Front. Optoelectron. China 2008, 1(1–2): 64–69
DOI 10.1007/s12200-008-0009-1

RESEARCH ARTICLE

Security of polarization-shift keying chaos optical communication system

Nian FANG (✉)[1], Lutang WANG[1], Shuqin GUO[2], Zhaoming HUANG[1]

1 School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China
2 College of Information and Engineering, Zhejiang University of Technology, Hangzhou 310014, China

Abstract To evaluate the security of a chaos optical communication system employing the polarization-shift keying (PolSK) modulation technology, its chaos characteristic needs to be verified. In this paper, an analysis was done for the signal of this system. Three methods were used to judge whether the signal was maintaining chaos characteristics or not: watching the strange attractor in three-dimensional phase space, computing the largest Lyapunov exponent by the equation which meets and Wolf's method, and evaluating the self-power spectrum density function. As a result, the strange attractor was clearly watched, the largest Lyapunov exponent was positive 0.0364 and 0.0106 respectively, and the self-power spectrum was wide and continuous with the noise background. The evaluation of chaos for the signal transmitted in the system is therefore presented. On the other hand, the minimal embodied dimension of the signal was given by the false nearest neighbors (FNN) method and it reached 6, which showed the higher dimension chaos characteristics of the system. Adding the analysis of the ability of anti-attack for the system, it is concluded that the system has higher security than the normal chaos masking schemes.

Keywords optical communication, security, strange attractor, the largest Lyapunov exponent, Wolf's method, false nearest neighbors (FNN) method, polarization-shift keying (PolSK) modulation, fiber ring laser

1 Introduction

In the parametric modulation method of the optical chaos transmission system, parameters that can be used include light wave intensity, wavelength (frequency), phase and polarization. At present, many studies have been focusing on the parametric modulation of light intensity [1], wavelength (frequency) [2] and phase [3] etc. Only a few of them are focusing on optical polarization modulation. According to the study results by Rajarshi Roy et al. [4], in a fiber ring laser chaotic system created by erbium-doped fiber amplifier (EDFA), the light wave has high-speed and high-dimensional (polymorphism) changes in the polarization state. Therefore, high confidentiality and high bit-rate for message transmission can be achieved by using the polarization modulation of the chaotic system.

Lutang Wang et al. [5,6] have reported the research findings for realizing optical chaos communication by utilizing the polarization technology, which mainly uses the optical chaos system polarization-shift keying (PolSK) modulation technology to realize the secure communication. The PolSK modulation technology modulates the digital code to the polarization state designated. When PolSK modulation technique is applied to a chaotic system, the corresponding relation of the polarization state and digital code state will be in a dynamic process. In a randomly changing process, instead of a fixed polarization state, a certain state of code is represented. This paper will concentrate on the analysis of the system's security.

2 Experimental system and operating principle

The experimental system of the PolSK chaos secure optical communication is shown in Fig. 1. The system is made of a semiconductor optical amplifier (SOA) based fiber ring laser as a dynamical chaotic transmitter, a 5-km single-mode fiber as the communication channel and an open-loop chaos receiver with the time-delayed configuration.

In the transmitter, the key device is the semiconductor optical amplifier. Here we use the SOA module

Translated from *Acta Optica Sinica*, 2006, 26(6): 812–817 [译自: 光学学报]

