Penguins Search Optimization Algorithm (PeSOA) for chaotic synchronization system

Maamri Fouzia [1], Bououden Sofiane [1], Djellab Hanane[2], Ilyes Boulkaibet [3]

[1:] *Laboratory of SATI, University Abbes Laghrour* Khenchela, Algeria
[2:] *Laboratory of LTI Guelma,University Larbi Tebessi, Tebessa*, Algeria
[3:] *College of Engineering and Technology, American University of the Middle East, Kuwait*

Abstract

Information encryption is a security process where data is encoded using chaotic signal. stabilization and synchronization in chaotic systems for secure information can be achieved using the metaheuristic algorithms. In this work Penguins Search Optimization Algorithm (PeSOA) which is inspired by penguin's social behavior is applied to synchronize chaotic encryption signal. PeSOA algorithm explores space with random and iterative search in order to find symmetric encryption key of the chaotic system in both transmission and reception. Identification based on metaheristic optimization Algorithm (PeSOA) is used to improve the accuracy of initial conditions and control parameters of Chua's chaotic generator by minimizing errors between the estimated and identified value. Simulation results show the effectiveness of the PeSOA algorithm to generating symmetric key of encryption process and synchronizing both chaotic circuit of transmitter and receiver one.

.

Keywords

Metaheuristic, PeSOA, Chaos, Encryption, Synchronization, Optimization.

1 Introduction

Information security has become one of the extreme important problems in communication. The simplicity of chaos generation and the rich trajectories of chaotic signals have been receiving significant attention in secure communication. Application for transmitting signals using chaos in nonlinear systems was proposed by Pecora and Carroll [1] and it is widely used in engineering topic [2, 3]. In secure communication, synchronization and chaotic encryption concepts are very important [4, 5, 6]. Synchronization is the notion of correlations between coupled systems [7] and chaotic encryption consists of adding a chaotic signal to the information signal to be transmitted. The transmitter sends this chaotic signal to the receiver. Chaotic signal is characterized by its high sensitivity to initial condition change and control parameters. The importance of identifying chaos parameters has more attraction among researchers in the field of engineering [8, 9, 10, 11]. Several optimization methods were proposed to improve the identification process of the systems' chaotic parameters [12, 13]. Meta-heuristic optimization has been widely used to identify parameters of the chaotic system [14, 15, 16].

In this work, a scheme of secure communication and synchronization using meta-heristic PeSOA algorithm has been proposed. The application of chaotic encryption process using PeSOA algorithm is based on collaborative hunting strategy of penguins to identify control parameters of Chua's chaotic circuit. Chua's circuit has been exploited as a simple and powerful source of chaotic signals for encrypting signal. To decrypt original information, it is necessary to know the characteristics of the chaotic signals. Identifying parameters of chaotic system using PeSOA algorithm permit to extract the sent information signal. The extraction of the original information signal is achieved after the synchronization step of chaotic signals.
The paper is organized as follows: Penguins Search Optimization Algorithm (PeSOA) is illustrated in section II. Section III describes the chaotic generator system, the section IV presents the synchronization simulations using PeSOA algorithm. Results of numerical simulation are given in section V. Finally, we conclude the paper and prospect for future works in Section VI.

2 PeSOA algorithm

The Penguins Search Optimization Algorithm (PeSOA) is one of the latest meta heuristic algorithms inspired by Penguin's social behavior and proposed by Geraibia and Moussaoui [17,18] in 2013, where this algorithm is based on the collaborative hunting strategy of penguins. In the PeSOA algorithm, each penguin is represented by its position and the number of fishe eaten. The distribution of penguins is based on probabilities of the existence of fish in a specific location. The main steps of this algorithm can be summarized as follows:
The penguins are divided into groups, and begin the research in random positions. After a fixed number of dives, penguins return to the ice and share information such as positions and the number of nutrients found [17]. Global (optimal) solution is then nominated by electing the best group of penguins who ate the maximum number of fish. The Penguins Search Optimization Algorithm has several parameters (population size, initial oxygen reserve, number of generations, etc.).

