Optics and Lasers in Engineering 102 (2018) 170–180

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

A novel image encryption algorithm based on synchronized random bit generated in cascade-coupled chaotic semiconductor ring lasers

Jiafu Li[a], Shuiying Xiang[a,b,*], Haoning Wang[a], Junkai Gong[a], Aijun Wen[a]

[a] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
[b] State Key Discipline Laboratory of Wide Bandgap Semiconductor Technology, School of Microelectronics, Xidian University, Xi'an 710071, China

ARTICLE INFO

Keywords:
Image encryption
semiconductor ring laser
Chaotic synchronization
Physical random bit generator

ABSTRACT

In this paper, a novel image encryption algorithm based on synchronization of physical random bit generated in a cascade-coupled semiconductor ring lasers (CCSRL) system is proposed, and the security analysis is performed. In both transmitter and receiver parts, the CCSRL system is a master-slave configuration consisting of a master semiconductor ring laser (M-SRL) with cross-feedback and a solitary SRL (S-SRL). The proposed image encryption algorithm includes image preprocessing based on conventional chaotic maps, pixel confusion based on control matrix extracted from physical random bit, and pixel diffusion based on random bit stream extracted from physical random bit. Firstly, the preprocessing method is used to eliminate the correlation between adjacent pixels. Secondly, physical random bit with verified randomness is generated based on chaos in the CCSRL system, and is used to simultaneously generate the control matrix and random bit stream. Finally, the control matrix and random bit stream are used for the encryption algorithm in order to change the position and the values of pixels, respectively. Simulation results and security analysis demonstrate that the proposed algorithm is effective and able to resist various typical attacks, and thus is an excellent candidate for secure image communication application.

1. Introduction

Along with the rapid advancement of internet and multimedia technologies, a vast number of digital images are now transmitted over the internet, and information security has become an increasingly serious issue. Recently, many image encryption technologies based on chaos, DNA, cellular automata and others have been introduced [1-23]. Image encryption is mostly divided into two stages: permutation (or confusion) and diffusion [1,4,5,11,12,15]. In the confusion stage, the image pixels are permuted to destroy the spatial distribution and local correlation. In the diffusion stage, the pixel values are changed, and diffusion can lead to higher security.

Since Fridrich proposed the chaotic image encryption scheme, cryptosystems based on chaos theory have drawn many researchers' attention and many chaos-based image encryption algorithms have been presented [1-4]. When chaotic systems are used in image encryption, the security levels of image encryption schemes are highly dependent on the performance of chaotic systems. Image encryption methods mostly use two kinds of chaotic systems, one-dimensional (1D) chaotic system and high-dimensional (HD) chaotic system [5,6,12,13]. For some simple chaotic systems such as 1D logistic map, their chaotic orbits are quite simple and may be predicted easily. Therefore, the corresponding image encryption scheme may be easily attacked with the development of signal processing technology [24,25]. The HD chaotic systems have complex chaotic behaviors and their chaotic orbits are difficult to be predicted. However, they also have some drawbacks, such as high implementation cost, complex performance analysis and low speed [10]. It is possible to improve the efficiency and security of image encryption by replacing the traditional chaotic system with optical chaotic system [16].

Chaos based random bit generator (RBG) is one of the common fields where chaotic systems are used for encryption [23,30,31,35,37,38]. For example, Xie et al. proposed a fast and secure symmetric image encryption-then-transmission scheme based on optical chaos. But in this scheme, an optical chaotic system is only used to generate the key [23]. Compared with traditional optical chaos systems, optical chaos generated by cascade-coupled semiconductor ring lasers (CCSRL) system exhibits several advantages, such as wide bandwidth, high security, relatively low implementation cost, high speed and easy to implement on chip [26-28,31-34].

Note that the majority works were focused on the security of the encryption algorithm. However, the efficiency and cost of the encryp-

* Corresponding author: State Key Laboratory of Integrated Service Networks, Xidian University, P.O. Box 119, 2 South Taibai Road, Xi'an, Shanxi 710071, China.
E-mail address: jxxsy@126.com (S. Xiang).

https://doi.org/10.1016/j.optlaseng.2017.11.001
Received 11 July 2017; Received in revised form 21 September 2017; Accepted 2 November 2017
0143-8166/

