Chaos-Shift-Keying Secure Digital Communications using Feedback to Synchronize Chua's Circuit :Simulation and Realization

Liu Jie,Cai Tao,Xiao Jinghua,Zhang Yinghai, Wu Yuexin
Dept. of Applied Science and Technology ,
Beijing University of Posts & Telecommunications, Beijing 100088

Abstract:In this paper,a chaotic secure communication system via CSK modulation using feedback controlling receiver is presented. The transmitter and the receiver are built with Chua's circuits. We successfully transmit single character between two computers using this system.

1. Chaos-Shift-Keying (CSK) Modulation and Feedback Controlling Synchronization Demodulation

It is known that chaotic signal can be used in secure communications due to its close correlation with initial conditions.In this kind of communication, the transmitter's components' parameters and the receiver's must be nearly identical, the intercepter whose circuit's parameters is not the same as the transmitter's and the receiver's can just receive noiselike singal.

Kennedy [1] has demonstrated one technique to transmit digital information using a chaotic carrier and to detect those message using self synchronizing Chua's circuit. The transmitter in their system is a typical Chua's oscillator.In this method, one key S's " open " and " close " represent the binary data"+1" and "-1" , which to be transmitted over the channel. The key's opening and closing have changed the non-linear resistor - " Chua's Diode" 's charateristic and consequently have changed the transmitter circuits' parameters. The signal , which will be transmitted over the channel, is the voltage on the capacitor C1 and is a noise-like chaotic signal.

We use a pulse voltage source instead of the key S, this means that a square wave pulse signal is used to modulate the chaotic signal which will be transmitted. The square wave with different polarity represent the binary message "+1" and "-1". (See Fig.1.)

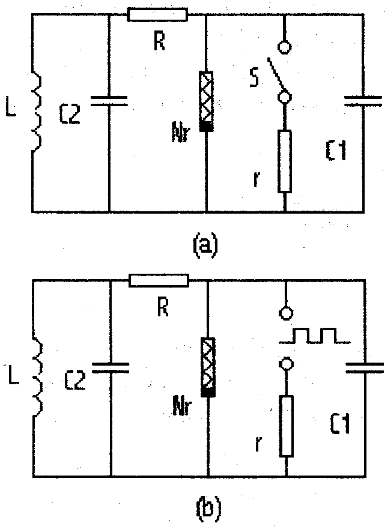

Fig.1 CSK Modulation Circuits,(a) Kennedy's transmitter(b)The transmitter used in present method

Meanwhile, We present one kind of decode circuits using feedback synchronization, as schematically shown in Fig. 2. [2] The transmitter is the same of Fig.1.The receiver is shown in Fig.3, one voltage controlled current source Is=K(Vc1-Vc12), is added as the method of feedback-controlling. K is the feedback coefficient.

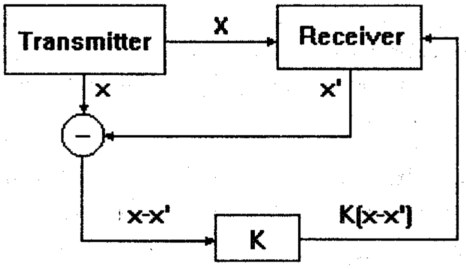

Fig.2 Scheme of feedback-controlling receiver circuits , K is the feedback coefficient

