Engineering Applications of Artificial Intelligence 25 (2012) 766–774

Contents lists available at SciVerse ScienceDirect

Engineering Applications of Artificial Intelligence

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

Chaotic secure communication based on a gravitational search algorithm filter

XiaoHong Han, XiaoMing Chang *

College of Computer Science and Technology & College of Software, Taiyuan University of Technology, No. 79 Yingze West Street, Taiyuan 030024, Shanxi, PR China

ARTICLE INFO

Article history:
Received 24 January 2011
Received in revised form
21 November 2011
Accepted 18 January 2012
Available online 7 February 2012

Keywords:
Secure communication
Message estimation
Gravitational search algorithm
Chaos

ABSTRACT

A new chaotic secure communication scheme based on a gravitational search algorithm (GSA) filter is proposed. In this scheme, useful signals are delivered via an encoder, a chaotic transmitter, a GSA-based filter, a chaotic receiver, and a decoder. The security of such a communication system is promoted due to the unpredictable features of the chaotic map and the unknown encoding-modulation scheme. By using a GSA filter technique the resistance of the system to noise is enhanced. To verify the effectiveness of the proposed scheme, it is compared with the current state-of-the-art schemes in simulations. At the same time, comparisons with a genetic algorithm (GA) filter and a particle swarm optimization (PSO) filter are made. Numerical simulations confirm that the proposed method is better in estimating the states and information symbols, and has a lower bit error rate than other schemes.

1. Introduction

Chaos, which exists in many highly complex fields of nonlinear science, is a bounded deterministic dynamic behavior that exhibits sensitive dependence on initial conditions and includes infinite unstable periodic motions. Chaotic signals can be considered as the carriers of messages in secure communication applications. The idea of applying chaotic systems to secure communication has existed since Pecora and Carroll (1990) presented the concept of chaotic synchronization for two identical chaotic systems with different initial conditions in 1990. Hua et al. (2005) proposed a secure communication scheme based on a unified chaotic system. Chang (2009) proposed a method of improving the security of chaotic encryption. Lin et al. (2010) proposed a means of secure communication based on synchronized chaotic systems. In the fields of secure communication, many techniques and methods have been proposed to tackle the problem of chaotic secure communication, including chaotic masking (Chen and Liao, 2005; Milanovic and Zaghloul, 2002), chaotic switching (Yang et al., 2002), chaos shift keying (CSK) (Galias and Maggio, 2001; Tam et al., 2006; Mirasso et al., 2002), differential chaos shift keying (DCSK) (Fan and Zhang, 2009), chaotic frequency modulation (Tse et al., 2003), and anti-phase synchronization (lazejczyk-Okolewska et al., 2001; Ho et al., 2002). It should be noted that all the methods mentioned above do not consider channel noise, which is unavoidable in the transmission of a masked signal. One of the most important problems which limits the capability of secure communication systems based on chaos is the distortion of signals owing to noise, which results in the loss of the transmitted information (Li et al., 2005). As a consequence, secure communication in the presence of channel noise is becoming an important issue. Some experimental work has already been undertaken. Sun et al. (2008) proposed an adaptive chaotic secure communication scheme with channel noise. Zhang et al. (2006) considered the problem of chaotic secure communication using the particle filtering technique. Moskalenko et al. (2010) investigated, numerically, secure communication based on generalized synchronization in the presence of noise. Arman et al. presented a fractional chaotic communication method using an extended fractional Kalman filter (Kiani-B et al., 2009).

A further step in order to decrease noise in chaotic secure communication systems is the technique of digital filters, which are employed to keep frequency content in the desired band and to eliminate noise when the external input signal passes the filter. Adaptive digital filters are currently used in many areas, such as noise reduction, communication systems, image processing, system identification, signal processing (Su and Cai, 2009; Saha and Roy, 2009; Farouk and Smith, 2000). The main aim of the adaptation is to adjust the coefficients of the digital filter to estimate the parameters of an actual unknown system through its inputs and outputs. In this case, minimization of an objective function (generally the mean square error between desired signal and estimated filter output) is often followed by gradient-based iterative search algorithms.

However, when the objective function is non-smooth, gradient-based methods often cannot converge towards the global

* Corresponding author. Tel./fax: +086 13485325973.
E-mail address: jmqchs@sohu.com (X. Chang).

0952-1976/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.engappai.2012.01.014

minimum. In this situation, heuristic optimization methods, in which the gradient is not required, can achieve a global optimal solution and offer remarkable advantages in solving these difficult optimization problems. Many well-known global optimization methods, such as genetic algorithms (GA) (Tang et al., 1996), ant colony optimization (ACO) (Dorigo et al., 1996), and particle swarm optimization (PSO) (Kennedy and Eberhart, 1995) are widely employed to solve filter problems and system identification (Badr and Fahmy, 2004; van den Bergh and Engelbrecht, 2006; Ellabib et al., 2007).

Recently, a new heuristic search algorithm, the gravitational search algorithm (GSA), has been proposed, inspired by the gravitational law and the laws of motion (Rashedi et al., 2009). Its main characteristics include both easy implementation and computational efficiency. GSA has a well-balanced and flexible mechanism to improve exploration and exploitation abilities. Filter modeling using GSA is reported in Rashedi et al. (2011). In their work, GSA was proposed to model IIR filters and nonlinear rational filters. But the GSA-based filter modeling has not yet been applied to the problem of chaotic secure communication in the presence of noise.

