Chaos synchronization and cryptography for network security

Name: Animesh Roy

Guide Name: Dr. Amar Prasad Misra

Department of Mathematics, Visva-Bharati

Santiniketan-731235, West Bengal, India.

Registration No. : VB- 2323 of 2016-2017

Date of Registration : 28.11.2016

Key words : Dynamical system, chaos, synchronisation, cryptography, network security.

Introduction: 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 systems 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 colour 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.

The idea of chaos based cryptography was first introduced by Shanon in 1949, though he did not implicitly use the word 'chaos', instead he mentioned "Well-mining transformation in good security system can be constructed on the base of the stretch and fold mechanism", which is nearly a 'chaotic system'. Synchronization is one type data transmission or pulse propagation from one system to another. A statistical investigation and computational algorithm are made for securing the network communication using the nonlinear dynamical model which exhibits chaos through the process of synchronization.

Objective: The main objective of this work is to study the synchronization and chaotic properties of different nonlinear dynamical systems such as semiconductor lasers, vertical cavity

surface emitting lasers which exhibit chaos. These systems are then used for data transmission by means of cryptosystem. We also plan to investigate various wireless networking models and its security analysis through chaotic dynamics.

References:

[1] Claude E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28-4, page 656–715, 1949.

[2] 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 .

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

[4] 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.

[5] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems", *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[6] M. S. Baptista, "Cryptography with Chaos", *Physics Letters A*, vol. 240, pp. 50–54, 1998.

[7] Jiyun Yang ,Tao Xiang and Di Xiao 'Cryptanalysis of a secure chaotic map based block cryptosystem with application to camera sensor networks' December 2015, Volume 74, Issue 23, pp 10873–10881