E-mail: nfang@staff.shu.edu.cn

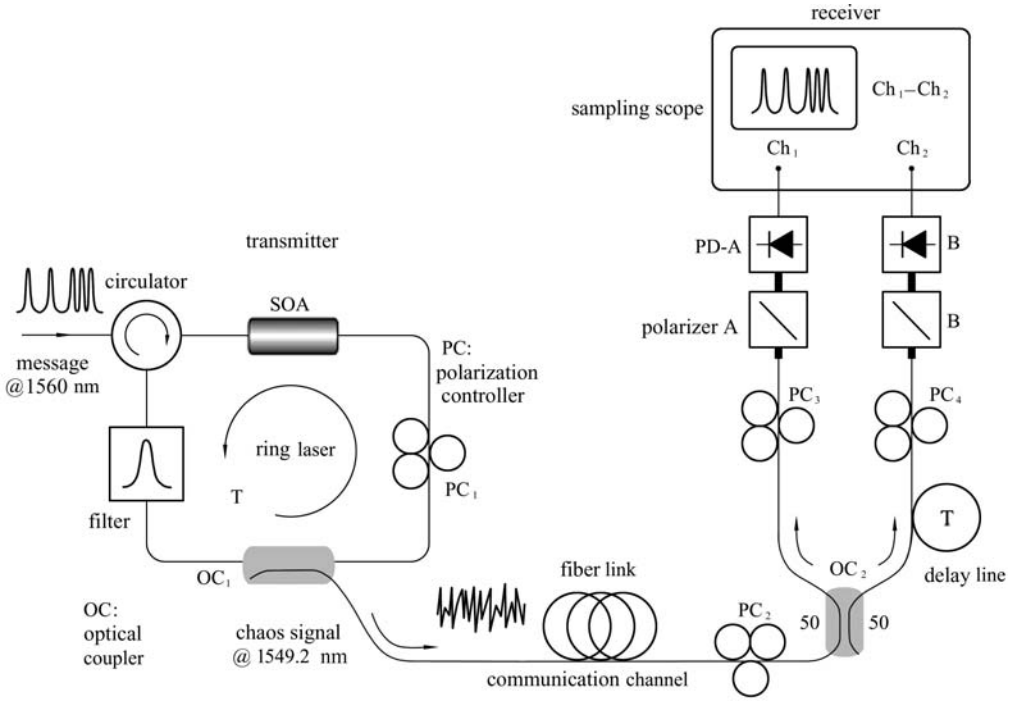

Fig. 1 Setup of the experimental system of PolSK chaos secure optical communication

(SOA1550MRI/X-1500) from OptoSpeed Corporation. The random distribution birefringence effect in the fiber results in the light transmitted in the fiber ring having a different polarization state in different parts, and changing with different cycle index. On the other hand, varieties of SOA's operating state and some external factors, such as temperature and vibration, lead to the change of light polarization state with time. Therefore, the fiber ring laser is a chaotic dynamical system in terms of light polarization state, and the output optical signal is a polarization chaotic one. When the light transmitted in the fiber ring passing through the SOA, it is to be enlarged and eventually outputted as the laser form. Its working wavelength is dependent on the center wavelength of the optical filter in the ring. The optical circulator is used for the input of the message signal and works as the optical isolator to restrict the propagation direction of light in the fiber ring too. The chaotic optical signal is outputted by the fiber coupler OC_1. The input optical signal passes through the SOA only once, and its propagation direction is opposite the chaotic light. The input message lights are a group of 27-bit pseudo random RZ coded circular sequence with the data bit rate of 630 Mb/s and the average optical power intensity of 2.1 dBm. When the input signal is code "0", the fiber ring stays constant. However, when the input signal is code "1", the change in the optical power leads to the alteration of the gain of SOA, and further leads to the change of refractive index of the SOA active medium, and finally leads to the chaotic light's phase change. Therefore, the input message light can control the phase change of chaotic light and further change its polarization state through the cross phase modulation (XPM) effect of SOA. That is to say, the information of the input signal can be modulated dynamically to the polarization state of the chaotic light. The polarization controller PC_1 in the fiber ring adopts the General Photonics Corporation's fiber extruder (PLC-001) and is used to set the initial equivalent birefringence of the fiber ring, which is a key parameter for the system synchronization [6].

At the receiver side, we use a polarization controller PC_2 to adjust the polarization state of the transmission light. The chaotic signal lights are divided into two equivalent routes to be received through optical coupler OC_2. Branch A receives the chaotic signal directly, and branch B receives it after proper delay. The outputs of two photodetectors connect to the two input channels of the oscilloscope respectively. In the oscilloscope, we subtract the signal intensity of the two channels to regenerate the transmitted signal. We use the Agilent digital sampling oscilloscope (Agilent Corporation's Infiniium, 1.5 GHz bandwidth and 8 GHz sampling rate).

