OPTICAL CHAOTIC SECURE ALGORITHM BASED ON SPACE LASER COMMUNICATION

RUIQIANG GUO
College of Electronic Information Engineering, Changchun University of Science and Technology, Changchun, China
College of Humanities & Information, Changchun University of Technology, Changchun, China

LU SONG*
College of Electronic Information Engineering, Changchun University of Science and Technology, Changchun, China

ABSTRACT. The traditional drive response synchronization control method has the poor robustness, which results in the low security performance of the optical chaotic secure communication. To address this problem, an optical chaotic secure algorithm based on space laser communication is proposed in this paper. With the advantage of space laser communication and full consideration of the influence of complex environment on signal transmission of laser wireless communication, a laser wireless communication channel model is built. Based on this, a hybrid self-synchronization chaotic system model is proposed. It can reduce the information needed for transmission, and only need to transmit a small amount of error correction signals on the channel to achieve synchronization of the receiving and the transmitting system, which greatly suppress the drawback of the traditional method. On the basis of chaotic synchronization, the erbium-doped fiber laser is used for information transmission. Different encryption techniques are used to achieve optical chaotic secure communication within the allowable range of error. Numerical simulation results show that the proposed algorithm has good security and robustness, and can realize the secure communication for different signals.

1. Introduction. With the more increased information, the disadvantages of wireless microwave communication in the volume and power consumption appear. As the constraint of the microwave communication bandwidth, it is difficult to achieve a high speed rate and the information capacity gradually exceeds the capacity of radio. In this case, the space optical communication technology with the carrier of laser emerges. Space laser communication refers to the realization of information communication between two or more terminals using laser instead of microwave as carrier. Compared with optical fiber communication, space satellite communication also has the characteristics of high speed and high bandwidth, but the cost is much lower. It can use laser to transmit all kinds of information between space and ground. It has broad prospects for development [1,4].

The traditional design idea of sequence cipher is the nonlinear transformation of linear sequence. Based on this guideline, the internal state transition of source

2010 Mathematics Subject Classification. 78A60.
Key words and phrases. Space laser communication, optical chaos, security.
* Corresponding author: Lu Song.
sequence generator is based on algebraic structure, and still has strong linear property. Therefore, there is a security hidden danger in the designed sequence cipher. However, chaos has the characteristics of periodicity, pseudorandom and complex dynamic behavior. Thus the designed chaotic secure system has a larger order than the internal state set of the traditional cipher, and its initial key space is infinitely large [12]. These excellent characteristics make the research on the theory and technology of chaotic secure communication with important scientific significance. Governments, universities, enterprises and research institutes in Europe, America and Japan have invested considerable manpower and financial resources to have a lot of deep research on chaotic secure communication. The research interests are in the theory and technology of secure communication based on chaotic synchronization, which includes the construction of chaos generator, the generation of high-speed wideband chaotic signal, the synchronization and robustness of chaos, information encryption technology, and chaotic modulation technology [5,17]. Recently, the key problems are as follows.

(1) Parameter mismatch. From the theoretical point of view, the more accurate the requirement of parameter adaptation is in the chaotic synchronization and the secure communication system, the higher the security of the system. But in the real environment, it is very difficult to build two or more chaotic systems with exactly the same parameters or exactly matched. Therefore, it is necessary to study the method consistent with the safety requirement, and the system can still maintain robust synchronization in the presence of parameter mismatch.

(2) Noise interference. There are some special effects, such as the nonlinear effect and dispersion of optical signal in transmission, as well as the effect of channel on the amplitude attenuation of optical signal, the linear and nonlinear distortion of phase. When the laser chaotic signal passes through such a channel, the distortion will occur, so the noise interference must exist in the actual transmission of the chaotic signal. Because chaotic signal are highly sensitive to the initial value and parameter, noise interference will directly affect the synchronization of chaotic systems, which may reduce the synchronization performance of the system. Therefore, how to reduce or eliminate the noise interference in the signal transmission of space laser communication is a problem to be solved.

(3) Safety. The synchronous control signal contains the track information of the power system, which may lead to the information leakage of the chaotic system. By using this information, the chaotic time series analysis is used to reconstruct the phase space of the system, and the macro characteristics are estimated. Based on fuzzy theory, neural network and wavelet analysis, it can effectively attack the security system by nonlinear prediction of the system, which leads to potential safety hazard.

For the above problems of the traditional algorithm, an optical chaotic secure algorithm based on space laser communication is proposed in this paper.

2. Research on optical chaotic secure algorithm based on space laser communication. The advantages of space laser communication are as follows.

(1) The transmitting light beam is narrow and with good direction, so the laser optical communication can solve the problems of the serious electromagnetic wave interference.
(2) Low cost, small size, small power consumption, light weight, convenient and flexible network, and low maintenance price.

