Signal Processing 88 (2008) 2442–2452

Contents lists available at ScienceDirect

Signal Processing

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

Self-synchronizing chaotic stream ciphers

Ajeesh P. Kurian, Sadasivan Puthusserypady *

Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 5 November 2007
Received in revised form
4 April 2008
Accepted 10 April 2008
Available online 18 April 2008

Keywords:
Chaotic systems
Synchronization
Symbolic dynamics
Secure communication
Stream ciphers

ABSTRACT

Chaotic communication schemes aim to provide security over the conventional communication schemes. The sensitivity of chaotic systems/maps to their initial conditions and the parameters is used to introduce the security, where the latter is used as the secret key. The applicability of conventional chaotic systems/maps in communication channels with significant noise and multi-path is limited. Symbolic dynamics (SD) based methods have been shown to provide high quality synchronization (HQS). In this paper, a new digital chaotic communication scheme, which utilizes the SD based synchronization, is proposed. This is similar to a self-synchronizing stream cipher where synchronization information is provided periodically. For the proposed scheme, a theoretical expression for the upper bound of the bit error rate (BER) is derived. Numerical simulations are carried out to assess the BER performances of the system in AWGN and multi-path channels. Some security aspects of the proposed system are also studied.

1. Introduction

Noise like appearance and broadband spectrum of the time series generated by chaotic systems/maps have attracted the researchers' interest in applying such systems for secure communication applications [1]. The sensitivity of the chaotic systems/maps to their initial conditions and control parameters are exploited in chaos based cryptography [2]. Although, the security aspects of the chaotic communication systems are not fully understood [3], it is generally believed that these class of systems can be used in applications which do not require a high level of security [4].

Application of chaotic systems/maps in secure communication can be classified broadly into two. In the first class of systems, the analog chaotic signals, which have noise like appearance, are used as the carrier of information [5–7]. Thus, the encryption and modulation are done at the same time. With a synchronized chaotic system/map at the receiver, the information is decoded. Chaotic masking, chaotic shift keying (CSK) and chaotic parameter modulations are examples of such chaotic communication schemes. The second approach is to use discrete chaotic maps for the encryption of the information signal [8]. These types of communication systems can again be classified into two subclasses. The first subclass is the chaotic stream ciphers, where the binary chaotic sequences generated from chaotic symbolic dynamics (SD) is XORed with the information signal in order to encrypt as in a conventional stream cipher [9]. At the receiver, a synchronized chaotic map is used to generate the same encryption key and the received signal is XORed to decrypt the message. The second subclass refers to the block encryption schemes using iterated chaotic maps [2,8,10].

As can be clearly seen, the synchronization between the transmitter and the receiver is a requirement for successful decryption of message at the receiver. Following the seminal paper by Pecora and Carrol [11], researchers have come up with a multitude of approaches for the synchronization of chaotic systems/maps. For a comprehensive survey on this topic, the reader may refer [12] and the references therein. It has been shown that intervals of desynchronization bursts can appear in synchronization when noise is present in the system

* Corresponding author. Tel.: +65 6516 2262; fax: +65 6779 1103.
E-mail address: elespk@nus.edu.sg (S. Puthusserypady).

0165-1684/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2008.04.003

[13]. A high quality synchronization (HQS) is said to have achieved when the transmitter and the receiver synchronizes with an error below a certain threshold [14]. HQS is ideal for setting up a reliable secure communication.

SD is the coarse–grain description of the chaotic dynamics and has been used for the analysis of chaotic systems/maps [15]. In [16], HQS is achieved using the SD based methods. Reformulation of the SD based synchronization from an information theoretic point of view is detailed in [17]. Recently, SD is being proposed for secure communication applications [18–21]. In [18], chaotic communication using the feedback of SD is proposed. Application of SD for the differential chaotic shift keying (DCSK) scheme is discussed in [19]. SD based noise reduction and coding is proposed in [20,21].

Dynamical degradation[1] is one of the main concerns when a stream cipher is implemented on the digital computer [22]. In this paper, a new self-synchronizing chaotic stream cipher is proposed using the SD based synchronization. In the proposed system, the synchronization information is provided periodically. The theoretical and numerical bit error rate (BER) performances for the new system are obtained. These results are compared with those of the binary phase shift keying (BPSK) and the CSK systems. Statistical tests are conducted to asses the security aspects of the proposed system. These test results show that the proposed system has good statistical properties to qualify as a random bit generator which in turn emphasizes the system security. The system's sensitivity to the changes in parameters is also studied.