The algorithm can be summarized in four steps:

1. All Penguins are distributed in groups where each member *i* represents a solution Xi.
2. Each group search for food in defined holes with differences levels.
3. Penguins are sorted in order and start searching in a specific hole and level according to the probability of food availability.
4. In each iteration, the position of the penguin with each new solution is adjusted as follows:

$$D_{new} = D_{Last} + rand()|X_{LocalBest} - X_{LocalLast}| \quad 1$$

where: *D*Last is the last best solution accord for the penguin *i*, rand() is a random number, and each penguin has three solutions: the best local solution (XLocalBest), the final solution (XLocalLast) and the new solution (*Dnew*). The evaluation of the solutions is repeated for every penguin in each group, and after several dives, penguins are then communicating to each other in order to transmit the best solution, which is represented by the number of fish consumed [24]. The algorithm can be summarized in four steps:

All Penguins are distributed in groups where each member *i* represents a solution Xi. Each group searches for food in defined holes with different levels.

Pseudocode of the PeSOA algorithm

1. Generate random population of P solutions (penguins) in groups ;
2. Initialize the probability of existence of fish in the holes and levels;

For i=1 to number of generations;

For each individual i $\in$ P do

While oxygen reserves are not depleted do

Take a random step.

Improve the penguin position using Eqs. (1)

Update quantities of fish eaten for this penguin.

End

End

3. Update quantities of eaten fish in the holes, levels and the best group.
4. Redistributes the probabilities of penguins in holes and levels (these probabilities are calculated based on the number of fish eaten).
5. Update best-solution

End

PeSOA metaheuristic algorithms have been employed to identify the chaotic search behavior. Using oscillators is necessary to generate a chaotic signal. In this work, the chaotic generator employed is the Chua’s circuit.

3 Chaotic generator

Chua’ circuit is considered as a very simple deterministic system invented by Leon Chua in 1983. This circuit generates a variety of chaos trajectories [20]. It consists of two capacitors C1 and C2, one inductance L and nonlinear resistor N_R (Chua's diode), placed on three parallel branches as shown in figure 1 [21].

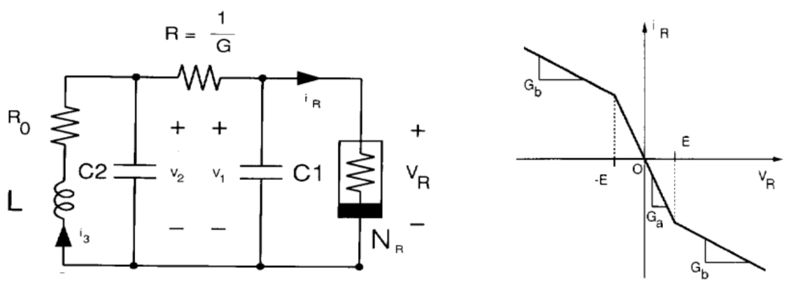

Figure 1 : Chua’ circuit and Characteristic of the nonlinear resistor N_R

Were:

V_1: the voltage across capacitor C_1 and the nonlinear resistance

V_2: the voltage across capacitor C_2 and the voltage across the inductor

I_3: the current through the inductor and N_R: the nonlinear resistor.

The state equations describing the Chua's circuit is given as follows [20, 21]:

$$C_1 \frac{dV_1}{dt} = \frac{1}{R}(V_2 - V_1) - F(V_1)$$
$$C_2 \frac{dV_2}{dt} = \frac{1}{R}(V_1 - V_2) + i_3 \quad 2$$
$$L \frac{di_3}{dt} = -(V_2 - R_0 i_3)$$

Were R is the nonlinear resistor; R_o is a small positive resistance of the inductor L.

$$F(V_1) = G_b V_1 + 0{,}5(G_a - G_b)(|V_1 + E| - |V_1 - E|) \quad 3$$

The resistor *R* represents a potentiometer and is used to adjust the oscillator over a range of bifurcation values:With these variable changes, State equations are transformed into the form below:

$$\dot{x}_1 = \alpha(x_2 - x_1 - g(x_1))$$
$$\dot{x}_2 = x_1 - x_2 + x_3 \quad 4$$
$$\dot{x}_3 = -\beta x_2 - \gamma x_3$$

The effect of nonlinear element in the circuit $g(x_1)$ is given by the nonlinear voltage-current characteristic of the Chua's diode, which is described by:

$$g(x_1) = b\, x_1 + 0{,}5(a - b)(|x_1 + 1| - |x_1 - 1|) \quad 5$$

Where X_1, X_2 and X_3 being the state variables. α, β, γ, a and b : system parameters.

