Optik - International Journal for Light and Electron Optics 176 (2019) 119–131

Contents lists available at ScienceDirect

Optik

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

Original research article

Chaos-based image encryption using vertical-cavity surface-emitting lasers

Animesh Roy[a], A.P. Misra[a,*], Santo Banerjee[b,c]

[a] Department of Mathematics, Siksha Bhavana, Visva-Bharati University, Santiniketan 731 235, West Bengal, India
[b] Malaysia-Italy Centre of Excellence for Mathematical Sciences, Universiti Putra Malaysia, Malaysia
[c] Institute for Mathematical Research, Universiti Putra Malaysia, Selangor, Malaysia

ARTICLE INFO

Keywords:
Image encryption
Bit-level permutation
Surface-emitting laser
Chaos
Synchronization

ABSTRACT

We study the encryption and decryption processes of color images using the synchronization of polarization dynamics in a free-running vertical-cavity surface-emitting laser (VCSEL). Here, we consider a bidirectional master-slave configuration or two-way coupling with two VCSELs. The latter are shown to exhibit hyperchaos and synchronization with a high level of similarity between their emission characteristics. The coupled VCSELs are then used as a transmitter and a receiver for the communication of image or data. Furthermore, we propose a modified chaos-based image encryption algorithm using the pixel- and bit-level permutations which provides robust, faster and simpler encryption/decryption compared to many other chaos-based cryptosystems. The performances of the new cryptosystem are analyzed and compared with a recently developed scheme [Opt. Laser Eng. 90 (2017) 238–246]. The security analysis and some statistical investigations show that the proposed cryptosystem is resistant to various types of attacks and is efficient for secure communications in nonlinear optical media.

1. Introduction

The advancement of public communication systems, such as satellite, mobile-phone, computer networking, Internet etc., has led to vulnerability in secure communication of e.g., the transmission of confidential data like military data, confidential videos, messages etc. In this way, the theory of cryptography has been developed (For some recent works, see, e.g., Refs. [1–7,10,11]). On the other hand, the invention of semiconductor laser diodes, e.g., the vertical-cavity surface-emitting lasers (VCSELs) has been gaining its potential applications in laser devices considering their numerous advantages over Light Emitting Diode (LED) and Edge Emitting Laser (EEL), such as low threshold, circular beam profile, and on-wafer testing capability [12,13]. Given their electro-optical characteristics and ability to modulate at frequencies ($\gtrsim$25 Gbps), VCSELs are ideal for high-speed communications and precision sensing applications. They are also used for reliable operation at distances ranging from very close proximity links (i.e., centimeters) up to 500 m in data center, enterprise, and campus networks. Furthermore, such VCSELs have been widely used in data communication industry for more than 15 years serving in data infrastructure links including 10, 40 and 100 Gbps Ethernet, 16 Gbps fiber channel, and 10, 14, and soon 25 Gbps lane Infinite Band. VCSELs are also emerging as an enabling technology across a wide range of applications, including touchless sensing, chip-to-chip interconnect, and gesture recognition.

It has been shown that VCSELs can also exhibit nonlinear polarization dynamics and chaos [6]. Such chaos can be obtained in a number of ways, e.g., when the lasers are driven (into chaos) due to optical feedback from an external reflector. Furthermore, optical

* Corresponding author.
E-mail addresses: aroyiitd@gmail.com (A. Roy), apmisra@visva-bharati.ac.in (A.P. Misra), santoban@gmail.com (S. Banerjee).

https://doi.org/10.1016/j.ijleo.2018.09.062
Received 16 October 2017; Received in revised form 12 August 2018; Accepted 14 September 2018

lasers like VCSELs or semiconductor lasers are used as secured media for transmission of confidential data, videos, messages etc. These lasers are also used for encryption-decryption of color images in the context of chaos based cryptography [7].

It is to be noted that two identical but independent chaotic systems cannot exhibit the same behaviors unless it is coupled or linked in some ways. In the latter, the system's evolution becomes identical, which is known as the chaos synchronization. Such exciting property of a dynamical system led to the development of secure chaos communication systems where the sender hides a message within the chaotic signal that can only be recovered by the receiver at the synchronized state. This approach has been applied in many secure communications, especially in optical chaos communication systems because of the added security and the speed of optical communications [7,8].

