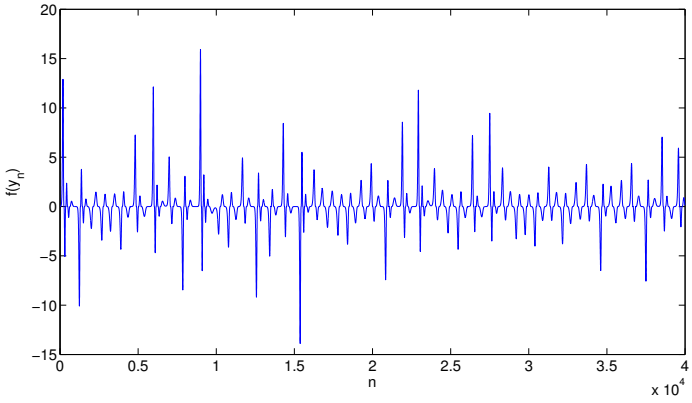

FIGURE 10. Driving signal of function transformation

The security of chaotic cryptosystem depends on the key composed of the parameters of chaotic system or some other supplementary parameters. A good encryption scheme should be sensitive to the key. To verify the sensitivity of the key, we assume that the intruder intercepts the ciphertext and synchronization signal and obtains an approximate estimate of the key, such as (h, a, b, c) = (0.00105,35,3,28), where the step size h is only slightly mismatched. Figure 13 shows the sensitivity when the key of the communication

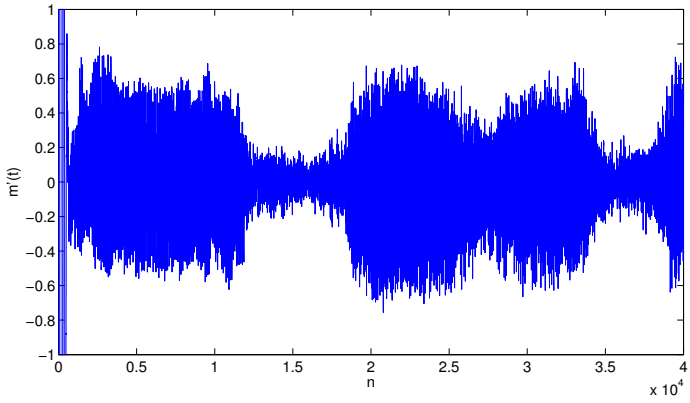

FIGURE 11. Speech signal after restoration

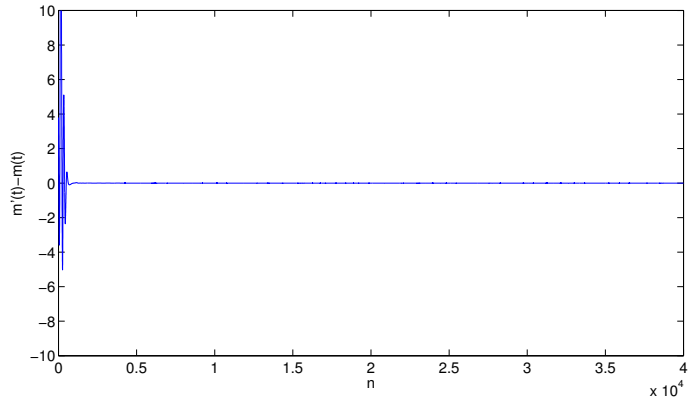

FIGURE 12. Error of restored speech signal and original speech signal

scheme is slightly mismatched. As we have seen, restored speech with an error key behaves randomly and is completely different from the original speech signal. There is no doubt that the key is secure even with the selected plaintext/ciphertext attack.

6. **Conclusion.** In this paper, the discrete method of continuous chaotic system is introduced, and the stability principle of Euler discrete system is obtained. Three methods are designed to realize the synchronization of discrete chaotic system through single variable driver, including driving - response, active - passive and self-adaptive methods. Lorenz and Chen chaotic system, for example, get the continuous chaotic system after discretization of three methods of synchronous driving and response system. The synchronization of the three synchronization methods under the basic conditions of synchronous control rate and adaptive rate is proved. The above result and experimental simulation respectively show that the error dynamics can be asymptotically stable, that is, the driving system and the response system can achieve synchronization. In this paper, a secure digital speech communication scheme based on chaotic two-channel cryptosystem is proposed. Finally, the security and stability of the scheme are proved by the system security analysis.