(3) No spectrum license is required. Because of its high bandwidth, space laser has no drawbacks in the same frequency interference and spectrum application.

(4) Protocol transparency. The space laser communication takes the laser as the carrier, so any transmission protocol can be easily applied to the light carrier.

(5) Large information capacity. By using light wave as an information carrier, it can achieve up to 1 OGb/s data transmission rate, which can be used for wideband access to solve the bottleneck problem of the last mile.

(6) Low transmission power and high reception power.

2.1. Channel model of laser wireless communication. The signal transmission of the laser wireless communication is affected by the complex space environment, which includes the influences of the atmosphere, the background noise, the Doppler effect in the transmission, and the human interference. In this paper, the discussion is focused on the influence of the atmospheric channel [2,6].

The influence of atmosphere on the laser radio communication mainly includes the absorption effect of the atmosphere, the scattering effect of the atmosphere, and the turbulence effect of the atmosphere. The absorption effect of the atmosphere is due to the absorption of energy by carbon dioxide, water, and ozone in transmission. Research results show that, by choosing suitable laser wavelength, it can restrain the absorption of atmospheric light signal and reduce the attenuation of optical signal. Therefore, when choosing suitable laser, the influence of atmospheric absorption on laser signal attenuation can be ignored. Previous researches have shown that the attenuation of laser signals is the lowest at 0.8um, 1.0um and 1.5um [3,14].

Atmospheric scattering refers to the receiver receives the intensity of light in each direction in the transmission of the light wave due to the influence of the medium. Atmospheric scattering results in the reduction of light power and uneven intensity distribution. In addition to the concentration of particles in the atmosphere, atmospheric scattering is related to the wavelength of the light.

Atmospheric turbulence is the change of temperature, pressure, velocity, and density due to the flow of the atmosphere. In the transmission in the atmosphere, laser is affected by atmospheric turbulence, which will produce light intensity scintillation, beam drift, spot spreading, phase fluctuation, and the fluctuation of angle of arrival. In this paper, the light intensity chaos generation method is used. As the light intensity scintillation affects the bit error rate of the system, the light intensity scintillation caused by atmospheric turbulence is discussed.

Light intensity scintillation refers to when the laser is transmitted in the atmosphere, the light intensity of the laser is too big or small, which is caused by the influence of the refractive index of the atmosphere. Assume \( A(r) \) is the amplitude of laser light wave in presence of turbulence, \( A_0(r) \) is the amplitude of laser light wave in absence of turbulence. Define \( a = \ln(A(r)/A_0(r)) \) is the log-amplitude fluctuation, and the computation of the logarithmic light intensity fluctuation is given by

\[
\ln \frac{I(r)}{I_0(r)} = \ln \left| \frac{A(r)}{A_0(r)} \right|^2 = 2a
\]

Assume the noise caused by the atmospheric turbulence on the amplitude of laser light wave is denoted as \( A_z(r) \) and ignore amplitude change caused by other noises. Then
\[
\ln \left( \frac{I(r)}{I_0(r)} \right) = \ln \left| \frac{A_0(r)}{A_n(r)} \right|^2 = 2 \ln(1 + \gamma) \tag{2}
\]

where \( \gamma = \frac{A_z(r)}{A_0(r)} \) is the ratio of the amplitude of the noise to the signal. When the noise is very small, it can be considered as \( a = \ln(1 + \gamma) \approx \gamma \).

The signal to noise ratio caused by atmospheric turbulence is given by

\[
SNR = \frac{I_0(r)}{\langle I_z(r) \rangle} = \frac{\langle A_0^2(r) \rangle}{\langle A_z^2(r) \rangle} = \frac{1}{\langle \gamma^2 \rangle} = \frac{1}{\langle a^2 \rangle} \tag{3}
\]

where \( \langle I_z(r) \rangle \) denotes the noise intensity.

Define scintillation index as the degree of the intensity scintillation, which is given by

\[
\sigma_i^2 = \frac{\langle (I - \langle I \rangle)^2 \rangle}{\langle I \rangle^2} \tag{4}
\]

where \( I \) is the instantaneous light intensity in the receiver, \( \langle I \rangle \) is the average light intensity.

The logarithmic intensity fluctuation variance is defined by

\[
\sigma_{\ln I}^2 = \langle \ln I - \langle \ln I \rangle^2 \rangle \tag{5}
\]

In the case of weak atmospheric turbulence, \( \sigma_{\ln I}^2 = 4a^2 \) and in the case of strong turbulence, \( SNR \) is approximated as

\[
SNR = \frac{1}{\langle a^2 + a^3 + \cdots \rangle} \approx \frac{1}{\alpha \langle a^2 \rangle} \tag{6}
\]

where \( \alpha \) is the scintillation intensity factor and the range of its value is between 1\~2.

