Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **2**, March **2016**

Synchronous Digital Signal Communication System Based on Chaotic Masking

Wangshu Li, Ziheng Yang* and Qun Ding

Heilongjiang University Electronic Engineering
*Corresponding author

Received September, 2015; revised October, 2015

Abstract. *In this paper, chaotic secure communications applications as the background, to explore a way to implement digital chaotic synchronization, using the driven response synchronization method, through chaos masking secure communication principle to realize. Through a variety of experimental observations, confirming the chaos masking secure communication can be applied to digital signal transmission, which build up the solid foundation for digital chaotic security communication.*
Keywords: Chaotic; Synchronization; Secure communication; Digitalization.

1. **Introduction.** Recently studies about chaotic encryption system and encryption chip continue to make new progress in the chaotic secure communication system, the system synchronization is still the key major research in chaotic secure communication system, and the main objective of the research is using the chaotic system to achieve secure communication. Chaotic secure communication principle is to make the communication system that both parties have agreed to some kind of synchronization control, in the response system through the synchronization feature or chaotic the transmit end uses the chaotic signal as a carrier, through a certain way to hide the useful information among the chaotic carrier. In response system by using the synchronous feature and chaotic dynamical properties demodulates information transmitted, thus achieving the whole process which starts from transmitting end encryption to receiving end decryption.

Chaos synchronization is the key to achieve secure communication for transmission communication system, since chaotic broadband noise characteristics, compound signal generally will be considered as noise signal, it is difficult to steal useful information, only through the chaotic synchronous system demodulation, the information transmitted can be demodulate, thus the secure communication will be realized [1, 2, 3, 4, 5]

Chaotic synchronized secure communication is a dynamic encryption method, processing speed is not related to the length of key, through the receiving end of chaotic system conducts driving control to achieve communication. Driving control is a forcing action, chaotic system continuously injects the data stream which contains a transmission signal to the receiving end, forcing receiving end and sending end operates synchronously, so the receiving end could demodulate useful information.

One of the advantages is of chaotic synchronization that transmission errors in a short time will not cause the error diffusion, and transmission errors of self-synchronizing encryption system can easily cause error diffusion, leading to decrypt error [6]. Chaotic synchronized secure communication is also very suitable when integrity requirements of

the information is not strict, such as video play, confidential meetings and other confidential multimedia streaming. In this paper, based on driving response synchronization method complete chaos masking secure communication, focusing on the experiment research of digital signal synchronization, in order to verify synchronization method of chaotic masked in terms of digital communication, lay the foundation for future digital signal synchronization applications.

2. **Driving – Response synchronization method.** Driving – response synchronization method is a chaotic synchronization method which is raised by the American scholar Pecora and Carroll in the early 1990s, also known as PC synchronization method [7]. The principle of this method is that the synchronous drive system is decomposed into two subsystems: one stable system which Lyapunov exponents are negative, and one unstable subsystems which Lyapunov exponent is at least one positive, and unstable sub-system will be copied as the response system. Using one of the system's output signal as a driving variable of another system, to achieve synchronization of two chaotic systems. The relationship between these two systems are driving and response, the state of the driving system determines the response system, but the state of the driving system is not affected by the response system.

n Dimensional autonomous dynamical systems can be defined by the function as following:

$$\dot{u} = f(u) \tag{1}$$

This system could be decomposed by v and w two sub-system, shown as following:

$$\begin{cases} \dot{v} = g(v, w) \\ \dot{w} = h(v, w) \end{cases} \tag{2}$$

Therein

$$u = \{u_1, u_2, u_3, \ldots, u_n\}^T, v = \{u_1, u_2, u_3, \ldots, u_{n_1}\}^T, w = \{u_{n_1+1}, u_{n_1+2}, u_{n_3+3}, \ldots, u_n\}^T$$
$$f = \{f_1, f_2, f_3, \ldots, f_n\}^T, g = \{f_1, f_2, f_3, \ldots, f_{n_1}\}^T, h = \{f_{n_1+1}, f_{n_1+2}, f_{n_1+3}, \ldots, f_n\}^T$$

Formula (2) is the driving system, in the form of sub-systems w copies another subsystem w', w' namely response system:

$$\dot{w}' = h(v, w') \tag{3}$$

In the formula v is generated by formula (2) systems as a driving variable input to the response system. Formula (2) and (3) compose the whole system:

$$\begin{cases} \dot{v} = g(v, w) \\ \dot{w} = h(v, w) \\ \dot{w}' = h(v, w') \end{cases} \tag{4}$$

Assigning $e = w' - w$, consequently the chaos synchronization error system is as following:

$$\dot{e} = h(v, w') - h(v, w) \tag{5}$$

Synchronization of chaotic systems is determined whether or not could be calculated by Lypaunov exponent (CLE, Conditional Lyapunov Exponent), if the response system (3) are all the CLE are negative, it can prove that response system and drive system achieve synchronization or construct Lypaunov synchronization error system function, then according to Lypaunov stability principles to determine the system synchronous stability.

When $t \to \infty$, if the two systems are progressive synchronized, then $e = w' - w \to 0$ so that:

$$e(t) = \lim_{t\to\infty} \|h(v, w') - h(v, w)\| = 0 \tag{6}$$

And the synchronization performance of the system is independent with the initial conditions.

3. **Chaos masking secure communication principal.** Chaos masking secure communication mode is firstly proposed by the Cuomo and Oppenheim in the year 1993, and they complete analog circuit experiment, it is also the first chaos communication method. Chaos covered is also known as chaotic masking, the basic principle is based on chaos synchronization, based on two interrelated chaotic system under certain synchronization method can be synchronized by passing the chaotic carrier, and this synchronization has a certain stability, namely add a little energy in the chaotic carrier signal which will not affect the performance of synchronization between the receiving system and transmitting system [**?**]. During communication, using pseudo-random characteristic of chaotic signal, the sender will be little information attached to the chaotic carrier signal, the information signal is hidden in the chaotic signals, generated compounded noise signal, realizing the encryption of the source information. At the receiving end, using the signal which is synchronized with sender and also separated from chaos system to achieve security of the information [8, 9, 10].