Acknowledgment. We would like to thank two researchers from Heilongjiang University, Chunlei Fan. for technical support on database inquiry and paper review the simulation computing environment and computer equipment provided by Heilongjiang University and the Nanjing 321 innovative talents program. The paper was supported by the

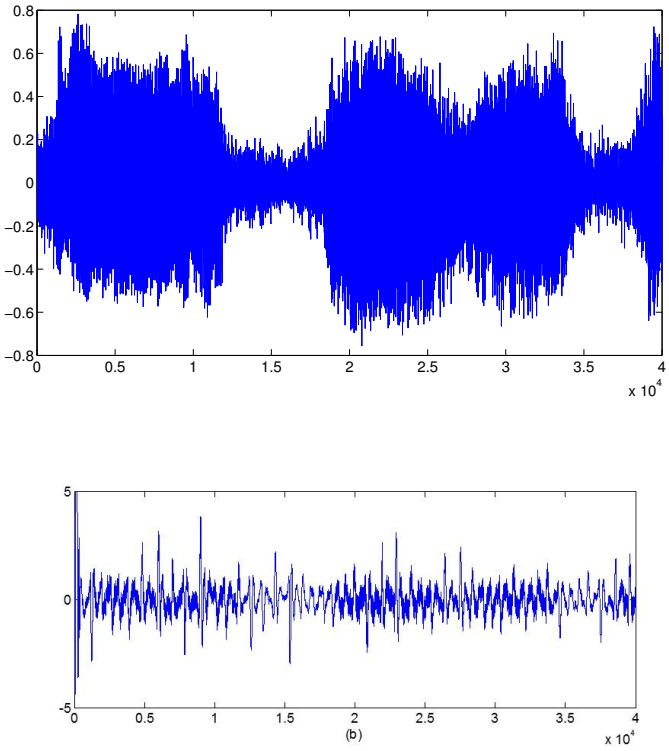

FIGURE 13. Sensitivity of current secure communication scheme to key mismatch: (a) original speech signal, (b) restored speech with an error key

National Natural Science Foundation of China (No. 61471158) and The Natural Science Foundation of Hebei province, China (No. A2015108010).

REFERENCES

[1] E.N. Lorenz. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*. 1963, 20:130∼141.
[2] E.N. Lorenz. The Essence of Chaos. *Meteorology Press*. 1997:7∼11.
[3] T.Y.Li, J.A.Yorke. Period Three Implies Chaos. *The American Mathematical Monthly*. 1975, 82(10):985∼992.
[4] L.O. Chua, T.Lin. Chaos in Digital Filters. *IEEE Transactions on Circuits and Systems*. 1988, 35(6):648∼658.
[5] L.O.Chua, M.Komuro and T.Matsumoto. The Double Scroll Family. *IEEE Transactions on Circuits and Systems*. 1986, 33(11):1072∼1118.
[6] T.Yang, C.W.Wu and L.O. Chua. Cryptography Based on Chaotic Systems. *IEEE Transactions on Circuits and Systems-I:Fundamental Theory and Applications*. 1997, 44(5):469∼472.
[7] J.Fridrich. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*. 1998, 8(6):1259∼1284.
[8] D.R.Frey. Chaotic Digital Encoding: An Approach to Secure Communication. *IEEE Transactions on Circuits and Systems II*. 1993, 40(10):660∼666.
[9] L.M. Pecora, T.L. Carroll. Synchronization in Chaotic Systems. *Physical Review Letters*. 1990, 64(8):821∼824.
[10] Carroll T.L., Pecora L.M. Synchronizing Hyperchaotic Volume-preserving Maps and Circuits. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1998, 45(6):656-659.
[11] Geng, Zhao, Jinqing Fang. Advances in the application of modern information security and chaotic security communication. *Advances in physics*. 2003, 23(2):212∼255. (in Chinese)
[12] Na Yu, Qun Ding, Hong Chen. Chaotic synchronization of heterogeneous systems and its application in secure communication. *Journal of communication*, 2007, 28(10):73-78. (in Chinese)

