Image encryption and decryption using vertical-cavity surface-emitting lasers (VCSEL)

Animesh Roy and A. P. Misra *

The development of data communication system, such as computer networking, mobile phones etc., has been gaining momentum in recent years [**?**, **?**, **?**]. The advent of such communication system leads to a major issue of security on transmission of confidential data like military data, confidential videos, messages etc. In this way, the theory of cryptography has been developed. 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 of fast encryption on large data scales, such as those in color image, video 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. In order to get rid of this situation, many authors have proposed chaos based cryptography schemes in which a nonlinear dynamical system, which exhibits chaos, is considered for encryption and decryption.

In this work, we consider a quantum spin-flip VCSEL model [**?**, **?**] as given below which considers the right- and left-circularly polarized (RCP, LCP) emission arising from recombination in two distinct carrier populations D_+ and D_-. This model is then used for encryption and decryption of a RGB image using the chaos based cryptography scheme [**?**].

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

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

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

where $E_\pm$ are the froward and backward electric fields for RCP and LCP emission, and $(N,\ n) = D_+ \pm D_-$. We have used the chaos sequence as in [**?**] and proposed a new algorithm for Encryption and decryption. Here, the synchronization of the VCSEL model with another one (sender-receiver) is established to transmit and decrypt the cipher data for recovering original one through the chaotic process. A pictorial diagram is given in Fig. **??** to show how a data is to be transmitted securely using the VCSEL model.

*Department of Mathematics, Siksha Bhavana, Visva-Bharati, Santiniketan-731 235. Emails: aroyiitd@gmail.com (A. Roy), apmisra@visva-bharati.ac.in (A. P. Misra)

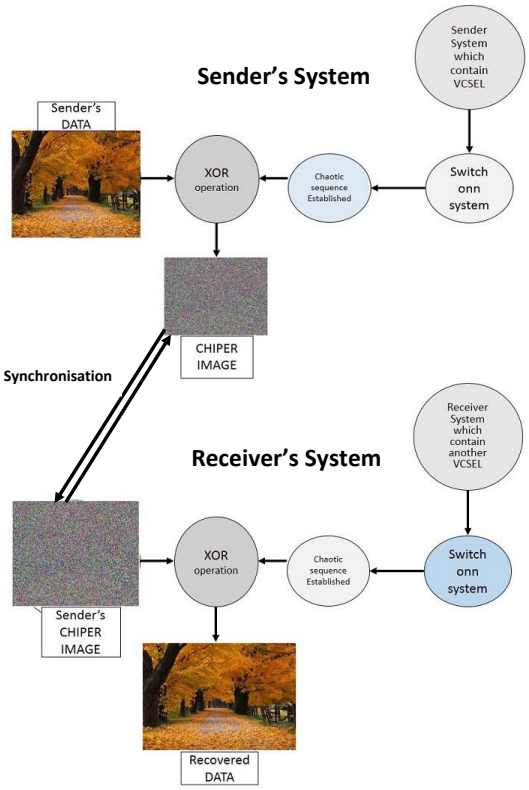

Figure 1: Example of Encryption and Decryption of RGB Image using VCSEL

We mention that the whole procedure is free from brute force attack as the relevant parameters and initial conditions are taken as key for the encryption and decryption.

The full paper is to be submitted to a journal

References

[1] Martin Virte, Krassimir Panajotov, Marc Sciamanna *Bifurcation to nonlinear polarization dynamics and chaos in vertical-cavity surface-emitting lasers*, PHYSICAL REVIEW A 87: 013834 [10 pages], 2013 .

[2] J. P Hermier, M. I. Kolobov, I. Maurin, E. Giacobino *Quantum spin-flip model of vertical-cavity surface emitting laser*, Physical Review A, 65: 053825 [13 pages], 2002.

[3] S. Banerjee, L. Rondoni, S. Mukhopadhyay, A. P. Misra. *Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption*, Optics Communications 284: 22782291, 2011.