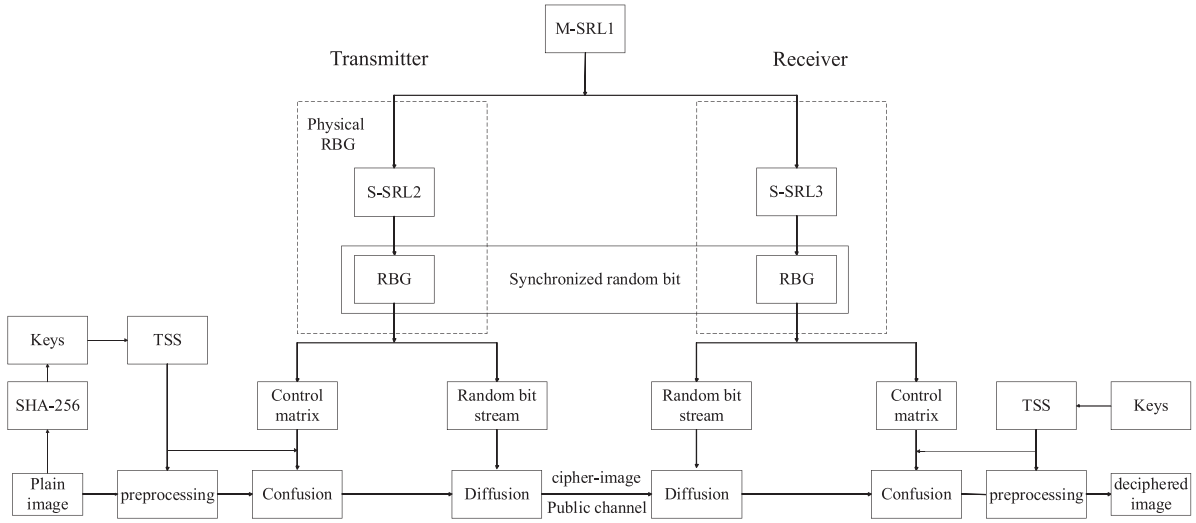

Fig. 1. The schematic diagram of the secure image encryption and decryption system. TSS: 1D Tent-Sine chaotic system, M-SRL: master SRL; S-SRL2 and S-SRL3: slave SRL; RBG: random bit generator.

tion algorithm are also critical to practical applications. In previous work, some scholars have proposed that image encryption using a synchronous permutation-diffusion technique to reduce time consumption [19]. However, it is still open and highly desirable to design an effective scheme to make encryption process faster and more secure with reduced complexity of the encryption system.

In this paper, we propose a novel image encryption algorithm based on synchronization of physical random bit generated in a CCSRL system, and concentrate on both the efficiency and security of the encryption algorithm. Firstly, the pixel value of the plain image is used to generate the initial values and parameters of chaotic systems for preprocessing and confusion stage, respectively. Secondly, the preprocessing method is used to eliminate the correlation between adjacent pixels. Thirdly, physical random bit with verified randomness is generated based chaos in the CCSRL system, and is used to simultaneously generate the control matrix and random bit stream. Finally, the control matrix and random bit stream are used for the encryption algorithm in order to change the position of pixels and the values of pixels, respectively.

The remainder of this paper is organized as follows. In Section 2, the theoretical models that describe the CCSRL system are derived from the Lang-Kobayashi (LK) equations [32,33]. In Section 3, the physical random bit with verified randomness generated based on CCSRL system is illustrated. In Section 4, the proposed image encryption process is illustrated and a new 1D Tent-Sine chaotic system (TSS) is presented [3]. Section 5 introduces simulation results and security analysis. Finally, conclusions are drawn in Section 6.

2. Theory and model

The schematic diagram of the secure image encryption and decryption system is presented in Fig. 1. Firstly, the SHA-256 hash function is used to generate the 256-bit key stream based on plain image. Secondly, the preprocessing method is used to eliminate the local correlation between adjacent pixels. Thirdly, the control matrix and random bit stream are used for the encryption algorithm in order to change the position of pixels and the values of pixels, respectively. Finally, cipher-image can be obtained after the diffusion stage. Decryption is an inverse process of the corresponding encryption process.

2.1. CCSRL system and rate equation models

The schematic representation of the CCSRL system is shown in Fig. 2. Chaos synchronization can be achieved by injecting a part of light intensity of one chaotic SRL into another one. Therefore, the CCSRL system is a master-slave configuration consisting of a master SRL (M-SRL1) with cross-feedback and a solitary SRL (S-SRL2 or S-SRL3). Due to the circular geometry, two counter-propagating modes, i.e., a clockwise (CW) and a counter-clockwise (CCW) mode can be supported in SRLs. For M-SRL1, the output of the CW (CCW) mode is feedback into the opposite mode, namely cross feedback, to obtain chaotic outputs. The output of the CW (CCW) mode of M-SRL1 is also injected into the same mode of the S-SRL2 (or S-SRL3), which corresponds to parallel injection, to obtain chaos synchronization.

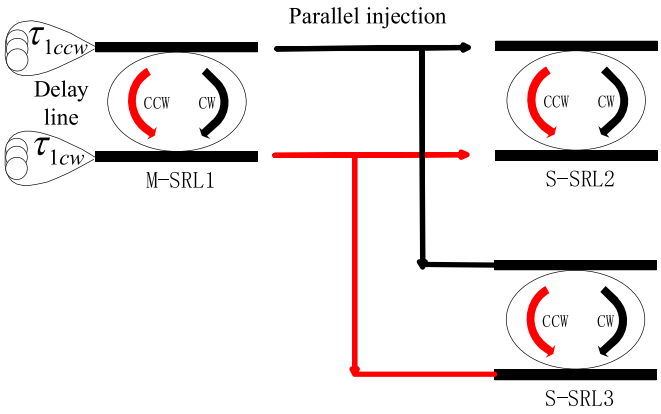

Fig. 2. The schematic representations of cascade-coupled semiconductor ring lasers system. M-SRL1, S-SRL2 and S-SRL3 are three SRLs.

Our rate equation model for a SRL operating in a single longitudinal and single transversal model can be derived from Maxwell-Bloch equations after adiabatic elimination of the material polarization dynamics [32]. We consider two mode rate equations for SRLs with parallel injection and cross feedback as follows [33]:

$$\frac{dE_{1cw}}{dt} = k(1+i\alpha_1)(G_{1cw}N_1 - 1)E_{1cw} - (k_d + ik_c)E_{1ccw} + kf_{1ccw}E_{1ccw}(t-\tau_{1ccw})e^{-i(\omega_1\tau_{1ccw})} \quad (1)$$

$$\frac{dE_{1ccw}}{dt} = k(1+i\alpha_1)(G_{1ccw}N_1 - 1)E_{1ccw} - (k_d + ik_c)E_{1cw} + kf_{1cw}E_{1cw}(t-\tau_{1cw})e^{-i(\omega_1\tau_{1cw})} \quad (2)$$