In classical cryptographic schemes (e.g., AES, DES, One time pad), public key cryptography is widely used for secure networking system. However, these schemes have some limitations in fast encryption on large data scales, such as those in color images, videos or audio data etc. These are not only sequences of large data sets, but also each sequence is highly correlated with another. Encryption of these data set with the classical schemes, as above, takes a longer time and thereby makes the system much slower (see, e.g., Ref. [14]). In order to resolve this issue, many authors have proposed chaos based cryptography schemes [1–4,9] in which a nonlinear dynamical system, which exhibits chaos, is considered for encryption and decryption [6,7]. On the other hand, the data encryption in chaotic medium is known to be much efficient than the traditional method in which it is more easier for hackers to recover the confidential data. Here, we consider a RGB color image which is a large set of data and its color distribution is highly correlated with the data set. So, although the transmission of these kind of data using the traditional encryption scheme is secured but security is much enhanced if we use a non-pattern medium like chaotic medium.

In this work, we consider a quantum spin-flip model (SFM) of VCSELs [6,15–17], to be given in Section 2, which is used for encryption and decryption of a RGB image using a modified chaos based cryptography scheme. It is shown that the coupled VCSELs can exhibit hyperchaos and synchronization with a wide range of values of the parameters. A new hyperchaos-based image encryption algorithm using the pixel- and bit-level permutations, which modifies the previous one [2], is proposed and tested with an RGB image. It is seen that the new cryptosystem is robust, faster, simpler and more secured in comparison with Ref. [2] and other chaos-based cryptosystems [1–5,9]. A statistical investigation is also carried out to ensure that the proposed encryption scheme is free from any brute force attack.

2. The model of VCSELs and their chaotic properties

We consider the nonlinear dynamics of right- and left-circularly polarized (RCP, LCP) emission arising from the recombination of two distinct carrier populations D_+ and D_- in VCSELs. The latter have a high quantum efficiency and low threshold which can operate on a very high rate optical communication in the range of several GHz. In terms of the slowly varying electromagnetic (EM) fields $E_\pm$ (normalized by the equilibrium value E_0) for RCP and LCP emission, we have the following set of equations [6,16,17]

$$\frac{dE_\pm}{dt} = \kappa(1 + i\alpha)(N \pm n - 1)E_\pm - i\gamma_p E_\mp - \gamma_a E_\mp, \tag{1}$$

$$\frac{dN}{dt} = -\gamma(N - \mu) - \gamma[(N + n)|E_+|^2 + (N - n)|E_-|^2]|E_0|^2, \tag{2}$$

$$\frac{dn}{dt} = -\gamma_s n - \gamma[(N + n)|E_+|^2 - (N - n)|E_-|^2]|E_0|^2, \tag{3}$$

where N, $n = D_+ \pm D_-$ are the normalized carrier populations, κ is the decay rate of the electric field in the cavity, α is the linewidth enhancement factor, and μ is the normalized injection current. Furthermore, γ is the carrier decay rate, γ_s is the spin-flip relaxation rate which models the process allowing the equilibration of the carrier population between the two reservoirs, and γ_p and γ_a are, respectively, the phase and amplitude anisotropies inside the laser cavity.

In order to establish chaos, we numerically solve the system of Eqs. (1)–(3) by a fourth order Runge-Kutta scheme with a time step size $t = 0.01$ and an initial conditions $E_\pm = 0.001$, $N = 0.003$, $n = 0.001$. The typical parameter values are considered as

- $1 \le \kappa \le 100\ \mathrm{ns}^{-1}$, $2 \le \kappa_{inj} \le 10\ \mathrm{ns}^{-1}$, $\alpha = 3$, $2 \le \Delta \le 10\ \mathrm{ns}^{-1}$,
- $0 \le \gamma_p \le 100\ \mathrm{ns}^{-1}$, $-7 \le \gamma_a \le 7\ \mathrm{ns}^{-1}$, $1.45 \le \gamma \le 1.5\ \mathrm{ns}^{-1}$, $0 \le \gamma_s \le 100\ \mathrm{ns}^{-1}$.

The results are displayed in Fig. 1 after the end of the simulation at $t = 1000$. From Fig. 1, it is seen that both the polarized electric fields $E_\pm$ of the master laser exhibit chaos along with the carrier population densities N and n. It is found that the chaotic state of the system can be reached due to the increasing values of the injection current parameter μ.

Furthermore, in order to have some confirmation of our results, we have computed the largest Lyapunov exponents as exhibited in Fig. 2 with the same parameter values as for Fig. 1. It is found that of the four exponents, two are always negative (not shown in the figure), and two others may be positive or negative depending on the values of the injection current parameter μ. From Fig. 2, it is evident that the two lyapunov exponents can turn over from negative to positive values as the values of μ increase, leading to chaos (more specifically hyperchaos) for a longer time. This is in consequence with the fact that the chaos in VCSELs is obtained when the lasers are driven due to the optical feedback from an external reflector.