The Secure Communication Technique Based on Lorenz Chaos System

YE Fei
Army Officer Academy, PLA
Anhui Hefei, China
yefeixyz@163.com

ZHOU Jie
Army Officer Academy, PLA
Anhui Hefei, China
962854399@qq.com

LUO Jun
Army Officer Academy, PLA
Anhui Hefei, China
luojun09@163.com

GAO Xingrong
Army Officer Academy, PLA
Anhui Hefei, China
happyrong4587@163.com

***Abstract*—Chaos system has important application to secure communication for its indeterminism. Based on studying the theory of chaotic encryption system, the Lorenz chaos system is applied to construct serial code and encrypt information, and then an experiment of encrypting speech validates that Lorenz chaos encryption system is validity.**

Keywords- ***chaos system; Lorenz model; secure communication***

I. Introduction

Chaos system is a determinate dynamics system, but presents quasi-stochastic specialty, it has characteristic as follow: (1) the action of chaos system is a set of many sequence actions, but each action is not dominant in natural condition; (2) chaos is determinate although it presents quasi-stochastic; (3) chaos system is sensitive to original condition. Two same chaos systems present completely different state quickly if their original state has litter difference[1]. Chaos signal can be used to product secret key stream because of its big periods and excellent stochastic specialty. It is more important that chaos system can provide many secret keys because it's sensitive to original value and parameter.

The paper researches the application of the Lorenz chaos series to secure communication and then speech cannot be intercepted and captured by the third party.

II. Lorenz Chaos System

The famous Lorenz model can be presented as:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = bx_1 - x_2 - x_1 \bullet x_3 \\ \dot{x}_3 = x_1 \bullet x_2 - cx_3 \end{cases} \qquad (1)$$

In formula x_1 is the action state of liquid; x_2 is the temperature change in level direction; x_3 is the temperature change in uprightness direction; a,b,c is Prandtl coefficient, Rayleigh coefficient and the geometry coefficient which is ratio to the size of considered area separately. If set a=10, b=28, c=8/3, the system is chaos system. The time response figure of state variable and the three dimension figure of state phase space shows as Fig1 and Fig2 separately.

The quality of chaos signal is the key of encrypting effect. Lorenz equation is three -dimension chaos system and this construction is more complicated for it's has multi-variable and multi-parameter, so the time series hasn't rule and indeterminism much more. Using Lorenz equation to construct series has virtue as follow[2]:

(1) Multi-variable is disposed to product time series. The original chaos floating point numbers series can be the series value with one chaos variable or the function value of multi- variable. The design of this series code is more agile and has bigger space, and it provides the probability to solve the short period effect which is brought by finite precision in order to increasing security.

(2) A great deal of secret key space can be provided. Lorenz equation has multi-variable and multi-parameter, these can be used as seed code to produce series code system. If adding part variables to the design process, the code space of algorithm will greatly bigger then the series code constructed by the chaos equation with low dimension.