3 Judgment to chaotic signal

Chaotic motion is the nonlinear property of a system, but not all of the nonlinearity is chaotic. Therefore,

nonlinearity is only the necessary condition for generating chaos, but not the sufficient condition [7]. Above all, we must judge whether the optical signal transmitted in the system is a chaotic signal or not.

First, we reconstruct the phase space of the experimental signal [8]. Phase space reconstruction is actually the projection from the system phase space to the reconstruction space. If the reconstruction dimension is too small, the phase space tracks of the system will project to the low-dimension space, which will produce many false crosses (that is, false neighbors). With dimensions of the reconstruction increased, the false neighbors will be reduced. When the reconstruction dimensions are large enough, it will be considered that the false neighbors are nonexistent. We call the reconstruction an embedding [9]. Usually, we call the suited (without false neighbors) reconstruction dimension the embedding dimension.

The delay-coordinate method constructs a multi-dimensional space vector by time series. For a time series with N points $x(t_0+n\Delta t)$ $(n=0,1,...,N-1)$, using Takens theorem, we can get the corresponding reconstruction track [10]

$$\begin{aligned} Y(n) &= [x(t_0)\ x(t_0+\Delta t)\ \cdots\ x[t_0+(k-1)\Delta t]] \\ &= \left(Y_{ij}\right)_{m\times k}, \\ Y_{ij} &= x(t_0+(i-1)J\Delta t+(j-1)\Delta t), \end{aligned} \tag{1}$$

where $x(t)$ is the state vector of the embedding space, J is reconstruction delay, m is the embedding dimension, Δt is sampling interval, and $k=N-(m-1)J$, $\tau=J\Delta t$ represents delay parameter.

In the following, we will judge whether the signal maintains chaos characteristics or not by combining three methods.

3.1 Direct observational method

According to the results of numerical calculation of the dynamical system, we were able to determine the changing relation with time for phase tracks and the changing course with time for state variables in phase space. By comparison and analysis we can determine the chaos phenomenon. In phase space, periodic motion corresponds to the closed curve, and the chaotic motion corresponds to the nonclosed tracks (strange attractors) of random distribution within a certain region [7]. The tracks that the random motion correspond to are disorderly and unsystematic, and without attractors.

We select the experimental signal with a data length of 402. After the calculation of phase space reconstruction, we get the changing figure with time of the phase tracks in phase space for the transmitted signal of this experimental system. We also give a phase track of a random noise signal with corresponding data length for comparison, as shown in Fig. 2. From Fig. 2(a), we can see that the optical signal transmitted in the system does contain an attractor, and it should be classified as a chaotic signal. However, in Fig. 2(b), we cannot see any law from changes with the time of the phase tracks of the random noise signal, and no attractor is seen.

