Optics and Laser Technology 107 (2018) 122–130

Contents lists available at ScienceDirect

Optics and Laser Technology

journal homepage: www.elsevier.com/locate/optlastec

Full length article

A novel double masking scheme for enhancing security of optical chaotic communication based on two groups of mutually asynchronous VCSELs

Bo-Cheng Liu [a], Yi-Yuan Xie [a,b,c,*], Yu-Zhu Liu [a], Yun Wang [a], Ying-Xue Du [a], Wen-Jing Zheng [a], Yong Liu [c]

[a] School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China
[b] Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Chongqing 400715, China
[c] School of Optoelectronic Information, University of Electronic Science and Technology of Chengdu, Sichuan 611731, China

ARTICLE INFO

Article history:
Received 24 November 2017
Received in revised form 26 February 2018
Accepted 13 May 2018

Keywords:
Optical chaotic
Double masking (DM) scheme
Chaos synchronization
Time-delay signature (TDS)
Long distance security communication

ABSTRACT

The emergence of optical chaotic secure communication has opened up an alternative path for information security. In this paper, based on two groups of mutually asynchronous vertical-cavity surface-emitting lasers (VCSELs), a novel double masking (DM) scheme for enhancing security of optical chaotic communication is proposed. We numerically analyze the synchronization characteristic of the lasers and the suppression of the time-delay signature (TDS). The self-correlation function (SF) and permutation entropy (PE) are employed to extract the TDS. Meanwhile, based on the high quality synchronization, we also investigate the communication performances of DM scheme in a long distance. Especially, the influence of the time delay due to delay fiber (DF) on the communication quality in different cases is studied. The results show that the TDS can be suppressed by the DM scheme to some certain degree. Four messages of 10 Gbit/s can be propagated in 138 km single mode fiber (SMF) after introducing the dispersion compensating fiber (DCF), bidirectionally and simultaneously. When the BER $\leqslant 10^{-9}$ and Q factor $\geqslant 6$, the DM scheme has smaller critical value of the time shift (Δt) than the single masking (SM) system, which indicate a good level of security.

1. Introduction

Optical chaotic secure communication has developed rapidly and plays an important role in the field of secure communication, attracting more and more researchers'attention. Compared to the conventional electrical chaos communication [1–4], optical chaotic secure communication has the advantages of high bandwidth, low loss, physical layer encryption, and compatibility with optical fiber systems. Therefore, many scholars have put forward multitudinous optical chaotic secure communication schemes and applications [5–10].

Recently, more advanced schemes of optical chaos secure communication in diverse application areas have been proposed. Several long-haul chaos communication systems are proposed [11–18]. Based on the consistency of a semiconductor laser, the effectiveness of a chaos mask signal is used for reservoir computing (RC) [19]. A security-enhanced chaos communication scheme is designed [20] with time delay signature (TD) suppression and phase-encrypted feedback light. In [21], a bidirectional dual-channel broadband chaos communication system based on two mutually coupled VCSELs subject to a bandwidth-enhanced chaotic signal injection has been proposed. Moreover, a fast and secure symmetric image encryption-then-transmission system based on optical chaos is reported [22]. In the above-mentioned schemes, all the systems exploit chaos masking (CM) technique to modulate information. Hence the information can be transmitted to the receiver with good communication performance, high security and high reliability. In order to enhance the privacy and hide the information better, a new chaotic communication scheme is proposed, which double masks the information by using optical chaos and the voltage chaotic waveform [23]. However, we have noted that no works are reported on optical chaotic communication applying double masking technique by two different optical chaos signals based on two groups of mutually asynchronous VCSELs.

In this work, to the best of our knowledge, we firstly proposed a double masking scheme for enhancing security by two different optical chaos signals. Here, we use two groups of mutually asynchronous lasers. One group is composed of a master laser (M1) and two slave lasers (S11 and S12), while the other group consists of a master laser (M2) and two slave lasers (S21 and S22) as well. The optical feedback of the master laser can make the laser into the chaotic state and strengthen the nonlinear dynamics characteris-

* Corresponding author at: School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China.
E-mail address: yyxie@swu.edu.cn (Y.-Y. Xie).

https://doi.org/10.1016/j.optlastec.2018.05.022
0030-3992/

tics. High quality properties of chaos synchronization between the two slave lasers in each group can be realized, however, the first group of lasers is out of synchronization with the second sets of lasers. Meanwhile, variable length of delay fiber (DF) is the key to control two groups of lasers to realize different synchronization. Furthermore, we investigate the security performance and communication quality of the double masking system.

The remainder of this paper is organized as follows. In Section 2, the system model and theory method are introduced in detail. In Section 3, the numerical simulations are demonstrated and analysed, including the chaos synchronization performance and the security analysis. In Section 4, the properties of long distance communication are studied and evaluated. Finally, Section 5 concludes the paper.

2. System model and methods

The schematic diagrams of our proposed system configuration are expounded in Fig. 1. As we can see from Fig. 1(a), the system consists of two groups of lasers. The first group is made up of M1, S11 and S12. The second group is made up of M2, S21 and S22. The output of M1 is divided into two parts via a beam splitter (BS). One part is fed back to M1 to strengthen the dynamic complicacy by a mirror (M), and the other is sent to another BS after passing an optical isolator (OI) and a neutral density filter (NDF). The OI can guarantee unidirectional coupling and the NDF can adjust the injection strength. Afterwards, the two optical beams are delivered through a pair of fibers (F) and unidirectionally injected into S11 and S12 over a long distance, respectively. For the sake of high-quality chaotic synchronization between S11 and S12, the configuration of the system ought to be symmetrical, and the two slave lasers should have similar inner parameters. The output of the S11 and S12 are transported into the adders via the delay fiber (DF). Meanwhile, the identical process with M2, S21 and S22 is also configured as mentioned above. It should be noted that M2, S21 and S22 possess different inner parameters with M1, S12 and S21. Then the output of the two adders are separated into two parts by the power splitter (PS). One part is used to encrypt the message (m(t) and m′(t)), and the other part is used to decrypt the message (M(t) and M′(t)).

