Optics and Lasers in Engineering 48 (2010) 398–404

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Chaos-based secure communication system using logistic map

Narendra Singh, Aloka Sinha *

Department of Physics, Indian Institute of Technology Delhi, Hauz Khas, New Delhi-110016, India

ARTICLE INFO

Article history:
Received 31 July 2009
Received in revised form
30 September 2009
Accepted 1 October 2009
Available online 12 November 2009

Keywords:
Opto-electronic encryption/decryption
Logistic map
Pulse position modulation

ABSTRACT

We propose a new opto-electronic secure communication system using logistic map and pulse position modulation. A modified version of the electronic circuit of the logistic map is used to generate the chaotic signal. Pulse position modulation scheme together with the logistic map has been used to encrypt the signal. Optical fiber has been used to demonstrate the proposed scheme. Eye pattern has been used to verify the noise-like nature of the encrypted signal. Opto-electronic implementation of the technique has been carried out. Experimental results are presented to verify the validity of the proposed technique.

1. Introduction

In recent years, hacking of data has become a serious problem due to which secure communication encryption schemes [1] is becoming a fundamental need for everyone. In order to fulfill these requirements, many optical encryption techniques have been proposed. These use Fourier transform (FT) [2–3], fractional Fourier transform (FRT) [4–5], extended FRT (EFRT) [6], gyrator transform (GT) [7], Hartley transform (HT) [8], and watermarking methods [9]. Other image encryption techniques have also been proposed recently [10–12]. As the need for secure communication increases, "chaos" has become an important tool for the realization of such secure system. Chaos is the term used for a variety of non-linear phenomenon that occur in both discrete and continuous dynamical systems. Due to the attractive properties of chaos such as noise-like behavior and sensitivity to the initial condition, it has become very important for both optical encryption methods [13–18] and electronic encryption methods. Chaotic signal can be generated by using relatively simple analog hardware such as electronic hardware for logistic map [19], tent map [20] and Chua circuit [21–23]. Various chaotic modulation schemes such as differential chaos shift key (DCSK) [24] and pulse position modulation (PPM) scheme [25–29] have been proposed. Along with the development of optical telecommunications systems, there is lot of interest in secure optical transmission and in opto-electronic technique for encryption. Several opto-electronic systems have been proposed [30–35] that exploit fast chaotic dynamics as a possible alternative to classical encryption techniques based on numerical algorithms. The noisiness of the encrypted data can be analyzed by using eye pattern [36–38].

In this paper, we propose a new opto-electronic secure communication system using logistic map and PPM. The generated chaotic signal is added to the input signal and a PPM scheme is performed over it. The obtained signal is the encrypted signal. The encrypted signal is communicated through an optical fiber from the transmitter side to the receiver side. At the receiver, pulse position demodulation (PPD) is performed and the same chaotic signal is subtracted from it. The obtained signal is the decrypted signal. The chaotic signal has been generated by designing the electronic circuit for implementation of the logistic map. A modified version of the electronic circuit has been designed. Optical fiber has been used as the communication channel to demonstrate the proposed technique. Eye pattern has been used to verify the noisy nature of the encrypted signal. Opto-electronic implementation of the technique has been carried out. Experimental results are presented to verify the validity of the proposed technique.

2. Logistic map

Logistic map [14–19] is a chaotic map that generates chaotic signal which has a random-like appearance and is very sensitive to the initial conditions. These random iterative values are limited between bounds. After any value of iterations, convergence of the iterative values can never be seen. Logistic map is used for our study and is defined as

$$f(x) = \lambda x(1-x) \tag{1}$$

* Corresponding author. Tel.: +91 11 2659 6003.
E-mail address: aloka@physics.iitd.ernet.in (A. Sinha).

0143-8166/$ - see front matter © 2009 Published by Elsevier Ltd.
doi:10.1016/j.optlaseng.2009.10.001

This function is bounded for $0 < \lambda \leq 4$.The iterative form of this function is written as

$$x_{n+1} = \lambda x_n(1 - x_n) \tag{2}$$

with 'x_0' as the initial value. This chaotic map is used to generate the chaotic signal.