$X_1 = \frac{V_1}{E}$ $\quad X_2 = \frac{V2}{E}$ $\quad X_3 = \frac{R}{E}\dot{i}_3$

$\alpha = C_2/C_1$, $\beta = C_2 R^2/L$, $\gamma = R R_0 C_2/L$, $a = RG_a$, $b = RG_b$

The Chua circuit exhibits chaotic behaviour, an example of the chaotic trajectory of this system is shown in figure 2.

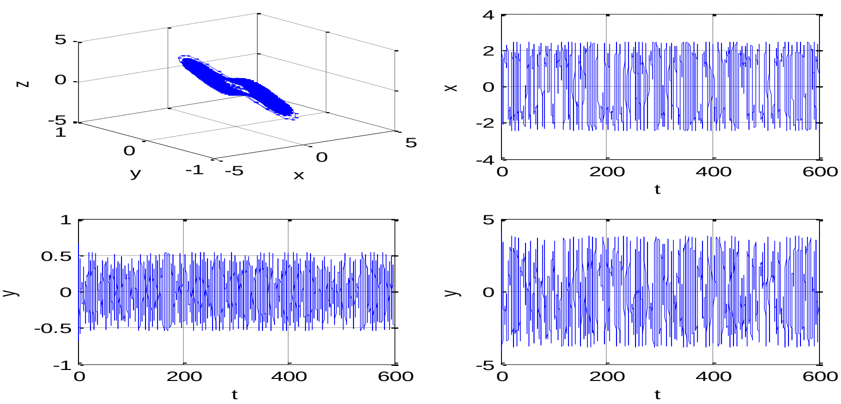

Figure 2 : Illustration of the chaotic dynamics of the Chua's circuit and time series of state variables

4 Synchronization using PeSOA algorithm process

In this section, we will illustrate the synchronization process in chaotic encryption. Synchronization is a fundamental step for chaotic encryption that duplicates the chaotic signal transmitted from the transmitter to the receiver and has received amount of attention in secure communication systems [22]. So, synchronization it is an important part of study of chaotic systems.

The main idea of this work is the identification of Chua ‘circuit parameters based on PeSOA meta-heristic algorithm in order to predict control parameters and consequently synchronize chaotic systems.