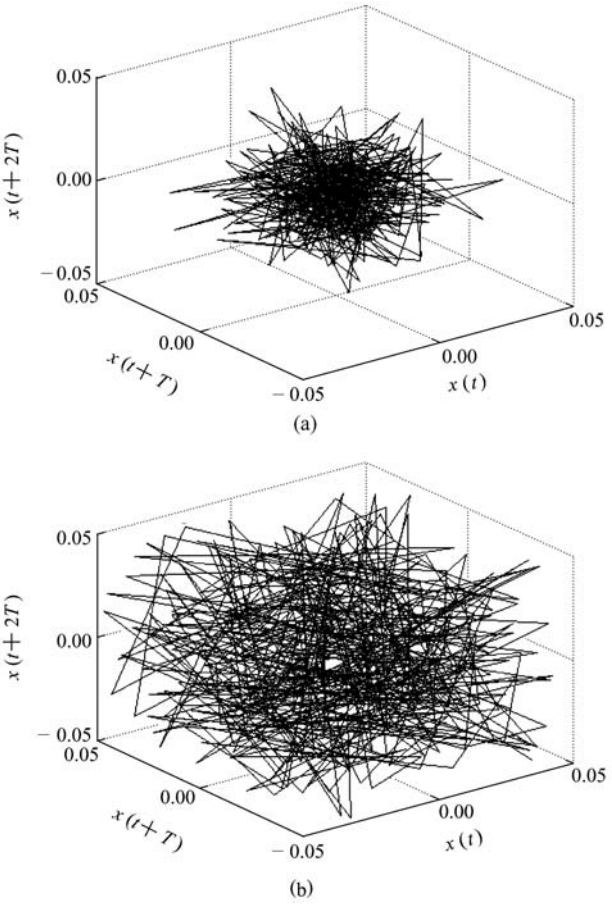

Fig. 2 Phase tracks. (a) Signal transmitted in the experimental system; (b) random noise signal

3.2 Lyapunov exponent analysis method

The Lyapunov exponent σ is a physical quantity used to measure the average divergent rate of adjacent tracks of a dynamical system. As the main parameter for determining whether the system is in chaos, σ shows the property of divergence or convergence by changes with time of little perturbations in the system. Therefore, the Lyapunov exponent can be applied to identify the chaotic state of the system.

A negative Lyapunov exponent means the average velocity of local convergence, while a positive Lyapunov exponent means the average velocity of divergence. The positive and negative Lyapunov exponents can coexist in the same dissipative system, and this dissipative system is a chaotic system.

For practical problems, since the system is bounded, only if the Lyapunov exponent is found to be greater

than zero could we judge the system as chaotic [11]. Therefore, the calculation of the largest Lyapunov exponent is significant.

First, we calculate the largest Lyapunov exponent of the experimental system signal from the equation that the largest Lyapunov exponent meets.

The largest Lyapunov exponent σ meets the following equation [8]:

$$d(t) = C\exp(\sigma t), \tag{2}$$

where $d(t)$ is the average diffusivity at t moment, C is normal constant.

For a certain point x_i reconstructed in phase space, assuming x_i' is the nearest point with x_i, $d_i(0) = \min_{x_i'} \|x_i - x_i'\|$ is the nearest distance between the adjacent two points. After time $k\tau$, from Eq. (2) we get

$$d_i(k) = \|x_{i+k} - x_{i+k}'\| = C_i\exp[\sigma(k\tau)]. \tag{3}$$

Calculating the logarithm to Eq. (3), we have

$$\ln d_i(k) = \ln C_i + \sigma(k\tau). \tag{4}$$

Equation (4) represents a group of subparallel straight lines with a slope of σ. Using the least squares fitting, we have

$$y(k) = \langle \ln d_i(k) \rangle / \tau, \tag{5}$$

where $\langle \ln d_i(k) \rangle$ represents the average of the entire variable i. The slope of the straight line is the largest Lyapunov exponent.

Selecting a data length of 256, according to the above method, we get the largest Lyapunov exponent of the signal transmitted in the experimental system as 0.0364.

To guarantee the accuracy of judgment and calculation, we also used Wolf's method [12] to calculate the same experimental signal.

Selecting initial point $Y(t_0)$ at the reconstruction space, we assume that the distance with its nearest adjacent point $Y_0(t_0)$ is L_0. We track the time evolution of the two points until t_1, at which intervals exceed a certain prescribed positive value of ε ($\varepsilon > 0$), $L' = |Y(t_1) - Y_0(t_1)| > \varepsilon$. We reserve $Y(t_1)$ and find another point $Y_1(t_1)$ near $Y(t_1)$, making $L_1 = |Y(t_1) - Y_1(t_1)| < \varepsilon$, with the cross angle as small as possible. We continue this process until $Y(t)$ arrives at the end of the time series. At this time, the total iterations of the tracked evolutionary process are M. Then, the largest Lyapunov exponent is

$$\sigma = \frac{1}{t_M - t_0} \sum_{i=0}^{M} \ln \frac{L_i'}{L_i}. \tag{6}$$

Using Wolf's method, we get the largest Lyapunov exponent of 0.0106.