Chaos covered secure communication system structure principal is shown in Figure 1. In the system transmitting end, the chaotic signal $x(t)$ generated by the drive system mixes with sending messages $m(t)$, consequently the compounded signal $u(t) = x(t) + m(t)$ is seemingly like noise when it is passing through the common channel transmission. In the system of receiving end, the chaotic system driven by the driving signal $u(t)$, response system synchronized progressively with driving system of sender, the receiver can copy all the state variables of the transmitter, so you can copy reconstructed chaotic signal $x'(t)$, subtract signal $u(t)$ from $x'(t)$, then obtain a demodulated information signal $m'(t)$. When the chaotic system to keep synchronizing, the effects of signal distortion which is caused by external noise and channel distortion is small, there is $x(t) \approx x'(t)$, as a result in this case $m(t) \approx m'(t)$.

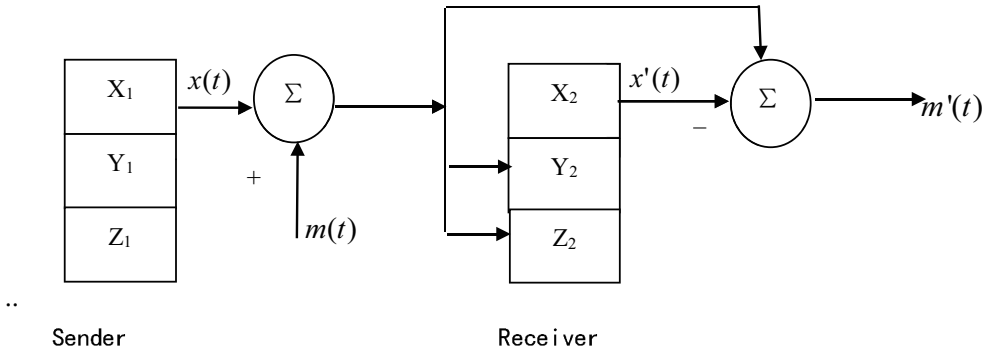


FIGURE 1. Chaotic covered secure communication principal diagram

Before source signal and chaos signal is superposed, the source signal converted by the function of $m(t)$, and then generate signal $x(t)$ superposes with chaos signal, generating compounded signal $f(x) = x^3 + 1$, sending to the channel. The Design of function $f(\cdot)$ can be diversified, as long as the system remains stable and chaos, and inverse function $f^{-1}(\cdot)$ exists.

Selected driving system is Lorenz system:

$$\begin{cases} \dot{x} = 10(y - x) + f(s(t)) \\ \dot{y} = 28x - y - xz \\ \dot{z} = xy - 8/3z \end{cases} \tag{7}$$

Response system is Chen System:

$$\begin{cases} \dot{x}' = 35(y' - x') + u_1 \\ \dot{y}' = -7x' - x'z' + 28y' + u_2 \\ \dot{z}' = x'y' - 3z' + u_3 \end{cases} \tag{8}$$

If $\dot{e}_1 = \dot{x}' - \dot{x}, \dot{e}_2 = \dot{y}' - \dot{y}, \dot{e}_3 = \dot{z}' - \dot{z}$.
Then system error equation will be:

$$\begin{cases} \dot{e}_1 = \dot{x}' - \dot{x} = 35(y' - x') - 10(y - x) + u_1 - f(s(t)) \\ \dot{e}_2 = \dot{y}' - \dot{y} = -7x' - x'z' + 28y' + u_2 - 28x + y + xz_1 \\ \dot{e}_3 = \dot{z}' - \dot{z} = x'y' - 3z' + u_3 - xy + 8/3z \end{cases} \tag{9}$$

$$\begin{aligned} \dot{e}_1 &= 35(y' - x') - 10(y - x) + u_1 - f(s(t)) \\ &= 7(e_2 - e_1) + 28y' - 28x' - 3y + 3x - f(s(t)) + u_1 \\ \dot{e}_2 &= -7x' - x'z' + 28y' + u_2 - 28x + y + xz \\ &= -7(e_1 + e_2) - x'z' + 35y' - 35x - 6y + xz + u_2 \\ \dot{e}_3 &= x'y' - 3z' + u_3 - xy + 8/3z \\ &= -3e_3 - 1/3z - xy + x'y' + u_3 \end{aligned}$$

Set

$$\begin{aligned} u_1 &= -28y' + 28x' + 3y - 3x \\ u_2 &= x'z' - 35y' + 35x + 6y - xz \\ u_3 &= 1/3z + xy - x'y' \end{aligned} \tag{10}$$

Then formula (4-4) applies in formula (4-2), obtaining response Chen system equation is:

$$\begin{cases} \dot{x}' = 7(y' - x') + 3(y - x) \\ \dot{y}' = 35x + 6y - 7(x' + y') - xz \\ \dot{z}' = 1/3z - 3z' + xy \end{cases} \tag{11}$$

Constructed Lyapunov function is:

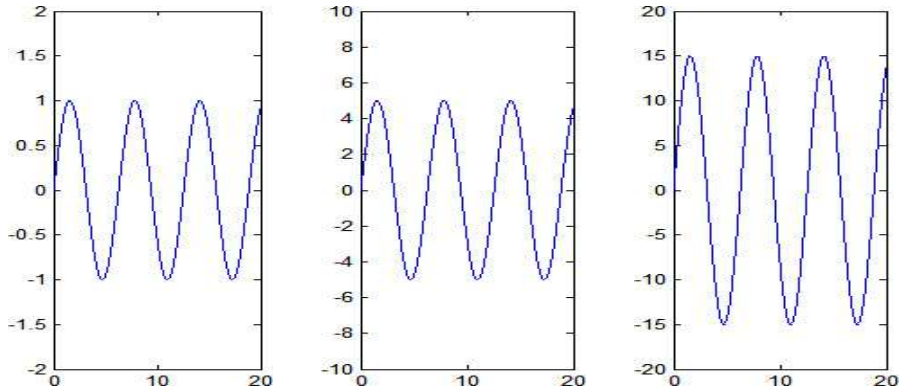
$$V = 1/2(e_1^2 + e_2^2 + e_3^2) \geq 0 \tag{12}$$

$$\begin{aligned} \dot{V} &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 \\ &= 7(e_2 - e_1)e_1 - 7(e_2 + e_1)e_2 - 3e_3e_3 \\ &= -7e_1^2 - 7e_2^2 - 3e_3^2 < 0 \end{aligned} \tag{13}$$

When $e_1 = e_2 = e_3 = 0$. Then $V = \dot{V} = 0$. According to Lyapunov stability theorem, error system (2-4) is progressively stable, so when $t \to \infty$, response system and driving system synchronize.

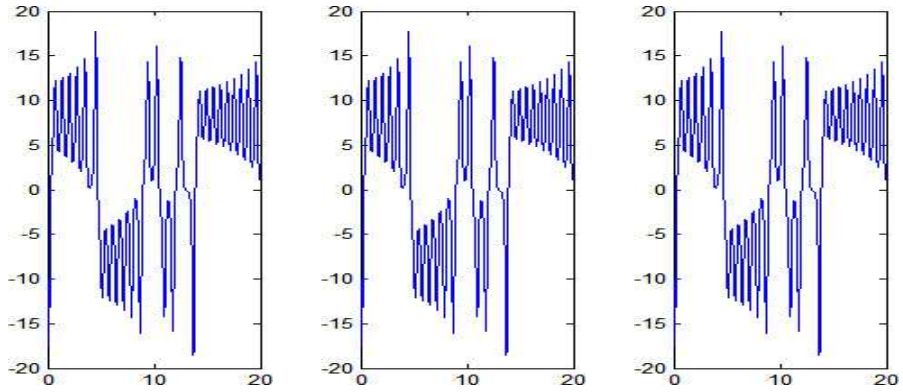
The system initial value is set as follows: The initial value of driving system is $(-10, -20, 15)$, response system initial value is $(1, 2, 3)$.

4. **Covered performance analysis of the analog signal.** 1.Through numerical analysis, let's discuss about the effectiveness of analog signal masking chaotic system encryption. Selecting one analog signal $m(t) = A\sin(wt)$, as in Figure 2 of (a), (b), (c) shown, the analog signal amplitude are respectively 1V, 10V, 15V when $w = 1$ before encryption. As in Figure 3 (a), (b), (c) shown, it is analog chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ before encryption. As in Figure 4 (a), (b), (c) shown, it is analog chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ after encryption. As in Figure 4 (a), (b), (c) shown, it is analog chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ after decryption.



(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 2. Original analog signal

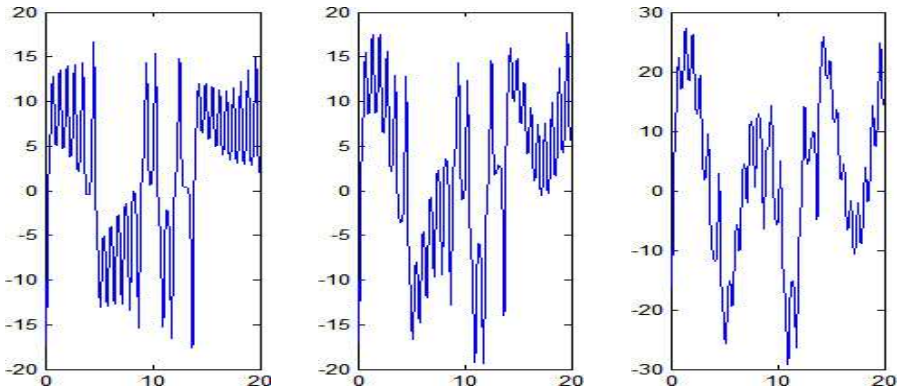


(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 3. Chaotic analog signal before encryption

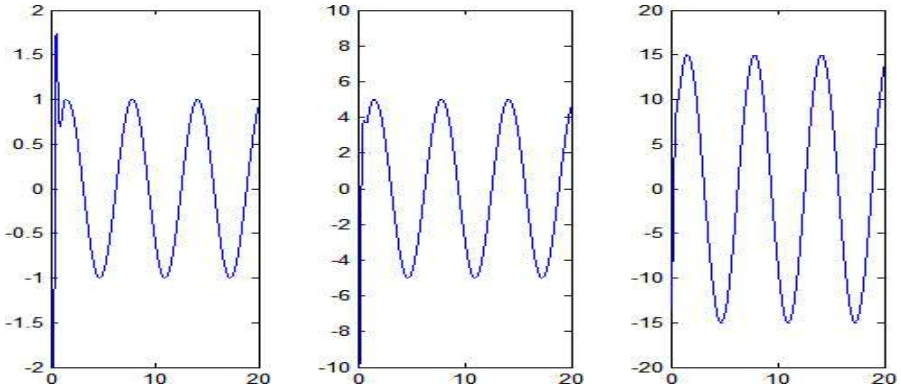
Through comparative analysis of figure 4 we know when analog signal at the same frequency, the chaotic signal is getting close to the shape of analog signal before encryption if the amplitude becomes larger. Therefore, if the signal amplitude becomes larger then confidentiality is getting worse which is getting easy to be deciphered. So that, along with the increasement of the original signal, the covering performance of driving response system is getting worse. Therefore, if the energy of the analog signal exceeds a certain value, the system can't be encrypted