As the random variation of the refractive index, a statistical method should be used, which is given by

\[
\sigma_{\ln I}^2 = C_n^2 k^{7/6} L^{11/6} \tag{7}
\]

where \( C_n^2 \) denotes the refraction structural constants of atmospheric turbulence for the strength of the turbulence, \( k = 2\pi/\lambda \) denotes the wavenumber, \( L \) denotes space laser transmission distance.

According to the division of the Davis refractive index, \( C_n^2 > 1.5 \times 10^{-13} \) is the strong turbulent zone, \( C_n^2 < 6.5 \times 10^{-13} \) is the weak turbulent zone, and \( 6.5 \times 10^{-13} < C_n^2 < 1.5 \times 10^{-13} \) is the medium turbulent zone.

The kolomogorov refractive index fluctuation power spectrum is used under weak fluctuation. The variance of logarithmic fluctuation is given by

\[
\sigma_{\ln I}^2 = 1.23 C_n^2 k^{7/6} L^{11/6} \tag{8}
\]

which is also called as Rytov variance.

In the practical laser communication, the transmitted laser is considered as plane wave. Under the condition of strong turbulent, the logarithmic fluctuation intensity of the plane wave is expressed as

\[
\sigma_{\ln I}^2 = 1 + \frac{0.86}{(\sigma_l^2)^2} \tag{9}
\]

where \( \sigma_l^2 \) is Rytov variance.
2.2. Chaotic synchronization control scheme based on space laser communication. Recently, the space laser secure communication is based on cryptography. However, the cryptography-based communication is limited by the security rules of confusion and diffusion and the bandwidth of the electronic device, which results in poor anti-interference ability and low speed of encryption and decryption. For the secure communication based on laser chaotic synchronization, because of the robustness of chaotic synchronization technology and the high frequency and low attenuation characteristics of the optical device, the anti-interference ability and transmission speed of laser chaotic secure communication system have been significantly improved [15].

As the limitation of chaotic security and synchronization, chaotic concealment and chaotic modulation have different degrees of constraints on the amplitude and frequency of signals, and because the continuous chaotic signal is transmitted on the channel, the security of the chaotic system is hidden. In this paper, the signal transmission of laser wireless communication affected by complex space environment is considered. Based on the above established laser wireless communication channel model, a synchronization control scheme based on optical chaos is proposed, which divides the synchronization process into two stages. In the first stage, the synchronization error gradually decreases from the initial value to the predetermined range. In the second stage, the synchronization error is kept in the set range, that is, to synchronize. In the second stage, it is not necessary to send the full state variable information of the drive system to the response system, but only part of the state information to ensure synchronization. This part of the information is similar to noise, so it cannot reconstruct the orbit of the chaotic system, thus the security of the system is improved. When the synchronization method is implemented with a high accuracy, a hybrid self-synchronization chaotic system model is further proposed, which can reduce the information needed for transmission, and only need a small amount of error correction signals in the channel to achieve synchronization between the two systems [13,16].

Based on pulse control theory, the driving response synchronization model of the power system is considered. The driving system can be expressed as

\[
\frac{dx}{dt} = (A + \Delta A_1(t))x + f(x(t))
\]  

(10)

where \(x(t) \in R^n\) is state vector, \(A, \Delta A_1(t) \in R^{n \times n}\), \(f: R^n \to R^{n \times n}\) is continuous nonlinear function. Then the response system is expressed as

\[
\begin{align*}
\frac{dx}{dt} &= (A + \Delta A_2(t))y + f(y(t)) \\
\Delta y &= y(t^+_i) - y(t^-_i) = y(t^+_1) - y(t_1) = \\
B_i(y(t) - x(t)), t = t_i, i = 1, 2, \ldots, p \\
\Delta y &= y(t^+_i) - y(t^-_i) = y(t^+_1) - y(t_1) = \\
B_i(y(t) - C(t), E(t)) - S(t), t = t_i, i = p + 1, p + 2, \ldots,
\end{align*}
\]

(11)

where \(y(t) \in R^n\) is state vector, \(y(t)\) is left continuous at \(t = t_i\), \(B_i\) is \(n \times n\) matrix, \(\Delta A_1(t)\) and \(\Delta A_2(t)\) is the parameter mismatch of the chaotic system, \(S(t) = x(t) - Q(x(t))\) is the synchronous signal of space laser communication transmitted to the response system by the drive system, \(Q(\cdot)\) is quantized function, which converts a real number to a finite precision binary number according to the preset accuracy,
$C(\cdot)$ is error correction function, $E(t)$ is space laser communication error correction signal sent to the response system by the drive system, pulse time sequence \{\(t_i\)\} satisfies $0 < t_1 < t_2 < \cdots < t_i < \cdots$, when $i \in \infty$, $t_i \in \infty$.