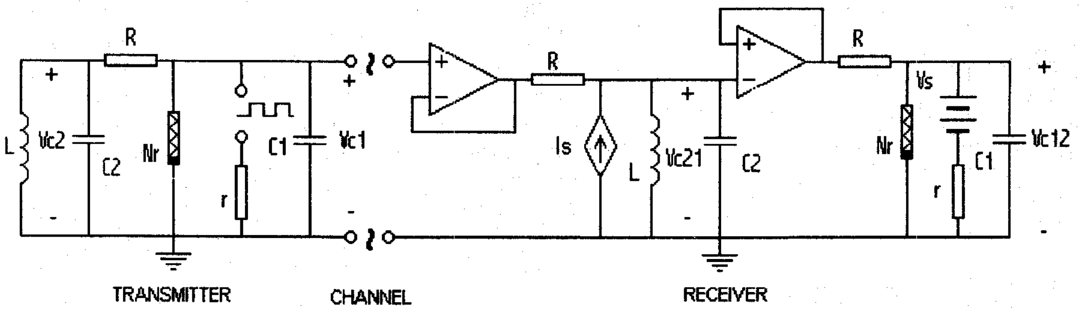

Fig.3 Feedback-controlling receiver

2.Computer Simulation

. In Fig.1, for bit "+1" and "-1" , the transmitter circuits can be described by eqs. (1) - (3) and eqs. (4) -(6),Vs is the amplitude of the pulse source.

$$(1)\quad C_1\frac{dv_{C1}(t)}{dt}=\frac{1}{R}(v_{C2}(t)-v_{C1}(t))-f(v_{C1}(t))$$

$$+\frac{1}{r}(v_S-v_{C1}(t))$$

$$(2)\quad C_2\frac{dv_{C2}(t)}{dt}=-\frac{1}{R}(v_{C2}(t)-v_{C1}(t))+i_{L1}(t)$$

$$(3)\quad L\frac{di_{L1}(t)}{dt}=-v_{C2}(t)$$

$$(4)\quad C_1\frac{dv_{C1}(t)}{dt}=\frac{1}{R}(v_{C2}(t)-v_{C1}(t))-f(v_{C1}(t))$$

$$+\frac{1}{r}(-v_S-v_{C1}(t))$$

$$(5)\quad C_2\frac{dv_{C2}(t)}{dt}=-\frac{1}{R}(v_{C2}(t)-v_{C1}(t))+i_{L1}(t)$$

$$(6)\quad L\frac{di_{L1}(t)}{dt}=-v_{C2}(t)$$

The receiver circuits (shown in Fig.3) can be described by:

$$(7)\quad C_1\frac{dv_{C12}(t)}{dt}=\frac{1}{R}(v_{C21}(t)-v_{C12}(t))-f(v_{C12}(t))$$

$$+\frac{1}{r}(v_S-v_{C12}(t))$$

$$(8)\quad C_2\frac{dv_{C21}(t)}{dt}=-\frac{1}{R}(v_{C21}(t)-v_{C1}(t))+i_{L2}(t)$$

$$+K(v_{C1}(t)-v_{C12}(t))$$

$$(9)\quad L\frac{di_{L2}(t)}{dt}=-v_{C21}(t)$$

In these equations, f(Vr)= Ir =G1Vr+(G0-G1) (|Vr+Bp|-|Vr-Bp|)/2 is the Vr-Ir characteristic of the three-segment piecewise-linear resistor which has a slope G0 in the cental region and a slope G1 in the outer region, Bp is the breakpoint.[3]

Using the fourth-order Runge-Kutta algorithm, we get the numerical simulations of eqs.(1)-(9) and draw the following conclusions:

(1) With the resistor r having appropriate value, the Chua' s circuits also operate on the chaotic double-scroll Chua's attractor, and it can transmit chaotic signal carrying binary digital information.

(2)During a bit "+1" transmission, the signal Vc12(t) of receiver circuits gets synchronization with the signal Vc1(t) of the transmitter circuits, the difference between two signals, (Vc1(t) - Vc12(t)), decrease exponentially to zero. During a bit " -1 " transmission, to the contrary, Vc1(t) do not synchronize with Vc12(t), this difference look like noise.(See Fig.4)

(3)When a binary data stream containing "+1" and "-1" bit is transmitted,it could be observed that the receiver circuits get synchronization and lose synchronization alternatively, as shown in Fig.5.

(4)By this method, we can restore the binary message " +1 " or " -1 " from the received chaotic singal.