2. As in figure 7 (a), (b), (c) shown, analog signal $m(t) = A\sin(wt)$ is before encryption when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively. As in figure 8 (a), (b), (c) shown, the chaotic analog signal $m(t) = A\sin(wt)$ is before encryption



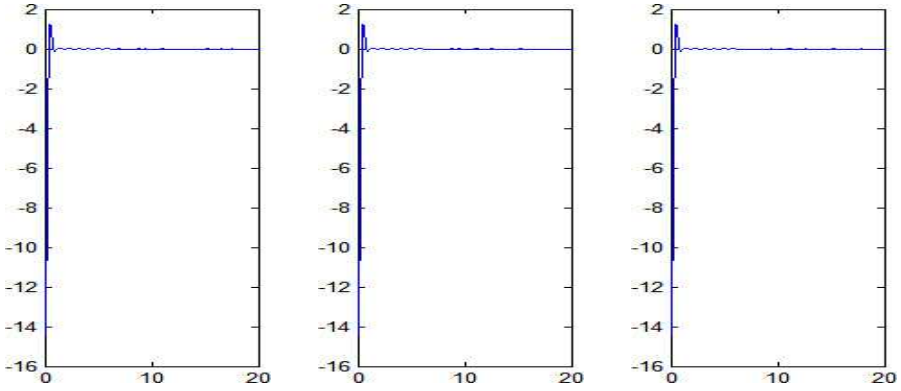
(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 4. Chaotic signal after encryption



(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 5. Chaotic analog signal after decryption

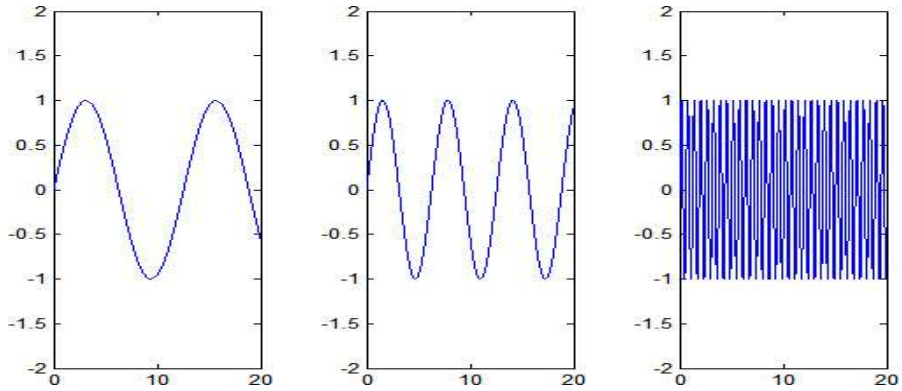


(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 6. The error of signal with the same frequency

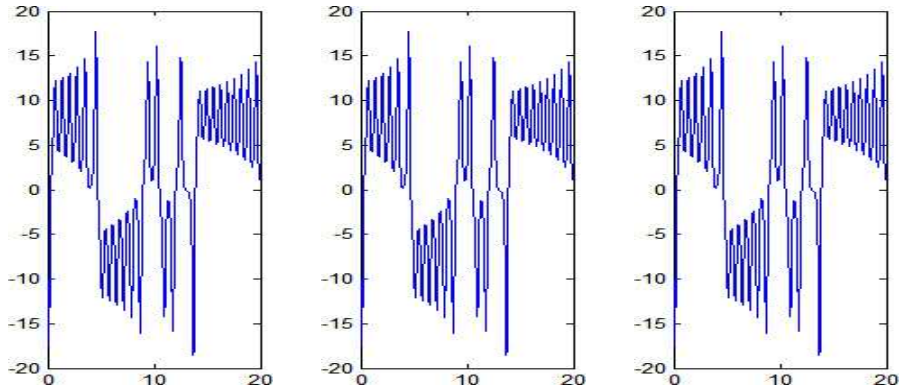
when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively. As in figure 9 (a), (b), (c) shown, the chaotic analog signal $m(t) = A\sin(wt)$ is after encryption. As in figure 10 (a), (b), (c) shown, the analog signal $m(t) = A\sin(wt)$ is after decryption when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively. As

in figure 11 (a), (b), (c) shown, it is the error of the signal when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively.



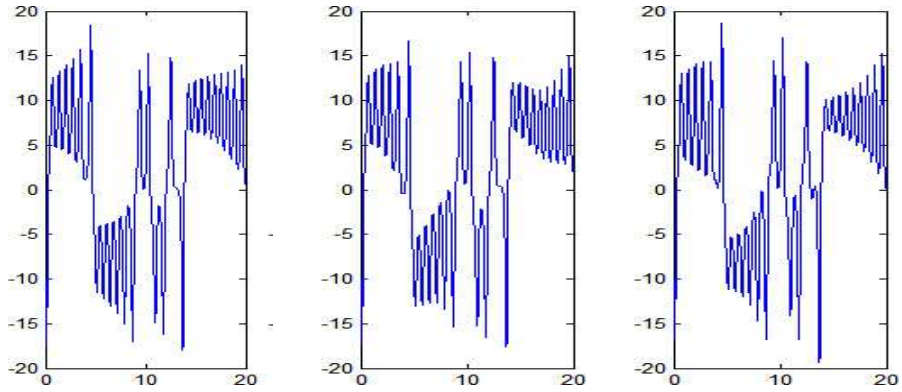
(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 7. The analog signal before encryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