The results of these two methods are both greater than zero. Therefore, it can be determined that the signal is a chaotic one, and the experimental system is a nonlinear dynamic system.

3.3 Self-power spectral density analytical method

To show the characteristics of the frequency domain of the chaotic signal, it can be resolved by calculating the Fourier transform of its autocorrelation function $R_{xx}(\tau)$. According to the self-power spectral density function $S_{xx}(f)$, we can analyze the chaotic frequency domain characteristics.

$$S_{xx}(f) = \int_{-\infty}^{\infty} R_{xx}(\tau) e^{-\mathrm{j}2\pi f\tau} d\tau,$$

$$R_{xx}(\tau) = \int_{-\infty}^{\infty} S_{xx}(f) e^{-\mathrm{j}2\pi f\tau} df.$$

For periodic motion, the power spectrum shows peaks only at fundamental frequency and multiple-frequency. The peaks of the power spectrum of quasi-periodic motion emerge at several irreducible fundamental frequencies and their overlapping frequencies. When period-doubling bifurcation occurs, a separate frequency and its multiple frequency will appear in the power spectrum, on which the power spectrum all have peaks. The characteristic of chaotic motion is the appearance of a noise background and a broad peak continuous spectrum in the power spectrum, which contains the peak corresponding to periodic movement. Based on these characteristics, it is easy to identify whether the motion characteristics is periodic, quasi-periodic, random or chaotic.

Taking 225 data points, we calculate the Fourier transform of its autocorrelation function to obtain the autopower spectrum of the experimental signal, as shown in Fig. 3. The spectrum has obviously chaotic characteristic.

Combining the three judgments, the signal transmitted in this experimental system is indeed chaotic signal, which indicates that this experimental system is an optical chaos communication system.

4 Security of the system

After confirming that the signal in the experimental system is chaotic, we can consider its performance of communication security as a chaotic system.

According to the studies of Rajarshi Roy et al, the dimension of chaotic light wave transmitted is very important to the security of chaotic communication. The higher the dimension, the stronger the security will be

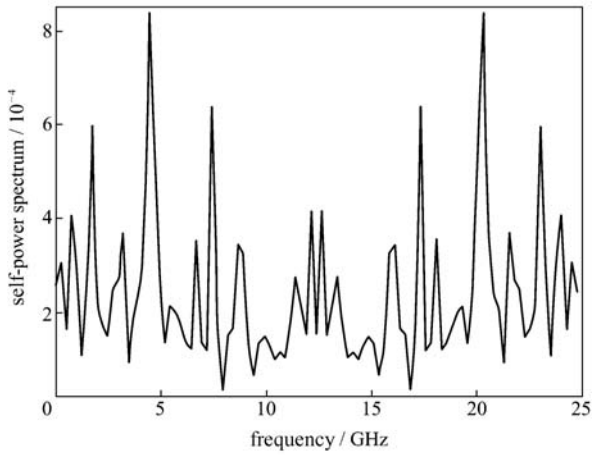

Fig. 3 Self-power spectrum of the signal of the experimental system

[13]. Therefore, we calculated the embedding dimension of the experimental system signal, and analyzed the anti-attack performance.

4.1 Calculation of the minimum embedding dimension

We calculate the minimum embedding dimension of the chaotic light signal in the system by false nearest neighbors (FNN) method.

Time series $X(n)$ is the projection of multi-dimensional state variables of a nonlinear dynamical system on the one-dimensional space. The purpose of dimension embedding is to unfold the projection to the multi-dimension space of the original system. Given a group of time series, how do we obtain the minimum embedding dimension d? In terms of mathematics, the minimum embedding dimension d and any other dimension $m > d$ can both unfold the attractors to a new higher dimensional space. However, for application, the minimum embedding dimension, which means the minimum calculating workload, at the same time, can reduce the impact of noise caused by truncation error and equipment measurement error. Choosing the minimum embedding dimension d is equivalent to calculating the invariants of attractors for these invariants represent the geometrical property of attractors.