We take two pairs of long messages in Fig. 1(b) and (c) to describe message encryption and decryption process in more detail, owing to the outputs of VCSELs generally contain x polarization component (x-PC) and y polarization component (y-PC). Here, Fig. 1(b) and (c) mainly describes modulation and demodulation modules of x-PC and y-PC, respectively. In Fig. 1(b), the output of S11 is split into x-PC and y-PC by a polarization beam splitter (PBS). After that, x-PC passing through an OI and a DF into the adder, and the transmission process of y-PC is shown in Fig. 1(c). In the meantime, similar processes is applied to S12, S21 and S22. The output of the adder that processed S11 and S21 is separated into two parts. One part is mixed with Message1 by chaos masking technique, and then is sent to the receiver through a long fiber for achieving declassified message1 (DM1). The other part is sent to the receiver in order to demodulate the Message2. Furthermore, the output of the adder that processed S12 and S22 is separated into two parts. One part is mixed with Message2 by chaos masking technique, and then is sent to the receiver through a long

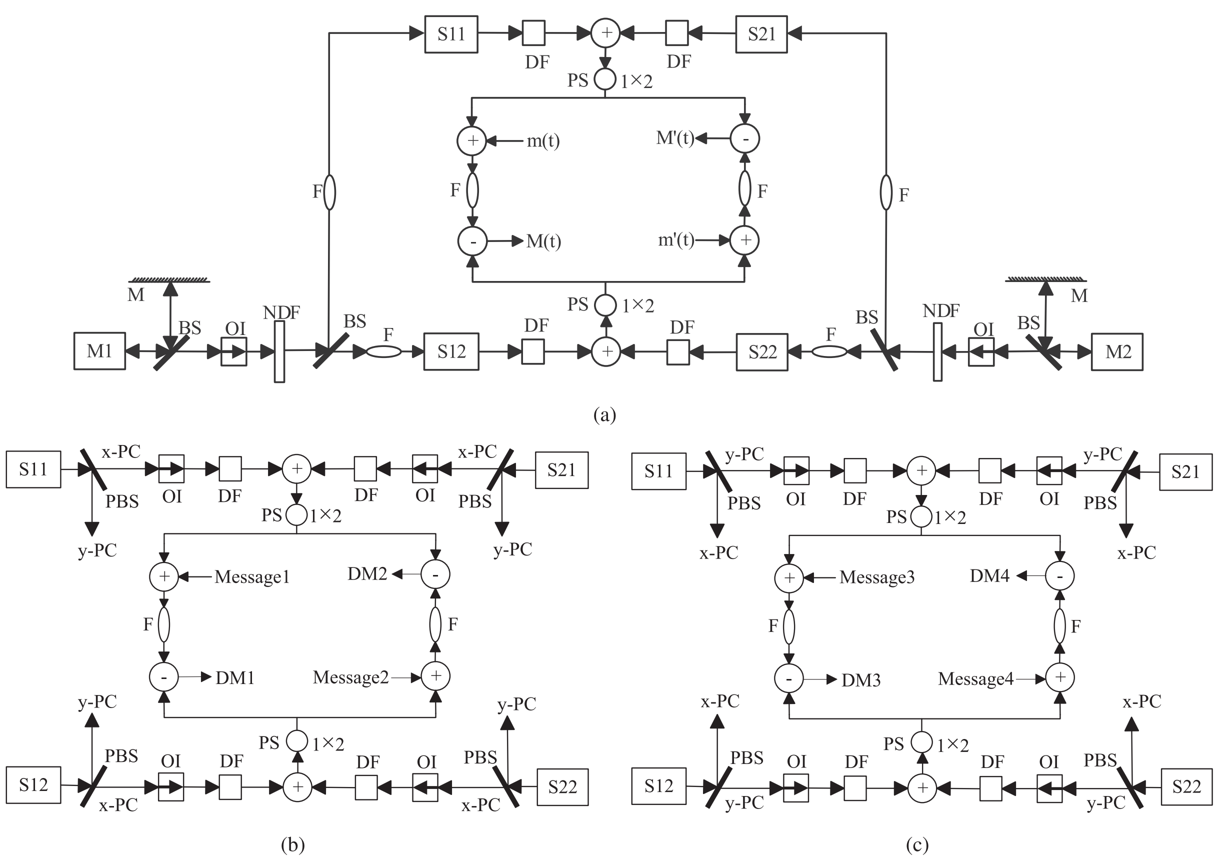

Fig. 1. The schematic diagram of double masking system: (a) total message transmission schematic, (b) message transmission schematic in x-PC, (c) message transmission schematic in y-PC. M1: master laser 1; M2: master laser 2; S11: slave laser 11; S12: slave laser 12; S21: slave laser 21; S22: slave laser 22; M: mirror; OI: optical isolator; NDF: neutral density filter; BS: beam splitter; F: fiber; DF: delay fiber; PS: power splitter; PBS: polarization beam splitter.