Assume the nonlinear part of the chaotic system $f$ satisfies Lipschitz condition, which is given by

$$\|f(y(t)) - f(x(t))\| \leq \mu \|y(t) - x(t)\|$$  \hspace{1cm} (12)

then

$$f(y(t)) - f(x(t)) = K(x(t), y(t))(y(t) - x(t))$$  \hspace{1cm} (13)

where $K \in \mathbb{R}^{n \times n}$ is bounded matrix $\|K\| \leq \mu$, and the elements are decided by $x(t)$ and $y(t)$.

Define the synchronization error of the chaotic system is $e(t) = y(t)x(t)$, then the error system is given by

$$\begin{cases}
\frac{dx}{dt} = (A + \Delta A_2(t) + K(x, y))e + (\Delta A_2(t) - \Delta A_1(t))x, t \neq t_i \\
\Delta e = B_1e, t = t_i, i = 1, 2, \ldots, p \\
\Delta e = B_1(e - C(y(t), E(t)) - Q(x(t))))), i = p + 1, p + 2, \ldots
\end{cases}$$  \hspace{1cm} (14)

The purpose of Eq. (14) is to obtain the condition required for the control gain $B_i$, the pulse interval $\tau_i = t_i - t_{i-1} < \infty (i = 1, 2, \ldots)$, which leads to the response system given by Eq. (10) and the driving system given by Eq. (9) synchronize in the actual acceptable range of error. For $t > t_s$, $|y(t) - x(t)| = |e(t)| \leq \varsigma$, where $\varsigma$ denotes a small enough positive value and $t_s$ is bounded.

From Eq. (12) an Eq. (13), it can be seen that the process of chaotic synchronization can be divided into two stages. In the first stage ($t \leq t_p$), as the traditional pulse synchronization method, the complete state variable sampling values $x(t_i)$ of each dimension of the drive system are sent to the response system. When the two chaotic system have reached the synchronization, that is, once $|e(t)| \leq \varsigma$, the second stage is entered ($t > t_p$). In this stage, if $|e(t)| \leq \varsigma$ can be guaranteed to any $t$, the synchronization state of the chaotic systems is maintained. According to Eq. (13), the space laser communication error correction signal $E(t)$ and the synchronization signal $S(t)$ are transmitted to the response system, not the complete chaotic system state variable.

From the above analysis, the redundant state information of the chaotic system is eliminated by the analog-to-digital conversion method. Intuitively, if the accuracy of analog-to-digital conversion can be controlled and the quantization interval of the quantizer $Q(\cdot)$ is larger than the synchronization error threshold $\varsigma$, $Q(x(t)) = Q(y(t))$ can be obtained, that is, this redundant information can be eliminated to obtain $S(t) = x(t) - Q(x(t))$ and transmitted to the responder to keep a synchronization. But in fact, such a situation is not valid. Even if the above condition is satisfied, the obtained digital signals will still be different, and the errors will gradually accumulate, which will eventually lead to the out-of-step of the chaotic system [8, 11].

Based on the above chaotic synchronization theory, when the chaotic synchronization scheme is implemented with a high-precision circuit, the synchronization error threshold $\varsigma$ is very small, and the quantization interval of the quantizer $Q(\cdot)$ is also smaller. Then the synchronization signal in Eq. (14) decreases greatly.
If there is no need to transmit $S(t)$, then in the space laser communication channel, it is necessary to transmit a very small amount of error correction signal in digital form to achieve the synchronization of the chaotic system [9]. The design scheme is shown in Fig. 1.

The system consists of two parts of the transmitter and the receiver. The transmitter includes the chaotic system module, the sampling module, the A/D conversion module, and the D/A conversion module. The receiver includes the chaotic system module, the sampling module, the A/D conversion module, the D/A conversion module, and the error correction module [7, 18]. The working steps of the system are as follows.

1. A chaotic signal generated by the transmitter using an optional initial value. The mathematical model of the chaotic system for generating the chaotic signal is given by

$$\frac{d}{dt} X(t) = F(X(t), A + \Delta A_1(t))$$  \hspace{1cm} (15)

where $X(t)$ is the $n$-dimensional state variable of the chaotic system, $A$ is parameter matrix, which is $n$ order constant matrix, $n$ is integer.

A chaotic signal generated by the receiver using an optional initial value. The mathematical model of the chaotic system for generating the chaotic signal is given by

$$\frac{d}{dt} Y(t) = F(Y(t), A + \Delta A_2(t))$$  \hspace{1cm} (16)

where $Y(t)$ is a randomly generated chaotic signal.