The FNN method [10] is an effective method for calculating the minimum embedding dimension. Its fundamental principle is: when the dimension changes from m to $m+1$, one can judge whether a certain point on track $Y(n)$ is a true neighbor or not. If it is the true neighbor, then $m > d$ is indicated. If it is the false neighbor, then $m < d$ is indicated. The generation of false neighbor is the result of observing tracks in smaller embedding space ($m < d$). When we observed in a larger space ($m \geqslant d$), all the points on the tracks became true neighbors.

Selecting 499 data points, we get the embedding dimension 6, which is a higher dimension. This means stronger security for the system. As shown in Fig. 4, a horizontal axis indicates the minimum embedding dimension, while a longitudinal axis indicates the percentage of false neighbors.

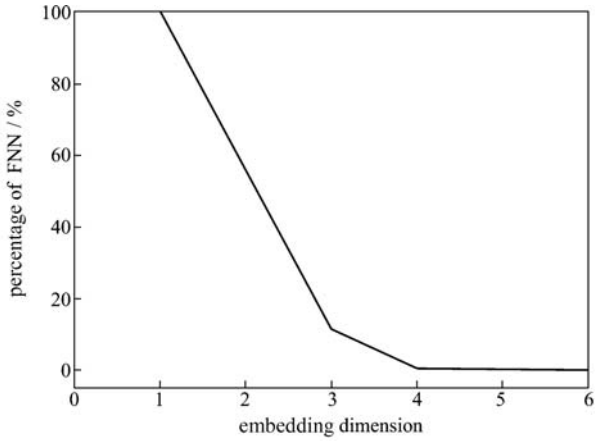

Fig. 4 Minimal embodied dimension of the signal of the experimental system by FNN method

4.2 Anti-attack faculty

The laser transmitted in a chaotic secure communication system in the polarization state is chaotic, but not in the intensity. When there is no signal input, the chaotic system at the two sides of the transceiver is in synchronization status, and the output of the subtractor is zero. When the input signal is code "0", which is equivalent to the state of no input signal, the transceiver chaotic system is still synchronous, and the subtractor output is also zero. When the input signal is code "1", the input signal and chaotic signal generate an XPM effect in the SOA. The polarization state of the chaotic signal of the transmitter side changes, because the signal phase is modulated. The chaotic signal in the polarization state signal at two sides of the transceiver is no longer synchronous, and the output of the subtractor is no longer zero. If the whole system has been in non-synchronous state, then there is no judging criterion. It is impossible to obtain the transmitted information from the chaotic signal. If the initial state parameters (fiber ring's cycle and polarization) are unknown, the synchronization for the system cannot be achieved, and it is impossible to access the transmitted information too.

On the other hand, there are many deciphering algorithms on the signal of chaotic secure communication. However, almost all of them are proposed on the chaotic masking scheme, such as regression mapping, phase space reconstruction, nonlinear forecasting method and so on. However, this system uses the chaotic polarization-keying modulation technique to realize secret communication,

which achieves the transmitted information from chaotic signal by judging whether the system is in synchronous or asynchronous state. Therefore, at the receiver side, whether the optical signal comes from branch A or B, neither can extract the message, because they are a group of chaotic signals with continuous and irregular change. Similarly, if a section of the optical chaotic signal alone is directly tapped, it is impossible to restore the original information using existing deciphering algorithms. Even when using the phase space reconstruction to construct the chaotic attractor and regenerate the chaotic signal, it is impossible to get the transmitted information. It does not matter whether one utilizes directly received chaotic signal subtracting chaotic signal of the regenerated (for chaotic masking mode) or dividing chaotic signal of the regenerated (for chaotic intensity modulation mode) signal, because the characteristics of the system lie in the use of digital modulation technology of chaotic polarization keying modulation. The judgment of "0" and "1" corresponds to the system state of synchronous or non-synchronous. Whether the system is in a synchronous or non-synchronous state, it is necessary to compare two branches of the received signals.