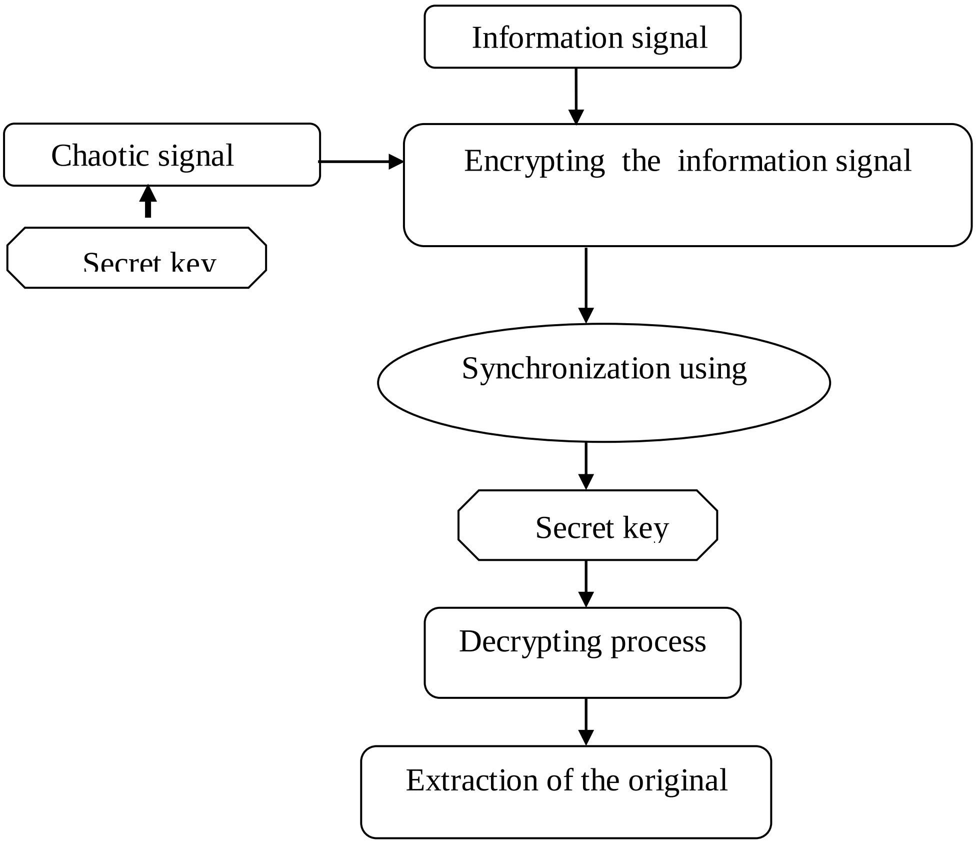

Figure 3 : Proposed scheme of Secure communication and Synchronization using meta-heristic PeSOA algorithm

5 Numerical simulations

Identification of chaotic system parameters can be usually described as follows [23]:

$$\dot{X} = F(X, X_0, \Phi) \qquad 6$$

Where:

- $X = (x_1, x_2, \ldots, x_n)^T \in R^n$ is the state vector. $(\Phi_1, \Phi_2, \ldots, \Phi_n)^T \in R^m$ is the unknown parameter vector of the original chaotic system. X_0 is the initial condition of state vector and *F* is a nonlinear function.

The estimated model of the system is given by:

$$\dot{\hat{X}} = F(\hat{X}, X_0, \hat{\Phi}) \qquad 7$$

Where: $\hat{X} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)^T \in R^n$ is the state vector. $\hat{\Phi} = (\hat{\Phi}_1, \hat{\Phi}_2, \ldots, \hat{\Phi}_n)^T \in R^m$ is an estimation of the unknown parameter vector of original chaotic system.

Generally, the meta-heuristic algorithms require only the evaluation of an objective function in order to guide the search process. The objective function is then defined as follows:

$$\min_{\text{objective function}} = \frac{1}{N}\sum \|X - \hat{X}\|^2 \qquad (8)$$

Where:

- N is the length of vector used for parameter estimation.
- X and $\hat{X}$: are the state variable of the original and the estimated systems.

Using simulation on MATLAB, identification of Chua's parameters using PeSOA algorithm is given in the following figure 4 (a= -0.65, b= -2.3, α =-32.92, β=17 and γ = -1.6).