2. Close the switch $k_1$. The transmitter performs pulse synchronization on the chaotic system of the receiver at a time interval of $\Delta T_1(\delta), 0 < \Delta T_1(\delta) < \Delta T_{\text{max}}, \delta = 1, 2, 3, \ldots$, until the chaotic system of the communication is synchronized. The mathematical model of the pulse synchronization can be described as the impulsive differential equations, which are given by

$$\begin{cases} 
\frac{d}{dt} Y(t) = F(Y(t), A + \Delta A_2(t)) \\
Y(t) |_{t = t_\delta} = -B(X(t_\delta) - Y(t_\delta)) 
\end{cases}$$  \hspace{1cm} (17)

where $B$ is diagonal matrix of synchronous coupling coefficient, $t = t_\delta$ is the time to synchronize the chaotic system with the synchronization vector, $t_\delta = \delta * \Delta T(\delta), X(t_\delta)$ and $Y(t_\delta)$ are the state values of the chaotic system of the transmitter and the receiver at $t = t_\delta$. $\Delta T(\delta)$ is the time interval between
the δth and δ + 1th synchronization. $\Delta T_{\text{max}}$ is the maximum time interval allowed by pulse synchronization.

(3) When the transmitter and the receiver are in synchronization, turn on the switch $k_1$ and turn off the switch $k_2, k_3,$ and $k_4$. The sampling interval of the transmitter is $\Delta T_2(\delta), 0 < \Delta T_2(\delta) < \Delta T_{\text{max}}$. Digital state vector $D_1$ and error correction signal $\beta$ are obtained after digital processing of the current state vector of the chaotic signal.

The traditional pulse synchronization method needs to transmit complete state variables. Even after analog-to-digital conversion, each synchronization pulse also needs to transmit at least 10bit or more information. Otherwise, the accuracy is too low, and the significance of synchronization is lost. The hybrid self-synchronization method, regardless of the accuracy of the synchronization, only needs to transmit the error correction signal of the 1bit to keep the synchronization. The efficiency is several times higher than the traditional pulse synchronization method. Finally, in terms of robustness, the traditional pulse synchronization method generally needs to transmit analog pulse signal in the channel, and is interfered by noise. The hybrid self-synchronization method only needs to transmit a small number of error correction signals in digital form, which is obviously more robust.

2.3. Optical chaos secure algorithm based on erbium-doped fiber laser.

Transmission of the secure communication by using chaotic system is approximately the same as other secure communication methods, which is to encrypt the transmitted information in the transmitter, after passing through public channel, obtain the transmitted information in the receiver by decryption with specific key. The difference is that the key is different. In chaos secure algorithm, the two systems with almost the same parameters are considered as the transmitter and the receiver. The noise chaotic synchronization signal transmitted by two system is taken as key. Because of the extreme sensitivity of the parameters of the chaotic synchronization system, this encryption method makes the performance of security greatly strengthened even if information is intercepted in the channel [10].

(1) Information concealment method

Assume dynamic characteristictic system of space laser communication transmision system is denoted as $F(\vec{x}, \vec{u})$, where $\vec{x}$ is the system variable, and $\vec{u}$ is system parameter. With appropriate selection of system parameters, the space laser communication launch system runs in the chaotic state, and the transmitted information $S_i(t)$ is modulated with the output signal $y(t)$ of the chaotic system to generate the encrypted information. The modulation method can be directly addition and nonlinear transformation. After this process, the plaintext information is hidden in the chaotic signal stream, which is called the information concealment method. The expression is given by

$$M(t) = S_i(t) \otimes y(t)$$  \hspace{1cm} (18)$$

Decryption refers to the process of extracting spatial laser communication information from encrypted information, which is the inverse operation of encryption. According to the different encryption methods, decryption is also different, but all of them are decrypted according to synchronous signal.

Assume the parameters of the receiving system $F'(\vec{x}', \vec{u}')$ and transmitting system $F(\vec{x}, \vec{u})$ of the space laser communication are the same. Two systems achieve chaotic synchronization under certain condition. The synchronization signal is $y(t)$. The plaintext of the space laser communication can be extracted from the encrypted
information flow $M(t)$ by using the chaotic synchronization signal, which is expressed as

$$M(t) = S_0(t) \otimes y(t)$$

(19)

Generally, $S_0(t)$ and $S_i(t)$ are impossible to be completely equal, but in a certain range of accuracy the two are approximately equal, that is, $S_0(t) \approx S_i(t)$. In this way, the decrypted space laser communication plaintext information is obtained in the receiver. Although the decrypted information is not exactly equal to the original information, it does not affect the information recognition within a certain accuracy range.