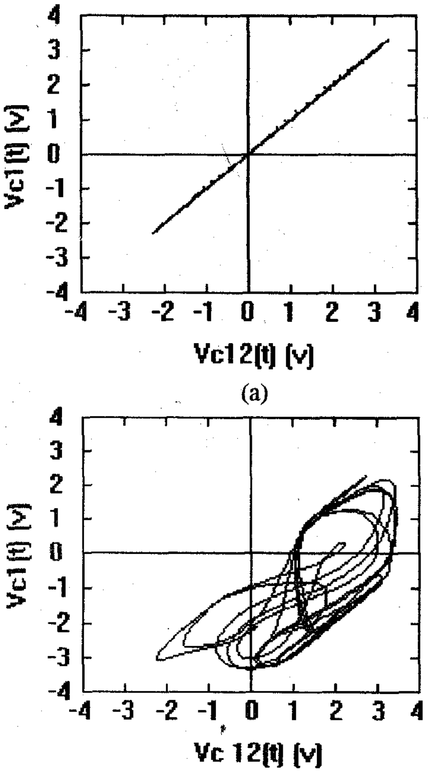

Fig.4 (a)Vc1(t) synchronize with Vc12(t) when bit "+1" transmitted, (b)do not synchronize with Vc12(t) when "-1" transmitted

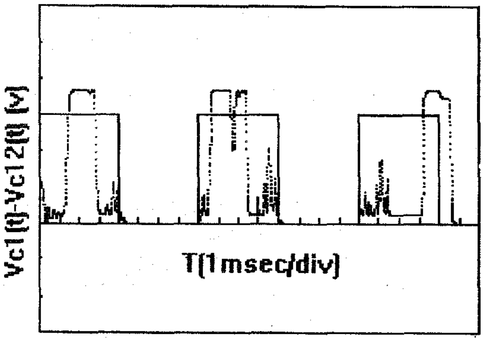

Fig.5 Modulation and Demodulation of digital signal

3. Experimental Realization

The experimental work in our laboratory has demonstrated that a 150 Bauds digital signal was successfully transmitted and decoded. (See Fig.6) From computer 1,one character, such as "a", is sent out,it's ASCII code stream act as the square wave source which is added on the transmitter(See Fig.1(b)), we get the signal Vc1(t)-Vc12(t) from the receiver circuits, and through some process,we restore this character 's ASC II code , and feed in computer 2 through it's communication port, and display this character. Now in our laboratory ,the speed of this transmission is 150 Bauds,the bit error ratio is below 10^{-3}. When the transmission speed is 300 Bauds,the bit error ratio is about 10^{-2}. And when the resistance R of the receiver circuits (See Fig.3) is changed by 5%,the bit error ratio is nearly 100%, which means the security communication can be realized through this method.

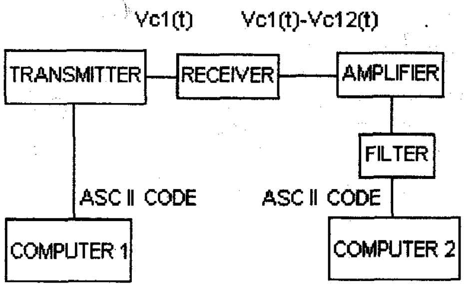

Fig.6 Experimental system of security digital communication

4. Conclusion

We have proposed one method of chaos-shift-keying modulation and feedback -controlling reception in chaos signal communications and realize one character's transmission between two computers using chaotic singal.

Theoretic calculation and experiment verify that with feedback-controlling method,one security digital communication system can be constructed.

References

[1] H. Dedieu , M. P. Kennedy, M. Hasler, " Chaos Shift Keying : Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS -|| : ANALOG AND DIGITAL SIGNAL PROCESSING,VOL.40,NO.10, OCTOBER 1993

[2]Liu Jie, Cai Tao, Xiao Jinghua, Zhang Yinghai, Wu Yuexin, "Chaos-Shift-Keying Secure Digital Communication using Feedback to Synchronize Chua's Circuit" , THE JOURNAL OF CHINA UNIVERSITIES OF POSTS ANDTELECOMMUNICATIONS, VOL.3, NO.2, 1996

[3] M. P. Kennedy," Three Steps to Chaos--Part || : A Chua's Circuit Primer, IEEE TRANSACTIONS ON CIRCUTS AND SYSTEMS | : FUNDAMENTAL THEORY AND APPLICATIONS, VOL . 40, NO.10, OCTOBER,1993