3. Pulse position modulation

In PPM,[29] the amplitude and width of the pulse is kept a constant, while the position of each pulse, in relation to the position of a recurrent reference pulse is varied by each instantaneous sampled value of the modulating wave i.e. position of the pulse depends on pulse width, which is determined by the signal amplitude at that instant. PPM has the advantage of requiring constant transmitter power output and it depends on the transmitter–receiver synchronization. The PPM is obtained by pulse width modulation (PWM) (i.e. the width of the carrier wave is changed according to the modulating wave) The method of obtaining PPM from PWM is thus accomplished by "getting rid off" the leading edges and bodies of the PWM pulse. PPM is generated when the circuit will work as astable multivibrator. The frequency of oscillation of PPM signal is calculated by the charging and the discharging time which is also calculated from the resistance and the capacitor. The charging time (output high) is given by

$$t_1 = 0.693(R_A + R_B)C \tag{3}$$

where R_A and R_B are the two charging and discharging resistances and C is a capacitor.

The discharge time (output low) is given by

$$t_2 = 0.693(R_B)C \tag{4}$$

Thus, the total time is

$$T = t_1 + t_2 = 0.693(R_A + 2R_B)C \tag{5}$$

The frequency of oscillation is given by

$$f = \frac{1}{T} = \frac{1.44}{(R_A + 2R_B)C} \tag{6}$$

The duty cycle is given by

$$D = \frac{R_B}{R_A + 2R_B} \tag{7}$$

When the PPM is demodulated at the receiver, it is again converted into PWM. This is done with a flip flop, or bistable multivibrator. One input of the multivibrator receiver triggers pulses from a local generator which is synchronized by trigger pulse received from the transmitter, and these triggers are used to switch OFF, the ON stage of the flip flop. The PPM pulses are fed to the other base of the flip flop which switches that stage of the flip-flop ON. The period of time during which this particular stage is OFF depends on the time difference between the two triggers, so that the resulting pulse has a width that depends on the time displacement of each individual PPM pulse. The resulting PWM pulse is then demodulated.

4. Proposed technique

The encryption process and the decryption process of the proposed technique are shown in Fig. 1. Let $S(t)$ be the input signal. The chaotic signal $C(t)$ is added to the input signal, where $C(t)$ is the random number sequence generated by the electronic circuit of the logistic map in time domain. The PPM is performed over this combination. The obtained signal is the encrypted signal which is expressed as $E(t)$and is given by

$$E(t) = PPM\{S(t) + C(t)\} \tag{8}$$

The decryption process is the inverse of the encryption process. PPD operation is performed over $E(t)$ and $C(t)$ is subtracted from this signal. The obtained signal is the decrypted signal which is expressed as $D(t)$and is given by

$$D(t) = PPD\{E(t)\} - C(t)\} \tag{9}$$

5. Proposed opto-electronic implementation of the encryption and decryption technique

Opto-electronic implementation of the proposed technique involves the construction of various block such as adder, subtractor, low pass filter (LPF) [38], logistic map, PPM and PPD. Circuit description of these blocks are explained below.

5.1. Circuit description of logistic map

The block diagram of the logistic map [19] is shown in Fig. 2. The block diagram of the logistic map is shown in the Fig. 2. This block diagram realizes the Eq. 2. Some modifications have been incorporated in the circuit diagram of the logistic map (as shown in Fig. 3) used in the proposed technique in comparison to the circuit diagram of the logistic map used in the earlier circuit design [19]. In the present design, there is an option to change the seed value of the electronic circuit of the logistic map. The seed value can be changed by using the variable resistance at pin no. 6 of the second multiplier if required. In the previous technique, a complicated circuit consisting of two LF398 ICs, one transistor 2N3904, some resistors and capacitors have been used to iterate the loop of the electronic circuit of logistic map. In the new design, a simple circuit using single LF398 IC (sample and hold IC) is used to iterate the loop of the electronic circuit of logistic map. IC 741 (single output general-purpose operational amplifier) is used to design the electronic circuit of subtractor and amplifier, respectively instead of LM1458 IC(dual output operational amplifier). MPY634 IC is replaced by LF633 IC to design the electronic circuit of first and second multipliers, respectively.

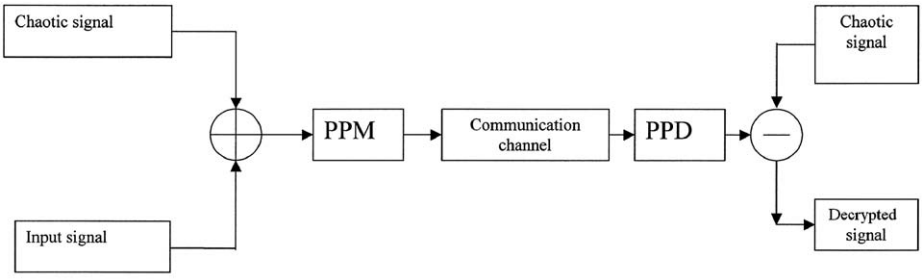

Fig. 1. The schematic block diagram for encryption and decryption process.