(2) Chaos shift keying method

As the plaintext information of the space laser communication is digital signal, shift keying method is a more effective method for the optical chaos encryption. It makes use of the same or not the parameters of the transmitting system and the receiving system of the space laser communication system to synchronize chaos synchronization between the two systems. When all the parameters of the two systems are exactly the same, full synchronization can be achieved under the specific synchronization method. Otherwise, if there is one different parameter, it is impossible to achieve synchronization. Considering the characteristics of the chaos system, digital signal is used to control the parameters of the transmitting system, and the transmitted digital signal is determined by synchronizing the two systems. Assume the parameter of the receiving system is $\vec{u}' = \vec{u}_1'$. If a binary digital signal is used as a modulated signal, two chaotic systems will not reach the synchronous state when the transmission signal is 0 to make $\vec{u} = \vec{u}_2$. Because of the large difference between the level values of digital signals, the error tolerance of digital signal demodulation is very wide. Therefore, the transmission quality of digital signal is much better than analog signal. When the parameters are the same, the two systems cannot reach the chaotic synchronization at once, but has a transient process. Therefore, the speed of transmission of the digital signal will decrease slightly, but with the increase of the speed of the fiber laser, the transient will become shorter and shorter. The transmitted digital signal can be demodulated by the difference between the characteristics of the two system signals.

(3) Chaotic modulation method

The basic idea of chaotic modulation is to encrypt an information signal and infuse it into the transmitter, thus changing the dynamic characteristics of the original chaotic system, so the information signal is modulated. The information signal is recovered with the corresponding demodulation and decryption methods at the receiving end. The advantages of this method are as follows. First, it uses the whole range of the chaotic signal spectrum to hide information. Secondly, it increases sensitivity to parameter changes and enhances secrecy.

The structure of analog signal communication system based on erbium-doped fiber single-ring laser is shown as Fig. 2. From Fig. 2, it can be seen that the structure of the transmitting system and the receiving system are very similar, all of which are composed of two wavelength division multiplexers, a segment of erbium-doped fiber and delay line. The transmitted information signal $S_i$ of the transmitting system passes through the couplers $C_5$ and $C_2$ to obtained the synchronous output signal $E_m(\tau)$ from $C_1$. The transmitted information signal $S_i$ enters the ring of the transmitting system by passing through $C_5$ and $C_2$. The receiving signal $E_m(\tau) + S_i$ is demodulated with the output signal of the coupler $C_9$. 
Figure 2. Optical chaotic secure communication structure based on erbium-doped fiber single-ring laser

The obtained recovered signal enters the receiving ring by passing through WDM coupler $C_{11}$. When the parameters are suitable, the recovered signal is equivalent to the transmitted signal, denoted as $S_0$. The kinetic equations of the whole transmitting and receiving system are given by

\begin{align}
\dot{E}_m(\tau) &= -\kappa_m [E_m(\tau) - a_0 S_i] + g_m E_m(\tau) D_m(\tau) - \varepsilon E_m(\tau - \tau_0) \quad (20) \\
\dot{D}_m(\tau) &= -\left[I_{pa} + 1 + |E_m(\tau)|^2 \right] D_m(\tau) + I_{pa} - 1 \quad (21)
\end{align}

where $I_{pa}$ is pumping light intensity, $m$ is modulation coefficient, $E$ is output laser field strength, $D$ is inversion population, $\kappa$ and $g$ are loss coefficient and gain coefficient, $\varepsilon$, $\tau_0$, and $\tau$ is delay rate, delay time and normalization time of delayed feedback optical path, respectively.

The kinetic equations of the receiving system are given by

\begin{align}
\dot{E}_s(\tau) &= -\kappa_s [E_s(\tau) - b_0 (S_i + E_s(\tau))] + g_s E_s(\tau) D_s(\tau) - \varepsilon E_s(\tau - \tau_0) \quad (22) \\
\dot{D}_s(\tau) &= -\left[I_{pa} + 1 + |E_s(\tau)|^2 \right] D_s(\tau) + I_{pa} - 1 \quad (23)
\end{align}

where $a_0$ and $b_0$ are the coupling coefficients of the transmitted signal $S_i$ and the synchronous signal. The parameters are normalized. From Fig. 2, it can be seen that, in the transmitter, the transmitted information signal $S_i$ is input into the transmitting system, in order to achieve stable transmission, the information signal into the receiving system is also needed, so the structure of chaotic secure communication do not need to make the amplitude of the space laser communication signal very small to achieve stable transmission of information.