The characteristics of the polarization-shift keying chaotic optical communication system also lie in the correlation of the light polarization state. The digital code state is in a dynamic process that is a random continuous changing process, and no polarization state fixedly represents a certain state of digital code. Therefore, even if one extracted a partial optical signal from channels, and used a polarizer to analyze the optical polarization direction to determine the polarization state, what will be obtained is a random signal, not the original information. This is because "0" and "1" codes do not fixedly correspond to a certain polarization of light, but to the states of synchronous and non-synchronous.

Thus, whether it is a hardware attack or a software deciphering, the polarization-shift keying optical communication system has strong immunity.

5 Conclusions

The security of a chaotic light transmission experimental system is analyzed by combining polarization-shift keying modulation technology and chaotic optical system. First, the characteristic parameters of the experimental system signal are computed. The signal transmitted in the experimental system is synthetically judged that it is really chaotic signal by three criterions. Then, the minimum embedding dimension of the chaotic signal is calculated by using false nearest neighbors method, which confirms that the experimental system is a higher dimension chaotic system, and the security is strong. By analyzing the necessary parameters and methods for correctly receiving chaotic signal of the system and limitations of existing deciphering algorithm, the anti-attack faculty of the system is analyzed from hardware and software. Finally, we conclude that polarization-shift keying chaos optical communication system has higher security.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 60577042) and the Key Subject Foundation of Shanghai (No.T102).

References

1. Yan Senlin. High rate chaos secure communication system of multiple quantum well lasers. Acta Optica Sinca, 2005, 25(2): 179–185 (in Chinese)
2. Yan Senlin, He Longqing, Wu Haiyong, et al. Studies on method of phase shift controlling chaos for dual ring erbium doped fiber lasers. Chinese Journal of Lasers, 2005, 32(5): 642–646 (in Chinese)
3. Yan Senlin. All-optical chaotic MQW laser repeater for long-haul chaotic communications. Chinese Optics Letters, 2005, 3(5): 283–286
4. van Winggeren G D, Roy R. High-speed fiber-optic polarization analyzer: measurements of the polarization dynamics of an erbium-doped fiber ring laser. Optics Communications, 1999, 164(1–3): 107–120
5. Wang Lutang, Huang Zhaoming. Optical chaos communication with a dynamical SOA-based fiber ring laser. In: APOC 2003: Asia-Pacific Optical and Wireless Communications: Optical Transmission, Switching and Subsystems. Bellingham: SPIE. 2003, 5281: 619–627
6. Wang Lutang, Wu Weijia, Fang Nian, et al. Experimental study on chaotic optical communication with PolSK modulation technology. In: Tucker R S, Chiaroni D, Gu Wanyi, et al. APOC 2005: Asia-Pacific Optical and Wireless Communications: Optical Transmission, Switching and Subsystems. Bellingham: SPIE. 2005, 6021: 60210S
7. Yang Xiuli. A study on polarization-shift keying technology and optic chaos communication system. Dissertation of the Master's Degree. Shanghai: Shanghai University, 2005 (in Chinese)
8. Li Guohui, Zhou Shiping, Xu Deming. Computing the largest Lyapunov exponent from time series. Journal of Applied Sciences. 2003, 21(2): 127–131 (in Chinese)
9. Lin Jiayu, Wang Yueke, Huang Zhiping, et al. A new voice activity detection method based on chaos theory. Journal of China Institute of Communications. 2001, 22(2): 123–128 (in Chinese)
10. Li Yaan, Xu Demin. State space reconstruction of nonlinear dynamic system. Ship Engineering, 2000, 22(5): 47–50 (in Chinese)
11. Wen Quan, Zhang Yongchuan, Cheng Shijie. Identify determinacy from chaotic time series. International Journal Hydroelectric Energy, 2001, 19(3): 72–75 (in Chinese)
12. Lü Jinhu, Lu Jun'an, Chen Shihua. The Analysis of Chaotic Time Series and Its Application. Wuhan: Wuhan University Press, 2002, 76–80 (in Chinese)
13. van Winggeren G D, Roy R. Chaotic communication using time-delayed optical systems. International Journal of Bifurcation and Chaos, 1999, 9(11): 2129–2156