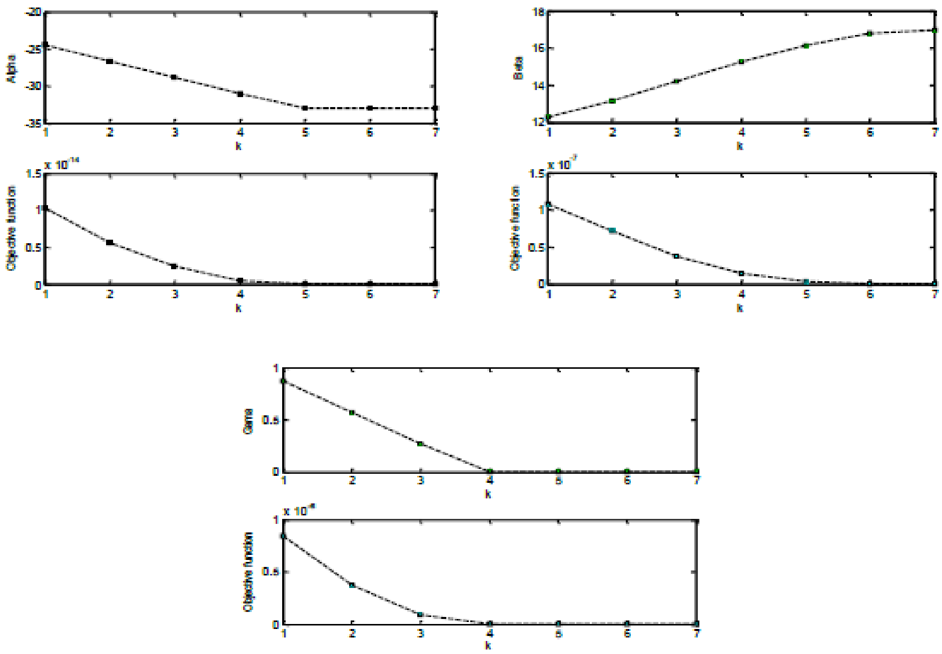

Figure 4 : Identification of α, β and γ

The synchronization process can be considered as a particular type of a control problem, in which the control objective is to keep the desired chaotic trajectory [22]. Original information generally based on the synchronization of transmitter receiver states. .Were: $\dot{x} = f1(x,u)$ and $\dot{\hat{x}} = f2(\hat{x},u)$

Because of the sensitivity to initial conditions of the chaotic signals, the both oscillators in the transmitter and the receiver will never have their identical states in any value of time. The principal process of synchronization is given by the following expression:

$$e = |\hat{x}(t) - x(t)| \rightarrow 0 \text{ if } t \rightarrow \infty \quad (9)$$

To test the synchronization of a secure chaos communication, we used the information signal shown in the following figure.

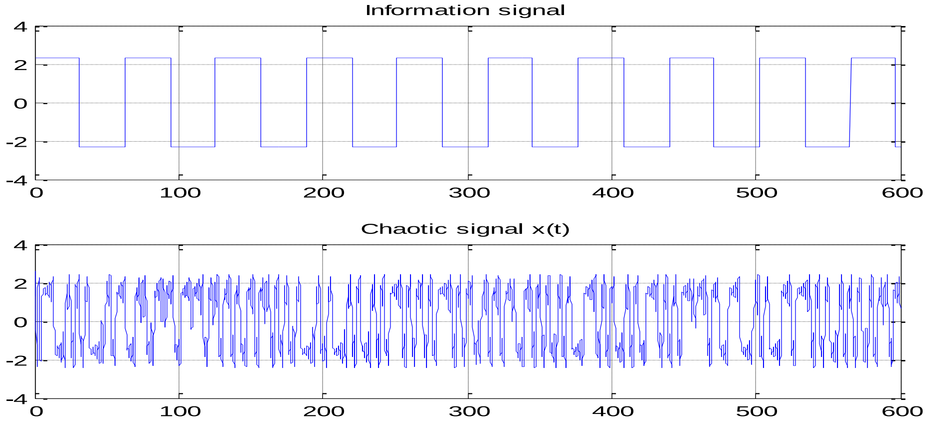

Figure 5 : Information signal and chaotic signal

In figure 6 we show the encrypted information signal and the received signal after decryption procedure without synchronization, the information signal is embedded in the chaotic signal.

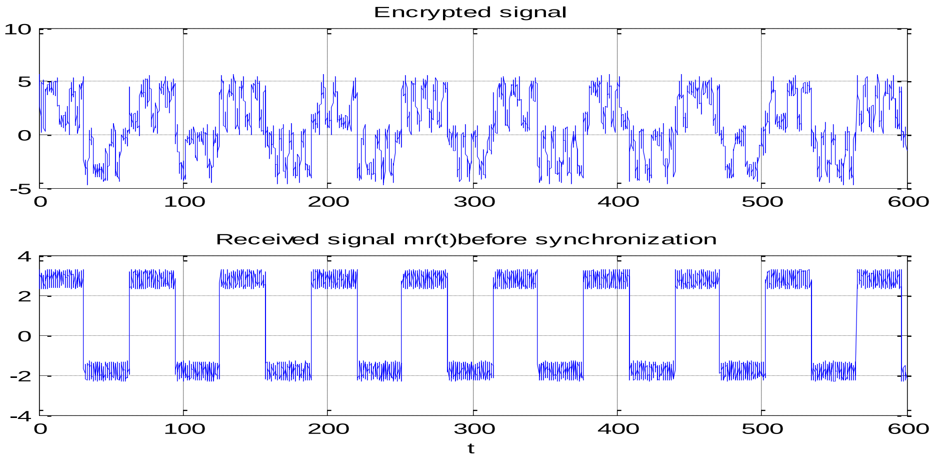

Figure 6 : Encrypted signal and received signal before synchronization

The encryption procedure is applied before information signal transmission. To decrypt the original information, it is necessary to know the characteristics of the chaotic signal. The extraction of the information signal given after the synchronization of chaotic signals process.