This paper is organized as follows. A brief overview of SD and synchronization of chaotic maps using SD is given in Section 2. In Section 3, the proposed communication scheme is explained in detail. A theoretical expression for the upper bound of the BER is derived in this section. Numerical results are discussed in Section 4 and the paper is concluded with some remarks in Section 5.

2. Symbolic dynamics

SD is the coarse–grain description of the actual system dynamics [15]. It is being widely applied for the analysis of chaotic systems/maps. By partitioning a chaotic state-space to arbitrary regions, and labeling each region with a specific symbol, the trajectories can be translated to a sequence of symbols. This coarse–grain formulation of the system makes the deterministic nature of the dynamical system to a stochastic one. Hence such systems can be treated as Markov systems which have finite topological entropies.

Let the state-space ($\mathscr{S}$) of the iterated chaotic map[2] be partitioned to m disjoint regions, $\beta = \{\mathscr{C}\}_{i=1}^{m}$, such that $\mathscr{C}_i \cap \mathscr{C}_j = \emptyset$ for $i \neq j$ and $\cup_{i=1}^{m} \mathscr{C}_i = \mathscr{S}$. If one can assign a letter each to each of the disjoint regions, the dynamics of the system can be represented by a sequence of finite alphabet $\mathbf{X} = [X_1, \ldots, X_m]$. This sequence is called the SD of the system/map. The entropy of the new information source is given by

$$H_n^{\beta} = -\sum_{\mathbf{Y}_n} P(\mathbf{Y}_n^i) \log P(\mathbf{Y}_n^i), \tag{1}$$

where $P(\mathbf{Y}_n^i)$ is the probability to find a code word $\mathbf{Y}_n^i$ of length n. The superscript i in Eq. (1) represents a specific combination of symbolic sequence. The summation is taken over all such possible sequences. The source entropy of a dynamical system is

$$h^{\beta} = \lim_{n\to\infty} h_n^{\beta} = \lim_{n\to\infty} \frac{1}{n} H_n^{\beta}. \tag{2}$$

The Kolmogorov–Sinai entropy of the system is defined as

$$h_{\mathrm{KS}} = \sup_{\beta} h^{\beta}. \tag{3}$$

From the above discussions, it is clear that an iterated chaotic map is an information source with entropy h_{KS}. In the next subsections, the SD of two chaotic maps used for this study, namely the tent map and logistic map, are defined.

2.1. SD of the tent map

Tent map is a special case of *skewed tent map*. It is a piecewise linear 1-D map. The dynamics of the skewed tent map is given in [20],

$$x_{k+1} = \begin{cases} \dfrac{x_k}{A}, & 0 < x_k \leqslant A, \\ \dfrac{1 - x_k}{A}, & A \leqslant x_k < 1, \end{cases} \tag{4}$$

where A $(0 < A < 1)$ is the parameter which controls the skewness of the tent map. The case $A = 0.5$ is the normal tent map and the corresponding phase-space representation is shown in Fig. 1. Binary partition (i.e., assigning 0 or 1 to regions of x_k) for generating SD is also shown in Fig. 1. Here, symbol '0' is assigned if $0 < x_k \leqslant A$ and '1' is assigned if $A < x_k < 1$. In this way, the binary sequence for the entire trajectory can be obtained.

2.2. SD of the logistic map

Logistic map [23] is one of the most widely studied 1-D maps; the dynamics of which is governed by

$$x_{k+1} = \mu x_k (1 - x_k), \tag{5}$$

where μ is a constant. For a range of values of μ, logistic map has chaotic dynamics. The dynamics of logistic map is defined in $(0, 1)$. For $\mu = 4$, the SD of the map is given in Fig. 2. Symbol 0 is assigned to the region $0 < x_k \leqslant 0.5$ and 1 is assigned to the region $0.5 < x_k < 1$.

2.3. Synchronization using SD

Using the tent map with binary partition, the SD based synchronization is explained in [17]. Consider the chaotic map described by Eq. (4). Assume that there are no messages transmitted and there is no channel noise. For an initial condition x_0, let $\mathscr{X} = [x_0, \ldots, x_{m-1}]$ be the fiducial

[1] When chaotic maps are implemented in digital computers, eventually all the trajectories become periodic due to the finite precision computations.

[2] For chaotic systems, corresponding discrete-time map can be obtained by constructing the Poincare return map.