[13] H.B. Fotsin, J. Daafouz. Adaptive synchronization of uncertain chaotic Colpitts oscillators based on parameter identification. *Physical Letters A*. vol. 339, no. 3-5, pp. 304-315, 2005.
[14] Ju H. Park. Adaptive modified projective synchronization of a unified chaotic system with an uncertain parameter, *Chaos, Solitons, and Fractals*. vol. 34, no. 5, pp. 1552-1559, 2007.
[15] Alexey A. Koronovskii, Olga I. Moskalenko, Vladimir I. Ponomarenkoa, Mikhail D. Prokhorovc, Alexander E. Hramovb. Binary generalized synchronization. *Chaos, Solitons and Fractals*. vol. 83, pp.133-139, 2016.
[16] Adel Ouannas, Zaid Odibat, Nabil Shawagfeh, Ahmed Alsaedi, BashirAhmad. Universal chaos synchronization control laws for general quadratic discrete system. *Applied Mathematical Modelling*. vol. 45, pp. 636-641, 2017.
[17] SangyunLee, MignonPark, JaehoBaek. Robust adapti- ve synchronization of a class of chaotic systems via fuzzybilinear observer using projection operator. *Information Sciences*. 402(2017):182-198.
[18] Hussein H. Waried Synchronization of quantum cascade lasers with mutual optoelectronic coupling. *Chinese Journal of Physics*. 2018, 56(3):1113-1120.
[19] G. Sivaganesh, A. Arulgnanam, A.N. Seethalakshmi. G-eneralized analytical solutions and experimental confirmation of complete synchronization in a class of mutually coupled simple nonlinear electronic circuits. *Chaos, Solitons & Fractals*. 113(2018): 294-307.
[20] Cuomo K.M., Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-based Chaotic Circuits with Applications to Communications. *IEEE Circuits and Systems II: Analog and Digital Signal Processing Transactions on*. 1993, 40(10): 626-633.
[21] Pisarchik A.N., Ruiz-Oliveras F.R. Optical Chaotic Communication Using Generalized and Complete Synchronization. *IEEE Journal of Quantum Electronics*. 2010, 46(3): 279-284.
[22] M. Eisencraft,R. D. Fanganiello,L. H. A. Monteiro. Chaotic Synchronization in Discrete-Time Systems Connected by Bandlimited Channels[J]. *IEEE Communications Letters*. 2011, 15(6):671-673.
[23] Rodrigo T. Fontes, Marcio Eisencraft. A digital bandlimited chaos-based communication system. *Commun Nonlinear Sci Numer Simulat*. 37(2016):374-385.
[24] Dayi Yi, Daoqi Chen. The theory of numerical analysis, Zhejiang university press. 1996.(in Chinese)
[25] T. Yang. A survey of chaotic secure communication systems. *Interntional journal of Computational Cognition*. vol. 2, no. 2, pp. 81-130, 2004.
[26] Z.P. Jiang. A note on chaotic secure communication systems. *IEEE Trans. on Circuits and Systems I*. vol. 49, no. 1, pp. 92-96, 2002.
[27] Z. Li, D. Xu. A secure communication scheme using projective chaos synchronization[J]. *Chaos Solitons Fractals*. vol. 22, no. 2, pp. 477-481, 2004.
[28] A.B. Orue, V. Fernandex, G. Alvarez, G. Pastor, M. Romera, S. Li, F. Montoya, Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems. *Physics Letters A*. vol. 372, no. 34, pp. 5588-5592, 2008.
[29] Mahmoud F. Abd Elzaher, Mohamed Shalaby, Yasser Kamal, Salwa El Ramly. Securing digital voice communication using non-autonomous modulated chaotic signal. *Journal of Information Security and Applications*. vol. 34, part 2, pp. 243-250, 2017.