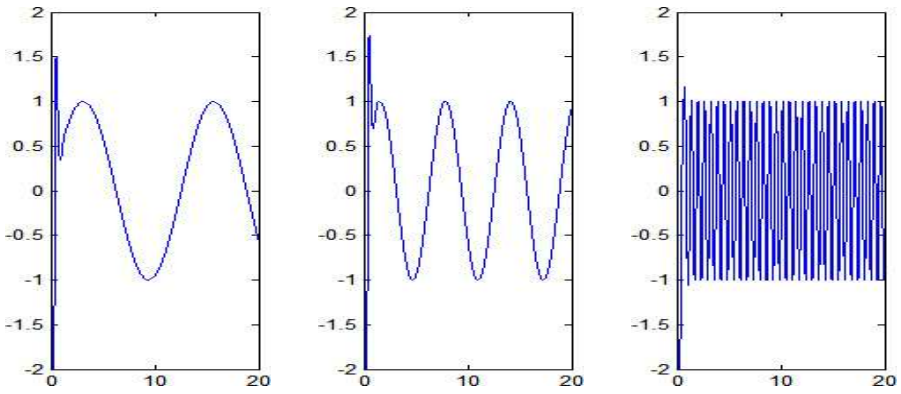
FIGURE 8. The chaotic analog signal before encryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

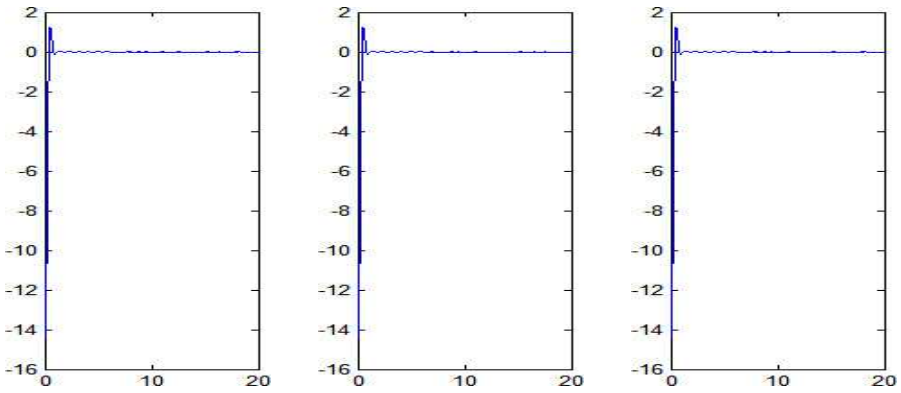
FIGURE 9. The chaotic signal after encryption

As in figure 9 shown, through Comparative analysis we get the result when the analog signal is at the same amplitude, there is no different in terms of security of the chaotic



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 10. The analog signal after decryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

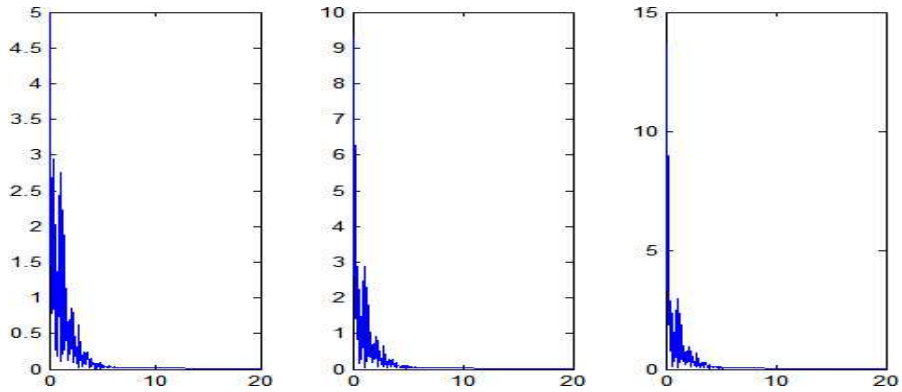
FIGURE 11. The error of signal with the same amplitude and different frequency

signal along with the changing of the frequency. This indicates that when the analog signal is encrypted during the transmission, analog chaotic signal masking effect and transmission signal are independent of frequency.

As in figure 12 shown, it is the spectrum of the chaotic signal after encryption when driving response system encrypts the analog signal, wherein the analog signal amplitude of figure (a), (b), (c) are respectively 1V, 5V, 15V.

Selecting several chaotic analog spectrum sample of amplitude, we have done the analysis of comparison, the frequency has no differences with the original chaotic analog signal.

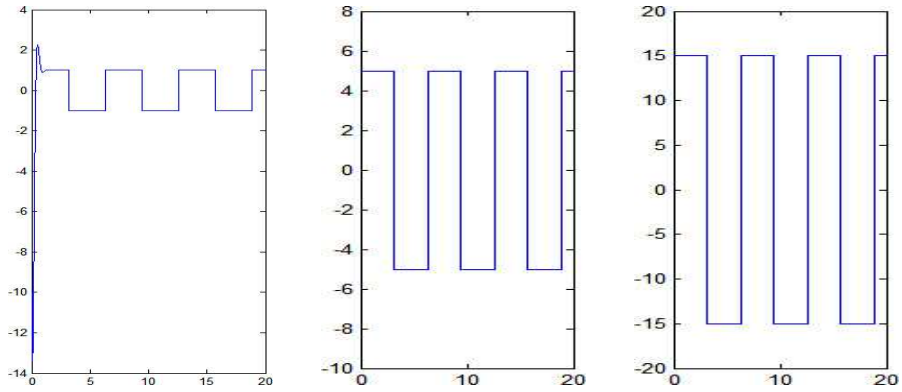
5. **Covered performance analysis of the digital signal.** Through numerical analysis, let's discuss about the effectiveness of digital signal masking chaotic system encryption. Selecting one digital signal $m(t) = A[0, 1]$, as in Figure 14 of (a), (b), (c) shown, the digital signal amplitude are respectively 1V, 10V, 15V when $w = 1$ before encryption. As in figure 15 (a), (b), (c) shown, it is digital chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ before encryption. As in figure 16 (a), (b), (c) shown, it is digital chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ after encryption. As in Figure 17 (a), (b), (c) shown, it is digital chaotic signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ after decryption. As in figure 17 (a), (b), (c)