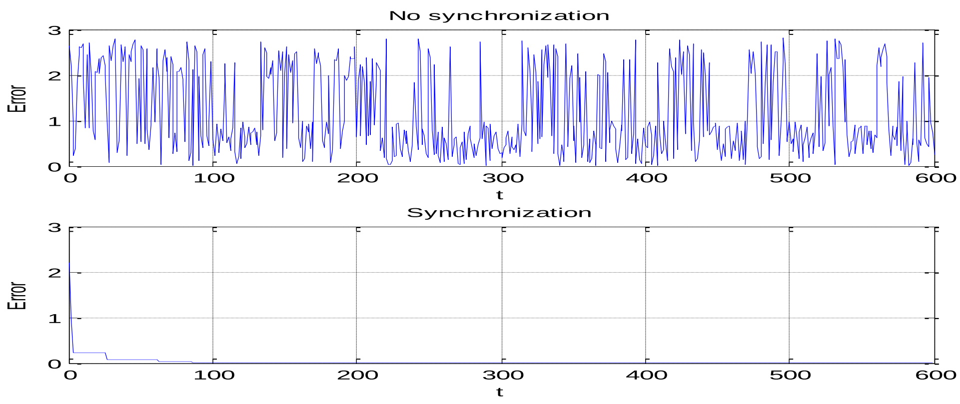

Figure 7 : Error before and after synchronization

In reception, the error between the original signal and the received signal is given by the following figures. The first one is in the case where there is no synchronization and in the second the two signals are synchronized.

PeSOA meta-heuristic algorithm identifies control parameters of Chua's chaotic system and gives symmetric key. So, the chaotic signal is synchronized and information signal hasbeen successfully encrypted.

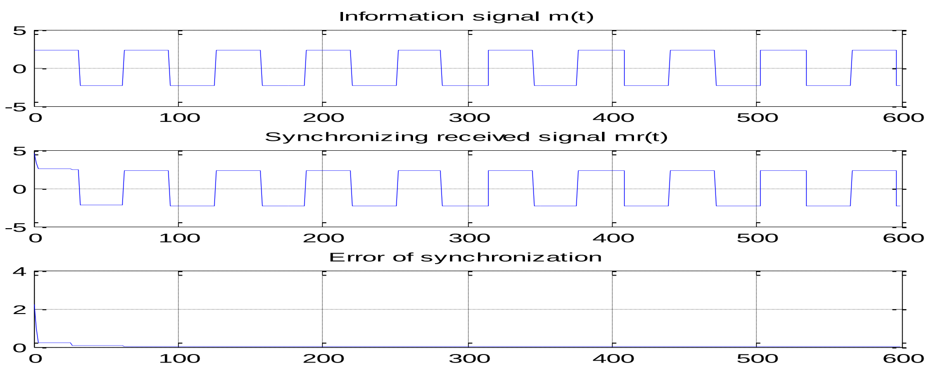

Figure 8 : Error of synchronization

As shown in Figure 8, the comparison of the original signal m(t) and synchronizing signal mr(t) is illustrated . We notice that the both trajectories achieve a common dynamical behavior after a period of transient and error signal tends towards zero.