According to the dynamic characteristics of the erbium-doped fiber double-ring laser, the double-ring system is more complex than the single-ring system with delayed feedback laser injection. Hyperchaos can occur in a large range, and its chaotic characteristics are complex and the attractor is more irregular. Therefore, the erbium-doped fiber single-ring laser system is used to realize the chaotic secure communication, and its security performance is better. For optical chaotic secure communication based on erbium-doped fiber double-ring laser, on the basis of the chaotic synchronization, the transmitted information signal is added, and the different encryption techniques can be used to realize the optical chaotic secure communication in the allowable range of error. Chaotic secure communication structure based on erbium-doped fiber double-ring laser is shown as Fig. 3. The transmitting system consists of erbium-doped fiber single-ring laser and erbium-doped fiber double-ring laser and the receiving system is only an erbium-doped fiber double-ring laser. In a certain range of parameters, two erbium-doped fiber double-ring lasers can be synchronized with a common single-ring system. If the combination
Figure 3. Optical chaotic secure communication structure based on erbium-doped fiber double-ring laser

of transmitter single-ring system and double-ring system is considered as a whole, it is called optical chaos communication based on P-C synchronization method. In the transmitting system, the transmitted signal $S_i$ and the output optical field $E_{ma}$ of the erbium-doped fiber double-ring laser is taken as the modulated signal to the receiving system by passing though the coupler $C_0$. In the receiving system, the interaction of the mixed signal and the synchronous output signal $E_{sa}$ is finally demodulated to recover the information signal $S_0$.

In this scheme, there are two transmission channels between the transmitting system and the receiving system, which is the disadvantage, but the two channels have their respective duties. The drive signal $E_m$ is to ensure the synchronization of the two erbium-doped fiber double-ring lasers and the mixed signal contains information to be transmitted. The amplitude of the information signal $S_i$ is a small amount relative to the output light field $E_{ma}$ of the laser. In this way, it can be submerged in the chaotic signal and play the role of security. The signals which drive two double-ring systems are the light field $E_m$. It is guaranteed that 3 different encryption techniques can be used to synchronize the two lasers well, so that the information signals are extracted completely at the receiving end [19]. The kinetic equations of two systems are the same as Eq. (22) and Eq. (23).

3. Numerical simulation of optical chaotic secure algorithm based on space laser communication. Numerical simulations are carried out to verify the validity of the proposed secure communication. Assume the signal of space laser communication $S_i = \sin t$ is simple sinusoidal signal. $S_i$ is substituted into the proposed optical chaotic secure system. The amplitude control factor is selected as 0.1, and the corresponding parameters are set to $a_0 = 16$ and $b_0 = 45.92$. The maximum Lyapunov index of the encryption system is 1.127, which represents the system is in a chaotic state. The synchronous drive signal generated by the encrypted operation of the space laser communication information signal is shown in Fig. 4. The space laser communication signal $\theta(t)$ obtained by adding the drive signal $E_m$ is shown in Fig. 5(a) and the time history is shown in Fig. 5(b). After receiving $\theta(t)$, the drive signal $E_m$ is extracted and added into the decryption system to achieve the synchronization of the encryption system and the decryption system. Then the space laser communication signal is recovered, as shown in Fig. 5(c). The error is shown in Fig. 5(d). When the space laser communication signal is a square wave signal, without changing other parameters, the test results obtained with the proposed method are shown in Fig. 6.
From Fig. 4 ∼ Fig. 6, it can be seen that, whether sinusoidal or square wave, the proposed algorithm can be encrypted and transmitted by the secure communication scheme and recover without distortion, which proves the effectiveness of the proposed algorithm. The information signal for the scheme is not strictly required, due to the extreme sensitivity of chaotic synchronization system parameters, any form of time series can be used for the secure communication scheme, which makes the scheme has a wide application range.

4. Conclusions. In this paper, the chaotic synchronization especially the application of pulse synchronization theory in optical secure communication system is researched, and some key problems in theory are solved, but the research and design of optical secure communication system is still in the primary stage, there are many important and meaningful problems need to be studied.
(1) The application of multimode laser chaotic system in secure communication. In this paper, the research is focused on the single-mode laser system. Research on multimode laser system is of great value to the design of multiplexed communication system. The multi-channel information transmission can be completed by loading the plaintext information on the intensity signal carrier of each mode of the multimode laser system. However, the multimode laser system has a serious signal delay effect, which results in the failure of the existing scheme, so further research is needed.

(2) Further research on the scheme of laser chaotic secure communication. In this paper, a novel chaotic shift keying secure communication scheme is proposed for transmission of digital signal. But for analog signal, chaos shift keying is not applicable. How to modulate analog signal to chaotic carrier for transmission and decryption safely, stably and efficiently, is of great significance for the application of chaotic secure communication technology.

(3) Systematic design method and evaluation criterion for laser chaotic signal with high dimension and high complexity. The high frequency and high bandwidth characteristics of the laser chaotic signal make it widely used in the design and research of the secure communication system. The security of chaotic secure communication system is based on the complexity of chaotic signal. Although a variety of laser chaotic signals and even hyperchaotic signal generation methods have been proposed, but there is not a complete set of design theory and evaluation methods to ensure the complexity and cryptography security.