(A) A = 1V (B) A = 5V (C) A = 15V

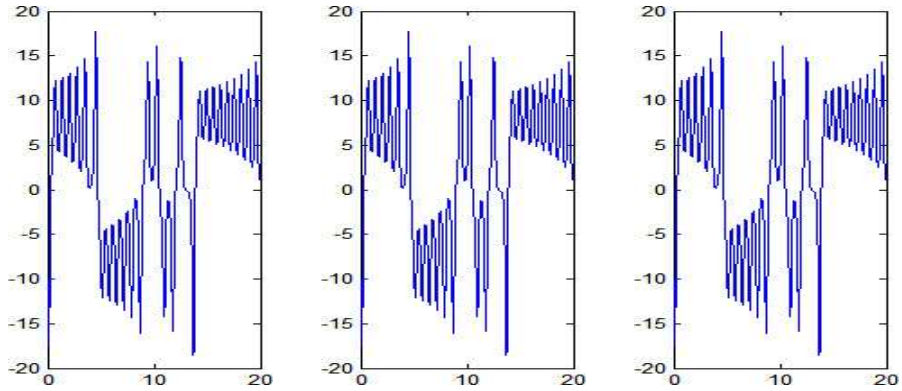
FIGURE 12. The spectrum after encryption

shown, it is the error of digital signal which amplitude are respectively 1V, 10V, 15V when $w = 1$ after decryption.



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

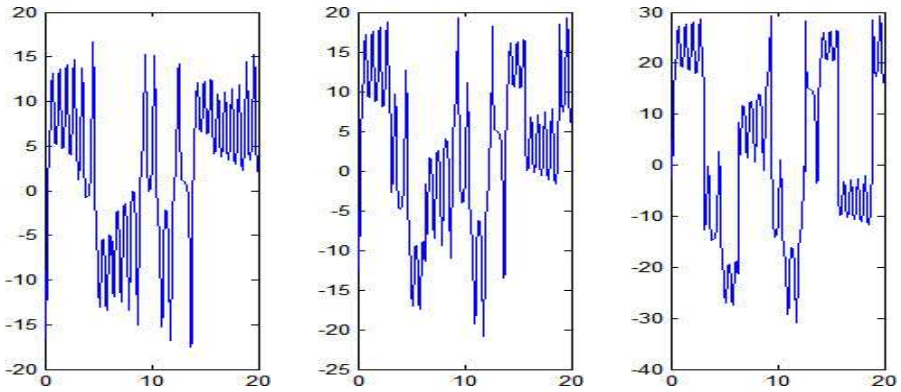
FIGURE 13. The digital signal before encryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

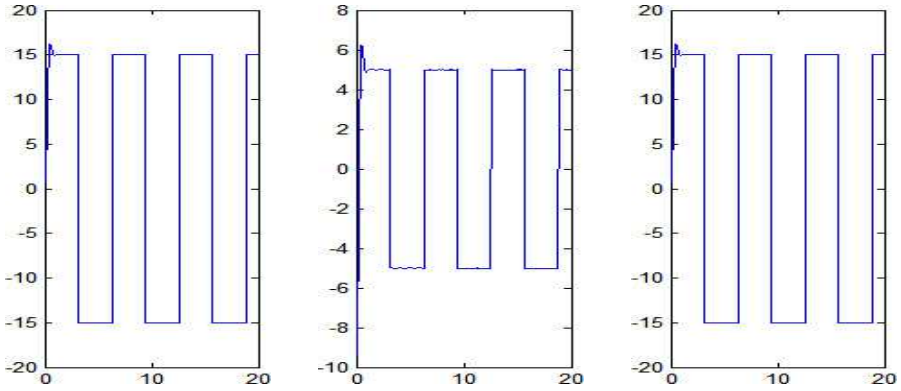
FIGURE 14. The digital chaotic signal before encryption

Through comparative analysis of Figure 15 we know when digital signal at the same frequency, the chaotic signal is getting close to the shape of digital signal before encryption



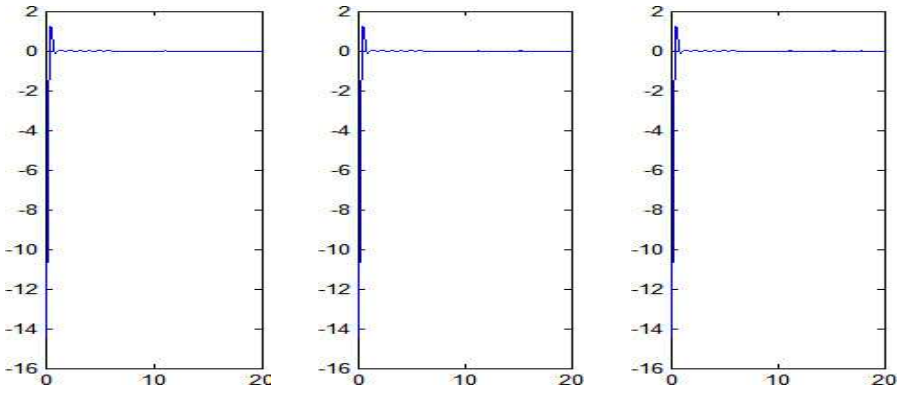
(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 15. The chaotic digital signal after encryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 16. The digital signal after decryption