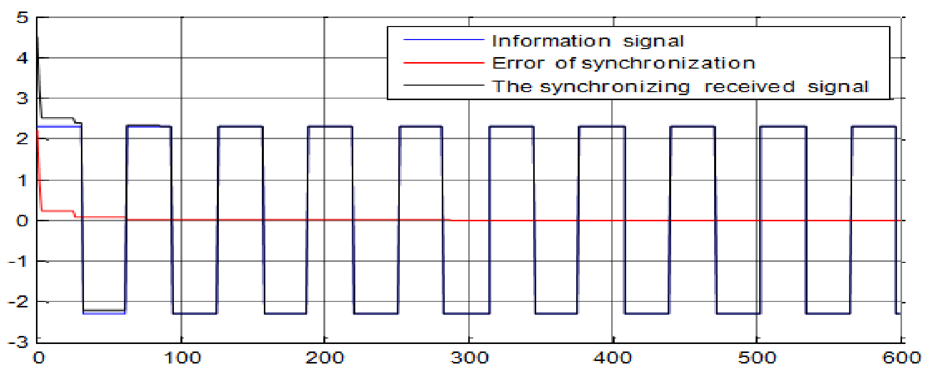

Figure 9 : Information signal, the synchrozing received signal and error of synchronization

Figure 9 shows that the synchronization between the original and received signals is perfectly carried out and the error signal tends towards zero. The convergence of the received signal to the original information signal is obtained by applying the PeSOA meta-heristic algorithm and after the encryption process.

Figure 10 illustrates the synchronization of transmitted and received signals after a transitory time of synchronizing process. The tests with the numerical simulations discussed show the effectiveness of the PeSOA algorithm for chaotic synchronization in secure communication problems.

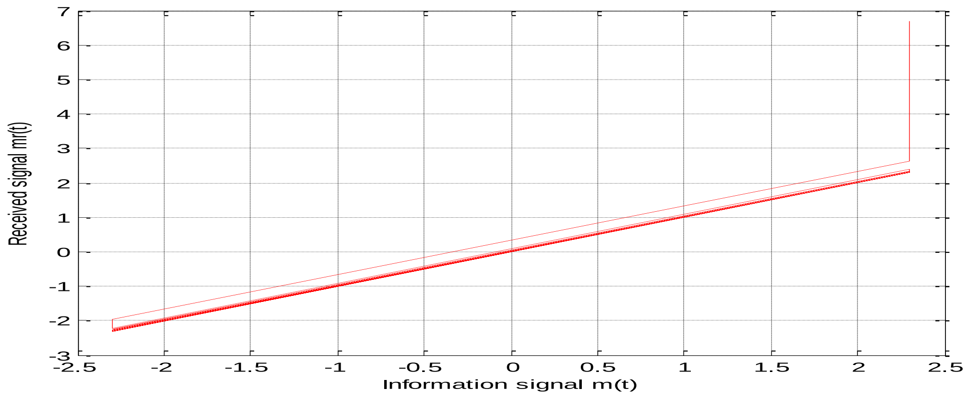

Figure 10 : Synchronization of transmitted and received signals

6 Conclusion

In this work a chaotic secure communication and synchronization scheme using meta-heuristic Penguins Search Optimization Algorithm is proposed. PeSOA algorithm has been applied in synchronization of two chaotic systems in order to seek out encryption secret key. We have used chua's circuit as a chaotic generator. A small perturbation in the initial conditions and in control parameters of the chaotic circuit can give a big difference in the system responses. The sensitivity to initial conditions is an important characteristic of a chaotic system. Synchronization between two chaotic systems forces the states of transmitted and received signals to converge. Chaos synchronization process has most applications in secure communication and other applications. Simulation using MATLAB presents numerical results and shows the effectiveness of the proposed approach. Future works will focus on the Synchronization behavior in the communication network and other practical system.

Références

[1] LM. Pecora, TL. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (8). 821–823. 1990.

[2] Xiao Xu, Truong N C, Sang-Do L & Sam-Sang Y. Secure communication system in maritime navigation using state observer with linear matrix inequality, Journal of International Maritime Safety, Environmental Affairs, and Shipping, 4:3, 70-75. 2020.

[3] Turgut, O. E. TURGUT, M ,ÇOBAN, M. Artificial Cooperative Search Algorithm for Parameter Identification of Chaotic Systems, Bitlis Eren Univ J Sci & Technol, 5(1), 11–17. 2015.

[4] Kanter, I. *et al*. Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography. *Opt. Express* **18,** 18292–18302. 2010.