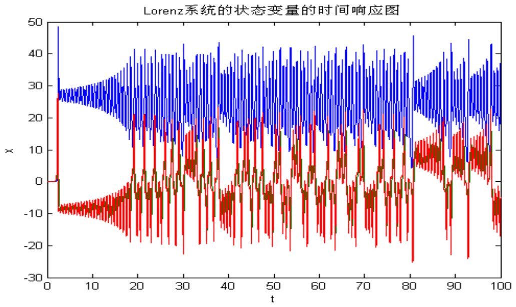


Fig.1 The time response figure of state variable of Lorenz

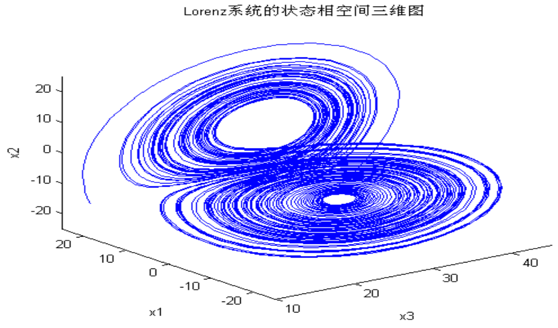


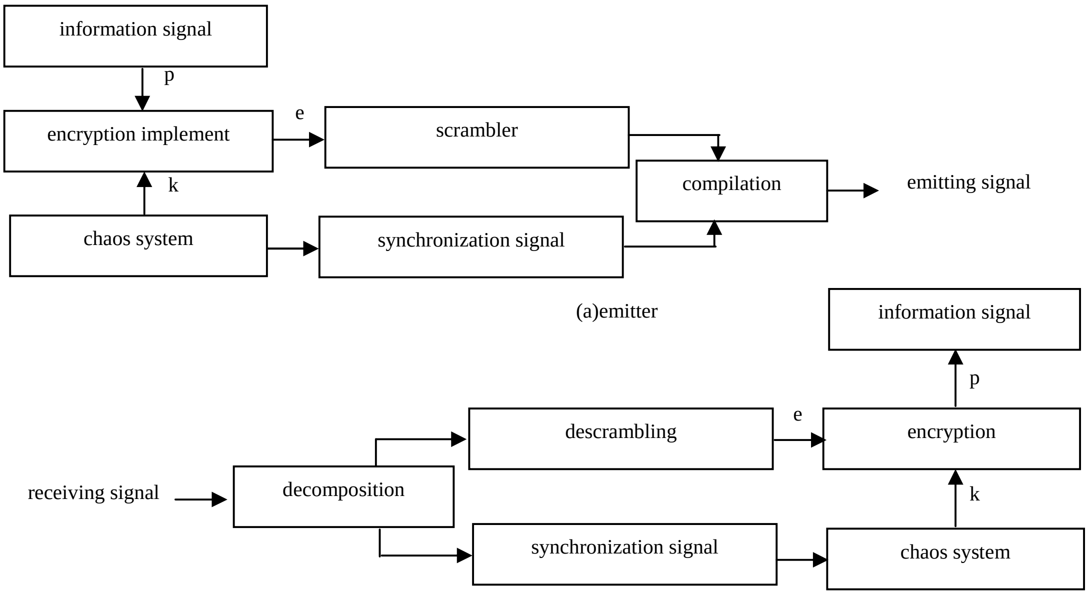
Fig.2 The three dimension figure of state phase space of Lorenz system

III. CHAOS ENCRYPTION SYSTEM

The various encryptions used chaos signal or chaos system belong to chaos encryption system. The basic theory of chaos secure communication is to make use of the aperiodic broadband chaos signal with statistic characteristic approached to Gauss white noise. Useful information signal is processed chaos cover in emitter and is disposed of cover by using synchronization chaos signal in receiver, and then the useful information signal is recovered. The theory frame figure of typical system shows as Fig1[3][4].

In emitter $e(t)=p(t)+k(t)$, $p(t)$ is information signal and calls plaintext in encryption system, and that is to say information signal will be encrypted. $k(t)$ is chaos signal, $e(t)$ is cipher. In receiver $\hat{p}(t)=e(t)-k(t)$, $\hat{p}(t)$ is the recovered information signal.

For ideal signal when the chaos signal in receiver is equal to the chaos signal in emitter, the information signal $\hat{p}(t)=p(t)$ can be recovered. There have two approaches: one is use of chaos synchronization method, the chaos circuit of receiver arrives at synchronization with the chaos circuit of emitter. The other adopts the same chaos circuit of receiver with emitter, and then their go all the way by controlling the original state of chaos circuit.



(a)emitter

(b) receiver

Fig3 Typical chaos encryption system

IV. The Secure Communication Based on Lorenz Chaos System

In order to show the application of Lorenz chaos system to secure communication, speech signal is used to make a simulation experiment. At section of speech signal is recorded at first and then is memorized in digital form. In matlab6.5 program, this speech signal is read and drawn original figure as Fig 4 (over), and be carried out three levels wavelet decomposition, so low frequency parts and high frequency parts can be found. Then a Lorenz chaos series is selected like Fig 4 (middle) and embedded to signal's low frequency parts, here corresponding embedding speech signal figure as Fig 4 (down).The signals before and after embedding are played, and original speech signal can be played naturally, but the played sound after embedding Lorenz chaos signal is similar to noise and unable to understand.