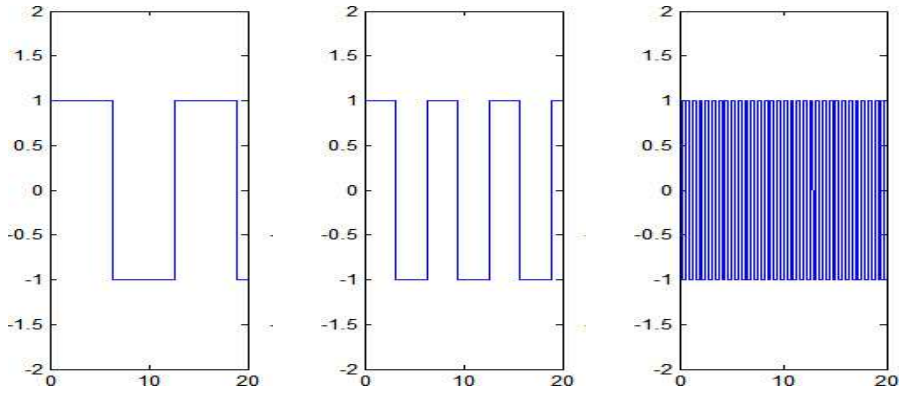
(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 17. The error of digital signal with the same amplitude and different frequency

if the amplitude becomes larger. Therefore, if the signal amplitude becomes larger then confidentiality is getting worse which is getting easy to be deciphered. So that, along with the increasement of the original signal, the covering performance of driving response

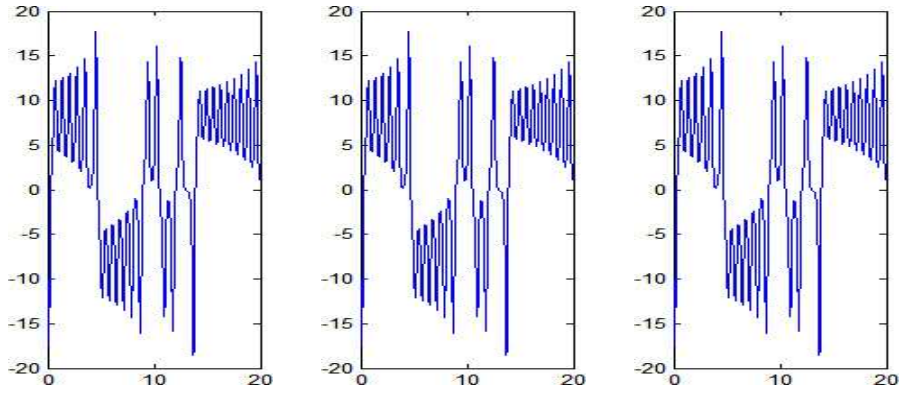
system is getting worse. Therefore, if the energy of the digital signal exceeds a certain value, the system can't be encrypted

As in figure 18 (a), (b), (c) shown, they are the digital modulated signal of $m(t) = A\sin(wt)$ before encryption when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively. As in figure 19 (a), (b), (c) shown, they are the chaotic digital signal before encryption when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively. As in figure 20 (a), (b), (c) shown, they are the chaotic digital signal after encryption. As in figure 21 (a), (b), (c) shown, they are the digital signal after decryption when the amplitude is 1, in addition with $w = 0.5$, $w = 1$, $w = 10$ respectively.



(A) (B) (C)

FIGURE 18. The digital signal before encryption



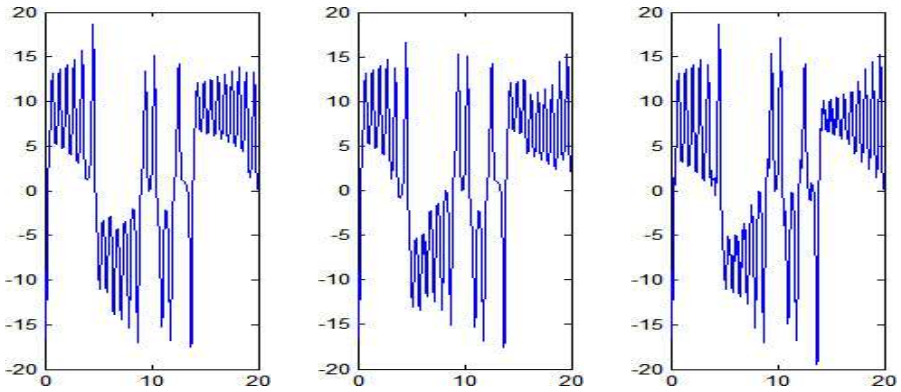
(A) (B) (C)

FIGURE 19. The digital chaotic signal before encryption

As in figure 20 shown, through Comparative analysis we get the result when the digital signal is at the same amplitude, there is no different in terms of security of the chaotic signal along with the changing of the frequency. This indicates that when the digital signal is encrypted during transmission, digital chaotic signal masking effect and transmission signal are independent of frequency.

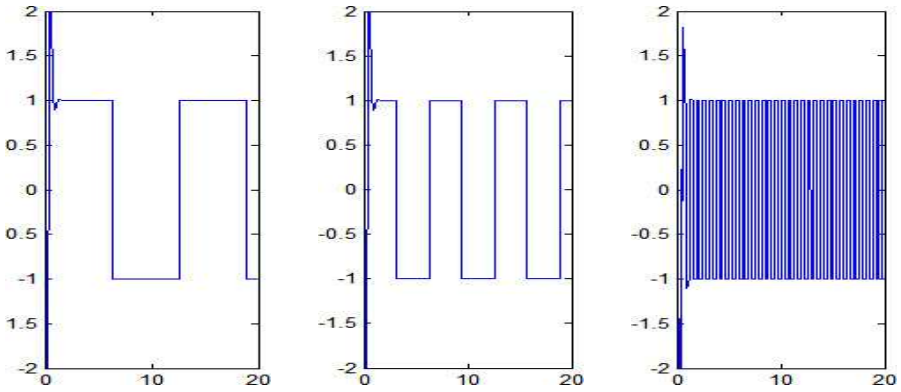
As in figure 23, when driving response system encrypts the digital signal, it is the spectrum of chaotic signal, wherein (a), (b), (c) 3 figures' digital signal's amplitude are respectively 1V, 5V, 15V.