In this work, GSA is employed to model a nonlinear rational filter, and then the nonlinear rational filter is applied to the problem of chaotic secure communication in the presence of noise. The effectiveness of the proposed secure communication scheme in the presence of noise in the communication channel is examined through comparisons between the proposed scheme and current state-of-the-art chaotic communication schemes. The main ideas of the proposed method are illustrated by unified chaotic maps. At the same time, different sets of initial population with the presence of noise are given and tested in simulations to verify the effectiveness of the GSA-based filter modeling. GA and PSO are also used to model the same examples, and some simulation results are compared.

The structure of the paper is organized as follows. In Section 2, a brief review of GSA is given to provide a proper background. This section is followed by a nonlinear filter modeling which estimates messages online, in Section 3. Section 4 is devoted to the description of the new chaotic secure communication scheme. Section 5 gives some numerical simulations to demonstrate the effectiveness of the scheme. Finally, the conclusions are given in Section 6.

2. Gravitational search algorithm (GSA)

GSA is one of the newest heuristic search algorithms, which mimics Newton's gravitational force laws (Rashedi et al., 2009). In Newton's gravitational law, each object draws each other object by a force called the "gravitational force" (Halliday et al., 1993). The performance of an object is evaluated by its mass.

The GSA algorithm is introduced as follows (Rashedi et al., 2009):

Consider a system with k objects. The position of the ith object is defined as Eq. (1):

$$X_i = (x_i^1, \ldots, x_i^d, \ldots, x_i^n),\ i = 1,2,\ldots,k, \tag{1}$$

where x_i^d denotes the position of ith object in the dth direction. The force exerting on the object i from the object j is defined as Eq. (2):

$$F_{ij}^d(t) = G\frac{M_i(t)\times M_j(t)}{R_{ij}(t)+\varepsilon}(x_j^d(t)-x_i^d(t)), \tag{2}$$

where M_j and M_i represent the gravitational mass of the object j and the object i, respectively, ε is a small constant, G is a gravitational constant, and $R_{ij}(t)$ is the Euclidian distance between the two objects i and j. The total force $F_i^d(t)$ exerting on the object i in the dth direction is calculated by a randomly weighted sum of the dth components of the forces from other objects:

$$F_i^d(t) = \sum_{j=1, j\neq i}^{k} \mathrm{rand}_j F_{ij}^d(t), \tag{3}$$

where rand_j is a random number from the interval [0,1].

The acceleration of the object i, $a_i^d(t)$, at time t and in the dth direction, is given as Eq. (4):

$$a_i^d(t) = \frac{F_i^d(t)}{M_{ii}(t)}, \tag{4}$$

where M_{ii} is the inertial mass of the object i. Its next velocity $v_i^d(t+1)$ and its next position $x_i^d(t+1)$ are calculated as Eqs. (5) and (6):

$$v_i^d(t+1) = \mathrm{rand}_i \times v_i^d(t) + a_i^d(t), \tag{5}$$

$$x_i^d(t+1) = x_i^d(t) + v_i^d(t), \tag{6}$$

where $v_i^d(t)$ and $x_i^d(t)$ are its current velocity and position, respectively.

The gravitational and inertia masses of the object are evaluated by the fitness function. Assuming the equality of the gravitational and inertia mass, the mass $M_i(t)$ is updated by Eqs. (8)–(11):

$$M_i = M_{ii}, i = 1,2,\ldots,k, \tag{7}$$

$$m_i(t) = \frac{\mathrm{fit}_i(t)-\mathrm{worst}(t)}{\mathrm{best}(t)-\mathrm{worst}(t)}, \tag{8}$$

$$M_i(t) = \frac{m_i(t)}{\sum_{j=1}^{k} m_j(t)}, \tag{9}$$

$$\mathrm{best}(t) = \min_{j\in\{1,\ldots,k\}} \mathrm{fit}_j(t), \tag{10}$$

$$\mathrm{worst}(t) = \max_{j\in\{1,\ldots,k\}} \mathrm{fit}_j(t), \tag{11}$$

where $\mathrm{fit}_i(t)$ represents the fitness value of the object i at time t. A larger mass indicates a more efficient object. This means that more efficient objects possess greater attractions and move more slowly. In this work, the fitness function is given as Eqs. (12) and (13):

$$\mathrm{fit}(t) = -\min(\mathrm{MSE}), \tag{12}$$

$$\mathrm{MSE} = \frac{1}{L}\sum_{t=1}^{L}(\hat{x}(t)-x(t))^2, \tag{13}$$

where $\hat{x}(t)$ is the estimated signal, $x(t)$ is the actual noisy signal, and L is the length of the input signal.

The main steps of the GSA algorithm are summarized as follows:

Step 1: Randomized initialization.
Step 2: Fitness evaluation of objects.
Step 3: Updating best(t), worst(t) and $M_i(t)$ for $i=1,2,\ldots,k$.
Step 4: Computation of the total force in different directions.
Step 5: Computation of acceleration and velocity.
Step 6: Updating objects' position.
Step 7: Repeat step 2 to step 6 until reaching the stop criteria.

3. Nonlinear filter modeling

When signals possess features such as impulse-like behavior, non-stationarity, and non-symmetry, linear filters designed by