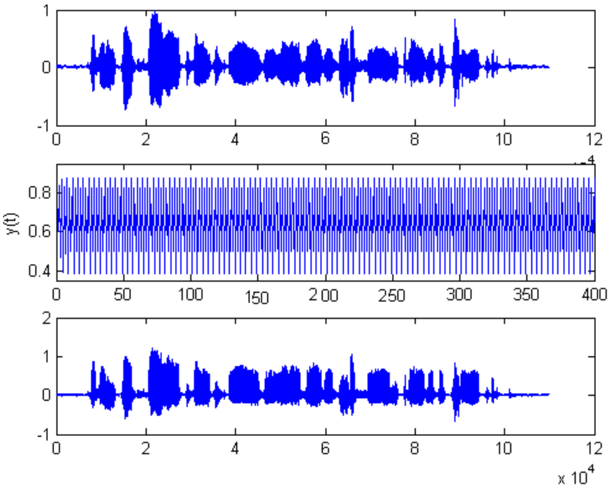


Fig4 Original speech signal, Lorenz chaos series, the speech signal after embedding

Time-frequency is adopted to analyze the speech signal before and after embedding, as Fig 5 and 6, two signals' local time-frequency characteristic have difference in time-frequency figure, original speech's time-frequency figure expresses speech signal change-with-time characteristic, but the speech signal embedded Lorenz chaos series expresses false noise's characteristic in time-frequency figure. Corresponding time figures and frequency figures have difference after comparing and analyzing. In Fig 6, the time signal wave has lots of difference from original speech wave, and presents tanglesome wave shape resembled noise. The frequency figure presents broad band characteristic resembled noise frequency spectrum, and again validates that Lorenz chaos series has better robustness and security as Lorenz chaos series to encrypt speech signal.

V. Conclusions

Chaos system can provide numerous, uncorrelated, quasi-stochastic but certain reproducible signal for it has sensitive dependence on initial values, so the chaos system has important application to the encryption algorithm of the data communication. The paper uses Lorenz chaos series to encrypt speech signal, and the speech signal before and after encrypting is analyzed in time-frequency domain, then the result indicates that chaos encryption system is effective.

References

[1] LIU Bingzheng, PENG Jianhua. Nonlinear Dynamics[M]. Beijing: Higher Education Publishing, 2003

[2] YE Fei, LUO Jingqing. Color Image Watermarking Algorithm Based on Lorenz Chaos Encryption[J]. Computer Applications and Software. Vol.25, No.12, 2008: 278-280

[3] WANG Jianan, DING Qun, Implementtation of a Novel FM-CDSK Digital Secure Communication System[J]. Communication Technology. Vol .44, No. 2, 2011: 75-77

[4] WANG Xin, NIE Chunyan, The Application of Chaotic Synchronization Technology in Secure Communication [J]. Journal of Changchun University. Vol.21, No.4, 2011: 25-28.

[5] ZHANG Junfeng, FENG Qiaojuan, ZHANG Xiaoli. Exponential Synchronization Method of Chaotic systems with Application in Secure Communications. Application Research of Computer. Vol. 28, No. 9, 2011:3495-3498

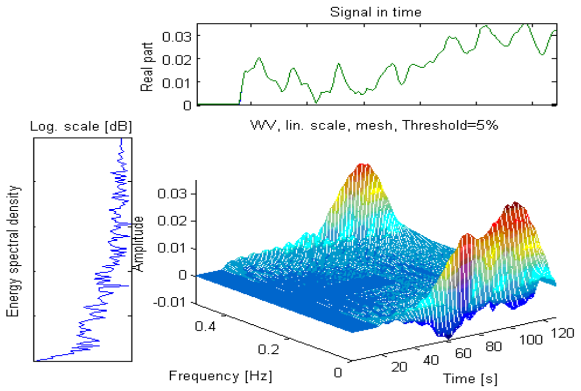


Fig5 Original speech time and frequency figure

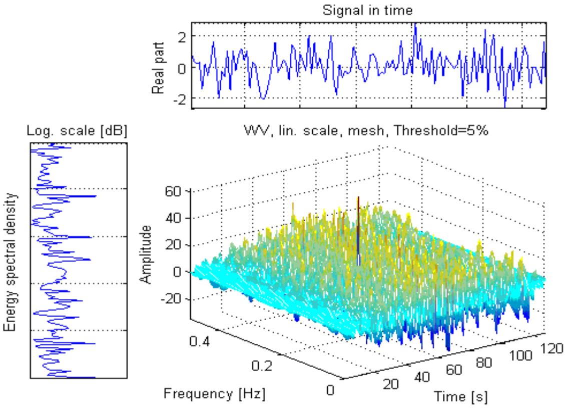


Fig6 Speech time and frequency figure after embedding