Selecting several chaotic digital spectrum sample of amplitude, we have done the analysis of comparison, the frequency has no differences with the original chaotic digital signal.



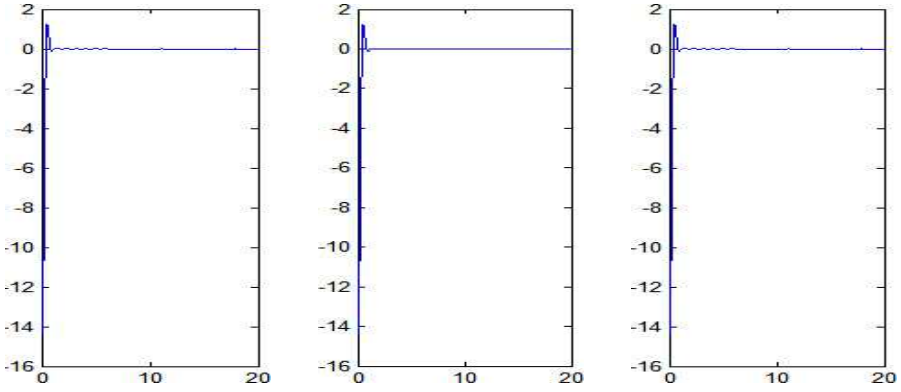
(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 20. The chaotic digital after encryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

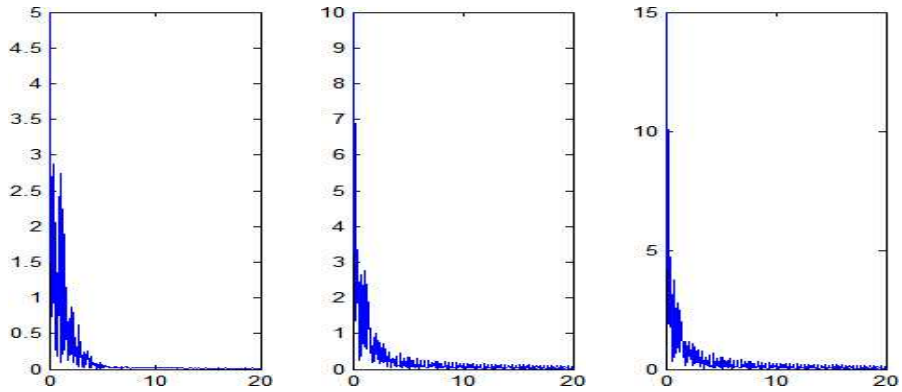
FIGURE 21. The digital signal after decryption



(A) $w = 0.5$ (B) $w = 1$ (C) $w = 10$

FIGURE 22. The error signal of the same frequency and different amplitude

6. **Conclusion.** The experiments show that the chaotic masking secure method of driving response system could encrypt both analog and digital signal, the effect of the encryption is only related to the energy of the signal. No matter analog or digital, as long as the original signal's energy is within the scope where chaotic signal could mask, the effect of encryption will be good. if it is beyond the scope of this energy, the effect of



(A) A = 1V (B) A = 5V (C) A = 15V

FIGURE 23. The spectrum after encryption

encryption will be lost. When the amplitude of the digital signal is 1, the chaotic signal after encryption can almost achieve the purpose of masking. The secure communication method could be digitized to explore the possibility of the application of digital secure equipment!

REFERENCES

[1] K. M. Cuomo, A. V. Oppenheim , S. H. Strogatz, Synchronization of Lorenz-based Chaotic Circuits with Applications to Communications, *Analog and Digital Signal Processing Transactions on [J]. IEEE Circuits and Systems II*, vol. 40, no. 10, pp. 626-633, 1993.

[2] T. Yang, X. F. Li, H. H. Shao, Chaotic Synchronization Using Backstepping Method with Application to the Chua's Circuit and Lorenz System, *Proceedings of the American Control Conference*, vol. 3, pp. 2299-2300, 2001.

[3] S. C. Qu, X. V. Wang, W. H. Tian, S. Li, The application research of Chaotic synchronization technology in secure communication, *Huazhong Normal University Periodical (Science version)*, vol. 44, no. 2, pp. 553-556, 2008.

[4] X. S. Luo, B. H. Wang, P. Q. Jiang, J. Q. Fang, One secure communication method base on chaotic progressive synchronization, *J. Communication periodical*, vol. 24, no. 1, pp. 60-65, 2003.

[5] Y. Liu, W. K. S. Tang, Cryptanalysis of Chaotic Masking Secure Communication Systems Using an Adaptive Observer, *J. IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 55, no. 11, pp. 1183-1187, 2008.

[6] M. Y. Chen, Chaos Synchronization in Complex Networks, *[J]. IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 46, no.3, pp. 1335-1346, 2008.

[7] T. L. Carroll , L. M. Pecora Synchronizing Hyperchaotic Volume-preserving Maps and Circuits, *J. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 45, no.6, pp. 656 - 659, 1998.

[8] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking Two Secure Communication Systems Based on Chaotic Masking, *J. IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 10, pp. 505-506, 2004.

[9] A. Uchida, Y. Liu, P. Davis, Characteristics of Chaotic Masking in Synchronized Semiconductor Lasers, *J. IEEE Journal of Quantum Electronics*, vol.39, no. 8, pp. 963-970, 2003.

[10] N. Yu, Q. Ding, H. Chen, Synchronization of different structure chaotic systems and applications in secure communication, *J. Communication periodical*, vol. 28, no. 10, pp. 73-78, 2007.