(4) Research on laser chaotic synchronization and secure communication system theory for the restriction of real environment. Recently, most of the research results are obtained at the theoretical level, or under the ideal conditions of the environment. In real environment, many restrictions seriously hinders
the laser chaotic secure communication system to the practical application, such as the difference between the parameters of chaotic system, the effect of the polarization of the electric field on the signal, the loss caused by a variety of optical signal converter (such as optical isolator), the optical signal influenced by the noise, fading, a variety of nonlinear effects (dispersion, phase disturbance etc.). How to research and improve the theory of laser chaotic secure communication under these restrictions, and make it able to apply to the actual environment to the greatest extent, is the focus of future research.

REFERENCES

[1] V. Annovazzi-Lodi and G. Aromataris, Privacy in two-laser and three-laser chaos communications, IEEE Journal of Quantum Electronics, 51 (2015), 1–5.

[2] H. W. Chen, G. C. Yang, C. Y. Chang, T. C. Lin and W. C. Kwong, Enhancing optical-CDMA confidentiality with multicode-keying encryption, Journal of Lightwave Technology, 27 (2015), 1708–1718.

[3] M. Cheng, X. Gao, L. Deng, L. Liu, Y. Deng, S. Fu, M. Zhang and D. Liu, Time-delay concealment in a three-dimensional electro-optic chaos system, IEEE Photonics Technology Letters, 27 (2015), 1030–1033.

[4] A. Elsonbaty, S. F. Hegazy and S. S. A. Obayya, Simultaneous suppression of time-delay signature in intensity and phase of dual-channel chaos communication, IEEE Journal of Quantum Electronics, 51 (2015), 1–9.

[5] L. I. Feng and Y. F. Zhang, Network communication encryption method based on the structure of semigroup simulation, Computer Simulation, 280–283.

[6] W. Gao and M. R. Farahani, The hyper-zagreb index for an infinite family of nanostar dendrimer, Journal of Discrete Mathematical Sciences & Cryptography, 20 (2016), 515–523.

[7] S. K. Y., C. F., W. T. T. and et al, Full state based adaptive control of fractional order chaotic system without equilibrium point, Journal of Jilin University (Engineering and Technology Edition), 138 (2017), 1225–1230.

[8] T. Lan, Y. Lan, P. Chen and W. Lo, A study of investigating adolescents’ eating out behavior by using analytic hierarchy process, Eurasia Journal of Mathematics Science and Technology Education, 13 (2016), 3227–3234.

[9] A. J. Lawrance, T. Papamarkou and A. Uchida, Synchronized laser chaos communication: Statistical investigation of an experimental system, IEEE Journal of Quantum Electronics, 1–1.

[10] N. Li, H. Susanto, B. Cemlyn, I. D. Henning and M. J. Adams, Secure communication systems based on chaos in optically pumped spin-vcsels, Optics Letters, 42 (2017), 3494–3497.

[11] L. Liu, Y. N. Wang, L. Hou and X. R. Feng, Easy encoding and low bit-error-rate chaos communication system based on reverse-time chaotic oscillator, Iet Signal Processing, 11 (2017), 869–876.

[12] D. S. Mao, Comnotation of quantum cascaded lasers technology and its application prospect, Journal of China Academy of Electronics & Information Technology, 333–340.

[13] S. Nazari-Shirouhi, S. Miri-Nargesi and A. Ansarinejad, A fuzzy decision making methodology based on fuzzy ahp and fuzzy topsis with a case study for information systems outsourcing decisions, Journal of Intelligent & Fuzzy Systems, 32 (2017), 3921–3943.

[14] L. Q. J., Information hiding algorithm based on frequency band division key frames coding, Bulletin of Science and Technology, 120–122.

[15] D. Rontani, E. Mercier, D. Wolflersberger and M. Sciamanna, Enhanced complexity of optical chaos in a laser diode with phase-conjugate feedback, Optics Letters, 41 (2016), 4637–4640.

[16] L. I. Shilei, C. Liu, H. U. Xiaoyu and N. I. Junkang, A chaotic oscillator with high security for secret communication, Journal of Xian Jiaotong University, 51 (2017), 35–40.

[17] L. Wang, Z. M. Wu, J. G. Wu and G. Q. Xia, Long-haul dual-channel bidirectional chaos communication based on polarization-resolved chaos synchronization between twin 1550 nm vcsels subject to variable-polarization optical injection, Optics Communications, 334 (2015), 214–221.

[18] T. T. Wang and C. H. Ma, A re-examination of expectation hypothesis with time varying term premium, Journal of Interdisciplinary Mathematics, 20 (2017), 1–12.
[19] C. Xue, N. Jiang, Y. Lv, C. Wang, G. Li, S. Lin and K. Qiu, Security-enhanced chaos communication with time-delay signature suppression and phase encryption, *Optics Letters*, 41 (2016), 3690.

Received June 2017; revised November 2017.

E-mail address: grq8888@163.com
E-mail address: usong@126.com