[5] Zelinka, I. Evolutionary identification of hidden chaotic attractors.Inginering. Applications of Artificial Intelligence,; 50, 159-167. 2016

[6] Zhou L. and Tan F., "A chaotic secure communication scheme based on synchronization of double-layered and multiple complex networks," *NonlinearDynamics*, vol. 96, no. 2, 869–883, 2019.

[7] Deniz Eroglu, Jeroen Lambb and Tiago Pereira. Synchronization of Chaos. Department of Mathematics, Imperial College London, UK.2017.

[8] Dedieu H, Ogorzałek MJ. Identifiability and identification of chaotic systems based on adaptive synchronization. IEEE Trans Circuits Syst-1: Fundamental Theory Appl. 1997;44 (10):948–996.

[9] Pluhacek M, Senkerik R, Davendra D, et al. Designing PID controller for DC motor system by means of enhanced PSO algorithm with discrete chaotic Lozi map. Soft Computing Models in Industrial and Environmental Applications; 2012; 5th–7th September; Ostrava, Czech Republic.Springer, Berlin, Heidelberg; 2013; p. 475–483.

[10] Maamri F, Bououden S, Boulkaibet S. An ant colony optimization approach for parameter identification of piezoelectric resonator chaotic system. 16thIEEE International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA); 2015; Monastir, Tunisia; p. 811–816.

[11] Kaveh A. Mtaheuristic algorithms for optimal design of structures. Switzerland; Springer International Publishing; 2014.

[12] Peng, Y.; Sun, K.; He, S.; Peng, D. Parameter Identification of Fractional-Order Discrete Chaotic Systems. *Entropy* **2019**.

[13] Maamri F, Bououden S & Boulkaibet I : Identification of Chua's chaotic circuit parameters using penguins search optimisation algorithm, Cyber-Physical Systems. 2021.

[14] Maamri F, Bououden S, Chadli M, et al. The pachycondyla apicalis metaheuristic algorithm for parameters identification of chaotic electrical systems. Int J Parallel Emergent Distrib Syst.;33(5):490–502. 2018.

[15] Bououden S, Chadli M, Karimi M, An Ant colony optimization-based fuzzy predictive control approach for nonlinear processes information sciences. Elsevier.;299: 143– 158. 2015.

[16] Mzili, I., Riffi, M.E. Discrete Penguins Search Optimization Algorithm to Solve The Traveling Salesman Problem. Journal of Theoretical and Applied Information Technology, 72(3), 331-336. 2015

[17] Gheraibia, Y., Moussaoui, A. Penguins Search Optimization Algorithm (PeSOA), In Recent Trends in Applied Artificial Intelligence, Springer Berlin Heidelberg; 7906, 222-231. 2013.

[18] Youcef Gheraibia, Abdelouahab MOUSSAOUI, Youcef Djenouri, Sohag KABIR, Peng-Yeng Yin, Smaine Mazouzi. Penguin Search Optimisation Algorithm for Finding Optimal Spaced Seeds. International Journal of Software Science and Computational Intelligence (IJSSCI). 7(2):85-99.2015.

[19] Gheraibia Y, Moussaoui A, Yin P.Y, Papadopoulos Y, and Maazouzi S, PeSOA: Penguins Search Optimisation Algorithm for Global Optimisation Problems, The International Arab Journal of Information Technology, 16(3). 2019.

[20] Chua,L. O. Wu., C. W., Huang,A. Zhong, G.G. A universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos, IEEE Transaction On Circuits and Systems—I: Fundamental Theory And Applications, 40(10), 732-744.1993.

[21] Luigi F., and Mattia F, and Gabriella, Xibilia M. Chua's Circuit Implementations: Yesterday, Today And Tomorrow, World Scientific, V.65. 2009

[22] Lars Keuninckx et al, Encryption key distribution via chaos synchronization, ScientificREPOrTS. 2017.

[23] Turgut, O. E. TURGUT, M ,ÇOBAN, M. Artificial Cooperative Search Algorithm forParameter Identification of Chaotic Systems, Bitlis Eren Univ J Sci & Technol, 5(1), 11–17. 2015.